

Integrated Dell Remote Access Controller 9

Attribute Registry

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: Introduction.....	4
New features added.....	4
Firmware version 7.10.50.00.....	4
Firmware version 7.10.30.00.....	4
Firmware version 7.00.60.00.....	5
Firmware version 7.00.30.00.....	5
Firmware version 7.00.00.00.....	5
Chapter 2: BIOS Attributes.....	6
Chapter 3: FC Attributes.....	346
Chapter 4: IDRAC Attributes.....	365
Chapter 5: InfiniBand Attributes.....	620
Chapter 6: LIFECYCLE Attributes.....	643
Chapter 7: NIC Attributes.....	652
Chapter 8: STORAGE Attributes.....	726
Chapter 9: SYSTEM Attributes.....	752

Introduction

This document provides information about the manageable attributes of iDRAC and its other components like BIOS, FC, NIC, Storage, InfiniBand, System, and Lifecycle Controller.

-  **NOTE:** All string values are limited to displayable ASCII characters, except where otherwise noted.
-  **NOTE:** Attribute information can also be accessed through the RACADM interface by running the Help command or through Redfish interface by running GET on redfish/v1/Registries.
-  **NOTE:** To access information on iDRAC attributes, visit <https://qrl.dell.com>, navigate to "Look Up," select "iDRAC Attributes," choose the appropriate attribute group, enter the attribute name, and select the attribute from the suggested list for quick access to relevant details.
-  **NOTE:** If an attribute is not present in the Attribute Registry guide, you can refer to Redfish([redfish/v1/Registries](https://redfish.dell.com/docs/v1/Registries)) to get the information.

Topics:

- [New features added](#)

New features added

-  **NOTE:** For details about the previous releases, if applicable, or to determine the most recent release for your platform, and for latest documentation version, see KB article 00178115 available at [Integrated Dell Remote Access Controller 9 Versions and Release Notes](#)

This section provides the list of new features added in the following releases:

- [Firmware version 7.10.50.00](#)
- [Firmware version 7.10.30.00](#)
- [Firmware version 7.00.60.00](#)
- [Firmware version 7.00.30.00](#)
- [Firmware version 7.00.00.00](#)

Firmware version 7.10.50.00

Following attributes were added in this release:

- Added support for BIOS.BootSettings.InteractiveMode attribute.
- Added support for BIOS.IntegratedDevices.NicAcpi attribute.
- Added support for BIOS.SysSecurity.MemoryEncryption attribute.
- Added support for iDRAC.PLDMConfiguration.PLDMLogRetrieval attribute.

Firmware version 7.10.30.00

Following attributes were added in this release:

- Added support for iDRAC.PlatformCapability.SharedStorageCapable attribute.
- Added support for BIOS.NetworkSettings.NvmeofEnDis attribute.
- Added support for BIOS.ProcSettings.ProcAvxP1 attribute.

Firmware version 7.00.60.00

Following features were added in this release:

- Added support for `iDRAC.SCV.CertificateVersion` attribute.
- Added support for `BIOS.MemSettings.PPRonUCE` attribute.
- Added support for `BIOS.SysSecurity.InFieldScan` attribute.

Firmware version 7.00.30.00

Following features were added in this release:

- Added support for `iDRAC.Logging.LCDuplicateEventEnable` attribute.
- Added support for `BIOS.ProcSettings.CpuAcpiCstC2Latency` attribute.
- Added support for `BIOS.ProcSettings.OptimizerMode` attribute.
- Added support for `BIOS.SysProfileSettings.CustomUncoreFrequency` attribute.
- Added support for `BIOS.SysProfileSettings.ProcessorApsRocketing` attribute.
- Added support for `BIOS.SysProfileSettings.ProcessorScalability` attribute.
- Added support for `BIOS.SysSecurity.StrongPassword` attribute.
- Added support for `BIOS.SysSecurity.StrongPasswordMinLength` attribute.

Firmware version 7.00.00.00

Following features were added in this release:

- Added support for `iDRAC.ACME.CA-URL` attribute.
- Added support for `iDRAC.ACME.Enable` attribute.
- Added support for `iDRAC.ACME.EnrollmentAction` attribute.
- Added support for `iDRAC.ACME.EnrollmentStatus` attribute.
- Added support for `iDRAC.ActiveDirectory.Connection` attribute.
- Added support for `iDRAC.LDAP.Connection` attribute.
- Added support for `iDRAC.SmartCard.CertificateValidation` attribute.
- Added support for `iDRAC.SmartCard.SmartCardOCSPEnable` attribute.

BIOS Attributes

BIOS.BiosBootSettings.BiosBootSeq

Description	This field tells the system where to find the operating system files needed for system startup. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeq

Description	This field tells the system where to find the operating system files needed for system startup. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis1

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis10

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis11

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis12

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis13

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis14

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis15

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis16

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis17

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis18

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis19

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis2

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis20

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis3

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis4

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis5

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis6

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis7

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis8

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BiosBootSettings.BootSeqEnDis9

Description	This field enables or disables this boot option in the Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.BootMode

Description	Determines whether the BIOS attempts to boot the OS via the method defined by the Unified Extensible Firmware Interface (UEFI) specification or via the legacy (BIOS) method. Selecting BIOS ensures compatibility with older operating systems that do not support the UEFI method. Many newer operating systems are UEFI-aware, and some of them may also support legacy boot methods.
Legal Values	• Bios • Uefi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.BootSeqRetry

Description	This field enables or disables the Boot Sequence Retry feature or resets the system. If the last attempt to boot has failed, the system immediately performs a cold reset or retries to boot after a 30 second time-out period, depending on if this field is set to Reset or Enabled.
Legal Values	• Enabled • Disabled • Reset
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.GenericUsbBoot

Description	When set to Enabled, a Generic USB Boot placeholder will be placed in the UEFI Boot Sequence, which will map to the first bootable USB device in the boot sequence. This allows the entry to remain present even if the USB device is not present. This is only available in UEFI Boot Mode.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.HddFailover

Description	When Boot Mode is BIOS, this field specifies the devices in the Hard-Disk Drive Sequence menu the BIOS will attempt to boot. This field has no effect when Boot Mode is UEFI. When set to Disabled, the BIOS will only attempt to boot the first Hard-Disk device in the list. When set to Enabled, the BIOS will attempt to boot each Hard-Disk device in order until it is successful or the entire Hard-Disk Drive Sequence has been attempted.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.HddPlaceholder

Description	When set to Enabled, a Generic RAID HDD placeholder will be placed into the UEFI Boot Sequence. The entry will remain present until an operating system or a bootable file is installed on the RAID disk. This setting is only available in UEFI Boot Mode.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.HddSeq

Description	This field specifies the order in which hard-disk drives will be configured in the system. The first hard drive in the system will be the bootable C: drive in DOS/DOS-like operating systems. This field applies only when Boot Mode is BIOS; it has no effect when Boot Mode is UEFI.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.InteractiveMode

Description	When set to Enabled, if the current boot option returns with a success (zero) status, the BIOS will stop processing further boot options and present the boot manager menu to the user. When set to Disabled, if the current boot option returns with a success (zero) status, the BIOS will proceed to the next boot option. This setting is only available in UEFI boot mode. This setting does not affect the behavior when the current boot option returns with a failed (non-zero) status; in that case, BIOS will always proceed to the next boot option.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.BootSettings.SetBootOrderDis

Description	The SetBootOrderDis fields specify a list of Fqdds representing the boot option. Disabled to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderEn

Description	The SetBootOrderEnDis fields specify a list of Fqdds representing the boot option. Enable to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd1

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd10

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd11

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd12

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd13

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd14

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd15

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd16

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd2

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd3

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd4

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd5

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd6

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd7

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd8

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetBootOrderFqdd9

Description	The SetBootOrderFqdd fields specify a list of Fqdds representing the boot list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd1

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd10

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd11

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd12

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd13

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd14

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd15

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd16

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd2

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd3

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd4

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd5

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd6

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd7

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd8

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SetLegacyHddOrderFqdd9

Description	The SetLegacyHddOrderFqdd fields specify a list of Fqdds representing the Legacy HDD list to be applied on the next boot.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.BootSettings.SysPrepClean

Description	When set to None, BIOS will do nothing. When set to Yes, BIOS will delete variables of SysPrep #### and SysPrepOrder on next booting. This option is onetime option, will reset to none when delete variables. This setting is only available in UEFI Boot Mode.
Legal Values	• None • Yes
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.EmbServerMgmt.FrontLcd

Description	This field allows you to select whether to display the Default (Model name and number) or a user-defined string in the front-panel LCD display. To modify the advanced features of the front-panel LCD, press F2 during boot to enter System Setup and then select iDRAC Settings.
Legal Values	• None • UserDefined • ModelNum • Advanced
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.EmbServerMgmt.UserLcdStr

Description	This field allows you to view/enter the User-Defined String to be displayed on the LCD. The string can be 62 characters long.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1DhcpEnDis

Description	DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Dns1

Description	Primary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Dns2

Description	Secondary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Gateway

Description	Gateway for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Interface

Description	NIC interface used for this HTTP device
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Ip

Description	IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Ipv6Address

Description	IPv6 Unicast address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Ipv6DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Mask

Description	Subnet mask for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Protocol

Description	Determines whether Internet Protocol version 4 (the most common, older version) or Internet Protocol version 6 (the newest version) is used for this device.
Legal Values	• IPv4 • IPv6
Default Value	IPv4
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1VlanEnDis

Description	Set this field to Enabled if your DNS or HTTP servers reside on a Virtual LAN (VLAN).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1VlanId

Description	When VLAN is enabled, identifies which of the 4094 possible VLANs contains the desired DNS or HTTP servers. This value can be from 1 to 4094 inclusive.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1VlanPriority

Description	When VLAN is enabled, identifies which of 8 possible priorities are assigned to the VLAN having the given ID. This value can be from 0 to 7 inclusive.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1v6AutoConfig

Description	IPv6 Auto Configuration Enabled/Disabled for this HTTP Device. Enabled : IPv6 address and Gateway will be assigned by DHCPv6 server dynamically. Disabled : IPv6 address and Gateway need to be assigned by user statically.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1v6Dns1

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1v6Dns2

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1v6Gateway

Description	Gateway for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1v6PrefixLen

Description	IPv6 Prefix Length (0~128) for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1Settings.HttpDev1v6Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev1TlsConfig.HttpDev1TlsMode

Description	This field is to set the authentication mode for this HTTP device.
Legal Values	• None • OneWay
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	bios.networkSettings.HttpDev1EnDis
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2DhcpEnDis

Description	DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Dns1

Description	Primary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Dns2

Description	Secondary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Gateway

Description	Gateway for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Interface

Description	NIC interface for this HTTP device
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Ip

Description	IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Ipv6Address

Description	IPv6 Unicast address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Ipv6DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Mask

Description	Subnet mask for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Protocol

Description	Determines whether Internet Protocol version 4 (the most common, older version) or Internet Protocol version 6 (the newest version) is used for this device.
Legal Values	• IPv4 • IPv6
Default Value	IPv4
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2VlanEnDis

Description	Set this field to Enabled if your DNS or HTTP servers reside on a Virtual LAN (VLAN).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2VlanId

Description	When VLAN is enabled, identifies which of the 4094 possible VLANs contains the desired DNS or HTTP servers. This value can be from 1 to 4094 inclusive.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2VlanPriority

Description	When VLAN is enabled, identifies which of 8 possible priorities are assigned to the VLAN having the given ID. This value can be from 0 to 7 inclusive.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2v6AutoConfig

Description	IPv6 Auto Configuration Enabled/Disabled for this HTTP Device. Enabled : IPv6 address and Gateway will be assigned by DHCPv6 server dynamically. Disabled : IPv6 address and Gateway need to be assigned by user statically.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2v6Dns1

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2v6Dns2

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2v6Gateway

Description	Gateway for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2v6PrefixLen

Description	IPv6 Prefix Length (0~128) for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2Settings.HttpDev2v6Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev2TlsConfig.HttpDev2TlsMode

Description	This field is to set the authentication mode for this HTTP device.
Legal Values	• None • OneWay
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	bios.networkSettings.HttpDev2EnDis
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3DhcpEnDis

Description	DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Dns1

Description	Primary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Dns2

Description	Secondary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Gateway

Description	Gateway for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Interface

Description	NIC interface for this HTTP device
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Ip

Description	IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Ipv6Address

Description	IPv6 Unicast address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Ipv6DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Mask

Description	Subnet mask for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Protocol

Description	Determines whether Internet Protocol version 4 (the most common, older version) or Internet Protocol version 6 (the newest version) is used for this device.
Legal Values	• IPv4 • IPv6
Default Value	IPv4
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3VlanEnDis

Description	Set this field to Enabled if your DNS or HTTP servers reside on a Virtual LAN (VLAN).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3VlanId

Description	When VLAN is enabled, identifies which of the 4094 possible VLANs contains the desired DNS or HTTP servers. This value can be from 1 to 4094 inclusive.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3VlanPriority

Description	When VLAN is enabled, identifies which of 8 possible priorities are assigned to the VLAN having the given ID. This value can be from 0 to 7 inclusive.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3v6AutoConfig

Description	IPv6 Auto Configuration Enabled/Disabled for this HTTP Device. Enabled : IPv6 address and Gateway will be assigned by DHCPv6 server dynamically. Disabled : IPv6 address and Gateway need to be assigned by user statically.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3v6Dns1

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3v6Dns2

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3v6Gateway

Description	Gateway for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3v6PrefixLen

Description	IPv6 Prefix Length (0~128) for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3Settings.HttpDev3v6Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev3TlsConfig.HttpDev3TlsMode

Description	This field is to set the authentication mode for this HTTP device.
Legal Values	• None • OneWay
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	bios.networkSettings.HttpDev3EnDis
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4DhcpEnDis

Description	DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Dns1

Description	Primary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Dns2

Description	Secondary DNS server IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device. When the protocol is set to IPv6, this field is forced to Enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Gateway

Description	Gateway for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Interface

Description	NIC interface for this HTTP device
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Ip

Description	IP address for this HTTP Device. When the protocol is set to IPv6, this field is configured automatically.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Ipv6Address

Description	IPv6 Unicast address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Ipv6DnsDhcpEnDis

Description	DNS information from DHCP Enable/Disable for this HTTP Device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Mask

Description	Subnet mask for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Protocol

Description	Determines whether Internet Protocol version 4 (the most common, older version) or Internet Protocol version 6 (the newest version) is used for this device.
Legal Values	• IPv4 • IPv6
Default Value	IPv4
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4Uri

Description	Contains the Uniform Resource Identifier (URI) that the BIOS should boot. If this field is blank, the BIOS will attempt to contact the networks DHCP server and ask it for the boot file name.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4VlanEnDis

Description	Set this field to Enabled if your DNS or HTTP servers reside on a Virtual LAN (VLAN).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4VlanId

Description	When VLAN is enabled, identifies which of the 4094 possible VLANs contains the desired DNS or HTTP servers. This value can be from 1 to 4094 inclusive.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4VlanPriority

Description	When VLAN is enabled, identifies which of 8 possible priorities are assigned to the VLAN having the given ID. This value can be from 0 to 7 inclusive.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4v6AutoConfig

Description	IPv6 Auto Configuration Enabled/Disabled for this HTTP Device. Enabled : IPv6 address and Gateway will be assigned by DHCPv6 server dynamically. Disabled : IPv6 address and Gateway need to be assigned by user statically.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4v6Dns1

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4v6Dns2

Description	DNS server IP address for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4v6Gateway

Description	Gateway for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4v6PrefixLen

Description	IPv6 Prefix Length (0~128) for this HTTP Device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4Settings.HttpDev4v6Uri

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.HttpDev4TlsConfig.HttpDev4TlsMode

Description	This field is to set the authentication mode for this HTTP device.
Legal Values	• None • OneWay
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	bios.networkSettings.HttpDev4EnDis
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.CurrentEmbVideoState

Description	Read-only. Indicates the current state of the Embedded Video Controller. If the Embedded Video Controller is the only display capability in the system (that is, no add-in graphics card is installed), then the Embedded Video Controller is automatically used as the primary display even if the Embedded Video Controller setting is Disabled.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic1

Description	Enables or disables the embedded NIC. NOTE: If set to Disabled (OS), the embedded NIC may still be available for shared network access by the embedded management controller. This function must be configured via the NIC management utilities provided with your system. There is only one onboard RJ45 port shared between BIOS and iDRAC. So it can only be enabled when iDRAC NIC selection is set to Shared. If the iDRAC setting is Dedicated, it will be grayed out and forced to Disabled.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic1Nic2

Description	Enables or disables the OS interface of the embedded NIC1 and NIC2 controller. NOTE: If set to Disabled (OS), the embedded NICs may still be available for shared network access by the embedded management controller. This function must be configured via the NIC management utilities provided with your system.
Legal Values	• Enabled • DisabledOs • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic1Nic2Nic3Nic4

Description	Enables or disables the OS interface of the embedded NIC1, NIC2, NIC3 and NIC4 controller. NOTE: If set to Disabled (OS), the embedded NICs may still be available for shared network access by the embedded management controller. This function must be configured via the NIC management utilities provided with your system.
Legal Values	• Enabled • DisabledOs • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic2

Description	No description information available.
Legal Values	• Enabled • EnabledPxe • EnablediScsi • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic3

Description	No description information available.
Legal Values	• Enabled • EnabledPxe • EnablediScsi • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic3Nic4

Description	Enables or disables the OS interface of the embedded NIC3 and NIC4 controller. NOTE: If set to Disabled (OS), the embedded NICs may still be available for shared network access by the embedded management controller. This function must be configured via the NIC management utilities provided with your system.
Legal Values	• Enabled • DisabledOs • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic4

Description	No description information available.
Legal Values	• Enabled • EnabledPxe • EnablediScsi • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic5Nic6Nic7Nic8

Description	Enables or disables the OS interface of the embedded NIC5, NIC6, NIC7 and NIC8 controller. NOTE: If set to Disabled (OS), the embedded NICs may still be available for shared network access by the embedded management controller. This function must be configured via the NIC management utilities provided with your system.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	- Embedded LOM1 with 4 ports with FQDD NIC.Embedded.1-* to NIC.Embedded.4-*. - Embedded LOM2 with 4 ports with FQDD NIC.Embedded.5-* to NIC.Embedded.8-*.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNic9Nic10Nic11Nic12

Description	Enables or disables the OS interface of the embedded NIC9, NIC10, NIC11 and NIC12 controller. NOTE: If set to Disabled (OS), the embedded NICs may still be available for shared network access by the embedded management controller. This function must be configured via the NIC management utilities provided with your system.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	- Embedded LOM1 with 4 ports with FQDD NIC.Embedded.1-* to NIC.Embedded.4-*. - Embedded LOM2 with 4 ports with FQDD NIC.Embedded.5-* to NIC.Embedded.8-*. - Embedded LOM3 with 4 ports with FQDD NIC.Embedded.9-* to NIC.Embedded.12-*.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNicPort1BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Embedded NIC port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNicPort2BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Embedded NIC port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNicPort3BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Embedded NIC port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbNicPort4BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Embedded NIC port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None

	• Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.EmbVideo

Description	Enables or disables the use of the Embedded Video Controller as the primary display. When set to Enabled, the Embedded Video Controller will be the primary display even if add-in graphics cards are installed. When set to Disabled, an add-in graphics card will be used as the primary display. BIOS will output displays to both the primary add-in video and the embedded video during POST and pre-boot environment. The embedded video will then be disabled right before the operating system boots. Note: When there are multiple add-in graphics cards installed in the system, the first card discovered during PCI enumeration is selected as the primary video. You may have to re-arrange the cards in the slots in order to control which card is the primary video controller.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.GlobalSlotDriverDisable

Description	If you set this field to Enabled, the BIOS will not load any legacy option ROMs (when Boot Mode is BIOS) or UEFI drivers (when Boot Mode is UEFI) for any cards in the system slots. If the boot support for some card is provided by the option ROM, then the system will not be able to boot from the card, nor will its pre-boot services be available. However, the card will be available for operating system use. If you do not want this behavior or you would like to limit which slots have this behavior, set this field to Disabled. Use the Slot Disablement setting to limit the slots having this behavior. This option does not apply to any slot containing a Dell RAID card.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic1Port1BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic1Port2BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic1Port3BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic1Port4BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic2Port1BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic2Port2BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read.

There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.

Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic2Port3BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntNic2Port4BootProto

Description	This is a Write-Only attribute to control the Legacy Boot Protocol of the LOM Port specified by the Integrated Network Card number and port number. This attribute is for system management software use, and does not appear in System BIOS Setup. This attribute always returns Unknown when read. There is no change to the LOM Port Legacy Boot Protocol setting when Unknown is written. An error is returned if written with a setting (None, PXE, or iSCSI) that is not supported by the LOM Port.
Legal Values	• Unknown • None • Pxe • Iscsi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntegratedNetwork1

Description	Enables or disables the integrated network card (NDC). When set to Disabled, the NDC is not available to the operating system (OS). NOTE: If set to Disabled (OS), the Integrated NICs may still be available for shared network access by iDRAC.
Legal Values	• DisabledOs • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntegratedNetwork2

Description	Enables or disables the second integrated network card (NDC). When set to Disabled, the NDC is not available to the operating system (OS). NOTE: If set to Disabled (OS), the Integrated NICs may still be available for shared network access by iDRAC.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntegratedRaid

Description	Enables or disables the integrated RAID controller. When set to Disabled, the device is not visible to the operating system (OS).
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.IntegratedSas

Description	Enables or disables the integrated SAS controller. When set to Disabled, the device is not visible to the operating system (OS).

Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalSdCard

Description	Enables or disables the internal SD Card port.
Legal Values	• On • Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalSdCardPresence

Description	Indicate the presence state of the Internal Dual SD module (IDSDM).
Legal Values	• None • SdCard1Only • SdCard2Only • Both
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalSdCardPrimaryCard

Description	When Redundancy is set to Disabled, either one of the SD card can be selected to present itself as mass storage device by setting it to be primary card. By default primary SD card is selected to be SD Card 1. If SD Card 1 is not present, then controller will select SD Card 2 to be primary SD card.
Legal Values	• SdCard1 • SdCard2
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalSdCardRedundancy

Description	Configures the redundancy mode of the Internal Dual SD module (IDSDM). When set to Mirror Mode, data is written to both SD cards. After failure of either card and replacement of the failed card, the data of the active card is copied to the offline card during the system boot. When Redundancy is set to disabled, only the primary SD Card is visible to the OS.
Legal Values	• Mirror • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalUsb

Description	Enables or disables the internal USB port.
Legal Values	• On • Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalUsb1

Description	Enables or disables the internal USB port 1.
Legal Values	• On • Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.InternalUsb2

Description	Enables or disables the internal USB port 2.
Legal Values	• On • Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.ioNonPostedPrefetch

Description	Controls the PCIe throughput by enabling or disabling the PCI IO non-posted prefetch mode. When set to Enabled, memory reads from PCI devices are optimized. However, performance may be reduced for writes from PCI devices.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.ioatEngine

Description	Enables or disables the I/O Acceleration Technology (I/OAT). I/OAT is a set of DMA features designed to accelerate network traffic and lower CPU utilization. This feature should be enabled only if the hardware and software support I/OAT.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.MemoryMappedIOH

Description	MMIO base default is 56TB. User should not change the default value unless addressing a known issue. When set to 12TB, the system will map MMIO base to 12TB. Enable this feature for an OS that requires

44bit PCIe addressing. When set to 512GB, the system will map MMIO base to 512GB, and reduce the maximum support for memory to less than 512GB. Enable this option only for the 4 GPU DGMA issue.

Legal Values	• 512GB • 12TB • 56TB
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.MmioAbove4Gb

Description	Enables support for PCIe devices that require large amount of MMIO resources. Enable this option only for 64-bit operating systems.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.MmioLimit

Description	When set to 1TB, the system will restrict maximum MMIO space to 1TB. Enable this feature for devices not support above 1TB addressing.
Legal Values	• 8TB • 1TB
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.Ndc1PcieLink1

Description	Enables or disables the integrated network card (NDC) PCIe link. When set to Disabled, the NDC link is not available to the operating system (OS). NOTE: If set to Disabled (OS), the Integrated NIC may still be available for shared network access by iDRAC.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This Attribute allows more granularity in controlling (Enabling/Disabling) NDC1 if present. This attribute is only displayed and used when NdcPcieLinkControl internal attribute default value is set to "Individual". This is most likely done in a PM (OEM ID).

BIOS.IntegratedDevices.Ndc1PcieLink2

Description	Enables or disables the integrated network card (NDC) PCIe link. When set to Disabled, the NDC link is not available to the operating system (OS). NOTE: If set to Disabled (OS), the Integrated NIC may still be available for shared network access by iDRAC.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This Attribute allows more granularity in controlling (Enabling/Disabling) NDC. This attribute is only displayed and used when NdcPcieLinkControl internal attribute default value is set to "Individual".This is most likely done in a PM (OEM ID).

BIOS.IntegratedDevices.Ndc1PcieLink3

Description	Enables or disables the integrated network card (NDC) PCIe link. When set to Disabled, the NDC link is not available to the operating system (OS). NOTE: If set to Disabled (OS), the Integrated NIC may still be available for shared network access by iDRAC.
Legal Values	• Enabled • DisabledOs
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This Attribute allows more granularity in controlling (Enabling/Disabling) NDC. This attribute is only displayed and used when NdcPcieLinkControl internal attribute default value is set to "Individual".This is most likely done in a PM (OEM ID).

BIOS.IntegratedDevices.NicAcpi

Description	"Enable/Disables NIC ACPI device name information. " "When set to Enabled, publish ACPI device name for NICs on PCIe slots. " "Warning: Changing this setting will cause the NIC name to change under Linux. "
Legal Values	String of ASCII characters.
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.OsWatchdogTimer

Description	If the system stops responding, this watchdog timer helps in the recovery of your operating system (OS). When set to Enabled, the OS is allowed to initialize the timer. When it is set to Disabled, the timer will have no effect on the system.
Legal Values	• Enabled • Disabled

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PCIRootDeviceUnhide

Description	If set to Enabled, root ports of all the empty slots will be accessible to the BIOS and OS.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PcieBusCustomization

Description	Common Help Text: Provide options for customizing the allocation of PCIe bus ranges to PCIe slots. This can be useful when connecting complex device sets to a slot. PCIe Bus System Allocation uses the normal rules of the system to allocate bus ranges. PCIe Bus Custom Allocation Option 1 increases the bus ranges allocated to the wider slots. PCIe Bus Custom Allocation Option 2 increases the bus range allocated to one of the wide slots more than with option 1. PCIe Bus Custom Allocation Option 3 allocates the largest bus range practical to one of the wide slots. Note that use of this option may cause insufficient resources to be available for remaining slots and prevent the system from functioning.
Legal Values	• PcieBusUniform • PcieBusCustomOpt1 • PcieBusCustomOpt2 • PcieBusCustomOpt3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available on R7920. Controlled by DPI feature: FeatureSupport.PcieBusCustomizable

BIOS.IntegratedDevices.PcieEnhancedPreferredIo

Description	When Enhanced Preferred IO is enabled the LCLK speed for the root complex where Preferred IO is enabled will automatically be set to 600 MHz (effective 593 MHz)
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PciePreferredIoBusVal

Description	This field sets the PCI bus address that preferred IO device resides. Bus address ranges from [0x0:0xFF].
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PciePreferredIoDevice

Description	In certain platform configurations it is possible to improve the performance of an endpoint by enabling Pcie Preferred IO Device. To select a particular addin device, references the PCI bus/device/function address(in decimal) of the add-in card when requesting Preferred I/O for the device
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PciePreferredIoDeviceBus

Description	This field sets the PCI bus address that preferred IO device resides. Bus address ranges from [0x0:0xFF].
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PciePreferredIoDeviceDev

Description	This field sets the PCI device address that preferred IO device resides. Device address ranges from [0x0:0x1F].
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.PciePreferredIoDeviceFun

Description	This field sets the PCI function address that preferred IO device resides. Function address ranges from [0x0:0x7].
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.RipsPresence

Description	Indicate the presence state of the RIPS (Redundant Internal Persistent Storage).
Legal Values	• RipsPresenceYes • RipsPresenceNo
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.SnoopHldOff

Description	Selects the number of cycles PCI I/O can withhold snoop requests, from the CPU, to allow time to complete its own write to LLC. This setting can help improve performance on workloads where throughput and latency are critical.
Legal Values	• Roll256Cycles • Roll512Cycles • Roll1KCycles • Roll2KCycles
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.SriovGlobalEnable

Description	Enables or disables the BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. Enable this feature if booting to a virtualization operating system that recognize SR-IOV devices.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.Usb3Setting

Description	Controls USB 3.0 support. When set to Disabled, BIOS disables USB 3.0 mode for all the USB3.0 ports. The USB devices operate at USB2.0 mode. When set to Enabled, BIOS operates all USB3.0 ports at USB2.0 mode during POST, and switches them to USB3.0 mode right after the operating system (OS) boots. You must select this option only if the operating system (such as. Windows Server 2012) has a native USB 3.0 driver. Otherwise none of the USB devices will work after boot. The Auto option is available only on workstation servers. If this option is selected, the BIOS leaves all USB 3.0 ports at USB 2.0 mode, and a special OS switching driver is required to set the USB3.0 port to USB3.0 mode. Microsoft Windows 7 has switching driver capability.
Legal Values	• Auto • Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.UsbEnableFrontPortsOnly

Description	This field enables/disables the front USB ports during the OS runtime when User Accessible USB Ports is set as All Ports Off (Dynamic).
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• Dynamic USB is only available on 600+ series servers and higher. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IntegratedDevices.UsbManagedPort

Description	The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. When set to OFF, iDRAC would not detect any USB devices installed in this managed port.
Legal Values	• On • Off
Default Value	On
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IntegratedDevices.UsbPorts

Description	All Ports On: All USB ports are enabled. Only Back Ports On: Disables the front USB ports. All Ports Off: Disables both front and back USB ports. All Ports Off (Dynamic): Disables both front and back USB ports but front ports can be enabled dynamically by an authorized user using Out-of-Band interfaces without resetting the system. Note using Out-of-Band interface to enable USB ports will be persistent setting and remain enabled in OS until the front ports setting is disabled in either BIOS setup or Out-of-Band interface. Note All Ports Off and All Ports Off (Dynamic) settings, all USB ports will still support USB keyboard and mouse during system boot process.
Legal Values	• AllOn • OnlyBackPortsOn • AllOff • AllOffDynamic
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Blades do not support setting the Attribute UsbPorts to the value OnlyBackPortsOn.
Notes	• Dynamic USB is only available on 600+ series servers and higher. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Auth

Description	Authentication type for this iSCSI connection.
Legal Values	• None • Chap
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1ChapName

Description	CHAP name for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1ChapSecret

Description	CHAP secret for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1ChapType

Description	CHAP type for this iSCSI connection.
Legal Values	• OneWay • Mutual
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1DhcpEnDis

Description	DHCP Enable/Disable for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Gateway

Description	Initiator Gateway for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Interface

Description	NIC interface used for this iSCSI connection
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Ip

Description	Initiator IP Address for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1IsId

Description	ISID for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Lun

Description	Target LUN for this iSCSI connection. The value format is a string containing a hexadecimal-encoded representation of the 64-bit SCSI Logical Unit Number in the format described in the T10 SCSI Architecture Model specification. This format consists of four 2-byte fields separated by dashes. In most cases, the human-oriented logical unit number will be in the high-order two bytes and the low-order six bytes will be zero. Examples are: 4752-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9 or 0.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Mask

Description	Initiator Subnet Mask for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Port

Description	Target Port for this iSCSI connection. The standard port number for iSCSI connections is 3260.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Protocol

Description	This field controls the Internet Protocol used for this iSCSI connection.
Legal Values	• IPv4 • IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Retry

Description	Retry Count for this iSCSI connection.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1RevChapName

Description	Reverse CHAP name for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1RevChapSecret

Description	Reverse CHAP secret for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1TargetIp

Description	Target IP Address for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1TargetName

Description	Target name for this iSCSI connection in IQN format.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1TgtDhcpEnDis

Description	Target DHCP Enable/Disable for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1Timeout

Description	Timeout for this iSCSI connection in milliseconds.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1VlanEnDis

Description	VLAN Enable/Disable for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1VlanId

Description	VLAN ID for this iSCSI connection.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con1Settings.IscsiDev1Con1VlanPriority

Description	VLAN priority for this iSCSI connection.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Auth

Description	Authentication type for this iSCSI connection.
Legal Values	• None • Chap
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2ChapName

Description	CHAP name for this iSCSI connection.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2ChapSecret

Description	CHAP secret for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2ChapType

Description	CHAP type for this iSCSI connection.
Legal Values	• OneWay • Mutual
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2DhcpEnDis

Description	DHCP Enable/Disable for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Gateway

Description	Initiator Gateway for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Interface

Description	NIC interface used for this iSCSI connection
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Ip

Description	Initiator IP Address for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Isid

Description	ISID for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Lun

Description	Target Lun for this iSCSI connection. The value format is a string containing a hexadecimal-encoded representation of the 64-bit SCSI Logical Unit Number in the format described in the T10 SCSI Architecture Model specification. This format consists of four 2-byte fields separated by dashes. In most cases, the human-oriented logical unit number will be in the high-order two bytes and the low-order six bytes will be zero. Examples are: 4752-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9 or 0.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Mask

Description	Initiator Subnet Mask for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Port

Description	Target Port for this iSCSI connection. The standard port number for iSCSI connections is 3260.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Protocol

Description	This field controls the Internet Protocol used for this iSCSI connection.
Legal Values	IPv4

	• IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Retry

Description	Retry Count for this iSCSI connection.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2RevChapName

Description	Reverse CHAP name for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2RevChapSecret

Description	Reverse CHAP secret for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2TargetIp

Description	Target IP Address for this iSCSI connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2TargetName

Description	Target name for this iSCSI connection in IQN format.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2TgtDhcpEnDis

Description	Target DHCP Enable/Disable for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2Timeout

Description	Timeout for this iSCSI connection in milliseconds.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2VlanEnDis

Description	VLAN Enable/Disable for this iSCSI connection.
Legal Values	• Enabled

	• Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2VlanId

Description	VLAN ID for this iSCSI connection.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDev1Con2Settings.IscsiDev1Con2VlanPriority

Description	VLAN priority for this iSCSI connection.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDevice1Settings.IscsiDev1Con1EnDis

Description	This field controls the configuration for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDevice1Settings.IscsiDev1Con2EnDis

Description	This field controls the configuration for this iSCSI connection.
Legal Values	• Enabled • Disabled
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.IscsiDevice1Settings.IscsiDev1ConOrder

Description	This field controls the order for which the iSCSI connections will be attempted.
Legal Values	• Con1Con2 • Con2Con1
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.IscsiDevice1Settings.IscsiF1F2ErrorPrompt

Description	This field determines whether the BIOS stops and displays a prompt when iSCSI connection errors occur during POST. The BIOS will display the prompt when this setting is Enabled; otherwise, the BIOS will continue through POST and attempt to boot an operating system. Note: This setting will be grayed out if F1/F2 Prompt on Error in the Miscellaneous Settings menu is Disabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.AdddcSetting

Description	When Adaptive Double DRAM Device Correction (ADDDC) is enabled, failing DRAMs are dynamically mapped out. This action can have some impact on system performance under certain workloads. This feature only applies to x4 DIMMs, and when Fault Resilient Mode (FRM) is disabled.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency that only x4 DIMMs be present or item is grayed out.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.AddrBasMir

Description	If the system is configured for Dell Fault Resilient Mode (FRM), controls the amount of memory for FRM per processor. The FRM memory is located on a single memory riser per processor. Only half of the FRM memory will be visible to the OS.
Legal Values	• AllMem • 64GB • HalfMem
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency where DIMM population within the system needs to support Mirror mode. Only System R6xx and up support this feature.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.AppDirectCapacity

Description	Total NVDIMM size configured as AppDirect mode in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.BankXor

Description	Enables Bank XORing to alleviate bank thrashing
Legal Values	• Enabled • Disabled •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.BatteryStatus

Description	Battery Status Present/Not Present/Ready/Not Ready.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.CECriticalSEL

Description	Enable/Disable logging of correctable memory threshold error.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity00

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity01

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity02

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity03

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity04

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity05

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity06

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity07

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity08

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity09

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity10

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity11

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity12

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity13

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity14

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity15

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity16

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity17

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity18

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity19

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity20

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity21

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity22

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.Capacity23

Description	The size of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.ClusterOnDie

Description	Enables or disables the Cluster on Die feature.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	Never released. Safe to remove?
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.CorrEccSmi

Description	Allows the system to log ECC corrected DRAM errors into the SEL log. Logging these rare errors can help identify marginal components; however the system will pause for a few milliseconds after an error while the log entry is created. Latency conscious customers may wish to disable the feature. Spare Mode, and Mirror mode require this feature to be enabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.CurrentMemOpModeState

Description	Read-only. Indicates the current state of the memory operating mode.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DarkMemoryAvailableMem

Description	No description information available.
Legal Values	• Disabled • DarkMemoryAvailable64 • DarkMemoryAvailable128 • DarkMemoryAvailable192 • DarkMemoryAvailable256 • DarkMemoryAvailable320 • DarkMemoryAvailable384 • DarkMemoryAvailable448 • DarkMemoryAvailable512 • DarkMemoryAvailable640 • DarkMemoryAvailable768
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator00

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator01

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator02

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator03

Description	The DIMM slot that this NVDIMM is being populated.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator04

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator05

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator06

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator07

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator08

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator09

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator10

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator11

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator12

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator13

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator14

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator15

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator16

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator17

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator18

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator19

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator20

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator21

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator22

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DeviceLocator23

Description	The DIMM slot that this NVDIMM is being populated.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot00

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot01

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot02

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot03

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot04

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot05

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.

Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot06

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot07

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot08

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot09

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot10

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot11

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot12

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled

	• Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot13

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot14

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot15

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot16

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot17

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot18

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot19

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot21

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot22

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot23

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot24

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot25

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot26

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot27

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot28

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot29

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot30

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DimmSlot31

Description	When set to Enabled, the DIMM slot is enabled. When set to Disabled, the DIMM slot is disabled.
Legal Values	• Enabled • Disabled
Default Value	"Enabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.DramRefreshDelay

Description	By enabling the CPU memory controller to delay running the REFRESH commands, you can improve the performance for some workloads. By minimizing the delay time, it is ensured that the memory controller runs the REFRESH command at regular intervals. However, this setting does not affect the Intel-based servers that are configured with DIMMs which use 16 Gb density DRAMs.
Legal Values	• Performance • Minimum
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FRMPercent

Description	Select to define the percent of total memory size that must be used by the fault resilient mode, when selected in the Memory Operating mode. When Fault Resilient Mode is not selected, this option is grayed out and not used by Fault Resilient Mode.
Legal Values	• 25 • 12.5
Default Value	25
Write Privilege	N/A
License Required	N/A
Dependency	This option is grayed out(read only) when "Fault Resilient Mode" is not selected in "Memory Operating Mode". This option is only available on Intel platforms.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion00

Description	The firmware revision of this NVDIMM.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion01

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion02

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion03

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion04

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion05

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion06

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion07

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion08

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion09

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion10

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion11

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion12

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion13

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion14

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion15

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion16

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion17

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion18

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion19

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion20

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion21

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion22

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.FirmwareVersion23

Description	The firmware revision of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.IntelPersistMemOperationTarget

Description	NVDIMM region creation target in per Platform or per Socket.
Legal Values	• PmPlatform • PmSocket
Default Value	PmPlatform
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MemSettings.LockState00

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState01

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState02

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState03

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState04

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState05

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState06

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState07

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState08

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState09

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState10

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState11

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState12

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState13

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState14

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState15

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState16

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState17

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState18

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState19

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState20

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState21

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState22

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.LockState23

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• Unknown • Disabled • Unlocked • Locked • Frozen • NotSupported
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MemLowPower

Description	Enables or disables the low-power mode of memory. When set to Disabled, the memory will run at full speed. When set to Enabled, the memory will run at a reduced speed to conserve power. Default: Disabled
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not used on 13G+.

BIOS.MemSettings.MemOpMode

Description	Allows the selection of the memory operating mode. Certain options are active only if a valid memory configuration is detected. When the Optimizer Mode is enabled, the DRAM controllers operate independently in 64-bit mode and provide optimized memory performance. When Advanced ECC Mode

is enabled, the two DRAM controllers are combined in 128-bit mode and provide optimized reliability. Memory that cannot be teamed by the controllers is not reported to the Operating System. When Mirror Mode is enabled, the system maintains two identical copies of data in the memory. This feature provides maximum reliability and enables the system to continue running even during a high severity memory failure. NOTE: In Mirror Mode, only half of the installed system memory is reported to the operating system. When Spare Mode is enabled, the BIOS reserves a rank of memory as a spare. At runtime, the memory controller can move a rank that exhibits a large number of correctable errors to the spare rank. NOTE: In Spare Mode, the system memory size reported to the Operating System does not include the spare portion. Spare with Advanced ECC Mode operates similarly to the Spare Mode. When this mode is enabled, the system runs under Advanced ECC mode with a spare rank reserved in each channel. NOTE: In Spare with Advanced ECC Mode, the system memory size reported to the Operating System does not include the spare portion. When Dell Fault Resilient Mode is enabled, the BIOS establishes an area of memory that is fault resilient. This mode can be used by an Operating System that supports the feature to load critical applications or enables the Operating System kernel to maximize system availability. Default: Optimizer Mode

Legal Values	• OptimizerMode • SingleRankSpareMode • MultiRankSpareMode • SpareMode • MirrorMode • AdvEccMode • SpareWithAdvEccMode • FaultResilientMode • NUMAFaultResilientMode
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	For FRM, need platform to support Mirror mode. For NUMA FRM, need to have 2 CPU installed + platform support Mirror mode. [MirrorMode, Lockstep] Needs identical memory configurations in channles behind each memory controller.

BIOS.MemSettings.MemOpVoltage

Description	No description information available.
Legal Values	• AutoVolt • Volt15V
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MemOptimizer

Description	When set to Disabled, the two DRAM controllers are combined in 128-bit mode and provide optimized reliability with Advanced ECC Mode. When set to Enabled, the two DRAM controllers operate independently in 64-bit mode and provide optimized performance without Advanced ECC Mode. Default: Disabled
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	Has a dependency on DIMM population where corresponding channels for each socket (Channel0 and Channel2, Channel1 and Channel 3) needs to be populated and populated identically. Not used on 13G+.

BIOS.MemSettings.MemTest

Description	Indicates whether or not the BIOS system memory tests are conducted during POST. When set to Enabled, memory tests are performed. NOTE: Enabling this feature will result in longer boot time. The extent of increased time depends on the size of the system memory.
Legal Values	• Enabled • Disabled • HardwareBasedTest
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MemTestType

Description	Indicates type of BIOS-based system memory test to perform during POST. When set to Hardware, the memory tests are performed via hardware. When set to Software, the memory tests are performed via software . Note: POST time will increase when memory test are enabled, with Software test taking longer than Hardware test.
Legal Values	• Hardware • Software
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Never released?

BIOS.MemSettings.MemThrottlingMode

Description	Displays MCDRAM thermal management/throttling modes of processor(s).
Legal Values	• Cltt • Oltt
Default Value	Cltt
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MemoryCapacity

Description	Total NVDIMM size configured as memory mode in the system.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MemoryInterleaving

Description	When set to Enabled, memory interleaving is supported if a symmetric memory configuration is installed. When set to Disabled, the system supports Non-Uniform Memory Access (NUMA) (asymmetric) memory configurations. Operating Systems that are NUMA-aware understand the distribution of memory in a particular system and can intelligently allocate memory in an optimal manner. Operating Systems that are not NUMA aware could allocate memory to a processor that is not local resulting in a loss of performance. Die and Socket Interleaving should only be enabled for Operating Systems that are not NUMA aware.
Legal Values	• Disabled • ChannelInterleaving • DiInterleaving • SocketInterleaving • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MemoryTraining

Description	Fast - Use previously saved memory training parameters to train the memory subsystem when memory configuration is not changed. System boot time is reduced when memory configurations is not changed. If memory configuration is changed, system automatically enables REFRAIN AT NEXT BOOT to force one-time full memory training steps, and then go back to FAST afterward. Retrain at Next Boot - Force one-time full memory training steps at next system power on. System boot time is slowed on next boot. Enable - Force full memory training steps on every system power on. System boot time is slowed on every boot.
Legal Values	• MemoryTrainingFast • MemoryTrainingOnce • MemoryTrainingEnable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.MltRnkSpr

Description	If the system is configured for Spare Mode or Spare With Advanced ECC Mode, this field controls the number of spare ranks per DDR channel. The default is one spare rank per DDR channel.
Legal Values	• 1 • 2 • 3 • Auto

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on DIMM population where within a channel, multi-rank DIMM needs to be populated Not used on 13G+.

BIOS.MemSettings.NGNFactoryResetClear

Description	Enable/Disable Factory Reset/Clear
Legal Values	- Disabled - Enabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NativeTrfcTiming

Description	Enables 16 Gb density DIMMs to operate at their programmed Row Refresh Cycle Time (tRFC). Enabling this feature may improve system performance for some memory configurations. However, enabling this feature will have no effect on configurations with 16 Gb 3DS/TSV DIMMs.
Legal Values	Enabled, Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NodeInterleave

Description	When set to Enabled, memory interleaving is supported if a symmetric memory configuration is installed. When set to Disabled, the system supports Non-Uniform Memory Access (NUMA) (asymmetric) memory configurations. Operating Systems that are NUMA-aware understand the distribution of memory in a particular system and can intelligently allocate memory in an optimal manner. Operating Systems that are not NUMA aware could allocate memory to a processor that is not local resulting in a loss of performance. Node Interleaving should only be enabled for Operating Systems that are not NUMA aware.
Legal Values	- Enabled - Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available if 2 or more CPUs are present.

BIOS.MemSettings.NvdimmFactoryDefault

Description	Reset all NVDIMM-Ns to their Factory Default state, and erase all NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault0

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault1

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault10

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault11

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault12

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault13

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault14

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault15

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault16

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault17

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault18

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault19

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault2

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault20

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault21

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault22

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault23

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault3

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault4

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault5

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault6

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault7

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmFactoryDefault8

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmmFactoryDefaultEnable • NvdimmmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFactoryDefault9

Description	Reset an NVDIMM-N to its Factory Default state, and erase the NVDIMM-N data. WARNING: All contents in NVDIMM-N will be lost if changes are saved when exiting BIOS!
Legal Values	• NvdimmFactoryDefaultEnable • NvdimmFactoryDefaultDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer0

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer1

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer10

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer11

Description	Indicates firmware version used in this NVDIMM-N.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer2

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer3

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer4

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer5

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer6

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer7

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer8

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFirmwareVer9

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq0

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq1

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq10

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq11

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq2

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq3

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq4

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq5

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq6

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq7

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq8

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmFreq9

Description	Indicates the clock frequency of NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmInterleaveSupport

Description	Enabling this setting interleaves NVDIMMs on a per-processor basis. When interleaving is enabled, Memory performance increases. However, if one NVDIMM fails, the data in all interleaved NVDIMMs is lost. When interleaving is disabled, if one NVDIMM fails, the data in other NVDIMMs remains intact.
Legal Values	• NvdimmInterleaveEnable • NvdimmInterleaveDisable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation0

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None

BIOS.MemSettings.NvdimmLocation1

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation10

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation11

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation2

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation3

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation4

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation5

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation6

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation7

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation8

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmLocation9

Description	Indicates the slot location of the NVDIMM-N. This location is printed right next to each DIMM slot on the main system board.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmReadOnly

Description	When set to enabled, NVDIMM-N is in write-protect mode.
Legal Values	• NvdimmReadOnlyEnable • NvdimmReadOnlyDisable:
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum0

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum1

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum10

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum11

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum2

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum3

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum4

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum5

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum6

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum7

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum8

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSerialNum9

Description	Indicates firmware version used in this NVDIMM-N.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize0

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize1

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize10

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize11

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize2

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize3

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmSize4

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmSize5

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmSize6

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmSize7

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmmSize8

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.NvdimmSize9

Description	Indicates the amount of NVDIMM-N in the DIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.OppSrefEn

Description	This field enables/disables opportunistic self-refresh feature.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PPROnUCE

Description	"Enable/Disable Post Package Repair(PPR) on Uncorrectable Memory Error."
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemPassphrase

Description	The Persistent Memory Passphrase unlocks secured Persistent Memory DIMMs. All Persistent Memory DIMMs are affected if the passphrase is modified. WARNING: Entering and confirming a blank passphrase disables passphrase security in all Persistent Memory DIMMs.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryMode

Description	When Select NVDIMM-N will enable NVDIMM-N Support. When select Off, all persistent memory access in OS will be disabled.
Legal Values	• NVDIMM • PersistentMemoryOff
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryScrubbing

Description	Set Persistent Memory Scrubbing mode. Auto: System automatically scrubs persistent memory during POST when multibit errors have been detected. One Shot: System will scrub persistent memory during POST on the entire persistent memory range once. Upon next boot, System will go back to AUTO persistent memory scrub mode. Enable: System will scrub persistent memory during POST on the entire persistent memory range on everyboot. Note: Scrubbing persistent memory on the entire persistent memory range could take more than 60 minutes during system POST depending on system memory population.
Legal Values	• Auto • OneShot • Enable
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryType

Description	Select the type of the persistent memory capacity to create.
Legal Values	• PmAppDirect • PmAppDirectNotInterleaved
Default Value	PmAppDirect
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryType0

Description	Persistent memory type
Legal Values	• AppDirect • AppDirectNotInterleaved
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryType1

Description	Persistent memory type
Legal Values	• AppDirect • AppDirectNotInterleaved
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryType2

Description	Persistent memory type
Legal Values	• AppDirect • AppDirectNotInterleaved
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PersistentMemoryType3

Description	Persistent memory type
Legal Values	• AppDirect • AppDirectNotInterleaved
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmCRQoS

Description	CR QoS tuning recipes. Recipe 1 - Enables tuning recipe 1 for CR QoS knobs (recommended for 2-2-2 memory configuration in AD) Recipe 2 - Enables tuning recipe 2 for CR QoS knobs (recommended for other memory configuration in AD) Recipe 3 - Enables tuning recipe 3 for CR QoS knobs (recommended for 1 DIMM per channel config)
Legal Values	• PmCRQoSRecipe1, PmCRQoSRecipe2, PmCRQoSRecipe3, Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A

Dependency Intel DCPMM

BIOS.MemSettings.PmControllerRevisionID00

Description No description information available.
Legal Values String of ASCII characters.
Default Value None
Write Privilege N/A
License Required N/A
Dependency [DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID01

Description No description information available.
Legal Values String of ASCII characters.
Default Value None
Write Privilege N/A
License Required N/A
Dependency [DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID02

Description No description information available.
Legal Values String of ASCII characters.
Default Value None
Write Privilege N/A
License Required N/A
Dependency [DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID03

Description No description information available.
Legal Values String of ASCII characters.
Default Value None
Write Privilege N/A
License Required N/A
Dependency [DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID04

Description No description information available.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID05

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID06

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID07

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmControllerRevisionID08

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID09

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID10

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID11

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID12

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID13

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID14

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID15

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID16

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID17

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID18

Description	No description information available.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID19

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID20

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID21

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID22

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmControllerRevisionID23

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmLockState00

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState01

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState02

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState03

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState04

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState05

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState06

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState07

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[DimmCapabilities==NVDIMM] [DimmCapabilities==AEP] [DimmCapabilities==PMEM]

BIOS.MemSettings.PmLockState08

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState09

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState10

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState11

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState12

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState13

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState14

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState15

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState16

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState17

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState18

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState19

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState20

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState21

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState22

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmLockState23

Description	The security state of this NVDIMM as unknown, disabled, unlocked, locked, frozen, max password, and not supported.
Legal Values	• PmLockStateUnknown • PmLockStateDisabled • PmLockStateUnlocked • PmLockStateLocked • PmLockStateFrozen • PmLockStateNotSupported • PmLockStateExceeded
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmMemoryMode

Description	Set the percentage of the total capacity to use in Memory Mode(0-100). Due to platform memory alignment requirements, the capacity will be aligned automatically.
Legal Values	• PmPercentNone • PmPercent0 • PmPercent5 • PmPercent10 • PmPercent15 • PmPercent20 • PmPercent25 • Percent30 • Percent35 • Percent40 • Percent45 • Percent50 • Percent55 • Percent60 • Percent65 • Percent70 • Percent75 • Percent80 • Percent85 • Percent90 • Percent95 • PmPercent100
Default Value	PmPercentNone
Write Privilege	N/A
License Required	N/A
Dependency	GEN>=16, then help text is as below: "Set the percentage of the total capacity to use in Memory Mode (0% to 100% with increment of 5%). " "Due to platform memory alignment requirements, this value will be aligned automatically. " "Note: when Persistent sets to 0%, 100% Memory Mode will be set automatically. When Persistent sets to 100%, " "Memory Mode will be set to 0%. When Persistent sets to X% (between 5% and 95%), Memory Mode will be set to (100-X)%."

BIOS.MemSettings.PmNVMPerformanceSetting

Description	NVM baseline performance settings depending on the workload behavior. BW Optimized - Optimized for DDR and DDRT Bandwidth. Latency Optimized - Better DDR latency in the presence. Balanced Profile - Optimized for Memory Mode.
Legal Values	• PmBWOptimized, PmLatencyOptimized, PmBalancedProfile
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmPersistentPercentage

Description	Reserve a percentage (0-100) of the requested AEP DIMM capacity that will be mapped into the system physical address space as Persistent Memory.
Legal Values	• PmPercentNone • PmPercent0 • Percent5 • Percent10 • Percent15 • Percent20 • Percent25 • Percent30 • Percent35 • Percent40 • Percent45 • Percent50 • Percent55 • Percent60 • Percent65 • Percent70 • Percent75 • Percent80 • Percent85 • Percent90 • Percent95 • PmPercent100
Default Value	PmPercentNone
Write Privilege	N/A
License Required	N/A
Dependency	if GEN>=16, then help text is as below: "Reserve a percentage (0% to 100% with increment of 5%) of the requested Intel Persistent Memory DCPMM capacity " "that will be mapped into the system physical address space as Persistent Memory. " "Due to platform memory alignment requirements, this value will be aligned automatically. " "Note: when Persistent sets to 0%, 100% Memory Mode will be set automatically. When Persistent sets to 100%, " "Memory Mode will be set to 0%. When Persistent sets to X% (between 5% and 95%), Mixed Mode will be set automatically."

BIOS.MemSettings.PmSecureEraseAll

Description	Secure Erase Intel Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PmSocket0

Description	NVDIMM pool creation for socket00
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	IntelPersistMemOperationTarget==Socket

BIOS.MemSettings.PmSocket1

Description	NVDIMM region creation for socket01
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	IntelPersistMemOperationTarget==Socket

BIOS.MemSettings.PmSocket2

Description	NVDIMM pool creation for socket02
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	IntelPersistMemOperationTarget==Socket

BIOS.MemSettings.PmSocket3

Description	NVDIMM pool creation for socket03
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	IntelPersistMemOperationTarget==Socket

BIOS.MemSettings.PoolCapacity0

Description	Pool Capacity
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolCapacity1

Description	Pool Capacity
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolCapacity2

Description	Pool Capacity
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolCapacity3

Description	Pool Capacity
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolID0

Description	Pool ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolID1

Description	Pool ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolID2

Description	Pool ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.PoolID3

Description	Pool ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.ProcEmbMemCacheSize

Description	Displays cache size of the MCDRAM
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.ProcEmbMemMode

Description	Displays 2LM memory modes of the processor(s). When configured as Cache mode, all the MCDRAM memory is used as memory side cache (MSC). When configured as Flat mode, all the MCDRAM memory is directly mapped to system address space. When configured as Hybrid mode, part of MCDRAM memory is mapped to system address space and the rest is used as MSC.
Legal Values	• Memory • Cache • Hybrid
Default Value	Cache
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.ProcEmbMemSystemSize

Description	Displays flat size of the MCDRAM
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.ProcEmbMemTotalSize

Description	Displays total size of the MCDRAM
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RawCapacity

Description	Total NVDIMM raw size in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RedundantMem

Description	Enables or disables the redundant memory feature. This feature can be enabled only if a valid redundant memory configuration is detected. When Mirror Mode is enabled, the server maintains two identical copies of data in memory. This feature allows the system to continue running even during a catastrophic memory failure. NOTE: In Mirror Mode, only half of the memory size is reported to the OS. When Spare Mode is enabled, certain sets of DIMMs or a portion of these DIMMs called a Rank will be set aside as the spare memory. When a preset threshold of correctable errors has been reached on an active DIMM rank, the contents of that rank will be copied to the spare memory to prevent catastrophic memory failure. Note that in Spare Mode, the memory size reported to the OS does not include the spare portion. Default: Disabled
Legal Values	• Disabled • Spare • Mirror • IntraNodeMirror • DimmSpare • Dddc
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	For Spare Mode: Has a dependency on DIMM population where within a given channel, multi-rank DIMM or multi single rank DIMM needs to be populated. For Mirror Mode and Lockstep Mode: Has a dependency on DIMM population where corresponding channels for each socket (Channel0 and Channel2, Channel1 and Channel 3) needs to be populated and populated identically. Not on 13G+.

BIOS.MemSettings.RedundantMemCfgValid

Description	Indicates whether the Redundant Memory Configuration is valid.
Legal Values	• Invalid • Valid
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not on 13G+.

BIOS.MemSettings.RedundantMemInUse

Description	Indicates that the Redundant Memory Configuration feature is in use.
Legal Values	• NotInUse • InUse
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not on 13G+.

BIOS.MemSettings.RemainingRatedWriteEndurance0

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance1

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance10

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance11

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance12

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance13

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance14

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance15

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance16

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance17

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance18

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance19

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance2

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance20

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance21

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance22

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance23

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance3

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance4

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance5

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance6

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance7

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance8

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.RemainingRatedWriteEndurance9

Description	Indicates remaining storage lifetime percentage of NVDIMM-N.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus00

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus01

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus02

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus03

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus04

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus05

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.

Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus06

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus07

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus08

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus09

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus10

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus11

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus12

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus13

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus14

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus15

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus16

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.

Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus17

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus18

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus19

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus20

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus21

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus22

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SanitizeStatus23

Description	The sanitize status of this NVDIMM as unknown, not started, in progress, and completed.
Legal Values	• Unknown • NotStarted • InProgress • Completed
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase00

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase01

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase02

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase03

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency None

BIOS.MemSettings.SecureErase04

Description Enable or Disable Secure Erase Persistent Memory.

Legal Values

- Enabled
- Disabled

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

BIOS.MemSettings.SecureErase05

Description Enable or Disable Secure Erase Persistent Memory.

Legal Values

- Enabled
- Disabled

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

BIOS.MemSettings.SecureErase06

Description Enable or Disable Secure Erase Persistent Memory.

Legal Values

- Enabled
- Disabled

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

BIOS.MemSettings.SecureErase07

Description Enable or Disable Secure Erase Persistent Memory.

Legal Values

- Enabled
- Disabled

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

BIOS.MemSettings.SecureErase08

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase09

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase10

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase11

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase12

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase13

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase14

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase15

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase16

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase17

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase18

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase19

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase20

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase21

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase22

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SecureErase23

Description	Enable or Disable Secure Erase Persistent Memory.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber00

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber01

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber02

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber03

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber04

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber05

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber06

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber07

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber08

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber09

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber10

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber11

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber12

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber13

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber14

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber15

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber16

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber17

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber18

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber19

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber20

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber21

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber22

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SerialNumber23

Description	The serial number of this NVDIMM.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SnoopFilter

Description	Enables or disables the snoop filter option.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not on 13G+.

BIOS.MemSettings.SnoopMode

Description	Allows tuning of memory performances under different memory bandwidths. The optimal Snoop Mode setting is highly dependent on workload type. Early Snoop is best used for latency sensitive workloads. This setting offers the best balance between workload effects. Home Snoop is best used for NUMA workloads that need maximum local and remote memory bandwidth. Cluster on Die is best used for highly NUMA optimized workloads. This setting offers the best case local memory latency, but worst case remote latency. Cluster On Die is only available when Node Interleaving is Disabled. Opportunistic Snoop Broadcast, available on select processor models, works well for workloads of mixed NUMA optimization. It offers a good balance of latency and bandwidth.
Legal Values	• HomeSnoop • EarlySnoop • ClusterOnDie • OpportunisticSnoopBroadcast
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	* Gen >= 13G * Value: COD: Proc must support COD. * Value:COD: Node Interleaving must be disabled (COD available in NUMA mode). * [MemPopulation] * If M830/FC830 with Haswell there is effectively no SnoopMode option. * If M830/FC830 with Broadwell SnoopMode is available with options HomeSnoop and ClusterOnDie (if available).

BIOS.MemSettings.SocketID0

Description	Socket ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SocketID1

Description	Socket ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SocketID2

Description	Socket ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SocketID3

Description	Socket ID
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz00

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz01

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz02

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz03

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz04

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz05

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz06

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz07

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz08

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz09

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz10

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz11

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz12

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz13

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz14

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz15

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz16

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz17

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz18

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz19

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz20

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz21

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz22

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SpeedMHz23

Description	The speed of this NVDIMM.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SysMemSize

Description	Indicates the amount of main memory in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SysMemSpeed

Description	Indicates the clock frequency of the main memory.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SysMemType

Description	Indicates the type of main memory installed in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SysMemVolt

Description	Indicates the current operating voltage of main memory.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.SystemMemoryModel

Description	Displays the memory model of the processor(s) When configured as All2All, all the cores will be serviced by all CHAs (caching/home agent - Caching architecture). When configured as SNC-2, all the CHAs, EDCs, MCs and DRAM/memory are equally split and assigned to each cluster. When configured as SNC-4, only the EDCs and DRAM memory are equally split and assigned to 4 clusters When configured as Hemisphere, all the CHAs, EDCs, MCs are equally split and assigned to each cluster (system address space is interleaved instead of split). When configured as Quadrant, all the CHAs, EDCs, MCs are equally split and assigned to 4 clusters (system address space is interleaved instead of split).
Legal Values	• All2All • SNC-2 • SNC-4 • Hemisphere • Quadrant
Default Value	Quadrant
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.UnconfiguredCapacity

Description	Total NVDIMM size that is unconfigured in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MemSettings.VideoMem

Description	Indicates the total amount of video memory available to the embedded video controller.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[Zhengyu]:Not used in 13G

BIOS.MiscSettings.AssetTag

Description	This field displays the Asset Tag and allows you to modify it. The Asset Tag is a string assigned to a system, usually by an administrator, for security or tracking purposes. The Asset Tag can be up to 63 printable US-ASCII characters.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • Using XML escape symbols such as &lt; or &gt; or &amp; as AssetTag or as a substring in the AssetTag will be configured as regular characters that they represent.

BIOS.MiscSettings.CapsuleFirmwareUpdate

Description	This field enables or disables BIOS update using a UEFI capsule update package. NOTE: If this option is disabled, you will not be able to update the BIOS using services such as Windows Update. This setting has effect only when Boot Mode is set to UEFI.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.Daylight

Description	Enable/Disable Daylight Savings Time.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.DellWyseP25BIOSAccess

Description	Controls remote user access to BIOS Setup via Dell Wyse P25/P45 Portal. When set to Disabled, pre-OS keyboard and mouse access is prevented, including to Diagnostics and Boot Options. It cannot be set back to Enabled from the P25/P45.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.Disabled

Description	"Enable/Disables ACPI FPDT information. " "When set to Enabled, publish ACPI Firmware Performance Data Table (FPDT) for OS." "This ACPI table provide platform initialization records with data pertaining to the boot process."
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.MiscSettings.ErrPrompt

Description	This field determines whether the BIOS stops and displays a prompt when certain types of errors occur during POST. The BIOS will display the prompt when this setting is Enabled; otherwise, the BIOS will continue through POST and attempt to boot an operating system.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.ForceInt10

Description	In UEFI Boot Mode, this field determines whether the system BIOS will load the legacy video (INT 10h) option ROM from the video controller. Normally there would be no reason to do so. However, you might need to do this in order to install certain older operating systems. During installation of these older operating systems, you may be presented with a blank screen (no visible screen output). Setting this field

to Enabled may fix this OS installation issue. This field has no effect when Boot Mode is set to BIOS. This field cannot be set to Enabled when Boot Mode is UEFI and Secure Boot is enabled.

Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.InSystemCharacterization

Description	When enabled, In-System Characterization (ISC) executes during POST upon detecting relevant change(s) in system configuration to optimize system power and performance. ISC takes about 20 seconds to execute, and system reset is required for ISC results to be applied. The Enabled - No Reboot option executes ISC and continues without applying ISC results until the next time system reset occurs. The Enabled option executes ISC and forces an immediate system reset so that ISC results can be applied right away. It takes the system longer to be ready due to the forced system reset. When disabled, ISC will not execute.
Legal Values	• Enabled • FastBoot • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	R530, R530XD, R430, T430, R330, T330, R230, and T130 do not support ISC.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.NumLock

Description	This field determines whether the system boots with Num Lock enabled or disabled. This does not apply to 84-key keyboards. When Num Lock is On, the rightmost keys on the keyboard function like those on a numeric calculator. With Num Lock Off, they function as cursor-control keys.
Legal Values	• On • Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.PowerCycleRequest

Description	This feature allows you to mimic a one-time AC power cycle. You will rarely need to use this feature. You may be directed to use it by Dell support. This feature is usually set to None. When you change it to Virtual AC, the system will do its best to mimic a temporary removal of AC power from the system (the AC Power Recovery feature will not be triggered by this action). The effect of this action is that some of the hardware components of the system that are always powered on when AC is present (even when the system appears to be off) will be reset. Using this feature is much more convenient than having to physically remove and reinsert the AC power cord, which would then trigger the AC Power Recovery feature when the cord was reinserted.
Legal Values	• None • FullPowerCycle
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.ReportKbdErr

Description	This field sets whether keyboard-related error messages are reported at system startup.
Legal Values	• Report • NoReport
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.SkHynixSmartTestEnable

Description	Enable - Enables memory test during normal boot. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable.
Legal Values	• Enabled • Disabled • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.SysMgmtNVByte1

Description	System Management NVRAM Byte that can be used as a state flag.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.SysMgmtNVByte2

Description	System Management NVRAM Byte that can be used as a state flag.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.SystemUefiShell

Description	This field enables or disables the System UEFI Shell as a UEFI boot option choice.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.MiscSettings.TimeZone

Description	Times offset from UTC.
Legal Values	• Standard Global Timezones
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.AdditionalPxeDevices

Description	When enabled, add 12 more PXE device.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.HttpDev1EnDis

Description	When this setting is Enabled, the BIOS will create a UEFI boot option for the HTTP device.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.HttpDev2EnDis

Description	When this setting is Enabled, the BIOS will create a UEFI boot option for the HTTP device.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.HttpDev3EnDis

Description	When this setting is Enabled, the BIOS will create a UEFI boot option for the HTTP device.
Legal Values	• Enabled

	• Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.HttpDev4EnDis

Description	When this setting is Enabled, the BIOS will create a UEFI boot option for the HTTP device.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.IscsiDev1EnDis

Description	This field controls the configuration for this iSCSI device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.IscsiInitiatorName

Description	This field specifies the name of the iSCSI Initiator in IQN format.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.NumberOfPxeDevices

Description	Number of PXE devices. Valid values are 4,8,12 and 16.
Legal Values	Integer values.
Default Value	4
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.NvmeofEnDis

Description	NVMe-oF feature Enable/Disable. When enabled, it allows to configuration of the host and target parameters needed for fabric connection.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.NvmeofHostId

Description	This field specifies a 16 bytes value of NVMe-oF Host Identifier that uniquely identifies this host with the controller in the NVM subsystem. Allowed input is a hexadecimal-encoded string in this format: 00112233-4455-6677-8899-aabbccddeeff Leave it empty to use system generated value. A value of all FF is not allowed.
Legal Values	String of ASCII characters.
Default Value	0
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.NvmeofHostNqn

Description	This field specifies the name of the NVMe-oF Host NQN. Allowed input is in following format:\ nqn.yyyy-mm.<Reversed Domain Name>:<Unique String> Leave it empty to use system generated value with following format: nqn.1988-11.com.dell:<Model Name>.<Model Number>.<Service Tag>
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.NvmeofHostSecurityPath

Description	This field specifies the Host security key path.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.PxeDev1EnDis

Description	PXE device Enable/Disable. When enabled, a UEFI boot option will be created for the PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.PxeDev2EnDis

Description	PXE device Enable/Disable. When enabled, a UEFI boot option will be created for the PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.PxeDev3EnDis

Description	PXE device Enable/Disable. When enabled, a UEFI boot option will be created for the PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NetworkSettings.PxeDev4EnDis

Description	PXE device Enable/Disable. When enabled, a UEFI boot option will be created for the PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Address

Description	NVMe-OF subsystems IP Address for this Connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Auth

Description	Authentication type for this NVMe-oF connection.
Legal Values	• None • Chap
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1ConInterface

Description	NIC interface used for this NVMe-oF connection.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1ConProtocol

Description	This field sets the value of protocol type for NVMe-oF connection. When IPv6 is selected, BIOS uses IPv6 Autoconfiguration to get the IPv6 address.
Legal Values	• IPv4 • IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	[GEN>=16]
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1ControllerId

Description	NVMe-oF subsystems Controller ID for this NVMe-oF connection.
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1EnDis

Description	This field controls the parameters for NVMe-oF subsystem1 connection.
Legal Values	• Enabled

	• Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1HostDhcp

Description	DHCP Enable/Disable for this NVMe-oF connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1HostGateway

Description	Host gateway for this NVMe-oF connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1HostIP

Description	Host IP Address for this NVMe-oF connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1HostMask

Description	Host Subnet Mask for this NVMe-oF connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1InfoDhcp

Description	NVMe-oF Subsystems DHCP Enable/Disable for this connection.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1NamespaceId

Description	NamespaceID(NID) for this NVMe-oF connection.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Nqn

Description	NVMe-oF subsystems NQN for this connection. Allowed input is in following format: nqn.yyy-mm.<Reversed Domain Name>:<Unique String>
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Port

Description	NVMe-oF subsystems Port for this connection.
Legal Values	Integer values.
Default Value	4420
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Retry

Description	Retry Count for this NVMe-oF connection.
Legal Values	Integer values.
Default Value	3
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Security

Description	Security Enable/Disable for this NVMe-oF connection.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1SecurityKeyPath

Description	Security Key path for this NVMe-oF connection.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1Timeout

Description	Timeout for this NVMe-oF connection.
Legal Values	Integer values.
Default Value	10000(ms)
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1TransType

Description	This field sets the value of transport type for NVMe-oF connection.
Legal Values	String of ASCII characters.
Default Value	TCP
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1VlanEnDis

Description	VLAN Enable/Disable for this NVMe-oF connection.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A

Dependency	NVMe-oF feature is available from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1VlanId

Description	VLAN Id for this NVMe-oF connection.
Legal Values	Integer values.
Default Value	1
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeOfSubSysSettings.NvmeofSubsys1VlanPriority

Description	VLAN priority for this NVMe-oF connection.
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	N/A
Dependency	NVMe-oF feature is available only from 16G onwards only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeSettings.BiosNvmeDriver

Description	Dell Qualified NVMe drives always use the UEFI NVMe driver built into the Dell BIOS. When this option is set to All Drives, the BIOS driver will also be used with any NVMe drives in the system that have not been qualified by Dell. NOTE: when this option is set to All Drives and non-Dell qualified NVMe drives are present, you have a configuration that has not been validated which may lead to unexpected behavior.
Legal Values	• DellQualifiedDrives : AllDrives
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.NvmeSettings.NvmeMode

Description	If the system contains NVMe drives that you want to configure in a RAID array, you must set both this field and the Embedded SATA field on the SATA Settings menu to RAID Mode. You may also need to change the Boot Mode setting to UEFI. Otherwise, you should set this field to Non-RAID Mode.
Legal Values	• NonRaid • Raid
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeBiosBootSeq

Description	This field determines the one-time boot device when the One-Time Boot Device List is set to BIOS Boot Sequence Device. If Boot Mode is set to UEFI, the system temporarily switches the Boot Mode to BIOS when attempting a one-time boot to the device.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeBootMode

Description	This field enables the boot device list from which a boot device can be selected. After selecting the One-Time Boot Device List, the desired boot device must be selected from the corresponding Sequence Device field. The system will attempt to boot once to the selected device on next startup.
Legal Values	• Disabled • OneTimeBootSeq • OneTimeHddSeq • OneTimeUefiBootSeq • OneTimeCustomBootSeqStr • OneTimeCustomHddSeqStr • OneTimeCustomUefiBootSeqStr
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeBootModeSeq

Description	No description information available.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeBootSeqDev

Description	This field determines the one-time boot device when the One-Time Boot Device List is set to BIOS Boot Sequence Device. If Boot Mode is set to UEFI, the system temporarily switches the Boot Mode to BIOS when attempting a one-time boot to the device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeCustomBootStr

Description	This field determines the one-time boot device when the One-Time Boot Device List is set to one of the Custom String options. The system may temporarily switch to the correct boot mode based on the One-Time Boot Device List setting.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeHddSeq

Description	This field determines the one-time boot hard disk when the One-Time Boot Device List is set to BIOS Hard-Disk Drive Sequence Device. If Boot Mode is set to UEFI, the system temporarily switches the Boot Mode to BIOS when attempting a one-time boot to the device.
Legal Values	No information available.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeHddSeqDev

Description	This field determines the one-time boot hard disk when the One-Time Boot Device List is set to BIOS Hard-Disk Drive Sequence Device. If Boot Mode is set to UEFI, the system temporarily switches the Boot Mode to BIOS when attempting a one-time boot to the device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeUefiBootPath

Description	Allows a one-time UEFI boot to the provided UEFI device path.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeUefiBootSeq

Description	This field determines the one-time boot device when the One-Time Boot Device List is set to UEFI Boot Sequence Device. If Boot Mode is set to BIOS, the system temporarily switches the Boot Mode to UEFI when attempting a one-time boot to the device.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.OneTimeBoot.OneTimeUefiBootSeqDev

Description	This field determines the one-time boot device when the One-Time Boot Device List is set to UEFI Boot Sequence Device. If Boot Mode is set to BIOS, the system temporarily switches the Boot Mode to UEFI when attempting a one-time boot to the device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PowerMgmtSettings.FanPwrPerf

Description	No description information available.
Legal Values	• MaxPerf • MinPwr
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PowerMgmtSettings.MemDynamicPwr

Description	No description information available.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PowerMgmtSettings.MemPwrPerf

Description	No description information available.
Legal Values	• MaxPerf • 1333Mhz • 1067Mhz • 978Mhz

	• 800Mhz • MinPwr
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PowerMgmtSettings.PowerMgmt

Description	No description information available.
Legal Values	• OsCtrl • ActivePwrCtrl • Custom • MaxPerf
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.AmdlohcWorkaround

Description	Enable the AMD IOHC workaround feature so all the "Request" traffic at the interface is temporarily stalled (paused). It also prevents the possibility of a processor abruptly stopping working or getting automatically reset.
Legal Values	String of ASCII characters.
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	Applicable only to 15G AMD platforms Rome Processor.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.AmdSpeculativeStoreMode

Description	Sets how quickly store instructions send out their invalidations to remote cacheline copies. Balanced/Auto: May delay sending when cacheline is present, but not in a writeable state in the local cache. More Speculative: Will send as soon as possible. Less Speculative: May delay sending when cacheline is not presenting the local cache or not in a writable state in the local cache.
Legal Values	• Auto • More Speculative • Less Speculative • Balanced

Default Value	Auto
Write Privilege	N/A
License Required	N/A
Dependency	Only on AMD Systems

BIOS.ProcSettings.AvxlccpPreGrantLevel

Description	Allows the system to select between different AVX ICCP transition levels"offered by Intel. The default level is 128 Heavy.
Legal Values	• lccpHeavy128 • lccpLight256 • lccpHeavy256 • lccpLight512 • lccpHeavy512
Default Value	lccpHeavy128
Write Privilege	N/A
License Required	N/A
Dependency	Only in use if on AVX ICCP Pre-Grant License is Enabled. Only applicable on Intel-based platforms.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.AvxlccpPreGrantLicense

Description	Allows the user to enable or disable the selection of different AVX ICCP transition levels offered by Intel. This option is set to Disabled by default.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	Intel only attribute
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CcdCores

Description	Enable number of Cores per CCD.
Legal Values	• Rome = All • TWO(1+1) • FOUR(2+2) • SIX(3+3) Milan= All • One1Plus0 • Two2Plus0 • Three3Plus0 • Four4Plus0 • Five5Plus0

	• Six6Plus0 • Seven7Plus0
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CcxAsNumaDomain

Description	This field specifies that each CCX within the processor will be declared as a NUMA Domain.
Legal Values	• Enabled • Disabled • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ControlledTurbo

Description	Helps to control the turbo engagement feature. It is active when System Profile is set to Performance, or when System Profile is set to Custom, CPU Power Management is set to Maximum Performance, and Turbo Boost enabled.
Legal Values	• Enabled • Disabled • ControlledTurboLimitMinus1 • ControlledTurboLimitMinus2 • ControlledTurboLimitMinus3 • Custom
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	No dependency, however this setting is only valid when the CPU Power Management is set to Maximum Performance.If the CPU Power Management is not set to Maximum Performance, the customer can still change it but it will have no effect.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ControlledTurboExtended

Description	Enables control of the turbo limit engagement. Effective only when the Dell Controlled Turbo feature is enabled.

Legal Values	- ControlledTurboLimitMinus1 - ControlledTurboLimitMinus2 - Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ControlledTurboMinusBin

Description	Enter a value from 0 to 12 bins. The value entered decreases the Dell AVX Scaling Technology frequency when the Dell Controlled Turbo feature is enabled.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CorePerfBoost

Description	No description information available.
Legal Values	- Enabled - Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuAcpiCstC2Latency

Description	"Enter in microseconds (decimal value)." "Larger C2 latency values will reduce both the number of C2 transitions and C2 residency." "Fewer transitions can help when performance is sensitive to the latency of C2 entry and exit." "Higher residency can improve performance by allowing higher frequency boost and reduce idle core power." "With Linux kernel 6.0 or later, the C2 transition cost is significantly reduced." "The best value will depend on the kernel version, use case, and workload."
Legal Values	Integer values.
Default Value	800
Write Privilege	N/A
License Required	N/A

Dependency	Only available on all 16G AMD processors.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuCrashLogControl

Description	This field controls the Intel CPU Crash Log feature for the collection of previous crash data from Shared SRAM of the Out-of-Band Management Services Module at post reset.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	Applicable to Intel CPUs only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuFeatureErms

Description	Enables or disables Enhanced REP MOVSB/STOSB support. This setting can affect performance, depending on the application running on the server.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuFeatureFsrn

Description	Enables or disables Fast Short REP MOVSB support. This setting can affect performance, depending on the application running on the server.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuFeatureRmss

Description	Enables or disables REP-MOV/STOS Streaming support. This setting can affect performance, depending on the application running on the server.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuInterconnectBusSpeed

Description	This setting governs the frequency of the communication links among the CPUs in the system. Note that standard and basic bin processors support lower link frequencies than the advanced parts do. Maximum Data Rate indicates that the BIOS will run the communication links at the maximum frequency supported by the processors. You can also select specific frequencies that the processors support, which can vary. For best performance, you should choose the Maximum Data setting. Any reduction in the communication link frequency will affect the performance of non-local memory accesses and cache coherency traffic. In addition, it can slow access to non-local I/O devices from a particular CPU. However, if power saving considerations outweigh performance, you may want to reduce the frequency of the CPU communication links. If you do this, you should localize memory and I/O accesses to the nearest NUMA node to minimize the impact to system performance.
Legal Values	• MaxDataRate • 10GTps • 9GTps
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available if 2 or more CPUs are present. On 14G only MaxDataRate, 10GTps, and 9GTps
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuMinSevAsid

Description	This field determines the number of Secure Encrypted Virtualization (SEV) ES and non-ES available Address Space IDs. The number specified is the dividing line between ES and non-ES ASIDs. ES - Encrypted State - the register save state area is also encrypted along with the entire guest memory area. The maximum number of SEV ASIDs available depends on installed CPU and memory configuration which can either be 15, 253 or 509. The default value is 1 and the value entered by user means the number of non-ES ASIDs starts from the value entered and ends at the maximum number of SEV ASIDs available. A value of 1 means there are only non-ES ASIDs available. Example 1: If the maximum number of ASIDs is 15, the default value 1 means there are 15 SEV non-ES ASIDs and 0 SEV ES ASIDs. Example 2: If the maximum number of ASIDs is 15, the value 4 means there are 12 SEV non-ES ASIDs and 3 SEV ES ASIDs. Example 3: If the maximum number of ASIDs is 509, the value 40 means there are 470 SEV non-ES ASIDs and 39 SEV ES ASIDs.
Legal Values	Integer values.
Default Value	1

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.CpuPaLimit

Description	Allows to Enable the 46 bit physical address limit. The address is 52 bit when the limit is disabled.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.DataReuse

Description	When set to Enabled, allows the processor to retain frequently used lines in all levels of cache at the expense of some control signals between the processor and cache.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.DculpPrefetcher

Description	Enables or disables Data Cache Unit (DCU) IP Prefetcher. This setting can affect performance, depending on the application running on the server. Recommended for High Performance Computing applications.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not on Value systems.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.DcuStreamerPrefetcher

Description	Enables or disables Data Cache Unit (DCU) Streamer Prefetcher. This setting can affect performance, depending on the application running on the server. Recommended for High Performance Computing applications.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not on Value systems.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.DirectoryMode

Description	Enable or Disable directory mode.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	TBU
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.DmaVirtualization

Description	When enabled, additional hardware capabilities for DMA Remapping and Virtualization are available.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.DynamicCoreAllocation

Description	Logical Processor Idling (LPI) is a collaborative interface between platform and Operating System that helps to improve the energy efficiency of a system. This feature is required in those cases where customer has a need to go for power budgeting. It uses Operating Systems core parking algorithm and parks some of the logical processors in the system which in turn lets the corresponding processor cores transition into a lower power idle state. If LPI is getting used instead of throttling, better performances

can be achieved when power budgeting is used. Setting to Disabled limits the OS capability to put the logical processors in idling state. Note: This feature is not supported if CPU Power Management is set to Maximum Performance.

Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.FastGoConfig

Description	Select CR QoS Configuration Profiles
Legal Values	• 6 • 0 • 1 • 2 • 3 • 4 • 5
Default Value	6
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.IommuSupport

Description	Enable or Disable IOMMU support. Required to create IVRS ACPI Table
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.IrqThrottle

Description	Throttles local requests that are targeting a remote address.
Legal Values	• 0

- 1
- 2
- 3
- 4

Default Value	1
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.KernelDmaProtection

Description	For Intel platforms: When set to Enabled, using Virtualization Technology, BIOS & Operating System will enable direct memory access protection for DMA capable peripheral devices. Enable Virtualization Technology to use this option. For AMD platforms: When set to Enabled, using IOMMU, BIOS & Operating System will enable direct memory access protection for DMA capable peripheral devices. Enable IOMMU Support to use this option.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L1Prefetcher

Description	Enables or disables the L1 Prefetcher. This setting can affect performance, depending on the application running on the server. Recommended for High Performance Computing applications.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L1RegionPrefetcher

Description	When set to Enabled, the processor provides additional fetch to data along with the data access to the given instruction for performance tuning by controlling the L1 region prefetcher setting. Use the recommended setting, and this option will allow for optimizing overall workloads.
Legal Values	• Enabled

	• Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L1StreamHwPrefetcher

Description	When set to Enabled, the processor provides advanced performance tuning by controlling the L1 Stream HW prefetcher setting. Use the recommended setting, and this option will allow for optimizing overall workloads.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L1StridePrefetcher

Description	When set to Enabled, the processor provides additional fetch to the data access for an individual instruction for performance tuning by controlling the L1 stride prefetcher setting. Use the recommended setting and this option will allow for optimizing overall workloads.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L2Prefetcher

Description	Enables or disables the L2 Prefetcher. This setting can affect performance, depending on the application running on the server. Recommended for High Performance Computing applications.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L2RfoPrefetch

Description	Enable or disable the L2 RFO(Read For Ownership) prefetch. The RFO is the process of reading a cache line from the memory into the cache before it can be written to.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	Intel only attribute
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L2StreamHwPrefetcher

Description	When set to Enabled, the processor provides advanced performance tuning by controlling the hardware prefetcher setting. Use the recommended setting, and this option will allow for optimizing overall workloads.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.L2UpDownPrefetcher

Description	When set to Enabled, the processor uses memory access to determine whether to fetch next or previous for all memory accesses for advanced performance tuning by controlling the L2 up/down prefetcher setting. Use the recommended setting and this option will allow for optimizing overall workloads.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.LmceEn

Description	Enable or disable the LMCE feature. This is an extension of the MCA Recovery mechanism providing the capability to deliver Uncorrected Recoverable (UCR) Software Recoverable Action Required (SRAR) errors to one or more specific logical processor threads receiving previously poisoned or corrupted data. When enabled, the UCR SRAR Machine Check Exception is delivered only to the affected thread rather than broadcast to all threads in the system. The feature supports Operating System recovery for cases of multiple, recoverable faults detected in close proximity which would otherwise result in a fatal machine check event. The feature is available only on Advanced RAS processors.
Legal Values	• Enabled • Disabled
Default Value	"Disabled"
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.LogicalProc

Description	Each processor core supports up to two logical processors. When set to Enabled, the BIOS reports all logical processors. When set to Disabled, the BIOS only reports one logical processor per core. Generally, higher processor count results in increased performance for most multi-threaded workloads and the recommendation is to keep this enabled. However, there are some floating point/scientific workloads, including HPC workloads, where disabling this feature may result in higher performance.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Processor must support HyperThreading.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.MadtCoreEnumeration

Description	This field determines how BIOS enumerates processor cores in the ACPI MADT table. When set to Round Robin, Processor cores are enumerated in a Round Robin order to evenly distribute interrupt controllers for the OS across all Sockets and Dies. When set to Linear, Processor cores are enumerated across all Dies within a Socket before enumerating additional Sockets for a linear distribution of interrupt controllers for the OS.
Legal Values	• RoundRobin • Linear
Default Value	RoundRobin
Write Privilege	N/A
License Required	N/A
Dependency	Only visible on systems with AMD processors.

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.NumaDistanceEnum

Description	This field determines how BIOS enumerate NUMA nodes distance in ACPI SLIT tables. When set to physical, NUMA node distance will enumerated by physical architecture. When set to logical, the level of NUMA node distance will simplified by logical distance for better OS capability.
Legal Values	• Physical • Logical
Default Value	Physical
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.NumaNodesPerSocket

Description	This field specifies the number of NUMA nodes per socket. The Zero option is for 2 socket configurations.
Legal Values	• 0 • 1 • 2 • 4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.OptimizerMode

Description	Manages the CPU performance based on the power management setting. Auto: Default setting. Enables Static ICA when CPU Power Management is set to Max Performance. If Static ICA is not supported in this system, then enables Adaptive ICA. Enabled: Enables Static ICA even if the CPU Power Management feature is enabled. Adaptive: Please use earlier proposal? Disabled: Disables the WHICH feature.
Legal Values	• Auto • Disabled • Enabled • Adaptive
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.PROCESSOR_CCD

Description	Core-Complex Die, its the container of CCX
Legal Values	• All • 2 • 3 • 4 • 6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.PROCESSOR_CCD_CCX

Description	Core Complex, all the cores in the same CCX share L3 Cache
Legal Values	• ALL, TWO(1+1) • FOUR(2+2) • SIX(3+3)
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.PerfMonitorDevices

Description	When set to Enabled, Performance Monitor Devices are visible to the OS.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1Brand

Description	This field displays the brand text provided by the processor manufacturer.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1ControlledTurbo

Description	Helps control the turbo engagement for processor 1. This option is active when System Profile is set to Performance, or when System Profile is set to Custom, CPU Power Management is set to Maximum Performance, and Turbo Boost enabled. A DPAT Pro license is needed to enable this feature.
Legal Values	• Disabled • ControlledTurboLimit • ControlledTurboLimitMinus1 • ControlledTurboLimitMinus2 • ControlledTurboLimitMinus3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	No dependency, however this setting is only valid when the CPU Power Management is set to Maximum Performance.If the CPU Power Management is not set to Maximum Performance, the customer can still change it but it will have no effect. A DPAT Pro license is needed to expose this field.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1ControlledTurboMinusBin

Description	For processor 1, when the Dell Controlled Turbo feature is enabled and set to Custom, the value entered decreases the Dell AVX Scaling Technology frequency.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1Cores

Description	Controls the number of enabled cores in the processor. Under certain circumstances, you may see limited performance improvements to Intel Turbo Boost Technology and benefit from potentially larger shared caches if you reduce the number of enabled cores. Most computing environments tend to benefit more from larger number of processing cores, so you must carefully weigh the disabling of cores to gain nominal performance enhancements.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This setting requires the DPAT Pro license to be visible. It can be edited only if the Number of Cores per Processor is set to Custom.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1Id

Description	Displays the processors family, model, and stepping values.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1L2Cache

Description	Displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1L3Cache

Description	Displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1MaxMemoryCapacity

Description	Displays the maximum amount of system memory supported by this processor.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Available only when "max memory capacity" data is provided by the processor.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1Microcode

Description	Indicates the microcode update signature.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• This attribute is only configurable through performance profiles. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc1NumCores

Description	Displays the number of cores in the processor package.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2Brand

Description	Displays the brand text provided by the processor manufacturer.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2ControlledTurbo

Description	Helps control the turbo engagement for processor 2. This option is active when System Profile is set to Performance, or when System Profile is set to Custom, CPU Power Management is set to Maximum Performance, and Turbo Boost enabled. A DPAT Pro license is needed to enable this feature.
Legal Values	• Disabled • ControlledTurboLimit • ControlledTurboLimitMinus1 • ControlledTurboLimitMinus2 • ControlledTurboLimitMinus3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	No dependency, however this setting is only valid when the CPU Power Management is set to Maximum Performance.If the CPU Power Management is not set to Maximum Performance, the customer can still change it but it will have no effect. A DPAT Pro license is needed to expose this field.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2ControlledTurboMinusBin

Description	For processor 2, when the Dell Controlled Turbo feature is enabled and set to Custom, the value entered decreases the Dell AVX Scaling Technology frequency.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2Cores

Description	Controls the number of enabled cores in the processor. Under certain circumstances, you may see limited performance improvements to Intel Turbo Boost Technology and benefit from potentially larger shared caches if you reduce the number of enabled cores. Most computing environments tend to benefit more from larger number of processing cores, so you must carefully weigh the disabling of cores to gain nominal performance enhancements.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This setting requires the DPAT Pro license to be visible. It can be edited only if the Number of Cores per Processor is set to Custom.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2Id

Description	Displays the processors family, model, and stepping values.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2L2Cache

Description	Displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2L3Cache

Description	Displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2MaxMemoryCapacity

Description	Displays the maximum amount of system memory supported by this processor.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Available only when "max memory capacity" data is provided by the processor.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2Microcode

Description	Indicates the microcode update signature.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc2NumCores

Description	Displays the number of cores in the processor package.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3Brand

Description	Displays the brand text provided by the processor manufacturer.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3ControlledTurbo

Description	Helps control the turbo engagement for processor 3. This option is active when System Profile is set to Performance, or when System Profile is set to Custom, CPU Power Management is set to Maximum Performance, and Turbo Boost enabled. A DPAT Pro license is needed to enable this feature.
Legal Values	• Disabled • ControlledTurboLimit • ControlledTurboLimitMinus1 • ControlledTurboLimitMinus2 • ControlledTurboLimitMinus3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	No dependency, however this setting is only valid when the CPU Power Management is set to Maximum Performance.If the CPU Power Management is not set to Maximum Performance, the customer can still change it but it will have no effect. A DPAT Pro license is needed to expose this field.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3ControlledTurboMinusBin

Description	For processor 3, when the Dell Controlled Turbo feature is enabled and set to Custom, the value entered decreases the Dell AVX Scaling Technology frequency.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3Cores

Description	Controls the number of enabled cores in the processor. Under certain circumstances, you may see limited performance improvements to Intel Turbo Boost Technology and benefit from potentially larger shared caches if you reduce the number of enabled cores. Most computing environments tend to benefit more from larger number of processing cores, so you must carefully weigh the disabling of cores to gain nominal performance enhancements.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This setting requires the DPAT Pro license to be visible. It can be edited only if the Number of Cores per Processor is set to Custom.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3Id

Description	Displays the processors family, model, and stepping values.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3L2Cache

Description	Displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3L3Cache

Description	Displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3MaxMemoryCapacity

Description	Displays the maximum amount of system memory supported by this processor.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Available only when "max memory capacity" data is provided by the processor.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3Microcode

Description	Indicates the microcode update signature.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc3NumCores

Description	Displays the number of cores in the processor package.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4Brand

Description	Displays the brand text provided by the processor manufacturer.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4ControlledTurbo

Description	Helps to control the turbo engagement for processor 4. This option is active when System Profile is set to Performance, or when System Profile is set to Custom, CPU Power Management is set to Maximum Performance, and Turbo Boost enabled. A DPAT Pro license is needed to enable this feature.
Legal Values	• Disabled • ControlledTurboLimit • ControlledTurboLimitMinus1 • ControlledTurboLimitMinus2 • ControlledTurboLimitMinus3
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	No dependency, however this setting is only valid when the CPU Power Management is set to Maximum Performance.If the CPU Power Management is not set to Maximum Performance, the customer can still change it but it will have no effect. A DPAT Pro license is needed to expose this field.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4ControlledTurboMinusBin

Description	For processor 4, when the Dell Controlled Turbo feature is enabled and set to Custom, the value entered decreases the Dell AVX Scaling Technology frequency.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4Cores

Description	Controls the number of enabled cores in the processor. Under certain circumstances, you may see limited performance improvements to Intel Turbo Boost Technology and benefit from potentially larger shared caches if you reduce the number of enabled cores. Most computing environments tend to benefit more from larger number of processing cores, so you must carefully weigh the disabling of cores to gain nominal performance enhancements.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This setting requires the DPAT Pro license to be visible. It can be edited only if the Number of Cores per Processor is set to Custom.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4Id

Description	Displays the processors family, model, and stepping values.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4L2Cache

Description	This field displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4L3Cache

Description	This field displays the amount of memory in the corresponding processor cache.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4MaxMemoryCapacity

Description	Displays the maximum amount of system memory supported by this processor.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Available only when "max memory capacity" data is provided by the processor.

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4Microcode

Description	Indicates the microcode update signature.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc4NumCores

Description	This field displays the number of cores in the processor package.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Proc64bit

Description	Indicates whether or not the installed processor(s) support 64-bit extensions.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcAdjCacheLine

Description	When set to Enabled, the system is optimized for applications that require high utilization of sequential memory access. Disable this option for applications that require high utilization of random memory access.
Legal Values	• Enabled • Disabled
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcAmpPrefetch

Description	When enabled, this option enables one of the Mid-Level Cache (MLC) AMP hardware Prefetcher.
Legal Values	• Disabled • Enabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcAts

Description	Defines the Address Translation Cache (ATC) behavior for devices to cache DMA translations. This field provides an interface to a chipsets Address Translation and Protection Table to translate DMA addresses to host addresses.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Can only be edited if Virtualization is set to Enabled. Supported on 13G, except value systems. Not supported on 14G.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcAvxP1

Description	Avx P1 level selection.
Legal Values	• Normal • Level1 • Level2
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcBusSpeed

Description	Displays the bus speed of the processor(s).
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcCcds

Description	Enable number of CCDs per Processor.
Legal Values	• All • 2 • 3 • 4 • 6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcConfigTdp

Description	Allows the reconfiguration of the processor Thermal Design Power (TDP) levels based on the power and thermal delivery capabilities of the system. TDP refers to the maximum amount of power the cooling system is required to dissipate. NOTE: This option is only available on certain SKUs of the processors, and the number of alternative levels varies as well.
Legal Values	• Nominal • Level1 • Level2 • Maximum • Minimum
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Value systems only support Nominaml (effectively not configurable).
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcCoreSpeed

Description	Displays the rated clock speed of the processor(s).
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcCores

Description	Controls the number of cores presented to the Operating System (OS) from each populated processor socket. In general, it is uncommon to artificially reduce the core count for a given system, but under some circumstances, limited performance improvements to Intel Turbo Boost Technology and potentially larger shared caches may benefit some customers. Most computing environments tend to benefit more from larger numbers of processing cores, so you must carefully weigh disabling cores to gain nominal performance enhancements.
Legal Values	• Single • All • Dual • Quad • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28 • 32 • Custom
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcCoresPerDie

Description	Controls the number of enabled cores in the processor. Under certain circumstances, you may see limited performance improvements to Boost Technology and benefit from potentially larger shared caches if you reduce the number of enabled cores. Most computing environments tend to benefit more from larger number of processing cores, so you must carefully weigh the disabling of cores to gain nominal performance enhancements.
Legal Values	• Auto • Two1Plus1 • Two2Plus0 • Three3Plus0 • Four2Plus2 • Four4Plus0 • Six3Plus3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcDramPrefetcher

Description	When set to Enabled, turns on the DRAM prefetch unit in the Northbridge. When set to Disabled, prevents DRAM references from triggering DRAM prefetch requests. Default: Enabled
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcExecuteDisable

Description	A security feature designed to prevent certain types of buffer overflow attacks by enforcing specific areas of memory that applications can execute code. In general, it is best practice to leave this option set to Enabled for the security benefits, as no real performance advantage has been detected by disabling this feature in BIOS.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcHomelessPrefetch

Description	When enabled, this option allows L1 Data Cache Unit (DCU) to prefetch when the Fill Buffers (FB) is full. Auto maps to hardware default setting.
Legal Values	• Auto • Enabled • Disabled
Default Value	Auto
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcHpcMode

Description	No description information available.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcHtAssist

Description	When enabled, it provides filtering of broadcast probes to improve HyperTransport I/O Link bandwidth and performance on multi-node systems. When set to Enabled, the probe filter is enabled if two or more processors are installed and all processors support the probe filter. If only one processor is installed, both nodes must have memory (at least 1067 MT/s) attached. The default is Disabled for single-processor systems and Enabled for multi-processor systems.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcHwPrefetcher

Description	When set to Enabled, the processor is able to prefetch extra cache lines for every memory request. This setting can affect performance, depending on the application running on the server and memory bandwidth utilization.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcHyperTransport

Description	Specifies the supported HyperTransport I/O Link Specification. If the system board and all installed processors support HT 3, this field is settable to HT 3 or HT 1, else this field will become Read-Only and set to HT 1.
Legal Values	• HT1 • HT3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcSoftwarePrefetcher

Description	When set to Enabled, the hardware prefetcher considers software prefetches when detecting strides for prefetch requests. When set to Disabled, prevents the hardware prefetcher from considering software prefetches when detecting strides for prefetch requests. Default: Enabled
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcSwPrefetcher

Description	When set to Enabled, the processor is able to prefetch extra cache lines for every memory request. This setting can affect performance, depending on the application running on the server and memory bandwidth utilization.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcUncoreFreqRapl

Description	This setting controls whether the Running Average Power Limit (RAPL) balancer is enabled. If enabled, it activates the uncore power budgeting.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcVirtualization

Description	When set to Enabled, the BIOS will enable processor Virtualization features and provide the virtualization support to the Operating System (OS) through the DMAR table. In general, only virtualized environments such as VMware(r) ESX(tm), Microsoft Hyper-V(r), Red Hat(r) KVM, and other virtualized operating systems will take advantage of these features. Disabling this feature is not known to significantly alter the performance or power characteristics of the system, so leaving this option Enabled is advised for most cases.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.ProcX2Apic

Description	Enable or Disable x2APIC mode. Compared to the traditional xAPIC architecture, x2APIC extends processor addressability and enhances interrupt delivery performance. BIOS will force x2APIC to be enabled if there are 256 or more processor threads
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.QpiBandwidthPriority

Description	Determines the number and priority of requests on the QuickPath Interconnect (QPI) bus. The QPI connects the processor sockets. The Compute setting favors computational traffic while the I/O setting is optimized for IO intensive workloads.
Legal Values	• InputOutput • Compute
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.QpiSpeed

Description	The Intel QuickPath Interconnect (QPI) Speed option in the Processor section governs the frequency of the QPI links between the populated processors. The user should be aware that standard and basic bin Intel processors of this architecture support slower QPI link speeds than the advanced parts provide. Maximum Data Rate indicates that the BIOS will run the QPI links at the maximum frequency supported by the processor. Specific frequencies supported by the processor, which can vary, can also be selected. For best performance, the QPI link speed should be left at the maximized setting, for any reduction in QPI speed will affect the performance of non-local memory accesses and cache coherency traffic. In addition, access to non-local I/O devices from a particular core can be slowed by the reduction of QPI link speed. However, in some cases it may be advisable to reduce QPI speed where power considerations outweigh the performance cost. For users considering reducing the QPI link speeds, memory and I/O accesses should be localized to the nearest NUMA node to minimize the performance impact.
Legal Values	• MaxDataRate • 9GTps • 8GTps • 7GTps • 6GTps
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	Only available if 2 or more CPUs are present.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.RtidSetting

Description	Manipulates Requestor Transaction IDs, which are QuickPath Interconnect (QPI) resources. Generally should be left at Disabled, as no workloads have been identified as benefitting from the manipulation of this feature. NOTE: Enabling this option almost always results in negative impacts to overall system performance.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Supported on 13G, except value systems. Not supported on 14G.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.SubNumaCluster

Description	Sub NUMA Clustering (SNC) is a feature for breaking up the LLC into disjoint clusters based on address range, with each cluster bound to a subset of the memory controllers in the system. It improves average latency to the LLC.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.UmaBasedClustering

Description	UMA Based Clustering options include Disable(ALL2ALL), Hemisphere(2 cluster), and Quadrant (4 cluster). These option are only valid when SNC is disabled. If SNC is enabled, UMA-Based Clustering is automatically disabled by BIOS.
Legal Values	• Disable • Hemisphere • Quadrant
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	SNC should be Disabled.

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.Upi3LinkCtrl

Description	Set the value of UPI3 which is the QPI Link Control for the CPUs. This field is provided due to CPU issue of crosstalk from UPI Port3 affecting Lane 0 Rx margins of PCIe Port3 (PE3) when operating at Gen5 Speed. Disabled - Disable UPI3 link and allow the PE3 port A to reach Gen 5 speed (32GT/s). Enabled - Enable UPI3 link and limit the PE3 port A to Gen4 speed (16GT/s).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.ProcSettings.UpiPrefetch

Description	UPI Prefetch is a mechanism too get the memory read started early on DDR bus, the UPI Rx path will spawn a MemSpecRd to iMC directly.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev1Settings.PxeDev1Interface

Description	NIC Interface used for this PXE device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev1Settings.PxeDev1Protocol

Description	This field controls the PXE protocol used for this PXE device.
Legal Values	• IPv4 • IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev1Settings.PxeDev1VlanEnDis

Description	VLAN Enable/Disable for this PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev1Settings.PxeDev1VlanId

Description	VLAN ID for this PXE device.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev1Settings.PxeDev1VlanPriority

Description	VLAN priority for this PXE device.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev2Settings.PxeDev2Interface

Description	NIC Interface used for this PXE device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev2Settings.PxeDev2Protocol

Description	This field controls the PXE protocol used for this PXE device.
Legal Values	• IPv4 • IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev2Settings.PxeDev2VlanEnDis

Description	VLAN Enable/Disable for this PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev2Settings.PxeDev2VlanId

Description	VLAN ID for this PXE device.
Legal Values	Integer values.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev2Settings.PxeDev2VlanPriority

Description	VLAN priority for this PXE device.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev3Settings.PxeDev3Interface

Description	NIC Interface used for this PXE device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev3Settings.PxeDev3Protocol

Description	This field controls the PXE protocol used for this PXE device.
Legal Values	• IPv4 • IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev3Settings.PxeDev3VlanEnDis

Description	VLAN Enable/Disable for this PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev3Settings.PxeDev3VlanId

Description	VLAN ID for this PXE device.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev3Settings.PxeDev3VlanPriority

Description	VLAN priority for this PXE device.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev4Settings.PxeDev4Interface

Description	NIC Interface used for this PXE device.
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev4Settings.PxeDev4Protocol

Description	This field controls the PXE protocol used for this PXE device.
Legal Values	• IPv4 • IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev4Settings.PxeDev4VlanEnDis

Description	VLAN Enable/Disable for this PXE device.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev4Settings.PxeDev4VlanId

Description	VLAN ID for this PXE device.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.PxeDev4Settings.PxeDev4VlanPriority

Description	VLAN priority for this PXE device.
Legal Values	Integer values.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.RedundantOsControl.RedundantOsBoot

Description	When set to Enabled, the BIOS will boot to the device specified by Redundant OS Location.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.RedundantOsControl.RedundantOsLocation

Description	Specifies the backup device for the Redundant OS Control feature. When Redundant OS Boot is set to Enabled, the BIOS will boot to this device. Note: 1) SD Card Port, Internal USB Port, M.2 cards - If a device is set as the Redundant OS Location, then the corresponding device setting will be set based on Redundant OS state and not be available to be changed in Integrated Devices. 2) Embedded SATA - must be set to anything other than Off for SATA ports to show up as optional backup devices
Legal Values	• *Dynamic*
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.RedundantOsControl.RedundantOsState

Description	When set to Hidden, the device specified by Redundant OS Location will be hidden. It will not be visible in the Operating System or the BIOS boot sequence.
Legal Values	• Visible • Hidden
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.EmbSata

Description	Configures the embedded SATA to be set to Off, AHCI, or RAID Mode.
Legal Values	• Off • AtaMode • RaidMode • AhciMode
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	RAID option is suppressed if platform does not support SWRAID. Does R330 support SW RAID based on chassis? Ata Mode was deprecated with 13G and is removed in 14G and later.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.EmbSataShadow

Description	For internal use.
Legal Values	• AtaMode • AhciMode • RaidMode • Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	No dependency, AND should NOT be used by any teams except BIOS.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortA

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 1 onboard SATA port. This attribute is grayed out if Sata Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortACapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 1 onboard SATA port.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortADriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 1 onboard SATA port.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortAModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 1 onboard SATA port.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortB

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	This attribute is shown if platform supports at least 2 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortBCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 2 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortBDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 2 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortBModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 2 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortC

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 3 onboard SATA ports. This attribute is grayed out if Sata Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortCCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 3 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortCDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 3 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortCModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 3 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortD

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 4 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortDCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 4 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortDDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 4 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortDModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 4 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortE

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 5 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortECapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 5 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortEDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 5 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortEModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 5 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortF

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 6 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortFCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 6 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortFDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 6 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortFModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 6 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortG

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 7 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortGCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortGDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortGModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortH

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 8 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortHCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 8 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortHDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 8 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortHModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 8 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortI

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	This attribute is shown if platform supports at least 9 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 9 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortDriveType

Description	This field indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 9 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 9 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortJ

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 10 onboard SATA ports. This attribute is grayed out if Sata Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortJCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 10 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortJDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 10 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortJModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 10 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortK

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 7 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortKCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortKDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortKModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortL

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 7 onboard SATA ports. This attribute is grayed out if Sata Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortLCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 7 onboard SATA
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortLDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortLModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Indicates the drive model of the selected device.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortM

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 7 onboard SATA ports. This attribute is grayed out if Sata Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortMCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortMDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortMModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if SATA Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortN

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is shown if platform supports at least 7 onboard SATA ports. This attribute is grayed out if SATA Mode is NOT ATA.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortNCapacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortNDriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SataPortNModel

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	SATA_MODEL
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is suppressed if Sata Mode is RAID or the platform supports less than 7 onboard SATA ports.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.SecurityFreezeLock

Description	When set to Enabled, the Security Freeze Lock command is sent to the Embedded SATA drives during POST. This option is only applicable to ATA, AHCI mode, and is not applicable to RAID mode.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	This has the value of Disabled (read-only) if SATA Mode is Raid or Off.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.WriteCache

Description	Sends Enable or Disable Write Cache command to the Embedded SATA drives during POST. This option is only applicable to ATA, AHCI mode, and is not applicable to RAID mode.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This has the value of Disabled (read-only) if SATA Mode is Raid or Off.

BIOS.SataSettings.eSataPort1

Description	Sets the drive type of the selected device. When the Embedded SATA setting is ATA Mode, set this field to Auto to enable BIOS support for the device. Select Off to turn off BIOS support for the device. When the Embedded SATA setting is AHCI Mode or RAID Mode, BIOS always enables support for the device and this field is read-only.
Legal Values	• Off • Auto
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.eSataPort1Capacity

Description	Indicates the total capacity of a hard-disk drive. This field is undefined for removable-media devices such as optical drives.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.eSataPort1DriveType

Description	Indicates type of device attached to this SATA port.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SataSettings.eSataPort1Model

Description	Indicates the drive model of the selected device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SerialCommSettings.ConTermType

Description	This field sets your remote consoles terminal type. The <Ctrl><Alt><Del> key sequence is mapped to <ESC><R><ESC><r><ESC><R> on the Terminal. The <Ctrl><H>, <Ctrl><I>, <Ctrl><J>, <Ctrl><M> key sequences are mapped to <ESC><Ctrl><H>, <ESC><Ctrl><I>, <ESC><Ctrl><J>, <ESC><Ctrl><M> on the Terminal. <Alt><x> key sequences are mapped to <ESC><X><X> on the Terminal, where x is any letter key, and X is the upper case of that key.
Legal Values	• Vt100Vt220 • Ansi
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SerialCommSettings.ExtSerialConnector

Description	Use this field to associate the External Serial Connector to Serial Device 1, Serial Device 2, or the Remote Access Device. Note: Only Serial Device 2 can be used for Serial Over LAN. Configuring the External Serial Connector to Serial Device 1 allows independent use of Serial Device 1 while Serial Device 2 can be used for Serial Over LAN. Please see the Users Guide for the various operating modes available.
Legal Values	• Serial1

	- Serial2 - RemoteAccDevice
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not supported on blades.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SerialCommSettings.FailSafeBaud

Description	If the BIOS fails to determine the baud rate automatically, then it will use the baud rate specified by this field.
Legal Values	115200 57600 19200 9600
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SerialCommSettings.RedirAfterBoot

Description	Determines whether console redirection is enabled when the operating system is loaded.
Legal Values	- Enabled - Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SerialCommSettings.SerialComm

Description	This field controls the Serial Communication options.
Legal Values	- Off - OnConRedirAuto - OnNoConRedir - OnConRedirCom1 - OnConRedirCom2 - OnConRedir

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Monolithics:Auto, Off, On without CR, On with CR via COM1, On with CR via COM2. Blades: Off, On without CR, On with CR.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SerialCommSettings.SerialPortAddress

Description	This field sets port address for the Serial Devices. (COM1=0x3F8, COM2=0x2F8) Note: Only Serial Device 2 can be used for Serial Over LAN (SOL). To get Console Redirection via SOL, configure the same port address for Console Redirection and Serial Device.
Legal Values	- Serial1Com1Serial2Com2 - Serial1Com2Serial2Com1 - Com1 - Com2
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Blades: Com1, Com2 Monolithics: Serial1Com1Serial2Com2, Serial1Com2Serial2Com1
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.DellAutoDiscovery

Description	Allow BIOS to dynamically scan for PCIe devices rather than relying strictly on system slot definitions. The Platform Default setting will strictly follow the system slot definitions when configuring each PCIe slot. The Auto Discovery setting will analyze the installed PCIe cards and determine the correct configuration for each slot. This may include bifurcation of the slot for multiple devices. Manual Control allows the user to override bifurcation settings for each slot. CAUTION: Improper configuration of PCIe slots can prevent the system from functioning properly!
Legal Values	- PlatformDefault - AutoDiscovery - ManualControl
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot10Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will

bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot11Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot12Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the

slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot13Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot14Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot1Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot2Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8

- Allx4
- x4
- x16
- x8
- x4x4x8
- x8x4x4

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

Notes To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot3Bif

Description Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

- Legal Values**
- Allx16
 - Allx8
 - Allx4
 - x4
 - x16
 - x8
 - x4x4x8
 - x8x4x4

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

Notes To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot4Bif

Description Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

- Legal Values**
- Allx16
 - Allx8
 - Allx4
 - x4

- x16
- x8
- x4x4x8
- x8x4x4

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

Notes To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot5Bif

Description Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

Legal Values

- Allx16
- Allx8
- Allx4
- x4
- x16
- x8
- x4x4x8
- x8x4x4

Default Value None

Write Privilege N/A

License Required N/A

Dependency None

Notes To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot6Bif

Description Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.

Legal Values

- Allx16
- Allx8
- Allx4
- x4
- x16
- x8

	• x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot7Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot8Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotBifurcation.Slot9Bif

Description	Controls the bifurcation of PCIe cards installed in the specified slot. When set to default, the slot will operate at the default bifurcation for that slot. When set to x4 All Bifurcation, the slot will bifurcate to either two or four x4 links depending on the slot capability. When set to x8 All Bifurcation the slot will bifurcate to two x8 links. When set to x16 All Bifurcation the slot will bifurcate to x16 links. When set to x4 x8 Bifurcation the slot will bifurcate to two 4 links plus a x8 link When set to x8 x4 x4 Bifurcation the slot will bifurcate x8 link plus two x4 links NOTE: Only bifurcation options that the slot can support will be shown.
Legal Values	• Allx16 • Allx8 • Allx4 • x4 • x16 • x8 • x4x4x8 • x8x4x4
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SlotDisablement.Slot1

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot10

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot11

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot12

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot13

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot2

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot3

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot4

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot5

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot6

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot7

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot8

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SlotDisablement.Slot9

Description	Controls the configuration of PCIe cards installed in the specified slot. Slot disablement must be used only when the installed peripheral card is preventing booting into the operating system or causing delays or lockups in system startup. When set to Disabled, both the Option ROM and UEFI driver are disabled, the card is not enumerated on the PCI bus, and will not be available to the operating system. When set to Boot Driver Disabled, the Option ROM and UEFI driver from that slot will not run during POST. As a result, the system will not boot from the card, and its pre-boot services will not be available. However, the card is available to the operating system. Note: This option is not available if the slot contains a Dell PowerEdge RAID card (PERC). This option is not available if the slot contains the primary video display adapter. Note: Some PCIe device manufacturers implement a master boot driver that can initialize and manage all the similar devices in the system. In this case, to make sure that the Option ROM and UEFI driver do not run, you must select Boot Driver Disabled for all the cards from the same manufacturer (including its integrated device versions such as NDCs).
Legal Values	• Enabled • Disabled • BootDriverDisabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysInformation.AgesaVersion

Description	No description information available.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysInformation.DxioVersion

Description	Display the DXIO firmware version.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysInformation.SmuVersion

Description	Display the SMU firmware version
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SysMfrContactInfo

Description	Indicates the contact information of the Original Equipment Manufacturer (OEM).
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemBiosVersion

Description	Indicates the current version of the BIOS firmware.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemCpld2Version

Description	Indicates the current firmware version of CPLD.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemCpldVersion

Description	Indicates the current firmware version of CPLD.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemManufacturer

Description	Indicates the name of the Original Equipment Manufacturer (OEM).
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemMeVersion

Description	Indicates the current version of the Management Engine (ME) firmware.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemModelName

Description	Indicates the product name of the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.SystemServiceTag

Description	Indicates the Service Tag of a system, a unique identifier assigned by the Original Equipment Manufacturer (OEM).
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysInformation.UefiComplianceVersion

Description	Indicates the UEFI compliance level of the system firmware.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

BIOS.SysProfileSettings.ApbDis

Description	When enabled a specific hard-fused Data Fabric (SoC) P-state is forced for optimizing workloads sensitive to latency or throughput. (For higher performance) When disabled P-states will be automatically managed by the Application Power Management, allowing the processor to provide maximum performance while remaining within a specified power-delivery and thermal envelope. (For power savings)
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.CollaborativeCpuPerfCtrl

Description	Allows for collaboration between the operating system and the hardware to dynamically control processor frequency for optimal power efficiency. This feature works only when CPU Power Management is set to System DBPM (DAPC), or Hardware P States. Otherwise, changing this setting does not impact system power or performance. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Disabled for all the other System Profiles.. This setting is only valid if the CPU Power Management is set to DAPC, or HWPM.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.CpuInterconnectBusLinkPower

Description	When enabled, CPU interconnect bus link power management is enabled
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.CustomUncoreFrequency

Description	Select a customized frequency number for the Maximum mode of Processor Uncore Frequency. The frequency options are displayed according to the supported range of the current CPU SKU.
Legal Values	• 0.5GHz • 0.6GHz • 0.7GHz • 0.8GHz • 0.9GHz • 1.0GHz • 1.1GHz • 1.2GHz • 1.3GHz • 1.4GHz • 1.5GHz • 1.6GHz • 1.7GHz • 1.8GHz • 1.9GHz

- 2.0GHz
- 2.1GHz
- 2.2GHz
- 2.3GHz
- 2.4GHz
- 2.5GHz
- 2.6GHz
- 2.7GHz
- 2.8GHz
- 2.9GHz
- 3.0GHz

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	To be updated
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.DeterminismSlider

Description	It controls whether BIOS will enable determinism to control performance. Performance - BIOS will enable 100% deterministic performance control. Power - BIOS will not enable deterministic performance control.
Legal Values	• PerfDeterminism • PowerDeterminism
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Performance Determinism if the System Profile is set to Performance Per Watt (OS) and Performance.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.DlwmForcedWidth

Description	None
Legal Values	• x16 • x8 • x2
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.DynamicL1

Description	This field only applies to the package level setting to allow dynamic entering lower power link state L1.
Legal Values	• Disabled • Enabled •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.DynamicLinkWidthManagement

Description	DLWM reduces the XGMI link width between sockets from x16 to x8 (default), when no traffic is detected on the link. As with Data Fabric and Memory Pstates, this feature is optimized to trade power between core and high IO/memory bandwidth workloads. Forced = Force link width to x16, x8, or x2. Unforced = Link width will be managed by DLWM engine.
Legal Values	• Forced • Unforced
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.EfficiencyOptimizedMode

Description	Efficiency Optimized Mode maximizes Performance-per-Watt by opportunistically reducing frequency/power. This field enables/disables Efficiency Optimized Mode.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.EnablePkgcCriteria

Description	This field enables power and system criteria for Package c state.

Legal Values	• Disabled • Enabled •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.EnergyEfficientTurbo

Description	Energy Efficient Turbo (EET) is a mode of operation where a processors core frequency is adjusted within the turbo range based on workload. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Enabled if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), or Performance Per Watt (HWPM). Is set to Disabled if the System Profile is set to Performance, or Dense.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.EnergyPerformanceBias

Description	The CPU uses the setting to manipulate the internal behavior of the processor and determine whether targeting higher performance or better power savings. Read-only unless System Profile is set to Custom.
Legal Values	• MaxPower • BalancedPerformance • BalancedEfficiency • LowPower
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Balanced Performance if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Dense. Is set to Performance if the System Profile is set to Performance. Only applicable on Intel-based platforms.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.FixedSocPstate

Description	This value defines the forced P-state when ApbDis is enabled.
Legal Values	• FixedSocPstate0 • FixedSocPstate1 • FixedSocPstate2 • FixedSocPstate3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	AMD only attribute.
Notes	• This attribute is only supported on AMD platforms. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.MemFrequency

Description	Governs the BIOS memory frequency. The variables that govern maximum memory frequency include the maximum rated frequency of the DIMMs, the DIMMs per channel population, the processor choice, and this BIOS option. Additional power savings can be achieved by reducing the memory frequency, at the expense of reduced performance. Read-only unless System Profile is set to Custom.
Legal Values	• MaxPerf • 2666MHz • 2600MHz • 2400MHz • 2133MHz • 1866MHz • 1600MHz • 1333MHz • 1067MHz • 800MHz • MaxReliability
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Maximum Performance for all the other System Profiles..
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.MemPatrolScrub

Description	Patrol Scrubbing searches the memory for errors and repairs correctable errors to prevent the accumulation of memory errors. When set to Disabled, no patrol scrubbing will occur. When set to Standard Mode, the entire memory array will be scrubbed once in a 24 hour period. When set to Extended Mode, the entire memory array will be scrubbed more frequently to further increase system reliability. Read-only unless System Profile is set to Custom.
Legal Values	• Standard

	• Extended • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Standard if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Performance. Is set to Extended if the System Profile is set to Dense.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.MemPwrMgmt

Description	When set to Enabled, the memory can operate in Power Management Mode. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not supported on 13G+.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.MemRefreshRate

Description	The memory controller will periodically refresh the data in memory. The frequency at which memory is normally refreshed is referred to as 1X refresh rate. When memory modules are operating at a higher than normal temperature or to further increase system reliability, the refresh rate can be set to 2X, but may have a negative impact on memory subsystem performance under some circumstances. Read-only unless System Profile is set to Custom.
Legal Values	• 1x • 2x
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to 1X if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Performance. Is set to 2X if the System Profile is set to Dense.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.MemVolt

Description	Sets the DIMM voltage selection. When set to Auto the system will automatically set the system voltage to the optimal setting based upon the DIMM capability and the installed DIMM population. Also enables

setting the system DIMM voltage to a higher (1.5V) setting if the DIMMs support multiple voltages and have been Auto set to a lower voltage. Read-only unless System Profile is set to Custom.

Legal Values	• AutoVolt • Volt135V • Volt15V
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.MonitorMwait

Description	Specifies whether Monitor/Mwait instructions are enabled. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Enabled for all the other System Profiles.. If the C-States are enabled, and the customer sets this field to Disabled, MonitorMWait is changed to Enabled in the next boot. For 14G - MWAIT is read-only if C-State is enabled. MWAIT is editable, only if C-State is disabled. For 15G - MWAIT is editable irrespective of whether C-State is enabled/disabled.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.OsAcpiCx

Description	This field sets the OS ACPI Cx to C2 or C3 state.
Legal Values	• OsCxC2 • OsCxC3 •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.PackageCStates

Description	This field allows enabling the package to transition to deeper C-state or limit to operational state.

Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• This attribute is only configurable through performance profiles. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.PcieAspmL1

Description	When enabled, PCIe Advanced State Power Management (ASPM) can reduce overall system power a bit while slightly reducing system performance. NOTE: Some devices may not perform properly (they may hang or cause the system to hang) when ASPM is enabled; for this reason L1 will only be enabled for validated qualified cards.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.PkgCLatNeg

Description	This field only applies to package c state latency negotiation when package C states is enabled.
Legal Values	• Disabled • Enabled •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.PowerDelivery

Description	No description information available.
Legal Values	• MaxReliability • MinPwr
Default Value	None
Write Privilege	N/A

License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.PowerSaver

Description	When set to Enabled, maximizes power savings, at the expense of performance. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.Proc1TurboCoreNum

Description	Controls the number of Turbo Boost enabled cores for processor 1. By reducing the number of cores enabled with Turbo Boost, the maximum turbo frequency on the cores with Turbo Boost may be higher. Read-only unless System Profile is set to Custom, Turbo Boost is set to Enabled and CPU Power Management is set to Maximum Performance.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to All for all the other System Profiles..
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.Proc2TurboCoreNum

Description	Controls the number of Turbo Boost enabled cores for processor 2. By reducing the number of cores enabled with Turbo Boost, the maximum turbo frequency on the cores with Turbo Boost may be higher. Read-only unless System Profile is set to Custom, Turbo Boost is set to Enabled and CPU Power Management is set to Maximum Performance.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to All for all the other System Profiles..
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.Proc3TurboCoreNum

Description	Controls the number of Turbo Boost enabled cores for processor 3. By reducing the number of cores enabled with Turbo Boost, the maximum turbo frequency on the cores with Turbo Boost may be higher. Read-only unless System Profile is set to Custom, Turbo Boost is set to Enabled and CPU Power Management is set to Maximum Performance.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to All for all the other System Profiles..
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.Proc4TurboCoreNum

Description	Controls the number of Turbo Boost enabled cores for processor 4. By reducing the number of cores enabled with Turbo Boost, the maximum turbo frequency on the cores with Turbo Boost may be higher. Read-only unless System Profile is set to Custom, Turbo Boost is set to Enabled and CPU Power Management is set to Maximum Performance.
Legal Values	• All • 1 • 2 • 4 • 6 • 8 • 10 • 12 • 14 • 16 • 18 • 20 • 22 • 24 • 26 • 28
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to All for all the other System Profiles..
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcC1E

Description	When set to Enabled, the processor is allowed to switch to minimum performance state when idle. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Enabled if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Dense. Is set to Disabled if the System Profile is set to Performance.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcCStates

Description	C States allow the processor to enter lower power states when idle. When set to Enabled (OS controlled) or when set to Autonomous (if Hardware controlled is supported), the processor can operate in all available Power States to save power, but may increase memory latency and frequency jitter. Read-only unless System Profile is set to Custom.
Legal Values	• Disabled • Enabled • Autonomous
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Enabled if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Dense. Is set to Disabled if the System Profile is set to Performance.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcPwrPerf

Description	Allows selection of CPU power management methodology. System DBPM (Demand-based Power Management) utilizes a BIOS-controlled dynamic frequency manipulation scheme to save power across a variety of utilization levels as part of the Dell Advanced Power Control (DAPC) capability. The power saving features of this option typically are greatest at mid-to-lower processor utilization levels. Maximum Performance is typically selected for performance-centric workloads where it is acceptable to consume additional power to achieve the highest possible performance for the computing environment. This mode drives processor frequency to the maximum across all cores (although idled cores can still be frequency reduced by C-state enforcement through BIOS or OS mechanisms if enabled). This mode also offers the lowest latency of the CPU Power Management Mode options, so is always preferred for latency-sensitive environments. OS DBPM is another performance-per-watt option that relies on the operating system to dynamically control individual core frequency. Both Windows and Linux can take advantage of this mode to reduce frequency of idled or underutilized cores in order to save power. System DBPM (Telco) is available only when Telco Workload Profiles are selected, and which sets Hardware P-States to Native with No Legacy and EPP to disable. Read-only unless System Profile is set to Custom.
Legal Values	• MaxPerf • SysDbpm • OsDbpm • SysDbpmTelco
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcTurboMode

Description	Governs the Intel Turbo Boost Technology. This feature allows the processor cores to be automatically clocked up in frequency beyond the advertised processor speed. The amount of increased frequency (or turbo upside) one can expect from a Xeon processor depends on the processor model, thermal limitations of the operating environment, and in some cases power consumption. In general terms, the fewer cores being exercised with work the higher the potential turbo upside. The potential drawbacks for Turbo Boost are mainly centered on increased power consumption and possible frequency jitter than can affect a small minority of latency-sensitive environments. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Enabled if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Performance. Is set to Disabled if the System Profile is set to Dense.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcessorApsRocketing

Description	Enable/Disable the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcessorC1AutoDemotion

Description	No description information available.
Legal Values	• Disabled • Enabled •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcessorC1AutoUnDemotion

Description	This field when enabled allows the CPU to automatically undemoted from demoted C1 state.
Legal Values	• Disabled • Enabled •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcessorEist

Description	This field enables or disables Processor EIST.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcessorGpssTimer

Description	This field allows the reduction of GPSS timer to be set from 0-500us (typical=500us)
Legal Values	• 0us • 50us • 500us
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• This attribute is only configurable through performance profiles. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.ProcessorScalability

Description	Enable/Disable Core Performance to Frequency Scalability Based Optimizations in the CPU.
Legal Values	• Enabled • Disabled

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	To be updated
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.PwrPerfSwitch

Description	Dynamic Load Line Switch control Dynamic Link Library (DLL) is a Power Management feature, which dynamically switches to the performance mode during periods of high CPU utilization. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available when System Profile is set to Custom.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.SysProfile

Description	Allows optimizing the system for a specific profile, which presets multiple sub-options, or customizing the individual sub-options. When set to a mode other than Custom, BIOS will set each option accordingly. When set to Custom, you can change setting of each sub-option. Performance Per Watt (DAPC) represents an excellent mix of performance balanced with power consumption reduction. Dell Active Power Control (or DAPC) relies on a BIOS-centric power control mechanism which offers excellent power efficiency advantages with minimal performance impact in most environments, and is the CPU Power Management choice for this overall System Profile. Performance-per-watt (OS), otherwise known as OS Control, is similar to the DAPC profile for all sub-options except for the CPU Power Management. The power management scheme used for this profile is called OS DBPM, which allows the Operating System to manipulate processor frequencies for higher power efficiency. However, the effectiveness of this profile for reducing overall system power consumption is based on how well the Operating System is able to effectively control hardware resources, so the impacts are mixed across all supported Operating Systems Performance profile provides potentially increased performance by maximizing processor frequency and disabling certain power saving features such as C-states. Although not optimal for all environments, this is an excellent starting point for performance optimization baseline comparisons. Dense Configuration enhances reliability features and reduces power consumption at the cost of considerable performance. This profile is targeted for operating environments where enhanced reliability is desired and temperatures may exceed the thresholds encountered in less densely-packed data centers. When set to Dense Configuration mode, Memory Performance is set one speed lower than the Maximum Frequency to improve reliability. Under Custom mode when C states are enabled, Monitor/Mwait must also be enabled.
Legal Values	• PerfPerWattOptimizedOs • PerfPerWattOptimizedDapc • PerfOptimized • Custom • DenseCfgOptimized • PerfOptimizedHwp • PerfWorkStationOptimized
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	Value-class systems do not support DAPC option.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.UncoreFrequency

Description	Selects the Processor Uncore Frequency. Dynamic mode allows processor to optimize power resources across the cores and uncore during runtime. The optimization of the uncore frequency to either save power or optimize performance is influenced by the setting of the Energy Efficiency Policy. Set Dynamic Optimized mode for possible power savings minimizing performance loss. Read-only unless System Profile is set to Custom.
Legal Values	• DynamicUFS • MaxUFS • OptimizedUFS
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Dynamic if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), or Dense. Is set to Maximum if the System Profile is set to Performance. Only applicable on Intel-based platforms.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.WorkloadConfiguration

Description	This field controls the energy performance BIAS settings to allow BIOS to choose a configuration that improve performance on certain workload.
Legal Values	• Balance • IoSensitive •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• This attribute is only configurable through performance profiles. • To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.WorkloadProfile

Description	Allows optimization of performance based on the workload type. The WorkloadProfile setting is not a state. Setting a workload profile is a one-time action that in turns modifies various BIOS settings to be optimized for the requested workload type.
Legal Values	• NotConfigured

- HpcProfile
- LowLatencyOptimizedProfile
- VtOptimizedProfile
- VtPerWattOptimizedProfile
- DbOptimizedProfile
- DbPerWattOptimizedProfile
- SdsOptimizedProfile
- SdsPerWattOptimizedProfile
- TelcoOptimizedProfile
- NfviFpOptimizedTurboProfile
- NfviFpEngBalTP

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This field is not displayed in the Hii GUI. It can only updated using external tools such as RACADM.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.WorkloadProfileHelper

Description	No description information available.
Legal Values	• NotConfigured • HpcProfile • LowLatencyOptimizedProfile • VtOptimizedProfile • VtPerWattOptimizedProfile • DbOptimizedProfile • DbPerWattOptimizedProfile • SdsOptimizedProfile • SdsPerWattOptimizedProfile • TelcoOptimizedProfile
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysProfileSettings.WriteDataCrc

Description	When set to Enabled, DDR4 data bus faults are detected and corrected during write operations. Two additional cycles are required for CRC bit generation which results in performance impact. Read-only unless System Profile is set to Custom.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	Has a dependency on the System Profile. Can only be set if the System Profile is set to Custom. Is set to Disabled if the System Profile is set to Performance Per Watt (DAPC), Performance Per Watt (OS), Performance Per Watt (HWPM), Performance, or Dense. This feature is available on Broadwell processors only.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.SysSecurity.EnableTdxSeamlr

Description	Enable TDX SEAM loader.
Legal Values	• EnableTdxSeamlr
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Applicable only to Intel platforms starting from 16G EMR.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.AcPwrRcvry

Description	Specifies how the system reacts after AC power has been restored to the system. It is especially useful when systems are turned off with a power strip. When set to Off, the system stays off after AC power is restored. When set to On, the system turns on after AC power is restored. When set to Last, the system turns on if the system was on at the moment when AC power was lost. The system will remain off if the system was turned off when AC power was lost. In case of an ungraceful shutdown, the system always turns on.
Legal Values	• On • Off • Last
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.AcPwrRcvryDelay

Description	Allows staggering of power up after AC power is restored to the system. When set to Immediate, there is no delay for power-up. When set to Random, the system creates a random delay for power-up. When set to User Defined, the system delays power-up by that amount. The system supported user defined power-up delay is defined by the User Defined Delay field.

Legal Values	• Immediate • User • Random
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not supported on blades.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.AcPwrRcvryUserDelay

Description	Controls the duration for which the power-on process is delayed after the AC power supply is restored. The value is only effective if AC Power Recovery Delay is set to User Defined. The valid range is between 60s and 240s.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not supported on blades.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.AesNi

Description	Indicates the status of the Intel Processor AES-NI feature. AES-NI improves the speed of applications by performing encryption and decryption using the Advanced Encryption Standard Instruction Set.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.AuthorizeDeviceFirmware

Description	When set to Enabled, this field adds the SHA-256 hash of each third-party device firmware to the Secure Boot Authorized Signature Database. After the hashes are added, the field automatically reverts to Disabled. Note: This field is read-only unless Secure Boot is Enabled and Secure Boot Policy is Custom. This field is available only in secure system management consoles.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.BiosUpdateControl

Description	When set to Unlocked, all BIOS update will be allowed. When set to Limited, local BIOS updates from DOS or UEFI shell based flash utilities, or from Lifecycle Controller User Interface are prohibited. Limited is recommended for environments that do not require local BIOS updates. These environments include Remote Enablement Update or executing Update Package from the OS.
Legal Values	• Unlocked • Limited • Locked
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.BootmanagerPassword

Description	Bootmanager password option is available only when Setup Password is enabled. If set to Always, setup password must be entered for accessing Boot Manager. If set to Never, setup password need not be entered for accessing Boot Manager, One-shot UEFI Boot Menu.
Legal Values	• Always • Never
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.DfxTdxDisable1MbCmrExclude

Description	Disable TDX excluding CMR below 1MB
Legal Values	• DfxTdxDisable1MbCmrExclude
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Applicable only to Intel platforms starting from 16G EMR
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.EnableTdx

Description	Enable Intel TDX
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Applicable only to Intel platforms starting from 16G EMR
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.EnableTmeBypass

Description	Allows to bypass the Intel Total Memory Encryption.
Legal Values	• EnableTmeBypass
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.GlbMemIntegrity

Description	Enable/Disable Intel Global Memory Integrity.
Legal Values	GlbMemIntegrity
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	This attribute is applicable to INTEL only and 16G SPR onwards.
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.InBandManageabilityInterface

Description	When set to Disabled, this setting will hide the Management Engines (ME) HECI devices and the systems IPMI devices from the operating system. This prevents the operating system from changing the ME power capping settings, and blocks access too all in-band management tools. All management must be managed via out-of-band. Note: BIOS update requires HECI devices to be operational and DUP updates require IPMI interface to be operational. This setting needs to be set to Enabled to avoid update errors. Note: ePSA requires the IPMI interface to be functional for certain features. Disabling this setting will also cause ePSA to not be fully functional.
Legal Values	- Enabled - Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.InFieldScan

Description	The Intel(R) In-field Scan feature allows software to scan processor cores for latent faults. The scan can be performed in the field after the server is deployed. When this setting is enabled, the BIOS configures all processors to respond to software scan requests. When this setting is disabled, the processors will not respond to software scan requests.
Legal Values	Enabled

	Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.IntelSgx

Description	Allows enabling or disabling of the Intel Software Guard Extension (SGX) Technology. When set to Off, BIOS disables the SGX technology. When set to On, BIOS enables the SGX technology. When set to Software, allows application to enable the SGX technology.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Intel only attribute
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.IntelTxt

Description	Allows enabling or disabling of the Intel Trusted Execution Technology (TXT). To enable Intel TXT, Virtualization Technology must be enabled, TPM Security must be set to On with Pre-boot Measurements, and TPM Status must be Enabled, Activated. When using TPM2, the hash algorithm must be set to SHA256.
Legal Values	- On - Off
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.KeySplit

Description	Designate the num of bits for TDX, rest will be used by TME-MK
Legal Values	• KeySplit
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Applicable only to Intel platforms starting from 16G EMR
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.MemoryEncryption

Description	Allows enabling or disabling of the Intel Total Memory Encryption and Multi-Tenant (Intel TME-MT). When set to Disable, BIOS disables both TME and TME-MT technology. When set to Single Key, BIOS enables the TME technology. When set to Multiple Keys, BIOS enables the TME-MT technology. The TME-MT can be enabled only if Processor Settings -> CPU Physical Address Limit is disabled.
Legal Values	• MEM_ENC_SINGLE_KEY • MEM_ENC_OFF •
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Applicable only to Intel, and CPU supported

BIOS.SysSecurity.NewSetupPassword

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.NewSysPassword

Description	No description information available.

Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.NmiButton

Description	Allows enabling or disabling of the NMI button on the front panel.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Not supported on blades.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.OldSetupPassword

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.OldSysPassword

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.PasswordStatus

Description	When set to Unlocked the system password can be changed without entering the setup password. This allows an administrator to maintain a setup password to protect against unauthorized BIOS Setup changes, while a user can freely change the system password. When set to Locked, the setup password must be entered to change the system password. To prevent the system password from being modified without providing the setup password, set this option to Locked and enable the setup password.
Legal Values	- Locked - Unlocked
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.PwrButton

Description	Allows enabling or disabling of the power button on the front panel.
Legal Values	- Enabled - Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SHA256SetupPassword

Description	SHA256 hash of the setup password.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SHA256SetupPasswordSalt

Description	Salt for hash of the setup password.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SHA256SystemPassword

Description	SHA256 hash of the system password.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SHA256SystemPasswordSalt

Description	Salt for hash of the system password.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SecureBoot

Description	Allows enabling of Secure Boot, where the BIOS authenticates each component that is executed during the boot process using the certificates in the Secure Boot Policy. The following components are validated in the boot process: - UEFI drivers that are loaded from PCIe cards - UEFI drivers and executables from mass storage devices - Operating system boot loaders Note: Secure Boot is not available unless the Boot Mode (in the Boot Settings menu) is set to UEFI. Note: Secure Boot is not available unless the Load Legacy Video Option ROM setting (in the Miscellaneous Settings menu) is disabled. Note: You should create a setup password if you enable Secure Boot.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	N/A
Dependency	When the value of SecureBootMode is DeployedMode AND the value of SecureBoot is Enabled, BIOS will append a ProgReadOnlyLocal modifier to SecureBoot, SecureBootPolicy, and SecureBootMode. This means that inband system management tools will not allow users to change these attributes when these conditions are true.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SecureBootMode

Description	This field configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx). In Setup Mode and Audit Mode, PK is not present, and BIOS does not authenticate programmatic updates to the policy objects. In User Mode and Deployed Mode, PK is present, and BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode is the most secure mode. Use Setup, Audit, or User Mode when provisioning the system, then use Deployed Mode for normal operation. Available mode transitions depend on the current mode and PK presence. Refer to Figure 77 in the UEFI 2.6 specification for more information on transitions between the four modes. In Audit Mode, the BIOS performs signature verification on pre-boot images and logs results in the Image Execution Information Table, but executes the images whether they pass or fail verification. Audit Mode is useful for programmatically determining a working set of policy objects.
Legal Values	• SetupMode • UserMode • AuditMode • DeployedMode
Default Value	DeployedMode
Write Privilege	N/A
License Required	N/A

Dependency	When the value of SecureBootMode is DeployedMode AND the value of SecureBoot is Enabled, BIOS will append a ProgReadOnlyLocal modifier to SecureBoot, SecureBootPolicy, and SecureBootMode. This means that inband system management tools will not allow users to change these attributes when these conditions are true. This attribute is always read-write in BIOS Setup and in out-of-band system management tools.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SecureBootPolicy

Description	Allows selecting the Secure Boot Policy. When set to Standard, the BIOS uses the key and certificates from the system manufacturer to authenticate pre-boot images. When set to Linux(R) Boot, VMware(R) Boot, or Microsoft(R) Boot, the Secure Boot Policy includes only certificates necessary for the corresponding operating system. When set to Custom, the BIOS uses the user-customized key and certificates. Note: If Custom mode is selected, the Secure Boot Custom Policy Settings menu is displayed. Note: Changing the default security certificates may cause the system to fail booting from certain boot options.
Legal Values	• Standard • Custom • LinuxBoot • VmwareBoot • MicrosoftBoot
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	When the value of SecureBootMode is DeployedMode AND the value of SecureBoot is Enabled, BIOS will append a ProgReadOnlyLocal modifier to SecureBoot, SecureBootPolicy, and SecureBootMode. This means that inband system management tools will not allow users to change these attributes when these conditions are true.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SetupPassword

Description	The setup password is the password that must be entered to change any BIOS settings. However, the system password can be changed without entering the correct setup password if Password Status is set to Unlocked. The password is read-only if the password jumper (PWRD_EN) is not installed in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

- After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SignedFirmwareUpdate

Description	When set to Enabled, this option supports the signed BIOS update feature. Warning! Once enabled, this option cannot be disabled. Note: When change the item from disabled to enabled, there will pup-up a Warning message: WARNING: This option enables the signed BIOS update feature. Once enabled, the BIOS will no longer support rollbacks to an unsigned image.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SmmSecurityMitigation

Description	This option enables or disables additional UEFI SMM Security Mitigation protections. This option is available only in UEFI boot mode. The operating system can use this feature to help protect the secure environment created by virtualization based security. Enabling this feature provides additional UEFI SMM Security Mitigation protections. However, this feature may cause compatibility issues or loss of functionality with some legacy tools or applications.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available on [Intel 15g], [$\geq$ Intel 16G & AMD 16G platforms] "Disabled If(BootMode=Bios)" "Suppress If(BootMode=Bios)"
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.StrongPassword

Description	If enabled, you must set up a password that has at least one character in lowercase, uppercase, digit, and a special character. Also, you have the option to set the minimum number of characters in both the new passwords. If disabled, you can set a password that has any character in it but the passwords must not have more than 32 characters. Changes made by enabling or disabling this feature become immediately effective.
Legal Values	• Enabled

	Disabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available on (15G-Yeti) XR12 and all 16G platforms
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.StrongPasswordMinLength

Description	Controls the minimum number of characters used when setting a system or setup password. You can specify 8-32 characters.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Only available on (15G-Yeti) XR12 and all 16G platforms
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.SysPassword

Description	The system password is the password that must be entered to allow the system to boot to an operating system. The password is read-only if the password jumper (PWRD_EN) is not installed in the system.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. - After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TcmActivation

Description	Indicates the operational state of the Trusted Cryptography Module (TCM). When set to Activate, the TCM will be enabled and activated. When set to Deactivate, the TCM will be disabled and deactivated. When set to No Change, the operational state of the TCM remains unaltered. This field is read-only when TCM Security is set to Off.

Legal Values	• NoChange • Activate • Deactivate
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TcmClear

Description	WARNING: Clearing the Trusted Cryptography Module (TCM) will clear all keys in the TCM. This could affect booting to the Operating System (OS). When set to Yes, all the contents of the TCM will be cleared. This field is Read-Only when TCM Security is set to Off.
Legal Values	• Yes • No
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TcmSecurity

Description	Controls the reporting of the Trusted Cryptography Module (TCM) in the system. When set to Off, presence of the TCM is not reported to the Operating System (OS). When set to On, presence of the TCM is reported to the OS.
Legal Values	• Off • On
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.Tpm2Hierarchy

Description	Allows enabling, disabling, or clearing the storage and endorsement hierarchies. When set to Enabled, the storage and endorsement hierarchies can be used. When set to Disabled, the storage and endorsement hierarchies cannot be used. When set to Clear, the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled.
Legal Values	• Enabled • Disabled • Clear
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	Requires TPM2 hardware to be installed and TPM Security set to On.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmActivation

Description	This field allows changing the operational state of the Trusted Platform Module (TPM). When set to Activate, the TPM will be enabled and activated. When set to Deactivate, the TPM will be disabled and deactivated. When set to No Change, the operational state of the TPM remains unaltered. This field is Read-Only when TPM Security is set to Off.
Legal Values	• NoChange • Activate • Deactivate
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmClear

Description	WARNING: Clearing the Trusted Platform Module (TPM) will cause loss of all keys in the TPM. This could affect booting to the Operating System (OS). When set to Yes, all the contents of the TPM will be cleared. This field is read-only when TPM Security is set to Off.
Legal Values	• Yes • No
Default Value	None
Write Privilege	N/A
License Required	N/A

Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmCommand

Description	Controls the Trusted Platform Module (TPM). When set to None, no command is sent to the TPM. When set to Activate, the TPM will be enabled and activated. When set to Deactivate, the TPM will be disabled and deactivated. When set to Clear, all the contents of the TPM will be cleared. WARNING: Clearing the TPM will result in losing all keys in the TPM. This could affect booting to the OS. This field is read-only when TPM Security is set to Off. The action requires an additional reboot before it can take effect.
Legal Values	• None • Activate • Deactivate • Clear
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmFirmware

Description	Indicates the firmware version of the Trusted Platform Module (TPM).
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmInfo

Description	Indicates the type of Trusted Platform Module, if present.
Legal Values	String of ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmSecurity

Description	Controls the reporting of the Trusted Platform Module (TPM) in the system. When set to Off, presence of the TPM is not reported to the Operating System (OS). When set to On with Pre-boot Measurements, BIOS will store Trusted Computing Group (TCG) compliant measurements to the TPM during POST. When set to On without Pre-boot Measurements, BIOS will bypass most pre-boot measurements. When set to On, presence of the TPM is reported to the OS and available for use.
Legal Values	• Off • OnPbm • OnNoPbm • On
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	TPM 1.2 hardware - Off, OnPbm, OnNoPbm TPM 2.0 hardware - Off, On
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.TpmStatus

Description	Displays the current status of the Trusted Platform Module (TPM), and is applicable only for TPM 1.2. If the TPM is not present or TPM Security is set to Off, the value is set to Unknown.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.UefiCaCertScope

Description	This field specifies how Secure Boot uses the UEFI CA certificate in the Authorized Signature Database (db). When this field is set to Device Firmware and OS, Secure Boot will apply the UEFI CA certificate to all images, including device firmware, operating system loaders, and UEFI applications. When this field is set to Device Firmware, Secure Boot will apply the UEFI CA certificate only to device boot firmware, such as UEFI drivers for RAID or NIC devices. In this case, operating system loaders and UEFI applications will not execute if they are signed only by the UEFI CA key, even though the UEFI CA certificate is in db. This field is configurable only when the Secure Boot Policy is Custom. Otherwise, the value of this field is selected automatically based on the Secure Boot Policy setting.
Legal Values	• DeviceFirmwareAndOs • DeviceFirmware
Default Value	DeviceFirmwareAndOs
Write Privilege	N/A
License Required	N/A
Dependency	Read-only if SecureBootPolicy is not Custom.
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.SysSecurity.UefiVariableAccess

Description	Provides varying degrees of securing UEFI variables. When set to Standard, UEFI variables are accessible and can be modified in the Operating System (OS) per the UEFI specification. When set to Controlled, select UEFI variables are protected and cannot be modified in an OS environment. New UEFI boot entries are forced to be at the end of the current boot order.
Legal Values	• Standard • Controlled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	• To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list. • After modifying the IntelTxt attribute value, the pending flag is enabled for the dependent attributes such as TpmActivation, TpmClear, and TpmSecurity.

BIOS.TpmAdvancedSettings.Tpm2Algorithm

Description	Allows the user to change the cryptographic algorithms used in the Trusted Platform Module (TPM). The available options are dependent on the TPM firmware. To enable TPM2 Algorithm Selection, Intel(R) TXT technology must be disabled.
Legal Values	• SHA1 • SHA256 • SHA384 • SHA512

	• SM3
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	To enable TPM2 Algorithm Selection, Intel(R) TXT technology must be disabled.
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.TpmAdvancedSettings.TpmPpiBypassClear

Description	When set to Enabled, allows the Operating System to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) clear operations.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.TpmAdvancedSettings.TpmPpiBypassProvision

Description	When set to Enabled, allows the Operating System to bypass Physical Presence Interface (PPI) prompts when issuing PPI Advanced Configuration and Power Interface (ACPI) provisioning operations.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeq

Description	This field controls the UEFI boot order. The first option in the list will be attempted first, and if unsuccessful, the second option will be attempted and so on. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None

Notes

- FQDD level options are available for configuring the boot sequence. Multiple UEFI boot options using the same hardware display the same FQDD device for each option.
- To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis1

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis10

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis11

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis12

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis13

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis14

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis15

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis16

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis17

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis18

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis19

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis2

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis20

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis3

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.

Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis4

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis5

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis6

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis7

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis8

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiBootSeqEnDis9

Description	This field enables or disables this boot option in the UEFI Boot Sequence. The system will attempt to launch enabled boot options only; it will not launch disabled boot options. This field applies only when Boot Mode is UEFI; it has no effect when Boot Mode is BIOS.
Legal Values	No information available.
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

BIOS.UefiBootSettings.UefiPxelpVersion

Description	This field enables you to select IPv4 PXE booting (default) or IPv6 PXE booting when in UEFI Boot Mode. This field is disabled in BIOS Boot Mode. Changing this field will cause the PXE options in the UEFI Boot Sequence to be replaced on the next reboot.
Legal Values	IPv4

	• IPv6
Default Value	None
Write Privilege	N/A
License Required	N/A
Dependency	None
Notes	To check if a BIOS attribute is Read Only or Read and Write, perform GET on URI redfish/v1/Systems/System.Embedded.1/Bios/BiosRegistry and find the attribute in the Attributes list.

FC Attributes

FC.FCDevice.BusDeviceFunction (Read Only)

Description	Indicates the PCI Address of the Physical Function assigned to the port.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCDevice.ChipMdl (Read Only)

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCDevice.EFIVersion (Read Only)

Description	No description information available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCDevice.FamilyVersion (Read Only)

Description	No description information available.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCDevice.PCIDeviceID (Read Only)

Description	No description information available.
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCTarget.BootScanSelection (Read or Write)

Description	Specifies the adapter initiator behavior for booting the system from specified Fibre Channel boot target(s) or fabric discovered target(s)
Legal Values	• Disabled • Specified LUN • First LUN • First LUN 0 • First NOT LUN 0 • Fabric Discovered
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCTarget.FirstFCTargetLUN (Read or Write)

Description	Specifies the LUN (Logical Unit Number) of the first Fibre Channel boot target
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCTarget.FirstFCTargetWWPN (Read or Write)

Description	Specifies the World Wide Port Name of the first Fibre Channel boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCTarget.SecondFCTargetLUN (Read or Write)

Description	Specifies the LUN (Logical Unit Number) of the second Fibre Channel boot target
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.FCTarget.SecondFCTargetWWPN (Read or Write)

Description	Specifies the World Wide Port Name of the second Fibre Channel boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.EighthNVMeTargetNQN (Read or Write)

Description	Specify the eighth targets NVMe Qualified Name
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.EighthNVMeTargetWWNN (Read or Write)

Description	Specify the World Wide Node Name of the eighth NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.EighthNVMeTargetWWPN (Read or Write)

Description	Specify the World Wide Port Name of the eighth NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.EighthNVMeTgtCntlrID (Read or Write)

Description	Specify the Controller ID of the eighth NVMe boot target.[VENDOR: specify format of value]
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.EighthNVMeTgtConn (Read or Write)

Description	Setting to enable whether connection to the eighth NVMe Target is attempted
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.EighthNVMeTgtNSID (Read or Write)

Description	Specify the Namespace ID of the eighth NVMe boot target to access.[VENDOR: specify format of value]
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.EnableNVMeBoot (Read or Write)

Description	Specifies the ports behavior for booting the system from specified NVMe boot target(s)
Legal Values	• Disabled • Enabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FCTape (Read or Write)

Description	Specifies the state of Fibre Channel Tape support
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.FabricLoginRetryCount (Read or Write)

Description	Specifies the number of times the initiator will attempt to login to devices on the Storage Area Network
Legal Values	Integer values.
Default Value	3
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.FabricLoginTimeout (Read or Write)

Description	Specifies the time in milliseconds that the initiator waits before it tries to login to the Fibre Channel Storage Area Network Fabric again
Legal Values	Integer values from 1 to 255000.
Default Value	3000
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.FifthNVMeTargetNQN (Read or Write)

Description	Specify the fifth targets NVMe Qualified Name
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FifthNVMeTargetWWNN (Read or Write)

Description	Specify the World Wide Node Name of the fifth NVMe boot target

Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FifthNVMeTargetWWPN (Read or Write)

Description	Specify the World Wide Port Name of the fifth NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FifthNVMeTgtCntlID (Read or Write)

Description	Specify the Controller ID of the fifth NVMe boot target.[VENDOR: specify format of value]
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FifthNVMeTgtConn (Read or Write)

Description	Setting to enable whether connection to the fifth NVMe Target is attempted
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FifthNVMeTgtNSID (Read or Write)

Description	Specify the Namespace ID of the fifth NVMe boot target to access.[VENDOR: specify format of value]
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable

Dependency None

FC.HBAConfig.FirstNVMeTargetNQN (Read or Write)

Description Specify the first targets NVMe Qualified Name
Legal Values String of up to 223 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FirstNVMeTargetWWNN (Read or Write)

Description Specify the World Wide Node Name of the first NVMe boot target
Legal Values String of up to 23 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FirstNVMeTargetWWPN (Read or Write)

Description Specify the World Wide Port Name of the first NVMe boot target
Legal Values String of up to 23 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FirstNVMeTgtCntlrID (Read or Write)

Description Specify the Controller ID of the first NVMe boot target.[VENDOR: specify format of value]
Legal Values String of up to 4 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FirstNVMeTgtConn (Read or Write)

Description Setting to enable whether connection to the first NVME target is attempted

Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FirstNVMeTgtNSID (Read or Write)

Description	Specify the Namespace ID of the first NVMe boot target to access.[VENDOR: specify format of value]
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FourthNVMeTargetNQN (Read or Write)

Description	Specify the fourth targets NVMe Qualified Name
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FourthNVMeTargetWWNN (Read or Write)

Description	Specify the World Wide Node Name of the fourth NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.FourthNVMeTargetWWPN (Read or Write)

Description	Specify the World Wide Port Name of the fourth NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable

Dependency None

FC.HBAConfig.FourthNVMeTgtCntlrlID (Read or Write)

Description Specify the Controller ID of the fourth NVMe boot target.[VENDOR: specify format of value]
Legal Values String of up to 4 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FourthNVMeTgtConn (Read or Write)

Description Setting to enable whether connection to the fourth NVMe Target is attempted
Legal Values

- Enabled
- Disabled

Default Value Disabled
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FourthNVMeTgtNSID (Read or Write)

Description Specify the Namespace ID of the fourth NVMe boot target to access.[VENDOR: specify format of value]
Legal Values String of up to 8 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.FramePayloadSize (Read or Write)

Description Specifies the maximum Fibre Channel frame payload size in bytes
Legal Values

- Auto
- 512
- 1024
- 2048
- 2112

Default Value Auto
Write Privilege N/A
License Required Express License
Dependency None

FC.HBAConfig.HardZone (Read or Write)

Description	Specifies the state of Fibre Channel hard zoning
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.HardZoneAddress (Read or Write)

Description	Specifies the Hard Zone address to be used if Fibre Channel hard zoning is enabled
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.LinkDownTimeout (Read or Write)

Description	Specifies the number of milliseconds the Fibre Channel uplink port can be offline before the system is notified that the SAN fabric connectivity is lost and the uplink port is marked as being down
Legal Values	Integer values from 1 to 255000.
Default Value	3000
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.LoopResetDelay (Read or Write)

Description	Specifies the Fibre Channel Arbitrated Loop Reset Delay for the port. After resetting the loop, the adapter firmware refrains from initiating any loop activity for the number of seconds specified in this setting
Legal Values	Integer values from 0 to 60.
Default Value	5
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.PortDownRetryCount (Read or Write)

Description	Specifies the number of times the Fibre Channel uplink port will try reconnecting to a target port before the port is marked as being down
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.PortDownTimeout (Read or Write)

Description	Specifies the timeout in milliseconds that the Fibre Channel uplink port will wait before trying to reconnect to a target device port before the port is marked as down
Legal Values	Integer values from 1 to 255000.
Default Value	3000
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.PortLoginRetryCount (Read or Write)

Description	Specifies the number of times the adapter firmware initiator will try logging into a target device port
Legal Values	Integer values.
Default Value	3
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.PortLoginTimeout (Read or Write)

Description	Specifies the timeout in milliseconds that the initiator uses when attempting to login to the target device port
Legal Values	Integer values from 1 to 255000.
Default Value	3000
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.HBAConfig.SecondNVMeTargetNQN (Read or Write)

Description	Specify the second targets NVMe Qualified Name

Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SecondNVMeTargetWWNN (Read or Write)

Description	Specify the World Wide Node Name of the second NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SecondNVMeTargetWWPN (Read or Write)

Description	Specify the World Wide Port Name of the second NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SecondNVMeTgtCntlID (Read or Write)

Description	Specify the Controller ID of the second NVMe boot target. [VENDOR: specify format of value]
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SecondNVMeTgtConn (Read or Write)

Description	Setting to enable whether connection to the second NVMe Target is attempted
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable

Dependency None

FC.HBAConfig.SecondNVMeTgtNSID (Read or Write)

Description Specify the Namespace ID of the second NVMe boot target to access

Legal Values String of up to 8 ASCII characters.

Default Value None

Write Privilege N/A

License Required Not Applicable

Dependency None

FC.HBAConfig.SeventhNVMeTargetNQN (Read or Write)

Description Specify the seventh targets NVMe Qualified Name

Legal Values String of up to 223 ASCII characters.

Default Value None

Write Privilege N/A

License Required Not Applicable

Dependency None

FC.HBAConfig.SeventhNVMeTargetWWNN (Read or Write)

Description Specify the World Wide Node Name of the seventh NVMe boot target

Legal Values String of up to 23 ASCII characters.

Default Value None

Write Privilege N/A

License Required Not Applicable

Dependency None

FC.HBAConfig.SeventhNVMeTargetWWPN (Read or Write)

Description Specify the World Wide Port Name of the seventh NVMe boot target

Legal Values String of up to 23 ASCII characters.

Default Value None

Write Privilege N/A

License Required Not Applicable

Dependency None

FC.HBAConfig.SeventhNVMeTgtCntlrID (Read or Write)

Description	Specify the Controller ID of the seventh NVMe boot target.[VENDOR: specify format of value]
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SeventhNVMeTgtConn (Read or Write)

Description	Setting to enable whether connection to the seventh NVMe Target is attempted
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SeventhNVMeTgtNSID (Read or Write)

Description	Specify the Namespace ID of the seventh NVMe boot target to access.[VENDOR: specify format of value]
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SixthNVMeTargetNQN (Read or Write)

Description	Specify the sixth targets NVMe Qualified Name
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SixthNVMeTargetWWNN (Read or Write)

Description	Specify the World Wide Node Name of the sixth NVMe boot target

Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SixthNVMeTargetWWPN (Read or Write)

Description	Specify the World Wide Port Name of the sixth NVMe boot target
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SixthNVMeTgtCntlID (Read or Write)

Description	Specify the Controller ID of the sixth NVMe boot target.[VENDOR: specify format of value]
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SixthNVMeTgtConn (Read or Write)

Description	Setting to enable whether connection to the sixth NVMe Target is attempted
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.SixthNVMeTgtNSID (Read or Write)

Description	Specify the Namespace ID of the sixth NVMe boot target to access.[VENDOR: specify format of value]
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable

Dependency None

FC.HBAConfig.ThirdNVMeTargetNQN (Read or Write)

Description Specify the third targets NVMe Qualified Name
Legal Values String of up to 223 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.ThirdNVMeTargetWWNN (Read or Write)

Description Specify the World Wide Node Name of the third NVMe boot target
Legal Values String of up to 23 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.ThirdNVMeTargetWWPN (Read or Write)

Description Specify the World Wide Port Name of the third NVMe boot target
Legal Values String of up to 23 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.ThirdNVMeTgtCntlrID (Read or Write)

Description Specify the Controller ID of the third NVMe boot target.[VENDOR: specify format of value]
Legal Values String of up to 4 ASCII characters.
Default Value None
Write Privilege N/A
License Required Not Applicable
Dependency None

FC.HBAConfig.ThirdNVMeTgtConn (Read or Write)

Description Setting to enable whether connection to the third NVMe Target is attempted

Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.HBAConfig.ThirdNVMeTgtNSID (Read or Write)

Description	Specify the Namespace ID of the third NVMe boot target to access.[VENDOR: specify format of value]
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

FC.PortConfig.DeviceName (Read Only)

Description	Product name of the Fibre Channel Host Bus Adapter.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.PortConfig.PortNumber (Read Only)

Description	The Fibre Channel Host Bus Adapter port number as labeled externally on the adapter.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.PortConfig.PortSpeed (Read or Write)

Description	Specifies the data rate of the Fibre Channel Host Bus Adapter port. Value can be Automatic or specified in Gbps.
Legal Values	• Auto • 1 Gbps • 2 Gbps • 4 Gbps

- 8 Gbps
- 16 Gbps
- 32 Gbps

Default Value	Auto
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.PortConfig.VirtualWWN (Read or Write)

Description	Virtual Fibre Channel World Wide Node Name is used instead of the permanent World Wide Node Name when its value is different
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.PortConfig.VirtualWWPN (Read or Write)

Description	Virtual Fibre Channel World Wide Port Name of the port is used instead of the permanent World Wide Port Name when its value is different
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.PortConfig.WWN (Read Only)

Description	Permanent Fibre Channel World Wide Node Name assigned during manufacturing.
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

FC.PortConfig.WWPN (Read Only)

Description	Permanent Fibre Channel World Wide Port Name assigned to the port during manufacturing
Legal Values	String of up to 23 ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	Express License
Dependency	None

IDRAC Attributes

iDRAC.8021XSecurity.ClientCertificateType (Read or Write)

Display Name	Client Certificate Type
Description	Client Certificate Type
Legal Values	• DefaultIDEVID - 0 • SigningLDEVID - 1 • CustomLDEVID - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.8021XSecurity.MacSecActive (Read Only)

Display Name	MACSec Session Active
Description	MACSec Session Active
Legal Values	• No - 0 • Yes - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.8021XSecurity.MacSecCapable (Read or Write)

Display Name	MACSec Capable
Description	MACSec Capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None

Is Platform Dependent	No

iDRAC.8021XSecurity.Use8021XSecurity (Read or Write)

Display Name	Use802.1X Security
Description	Use 802.1X Security
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	Yes

iDRAC.8021XSecurity.ValidateAuthenticationServerCertificate (Read or Write)

Display Name	Validate Authentication Server Certificate
Description	Validate Authentication Server Certificate
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.ACME.CA-URL (Read or Write)

Display Name	CA URL
Description	Specifies the URL of the Certificate Authority.
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.ACME.Enable (Read or Write)

Display Name	Enable
Description	Enables or disables Automated Certificate Management Environment.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.ACME.EnrollmentAction (Read or Write)

Display Name	Enrollment Action
Description	Enrollment Actions
Legal Values	• Halt - 0 • Monitor - 1 • Enroll - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.ACME.EnrollmentStatus (Read Only)

Display Name	Enrollment Status
Description	Provides the enrollment status.
Legal Values	• None - 0 • Enrolling - 1 • Enrolled - 2 • Error - 3
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.ADGroup.Domain (Read or Write)

Display Name	AD Group Domain
Description	Active Directory Domain in which the Role Group resides.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ADGroup.Name (Read or Write)

Display Name	AD Role Group Name
Description	Name of the Role Group as recorded in the Active Directory forest.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ADGroup.Privilege (Read or Write)

Display Name	AD Group Privilege
Description	Role-based authority privileges for a Role Group
Legal Values	Integer values from 0 to 511.
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ASRConfig.Enable (Read or Write)

Display Name	Enable
Description	Status of ASR Config
Legal Values	• Disabled - 0 • Enabled - 1

Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveBezelFilter.FilterCheckIntervalDay (Read or Write)

Display Name	Filter Check Interval Day
Description	Active mode starting day. This is applicable to XR-series platforms only.
Legal Values	• Sunday - 0 • Monday - 1 • Tuesday - 2 • Wednesday - 3 • Thursday - 4 • Friday - 5 • Saturday - 6
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveBezelFilter.FilterCheckIntervalTimeHour (Read or Write)

Display Name	Filter Check Interval Time Hour
Description	Active mode starting Hour. This is applicable to XR-series platforms only.
Legal Values	Integer values from 0 to 23.
Default Value	3
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveBezelFilter.FilterMode (Read or Write)

Display Name	Filter Mode
Description	Air Filter Monitoring Modes. This is applicable to XR-series platforms only.

Legal Values	• CountdownMode - 0 • ActiveSensingMode - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.ActiveDirectory.AuthTimeout (Read or Write)

Display Name	Active Directory Authentication Timeout
Description	Specifies the number of seconds to wait for Active Directory authentication requests to complete before timing out.
Legal Values	Integer values from 15 to 300.
Default Value	120
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.CertValidationEnable (Read or Write)

Display Name	Certificate Validation Enable
Description	Enables or disables Active Directory certificate validation as a part of the Active Directory configuration process.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.Connection (Read or Write)

Display Name	Active Directory Connection
Description	Selects Active Directory connection protocol
Legal Values	• StartTLS - 0 • LDAPS - 1

Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.DCLookupByUserDomain (Read or Write)

Display Name	Domain Controller Lookup By User Domain
Description	Chooses the way the user domain is looked up for Active Directory.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	Cannot be Disabled unless DC Lookup Domain Name is set
Is Platform Dependent	No

iDRAC.ActiveDirectory.DCLookupDomainName (Read or Write)

Display Name	Active Directory Lookup Domain Name
Description	This is the configured search domain to use when DCLookupByUserDomain is disabled
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.DCLookupEnable (Read or Write)

Display Name	Domain Controller Lookup Enable
Description	Configures iDRAC to use pre-configured domain controllers or to use DNS to find the domain controller.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users

License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.DomainController1 (Read or Write)

Display Name	Domain Controller 1
Description	Specifies the LDAP server from which you want the iDRAC to obtain user names
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.DomainController2 (Read or Write)

Display Name	Domain Controller 2
Description	Specifies the LDAP server from which you want the iDRAC to obtain user names
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.DomainController3 (Read or Write)

Display Name	Domain Controller 3
Description	Specifies the LDAP server from which you want the iDRAC to obtain user names
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.Enable (Read or Write)

Display Name	Active Directory Enable
Description	Enables or disables Active Directory user authentication on iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.GCLookupEnable (Read or Write)

Display Name	Global Catalog Server Lookup Enable
Description	Determines how the global catalog server is looked up.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.GCRootDomain (Read or Write)

Display Name	Active Directory Root Domain
Description	The name of the Active Directory root domain used for DNS look up, to locate Global Catalog servers.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.GlobalCatalog1 (Read or Write)

Display Name	Global Catalog 1
Description	Specifies the Global Catalog server from which you want the iDRAC to obtain user names.

Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.GlobalCatalog2 (Read or Write)

Display Name	Global Catalog 2
Description	Specifies the Global Catalog server from which you want the iDRAC to obtain user names.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.GlobalCatalog3 (Read or Write)

Display Name	Global Catalog 3
Description	Specifies the Global Catalog server from which you want the iDRAC to obtain user names.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.RSASecurID2FAAD (Read or Write)

Display Name	RSA SecurID 2FA AD
Description	Enables or disables RSA SecurID 2 Factor Authentication for AD users.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	LM_RSA_SECURID
Dependency	Microsoft Active Directory must be Enabled prior to setting to Enabled.

Is Platform Dependent	No

iDRAC.ActiveDirectory.RacDomain (Read or Write)

Display Name	Active Directory RAC Domain
Description	Active Directory Domain in which iDRAC resides.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.RacName (Read or Write)

Display Name	Active Directory RAC Name
Description	Name of iDRAC as recorded in the Active Directory forest.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.ActiveDirectory.SSOEnable (Read or Write)

Display Name	SSO Enable
Description	Enables or disables Active Directory single sign-on authentication on iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	Cannot be Enabled unless SmartCard Logon Enable is Disabled
Is Platform Dependent	No

iDRAC.ActiveDirectory.Schema (Read or Write)

Display Name	Active Directory Schema Type

Description	Determines the schema type to use with Active Directory.
Legal Values	• Extended Schema - 1 • Standard Schema - 2
Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.AutoOSLockGroup.AutoOSLockState (Read or Write)

Display Name	Auto OS Lock State
Description	Enable Auto OS Lock State
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Autodiscovery.EnableIPChangeAnnounce (Read or Write)

Display Name	Enable IP Change Announce
Description	Enable Auto Discovery to allow 1:many consoles to discover iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Autodiscovery.EnableIPChangeAnnounceFromDHCP (Read or Write)

Display Name	Enable IP Change Announce from DHCP

Description	Enable iDRAC to obtain list of consoles through DHCP.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Autodiscovery.EnableIPChangeAnnounceFromUnicas tDNS (Read or Write)

Display Name	Enable IP Change Announce Unicast DNS
Description	Enable iDRAC to obtain list of consoles through unicast DNS.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Autodiscovery.EnableIPChangeAnnounceFrommDNS (Read or Write)

Display Name	Enable IP Change Announce From mDNS
Description	Enable iDRAC to obtain list of consoles through mDNS
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Autodiscovery.SendTestAnnouncement (Read or Write)

Display Name	Send Test Announcement

Description	Send an IP Change announcement for debugging purposes
Legal Values	• Disabled - 0 • SendOnce - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Autodiscovery.UnsolicitedIPChangeAnnounceRate (Read or Write)

Display Name	Unsolicited IP Change Announce Rate
Description	Rate of periodic refresh of IP address to consoles
Legal Values	• Disabled - 0 • 1 hour - 1 • 6 hours - 2 • 12 hours - 3 • 1 day - 4 • 3 days - 5 • 1 week - 6 • 2 weeks - 7 • 4 weeks - 8 • 6 weeks - 9
Default Value	4
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CertificateManagement.ExpiryNotificationFrequency (Read Only)

Display Name	Expiry Notification Frequency
Description	Expiry Notification Frequency in Days
Legal Values	Integer values from 1 to 7.
Default Value	7
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CertificateManagement.ExpiryNotificationInterval (Read Only)

Display Name	Expiry Notification Interval in Days
Description	Expiry Notification Interval in Days
Legal Values	Integer values from 1 to 100.
Default Value	30
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CertificateManagement.ExpiryNotificationSupport (Read or Write)

Display Name	Expiry Notification Support
Description	Certificate Expiry Notification Support
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.Address (Read Only)

Display Name	IPv4 Address
Description	The current IPv4 address assigned to the iDRAC
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.DHCPEnable (Read Only)

Display Name	IPv4 DHCP Enable
Description	Specifies if DHCP is used to assign the iDRAC IPv4 address
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.DNS1 (Read Only)

Display Name	DNS Server 1
Description	IPv4 address for DNS server 1
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.DNS2 (Read Only)

Display Name	DNS Server 2
Description	IPv4 address for DNS Server 2
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.DNS3 (Read Only)

Display Name	DNS Server 3
Description	IPv4 address for DNS Server 3
Legal Values	String of up to 16 ASCII characters.

Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.DNSFromDHCP (Read Only)

Display Name	DNS Servers From DHCP
Description	Specifies if the DNS server IPv4 addresses should be assigned from the DHCP server on the network.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.DupAddrDetected (Read Only)

Display Name	IPv4 Address
Description	The current IPv4 address assigned to the iDRAC
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.Enable (Read Only)

Display Name	IPv4 Enable
Description	Enables or Disables the iDRAC IPv4 stack
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

iDRAC.CurrentIPv4.Gateway (Read Only)

Display Name	Gateway
Description	The gateway for the iDRAC IPv4 address
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv4.Netmask (Read Only)

Display Name	Net Mask
Description	The subnet mask used for the iDRAC IPv4 address
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address1 (Read Only)

Display Name	IPV6 Address 1
Description	iDRAC IPv6 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address10 (Read Only)

Display Name	IPV6 Address 10

Description	iDRAC IPv6 tenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address11 (Read Only)

Display Name	IPv6 Address 11
Description	iDRAC IPv6 eleventh address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address12 (Read Only)

Display Name	IPv6 Address 12
Description	iDRAC IPv6 twelfth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address13 (Read Only)

Display Name	IPv6 Address 13
Description	iDRAC IPv6 thirteenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

iDRAC.CurrentIPv6.Address14 (Read Only)

Display Name	IPv6 Address 14
Description	iDRAC IPv6 fourteenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address15 (Read Only)

Display Name	IPv6 Address 15
Description	iDRAC IPv6 fifteenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address2 (Read Only)

Display Name	IPv6 Address 2
Description	iDRAC IPv6 second address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address3 (Read Only)

Display Name	IPv6 Address 3

Description	iDRAC IPv6 third address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address4 (Read Only)

Display Name	IPV6 Address 4
Description	iDRAC IPv6 fourth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address5 (Read Only)

Display Name	IPV6 Address 5
Description	iDRAC IPv6 fifth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address6 (Read Only)

Display Name	IPV6 Address 6
Description	iDRAC IPv6 sixth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

iDRAC.CurrentIPv6.Address7 (Read Only)

Display Name	IPv6 Address 7
Description	iDRAC IPv6 seventh address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address8 (Read Only)

Display Name	IPv6 Address 8
Description	iDRAC IPv6 eighth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Address9 (Read Only)

Display Name	IPv6 Address 9
Description	iDRAC IPv6 ninth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.AddressGenerationMode (Read Only)

Display Name	IPv6 Address Generation Mode

Description	IPv6 Address Generation Mode
Legal Values	• StablePrivacy - 0 • EUI64 - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.AutoConfig (Read Only)

Display Name	IPV6 Auto Config
Description	Enables or Disables the iDRAC IPv6 auto configuration option
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.DHCPv6Address (Read Only)

Display Name	DHCPv6 Address
Description	Specifies the iDRAC DHCPv6 Address.
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.DNS1 (Read Only)

Display Name	IPV6 DNS Server1
Description	IPv6 DNS Server 1 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.DNS2 (Read Only)

Display Name	IPV6 DNS Server2
Description	IPv6 DNS Server 2 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.DNS3 (Read Only)

Display Name	IPV6 DNS Server3
Description	IPv6 DNS Server 3 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.DNSFromDHCP6 (Read Only)

Display Name	DNS Server From DHCP6
Description	Specifies if the DNS Server addresses are obtained from DHCP or not
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.DUID (Read Only)

Display Name	IPv6 DUID
Description	DHCP Unique Identifier
Legal Values	String of up to 144 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Enable (Read Only)

Display Name	IPV6 Enable
Description	Enables or Disables iDRAC IPv6 stack
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.Gateway (Read Only)

Display Name	IPV6 Gateway
Description	iDRAC IPv6 Gateway
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.IPV6NumOfExtAddress (Read Only)

Display Name	Total Number of Extended IP
Description	Total number of extended IP
Legal Values	Integer values from 0 to 255.

Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.LinkLocalAddress (Read Only)

Display Name	IPV6 Link Local Address
Description	iDRAC IPv6 Link Local Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentIPv6.PrefixLength (Read Only)

Display Name	IPV6 Link Local Prefix Length
Description	Prefix length for the iDRAC IPv6 Address
Legal Values	Integer values from 1 to 128.
Default Value	64
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.ActiveNIC (Read Only)

Display Name	Active NIC
Description	Currently Active iDRAC network interface
Legal Values	• None - 0 • Dedicated - 1 • LOM1 - 2 • LOM2 - 3 • LOM3 - 4 • LOM4 - 5 • LOM5 - 6 • LOM6 - 7 • LOM7 - 8

- LOM8 - 9
- LOM9 - 10
- LOM10 - 11
- LOM11 - 12
- LOM12 - 13
- LOM13 - 14
- LOM14 - 15
- LOM15 - 16
- LOM16 - 17

Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.ActiveSharedLOM (Read Only)

Display Name	Active Shared LOM
Description	Currently Active iDRAC shared network interface
Legal Values	• None - 0 • LOM1 - 1 • LOM2 - 2 • LOM3 - 3 • LOM4 - 4 • LOM5 - 5 • LOM6 - 6 • LOM7 - 7 • LOM8 - 8 • LOM9 - 9 • LOM10 - 10 • LOM11 - 11 • LOM12 - 12 • LOM13 - 13 • LOM14 - 14 • LOM15 - 15 • LOM16 - 16
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.AutoDetect (Read Only)

Display Name	Auto NIC Enable
Description	Enable or disable auto detection feature of iDRAC

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.Autoneg (Read Only)

Display Name	NIC Auto Negotiation
Description	Enables autonegotiation of physical link speed and duplex
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.CurrentNIC.DNSDomainFromDHCP (Read Only)

Display Name	DNS Domain From DHCP
Description	Specifies that the iDRAC DNS Domain Name should be assigned from the network DHCP server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.DNSDomainName (Read Only)

Display Name	DNS Domain Name
Description	The DNS Domain Name
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.DNSRacName (Read Only)

Display Name	DNS RAC Name
Description	The iDRAC name, which is iDRAC-<SVCTAG> by default
Legal Values	String of up to 63 ASCII characters.
Default Value	idrac-SVCTAG
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.DNSRegister (Read Only)

Display Name	DNS Register RAC
Description	Registers the iDRAC name with the DNS server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.DedicatedNICScanTime (Read Only)

Display Name	Shared to Dedicated Failover Timeout
Description	Shared to Dedicated Failover Timeout
Legal Values	Integer values from 5 to 255.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.Duplex (Read Only)

Display Name	NIC Duplex
Description	Specifies the duplex setting for the iDRAC NIC
Legal Values	• Half - 0 • Full - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.CurrentNIC.Enable (Read Only)

Display Name	NIC Enable
Description	Enables or Disables the iDRAC network interface controller.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.CurrentNIC.Failover (Read Only)

Display Name	NIC Failover
Description	Specifies the NIC Failover LOM
Legal Values	• None - 0 • LOM1 - 1 • LOM2 - 2 • LOM3 - 3 • LOM4 - 4 • ALL - 5
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.CurrentNIC.LinkStatus (Read Only)

Display Name	Link Status
Description	iDRAC Link Status.
Legal Values	• No - 0 • Yes - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.MACAddress (Read Only)

Display Name	MAC Address
Description	The MAC Address of the iDRAC
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.MACAddress2 (Read Only)

Display Name	MAC Address 2
Description	The MAC Address 2 of the iDRAC
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:02
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.MTU (Read Only)

Display Name	NIC Maximum Transmission Unit
Description	The size in bytes of the maximum transmission unit used by the iDRAC NIC
Legal Values	Integer values from 576 to 1500.

Default Value	1500
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.MgmtIfaceName (Read Only)

Display Name	Management Interface Name
Description	The name of the Management Network Interface
Legal Values	String of up to 11 ASCII characters.
Default Value	bond0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.NumberOfLOM (Read Only)

Display Name	Number of LOM
Description	Number of shared LOM available for iDRAC network interface
Legal Values	Integer values from 0 to 16.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.PingEnable (Read Only)

Display Name	Ping Enable
Description	Enables iDRAC to respond to pings
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.Selection (Read Only)

Display Name	NIC Selection
Description	Specifies the current mode of operation for the iDRAC network interface controller
Legal Values	• Dedicated - 1 • LOM1 - 2 • LOM2 - 3 • LOM3 - 4 • LOM4 - 5
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.CurrentNIC.SharedNICScanTime (Read Only)

Display Name	Dedicated to Shared Failover Timeout
Description	Dedicated to Shared Failover Timeout
Legal Values	Integer values from 5 to 255.
Default Value	30
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.Speed (Read Only)

Display Name	NIC Speed
Description	Specifies the speed for the iDRAC NIC
Legal Values	• 10 - 0 • 100 - 1 • 1000 - 2 • 2500 - 3 • 10000 - 4 • 20000 - 5 • 25000 - 6 • 40000 - 7 • 50000 - 8 • 100000 - 9
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	Yes

iDRAC.CurrentNIC.VLanEnable (Read Only)

Display Name	Enable VLAN
Description	Enables or Disables the VLAN capabilities of the iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.VLanID (Read Only)

Display Name	VLAN ID
Description	Specifies the VLAN ID for the network VLAN configuration
Legal Values	Integer values from 1 to 4094.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.VLanPriority (Read Only)

Display Name	VLAN Priority
Description	Specifies the VLAN priority for the network VLAN configuration
Legal Values	Integer values from 0 to 7.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.CurrentNIC.VLanSetting (Read Only)

Display Name	Auto Vlan Setting
Description	Auto VLAN Setting
Legal Values	• Both Enable - 0 • Disabled on Dedicated - 1 • Disabled on share - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.DefaultCredentialMitigationConfigGroup.DefaultCredentialMitigation (Read or Write)

Display Name	Default Credential Mitigation
Description	Enable Default Credential Mitigation
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuth.Issuer (Read or Write)

Display Name	Delegated Authentication Static Issuer
Description	Issuer string "iss" value in tokens signed by the configured static key (s)
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuth.Mode (Read or Write)

Display Name	Delegated Authentication Service Mode
Description	Mode of operation for Delegated Server instance
Legal Values	• Mixed - 0 • Discovery - 1 • Offline - 2
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuth.Name (Read or Write)

Display Name	Delegated Authentication Name tag
Description	Name tag for the Delegated authentication, used for configuration
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuth.PublicSigningKey (Read or Write)

Display Name	Delegated Authentication Static Public Signing Key
Description	The public signing key as defined in rfc7517 or a JWK set document as specified in rfc8414
Legal Values	String of up to 3071 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuth.ServerURL (Read or Write)

Display Name	Delegated Authentication Server Address
Description	The Oauth Metadata document URL of the Authorization Server

Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuth.ServiceEnabled (Read or Write)

Display Name	Delegated Authentication Service Enabled
Description	Enable or Disable this Delegated Server instance
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.DelegatedAuthConfig.JwkCacheTime (Read or Write)

Display Name	Delegated Authentication JWK Cache Time
Description	Maximum time in seconds a JWK will be cached. A value of -1 indicates that there is no cache timeout, 0 disables the cache.
Legal Values	Integer values from -1 to 604800.
Default Value	10800
Write Privilege	Configure iDRAC, Configure Users
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.EmailAlert.Address (Read or Write)

Display Name	Email Alert Address
Description	Specifies the destination email address for email alerts
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC

License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.EmailAlert.CustomMsg (Read or Write)

Display Name	Email Alert Custom Message
Description	Specifies the custom message that forms the subject of the alert
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.EmailAlert.Enable (Read or Write)

Display Name	Enable Email Alerts
Description	Enables or Disables the destination to receive alerts
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.GUI.SecurityPolicyMessage (Read or Write)

Display Name	Security Policy Message
Description	Security Policy Message Displayed on the GUI login screen
Legal Values	String of up to 1024 ASCII characters.
Default Value	By accessing this computer, you confirm that such access complies with your organization's security policy.
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.GroupManager.GroupName (Read Only)

Display Name	Group Name
Description	GroupName is the user specified name of the iDRAC Group Manager local group.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.GroupManager.GroupUUID (Read Only)

Display Name	Group UUID
Description	GroupUUID is a universally unique identifier that is automatically generated when the iDRAC Group Manager local group is created. This is used to track a group and remains constant for the life of the group.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.GroupManager.Status (Read or Write)

Display Name	Feature Status
Description	Enables or disables Group Management. iDRAC Group Manager feature offers simplified basic management of iDRACs on the same local network using the iDRAC GUI. When enabled a link local IPv6 address is used to discover and communicate with other iDRACs.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.IOIDOpt.IOIDOptEnable (Read or Write)

Display Name	IOIDOpt Enable

Description	Enable IO Identity Optimization
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IOIDOpt.InitiatorPersistencePolicy (Read or Write)

Display Name	Initiator Persistence Policy
Description	Initiator Persistence Policy
Legal Values	• None - 0 • WarmReset - 1 • ColdReset - 2 • WarmReset, ColdReset - 3 • ACPowerLoss - 4 • WarmReset, ACPowerLoss - 5 • ColdReset, ACPowerLoss - 6 • WarmReset, ColdReset, ACPowerLoss - 7
Default Value	7
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IOIDOpt.PersistencePolicyOnPartReplacement (Read or Write)

Display Name	Persistence Policy On Part Replacement
Description	No description information available.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IODOpt.StorageTargetPersistencePolicy (Read or Write)

Display Name	Storage Target Persistence Policy
Description	Storage Target Persistence Policy
Legal Values	• None - 0 • WarmReset - 1 • ColdReset - 2 • WarmReset, ColdReset - 3 • ACPowerLoss - 4 • WarmReset, ACPowerLoss - 5 • ColdReset, ACPowerLoss - 6 • WarmReset, ColdReset, ACPowerLoss - 7
Default Value	7
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IODOpt.VirtualAddressPersistencePolicyAuxPwr (Read or Write)

Display Name	Virtual Address Persistence Policy Auxiliary Powered
Description	Virtual Address Persistence Policy Auxiliary Powered
Legal Values	• None - 0 • WarmReset - 1 • ColdReset - 2 • WarmReset, ColdReset - 3 • ACPowerLoss - 4 • WarmReset, ACPowerLoss - 5 • ColdReset, ACPowerLoss - 6 • WarmReset, ColdReset, ACPowerLoss - 7
Default Value	3
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IODOpt.VirtualAddressPersistencePolicyNonAuxPwr (Read or Write)

Display Name	Virtual Address Persistence Policy Non Auxiliary Powered

Description	Virtual Address Persistence Policy Non Auxiliary Powered
Legal Values	• None - 0 • WarmReset - 1 • ColdReset - 2 • WarmReset, ColdReset - 3 • ACPowerLoss - 4 • WarmReset, ACPowerLoss - 5 • ColdReset, ACPowerLoss - 6 • WarmReset, ColdReset, ACPowerLoss - 7
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.BlockEnable (Read or Write)

Display Name	Tune IP Block Enable
Description	Enables or disables the IPv4 address blocking feature of iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.FailCount (Read or Write)

Display Name	Tune IP Fail Count
Description	Specifies the maximum number of login failures to occur within the window before login attempts from the IP address are rejected.
Legal Values	Integer values from 2 to 16.
Default Value	3
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.FailWindow (Read or Write)

Display Name	Tune IP Block Fail Window

Description	Defines the time span in seconds that the failed attempts are counted.
Legal Values	Integer values from 10 to 65535.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.PenaltyTime (Read or Write)

Display Name	Tune IP Block Penalty Time
Description	Defines the time span in seconds that session requests from an IP address with excessive failures are rejected.
Legal Values	Integer values from 2 to 65535.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeAddr (Read or Write)

Display Name	Tune IP Range Address
Description	Specifies the IPv4 address of IPv4 Address Range 1 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.1.1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeAddr2 (Read or Write)

Display Name	Tune IP Range Address 2
Description	Specifies the IPv4 address of IPv4 Address Range 2 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.1.1
Write Privilege	Configure iDRAC
License Required	Express License

Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeAddr3 (Read or Write)

Display Name	Tune IP Range Address 3
Description	Specifies the IPv4 address of IPv4 Address Range 3 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.1.1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeAddr4 (Read or Write)

Display Name	Tune IP Range Address 4
Description	Specifies the IPv4 address of IPv4 Address Range 4 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.1.1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeAddr5 (Read or Write)

Display Name	Tune IP Range Address 5
Description	Specifies the IPv4 address of IPv4 Address Range 5 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.1.1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeEnable (Read or Write)

Display Name	Tune IP Range Enable
Description	Enables or disables IPv4 Address Range 1 of the IP blocking feature of iDRAC. t
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeEnable2 (Read or Write)

Display Name	Tune IP Range Enable 2
Description	Enables or disables IPv4 Address Range 2 of the IP blocking feature of iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeEnable3 (Read or Write)

Display Name	Tune IP Range Enable 3
Description	Enables or disables IPv4 Address Range 3 of the IP blocking feature of iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeEnable4 (Read or Write)

Display Name	Tune IP Range Enable 4
Description	Enables or disables IPv4 Address Range 4 of the IP blocking feature of iDRAC.

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeEnable5 (Read or Write)

Display Name	Tune IP Range Enable 5
Description	Enables or disables IPv4 Address Range 5 of the IP blocking feature of iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeMask (Read or Write)

Display Name	Tune IP Range Mask
Description	Specifies the IPv4 subnet mask of IPv4 Address Range 1 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	255.255.255.0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPBlocking.RangeMask2 (Read or Write)

Display Name	Tune IP Range Mask 2
Description	Specifies the IPv4 subnet mask of IPv4 Address Range 2 of the IP blocking feature of iDRAC.
Legal Values	String of up to 16 ASCII characters.
Default Value	255.255.255.0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None

**Is Platform
Dependent** No

iDRAC.IPBlocking.RangeMask3 (Read or Write)

Display Name Tune IP Range Mask 3

Description Specifies the IPv4 subnet mask of IPv4 Address Range 3 of the IP blocking feature of iDRAC.

Legal Values String of up to 16 ASCII characters.

Default Value 255.255.255.0

Write Privilege Configure iDRAC

License Required Express License

Dependency None

**Is Platform
Dependent** No

iDRAC.IPBlocking.RangeMask4 (Read or Write)

Display Name Tune IP Range Mask 4

Description Specifies the IPv4 subnet mask of IPv4 Address Range 4 of the IP blocking feature of iDRAC.

Legal Values String of up to 16 ASCII characters.

Default Value 255.255.255.0

Write Privilege Configure iDRAC

License Required Express License

Dependency None

**Is Platform
Dependent** No

iDRAC.IPBlocking.RangeMask5 (Read or Write)

Display Name Tune IP Range Mask 5

Description Specifies the IPv4 subnet mask of IPv4 Address Range 5 of the IP blocking feature of iDRAC.

Legal Values String of up to 16 ASCII characters.

Default Value 255.255.255.0

Write Privilege Configure iDRAC

License Required Express License

Dependency None

**Is Platform
Dependent** No

iDRAC.IPMIIPConfig.ArpInterval (Read or Write)

Display Name Arp Interval

Description	Gratuitous ARP interval
Legal Values	String of up to 2 ASCII characters.
Default Value	03
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMIIPConfig.BackupGatewayIP (Read or Write)

Display Name	Backup Gateway IP
Description	IP address of an alternate gateway.
Legal Values	String of up to 8 ASCII characters.
Default Value	00000000
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMIIPConfig.BackupGatewayMac (Read or Write)

Display Name	Backup Gateway MAC
Description	Mac address of the alternate gateway.
Legal Values	String of up to 12 ASCII characters.
Default Value	000000000000
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMIIPConfig.DefaultGatewayMAC (Read or Write)

Display Name	Default gateway MAC
Description	Mac address of the default gateway
Legal Values	String of up to 12 ASCII characters.
Default Value	000000000000
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

iDRAC.IPMIIPConfig.IPHeader (Read or Write)

Display Name	IP Header
Description	IPMI configuration for RMCP IPV4 header parameter. Check IPMI specification for more info
Legal Values	String of up to 6 ASCII characters.
Default Value	404010
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMILan.AlertEnable (Read or Write)

Display Name	Alert Enable
Description	Enables or Disables global email alerting
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMILan.CommunityName (Read or Write)

Display Name	Community Name
Description	Specifies the SNMP community name for traps
Legal Values	String of up to 18 ASCII characters.
Default Value	public
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMILan.Enable (Read or Write)

Display Name	Enable or Disable IPMI over LAN

Description	Enables or Disables the IPMI over LAN interface
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMILan.EncryptionKey (Read or Write)

Display Name	Encryption Key
Description	Specifies the IPMI Encryption key
Legal Values	String of up to 40 ASCII characters.
Default Value	000000000000000000000000000000000000
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMILan.PrivLimit (Read or Write)

Display Name	Privilege Limit
Description	Specifies the maximum privilege level for IPMI over LAN access
Legal Values	• User - 2 • Operator - 3 • Administrator - 4
Default Value	4
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMIPEFSeldomFilter.FilterEntry (Read or Write)

Display Name	Filter Entry
Description	Attribute for FilterEntry
Legal Values	String of up to 40 ASCII characters.
Default Value	000000000000000000000000000000000000
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMIPefSeldom.GlobalControl (Read or Write)

Display Name	Global Control
Description	Global control
Legal Values	String of up to 2 ASCII characters.
Default Value	0F
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMISOL.AccumulateInterval (Read or Write)

Display Name	IPMI SOL Accumulate Interval
Description	Specifies the typical amount of time that iDRAC waits before transmitting a partial SOL character data packet
Legal Values	Integer values from 1 to 255.
Default Value	10
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMISOL.BaudRate (Read or Write)

Display Name	IPMI SOL Baud Rate
Description	Specifies the Baud rate for serial communication over LAN
Legal Values	• 9600 - 9600 • 19200 - 19200 • 57600 - 57600 • 115200 - 115200
Default Value	115200
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMISOL.Enable (Read or Write)

Display Name	IPMI SOL Enable
Description	Enables or disables Serial Over LAN (SOL)
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMISOL.MinPrivilege (Read or Write)

Display Name	IPMI SOL Min Privilege
Description	Specifies the minimum privilege level required for serial access
Legal Values	• User - 2 • Operator - 3 • Administrator - 4
Default Value	4
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMISOL.SendThreshold (Read or Write)

Display Name	IPMI SOL Send Threshold
Description	Specifies the SOL threshold limit value and the maximum number of bytes to buffer before sending an SOL data packet
Legal Values	Integer values from 1 to 255.
Default Value	255
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPMISerial.BaudRate (Read or Write)

Display Name	IPMI Serial Baud Rate

Description	Specifies the baud rate for serial connection over IPMI
Legal Values	• 9600 - 9600 • 19200 - 19200 • 57600 - 57600 • 115200 - 115200
Default Value	57600
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.ChanPrivLimit (Read or Write)

Display Name	IPMI Serial Channel Privilege Limit
Description	Specifies the maximum privilege limit allowed on the IPMI serial channel
Legal Values	• User - 2 • Operator - 3 • Administrator - 4
Default Value	4
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.ConnectionMode (Read or Write)

Display Name	IPMI Serial Connection Mode
Description	Determines the IPMI defined mode of the serial port
Legal Values	• Terminal - 0 • Basic - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.DeleteControl (Read or Write)

Display Name	IPMI Serial Delete Control
Description	Enables or Disables delete control on the IPMI serial interface
Legal Values	• Disabled - 0

	• Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.EchoControl (Read or Write)

Display Name	IPMI Serial Echo Control
Description	Enables or Disables echo control on the IPMI serial interface
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.FlowControl (Read or Write)

Display Name	IPMI Serial Flow Control
Description	Specifies the Flow Control setting for IPMI serial port
Legal Values	• None - 0 • RTS/CTS - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.HandshakeControl (Read or Write)

Display Name	IPMI Serial Handshake Control
Description	Enables or Disables the IPMI terminal mode handshake control
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.InputNewLineSeq (Read or Write)

Display Name	IPMI Serial Input New Line Sequence
Description	Specifies the input new line sequence for the IPMI serial interface
Legal Values	• Enter - 1 • Null - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.LineEdit (Read or Write)

Display Name	IPMI Serial Line Edit
Description	Enables or Disables line editing on the IPMI serial interface
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPMISerial.NewLineSeq (Read or Write)

Display Name	IPMI Serial New Line Sequence
Description	Specifies the new line sequence for the IPMI serial interface
Legal Values	• None - 0 • CR-LF - 1 • NULL - 2 • CR - 3 • LF-CR - 4 • LF - 5
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** Yes

iDRAC.IPv4.Address (Read or Write)

Display Name IPv4 Address

Description The current IPv4 address assigned to the iDRAC

Legal Values String of up to 16 ASCII characters.

Default Value 192.168.0.120

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** Yes

iDRAC.IPv4.DHCPEnable (Read or Write)

Display Name IPv4 DHCP Enable

Description Specifies if DHCP is used to assign the iDRAC IPv4 address

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 1

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** Yes

iDRAC.IPv4.DNS1 (Read or Write)

Display Name DNS Server 1

Description IPv4 address for DNS server 1

Legal Values String of up to 16 ASCII characters.

Default Value 0.0.0.0

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.IPv4.DNS2 (Read or Write)

Display Name DNS Server 2

Description	IPv4 address for DNS Server 2
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4.DNS3 (Read or Write)

Display Name	DNS Server 3
Description	IPv4 address for DNS Server 3
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4.DNSFromDHCP (Read or Write)

Display Name	DNS Servers From DHCP
Description	Specifies if the DNS server IPv4 addresses should be assigned from the DHCP server on the network.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4.Enable (Read or Write)

Display Name	IPv4 Enable
Description	Enables or Disables the iDRAC IPv4 stack
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

iDRAC.IPv4.Gateway (Read or Write)

Display Name	Gateway
Description	The gateway for the iDRAC IPv4 address
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.0.1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPv4.Netmask (Read or Write)

Display Name	Net Mask
Description	The subnet mask used for the iDRAC IPv4 address
Legal Values	String of up to 16 ASCII characters.
Default Value	255.255.255.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4Static.Address (Read or Write)

Display Name	IPv4 Address
Description	iDRAC static IPv4 address (can be configured even when DHCP is enabled)
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.0.120
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPv4Static.DNS1 (Read or Write)

Display Name	DNS Server 1
Description	Statically configurable DNS Server 1
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4Static.DNS2 (Read or Write)

Display Name	DNS Server 2
Description	Statically configurable DNS Server 2
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4Static.DNS3 (Read or Write)

Display Name	DNS Server 3
Description	Statically configurable DNS Server 3
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4Static.DNSFromDHCP (Read or Write)

Display Name	DNS Servers From DHCP
Description	Specifies if the DNS server IPv4 addresses should be assigned from the DHCP server on the network.
Legal Values	• Disabled - 0 • Enabled - 1

Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv4Static.Gateway (Read or Write)

Display Name	Gateway
Description	iDRAC static IPv4 gateway (can be configured even when DHCP is enabled)
Legal Values	String of up to 16 ASCII characters.
Default Value	192.168.0.1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.IPv4Static.Netmask (Read or Write)

Display Name	Net Mask
Description	iDRAC static IPv4 subnet mask(can be configured even when DHCP is enabled)
Legal Values	String of up to 16 ASCII characters.
Default Value	255.255.255.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address1 (Read or Write)

Display Name	IPV6 Address 1
Description	iDRAC IPv6 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address10 (Read Only)

Display Name	IPV6 Address 10
Description	iDRAC IPv6 tenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address11 (Read Only)

Display Name	IPV6 Address 11
Description	iDRAC IPv6 eleventh address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address12 (Read Only)

Display Name	IPV6 Address 12
Description	iDRAC IPv6 twelfth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address13 (Read Only)

Display Name	IPV6 Address 13
Description	iDRAC IPv6 thirteenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::

Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address14 (Read Only)

Display Name	IPv6 Address 14
Description	iDRAC IPv6 fourteenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address15 (Read Only)

Display Name	IPv6 Address 15
Description	iDRAC IPv6 fifteenth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address2 (Read Only)

Display Name	IPv6 Address 2
Description	iDRAC IPv6 second address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address3 (Read Only)

Display Name	IPV6 Address 3
Description	iDRAC IPv6 third address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address4 (Read Only)

Display Name	IPV6 Address 4
Description	iDRAC IPv6 fourth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address5 (Read Only)

Display Name	IPV6 Address 5
Description	iDRAC IPv6 fifth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address6 (Read Only)

Display Name	IPV6 Address 6
Description	iDRAC IPv6 sixth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::

Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address7 (Read Only)

Display Name	IPv6 Address 7
Description	iDRAC IPv6 seventh address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address8 (Read Only)

Display Name	IPv6 Address 8
Description	iDRAC IPv6 eighth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Address9 (Read Only)

Display Name	IPv6 Address 9
Description	iDRAC IPv6 ninth address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.AddressGenerationMode (Read or Write)

Display Name	IPv6 Address Generation Mode
Description	IPv6 Address Generation Mode
Legal Values	• StablePrivacy - 0 • EUI64 - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.AddressState (Read Only)

Display Name	Address State
Description	IPV6 Address State
Legal Values	• Active - 0 • Disabled - 1 • Pending - 2 • Failed - 3 • Deprecated - 4 • Invalid - 5
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.AutoConfig (Read or Write)

Display Name	IPV6 Auto Config
Description	Enables or Disables the iDRAC IPv6 auto configuration option
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.DNS1 (Read or Write)

Display Name	IPV6 DNS Server1
Description	IPv6 DNS Server 1 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.DNS2 (Read or Write)

Display Name	IPV6 DNS Server2
Description	IPv6 DNS Server 2 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.DNS3 (Read or Write)

Display Name	IPV6 DNS Server3
Description	IPv6 DNS Server 3 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.DNSFromDHCP6 (Read or Write)

Display Name	DNS Server From DHCP6
Description	Specifies if the DNS Server addresses are obtained from DHCP or not
Legal Values	• Disabled - 0 • Enabled - 1

Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.DUID (Read Only)

Display Name	IPV6 DUID
Description	DHCP Unique Identifier
Legal Values	String of up to 144 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Enable (Read or Write)

Display Name	IPV6 Enable
Description	Enables or Disables iDRAC IPv6 stack
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.Gateway (Read or Write)

Display Name	IPV6 Gateway
Description	iDRAC IPv6 Gateway
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.LinkLocalAddress (Read Only)

Display Name	IPV6 Link Local Address
Description	iDRAC IPv6 Link Local Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6.PrefixLength (Read or Write)

Display Name	IPV6 Link Local Prefix Length
Description	Prefix length for the iDRAC IPv6 Address
Legal Values	Integer values from 1 to 128.
Default Value	64
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.Address1 (Read or Write)

Display Name	IPv6 Address 1
Description	iDRAC static IPv6 address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.DNS1 (Read or Write)

Display Name	IPV6 DNS Server 1
Description	Statically configurable DNS Server 1
Legal Values	String of up to 63 ASCII characters.
Default Value	::

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.DNS2 (Read or Write)

Display Name	IPv6 DNS Server 2
Description	Statically configurable DNS Server 1
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.DNS3 (Read or Write)

Display Name	IPV6 DNS Server 3
Description	Statically configurable DNS Server 3
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.DNSFromDHCP6 (Read or Write)

Display Name	DNS Server From DHCP6
Description	Specifies if the DNS server IPv6 addresses should be assigned from the DHCP server on the network.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.Gateway (Read or Write)

Display Name	IPv6 Gateway
Description	iDRAC static IPv6 gateway
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6Static.PrefixLength (Read or Write)

Display Name	IPV6 Link Local Prefix Length
Description	Prefix length for the iDRAC IPv6 Address
Legal Values	Integer values from 1 to 128.
Default Value	64
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.IPv6URL.URL (Read Only)

Display Name	iDRAC IPv6 URL
Description	Provides the IPv6 URL for the iDRAC.
Legal Values	String of up to 80 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.Info.Build (Read Only)

Display Name	iDRAC Build Information
Description	String containing the current product build version
Legal Values	String of up to 16 ASCII characters.
Default Value	25

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.CPLDVersion (Read Only)

Display Name	CPLD Version
Description	Specifies the CPLD firmware version of the server.
Legal Values	String of up to 8 ASCII characters.
Default Value	0.0.0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.Description (Read Only)

Display Name	iDRAC Description Information
Description	Text description of the iDRAC
Legal Values	String of up to 512 ASCII characters.
Default Value	This system component provides a complete set of remote management functions for Dell PowerEdge Server.
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.HWModel (Read Only)

Display Name	iDRAC Hardware Model Information
Description	Specifies the iDRAC Hardware Model
Legal Values	String of up to 10 ASCII characters.
Default Value	iDRAC 9
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.HWRev (Read Only)

Display Name	iDRAC Hardware Revision
Description	Specifies the iDRAC hardware revision.
Legal Values	String of up to 256 ASCII characters.
Default Value	.0.1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.IPMIVersion (Read Only)

Display Name	IPMI Version
Description	Current IPMI Version supported on iDRAC
Legal Values	String of up to 20 ASCII characters.
Default Value	2.0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.Name (Read Only)

Display Name	iDRAC Name
Description	User assigned name identifying this controller
Legal Values	String of up to 15 ASCII characters.
Default Value	iDRAC
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.Product (Read Only)

Display Name	iDRAC Product Information
Description	String identifying the Product
Legal Values	String of up to 71 ASCII characters.
Default Value	Integrated Dell Remote Access Controller

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.RollbackBuild (Read Only)

Display Name	iDRAC Rollback Build Number
Description	Specifies the iDRAC rollback build number.
Legal Values	String of up to 256 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.RollbackVersion (Read Only)

Display Name	iDRAC Rollback Version
Description	Specifies the iDRAC rollback version.
Legal Values	String of up to 256 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Info.ServerGen (Read Only)

Display Name	Server Generation
Description	String containing the current server generation
Legal Values	• 12G - 1 • 13G - 2 • 14G - 3 • 15G - 4 • 16G - 5
Default Value	3
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** Yes

iDRAC.Info.Type (Read Only)

Display Name iDRAC Type

Description Identifies the remote access controller type as iDRAC

Legal Values

- 12G/13G/14G/15G - 0
- Other - 1
- Unknown - 2
- 12G Monolithic - 16
- 12G Modular - 17
- 13G Monolithic - 32
- 13G Modular - 33
- 12G DCS - 21
- 13G DCS - 34
- 14G Monolithic - 48
- 14G Modular - 49
- 14G DCS - 50
- 15G Monolithic - 64
- 15G Modular - 65
- 15G DCS - 66

Default Value 1

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** Yes

iDRAC.Info.Version (Read Only)

Display Name iDRAC Version Information

Description String containing the current product firmware version

Legal Values String of up to 63 ASCII characters.

Default Value None

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.IntegratedDatacenter.DiscoveryEnable (Read or Write)

Display Name Enable Autodiscovery

Description	Enable Autodiscovery
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.InventoryHash.HWInventoryHash (Read Only)

Display Name	Hardware Inventory Hash
Description	Provides hash value for available hardware inventory.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.InventoryHash.HashCalculationInterval (Read or Write)

Display Name	Hash Calculation Interval
Description	Set hash value generation interval
Legal Values	Integer values from 15 to 1440.
Default Value	15
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.InventoryHash.SWInventoryHash (Read Only)

Display Name	Software Inventory Hash
Description	Provides hash value for available software inventory
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.InventoryHash.SystemConfigHash (Read Only)

Display Name	System Configuration Hash
Description	Provides hash value for current server configuration
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.KMS.KMIPPortNumber (Read or Write)

Display Name	Key Management Server KMIP Port Number
Description	Specifies the KMIP Port Number for the Primary and Redundant Key Management Server.
Legal Values	Integer values from 0 to 65535.
Default Value	5696
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.PrimaryServerAddress (Read or Write)

Display Name	Primary Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the Primary Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantKMIPPortNumber (Read or Write)

Display Name	Redundant KMIP Port Number
Description	Specifies the KMIP Port Number for the Redundant Server.
Legal Values	Integer values from 0 to 65535.
Default Value	5696
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress1 (Read or Write)

Display Name	First Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the first Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress2 (Read or Write)

Display Name	Second Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the second Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress3 (Read or Write)

Display Name	Third Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the third Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress4 (Read or Write)

Display Name	Fourth Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the fourth Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress5 (Read or Write)

Display Name	Fifth Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the fifth Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress6 (Read or Write)

Display Name	Sixth Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the sixth Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress7 (Read or Write)

Display Name	Seventh Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the seventh Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.RedundantServerAddress8 (Read or Write)

Display Name	Eighth Redundant Server Address
Description	Specifies the FQDN, IPv4 address or IPv6 address of the eighth Redundant Key Management Server.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.Timeout (Read or Write)

Display Name	SSL Connection Timeout
Description	Specifies the SSL connection timeout value in seconds.
Legal Values	Integer values from 0 to 300.
Default Value	10
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.iDRACPassword (Read or Write)

Display Name	iDRAC Password
Description	Specifies the password for the iDRAC account on the Key Management server.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.KMS.iDRACUserName (Read or Write)

Display Name	iDRAC User Name
Description	Specifies the User Id on the Key Management server for this iDRAC.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

Notes	Run the racadm sekm enable command after changing any iDRAC KMS attributes. This action validates if the changes are valid and iDRAC can communicate with the KMS.

iDRAC.LDAP.BaseDN (Read or Write)

Display Name	LDAP Base Domain Name
Description	The Domain Name of the branch of the directory where all searches should start from.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.BindDN (Read or Write)

Display Name	LDAP Bind User Distinguished Name
Description	The distinguished name of a user used to bind to the server when searching for the login user's DN.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.BindPassword (Read or Write)

Display Name	LDAP Bind Password
Description	A bind password to use in conjunction with the bindDN.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.CertValidationEnable (Read or Write)

Display Name	Enable LDAP Certificate Validation

Description	Controls certificate validation during SSL handshake.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.Connection (Read or Write)

Display Name	LDAP Connection
Description	Selects LDAP connection protocol
Legal Values	• StartTLS - 0 • LDAPS - 1
Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.Enable (Read or Write)

Display Name	Enable LDAP
Description	Turns LDAP service on or off.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.GroupAttribute (Read or Write)

Display Name	LDAP Group Attribute
Description	Specifies which LDAP attribute is used to check for group membership.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users

License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.GroupAttributeIsDN (Read or Write)

Display Name	LDAP Group Attribute Is Domain Name
Description	Specifies whether the user domain name should be used from the LDAP server or from what was provided by user at login
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.Port (Read or Write)

Display Name	LDAP Port
Description	Port of LDAP over SSL.
Legal Values	Integer values from 1 to 65535.
Default Value	636
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.RSASecurID2FALDAP (Read or Write)

Display Name	RSA SecurID 2FA LDAP
Description	Enables or disables RSA SecurID 2 Factor Authentication for LDAP users.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	LM_RSA_SECURID
Dependency	Generic LDAP must be Enabled prior to setting to Enabled.
Is Platform Dependent	No

iDRAC.LDAP.SearchFilter (Read or Write)

Display Name	LDAP Search Filter
Description	A valid LDAP search filter to be used if the user attribute cannot uniquely identify the login user within the chosen baseDN.
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.Server (Read or Write)

Display Name	LDAP Server
Description	Configures the address of the LDAP Server
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAP.UserAttribute (Read or Write)

Display Name	LDAP User Attribute
Description	Specifies the user attribute to search for.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAPRoleGroup.DN (Read or Write)

Display Name	LDAP Role Group Domain Name
Description	This is the Domain Name of the group.
Legal Values	String of up to 1024 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LDAPRoleGroup.Privilege (Read or Write)

Display Name	LDAP Role Group Privilege
Description	A bit-mask defining the privileges associated with this particular group.
Legal Values	Integer values from 0 to 511.
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.LocalSecurity.LocalConfig (Read or Write)

Display Name	Local Config
Description	Enable local security
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.LocalSecurity.PrebootConfig (Read or Write)

Display Name	Preboot Config
Description	Enables or disables the ability of the local user to configure iDRAC from the BIOS POST option-ROM.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** No

iDRAC.Lockdown.SystemLockdown (Read or Write)

Display Name System Lockdown

Description Specifies if the System Lockdown is enabled or disabled

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 0

Write Privilege Configure iDRAC, Server Control and Configuration

License Required LM_LOCKDOWN_MODE

Dependency None

**Is Platform
Dependent** No

iDRAC.Logging.LCDuplicateEventEnable (Read or Write)

Display Name LCDuplicateEventEnable

Description Lifecycle Log Duplicate Entry

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 0

Write Privilege N/A

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.Logging.LCLogAggregation (Read or Write)

Display Name LCLogAggregation

Description Lifecycle Log aggregation

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 0

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.Logging.LCLogAggregationTimeout (Read or Write)

Display Name	LCLogAggregationTimeout
Description	LCLoggingAggregationTimeout in Minutes
Legal Values	Integer values from 1 to 1440.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Logging.SELBufferType (Read or Write)

Display Name	Control SEL Buffer Type
Description	Configurable attribute to modify the SEL behavior to make it linear instead of default circular.
Legal Values	• Circular - 0 • Linear - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Logging.SELOEMEventFilterEnable (Read or Write)

Display Name	SEL OEM Event Filter Enable
Description	Enable SEL OEM Event Filter
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.AutoConfig (Read or Write)

Display Name	Auto Configuration enable
Description	Enable Auto Configuration

Legal Values	• Disabled - 0 • Enable Once - 1 • Enable Once After Reset - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.AutoDetect (Read or Write)

Display Name	Auto NIC Enable
Description	Enable or disable auto detection feature of iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.Autoneg (Read or Write)

Display Name	NIC Auto Negotiation
Description	Enables autonegotiation of physical link speed and duplex
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.DNSDomainFromDHCP (Read or Write)

Display Name	DNS Domain From DHCP
Description	Specifies that the iDRAC DNS Domain Name should be assigned from the network DHCP server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1

Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.DNSDomainName (Read or Write)

Display Name	DNS Domain Name
Description	The DNS Domain Name
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.DNSDomainNameFromDHCP (Read or Write)

Display Name	DNS Domain Name from DHCP
Description	Specifies that the iDRAC DNS Domain Name should be assigned from the network DHCP server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.DNSRacName (Read or Write)

Display Name	DNS RAC Name
Description	The iDRAC name, which is iDRAC-<SVCTAG> by default
Legal Values	String of up to 63 ASCII characters.
Default Value	idrac-SVCTAG
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.DNSRegister (Read or Write)

Display Name	DNS Register RAC
Description	Registers the iDRAC name with the DNS server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.DNSRegisterInterval (Read or Write)

Display Name	DNS Registration Interval
Description	Specifies the DNS registration refresh interval. Valid values are 0 or 60 to 7776000.
Legal Values	Integer values from 60 to 7776000.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.DedicatedNICScanTime (Read or Write)

Display Name	Shared to Dedicated Failover Timeout
Description	Wait time for the iDRAC to switch from dedicated mode to shared mode.
Legal Values	Integer values from 5 to 255.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.DiscoveryLLDP (Read or Write)

Display Name	Discovery LLDP
Description	Enables LLDP over active NIC Interface.
Legal Values	• Disabled - 0

	• Dedicated - 1 • SharedLOM - 2 • Enabled - 3
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.Duplex (Read or Write)

Display Name	NIC Duplex
Description	Specifies the duplex setting for the iDRAC NIC
Legal Values	• Half - 0 • Full - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.Enable (Read or Write)

Display Name	NIC Enable
Description	Enables or Disables the iDRAC network interface controller.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.Failover (Read or Write)

Display Name	NIC Failover
Description	Specifies the NIC Failover LOM.
Legal Values	• None - 0 • LOM1 - 1 • LOM2 - 2 • LOM3 - 3

	• LOM4 - 4 • All - 5
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.MACAddress (Read Only)

Display Name	MAC Address
Description	The MAC Address of the iDRAC
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.MTU (Read or Write)

Display Name	NIC Maximum Transmission Unit
Description	The size in bytes of the maximum transmission unit used by the iDRAC NIC
Legal Values	Integer values from 576 to 1500.
Default Value	1500
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.PingEnable (Read or Write)

Display Name	Ping Enable
Description	Enables iDRAC to respond to pings
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** No

iDRAC.NIC.Selection (Read or Write)

Display Name NIC Selection

Description Specifies the current mode of operation for the iDRAC network interface controller

Legal Values

- Dedicated - 1
- LOM1 - 2
- LOM2 - 3
- LOM3 - 4
- LOM4 - 5

Default Value 1

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** Yes

iDRAC.NIC.SharedNICScanTime (Read or Write)

Display Name Dedicated to Shared Failover Timeout

Description Wait time for the iDRAC to switch from shared mode to dedicated mode.

Legal Values Integer values from 5 to 255.

Default Value 30

Write Privilege Configure iDRAC

License Required Express License

Dependency None

**Is Platform
Dependent** Yes

iDRAC.NIC.Speed (Read or Write)

Display Name NIC Speed

Description Specifies the speed for the iDRAC NIC

Legal Values

- 10 - 0
- 100 - 1
- 1000 - 2
- 2500 - 3
- 10000 - 4
- 20000 - 5
- 25000 - 6
- 40000 - 7
- 50000 - 8
- 100000 - 9

Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.SwitchConnection (Read Only)

Display Name	Switch Connection
Description	Specifies the Chassis ID extracted from LLDP packet
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.SwitchPortConnection (Read Only)

Display Name	Switch Port Connection
Description	Specifies the Port ID extracted from LLDP packet.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.TopologyLldp (Read or Write)

Display Name	TopologyLLDP
Description	Enable/Disable LLDP topology information
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.NIC.VLanEnable (Read or Write)

Display Name	Enable VLAN
Description	Enables or Disables the VLAN capabilities of the iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.VLanID (Read or Write)

Display Name	VLAN ID
Description	Specifies the VLAN ID for the network VLAN configuration
Legal Values	Integer values from 1 to 4094.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.VLanPort (Read or Write)

Display Name	VLAN Port
Description	VLAN Port
Legal Values	• Both - 0 • Dedicated port only - 1 • LOM ports only - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NIC.VLanPriority (Read or Write)

Display Name	VLAN Priority
Description	Specifies the VLAN priority for the network VLAN configuration

Legal Values	Integer values from 0 to 7.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.NICStatic.DNSDomainFromDHCP (Read or Write)

Display Name	DNS Domain From DHCP
Description	Specifies that the iDRAC DNS Domain Name should be assigned from the network DHCP server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The following objects are not valid for modular systems: • Auto negotiation • Auto dedicated NIC • Network speed • Duplex • Dedicated NIC scan time • Shared NIC scan time

iDRAC.NICStatic.DNSDomainName (Read or Write)

Display Name	DNS Domain Name
Description	The DNS Domain Name
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The following objects are not valid for modular systems: • Auto negotiation • Auto dedicated NIC • Network speed • Duplex • Dedicated NIC scan time • Shared NIC scan time

iDRAC.NTPConfigGroup.NTP1 (Read or Write)

Display Name	NTP Server 1
Description	Name of NTP Server 1
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP1SecurityKey (Read or Write)

Display Name	Security Key for NTP Server 1
Description	Security Key for NTP Server 1
Legal Values	String of up to 64 ASCII characters.
Default Value	""
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP1SecurityKeyNumber (Read or Write)

Display Name	Security Key Number for NTP Server 1
Description	Security Key Number for NTP Server 1
Legal Values	Integer values from 1 to 65535.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP1SecurityType (Read or Write)

Display Name	Security Type for NTP Server 1
Description	Security type for NTP server 1

Legal Values	• Disabled - 0 • MD5 - 1 • SHA1 - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP2 (Read or Write)

Display Name	NTP Server 2
Description	Name of NTP Server 2
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP2SecurityKey (Read or Write)

Display Name	Security Key for NTP Server 2
Description	Security Key for NTP Server 2
Legal Values	String of up to 64 ASCII characters.
Default Value	""
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP2SecurityKeyNumber (Read or Write)

Display Name	Security Key Number for NTP Server 2
Description	Security Key Number for NTP Server 2
Legal Values	Integer values from 1 to 65535.
Default Value	1
Write Privilege	Configure iDRAC

License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP2SecurityType (Read or Write)

Display Name	Security Type for NTP Server 2
Description	Security type for NTP server 2
Legal Values	• Disabled - 0 • MD5 - 1 • SHA1 - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP3 (Read or Write)

Display Name	NTP Server 3
Description	Name of NTP Server 3
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP3SecurityKey (Read or Write)

Display Name	Security Key for NTP Server 3
Description	Security Key for NTP Server 3
Legal Values	String of up to 64 ASCII characters.
Default Value	""
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP3SecurityKeyNumber (Read or Write)

Display Name	Security Key Number for NTP Server 3
Description	Security Key Number for NTP Server 3
Legal Values	Integer values from 1 to 65535.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTP3SecurityType (Read or Write)

Display Name	Security Type for NTP Server 3
Description	Security type for NTP server 3
Legal Values	• Disabled - 0 • MD5 - 1 • SHA1 - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.NTPConfigGroup.NTPEnable (Read or Write)

Display Name	NTP Enable
Description	Enable Network Time Protocol
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	Yes

iDRAC.NTPConfigGroup.NTPMaxDist (Read or Write)

Display Name	NTP Maximum Distance
Description	NTP Maximum Distance
Legal Values	Integer values from 1 to 128.
Default Value	16
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.OS-BMC.AdminState (Read or Write)

Display Name	LC and Host Private Channel State
Description	Manages the administrative state of the IMC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.OslpAddress (Read or Write)

Display Name	OS-BMC PT HOST IP Address
Description	OS-BMC Passthrough Host IP Address. Enter a valid IPv4 address.
Legal Values	String of up to 16 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.PTCapability (Read Only)

Display Name	OS-BMC Pass Through Capability

Description	OS-BMC Pass Through Capability
Legal Values	• Not Capable - 0 • Capable - 1 • Unavailable - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.PTMode (Read or Write)

Display Name	OS-BMC PT Mode
Description	Specifies the OS-BMC Passthrough mode. Note: Starting in iDRAC9 4.00, lom-p2p is not supported when NIC Selection is set to Dedicated.
Legal Values	• lom-p2p - 0 • usb-p2p - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	OS-BMC.PTCompatibility must be set to Capable.
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.UsbNicIpAddress (Read or Write)

Display Name	USB NIC IP Address
Description	Specifies the USB NIC IP Address. Enter a valid IPv4 address.
Legal Values	String of up to 16 ASCII characters.
Default Value	169.254.1.1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.UsbNicIpNetmask (Read or Write)

Display Name	USB NIC IP Netmask

Description	USB NIC IP Netmask
Legal Values	String of up to 16 ASCII characters.
Default Value	255.255.255.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.UsbNicIpV6Address (Read Only)

Display Name	USB NIC IPv6 Address
Description	USB NIC IPv6 Address
Legal Values	String of up to 63 ASCII characters.
Default Value	::
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.UsbNicIpv4AddressSupport (Read or Write)

Display Name	USB NIC IPv4 Address Support
Description	Specifies whether the USB NIC IP Address can support IPv4 or NOT. Select Enabled to allow IPv4 address.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.OS-BMC.UsbNicULA (Read or Write)

Display Name	USB-NIC IPv6 Unique Local Address

Description	Specifies the USB-NIC IPv6 unique local address. Address cannot be in the ranges fde1:53ba:e9a0:de12::/64, fde1:53ba:e9a0:de13::/64, fde1:53ba:e9a0:de14::/64, fde1:53ba:e9a0:de15::/64 and fde1:53ba:e9a0:de16::/64.
Legal Values	String of up to 63 ASCII characters.
Default Value	fde1:53ba:e9a0:de11::1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	In Autocomplete mode, the group OS-BMC is autocompleted as OS_BMC.

iDRAC.PCLeVDM.AllowFQDD (Read or Write)

Display Name	AllowFQDD
Description	FQDD of the device to enable PCIe VDM communication when the device supports PCIe VDM.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.BroadcastEnable (Read or Write)

Display Name	BroadcastEnable
Description	BroadcastEnable enforces iDRAC to discover PCIe VDM capable devices by broadcasting discovery commands from PCIe root complex. If disabled then iDRAC uses unicast (P2P) method to discover PCIe VDM devices.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.CheckPCIID (Read or Write)

Display Name	CheckPCIID
Description	Check the status of PCI ID for PCIe VDM
Legal Values	String of up to 20 ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.DenyFQDD (Read or Write)

Display Name	DenyFQDD
Description	FQDD of the device to disable PCIe VDM communication when the device supports PCIe VDM.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.Enable (Read or Write)

Display Name	PCIe VDM Enable
Description	Enable/Disable the PCIe VDM capability.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.FQDDDenyList (Read or Write)

Display Name	FQDDDenyList
Description	iDRAC will not issue P2P PCIe VDM commands to the device in FQDDDenyList even if the device supports PCIe VDM.
Legal Values	String of up to 4096 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** No

iDRAC.PCLeVDM.NVMeHotplugEnable (Read or Write)

Display Name NVMeHotplugEnable

Description NVMeHotplugEnable enforces iDRAC to discover NVMe Hotplug devices over PCIe VDM

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 1

Write Privilege N/A

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.PCLeVDM.PCIIDAllowOnlyList (Read or Write)

Display Name PCIIDAllowOnlyList

Description PCIIDs in this List are only allowed for PCIe VDM communication and rest of all other PCIIDs are denied.

Legal Values String of up to 4000 ASCII characters.

Default Value None

Write Privilege N/A

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.PCLeVDM.PCIIDDenyList (Read or Write)

Display Name PCIIDDenyList

Description PCIID Deny List for PCIe VDM

Legal Values String of up to 4000 ASCII characters.

Default Value None

Write Privilege N/A

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.PCLeVDM.PCIIDExtendedList (Read or Write)

Display Name PCIIDExtendedList

Description	Extended list for the default list of allowed PCIIDs of iDRAC for PCIe VDM devices.
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCIeVDM.PCIIDList1 (Read or Write)

Display Name	PCIIDList1
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCIeVDM.PCIIDList2 (Read or Write)

Display Name	PCIIDList2
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCIeVDM.PCIIDList3 (Read or Write)

Display Name	PCIIDList3
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

iDRAC.PCLeVDM.PCIIDList4 (Read or Write)

Display Name	PCIIDList4
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.PCIIDList5 (Read or Write)

Display Name	PCIIDList5
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.PCIIDList6 (Read or Write)

Display Name	PCIIDList6
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCLeVDM.PCIIDList7 (Read or Write)

Display Name	PCIIDList7

Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PCIeVDM.PCIIDList8 (Read or Write)

Display Name	PCIIDList8
Description	List of PCI IDs allowed for PCIe VDM
Legal Values	String of up to 4000 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PLDMConfiguration.PLDMLogRetrieval (Read or Write)

Display Name	PLDM Log Retrieval
Description	Enable/disable PLDM firmware update for PCIe cards.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PlatformCapability.ASHRAECapable (Read Only)

Display Name	ASHRAE Capable
Description	Indicates if system is ASHRAE capable.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.AirFilterCapable (Read Only)

Display Name	AirFilter Capable
Description	Air Filter supported or not
Legal Values	• NoFilter - 0 • PassiveFilter - 1 • ActiveFilter - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.BackupRestoreCapable (Read Only)

Display Name	BackupRestore Capable
Description	Indicates if Backup and Restore is supported.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.CUPSCapable (Read Only)

Display Name	CUPS Capable
Description	Indicates hardware is CUPS capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.ExtendedInfoCapable (Read Only)

Display Name	Extended Information Capable
Description	Heater Manager Extended Information Capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.FrontPanelCapable (Read Only)

Display Name	Front Panel Capable
Description	Indicates hardware is front panel capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.FrontPanelUSBCapable (Read Only)

Display Name	Front Panel USB Capable
Description	Indicates hardware is Front Panel USB capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.FrontPortUSBConfiguration (Read Only)

Display Name	Front Port USB Configuration
Description	When BIOS is configured as "All Ports Off (Dynamic)" the above capability attribute will be set to true, otherwise false.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	Dynamic USB is only available on 600+ series servers and higher.

iDRAC.PlatformCapability.GridCurrentCapCapable (Read Only)

Display Name	GridCurrentCapCapable
Description	System current cap capability
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PlatformCapability.LCDCapable (Read Only)

Display Name	LCD Capable
Description	Indicates platform is LCD capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.LiveScanCapable (Read Only)

Display Name	Live Scan Capable
Description	Indicates if Live Scan is supported.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.NICRoTCapable (Read Only)

Display Name	NIC Root of Trust Capable
Description	No description information available.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.NicVLANCapable (Read Only)

Display Name	NIC VLAN Capable
Description	Indicates Platform support for VLAN in Dedicated and/or Shared
Legal Values	• None - 0 • Dedicated - 1 • SharedLOM - 2 • Both - 3
Default Value	3
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.NvidiaGPUBaseboardMgtEnable (Read Only)

Display Name	Nvidia GPU Baseboard Management Enable
Description	Enable or disable NVIDIA GPU baseboard management
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.PDBPresence (Read Only)

Display Name	PDBPresence
Description	Indicates PDB Presence
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.PMBUSCapablePSU (Read Only)

Display Name	PMBUS Capable PSU
Description	Indicates PMBUS PSU Capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.PowerBudgetCapable (Read Only)

Display Name	Power Budget Capable
Description	Indicates hardware is Power Budgetcapable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.PowerMonitoringCapable (Read Only)

Display Name	Power Monitoring Capable
Description	Indicates hardware is Power Monitoring capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.SDPMCapable (Read Only)

Display Name	SDPM Capable
Description	Indicates whether the system is capable to support Software Defined Persistent Memory.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.SerialDB9PCapable (Read Only)

Display Name	Serial DB9 Capable
Description	Indicates if hardware is Serial DB9 Capable.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.ServerAllocationCapable (Read Only)

Display Name	Server Allocation Capable
Description	Indicates whether the ServerAllocation field in HW inventory is used or not.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.SharedStorageCapable (Read Only)

Display Name	Shared Storage Capable
Description	Indicates whether Platform is capable of supporting shared storage
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.SystemCurrentCapCapable (Read Only)

Display Name	SystemCurrentCapCapable
Description	Grid current cap capability
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PlatformCapability.Telco-EdgeCapable (Read Only)

Display Name	Telco-Edge Capable
Description	Telco-Edge features supported or not
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.UserPowerCapBoundCapable (Read Only)

Display Name	User Power cap Boundary Capable
Description	Indicated User Power Cap boundary Capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.UserPowerCapCapable (Read Only)

Display Name	User Power Cap Capable
Description	Indicates User Power cap Capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.WiFiCapable (Read Only)

Display Name	WiFi Capable
Description	Indicates hardware is WiFi capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.WitnessCapable (Read Only)

Display Name	Witness Capable
Description	Witness Sled supported or not
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.PlatformCapability.thermalmanagedbyparent (Read Only)

Display Name	thermal managed by parent
Description	Gives info on whether it is Self Powered or Powered By Chassis
Legal Values	• SelfPowered - 0 • PoweredByChassis - 1 • Unknown - 255
Default Value	255
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.PlatformCapability.vFlashCapable (Read Only)

Display Name	vFlash Capable
Description	Indicates hardware is vFlash capable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.RFS.AttachMode (Read or Write)

Display Name	Media Attach Mode
Description	RFS Media attach mode
Legal Values	• Detached - 0 • Attached - 1 • Auto Attach - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second

instance respectively.

iDRAC.RFS.Enable (Read or Write)

Display Name	Enable
Description	RFS Enable State
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.IgnoreCertWarning (Read or Write)

Display Name	Ignore Certificate Warning
Description	Ignore certificate warning message
Legal Values	• No - 0 • Yes - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.Image (Read or Write)

Display Name	iDRAC Remote File Share Image Path
Description	RFS Image path
Legal Values	String of up to 511 ASCII characters.
Default Value	None
Write Privilege	Server Control and Configuration
License Required	Enterprise License

Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.MediaAttachState (Read Only)

Display Name	Media Attach State
Description	RFS Media attach state
Legal Values	• Detached - 0 • Attached - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.Password (Read or Write)

Display Name	Remote File Share Password
Description	Specifies the remote file share password.
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.Status (Read or Write)

Display Name	Status
Description	RFS connection status

Legal Values	• Done - 0 • Pending - 1 • Error - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.User (Read or Write)

Display Name	Remote File Share User
Description	Specifies the remote file share user.
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RFS.WriteProtected (Read or Write)

Display Name	iDRAC Remote File Share Write protected
Description	RFS Write Protection
Legal Values	• Read Only - 0 • Read Write - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	• To perform the complete workflow for RFS and set attributes, refer to remoteimage. • RFS now supports two instances, use iDRAC.RFS.1 and iDRAC.RFS.2 to reference the first and second instance respectively.

iDRAC.RSASecurID2FA.RSASecurIDAccessKey (Read or Write)

Display Name	RSA SecurID Authentication Access IDRSA SecurID Authentication Access Key
Description	Displays the RSA Authentication Key
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	LM_RSA_SECURID
Dependency	None
Is Platform Dependent	No

iDRAC.RSASecurID2FA.RSASecurIDAuthenticationServer (Read or Write)

Display Name	RSA SecurID Authentication Server
Description	Displays the RSA Authentication server URL
Legal Values	String of up to 2048 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	LM_RSA_SECURID
Dependency	None
Is Platform Dependent	No

iDRAC.RSASecurID2FA.RSASecurIDClientID (Read or Write)

Display Name	RSA SecurID Authentication Client ID
Description	Displays the RSA Authentication Key
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	LM_RSA_SECURID
Dependency	None
Is Platform Dependent	No

iDRAC.Racadm.Enable (Read or Write)

Display Name	Remote Racadm Enable
Description	Enables or disables the Remote Racadm interface.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Racadm.MaxSessions (Read Only)

Display Name	Remote Racadm Maximum Sessions
Description	Specifies the maximum number of active Remote Racadm sessions allowed.
Legal Values	Integer values from 0 to 8.
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Racadm.Timeout (Read or Write)

Display Name	Remote Racadm Timeout
Description	Defines the idle timeout in seconds of the Remote Racadm interface.
Legal Values	Integer values from 10 to 1920.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Redfish.Enable (Read or Write)

Display Name	Enable
Description	Redfish Enable
Legal Values	• Disabled - 0

	Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Redfish.NumericDynamicSegmentsEnable (Read or Write)

Display Name	NumericDynamicSegmentsEnable
Description	Set this attribute to Enabled to enable the Numeric Dynamic Segments feature. Default is Disabled.
Legal Values	- Disabled - 0 - Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.Redfish.iDRACRebootInProgress (Read Only)

Display Name	iDRAC Reboot in progress
Description	To check for iDRAC reboot status
Legal Values	- False - 0 - True - 1
Default Value	0
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.RedfishEventing.DeliveryRetryAttempts (Read or Write)

Display Name	Delivery Retry Attempts
Description	This is the number of attempts an event posting is retried before the subscription is terminated.
Legal Values	Integer values from 0 to 5.
Default Value	3

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.RedfishEventing.DeliveryRetryIntervalInSeconds (Read or Write)

Display Name	Delivery Retry Interval In Seconds
Description	This represents the number of seconds between retry attempts for sending any given Event.
Legal Values	Integer values from 5 to 60.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.RedfishEventing.EventEnable (Read or Write)

Display Name	Enable Redfish Eventing
Description	Indicates if Redfish Eventing is enabled or disabled on iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.RedfishEventing.IgnoreCertificateErrors (Read or Write)

Display Name	Ignore Certificate Errors
Description	To ignore any SSL certificate warnings that may arise during SSL handshake with Event Listener.
Legal Values	• No - 0 • Yes - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.ConnectionEncryption (Read or Write)

Display Name	Connection Encryption
Description	Specifies how encryption on the connection to the SMTP server will be configured.
Legal Values	• None - 0 • SSL/TLS - 1 • STARTTLS - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.MessageSubjectPrefix (Read or Write)

Display Name	Message Subject Prefix
Description	Specifies a custom message subject prefix for email alert messages.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.SMTPAuthentication (Read or Write)

Display Name	SMTP Authentication
Description	Enable SMTP Authentication
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.SMTPPassword (Read or Write)

Display Name	SMTP Password
Description	SMTP Password
Legal Values	String of up to 50 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.SMTPPort (Read or Write)

Display Name	SMTP Port
Description	Specifies the SMTP Port
Legal Values	Integer values from 1 to 65535.
Default Value	25
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.SMTPServerIPAddress (Read or Write)

Display Name	SMTP Server IP Address
Description	Address of the network SMTP server
Legal Values	String of up to 254 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.SMTPUserName (Read or Write)

Display Name	SMTP UserName
Description	SMTP User Name
Legal Values	String of up to 50 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.RemoteHosts.SenderEmail (Read or Write)

Display Name	Sender Email Address
Description	Specifies the address of emails sent by iDRAC
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SCEP.CA-URL (Read or Write)

Display Name	Certificate Authority URL
Description	Specifies the URL of the Certificate Authority.
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.SCEP.ChallengePassword (Read or Write)

Display Name	Challenge Password
Description	Specifies the challenge password for the Certificate Authority.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.SCEP.Enable (Read or Write)

Display Name	Enable
Description	Enables or disables Simple Certificate Enrollment.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	SCEP CA-URL must be configured before SCEP can be enabled.
Is Platform Dependent	No

iDRAC.SCEP.EnrollmentAction (Read or Write)

Display Name	Enrollment Action
Description	Enrollment Actions
Legal Values	• Halt - 0 • Monitor - 1 • Enroll - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.SCEP.EnrollmentStatus (Read Only)

Display Name	Enrollment Status
Description	Provides the enrollment status.
Legal Values	• None - 0 • Enrolling - 1 • Enrolled - 2 • Error - 3
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.SCV.CertificateVersion (Read Only)

Display Name	Certificate Version
Description	Specifies the certificate version. Introduced to capture the SCV certificate version which is a Profile version
Legal Values	String of up to 12 ASCII characters.
Default Value	NA
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.AutoSecure (Read or Write)

Display Name	Auto Secure Security Capable Drives
Description	Indicates if iDRAC will auto secure all security capable drives.
Legal Values	• Disabled - 1 • Enabled - 2
Default Value	2
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.IPAddressInCertificate (Read or Write)

Display Name	IP Address In Certificate
Description	Indicates if use of iDRAC IP address in SEKM SSL Certificate is enabled or disabled.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KMSKeyPurgePolicy (Read or Write)

Display Name	KMS Key Purge Policy

Description	Attribute that specifies if iDRAC should delete old keys on the Key Management Server every time iDRAC generates a new key to rekey security capable devices.
Legal Values	• Keep All Keys - 1 • Keep N and N-1 keys - 2
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KeyAlgorithm (Read or Write)

Display Name	Key Algorithm
Description	Indicates the key algorithm to be used by iDRAC when requesting the Key Management Server to generate a key.
Legal Values	• AES-256 - 1
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KeyCachingPolicy (Read or Write)

Display Name	Key Caching Policy
Description	Indicates if iDRAC will cache the SEKM key in volatile memory.
Legal Values	• No Caching - 1 • Cache in Volatile Memory - 2
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KeyCachingStatus (Read Only)

Display Name	Key Caching Status
Description	Indicates the current status of the key caching policy on iDRAC.
Legal Values	• Key Not Cached - 1 • Key cached in Volatile Memory - 2
Default Value	1

Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KeyCreationPolicy (Read Only)

Display Name	Key Creation Policy
Description	Attribute that specifies the number of keys iDRAC should generate to secure storage devices on a system.
Legal Values	• Key per iDRAC - 1
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KeyIdentifierN (Read Only)

Display Name	Key Identifier N
Description	Attribute that specifies the current key identifier of the authentication key used to secure storage devices on the server when iDRAC is in single key mode.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM.KeyIdentifierNMinusOne (Read Only)

Display Name	Key Identifier NMinusOne
Description	Attribute that specifies the previous key identifier of the authentication key used to secure storage devices on the server when iDRAC is in single key mode.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None

**Is Platform
Dependent** No

iDRAC.SEKM.RekeyMode (Read Only)

Display Name Rekey Mode

Description To check or update for iDRAC Rekey Mode

Legal Values

- Manual Rekey - 1
- Scheduled Rekey - 2
- Periodic Sync with KMS - 3

Default Value 1

Write Privilege Configure iDRAC

License Required SEKM License

Dependency None

**Is Platform
Dependent** No

iDRAC.SEKM.SEKMStatus (Read Only)

Display Name SEKM Status

Description Indicates if SEKM is enabled or disabled on iDRAC.

Legal Values

- Disabled - 0
- Enabled - 1
- Failed - 2
- Unverified Changes Exist - 3

Default Value 0

Write Privilege Configure iDRAC, Server Control and Configuration

License Required SEKM License

Dependency None

**Is Platform
Dependent** No

iDRAC.SEKM.SecurityMode (Read Only)

Display Name Current Security Mode

Description Indicates iDRAC LKM status

Legal Values

- None - 1
- iLKM - 2
- SEKM - 3

Default Value 1

Write Privilege Configure iDRAC, Server Control and Configuration

License Required SEKM License

Dependency None

**Is Platform
Dependent** No

iDRAC.SEKM.SupportStatus (Read Only)

Display Name SEKM Support Status

Description Indicates the status of the SEKM setup on iDRAC.

Legal Values

- Unknown - 0
- NotInstalled - 1
- Installed - 2
- NoLicense - 3
- LicenseOnly - 4

Default Value 0

Write Privilege Configure iDRAC, Server Control and Configuration

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.SEKM.VossSdpmReducedRebootSupport (Read Only)

Display Name Voss Sdpm Support with Reduced Reboot

Description Allows performing Cryptographic Erase on Secured SDPM Drive as a RealTime Job

Legal Values

- Supported - 1

Default Value 1

Write Privilege Configure iDRAC

License Required SEKM License

Dependency None

**Is Platform
Dependent** No

iDRAC.SEKM.iLKMSStatus (Read Only)

Display Name iDRAC Local Key Management Status

Description Indicates iDRAC LKM status

Legal Values

- Disabled - 1
- Enabled - 2

Default Value 1

Write Privilege Configure iDRAC, Server Control and Configuration

License Required SEKM License

Dependency None

Is Platform Dependent	No

iDRAC.SEKM-LKC.KMSConnectionTimeout (Read or Write)

Display Name	KMS Connection Timeout
Description	Time interval since the first KMS connection failure for which the key is considered valid on iDRAC - after this time interval iDRAC purges the authentication key
Legal Values	Integer values from 1 to 48.
Default Value	24
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	LM_SEKM_LKC_FEATURE
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM-LKC.KMSHeartbeatInterval (Read or Write)

Display Name	KMS Heartbeat Interval
Description	Time interval at which iDRAC sends a heartbeat to the external KMS
Legal Values	Integer values from 1 to 24.
Default Value	4
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	LM_SEKM_LKC_FEATURE
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM-LKC.KMSValidationFailurePolicy (Read or Write)

Display Name	KMS Validation Failure Policy
Description	This determines if iDRAC should use stored key in cases where KMS is reachable but iDRAC cannot get the key from the KMS (for ex.: authentication issues/key not present)
Legal Values	• Do not use the cached key - 1 • Use the cached key - 2
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	LM_SEKM_LKC_FEATURE
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM-LKC.KeyCachingPolicy (Read or Write)

Display Name	Key Caching Policy
Description	Indicates the key caching policy on iDRAC
Legal Values	• No Caching - 1 • Cache in non-volatile memory - 2
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	LM_SEKM_LKC_FEATURE
Dependency	None
Is Platform Dependent	No

iDRAC.SEKM-LKC.KeyCachingStatus (Read Only)

Display Name	Key Caching Status
Description	Indicates the current key caching status on iDRAC
Legal Values	• Key Not Cached - 1 • Key Cached in non-volatile memory - 2
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	LM_SEKM_LKC_FEATURE
Dependency	None
Is Platform Dependent	No

iDRAC.SEKMCert.CertificateStatus (Read Only)

Display Name	SEKM Certificate Status
Description	Specifies the SEKM CSR Certificate Status.
Legal Values	• NOT_PENDING - 0 • REQUEST_IN_PROGRESS - 1 • PENDING - 2 • FAILED - 3
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.CommonName (Read or Write)

Display Name	SEKM CSR Common Name
Description	Specifies the SEKM CSR Common Name (CN) - must be a UserId as given in the certificate if the Key Management Server is setup to use CN for user id.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.CountryCode (Read or Write)

Display Name	SEKM CSR Country Code
Description	Specifies the SEKM CSR Country Code (CC).
Legal Values	String of up to 2 ASCII characters.
Default Value	US
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.EmailAddress (Read or Write)

Display Name	SEKM CSR Email Address
Description	Specifies the SEKM CSR Email Address.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None

Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.LocalityName (Read or Write)

Display Name	SEKM CSR Locality Name
Description	Specifies the SEKM CSR Locality Name (L).
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.OrganizationName (Read or Write)

Display Name	SEKM CSR Organization Name
Description	Specifies the SEKM CSR Organization Name (O).
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.OrganizationUnit (Read or Write)

Display Name	SEKM CSR Organization Unit

Description	Specifies the SEKM CSR Organization Unit (OU) - must be a Userld as given in the certificate if the Key Management Server is setup to use OU for user id.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.StateName (Read or Write)

Display Name	SEKM CSR State Name
Description	Specifies the SEKM CSR State Name (S).
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMCert.SubjectAltName (Read or Write)

Display Name	SEKM CSR Subject Alternate Name
Description	Specifies the SEKM CSR Subject Alternate Name.
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to:

- Regenerate CSR
- Get it signed on the key management server
- Reupload to iDRAC

iDRAC.SEKMCert.UserId (Read or Write)

Display Name	SEKM CSR iDRAC User Id
Description	Specifies the SEKM CSR UserId. This is the user name that represents iDRAC on the Key Management Server. Specify this if the user name in client certificate is set to UID.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	SEKM License
Dependency	None
Is Platform Dependent	No
Notes	If you have a signed SSL SEKM cert that is already uploaded, and if you change iDRAC SEKM cert attributes, you have to: • Regenerate CSR • Get it signed on the key management server • Reupload to iDRAC

iDRAC.SEKMServices.BOSSStatus (Read Only)

Display Name	Status of BOSS SEKM Service
Description	Indicates if BOSS is ready for SEKM Configuration.
Legal Values	• Not Supported - 0 • Not Ready - 1 • Ready - 2
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SEKMServices.HBAStatus (Read Only)

Display Name	Status of HBA SEKM Service
Description	Indicates if HBA is ready for SEKM Configuration.
Legal Values	• Not Supported - 0 • Not Ready - 1 • Ready - 2
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SEKMServices.NVMeStatus (Read Only)

Display Name	Status of NVMe SEKM Service
Description	Indicates if NVMe is ready for SEKM Configuration.
Legal Values	• Not Supported - 0 • Not Ready - 1 • Ready - 2
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SEKMServices.OverallStatus (Read Only)

Display Name	OverallStatus of SEKM Services
Description	Indicates if all SEKM services are ready for Configuration.
Legal Values	• Not Ready - 0 • Ready - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SEKMServices.PERCStatus (Read Only)

Display Name	Status of PERC SEKM Service
Description	Indicates if PERC is ready for SEKM Configuration.
Legal Values	• Not Supported - 0 • Not Ready - 1 • Ready - 2
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** No

iDRAC.SEKMServices.VOSSStatus (Read Only)

Display Name Status of VOSS SEKM Service

Description Indicates if VOSS drive is ready for SEKM Configuration.

Legal Values

- Not Supported - 0
- Not Ready - 1
- Ready - 2

Default Value 0

Write Privilege Configure iDRAC, Server Control and Configuration

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.SNMP.AgentCommunity (Read or Write)

Display Name SNMP Agent Community

Description Specifies the SNMP community name to be used for SNMP Agents

Legal Values String of up to 31 ASCII characters.

Default Value public

Write Privilege Configure iDRAC

License Required Express License

Dependency None

**Is Platform
Dependent** No

iDRAC.SNMP.AgentEnable (Read or Write)

Display Name SNMP Agent Enable

Description Enables or Disables the SNMP Agent on the iDRAC

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 1

Write Privilege Configure iDRAC

License Required Express License

Dependency None

**Is Platform
Dependent** No

iDRAC.SNMP.AlertPort (Read or Write)

Display Name	Alert Port
Description	Specifies the SNMP Alert Port
Legal Values	Integer values from 1 to 65535.
Default Value	162
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMP.CustomEngineID (Read or Write)

Display Name	CustomEngineID
Description	UserEngineID User given EngineID
Legal Values	String of up to 24 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SNMP.DiscoveryPort (Read or Write)

Display Name	Discovery Port
Description	Specifies the SNMP Discovery Port
Legal Values	Integer values from 1 to 65535.
Default Value	161
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	The port number to be set can not be the same as any other services port number.
Is Platform Dependent	No

iDRAC.SNMP.EngineID (Read Only)

Display Name	SNMP V3 Engine ID
Description	Specifies SNMP V3 Engine ID to be used to receive the SNMP v3 Trap
Legal Values	String of up to 60 ASCII characters.
Default Value	0x800002A204010203040506070809

Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMP.SNMPProtocol (Read or Write)

Display Name	SNMP Protocol
Description	SNMP Protocol
Legal Values	• All - 0 • SNMPv3 - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMP.TrapFormat (Read or Write)

Display Name	SNMP Trap Format
Description	SNMP Trap Format
Legal Values	• SNMPv1 - 0 • SNMPv2 - 1 • SNMPv3 - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPAlert.Destination (Read or Write)

Display Name	Alert Destination
Description	Specifies the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None

Is Platform Dependent	No

iDRAC.SNMPAlert.SNMPv3UserID (Read Only)

Display Name	SNMP V3 User Index
Description	Indicates the index of the iDRAC user that this SNMP alert destination has been configured to use when sending SNMP v3 traps.
Legal Values	Integer values from 0 to 16.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPAlert.SNMPv3Username (Read or Write)

Display Name	SNMP V3 User Name
Description	Specifies the name of the iDRAC user that this SNMP alert destination is configured to use when sending SNMP v3 traps.
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	Value to be set must be an existing iDRAC user name, and that iDRAC user must be enabled with SNMPv3 support also enabled for that user.
Is Platform Dependent	No

iDRAC.SNMPAlert.State (Read or Write)

Display Name	State
Description	Enable SNMP Alert State
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPTrapIPv4.DestIPv4Addr (Read or Write)

Display Name	Destination IPv4 Address
Description	See SNMPAlert.1-4.Destination
Legal Values	String of up to 15 ASCII characters.
Default Value	0.0.0.0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPTrapIPv4.DestinationNum (Read Only)

Display Name	Destination Number
Description	idrac.embedded.1#
Legal Values	Integer values from 1 to 4.
Default Value	1
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPTrapIPv4.State (Read or Write)

Display Name	State
Description	See SNMPAlert.1-4.Enable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPTrapIPv6.DestIPv6Addr (Read or Write)

Display Name	Destination IPv6 Address
Description	See SNMPAlert.5-8.Destination
Legal Values	String of up to 39 ASCII characters.

Default Value	::
Write Privilege	Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPTrapIPv6.DestinationNum (Read Only)

Display Name	Destination Number
Description	Identifier number for the trap destination.
Legal Values	Integer values from 1 to 4.
Default Value	1
Write Privilege	Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SNMPTrapIPv6.State (Read or Write)

Display Name	State
Description	See SNMPAlert.5-8.Enable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SPDM.DeviceList (Read or Write)

Display Name	DeviceList
Description	Device List for allow list/ deny list based on ListType
Legal Values	String of up to 4000 ASCII characters.
Default Value	1000:00A5:1028:2114,1000:00A5:1028:2115,1000:00A5:1028:2117,1000:00A5:1028:213A,1000:00A5:1028:213B,1000:00A5:1028:213C,1000:00A5:1028:213D,1000:00A5:1028:213E,1000:00A5:1028:213F,1000:00A5:1028:2140,1000:00A5:1028:2141,1000:00A5:1028:2142,1000:00A5:1028:2143,1000:00A5:1028:2144,1000:00A5:1028:2145,1000:00A5:1028:2146,1000:00A5:1028:2147,1000:00A5:1028:2148,1000:00A5:1028:2149,1000:00A5:1028:214A,1000:00A5:1028:214B,1000:00A5:1028:214C,1000:00A5:1028:214D,1000:00A5:1028:214E,1000:00A5:1028:214F,1000:00A5:1028:2150,1000:00A5:1028:2151,1000:00A5:1028:2152,1000:00A5:1028:2153,1000:00A5:1028:2154,1000:00A5:1028:2155,1000:00A5:1028:2156,1000:00A5:1028:2157,1000:00A5:1028:2158,1000:00A5:1028:2159,1000:00A5:1028:215A,1000:00A5:1028:215B,1000:00A5:1028:215C,1000:00A5:1028:215D,1000:00A5:1028:215E,1000:00A5:1028:215F,1000:00A5:1028:2160,1000:00A5:1028:2161,1000:00A5:1028:2162,1000:00A5:1028:2163,1000:00A5:1028:2164,1000:00A5:1028:2165,1000:00A5:1028:2166,1000:00A5:1028:2167,1000:00A5:1028:2168,1000:00A5:1028:2169,1000:00A5:1028:216A,1000:00A5:1028:216B,1000:00A5:1028:216C,1000:00A5:1028:216D,1000:00A5:1028:216E,1000:00A5:1028:216F,1000:00A5:1028:2170,1000:00A5:1028:2171,1000:00A5:1028:2172,1000:00A5:1028:2173,1000:00A5:1028:2174,1000:00A5:1028:2175,1000:00A5:1028:2176,1000:00A5:1028:2177,1000:00A5:1028:2178,1000:00A5:1028:2179,1000:00A5:1028:217A,1000:00A5:1028:217B,1000:00A5:1028:217C,1000:00A5:1028:217D,1000:00A5:1028:217E,1000:00A5:1028:217F,1000:00A5:1028:2180,1000:00A5:1028:2181,1000:00A5:1028:2182,1000:00A5:1028:2183,1000:00A5:1028:2184,1000:00A5:1028:2185,1000:00A5:1028:2186,1000:00A5:1028:2187,1000:00A5:1028:2188,1000:00A5:1028:2189,1000:00A5:1028:218A,1000:00A5:1028:218B,1000:00A5:1028:218C,1000:00A5:1028:218D,1000:00A5:1028:218E,1000:00A5:1028:218F,1000:00A5:1028:2190,1000:00A5:1028:2191,1000:00A5:1028:2192,1000:00A5:1028:2193,1000:00A5:1028:2194,1000:00A5:1028:2195,1000:00A5:1028:2196,1000:00A5:1028:2197,1000:00A5:1028:2198,1000:00A5:1028:2199,1000:00A5:1028:219A,1000:00A5:1028:219B,1000:00A5:1028:219C,1000:00A5:1028:219D,1000:00A5:1028:219E,1000:00A5:1028:219F,1000:00A5:1028:21A0,1000:00A5:1028:21A1,1000:00A5:1028:21A2,1000:00A5:1028:21A3,1000:00A5:1028:21A4,1000:00A5:1028:21A5,1000:00A5:1028:21A6,1000:00A5:1028:21A7,1000:00A5:1028:21A8,1000:00A5:1028:21A9,1000:00A5:1028:21AA,1000:00A5:1028:21AB,1000:00A5:1028:21AC,1000:00A5:1028:21AD,1000:00A5:1028:21AE,1000:00A5:1028:21AF,1000:00A5:1028:21B0,1000:00A5:1028:21B1,1000:00A5:1028:21B2,1000:00A5:1028:21B3,1000:00A5:1028:21B4,1000:00A5:1028:21B5,1000:00A5:1028:21B6,1000:00A5:1028:21B7,1000:00A5:1028:21B8,1000:00A5:1028:21B9,1000:00A5:1028:21BA,1000:00A5:1028:21BB,1000:00A5:1028:21BC,1000:00A5:1028:21BD,1000:00A5:1028:21BE,1000:00A5:1028:21BF,1000:00A5:1028:21C0,1000:00A5:1028:21C1,1000:00A5:1028:21C2,1000:00A5:1028:21C3,1000:00A5:1028:21C4,1000:00A5:1028:21C5,1000:00A5:1028:21C6,1000:00A5:1028:21C7,1000:00A5:1028:21C8,1000:00A5:1028:21C9,1000:00A5:1028:21CA,1000:00A5:1028:21CB,1000:00A5:1028:21CC,1000:00A5:1028:21CD,1000:00A5:1028:21CE,1000:00A5:1028:21CF,1000:00A5:1028:21D0,1000:00A5:1028:21D1,1000:00A5:1028:21D2,1000:00A5:1028:21D3,1000:00A5:1028:21D4,1000:00A5:1028:21D5,1000:00A5:1028:21D6,1000:00A5:1028:21D7,1000:00A5:1028:21D8,1000:00A5:1028:21D9,1000:00A5:1028:21DA,1000:00A5:1028:21DB,1000:00A5:1028:21DC,1000:00A5:1028:21DD,1000:00A5:1028:21DE,1000:00A5:1028:21DF,1000:00A5:1028:21E0,1000:00A5:1028:21E1,1000:00A5:1028:21E2,1000:00A5:1028:21E3,1000:00A5:1028:21E4,1000:00A5:1028:21E5,1000:00A5:1028:21E6,1000:00A5:1028:21E7,1000:00A5:1028:21E8,1000:00A5:1028:21E9,1000:00A5:1028:21EA,1000:00A5:1028:21EB,1000:00A5:1028:21EC,1000:00A5:1028:21ED,1000:00A5:1028:21EE,1000:00A5:1028:21EF,1000:00A5:1028:21F0,1000:00A5:1028:21F1,1000:00A5:1028:21F2,1000:00A5:1028:21F3,1000:00A5:1028:21F4,1000:00A5:1028:21F5,1000:00A5:1028:21F6,1000:00A5:1028:21F7,1000:00A5:1028:21F8,1000:00A5:1028:21F9,1000:00A5:1028:21FA,1000:00A5:1028:21FB,1000:00A5:1028:21FC,1000:00A5:1028:21FD,1000:00A5:1028:21FE,1000:00A5:1028:21FF
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

Notes These attributes are only available if you have SPDM supported devices installed.

iDRAC.SPDM.Enable (Read or Write)

Display Name	Enable
Description	SPDM feature enable status
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	These attributes are only available if you have SPDM supported devices installed.

iDRAC.SPDM.ListType (Read or Write)

Display Name	ListType
Description	List type for DeviceList attribute
Legal Values	• Allowlist - 0 • Denylist - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	These attributes are only available if you have SPDM supported devices installed.

iDRAC.SSH.Banner (Read or Write)

Display Name	SSH Banner
Description	Custom banner message showed in iDRAC SSH login prompt
Legal Values	String of up to 2048 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SSH.Enable (Read or Write)

Display Name	SSH Enable
Description	Enables or Disables SSH
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SSH.MaxSessions (Read Only)

Display Name	SSH Maximum Sessions
Description	Maximum number of SSH sessions allowed
Legal Values	Integer values from 1 to 4.
Default Value	4
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SSH.Port (Read or Write)

Display Name	SSH Port
Description	Specifies the port number for the iDRAC SSH interface
Legal Values	Integer values from 1 to 65535.
Default Value	22
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	The port number to be set can not be the same as any other services port number.
Is Platform Dependent	No

iDRAC.SSH.Timeout (Read or Write)

Display Name	SSH Idle Timeout
Description	Defines the secure shell idle timeout. The special value 0 disables the timeout.
Legal Values	Integer values from 60 to 10800.

Default Value	1800
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.SSHCrypto.Ciphers (Read or Write)

Display Name	Ciphers
Description	Specifies the SSH ciphers.
Legal Values	String of up to 1024 ASCII characters.
Default Value	chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SSHCrypto.HostKeyAlgorithms (Read or Write)

Display Name	Host Key Algorithms
Description	Specifies the SSH host key algorithms.
Legal Values	String of up to 1024 ASCII characters.
Default Value	rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SSHCrypto.KexAlgorithms (Read or Write)

Display Name	Key Exchange Algorithms
Description	Specifies the SSH key exchange algorithms.
Legal Values	String of up to 1024 ASCII characters.
Default Value	curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** No

iDRAC.SSHCrypto.MACs (Read or Write)

Display Name MACs

Description Specifies the SSH MACs.

Legal Values String of up to 1024 ASCII characters.

Default Value umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.SecureDefaultPassword.ForceChangePassword (Read or Write)

Display Name Force Change Password

Description Force change of password if default password is still in effect.

Legal Values

- False - 0
- True - 1

Default Value 0

Write Privilege Configure Users

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.Security.CsrCommonName (Read or Write)

Display Name CSR Common Name

Description Specifies the CSR Common Name (CN) being certified (usually the web servers Fully Qualified Domain Name (FQDN)).

Legal Values String of up to 64 ASCII characters.

Default Value None

Write Privilege Configure iDRAC

License Required Not Applicable

Dependency None

**Is Platform
Dependent** No

iDRAC.Security.CsrCountryCode (Read or Write)

Display Name	CSR Country Code
Description	Specifies the CSR Country Code (CC).
Legal Values	String of up to 2 ASCII characters.
Default Value	US
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrEmailAddr (Read or Write)

Display Name	CSR Email Address
Description	Specifies the CSR email address.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrKeySize (Read or Write)

Display Name	CSR Key Size
Description	Specifies the SSL asymmetric key size for the CSRs.
Legal Values	• 2048 - 2048 • 4096 - 4096
Default Value	2048
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrLocalityName (Read or Write)

Display Name	CSR Locality Name
Description	Specifies the CSR Locality (L).
Legal Values	String of up to 64 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrOrganizationName (Read or Write)

Display Name	CSR Organization Name
Description	Specifies the CSR Organization Name (O)
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrOrganizationUnit (Read or Write)

Display Name	CSR Organization Unit
Description	Specifies the CSR Organization Unit (OU)
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrStateName (Read or Write)

Display Name	CSR State Name
Description	Specifies the CSR State Name (S).
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.CsrSubjectAltName (Read or Write)

Display Name	CSR Subject Alternate Name
Description	Specifies the CSR Subject Alternative Name
Legal Values	String of up to 2048 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.FIPSMODE (Read or Write)

Display Name	FIPS Mode
Description	Enables or Disables the FIPS mode compliance. Enabling FIPS mode resets iDRAC configuration to factory defaults.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.FIPSVersion (Read Only)

Display Name	FIPS Version
Description	FIPS canister version.
Legal Values	String of up to 40 ASCII characters.
Default Value	DELL OpenSSL FIPS Crypto Module v2.6
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.IPMIBootstrapCredentialProvisioning (Read or Write)

Display Name	IPMI Bootstrap Credential Provisioning

Description	Enable or Disable IPMI Bootstrap Credential provisioning
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.Security.MaxIPMIBootstrapCredentialAccounts (Read Only)

Display Name	Max IPMI Bootstrap Credential Accounts
Description	Max Number Of Allowed IPMI Bootstrap Credential Accounts
Legal Values	Integer values from 1 to 10.
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.MinimumPasswordScore (Read or Write)

Display Name	Minimum Score
Description	Password must have this minimum strength score.
Legal Values	• No Protection - 0 • Weak Protection - 1 • Moderate Protection - 2 • Strong Protection - 3
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Security.PasswordMinimumLength (Read or Write)

Display Name	Minimum Length
Description	Password must be a minimum of the specified characters.
Legal Values	Integer values from 0 to 20.

Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Property will be ignored if PasswordRequireRegex is not blank.
Is Platform Dependent	No

iDRAC.Security.PasswordRequireNumbers (Read or Write)

Display Name	Numbers
Description	Password must include at least 1 Numeric character
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Property will be ignored if PasswordRequireRegex is not blank.
Is Platform Dependent	No

iDRAC.Security.PasswordRequireRegex (Read or Write)

Display Name	Regex
Description	Password must pass this Regular Expression.
Legal Values	String of up to 100 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Property will override other policies except for MinimumPasswordScore
Is Platform Dependent	No

iDRAC.Security.PasswordRequireSymbols (Read or Write)

Display Name	Symbols
Description	Password must include at least 1 Symbolic character
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Property will be ignored if PasswordRequireRegex is not blank.

Is Platform Dependent	No

iDRAC.Security.PasswordRequireUpperCase (Read or Write)

Display Name	Upper Case Letters
Description	Password must include at least 1 Upper Case Letter
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Property will be ignored if PasswordRequireRegex is not blank.
Is Platform Dependent	No

iDRAC.Security.ReservedAccountUserEnable (Read or Write)

Display Name	Reserved Account User Enable
Description	Enable or disable the Reserved Account user feature.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	This attribute is only available when a supported .pm file is installed.

iDRAC.Security.ReservedAccountUserID (Read or Write)

Display Name	Reserved Account User ID
Description	The user id of the Reserved Account User. Valid user id 3..16 or 0 for none.
Legal Values	Integer values from 0 to 16.
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	This attribute is only available when a supported .pm file is installed.

iDRAC.SecurityCertificate.CertValidFrom (Read Only)

Display Name	Cert Valid From
Description	Specifies the earliest time and date on which the certificate is valid.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.CertValidTo (Read Only)

Display Name	Cert Valid To
Description	Specifies the time and date past which the certificate is no longer valid.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.CertificateInstance (Read Only)

Display Name	Certificate Instance
Description	Represents the instance of that type of certificate.
Legal Values	Integer values from 1 to 16.
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.CertificateType (Read Only)

Display Name	Certificate Type
Description	Specifies the type of certificate.
Legal Values	• WEBSERVER_SSL - 1 • LDAP_CA - 2 • CUSTOM_SIGNING_CERT - 3 • CLIENT_TRUST_CERT - 4 • FACTORY_IDENTITY_CERT - 5 • SEKM_SSL_CERT - 6 • KMS_SERVER_CA - 7 • RSYSLOG_SERVER_CA - 8 • BIOS_HTTPS_BOOT_CERT - 9 • SMARTCARD_USER - 10 • SMARTCARD_CA - 11 • RSA_CA - 12 • SCEP_CA - 13 • SCV_INVENTORY_CERT_CUSTOMER - 14 • DEL_AUTH_HTTPS - 15 • REMOTE_SYSLOG_CLIENT - 17 • REMOTE_SYSLOG_SERVER - 18 • IEEE802_CLIENT_CERT - 21 • IEEE802_SERVER_CA_CERT - 22 • IEEE802_CUSTOM_SIGNING_CERT - 24 • TPM_IDEVID - 25 • TPM_IAK - 26 • TPM_EK_ECC - 27 • TPM_EK_RSA - 28 • SCV_FW_INVENTORY - 31
Default Value	6
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.ExpiryState (Read Only)

Display Name	Expiry State
Description	Expiry State
Legal Values	• Valid - 0 • AboutToExpire - 1 • Expired - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.IssuerCommonName (Read Only)

Display Name	Issuer Common Name
Description	Specifies the common name of the entity that verified the information and signed the certificate.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.IssuerCountryCode (Read Only)

Display Name	Issuer Country Code
Description	Specifies the country code of the entity that verified the information and signed the certificate.
Legal Values	String of up to 2 ASCII characters.
Default Value	US
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.IssuerLocality (Read Only)

Display Name	Issuer Locality
Description	Specifies the locality of the entity that verified the information and signed the certificate.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.IssuerOrganization (Read Only)

Display Name	Issuer Organization
Description	Specifies the organization of the entity that verified the information and signed the certificate.
Legal Values	String of up to 64 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.IssuerOrganizationalUnit (Read Only)

Display Name	Issuer Organizational Unit
Description	Specifies the organizational unit of the entity that verified the information and signed the certificate.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.IssuerState (Read Only)

Display Name	Issuer State
Description	Specifies the state name of the entity that verified the information and signed the certificate.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SerialNumber (Read Only)

Display Name	Serial Number
Description	Specifies a unique number to identify the certificate.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SubjectCommonName (Read Only)

Display Name	Subject Common Name
Description	Specifies the common name of the entity a certificate belongs to.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SubjectCountryCode (Read Only)

Display Name	Subject Country Code
Description	Specifies the country code of the entity a certificate belongs to.
Legal Values	String of up to 2 ASCII characters.
Default Value	US
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SubjectLocality (Read Only)

Display Name	Subject Locality
Description	Specifies the locality of the entity a certificate belongs to.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SubjectOrganization (Read Only)

Display Name	Subject Organization
Description	Specifies the organization of the entity a certificate belongs to.
Legal Values	String of up to 64 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SubjectOrganizationalUnit (Read Only)

Display Name	Subject Organizational Unit
Description	Specifies the organizational unit of the entity a certificate belongs to.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SecurityCertificate.SubjectState (Read Only)

Display Name	Subject State
Description	Specifies the state of the entity a certificate belongs to.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Serial.BaudRate (Read or Write)

Display Name	Serial Baud Rate
Description	Sets the Baud rate on the iDRAC serial port
Legal Values	• 9600 - 9600 • 19200 - 19200 • 57600 - 57600 • 115200 - 115200
Default Value	57600
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.Serial.Command (Read or Write)

Display Name	Serial Console Command
Description	Specifies a serial command that is executed after the user logs into the serial console interface
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.Serial.Enable (Read or Write)

Display Name	Serial Console Enable
Description	Enables or Disables the iDRAC serial console interface
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.Serial.FlowControl (Read or Write)

Display Name	Serial Flow Control
Description	RAC Serial Flow Control
Legal Values	• None - 0 • RTS/CTS - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	Yes
Notes	This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.Serial.HistorySize (Read or Write)

Display Name	Serial History Size
Description	Specifies the maximum size of the serial history buffer
Legal Values	Integer values from 0 to 8192.
Default Value	8192
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.Serial.IdleTimeout (Read or Write)

Display Name	Serial Console Idle Timeout
Description	The maximum number of seconds to wait before an idle serial console session is disconnected. The special value 0 disables the timeout.
Legal Values	Integer values from 60 to 1920.
Default Value	300
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.Serial.NoAuth (Read or Write)

Display Name	Serial Console No Authentication
Description	Enables or Disables iDRAC serial console login authentication
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

Notes This group will only be available if a physical DB9 serial port is present in the server.

iDRAC.SerialCapture.Enable (Read or Write)

Display Name	Serial Capture Enable
Description	Enables or disables serial data capture operation.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.SerialCapture.SerialDataSize (Read Only)

Display Name	Serial Data Size
Description	Specifies the size of the serial data captured.
Legal Values	Integer values from 0 to 524288.
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.SerialRedirection.Enable (Read or Write)

Display Name	Serial Communication Redirection Enable
Description	Enables or Disables the console for COM2 port redirection
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	This is supported only for rack and tower systems.

iDRAC.SerialRedirection.QuitKey (Read or Write)

Display Name	Serial Console Quit Key
Description	This key or key combination terminates the Virtual Console when using the console COM2 command. The valid quitkey should start with ^ and has to end with any of the following characters: a-zA-Z[]\^_ (i.e. letter or one of 5 special characters).
Legal Values	String of up to 2 ASCII characters.
Default Value	^\
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	This is supported only for rack and tower systems.

iDRAC.ServerBoot.BootOnce (Read or Write)

Display Name	Boot Once
Description	Enable Boot Once
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServerBoot.FirstBootDevice (Read or Write)

Display Name	First Boot Device
Description	Specify the First Boot Device.
Legal Values	String of up to 64 ASCII characters.
Default Value	Normal
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.ChipsetSATASupported (Read or Write)

Display Name	SMART Monitoring of Chipset SATA
Description	Monitors SMART attributes of devices behind chipset SATA controller and audits appropriately in Lifecycle Log.
Legal Values	• Disabled - 0 • Enabled - 1 • NA - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.EnableOSMetricInjection (Read or Write)

Display Name	Enable OS Metrics to inject from the host OS to iDRAC
Description	Enable OS Metric Injection from host OS to iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.HostSNMPAlert (Read or Write)

Display Name	Host SNMP Alert
Description	Host SNMP Alert
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.HostSNMPGet (Read or Write)

Display Name	Host SNMP Get
Description	Host SNMP Get
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.HostSNMPOMSAAlert (Read or Write)

Display Name	iDRAC To OMSA SNMP Alert Mapping
Description	Maps the iDRAC LCL into OMSA SNMP traps.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	iDRAC.ServiceModule.HostSNMPAlert should be Enabled
Is Platform Dependent	No

iDRAC.ServiceModule.LCLReplication (Read or Write)

Display Name	LCL Replication
Description	Enable Lifecycle Log Replication
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	With OMSA presence automatically set to Disabled.
Is Platform Dependent	No

iDRAC.ServiceModule.OMSAPresence (Read Only)

Display Name	OMSA Presence
Description	Indicates if OMSA is present on the host or not.
Legal Values	• Not Present - 0 • Present - 1 • NA - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.OSInfo (Read or Write)

Display Name	Sharing OS information via service module
Description	Enable Sharing OS Information via service module
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	Provide OS information via iDRAC Service Module
Is Platform Dependent	No

iDRAC.ServiceModule.SSEventCorrelation (Read or Write)

Display Name	SDS Event Correlation
Description	Maps the Storage Spaces events on host OS onto Lifecycle Log.
Legal Values	• Disabled - 0 • Enabled - 1 • NA - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.ServiceModuleEnable (Read or Write)

Display Name	Service Module Enabled
Description	Enable Service Module
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.ServiceModuleState (Read Only)

Display Name	ServiceModule service state on host
Description	Specifies the state of the service module on the system
Legal Values	• Not Running - 0 • Running - 1 • Not running (TLS error) - 2 • Running (Limited functionality) - 3
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.ServiceModuleVersion (Read Only)

Display Name	iDRAC Service Module Version
Description	Provides the installed version of iDRAC Service Module (iSM).
Legal Values	String of up to 256 ASCII characters.
Default Value	NA
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.SoftwareRAIDSupported (Read Only)

Display Name	Software RAID
Description	Enables or disables SWRAID feature on the host
Legal Values	• Disabled - 0 • Enabled - 1 • NA - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.WMIInfo (Read or Write)

Display Name	Populate WMI information via ServiceModule
Description	Populate WMI information via ServiceModule
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.ServiceModule.WatchdogRecoveryAction (Read or Write)

Display Name	Recovery action on watchdog alert
Description	Specifies the recovery action on watchdog alert
Legal Values	• None - 0 • Reboot - 1 • Poweroff - 2 • Powercycle - 3
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	The value cannot be set if WatchdogState is Disabled.
Is Platform Dependent	No

iDRAC.ServiceModule.WatchdogResetTime (Read or Write)

Display Name	System reset time on watchdog alert
Description	Specifies the System reset time on watchdog alert
Legal Values	Integer values from 60 to 720.
Default Value	480
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	The value cannot be set if WatchdogState is Disabled.
Is Platform Dependent	No

iDRAC.ServiceModule.WatchdogState (Read or Write)

Display Name	Watchdog timer via service module
Description	Enable watchdog timer via service module
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	The value will be disabled if OMSA is detected or OS Watchdog is enabled.
Is Platform Dependent	No

iDRAC.ServiceModule.iDRACHardReset (Read or Write)

Display Name	iDRAC Hard Reset
Description	ServiceModule Attribute for iDRAC reset
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Server Control and Configuration
License Required	Not Applicable
Dependency	iDRAC.ServiceModule.ServiceModuleEnable should be Enabled
Is Platform Dependent	No

iDRAC.ServiceModule.iDRACSSOLauncher (Read or Write)

Display Name	iDRAC SSO Launcher
Description	iDRAC SSO login via Host OS

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SmartCard.SmartCardCRLEnable (Read or Write)

Display Name	Smart Card CRL Enable
Description	Enables or disables the Certificate Revocation List (CRL).
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SmartCard.SmartCardLogonEnable (Read or Write)

Display Name	Smart Card Logon Enable
Description	Enables, disables, or enables with Remote RACADM support for access to iDRAC using a smart card
Legal Values	• Disabled - 0 • Enabled - 1 • Enabled With Racadm - 2
Default Value	0
Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SmartCard.SmartCardOCSPEnable (Read or Write)

Display Name	Smart Card OCSP Enable
Description	Enables or disables the Online Certificate Status Protocol (OCSP)
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0

Write Privilege	Configure iDRAC, Configure Users
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultIPAddress (Read or Write)

Display Name	Default IP Address
Description	Default IP address for saving SupportAssist collections to network share.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultPassword (Read or Write)

Display Name	Default Password
Description	Default password for saving SupportAssist collections to network share.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultProtocol (Read or Write)

Display Name	Default Protocol
Description	Default protocol (NFS/CIFS Only) for saving SupportAssist collections.
Legal Values	• NFS - 1 • CIFS - 2 • HTTP - 3 • HTTPS - 4 • TFTP - 5 • FTP - 6
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultProtocolPort (Read or Write)

Display Name	Default Protocol Port
Description	Default Protocol Port value
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultShareName (Read or Write)

Display Name	Default Share Name
Description	Default share name for saving SupportAssist collections to network share.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultUserName (Read or Write)

Display Name	Default User Name
Description	Default user name for saving SupportAssist collections to network share.
Legal Values	String of up to 320 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.DefaultWorkgroupName (Read or Write)

Display Name	Default Workgroup Name
Description	Default workgroup name for saving SupportAssist collections to network share.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.EmailOptIn (Read Only)

Display Name	Email Opt In
Description	Option to receive E-mails from Dell on case creation and collection upload.
Legal Values	• No - 0 • Yes - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Registration ID needs to be obtained before Email option configuration
Is Platform Dependent	No

iDRAC.SupportAssist.EventBasedAutoCollection (Read Only)

Display Name	SupportAssist Event Based Auto Collection
Description	Indicates whether SupportAssist event based auto collection features is enabled on this system.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Can be enabled only when SupportAssistEnableState is configured to 1-Enabled
Is Platform Dependent	No

iDRAC.SupportAssist.FilterAutoCollections (Read Only)

Display Name	Filter Auto Collections
Description	Indicates whether auto collections need to be filtered for identification information.
Legal Values	• No - 0 • Yes - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.HostOSProxyAddress (Read Only)

Display Name	Host OS Proxy Address
Description	Host OS proxy address
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	HostOSProxyConfigured should be Yes-1
Is Platform Dependent	No

iDRAC.SupportAssist.HostOSProxyConfigured (Read Only)

Display Name	Host OS Proxy Configured
Description	Indicates whether Host OS uses proxy configuration to connect to Internet.
Legal Values	• No - 0 • Yes - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.HostOSProxyPassword (Read Only)

Display Name	Host OS Proxy Password
Description	Host OS proxy password

Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	HostOSProxyConfigured should be Yes-1
Is Platform Dependent	No

iDRAC.SupportAssist.HostOSProxyPort (Read Only)

Display Name	Host OS Proxy Port
Description	Host OS proxy port
Legal Values	Integer values from 1 to 65535.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	HostOSProxyConfigured should be Yes-1
Is Platform Dependent	No

iDRAC.SupportAssist.HostOSProxyUserName (Read Only)

Display Name	Host OS Proxy User Name
Description	Host OS proxy username
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	HostOSProxyConfigured should be Yes-1
Is Platform Dependent	No

iDRAC.SupportAssist.NativeOSLogsCollectionSupported (Read Only)

Display Name	Native OS Logs Collection Supported
Description	Indicates whether Host OS supports native OS logs collection.
Legal Values	• None - 0 • FullReport - 1 • FilteredReport - 2 • Both - 3
Default Value	0

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.PreferredLanguage (Read or Write)

Display Name	Preferred Language
Description	Preferred Language for E-mail communication from Dell
Legal Values	• English - 0 • German - 1 • French - 2 • Japanese - 3 • Spanish - 4 • Simplified Chinese - 5
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Registration ID needs to be obtained before changing language settings.
Is Platform Dependent	No

iDRAC.SupportAssist.ProSupportPlusRecommendationsReport (Read Only)

Display Name	ProSupport Plus Recommendations Report
Description	Indicates whether this server will be included for recommendations in ProSupport Plus Recommendations Report
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	ScheduleBasedAutoCollection is Enabled and set to Weekly or Monthly Schedule
Is Platform Dependent	No

iDRAC.SupportAssist.RegistrationID (Read Only)

Display Name	SupportAssist Registration ID
Description	Specifies the SupportAssist Registration ID if the system was registered with Dell.
Legal Values	String of up to 64 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.RequestTechnicianForPartsDispatch (Read Only)

Display Name	Request Technician For Parts Dispatch
Description	Indicates whether onsite technician is required to replace the part that is being dispatched for the alert that is being monitored.
Legal Values	• No - 0 • Yes - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SupportAssist.SupportAssistEnableState (Read Only)

Display Name	SupportAssist Enable State
Description	Indicates whether SupportAssist auto collection features are enabled on this system.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Registration ID needs to be obtained before SupportAssistEnabledState can be toggled.
Is Platform Dependent	No

iDRAC.SupportAssist.iDRACFirstPowerUpDateTime (Read Only)

Display Name	iDRAC First Power Up Date Time
Description	iDRACs First Power Up Date / Time
Legal Values	String of up to 64 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SwitchConnectionView.Enable (Read or Write)

Display Name	Enable
Description	This Attribute is for Enabling/Disabling the Switch Connection View.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.AcSysRecovery (Read or Write)

Display Name	AcSysRecovery
Description	Specifies what State the System will be after AC Recovery
Legal Values	String of up to 18 ASCII characters.
Default Value	003c003c0058020000
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.BIOSStatus (Read or Write)

Display Name	BIOS Status
Description	Provides BIOS status.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.BladeSlotInfo (Read Only)

Display Name	Blade Slot Info
Description	Provides blade slot information.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.CMCIPv6Info (Read Only)

Display Name	CMC IPv6 Info
Description	Provides CMC IPv6 information.
Legal Values	String of up to 160 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.CMCIPv6Url (Read Only)

Display Name	CMC IPv6 URL
Description	Provides the CMC IPv6 URL.
Legal Values	String of up to 160 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.CMCInfo (Read Only)

Display Name	CMC Info
Description	Provides CMC information.
Legal Values	String of up to 128 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.CMCUrl (Read Only)

Display Name	CMC URL
Description	Provides the CMC URL.
Legal Values	String of up to 160 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.FWVersion (Read or Write)

Display Name	BIOS Version
Description	String displays the current System BIOS Version Number
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.GUID (Read or Write)

Display Name	GUID
Description	Specifies the system GUID.
Legal Values	String of up to 34 ASCII characters.
Default Value	00000000000000000000000000000000
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.LocalConsoleLockOut (Read or Write)

Display Name	Local Console Lockout State
Description	Specifies the local console lockout state.
Legal Values	Integer values from 0 to 65535.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.POSTCode (Read Only)

Display Name	POST Code For System
Description	System POST Code.
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.RebrandInfo (Read or Write)

Display Name	Rebrand Info
Description	Provides rebrand information.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.SystemId (Read Only)

Display Name	System ID
Description	Provides the system ID.
Legal Values	String of up to 4 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.SystemModel (Read Only)

Display Name	System Model
Description	Provides the system model.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysInfo.SystemRev (Read or Write)

Display Name	System Revision
Description	Provides the system revision.
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.Port (Read or Write)

Display Name	Sys Log Port
Description	Remote syslog port number
Legal Values	Integer values from 1 to 65535.
Default Value	514
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.PowerLogEnable (Read or Write)

Display Name	Power Log Enable
Description	Enable Power Logs
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.PowerLogInterval (Read or Write)

Display Name	Power Log Interval
Description	Set Power Log Interval
Legal Values	Integer values from 1 to 1440.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.Server1 (Read or Write)

Display Name	Sys Log Server 1
Description	Name of remote syslog server
Legal Values	String of up to 63 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.Server2 (Read or Write)

Display Name	Sys Log Server 2
Description	Name of remote syslog server
Legal Values	String of up to 63 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.Server3 (Read or Write)

Display Name	Sys Log Server 3
Description	Name of remote syslog server
Legal Values	String of up to 63 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.SysLogEnable (Read or Write)

Display Name	Sys Log Enable
Description	Enables or disables remote syslog
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.secureclientauth (Read or Write)

Display Name	Secure Sys Log Client Auth Mode
Description	Secure remote syslog client authentication mode
Legal Values	• Anonymous - 0 • Certificate - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None

Is Platform Dependent	No

iDRAC.SysLog.secureport (Read or Write)

Display Name	Sys Log Secure Port
Description	Secure remote syslog port number
Legal Values	Integer values from 1 to 65535.
Default Value	6514
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.secureserver1 (Read or Write)

Display Name	Sys Log Secure Server 1
Description	Name of secure remote syslog server
Legal Values	String of up to 63 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.SysLog.securesyslogenable (Read or Write)

Display Name	Secure Sys Log Enable
Description	Enables or disables secure remote syslog
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.Telco-EdgeServer.HeartBeatEnable (Read or Write)

Display Name	HeartBeat Enable

Description	HeartBeat monitoring for Witness Node Enable/disable
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.Telemetry.EnableMetricInjection (Read or Write)

Display Name	Enable injection of external metrics into iDRAC Telemetry Service
Description	Indicates Metric Injection enabled or disabled on iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Indicates if Telemetry is enabled or disabled on iDRAC.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription1 (Read Only)

Display Name	Telemetry Subscription 1
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC

License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription2 (Read Only)

Display Name	Telemetry Subscription 2
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription3 (Read Only)

Display Name	Telemetry Subscription 3
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription4 (Read Only)

Display Name	Telemetry Subscription 4
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription5 (Read Only)

Display Name	Telemetry Subscription 5
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription6 (Read Only)

Display Name	Telemetry Subscription 6
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription7 (Read Only)

Display Name	Telemetry Subscription 7
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Telemetry.TelemetrySubscription8 (Read Only)

Display Name	Telemetry Subscription 8
Description	Displays the JSON string describing the current Telemetry subscription by a Redfish client.
Legal Values	String of up to 256 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryAggregationMetrics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryAggregationMetrics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryAggregationMetrics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	0

Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No
Notes	Configuring Telemetry reports using RACADM is limited to a few properties for reports of default "Periodic" type only. For example, configuring ReportInterval on AggregationMetrics report of type OnRequest gets ignored through RACADM interface. To update the ReportInterval and ReportTriggers properties, perform a PATCH method using Redfish interface on the following URI: /redfish/v1/TelemetryService/MetricReportDefinitions/<MetricReportDefinitions -Id>.

iDRAC.TelemetryAggregationMetrics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUMemMetrics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUMemMetrics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUMemMetrics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUMemMetrics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPURegisters.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.

Legal Values	Integer values from 0 to 600.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPURegisters.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPURegisters.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPURegisters.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.

Legal Values	String of up to 512 ASCII characters.
Default Value	IERRCriticalTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUSensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUSensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUSensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60

Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryCPUSensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	CPUCriticalTrigger, CPUWarnTrigger, TMPCpuCriticalTrigger, TMPCpuWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCPortStatistics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCPortStatistics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC

License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCPortStatistics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCPortStatistics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCSensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License

Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCSensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCSensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFCSensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFPGASensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFPGASensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFPGASensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFPGASensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFanSensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFanSensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFanSensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryFanSensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	FANCriticalTrigger, FANWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUMetrics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUMetrics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUMetrics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUMetrics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUStatistics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	600
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUStatistics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUStatistics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	600
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryGPUStatistics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryMemorySensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryMemorySensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryMemorySensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryMemorySensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	MEMCriticalTrigger, MEMWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICSensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICSensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICSensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICSensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICStatistics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICStatistics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICStatistics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNICStatistics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNVMeSMARTData.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 3600.
Default Value	3600
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNVMeSMARTData.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNVMeSMARTData.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	3600
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryNVMeSMARTData.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	NVMeCriticalTrigger, NVMeWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPSUMetrics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPSUMetrics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPSUMetrics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPSUMetrics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	VLTCriticalTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerMetrics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerMetrics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerMetrics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerMetrics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerStatistics.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerStatistics.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerStatistics.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryPowerStatistics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySerialLog.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency

Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySerialLog.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySerialLog.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	40
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySerialLog.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License

Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageDiskSMARTData.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 3600.
Default Value	3600
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageDiskSMARTData.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageDiskSMARTData.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	3600
Write Privilege	Configure iDRAC
License Required	Datacenter License

Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageDiskSMARTData.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	PDRCriticalTrigger, PDRWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageSensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageSensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None

Is Platform Dependent	No

iDRAC.TelemetryStorageSensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryStorageSensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySystemUsage.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None

Is Platform Dependent	No

iDRAC.TelemetrySystemUsage.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySystemUsage.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetrySystemUsage.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	TMPCpuCriticalTrigger, TMPCpuWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None

**Is Platform
Dependent** No

iDRAC.TelemetryThermalMetrics.DevicePollFrequency (Read Only)

Display Name Device Poll Frequency
Description Displays the frequency at which the devices are polled.
Legal Values Integer values from 0 to 600.
Default Value 5
Write Privilege Configure iDRAC
License Required Datacenter License
Dependency None
**Is Platform
Dependent** No

iDRAC.TelemetryThermalMetrics.EnableTelemetry (Read or Write)

Display Name Enable Telemetry
Description Enables or disables the Telemetry Report.
Legal Values

- Disabled - 0
- Enabled - 1

Default Value 0
Write Privilege Configure iDRAC
License Required Datacenter License
Dependency None
**Is Platform
Dependent** No

iDRAC.TelemetryThermalMetrics.ReportInterval (Read or Write)

Display Name Report Interval
Description Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values Integer values from 10 to 7200.
Default Value 60
Write Privilege Configure iDRAC
License Required Datacenter License
Dependency None

Is Platform Dependent	No

iDRAC.TelemetryThermalMetrics.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	TMPDiskCriticalTrigger, TMPDiskWarnTrigger, TMPCriticalTrigger, TMPWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryThermalSensor.DevicePollFrequency (Read Only)

Display Name	Device Poll Frequency
Description	Displays the frequency at which the devices are polled.
Legal Values	Integer values from 0 to 600.
Default Value	5
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryThermalSensor.EnableTelemetry (Read or Write)

Display Name	Enable Telemetry
Description	Enables or disables the Telemetry Report.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None

Is Platform Dependent	No

iDRAC.TelemetryThermalSensor.ReportInterval (Read or Write)

Display Name	Report Interval
Description	Allows to configure the interval in seconds at which the reports are generated. Configuring the value 0 will stop the interval-based report generation.
Legal Values	Integer values from 10 to 7200.
Default Value	60
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.TelemetryThermalSensor.ReportTriggers (Read or Write)

Display Name	Report Triggers
Description	Allows to configure the predefined triggers for report generation.
Legal Values	String of up to 512 ASCII characters.
Default Value	TMPCriticalTrigger, TMPWarnTrigger
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No

iDRAC.Time.DayLightOffset (Read or Write)

Display Name	Tune Day Light Offset
Description	Specifies the daylight savings offset (in minutes) to use for the iDRAC Time.
Legal Values	Integer values from 0 to 60.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Time.TimeZoneOffset (Read or Write)

Display Name	Tune Time Zone Offset
Description	Specifies the time zone offset (in minutes) from Greenwich Mean Time (GMT)/Coordinated Universal Time (UTC) to use for the iDRAC Time
Legal Values	Integer values from -43200 to 46800.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Time.Timezone (Read or Write)

Display Name	Time Zone String
Description	Time Zone String
Legal Values	String of up to 32 ASCII characters.
Default Value	CST6CDT
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	For supported possible string values refer to iDRAC GUI Time Zone Settings page, time zone attribute drop down menu.

iDRAC.USB.ConfigurationXML (Read or Write)

Display Name	Configuration XML Mode
Description	Specifies whether configuration can be performed using USB management port.
Legal Values	• Disabled - 0 • Enabled while server has default credential settings only - 1 • Enabled - 2 • Enabled only for compressed configuration files - 3
Default Value	1
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	ConfigurationXML means Server Configuration Profile (SCP) feature.

iDRAC.USB.ManagementPortMode (Read Only)

Display Name	USB Management Port Mode
Description	Provides how USB Management Port is used.
Legal Values	• iDRAC Direct Only - 0
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.USB.PortStatus (Read or Write)

Display Name	iDRAC Front USB Port Status
Description	Enables or disables the iDRAC front USB port.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.USB.ZipPassword (Read or Write)

Display Name	Password for zip file on USB
Description	Specifies password that is used to unlock zip file containing Server Configuration Profile on USB drive.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Server Control and Configuration
License Required	Express License
Dependency	None
Is Platform Dependent	No

iDRAC.Update.FwUpdateIPAddr (Read or Write)

Display Name	Firmware Update IP Address
Description	Specifies the TFTP server address to be used for iDRAC firmware update operations
Legal Values	String of up to 254 ASCII characters.

Default Value	0.0.0.0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	fwUpdateIPAddr attribute is applicable for Monolithic & FX2/FX2s only.

iDRAC.Update.FwUpdatePath (Read or Write)

Display Name	Firmware Update File Path
Description	Specifies TFTP path where iDRAC firmware image resides on TFTP server
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Update.FwUpdateTFTPEnable (Read or Write)

Display Name	Enable or Disable TFTP for Firmware Update
Description	Enables or Disables iDRAC firmware updates from a TFTP server
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.UserDomain.Name (Read or Write)

Display Name	User Domain Name
Description	Specifies the Active Directory user domain name. Must be fully qualified domain name or IP address of the domain controller.
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None

**Is Platform
Dependent** No

iDRAC.Users.AuthenticationProtocol (Read or Write)

Display Name SNMP V3 Authentication Protocol

Description The Authentication Protocol for SNMP v3

Legal Values

- None - 0
- MD5 - 1
- SHA - 2

Default Value 2

Write Privilege Configure Users

License Required Not Applicable

Dependency Need valid username and password to set the attribute. The value could not be set to none if privacy protocol is not none.

**Is Platform
Dependent** No

iDRAC.Users.EmailAddress (Read or Write)

Display Name Email Address

Description Specifies the email address to use for Simple 2FA for the user.

Legal Values String of up to 254 ASCII characters.

Default Value None

Write Privilege Configure Users

License Required Enterprise License

Dependency Both UserName and Password must be configured prior to setting a value.

**Is Platform
Dependent** No

iDRAC.Users.Enable (Read or Write)

Display Name User Admin Enable

Description Enables or Disables an individual user

Legal Values

- Disabled - 0
- Enabled - 1

Default Value 0

Write Privilege Configure Users

License Required Not Applicable

Dependency Both UserName and Password must be configured prior to enabling user

**Is Platform
Dependent** No

iDRAC.Users.EnableSNMPv3Passphrase (Read or Write)

Display Name	EnableSNMPv3Passphrase
Description	Enable SNMP Passphrase
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Editable only if both SNMPv3AuthenticationPassphrase and SNMPv3PrivacyPassphrases are configured.
Is Platform Dependent	No

iDRAC.Users.IPMIKey (Read or Write)

Display Name	Key used for IPMI authentication
Description	IPMI key is used for IPMI authentication
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Need valid username to set the attribute.
Is Platform Dependent	No

iDRAC.Users.IpmiLanPrivilege (Read or Write)

Display Name	User Admin IPMI LAN Privilege
Description	Specifies the maximum privilege on the IPMI LAN channel
Legal Values	• User - 2 • Operator - 3 • Administrator - 4 • No Access - 15
Default Value	15
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Both UserName and Password must be configured prior to sets
Is Platform Dependent	No

iDRAC.Users.IpmiSerialPrivilege (Read or Write)

Display Name	User Admin IPMI Serial Privilege

Description	Specifies the maximum IPMI Serial privilege
Legal Values	• User - 2 • Operator - 3 • Administrator - 4 • No Access - 15
Default Value	15
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Both UserName and Password must be configured prior to sets
Is Platform Dependent	Yes

iDRAC.Users.MD5v3Key (Read or Write)

Display Name	MD5 hash of the SNMPv3 key
Description	Specifies the MD5 hash of the SNMPv3 key
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Cannot be set without User Name being set first
Is Platform Dependent	No

iDRAC.Users.Password (Read or Write)

Display Name	User Admin Password
Description	iDRAC User Password
Legal Values	String of up to 127 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Cannot be set without User Name being set first
Is Platform Dependent	No

iDRAC.Users.PrivacyProtocol (Read or Write)

Display Name	SNMP V3 Privacy Protocol
Description	The Privacy Protocol for SNMP v3
Legal Values	• None - 0 • DES - 1 • AES - 2 • AES-256 - 3

Default Value	2
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Need valid username and password to set the attribute. The value could not be set to AES or DES if authentication protocol is none.
Is Platform Dependent	No

iDRAC.Users.Privilege (Read or Write)

Display Name	User Admin Privilege
Description	Specifies the role-based authority privileges allowed for the user. Below list shows the decimal values for each individual privilege. To create a custom privilege, add up the privilege decimal values and set the attribute to the value. Login - 1, Configure - 2, Configure Users - 4, Logs - 8, System Control - 16, Access Virtual Console - 32, Access Virtual Media - 64, System Operations - 128, Debug - 256
Legal Values	Integer values from 0 to 511.
Default Value	0
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Both UserName and Password must be configured prior to sets
Is Platform Dependent	No

iDRAC.Users.ProtocolEnable (Read or Write)

Display Name	SNMP V3 Protocol Enable
Description	Enable SNMP v3 Protocol
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Users.RSASecurID2FA (Read or Write)

Display Name	RSA SecurID 2FA
Description	Enables or disables RSA SecurID 2 Factor Authentication for the user.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users

License Required	LM_RSA_SECURID
Dependency	Both UserName and Password must be configured prior to any setting.
Is Platform Dependent	No

iDRAC.Users.SHA1v3Key (Read or Write)

Display Name	SHA1 hash of the SNMPv3 key
Description	Specifies the SHA1 hash of the SNMPv3 key
Legal Values	String of up to 40 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Cannot be set without User Name being set first
Is Platform Dependent	No

iDRAC.Users.SHA256Password (Read or Write)

Display Name	SHA256 hash of the password
Description	Specifies the SHA256 hash of the password
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Cannot be set without User Name being set first
Is Platform Dependent	No

iDRAC.Users.SHA256PasswordSalt (Read or Write)

Display Name	Salt String Appended To Password Prior To Hash
Description	Specifies the Salt String appended to the password prior to hash
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Both User Name and SHA256 User password must be configured prior to sets
Is Platform Dependent	No

iDRAC.Users.SMSNumber (Read or Write)

Display Name	SMS Number
Description	Specifies the SMS number to use for Simple 2FA for the user.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Enterprise License
Dependency	Both UserName and Password must be configured prior to setting a value.
Is Platform Dependent	No

iDRAC.Users.SNMPv3AuthenticationPassphrase (Read or Write)

Display Name	SNMPv3AuthenticationPassphrase
Description	SNMP Authentication Passphrase
Legal Values	String of up to 40 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Users.SNMPv3PrivacyPassphrase (Read or Write)

Display Name	SNMPv3PrivacyPassphrase
Description	SNMP Privacy Passphrase
Legal Values	String of up to 40 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Users.Simple2FA (Read or Write)

Display Name	Simple 2FA
Description	Enables or disables Simple 2 Factor Authentication for the user.

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	Enterprise License
Dependency	Both UserName and Password must be configured prior to setting to Enabled.
Is Platform Dependent	No

iDRAC.Users.SolEnable (Read or Write)

Display Name	User Admin SOL Enable
Description	Enables or Disables SOL for the user
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	Both UserName and Password must be configured prior to enabling user
Is Platform Dependent	No

iDRAC.Users.SourceIPTimeout (Read or Write)

Display Name	Source IP Timeout
Description	Source network address timeout period in hours.
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.Users.UseEmail (Read or Write)

Display Name	Use Email Address
Description	Enables or disables the use of email to communicate the 2FA code to destination defined in EmailAddress for the user.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users

License Required	Enterprise License
Dependency	Both UserName and Password must be configured prior to setting to Enabled.
Is Platform Dependent	No

iDRAC.Users.UseSMS (Read or Write)

Display Name	Use SMS
Description	Enables or disables the use of SMS to communicate the 2FA code to destination defined in SMSNumber for the user.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure Users
License Required	Enterprise License
Dependency	Both UserName and Password must be configured prior to setting to Enabled.
Is Platform Dependent	No

iDRAC.Users.UserName (Read or Write)

Display Name	User Admin User Name
Description	iDRAC User Name
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	Configure Users
License Required	Not Applicable
Dependency	No duplicate User Names are allowed
Is Platform Dependent	No

iDRAC.VNCServer.ActiveSessions (Read Only)

Display Name	ActiveSessions
Description	VNC Server Current Active VNC Sessions
Legal Values	Integer values from 0 to 2.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.Enable (Read or Write)

Display Name	Enable
Description	Enable VNC Server
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.LowerEncryptionBitLength (Read or Write)

Display Name	Lower Encryption Bit Length
Description	Enable VNC Lower Encryption Bit Length
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.MaxSessions (Read or Write)

Display Name	MaxSessions
Description	VNC Server Maximum Session Allowed
Legal Values	Integer values from 1 to 2.
Default Value	2
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.Password (Read or Write)

Display Name	Password

Description	VNC Server Password
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.Port (Read or Write)

Display Name	KVM Port
Description	VNC Server Port
Legal Values	Integer values from 1024 to 65535.
Default Value	5901
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.SSLEncryptionBitLength (Read or Write)

Display Name	SSL Encryption Bit Length
Description	VNC SSL Encryption Bit Length
Legal Values	• Disabled - 0 • Auto Negotiate - 1 • 128-Bit or higher - 2 • 168-Bit or higher - 3 • 256-Bit or higher - 4
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VNCServer.Timeout (Read or Write)

Display Name	Timeout
Description	VNC Server Timeout
Legal Values	Integer values from 60 to 10800.
Default Value	300

Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.AccessPrivilege (Read or Write)

Display Name	Default action upon session sharing request timeout
Description	Specifies the default action upon session sharing request timeout
Legal Values	• Full Access - 0 • Read Only Access - 1 • Deny Access - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.ActiveSessions (Read Only)

Display Name	Active Sessions
Description	Specifies current active number of Virtual Console sessions.
Legal Values	Integer values from 0 to 6.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.AttachState (Read or Write)

Display Name	Attach State
Description	Specifies the attach state for the Virtual Console.
Legal Values	• Detached - 0 • Attached - 1 • Auto-attach - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None

Is Platform Dependent	No

iDRAC.VirtualConsole.CloseUnusedPort (Read or Write)

Display Name	CloseUnusedPort
Description	Close the generic virtual console port (normally 5900) when virtual console and virtual media traffic setting is set to redirect through the iDRAC web server port.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.CrashVideoCaptureEnable (Read or Write)

Display Name	Crash Video Capture Enable
Description	Disable/Enable Crash Video Capture
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.Enable (Read or Write)

Display Name	Enable
Description	Enables or disables the Virtual Console.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.EncryptEnable (Read or Write)

Display Name	Encrypt Enable
Description	Encrypts the video in a Virtual Console session.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.LocalDisable (Read or Write)

Display Name	Local Disable
Description	Enables/disables the video signal on the local video port of the server.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.LocalVideo (Read or Write)

Display Name	Local Video
Description	Enables or disables the local server video.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.MaxSessions (Read or Write)

Display Name	Max Sessions
Description	Specifies maximum number of Virtual Console sessions.

Legal Values	Integer values from 1 to 6.
Default Value	6
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.Timeout (Read or Write)

Display Name	Timeout
Description	Specifies the idle timeout in seconds for the Virtual Console.
Legal Values	Integer values from 60 to 10800.
Default Value	1800
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.TimeoutEnable (Read or Write)

Display Name	Timeout Enable
Description	Specifies if timeout is enabled for the Virtual Console
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualConsole.WebRedirect (Read or Write)

Display Name	Redirect through webserver port
Description	Redirect virtual console and virtual media traffic through the iDRAC web server port.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None

Is Platform Dependent	No

iDRAC.VirtualMedia.ActiveSessions (Read Only)

Display Name	Active Sessions
Description	Provides the number of Virtual Media sessions that are currently active.
Legal Values	Integer values from 0 to 1.
Default Value	0
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.Attached (Read or Write)

Display Name	Virtual Media Attached
Description	Used to attach virtual devices to the system via the USB bus
Legal Values	• Detached - 0 • Attached - 1 • AutoAttach - 2
Default Value	2
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.BootOnce (Read or Write)

Display Name	Virtual Media Boot Once
Description	Enables or Disables the virtual media boot once feature of the iDRAC
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.Enable (Read or Write)

Display Name	Enable
Description	Enables or disables the Virtual Media.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.EncryptEnable (Read or Write)

Display Name	Encrypt Enable
Description	Encrypts the video in a Virtual Media session
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.FloppyEmulation (Read or Write)

Display Name	Virtual Media Floppy Emulation
Description	When Disabled, the virtual floppy disk is recognized as a removable disk by Windows OS
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.KeyEnable (Read or Write)

Display Name	Virtual Media Key Enable
Description	Enables or Disables the virtual media key feature of the iDRAC

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.VirtualMedia.MaxSessions (Read Only)

Display Name	Maximum Sessions
Description	Provides the maximum number of the Virtual Media sessions allowed.
Legal Values	Integer values from 0 to 1.
Default Value	1
Write Privilege	Configure iDRAC, Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.BlockHTTPPort (Read or Write)

Display Name	Block HTTP Port
Description	Block HTTP Port for HTTP requests
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.CustomCipherString (Read or Write)

Display Name	Custom Cipher String
Description	This attribute does not support TLS 1.3 cipher suites
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	Custom Cipher String is not supported with TLS version 1.3.

iDRAC.WebServer.Enable (Read or Write)

Display Name	Enable
Description	Enables or Disables iDRAC WebServer
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.HostHeaderCheck (Read or Write)

Display Name	Host Header Check
Description	Enable HTTP Host Header Validation
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.Http2Enable (Read or Write)

Display Name	Http2 Enable.
Description	Enables or Disables HTTP2 support for iDRAC webserver
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.HttpPort (Read or Write)

Display Name	Http Port
Description	Specifies the port number for HTTP communication with the iDRAC
Legal Values	Integer values from 1 to 65535.
Default Value	80
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.HttpsPort (Read or Write)

Display Name	Https Port
Description	Specifies the port number for HTTPS communication with the iDRAC
Legal Values	Integer values from 1 to 65535.
Default Value	443
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.HttpsRedirection (Read or Write)

Display Name	Https Redirection
Description	Enable HTTPS redirection
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.LowerEncryptionBitLength (Read or Write)

Display Name	Lower Encryption Bit Length
Description	Lower Encryption Bit Length

Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.ManualDNSEntry (Read or Write)

Display Name	Manual DNS Entry
Description	Manual FQDN/Hostname or TLS SAN domain name/s for validating HTTP Host header.
Legal Values	String of up to 1023 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.MaxNumberOfSessions (Read Only)

Display Name	Max Number Of Sessions
Description	Max session allowed
Legal Values	Integer values from 1 to 8.
Default Value	8
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.SSLEncryptionBitLength (Read or Write)

Display Name	SSL Encryption Bit Length
Description	Specifies the SSL encryption bit length.
Legal Values	• Auto-Negotiate - 0 • 128-Bit or higher - 1 • 168-Bit or higher - 2 • 256-Bit or higher - 3
Default Value	1
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.TLSProtocol (Read or Write)

Display Name	TLS Protocol
Description	Specifies the TLS protocol version support.
Legal Values	• TLS 1.1 and Higher - 1 • TLS 1.2 Only - 2 • TLS 1.2 and Higher - 3 • TLS 1.3 Only - 4
Default Value	3
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.Timeout (Read or Write)

Display Name	Web Server Idle Timeout
Description	Specifies the web server idle timeout.
Legal Values	Integer values from 60 to 10800.
Default Value	1800
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.TitleBarOption (Read or Write)

Display Name	Title Bar Option
Description	Specifies what to display in the title bar.
Legal Values	• Auto - 1 • DNS RAC Name - 2 • IP Address - 3 • Service Tag - 4 • System Host Name - 5 • Custom - 6
Default Value	1
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.WebServer.TitleBarOptionCustom (Read or Write)

Display Name	Title Bar Option Custom
Description	Specifies the custom title when the title bar option is Custom.
Legal Values	String of up to 30 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

iDRAC.vFlashPartition.AccessType (Read or Write)

Display Name	Access Type
Description	vFlash Partition Access Type
Legal Values	• Read Write - 0 • Read Only - 1
Default Value	1
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlash SD card has to be enabled. Partition at the specified index has to be created. AttachState should be Detached.
Is Platform Dependent	No

iDRAC.vFlashPartition.AttachState (Read or Write)

Display Name	Attach State
Description	vFlash Partition Attach State
Legal Values	• Detached - 0 • Attached - 1
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlash SD card has to be enabled. Partition at the specified index has to be created.
Is Platform Dependent	No

iDRAC.vFlashPartition.EmulationType (Read or Write)

Display Name	Emulation Type
Description	vFlash Partition Emulation Type
Legal Values	• CD-DVD - 0 • HDD - 1 • Floppy - 2
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlash SD card has to be enabled. Partition at the specified index has to be created. AttachState should be Detached.
Is Platform Dependent	No

iDRAC.vFlashPartition.FormatType (Read Only)

Display Name	Format Type
Description	vFlash Partition Format Type
Legal Values	• RAW - 0 • EXT2 - 1 • EXT3 - 2 • FAT16 - 3 • FAT32 - 4
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlash SD card has to be enabled. Partition at the specified index has to be created.
Is Platform Dependent	No

iDRAC.vFlashPartition.IsGroupInstanceValid (Read or Write)

Display Name	Is Group Instance Valid
Description	vFlash Partition Valid Group
Legal Values	• Invalid - 0 • Valid - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No

iDRAC.vFlashPartition.Size (Read Only)

Display Name	Size
Description	vFlash Partition Size
Legal Values	String of up to 17 ASCII characters.
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlash SD card has to be enabled. Partition at the specified index has to be created.
Is Platform Dependent	No

iDRAC.vFlashPartition.VolumeLabel (Read Only)

Display Name	Volume Label
Description	vFlash Partition Volume Label
Legal Values	String of up to 65 ASCII characters.
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlash SD card has to be enabled. Partition at the specified index has to be created.
Is Platform Dependent	No

iDRAC.vFlashSD.AvailableSize (Read Only)

Display Name	Available Size
Description	vFlash SD Available Size
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlashSD has to be enabled
Is Platform Dependent	Yes

iDRAC.vFlashSD.Bitmap (Read or Write)

Display Name	Bitmap
Description	Bitmap
Legal Values	String of up to 64 ASCII characters.
Default Value	0x0000000000000000

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.vFlashSD.Enable (Read or Write)

Display Name	Enable
Description	Enable vFlash SD
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	None
Is Platform Dependent	Yes

iDRAC.vFlashSD.Health (Read Only)

Display Name	Health
Description	vFlash SD Health
Legal Values	• OK - 0 • Critical - 1 • Warning - 2 • Unknown - 3
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlashSD has to be enabled
Is Platform Dependent	Yes

iDRAC.vFlashSD.Initialized (Read Only)

Display Name	Initialized
Description	Specifies if vFlash SD is initialized
Legal Values	• Not Initialized - 0 • Initialized - 1
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License

Dependency	vFlashSD has to be enabled
Is Platform Dependent	Yes

iDRAC.vFlashSD.Licensed (Read Only)

Display Name	Licensed
Description	Specifies if the vFlash SD is licensed
Legal Values	• Not Licensed - 0 • Licensed - 1
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlashSD has to be enabled
Is Platform Dependent	Yes

iDRAC.vFlashSD.Presence (Read or Write)

Display Name	Presence
Description	vFlash SD card presence
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.vFlashSD.Signature (Read or Write)

Display Name	Signature
Description	Signature
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

iDRAC.vFlashSD.Size (Read Only)

Display Name	Size
Description	vFlash SD Size
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlashSD has to be enabled
Is Platform Dependent	Yes

iDRAC.vFlashSD.WriteProtect (Read Only)

Display Name	Write Protect
Description	Enable vFlash SD Write Protect
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Access Virtual Media
License Required	Enterprise License
Dependency	vFlashSD has to be enabled
Is Platform Dependent	Yes

InfiniBand Attributes

InfiniBand.VndrConfigPage.LinkStatus (Read Only)

Description	Physical link status of the network port as reported by the controller.
Help Text	Physical link status of the network port as reported by the controller.
Legal Values	Connected;Disconnected
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiGenParams.TcplpViaDHCP (Read or Write)

Description	Setting to enable acquisition of IPv4 TCP/IP parameters from DHCP
Help Text	This option is specific to IPv4. Controls the source of the initiator IP address, DHCP or static assignment.
Legal Values	Enabled;Disabled
Default Value	Disabled
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICConfig.LegacyBootProto (Read or Write)

Description	Selection of the boot protocol for the port to use in legacy BIOS (non-UEFI) boot mode. The default value of the setting varies by implementation and is defined in ENG0012856.
Help Text	Select a boot protocol to be used in legacy BIOS (non-UEFI) boot mode.
Legal Values	PXE;iSCSI;FCoE;None;iSCSI Primary;iSCSI Secondary;iPXE without failover; iSCSI without failover
Default Value	varies
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiGenParams.IscsiViaDHCP (Read or Write)

Description	Setting to enable acquisition of iSCSI target parameters from DHCP.
Help Text	Enables the acquisition of iSCSI target parameters from DHCP.
Legal Values	Enabled;Disabled

Default Value	Disabled
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiGenParams.IscsiTgtBoot (Read or Write)

Description	Controls whether the iSCSI initiator will boot to the specified iSCSI target after connection. One Time Disabled disables iSCSI boot for the next (current) boot, after which it is enabled.
Help Text	Specify whether the iSCSI initiator will boot to the specified iSCSI target after connection. One Time Disabled disables iSCSI boot for the next (current) boot, after which it is enabled.
Legal Values	Enabled;Disabled;One Time Disabled
Default Value	Disabled
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.ConnectFirstTgt (Read or Write)

Description	Setting to enable whether connection to the first target is attempted.Enables or disables connecting to the first iSCSI target. Not available if VndrConfigPage.iSCSIBootSupport is unavailable.
Help Text	Enable connecting to the first iSCSI target.
Legal Values	Enabled;Disabled
Default Value	Disabled
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiGenParams.IpVer (Read or Write)

Description	Setting displays and allows configuration of the IP version used by iSCSI initiator and targets (Initiator only when a separate target ipver is implemented). If only one IP version is supported, this attribute should be set to that version and be made Read Only.
Help Text	Specify whether IPv4 or IPv6 network addressing will be used for iSCSI initiator and targets (Applies to the Initiator only when a separate target IP Version is implemented). [Vendor to provide implementation-specific language].
Legal Values	IPv4;IPv6;None
Default Value	IPv4
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICConfig.LnkSpeed (Read or Write)

Description	Selector for link speed(s) to be advertised to link partner for boot operations. Implementations should only include supported link speeds. Existing implementations may remain unchanged, new implementations should not use those speeds listed as deprecated but use the new speeds that have been added that infer what modulation scheme is in use, NRZ or PAM4. New implementations should transition to allow multiple speeds to be selected instead of just one in a simple enumeration scheme.
Help Text	Specifies the port link speed to be used when booting the selected protocol.
Legal Values	Auto Negotiated;10 Mbps Half;10 Mbps Full;100 Mbps Half;100 Mbps Full;1 Gbps;10 Gbps;25 Gbps;40 Gbps;50 Gbps (2x25);50 Gbps (1x50);100 Gbps (4x25);100 Gbps (2x50);100 Gbps (1x100);200 Gbps (4x50);200 Gbps (2x100);200 Gbps (1x200)
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.NicMode (Read or Write)

Description	Enable/Disable the NIC personality on the port. This setting is for when operating in non-NPar mode only. Note: This personality type should be specified as the port default if RDMA is not supported or has dependencies on other device modes or settings.
Help Text	Specify use of the port for L2-Ethernet traffic.
Legal Values	Enabled;Disabled
Default Value	Varies
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.DCBXSupport (Read Only)

Description	Indicates whether Data Center Bridging eXchange Protocol (DCBX) is supported.
Help Text	Specify whether Data Center Bridging eXchange Protocol (DCBX) is supported.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

Infiniband.VndrConfigPage.TOESupport (Read Only)

Description	Indicates whether TCP/IP Offload Engine capability is supported
Help Text	Indicates whether TCP/IP Offload Engine capability is supported.
Legal Values	None

Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.OnChipThermalSensor (Read Only)

Description	Indicates whether an on-chip thermal sensor is available.
Help Text	Indicates whether an on-chip thermal sensor is available.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.PXEBootSupport (Read Only)

Description	Indicates whether the PXE Boot capability is supported.
Help Text	Indicates whether PXE Boot capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.FCoEOffloadSupport (Read Only)

Description	Indicates whether FCoE is supported.
Help Text	Indicates whether FCoE is supported.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.iSCSIBootSupport (Read Only)

Description	Indicates whether iSCSI Boot is supported.

Help Text	Indicates whether iSCSI Boot is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.FCoEBootSupport (Read Only)

Description	Indicates whether Fibre Channel over Ethernet Boot capability is supported.
Help Text	Indicates whether Fibre Channel over Ethernet Boot capability is supported.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.iSCSIOffloadSupport (Read Only)

Description	Indicates whether the iSCSI Offload capability is supported.
Help Text	Indicates whether the iSCSI Offload capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.FlexAddressing (Read Only)

Description	Indicates whether the Dell FlexAddressing feature is supported.
Help Text	Indicates whether the Dell FlexAddressing feature is supported.
Legal Values	None.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.NWManagementPassThrough (Read Only)

Description	Indicates whether the Network Management Pass Through capability is supported.
Help Text	Indicates whether the Network Management Pass Through capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.EnergyEfficientEthernet (Read Only)

Description	Indicates whether Energy Efficient Ethernet capability is supported.
Help Text	Indicates whether Energy Efficient Ethernet capability is supported.
Legal Values	String value
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.NicPartitioningSupport (Read Only)

Description	Indicates whether the NIC Partitioning capability is supported.
Help Text	Indicates whether NIC Partitioning capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.TXFlowControl (Read Only)

Description	Indicates whether Transmit (TX) Flow Control capability is supported
Help Text	Indicates whether Transmit (TX) Flow Control capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable

License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.TXBandwidthControlMinimum (Read Only)

Description	Indicates whether Transmit (TX) Bandwidth Control Minimum capability is supported
Help Text	Indicates whether Transmit (TX) Bandwidth Control Minimum capability is supported.
Legal Values	VndrConfigPage.TXBandwidthControlMinimum
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.RemotePHY (Read Only)

Description	Indicates whether RemotePHY capability is supported.
Help Text	Indicates whether RemotePHY capability is supported.
Legal Values	String value
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.TXBandwidthControlMaximum (Read Only)

Description	Indicates whether Transmit(TX) Bandwidth Control Maximum capability is supported
Help Text	Indicates whether Transmit(TX) Bandwidth Control Maximum capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DeviceLevelConfig.SRIOVSupport (Read Only)

Description	Indicates whether SR-IOV capability is supported
Help Text	Indicates whether SR-IOV capability is supported.
Legal Values	Available;Unavailable

Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.RXFlowControl (Read Only)

Description	Indicates whether Receive (RX) Flow control capability is supported.
Help Text	Indicates whether Receive (RX) Flow control capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DCBSettings.CongestionNotification (Read Only)

Description	Indicates whether Congestion Notification capability is supported.
Help Text	Indicates whether Congestion Notification capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.FeatureLicensingSupport (Read Only)

Description	Indicates whether the Dell Feature Licensing capability is supported.
Help Text	Indicates whether Dell Feature Licensing capability is supported.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.OSBMCManagementPassThrough (Read Only)

Description	Indicates whether OS-BMC Management Pass Through capability is supported.

Help Text	Indicates whether OS-BMC Management Pass Through capability is supported.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DeviceLevelConfig.EVBModesSupport (Read Only)

Description	Indicates the type of EVB Modes supported.
Help Text	Indicates the type of EVB Modes supported.
Legal Values	VEB;VEPA;PE;Multi-channel
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DCBSettings.EnhancedTransmissionSelection (Read Only)

Description	Indicates whether Enhanced Transmission Selection capability is supported.
Help Text	Indicates whether Enhanced Transmission Selection capability is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DCBSettings.PriorityFlowControl (Read Only)

Description	Indicates whether the Priority Flow Control capability is supported.
Help Text	No Help information available.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiInitiatorParams.IscsiInitiatorIpAddr (Read or Write)

Description	The iSCSI initiator IP address. Will be either in IPv4 or IPv6 format depending on value of the IpVer attribute.
Help Text	Specify the IP address of the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiInitiatorParams.IscsiInitiatorSubnet (Read or Write)

Description	The iSCSI initiator Subnet Mask for an IPv4 initiator configuration.
Help Text	Specify the IPv4 Subnet Mask of the iSCSI initiator.
Legal Values	String from 7 to 15 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiInitiatorParams.IscsiInitiatorPrimDns (Read or Write)

Description	The iSCSI initiator Primary DNS IP Address. Will be in either IPv4 or IPv6 format depending on the value of the IpVer attribute.
Help Text	Specify the Primary DNS IP address used by the iSCSI initiator.
Legal Values	String from 2 to 39 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.FirstTgtIscsiName (Read or Write)

Description	The iSCSI Qualified Name (IQN) of the first target.
Help Text	Specify the iSCSI Qualified Name (IQN) of the first iSCSI storage target.

Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiInitiatorParams.IscsiInitiatorName (Read or Write)

Description	Setting to represent and set the iSCSI initiator iSCSI Qualified Name (IQN).
Help Text	Specify the initiators iSCSI Qualified Name (IQN).
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.FirstTgtChapId (Read or Write)

Description	First Target CHAP ID (up to 128 characters in length). If only a single value of CHAP ID supported then it is stored here.
Help Text	Specify the first iSCSI storage target Challenge-Handshake Authentication Protocol (CHAP) ID. [vendor to specify what is allowed].
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiInitiatorParams.IscsiInitiatorChapId (Read or Write)

Description	Initiator CHAP ID (up to 128 characters in length). If this can be set on a per target basis, then the first target value shall be stored here.
Help Text	Specify the iSCSI initiator Challenge-Handshake Authentication Protocol (CHAP) ID. [Vendor to describe what is allowed].
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License

Dependency	None

InfiniBand.IscsiInitiatorParams.IscsiInitiatorGateway (Read or Write)

Description	iSCSI initiator default Gateway IP address. Will be in either IPv4 or IPv6 format depending on the value of the IpVer attribute.
Help Text	Specify the IP address of the default Gateway used by the iSCSI initiator.
Legal Values	String from 2 to 39 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.BusDeviceFunction (Read Only)

Description	The value of this attribute depends on the state of the NParEP Mode setting. If NParEP Mode is Disabled, the value is the BIOS assigned PCIe Bus:Device:Function identifier. If NParEP Mode is Enabled, the value is the BIOS assigned PCIe Bus:Function identifier.
Help Text	Indicates the PCI Address of the Physical Function assigned to the port.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.ChipMdl (Read Only)

Description	This attribute consists of the concatenation of 2 different elements, a vendor-defined silicon marketing name and the silicon revision information as specified in PCI configuration space, separated by space. For example: R720 B0.
Help Text	Specifies the Chip Type.
Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.DeviceName (Read Only)

Description	Official product name of the device.
Help Text	Official product name of the device.

Legal Values	None
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.PCIDeviceID (Read Only)

Description	PCI Device ID reported by the controller when operating in non-NPar mode only. The value of the attribute is undefined for controllers operating in NPar mode that change their device IDs or support multiple PCI Device IDs at the partition level.
Help Text	PCI Device ID of the controller.
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.FirstTgtIpAddress (Read or Write)

Description	First iSCSI target IP address. Will be either IPv4 or IPv6 format depending on the value of the FirstTgtIpVer attribute.
Help Text	Specify the IP address of the first iSCSI target.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.VirtMacAddr (Read or Write)

Description	Programmatically assignable MAC address. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent MAC address is by writing 0s to the virtual MAC. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature enablement.
Help Text	Programmatically assignable MAC address for port.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.MacAddr (Read Only)

Description	The Permanent MAC address assigned during manufacturing.
Help Text	Permanent MAC address assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IsctlInitiatorParams.IsctlInitiatorChapPwd (Read or Write)

Description	iSCSI initiator CHAP secret (0 or 12 to 16 characters in length). If this can be set on a per target basis, then the value for the first target shall be stored here.
Help Text	Specify the iSCSI initiator Challenge-Handshake Authentication Protocol (CHAP) secret (password). [Vendor to describe what is allowed].
Legal Values	String from 12 to 16 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICPartitioningConfig.NumberPCIFunctionsEnabled (Read Only)

Description	The number of PCI Physical Functions currently enabled on this port.
Help Text	The number of PCI Physical Functions currently enabled on this port.
Legal Values	integer values
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICPartitioningConfig.NumberPCIFunctionsSupported (Read Only)

Description	The number of PCI Physical Functions supported on this port. This value may change depending on the support and configuration of NParEP.
Help Text	The number of PCI Physical Functions supported on this port. This value may change depending on the support and configuration of NParEP.

Legal Values	Integer values .
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.FirstTgtTcpPort (Read or Write)

Description	TCP Port number of the first iSCSI target.
Help Text	Specify the TCP Port number of the first iSCSI target.
Legal Values	Integer values from 1 to 65535.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.FrmwImgMenu.FamilyVersion (Read Only)

Description	Firmware family version information. Same as what is returned in the PackageVersionName field by the Firmware Management Protocol GetPackageInfo() call.
Help Text	Installed device firmware family version information.
Legal Values	String of up to 11 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.BlnkLeds (Read or Write)

Description	Blink LEDs for a duration of up to 15 seconds. Only valid for adapters with link LEDs.
Help Text	Specify the number of seconds the LEDs on the physical network port should blink to assist with port identification.
Legal Values	Integer values from 0 to 15.
Default Value	15
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiGenParams.ChapMutualAuth (Read or Write)

Description	Setting to enable mutual CHAP authentication between the iSCSI initiator and target.
Help Text	To use mutual CHAP authentication, specify an initiator secret on the Initiator Parameters page and configure that secret on the target.
Legal Values	Enabled;Disabled
Default Value	Disabled
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiGenParams.ChapAuthEnable (Read or Write)

Description	Setting to enable CHAP Authentication for iSCSI initiator.
Help Text	Enable the ability of the initiator to use CHAP authentication when connecting to the iSCSI target.
Legal Values	Enabled;Disabled
Default Value	Disabled
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.FirstTgtBootLun (Read or Write)

Description	Specifies the first iSCSI target boot LUN.
Help Text	Specify the boot Logical Unit Number (LUN) on the first iSCSI storage target.
Legal Values	Integer values from 0 to 18446744073709551615.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.FrmwImgMenu.EFIVersion (Read Only)

Description	EFI device driver version information.
Help Text	Installed device EFI driver version information.
Legal Values	String value.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICConfig.BootStrapType (Read or Write)

Description	Configure the boot strap mechanism used to boot to the OS.
Help Text	Specify the boot strap method used to boot to the operating system.
Legal Values	Auto Detect-0;BBS-1;Int 18h-2;Int 19h-3
Default Value	AutoDetect
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DeviceLevelConfig.VirtualizationMode (Read or Write)

Description	The Virtualization Mode setting for the device. Note: Not all PCI slots in all servers are capable of supporting virtualization features based on ARI and SR-IOV. The implementation shall check the state of the ARI forwarding bit in the immediate upstream PCI ports config space settings (Device Control Register 2, bit 5) to ensure that it is set before allowing the selection of SR-IOV and NParEP by the user, if not, those selections shall be disallowed.
Help Text	Specify the type of virtualization used by the controller on all ports.
Legal Values	None;NPar;SR-IOV;NPar + SR-IOV;Advanced NPar;Advanced NPar + SR-IOV
Default Value	NONE
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICConfig.BannerMessageTimeout (Read or Write)

Description	Timeout in seconds for banner display during POST
Help Text	Specify the number of seconds that the OptionROM banner is displayed during POST.
Legal Values	Integer values from 0 to 14.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.IscsiFirstTgtParams.FirstTgtChapPwd (Read or Write)

Description	First Target CHAP Secret (0 or 12 to 16 characters in length). If only a single value of CHAP Secret is supported then it is stored here.

Help Text	Specify the Challenge-Handshake Authentication Protocol secret (CHAP password) of the first iSCSI storage target. [Vendor to specify what is allowed].
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.iSCSIDualIPVersionSupport (Read Only)

Description	Indicates support for simultaneous IPv4 and IPv6 configurations of the iSCSI initiator and iSCSI primary and secondary targets.
Help Text	Indicates support for simultaneous IPv4 and IPv6 configurations of iSCSI initiator and iSCSI primary and secondary targets.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.NICConfig.BootRetryCnt (Read or Write)

Description	Configure the number of retries in case of boot failure.
Help Text	Specify the number of retries to attempt in case of a boot failure.
Legal Values	No Retry;1 Retry;2 Retries;3 Retries;4 Retries;5 Retries;6 Retries;Indefinite Retries
Default Value	NoRetry
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DeviceLevelConfig.NumberVFSupported (Read Only)

Description	The total number of PCI Virtual Functions supported on this port (or device). Whether the number applies to the device as a whole, or to an individual port, is indicated by the value of the Virtual Function Allocation Basis.
Help Text	The number of virtual functions supported on this port (or device) [VENDOR modify appropriately for the implementation].
Legal Values	Integer values from 0 to 256.
Default Value	0
Write Privilege	Not Applicable

License Required	Express License
Dependency	None

InfiniBand.DeviceLevelConfig.RDMASupport (Read Only)

Description	Capability indicator for controllers supporting Remote Direct Memory Management (RDMA), the remote memory management capability that allows server to server data movement directly between application memory without any CPU involvement.
Help Text	Indicates whether any RDMA protocol is supported by the controller.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.DeviceLevelConfig.RDMAProtocolSupport (Read Only)

Description	Indicates what RDMA protocol support is enabled by the controller. Implement as ReadOnly and browser suppressed if the controller only supports one type of RDMA; R/W and not browser suppressed if multiple settings are supported and selectable. [Vendor to provide default setting information]
Help Text	Specify what RDMA Protocol is to be used in operation. [Vendor modify as appropriate].
Legal Values	iWARP;RoCE;iWARP + RoCE
Default Value	None
Write Privilege	Not Applicable
License Required	Express License
Dependency	None

InfiniBand.VndrConfigPage.RDMANICModeOnPort (Read or Write)

Description	Enable/Disable the NIC + RDMA personality on the port. This setting is for when operating in non-NPar mode only. Note: This personality type may be specified as the port default if RDMA traffic can be supported irrespective of any other device mode or setting.
Help Text	Specify use of the port for both L2-Ethernet and RDMA traffic. [Vendor may want to customize type of RDMA supported].
Legal Values	Enabled;Disabled
Default Value	Varies
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.DeviceLevelConfig.VFAllocBasis (Read Only)

Description	Defines the domain in which Virtual Functions are allocated; either Port or Device. Note: A device which implements less than 1 PF per physical port must use Device level VF allocation.
Help Text	Defines the domain in which Virtual Functions are allocated.
Legal Values	Port;Device
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.DeviceLevelConfig.VFAllocMult (Read Only)

Description	Defines the multiple (e.g. x1, x4, x8, etc.) in which VFs must be allocated to a PF.
Help Text	[VENDOR provide appropriate help text for the implementation - what is allowed, etc].
Legal Values	Integer values from 1 to 255.
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.DeviceLevelConfig.VFDistribution (Read or Write)

Description	The value is a string of numbers, each separated by a colon that defines the distribution of VFs to PFs within the domain specified by VFAllocBasis. Each number represents the number of PVI Virtual Functions to be advertised in PCI config space by each partition (PF). The numbers must sum to an amount less than or equal to the NumberVFSupported attribute value. A value appears in the colon separated list for each Physical Function that can potentially be present within the allocation domain, independent of its enablement state. Values in the list from left to right apply to function numbers in the domain from least to greatest.
Help Text	The value is a string of numbers, each separated by a colon that defines the distribution of VFs to PFs within the domain specified by VFAllocBasis. Each number represents the number of PVI Virtual Functions to be advertised in PCI config space by each partition (PF). The numbers must sum to an amount less than or equal to the NumberVFSupported attribute value. A value appears in the colon separated list for each Physical Function that can potentially be present within the allocation domain, independent of its enablement state. Values in the list from left to right apply to function numbers in the domain from least to greatest.
Legal Values	Integer values.
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.DeviceLevelConfig.PartitionStateInterpretation (Read Only)

Description	Describes how partitioning is implemented and how the PartitionState attribute is used in the controller. A value of Fixed signifies that partition states are locked and that the current values of PartitionState[n] will not change. A value of Variable signifies that PartitionState[n] may/will change values during the course of device operation as a result of user configuration. Implementations that support changes in PartitionState must implement this attribute. The Default value is implementation dependent.
Help Text	Describes how partitioning is implemented and how the PartitionState attribute is used in the controller.
Legal Values	Fixed; Variable
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.NICConfig.PKey (Read or Write)

Description	PKey ID to be used by PXE boot in the InfiniBand environment
Help Text	PKey ID to be used by PXE boot in InfiniBand fabrics.
Legal Values	Integer values.
Default Value	0
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.SNAPIState (Read Only)

Description	Indicates whether SNAPI functionality is enabled. Note: Implement only if SNAPI support is set to Available
Help Text	Indicates whether SNAPI functionality is enabled
Legal Values	Enabled;Disabled
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.NodeGUID (Read Only)

Description	The Permanent Node GUID assigned during manufacturing.
Help Text	Permanent Node GUID assigned during manufacturing.
Legal Values	String values
Default Value	None

Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.PortGUID (Read Only)

Description	The Permanent Port GUID assigned during manufacturing.
Help Text	Permanent Port GUID assigned during manufacturing.
Legal Values	String values
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.SNAPI (Read Only)

Description	Indicates the adapter supports SNAPI functionality by either special interfacing to the PCI slot connector or via cabling to another PCI slot.
Help Text	Indicates whether SNAPI functionality is supported.
Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.NetworkLinkType (Read or Write)

Description	Select the protocol type to be used on a port that supports multiple fabric types. NOTE: Implement ONLY if VPI Mode is supported
Help Text	Select port network protocol (Ethernet/InfiniBand)
Legal Values	Ethernet;InfiniBand
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.VPI (Read Only)

Description	Indicates whether Virtual Protocol Interconnect (VPI) functionality is supported.
Help Text	Indicates whether Virtual Protocol Interconnect (VPI) functionality is supported.

Legal Values	Available;Unavailable
Default Value	None
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

InfiniBand.VndrConfigPage.VirtNodeGuid (Read or Write)

Description	Programmatically assignable Node GUID address used when only one PF is assigned to the port. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent Node GUID address is by writing 0s to the virtual Node GUID. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s.
Help Text	Programmatically assignable Node GUID address.
Legal Values	String of up to 19 ASCII characters.
Default Value	0000:0000:0000:0000
Write Privilege	Not Applicable
License Required	Not Applicable
Dependency	None

LIFECYCLE Attributes

LifecycleController.LCAttributes.AutoBackup (Read or Write)

Display Name	Automatic Backup Feature
Description	Enables or disables the automatic backup scheduler.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Found
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.AutoDiscovery (Read Only)

Display Name	Auto Discovery
Description	Indicates if Auto Discovery feature is turned off or on.
Legal Values	• Off - 0 • On - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.AutoUpdate (Read or Write)

Display Name	Automatic Update Feature
Description	Enables or disables the automatic update scheduler.
Legal Values	• Disabled - 0

	• Enabled - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Enterprise License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.BIOSRTDRequested (Read or Write)

Display Name	BIOS Reset To Defaults Requested
Description	Allows to reset all the BIOS attributes to the default state. After this property is enabled, restart the server to view the default values of BIOS.
Legal Values	• False - 0 • True - 1 • OEMIDDefaults - 2
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.CollectSystemInventoryOnRestart (Read or Write)

Display Name	Collect System Inventory on Restart
Description	Enables or disables collection of system inventory on host reboot.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.DiscoveryFactoryDefaults (Read Only)

Display Name	Discovery Factory Defaults
Description	Off- Do not reset to factory defaults when performing auto discovery. On-Reset to defaults when performing auto discovery.
Legal Values	• Off - 0 • On - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.IPAddress (Read or Write)

Display Name	IPAddress
Description	IP Address of the network share
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.IPChangeNotifyPS (Read or Write)

Display Name	IPChangeNotifyPS
Description	On- Notify provisioning server of an IP change. Off- Do not notify provisioning server of an IP change.
Legal Values	• Off - 0 • On - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.IgnoreCertWarning (Read or Write)

Display Name	Default Ignore Certificate warning
Description	Ignore Certificate warning default when not provided.
Legal Values	• Off - 0 • On - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.Licensed (Read Only)

Display Name	Licensed
Description	Indicates if the Part Replacement feature is licensed or not
Legal Values	• No - 0 • Yes - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.LifecycleControllerState (Read or Write)

Display Name	Lifecycle Controller State
Description	Enables or disables Lifecycle Controller.
Legal Values	• Disabled - 0 • Enabled - 1

	Recovery - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.PartConfigurationUpdate (Read or Write)

Display Name	Part Configuration Update
Description	Apply hardware configuration to the replaced part on part replacement.
Legal Values	- Disabled - 0 - Apply Always - 1 - Apply only if Firmware Match - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.PartFirmwareUpdate (Read or Write)

Display Name	Part Firmware Update
Description	Apply firmware changes to the replaced part on part replacement.
Legal Values	- Disable - 0 - Allow version upgrade only - 1 - Match firmware of replaced part - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.ProvisioningServer (Read or Write)

Display Name	Provisioning Server
Description	Provisioning server address and port.
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.StorageHealthRollupStatus (Read Only)

Display Name	Storage Health Rollup Status
Description	No description information available.
Legal Values	Integer values from 1 to 4.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.SystemID (Read Only)

Display Name	SYSID
Description	Dell System ID
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.UserProxyPassword (Read or Write)

Display Name	Default Proxy Password
Description	Proxy Password default if not provided
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.UserProxyPort (Read or Write)

Display Name	Default Proxy Port setting
Description	Proxy Port default if not provided. Proxy Port is limited to values in the range of 0 - 65535.
Legal Values	String of up to 5 ASCII characters.
Default Value	80
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.UserProxyServer (Read or Write)

Display Name	Default Proxy Server setting
Description	Proxy Server default if not provided.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.UserProxyType (Read or Write)

Display Name	Default Proxy type
Description	Proxy Type default if not provided
Legal Values	• HTTP - 0 • SOCKS - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.UserProxyUserName (Read or Write)

Display Name	Default Proxy User name
Description	Proxy User name default if not provided.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.LCAttributes.VirtualAddressManagementApplication (Read or Write)

Display Name	VirtualAddressManagementApplication

Description	The console name of the Virtual Address Management Application,VirtualAddressManagement attribute is set to CurrentValue equals "Console".
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	No
Notes	A job successfully configured using the autoupdate or autobackup feature settings can be deleted only if the job is currently not running or downloading.

LifecycleController.OSD.SupportedOSList (Read Only)

Display Name	Supported OS List
Description	Lists all the supported Operating Systems for OS Deployment.
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

NIC Attributes

NIC.ConfigureFormn.BusDeviceFunction[Partition:n] (Read Only)

Description	The value of this attribute depends on the state of the NParEP Mode setting. If NParEP Mode is Disabled, the value is the BIOS assigned PCIe Bus:Device:Function identifier. If NParEP Mode is Enabled, the value is the BIOS assigned PCIe Bus:Function identifier. Replace n with the number of the partition. Indicates the PCI Address of the partitions Physical Function.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.FCoEOffloadMode[Partition:n] (Read or Write)

Description	Enable/Disable the FCoE personality on the partition. Replace n with the number of the partition. Enables the partition for FCoE storage traffic.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.FIPMacAddr[Partition:n] (Read Only)

Description	Permanent FIP-MAC address for FCoE assigned during manufacturing. Specified on a per partition basis. Replace n with the number of the partition. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Permanent FIP-MAC address for FCoE assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.InstanceNumber[Partition:n] (Read Only)

Description	Numeric instance of the partition (e.g. 1st, 2nd, etc.) on the port it belongs to. This identifier is unique for each partition on the port. Replace n with the number of the partition. Instance Number of the partition.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.IscsiFIPMacAddr[Partition:n] (Read Only)

Description	Permanent combination MAC address for iSCSI offload and FIP for FCoE assigned during manufacturing. Specified on a per partition basis. Replace n with the number of the partition. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Permanent combination MAC address for iSCSI offload and FCoE FIP assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.IscsiMacAddr[Partition:n] (Read Only)

Description	Permanent MAC address for iSCSI offload assigned during manufacturing. Specified on a per partition basis. Replace n with the number of the partition. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Permanent MAC address for iSCSI offload assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.L2FIPMacAddr[Partition:n] (Read Only)

Description	Permanent combination Ethernet and FIP-MAC address for FCoE assigned during manufacturing. Specified on a per partition basis. Replace n with the number of the partition. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Permanent combination MAC address for Ethernet and FCoE FIP assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.L2IscsiFIPMacAddr[Partition:n] (Read Only)

Description	The Permanent combination Ethernet, iSCSI Offload and FIP for FCoE MAC address of the partition assigned during manufacturing. Replace n with the number of the partition. The current address value should be readable at all times, irrespective of feature and partition enablement. Permanent combination MAC address for Ethernet, iSCSI Offload and FCoE FIP assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.L2IscsiMacAddr[Partition:n] (Read Only)

Description	The Permanent combination Ethernet and iSCSI Offload MAC address of the partition assigned during manufacturing. Replace n with the number of the partition. The current address value should be readable at all times, irrespective of feature and partition enablement. Permanent combination MAC address for Ethernet and iSCSI Offload assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable

Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.MacAddr[Partition:n] (Read Only)

Description	The Permanent MAC address of the partition assigned during manufacturing. Replace n with the number of the partition. The current address value should be readable at all times, irrespective of feature and partition enablement. Permanent MAC address assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NicMode[Partition:n] (Read or Write)

Description	Enable/Disable the NIC personality on the partition. Replace n with the number of the partition. Note: This personality type should be specified as the partition 1 default if RDMA is not supported or has dependencies on other device modes or settings. The default setting should be disabled for other partitions on the port. Specify use of the partition for L2-Ethernet traffic.
Legal Values	• Enabled • Disabled
Default Value	Varies
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NodeGuid[Partition:n] (Read Only)

Description	The permanent partition Node GUID assigned to the partition (PF) during manufacturing used when more than one PF is assigned to the port. The permanent Node GUID assigned to the partition during manufacturing
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NumberVFAdvertised[Partition:n] (Read or Write)

Description	This value is the number of PCI Virtual Functions Advertised by the partition in PCI config space when operating in the NPar+SR-IOV virtualization mode. The value of this attribute may be the same across partitions or be settable on an individual partition basis depending on implementation. Note: This attribute is only defined for the browser and does NOT have any x-UEFI mapping. VF allocation is set via the VFDistribution attribute in x-UEFI. There will be an instance of this attribute for each partition. Replace n in the AttributeName with the number of the partition. Specify the number of PCI Virtual Functions (VFs) to be advertised on this partition (PF) in PCI config space. The number of advertised VFs on each partition must add up to be less than or equal to the number of PCI Virtual Functions supported by the device or port. [VENDOR modify appropriately for the implementation].
Legal Values	Integer values from 0 to 256.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NvmeTcpBusDeviceFunction[Partition:n] (Read Only)

Description	The value of this attribute depends on the state of the NParEP Mode setting. If NParEP Mode is Disabled, the value is the BIOS assigned PCIe Bus:Device:Function identifier of the NVMe/TCP PF . If NParEP Mode is Enabled, the value is the BIOS assigned PCIe Bus:Function identifier of the NVMe/TCP PF. Indicates the PCI Address of the NVMe/TCP partitions Physical Function.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NvmeTcpMacAddr[Partition:n] (Read Only)

Description	Permanent MAC address for NVMe/TCP Offload operation assigned during manufacturing. If supported, the current address value should be readable at all times, irrespective of feature enablement. Permanent MAC address for NVMe/TCP assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable

Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NvmeTcpOffloadMode[Partition:n] (Read or Write)

Description	Enable/Disable the NVMe/TCP offload personality on the partition. Replace n with the number of the partition. Specify use of the partition for NVMe/TCP offload storage traffic.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.NvmeTcpPCIDeviceID[Partition:n] (Read Only)

Description	PCI Device ID reported by the NVMe/TCP PF when operating in NPar modes. PCI Device ID of the NVMe/TCP partitions Physical Function.
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.PCIDeviceID[Partition:n] (Read Only)

Description	PCI Device ID of the partition. Replace n with the number of the partition. PCI Device ID of the partition.
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.PortGuid[Partition:n] (Read Only)

Description	The permanent Port GUID assigned to the partition (PF) during manufacturing used when more than one PF is assigned to the port. The permanent Port GUID assigned to the partition during manufacturing.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.PortNumber[Partition:n] (Read Only)

Description	Port that the partition belongs to. Replace n with the number of the partition. Port that the partition belongs to. Replace n with the number of the partition.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.RDMANICModeOnPartition (Read or Write)

Description	Enable/Disable the NIC + RDMA personality on the partition. This setting is for when operating in NPar mode only. Replace n with the number of the partition. Note: This personality type may be specified as the partition default if RDMA traffic can be supported irrespective of any other device setting. Specify use of the partition for both L2-Ethernet and RDMA traffic. [Vendor may want to customize type of RDMA supported].
Legal Values	• Enabled • Disabled
Default Value	Varies
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.RDMANICModeOnPartition[Partition:n] (Read or Write)

Description	Enable/Disable the NIC + RDMA personality on the partition. This setting is for when operating in NPar mode only. Replace n with the number of the partition. Note: This personality type may be specified as the partition default if RDMA traffic can be supported irrespective of any other device setting. Specify use of the partition for both L2-Ethernet and RDMA traffic. [Vendor may want to customize type of RDMA supported].
Legal Values	• Enabled • Disabled
Default Value	Varies
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.SVLanId[Partition:n] (Read or Write)

Description	Specify the value of the S-VLAN ID to be used by the partition for all traffic when operating in the Advanced NPar mode. The S-VLAN ID must be unique per partition and in the range from 3 to 4094. NOTE : This attribute shall only be implemented when Advanced NPar is supported. Specify the S-VLAN ID to be used by the partition in Advanced NPar mode. The S-VLAN ID must be unique per partition and in the range from 3 to 4094. Default value will be partition number + 2
Legal Values	Integer values from 3 to 4094.
Default Value	Partition number + 2
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtFIPMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable FIP-MAC address for FCoE. Virtual addresses written will also generate corresponding VWWNN and VWWPN addresses as defined in Y741D. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable FIP-MAC address for the FCoE partition.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License

Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtIscsiFIPMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable combination iSCSI Offload and FIP-MAC address for FCoE. Virtual addresses written will also generate corresponding VWWNN and VWWPN addresses as defined in Y741D. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable combination MAC address for iSCSI Offload and FCoE FIP.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtIscsiMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable MAC address for iSCSI offload. Programmatic write for support of I/O Identity feature. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable MAC address for the iSCSI offload partition.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtL2FIPMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable combination FIP-MAC address for FCoE. Virtual addresses written will also generate corresponding VWWNN and VWWPN addresses as defined in Y741D. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method,

its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable combination MAC address for Ethernet and FCoE FIP.

Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtL2IscsiFIPMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable combination Ethernet, iSCSI Offload and FIP-MAC address for FCoE. Virtual addresses written will also generate corresponding VWWNN and VWWPN addresses as defined in Y741D. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable combination MAC address for Ethernet, iSCSI Offload and FCoE FIP.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtL2IscsiMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable combination MAC address for Ethernet and iSCSI offload. Programmatic write for support of I/O Identity feature. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable combination MAC address for Ethernet and iSCSI Offload.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable MAC address. Programmatic write for support of I/O Identity feature. Replace n with the number of the partition. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature and partition enablement. Programmatically assignable MAC address for partition.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtNodeGuid[Partition:n] (Read or Write)

Description	Programmatically assignable partition Node GUID address used when more than one PF is assigned to the port. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent partition Node GUID address is by writing 0s to the virtual partition Node GUID. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. Programmatically assignable Node GUID address of the partition.
Legal Values	String of up to 19 ASCII characters.
Default Value	0000:0000:0000:0000
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtNvmeTcpMacAddr[Partition:n] (Read or Write)

Description	Programmatically assignable MAC address for NVMe/TCP offload. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address should be readable at all times, irrespective of feature enablement. Programmatically assignable MAC address for the NVMe/TCP offload partition.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A

License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtPortGuid[Partition:n] (Read or Write)

Description	Programmatically assignable partition Port GUID address used when more than one PF is assigned to the port. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent partition GUID address is by writing 0s to the virtual partition GUID. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. Programmatically assignable Port GUID address of the partition.
Legal Values	String of up to 19 ASCII characters.
Default Value	0000:0000:0000:0000
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtWWN[Partition:n] (Read or Write)

Description	Programmatically assignable Fibre Channel World Wide Node Name identifier for FCoE. Virtual addresses written will also be modified by subsequent writes to the VirtFIP-MAC addresss as defined in Y741D. Replace n with the number of the partition. The supported method of clearing this virtual address is by writing 0s as the address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. . Programmatically assignable Fibre Channel World Wide Node Name identifier for partition FCoE.
Legal Values	String of up to 23 ASCII characters.
Default Value	00:00:00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.VirtWWPN[Partition:n] (Read or Write)

Description	Programmatically assignable Fibre Channel World Wide Port Name identifier for FCoE. Virtual addresses written will also be modified by subsequent writes to the VirtFIP-MAC addresss as defined in Y741D. Replace n with the number of the partition. The supported method of clearing this virtual address is by writing 0s as the address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. Programmatically assignable Fibre Channel World Wide Port Name identifier for partition FCoE.

Legal Values	String of up to 23 ASCII characters.
Default Value	00:00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.WWN[Partition:n] (Read Only)

Description	Fibre Channel World Wide Node Name identifier for FCoE. Replace n with the number of the partition. Fibre Channel World Wide Node Name identifier for FCoE. Replace n with the number of the partition.
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.WWPN[Partition:n] (Read Only)

Description	Fibre Channel World Wide Port Name identifier for FCoE assigned during manufacturing. Replace n with the number of the partition. Fibre Channel World Wide Port Name identifier for FCoE assigned during manufacturing. Replace n with the number of the partition.
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.ConfigureFormn.iScsiOffloadMode[Partition:n] (Read or Write)

Description	Enable/Disable the iSCSI offload personality on the partition. Replace n with the number of the partition. Specify use of the partition for iSCSI offload storage traffic.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License

Dependency	None
Notes	Autocomplete will not work if you replace n with the index in this object. You have to type NIC.ConfigureFormn and press tab to view the list of attributes.

NIC.DCBSettings.CongestionNotification (Read Only)

Description	Indicates whether Congestion Notification capability is supported. Indicates whether Congestion Notification capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.DCBSettings.EnhancedTransmissionSelection (Read Only)

Description	Indicates whether Enhanced Transmission Selection capability is supported. Indicates whether Enhanced Transmission Selection capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.DCBSettings.PriorityFlowControl (Read Only)

Description	Indicates whether the Priority Flow Control capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.DeviceLevelConfig.AdvNParSupport (Read Only)

Description	Indicates whether Advanced NPar S-Tag functionality is supported. Indicates whether Advanced NPar S-Tag functionality is supported.
Legal Values	String of ASCII characters.
Default Value	N/A
Write Privilege	N/A
License Required	Not Applicable

Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.EVBModesSupport (Read Only)

Description	Indicates the type of EVB Modes supported. Indicates the type of EVB Modes supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.NParEP (Read or Write)

Description	Controls enablement of NParEP mode in which more than 8 PCI Physical Functions are exposed by the device. When disabled, the device must expose only a maximum of 8 PFs in the traditional PCI B:D:F addressing mode, regardless of any ARI capability being advertised for SR-IOV support. [Not to be implemented if not supported] Note: Not all PCI slots in all servers are capable of supporting virtualization features based on ARI and SR-IOV. The controller should check PCI config space settings to ensure that virtualization modes are available before allowing their selection by the user. NParEP mode enables more than 8 partitions on the device. It must not be enabled if the system and OS do not support devices with more than 8 PCI Physical Functions.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.NumPorts (Read or Write)

Description	Configuration control for Controllers that have the ability to support different port counts per SFF (e.g., SFP-DD, QSFP) or backplane interface. Controllers on implementations that are fixed in their number of ports shall not implement this attribute. This attribute is defined as device-level due to symmetry expectations, if symmetry is not a requirement, it should be implemented at the port level. Specify the total number of ports to be configured on the physical interfaces. [VENDOR to modify appropriately]
Legal Values	• 1 • 2 • 4 • 8
Default Value	varies
Write Privilege	N/A

License Required	Not Applicable
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.NumberVFSupported (Read Only)

Description	The total number of PCI Virtual Functions supported on this port (or device). Whether the number applies to the device as a whole, or to an individual port, is indicated by the value of the Virtual Function Allocation Basis. The number of virtual functions supported on this port (or device) [VENDOR modify appropriately for the implementation].
Legal Values	Integer values from 0 to 256.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.PTMSupport (Read Only)

Description	Indicates whether the controller and the overall implementation supports Precision Time Management as defined by the PCI SIG. Indicates whether the controller as implemented supports Precision Time Management
Legal Values	String of ASCII characters.
Default Value	N/A
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.PartitionStateInterpretation (Read Only)

Description	Describes how partitioning is implemented and how the PartitionState attribute is used in the controller. A value of Fixed signifies that partition states are locked and that the current values of PartitionState[n] will not change. A value of Variable signifies that PartitionState[n] may/will change values during the course of device operation as a result of user configuration. Implementations that support changes in PartitionState must implement this attribute. The Default value is implementation dependent. Describes how partitioning is implemented and how the PartitionState attribute is used in the controller.
Legal Values	• Fixed • Variable
Default Value	None
Write Privilege	N/A

License Required	Not Applicable
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.RDMAApplicationProfile (Read or Write)

Description	Indicates what RDMA configuration profiles are supported by the controller. [Vendor input requested if 1) additional profiles are thought to be needed, 2) if the appl profile can vary by port or partitionm and 3) if appl profiles are supported on a partition basis]. Note: RoCE 1 and RoCE 2 are vendor-specific profiles and should not be interpreted as a version of RoCE. Specify the RDMA application profile setting to use in operation. [Vendor to clarify availability and usage].
Legal Values	• Storage • HPCC • RoCE 1 • RoCE 2
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.RDMAProtocolSupport (Read Only)

Description	Indicates what RDMA protocol support is enabled by the controller. Implement as ReadOnly and browser suppressed if the controller only supports one type of RDMA; R/W and not browser suppressed if multiple settings are supported and selectable. [Vendor to provide default setting information] Specify what RDMA Protocol is to be used in operation. [Vendor modify as appropriate].
Legal Values	• iWARP • RoCE • iWARP + RoCE
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.RDMASupport (Read Only)

Description	Capability indicator for controllers supporting Remote Direct Memory Management (RDMA), the remote memory management capability that allows server to server data movement directly between application memory without any CPU involvement. Indicates whether any RDMA protocol is supported by the controller.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.SRIOVSupport (Read Only)

Description	Indicates whether SR-IOV capability is supported Indicates whether SR-IOV capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.STagEtherType (Read or Write)

Description	Specifies the EtherType to be used by all partitions on the port when Advanced NPar S-tagging is enabled in the Virtualization Mode setting. NOTE: This attribute shall only be implemented when Advanced NPar is supported. Specify the EtherType to be used when using Advanced NPar S-tagging.
Legal Values	• 0x88a8 • 0x9100
Default Value	0x88a8
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.VFAllocBasis (Read Only)

Description	Defines the domain in which Virtual Functions are allocated; either Port or Device. Note: A device which implements less than 1 PF per physical port must use Device level VF allocation. Defines the domain in which Virtual Functions are allocated.
Legal Values	• Port • Device
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.VFAllocMult (Read Only)

Description	Defines the multiple (e.g. x1, x4, x8, etc.) in which VFs must be allocated to a PF. [VENDOR provide appropriate help text for the implementation - what is allowed, etc].
Legal Values	Integer values from 1 to 255.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.DeviceLevelConfig.VirtualizationMode (Read or Write)

Description	The Virtualization Mode setting for the device. Note: Not all PCI slots in all servers are capable of supporting virtualization features based on ARI and SR-IOV. The implementation shall check the state of the ARI forwarding bit in the immediate upstream PCI ports config space settings (Device Control Register 2, bit 5) to ensure that it is set before allowing the selection of SR-IOV and NParEP by the user, if not, those selections shall be disallowed. Specify the type of virtualization used by the controller on all ports.
Legal Values	• None • NPar • SR-IOV • NPar + SR-IOV • Advanced NPar • Advanced NPar + SR-IOV
Default Value	NONE
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	To get the actual supported values for BIOS, NIC, and FC components, query the help with an index. If you query without an index, the generic help is displayed.

NIC.FCOECapabilities.AddressingMode (Read Only)

Description	Addressing Mode utilized for FCoE transactions Specify whether SPMA or FPMA addressing will be used for FCoE transactions.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MTUReconfigurationSupport (Read Only)

Description	Indicates whether the MTU Reconfiguration capability is supported. Indicates whether the MTU Reconfiguration capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxFrameSize (Read Only)

Description	The maximum frame size of each FCoE frame. Maximum frame size of each FCoE frame.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxIOsPerSession (Read Only)

Description	The maximum number of IOs supported per session. Maximum number of IOs supported per session.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxNPIVPerPort (Read Only)

Description	The maximum number of NPIV WWNs per port. Maximum number of NPIV WWNs per port.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxNumberExchanges (Read Only)

Description	The maximum number of exchanges supported. Maximum number of exchanges supported.

Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxNumberLogins (Read Only)

Description	The maximum number of logins supported per port. Maximum number of logins supported per port.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxNumberOfFCTargets (Read Only)

Description	The maximum number of FC targets supported. Maximum number of FC targets supported.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCOECapabilities.MaxNumberOutStandingCommands (Read Only)

Description	The maximum number of outstanding commands supported across all sessions. Maximum number of outstanding commands supported across all sessions.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.BootOrderFirstFCoETarget (Read or Write)

Description	Setting to specify whether and in what order a boot from the ports first defined target is attempted. The current implementation allows for four potential boot targets to be defined per FCoE boot-capable port. Each target carries a boot order attribute. From all of the targets defined in all the vendors FCoE boot ports in the system, the user may select a maximum of four targets to attempt to boot from, assigning a boot order value from one to four (first to last). Targets not selected must be given a value of 0. The settings of one to four must be unique in the system; there must be no duplication of the values one to four in either the same port or in different ports across the system. The driver will enforce this requirement (a target previously assigned a boot order value of x is set to 0 when a new target is assigned a value of x). Specify this ports place in the FCoE boot order 1-4 or 0=disabled.
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.BootOrderFourthFCoETarget (Read or Write)

Description	Setting to specify whether and in what order a boot from the ports fourth defined target is attempted. Specify this ports place in the FCoE boot order 1-4 or 0=disabled.
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.BootOrderSecondFCoETarget (Read or Write)

Description	Setting to specify whether and in what order a boot from the ports second defined target is attempted. Specify this ports place in the FCoE boot order 1-4 or 0=disabled.
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.BootOrderThirdFCoETarget (Read or Write)

Description	Setting to specify whether and in what order a boot from the ports third defined target is attempted. Specify this ports place in the FCoE boot order 1-4 or 0=disabled.
Legal Values	Integer values.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.ConnectFirstFCoETarget (Read or Write)

Description	Setting to enable whether first target connection is attempted. Specify whether the FCoE initiator is to connect to the first FCoE storage target.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.FirstFCoEBootTargetLUN (Read or Write)

Description	LUN of the first FCoE storage target that the FCoE initiator will boot the system from when the Connect attribute is enabled. Specify the boot Logical Unit Number (LUN) of the first FCoE storage target that will be used by the FCoE initiator.
Legal Values	Integer values from 0 to 18446744073709551615.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.FirstFCoEFCFVLANID (Read or Write)

Description	Attribute for configuring the VLAN ID to be used to connect to the first FC storage target. Specify the VLAN ID to be used in connecting to the first FC storage target.
Legal Values	Integer values from 1 to 4094.

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.FirstFCoEWWPNTarget (Read or Write)

Description	World Wide Port Name of the first FCoE storage target. Note: At present, the Dell FCoE information model only defines one storage target. Specify the World Wide Port Name (WWPN) of the first FCoE storage target.
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEConfiguration.MTUParams (Read or Write)

Description	Configure scoping of the MTU setting. Specify the scope of the MTU (Maximum Transmission Unit) parameter.
Legal Values	• Global • Per DCB Priority • Per VLAN
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEGenParams.FCoEBootScanSelection (Read or Write)

Description	Configuration of the ports behavior in booting the system from FC Target(s). Only behaviors supported by the option-ROM need to be implemented. In the following cases, no fabric discovery shall be attempted: Disabled - Initiator does not attempt to boot. Specified LUN - Initiator attempts to boot to the specified World Wide Port Name and LUN for 1st target, if that fails then a boot using the 2nd target parameters shall be attempted. In the following cases, fabric discovery shall be attempted and the resulting discovered targets will be put in a list sorted by the reported FC destination ID. This list will be checked in order until the selected LUN policy is met: First LUN - attempt boot from the first bootable LUN of the targets discovered by adapter. First LUN 0 - attempt boot from the first bootable LUN 0 of the targets discovered by adapter. First LUN Not LUN 0 - attempt boot from the first bootable LUN that is not LUN 0 of the targets discovered by adapter. Fabric Discovered LUN - attempt boot based on the LUN assignment provided by management infrastructure in the fabric. Specify the FCoE initiator behavior for booting the system from specified Fibre Channel boot target(s) or fabric discovered target(s).
Legal Values	• Disabled • First LUN

- First LUN 0
- First LUN Not LUN 0
- Fabric Discovered LUN
- Specified LUN

Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEGenParams.FCoEFabricDiscoveryRetryCnt (Read or Write)

Description	Retry count for FCoE fabric discovery. Specify the retry count for FCoE fabric discovery.
Legal Values	Integer values from 0 to 60.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEGenParams.FCoEFirstHddTarget (Read or Write)

Description	Specifies whether the FCoE target is represented as the first HDD to the system. Specify whether the FCoE target is represented as the first HDD to the system.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEGenParams.FCoELnkUpDelayTime (Read or Write)

Description	Controls how long the FCoE initiator waits, in seconds, after an Ethernet link is established before sending any data over the network Specify how long the FCoE Initiator waits after an Ethernet link is established before sending any data over the network. Units are in seconds.
Legal Values	Integer values from 0 to 255.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEGenParams.FCoELunBusyRetryCnt (Read or Write)

Description	Controls the number of connection retries the FCoE boot initiator will attempt if the FCoE target LUN is busy. Specify the number of connection retries the FCoE boot initiator will attempt if the FCoE target LUN is busy.
Legal Values	Integer values from 0 to 60.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FCoEGenParams.FCoETgtBoot (Read or Write)

Description	Attribute for setting whether system boot to the FCoE target is attempted. Enables the FCoE initiator to boot the system to the FCoE target. One Time Disabled disables FCoE boot for the next (current) boot, after which it is enabled.
Legal Values	• Enabled • Disabled • One Time Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FrmwImgMenu.ControllerBIOSVersion (Read Only)

Description	Controller BIOS version information Installed device BIOS version information.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FrmwImgMenu.EFIVersion (Read Only)

Description	EFI device driver version information. Installed device EFI driver version information.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.FrmwImgMenu.FamilyVersion (Read Only)

Description	Firmware family version information. Same as what is returned in the PackageVersionName field by the Firmware Management Protocol GetPackageInfo() call. Installed device firmware family version information.
Legal Values	String of up to 11 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.GlobalBandwidthAllocation.MaxBandwidth[Partition:n] (Read or Write)

Description	The maximum percentage of port TX bandwidth allocated to the partition. Oversubscription is allowed. Specified on a per partition basis. Replace n with the number of the partition. Maximum Bandwidth represents the maximum transmit bandwidth of the partition as a percentage of the full physical port link speed. The Maximum Bandwidth range is 0-100 percent for each enabled partition.
Legal Values	Integer values from 0 to 100.
Default Value	100
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.GlobalBandwidthAllocation.MinBandwidth[Partition:n] (Read or Write)

Description	The minimum percentage of port TX bandwidth allocated to the partition. Alternatively, this value represents a relative bandwidth weighting of partition traffic to other partitions. Specified on a per partition basis. Replace n with the number of the partition. [Vendor: modify as appropriate.] Minimum Bandwidth represents the minimum transmit bandwidth of the partition as a percentage of the full physical port link speed. The Minimum Bandwidth range is 0-100 percent for each enabled partition.
Legal Values	Integer values from 0 to 100.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.ConnectFirstTgt (Read or Write)

Description	Setting to enable whether connection to the first target is attempted. Enable connecting to the first iSCSI target.
Legal Values	• Enabled • Disabled

Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtBootLun (Read or Write)

Description	Specifies the first iSCSI target boot LUN. Specify the boot Logical Unit Number (LUN) on the first iSCSI storage target.
Legal Values	Integer values from 0 to 18446744073709551615.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtChapId (Read or Write)

Description	First Target CHAP ID (up to 128 characters in length). If only a single value of CHAP ID supported then it is stored here. Specify the first iSCSI storage target Challenge-Handshake Authentication Protocol (CHAP) ID. [vendor to specify what is allowed].
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtChapPwd (Read or Write)

Description	First Target CHAP Secret (0 or 12 to 16 characters in length). If only a single value of CHAP Secret is supported then it is stored here. Specify the Challenge-Handshake Authentication Protocol secret (CHAP password) of the first iSCSI storage target. [Vendor to specify what is allowed].
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtIpAddress (Read or Write)

Description	First iSCSI target IP address. Will be either IPv4 or IPv6 format depending on the value of the FirstTgtIpVer attribute. Specify the IP address of the first iSCSI target.
Legal Values	String of up to 39 ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtIpVer (Read or Write)

Description	Setting displays and allows configuration of IP version used for first iSCSI target when iSCSIDualIPVersionSupport is available. Specify whether IPv4 or IPv6 network addressing will be used for first iSCSI target.
Legal Values	• IPv4 • IPv6
Default Value	IPv4
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtIscsiName (Read or Write)

Description	The iSCSI Qualified Name (IQN) of the first target. Specify the iSCSI Qualified Name (IQN) of the first iSCSI storage target.
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiFirstTgtParams.FirstTgtTcpPort (Read or Write)

Description	TCP Port number of the first iSCSI target. Specify the TCP Port number of the first iSCSI target.
Legal Values	Integer values from 1 to 65535.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.ChapAuthEnable (Read or Write)

Description	Setting to enable CHAP Authentication for iSCSI initiator. Enable the ability of the initiator to use CHAP authentication when connecting to the iSCSI target.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A

License Required	Express License
Dependency	None

NIC.IscsiGenParams.ChapMutualAuth (Read or Write)

Description	Setting to enable mutual CHAP authentication between the iSCSI initiator and target. To use mutual CHAP authentication, specify an initiator secret on the Initiator Parameters page and configure that secret on the target.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.DhcpVendId (Read or Write)

Description	Vendor ID as presented to DHCP service. Control what Vendor ID is presented to the DHCP service.
Legal Values	String of up to 255 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.FirstHddTarget (Read or Write)

Description	Enable/Disable the target appearing as the first hard disk drive (HDD) in the system when iSCSI booting. Specify whether the iSCSI target appears as the first hard disk drive (HDD) in the system.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.IpAutoConfig (Read or Write)

Description	Setting to enable acquisition of IPv6 TCP/IP parameters from DHCP. This option is specific to IPv6. Controls the source of the initiator IP address, DHCP or static assignment.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A

License Required	Express License
Dependency	None

NIC.IscsiGenParams.IpVer (Read or Write)

Description	Setting displays and allows configuration of the IP version used by iSCSI initiator and targets (Initiator only when a separate target ipver is implemented). If only one IP version is supported, this attribute should be set to that version and be made Read Only. Specify whether IPv4 or IPv6 network addressing will be used for iSCSI initiator and targets (Applies to the Initiator only when a separate target IP Version is implemented). [Vendor to provide implementation-specific language].
Legal Values	• IPv4 • IPv6 • None
Default Value	IPv4
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.IscsiTgtBoot (Read or Write)

Description	Boot to iSCSI target after connection. Specify whether the iSCSI initiator will boot to the specified iSCSI target after connection. One Time Disabled disables iSCSI boot for the next (current) boot, after which it is enabled.
Legal Values	• Enabled • Disabled • One Time Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.IscsiVlanId (Read or Write)

Description	VLAN ID used for iSCSI boot. Specify the VLAN ID to be used for iSCSI boot mode. The VLAN ID must be in the range from 1 to 4094. [Vendor confirm support for this range].
Legal Values	Integer values from 1 to 4094.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.IscsiVlanMode (Read or Write)

Description	Enable/Disable Virtual LAN mode for iSCSI boot. Specify use of a VLAN tag to be used by iSCSI boot.

Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.IscsiViaDHCP (Read or Write)

Description	Setting to enable acquisition of iSCSI target parameters from DHCP. Enables the acquisition of iSCSI target parameters from DHCP.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.LnkUpDelayTime (Read or Write)

Description	The time to wait for the link to establish before driver initialization. Specifies how long the iSCSI boot host software should wait, in seconds, after an Ethernet link is established before sending any data over the network.
Legal Values	Integer values from 0 to 255.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.LunBusyRetryCnt (Read or Write)

Description	Controls the retry count for target. Specify the number of connection attempts the iSCSI boot initiator will attempt if the iSCSI target LUN is busy.
Legal Values	Integer values from 0 to 60.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.TcplpViaDHCP (Read or Write)

Description	Setting to enable acquisition of IPv4 TCP/IP parameters from DHCP This option is specific to IPv4. Controls the source of the initiator IP address, DHCP or static assignment.

Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.TcpTimestmp (Read or Write)

Description	Enable/Disable use of TCP timestamps in network packets Specify use of TCP timestamps in network packets, as defined in RFC 1323.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiGenParams.WinHbaBootMode (Read or Write)

Description	Controls if adapter boots as an iSCSI Offload HBA or uses software initiator mode Enable iSCSI Offload HBA boot mode and disables iSCSI software initiator boot mode.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorChapId (Read or Write)

Description	Initiator CHAP ID (up to 128 characters in length). If this can be set on a per target basis, then the first target value shall be stored here. Specify the iSCSI initiator Challenge-Handshake Authentication Protocol (CHAP) ID. [Vendor to describe what is allowed].
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorChapPwd (Read or Write)

Description	iSCSI initiator CHAP secret (0 or 12 to 16 characters in length). If this can be set on a per target basis, then the value for the first target shall be stored here. Specify the iSCSI initiator Challenge-Handshake Authentication Protocol (CHAP) secret (password). [Vendor to describe what is allowed].
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorGateway (Read or Write)

Description	iSCSI initiator default Gateway IP address. Will be in either IPv4 or IPv6 format depending on the value of the IpVer attribute. Specify the IP address of the default Gateway used by the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpAddr (Read or Write)

Description	The iSCSI initiator IP address. Will be either in IPv4 or IPv6 format depending on value of the IpVer attribute. Specify the IP address of the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv4Addr (Read or Write)

Description	The iSCSI initiator IP address in IPv4 format when iSCSIDualIPVersionSupport is available. Specify the IPv4 address of the iSCSI initiator.
Legal Values	String of up to 15 ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv4Gateway (Read or Write)

Description	The iSCSI initiator default Gateway IP address in IPv4 format when iSCSIDualIPVersionSupport is available. Specify the IPv4 IP address of the default Gateway used by the iSCSI initiator.
Legal Values	String of up to 15 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv4PrimDns (Read or Write)

Description	iSCSI initiator Primary DNS IP Address in IPv4 format when iSCSIDualIPVersionSupport is Available. Specify the IPv4 IP address of the Primary DNS used by the iSCSI initiator.
Legal Values	String of up to 15 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv4SecDns (Read or Write)

Description	iSCSI initiator Secondary DNS IP address in IPv4 format when iSCSIDualIPVersionSupport is Available. Specify the IPv4 IP address of the Secondary DNS used by the iSCSI initiator.
Legal Values	String of up to 15 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv6Addr (Read or Write)

Description	The iSCSI initiator IP address in IPv6 format when iSCSIDualIPVersionSupport is available. Specify the IPv6 IP address of the iSCSI initiator.

Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv6Gateway (Read or Write)

Description	The iSCSI initiator default Gateway IP address in IPv6 format when iSCSIDualIPVersionSupport is available. Specify the IPv6 IP address of the default Gateway used by the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv6PrimDns (Read or Write)

Description	The iSCSI initiator Primary DNS IP Address in IPv6 format when iSCSIDualIPVersionSupport is Available. Specify the IPv6 IP address of the Primary DNS used by the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorIpv6SecDns (Read or Write)

Description	The iSCSI initiator Secondary DNS IP address in IPv6 format when iSCSIDualIPVersionSupport is Available. Specify the IPv6 IP address of the Secondary DNS used by the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorName (Read or Write)

Description	Setting to represent and set the iSCSI initiator iSCSI Qualified Name (IQN). Specify the initiators iSCSI Qualified Name (IQN).
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorPrimDns (Read or Write)

Description	The iSCSI initiator Primary DNS IP Address. Will be in either IPv4 or IPv6 format depending on the value of the IpVer attribute. Specify the Primary DNS IP address used by the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorSecDns (Read or Write)

Description	The iSCSI initiator Secondary DNS IP address. Will be in either IPv4 or IPv6 format depending on the value of the IpVer attribute. Specify the Secondary DNS IP address used by the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorSubnet (Read or Write)

Description	The iSCSI initiator Subnet Mask for an IPv4 initiator configuration. Specify the IPv4 Subnet Mask of the iSCSI initiator.
Legal Values	String of up to 15 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiInitiatorParams.IscsiInitiatorSubnetPrefix (Read or Write)

Description	The iSCSI initiator Subnet Mask Prefix for an IPv6 initiator configuration. Specify the IPv6 Subnet Mask Prefix of the iSCSI initiator.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.ConnectSecondTgt (Read or Write)

Description	Setting to enable whether connection to the second target is attempted. Enable connecting to the second iSCSI target.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtBootLun (Read or Write)

Description	Specifies the second iSCSI target boot LUN. Specify the boot Logical Unit Number (LUN) on the second iSCSI storage target.
Legal Values	Integer values from 0 to 18446744073709551615.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtChapId (Read or Write)

Description	Second Target CHAP ID (up to 128 characters in length). If only a single value of CHAP ID supported for all targets then it is stored here Specify the Challenge-Handshake Authentication Protocol (CHAP) ID of the second iSCSI storage target. [Vendor to specify what is allowed].
Legal Values	String of up to 128 ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtChapPwd (Read or Write)

Description	Second Target CHAP Secret (0 or 12 to 16 characters in length). If only a single value of CHAP Secret is supported then it is stored here Specify the Challenge-Handshake Authentication Protocol (CHAP) secret (target CHAP password) of the second iSCSI storage target. [Vendor to specify what is allowed].
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtIpAddress (Read or Write)

Description	Second iSCSI target IP address. Will be either IPv4 or IPv6 format depending on the value of the SecondTgtIpVer attribute Specify the IP address of the second iSCSI target.
Legal Values	String of up to 39 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtIpVer (Read or Write)

Description	Setting displays and allows configuration of IP version used for second iSCSI target when iSCSIDualIPVersionSupport is available Specify whether IPv4 or IPv6 network addressing will be used for the second iSCSI target.
Legal Values	• IPv4 • IPv6
Default Value	IPv4
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtIscsiName (Read or Write)

Description	The iSCSI Qualified Name (IQN) of the second target Specify the iSCSI Qualified Name (IQN) of the second iSCSI storage target.
Legal Values	String of up to 223 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondTgtParams.SecondTgtTcpPort (Read or Write)

Description	TCP Port number of second iSCSI target Specify the TCP Port number of the second iSCSI target.
Legal Values	Integer values from 1 to 65535.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondaryDeviceParams.SecondaryDeviceMacAddr (Read or Write)

Description	MAC address of the secondary iSCSI boot adapter. Specify the MAC address of a secondary iSCSI boot adapter for redundancy in case of a boot failure.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.IscsiSecondaryDeviceParams.UseIndTgtName (Read or Write)

Description	Use Independent Target Name when multipath I/O is enabled Specify whether to use Independent Target Name when MPIO is enabled.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A

License Required	Express License
Dependency	None

NIC.IscsiSecondaryDeviceParams.UseIndTgtPortal (Read or Write)

Description	Setting to use independent target portal when multipath I/O is enabled Specify whether to use Independent Target Portal (Enable when using MPIO mode).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.LnkSpeedConfig.100Gbps1 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Gbps (1 lane of 100 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.100Gbps2 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Gbps (2 lanes of 50 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.100Gbps4 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Gbps (4 lanes of 25 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.100Mbps (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Mbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.10Gbps (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 10 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.10Mbps (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and

should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 10 Mbps

Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.1Gbps (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 1000 Mbps/1 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.200Gbps1 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 200 Gbps (1 lane of 200 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.200Gbps2 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 200 Gbps (2 lanes of 100 Gb)
Legal Values	• True • False
Default Value	True

Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.200Gbps4 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 200 Gbps (4 lanes of 50 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.25Gbps (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 25 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.40Gbps (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 40 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.50Gbps1 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 50 Gbps (1 lane of 50 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.LnkSpeedConfig.50Gbps2 (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for boot protocol operations and possibly including Wake On LAN and shared LOM management features if separate Vaux link speed control is not supported. This setting is only valid when LnkSpeedMethod is set to Manual and should be greyed out when set to Auto. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 50 Gbps (2 lanes of 25 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.NICConfig.BannerMessageTimeout (Read or Write)

Description	Timeout in seconds for banner display during POST Specify the number of seconds that the OptionROM banner is displayed during POST.
Legal Values	Integer values from 0 to 14.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.BootOptionROM (Read or Write)

Description	This attribute provides enable/disable functionality to the boot entry point (i.e. undi_init) of the legacy Option ROM of the port, effectively controlling the ability to legacy boot via PXE, iSCSI or FCoE. The Option ROM is still required to advertise itself to BIOS and to expose other entry points (such as CLP and UEFI) for configuration purposes if this control is set to disabled. This control must be prohibited from being set to Disabled if the Legacy Boot Protocol attribute is set to anything but None. Controls the enablement of legacy Boot Protocols in the Option ROM.

Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.BootRetryCnt (Read or Write)

Description	Configure the number of retries in case of boot failure. Specify the number of retries to attempt in case of a boot failure.
Legal Values	• No Retry • 1 Retry • 2 Retries • 3 Retries • 4 Retries • 5 Retries • 6 Retries • Indefinite Retries
Default Value	NoRetry
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.BootStrapType (Read or Write)

Description	Configure the boot strap mechanism used to boot to the OS. Specify the boot strap method used to boot to the operating system.
Legal Values	• Auto Detect • BBS • Int 18h • Int 19h
Default Value	AutoDetect
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.FWBootProtocol (Read or Write)

Description	Selection of the boot protocol for the CNA port when the boot process is local to the controller. Select the boot protocol to be used for boot operations handled by the adapter. Legacy PXE must be selected when the System Boot Mode is set to Legacy.
Legal Values	• Legacy PXE • UEFI iSCSI HBA • UEFI FCoE • None

Default Value	varies
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.NICConfig.HideSetupPrompt (Read or Write)

Description	Enable/Disable the option ROM setup prompt (banner) during POST. Specify whether to display or hide the legacy Option ROM setup prompt during system Power On Self Test (POST).
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.LegacyBootProto (Read or Write)

Description	Selection of the boot protocol for the port to use in legacy BIOS (non-UEFI) boot mode. The default value of the setting varies by implementation and is defined in ENG0012856. Select a boot protocol to be used in legacy BIOS (non-UEFI) boot mode.
Legal Values	• PXE • iSCSI • FCoE • None • iSCSI Primary • iSCSI Secondary • iPXE without failover • iSCSI without failover
Default Value	varies
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.LnkSpeed (Read or Write)

Description	Selector for link speed(s) to be advertised to link partner for boot operations. Implementations should only include supported link speeds. Existing implementations may remain unchanged, new implementations should not use those speeds listed as deprecated but use the new speeds that have been added that infer what modulation scheme is in use, NRZ or PAM4. New implementations should transition to allow multiple speeds to be selected instead of just one in a simple enumeration scheme. Specifies the port link speed to be used when booting the selected protocol.
Legal Values	• Auto Negotiated • 10 Mbps Half • 10 Mbps Full • 100 Mbps Half • 100 Mbps Full

- 1 Gbps
- 10 Gbps
- 25 Gbps
- 40 Gbps
- 50 Gbps (2x25)
- 50 Gbps (1x50)
- 100 Gbps (4x25)
- 100 Gbps (2x50)
- 100 Gbps (1x100)
- 200 Gbps (4x50)
- 200 Gbps (2x100)
- 200 Gbps (1x200)

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.LnkSpeedMethod (Read or Write)

Description	Replacement for the previously defined LinkSpeed attribute to be used (at least) for those controllers that support speeds above 25 Gbps. This attribute allows the user to select between auto and manual modes of configuring what the port advertises for link negotiation. Select how to choose which port link parameters to advertise for system boot operation, automatically or by user selection. [VENDOR: modify to suit your implementation]
Legal Values	• Auto • Manual
Default Value	Auto
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.NICConfig.NumberVFAdvertised (Read or Write)

Description	This value is the number of PCI Virtual Functions Advertised by the port (function) in PCI config space when SR-IOV is enabled in non-NPar mode. Specify the number of PCI Virtual Functions (VFs) to be advertised on this port in non-NPAR mode.
Legal Values	Integer values from 0 to 256.
Default Value	0
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.PermitTotalPortShutdown (Read or Write)

Description	When implemented and enabled, any port down command from the host OS or driver will cause the network port to completely shut down and cease all operations including support of WoL and NC-SI Pass-through. Shutdown is defined as no electrical activity (e.g., PHY disabled) and no LED

activity. It does not imply or require any physical or electrical isolation. Not intended for implementation or use on backplane designs. External network traffic to and from any VF instantiated on any PF on the shut down port is similarly shut down. Maintaining traffic flow between internal functions when the port is shutdown is implementation dependent. Specifies whether or not to allow the port to be completely disabled when a Port Down command is received from the Host OS or driver. NOTE: Use with caution, port shutdown will halt all operations configured on the port including WakeOnLAN and shared LOM. [VENDOR: modify to include any corner cases of the implementation]

Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.NICConfig.VLanId (Read or Write)

Description	Specifies the VLAN tag to be used with the selected boot protocol. Specify the VLAN tag to be used with the selected boot protocol. The VLAN ID must be in the range from 1 to 4094. [Vendor to provide implementation-specific language].
Legal Values	Integer values from 1 to 4094.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.VLanMode (Read or Write)

Description	Enable/Disable VLAN tagging on the selected boot protocol. Note: The vendor will have to customize help text to define what boot protocols can use VLAN tagging. Virtual LAN mode enables use of a VLAN tag to be used by [vendor specify boot protocols that support VLAN].
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.WakeOnLan (Read or Write)

Description	Enable/Disable Wake On LAN feature Enables the server to be powered on using an in-band magic packet.
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	Express License

Dependency None

NIC.NICConfig.WakeOnLanLnkSpeed (Read or Write)

Description	Selector for link speed(s) to be advertised to link partner for Vaux operations including Wake On LAN and shared LOM management features. Implementations should only include supported link speeds. Existing implementations may remain unchanged, new implementations should not use those speeds listed as deprecated but use the new speeds that have been added that infer what modulation scheme is in use, NRZ or PAM4. New implementations should transition to allow multiple speeds to be selected instead of just one in a simple enumeration scheme. Select the port speed used for Wake on LAN mode and Vaux Management traffic. [VENDOR to modify appropriately]
Legal Values	• Auto Negotiated • 10 Mbps Half • 10 Mbps Full • 100 Mbps Half • 100 Mbps Full • 1 Gbps • 10 Gbps • 25 Gbps • 40 Gbps • 50 Gbps (2x25) • 50 Gbps (1x50) • 100 Gbps (4x25) • 100 Gbps (2x50) • 100 Gbps (1x100) • 200 Gbps (4x50) • 200 Gbps (2x100) • 200 Gbps (1x200)
Default Value	AutoNeg
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICConfig.WakeOnLanLnkSpeedMethod (Read or Write)

Description	Replacement for the previously defined WakeOnLanLnkSpeed attribute to be used (at least) for those controllers that support speeds above 25 Gbps. This attribute allows the user to select between auto and manual modes of configuring what the port advertises for link negotiation. Note: If an implementation only supports one pre-OS link speed configuration, this attribute should not be implemented. Select how to choose which port link parameters to advertise for Wake On LAN and shared LOM modes of operation, automatically or by user selection . [VENDOR: modify to suit your implementation]
Legal Values	• Auto • Manual
Default Value	Auto
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.NICPartitioningConfig.FlowControlSetting (Read or Write)

Description	Representation and configuration field for Ethernet Flow Control. Note: This setting only controls the ports Flow Control behavior when in NPar modes of operation, but not when PFC is enabled; The OS driver retains control of Flow Control when NPar is not enabled. Specify the type of Ethernet Flow Control to be used by the port when operating in NPar mode.
Legal Values	• Auto • TX:Send Pause on RX Overflow • RX:Throttle TX on Pause Received • TX / RX Flow Control • None
Default Value	Auto
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICPartitioningConfig.NicPartitioning (Read or Write)

Description	Representation and configuration of enablement of partitioning for the device. Note: This attribute is for current HII/UEFI drivers that implement the control ONLY. New HII implementations should only implement the Virtualization Mode attribute. Existing implementations should maintain support for legacy reasons. Enables or disables NIC partitioning for all device ports.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICPartitioningConfig.NumberPCIFunctionsEnabled (Read Only)

Description	The number of PCI Physical Functions currently enabled on this port. The number of PCI Physical Functions currently enabled on this port.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICPartitioningConfig.NumberPCIFunctionsSupported (Read Only)

Description	The number of PCI Physical Functions supported on this port. This value may change depending on the support and configuration of NParEP. The number of PCI Physical Functions supported on this port. This value may change depending on the support and configuration of NParEP.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.NICPartitioningConfig.PartitionState[Partition:n] (Read Only)

Description	Representation of the current enablement state of the partition. There will be an instance of this attribute for each partition. Replace n with the number of the partition. Representation of the current enablement state of the partition.
Legal Values	• Enabled • Disabled
Default Value	Enabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.PortLevelConfig.VFDistribution (Read or Write)

Description	The value is a string of numbers, each separated by a colon that defines the distribution of VFs to PFs within the domain specified by VFAllocBasis. Each number represents the number of PVI Virtual Functions to be advertised in PCI config space by each partition (PF). The numbers must sum to an amount less than or equal to the NumberVFSupported attribute value. A value appears in the colon separated list for each Physical Function that can potentially be present within the allocation domain, independent of its enablement state. Values in the list from left to right apply to function numbers in the domain from least to greatest. Note1: The regex can only perform basic validation of the string format. Note2: Implementers should replace the "*" in the regex with a bound expression that accurately describes the expected string in the context of a given solution (e.g. where NumberVFSupported is 4, the "*" will be replaced with "{3}"). The vendor must provide the appropriate default string for the implementation. Defines the distribution of VFs to PFs within the domain specified by VFAllocBasis. A value appears in the colon separated list for each Physical Function that can potentially be present within the allocation domain. Values in the list from left to right apply to function numbers in the domain from least to greatest. [VENDOR modify appropriately]
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.BlinkLeds (Read or Write)

Description	Blink LEDs for a duration of up to 15 seconds. Only valid for adapters with link LEDs. Specify the number of seconds the LEDs on the physical network port should blink to assist with port identification.
Legal Values	Integer values from 0 to 15.
Default Value	15
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.BusDeviceFunction (Read Only)

Description	The value of this attribute depends on the state of the NParEP Mode setting. If NParEP Mode is Disabled, the value is the BIOS assigned PCIe Bus:Device:Function identifier. If NParEP Mode is Enabled, the value is the BIOS assigned PCIe Bus:Function identifier. Indicates the PCI Address of the Physical Function assigned to the port.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.ChipMdl (Read Only)

Description	This attribute consists of the concatenation of 2 different elements, a vendor-defined silicon marketing name and the silicon revision information as specified in PCI configuration space, separated by space. For example: R720 B0. Specifies the Chip Type.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.DCBXSupport (Read Only)

Description	Indicates whether Data Center Bridging eXchange Protocol (DCBX) is supported. Specify whether Data Center Bridging eXchange Protocol (DCBX) is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.DeviceName (Read Only)

Description	Official product name of the device. Official product name of the device.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.EEEControl (Read or Write)

Description	Enables or Disables the Energy Efficient Ethernet feature on the port if supported by the device. If the scope of the control is not port level, then consultation with Dell is required. The default value of this attribute is specified in the EHRD for the implementation and will not be the same for all adapters. Note: Do not implement if EEE is not supported by the implementation (i.e., the EnergyEfficientEthernet attribute setting). Enables or Disables the Energy Efficient Ethernet feature on the [VENDOR: specify the scope of control, (e.g., port, controller, adapter)]
Legal Values	• Maximum Power Savings • Disabled
Default Value	varies
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.EnergyEfficientEthernet (Read Only)

Description	Indicates whether Energy Efficient Ethernet capability is supported. Indicates whether Energy Efficient Ethernet capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.FCoEBootSupport (Read Only)

Description	Indicates whether Fibre Channel over Ethernet Boot capability is supported. Indicates whether Fibre Channel over Ethernet Boot capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.FCoEOffloadMode (Read or Write)

Description	Enable/Disable the FCoE personality on the port. This setting is for when operating in non-NPar mode only. Enables the port for FCoE storage traffic.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.FCoEOffloadSupport (Read Only)

Description	Indicates whether FCoE is supported. Indicates whether FCoE is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.FIPMacAddr (Read Only)

Description	Permanent FIP-MAC address for FCoE assigned during manufacturing. If supported, the current address value should be readable at all times, irrespective of feature enablement. Permanent FIP-MAC address for FCoE assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.FeatureLicensingSupport (Read Only)

Description	Indicates whether the Dell Feature Licensing capability is supported. Indicates whether Dell Feature Licensing capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.FlexAddressing (Read Only)

Description	Indicates whether the Dell FlexAddressing feature is supported. Indicates whether the Dell FlexAddressing feature is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.ForwardErrorCorrection (Read or Write)

Description	Type of FEC to use on the link. Shall not be implemented on adapters where it is not appropriate. Specify the type of Forward Error Correction to use on the link (if appropriate)
Legal Values	• Auto • Fire Code (Clause 74) • RS-FEC (Clause 91, 108, 134) • Disabled
Default Value	Auto
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.InfiniBand (Read Only)

Description	Indicates whether InfiniBand functionality is supported. Indicates whether InfiniBand functionality is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.IscsiMacAddr (Read Only)

Description	Permanent MAC address for iSCSI offload assigned during manufacturing. If supported, the current address value should be readable at all times, irrespective of feature enablement. Permanent MAC address for iSCSI offload assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License

Dependency None

NIC.VndrConfigPage.LinkStatus (Read Only)

Description Physical link status of the network port as reported by the controller. Physical link status of the network port as reported by the controller.

Legal Values

- Connected
- Disconnected

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

NIC.VndrConfigPage.MacAddr (Read Only)

Description The Permanent MAC address assigned during manufacturing. Permanent MAC address assigned during manufacturing.

Legal Values String of up to 17 ASCII characters.

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

NIC.VndrConfigPage.MediaDetection (Read or Write)

Description Optional attribute for those implementations that support the querying of the installed SFF device capabilities to assist in link configuration. How this information is used may differ between implementations. Should not be implemented on adapters where it is not used. Query the installed SFF device capabilities to assist in link configuration [VENDOR to modify appropriately]

Legal Values

- Enabled
- Disabled

Default Value varies

Write Privilege N/A

License Required Not Applicable

Dependency None

NIC.VndrConfigPage.NVMeTCPOffloadSupport (Read Only)

Description Indicates whether the NVMe/TCP Offload capability is supported. Indicates whether the NVMe/TCP Offload capability is supported.

Legal Values String of ASCII characters.

Default Value None

Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.NWManagementPassThrough (Read Only)

Description	Indicates whether the Network Management Pass Through capability is supported. Indicates whether the Network Management Pass Through capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.NetworkLinkType (Read or Write)

Description	Select the protocol type to be used on a port that supports multiple fabric types. NOTE: Implement ONLY if VPI Mode is supported Select port network protocol (Ethernet/InfiniBand)
Legal Values	• Ethernet • InfiniBand
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.NicMode (Read or Write)

Description	Enable/Disable the NIC personality on the port. This setting is for when operating in non-NPar mode only. Note: This personality type should be specified as the port default if RDMA is not supported or has dependencies on other device modes or settings. Specify use of the port for L2-Ethernet traffic.
Legal Values	• Enabled • Disabled
Default Value	Varies
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.NicPartitioningSupport (Read Only)

Description	Indicates whether the NIC Partitioning capability is supported. Indicates whether NIC Partitioning capability is supported.
Legal Values	String of ASCII characters.

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.NodeGUID (Read Only)

Description	The Permanent Node GUID assigned during manufacturing. Permanent Node GUID assigned during manufacturing.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.NvmeTcpBusDeviceFunction (Read Only)

Description	The value of this attribute depends on the state of the NParEP Mode setting. If NParEP Mode is Disabled, the value is the BIOS assigned PCIe Bus:Device:Function identifier of the NVMe/TCP PF . If NParEP Mode is Enabled, the value is the BIOS assigned PCIe Bus:Function identifier of the NVMe/TCP PF . Indicates the PCI Address of the NVMe/TCP Physical Function on the port.
Legal Values	String of up to 8 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.NvmeTcpMacAddr (Read Only)

Description	Permanent MAC address for NVMe/TCP Offload operation assigned during manufacturing. If supported, the current address value should be readable at all times, irrespective of feature enablement. Permanent MAC address for NVMe/TCP assigned during manufacturing.
Legal Values	String of up to 17 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.NvmeTcpMode (Read or Write)

Description	Enable/Disable the NVMe/TCP personality on the port. This setting is for when operating in non-NPar mode Enables the port for NVMe/TCP storage traffic after boot. If disabled, the user may enable it in the OS, but a reboot is required for activation.
Legal Values	• Enabled • Disabled
Default Value	Disabled
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.NvmeTcpPCIDeviceID (Read Only)

Description	PCI Device ID reported by the NVMe/TCP PF when operating in non-NPar mode only. This value is also reported as the Device ID of NVMe/TCP PF at the partition level in NPar modes. PCI Device ID of the NVMe/TCP Physical Function.
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.OSBMCManagementPassThrough (Read Only)

Description	Indicates whether OS-BMC Management Pass Through capability is supported. Indicates whether OS-BMC Management Pass Through capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.OmniPath (Read Only)

Description	Indicates whether Omni-Path functionality is supported. Indicates whether Omni-Path functionality is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.OnChipThermalSensor (Read Only)

Description	Indicates whether an on-chip thermal sensor is available. Indicates whether an on-chip thermal sensor is available.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.PCIDeviceID (Read Only)

Description	PCI Device ID reported by the controller when operating in non-NPar mode only. The value of the attribute is undefined for controllers operating in NPar mode that change their device IDs or support multiple PCI Device IDs at the partition level. PCI Device ID of the controller.
Legal Values	String of up to 4 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.PKey (Read or Write)

Description	PKey ID to be used by PXE boot in the InfiniBand environment PKey ID to be used by PXE boot in InfiniBand fabrics. Enter a number in the range 0-65535.
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.PXEBootSupport (Read Only)

Description	Indicates whether the PXE Boot capability is supported. Indicates whether PXE Boot capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.PortGUID (Read Only)

Description	The Permanent Port GUID assigned during manufacturing. Permanent Port GUID assigned during manufacturing.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.RDMANICModeOnPort (Read or Write)

Description	Enable/Disable the NIC + RDMA personality on the port. This setting is for when operating in non-NPar mode only. Note: This personality type may be specified as the port default if RDMA traffic can be supported irrespective of any other device mode or setting. Specify use of the port for both L2-Ethernet and RDMA traffic. [Vendor may want to customize type of RDMA supported].
Legal Values	• Enabled • Disabled
Default Value	Varies
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.RXFlowControl (Read Only)

Description	Indicates whether Receive (RX) Flow control capability is supported. Indicates whether Receive (RX) Flow control capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.RemotePHY (Read Only)

Description	Indicates whether RemotePHY capability is supported. Indicates whether RemotePHY capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.SNAPI (Read Only)

Description	Indicates the adapter supports SNAPI functionality by either special interfacing to the PCI slot connector or via cabling to another PCI slot. Indicates whether SNAPI functionality is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.SNAPIState (Read Only)

Description	Indicates whether SNAPI functionality is enabled. Note: Implement only if SNAPI support is set to Available Indicates whether SNAPI functionality is enabled
Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.SocketDirect (Read Only)

Description	Indicates whether Socket Direct functionality is supported. Indicates whether Socket Direct functionality is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.SocketDirectState (Read Only)

Description	Indicates whether Socket Direct functionality is enabled. Indicates whether Socket Direct functionality is enabled
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.TOESupport (Read Only)

Description	Indicates whether TCP/IP Offload Engine capability is supported Indicates whether TCP/IP Offload Engine capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.TXBandwidthControlMaximum (Read Only)

Description	Indicates whether Transmit(TX) Bandwidth Control Maximum capability is supported Indicates whether Transmit(TX) Bandwidth Control Maximum capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.TXBandwidthControlMinimum (Read Only)

Description	Indicates whether Transmit (TX) Bandwidth Control Minimum capability is supported Indicates whether Transmit (TX) Bandwidth Control Minimum capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.TXFlowControl (Read Only)

Description	Indicates whether Transmit (TX) Flow Control capability is supported Indicates whether Transmit (TX) Flow Control capability is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.VPI (Read Only)

Description	Indicates whether Virtual Protocol Interconnect (VPI) functionality is supported. Indicates whether Virtual Protocol Interconnect (VPI) functionality is supported.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.VirtFIPMacAddr (Read or Write)

Description	Programmatically assignable FIP-MAC address for FCoE. Virtual addresses written will also generate corresponding VWWNN and VWWPN addresses as defined in Y741D. The supported method of reverting to the permanent FIP-MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature enablement. Programmatically assignable FIP-MAC address for FCoE.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.VirtIscsiMacAddr (Read or Write)

Description	Programmatically assignable MAC address for iSCSI offload. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature enablement. Programmatically assignable MAC address for iSCSI offload.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.VirtMacAddr (Read or Write)

Description	Programmatically assignable MAC address. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent MAC address is by writing 0s to the virtual MAC. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature enablement. Programmatically assignable MAC address for port.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00

Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.VirtNodeGuid (Read or Write)

Description	Programmatically assignable Node GUID address used when only one PF is assigned to the port. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent Node GUID address is by writing 0s to the virtual Node GUID. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. Programmatically assignable Node GUID address.
Legal Values	String of up to 19 ASCII characters.
Default Value	0000:0000:0000:0000
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.VirtNvmeTcpMacAddr (Read or Write)

Description	Programmatically assignable MAC address for NVMe/TCP offload. Programmatic write for support of I/O Identity feature. The supported method of reverting to the permanent MAC address is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address should be readable at all times, irrespective of feature enablement. Programmatically assignable MAC address for NVMe/TCP offload.
Legal Values	String of up to 17 ASCII characters.
Default Value	00:00:00:00:00:00
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.VirtPortGUID (Read or Write)

Description	Programmatically assignable Port GUID. Virtual addresses written will also generate corresponding GUID as defined in Y741D. The supported method of reverting to the permanent GUID is by writing 0s as the virtual address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. If supported, the current address value should be readable at all times, irrespective of feature enablement. Programmatically assignable Port GUID assigned during manufacturing.
Legal Values	String of up to 19 ASCII characters.
Default Value	0000:0000:0000:0000
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.VndrConfigPage.VirtWWN (Read or Write)

Description	Programmatically assignable Fibre Channel World Wide Node Name identifier for FCoE. Virtual addresses written will also be modified by subsequent writes to the VirtFIP-MAC addresss as defined in Y741D. The supported method of clearing this virtual address is by writing 0s as the address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. Programmatically assignable Fibre Channel World Wide Node Name identifier for FCoE.
Legal Values	String of up to 23 ASCII characters.
Default Value	00:00:00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.VirtWWPN (Read or Write)

Description	Programmatically assignable Fibre Channel World Wide Port Name identifier for FCoE. Virtual addresses written will also be modified by subsequent writes to the VirtFIP-MAC addresss as defined in Y741D. The supported method of clearing this virtual address is by writing 0s as the address. If the virtual address has not been set or if it has been cleared by the defined method, its value shall be returned as 0s. . Programmatically assignable Fibre Channel World Wide Port Name identifier for FCoE.
Legal Values	String of up to 23 ASCII characters.
Default Value	00:00:00:00:00:00:00:00
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.WWN (Read Only)

Description	Fibre Channel World Wide Node Name identifier for FCoE Fibre Channel World Wide Node Name identifier for FCoE
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

NIC.VndrConfigPage.WWPN (Read Only)

Description	Fibre Channel World Wide Port Name identifier for FCoE Fibre Channel World Wide Port Name identifier for FCoE.
Legal Values	String of up to 23 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License

Dependency None

NIC.VndrConfigPage.iSCSIBootSupport (Read Only)

Description Indicates whether iSCSI Boot is supported. Indicates whether iSCSI Boot is supported.

Legal Values String of ASCII characters.

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

NIC.VndrConfigPage.iSCSIDualIPVersionSupport (Read Only)

Description Indicates support for simultaneous IPv4 and IPv6 configurations of the iSCSI initiator and iSCSI primary and secondary targets. Indicates support for simultaneous IPv4 and IPv6 configurations of iSCSI initiator and iSCSI primary and secondary targets.

Legal Values String of ASCII characters.

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

NIC.VndrConfigPage.iSCSIOffloadSupport (Read Only)

Description Indicates whether the iSCSI Offload capability is supported. Indicates whether the iSCSI Offload capability is supported.

Legal Values String of ASCII characters.

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

NIC.VndrConfigPage.iScsiOffloadMode (Read or Write)

Description Enable/Disable the iSCSI offload personality on the port. This setting is for when operating in non-NPar mode only. Specify use of the port for iSCSI offload storage traffic.

Legal Values

- Enabled
- Disabled

Default Value Disabled

Write Privilege N/A

License Required Express License

Dependency None

NIC.WakeOnLanLnkSpeedConfig.100Gbps1WoL (Read or Write)

Description Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Gbps (1 lane of 100 Gb)

Legal Values

- True
- False

Default Value True

Write Privilege N/A

License Required Not Applicable

Dependency None

NIC.WakeOnLanLnkSpeedConfig.100Gbps2WoL (Read or Write)

Description Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Gbps (2 lanes of 50 Gb)

Legal Values

- True
- False

Default Value True

Write Privilege N/A

License Required Not Applicable

Dependency None

NIC.WakeOnLanLnkSpeedConfig.100Gbps4WoL (Read or Write)

Description Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Gbps (4 lanes of 25 Gb)

Legal Values

- True
- False

Default Value True

Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.100MbpsWoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 100 Mbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.10GbpsWoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 10 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.10MbpsWoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 10 Mbps

Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.1GbpsWoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 1000 Mbps/1 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.200Gbps1WoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 200 Gbps (1 lane of 200 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.200Gbps2WoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be

implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out.
Note: The speed selection shall only be included if it is supported in the implementation. Advertise 200 Gbps (2 lanes of 100 Gb)

Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.200Gbps4WoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 200 Gbps (4 lanes of 50 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.25GbpsWoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 25 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.40GbpsWoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 40 Gbps
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.50Gbps1WoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 50 Gbps (1 lane of 50 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

NIC.WakeOnLanLnkSpeedConfig.50Gbps2WoL (Read or Write)

Description	Speed selector for the specified link speed to be advertised to the link partner for Vaux operations including Wake On LAN and shared LOM management features. If an implementation only supports one pre-OS link speed configuration for boot, WoL and management, then this speed attribute should not be implemented. When WakeOnLanLnkSpeedMethod is set to Auto, then this attribute should be greyed-out. Note: The speed selection shall only be included if it is supported in the implementation. Advertise 50 Gbps (2 lanes of 25 Gb)
Legal Values	• True • False
Default Value	True
Write Privilege	N/A
License Required	Not Applicable

Dependency None

STORAGE Attributes

Storage.Controller.BatteryLearnMode (Read or Write)

Description	Battery Learn Mode controls a RAID Controllers Battery Learn Cycle.
Legal Values	• Automatic • Warn only • Disabled
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	A battery should be present on the controller.

Storage.Controller.BackgroundInitializationRate (Read or Write)

Description	The Background Initialization (BGI) rate is the percentage of the systems resources dedicated to performing the background initialization of a virtual disk after it is created
Legal Values	Integer values from 1 to 100.
Default Value	100
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.CheckConsistencyMode (Read or Write)

Description	Check Consistency feature is used to verify the accuracy of the redundant (parity) information.
Legal Values	• Normal • Stop on Error
Default Value	Normal
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.MaxCapableSpeed (Read Only)

Description	This attribute represents the maximum link speed supported by the controller.
Legal Values	• 1_5_GBS

- 3_GBS
- 6_GBS
- 12_GBS

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.CopybackMode (Read or Write)

Description	This attribute represents the mode of restoring configuration of a virtual disk when a failed physical disk is replaced in an array.
Legal Values	• On • On with SMART • Off
Default Value	On
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.RAIDmaxPDsInSpan (Read Only)

Description	This attribute represents the maximum number of Physical Disks in a single Span, as supported by the controller.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.CheckConsistencyRate (Read or Write)

Description	The Check Consistency rate is the percentage of the systems resources dedicated to performing a check consistency on a redundant virtual disk.
Legal Values	Integer values from 1 to 100.
Default Value	100
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.RAIDloadBalancedMode (Read or Write)

Description	This attribute represents the ability to automatically use both controller ports connected to the same enclosure to route I/O requests.
Legal Values	• Automatic • Disabled
Default Value	Automatic
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	RACADM supports the attribute Storage.Controller.PossibleloadBalancedMode and WSMAN supports the attribute Storage.Controller.LoadBalancedMode.

Storage.Controller.RAIDmaxSpansInVD (Read Only)

Description	This attribute represents the maximum number of spans in a Virtual Disk, as supported by the controller.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.PatrolReadMode (Read or Write)

Description	Patrol Read is a feature for identifying disk errors in order to avoid disk failures and data loss or corruption. The Patrol Read only runs on disks that are being used in a virtual disk or that are hot spares.
Legal Values	• Automatic • Manual • Disabled
Default Value	Automatic
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.PatrolReadRate (Read Only)

Description	The Patrol Read Rate is the percentage of the systems resources dedicated to perform Patrol Read.
Legal Values	Integer values from 1 to 100.
Default Value	30
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	This attribute is not supported from Server Configuration Profile (SCP)

Storage.Controller.RAIDmaxSupportedVD (Read Only)

Description	This attribute represents the maximum number of virtual disks supported by the controller.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.RebuildRate (Read or Write)

Description	The Rebuild Rate is the percentage of the systems resources dedicated to rebuilding a failed disk when a rebuild is necessary.
Legal Values	Integer values from 1 to 100.
Default Value	100
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.ReconstructionRate (Read or Write)

Description	The Reconstruct Rate is the percentage of the systems resources dedicated to reconstructing a disk group after adding a physical disk or changing the RAID level of a virtual disk residing on the disk group
Legal Values	Integer values from 1 to 100.
Default Value	100
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.RAIDSupportedRAIDLevels (Read Only)

Description	This attribute provides a list of RAID levels supported by the controller.
Legal Values	• RAID-0 • RAID-1 • RAID-5 • RAID-10 • RAID-50 • RAID-60
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.RAIDsupportedDiskProt (Read Only)

Description	This attribute provides a list of Disk Protocols supported by the controller.
Legal Values	• SAS • SATA • SAS SATA • SAS SATA NVMe • NVMe
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.VirtualDisk.WritePolicy (Read or Write)

Description	The write policies specify whether the controller sends a write-request completion signal as soon as the data is in the cache or after it has been written to disk.
Legal Values	• Write Through • Write Back • Write Back Force
Default Value	WriteBack
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	This attribute is displayed as read-only when there is only one legal value to set.

Storage.Controller.RAIDspinDownIdleTime (Read Only)

Description	Spindown idle time is the amount of time in seconds an unconfigured or hotspare can be idle before being spinned down by the controller.
Legal Values	Integer values from 1 to 65535.
Default Value	30
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.VirtualDisk.ReadPolicy (Read or Write)

Description	The read policies indicate whether or not the controller should read sequential sectors of the virtual disk when seeking data.
Legal Values	• No Read-Ahead • Read-Ahead • AdaptiveReadAhead
Default Value	ReadAhead

Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	This attribute is displayed as read-only when there is only one legal value to set.

Storage.PhysicalDisk.RAIDPDState (Read Only)

Description	Physical Disk State shows the state of Physical disk that is part of a Virtual Disk.Configurable via XML configuration feature only.
Legal Values	• Unknown • Ready • Online • Foreign • Blocked • Failed • Non-RAID • Missing
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.VirtualDisk.DiskCachePolicy (Read or Write)

Description	Set the physical disk caching policy of all members of a Virtual Disk by enabling the Disk Cache Policy. When this feature is enabled, the physical disk writes data to the physical disk cache before writing it to the physical disk. Because it is faster to write data to the cache than to a disk, enabling this feature can improve system performance.
Legal Values	• Default • Enabled • Disabled
Default Value	Default
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.PhysicalDisk.RAIDHotSpareStatus (Read Only)

Description	On RAID controllers, a hot spare is a backup for a disk that fails. The attribute indicates whether a physical disk is Hot Spare and/or the type of hot spare.Configurable via XML configuration only.
Legal Values	• No • Dedicated • Global
Default Value	No
Write Privilege	N/A

License Required	Express License
Dependency	None
Notes	• These attributes are applicable only for SAS/SATA drives and not for PCIeSSD. • Dedicated is a read only value and cant be used to assign a dedicated hotspare. To assign a dedicated hotspare to a volume use attribute RAIDdedicatedSpare.

Storage.Enclosure.AssetTag (Read Only)

Description	Displays the Asset Tag information for the enclosure.
Legal Values	String of up to 10 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	• AssetName and AssetTag are applicable only for external enclosures. • If the enclosure is in Failed state, the information about the slots and their occupancy is not displayed.

Storage.PhysicalDisk.RAIDNegotiatedSpeed (Read Only)

Description	Negotiated Speed shows the speed of data transfer that the disk negotiated while spinning up and upon initial communication with the controller. This speed is dependent on the speed of the disk, the capable speed of the controller, the current speed of the controller on that connector, and the speed of the EMM (Enclosure Management Module) on the enclosure.
Legal Values	• 1_5_GBS • 3_GBS • 6_GBS • 12_GBS
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.VirtualDisk.Name (Read Only)

Description	Displays the name associated with a Virtual Disk.
Legal Values	String of up to 15 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.PhysicalDisk.RAIDNominalMediumRotationRate (Read Only)

Description	This attribute represents the nominal medium rotation speed of a physical disk.
Legal Values	Integer values from 2 to 4294967295.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.EncryptionMode (Read Only)

Description	This attribute represents encryption mode on the controller. It could be used to set the encryption mode to Local Key Management or Dell Key Management on the controller through XML configuration feature.Configurable via XML configuration feature only.
Legal Values	• None • Local Key Management • Dell Key Management
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	If set to Local Key Management you must set KeyID and NewControllerKey.

Storage.Enclosure.RAIDEffectiveSASAddress (Read Only)

Description	This attribute represents the effective SAS Address of an enclosure.
Legal Values	String of up to 16 ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	• AssetName and AssetTag are applicable only for external enclosures. • If the enclosure is in Failed state, the information about the slots and their occupancy is not displayed.

Storage.VirtualDisk.IncludedPhysicalDiskID (Read or Write)

Description	This is a pseudo attribute for XML configuration feature. It is used for specifying physical disk FQDD for creating a virtual disk. Configurable via XML configuration feature only.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A

License Required	Express License
Dependency	Applicable only if RAIDaction is Create

Storage.VirtualDisk.LockStatus (Read Only)

Description	This attribute represents security status of the virtual disk. It is used to secure a virtual disk using XML configuration feature. Configurable via XML configuration feature only.
Legal Values	• Unlocked • Locked
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if EncryptionMode is Local Key Mananegment or Dell Key Management and KeyID is set to any valid value.

Storage.Controller.OldControllerKey (Read or Write)

Description	This attribute represents the controller passphrase for Local Key Management encryption mode. This is used during a ReKey operation to specify the old controller key. Configurable via XML configuration feature only.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDrekey is set to True

Storage.Controller.NewControllerKey (Read or Write)

Description	This attribute represents the controller passphrase for Local Key Management encryption mode. This is used during a ReKey operation to specify the new controller key. Configurable via XML configuration feature only.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if EncryptionMode is Local Key Management and KeyID is set to any valid value.

Storage.VirtualDisk.RAIDaction (Read or Write)

Description	This pseudo attribute represents RAID action to be performed on the virtual disk. It is used to specify Delete, Create , CreateAuto or Update virtual disk operations. Configurable via XML configuration feature only.
Legal Values	• Create • CreateAuto

	• Delete • Update
Default Value	Update
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.VirtualDisk.Cachecade (Read Only)

Description	This attribute represents the cachecade state of the virtual disk. It can be modified to create a cachecaded virtual disk using XML configuration feature. Configurable via XML configuration feature only.
Legal Values	• Cachecade Virtual Disk • Not a Cachecade Virtual Disk
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDAction is Create

Storage.Controller.RAIDrekey (Read or Write)

Description	This pseudo attribute represents whether a rekey operation needs to be performed on the RAID controller. Configurable via XML configuration feature only.
Legal Values	• True • False
Default Value	False
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.KeyID (Read Only)

Description	This attribute represents the controller key identifier for Local Key Management or Dell Key Management controller encryption modes. Configurable via XML configuration feature only.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if EncryptionMode is Local Key Management and NewControllerKey is set to any valid value.

Storage.Controller.RAIDforeignConfig (Read or Write)

Description	This pseudo attribute represents foreign configuration operation to be performed on the RAID controller via XML configuration feature.Configurable via XML configuration feature only.
Legal Values	• Ignore • Import • Clear
Default Value	Ignore
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.VirtualDisk.RAIDdedicatedSpare (Read or Write)

Description	This pseudo attribute represents the dedicated spare to be assigned to a virtual disk. It could be set to physical disk FQDD to be assigned as a dedicated spare to the virtual disk. If a Spare is intended to be assigned when RAIDaction is set as CreateAuto, this attribute value should be set to AutoSelect. Configurable via XML configuration feature only.
Legal Values	String of ASCII characters.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.VirtualDisk.RAIDinitOperation (Read or Write)

Description	This pseudo attribute represents initialization configuration operation to be performed on the virtual disk via XML configuration feature. Configurable via XML configuration feature only.
Legal Values	• None • Fast
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDaction is Update or Create

Storage.Controller.RAIDremovecontrollerKey (Read or Write)

Description	This pseudo attribute represents whether a rekey operation needs to be performed on the RAID controller.Configurable via XML configuration feature only.
Legal Values	• True • False
Default Value	False
Write Privilege	N/A

License Required	Express License
Dependency	None

Storage.VirtualDisk.RAIDTypes (Read Only)

Description	This indicates the type of RAID level on the virtual disk. Configurable via XML configuration feature only.
Legal Values	• RAID 0 • RAID 1 • RAID 5 • RAID 6 • RAID 10 • RAID 50 • RAID 60
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDAction is Create

Storage.Controller.RAIDresetConfig (Read or Write)

Description	This pseudo attribute represents whether a reset config operation needs to be performed on the RAID controller.Reset Config operation deletes all the virtual disks that exists on the RAID controller. Configurable via XML configuration feature only.
Legal Values	• True • False
Default Value	False
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.VirtualDisk.SpanDepth (Read Only)

Description	This indicates number of spans in the virtual disk.Configurable via XML configuration feature only.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDAction is Create

Storage.VirtualDisk.SpanLength (Read Only)

Description	This indicates the number of physical disks per span on a virtual disk.Configurable via XML configuration feature only.
Legal Values	Integer values.

Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDaction is Create

Storage.VirtualDisk.Size (Read Only)

Description	This indicates the size in bytes of the virtual disk. When creating a virtual disk, size of 0 indicates using full size of the physical disks for the specified RAIDTypes.Configurable via XML configuration feature only.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDaction is Create

Storage.Controller.EnhancedAutoImportForeignConfig (Read or Write)

Description	This indicates the current EnhancedAutoImportForeignConfig setting of the controller. Configurable via XML configuration feature only.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.Controller.ControllerBootMode (Read or Write)

Description	This indicates the current BootMode setting of the Controller. Configurable via XML configuration feature only.
Legal Values	• User Mode • Continue Boot On Error • Headless Mode Continue On Error • Headless Safe Mode
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.VirtualDisk.T10PIStatus (Read or Write)

Description	This indicates virtual disks T10PIStatus.

Legal Values	• Enabled • Disabled
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Controller needs to support.
Notes	This attribute is displayed as read-only when there is only one legal value to set.

Storage.VirtualDisk.StripeSize (Read Only)

Description	This indicates the stripe size of the virtual disk. Configurable via XML configuration feature only.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Applicable only if RAIDAction is Create

Storage.Controller.CurrentControllerMode (Read Only)

Description	This indicates controllers current personality mode , which could be RAID or Non-RAID. PERC9 supports RAID and HBA.Starting PERC 10, modes supported are RAID and Enhanced HBA. PERC 11 and above controllers will only support RAID mode.
Legal Values	• RAID • HBA • Enhanced HBA
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	Controller needs to support.

Storage.Enclosure.RAIDEnclosureRequestedCfgMode (Read or Write)

Description	This indicates enclosures requested configuration mode setting.
Legal Values	• Unified Mode • Split Mode • None
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	Backplane needs to support it.

Notes	• AssetName and AssetTag are applicable only for external enclosures. • If the enclosure is in Failed state, the information about the slots and their occupancy is not displayed. • This value is only valid for C-series platforms.

Storage.Enclosure.RAIDEnclosureCurrentCfgMode (Read Only)

Description	This indicates enclosures current configuration mode setting
Legal Values	• Unified Mode • Split Mode
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	Backplane needs to support it.
Notes	• AssetName and AssetTag are applicable only for external enclosures. • If the enclosure is in Failed state, the information about the slots and their occupancy is not displayed. • This value is only valid for C-series platforms.

Storage.Enclosure.BackplaneType (Read Only)

Description	This indicates enclosures type.
Legal Values	• Shared • Not Shared
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	Backplane needs to support it.
Notes	• AssetName and AssetTag are applicable only for external enclosures. • If the enclosure is in Failed state, the information about the slots and their occupancy is not displayed.

Storage.PhysicalDisk.PCLeSSDSecureErase (Read or Write)

Description	Performs full initialization on the selected physical device. This operation deletes all data on the device.
Legal Values	• True • False
Default Value	False
Write Privilege	N/A
License Required	Express License
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCLeSSD.

Storage.Controller.RAIDPatrolReadUnconfiguredArea (Read or Write)

Description	Patrol Read is Performed on area of physical disk not configured for use.
Legal Values	• Disabled • Enabled
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Enclosure.BlockSizeInBytes (Read Only)

Description	Each Physical and Logical Disk has user data written in blocks. The size of this block in bytes is represented by this attribute.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	• AssetName and AssetTag are applicable only for external enclosures. • If the enclosure is in Failed state, the information about the slots and their occupancy is not displayed.

Storage.PhysicalDisk.MediaType (Read Only)

Description	The drive media could be rotational (Hard Disk Drive) or solid state (SSD). This attribute indicates the drive media type.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.RAIDSupportedInitTypes (Read Only)

Description	No description information available.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.PhysicalDisk.BusProtocol (Read Only)

Description	The communication protocol supported by physical and logical disks. The same attribute is exported for both PDs and LDs.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.RAIDprIterations (Read Only)

Description	No description information available.
Legal Values	Integer values.
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.Controller.SupportedEncryptionTypes (Read Only)

Description	No description information available.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.PhysicalDisk.T10PICapability (Read Only)

Description	No description information available.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.RequestedControllerMode (Read or Write)

Description	This indicates controllers requested personality mode and can be RAID or Non-RAID. PERC 9 supports RAID and HBA. Starting PERC 10, modes supported are RAID and Enhanced HBA. Supported with SET command and not SCP
Legal Values	• RAID • HBA • Enhanced HBA
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	Controller needs to support.

Storage.PhysicalDisk.SoftwareRAIDMode (Read or Write)

Description	No description information available.
Legal Values	• Windows • Linux
Default Value	Windows
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.SupportedDeviceInterfaces (Read or Write)

Description	The drive communication protocols supported by the controller.
Legal Values	• None • SAS SATA • SAS SATA NVMe • NVMe
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.PhysicalDisk.PCIeCapableLinkWidth (Read or Write)

Description	The maximum PCIe Link Width supported by the device

Legal Values	• None • x4
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.PhysicalDisk.PClenegotiatedLinkWidth (Read or Write)

Description	The negotiated PCIe link width of the device
Legal Values	• None • x1 • x2 • x4
Default Value	None
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.PhysicalDisk.NonRAIDDiskCachePolicy (Read or Write)

Description	The disk cache policy for non-raid (PERC 9 system) drives
Legal Values	• Default • Enabled • Disabled
Default Value	Default
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.PhysicalDisk.Certified (Read or Write)

Description	Indicates if the drive is DELL certified or not.
Legal Values	• Unknown • Yes • No
Default Value	Unknown

Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.AutoConfigBehavior (Read or Write)

Description	Indicates the current value of the auto config behavior of the controller.
Legal Values	• Not Applicable • Off • Non-RAID Disk
Default Value	Off
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.HostLEDManagementNonRAIDDisks (Read or Write)

Description	Enables Enclosure devices property of the controller and provides information whether SEP device is exposed to the host OS for Non-RAID disk LED management.
Legal Values	• Not Applicable • Disabled • Enabled •
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.UnmapSupport (Read or Write)

Description	Indicates if the controller supports the Unmap feature to enhance Wear-leveling for SAS drives.
Legal Values	• Not Supported • Supported
Default Value	Supported
Write Privilege	N/A
License Required	Not Applicable
Dependency	None

Storage.Controller.UnmapState (Read or Write)

Description	This attribute applies to Controller and Virtual Disk
Legal Values	• Not Applicable • Disabled • Enabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.PhysicalDisk.UnmapCapability (Read or Write)

Description	This attribute applies to Physical Disk and Virtual Disk
Legal Values	• Not Capable • Capable
Default Value	Not Capable
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.PhysicalDisk.UnmapCapabilityForVDConfig (Read or Write)

Description	Indicates whether PD is capable of supporting Unmap feature for RAID VDs
Legal Values	• Not Capable • Capable
Default Value	Not Capable
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.PhysicalDisk.EncryptionProtocol (Read or Write)

Description	The security protocol supported by the drive
Legal Values	• None • TCG Enterprise SSC • TCG Enterprise Opal
Default Value	None
Write Privilege	N/A

License Required	Not Applicable
Dependency	None
Notes	These attributes are applicable only for SAS/SATA drives and not for PCIeSSD.

Storage.Controller.PersistHotspare (Read or Write)

Description	Enable or Disable the persistent hot spare of the controller
Legal Values	• Disabled • Enabled
Default Value	Disabled
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.RaidMode (Read or Write)

Description	This property will indicate the meta data mode controller in, applicable only for SW RAID controller
Legal Values	• None • Linux • Windows • Mixed
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.PossibleloadBalancedMode (Read Only)

Description	This attribute represents the ability to automatically use both controller ports connected to the same enclosure to route I/O requests.
Legal Values	• Auto • Disabled
Default Value	Auto
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.SupportControllerBootMode (Read Only)

Description	This property will indicate if this controller supports setting of controller boot mode.
Legal Values	• Not Supported • Supported
Default Value	None

Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.SupportEnhancedAutoForeignImport (Read Only)

Description	This property will indicate if this controller supports enhanced auto import of foreign config.
Legal Values	• Not Supported • Supported
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.SupportRAID10UnevenSpans (Read Only)

Description	This property will indicate if this controller supports uneven spans for RAID 10.
Legal Values	• Not Supported • Supported
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Controller.T10PICapability (Read Only)

Description	This property will indicate if this controller supports T10 PI.
Legal Values	• Not Capable • Capable
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Enclosure.AssetName (Read or Write)

Description	Displays the Asset Name information for the enclosure. Applicable only for external enclosure.
Legal Values	String of up to 32 ASCII characters.
Default Value	None

Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Enclosure.BackplaneCurrentMode (Read Only)

Description	Displays the current mode of the backplane.SupportedSplitModes object will provide split modes supported on current platform.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Enclosure.BackplaneRequestedMode (Read or Write)

Description	Sets the backplane mode.SupportedSplitModes object will provide split modes supported on current platform.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.Enclosure.SupportedSplitModes (Read Only)

Description	List of supported splitmodes on this backplane.
Legal Values	•
Default Value	None
Write Privilege	N/A
License Required	Express License
Dependency	None

Storage.PhysicalDisk.BlockSizeInBytes (Read Only)

Description	This property will indicate the logical block size of the physical drive that this VD belongs to.
Legal Values	• 512 or 4096
Default Value	None
Write Privilege	N/A
License Required	Express License

Dependency None

Storage.PhysicalDisk.RaidType (Read Only)

Description This property will indicate the meta data type resides on the disk

Legal Values

- Unknown
- MD SoftWare RAID
- Windows Software RAID

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

Storage.PhysicalDisk.SystemEraseCapability (Read Only)

Description This property will indicate the erase capability of the disk

Legal Values

- CryptographicErasePD
- OverwritePD
- Not Supported

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

Storage.VirtualDisk.BlockSizeInBytes (Read Only)

Description This property will indicate the logical block size of the physical drive that this VD belongs to.

Legal Values

- 512
- 4096

Default Value None

Write Privilege N/A

License Required Express License

Dependency None

Storage.Controller.PatrolReadUnconfiguredArea (Read or Write)

Description Enable or Disable the patrol read in unconfigured areas

Legal Values

- Disabled
- Enabled

Default Value None

Write Privilege N/A

License Required Express License
Dependency None

SYSTEM Attributes

System.AcquisitionInfo.CostCenter (Read or Write)

Display Name	Cost Center
Description	Identifying information for the accounting unit within the purchasing company that authorized the purchase.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.Expensed (Read or Write)

Display Name	Expensed
Description	Determines whether the cost of the system was subtracted from the budget of a particular person or department in the purchasing company.
Legal Values	• Yes - 0 • No - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.InstallDate (Read or Write)

Display Name	Installation Date
Description	Date the system was put into service by the purchasing company.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.PONumber (Read or Write)

Display Name	Purchase Order Number
Description	Number of the purchase order that authorized buying the system.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.PurchaseCost (Read or Write)

Display Name	Purchase Cost
Description	Value expressed in currency unit that was paid for the system, for example, 25000.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.PurchaseDate (Read or Write)

Display Name	Purchase Date
Description	Date the transaction for acquiring the system was completed.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.Vendor (Read Only)

Display Name	Vendor
Description	Company who sold the system to the purchaser.
Legal Values	String of up to 64 ASCII characters.
Default Value	Dell

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.WayBill (Read or Write)

Display Name	Reference to Delivery Slip Number
Description	Identifying information for the waybill or delivery slip, such as a waybill number.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.AcquisitionInfo.WhoSigned (Read or Write)

Display Name	Who Signed
Description	Person who accepted delivery of the system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.Backplane.BackplaneBusMode (Read Only)

Display Name	Backplane Bus Mode
Description	Enclosure serial interface type, either SGPIO or I2C
Legal Values	• Unknown - 0 • I2C - 1 • SGPIO - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.Backplane.BackplaneSplitMode (Read or Write)

Display Name	Backplane Split Mode
Description	Enclosure split mode setting
Legal Values	Integer values from 0 to 255.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ChassisInfo.CMStatus (Read Only)

Display Name	ChassisManagerStatus
Description	Chassis Manager status
Legal Values	• CM OFFLINE - 0 • CM ONLINE - 1
Default Value	0
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.CustomAsset.Label (Read or Write)

Display Name	Custom Asset Label
Description	Custom Asset label.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.CustomAsset.Value (Read or Write)

Display Name	Custom Asset Value
Description	Custom Asset value
Legal Values	String of up to 255 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.DepreciationInfo.Duration (Read or Write)

Display Name	Duration
Description	Displays the duration for which the depreciation value is being calculated.
Legal Values	String of up to 64 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.DepreciationInfo.DurationUnit (Read or Write)

Display Name	Duration Unit
Description	Indicates the duration in months or years.
Legal Values	• Months - 0 • Years - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.DepreciationInfo.Method (Read or Write)

Display Name	Method
Description	Displays the steps and assumptions used to compute the systems depreciation.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.DepreciationInfo.Percentage (Read or Write)

Display Name	Percentage
Description	Indicates the portion of 100 that an asset is devalued or depreciated. If the duration of depreciation is 5 years, and the method is straight line, then the percentage is 20 percent.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.Diagnostics.OSAppCollectionTime (Read Only)

Display Name	OS App Collection Time
Description	Displays the last OS and Application Data collection time in GMT/UTC
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ExtWarrantyInfo.Cost (Read or Write)

Display Name	Cost
Description	Displays the total cost of the warranty service on a system.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ExtWarrantyInfo.EndDate (Read or Write)

Display Name	End Date
Description	Displays the date that extended warranty service ends.
Legal Values	String of up to 32 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ExtWarrantyInfo.Provider (Read or Write)

Display Name	Provider
Description	Displays the name of the business that is providing warranty service to the system owner.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ExtWarrantyInfo.StartDate (Read or Write)

Display Name	Start Date
Description	Displays the date that extended warranty service begins. This date usually follows the standard warranty service.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.IdleServerDetection.IdleServerScanInterval (Read or Write)

Display Name	Idle Server Scan Interval
Description	Scan interval time in hours for which server utilization to be monitored.
Legal Values	Integer values from 1 to 9000.
Default Value	240
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None

Is Platform Dependent	No
Notes	These attributes are only available for supported CUPS capable Intel processors.

System.IdleServerDetection.IdleServerStatus (Read Only)

Display Name	Idle Server Status
Description	Idle server status: Idle or Utilized
Legal Values	- Utilized - 0 - Idle - 1
Default Value	0
Write Privilege	N/A
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No
Notes	These attributes are only available for supported CUPS capable Intel processors.

System.IdleServerDetection.IdleServerThreshold (Read or Write)

Display Name	Idle Server Threshold
Description	Idle server detection threshold in %
Legal Values	Integer values from 0 to 50.
Default Value	20
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	None
Is Platform Dependent	No
Notes	These attributes are only available for supported CUPS capable Intel processors.

System.IdleServerDetection.ServerUtilizationPercentile (Read or Write)

Display Name	Server Utilization Percentile
Description	Server utilization percentile indicates how many % of samples are above utilization threshold
Legal Values	Integer values from 80 to 100.
Default Value	80
Write Privilege	Configure iDRAC
License Required	Datacenter License

Dependency	None
Is Platform Dependent	No
Notes	These attributes are only available for supported CUPS capable Intel processors.

System.LCD.ChassisIdentifyDuration (Read or Write)

Display Name	Chassis Identify Duration
Description	Enable/Disable chassis Identify. A value of -1 = force on indefinitely; 0 = Off; > 0 number of seconds chassis identify is on
Legal Values	Integer values from -1 to 2592000.
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	- The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. - You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.Configuration (Read or Write)

Display Name	LCD Configuration
Description	Current LCD configuration. If this is set to User Defined, the User defined string will be displayed on the LCD.
Legal Values	- User Defined - 0 - Model Name - 1 - None - 2 - iDRAC IPv4 Address - 4 - iDRAC MAC Address - 8 - OS System Name - 16 - Service Tag - 32 - IPv6 Address - 64 - Ambient Temperature - 128 - Airflow - 129 - System Watts - 256 - Asset Tag - 512 - Post - 1024 - ADStat - 2048 - ADTime - 2049 - ADComp - 2050 - ADErr - 2051
Default Value	32
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	When hostsetting is not zero only zero maybe written to LCD configuration

Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.CurrentDisplay (Read Only)

Display Name	Current LCD Display String
Description	The string currently displayed on the LCD
Legal Values	String of up to 256 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.ErrorDisplayMode (Read or Write)

Display Name	Error Display Mode
Description	LCD error message format selection SEL or simple where simple format include the message ID.
Legal Values	• SEL - 1 • simple - 2
Default Value	1
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.FrontPanelLocking (Read or Write)

Display Name	Front Panel Locking
Description	Sets LCD button interface to Full-Access;View-Only; or No access (Locked)
Legal Values	• Full-Access - 0

	• View-Only - 1 • Locked - 2
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.HideErrs (Read or Write)

Display Name	Hide Errors
Description	Hide or unhide errors displayed on LCD screen.
Legal Values	• hide - 0 • unhide - 1
Default Value	1
Write Privilege	N/A
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.LicenseMsgEnable (Read or Write)

Display Name	Enable License Message
Description	Enable/disable display of no license available for certain licensable features.
Legal Values	• No-License-Msg - 0 • Display-Licens-Msg - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.NMIResetOverride (Read or Write)

Display Name	NMI Reset Override
Description	Enable/disables iDRAC reset capability via the Chassis ID button
Legal Values	• Disabled - 0 • IDButtonResets - 1 • IDButtonDoesNotReset - 2
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.NumberErrsHidden (Read Only)

Display Name	Number of errors hidden
Description	The number of hidden LCD active errors
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.NumberErrsVisible (Read Only)

Display Name	Number of errors visible
Description	The number of visible LCD active errors
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.QualifierTemp (Read or Write)

Display Name	Ambient Temperature Qualifier
Description	Specifies Ambient Temperature Qualifier
Legal Values	• C - 0 • F - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.QualifierWatt (Read or Write)

Display Name	System Watt Qualifier
Description	Specifies System Watt Qualifier
Legal Values	• Watts - 0 • BTU/hr - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.UserDefinedString (Read or Write)

Display Name	User Defined String for LCD
Description	User defined custom string for display on LCD
Legal Values	String of up to 62 ASCII characters.
Default Value	None

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	System.LCD.Configuration has to be set to User Defined mode
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LCD.vConsoleIndication (Read or Write)

Display Name	vConsole Indication
Description	Virtual Console Indication
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• The System.LCD get and set commands work on iDRAC on Blade Server, even if the LCD is not present on the server. • You can change the LCD group attributes for monolithic servers even if the LCD is not present on servers.

System.LeaseInfo.Buyout (Read or Write)

Display Name	Buyout Amount
Description	Indicates the amount of money you would have to pay to own a system you are leasing.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.LeaseInfo.EndDate (Read or Write)

Display Name	End Date
Description	Displays the agreed upon day, month, and year that the lease is no longer in force.
Legal Values	String of up to 32 ASCII characters.

Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.LeaseInfo.FairValue (Read or Write)

Display Name	Fair Market Value
Description	Refers to an arrangement that allows a customer to purchase systems at the end of the lease for its then current fair market value.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.LeaseInfo.Lessor (Read or Write)

Display Name	Lessor
Description	Displays the name of the business entity that is leasing the system to the user.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.LeaseInfo.MultiSched (Read or Write)

Display Name	Multiple Schedules
Description	Indicates whether the cost of leasing the system is computed by more than one rate schedule.
Legal Values	• Yes - 0 • No - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

System.LeaseInfo.RateFactor (Read or Write)

Display Name	Rate Factor
Description	Displays the factor used to calculate the lease payment.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.MaintenanceInfo.EndDate (Read or Write)

Display Name	End Date
Description	The date that maintenance ends.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.MaintenanceInfo.Provider (Read or Write)

Display Name	Provider
Description	The business entity that provides maintenance on a system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.MaintenanceInfo.Restrictions (Read or Write)

Display Name	Restrictions

Description	Any exclusions that apply to the maintenance agreement for the system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.MaintenanceInfo.StartDate (Read or Write)

Display Name	Start Date
Description	The date that maintenance begins.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OpenIDConnectServer.DiscoveryURL (Read or Write)

Display Name	Server Discovery URL
Description	Discovery URL
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.OpenIDConnectServer.Enabled (Read or Write)

Display Name	Server is enabled
Description	Server state
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC, Configure Users

License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.OpenIDConnectServer.Name (Read or Write)

Display Name	Server Name
Description	Server name
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.OpenIDConnectServer.RegistrationDetails (Read or Write)

Display Name	Credentials needed to register on server
Description	Registration details
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.OpenIDConnectServer.RegistrationStatus (Read Only)

Display Name	Status of registration on server
Description	Registration status
Legal Values	String of up to 1024 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC, Configure Users
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.OutsourceInfo.ProbComp (Read or Write)

Display Name	Problem Component
Description	Component of the system that requires corrective action such as repair or replacement.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OutsourceInfo.ProviderFee (Read or Write)

Display Name	Provider Fee
Description	Defines any additional fee invoiced by the outsource service provider.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OutsourceInfo.SLALevel (Read or Write)

Display Name	SLA Level
Description	Service Level Agreement (SLA) between the service provider and the system owner spells out when service is available (for example, how many hours and days per week) and what components are excluded. Levels of service to which the system owner is entitled.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OutsourceInfo.ServiceFee (Read or Write)

Display Name	Service Fee
Description	Amount of money paid for either the service contract or for corrective action on a specific problem component.

Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OutsourceInfo.SignedFor (Read or Write)

Display Name	Signed For
Description	Person who authorized the repair of the component.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OwnerInfo.InsComp (Read or Write)

Display Name	Insurance Company
Description	The company that insures the system against theft or other loss.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.OwnerInfo.OwnerName (Read or Write)

Display Name	Owner Name
Description	The individual or business entity that holds legal title to the system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

System.OwnerInfo.Type (Read or Write)

Display Name	Type
Description	Whether the system is owned or leased.
Legal Values	• Owned - 0 • Leased - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.PCIESlotLFM.3rdPartyCard (Read Only)

Display Name	3rd Party Card
Description	3rd Party PCIe Card may benefit from additional settings
Legal Values	• No - 0 • Yes - 1 • N/A - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.PCIESlotLFM.CardType (Read Only)

Display Name	Card Type
Description	Type of PCIe card installed
Legal Values	String of up to 512 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.PCIESlotLFM.CustomLFM (Read or Write)

Display Name	Custom LFM
Description	Minimum airflow to be delivered the installed PCIe card
Legal Values	Integer values from 0 to 5000.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	CustomLFM is read/write when LFMMode is set to custom
Is Platform Dependent	No

System.PCIESlotLFM.LFMMode (Read or Write)

Display Name	LFM Mode
Description	Cooling Response Mode
Legal Values	• Automatic - 0 • Disabled - 1 • Custom - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	LFMMode is read/write when 3rdPartyCard is set to Yes
Is Platform Dependent	No

System.PCIESlotLFM.MaxLFM (Read Only)

Display Name	Maximum LFM
Description	Estimated airflow delivered to the slot at full fan speed
Legal Values	Integer values from 0 to 65536.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.PCIESlotLFM.PCIEInletTemperature (Read Only)

Display Name	PCIe Inlet Temperature
Description	Indicates the current PCIe Inlet Temperature for the PCIe Slot.

Legal Values	Integer values from 0 to 127.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.PCIESlotLFM.SlotState (Read Only)

Display Name	Slot State
Description	PCIe slot physically exists
Legal Values	• Not-Defined - 0 • Defined - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.PCIESlotLFM.TargetLFM (Read Only)

Display Name	Target LFM
Description	Minimum airflow provisioned for the installed PCIe card
Legal Values	String of up to 512 ASCII characters.
Default Value	-
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.QuickSync.Access (Read or Write)

Display Name	Quick Sync Access
Description	Sets QuickSync access permission
Legal Values	• Disabled - 0 • Read-only - 1 • Read-write - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	System.QuickSync.Presence has to be Absent or Present
Is Platform Dependent	Yes

System.QuickSync.InactivityTimeout (Read or Write)

Display Name	Quick Sync Inactivity Timeout
Description	Quick Sync Inactivity Timeout value specified in seconds with max value of 3600 seconds
Legal Values	Integer values from 120 to 3600.
Default Value	120
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	Cannot be set unless InactivityTimerEnable is Enabled
Is Platform Dependent	Yes

System.QuickSync.InactivityTimerEnable (Read or Write)

Display Name	Quick Sync Inactivity Timer Enable
Description	Enables or disables the QuickSync inactivity timer
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	System.QuickSync.Presence has to be Absent or Present
Is Platform Dependent	Yes

System.QuickSync.Presence (Read Only)

Display Name	Quick Sync Presence
Description	Indicates the presence or absence of the QuickSync hardware
Legal Values	• Not Supported - 0 • Absent - 1 • Present - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	System.QuickSync.Presence has to be Absent or Present
Is Platform Dependent	Yes

System.QuickSync.ReadAuthentication (Read or Write)

Display Name	Quick Sync Read Authentication
Description	Enables or disables QuickSync read authentication to the server
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	System.QuickSync.Presence has to be Absent or Present
Is Platform Dependent	Yes

System.QuickSync.WifiEnable (Read or Write)

Display Name	Quick Sync WiFi Enable
Description	Enables or disables QuickSync WiFi access
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	System.QuickSync.Presence has to be Absent or Present
Is Platform Dependent	Yes

System.SC-BMC.PowerMonitoring (Read or Write)

Display Name	Power Monitoring
Description	Power monitoring
Legal Values	Integer values from 0 to 1.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	The System.Chassis group is deprecated and replaced with System.SC-BMC group.

System.ServerInfo.NodeID (Read Only)

Display Name	System Node ID

Description	Specifies the system node ID.
Legal Values	String of up to 124 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerInfo.RChassisServiceTag (Read Only)

Display Name	System Chassis-related Service Tag
Description	Provides the system chassis-related service tag.
Legal Values	String of up to 10 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerInfo.ServerType (Read Only)

Display Name	Server Type
Description	The type of physical form factor of the Server
Legal Values	• Rack - 0 • Blade - 1 • Tower - 2 • Sled - 3
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.ServerInfo.ServiceTag (Read Only)

Display Name	Service Tag
Description	Specifies the system service tag.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC

License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerOS.HostName (Read or Write)

Display Name	Server Host Name
Description	Server Host Name
Legal Values	String of up to 253 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerOS.InstallCompletedTime (Read Only)

Display Name	OS Installation Completed Time
Description	Indicates the time when the Host OS installation Completed (seconds).
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerOS.OEMOSVersion (Read Only)

Display Name	OEM OS Version
Description	Server OEM OS Version
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerOS.OSName (Read or Write)

Display Name	OS Name
Description	Server Operating System
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerOS.OSVersion (Read Only)

Display Name	OS Version
Description	Server OS Version
Legal Values	String of up to 254 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerOS.ProductKey (Read Only)

Display Name	Windows Product Key
Description	Windows OS Product Key associated with the server
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerOS.ServerPoweredOnTime (Read Only)

Display Name	Server Powered On Time Duration
Description	Indicates the time since the Host OS has been powered on (seconds).
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	system.serveros.productkey value is shown only if OA3.x is available, which may be available with future generations of MSFT and newer version of Windows Server OS.

System.ServerPwr.ActivePolicyName (Read Only)

Display Name	Active Power Cap Policy Name
Description	The active power cap policy name
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.ActivePowerCapVal (Read Only)

Display Name	Active Power Cap Value
Description	Set the Active Power Cap value
Legal Values	Integer values from 0 to 32767.
Default Value	32767
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None

Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PSPFCEnabled (Read or Write)

Display Name	Power Supply PFC Enable
Description	Enable the Power Supply Power Factor Correction
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PSRapidOn (Read or Write)

Display Name	Power Supply Rapid On Enable
Description	Enable the Power Supply Rapid On. Rapid On is exactly same as Hotspare as listed in idrac GUI.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PSRedPolicy (Read or Write)

Display Name	Power Supply Redundancy Policy
Description	Specify the Power Supply redundancy policy
Legal Values	• Not Redundant - 0 • A/B Grid Redundant - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License

Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PowerCapMaxThres (Read Only)

Display Name	Power Cap Max Threshold
Description	Maximum threshold for Power Cap
Legal Values	Integer values from 0 to 32767.
Default Value	32767
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PowerCapMinThres (Read Only)

Display Name	Power Cap Min Threshold
Description	Minimum threshold for Power Cap
Legal Values	Integer values from 0 to 32767.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PowerCapSetting (Read or Write)

Display Name	Power Cap Setting
Description	Enables or Disables setting the power cap value
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Enterprise License

Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.PowerCapValue (Read or Write)

Display Name	Power Cap Value
Description	Indicates maximum power consumption limit in Watts
Legal Values	Integer values from 0 to 32767.
Default Value	32767
Write Privilege	Configure iDRAC
License Required	Enterprise License
Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.Poweredbyparent (Read or Write)

Display Name	Powered By Parent
Description	Gives info on whether it is Self Powered or Powered By Chassis
Legal Values	- SelfPowered - 0 - PoweredByChassis - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwr.RapidOnPrimaryPSU (Read or Write)

Display Name	Rapid On Primary PSU
Description	The Rapid On Primary PSU
Legal Values	- PSU1 - 1 - PSU2 - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Express License

Dependency	None
Is Platform Dependent	Yes
Notes	For Dell PowerEdge FM120x4 server with more than one iDRAC, the power is received and shared from CMC. Hence, the information about power and temperature for individual iDRACs are not displayed.

System.ServerPwrMon.AccumulativePower (Read Only)

Display Name	Accumulative Power
Description	Total power in energy consumed by server from start time.
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.CumulativePowerStartTime (Read Only)

Display Name	Cumulative Power Start Time
Description	Start of time period from which cumulative power is calculated.
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.CumulativePowerStartTimeStr (Read Only)

Display Name	Cumulative Power Start Time
Description	The start time when cumulative power is recorded.
Legal Values	String of up to 128 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No

System.ServerPwrMon.MinPowerTime (Read Only)

Display Name	Minimum Power Time
Description	The time when minimum power is recorded.
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.MinPowerTimeStr (Read Only)

Display Name	Minimum Power Time
Description	The time when minimum power is recorded.
Legal Values	String of up to 128 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.MinPowerWatts (Read Only)

Display Name	Minimum Power Watts
Description	Minimum Power Historical
Legal Values	Integer values from 0 to 65553.
Default Value	65553
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakCurrentTime (Read Only)

Display Name	Peak Current Time

Description	Time at which the server observed the maximum current from start time.
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakCurrentTimeStr (Read Only)

Display Name	Peak Current Time
Description	The time when peak current is recorded.
Legal Values	String of up to 128 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakPowerStartTime (Read Only)

Display Name	Peak Power Start Time
Description	Start of time period for which peak power is recorded.
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakPowerStartTimeStr (Read Only)

Display Name	Peak Power Start Time
Description	The start time when peak power is recorded.
Legal Values	String of up to 128 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakPowerTime (Read Only)

Display Name	Peak Power Time
Description	Time at which the server consumed the maximum power from start time.
Legal Values	Integer values from 0 to 2147483647.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakPowerTimeStr (Read Only)

Display Name	Peak Power Time
Description	The time when peak power is recorded.
Legal Values	String of up to 128 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PeakPowerWatts (Read Only)

Display Name	Peak Power Watts
Description	Maximum power consumed by server from the start time.
Legal Values	Integer values from 0 to 32767.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServerPwrMon.PowerConfigReset (Read or Write)

Display Name	Power Config Data Reset
Description	Resets the power statistics starting time. (Write only).
Legal Values	• None - 0 • ClrCumulaPowerAndTime - 1 • ClrPeakValueAndTime - 2 • ClrAll - 3 • ClrPeakAndCumulaValue - 4
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes

System.ServerTopology.AisleName (Read or Write)

Display Name	Aisle Name
Description	The aisle the system is located in.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.DataCenterName (Read or Write)

Display Name	Data Center Name
Description	The data center the system is located in.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.ManagedSystemSizeInU (Read Only)

Display Name	Size of Managed System in U
Description	Measure of thickness of the system in U
Legal Values	• 1 - 1 • 2 - 2 • 3 - 3 • 4 - 4 • 5 - 5 • 6 - 6 • 7 - 7 • 8 - 8 • 9 - 9 • 10 - 10 • 1.5 - 11 • 2.5 - 12 • 3.5 - 13 • 4.5 - 14 • 5.5 - 15 • 6.5 - 16 • 7.5 - 17 • 8.5 - 18 • 9.5 - 19
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.RackName (Read or Write)

Display Name	Rack Name
Description	Name of the rack on which the system is located.
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.RackOffsetUnits (Read or Write)

Display Name	Rack Offset Units
Description	Indicates the type of Rack Units in use.
Legal Values	• OpenU - 0 • EIA_310 - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.RackSlot (Read or Write)

Display Name	Rack Slot
Description	Slot in the rack where the system is located.
Legal Values	Integer values from 0 to 255.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.RoomName (Read or Write)

Display Name	Room Name
Description	Room Name
Legal Values	String of up to 128 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServerTopology.SizeOfManagedSystemInU (Read Only)

Display Name	Size of Managed System in U
Description	Measure of thickness of the system in U
Legal Values	Integer values from 1 to 255.
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	The System.Location group is deprecated and replaced with System.ServerTopology group.

System.ServiceContract.Renewed (Read or Write)

Display Name	Renewed
Description	Whether the service contract was renewed or not (Yes or No).
Legal Values	• Yes - 0 • No - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServiceContract.Type (Read or Write)

Display Name	Type
Description	Type refers to the name or feature of the system covered by the service contract. For example, Installation Service, Maintenance Service, Return Service, Gold Service, Premier Service.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ServiceContract.Vendor (Read or Write)

Display Name	Vendor
Description	The business entity contracting to service the system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.Storage.AvailableSpareAlertThreshold (Read or Write)

Display Name	AvailableSpareAlertThreshold
Description	Displays the system level user configured threshold value for available spare value of the SSD devices connected to system.
Legal Values	Integer values from 1 to 99.
Default Value	10
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.Storage.RemainingRatedWriteEnduranceAlertThreshold (Read or Write)

Display Name	RemainingRatedWriteEnduranceAlertThreshold
Description	Displays the system level user configured threshold value for write endurance value of the SSD devices connected to system.
Legal Values	Integer values from 1 to 99.
Default Value	10
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SupportInfo.AutoFix (Read or Write)

Display Name	Automatic Fix
Description	Method used to fix the problem
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SupportInfo.HelpDesk (Read or Write)

Display Name	Help Desk
Description	Name of the help desk that provides technical support for your system; information provided by the help desk.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SupportInfo.Outsourced (Read or Write)

Display Name	Outsourced
Description	Indicates whether you have contracted with an outside business entity to provide technical support for your system.
Legal Values	• Yes - 0 • No - 1
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SupportInfo.Type (Read or Write)

Display Name	Type

Description	Indicates whether a support request is for a problem with your systems network connectivity or with a particular system component.
Legal Values	• Network - 0 • Storage - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SystemInfo.BootTime (Read Only)

Display Name	System Boot Time
Description	Time of the last system boot.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SystemInfo.PrimaryTelephone (Read or Write)

Display Name	Primary Telephone
Description	Telephone number for the person responsible for managing the system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SystemInfo.PrimaryUser (Read or Write)

Display Name	Primary User
Description	Text that provides the name for the person responsible for managing the system.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable

Dependency	None
Is Platform Dependent	No

System.SystemInfo.SysLocation (Read or Write)

Display Name	System Location
Description	Alphanumeric text that specifies where the system is, such as building and room.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.SystemInfo.SysTime (Read Only)

Display Name	System Time
Description	Current time configured on the system clock.
Legal Values	String of up to 64 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalConfig.ASHRAEEnvironmentalClass (Read Only)

Display Name	ASHRAE Environmental Class
Description	Defines the supported ASHRAE Environmental Class for the system.
Legal Values	• N/A - 0 • A2 - 1 • A3 - 2 • A4 - 3
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalConfig.CriticalEventGenerationInterval (Read or Write)

Display Name	Critical Event Generation Interval
Description	Indicates time interval in days for critical events to be generated
Legal Values	Integer values from 0 to 365.
Default Value	30
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalConfig.EventGenerationInterval (Read or Write)

Display Name	Event Generation Interval
Description	Indicates time interval in days for warning events to be generated
Legal Values	Integer values from 0 to 365.
Default Value	30
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalConfig.FreshAirCompliantConfiguration (Read Only)

Display Name	Fresh Air Compliant Configuration
Description	Indicates if the system is a Fresh Air compliant configuration
Legal Values	• Not Applicable - 0 • Yes - 1 • No - 2
Default Value	1
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalConfig.LiquidCoolSetting (Read Only)

Display Name	Liquid Cool Setting
Description	Specifies the Liquid Cooling Setting.
Legal Values	• Disabled - 0 • Enabled - 1 • Unknown - 255
Default Value	255
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalConfig.MaxCFM (Read Only)

Display Name	Maximum CFM
Description	Indicates potential system airflow consumption at 100% fan speed - in cubic feet per minute (CFM)
Legal Values	Integer values from 0 to 1000.
Default Value	0
Write Privilege	N/A
License Required	Not Applicable
Dependency	Not shown if system.embedded.1#thermalsettings.1#systemCFMsupport is not supported.
Is Platform Dependent	No

System.ThermalConfig.ValidFanConfiguration (Read Only)

Display Name	Valid Fan Configuration
Description	Valid Fan Configuration
Legal Values	• No - 0 • Yes - 1 • NotApplicable - 2
Default Value	2
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalHistorical.IntervalInSeconds (Read or Write)

Display Name	Interval In Seconds

Description	Specifies the time resolution
Legal Values	Integer values from 0 to 0.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.ThermalSettings.AirExhaustTemp (Read or Write)

Display Name	Average Air Exhaust Temperature
Description	Specifies the Average Air Exhaust Temperature
Legal Values	• 40 - 0 • 45 - 1 • 50 - 2 • 55 - 3 • 60 - 4 • 65 - 5 • 70 - 255
Default Value	255
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	Feature must be supported to set the value.
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.AirExhaustTempSupport (Read Only)

Display Name	Air Exhaust Temp Support
Description	Specifies if the Average Air Exhaust Temperature is supported
Legal Values	• Not Supported - 0 • Supported - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.AirTemperatureRiseLimit (Read or Write)

Display Name	Air Temperature Rise Limit
Description	Defines the Air Temperature Rise Limit
Legal Values	• 15 - 0 • 20 - 1 • 25 - 2 • 30 - 3 • 35 - 4 • 40 - 5 • 45 - 6 • NO LIMIT - 255
Default Value	255
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	Feature must be supported to set the value.
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.AirTemperatureRiseLimitSupport (Read Only)

Display Name	Air Temperature Rise Limit Support
Description	Defines if the Air Temperature Rise Limit configuration is supported
Legal Values	• Not Supported - 0 • Supported - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.CurrentSystemProfileValue (Read Only)

Display Name	Current System Profile Value
Description	Displays current system profile value

Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.DriveTemperaturePolling (Read or Write)

Display Name	Drive Temperature Polling
Description	Specifies if drive temperature polling is enabled, disabled, or set to default for drives attached to an HBA.
Legal Values	• Default - 0 • Enabled - 1 • Disabled - 2
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.FanSpeedHighOffsetVal (Read Only)

Display Name	Fan Speed High Offset Value
Description	Specifies the Fan Speed High Offset Value
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.FanSpeedLowOffsetVal (Read Only)

Display Name	Fan Speed Low Offset Value
Description	Specifies the Fan Speed Low Offset Value
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.FanSpeedMaxOffsetVal (Read Only)

Display Name	Fan Speed Max Offset Value
Description	Specifies the Fan Speed Max Offset Value
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.FanSpeedMediumOffsetVal (Read Only)

Display Name	Fan Speed Medium Offset Value
Description	Specifies the Fan Speed Medium Offset Value
Legal Values	Integer values from 0 to 65535.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.FanSpeedOffset (Read or Write)

Display Name	Fan Speed Offset
Description	Specifies the Fan Speed Offset
Legal Values	• Low - 0 • High - 1 • Medium - 2 • Max - 3 • Off - 255
Default Value	255
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.MFSMaximumLimit (Read Only)

Display Name	MFS Maximum Limit
Description	Specifies the MFS Maximum Limit
Legal Values	Integer values from 0 to 100.
Default Value	100
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.MFSMinimumLimit (Read Only)

Display Name	MFS Minimum Limit
Description	Specifies the MFS Minimum Limit
Legal Values	Integer values from 0 to 100.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.MaximumPCleInletTemperatureLimit (Read or Write)

Display Name	Maximum PCIe Inlet Temperature Limit
Description	Defines the Maximum PCIe Inlet Temperature Limit.
Legal Values	• 55 - 0 • 45 - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	Feature must be supported to set the value.
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.MaximumPCleInletTemperatureLimitSupport (Read Only)

Display Name	Maximum PCIe Inlet Temperature Limit Support
Description	Defines if the Maximum PCIe Inlet Temperature Limit configuration is supported.
Legal Values	• Not Supported - 0 • Supported - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.MinimumFanSpeed (Read or Write)

Display Name	Minimum Fan Speed
Description	Minimum Fan Speed

Legal Values	Integer values from 0 to 255.
Default Value	255
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.PCLeSlotLFMSupport (Read Only)

Display Name	PCIe Slot LFM Support
Description	Specifies if the PCIe LFM feature is supported
Legal Values	• Not Supported - 0 • Supported - 1
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SetAirTemperatureRiseLimit (Read or Write)

Display Name	Set Air Temperature Rise Limit
Description	Defines if the Air Temperature Rise Limit configuration is enabled/disabled.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Datacenter License
Dependency	Feature must be supported to set the value.
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SetMaximumExhaustTemperature Limit (Read or Write)

Display Name	Set Maximum Exhaust Temperature Limit
Description	Defines if the Exhaust Temperature Limit configuration is disabled or enabled.
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Express License
Dependency	Feature must be supported to set the value.
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SoundCapState (Read Only)

Display Name	SoundCap State
Description	Specifies whether the Sound Cap 2.0 max fan speed bound is enabled or disabled
Legal Values	• Disabled - 0 • Enabled - 1 • Not Applicable - 2
Default Value	2
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SystemCFMSupport (Read Only)

Display Name	System CFM Support
Description	Specifies if the System CFM is supported
Legal Values	• Not Supported - 0 • Supported - 1 • Not Licensed - 2
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	None

Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SystemExhaustTemperature (Read Only)

Display Name	System Exhaust Temperature
Description	Indicates the current system exhaust temperature.
Legal Values	Integer values from 0 to 127.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SystemInletTemperature (Read Only)

Display Name	System Inlet Temperature
Description	Indicates the current system inlet (ambient) temperature.
Legal Values	Integer values from 0 to 127.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.SystemInletTemperatureSupportLimitPerConfiguration (Read Only)

Display Name	System Inlet Temperature Support Limit Per Configuration
Description	Indicates the system inlet temperature limit supported for system configuration.
Legal Values	Integer values from 0 to 127.
Default Value	0

Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.TargetExhaustTemperatureLimit (Read Only)

Display Name	Target Exhaust Temperature Limit
Description	Indicates the current effective target exhaust temperature limit.
Legal Values	Integer values from 0 to 127.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.ThermalSettings.ThermalProfile (Read or Write)

Display Name	Thermal Profile Optimization
Description	Specifies the Thermal Profile
Legal Values	• Default Thermal Profile Settings - 0 • Maximum Performance - 1 • Minimum Power - 2 • Sound Cap - 3
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	Yes
Notes	• You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license. • Restart the system to activate the power and thermal settings.

System.ThermalSettings.ThirdPartyPCIFanResponse (Read or Write)

Display Name	Fan Response
Description	Third Party PCI fan response
Legal Values	• Disabled - 0 • Enabled - 1
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No
Notes	You may encounter an error when running an operation with attributes requiring iDRAC Datacenter license, on a system without this required license.

System.USBFront.Enable (Read or Write)

Display Name	Enable
Description	Enables or disables the host front USB port. This setting can be overwritten by BIOS Menu setting.
Legal Values	• Enabled - 2 • Disabled - 1 • Not Applicable - 0
Default Value	0
Write Privilege	Server Control and Configuration
License Required	Not Applicable
Dependency	System.USBFront.Enable can only be set to Enable/Disable if iDRAC.PlatformCapability.FrontPortUSBConfiguration is Enabled. System. USBFront.Enable can only be set to NotApplicable if iDRAC.PlatformCapability.FrontPortUSBConfiguration is Disabled.
Is Platform Dependent	No
Notes	This setting can be overwritten by BIOS Menu setting.

System.WarrantyInfo.Cost (Read or Write)

Display Name	Cost
Description	The total cost of the warranty service on a system.
Legal Values	String of up to 32 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.WarrantyInfo.Duration (Read or Write)

Display Name	Duration
Description	The number of days or months that the warranty is to be in force.
Legal Values	String of up to 64 ASCII characters.
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.WarrantyInfo.EndDate (Read or Write)

Display Name	End Date
Description	The date that extended warranty service ends.
Legal Values	String of up to 32 ASCII characters.
Default Value	None
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

System.WarrantyInfo.UnitType (Read or Write)

Display Name	Unit Type
Description	Indicates whether the length of the warranty is measured in days or months.
Legal Values	• Days - 0 • Months - 1
Default Value	0
Write Privilege	Configure iDRAC
License Required	Not Applicable
Dependency	None
Is Platform Dependent	No

BALANÇO PATRIMONIAL



Entidade: CompethiCS IT Soluções em Tecnologia da Informação EIRELI - ME

Período da Escrituração: 01/01/2024 a 31/12/2024 CNPJ: 28.452.362/0001-32

Número de Ordem do Livro: 7

Período Selecionado: 01 de janeiro de 2024 a 31 de dezembro de 2024

Descrição	Nota	Saldo Inicial	Saldo Final
ATIVO		R\$ 840.109,30	R\$ 880.708,09
ATIVO CIRCULANTE		R\$ 599.479,34	R\$ 640.078,13
DISPONIBILIDADES		R\$ 412.011,98	R\$ 593.296,66
DEPÓSITOS BANCÁRIOS À VISTA		R\$ 412.011,98	R\$ 593.296,66
Bancos Conta Movimento - No País		R\$ 412.011,98	R\$ 593.296,66
CRÉDITOS		R\$ 187.467,36	R\$ 434,91
ADIANTAMENTOS		R\$ 1.092,36	R\$ 434,91
Adiantamentos a Terceiros - Circulante		R\$ 1.092,36	R\$ 434,91
DUPLICATAS A RECEBER		R\$ 186.375,00	R\$ 0,00
Duplicatas a Receber - Operações com Partes Não Relacionadas - no País		R\$ 186.375,00	R\$ 0,00
ESTOQUES		R\$ 0,00	R\$ 46.346,56
ESTOQUES DE MERCADORIAS		R\$ 0,00	R\$ 46.346,56
Mercadorias para Revenda		R\$ 0,00	R\$ 46.346,56
ATIVO NÃO CIRCULANTE		R\$ 240.629,96	R\$ 240.629,96
REALIZÁVEL A LONGO PRAZO		R\$ 240.629,96	R\$ 240.629,96
VALORES MOBILIÁRIOS - NO PAÍS		R\$ 240.629,96	R\$ 240.629,96
Outros Empréstimos e Recebíveis - No País - Longo Prazo		R\$ 240.629,96	R\$ 240.629,96
PASSIVO		R\$ 840.109,30	R\$ 880.708,09
PASSIVO CIRCULANTE		R\$ 143.399,47	R\$ 158.469,25
OBRIGAÇÕES DO CIRCULANTE		R\$ 143.399,47	R\$ 158.469,25
BENEFÍCIOS E ENCARGOS SOCIAIS - CIRCULANTE		R\$ 1.320,00	R\$ 1.412,00
Salários e Remunerações a Pagar		R\$ 1.174,80	R\$ 1.256,68
INSS a Recolher		R\$ 145,20	R\$ 155,32
FORNECEDORES □ CIRCULANTE		R\$ 142.062,83	R\$ 157.044,50
Fornecedores - Operações com Partes Não Relacionadas - No País - Circulante		R\$ 142.062,83	R\$ 157.044,50
OBRIGAÇÕES FISCAIS □ CIRCULANTE		R\$ 16,64	R\$ 12,75
IRRF a Recolher - Circulante		R\$ 16,64	R\$ 12,75
PATRIMÔNIO LÍQUIDO		R\$ 696.709,83	R\$ 722.238,84
CAPITAL SOCIAL		R\$ 500.000,00	R\$ 500.000,00
CAPITAL REALIZADO - DE RESIDENTE NO PAÍS		R\$ 500.000,00	R\$ 500.000,00
Capital Subscrito de Domiciliados e Residentes no País		R\$ 500.000,00	R\$ 500.000,00
OUTRAS CONTAS DO PATRIMÔNIO LÍQUIDO		R\$ 196.709,83	R\$ 222.238,84
OUTRAS CONTAS DO PATRIMÔNIO LÍQUIDO		R\$ 196.709,83	R\$ 222.238,84
Lucros Acumulados e/ou Saldo à Disposição da Assembléia		R\$ 196.709,83	R\$ 222.238,84

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 91.2E.06.2F.CF.68.84.8D.D6.42.2A.EF.29.04.58.AB.1E.7F.52.44-0, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

DEMONSTRAÇÃO DE RESULTADO DO EXERCÍCIO



Entidade: CompethiCS IT Soluções em Tecnologia da Informação EIRELI - ME

Período da Escrituração: 01/01/2024 a 31/12/2024 CNPJ: 28.452.362/0001-32

Número de Ordem do Livro: 7

Período Selecionado: 01 de janeiro de 2024 a 31 de dezembro de 2024

Descrição	Nota	Saldo anterior	Saldo atual
RESULTADO LÍQUIDO DO PERÍODO		R\$ 133.581,62	R\$ 25.529,01
RESULTADO LÍQUIDO DO PERÍODO ANTES DO IRPJ E DA CSLL - ATIVIDADE GERAL		R\$ 133.581,62	R\$ 25.529,01
RESULTADO OPERACIONAL		R\$ 133.581,62	R\$ 25.529,01
RECEITA LIQUIDA		R\$ 813.319,70	R\$ 238.987,79
RECEITA BRUTA		R\$ 815.373,15	R\$ 242.012,00
Receita da Revenda de Mercadorias no Mercado Interno		R\$ 769.125,00	R\$ 242.012,00
(-) Receita da Prestação de Serviços no Mercado Interno		R\$ 46.248,15	R\$ (0,00)
(-) DEDUÇÕES DA RECEITA BRUTA		R\$ (2.053,45)	R\$ (3.024,21)
(-) (-) ICMS		R\$ (512,38)	R\$ (3.024,21)
(-) ISS		R\$ (1.541,07)	R\$ 0,00
(-) CUSTO DOS BENS E SERVIÇOS		R\$ (695.390,41)	R\$ (217.459,61)
(-) CUSTO DOS BENS E SERVIÇOS VENDIDOS DAS ATIVIDADES EM GERAL		R\$ (695.390,41)	R\$ (217.459,61)
(-) (-) Custo das Mercadorias Revendidas		R\$ (695.390,41)	R\$ (217.459,61)
OUTRAS RECEITAS OPERACIONAIS		R\$ 42.466,20	R\$ 36.405,19
OUTRAS RECEITAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R\$ 42.466,20	R\$ 36.405,19
Ganhos Auferidos no Mercado de Renda Variável, exceto Day-Trade		R\$ 42.466,18	R\$ 36.405,19
(-) Multas e Outras Vantagens Recebidas		R\$ 0,02	R\$ (0,00)
(-) DESPESAS OPERACIONAIS		R\$ (16.807,30)	R\$ (19.050,23)
(-) DESPESAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R\$ (16.807,30)	R\$ (19.050,23)
(-) (-) Ordenados, Salários, Gratificações e Outras Remunerações a Empregados		R\$ (15.768,00)	R\$ (16.944,00)
(-) (-) Despesas com Telefone e Internet		R\$ (1.039,30)	R\$ (2.106,23)
(-) OUTRAS DESPESAS OPERACIONAIS		R\$ (10.006,57)	R\$ (13.354,13)
(-) OUTRAS DESPESAS OPERACIONAIS DAS ATIVIDADES EM GERAL		R\$ (10.006,57)	R\$ (13.354,13)
(-) (-) Perdas Incorridas no Mercado de Renda Variável, exceto Day-Trade		R\$ 0,00	R\$ (0,01)
(-) (-) Juros com Empréstimos de Pessoas Vinculadas ou Situadas em País com Tributação favorecida		R\$ 0,00	R\$ (3,76)
(-) (-) Outras Despesas Financeiras		R\$ (2.158,56)	R\$ (2.305,03)
(-) (-) Outras Despesas Operacionais		R\$ (7.848,01)	R\$ (11.045,33)

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 91.2E.06.2F.CF.68.84.8D.D6.42.2A.EF.29.04.58.AB.1E.7F.52.44-0, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

TERMOS DE ABERTURA E ENCERRAMENTO



Entidade:	CompethiCS IT Soluções em Tecnologia da Informação EIRELI - ME		
Período da Escrituração:	01/01/2024 a 31/12/2024	CNPJ:	28.452.362/0001-32
Número de Ordem do Livro:	7		
Período Selecionado:	01 de janeiro de 2024 a 31 de dezembro de 2024		

TERMO DE ABERTURA

Nome Empresarial	CompethiCS IT Soluções em Tecnologia da Informação EIRELI - ME
NIRE	43600281952
CNPJ	28.452.362/0001-32
Número de Ordem	7
Natureza do Livro	Livro Diário
Município	PORTO ALEGRE
Data do arquivamento dos atos constitutivos	
Data de arquivamento do ato de conversão de sociedade simples em sociedade empresária	
Data de encerramento do exercício social	31/12/2024
Quantidade total de linhas do arquivo digital	1944

TERMO DE ENCERRAMENTO

Nome Empresarial	CompethiCS IT Soluções em Tecnologia da Informação EIRELI - ME
Natureza do Livro	Livro Diário
Número de ordem	7
Quantidade total de linhas do arquivo digital	1944
Data de início	01/01/2024
Data de término	31/12/2024

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 91.2E.06.2F.CF.68.84.8D.D6.42.2A.EF.29.04.58.AB.1E.7F.52.44-0, nos termos do Decreto nº 8.683/2016.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

RECIBO DE ENTREGA DE ESCRITURAÇÃO CONTÁBIL DIGITAL

IDENTIFICAÇÃO DO TITULAR DA ESCRITURAÇÃO

NIRE 43600281952	CNPJ 28.452.362/0001-32	
NOME EMPRESARIAL CompethiCS IT Soluções em Tecnologia da Informação EIRELI - ME		

IDENTIFICAÇÃO DA ESCRITURAÇÃO

FORMA DA ESCRITURAÇÃO CONTÁBIL Livro Diário (Completo - sem escrituração Auxiliar)	PERÍODO DA ESCRITURAÇÃO 01/01/2024 a 31/12/2024
NATUREZA DO LIVRO Livro Diario	NÚMERO DO LIVRO 7
IDENTIFICAÇÃO DO ARQUIVO (HASH) 91.2E.06.2F.CF.68.84.8D.D6.42.2A.EF.29.04.58.AB.1E.7F.52.44	
ARQUIVOS SUBSTITUÍDOS (HASH)	

ESTE LIVRO FOI ASSINADO COM OS SEGUINTE CERTIFICADOS DIGITAIS:

QUALIFICAÇÃO DO SIGNATARIO	CPF/CNPJ	NOME	Nº SÉRIE DO CERTIFICADO	VALIDADE	RESPONSÁVEL LEGAL
CONTADOR	48332992087	MARIEL SANTOS REIS: 48332992087	59041317251254302	20/05/2024 a 20/05/2025	Não
Pessoa Jurídica (e-CNPJ ou e-PJ)	28452362000132	COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACA: 28452362000132	600369705582556886 3	18/09/2024 a 18/09/2025	Sim

NÚMERO DO RECIBO:

91.2E.06.2F.CF.68.84.8D.D6.42.2A.EF.
29.04.58.AB.1E.7F.52.44-0

Escrituração recebida via Internet
pelo Agente Receptor SERPRO

em 04/04/2025 às 11:46:41

07.F6.1F.D4.11.C7.62.90
7D.FB.93.AE.85.52.D9.B9

Considera-se autenticado o livro contábil a que se refere este recibo, dispensando-se a autenticação de que trata o art. 39 da Lei nº 8.934/1994. Este recibo comprova a autenticação.

BASE LEGAL: Decreto nº 1.800/1996, com a alteração do Decreto nº 8.683/2016, e arts. 39, 39-A, 39-B da Lei nº 8.934/1994 com a alteração da Lei Complementar nº 1247/2014.

Emulex®-branded Fibre Channel HBA Product Line

Emulex-branded Fibre Channel (FC) Host Bus Adapters (HBAs) by Broadcom are designed to address the demanding performance, reliability and management requirements of today's enterprises that are deploying low latency all-flash and NVMe networked storage arrays.

Emulex HBAs are available in Gen 7 (64/32GFC), and Gen 6 (32/16GFC) models. All 32G/16GFC HBAs are available in single, dual and quad-port configurations. The product line offers a variety of performance and feature options such as diagnostics and advanced security, and troubleshooting features to meet the needs of a wide range of enterprise applications.

Emulex fully supports new industry standards that further enhance Broadcom's Autonomous SAN innovations to self-learn, self-optimize, and self-heal in order to proactively keep the SAN running at maximum speed and avoid down-times. The new industry standards supported by Emulex around Fabric Performance Impact Notifications (FPIN) function include Link Integrity Notification (FPIN-LI), Congestion notification (FPIN-CN), Peer Congestion notification (FPIN-PN), and Delivery notification (FPIN-DN). The Emulex SAN Manager application is the first application in the industry to automatically identify, minimize and mitigate

application performance problems caused by SAN congestion utilizing the FPIN-CN standard.

With a common driver model supporting all Emulex HBAs for each operating system, upgrading to next generation Emulex HBAs guarantees seamless migration.

Additionally, Fibre Channel technology is backward compatible with the two previous generations. For example, Gen 7 64GFC Fibre Channel switches, HBAs and optics (transceivers) are backward compatible with 32GFC and 16GFC equipment. This provides a smooth upgrade path and investment protection for enterprises.

Emulex Fibre Channel HBA Portfolio

Models	Series	IOPS Per Single-Port	Bandwidth Per Single Port (read/write, bi-directional)	NVMe Over FC	Mission-Critical Features
Gen 7 64GFC	LPe36000	Up to 10M	12,800 MB/s	Yes	• 3x better latency than LPe31000/32000-series • Silicon Root of Trust: hardware-based firmware authentication • PCIe 4.0 bus for latest AMD and Intel servers • 128GFC Trunking
Gen 7 32GFC	LPe35000	Up to 5M	6,400 MB/s	Yes	• LPe35000-series can be upgraded from 32GFC to 64GFC with hot-plug optics kits¹ • + features below
Gen 6 32GFC	LPe32000	1.6M	6,400 MB/s	Yes	• Registration and support for Fabric Performance Impact Notifications (FPINs) and congestion signaling • Buffer-to-buffer (BB) credit recovery - automatic buffer credit loss detection and recovery for reliable performance • Forward Error Correction (FEC) • Secure Firmware Updates • Brocade® I/O Insight
Gen 6 16GFC	LPe31000	1.6M	3,200 MB/s	Yes	• ClearLink(D_port), Link Cable Beaconsing, Host Name Registration, Read Diagnostic Parameters, VMID, BB_Credit Recovery, Fabric-assigned Boot LUN, Fabric-assigned PWWN, FC-Trace, FC-Ping, Rest APIs & more • T10-PI data integrity offload • Emulex HBA Capture • Hot plug optics

1 - With Emulex approved optics kits

Accelerate

The unique Emulex Dynamic Multi-core Architecture introduced on Gen 5 HBAs delivers unparalleled performance and more efficient port utilization than other HBAs, providing up to 10 million IOPS on Emulex Gen 7 FC HBAs.

NVMe provides substantially lower latency for storage I/O operations and significantly higher IOPS per device. NVMe will scale-up the number of devices it can address by adopting NVMe over Fabrics technology. Fibre Channel is one of the fabric technologies that is supported by NVMe over Fabrics. Emulex NVMe-enabled HBAs deliver 55% lower latency than SCSI over Fibre Channel and support NVMe over Fibre Channel and SCSI over Fibre Channel concurrently. Concurrency provides data centers the ability to run SCSI and NVMe all-flash arrays at the same time for a seamless transition to an NVMe all-flash data center.

Protect

Emulex HBAs are renowned for reliability, ensuring maximum SAN uptime. Their “It Just Works” reputation is based on 17 million installed ports with proven industry-leading reliability of 10 million hours field Mean Time Between Failures (MTBF).

Emulex Gen 7 HBAs provide unmatched security for Fibre Channel environments. LPe36000/35000-series feature Silicon Root of Trust security embedded into the hardware itself. Firmware digital signatures are verified each time the system is booted as well as before installing any new firmware, providing a tamper proof solution.

Emulex’s digitally signed drivers are integrated with all the major enterprise operating systems. Drivers are digitally signed and are verified to be authentic code written by Broadcom before they can be installed.

T10 Protection Information (T10-PI) data integrity provides data protection from the server to the storage array. As one of the founders of the Data Integrity Initiative, Emulex, along with Oracle and Seagate, was instrumental in defining the T10-PI standard, which, along with the Data Integrity Extensions standard, delivers full end-to-end data integrity.

Forward Error Correction (FEC) is a Fibre Channel standard feature for HBAs and switches that provides enhanced data reliability and performance by automatically detecting and recovering from bit errors. It is especially useful in diverse and complex user environments such as blade server system implementations. FEC is a digital signal processing technique that introduces redundant data, called an error correcting code, prior to data transmission or storage. FEC then provides the receiver with the ability to correct errors without a reverse channel to request the retransmission of data, thereby improving performance. FEC is standard on Gen 7/6 at 32GFC and higher speeds. It can be enabled on Gen 7/6 at 16GFC speed.

Control

The flagship Emulex HBA Manager enterprise-class management application features a multiprotocol, cross-platform architecture that provides centralized management of all current and previous generations of Emulex FC HBAs.

This enables IT administrators to manage network connectivity with one tool for maximum efficiency.

Troubleshooting Emulex HBAs is simplified with Emulex HBA Capture, an Emulex device driver utility that gathers system, adapter, device driver, and applications information. Data collected by Emulex HBA Capture is compressed into a single file and can be sent to Broadcom Technical Support for analysis when debugging system issues or for diagnostic purposes.

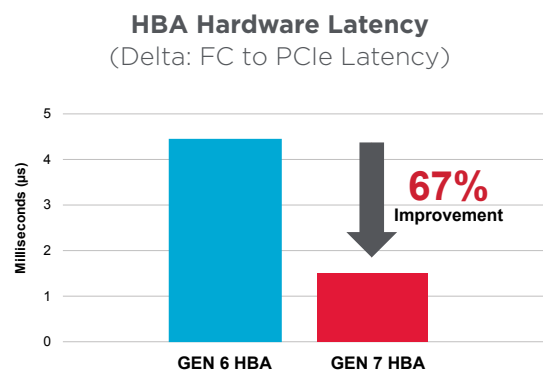
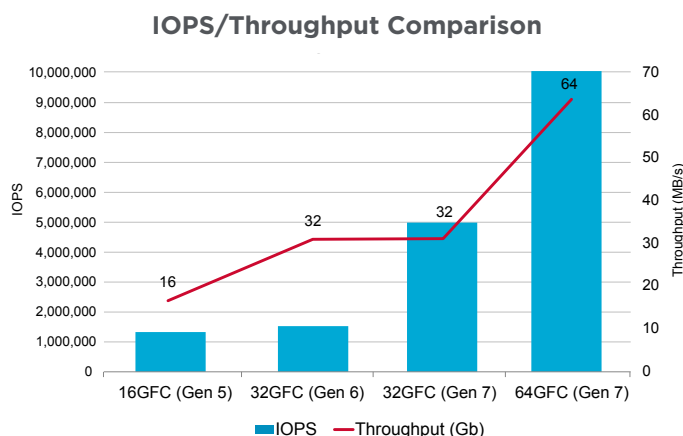
Additionally, Emulex-branded Gen 7 and Gen 6 FC HBAs support a range of Brocade features including Brocade I/O Insight, ClearLink (D_Port), Link Cable Beacons, Host Name Registration and Read Diagnostic Parameters and more.

Emulex Gen 7 and Gen 6 HBAs are managed HBAs—intelligent adapters designed to work with the Emulex SAN Manager application (available separately) to reduce the cost and complexity of managing enterprise-class SANs via the following:

- Centralized in-band access to managed HBAs across the SAN including access to optical transceiver statistics that can be downloaded for analysis to help detect optic degradation; lists queue depths by port.
- Visibility into the endpoints of the fabric, including complete SAN HBA host inventory, host names, and OS, software, and firmware versions; identifies multipath misconfiguration errors.
- Automatic identification and mitigation of application performance problems with direct communication between Emulex HBAs and Brocade fabric switches and directors.



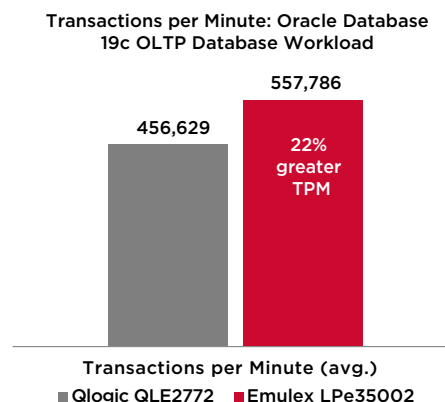
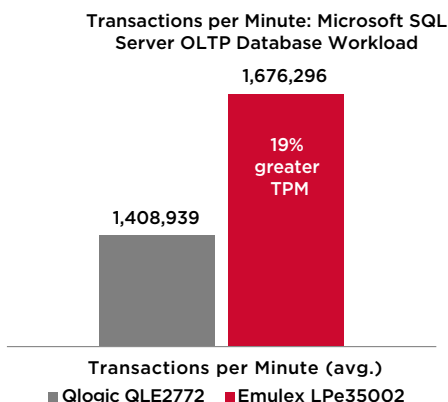
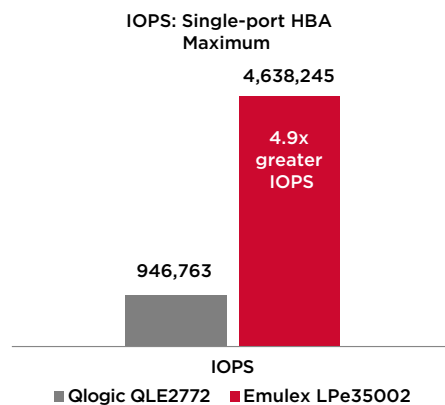
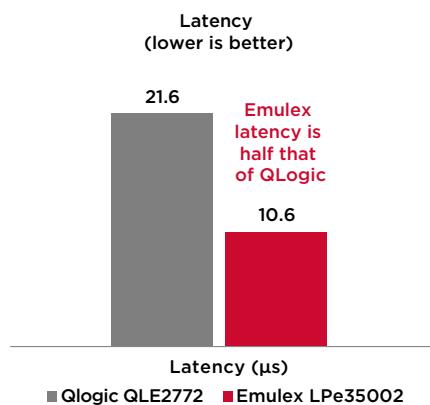
Performance Comparisons of Emulex Fibre Channel HBA Generations



- Emulex Gen 7 HBAs deliver an industry leading 10 million IOPS²
- Up to 5x more than the competitors best performing 32GFC HBA

Emulex Gen 7 HBAs were designed to address the revolution of low storage communication latency in modern NVMe datacenters. The fast path hardware architecture design **reduces average hardware latency to one third** of the latency seen in the previous generation Emulex Gen 6 HBA³

Emulex Gen 7 32GFC Performance vs. Other 32GFC HBAs⁴



2 - The Tolly Group, Emulex LPe36000-series Performance, 5-2021

3 - Demartek testing 12-2018

4 - The Tolly Group, Emulex LPe35002 HBA 32G performance versus Marvell QLogic QLE2772, 4-2020

Maximum performance and superior management efficiency for the broadest range of data center environments

Feature	Description	PCIe 4.0 HBAs		PCIe 3.0 HBAs	
		LPe36000 LPe36002	LPe35000 LPe35002 LPe35004	LPe32000 LPe32002 LPe32004	LPe31000 LPe31002 LPe31004
Link speed support	4GFC				•
	8GFC		•	•	•
	16GFC	•	•	•	•
	32GFC	•	• Upgradeable to 64GFC ¹ (except 4-port model)	•	• Upgradeable to 32GFC (except 4 port model)
	64GFC	•			
Ports	Number of Fibre Channel connections on one HBA	1, 2	1, 2, 4	1, 2, 4	1, 2, 4
Throughput per model (MB/s, full duplex)	Large block transfer speed	LPe36000: 12,800 LPe36002: 25,600	LPe35000: 6,400 LPe35002: 12,800 LPe35004: 25,600	LPe32000: 6,400 LPe32002: 12,800 LPe32004: 25,600	LPe31000: 3,200 LPe31002: 6,400 LPe31004: 12,800
IOPS	Input/output operations per second per port	10M	5M	1.6M (total)	1.6M (total)
PCIe bus		4.0	4.0 ⁵	3.0	3.0
HBA port virtualization	N_Port ID Virtualization (NPIV)	•	•	•	•
NVMe over Fibre Channel (NVMe/FC)	Supports NVMe/FC and SCSI over FC concurrently.	•	•	•	•
Emulex SAN Manager (ESM) compatible	Automatic congestion management, transceiver health statistics, inventory feature, and multi-path misconfiguration reporting.	•	•	•	•
Fabric Performance Impact Notifications (FPIN)	Supports FPINs including Link Integrity Notification (FPIN-LI), Congestion notification (FPIN-CN), Peer Congestion notification (FPIN-PN), and Delivery notification (FPIN-DN).	•	•	•	•
Dynamic Multi-core Architecture	Unparalleled performance and port utilization with eight processing cores that dynamically apply ASIC resources to any port.	•	•	•	•
Buffer Credit Recovery (B2B credit recovery)	Maintains maximum performance between ports under marginal link conditions.	•	•	•	•
T10-PI with offload	T10-PI end-to-end data integrity support with hardware offload	•	•	•	•
ClearLink diagnostics port (D_Port)	Optical and signal integrity for optics and cables	•	•	•	•
Forward Error Correction	Enhanced data reliability and performance by automatically detecting and recovering from bit errors.	•	•	•	•
Secure Firmware Updates (software-based solution)	Protects the integrity of firmware with compliance to NIST SP 800-193 standards			•	•
Silicon Root of Trust (hardware-based solution)	Hardware-based protection against malicious firmware downloads. Complies to NIST SP 800-193 standards.	•	•		
Brocade I/O Insight, Link Cable Beaconsing, Host Name Registration, Read Diagnostic Parameters	Advanced I/O monitoring and diagnostics.	•	•	•	•
Trunking (port aggregation)	Aggregates physical ports to form a single, logical, high-bandwidth port up to 128GFC.	•	•		
HBA resources	Exchanges and logins	12,288	12,288	12,288	12,288
	Virtual functions	32	32	32	32
Message-Signaled Interrupts support	MSI	•	•	•	•
	MSI-X	•	•	•	•
	Number of MSI-X vectors supported	1,024	1,024	1,024	1,024

5 - LPe35004 supports PCIe 3.0 x16

Maximum performance and superior management efficiency for the broadest range of data center environments

Feature	Description	PCIe 4.0 HBAs		PCI 3.0 HBAs	
		LPe36000 LPe36002	LPe35000 LPe35002 LPe35004	LPe32000 LPe32002 LPe32004	LPe31000 LPe31002 LPe31004
Operating system	Windows	•	•	•	•
	Linux	•	•	•	•
	VMware	•	•	•	•
	Solaris	•	•	•	•
FC-Tape		•	•	•	•
All topologies	Auto detect — P To P; FC-AL; fabric	No auto detect for FC-AL	No auto detect for FC-AL	No auto detect for FC-AL	No auto detect for FC-AL
Fibre Channel fabric boot	X86 BootBIOS	•	•	•	•
	UEFI	•	•	•	•
	OpenBoot	•	•	•	•
FC-SP-2 compliance	Fibre Channel Security Protocol with DH-CHAP authentication (host to switch)	•	•	•	•
Common management interface (FDMI)	Industry-standard interface across all operating system environments	•	•	•	•
Firmware upgrade	Upgradeable features on installed base	•	•	•	•
Firmware independent drivers	Update F/W or drivers separately simplifies SAN management	•	•	•	•
End-to-end Parity/CRC	Data protection	•	•	•	•
Host PCI slot compatibility	Short length (standard height)	•	•	•	• 4 port low profile model available
	Low profile compatible	•	• 4-port is full-height	•	•
Media interface	LC multi-mode/short wave	•	•	•	•
	Digital diagnostics	•	•	•	•
	Long-wave optics (optional kits)	•	•	•	•

Options

Part number	Description
LPe16100-OPT	16GFC optic (short wave laser with LC connector SFP+ optic) — 1 pack
LPe16100-OPTx2	16GFC optics (short wave laser with LC connector SFP+ optic) — 2 pack
LP16-LW-OPT-1	16GFC long wave optic (long wave laser with LC connector SFP+ optic) — 1 pack
LP16-LW-OPT-2	16GFC long wave optics (long wave laser with LC connector SFP+ optic) — 2 pack
LP32-SW-OPT-1	Gen 6 (32GFC) spare optic (short wave laser with LC connector SFP+ optic) — 1 pack
LP32-SW-OPT-2	Gen 6 (32GFC) spare optics (short wave laser with LC connector SFP+ optic) — 2 pack
LP32-LW-OPT-1	32GFC long wave optic (long wave laser with LC connector SFP+ optic) — 1 pack
LP32-LW-OPT-2	32GFC long wave optics (long wave laser with LC connector SFP+ optic) — 2 pack
LP64-SW-OPT-1	64GFC shortwave optic (short wave laser with LC connector SFP+ optic) — 1 pack
LP64-SW-OPT-2	64GFC shortwave optics (short wave laser with LC connector SFP+ optic) — 2 pack
LP64-LW-OPT-1	64GFC long wave optic (long wave laser with LC connector SFP+ optic) — 1 pack
ECD-ESM-EN1Y	Emulex SAN Manager, Enterprise Product, 1 YR

Dell PowerEdge Server BIOS Security Configuration Guide

For 16G Intel-based PowerEdge servers

Abstract

This PowerEdge server BIOS Security Configuration Guide (SCG) describes the BIOS security features that you can use to manage and customize your PowerEdge servers with Intel processors. It also defines the fields used to configure these attributes and best practices for defining values in each field, where appropriate.

April 2024

Revisions

Date	Version	Author	Description
February 29, 2024	V1.1	Cecil Sheng and Ivy Yang	Combined 16G Intel Security Configuration Guides.

Acknowledgments

Author: **Cecil Sheng**—Firmware Senior Principal Engineer

Ivy Yang—Firmware Principal Engineer

Other: **Samiksha Aggarwal**—Content Engineering and Translation

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third party content is updated by the relevant third parties, this document will be revised accordingly.

Copyright © 2024 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [4/2/2024] [Security Configuration Guide] [617]

Contents

Revisions.....	2
Acknowledgments.....	2
Contents.....	3
Prefaces.....	5
Where to get help.....	5
1 Overview.....	6
1.1 Security development lifecycle	6
1.2 Threat and Dell server BIOS solution	6
2 Protect a PowerEdge server using BIOS	8
2.1 Cryptographically verified Trusted Boot	8
2.1.1 iDRAC Root-of-Trust and Silicon-based Root-of-Trust	8
2.1.2 UEFI Secure Boot Support	9
2.1.3 TPM support	10
2.1.4 Intel TXT support	11
2.1.5 Signed firmware updates	12
2.2 Disable USB ports	13
2.3 Create a setup password in BIOS	13
2.3.1 Secure system using system password	14
2.3.2 Delete or change system and setup password	14
2.3.3 Operating with setup password enabled	15
2.3.4 Password status	15
2.4 Persistent memory passphrase feature.....	15
2.5 UEFI variable access.....	16
2.6 Intel Total Memory Encryption (TME) and Multi-Tenant (MT)	17
2.6.1 Intel Software Guard Extensions	18
2.7 SMM Security Mitigation	20
2.8 HTTPS boot	20
3 Detect issues in server configuration and health status.....	25
3.1 Comprehensive Monitoring via iDRAC	25
3.1.1 Lifecycle log	25
4 Recover server to a known state.....	26
4.1 Rapid response to new vulnerabilities	26
4.2 Recover the BIOS state	26
4.3 Roll back a server firmware	27

- 4.4 Restore server configuration after hardware servicing.....27
 - 4.4.1 Easy Restore (for motherboard replacement) 27
 - 4.5 System Erase 28
 - 4.6 Full Power Cycle.....28
- 5 Summary 29
- A Technical support and resources 30

Prefaces

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this SCG are not supported by all versions of the software or hardware currently in use. The product Release Notes provides the most up-to-date information about product features. Contact your service provider if a product does not function properly or does not function as described in this SCG.

Where to get help

For information about support, product, and licensing, visit the following websites:

- Product information and troubleshooting—For product and feature documentation or Release Notes, go to <https://www.dell.com/support> and locate the appropriate product support page.
- Technical support—For technical support and service requests, go to <https://www.dell.com/support> and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

1 Overview

The PowerEdge servers have provided robust security for several generations, including the innovation of using silicon-based data security. Starting from 15G, Dell introduced iDRAC Root-of-Trust (RoT) to authenticate BIOS at a higher security level. The Dell product team has considered several key requirements during the design of 16G PowerEdge servers in response to security threats faced by modern IT environments:

- **Protect**—Protect server during every aspect of lifecycle, including BIOS, firmware, data, and physical hardware.
- **Detect**—Detect malicious cyberattacks and unapproved changes; engage IT administrators proactively.
- **Recover**—Recover BIOS, firmware, and OS to a known good state; securely retire or repurpose servers.

The PowerEdge servers conform to key industry standards on cryptography and security as elaborated throughout this technical white paper and perform on-going tracking and management of new vulnerabilities. The intended audience for this document includes system administrators, who are responsible to maintain and deploy servers and ensure that network and infrastructure security best practices are followed.

Note—THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.

This SCG is a reference document. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk or guidance to your local installation and individual environment. It is recommended that you determine the applicability of this information to your individual environments and take appropriate actions. All aspects of this Security Configuration Guide (SCG) are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

1.1 Security development lifecycle

Dell has implemented the security development lifecycle process with security as a key element in every aspect of development, procurement, manufacturing, shipping, and support resulting in a Cyber Resilient Architecture in PowerEdge servers.

1.2 Threat and Dell server BIOS solution

Table 1 Dell server BIOS solution

Security Layer	Threat Vector	Dell Solution
Physical server	Server tampering	Physical deterrents

Firmware and software	Corrupted firmware, malware injection	• iDRAC Root-of-Trust • Intel Boot Guard • Cryptographically signed and validated firmware
Attestation trust features	Server identity spoofing	• TPM • TXT • Chain of trust • TME • SGX* • TDX*
Server Management	Rogue configuration and updates, unauthorized open-port attacks, data leak, and corruption	• iDRAC9 • Persistent memory passphrase*

*This feature is currently not supported on one-socket, Intel based, PowerEdge servers.

2 Protect a PowerEdge server using BIOS

2.1 Cryptographically verified Trusted Boot

2.1.1 iDRAC Root-of-Trust and Silicon-based Root-of-Trust

Starting from 14G, the PowerEdge servers use an immutable, silicon-based Root-of-Trust (RoT) to cryptographically attest the integrity of BIOS and iDRAC firmware. This Root-of-trust is based on one-time programmable, read-only public keys that provide protection against malware tampering.

The BIOS boot process leverages Intel Boot Guard technology which verifies that the digital signature of the cryptographic hash of the boot image matches the signature stored in silicon by Dell during manufacturing. A failure to verify results in a shutdown of the server, user notification in the Lifecycle Controller Log, and the BIOS recovery process can then be initiated by the user. If Boot Guard validates successfully, the rest of the BIOS modules are validated by using a chain of trust procedure until control is handed off to the Operating System (OS) or hypervisor.

Starting from 15G, the PowerEdge servers provides even higher security level by introducing iDRAC Root-of-Trust. The iDRAC Root-of-Trust provides a critical trust anchor for authenticating the signatures of Dell firmware Update Packages (DUPs) including BIOS firmware update.

More information about the chain of trust provided in this section. Each BIOS module contains a hash of the next module in the chain. The key modules in BIOS are the Initial Boot Block (IBB), Security/Pre-EFI Initialization (SEC/PEI), Driver Execution Environment (DXE), and Boot Device Selection (BDS). The iDRAC RoT first checks the signature stored in the BIOS image file. Only if the signature is valid, the system can boot. The Intel BootGuard then authenticates the IBB (Initial Boot Block), a module in the IBB authenticates the next part of BIOS, the SEC/PEI section. A module in the section then authenticates the DXE/BDS section of the BIOS image file. In the BDS phase, if Secure Boot is enabled, the authentication process is handled by the secure boot driver.

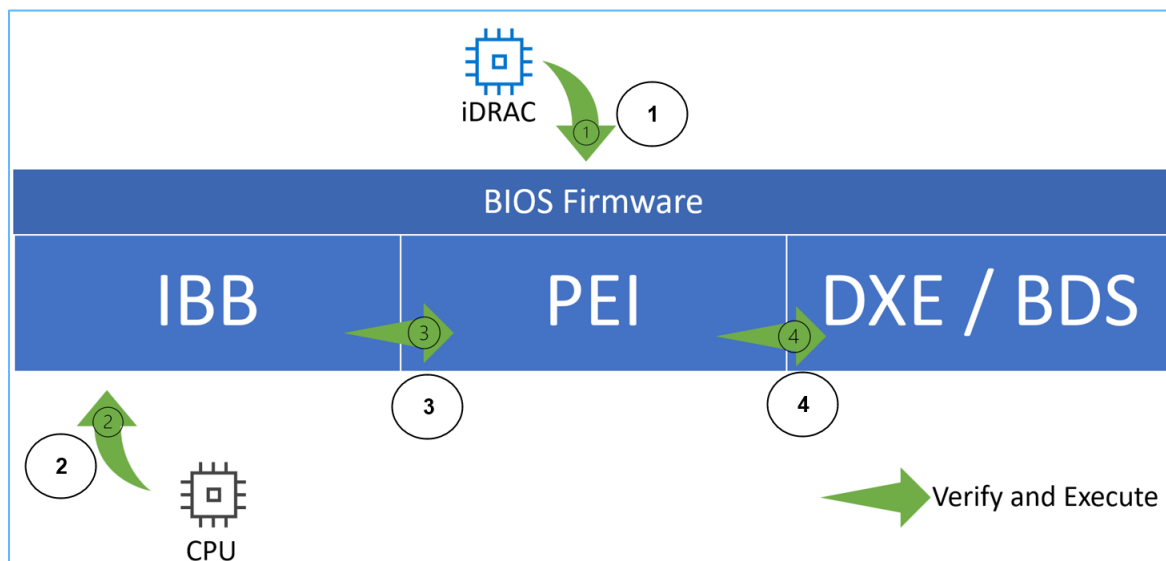


Figure 1 Process of authentication using the Chain of Trust feature in iDRAC

2.1.2 UEFI Secure Boot Support

The PowerEdge servers also support industry standard Unified Extensible Firmware Interface (UEFI) Secure Boot which checks the cryptographic signatures of UEFI drivers and other code loaded prior to the OS running. Secure Boot represents an industry-wide standard for security in the pre-boot environment. Computer system vendors, expansion card vendors, and operating system providers collaborate on this specification to promote interoperability.

When enabled, UEFI Secure Boot prevents unsigned (that is, untrusted) UEFI device drivers from being loaded, displays an error message, and does not allow the device to function. You must disable Secure Boot to load unsigned device drivers.

In addition, PowerEdge servers offer customers the unique flexibility of using a customized boot loader certificate not signed by Microsoft. This is primarily a feature for administrators of Linux environments that want to sign their own OS boot loaders. Custom certificates can be uploaded via the preferred iDRAC API to authenticate the customer's specific OS boot loader.

The default configuration for Secure Boot is disabled. Do the following to enable the Secure Boot:

1. Power on the system.
2. When the company logo is displayed, press F2 to open the System Setup page.
3. On the System Setup Main Menu page, click **System BIOS** → **System Security**.
4. To enable the Secure Boot feature, click **Enable**.

Table 2 Options and Descriptions to enable the Secure Boot

Option	Description
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to Disabled by default.
Secure Boot Policy	When Secure Boot policy is set to Standard, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot policy is set to Custom, the BIOS uses the user-defined key and certificates. Secure Boot policy is set to Standard by default.
Secure Boot Mode	Configures how the BIOS uses the Secure Boot Policy Objects: • Platform Key (PK) • Key Exchange Key Database (KEK) • Authorized Signature Database (db) • Forbidden Signature Database (dbx) If the current mode is set to Deployed Mode, the available options are User Mode and Deployed Mode. If the current mode is set to User Mode, the available options are User Mode, Audit Mode, and Deployed Mode. • User Mode—In User Mode, PK must be installed, and BIOS performs signature verification on programmatic

	attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes. • Audit Mode—In Audit Mode, PK is not present. BIOS does not authenticate programmatic update to the policy objects and transitions between modes. The BIOS performs a signature verification on pre-boot images and logs the results in the image Execution Information Table but executes the images whether they pass or fail verification. Audit Mode is useful for programmatic determination of a working set of policy objects. • Deployed Mode—Deployed Mode is the most secure mode. In Deployed Mode, PK must be installed, and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.
Secure Boot Policy Summary	Specifies the list of certificates and hashes that secure boot uses to authenticate images.
Secure Boot Custom Policy Settings	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to Custom option.

2.1.3 TPM support

PowerEdge servers support two versions of Trusted Platform Module (TPM):

- TPM 1.2 FIPS + Common Criteria+ TCG certified (Nuvoton)
- TPM 2.0 FIPS + Common Criteria+ TCG certified (Nuvoton)

TPM can perform public key cryptographic functions, computing hash functions, generating, managing and securely storing keys, and attestation. The Intel Trusted Execution Technology (TXT) functionality and Microsoft Platform Assurance feature in Windows Server 2016 and later are also supported. TPM can be used to enable the BitLocker™ hard drive encryption feature in Windows Server 2012 and later. TPM is compatible with the remote attestation HyTrust CloudControl solution. Attestation and remote attestation systems can employ the TPM to take measurements of a server's hardware, hypervisor, BIOS, and OS during startup time and compare them to base measurements recorded in the TPM in a cryptographically secure way. If they are not the same, the server identity has been compromised, and system administrators can shut and disconnect the server locally or remotely.

TPM is enabled through a BIOS option. It is offered as a Plug-In Module solution, the planar has a connector for this plug-in module. However, once the TPM module is enabled on any Dell PowerEdge 13G server (or later), that physical chip is now permanently tied to that specific server and cannot be moved to any other system. This physical and cryptographic binding ensures that the platform integrity cannot be breached or the data cannot simply be moved to another platform along with the TPM.

Do the following to enable the TPM:

1. Power on the server.
2. When the company logo is displayed, press F2 to open the **System Setup** page.

- On the System Setup Main Menu page, click **System Setup Main Menu → System BIOS → System Security**.
- Set the TPM Security from Off to the required state. For TPM 1.2, ensure that TPM is activated.

Table 3 TPM 1.2 Setup option details

Option	Description
TPM Security	Note—The TPM menu is available only when the TPM module is installed. Enables you to control the reporting mode of the TPM. The TPM Security option is set to Off by default. You can only modify the TPM Status, and TPM Activation if the TPM Status field is set to either On with Pre-boot Measurements or On without Pre-boot Measurements. When TPM 1.2 is installed, the TPM Security option is set to Off, On with Pre-boot Measurements, or On without Pre-boot Measurements.
TPM Information	Changes the operational state of the TPM. This option is set to No Change by default.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Status	Specifies the TPM status.
TPM Command	Controls the Trusted Platform Module (TPM). When set to None, no command is sent to the TPM. When set to Activate, the TPM is enabled and activated. When set to Deactivate, the TPM is disabled and deactivated. When set to Clear, all the contents of the TPM are cleared. This option is set to None by default.

Table 4 TPM 2.0 security information

Option	Description
TPM Security	Note—The TPM menu is available only when the TPM module is installed. Enables you to control the reporting mode of the TPM. The TPM Security option is set to Off by default. You can only modify the TPM Status, and TPM Activation if the TPM Status field is set to On. When TPM 2.0 is installed, the TPM Security option is set to Off or On. This option is set to Off by default.
TPM Information	Changes the operational state of the TPM. This option is set to No Change by default.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Hierarchy	Enables, disables, or clears the storage and endorsement hierarchies. - When set to Enabled, the storage and endorsement hierarchies can be used. - When set to Disabled, the storage and endorsement hierarchies cannot be used. - When set to Clear, the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled.
TPM Advanced Settings	Specifies TPM Advanced Settings.

2.1.4 Intel TXT support

The Intel TXT feature provides the hardware basis for platform to validate platform trustworthiness during boot. It allows integrity verifications on BIOS, operating system loader, and hypervisor.

Prerequisites

To enable the **Intel TXT** option, another option **Virtualization Technology** must be set to ON. Also, **TPM Security** must be set to ON for TPM2.0.

To enable TXT, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click **System BIOS → System Security**.
3. On the System Security screen, set the **Intel TXT** option to **On**.
4. Save settings and close the System Setup page. Restart for the new settings to become effective.

Table 5 Option to enable Intel TXT

Option	Description
Intel(R) TXT	Enables you to set the Intel Trusted Execution Technology (TXT) option. To enable the Intel TXT option, virtualization technology and TPM Security must be enabled with Pre-boot measurements. This option is set to Off by default.

2.1.5 Signed firmware updates

PowerEdge servers have used digital signatures on firmware updates for several generations to assure that only authentic firmware is running on the server platform. We digitally sign our firmware packages using SHA-384 hashing with 3072-bit RSAPSS encryption for the signature for BIOS. The iDRAC scans the firmware updates and compare their signatures to what is expected using the silicon-based Root-of-Trust; any firmware package that fails validation is aborted and an error message is logged into the Lifecycle Log (LCL) to alert IT administrators.

Enhanced firmware authentication is embedded within many third party devices which provide signature validation using their own Root-of-Trust mechanisms. This prevents the possible use of a compromised third party update tool from being used to load malicious firmware. For example, a NIC or storage drive (and bypassing the use of signed Dell update packages). Many of the third party PCIe and storage devices shipped with PowerEdge servers use a hardware Root-of-Trust to validate their respective firmware updates.

If any firmware in any device is suspected of malicious tampering, IT administrators can roll back many of the platform firmware images to a prior trusted version stored in iDRAC. As an example, keep two versions of device firmware on the server:

- The existing production version (N).
- A prior trusted version (N-1).

Also, for 15G, an unsigned image file update from production level BIOS image file is not supported. To update the System BIOS, download DUP or EFI image files from Dell websites. To ensure the image file integrity, th verify the checksum value of downloaded image files. The Checksum value is displayed on the Download page. For example, the checksum values of a BIOS DUP file are shown in the sample screen shot:

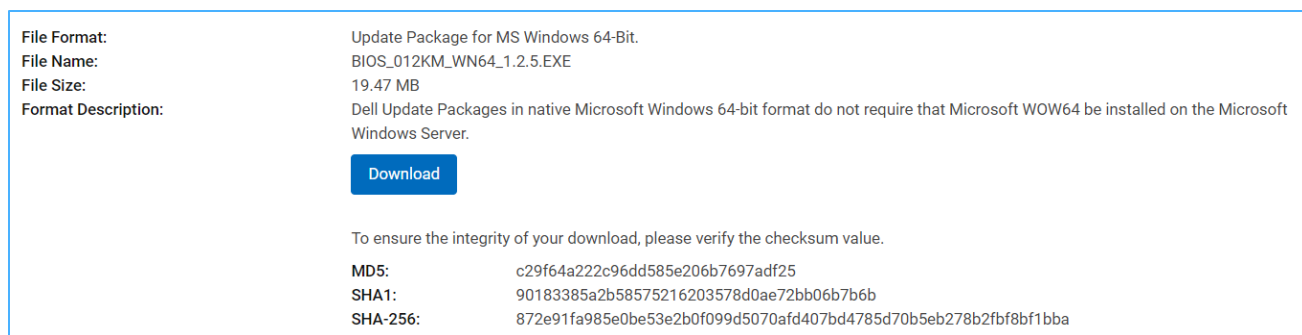


Figure 2 Example of a BIOS DUP files checksum

2.2 Disable USB ports

You can entirely disable USB ports for added protection. You can also disable only the USB ports on the front of the device. USB ports, for example, can be deactivated for production use and then temporarily enabled to allow debugging access to a crash cart. Following are the options to configure USB ports:

Table 6 Options to configure USB ports

Option	Description
User Accessible USB Ports	- Configures the user-accessible USB ports. - Selecting Only Back Ports On disables the front USB ports. - Selecting All Ports Off disables all front and back USB ports. - Selecting All Ports Off (Dynamic) disables all front and back USB ports during POST and front ports can be enabled or disabled dynamically by authorized user without resetting the system. This option is set to All Ports On by default. When user-accessible USB ports are set to All Ports Off (Dynamic), the Enable Front Ports Only option is enabled. - Enable Front Ports Only: Enables or disables the front USB ports during the OS runtime. The USB keyboard and mouse still function in certain USB ports during the boot process, depending on the selection. After the boot process is complete, the USB ports will be enabled or disabled as per the setting.
iDRAC Direct USB Port	The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. This option is set to ON or OFF. When set to OFF, iDRAC does not detect any USB devices installed in this managed port. This option is set to ON by default.

2.3 Create a setup password in BIOS

When you receive a PowerEdge server, you must create a BIOS System Password and a BIOS Setup Password to protect the BIOS and the boot sequence.

Prerequisites

Ensure that the password jumper is enabled. The password jumper enables or disables the system password and setup password features. For how to use password jumper, see the **System board jumper settings** section in the **Installation and Service Manual** of the server.

NOTE—If the password jumper is set to disabled, the existing system password and setup password are deleted, and you need not provide the system password to boot the system. The server case must be opened to access the password jumper, which will be logged as an intrusion event.

Do the following to create a system and setup password:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click **System BIOS → System Security**.
3. On the System Security screen, verify that Password Status is set to Unlocked.
4. In the **System Password** field, type your system password, and press Enter or Tab. Use the following guidelines to assign the system password:
A password can have up to 32 characters.
A message prompts you to reenter the system password.
5. Re-enter the system password and click **OK**.
6. In the Setup Password field, type your setup password and press Enter or Tab. A message prompts you to reenter the setup password.
7. Re-enter the setup password and click **OK**.
8. Press Esc to return to the System BIOS screen. Press **Esc** again. A message prompts you to save the changes.

NOTE—The Password protection feature will not be effective until the server is restarted.

2.3.1 Secure system using system password

If you have assigned a setup password, the system accepts your setup password as an alternate system password.

Do the following to secure the system using password:

1. Power on the system.
2. Type the system password and press **Enter**.

When the **Password Status** is set to **Locked**, type the system password, and press **Enter** when prompted to reboot.

NOTE—If an incorrect system password is typed, the system displays a message and prompts you to re-enter your password. You have three attempts to type the correct password. After the third unsuccessful attempt, the system displays an error message that the system has stopped functioning and must be turned off. Even after you power off and restart the system, the error message is displayed until the correct password is entered.

2.3.2 Delete or change system and setup password

Prerequisites

NOTE—You cannot delete or change an existing system or setup password if the **Password Status** is set to **Locked**.

To change or delete the server and setup password, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click System BIOS → System Security.
3. On the System Security screen, ensure that Password Status is set to Unlocked.
4. In the **System Password** box, alter or delete the existing system password, and then press Enter or Tab.
5. In the **Setup Password** field, alter or delete the existing setup password, and then press Enter or Tab.
6. If you change the system and setup password, a message prompts you to re-enter the new password. If you delete the system and setup password, a message prompts you to confirm the deletion.
7. Press Esc to return to the **System BIOS** screen. Press Esc again. A message prompts you to save the changes.
8. Select **Setup Password**, change or delete the existing setup password and press Enter or Tab.

NOTE—If you change the system password or setup password, a message prompts you to re-enter the new password. If you delete the system password or setup password, a message prompts you to confirm the deletion.

2.3.3 Operating with setup password enabled

If **Setup Password** is set to **Enabled**, type the correct setup password before modifying the system setup options. If you do not type the correct password in three attempts, the system displays the following message:

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted!
Must power down.
```

Even if you turn off and restart the system, the error message is displayed until the right password is entered. There are a few exceptions:

- If System Password is not set to Enabled and is not locked through the Password Status option, you can assign a system password.
- You cannot disable or change an existing system password.

NOTE—You can use the password status option with the setup password option to protect the system password from unauthorized changes.

2.3.4 Password status

Password status allows an administrator to maintain a setup password to protect against unauthorized BIOS Setup changes, while a user can freely change the system password.

Table 7 Option for the password status

Option	Description
Password status	Unlocked—the system password can be changed without entering the setup password. Locked—the setup password must be entered to change the system password. To prevent the system password from being modified without providing the setup password, set this option to Locked and enable the setup password.

2.4 Persistent memory passphrase feature

NOTE— This feature is currently not supported on one-socket, Intel based, PowerEdge servers.

The purpose of persistent memory security is to protect data located in the persistent memory region of an Intel Optane memory module. The data is secured (no read or write access) if a passphrase in the memory module is set. The passphrase is stored in encrypted format. After a system reset, the data is inaccessible until the Dell security driver unlocks the memory module with the correct passphrase. Note that the user does not need to re-enter the passphrase at this point. The memory modules are unlocked automatically by BIOS if the passphrase is correct.

This is to protect the Optane memory modules from being physically removed from a system and installed in another system so that the data can be accessed.

The Dell Persistent Memory Security BIOS feature provides the following functionality:

- A Setup option Persistent Memory Passphrase to config the passphrase.
- If a passphrase is set, the persistent area of the Optane memory modules are encrypted during POST.

The Setup option allows the user to set, change, or delete the passphrase. All Optane Memory modules with or without a persistent memory region are affected if the passphrase is modified. Entering an empty passphrase will delete the passphrase and disable security in the Optane memory modules.

The setup option **Persistent Memory Passphrase** field is only available if at least one Optane memory module is installed on the system.

To set up persistent memory passphrase, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click **System BIOS → Memory Settings → Persistent Memory → Intel Persistent Memory**.
3. In the **Persistent Memory Passphrase** option, set or change or remove the passphrase.
4. Save settings and exit Setup. Reboot for new passphrase to take effect.

If a secured Optane memory module cannot be unlocked with the passphrase, BIOS displays an error message to the screen and lifecycle Log, and pauses at the F1 or F2 prompt.

Message

The data in the Persistent Memory DIMM located in memory slot <slot label> is not accessible because the DIMM is locked and the passphrase is incorrect.

Recommended Response Action

Update the Persistent Memory Passphrase to the correct passphrase or perform a Secure Erase operation on the failed DIMM.

NOTE—Secure erase will erase all persistent data.

2.5 UEFI variable access

UEFI variables are used for various system configurations and some variables are very critical and essential. Adding the access restriction (write-protected) is a feature to protect those UEFI variables and mitigate the vulnerability caused by unexpected system configuration.

A BIOS setup item **UEFI Variable Access** is provided to control the access restriction of UEFI variable:

- **Standard**—Default setting indicates the access is based on the definition of UEFI specification.
- **Controlled**—Indicates some specific UEFI variables are protected and cannot be modified in an OS environment.

The following UEFI variables are write-protected when BIOS attribute `UefiVariableAccess` is set to **“Controlled”** mode.

Table 8 List of UEFI variable names and variable GUID

UEFI Variable Name	UEFI Variable GUID
L"BootNext"	EFI_GLOBAL_VARIABLE
L"DriverOrder"	EFI_GLOBAL_VARIABLE
L"ConIn"	EFI_GLOBAL_VARIABLE
L"ConOut"	EFI_GLOBAL_VARIABLE
L"BootState"	EFI_GLOBAL_VARIABLE
L"ReserveMemFlag"	EFI_GLOBAL_VARIABLE
L"UefiOptimizedBoot"	{0x356471b1, 0xb483, 0x42ae, 0xb6, 0xe7, 0x3b, 0x2e, 0xba, 0xb1, 0x4e, 0x15}

NOTE—The setting `UefiVariableAccess` to **Controlled** may cause Linux DUP support to stop working. For example, if Linux DUP attempts to write to variables such as **BootNext**, those variables are now write-protected. This is expected behavior since the user opted-in to the extra protection.

To control UEFI Variable Access, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the **System Setup Main Menu** screen, click **System BIOS → System Security**.
3. Enable UEFI Variable Access by setting it to Controlled.
4. Save settings and exit Setup. Restart the server to make the updated settings become effective.

2.6 Intel Total Memory Encryption (TME) and Multi-Tenant (MT)

NOTE— This feature is currently not supported on one-socket, Intel based, PowerEdge servers.

Intel TME enables the encryption of memory pages across system. When you use the single key, software code modification is not required. It uses the National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES) XTS based algorithm with 128-bit keys or 256-bit keys depending on availability and selection of algorithm. The key to encrypt the entire physical memory of the system comes from hardware random number generator in Intel System on Chip (SoC). Ensure that the key is not accessible to software or use external interfaces to Intel SoC.

TME-MT uses the same hardware architecture with TME. The difference is that it allows multiple keys to be used.

Prerequisite

Platform must meet certain requirements before TME can be enabled:

- Processor must be **Total Memory Encryption** capable.

To enable the Memory Encryption, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click System BIOS → System Security.
3. Enable “**Memory Encryption**” by setting it to either “**Single Key**” or “**Multiple Key**”.
4. Save settings and exit Setup. Restart the server to make the changes effective.

Table 9 Memory Encryption setup options

Option	Description
Intel® Memory Encryption	Enables or disables the Intel Total Memory Encryption (TME and TME-MT). • Disabled—BIOS disables both TME and TME-MT technology. This is the default value. • Single Key—BIOS enables the TME technology. • Multiple Keys—BIOS enables the TME-MT technology.

2.6.1 Intel Software Guard Extensions

NOTE—This feature is currently not supported on one-socket, Intel based, PowerEdge servers.

The PowerEdge servers support Intel Software Guard Extensions (Intel® SGX), CPU instructions, and platform enhancements. It allows software to protect its sensitive information by creating secure enclave. With significantly smaller trusted computing base, software sensitive information is protected from hardware or software attacks even if OS ring0 and BIOS/SMM are compromised. It also helps prevent memory snooping by keeping the secure perimeter to CPU package boundary. In other words, code and data are encrypted outside of CPU package so external memory read only sees encrypted code and data.

During the Initial Platform Establishment boot flow, the BIOS checks the key blobs for each CPU package to verify that they are all consistent with the platform. Microcode sees that there are no key blobs provided and generates the new platform keys. The new platform keys are randomly generated for this platform instance. Each CPU package uses its HW key to encrypt the shared platform keys and generate a key blob. BIOS stores the key blobs in flash for future boots. Microcode also generates a new platform manifest for the new platform instance. BIOS provides the new platform manifest to software via the `SGXRegistrationServerRequest` UEFI variable and indicates that a registration flow is required using the `SGXRegistrationStatus` UEFI variable. The registration authority service must evaluate the new platform manifest before it can generate any PCK Certificates for the new platform.

Prerequisite

Platform must meet certain requirements before SGX can be enabled:

- Processor must be SGX capable.
- Memory population must be compatible. Minimum configuration is 8 identical DIMMs per CPU socket (DIMM1 to DIMM8). See the following table.
- Memory operating mode must be set to the **Optimizer** mode.

- Memory encryption must be enabled.
- Node interleaving must be disabled.

DDR4	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1	Slot0	Slot1
8	DDR4		DDR4		DDR4		DDR4		DDR4		DDR4		DDR4		DDR4	
12	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	
16	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4

Figure 3 List of platform with DIMM per channel

Note: The table displays the platforms that have two DIMMs per channel. Some platforms might have only one DIMM per channel. In that case, SGX supported configuration will be fully populated.

To enable SGX, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the System Setup Main Menu screen, click **System BIOS → System Security**.
3. Enable **Intel SGX** by setting it to **On**.
4. Set the **PRMRR size** to desired size. After the next boot operation, BIOS will try to allocate one PRMRR with selected **PRMRR size** per **NUMA/Sub NUMA** domain.
5. Save the settings and exit Setup. Restart the server to make the changes effective.

Table 10 SGX setup options

Option	Description
Intel® SGX	Enables you to set the Intel Software Guard Extension (SGX) option. This option is set to Off by default. When this option is to Off , BIOS disables the SGX technology. When this option is to On , BIOS enables the SGX technology.
SGX Package Info In-Band Access	Enables you to access the Intel Software Guard Extension (SGX) package info in-band option. This option is set to Off by default. Each CPU package on the platform has a key blob when SGX is enabled on a multi-package platform. BIOS provides a mechanism for retrieving the key blobs. Platform owners may want to maintain a copy of the key blobs in case they need to be restored after they are deleted from BIOS persistent store (for example, the FLASH was erased or SGX was reset). The <i>SgrRegistrationPackageInfo</i> UEFI variable provides the key blobs. By default, BIOS does not present the key blobs to the software. The platform owner needs to 'opt-in' by enabling this option before BIOS provides the key blobs.
PPMRR Size	Sets the PPMRR size. PPMRR stands for Processor Reserved Memory Region Registers. It defines the Enclave Page Cache size for SGX application execution. System BIOS would try to allocate the PPMRR. The allocation is based on current memory map, memory DIMM population, and PPMRR allocation rules. In some configurations, BIOS may not be able to allocate PPMRR or PPMRR may be less than expected.

SGX QoS	Enables or disables the SGX quality of service. When Intel® SGX QoS is enabled, the processor reserves LLC cache for EPC to increase secure enclave performance at the cost of other workload performance.
Select Owner EPOCH input type	Enables you to select Change to New random Owner EPOCHs or Manual User Defined Owner EPOCHs. Each EPOCH is 64-bit. After generating new EPOCH by selecting Change to New random Owner EPOCHs, the selection reverts to Manual User Defined Owner EPOCHs. Software Guard Extensions Epoch n: Sets the Software Guard Extensions Epoch values.
Enable writes to SGXLEPUBKEYHASH[3:0] from OS/SW	Enables or disables the Enable writes to SGXLEPUBKEYHASH[3:0] from OS/SW. SGX LE Public Key Hash0: Sets the bytes from 0-7 for SGX Launch Enclave Public Key Hash. SGX LE Public Key Hash1: Sets the bytes from 8-15 for SGX Launch Enclave Public Key Hash. SGX LE Public Key Hash2: Sets the bytes from 16-23 for SGX Launch Enclave Public Key Hash. SGX LE Public Key Hash3: Sets the bytes from 24-31 for SGX Launch Enclave Public Key Hash.
Enable/Disable SGX Auto MP Registration Agent	Enables or disables the SGX Auto MP Registration . The MP registration agent (MPA) is responsible to register the platform. This option allows the user to enable/disable the MPA from running automatically at OS boot. By default, the MPA does not automatically run at boot.
SGX Factory Reset	When enables, set SGX setup options (except Intel SGX option) back to default. All the key blobs for that platform will be deleted and system will be forced to run a new Initial Platform Establishment flow. This option is reset back to Off after factory reset operations are done after reboot. This option is set to Off by default.

2.7 SMM Security Mitigation

System Management Mode (SMM) operations are transparent to operating systems. Over the years, SMM has become a significant attack surface. Numerous SMM security mitigations are therefore introduced to protect from threats. SMM Security Mitigation provides a way for firmware to indicate what specific mitigations are present. Firmware indicates these flags in an ACPI table called Windows SMM Security Mitigation Table (WSMT).

To enable to disable the SMM security mitigation, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server.
2. On the **System Setup Main Menu** screen, click **System BIOS → System Security**.
3. Enable or disable SMM security mitigation with **SMM Security Mitigation** setup option.

2.8 HTTPS boot

HTTPS boot enables you to use HTTP protocol to transfer the boot file over Transport Layer Security protocol to authenticate HTTPS server. To use HTTPS boot on Dell PowerEdge server, you need to setup DHCP server and HTTPS server. After generating the certificate on HTTPS server, you must import the certificate to the PowerEdge server so it can obtain boot file over HTTPS boot process.

Prerequisite

Setup DHCP server, DNS server and HTTPS server. You can setup based on your requirement. Also, get HTTPS server root certificate from HTTPS server so it can be later imported to HTTPS boot client.

To enable the HTTPS boot settings, do the following:

1. To open the **System Setup** page, press F2 immediately after powering on or restarting your server. Ensure that this server receives boot image via HTTPS boot support.
2. On the **System Setup Main Menu** screen, click **System BIOS**.
3. Click **Network Settings**.
4. On the **Network Settings** page, enable HTTP Device 1 through 4 as necessary, of your choice, and enter HTTP device settings.

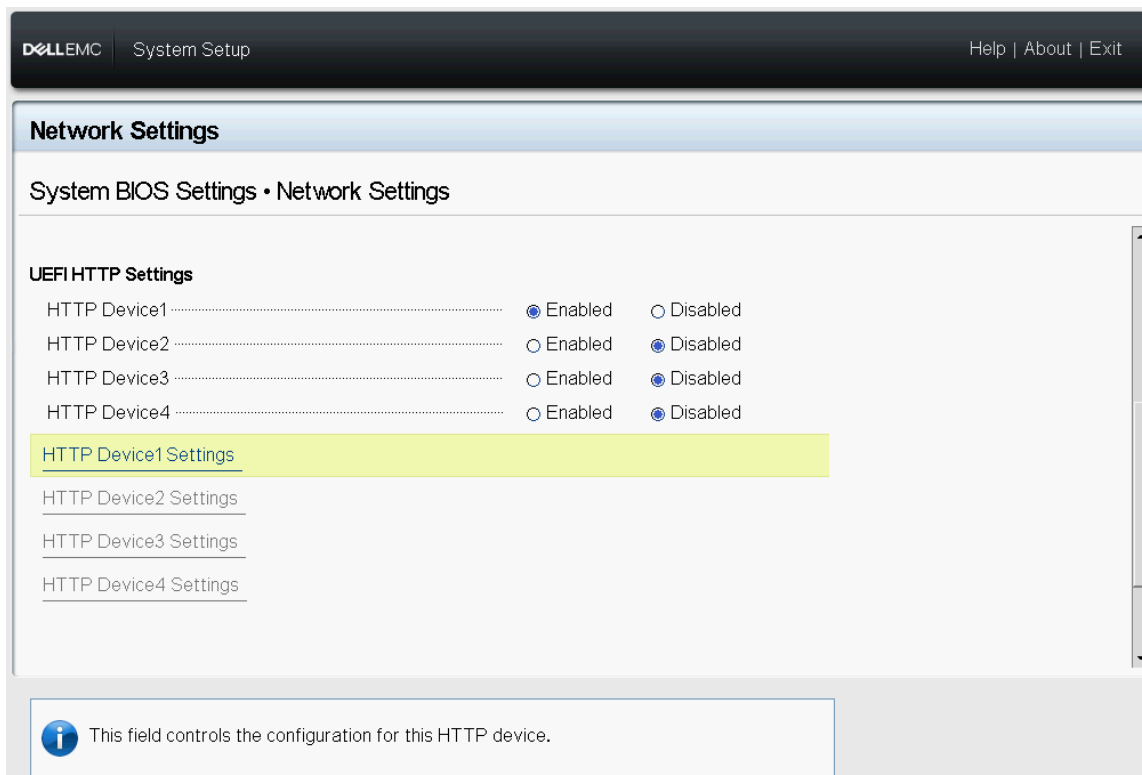


Figure 4 Dell UEFI HTTP settings

5. In **HTTP Device1/2/3/4 Settings**, setup HTTP boot based on network environment. For HTTPS boot, **URI** should start with `https://`. When the URI is obtained through DHCP server, enter the **TLS Authentication Configuration**.

The screenshot shows the 'System Setup' utility with the 'Network Settings' tab selected. The breadcrumb trail is 'System BIOS Settings • Network Settings • HTTP Device1 Settings'. The configuration fields are as follows:

Field	Value / Option
VLAN	☐ Enabled ☒ Disabled
VLAN ID	1
VLAN Priority	0
DHCP	☒ Enabled ☐ Disabled
IP Address	
Subnet Mask	
Gateway	
DNS info via DHCP	☒ Enabled ☐ Disabled
Primary DNS	
Secondary DNS	
URI (will obtain from DHCP server if not specified)	https://

A yellow highlight is under the 'URI' field. Below the settings is a yellow bar with the text 'TLS Authentication Configuration'. At the bottom, an information box states: 'View and/or modify this device's boot TLS authentication configuration.'

Figure 5 HTTP Device 1/2/3/4 Settings

- For current design, TLS mode needs to be **One Way** for HTTPS boot. Enter the **Root Certificate Configuration** to manage certificate.

The screenshot shows the 'System Setup' utility with the 'Network Settings' tab selected. The breadcrumb trail is 'System BIOS Settings • Network Settings • TLS Authentication Configuration'. The configuration is as follows:

Field	Value / Option
TLS Authentication Mode	☐ None ☒ One Way

A yellow highlight is under the 'Root Certificate Configuration' link. At the bottom, an information box states: 'Import, delete or export the root certificate.'

Figure 6 TLS Authentication Configuration

7. On the Root Certificate page, select Import Root Certificate.

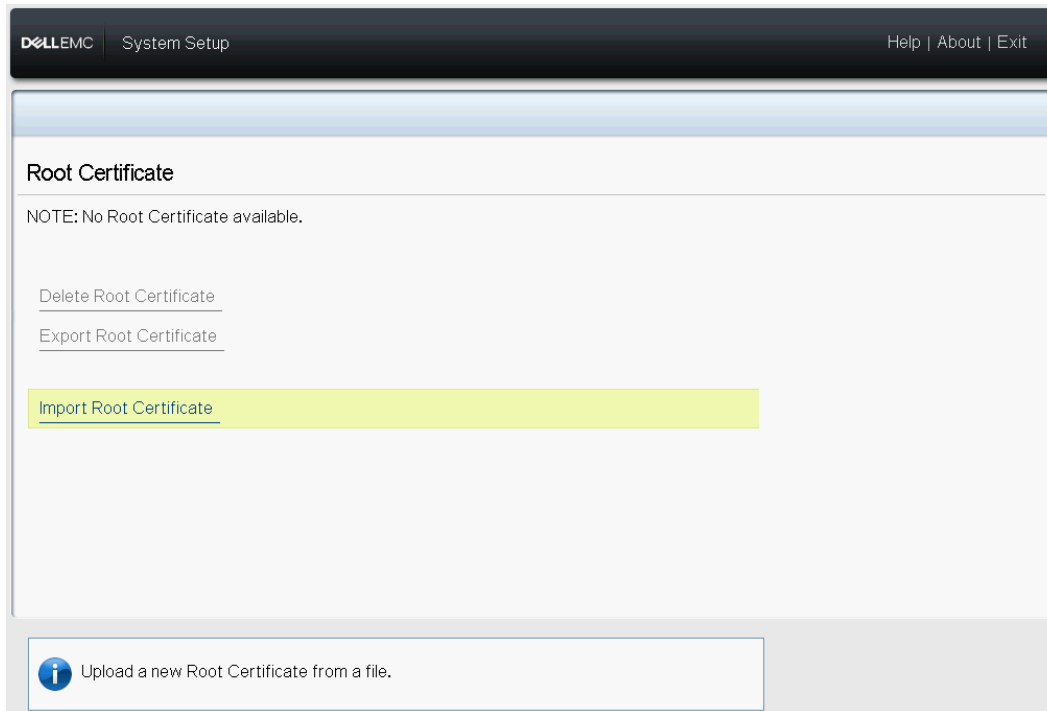


Figure 7 Import Root Certificate page

8. On the **Import Root Certificate** page, select the file system that contains the server root certificate.

Note—DER/PEM are the only supported certificate encoding format.

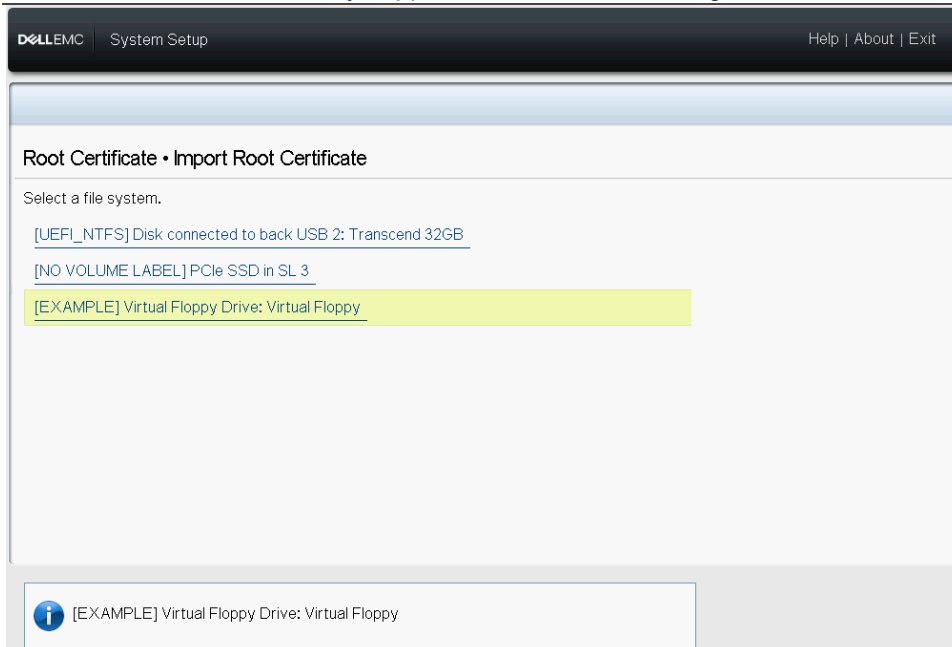


Figure 8 Import Root Certificate

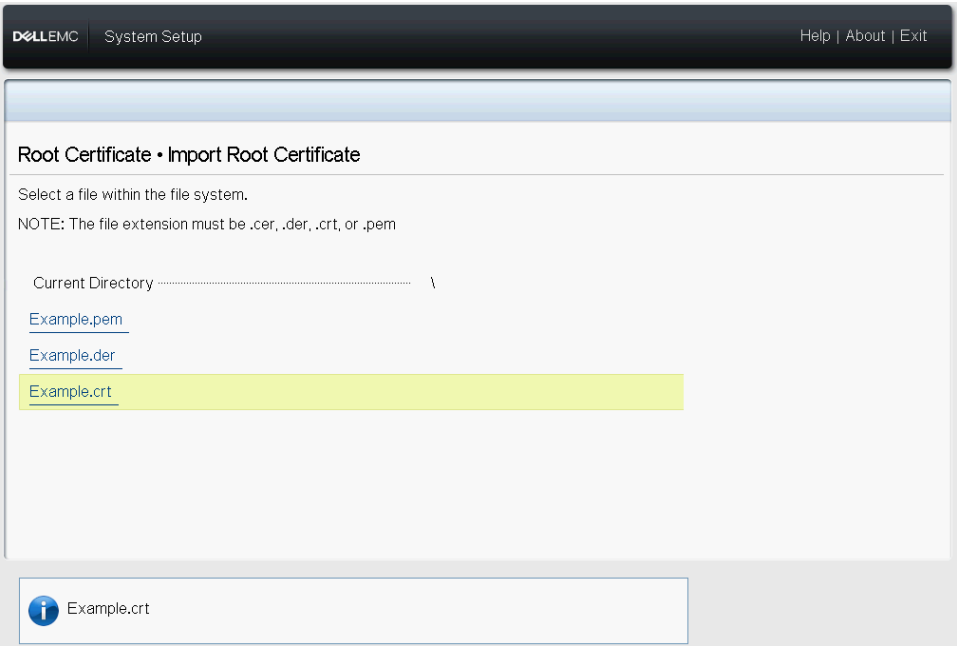


Figure 9 Select cert file in Import Root Certificate

9. Select the certificate of your choice. For example, select **Example.crt** and click **Import**.

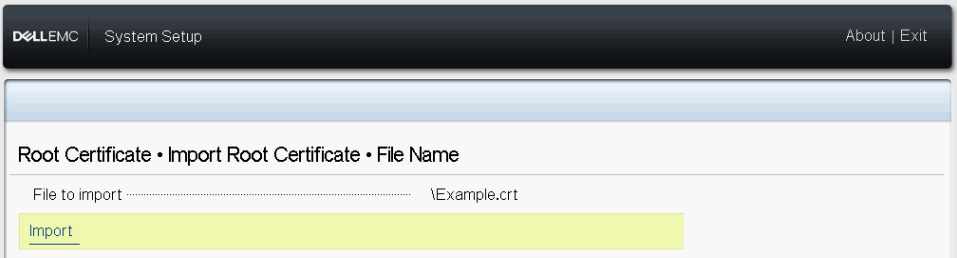


Figure 10 Importing a certificate

After the certificate is imported successfully, system displays the message: The Root Certificate was imported successfully.

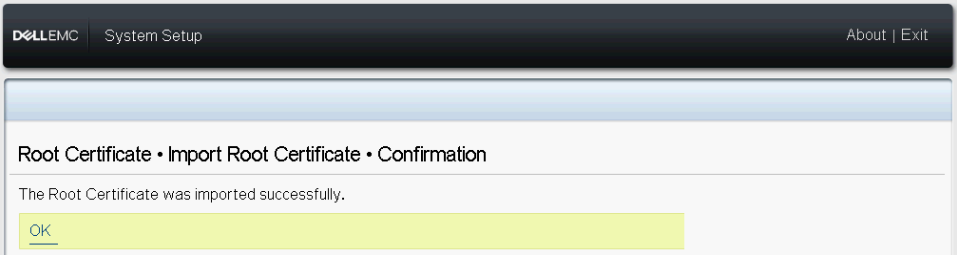


Figure 11 System message to indicate certificate import status

10. Click **OK** to complete the operation and return to the **Root Certificate** page.

3 Detect issues in server configuration and health status

It is critical to detect any issues among the configuration, health status, and change events on a server system. It is also important to detect malicious changes to BIOS, firmware, and Option ROMs within the boot and OS runtime process. Proactive polling must be coupled with the ability to send alerts for all events within the system. Logs must provide complete information about access and changes to the server. Most importantly, the server must extend these capabilities to all components.

3.1 Comprehensive Monitoring via iDRAC

Rather than depending upon OS agents to communicate with managed resources in a server, iDRAC employs a direct side-band path to each device. Dell has leveraged industry standard protocols, such as, MCTP, NC-SI and NVMe-MI to communicate to peripheral devices such as PERC RAID controllers, Ethernet NICs, Fibre Channel HBAs, SAS HBAs, and NVMe drives. This architecture is the result of lengthy, multi-year partnerships with industry-leading vendors to provide agent-free device management in our PowerEdge servers. Configuration and firmware update operations also leverage the powerful UEFI and HII features that Dell and our partners support.

With this capability, iDRAC can monitor the system for configuration events, intrusion events (such as chassis intrusion detection mentioned earlier in this paper), and health changes. Configuration events are linked directly to the identity of the user who initiates the change, for example, GUI user, API user, or console user.

3.1.1 Lifecycle log

The lifecycle log is a collection of events that occur in the server over a period of time. Lifecycle log provides a description of events with timestamps, severity, user ID or source, recommended actions, and other technical information that could come very handy for tracking or alert purposes.

BIOS configuration change is among the various types of information recorded in the Lifecycle Log (LCL):

- Configuration changes on the system hardware components
- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Information about replaced parts
- Information about failed parts
- Event and error message IDs
- Host power-related events
- POST errors
- User login events
- Sensor state change events

4 Recover server to a known state

Server solutions must support recovery to a known, consistent state as a response to a variety of events:

- Newly discovered vulnerabilities.
- Malicious attacks and data tampering.
- Corruption of firmware due to memory failures or improper update procedures.
- Replacement of server components.
- Retiring or repurposing a server.

The following sections describe how to respond to new vulnerabilities and corruption issues, and how to recover the server to its original state if necessary.

4.1 Rapid response to new vulnerabilities

Common Vulnerabilities and Exposures (CVEs) are entries for discovered attack vectors that compromise software and hardware products. Timely responses to newly discovered CVEs are critical to Dell Technologies so that we can swiftly assess the exposure and take appropriate action to protect our customers.

When a new security vulnerability is discovered and reported, a new CVE is issued in response. A typical CVE may come from:

- Open-source components such as OpenSSL.
- Web browsers and other Internet access software.
- A Hardware or firmware component.
- Operating systems and hypervisors.

Dell Technologies works aggressively to quickly respond to new CVEs in PowerEdge servers and provide customers timely information including the following:

- Which products are affected.
- What remediation steps may be taken.
- If needed when updates will be available to address the CVE.

4.2 Recover the BIOS state

The BIOS Recovery feature of the PowerEdge servers enables the rapid recovery when the BIOS image file is corrupted. A special storage area is hidden from run-time software (BIOS, OS, and device firmware). These storage areas contain pristine and verified image files that can be used to recover system functionality.

In some cases, the BIOS image file may be corrupted. It is important to recover the BIOS to a working state. A backup BIOS image file is stored in the iDRAC so it can be used to recover the BIOS image if needed. iDRAC orchestrates the entire end-to-end recovery process.

- Automatic BIOS recovery is initiated by iDRAC Root-of-Trust protection.
- On-demand BIOS recovery can be initiated by you using the RACADM or other management tools.

4.3 Roll back a server firmware

It is recommended to use the latest firmware to ensure that the system is running with the up-to-date security fixes. However, there are cases when a rollback to an earlier version is required. In general, you can roll back the BIOS firmware version from only an existing production version **N** to a previous version **N-1**. You can roll back the firmware to the previously installed version **N-1** using any of the following methods:

- iDRAC web interface.
- Chassis Management Controller (CMC) web interface.
- RACADM Command Line Interface (CLI)—iDRAC and CMC.
- Lifecycle Controller User Interface (UI).
- Lifecycle Controller Remote Services.

You can roll back the firmware even if the upgrade was previously performed using another interface. For example, if the firmware was upgraded using the Lifecycle Controller UI, you can roll back the firmware using an iDRAC web interface. You can perform firmware rollback for multiple devices with one system reboot.

4.4 Restore server configuration after hardware servicing

To remediate the service events is a critical part of any IT operation. The ability to meet recovery time objectives and recovery point objectives has direct implications on the security of the solution. Restoring server configuration and firmware assures that security policies for server operation are automatically met.

PowerEdge servers provide functionality that quickly restores server configuration in the following situations:

- Individual part replacement
- Motherboard replacement (full server profile backup and restore)
- Motherboard replacement (Easy Restore)

4.4.1 Easy Restore (for motherboard replacement)

Motherboard replacements can be time-consuming and affect productivity. iDRAC offers the ability to backup and restore a PowerEdge server configuration and firmware to minimize the effort needed to replace a failed motherboard.

There are two ways the PowerEdge server can backup and restore server configurations:

- PowerEdge servers automatically backup system configuration settings (BIOS, iDRAC, NIC), Service Tag, UEFI diagnostics app, and other licensed data to the flash memory. After you replace the motherboard on your server, **Easy Restore** prompts you to automatically restore this data.
- For a more comprehensive backup, you can back up the system configuration, including the installed firmware image files on various components such as BIOS, RAID, NIC, iDRAC, Lifecycle Controller, and Network Daughter Cards (NDCs) and the configuration settings of those components. The backup operation also includes the hard disk configuration data, motherboard, and replaced parts. The backup creates a single file that you can save to a vFlash SD card or network share (CIFS, NFS, HTTP or HTTPS).

You can restore this profile backup anytime. Dell recommends that you perform the backup operation for every system profile you think you might want to restore at some point.

4.5 System Erase

At the end of a system lifecycle, it must be either retired or repurposed. The goal of the System Erase feature is to erase sensitive data and settings so that no confidential information is unintentionally compromised. It is a utility in Lifecycle Controller that is designed to erase the logs, configuration data, storage data, cache, and any embedded apps.

The following devices, configuration settings, and applications can be erased by using the System Erase feature:

- iDRAC is reset to default
- Lifecycle Controller data
- BIOS
- Embedded diagnostics and OS driver packs
- iSM
- SupportAssist Collection reports

Additionally, the following components can also be erased:

- Hardware Cache (clear PERC NVCache)
- vFlash SD Card (initialize card)

Data on the following components are cryptographically disposed by System Erase:

- Self Encrypting Drives (SED)
- Instant Secure Erase drives (ISE)
- NVM devices (Intel Optane, or NVMe drives) - not available on 1S systems
- Additionally, non-ISE SATA hard drives can be erased using data overwrite.

4.6 Full Power Cycle

In a Full Power Cycle, the server and its components are rebooted. It drains main and auxiliary power from the server and all components. The data in volatile memory is also erased.

A physical Full Power Cycle requires removing the AC power cable, wait for 30 seconds, and then insert the cable back. This poses a challenge when working with a remote system. This feature allows you to do an effective Full Power Cycle from iSM, iDRAC GUI, BIOS, or a script. Full Power Cycle takes effect at the next power cycle.

Full Power Cycle feature eliminates the need for anyone to be physically present in the data center, thus reducing time to troubleshoot. It can eliminate, for example, any malware that is still memory-resident.

5 Summary

The data center security is crucial to the business success and the security of the underlying server infrastructure. Cyberattacks have the potential for extended system and business downtime, lost revenue and customers, legal damages, and tarnished corporate reputation. To protect, detect, and recover from hardware-targeted cyberattacks, security needs to be built into server hardware design, not added on after the fact.

Dell has been a leader in leveraging silicon-based security to secure firmware and protect sensitive user data in PowerEdge servers for the past two generations. The new 15G PowerEdge product line features an enhanced Cyber Resilient Architecture that uses iDRAC Root-of-Trust to further harden server security. Furthermore, 16G PowerEdge BIOS also introduced the following new security features to provide users even higher security level:

- Persistent memory passphrase

In conclusion, the 16G PowerEdge servers, with their industry leading security, form the trusted bedrock of the modern data center upon which customers can securely run their IT operations and workloads.

A Technical support and resources

[Dell.com/support](https://dell.com/support) is focused on meeting customer needs with proven services and support.



Ethernet Network Adapter User Guide for Dell Platforms

User Guide

Broadcom, the pulse logo, NetXtreme, TruTrust, Connecting everything, Avago Technologies, Avago, and the A logo are among the trademarks of Broadcom and/or its affiliates in the United States, certain other countries, and/or the EU.

Copyright © 2020 – 2024 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Table of Contents

1 Regulatory and Safety Approvals	8
1.1 Class A Warning Statements	9
1.2 Class B Warning Statements	10
2 Functional Description	11
3 Network Link and Activity Indication	24
3.1 BCM957412AXXXX	25
3.2 BCM957414AXXXX	26
3.3 BCM957416AXXXX	27
3.4 BCM957414M4140D	28
3.5 BCM957412M4120D	29
3.6 BCM957416M4160	30
3.7 BCM957412N4120DC	31
3.8 BCM957414N4140DC	32
3.9 BCM957416N4160DC	33
3.10 BCM957504-N425D	34
3.11 BCM957504-P425D	35
3.12 BCM957508-P2100D	36
3.13 BCM957508-N2100D	37
3.14 BCM957454-P410SDBT	38
3.15 BCM957454-N410SDBT	39
4 Features	40
4.1 Software and Hardware Features	40
4.2 Virtualization Features	41
4.3 VXLAN	42
4.4 NVGRE/GRE/IP-in-IP/Geneve	42
4.5 Stateless Offloads	43
4.5.1 IP, TCP, UDP Checksum Offload	43
4.5.2 UDP Fragmentation Offload	43
4.5.3 TCP Segmentation Offload and Large Send Offload	43
4.5.4 Generic Receive Offload (GRO) and Large Receive Offload (LRO)	43
4.5.5 Header and Data Split	43
4.5.6 VLAN Tag Insertion and Removal	44
4.5.7 Packet Steering	44
4.5.8 Data Center Bridging	44
4.6 Priority Flow Control	44
4.7 Virtualization Offload	45
4.7.1 Multiqueue Support	45
4.7.2 KVM/Xen Multiqueue	45

4.7.3 Virtual Machine Queue	45
4.7.4 Tunneling Offload	45
4.8 SR-IOV	48
4.8.1 SR-IOV Configuration Support Matrix.....	49
4.9 Network Partitioning (NPAR)	49
4.10 Security (BCM575XX Only)	49
4.11 RDMA over Converged Ethernet – RoCE.....	50
4.12 VMWare Enhanced Networking Stack (ENS).....	50
4.12.1 Features.....	50
4.12.2 ENS Design Choices	50
4.12.3 ENS Performance.....	51
4.12.4 Limitations and Restrictions.....	51
4.13 Supported Combinations	52
4.13.1 NPAR, SR-IOV, and RoCE.....	52
4.13.2 NPAR, SR-IOV, and DPDK	52
4.14 Unsupported Combinations	52
5 Installing the Hardware.....	53
5.1 Safety Precautions.....	53
5.2 System Requirements.....	53
5.2.1 Hardware Requirements.....	53
5.2.2 Memory Requirements	53
5.2.3 Preinstallation Checklist.....	54
5.3 Installing the Adapter	55
5.4 Connecting the Network Cables	55
5.4.1 Validated Cables and Modules	55
6 Software Packages and Installation	57
6.1 Supported Operating Systems.....	57
6.2 Installing the Linux Driver.....	57
6.2.1 Compile and Install from the Source RPM.....	57
6.2.2 Compile and Install Directly from the Source.....	57
6.2.3 Updating Initramfs.....	58
6.2.4 Useful Linux Commands.....	59
6.3 Installing the VMware Driver	60
6.4 Installing the Windows Driver.....	60
7 Updating the Firmware	61
7.1 Dell Update Package	61
7.1.1 Windows	61
7.1.2 Linux	61
8 Link Aggregation.....	62
8.1 Windows	62

8.2 Linux	62
8.2.1 Ephemeral Bonds	62
8.2.2 Bonding Interface Queries	63
9 System-Level Configuration	64
9.1 UEFI HII Menu	64
9.1.1 Main Configuration Page	64
9.1.2 Firmware Image Menu	66
9.1.3 Device Configuration Menu	67
9.1.4 NIC Configuration	70
9.1.5 NIC Partitioning Configuration Menu	71
9.2 Auto-Negotiation Configuration	75
9.2.1 Operational Link Speed	79
9.2.2 Auto-Negotiation Protocol	79
9.2.3 Windows Driver Settings	79
9.2.4 Linux Driver Settings	79
9.2.5 ESXi Driver Settings	80
9.3 Configuring 200G Link Speeds	80
9.3.1 Auto-Negotiation Configuration for 200G	81
9.3.2 Forced 200G Configuration	82
9.3.3 Configuring Dell Switches	82
10 PXE Boot	83
10.1 UEFI Mode	83
10.1.1 iPXE	83
10.1.2 PXE	84
10.1.3 Secure Boot	85
10.2 PXE Server Configuration	86
10.2.1 DHCP Configuration for PXE/iPXE	87
10.2.2 TFTP Configuration	91
10.2.3 HTTP Configuration	93
11 SR-IOV – Configuration and Use Case Examples	94
11.1 Enable SR-IOV in BIOS/UEFI and Device	94
11.2 Linux Use Case Example: SR-IOV Pass-Through to libvirt Virtual Machine	94
11.2.1 Setting MAC Address for the VF	95
11.3 Windows SR-IOV Use Case Example	95
11.4 VMware SR-IOV Use Case Example	96
12 NPAR – Configuration and Use Case Example	97
12.1 Features and Requirements	97
12.2 Limitations	97
12.3 Configuration	98
12.4 Reducing NIC Memory Consumption with NPAR	101

12.5 Advanced NPAR	102
12.5.1 Supported Broadcom Devices	102
12.5.2 Supported Operating Systems.....	102
12.5.3 Supported Features and Limitations.....	103
12.5.4 Supported Hardware Configurations	103
12.5.5 Required Hardware Settings.....	103
12.6 Ethernet Adapter Operations	105
13 Tunneling Configuration Examples.....	106
13.1 Network Diagram	106
13.2 VEB and VEPA Modes	106
13.2.1 VLAN Configuration	106
13.3 VLAN Double Tagging	107
13.4 GRE Tunnelling.....	107
13.5 IP-in-IP Tunnelling	107
13.6 VXLAN – Configuration and Use Case Examples	107
14 RoCE – Configuration and Use Case Examples	108
14.1 Enabling RoCE	108
14.2 Disabling DCBx and LLDPs	109
14.3 Linux Configuration and Use Case Examples	109
14.3.1 Requirements	109
14.3.2 Installing Drivers and the RoCE Library.....	109
14.3.3 Verifying RoCE Functionality	111
14.3.4 RoCE Connectivity Tests	112
14.3.5 RoCE Congestion Control	115
14.4 Windows and Use Case Examples.....	129
14.4.1 SMB Direct.....	129
14.5 VMware ESX and Use Case Examples	138
14.5.1 Limitations.....	138
14.5.2 BNXT RoCE Driver Requirements.....	138
14.5.3 Installation.....	139
14.5.4 Configuring Paravirtualized RDMA Network Adapters	139
14.5.5 Configuring the VM on Linux Guest OS.....	140
15 DCBX – Data Center Bridging	141
15.1 QoS Profile – Default QoS Queue Profile	141
15.2 DCBX Mode – Enable (IEEE only).....	142
15.3 DCBX Willing Bit	142
16 DPDK – Configuration and Use Case Examples	145
16.1 Compiling the Application	145
16.2 Running the Application	145
16.3 Testpmd Runtime Functions	146

- 16.4 Control Functions..... 146
- 16.5 Display Functions..... 146
- 16.6 Configuration Functions 147
- 17 Collecting Support Data 147**
 - 17.1 Introduction 147
 - 17.2 Features 147
 - 17.3 Installing the SOS Reporting Tool Automatically 147
 - 17.4 Installing the SOS Reporting Tool Manually 147
 - 17.4.1 Installing the sosreport from pip..... 147
 - 17.4.2 Installing the bcm_sosreport Package 148
 - 17.4.3 Installing bcm_sosreport Manually 148
 - 17.5 Running the Report..... 148
 - 17.6 Using the Report 148
 - 17.6.1 Viewing the File Contents 148
- Revision History 149**

1 Regulatory and Safety Approvals

The following sections detail the regulatory approvals, safety approvals, and warning statements for Broadcom Ethernet Network Adapters. See the individual data sheets for the product classification and referenced standard dates.

Table 1: Regulatory Approvals

Standard/Country	Certification Type	Compliance
CE/EU	EN 55032 EN 55024/EN 55035 EN 61000-3-2 EN 61000-3-3	CE report and CE sDoC
UKCA/United Kingdom	EN 55032 EN 55024/EN 55035 EN 61000-3-2 EN 61000-3-3	UKCA DoC
FCC/USA	CFR47, Part 15	FCC sDoC and EMC report referencing FCC part 15 regulations
IC/Canada	ICES-003	Report referencing IC standards
ACA/Australia, New Zealand	AS/NZS CISPR 32	sDoC certificate RCM Mark
BSMI/Taiwan	CNS13438, CNS15663	BSMI certificate
MIC/S. Korea	KN 32 and KN 35	Korea certificate MSIP Mark
VCCI/Japan	V-3/VCCI CISPR 32	Copy of VCCI on-line certificate

Table 2: Safety Approvals

Item	Applicable Standard	Approval/Certificate
CE/European Union	IEC 62368-1	CB report and certificate
UL/USA	IEC 62368-1 CTUVus UL	UL report and certificate
CSA/Canada	CSA 22.2 No. 950	CSA report and certificate

1.1 Class A Warning Statements

FCC Warning Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

CAUTION! Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment.

Japan (VCCI) Warning Statement

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI - A

Korea Warning Statement

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

1.2 Class B Warning Statements

FCC Warning Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Japan (VCCI) Warning Statement

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI — B

Korea Warning Statement

이 기기는 가정용 (B급) 전자파적합기기로서
주로 가정에서 사용하는 것을 목적으로 하며,
모든 지역에서 사용할 수 있습니다.

2 Functional Description

Broadcom Ethernet Adapters(BCM9574XX and BCM9575XX) family of Ethernet controllers are highly-integrated, full-featured Ethernet LAN controllers optimized for data center and cloud infrastructures. These controllers support 200G/100G/50G/25G/10G/1G in single, dual, or quad-port configurations. These controllers can support up to sixteen lanes of PCIe Gen 3. The BCM9575XX family additionally supports PCIe Gen 4. An extensive set of stateless offloads and virtualization offloads to enhance packet processing efficiency are included to enable low-overhead, high-speed network communications. These NICs are described in [Table 3](#).

Table 3: Functional Description

Network Interface Card	Description
BCM957412A4120D/BCM957412M4120D/BCM957412N4120DC	
Speed	Dual-Port 10 Gb/s Ethernet
PCIe	Gen 3 x8 ^a
Interface	SFP+ for 10 Gb/s
Device	Broadcom BCM57412 10 Gb/s MAC controller with integrated dual-channel 10 Gb/s SFI transceiver.
NDIS Name	Broadcom NetXtreme-E Series Dual-Port 10Gb SFP+ Ethernet PCIe Adapter
UEFI Name	Broadcom Dual 10Gb SFP+ Ethernet
BCM957414A4141D/BCM957414M4140D/BCM957414N4140DC	
Speed	Dual-Port 25 Gb/s or 10 Gb/s Ethernet
PCIe	Gen 3 x8 ^a
Interface	SFP28 for 25 Gb/s and SFP+ for 10 Gb/s
Device	Broadcom BCM57414 25 Gb/s MAC controller with integrated dual-channel 25 Gb/s SFI transceiver.
NDIS Name	Broadcom NetXtreme- E Series Dual-Port 25 Gb SFP28 Ethernet PCIe Adapter
UEFI Name	Broadcom Dual 25 Gb SFP 28 Ethernet
BCM957504-NGM250D	
Speed	Quad Port 25 Gb/s Ethernet
PCIe	Gen4 x16
Interface	Fabric connector for 25 Gb/s
Device	Broadcom BCM57504 100G Gb/s MAC controller with integrated quad-channel 25 GB/s SFI transceiver.
NDIS Name	Broadcom NetXtreme E-Series Quad-Port 25 Gb Ethernet Network Daughter Card
UEFI Name	Broadcom Advance Quad 25 GB Ethernet
BCM957416A4160D/BCM957416M4160/BCM957416N4160DC	
Speed	Dual-Port 10GBASE-T Ethernet
PCIe	Gen 3 x8 ^a
Interface	RJ-45 for 10 Gb/s
Device	Broadcom BCM57416 10 Gb/s MAC controller with integrated dual-channel 10GBASE-T transceiver.
NDIS Name	Broadcom NetXtreme-E Series Dual-Port 10GBASE-T Ethernet PCIe Adapter
UEFI Name	Broadcom Dual 10GBASE-T Ethernet

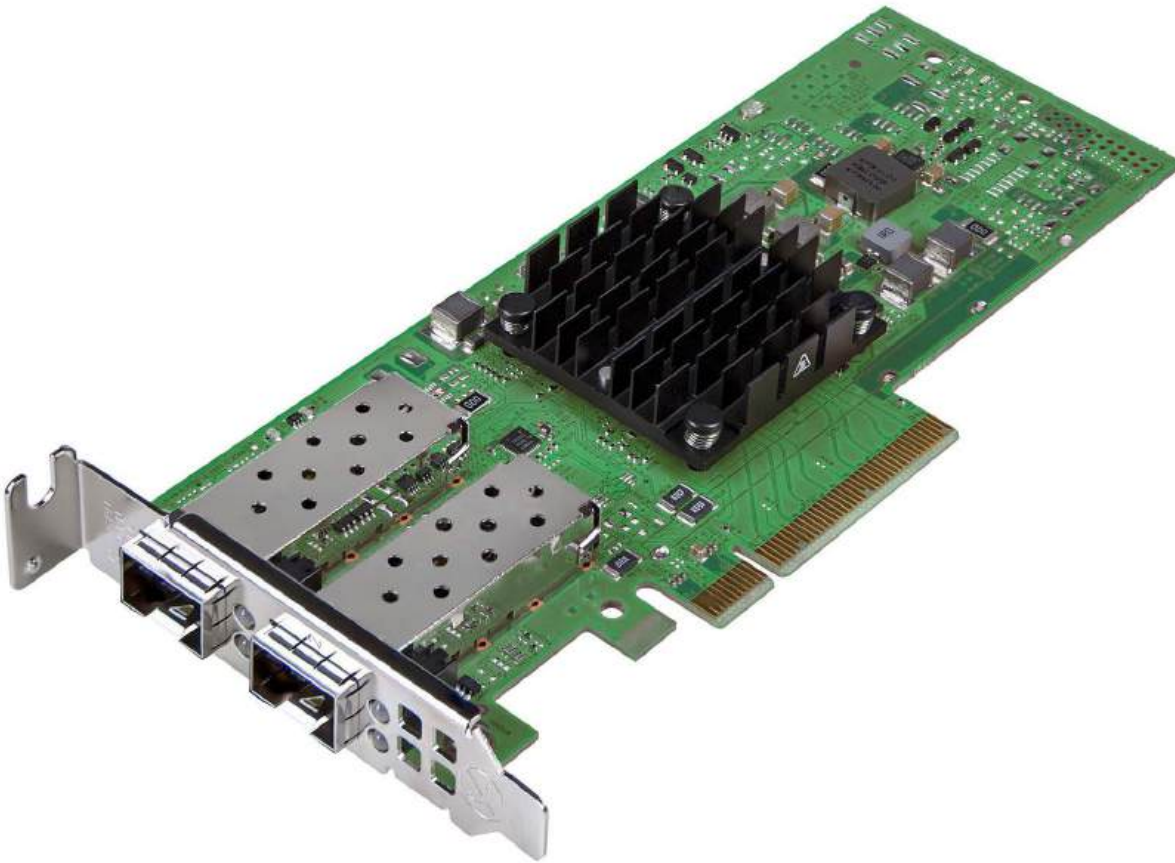
Table 3: Functional Description (Continued)

Network Interface Card	Description
BCM957504-P425D/BCM957504-N425D	
Speed	Quad-Port 25 Gb/s Ethernet
PCIe	Gen4 x16
Interface	SFP28 for 25 Gb/s
Device	Broadcom BCM57504 25G Gb/s MAC controller with integrated quad-channel 25 Gb/s SFI transceiver.
NDIS Name	Broadcom NetXtreme-E P425D BCM57504 4x25G SFP28 PCIe Ethernet
UEFI Name	Broadcom BCM57504 4x25G SFP28 PCIe
BCM957508-P2100D/BCM57508-N2100D	
Speed	Dual-Port 100 Gb/s Ethernet and Single-Port 200 Gb/s Ethernet
PCIe	Gen4 x16
Interface	Two QSFP28 for 100 Gb/s or one QSFP56 for 200 Gb/s
Device	Broadcom BCM57508 100 Gb/s MAC controller with integrated dual-channel 100 Gb/s SFI transceiver.
NDIS Name	Broadcom NetXtreme-E P2100D BCM57508 2x100G QSFP PCIe Ethernet
UEFI Name	BCM57508 2x100G QSFP PCIe
BCM957508-NGM2100D	
Speed	Dual-Port 100 Gb/s Ethernet
PCIe	Gen4 x16
Interface	Fabric connector for 25 Gb/s or 100 Gb/s
Device	Broadcom BCM57508 100 Gb/s MAC controller with integrated dual-channel 100 Gb/s SFI transceiver.
NDIS Name	Broadcom NetXtreme-E NGM2100D BCM57508 2x100G KR Mezz Ethernet
UEFI Name	BCM57508 2x100G KR Mezz
BCM957454-P410SDBT/BCM57545-N410SDBT	
Speed	Quad-Port 10GBASE-T Ethernet
PCIe	Gen 3 x 8
Interface	10GBASE-T
Device	Network adapter with Quad-Port 10GBaseT Ethernet PCIe Gen3 x8
NDIS Name	Broadcom NetXtreme-E P410SDBT BCM57454 4x10G BT PCIE Ethernet
UEFI Name	Broadcom BCM57454 4x10G BT PCIE

- a. The NIC supports PCIe 3, 2, and 1 speeds, however, PCIe Gen 3 is recommended to achieve nominal throughput when 2 ports of 25G links transmit and receive traffic at the same time.

Figure 1: BCM957412A4120D Network Interface Card

NOTE: [Figure 1](#) shows the standard-profile bracket installed. The surface markings of the component may not reflect the product received. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Figure 2: BCM957414A4141D Network Interface Card

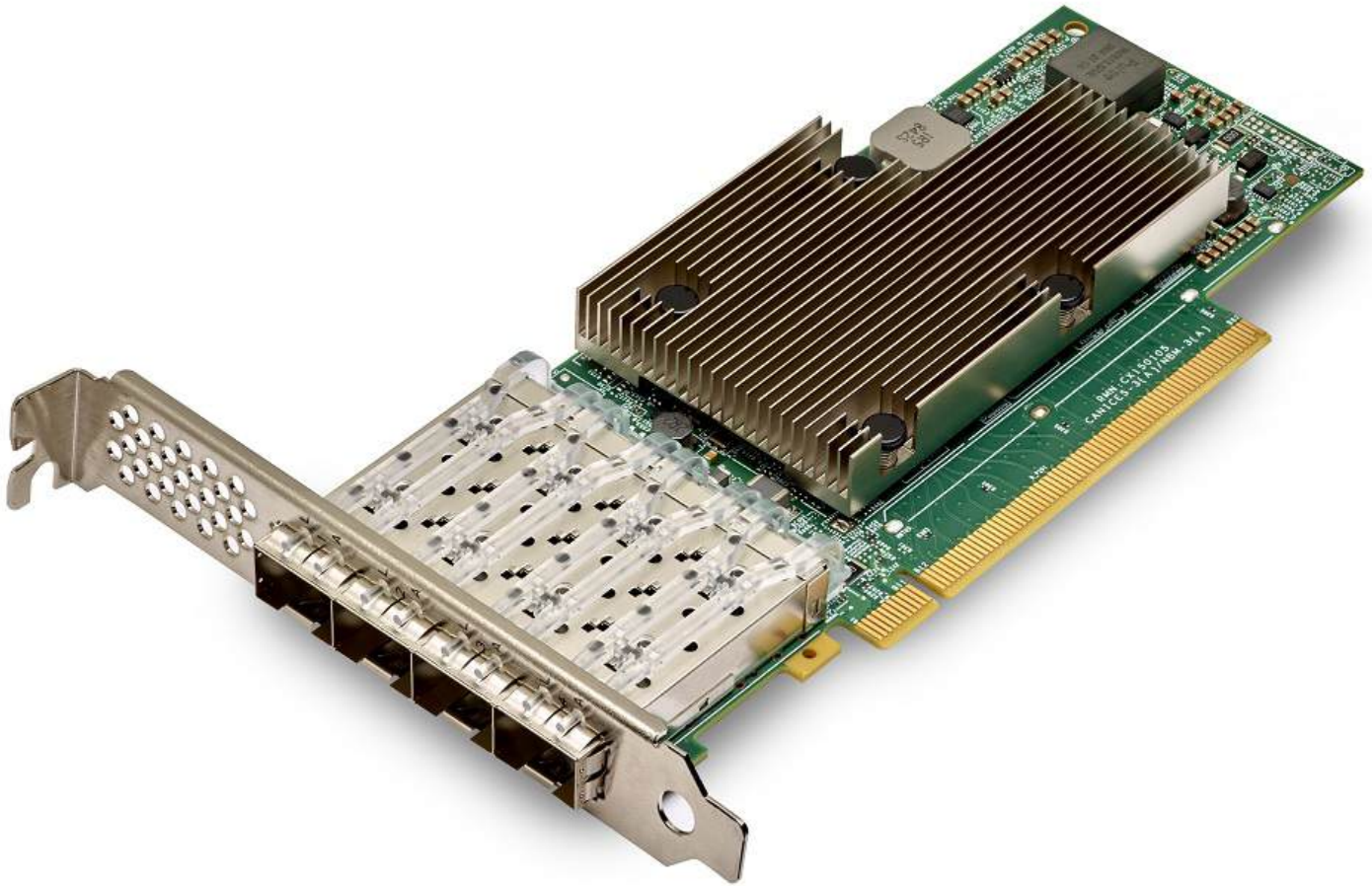
NOTE: [Figure 2](#) shows the low-profile bracket installed. The surface markings of the component may not reflect the product received. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Figure 3: BCM957416A4160D Network Interface Card

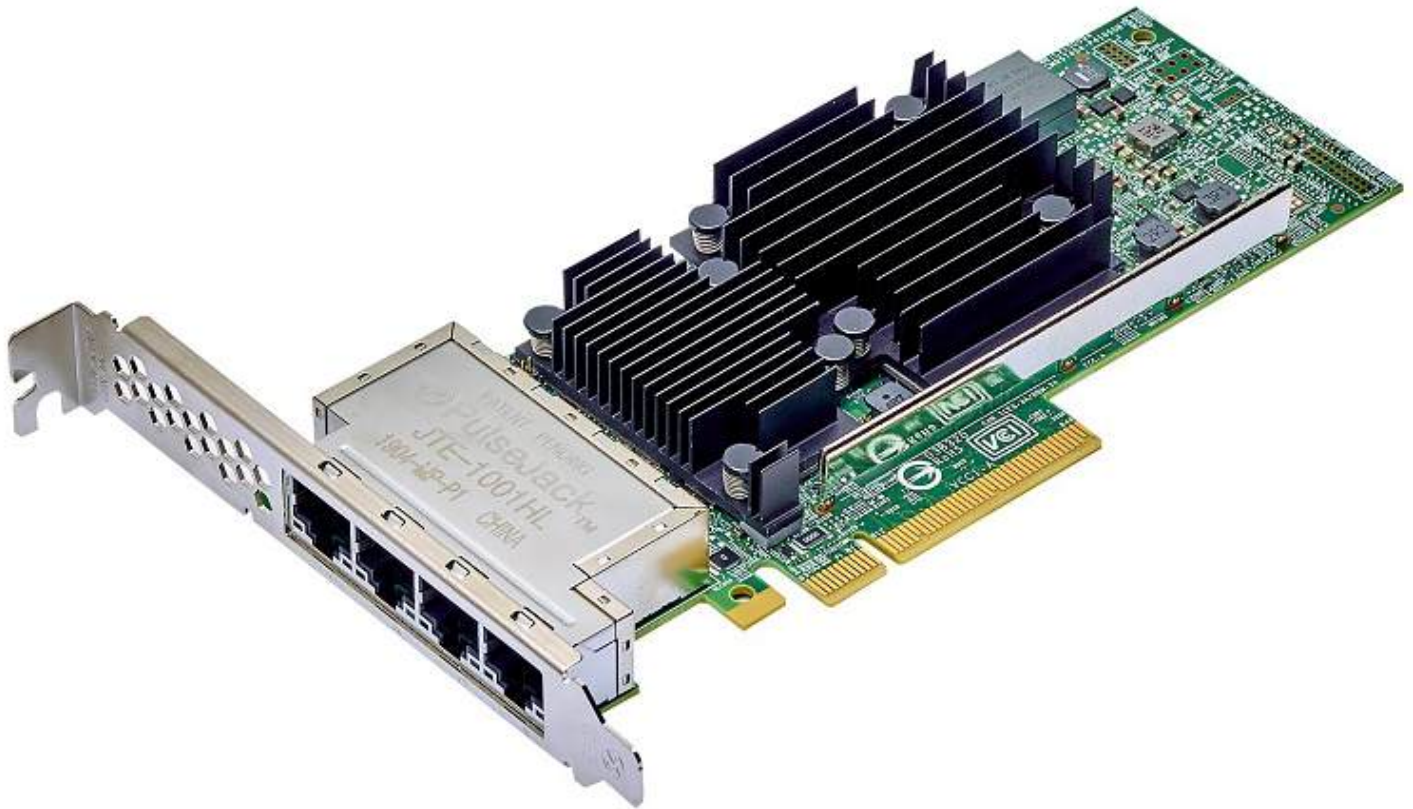
NOTE: [Figure 3](#) shows the low-profile bracket installed. The surface markings of the component may not reflect the product received. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Figure 4: BCM957508-P2100D Network Interface Card

NOTE: The surface markings of the component may not reflect the product received. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Figure 5: BCM957504-P425D Network Interface Card

NOTE: [Figure 3](#) shows the standard-profile bracket installed. The surface markings of the component may not reflect the product received. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Figure 6: BCM957454-P410SDBT Network Interface Card

NOTE: The surface markings of the component may not reflect the product received. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

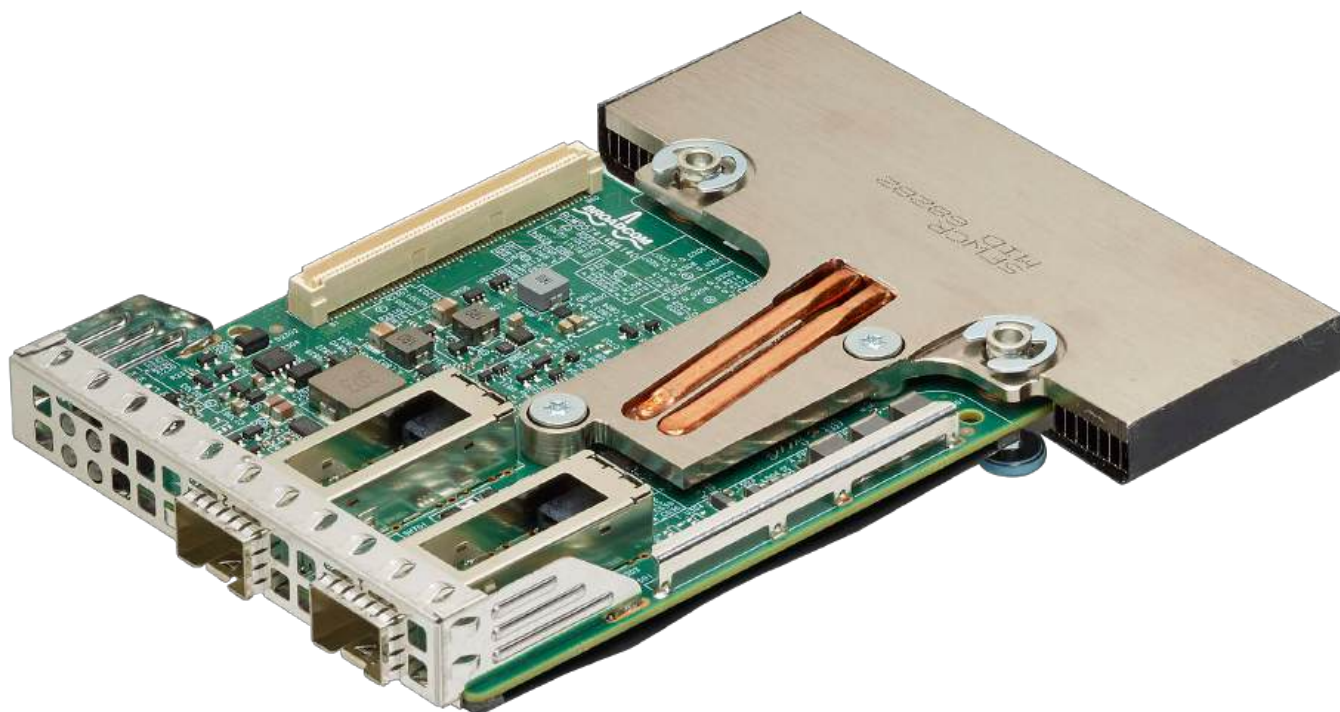
Figure 7: BCM957414M4140D Network Daughtercard (rNDC)**Figure 8: BCM957412M4120D Network Daughtercard (rNDC)**

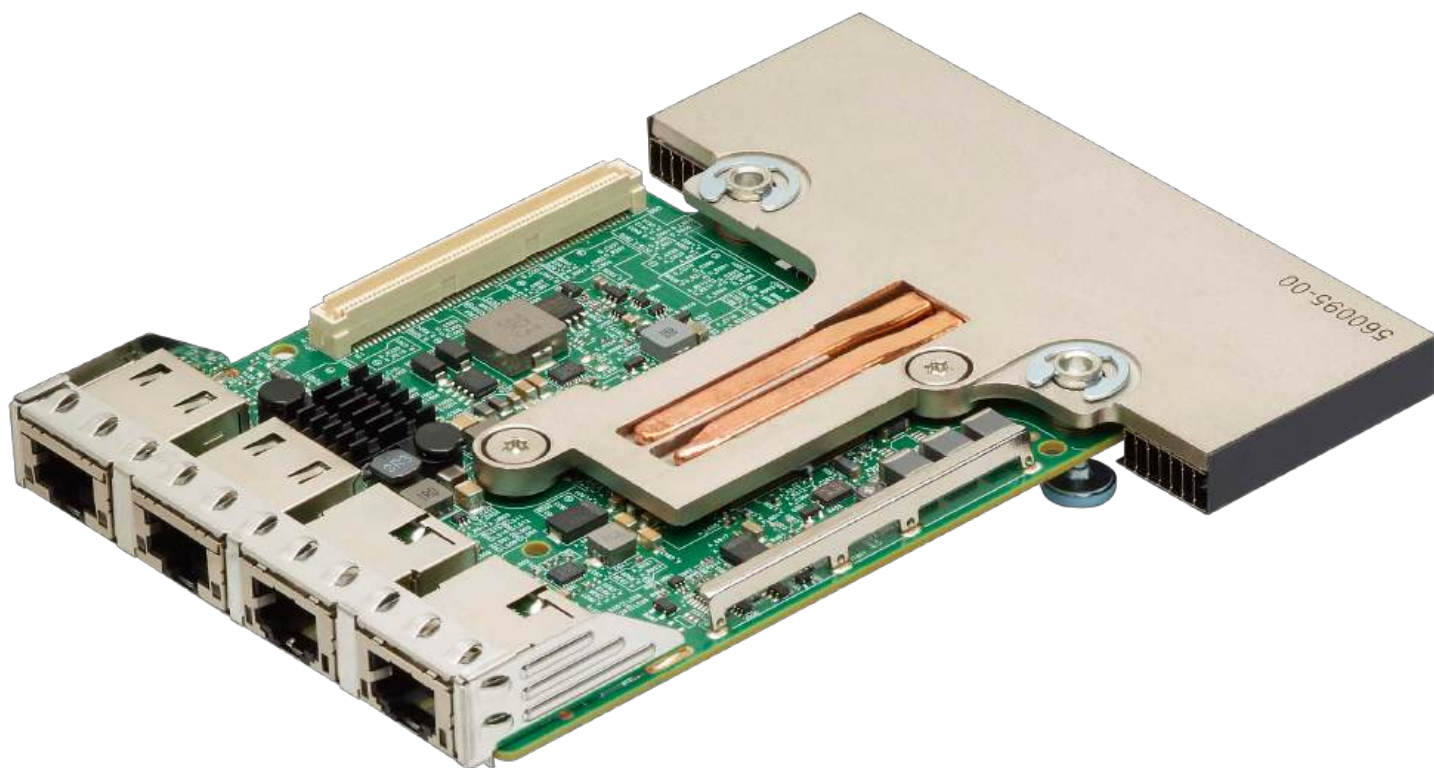
Figure 9: BCM95416M4160 Network Daughtercard (rNDC)**Figure 10: BCM957412N4120 OCP 3.0 SFF Card**

Figure 11: BCM957414N4140 OCP 3.0 SFF Card**Figure 12: BCM957416N4160 OCP 3.0 SFF Card**

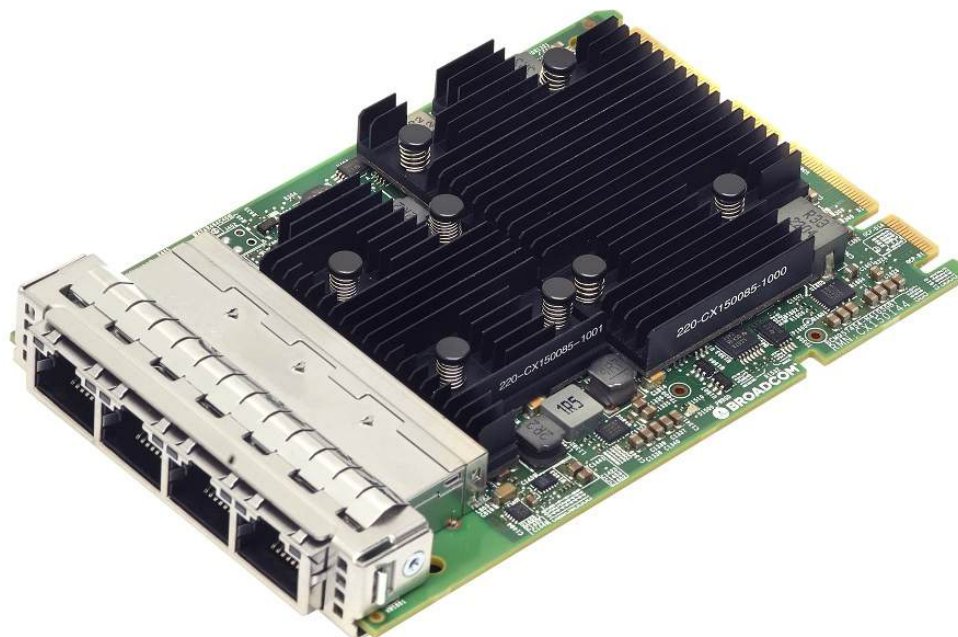
Figure 13: BCM957504-N425D OCP 3.0 SFF Card**Figure 14: BCM957454-N410SDBT OCP 3.0 SFF Card**

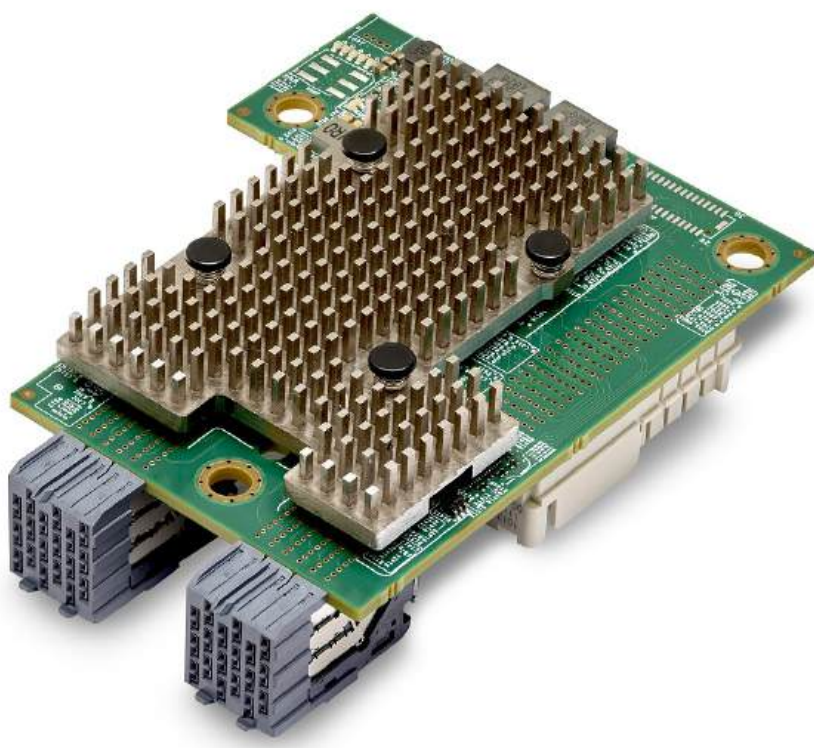
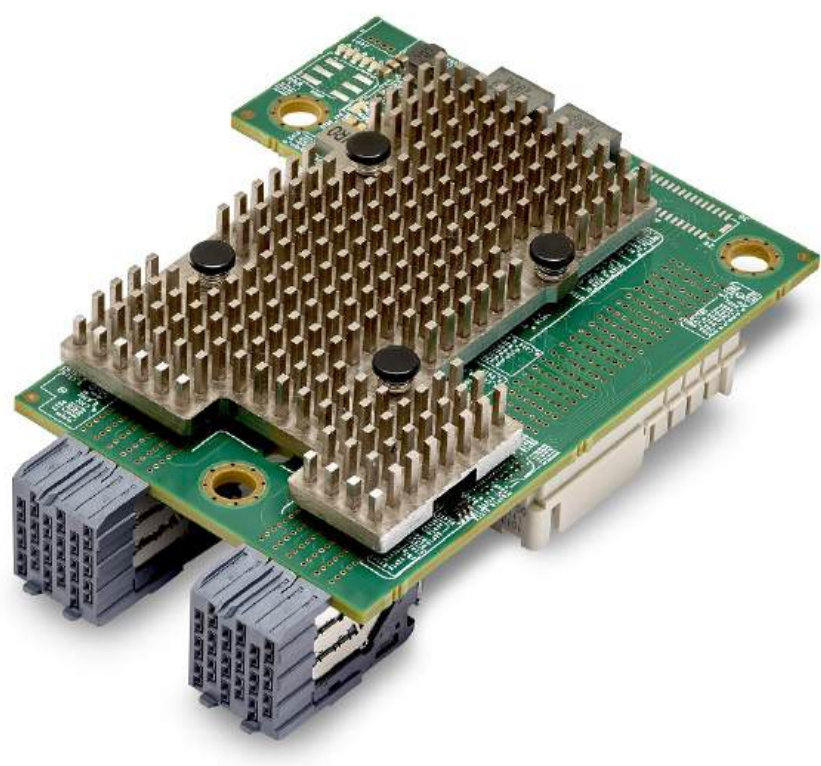
Figure 15: BCM957508-N2100D OCP 3.0 SFF Card**Figure 16: BCM957504-NGM250D Mezzanine Card**

Figure 17: BCM957508-NGM2100D Mezzanine Card



3 Network Link and Activity Indication

Ethernet connections, the state of the network link, and activity are indicated by the LEDs on the rear connector as shown in [Table 4](#).

See the individual board data sheets for specific media design.

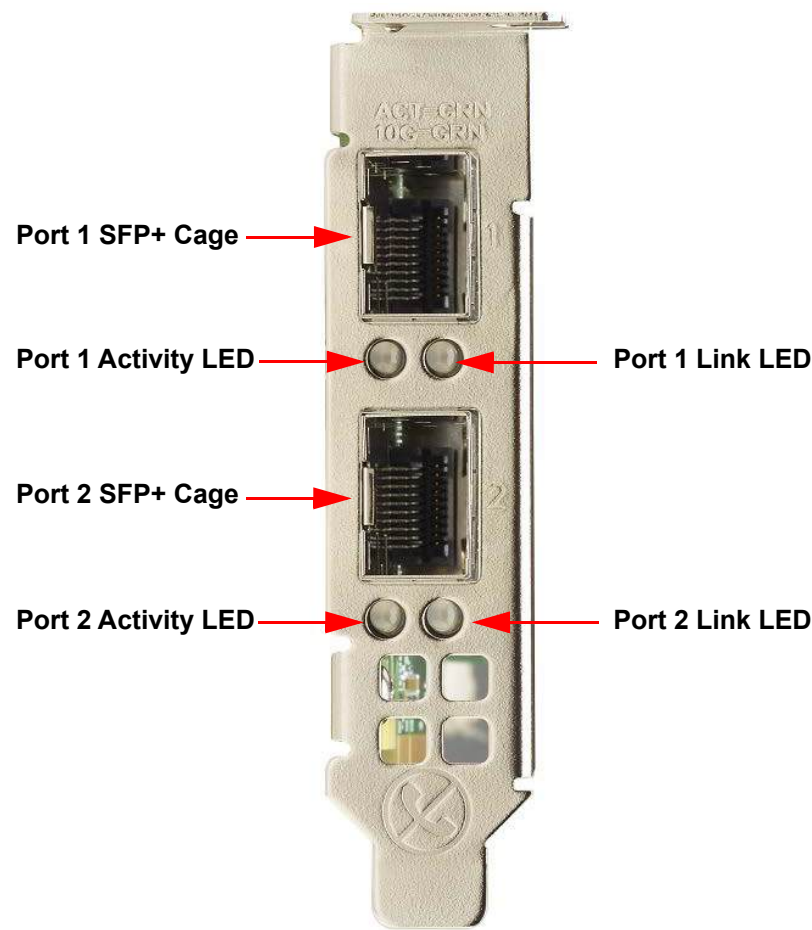
Table 4: Network Link and Activity Indicated by Port LEDs

Port LED	LED Appearance	Network State
Link LED	Off	No link (cable disconnected)
	Continuously illuminated	Link
Activity LED	Off	No network activity
	Blinking	Network activity

3.1 BCM957412AXXXX

The SFP+ port has two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 18](#) and described in [Table 5](#).

Figure 18: BCM957412AXXXX Activity and Link LED Locations



NOTE: [Figure 18](#) shows the low-profile bracket installed. The surface markings of the component may not reflect the product upon receipt. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

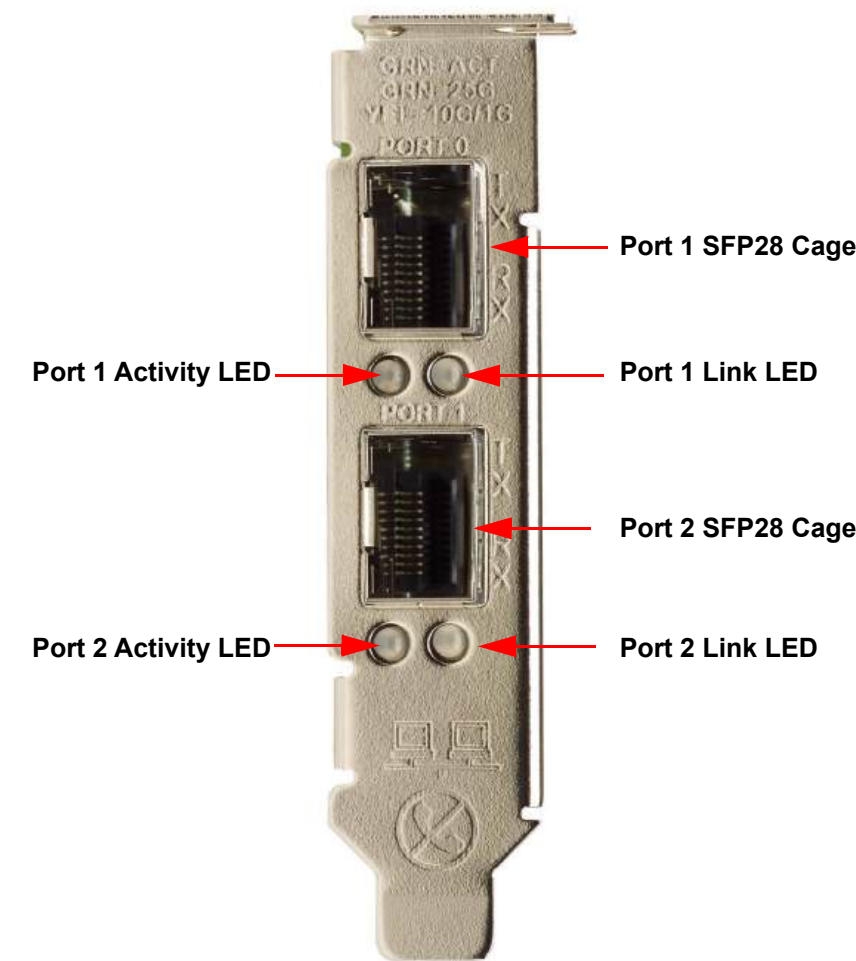
Table 5: BCM957412AXXXX Activity and Link LED Locations

LED Type	Color/Behavior	Note
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 10 Gb/s
	Yellow	Linked at 1 Gb/s

3.2 BCM957414AXXXX

The SFP28 port has two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 19](#) and described in [Table 6](#).

Figure 19: BCM957414AXXXX Activity and Link LED Locations



NOTE: [Figure 19](#) shows the low-profile bracket installed. The surface markings of the component may not reflect the product upon receipt. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Table 6: BCM957414AXXXX Activity and Link LED Locations

LED Type	Color/Behavior	Note
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 25 Gb/s
	Yellow	Linked at 10 Gb/s

3.3 BCM957416AXXXX

Each Ethernet interface has a link LED to indicate Link status and an activity LED to indicate data traffic. The LEDs are shown in [Figure 20](#) and described in [Table 7](#).

Figure 20: BCM957416AXXXX Activity and Link LED Locations

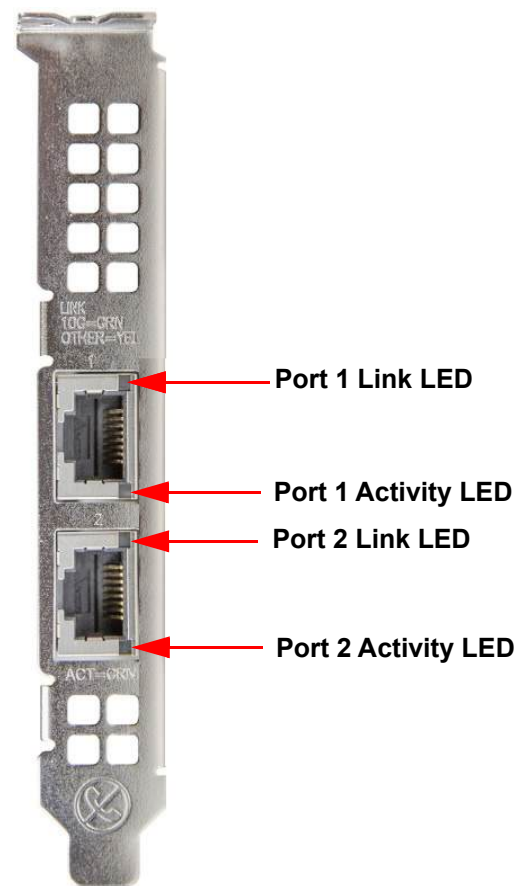


Table 7: BCM957416AXXXX Activity and Link LED Locations

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 10 Gb/s
	Amber	Linked at 1 Gb/s

3.4 BCM957414M4140D

The SFP28 port has two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 21](#) and described in [Table 8](#).

Figure 21: BCM957414M4140D Network Daughtercard (rNDC) Activity and Link LED Locations

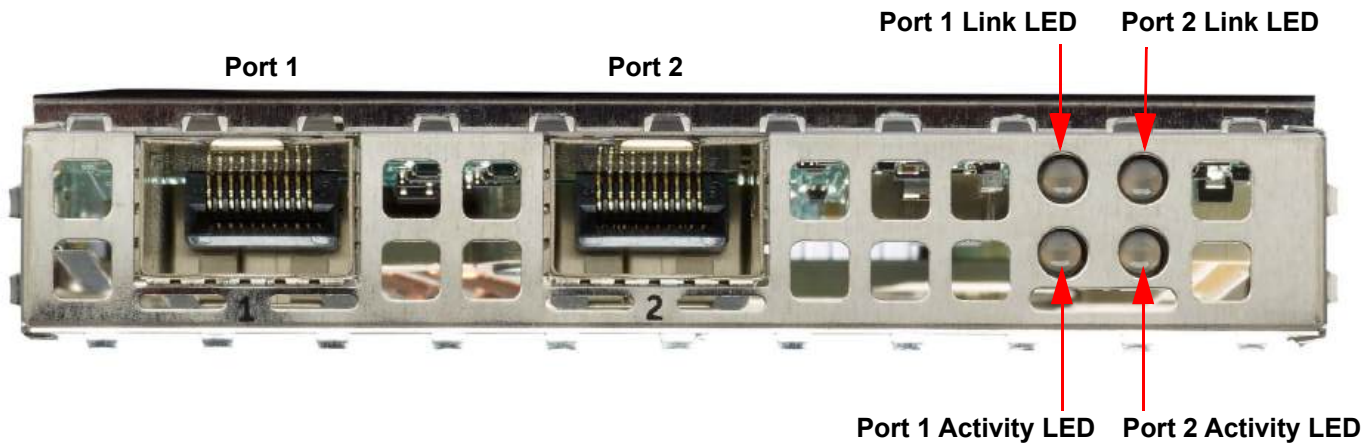


Table 8: BCM957414M4140D Network Daughtercard (rNDC) Activity and Link LED Locations

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 25 Gb/s
	Yellow	Linked at 10 Gb/s

NOTE: When a XTY28 transceiver is connected to a 25 Gb/s controller and if the link establishes at 1 Gb/s, the link LED is off and the activity LED blinks.

3.5 BCM957412M4120D

This rNDC has SFP+ and RJ-45 ports, each with two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 22](#) and described in [Table 9](#) (Ports 1 and 2)/[Table 10](#) (Ports 3 and 4).

Figure 22: BCM957412M4120D Network Daughtercard (rNDC) Activity and Link LED Locations

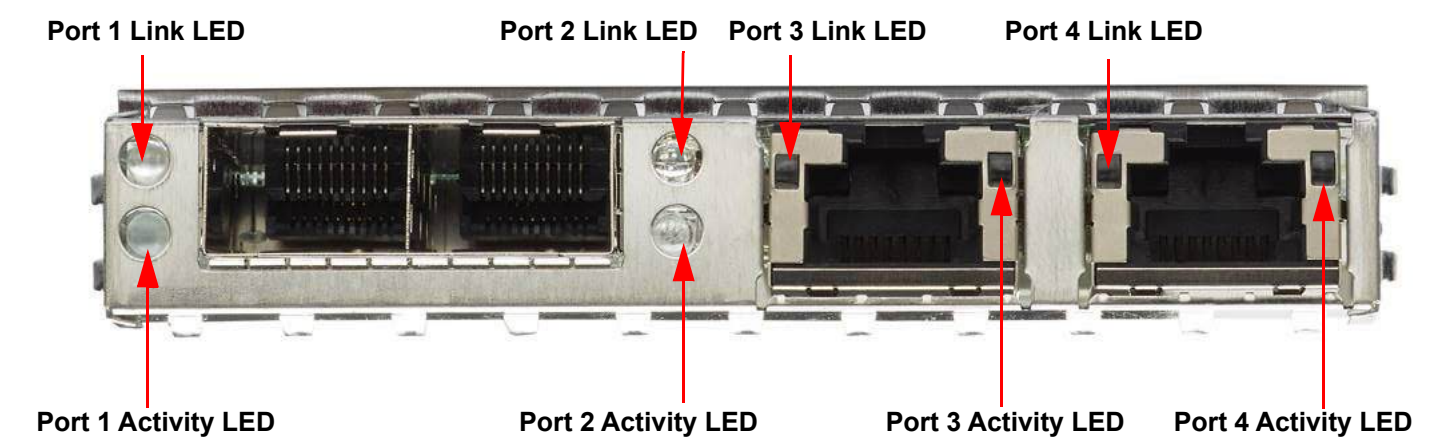


Table 9: BCM957412M4120D Network Daughtercard (rNDC) Activity and Link LED Locations SFP+ Port 1 and 2

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 10 Gb/s

NOTE: When a XTY28 transceiver is connected to a 10 Gb/s controller and if the link establishes at 1 Gb/s, the link LED is off and the activity LED blinks.

Table 10: 1000BASE-T Port 3 and 4

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 1 Gb/s
	Amber	Linked at 10/100 Mb/s

3.6 BCM957416M4160

This rNDC has 10GBaseT and 1000BaseT RJ-45 ports, each with two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 23](#) and described in [Table 11](#).

Figure 23: BCM957416M4160 Network Daughtercard (rNDC) Activity and Link LED Locations

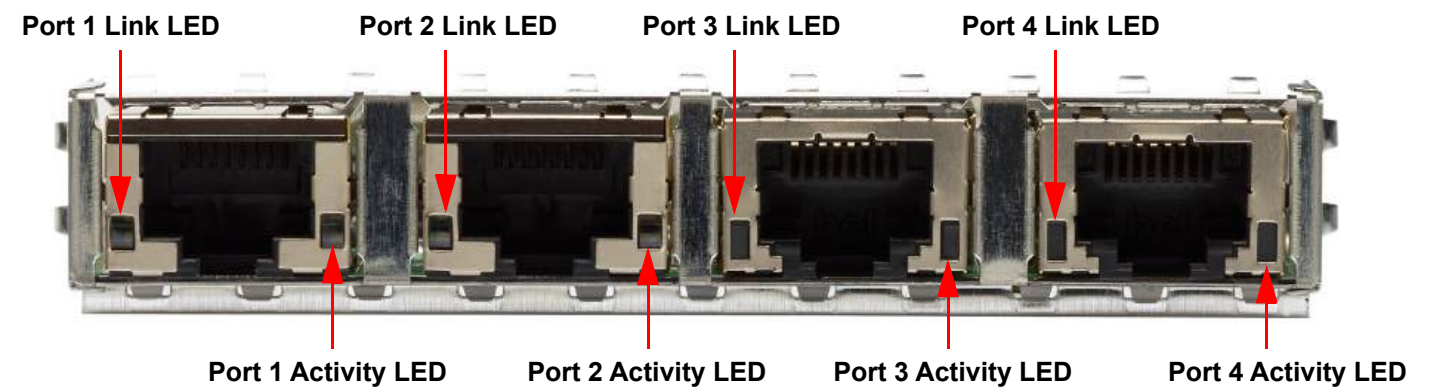


Table 11: BCM957416M4160 Network Daughtercard (rNDC) Activity and Link LED Locations 10GBASET Port 1 and 2

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 10 Gb/s
	Amber	Linked at 1 Gb/s

3.7 BCM957412N4120DC

The SFP+ port supports two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 23](#) and described in [Table 12](#). Its locations and form factors conform to the OCP 3.0 Design Specification.

Figure 24: BCM957412N4120DC Network Adapter Activity and Link LED Locations



Table 12: BCM957412N4120DC Network Adapter Activity and Link LED Locations

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 10 Gb/s

NOTE: When a XTY28 transceiver is connected to a 10 Gb/s controller and if the link establishes at 1 Gb/s, the link LED is off and the activity LED blinks.

3.8 BCM957414N4140DC

The SFP+ port supports two LEDs to indicate traffic activities and link speed. The LEDs are shown in [Figure 25](#) and described in [Table 13](#). Its locations and form factors conform to the OCP 3.0 Design Specification.

Figure 25: BCM957414N4140DC Network Adapter Activity and Link LED Locations



Table 13: BCM957414N4140DC Network Adapter Activity and Link LED Locations

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 25 Gb/s
	Amber	Linked at 10 Gb/s

NOTE: When a XTY28 transceiver is connected to a 25 Gb/s controller and if the link establishes at 1 Gb/s, the link LED is off and the activity LED blinks.

3.9 BCM957416N4160DC

Each Ethernet interface has a link LED to indicate Link status and an activity LED to indicate data traffic. The LEDs are shown in [Figure 26](#) and described in [Table 14](#). Its locations and form factors conform to the OCP 3.0 Design Specification.

Figure 26: BCM957416N4160DC Network Adapter Activity and Link LED Locations

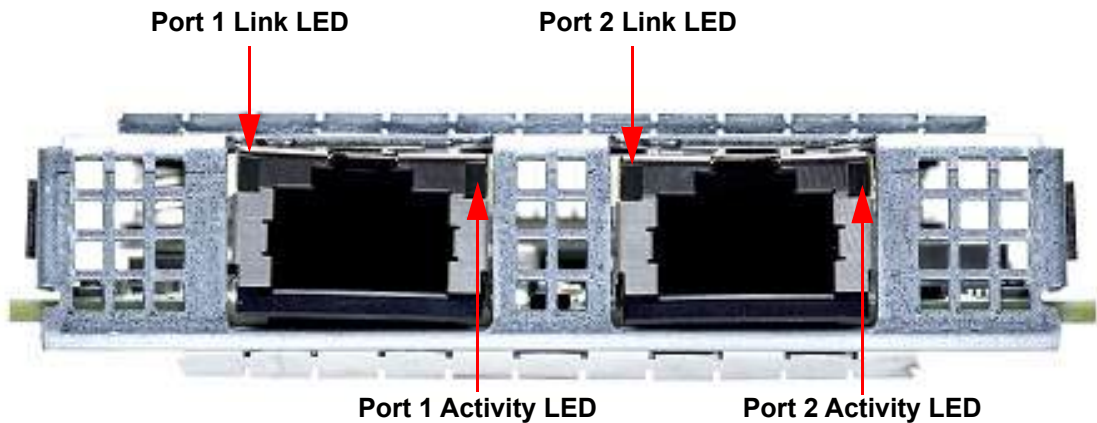


Table 14: BCM957416N4160DC Network Adapter Activity and Link LED Locations

LED Type	Color/Behavior	Notes
Activity	Off	No Activity
	Green blinking	Traffic Flowing Activity
Link	Off	No Link
	Green	Linked at 10 Gb/s
	Amber	Linked at 1 Gb/s

3.10 BCM957504-N425D

The SFP28 port supports two LEDs to indicate traffic activities and link speed. The LEDs are visible as shown in [Figure 27](#). Its locations and form factors conform to the OCP 3.0 Design Specification. The LED functionality is described in [Table 15](#).

Figure 27: Activity and Link LED Locations

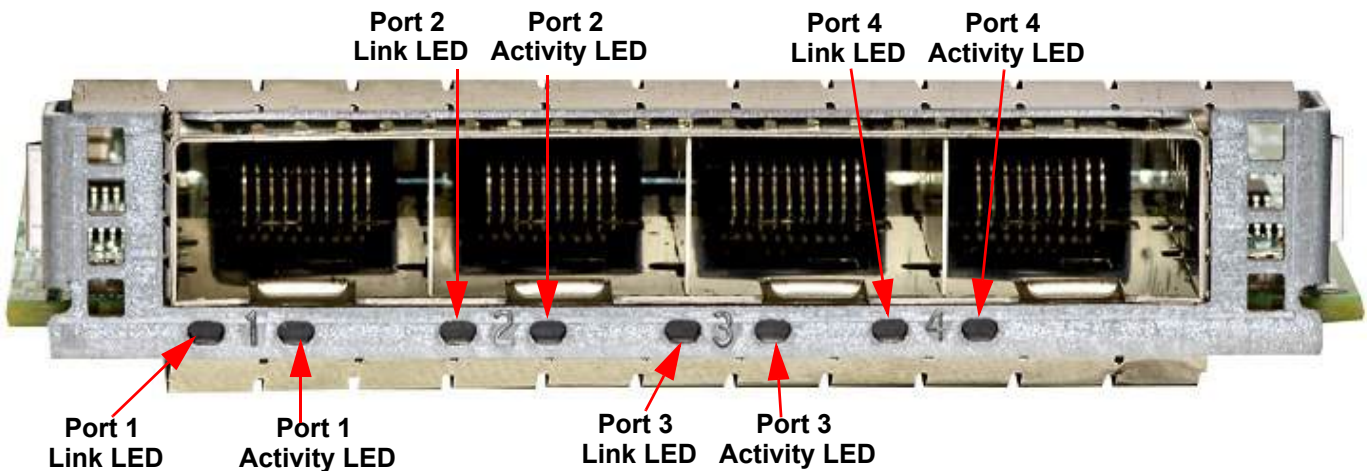


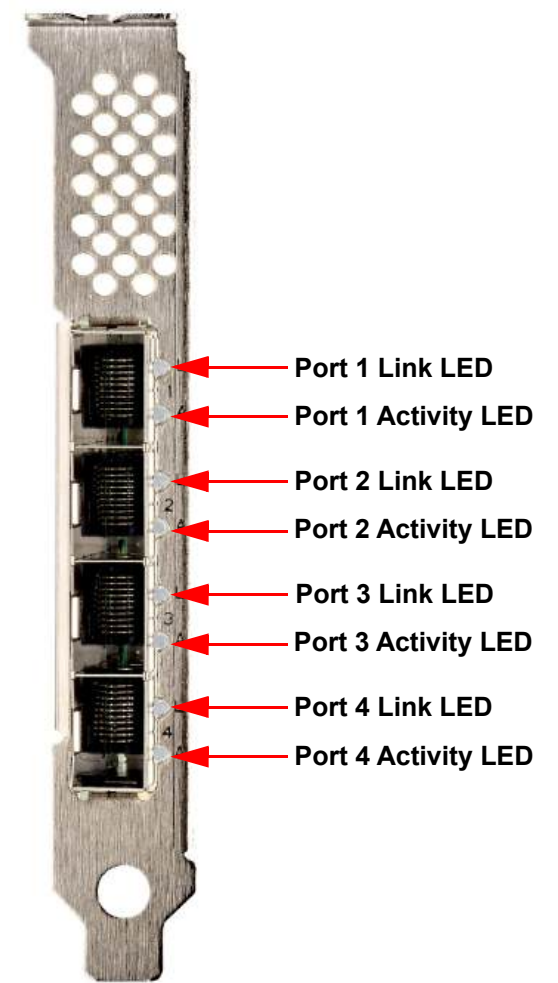
Table 15: BCM957504-N425D LED Functions

LED Type	Color/Behavior	Note
Activity	Off	No Link
	Green (blinking)	Link up (traffic flowing)
Link	Off	No Link
	Green	Linked at 25 Gb/s
	Amber	Linked at lower speed

3.11 BCM957504-P425D

The SFP28 port supports two LEDs to indicate traffic activities and link speed. The LEDs are visible through the cutout on the bracket as shown in [Figure 28](#).

Figure 28: Activity and Link LED Locations



NOTE: [Figure 28](#) shows the standard-profile bracket installed. The surface markings of the component may not reflect the product upon receipt. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

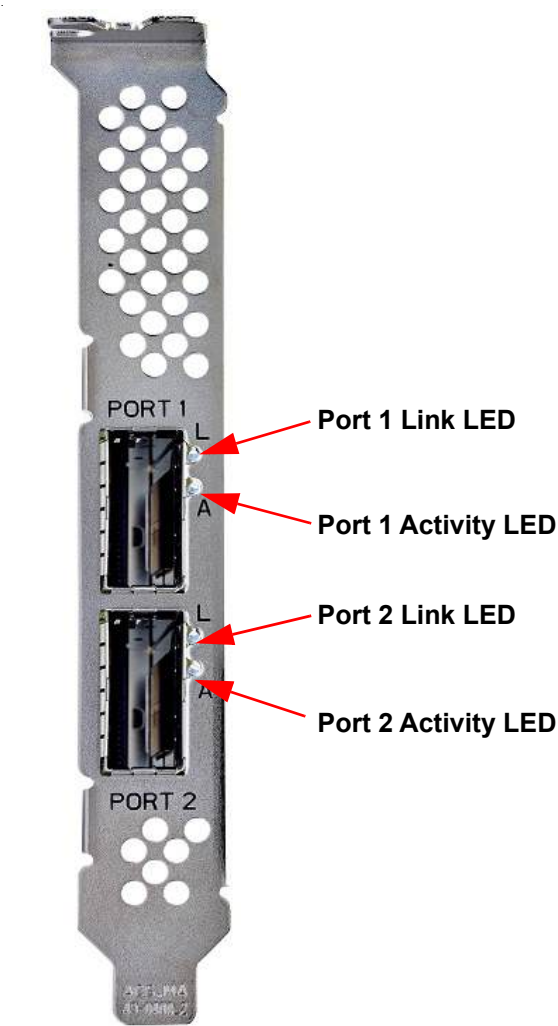
Table 16: LED Functions

LED Type	Color/Behavior	Note
Activity	Off	No Link
	Green (blinking)	Link up (traffic flowing)
Link	Off	No Link
	Green	Linked at 25 Gb/s
	Amber	Linked at lower speed

3.12 BCM957508-P2100D

The QSFP28/QSFP56 port supports two LEDs to indicate traffic activities and link speed. The LEDs are visible through the cutout on the bracket as shown in [Figure 29](#). The LED functionality is described in [Table 17](#).

Figure 29: Activity and Link LED Locations



NOTE: [Figure 29](#) shows the standard-profile bracket installed. The surface markings of the component may not reflect the product upon receipt. Broadcom reserves the right to change any component on the printed circuit board with the same functionality.

Table 17: LED Functions

LED Type	Color/Behavior	Note
Activity	Off	No Link
	Green (blinking)	Link up (traffic flowing)
Link	Off	No Link
	Green	Linked at 100 Gb/s and 200 Gb/s
	Amber	Linked at lower speed

3.13 BCM957508-N2100D

The QSFP28/QSFP56 port supports two LEDs to indicate traffic activities and link speed. The LEDs are visible as shown in [Figure 30](#). Its locations and form factors conform to the OCP 3.0 Design Specification.

Figure 30: Activity and Link LED Locations

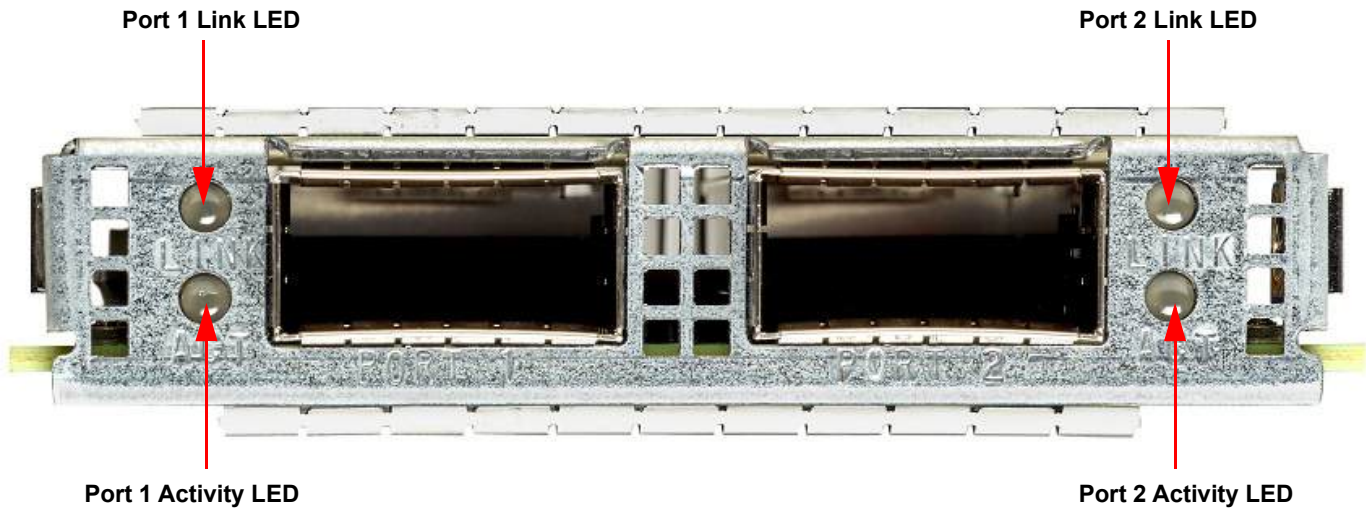


Table 18: LED Functions

LED Type	Color/Behavior	Note
Activity	Off	No Activity
	Green (blinking)	Link up (traffic flowing)
Link	Off	No Link
	Green	Linked at 100 Gb/s and 200 Gb/s
	Amber	Linked at lower speed

3.14 BCM957454-P410SDBT

The 10GBASE-T port supports two LEDs to indicate traffic activities and link speed. The LEDs are visible through the cutout on the bracket as shown in [Figure 31](#). The LED functionality is described in [Table 19](#).

Figure 31: Activity and Link LED Locations

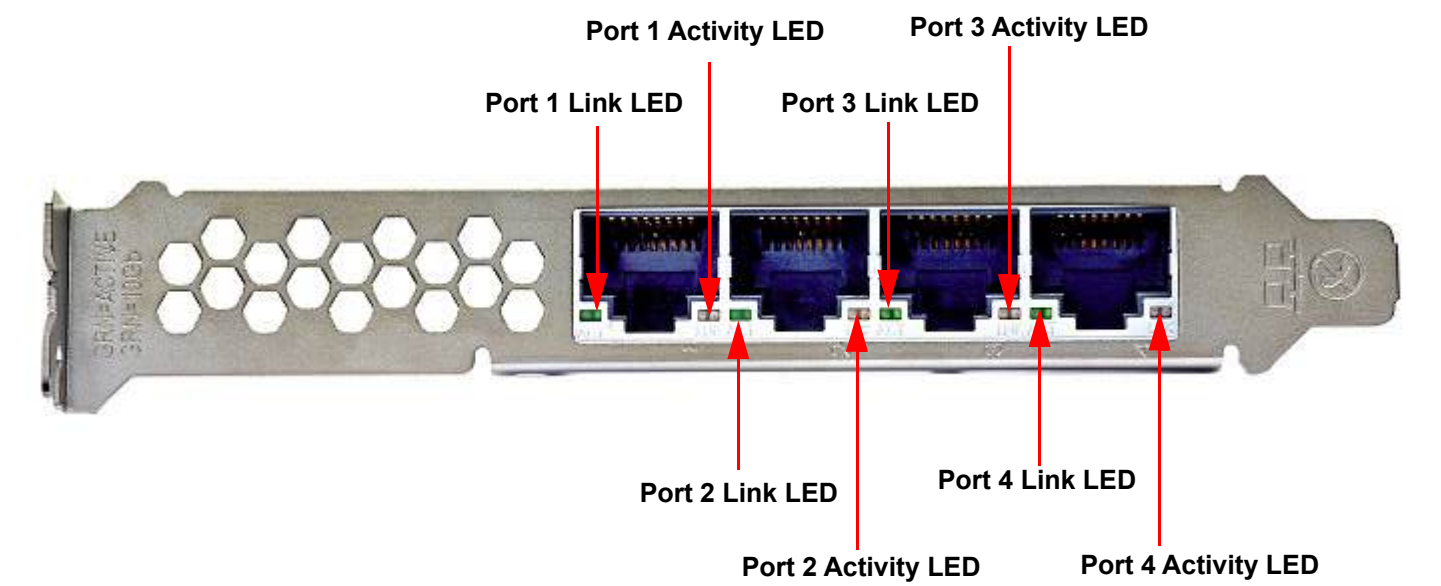


Table 19: LED Functions

NVRAM Manufacturer	Device	Mbit
Activity	Off	No activity
	Green blinking	Traffic flowing activity
Link	Off	No link
	Green	Linked at 10 Gb/s
	Orange	Linked at 1 Gb/s

3.15 BCM957454-N410SDBT

Each of the four RJ-45 ports supports an LED for traffic activity and a dual-color (G/O) LED for link speed. The LEDs are integrated into the RJ-45 connector as shown in [Figure 31](#). Their locations and form factors conform to the OCP NIC 3.0 design specification.

Figure 32: Activity and Link LED Locations

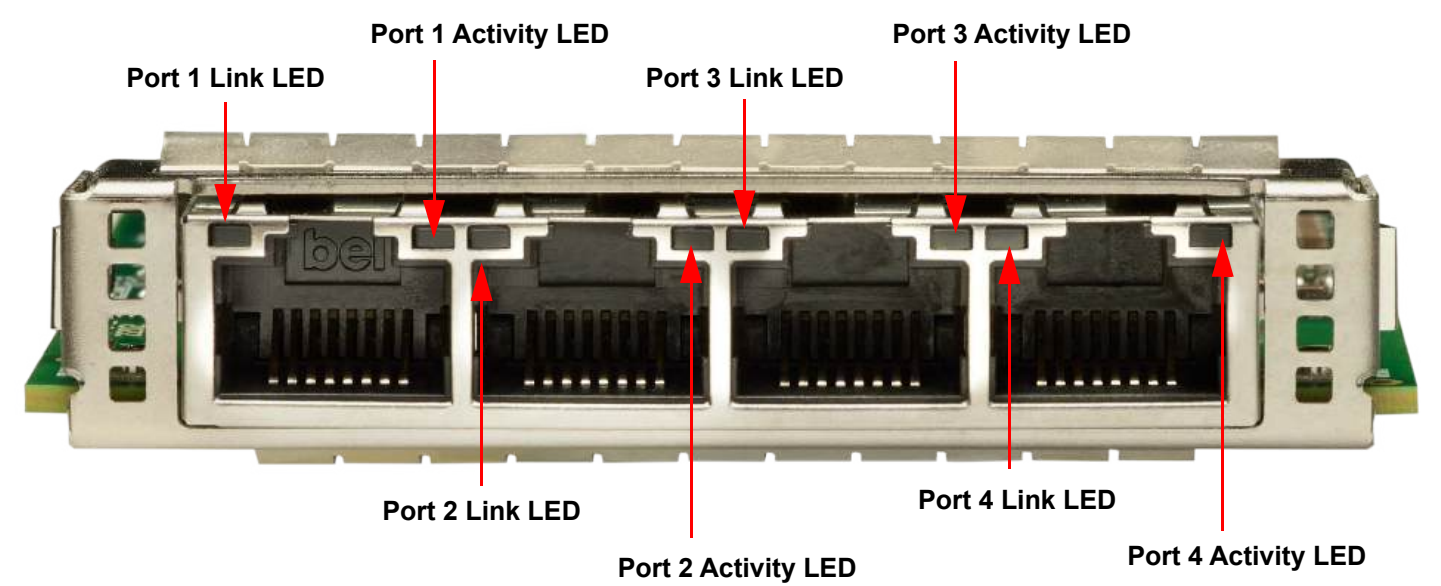


Table 20: LED Functions

NVRAM Manufacturer	Device	Mbit
Activity	Off	No activity
	Green blinking	Traffic flowing activity
Link	Off	No link
	Green	Linked at 10 Gb/s
	Orange	Linked at 1 Gb/s

4 Features

See the following sections for device features.

4.1 Software and Hardware Features

Table 21 provides a list of host interface features.

Table 21: Host Interface Features

Feature	Details
Host Interface	BCM9574XX – PCIe 3.0 (Gen 3: 8 GT/s; Gen 2: 5 GT/s; Gen 1: 2.5 GT/s). BCM9575XX – PCIe 4.0 (Gen 4: 16.0 GT/s; Gen 3: 8 GT/s, Gen 2: 5 GT/s, Gen 1: 2.5 GT/s)
Number of PCIe lanes	PCIe Edge Connectors: ■ BCM9574XX – x8 ■ BCM9575XX – x16 NOTE: N series adapters support OCP 3.0 interfaces.
Vital Product Data (VPD)	Supported.
Alternate Routing ID (ARI)	Supported.
Function Level Reset (FLR)	Supported.
Advanced Error Reporting	Supported.
PCIe ECNs	Support for TLP Processing Hints (TPH), Latency Tolerance Reporting (LTR), and Optimized Buffer Flush/Fill (OBFF).
MSI-X Interrupt vector per queue	1 per RSS queue, 1 per NetQueue, 1 per Virtual Machine Queue (VMQ).
IP Checksum Offload	Support for transmit and receive side.
TCP Checksum Offload	Support for transmit and receive side.
UDP Checksum Offload	Support for transmit and receive side.
NDIS TCP Large Send Offload	Support for LSOV1 and LSOV2.
NDIS Receive Segment Coalescing (RSC)	Support for Windows environments.
TCP Segmentation Offload (TSO)	Hardware acceleration support for Linux and VMware environments.
Large Receive Offload (LRO)	Hardware acceleration support for Linux and VMware environments.
Generic Receive Offload (GRO)	Hardware acceleration support for Linux and VMware environments.
Receive Side Scaling (RSS)	Support for Windows, Linux, and VMware environments.
Header-Payload Split	Enables the software TCP/IP stack to receive TCP/IP packets with header and payload data split into separate buffers. Supports Windows, Linux, and VMware environments.
Accelerated Receive Flow Steering (aRFS)	Hardware acceleration support for Linux.
Jumbo Frames	Supported.
NIC Partitioning (NPAR)	Supports up to eight Physical Functions (PFs) per port, or up to 16 PFs per silicon.
RDMA over Converged Ethernet (RoCE)	BCM9575XX and BCM95741X support RoCE v2 for Windows, Linux, and VMware. NOTE: The BCM57454 does not support RoCE.
Data Center Bridging (DCB)	BCM9575XX and BCM9574XX support DCBX (IEEE and CEE specification), PFC, and AVB.
NC-SI (Network Controller Sideband Interface)	Supported.
Wake on LAN (WOL) ^a	Supported in OCP, rNDC, and NGM devices.
PXE boot	Supported.
UEFI boot	Supported.

Table 21: Host Interface Features (Continued)

Feature	Details
Pause Flow Control (IEEE 802.3x)	Supported.
Priority Flow Control (IEEE 802.1Qbb)	Supported.
Auto negotiation	Supported.
IEEE 802.1q VLAN	Supported.
Interrupt Aggregation	Supported.
MAC/VLAN filters	Supported.
PTP	Supported only in Linux.

a. The Wake on LAN feature is only available in Linux.

4.2 Virtualization Features

[Table 22](#) lists the virtualization features of the Ethernet Network Adapter.

Table 22: Virtualization Features

Feature	Details
Linux KVM Multiqueue	Supported.
VMware NetQueue	Supported.
NDIS Virtual Machine Queue (VMQ)	Supported.
Virtual eXtensible LAN (VXLAN) – Aware stateless offloads (IP/UDP/TCP checksum offloads, VLAN insertion/removal, NetQueue, VMQ, RSS, TCP segmentation offload, Large Send Offload, Generic Receive Offload).	Supported.
Generic Routing Encapsulation (GRE) – Aware stateless offloads (IP/UDP/TCP checksum offloads, VLAN insertion/removal, VMQ, RSS, TCP segmentation offload, Generic Receive Offload).	Supported.
Network Virtualization using Generic Routing Encapsulation (NVGRE) – Aware stateless offloads (IP/UDP/TCP checksum offloads, VLAN insertion/removal, VMQ, RSS, Large Send Offload).	Supported.
Generic Network Virtualization Encapsulation (Geneve) – Aware Stateless offloads (IP/UDP/TCP checksum offloads, VLAN insertion/removal, NetQueue, RSS, TCP segmentation offload, Generic Receive Offload).	Supported.
IP-in-IP aware stateless offloads (IP/UDP/TCP checksum offloads, VLAN insertion/removal, NetQueue, RSS, TCP segmentation offload, Generic Receive Offload).	Supported.
SR-IOV v1.0	BCM9574XX – 128 Virtual Functions (VFs) for Guest Operating Systems (GOS) per device. BCM9575XX – 128 Virtual Functions (VFs) for Guest Operating Systems (GOS) per device

Table 22: Virtualization Features (Continued)

Feature	Details
Edge Virtual Bridging (EVB) (IEEE 802.1Qbg)	BCM9575XX – Edge Virtual Bridging (EVB) enables switching of traffic between PFs/VFs, forwarding of outgoing network traffic from PFs/VFs to appropriate network ports, and steering of incoming network traffic to appropriate PFs/VFs. Both VEB (local switching in the NIC) and VEPA (switching in the adjacent switch) EVB modes of operation are supported. The EVB features supported are: ■ 128 VFs and up to 128 queues per VF (flexible allocation across PFs/VFs). ■ PCIe AER, TPH, FLR support. ■ Virtual Ethernet Bridge (VEB)/Virtual Ethernet Port Aggregator (VEPA). ■ MAC/VLAN filtering and mirroring. ■ VF isolation, source pruning, anti-spoofing checks. ■ Stateless and packet steering offloads per VF. ■ Forwarding of unicast frames based on {Tunnel ID (optional), Destination MAC, VLAN ID (optional)}. ■ Frame replication for multicast, broadcast, and promiscuous mode. ■ Source pruning – Provide support for source knockout (prevent sending a multicast or broadcast frame back to the source). ■ Mirroring of traffic to a specific PF or VF. ■ Packet editing – VLAN insert/swap/delete. ■ Anti-spoof checks.
MSI-X vector port	74 per port default value (two port configuration). 16 per VF and is configurable in HII.

4.3 VXLAN

A Virtual eXtensible Local Area Network (VXLAN), defined in IETF RFC 7348, is used to address the need for overlay networks within virtualized data centers accommodating multiple tenants. VXLAN is a Layer 2 overlay or tunneling scheme over a Layer 3 network. Only VMs within the same VXLAN segment can communicate with each other.

4.4 NVGRE/GRE/IP-in-IP/Geneve

Network Virtualization using GRE (NVGRE), defined in IETF RFC 7637, is similar to a VXLAN.

NOTE: Checksum offload must be enabled when using NVGRE.

4.5 Stateless Offloads

4.5.1 IP, TCP, UDP Checksum Offload

Host software can configure the Ethernet controller to calculate IP, TCP, and UDP checksums as described in RFC 791, RFC 793, and RFC 768 respectively. The first step in checksum calculation is determining the start of an IP and UDP datagram and TCP segment within a frame, which could vary depending on whether the frame is tagged (VLAN) or encapsulated with an LLC/SNAP header. Then the checksum is computed from the start to the end of the datagram and inserted into the appropriate location in the protocol header. The Ethernet controller is designed to support checksum calculation on all frame types and also on IP datagram and TCP segments containing options.

4.5.2 UDP Fragmentation Offload

UDP Fragmentation Offload (UFO) is a feature that enables the software stack to offload fragmentation of large UDP/IP datagrams into multiple UDP/IP packets of size suitable for transmission. Enabling UFO can result in reduced CPU load for UDP applications. Support for this feature is only available in the Linux environment.

4.5.3 TCP Segmentation Offload and Large Send Offload

Large Segment Offload (LSO) is a feature that enables the software stack to offload segmentation of large TCP messages into multiple TCP/IP packets of size suitable for transmission. Enabling LSO can result in reduced CPU load for TCP applications. This is also called TCP Segmentation Offload (TSO).

4.5.4 Generic Receive Offload (GRO) and Large Receive Offload (LRO)

NOTE: BCM5741X adapters do not support hardware LRO if Geneve traffic is present. BCM5750X adapters support hardware LRO if Geneve traffic is present.

Generic Receive Offload (GRO) and Large Receive Offload (LRO) are hardware acceleration for TCP data reception. Both GRO and LRO modes of TCP receive offload are supported by the Ethernet Controller's Transparent Packet Aggregation (TPA) feature. Enabling GRO and LRO can significantly reduce CPU load and increase throughput for TCP applications by reducing the number of received messages, interrupts, and DMA operations.

TPA aggregates TCP streams by managing context entries. Each entry in the TPA context is identified by the 4-tuple: Source IP, destination IP, source TCP port, and destination TCP port.

GRO is the preferred TPA mode as packet boundaries are preserved for network routing applications, which may enable LSO for transmission.

4.5.5 Header and Data Split

Header-payload split is a feature that enables the software TCP/IP stack to receive TCP/IP packets with header and payload data split into separate buffers. The support for this feature is available in both Windows and Linux environments. The following are potential benefits of header-payload split:

- The header-payload split enables compact and efficient caching of packet headers into host CPU caches. This can result in a receive side TCP/IP performance improvement.
- Header-payload splitting enables page flipping and zero copy operations by the host TCP/IP stack. This can further improve the performance of the receive path.

4.5.6 VLAN Tag Insertion and Removal

On the TX Path, the Ethernet controller is capable of inserting IEEE 802.1Q-compliant VLAN tags into transmitted frames and extracting the VLAN tags from received frames.

On the RX path, receiving VLAN-tagged (IEEE 802.1q-compliant) packets is supported by the Ethernet controller. If a function is configured to strip VLAN tag, then the VLAN tag is stripped from the IEEE 802.1q-compliant packet at reception and placed in a receive completion record.

4.5.7 Packet Steering

4.5.7.1 Receive Side Scaling (RSS)

RSS is a scalable networking technology that enables receive packet processing to be balanced across multiple processors in the system while maintaining in-order delivery of the data. RSS enables different packets, received by a single network adapter, to be processed on different CPUs/cores in parallel while preserving in-order delivery of TCP connections.

Receive Side Scaling (RSS) uses a Toeplitz algorithm which uses 4-tuple match on the received frames and forwards it to a deterministic CPU for frame processing. This allows streamlined frame processing and balances CPU utilization. An indirection table is used to map the stream to a CPU.

Symmetric RSS allows the mapping of packets of a given TCP or UDP flow to the same receive queue.

4.5.7.2 Accelerated Receive Flow Steering

Accelerated RFS (aRFS, or RFS) is an Ethernet controller feature that improves packet reception efficiency by delivering packets to queues based on CPU locality of the application. This reduces memory access latency and improves performance. Accelerated RFS takes precedence over RSS when enabled and configured. If the incoming flow does not match any existing n-tuple filters, it is steered according to the RSS hash.

4.5.8 Data Center Bridging

Data Center Bridging (DCB) is a set of protocols and capabilities (for example, DCBX, LLDP, ETS, and PFC) for use in a data center environment. The Ethernet Network Adapter family of Ethernet controllers support for priority flow control is described in the section on Priority Flow Control.

4.6 Priority Flow Control

Priority Flow Control (PFC) is a standard-compliant backpressure mechanism implemented in Broadcom Ethernet Network Adapters. The goal of PFC is to backpressure congested priority traffic flow without affecting the traffic flows of uncongested priorities and to ensure that packets are not dropped in burst or transient scenarios. PFC can be used in a network with real-time or time-sensitive traffic because of its capability to provide differential treatment to Traffic Classes. For example, using PFC lower priority Internet traffic can be backpressured leaving the higher priority traffic like VOIP and Streaming Video flowing through the link without flow control.

4.7 Virtualization Offload

4.7.1 Multiqueue Support

Broadcom Ethernet Network Adapters support Multiqueue in the hardware

4.7.2 KVM/Xen Multiqueue

KVM/Multiqueue returns the frames to different queues of the host stack by classifying the incoming frame by processing the received packet's destination MAC address and or IEEE 802.1Q VLAN tag. The classification combined with the ability to DMA the frames directly into a virtual machine's memory allows scaling of virtual machines across multiple processors.

4.7.3 Virtual Machine Queue

The NDIS Virtual Machine Queue (VMQ) is a feature that is supported by Microsoft to improve Hyper-V network performance. The VMQ feature supports packet classification based on the destination MAC address to return received packets on different completion queues. This packet classification combined with the ability to DMA packets directly into a virtual machine's memory allows the scaling of virtual machines across multiple processors.

4.7.3.1 VMware NetQueue

The VMware NetQueue is a feature that is similar to Microsoft's NDIS VMQ feature. The NetQueue feature supports packet classification based on the destination MAC address and VLAN to return received packets on different NetQueues. This packet classification combined with the ability to DMA packets directly into a virtual machine's memory allows the scaling of virtual machines across multiple processors.

4.7.3.2 Xen Multiqueue

Xen multiqueue enables network device drivers to dedicate each Rx queue to a specific guest operating system. This means the network device drivers should be able to allocate physical memory from the set of memory pages assigned to a specific guest operating system.

4.7.4 Tunneling Offload

Stateless Transport Tunnel Offload (STT) is a tunnel encapsulation that enables overlay networks in virtualized data centers. STT uses IP-based encapsulation with a TCP-like header. There is no TCP connection state associated with the tunnel and that is why STT is stateless. Open Virtual Switch (OVS) uses STT.

An STT frame contains the STT frame header and payload. The payload of the STT frame is an untagged Ethernet frame. The STT frame header and encapsulated payload are treated as the TCP payload and TCP-like header. The IP header (IPv4 or IPv6) and Ethernet header are created for each STT segment that is transmitted.

Broadcom Ethernet Network Adapters support Network Overlays or Tunneling, specifically VXLAN, variants of GRE, and IP-in-IP. Both VXLAN and NVGRE are defined to support larger scale than basic IEEE 802.1Q VLANs, using a 24-bit label space rather than 12-bit VID. Both are L2-in-L3 tunneling methods with NVGRE using GRE to carry the tunnel label and VXLAN using UDP to identify the tunnel label.

Stateless offload for tunneling and encapsulated frames in Broadcom Ethernet Network Adapters applies to VXLAN, Geneve, L2GRE, NVGRE, and also IP-in-IP scheme. The section below describes VXLAN as an example to discuss the general support for this feature. The difference between different tunneling/encapsulation schemes is noted when it is applicable.

All the offloads described in this section are supported on both physical and virtual functions. (PFs and VFs).

4.7.4.1 VXLAN

A Virtual eXtensible Local Area Network (VXLAN), defined in IETF RFC 7348, is used to address the need for overlay networks within virtualized data centers accommodating multiple tenants. The VXLAN scheme and related protocols are defined in IETF RFC 7348.

VXLAN is a Layer 2 overlay or tunneling scheme over a Layer 3 network. Each overlay is termed a VXLAN segment. Only VMs within the same VXLAN segment can communicate with each other. Each VXLAN segment is scoped through a 24-bit segment ID, VXLAN Network Identifier (VNI). This allows up to 16M VXLAN segments to coexist within the same administrative domain. The UDP destination port identifies the presence of a VXLAN tunnel.

4.7.4.2 GRE and NVGRE

Broadcom Ethernet Network Adapters support Generic Routing Encapsulation (GRE) per RFC 2784 and RFC 2890. Network Virtualization using GRE (NVGRE) is a Layer 2 overlay, used to address the need of subnets for overlay networks with larger numbers of VLANs. As with the VXLAN scheme, each NVGRE segment is scoped through a 24-bit identifier, called Virtual Subnet Identifier (VSID), in a GRE header to support up to 16M virtual network segments.

NVGRE is a method for network virtualization, similar to VXLAN in purpose. NVGRE uses a GRE header. The key field defined in RFC 2890 is used to carry a virtual subnet identifier. NVGRE is identified using EtherType = 0x6558, the EtherType for Transparent Ethernet Bridging (carrying a full Ethernet frame as the payload).

4.7.4.3 Geneve

Broadcom Ethernet Network Adapters support Generic Network Virtualization Encapsulation (Geneve, also known as Next Generation Encapsulation). It leverages the same concepts as VXLAN, using UDP destination port to identify the presence of the Geneve tunnel header. A primary goal for Geneve is to enable transport of metadata (system state) between source and destination.

4.7.4.4 IP-in-IP

IP-in-IP is a Layer 3 overlay or tunneling scheme over a Layer 3 network. It is a method by which an IP datagram may be encapsulated (carried as payload) within another IP datagram for the purpose of altering the routing of the inner IP packets and allowing them to be delivered to an intermediate destination that would otherwise not be selected by the destination Address field in the inner IP header. IP Encapsulation with IP is defined in RFC 2003.

4.7.4.5 Checksum Offload

The following checksums are computed on transmit path and then computed and verified on the receive path.

- Outer IPv4 checksum if the outer IP datagram is an IPv4 datagram.
- Outer UDP checksum (if non-zero): The current VXLAN IETF draft suggests that the outer UDP checksum should be transmitted as zero. If the outer UDP checksum field in the VXLAN frame received is zero, then the frame is accepted without computing outer UDP checksum. If the outer UDP checksum field in the VXLAN frame received is non-zero, then the outer UDP checksum should be computed. (Note: The current IETF draft allows the receiver to ignore outer UDP checksum when it is set to non-zero.) This item is not available in L2GRE/NVGRE/IP-in-IP -aware offload.
- Inner IPv4 checksum if the inner IP datagram is an IPv4 datagram.
- Inner UDP or TCP checksum.

4.7.4.6 VLAN Tagging

A VXLAN-frame supports the following tagging options:

- No IEEE 802.1Q tag in inner and outer datagrams.
- IEEE 802.1Q tag in the outer IP datagram only.
- IEEE 802.1Q tag in the inner IP datagram only.
- IEEE 802.1Q tags in both the inner and outer IP datagrams.

NOTE: The device supports insertion and removal of outer IEEE 801.Q Tag for VXLAN/GRE/IP-in-IP frames. It also supports insertion and removal of inner IEEE 801.Q Tag for VXLAN.frames. The device retains inner IEEE 801.Q Tag for NVGRE frames in the inner packet.

4.7.4.7 VMQ

For VXLAN frames, the NetQueue uses the following fields for the queue selection:

- Inner destination MAC address.
- Outer destination MAC address.
- VXLAN Network Identifier (VNI).

The device supports NetQueue selection based on any combination of the fields above.

NOTE: For GRE/IP-in-IP frames, the VMQ selection is performed using the Ethernet header of the encapsulated packet (inner packet) that includes inner destination MAC address and inner 802.1Q Tag (optional).

4.7.4.8 RSS

For VXLAN frames, there are two options for RSS queue selection:

- RSS hash computation based on outer UDP/IP headers: The VXLAN IETF draft recommends that the source port is set based on the hash of inner headers. This allows the RSS hash computation based on outer UDP/IP headers a viable option.
- RSS hash computation based on inner UDP/IP or TCP/IP headers: This option requires 2-tuple or 4-tuple hash computation based on inner headers. The inner header is parsed for RSS hash computation. The RSS hash computation is performed in parallel with other checksum computations. In some exceptional cases, this may lead to inaccurate hash computations where one or more checksum validation fails.

For GRE/IP-in-IP frames, the RSS queue selection is performed using inner headers. The following are possible combinations:

- GRE/IP-in-IP frame with inner TCP/IP or UDP/IP headers: The RSS is performed using 4-tuple (src IP, dst IP, src port, dst port) hash on the inner IP header and TCP or UDP header.
- GRE/IP-in-IP frame without inner TCP or UDP header: The RSS is performed using 2-tuple (src IP, dst IP) hash on the inner IP header.
- Other encapsulated frames (for example, GRE/IP-in-IP frames that cannot be parsed): The RSS is performed using 2-tuple (src IP, dst IP) hash on the outer IP header.

4.7.4.9 TCP Segmentation Offload

For VXLAN, the TCP Segmentation Offload (TSO) algorithm is performed on the inner TCP segment. The hypervisor provides template TCP/IP headers for the inner TCP segment as well as template VXLAN/UDP/IP headers for the outer UDP datagram. For every inner TCP segment generated by the VXLAN-aware TSO, the outer VXLAN, UDP, IP, and MAC headers are inserted and outer IPv4 checksum, outer UDP checksum (not for GRE frames), inner IP checksum (for inner IPv4 datagram only), and inner TCP checksum is computed and inserted. The device updates the IP ID field for every inner TCP segment.

For GRE/IP-in-IP, the LSO (Large Send offload) algorithm is performed on the inner TCP segment. The hypervisor provides template TCP/IP headers for the inner TCP segment as well as template GRE/IP/Ethernet headers for the outer IP datagram. For every inner TCP segment generated by the GRE/IP-in-IP-aware LSO, the outer GRE (not applicable for IP-in-IP frames), IP, and MAC headers are inserted and outer IPv4 checksum (for outer IPv4 datagrams only), inner IP checksum (for inner IPv4 datagram only), and inner TCP checksum is computed and inserted. The device updates the IP ID field for every inner TCP segment.

4.7.4.10 Large Receive Offload

Tunneling Offload support for LRO, RSC, TSO, LSO, GSO, and GRO.

4.8 SR-IOV

The PCI-SIG defines optional support for Single-Root IO Virtualization (SR-IOV). SR-IOV is designed to allow access of the VM directly to the device using Virtual Functions (VFs). The NIC Physical Function (PF) is divided into multiple virtual functions and each VF is presented as a PF to VMs.

SR-IOV uses IOMMU functionality to translate PCIe virtual addresses to physical addresses by using a translation table.

The number of Physical Functions (PFs) and Virtual Functions (VFs) are managed through the UEFI HII menu and NVRAM configurations. SR-IOV can be supported in combination with NPAR mode.

The SR-IOV feature requires corresponding SR-IOV support in the BIOS (Intel VT-d or AMD IOMMU) and Operating System/Hypervisor as well as the PCIe endpoint device (the NIC in this case).

The Ethernet Network Adapter family of Ethernet Controllers offers the following offload functionality to the VF that are available to the PF:

- TX and RX IP/TCP/UDP checksum offload
- Large Send offload (LSO) or TCP segmentation offload (TSO, GSO)
- Receive Segmentation offload (RSC) or Large Receive offload (LRO, GRO)
- Receive Side Scaling (RSS) – up to 64 queues per VF
- Multiple COS queues – up to 4 queues per VF
- Network Virtualization Generic Routing Encapsulation, Virtual Extensible LAN – NVGRE/VXLAN

4.8.1 SR-IOV Configuration Support Matrix

Table 23 provides a SR-IOV support matrix.

Table 23: SR-IOV Support Matrix

SR-IOV Support	Guest OS – VF					
Host OS	Win2k19	Win2k22	RH8.0+	RH9.x	SLES12.2+	SLES15.x
Windows 2019	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2022	Yes	Yes	Yes	Yes	Yes	Yes
Windows 2025	Yes	Yes	Yes	Yes	Yes	Yes
RH8.x+	Yes	Yes	Yes	Yes	Yes	Yes
RH9.x	Yes	Yes	Yes	Yes	Yes	Yes
SLES15.x	Yes	Yes	Yes	Yes	Yes	Yes
ESX7.x+	Yes	Yes	Yes	Yes	Yes	Yes
ESX8.x	Yes	Yes	Yes	Yes	Yes	Yes

4.9 Network Partitioning (NPAR)

The Network Partitioning (NPAR) feature allows a single physical network interface port to appear to the system as multiple network device functions. When NPAR mode is enabled, Broadcom Ethernet Network Adapters are enumerated as multiple PCIe physical functions (PF). Each PF or partition is assigned a separate PCIe function ID on initial power on. Each partition is assigned its own configuration space, BAR address, and MAC address allowing it to operate independently. Partitions support direct assignment to VMs, VLANs, and so on, just as any other physical interface.

The original PCIe definition allowed for eight PFs per device. For Alternative Routing-ID (ARI) capable systems, Broadcom Ethernet Network adapters support up to 16 PFs per device.

4.10 Security (BCM575XX Only)

The BCM575XX TruTrust™ technology is capable of secure boot meaning it only executes boot images authenticated by the secure boot loader (SBL). Secure boot functionality is the cornerstone of a security enabled system since it is the root of trust from which all subsequent applications are run. The secure boot capability provides the following functionality:

- Secure boot Core Root of Trust – The Secure Boot Loader is based in device ROM, and outside the scope of modification. It functions as the Core Root of Trust for software, meaning that the system is in a trusted state from reset to when a secure image has been authenticated.
- Boot Image Authentication – Only Images authenticated by the SBL are executed by the system.
- Boot Image Integrity – The SBL cryptographically validates the integrity of the Secure Boot Image before it is executed to ensure that it has not been tampered with maliciously or errantly.
- Boot Image Confidentiality – The secure processor has the hardware support to execute encrypted images which ensures that device images are never in the clear and protected from reverse engineering or used in device cloning.

Secure devices can be delivered to the customer in a state pending final customization. This customization step is executed by the customer, and once complete, only customer signed images execute on the device. Customization provides the following capabilities:

- Customer takes responsibility for the creation and management of keys used in signing their code. This allows the customer to apply their own security policies in managing their keys and ensures that no code can be signed for their devices by a third party.

- Only code signed by the customer runs on their customized device. This ensures that device code cannot be tampered with in the field and verifies the authenticity of the image.
- Customer signed images do not run on other customers secure devices. This prevents piracy of customer images. However, it does not relieve the customer of the responsibility for protecting unsecured binaries from reverse engineering.
- Device or customer-specific encrypted execution images can be generated. This prevents piracy of customer images and cloning of devices.

4.11 RDMA over Converged Ethernet – RoCE

Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) is a complete hardware offload feature in the Broadcom Ethernet Network adapters allow RDMA functionality over an Ethernet network. RoCE functionality is available for both user mode and kernel mode applications. RoCE is supported under Linux, Windows, and VMware operating systems.

NOTE: The BCM57454 does not support RoCE.

See the following links for RDMA support for each operating system:

Windows

[Microsoft SMB Direct](#)

Linux

[Red Hat Infiniband and RDMA Networking](#)

VMware

[VMware Network Requirements for RDMA](#)

4.12 VMWare Enhanced Networking Stack (ENS)

VMware with Intel designed ENS to support DPDK (Data Plane Development Kit) based NFV (Network Functions Virtualization) applications.

4.12.1 Features

This section contains the supported features of ENS:

- New and faster vSphere networking stack targeted for NFV applications.
- DPDK techniques employed with new vmxnet3 virtual device backend.
- New poll mode and interrupt mode physical device drivers.
- Faster switching using flow cache.
- Deliver improved performance while supporting vSphere features.

4.12.2 ENS Design Choices

This section contains ENS design choices for improved and deterministic performance:

- Dedicated CPU allocation to system thread and polling.
- NUMA-aware placement of VM and system threads.
- NUMA-aware allocation with large pages.

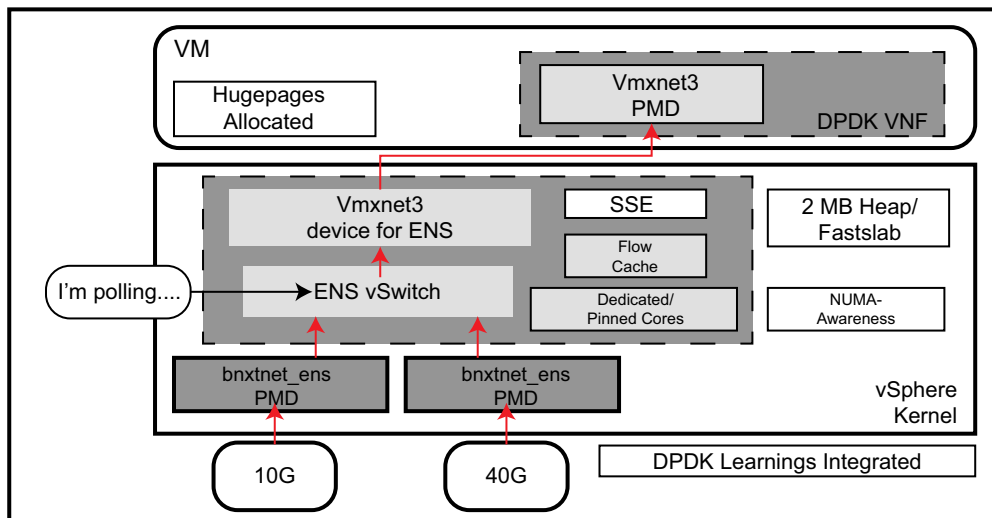
- Simplified packet representation.
- Use of flow cache.
- Lockless datapath.
- Vmxnet3 optimizations.
- Streaming SIMD Extension(SSE) instructions faster packet processing.

4.12.3 ENS Performance

This section contains ENS performance information:

- 3-5x improvement in packet rate over the existing vSphere networking stack performance scales with the number of system threads.
- Acceptable packet loss.
- Low jitter and latency 1x 3-5x Guest: DPDK API + App Host: Default vSwitch Guest: DPDK API + App Host: ENS vSwitch.

Figure 33: VMware ENS stack



For additional information, see <https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.5/administration/GUID-668EB7EF-3E39-46C8-AF2F-43B7DAB6D42E.html>

4.12.4 Limitations and Restrictions

This section contains the limitations and Broadcom support restrictions:

- LRO is not supported by the current ENS stack. RO is not supported in the ENS path.
- RSS is not supported by the current ENS stack. RSS is not supported in the ENS path.
- SR-IOV is disabled when ENS is enabled on the PF.
- ENS is supported with ESXi 7.0 or higher.

4.13 Supported Combinations

The following sections describe the supported feature combinations for this device.

4.13.1 NPAR, SR-IOV, and RoCE

[Table 24](#) shows the supported feature combinations of NPAR, SR-IOV, and RoCE.

Table 24: NPAR, SR-IOV, and RoCE

SW Feature	Notes
NPAR	Up to 8 PFs or 16 PFs
SR-IOV	Up to 128 VFs (total per chip)
RoCE on PFs	Up to 4 PFs for the BCM5741X devices and 16 PFs for BCM575XX devices
RoCE on VFs	BCM575XX supports RoCE SRIOV over up to 128 VFs in the 219.x Release. The 218.x release does not support RoCE SRIOV for BCM575XX. BCM541X does not support RoCE on VFs.
Host OS	Linux, Windows, ESXi (no vRDMA support)
Guest OS	Linux and Windows
DCB	Up to two COS per port with non-shared reserved memory

NOTE: Certain 4 port BCM9575XX adapters support up to 32 VF and 4 NPAR per port. When NPAR and SR-IOV are enabled, certain ESXi OS are not able to configure more than 8 VFs on partitions 3 and above.

4.13.2 NPAR, SR-IOV, and DPDK

[Table 25](#) shows the supported feature combinations for NPAR, SR-IOV, and DPDK.

Table 25: NPAR, SR-IOV, and DPDK

SW Feature	Notes
NPAR	Up to 8 PFs or 16 PFs
SR-IOV	Up to 128 VFs (total per chip)
DPDK	Supported over all VFs
Host OS	Linux
Guest OS	Linux

4.14 Unsupported Combinations

RoCE SRIOV + NPAR is not supported. BCM5741X does not support RoCE SRIOV. BCM575XX does not support RoCE SRIOV in 218.x release. 2.19 release supports RoCE SRIOV for BCM575XX.

5 Installing the Hardware

5.1 Safety Precautions

CAUTION! Server class system power supplies with higher current may be hazardous when normal operating procedures are not used. Before removing the cover of the system, observe the following precautions to protect yourself and to prevent damage to the system components:

- Remove any metallic objects or jewelry from your hands and wrists.
- Make sure to use only insulated or nonconducting tools.
- Verify that the system is powered OFF and unplugged before you touch internal components.
- Install or remove adapters in a static-free environment. The use of a properly grounded wrist strap or other personal antistatic devices and an antistatic mat is strongly recommended.

5.2 System Requirements

Before installing the Broadcom Ethernet Network Adapter adapter, verify that the system meets the requirements listed for the operating system.

5.2.1 Hardware Requirements

See the following list of hardware requirements:

- One open PCIe Gen 3 or Gen 4 slot in x8, x16, or x32 mode.
 - 574XXA41XX – PCIe Gen 3 slot in X8 mode.
 - 574XXM41XX – OCP 2.0 or rNDC slots.
 - 57XXXNXXXX – OCP 3.0 slot
- 16 GB memory or more (32 GB or more is recommended for virtualization applications and nominal network throughput performance).

5.2.2 Memory Requirements

The Ethernet Network Adapter driver and firmware use PCIe DMA transactions between the host memory and Ethernet Network Adapter devices. The amount of host memory required for traffic varies for each operating system. The memory requirements also change when features are enabled such as NPAR and RoCE. This section provides the maximum memory requirements for the Windows operating system when enabling features that require memory allocations.

5.2.2.1 Maximum Memory Requirements for Windows

The following NIC features and OS functions are enabled during the maximum memory requirement calculations:

- Ethernet Network Adapter features – NPAR-EP, RDMA, SR-IOV, and 16 RSS rings.
 - Windows 2019 – Disable VMMQ on each NPAR function (VMQ is used in this mode). Each function is bound to a vSwitch. Do not assign VM to vSwitch. Disable **Virtual Switch RSS**.
 - Memory requirements – 3.2 GB per function.

5.2.2.2 Minimum Memory Requirements for Windows

The following NIC features and OS functions are enabled during the minimum memory requirement calculations:

- Ethernet Network Adapter features – Single physical function, features such as RDMA or SR-IOV are not enabled.
 - Windows 2019 – Driver load only.
 - Memory requirements – 1 GB per function.

5.2.3 Preinstallation Checklist

See the following list before installing the Ethernet Network Adapter device:

1. Verify that the server meets the hardware and software requirements listed in System Requirements.
2. Verify that the server is using the latest BIOS.
3. If the system is active, shut it down.
4. When the system shutdown is complete, turn off the power and unplug the power cord.
5. Holding the adapter card by the edges, remove it from its shipping package and place it on an antistatic surface.
6. Check the adapter for visible signs of damage, particularly on the card edge connector. Never attempt to install a damaged adapter.

5.3 Installing the Adapter

The following instructions apply to installing the Broadcom Ethernet Network Adapter Ethernet adapter (add-in NIC) into most servers. See the manuals that are supplied with the server for details about performing these tasks on this particular server.

1. Review the Safety Precautions and Preinstallation Checklist before installing the adapter. Ensure that the system power is OFF and unplugged from the power outlet, and that proper electrical grounding procedures have been followed.
2. Open the system case and select any empty PCIe 3 or 4 x8 or x16 slot.
3. Remove the blank cover plate from the slot.
4. Align the adapter connector edge with the connector slot in the system.
5. Secure the adapter with the adapter clip or screw.
6. Close the system case and disconnect any personal antistatic devices.

5.4 Connecting the Network Cables

The Broadcom Ethernet Network Adapter adapters support SFP+/SFP28/SFP56/QSFP+/QSFPcables with speeds up to 200 Gb/s. The various Broadcom network adapters interoperate with a wide range of cables. See the [Ethernet Cable and Transceiver Interoperability Testing Report](#) located on Broadcom.com.

5.4.1 Validated Cables and Modules

Table 26: Validated Cables and Modules

Modules and Cables	Dell Part Number	Adapters	Descriptions
SFP+ to 1000BASE-T Transceiver	XTY28	BCM957412 BCM957414	SFP+ to 1000BASE-T Transceiver
FTLX1471D3BCL-FC	RN84N	BCM957412 BCM957414 BCM957504	10 Gb/s LR SFP+ Transceiver
FTLX8574D3BNL	N8TDR	BCM957412 BCM957414 BCM957504	85°C extended temperature range 10 Gb/s SFP+ Transceiver
FTLF8536P4BNL-FC	HHHHC	BCM957414 BCM957504	85°C extended temperature range 25 Gb/s SFP+ Transceiver
FTLX8574D3BCL-FC or PLRXPLSCS43811	WTRD1 C5RNH	BCM957412 BCM957414 BCM957504	10 Gb/s-SR SFP+ Transceiver
Dual-rate ^a 10/25G SFP28	M14MK	BCM957414 BCM957504	Dual-rate 10/25G SFP28
25G SFP28 LR Optic	OYR96	BCM957414 - OCP3.0 BCM957504 - OCP3.0	25G SFP28 LR Optic
SFP28 25Gb	W4GPP	BCM957414 BCM95750X	SFP28 25Gb

Table 26: Validated Cables and Modules (Continued)

Modules and Cables	Dell Part Number	Adapters	Descriptions
10G and 25G Active Optical Cable	YJF03, P9GND, T1KCN, 1DXKP, MT7R2, K0T7R, W5G04, HHFK0, 3YWG7, 5CMT2, RCVP5, X5DH4	BCM957412 BCM957414 BCM957504	10G and 25G Active Optical Cable
Power-Edge QSFP28 SR4 Optic	4WGYD	BCM957508	Power-Edge QSFP28 SR4 Optic
10GBase-T SFP+ Transceiver	PKR0R	BCM957412 BCM957414 BCM957504	10GBase-T SFP+ Transceiver

NOTE:

1. Direct Attach Cables (DAC) that conform to IEEE standards can be connected to the adapter.

- a. When using the dual-rate 10G/25G SR optics module (DN# M14MK), linking at 10G requires that both the switch and the Ethernet adapter have auto-negotiation disabled and set forced speed.

5.4.1.1 Copper

The BCM957416AXXXX and BCM957416XXXX adapters have two RJ-45 connectors used for attaching the system to a CAT 6E Ethernet copper-wire segment.

5.4.1.2 SFP+

The BCM957412AXXXX and BCM957412MXXXX adapters have two SFP+ connectors used for attaching the system to a 10 Gb/s Ethernet switch.

5.4.1.3 SFP28

The BCM957414XXXX, BCM957414AXXXX, BCM957504 adapters have two SFP28 connectors used for attaching the system to a 25 Gb/s Ethernet switch.

5.4.1.4 QSFP

The BCM957508 adapter has QSFP connectors for attaching the system to a 200 Gb/s, 100 Gb/s, or 50 Gb/s PAM-4 Ethernet switch. For additional 200G information, see [Configuring 200G Link Speeds](#).

6 Software Packages and Installation

The software is comprised of the driver, firmware, library, and utility components. All components are bundled in files available from <http://support.dell.com>.

6.1 Supported Operating Systems

Table 27 provides a list of supported operating systems.

Table 27: Supported Operating Systems

Operating System	Distribution
Windows Server	Windows 2019, 2022, and 2025
Redhat	8.8, 8.9, 8.10, 9.2, 9.3, 9.4
SuSE SLES	15 SP4, 15 SP5, and 15 SP6
Azure HCI	OS 23H2 and OS 22H2
VMware	ESXi 7.0 U3, ESXi 8.0 U3, ESXi 8.0 U2, and ESXi 8.0 U1
Ubuntu	Ubuntu 22.04.03 and 22.04.04

6.2 Installing the Linux Driver

This section is based on a ZIP file (Broadcom Ethernet Network adapter Linux Installer) which is extracted to a directory referenced as follows as \$REL_DIR.

Included with the installation package is an automation tool for software installation and system configuration. This is the preferred installation method. The installer installs the included drivers, firmware, RDMA library, and utility tools. Additional system packages are automatically installed as needed:

- ansible, libibverbs-utils, rdmacm-utils, perftest
- gcc, make, rpmbuild, kernel headers: if necessary to compile drivers or library

6.2.1 Compile and Install from the Source RPM

```
cd $REL_DIR/Linux/KMP-L2-RoCE/KMP/<Distro>/<Distro Version>
sudo rpmbuild --rebuild bnxt_en-x.y.z.src.rpm
sudo rpm -i /root/rpmbuild/RPMS/x86_64/kmod-bnxt_en-x.y.z.rpm
sudo depmod -a
sudo modprobe bnxt_en
sudo modprobe bnxt_re
```

6.2.2 Compile and Install Directly from the Source

```
cd $REL_DIR/Linux/Linux_Driver
tar xf netxtreme-bnxt_en-x.y.z.tar.gz
cd netxtreme-bnxt_en-x.y.z
sudo make
sudo make install
sudo depmod -a
sudo modprobe bnxt_en
sudo modprobe bnxt_re61
```

6.2.3 Updating Initramfs

Most Linux distributions use a ramdisk image to store the drivers for boot-up. These kernel modules take precedence, therefore, the initramfs must be updated after installing the new `bnxt_en/bnxt_re` modules:

6.2.3.1 Debian/Ubuntu

```
sudo update-initramfs -u
```

6.2.3.2 Red Hat/CentOS/Fedora

```
sudo dracut -f
```

6.2.4 Useful Linux Commands

In [Table 28](#), ethX should be replaced with the actual interface name.

Table 28: Useful Linux Commands

Command	Description
<code>ethtool -s ethX speed 25000 autoneg off</code>	Force the speed to 25G. If the link is up on one port, the driver does not allow the other port to be set to a different speed.
<code>ethtool -i ethX</code>	Output includes driver, firmware, and package version.
<code>ethtool -k ethX</code>	Show offload features.
<code>ethtool -K ethX tso off</code>	Turn off TSO.
<code>ethtool -K ethX gro off lro off</code>	Turn off GRO/LRO.
<code>ethtool -g ethX</code>	Show ring sizes.
<code>ethtool -G ethX rx N</code>	Set Ring sizes.
<code>ethtool -S ethX</code>	Get statistics.
<code>ethtool -l ethX</code>	Show number of rings.
<code>ethtool -L ethX rx 0 tx 0 combined M</code>	Set number of rings.
<code>ethtool -C ethX rx-frames N</code>	Set interrupt coalescing. Other parameters supported are: rx-usecs, rx-frames, rx-usecs-irq, rx-frames-irq, tx-usecs, tx-frames, tx-usecs-irq, tx-frames-irq.
<code>ethtool -x ethX</code>	Show RSS flow hash indirection table and RSS key.
<code>ethtool -s ethX autoneg on speed 10000 duplex full</code>	Enable Autoneg (see Auto-Negotiation Configuration for additional information).
<code>ethtool --show-eee ethX</code>	Show EEE state.
<code>ethtool --set-eee ethX eee off</code>	Disable EEE.
<code>ethtool --set-eee ethX eee on tx-lpi off</code>	Enable EEE, but disable LPI.
<code>ethtool -L ethX combined 1 rx 0 tx 0</code>	Disable RSS. Set the combined channels to 1.
<code>ethtool -K ethX ntuple off</code>	Disable Accelerated RFS by disabling ntuple filters.
<code>ethtool -K ethX ntuple on</code>	Enable Accelerated RFS.
<code>ethtool -t ethX</code>	Performs various diagnostic self-tests.
<code>ethtool -m ethX</code>	Query/Decode Module EEPROM information and optical diagnostics if available.
<code>echo 32768 > /proc/sys/net/core/rps_sock_flow_entries</code> <code>echo 2048 > /sys/class/net/ethX/queues/rx-X/rps_flow_cnt</code>	Enable RFS for Ring X.
<code>sysctl -w net.core.busy_read=50</code>	This sets the time to read the device's receive ring to 50 µsecs. For socket applications waiting for data to arrive, using this method can decrease latency by 2 or 3 us typically at the expense of higher CPU utilization.
<code>echo 4 > /sys/class/net/<NAME>/device/sriov_numvfs</code>	Enable SR-IOV with four VFs on named interface.
<code>ip link set ethX vf 0 mac 00:12:34:56:78:9a</code>	Set VF MAC address.
<code>ip link set ethX vf 0 state enable</code>	Set VF link state for VF 0.
<code>ip link set ethX vf 0 vlan 100</code>	Set VF 0 modprobe 8021q; ip link add link <NAME> name <VLAN Interface Name> type vlan id <VLAN ID> Example: modprobe 8021q; ip link add link ens3 name ens3.2 type vlan id 2

6.3 Installing the VMware Driver

The ESX drivers are provided in VMware standard VIB format and can be downloaded from VMware.com.

1. To install the Ethernet and RDMA driver, issue the following commands:

```
$ esxcli software vib install -v <bnxtnet>--<driver version>.vib
```

```
$ esxcli software vib install -v <bnxtroce>--<driver version>.vib
```

2. A system reboot is required for the new driver to take effect.

Other useful VMware commands are shown in [Table 29](#).

NOTE: In [Table 29](#), replace vmnicX with the actual interface name.

NOTE: `$ kill -HUP $(cat /var/run/vmware/vmkdevmgr.pid)`
This command is required after `vmkload_mod bnxtnet` for successful module bring up.

NOTE: NPAR + SR-IOV and NPAR + MultiRSS are currently not supported due to resource constraints.

Table 29: VMware Commands

Command	Description
<code>esxcli software vib list grep bnx</code>	List the VIBs installed to see whether the bnxt driver installed successfully.
<code>esxcfg-module -I bnxtnet</code>	Print module info on to screen.
<code>esxcli network get -n vmnicX</code>	Get vmnicX properties.
<code>esxcfg-module -g bnxtnet</code>	Print module parameters.
<code>esxcfg-module -s 'multi_rx_filters=2 disable_tap=0 max_vfs=0,0 RSS=0'</code>	Set the module parameters.
<code>vmkload_mod -u bnxtnet</code>	Unload bnxtnet module.
<code>vmkload_mod bnxtnet</code>	Load bnxtnet module.
<code>esxcli network nic set -n vmnicX -D full -S 25000</code>	Set the speed and duplex of vmnicX.
<code>esxcli network nic down -n vmnicX</code>	Disable vmnicX.
<code>esxcli network nic up -n vmnic6</code>	Enable vmnicX.

6.4 Installing the Windows Driver

The driver installer can be downloaded from the following Dell Support website:

- <http://support.dell.com>

Download the installer for your platform and adapter using the URL and follow the instructions in the readme.txt file to install the driver.

7 Updating the Firmware

This section provides information for updating the adapter firmware.

7.1 Dell Update Package

DUP packages can be downloaded from <http://support.dell.com>. See the following sections to use the Dell Update Package (DUP):

7.1.1 Windows

Broadcom Ethernet Network adapter firmware can be upgraded using the Dell DUP package. The executable is provided in standard Windows x64 executable format. Double-click on the file to execute it.

NOTE: During a hot firmware upgrade or error recovery, there may be a period of time when the firmware can not respond to a command sent from the drivers while the firmware is performing a reset. The driver logs this as an error in the event log. During normal operation, the firmware continues the reset and returns to normal operation. As long as the firmware hot upgrade/error recovery is completed successfully, this error can be ignored. This is verified by observing the *Firmware became responsive* and *Firmware reset sequence completed* events in the event log.

NOTE: DUP packages can be downloaded from <http://support.dell.com>

7.1.2 Linux

The Dell Linux DUP is provided in `x86_64` executable format. Use the standard Linux `chmod` to update the execute permission and run the executable. See the following example:

1. Login to Linux.
2. `scp` or `cp` the DUP executable on to file system. A typical example is:

```
cp /var/run/media/usb/Network_Firmware_<version>.BIN /root/
```

3. Execute the following command:

```
chmod 755 Network_Firmware_<version>.BIN
```

4. Execute the following command:

```
./Network_Firmware_<version>.BIN
```

A reboot is needed to activate the new firmware.

8 Link Aggregation

The following sections provide information on link aggregation.

8.1 Windows

Broadcom Ethernet Network adapters can aggregate network links using the Microsoft teaming feature. For more information on the NIC teaming functionality, see the Microsoft public documentation on [Microsoft.com](https://docs.microsoft.com/en-us/windows/networking/network-load-balancing-floppy-olb).

Microsoft LBFO is a native teaming driver that can be used in the Windows OS. The teaming driver also provides VLAN tagging capabilities.

8.2 Linux

The Linux bonding module is used for link aggregation under Linux. For additional documentation on Linux bonding, see <https://www.kernel.org/doc/Documentation/networking/bonding.txt>.

8.2.1 Ephemeral Bonds

Use the following steps as an example to create a bond interface that is ephemeral:

1. Load the bonding module using the following command:

```
sudo modprobe bonding
```

2. Create a bond interface named bond0 and mode balance-alb using the following command:

```
sudo ip link add bond0 type bond
```

3. Bring down the first interface that will be added to the bond interface using the following command:

```
sudo ip link set enp9s0f0np0 down
```

4. Add the first interface to the bond interface using the following command:

```
sudo ip link set enp9s0f0np0 master bond0
```

5. Bring down the second interface that will be added to the bond interface using the following command:

```
sudo ip link set enp9s0f1np1 down
```

6. Add the second interface to the bond interface using the following command:

```
sudo ip link set enp9s0f1np1 master bond0
```

7. Assign an IP address to the bond interface using the following command:

```
sudo ip addr add 192.168.2.35/16 dev bond0
```

8. Bring up the bond interface using the following command:

```
sudo ip link set bond0 up
```

8.2.2 Bonding Interface Queries

Details of the bonding interface can be queried using the following command

```
cat /proc/net/bonding/bond0
```

Use the following steps to setup basic Linux bonding:

1. Load the bonding module using the following command:

```
modprobe bonding mode="balance-alb"
```

2. Add physical network interfaces to the bond interface using the following commands:

```
ifenslave bond0 ethX  
ifenslave bond0 ethY
```

3. Assign an IP address to bond the interface. IPV4Address and NetMask are an IPv4 address and the associated network mask.

```
ifconfig bond0 <IP address> netmask <netmask>
```

9 System-Level Configuration

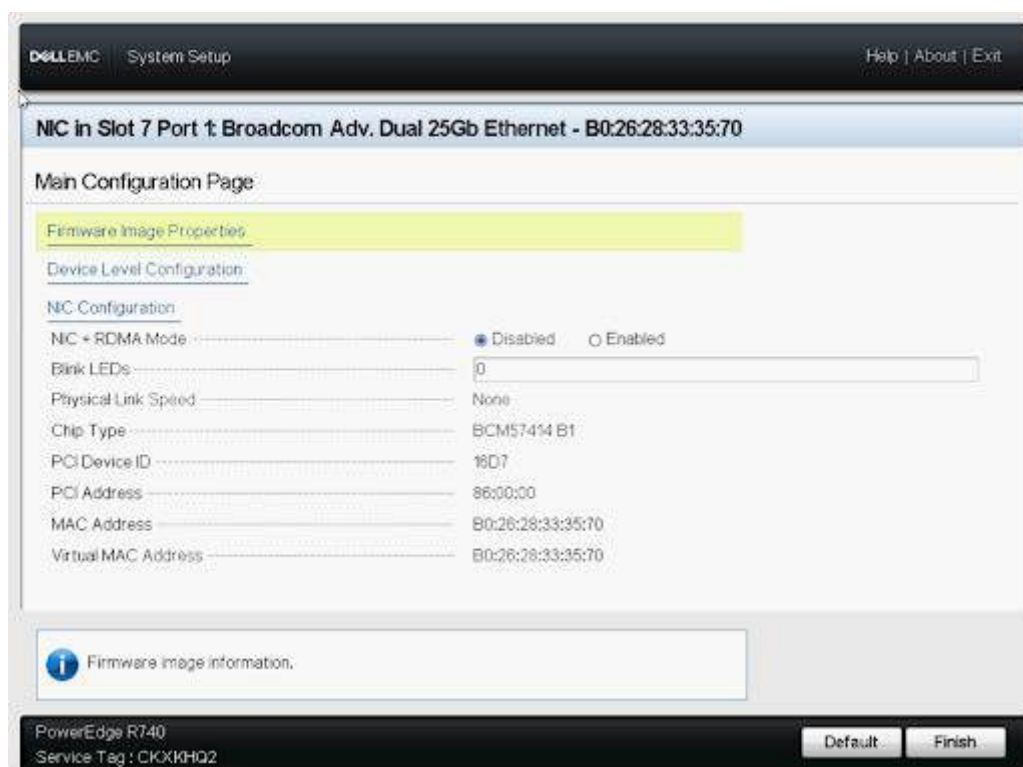
The following sections provide information on system-level NIC configuration.

9.1 UEFI HII Menu

Broadcom Ethernet Network adapters can be configured using the HII (Human Interface Infrastructure) menu at boot time. This menu system allows configuration of all persistent settings such as boot protocol (PXE) and virtualization modes (SR-IOV, NPAR), and so on. To enter the HII configuration menu, follow boot-time prompts to BIOS, then device configuration. The layout of the menus of an adapter may not look the same as the others and some settings may not be available or found on the same menu for a different adapter type.

9.1.1 Main Configuration Page

Figure 34: Main Configuration Page



This page displays the following information (see [Figure 34](#)):

- **Firmware Image Menu** – This menu presents the various component versions present in the current firmware package.
- **Device Configuration Menu** – This menu presents adapter specific parameters for configuration.
- **NIC Configuration** – This menu presents PXE boot related parameters for configuration.
- **NIC Partitioning Configuration Menu** – This menu presents NIC partition related parameters for configuration.

- **NIC + RDMA Mode** – This setting configures Remote Direct Memory Access (RDMA) support on the port. RDMA is a technology that permits computers on a network to exchange data in main memory without the involvement of the processor, cache or operating system of either computer. RDMA allows high throughput and low-latency networking. This setting is available only when RDMA is supported on the adapter. This setting will be displayed on the Device Configuration menu in SF mode and in the NIC Partition Configuration menu in NPAR mode.
 - **Enabled** – Turn on RDMA
 - **Disabled** – Turn off RDMA

NOTE: When NIC + RDMA Mode is enabled, UDP port 4791 is reserved for RDMA use. Therefore, is not available to clients and services running on the host operating system.

- **Blink LEDs** – This setting allows the user to configure the duration for which the LEDs on the physical network port should blink to assist with port identification. This is a numeric setting. The value must be specified in the range 0 to 15 seconds.
- **Link Status** – This field displays the physical link status of the network port as reported by the controller. This is a read-only field.
 - **Connected** – Link is up
 - **Disconnected** – Link is down
- **Physical Link Speed** – This field displays the current link speed of the network port as reported by the controller. This is a read-only field. Speed is reported in Mb/s/Gb/s.
- **Chip Type** – This field displays the Broadcom-specific identifier which denoted the adapter family to which the chip belongs and the revision. This is a read-only field.
- **PCI Device ID** – This field displays the 16-bit PCI Device ID reported by the controller. This is a vendor defined ID that varies across non-NPAR, NPAR, and RDMA mode. Refer to MF mode and Support RDMA sections for more information on these modes. This is a read-only field.
- **Bus Device Function** – This field displays the BIOS assigned PCI Bus:Device:Function identifier of the card. This is a read-only field.
- **Permanent MAC Address** – This field displays the Permanent MAC address assigned during manufacturing. This is a read-only field.
- **Virtual MAC Address** – This field displays the Virtual MAC address assigned to the device. This is a read-only field from the HII menu. The value for this parameter can be configured using remote utilities.

9.1.2 Firmware Image Menu

This menu presents the various component versions present in the current firmware build. Depending on the adapter type, some components may not be available. All fields in this menu are read-only.

Figure 35: Firmware Image Menu



This page displays the following information (see [Figure 35](#)):

- **Family Firmware Version** – This field displays the family firmware version. This field may be displayed as Firmware Bundle on some adapters.
- **Boot Code** – This field displays the firmware boot code version.
- **MBA** – This field displays the legacy pre-boot driver version.
- **EFI** – This field displays the UEFI pre-boot driver version.
- **NC-SI** – This field displays the NCSI firmware version.
- **RDMA FW** – This field displays the RoCE firmware version.

9.1.3 Device Configuration Menu

This menu presents adapter-specific parameters for configuration. Depending on the adapter type, some settings may not be available.

Figure 36: Device Configuration Menu

Integrated NIC 1 Port 1: Broadcom Adv. Dual 25Gb Ethernet - 00:0A:F7:31:43:40

Main Configuration Page • Device Level Configuration

Broadcom Adv. Dual 25Gb Ethernet - 00:0A:F7:31:43:40

Virtualization Mode	None
NParEP Mode	☐ Disabled ☒ Enabled
PCI Virtual Functions Advertised	8
Number of MSI-X Vectors per VF	16
Maximum Number of PF MSI-X Vectors	74
Link FEC	Disabled
Operational Link Speed	Auto Negotiated
DCBX Mode	Disabled
LLDP nearest bridge	☐ Disabled ☒ Enabled
LLDP nearest non-TPMR bridge	☐ Disabled ☒ Enabled
Auto-negotiation Protocol	IEEE and Consortium
Media Auto Detect	☐ Disabled ☒ Enabled
Default EVB Mode	☒ VEB ☐ VEPA ☐ None
Flow Offload	☒ Disabled ☐ Enabled
Adapter Error Recovery	☒ Disabled ☐ Enabled

This page allows the user to configure the following items (see [Figure 36](#)):

- **Virtualization Mode** – This setting configures the type of virtualization to be used by the controller on all ports. This is available only when NPAR is supported on the adapter.
 - **Single Function Mode (SF)** – In this mode, a single PCIe PF is assigned to each network port.
 - **Network Partitioning Mode (NPAR)** – This mode allows a single physical network port to appear to the system as multiple network device functions. Each PF or partition is assigned a separate PCIe function ID on initial power on, and a menu is made visible in setup to configure each partition. The 16 configurable partitions are distributed equally across the network ports.
 - **SR-IOV** – This setting configures Single Root - I/O Virtualization (SR-IOV) which allows different virtual machines (VMs) in a virtual environment to share a single PCI Express hardware interface.
 - **Enabled** – Enable support for SR-IOV
 - **Disabled** – Disable support for SR-IOV

NOTE: This setting is available only on adapters that support SR-IOV.

- **PCI Virtual Functions Advertised** – This setting allows the user to configure the number of PCI Virtual Functions Advertised by the port in PCI config space when SR-IOV is enabled in non-NPAR mode. This setting is available for configuration only in non-NPAR mode. This is a numeric setting. The value must be specified in multiples of 8.

NOTE: The maximum number of VFs supported by software is 128 VFs per device.

■ **Number of MSI-X Vectors per VF**

This setting configures the MSI-X Vectors per VF. Message Signaled Interrupts (MSI) are an alternative in-band method of signaling an interrupt using special in-band messages to replace traditional out-of-band assertion of dedicated interrupt lines. This is a numeric setting. The maximum number of virtual functions supported by the adapter is shared across the number of physical ports on the adapter. The default value for BCM574XX is 16 and 8 for the BCM5750X.

■ **Maximum Number of PF MSI-X Vectors**

This setting allows the user to configure the Maximum Number of MSI-X Vectors for a physical function. This is a numeric setting. The minimum value for this setting is 0. The maximum value varies across adapters. The default value for this option is 74.

NOTE: See [Table 30](#) for a list of recommended settings for maximum VF support. Exceeding the recommended settings may result in undesirable behavior, such as failure of network interfaces to start.

Table 30: Recommended Configurations (BCM5750X Only)

	PCIe Physical Functions	VFs per PF	MSI-X Vector per PF (absolute maximum)	MSI-X Vector per VF
Single-Port Adapter	1	128	240	8
Dual-Port Adapter	2	64	120	8
Quad-Port Adapter	4	32	60	8
With NPAR Enabled (any port count)	8	16	94	4
With NPAR EP Enabled (any port count)	16	8	47	4

■ **Link FEC** – This setting configures the Forward Error Correction (FEC) mode which is a technique used for controlling errors in data transmission over unreliable or noisy communication channels. This option is useful when longer fiber cables are utilized. This setting is not available on 10G BaseT controllers. Only a subset of the possible values display on some adapters, based on the configuration. Possible values are:

- Disabled
- CL74 – Fire Code
- CL91 – Reed Solomon
- RS544 – RS544, using 1 x N RS
- RS272 – RS272, using 1 x N RS
- RS544 – RS544, using 2 x N RS
- RS272 – RS272, using 2 x N RS

NOTE: When Media Auto Detect and Auto-negotiation are enabled, FEC is negotiated based on the link partner advertisement.

■ **Energy Efficient Ethernet** – This setting configures the Energy Efficient Ethernet (EEE) mode that allows for less power consumption during periods of low-data activity. This setting is available only on 10GBASE-T controllers.

- **Enabled** – Turn on EEE mode
- **Disabled** – Turn off EEE mode

■ **Operational Link Speed** – This setting configures the default link speed for pre-OS environment in full-power (D0) state. The possible values for this setting depend on the link speeds supported by the adapter.

NOTE: The value for this setting is fixed on some adapters based on the configuration.

- **DCB Protocol** – This setting configures the Data Center Bridging (DCB) settings for the controller. Some of the following options may not be available depending on the adapter in use.
 - **Enabled (IEEE only)**
 - **CEE (only)**
 - **Both (IEEE preferred with fallback to CEE)**
- **LLDP nearest bridge** – This setting configures the Link Layer Discovery Protocol (LLDP) which is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet. An LLDP agent is a mapping of an entity where LLDP runs.
 - **Enabled** – Turn on LLDP nearest bridge
 - **Disabled** – Turn off LLDP nearest bridge
- **LLDP nearest non-TPMR bridge** – This setting configures the Link Layer Discovery Protocol (LLDP) which is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network based on IEEE 802 technology, principally wired Ethernet. An LLDP agent is a mapping of an entity where LLDP runs. This setting enables LLDP on the nearest non-TPMR bridge agent.
 - **Enabled** – Turn on LLDP nearest non-TPMRbridge
 - **Disabled** – Turn off LLDP nearest non-TPMRbridge
- **Auto-negotiation Protocol** – This setting configures the Auto-negotiation protocol for the adapter. Auto-negotiation is a feature that allows a port on a switch, router, server, or other device to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection. This setting is not available on 10GBASE-T controllers.
 - **IEEE and BAM**
 - **IEEE and Consortium**
 - **BAM Only**
 - **Consortium Only**
 - **IEEE 802.3by**
- **Media Auto Detect** – This setting allows the user to configure the Media Auto Detect feature. This setting is not available on 10GBASE-T controllers.
 - **Enabled** – Turn on Media Auto Detect.
 - **Disabled** – Turn off Media Auto Detect.
- **Default EVB Mode** – This setting configures the Edge Virtual Bridging (EVB) mode which is an IEEE standard that involves the interaction between virtual switching environments in a hypervisor and the first layer of the physical switching infrastructure.
 - **VEB**
 - **VEPA**
 - **None**
- **Port Link Training** – This setting configures port link training when using force link speed. Link training should be enabled when using PAM-4. Link training should be disabled when the attached switch does not support link training.
 - **Enabled** – Port Link Training
 - **Disabled** – Port Link Training
- **Adapter Error Recovery** – This feature enables the recovery of firmware from fatal errors without manual intervention, host reboot, or power cycle. This feature is supported on Linux only.
 - **Enabled** – Adapter Error Recovery
 - **Disabled** – Adapter Error Recovery

9.1.4 NIC Configuration

This menu presents legacy boot related parameters for configuration. Depending on the adapter type, some settings may not be available.

Figure 37: NIC Configuration

The screenshot shows the 'NIC Configuration' page for a 'Broadcom Adv. Quad 25Gb Ethernet - BC:97:E1D3:2B:40' adapter. The page is titled 'Main Configuration Page • NIC Configuration'. It lists various settings with radio buttons or dropdown menus. The 'Option ROM' is set to 'Enabled', 'Legacy Boot Protocol' to 'None', 'Boot Strap Type' to 'Auto Detect', 'Hide Setup Prompt' to 'Disabled', 'Setup Key Stroke' to 'Ctrl-S', 'Banner Message Timeout' to '5', 'Wake On LAN' to 'Disabled', 'Virtual LAN Mode' to 'Disabled', 'Virtual LAN ID' to '1', 'Boot Retry Count' to '3 Retries', and 'Permit Total Port Shutdown' to 'Disabled'. At the bottom, there is a 'Back' button and a footer showing 'PowerEdge R750' and 'Service Tag : 1234567'.

Setting	Value
Option ROM	☒ Enabled
Legacy Boot Protocol	☒ None
Boot Strap Type	Auto Detect
Hide Setup Prompt	☒ Disabled
Setup Key Stroke	☒ Ctrl-S
Banner Message Timeout	5
Wake On LAN	☒ Disabled
Virtual LAN Mode	☒ Disabled
Virtual LAN ID	1
Boot Retry Count	3 Retries
Permit Total Port Shutdown	☒ Disabled

Configure Multiple Boot Agent (MBA) parameters.

PowerEdge R750
Service Tag : 1234567

Back

The NIC Configuration menu consists of the following items (see [Figure 37](#)):

- **Option ROM** – This setting allows the user to control whether the Broadcom legacy option ROM driver should be advertised or not.
 - **Enabled** – Load legacy option ROM driver
 - **Disabled** – Do not load legacy option ROM driver
- **Boot Strap Type** – This setting configures the bootstrap protocol for legacy PXE boot.
 - **Auto Detect**
 - **BBS**
 - **Int 18h**
 - **Int 19h**
- **Banner Message Timeout** – This setting configures the duration for which the Broadcom legacy option ROM banner is to be displayed on the screen during POST. This is a numeric setting. The value must be specified in the range 0 to 15 seconds.
- **Pre-boot Wake on LAN** – This setting configures Wake on LAN (WoL) which is the ability to remotely power on a server or to wake it up from sleep mode. This setting is available only on adapters that support the Wake on LAN feature. This setting is available only on adapters that support the **Wake on LAN** feature.
 - **Enabled** – Turn on WoL

- **Disabled** – Turn off WoL
- **VLAN Mode** – This setting configures a virtual LAN.
 - **Enabled** – Turn on VLAN mode
 - **Disabled** – Turn off VLAN mode
- **VLAN ID** – This setting configures a VLAN tag when VLAN mode is enabled. This is a numeric setting. The value must be specified in the range 1 to 4094.
- **Boot Retry Count** – This setting configures the number of times legacy boot must be attempted in case of failure.
 - **No Retry**
 - **1 Retry**
 - **2 Retries**
 - **3 Retries**
 - **4 Retries**
 - **5 Retries**
 - **6 Retries**
 - **Indefinite Retries**
- **Permit Total Port Shutdown** – This feature is supported on Linux OS only. This setting allows the port to be completely disabled when a port down command is received from the host OS or drive. This feature is not supported when virtualization mode is NPAR or NPAR + SRIOV.
 - **Enabled** – Permit Total Port Shutdown
 - **Disabled** – Permit Total Port Shutdown

9.1.5 NIC Partitioning Configuration Menu

Figure 38: NIC Partitioning Configuration Menu

Integrated NIC 1 Port 1: Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Main Configuration Page • NIC Partitioning Configuration

Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Partition 1	Enabled
Partition 2	Disabled
Partition 3	Disabled
Partition 4	Disabled
Partition 5	Disabled
Partition 6	Disabled
Partition 7	Disabled
Partition 8	Disabled
Number of Partitions	8

[Global Bandwidth Allocation](#)

[Partition 1 Configuration](#)

 Configure Global Bandwidth Allocation.

The **NIC Partitioning Configuration** screen has the following sub-menus (see [Figure 38](#)):

- **Number of Partitions Per Port** – This field displays the number of PCI Physical functions currently enabled on the current network port when MF mode is set to NPAR. This is a read-only field.
- **Partition <n> Configuration** – This menu presents configuration parameters for the 'n'th partition on the network port in NPar mode. The number of menus presented depends on the value of the **Number of Partitions** field.

9.1.5.1 Partition <n> Configuration Menu

This menu presents partition related parameters for configuration. Depending on the adapter type, some settings may not be available (see [Figure 39](#)).

Figure 39: Partition <n> Configuration

Integrated NIC 1 Port 1: Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Main Configuration Page • NIC Partitioning Configuration • Partition 1 Configuration

Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

BW Reservation Valid	☒ False ☐ True
BW Limit Valid	☒ False ☐ True
NIC + RDMA Mode	☒ Disabled ☐ Enabled
MAC Address	B0:26:28:C4:06:7A
Virtual MAC Address	B0:26:28:C4:06:7A
PCI Device ID	16D7
PCI Address	01:00

 Configure BW Reservation Valid. Functions as an on/off switch for the BW Reservation setting.

Integrated NIC 1 Port 1: Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Main Configuration Page • NIC Partitioning Configuration • Global Bandwidth Allocation

Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Partition 1 Minimum TX Bandwidth	0
Partition 1 Maximum TX Bandwidth	100
Partition 2 Minimum TX Bandwidth	0
Partition 2 Maximum TX Bandwidth	100
Partition 3 Minimum TX Bandwidth	0
Partition 3 Maximum TX Bandwidth	100
Partition 4 Minimum TX Bandwidth	0
Partition 4 Maximum TX Bandwidth	100
Partition 5 Minimum TX Bandwidth	0
Partition 5 Maximum TX Bandwidth	100
Partition 6 Minimum TX Bandwidth	0

 Configure BW Reservation. Percentage of total available bandwidth that should be reserved for this partition. Combined values for all active ... (Press <F1> for more help)

- **BW Reservation** – This setting configures the percentage of total available bandwidth that should be reserved for this partition. The total Bandwidth Reservation assigned for all active partitions cannot exceed 100. A value of 0 on all partitions indicates equal division of bandwidth between all partitions. This setting is available only on adapters that support the Bandwidth Reservation feature. This is a numeric setting. The value must be specified in the range 0 to 100.
- **BW Limit** – This setting configures the maximum percentage of available bandwidth this partition is allowed. This is a numeric setting. The value must be specified in the range 0 to 100.
- **BW Reservation Valid** – This setting configures whether BW Reservation is applicable on the current partition. When this setting is disabled, the BW Reservation value for the current partition will be ignored. This setting is available only on adapters that support the Bandwidth Reservation feature.
 - **Enabled** – Turn on BW Reservation
 - **Disabled** – Turn off BW Reservation
- **BW Limit Valid** – This setting configures whether BW Limit is applicable on the current partition. When this setting is disabled, the BW Limit value for the current partition will be ignored.
 - **Enabled** – Turn on BW Limit
 - **Disabled** – Turn off BW Limit

NOTE: Not all devices have all of the options available.

- **NIC + RDMA Mode** – This setting configures the RoCE support for the current partition. This setting is available only when RDMA is supported on the current partition. This setting will be displayed on the Device Configuration menu in SF mode and in the **NIC Partition Configuration** menu in NPar mode.
 - **Enabled** – Turn on RDMA
 - **Disabled** – Turn off RDMA

NOTE: When NIC + RDMA Mode is enabled, UDP port 4791 is reserved for RDMA use. Therefore, is not available to clients and services running on the host operating system.

- **MAC Address** – This field displays the Permanent MAC address assigned during manufacturing for the current partition. This is a read-only field.
- **Virtual MAC Address** – This field displays the Virtual MAC address assigned to the current partition. This is a read-only field from the HII menu. The value for this parameter can be configured using remote utilities.

9.2 Auto-Negotiation Configuration

NOTE: In NPAR (NIC partitioning) devices where one port is shared by multiple PCI functions, the port speed is preconfigured and cannot be changed by the driver.

Broadcom Ethernet Network adapters support the following auto-negotiation features:

- Link speed auto-negotiation
- FEC auto-negotiation
- Pause/Flow Control auto-negotiation

NOTE: When using SFP+, SFP28 connectors, use DAC or multimode optical transceivers capable of supporting auto-negotiation. Ensure that the link partner port has been set to the matching auto-negotiation protocol. For example, if the local Broadcom port is set to IEEE 802.3by AN protocol, the link partner must support auto-negotiation and must be set to IEEE 802.3by auto-negotiation protocol. When Media Auto Detect and IEEE 802.by + Consortium are enabled, the controller auto detects the Ethernet cables and transceivers to start auto-negotiation with the link partner. FEC is negotiated during auto-negotiation and forced FEC does not take effect in this mode. The default setting enables IEEE 802.by + Consortium and Media Auto Detect.

The supported combination of link speed settings for two port Broadcom Ethernet Network adapters is shown in [Table 31](#).

Table 31: Supported Link Speeds for the BCM95741X and BCM95750X

Dual-Port	BCM95741X	BCM9575XX
1G, 1G	Yes	No
1G, 10G	Yes	No
1G, 25G	Yes	No
10G, 10G	Yes	Yes
10G, 25G	No	Yes
25G, 25G	Yes	Yes
50G, 50G	No	Yes
100G, 100G	No	Yes
200G ^a	No	Yes, single port only.
Quad-Port		
10G, 10G, 10G, 10G	N/A	Yes
10G, 10G, 10G, 25G	N/A	Yes
10G, 10G, 25G, 25G	N/A	Yes
10G, 25G, 25G, 25G	N/A	Yes
25G, 25G, 25G, 25G	N/A	Yes

a. BCM57508-P2100D and BC57508-N2100D adapters only.

NOTE: 1 Gb/s link speed for SFP+/SFP28 is currently not supported in this release.

- P1 – Port 1 setting.
- P2 – Port 2 setting.
- AN – Auto-negotiation.
- No AN – Forced speed.
- {link speed} – Expected link speed.
- The BCM57414 does not support independent link speed. All ports must operate at the same speed. For example, the ports cannot be set for port1 = 10G and port2 = 25G. Only the BCM5750X supports independent port speeds.

BCM957504 Supported Combinations of Link Speed Settings (10/25G-NRZ)

- All port link speeds are independent of each other.
- Each port can be configured as forced for any speed supported by the device.
- AN {link speeds} – Advertised supported auto-negotiation link speeds.

BCM957508 Supported Combinations of Link Speed Settings (25/50/100G NRZ and 50/100/200G PAM-4)

- All port link speeds are independent of each other.
- Each port can be configured as forced or auto-negotiate (NRZ Only) for any speed supported by the device.
- AN {link speeds} – Advertised supported auto-negotiation link speeds.
- PAM-4 support is enabled at a feature preview level with the following notes/restrictions:
 - PAM-4 operation on both ports is supported. NRZ operation on both ports is supported. PAM-4 operation on one port with NRZ operation on the other is not supported.
 - PAM-4 supports fixed speed mode only and must be configured through UEFI/HII.
 - PAM-4 support in this release is limited to DAC/Twinax cables.
 - PAM-4 operation on DAC/Twinax cables requires link training to be enabled. This requires a switch that supports link training an PAM-4.
 - PAM-4 requires FEC mode as RS544_1xN for 50G and 100G operation.
 - PAM-4 has been tested with the following DAC:
 - DAC Cable: Vendor: Amphenol QSFP56, Part num: NDAAXJ-0003
 - AOC Cable: Vendor: Optomind Inc, Part num: C4R448GA005AZZ
 - PAM-4 on Linux requires that 50/100G PAM-4 is enabled via UEFI menus only.
 - Currently the Linux kernel and associated tools have infrastructure to report link mode. From the reported link mode one can derive the encoding or lanes that may be used for that link. In a case where this is auto-negotiated, this works well. A device reporting a link mode of 100000baseCR2/Full uses a different number of lanes (and therefore encoding) than a device reporting 100000baseCR4/Full. Unfortunately when auto-negotiation is not used there is not ample infrastructure to specify speed and encoding and differentiate between a card using NRZ vs PAM-4 encoding. Currently ethtool supports setting speed, but does not have support for setting encoding or lanes used:

- **ethtool -s|--change DEVNAME** Change generic options

```
[ speed %d ]
[ duplex half|full ]
[ port tp|aui|bnc|mii|fibre ]
[ mdix auto|on|off ]
[ autoneg on|off ]
[ advertise %x ]
[ phyad %d ]
[ xcvr internal|external ]
[ wol p|u|m|b|a|g|s|d... ]
[ sopass %x:%x:%x:%x:%x:%x ]
[ msglvl %d | msglvl type on|off ... ]
```

Recent discussions have been occurring on the upstream Linux networking mailing list to address this problem.

- PAM-4 operation on VMware requires that 50/100G PAM-4 is configured via HII menu and also configured via ESXCLI commands. A reboot is required to ensure proper persistence of these parameters.
 - The command is: `esxcli network nic set -n <interface> -S <speed> -D full`

Example: `esxcli network nic set -n vmnic4 -S 200000 -D full`

- PAM-4 operation with 50/100G on Windows Server requires registry key modification.

Windows does not contain a PAM-4 signaling configuration parameter in adapter device advanced properties. For speeds supported by both NRZ and PAM-4, Windows will default to NRZ.

The following work around is required for PAM-4:

- a. Examine the NXE device in Windows Device Manager, Network Adapters, Broadcom xxx.
- b. Right mouse click and select properties, select Details tab, select Driver Key from the Property drop down, and record the last 4 digits after the backslash.
- c. Enter the registry editor (regedit.exe) and navigate to:
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}\xxx" where xxx is the number recorded previously.
 - Add a DWORD type value named "PreferredSignalingMode", and set the value to 1.
 - Save and exit the registry editor.
 - Disable and Enable device or Reboot server.

The expected link speeds based on the local and link partner settings are shown in [Table 32](#) and [Table 33](#).

Table 32: Expected Link Speeds (Forced)

Local Speed Settings	Link Partner Speed Settings						
	Forced 1G	Forced 10G	Forced 25G	Forced 50G	Forced 100G	Forced 200G	AN Enabled
Forced 1G	1G	No link	No link	No link	No link	No link	No link
Forced 10G	No link	10G	No link	No link	No link	No link	No link
Forced 25G	No link	No link	25G	No link	No link	No link	No link
Forced 50G	No link	No link	No link	50G	No link	No link	No link
Forced 100G	No link	No link	No link	No link	100G	No link	No link
Forced 200G	No link	No link	No link	No link	No link	200G	No link

Table 33: Expected Link Speeds (Auto-Negotiate)

Local Speed Settings	Link Partner Speed Settings								
	AN Enabled 1G	AN Enabled 10G	AN Enabled 25G	AN Enabled 1/10G	AN Enabled 1/25G	AN Enabled 10/25G	AN Enabled 1/10/25G	AN Enabled 10/25/50	AN Enabled 10/25/50/100
AN 1G	1G	No link	No link	1G	1G	No link	1G	No link	No link
AN 10G	No link	10G	No link	10G	No link	10G	10G	10G	10G
AN 25G	No link	No link	25G	No link	25G	25G	25G	25G	25G
AN 1/10G	1G	10G	No link	10G	1G	10G	10G	10G	10G
AN 1/25G	1G	No link	25G	1G	25G	25G	25G	25G	25G
AN 10/25G	No link	10G	25G	10G	25G	25G	25G	25G	25G
AN 1/10/25G	1G	10G	25G	10G	25G	25G	25G	25G	25G
AN 10/25/50G	No link	10G	25G	10G	25G	25G	25G	50G	50G
AN 10/25/50/100G	No link	10G	25G	10G	25G	25G	25G	50G	100G

To enable link speed auto-negotiation, the following options can be enabled in system BIOS HII menu:

System BIOS→NetXtreme-E NIC→Device Level Configuration

9.2.1 Operational Link Speed

This option configures the link speed used by the OS driver and firmware. This setting is overridden by the driver setting in the OS present state.

9.2.2 Auto-Negotiation Protocol

This is the supported auto-negotiation protocol used to negotiate the link speed with the link partner. This option must match the AN protocol setting in the link partner port. Broadcom Ethernet Network adapters support the following auto-negotiation protocols: IEEE 802.3by, 25G/50G consortiums and 25G/50G BAM. By default, this option is set to IEEE 802.3by + Consortium and Media Auto Detect enabled.

Link speed and flow control/pause must be configured in the driver in the host OS.

9.2.3 Windows Driver Settings

To access the Windows driver settings:

- Open **Windows Manager**→**Broadcom NetXtreme E Series adapter**→**Advanced Properties**→**Advanced** tab

To enable Flow Control/Pause frame AN:

- Flow Control = Auto-Negotiation

To enable link speed AN:

- Speed and Duplex = Auto-Negotiation

9.2.4 Linux Driver Settings

NOTE: For 10GBASE-T Broadcom Ethernet Network adapters, auto-negotiation must be enabled.

- `ethtool -s eth0 speed 25000 autoneg off` – This command turns off auto-negotiation and forces the link speed to 25 Gb/s.
- `ethtool -s eth0 autoneg on advertise 0x0` – This command enables auto-negotiation and advertises that the device supports all speeds: 1G, 10G, 25G (and 40G, 50G if applicable).

The following are supported advertised speeds.

- 0x020 – 1000BASE-T Full
- 0x1000 – 1000BASE-T Full
- 0x80000000 – 25000BASE-CR Full
- `ethtool -A eth0 autoneg on|off` – Use this command to enable/disable pause frame auto-negotiation.
- `ethtool -a eth0` – Use this command to display the current flow control auto-negotiation setting.

9.2.5 ESXi Driver Settings

NOTE: For 10GBASE-T Broadcom Ethernet Network adapters, auto-negotiation must be enabled. Using forced speed on a 10GBASE-T adapter results in ESXCLI command failure.

- `$ esxcli network nic get -n <iface>` – This command shows the current speed, duplex, driver version, firmware version and link status.
- `$ esxcli network nic set -S 10000 -D full -n <iface>` – This command sets the forced speed to 10 Gb/s.
- `$ esxcli network nic set -a -n <iface>` – This enables link speed auto-negotiation on interface <iface>.
- `$ esxcli network nic pauseParams list` – Use this command to get pause Parameters list.
- `$ esxcli network nic pauseParams set --auto <1/0> --rx <1/0> --tx <1/0> -n <iface>` – Use this command to set pause parameters.

NOTE: Flow control/pause auto-negotiation can be set only when the interface is configured in link speed auto-negotiation mode.

9.3 Configuring 200G Link Speeds

Provides information for manually configuring 200G link speeds on Ethernet network adapters and switches.

The BCM57508 network adapter supports 200 gigabit per second link speed using QSFP56 optical transceivers or direct attach copper (DAC) cables. By default, 200G speed is disabled, allowing the more common 2 x 100G configuration to operate as expected. To use 200G speeds, the BCM57508 network adapter must be updated and special care must be taken with configuration of the network switch to enable the required PAM-4 modulation parameters and Forward Error Correction (FEC) mode.

NOTE: 200G link speeds are only supported on BCM57508-N2100D and BCM57508-P2100D network adapters.

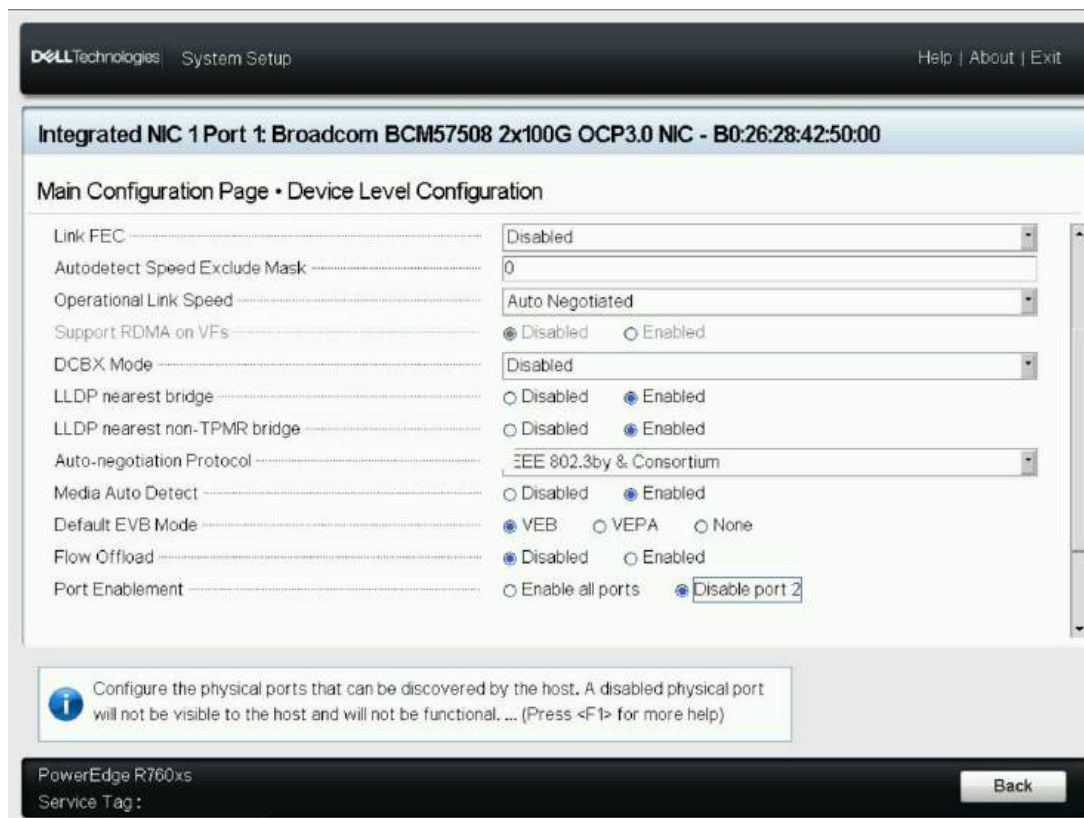
By default, the BCM57508 network adapter is configured as a 2-port device, supporting up to 100G on each port. To use 200G speed, the device must be reconfigured as a 1-port device and the 200G link speed must be enabled.

9.3.1 Auto-Negotiation Configuration for 200G

Provides information for auto-negotiating 200G link speeds on Ethernet network adapters.

9.3.1.1 UEFI Configuration

1. Set the Autodetect Speed Exclude Mask to 0.
2. Set Port Enablement to Disable port 2 as shown in the following figure.



A system reboot is required for this change to take effect.

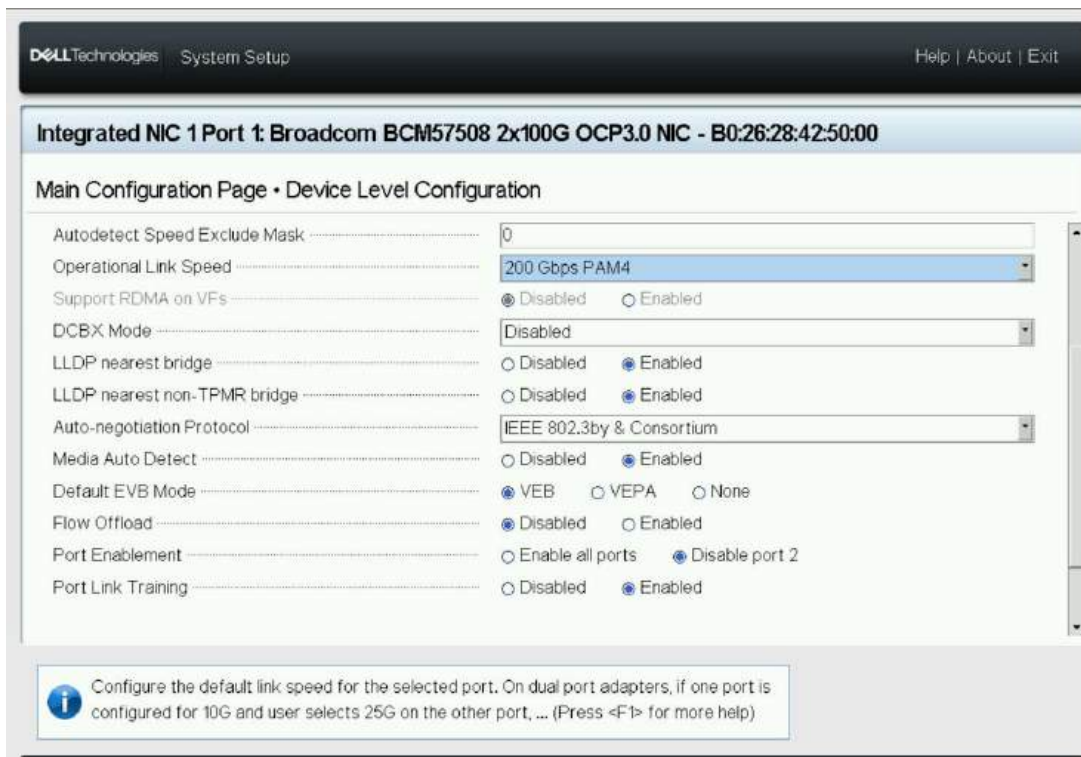
9.3.2 Forced 200G Configuration

Provides information for manually configuring 200G link speeds on Ethernet network adapters.

9.3.2.1 UEFI Configuration

To reconfigure the BCM57508 network adapter as a 1-port, 200G device.

1. Set the port speed to 200Gbps PAM-4.
2. Set Port Enablement to Disable port 2 as shown in the following figure.
3. Set Port Link Training to match the switch settings (Dell switch default setting is enabled).



9.3.3 Configuring Dell Switches

When using a Dell OS10 switch for 200G operation with DAC cables, the default interface configuration must be changed to set the port group profile to 200x2, enable Link Training, and Forward Error Correction. When using 200G optical transceivers only the speed must be set.

NOTE: OS10 version 10.5.3.4 or later must be used.

```
enable
configure
port-group <Group ID>
port <Port ID> mode Eth 200g-2x
exit
```

```
interface range ethernet <Port ID>:1-ethernet<Port ID>:5
fec CL119-RS
negotiation off
```

10 PXE Boot

To serve PXE requests from PXE clients, a PXE server must be configured. The PXE server can be configured to run regular PXE or iPXE. Regular PXE is a network boot program that downloads config files over TFTP from the PXE server. iPXE is an enhanced implementation of the PXE client firmware and a network boot program that uses iPXE scripts rather than config files and can download scripts and images with HTTP.

NOTE: UEFI mode PXE boot is supported on physical functions as well as NIC partitions, whereas legacy mode PXE boot is supported only on physical functions.

The procedure for configuring the PXE server is discussed in [PXE Server Configuration](#).

10.1 UEFI Mode

Enable PXE for the Broadcom adapter interface in **Network Configuration** under **System Setup**. Refer to the documentation from the server manufacturer on how to enable PXE on the particular server model.

10.1.1 iPXE

Download the `ipxe.efi` boot loader file using TFTP from the PXE server.

```
Booting from PXE Device 1: NIC in Slot 1 Port 1 Partition 1

>>Start PXE over IPv4.
  Station IP address is 174.30.10.18

  Server IP address is 174.30.10.10
  NBP filename is ipxe/ipxe.efi
  NBP filesize is 974496 Bytes
  Downloading NBP file...

  NBP file downloaded successfully.
  iPXE initialising devices...ok

iPXE 1.0.0+ -- Open Source Network Boot Firmware -- http://ipxe.org
Features: DNS HTTP iSCSI TFTP SRP ULAN AoE EFI Menu

net4: b0:26:28:cb:12:70 using 14e4-16d7 on 0000:3b:00.0 (open)
  Link:up, TX:0 TXE:0 RX:0 RXE:01
Configuring (net4 b0:26:28:cb:12:70) ..... ok
net4: 174.30.10.12/255.255.0.0 gw 174.30.10.10
Next server: 174.30.10.10
Filename: ipxe/legacymenu.ipxe
tftp://174.30.10.10/ipxe/menu.ipxe...
```

10.1.2 PXE

The boot loader file is downloaded via TFTP from the PXE server automatically.

```
Booting from PXE Device 1: NIC in Slot 1 Port 1 Partition 1

>>Start PXE over IPv4.
  Station IP address is 174.30.10.18

  Server IP address is 174.30.10.10
  NBP filename is BOOTX64.EFI
  NBP filesize is 1301312 Bytes
  Downloading NBP file...

  NBP file downloaded successfully.
  Fetching Netboot Image
  -
```

The menu items from the `grub.cfg` file are listed.

```
RHEL 6.5
RHEL 7.3
SLES11 SP3
SLES 12
CentOS 7
Windows 2019 Datacentre
ESX 6.7
```

```
Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

Additional files are downloaded from the PXE server over TFTP based on the menu selection and the PXE boot continues.

10.1.3 Secure Boot

Secure boot is a UEFI based feature developed by UEFI forum to increase security in the pre-boot environment. Secure boot minimizes the threat of potential attacks between firmware initiation and operating system loading.

This feature halts the execution of unsigned code before the operating system boots. Any unsigned firmware running on the adapter is not allowed to run. Only adapters running digitally signed firmware images are listed in preboot configuration menus and network boot options.

To enable this security feature, select **Enable Secure Boot** in the **System Setup Menu**. This option is only available on server platforms that support secure boot. The menu under which the secure boot option is listed varies between server vendors.

Figure 40: Security Menu Example

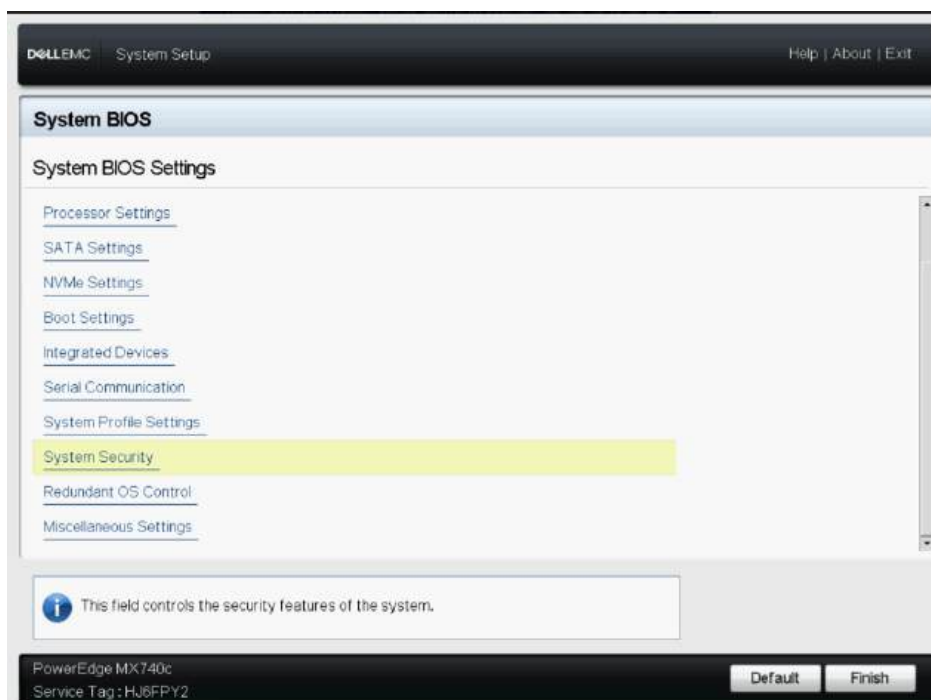


Figure 41: Enable Secure Boot Example

10.2 PXE Server Configuration

The PXE server is operating system independent. A PXE server is any host that can lease out DHCP IPs to any requesting PXE Client, point to a boot loader file, and transfer further configuration and boot files to the PXE client over any application level protocol.

This section explains how to setup a PXE server on a RHEL/CentOS-based OS. For Windows deployment services, refer to documentation provided on the Microsoft Technet website. For setting up PXE servers on any other operating system, refer to the documentation provided by the respective operating system.

10.2.1 DHCP Configuration for PXE/iPXE

To add the DHCP feature on the PXE server, use the following command:

```
yum install dhcp
```

NOTE: All IP addresses mentioned in this section are for illustration purposes only. They can be modified to match the subnet that the PXE server is configured in.

10.2.1.1 IPv4 DHCP Configuration

To configure an interface with static network settings using `ifcfg` files, for an interface with the name `p1p1`, create a file with name `ifcfg-p1p1` in the `/etc/sysconfig/network-scripts/` directory as follows:

```
DEVICE=p1p1
TYPE=Ethernet
BOOTPROTO=none
ONBOOT=yes
IPADDR=174.30.10.10
NETMASK=255.255.0.0
```

10.2.1.1.1 iPXE

To run iPXE, in the `/etc/dhcp/dhcpd.conf` file, make the following changes:

NOTE: The IP addresses used in this section are for examples only.

```
option ipxe.no-pxedhcp 1;

subnet 174.30.10.0 netmask 255.255.0.0 {
    option routers 174.30.10.10;
    range 174.30.10.11 174.30.10.50;
    next-server 174.30.10.10;
    option subnet-mask 255.255.0.0;
    default-lease-time 3600;
    max-lease-time 4800;
    class "pxeclients" {
        match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
        if not exists ipxe.bus-id {
            next-server 174.30.10.10;
            if option arch = 00:06 {
                filename "ipxe/ipxe-x86.efi";
            } elseif option arch = 00:07 {
                filename "ipxe/ipxe.efi"; # iPXE.efi built with support for Broadcom adapters
            } elseif option arch = 00:00 {
                filename "ipxe/ipxe.pxe"; # iPXE.pxe built with support for Broadcom adapters
            }
        } else {
            next-server 174.30.10.10;
            filename "ipxe/menu.ipxe"; # iPXE boot menu
        }
    }
}
```

10.2.1.1.2 PXE

To run PXE, in the `/etc/dhcp/dhcpd.conf` file, make the following changes:

```
ddns-update-style none;
default-lease-time 600;

option space PXE;
option PXE.mtftp-rcode 1 = ip-address;
option PXE.mtftp-cport code 2 = unsigned integer 16;
option PXE.mtftp-sport code 3 = unsigned integer 16;
option PXE.mtftp-tmout code 4 = unsigned integer 8;
option PXE.mtftp-delay code 5 = unsigned integer 8;
option arch code 93 = unsigned integer 16;
allow booting;
allow bootp;
allow unknown-clients;

subnet 174.30.0.0 netmask 255.255.0.0 {
    default-lease-time 600;
    max-lease-time 6000;
    range 174.30.10.11 174.30.10.50; #
    class "pxeclients" {
        match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
        next-server 174.30.10.10;
        if option arch = 00:06 {
            filename "bootia32.efi";
        } else if option arch = 00:07 {
            filename "BOOTX64.EFI";
        } else {
            filename "pxelinux/pxelinux.0";
        }
    }
}
```

To bind a certain hardware MAC address to an IP in the DHCP range, add the following to the `dhcpd.conf` file.

```
host server1-adapter1-port1 {
    hardware ethernet 00:0A:F7:94:F7:A4;
    fixed-address 174.30.10.15;
}
```

To restart the network service, run the following command:

```
service network restart
```

To restart the DHCP service, run the following command:

```
service dhcpd restart
```

10.2.1.2 IPv6 DHCP Configuration

In `/etc/sysconfig/network`, make the following changes:

```
NETWORKING_IPV6=yes
IPV6FORWARDING=no
IPV6_AUTOCONF=no
IPV6_AUTOTUNNEL=no
```

In `/etc/sysconfig/network-scripts/ifcfg-<interface_name>` make the following changes:

```
IPV6_AUTOCONF=no
IPV6INIT=yes
IPV6ADDR=2015:9:19:ffff::10/64 # Replace with your static address
```

10.2.1.2.1 iPXE

In `/etc/dhcpd/dhcpd6.conf` file, make the following changes:

```
default-lease-time 2592000;
preferred-lifetime 604800;
option dhcp-renewal-time 3600;
option dhcp-rebinding-time 7200;
allow leasequery;
option dhcp6.info-refresh-time 21600;
dhcpv6-lease-file-name "/var/lib/dhcpd/dhcpd6.leases";

option dhcp6.user-class code 15 = string;
option dhcp6.bootfile-url code 59 = string;
option dhcp6.client-arch-type code 61 = array of unsigned integer 16;
option dhcp6.name-servers 2015:9:19:ffff::10;

subnet6 2015:9:19:ffff::/64 {
    range6 2015:9:19:ffff::11 2015:9:19:ffff::500;
    if exists dhcp6.client-arch-type and option dhcp6.client-arch-type = 00:07 {
        option dhcp6.bootfile-url "tftp://[2015:9:19:ffff::10]/ipxe/ipxe.efi";
    } elsif exists dhcp6.client-arch-type and option dhcp6.client-arch-type = 00:00 {
        option dhcp6.bootfile-url "tftp://[ 2015:9:19:ffff::10]/pxelinux/pxelinux.0";
    } elsif exists dhcp6.user-class and substring(option dhcp6.user-class, 2, 4) = "iPXE" {
        option dhcp6.bootfile-url "tftp://[2015:9:19:ffff::10]/ipxe/menu.ipxe";
    }
}
```

10.2.1.2.2 PXE

In `/etc/dhcpd/dhcpd6.conf` file, make the following changes:

```
default-lease-time 2592000;
preferred-lifetime 604800;
option dhcp-renewal-time 3600;
option dhcp-rebinding-time 7200;
allow leasequery;
option dhcp6.info-refresh-time 21600;
dhcpv6-lease-file-name "/var/lib/dhcpd/dhcpd6.leases";

option dhcp6.user-class code 15 = string;
option dhcp6.bootfile-url code 59 = string;
```

```
option dhcp6.client-arch-type code 61 = array of unsigned integer 16;
option dhcp6.name-servers 2015:9:19:ffff::10;

subnet6 2015:9:19:ffff::/64 {
    range6 2015:9:19:ffff::11 2015:9:19:ffff::500;
    if exists dhcp6.client-arch-type and option dhcp6.client-arch-type = 00:07 {
        option dhcp6.bootfile-url "tftp://[2015:9:19:ffff::10]/BOOTX64.EFI ";
    } elsif exists dhcp6.client-arch-type and option dhcp6.client-arch-type = 00:00 {
        option dhcp6.bootfile-url "tftp://[ 2015:9:19:ffff::10]/pxelinux/pxelinux.0";
    }
}
```

To restart the network service, run the following command:

```
service network restart
```

To restart the DHCPv6 service, run the following command:

```
service dhcpd6 restart
```

10.2.1.3 DHCP with VLAN

In `/etc/sysconfig/network-scripts`, make a copy of the interface file for the interface over which VLAN must be configured.

Example: `ifcfg-p1p1` and `ifcfg-p1p1.5`

NOTE: 5 indicates that the interface will use VLAN ID 5.

In the new VLAN interface file, add the parameter `VLAN=yes`.

UUID can be generated for this new interface using the command `uuidgen p1p1.5`.

In the file `/etc/dhcp/dhcpd`, add a scope for the VLAN interface so that the DHCP server leases DHCP IPs on the VLAN interface.

10.2.2 TFTP Configuration

To configure TFTP:

1. Add the TFTP, XINET packages.

```
yum install xinetd tftp-server
```

2. In the `/etc/xinetd.d/tftp` file, make the following changes.

```
service tftp
{
    socket_type= dgram
    protocol= udp
    wait      = yes
    user      = root
    server    = /usr/sbin/in.tftpd
    server_args= -s /var/lib/tftpboot -6
    disable   = no
    per_source= 11
    cps       = 100 2
    flags     = IPv6
}
```

The base path for the TFTP server is `/var/lib/tftpboot/`.

10.2.2.1 IPXE

Under the TFTP root directory, create a new folder called `ipxe` and add the `ipxe.efi` and `ipxe.pxe` files to it. Also add the `menu.ipxe` file to it, which can chain more iPXE files to list the menu based on the boot mode.

```
#!/ipxe
iseq ${platform} efi && goto uefibios || goto legacybios

:uefibios
echo Loading the UEFI Menu
chain --replace --autofree ${menu-url}efimenu.ipxe

:legacybios
echo Loading the LEGACY Menu
chain --replace --autofree ${menu-url}biosmenu.ipxe
```

All the chained files are to be present in the `<TFTP_root>/ipxe` directory.

10.2.2.2 PXE

Create a new directory `pxelinux` in the TFTP root. Extract the Syslinux package and move the contents to the `<TFTP_root>/pxelinux` directory.

The TFTP root must contain the boot loader file from the target OS. The boot loader file can be copied from the `/boot/efi/EFI/<OS_flavor>` directory on the target OS. It should be renamed to `BOOTX64.EFI`.

Create `grub.cfg` file in the TFTP root and add UEFI mode PXE boot menu items to the same.

```
default=0
timeout=10

title RedHat 7u5
    root (nd)
    kernel /images/rhel75/vmlinuz inst.driver=vesa nomodeset method=http:// 174.30.10.10/images/
RHEL75linux dd
    initrd /images/RHEL7.2/initrd.img ip=dhcp

title SLES12SP4
    root (nd)
    kernel images/sles12sp4/vmlinuz inst.driver=vesa nomodeset inst.repo=http:// 174.30.10.10/
images/SLES12SP4
    initrd /images/sles12sp4/initrd.img ip=dhcp
```

Create `pxelinux.cfg/default` file and add BIOS mode PXE boot menu items to it.

```
DEFAULT menu.c32
PROMPT 0
TIMEOUT 10
MENU TITLE BIOS mode PXE menu

LABEL localdisk
MENU LABEL ^Local Hard Drive
LOCALBOOT 0

LABEL RHEL75
MENU LABEL ^RedHat 7u5
KERNEL images/rhel75/vmlinuz
APPEND initrd=images/rhel75/initrd.img ramdisk_size=200000 ip=dhcp inst.xdriver=vesa nomodeset
inst.repo=http://174.30.10.10/images/RHEL75

LABEL SLES12SP4
MENU LABEL ^SLES 12 SP 4
KERNEL images/sles12sp4/vmlinuz
APPEND initrd=images/sles12sp4/initrd.img ramdisk_size=200000 ip=dhcp inst.xdriver=vesa nomodeset
inst.repo=http://174.30.10.10/images/SLES12SP4
```

Create a new directory `images` in the TFTP root. Sub-directories can be created to match the kernel image path specified in `grub.cfg` and `pxelinux.cfg/default` files. Copy the `vmlinuz` and `initrd.img` files from the `/boot` directory of the target OS's to these sub-directories.

To restart the TFTP service, run the following command:

```
service xinetd restart
```


10.2.3 HTTP Configuration

To configure HTTP:

1. Add the HTTP feature using the following command:

```
yum install httpd
```

`/var/www/html/` is the base path for the HTTP server. The conf file is present in `/etc/httpd/conf/httpd.conf`.

2. To restart the HTTP service, run the following command:

```
service httpd restart
```

To specifically make HTTP listen on certain interfaces, in the `/etc/httpd/conf/httpd.conf` file, add the `LISTEN` directive for all the required interfaces.

```
Listen 192.0.2.1:80
Listen 192.0.2.5:8000
Listen 174.30.10.10:80
```

If this is not specified, the server listens on all interfaces.

3. Create a new directory `images` in the HTTP root. Subdirectories can be created to match the installation repository path specified in `grub.cfg` and `pxelinux.cfg/default` files. Extract the contents of the installation media of the target OS's to these sub-directories.

11 SR-IOV – Configuration and Use Case Examples

11.1 Enable SR-IOV in BIOS/UEFI and Device

To enable SR-IOV in BIOS/UEFI and Device:

1. Enable SR-IOV in the NIC cards:
 - a. SR-IOV in the NIC card can be enabled using the HII menu. During system boot, access the system **BIOS**→**NetXtreme-E NIC**→**Device Level Configuration** menu.
 - b. Set the **Virtualization** mode to **SR-IOV**.
 - c. Set the number of virtual functions per physical function.
 - d. Set the number of MSI-X vectors per the VF and Max number of physical function MSI-X vectors. If the VF is running out of resources, balance the number of MSI-X vectors per VM.
2. Enable virtualization in the BIOS:
 - a. During system boot, enter the system **BIOS** →**Processor settings**→**Virtualization Technologies** and set it to **Enabled**.
 - b. During system boot, enter the system **BIOS** →**SR-IOV Global** and set it to **Enabled**.

11.2 Linux Use Case Example: SR-IOV Pass-Through to libvirt Virtual Machine

1. Install the desired Linux version with Virtualization enabled (libvirt and Qemu).
2. Enable the IOMMU kernel parameter.
 - a. The IOMMU kernel parameter is set by appending `intel_iommu=on` to the kernel command line
3. Use in-box driver, or install the driver as shown in [Installing the Linux Driver](#).
4. Enable Virtual Functions through kernel parameters:
 - a. Once the driver is installed, `lspci` displays the Broadcom Ethernet Network adapter physical interfaces present in the system.
 - b. To activate Virtual functions, use the following command:

```
echo X > /sys/class/net/<ifname>/device/sriov_numvfs
```

NOTE: Ensure that the physical interface (<interface>) is up. VFs are only created if PFs are up. X is the number of VFs that are exported to the OS.

Example: `echo 4 > /sys/class/net/eth1/device/sriov_numvfs`

5. Check the PCIe virtual functions exist with `lspci`.
6. Create new virtual machine from installation ISO file.
7. Select **Customize configuration before install**.
8. Select **Add Hardware** → **PCI Host Device** → **Virtual Function**.
9. Finish installation. The VM detects Broadcom Ethernet Network adapter. Use either the in-box driver from the installed operating system or the install driver as shown in [Installing the Linux Driver](#).

11.2.1 Setting MAC Address for the VF

The MAC address of each VFs can set using the `ip link set MAC` command.

Example:

```
ip link set <pf ifname> vf 0 mac xx:xx:xx:xx:xx:xx
```

"ip link show" can show the VFs and associated MAC addresses.

Use "virsh start <VM name>"

Optional: `virsh vcpupin <VM-Name> 0 <CPU Number>` can be used to run the VM on a specific CPU.

11.3 Windows SR-IOV Use Case Example

NOTE: To obtain the maximum number of virtual functions per PF, disable **Virtual Switch RSS** and set the **Maximum Number of RSS Queues** to 1 from the driver advanced properties.

1. Install the latest KB update for your Windows 2012 R2 or Windows 2016 OS.
2. Install the appropriate Virtualization (Hyper-V) options. For more detail requirements and steps on setting up Hyper-V, Virtual Switch, and Virtual Machine, visit [Microsoft.com](https://www.microsoft.com).
3. Install the latest Broadcom Ethernet Network adapter driver on the Hyper-V as shown in [Installing the Windows Driver](#).
4. Enable SR-IOV in the NDIS miniport driver advanced properties.
5. In Hyper-V Manager, create your Virtual Switch with the selected Broadcom Ethernet Network adapter interface.
6. Check the **Enable Single-Root I/O Virtualization (SR-IOV)** box while creating the Hyper-V Virtual Adapter.
7. Create a Virtual Machine (VM) and add the desired number of Virtual Adapters.
8. Under the Virtual Machine's Network Adapter settings for each Virtual Adapter, check **Enable SR-IOV** under the **Hardware Acceleration** section.
9. Launch your VM and install the desired guest OS.
10. Use the in-box driver from the VM operating system, or install the Broadcom Ethernet Network adapter driver as shown in [Installing the Windows Driver](#).

NOTE: The Virtual Function (VF) driver for Broadcom Ethernet Network adapters is the same driver as the base driver. For example, if the guest OS is Windows 2012 R2, the user needs to install Bnxtnd64.sys in VM. The user can do this by running the Broadcom Ethernet Network adapter driver installer executable. Once the driver has been installed in the guest OS, the user can see the VF driver interface(s) appearing in Device Manager of the guest OS in the VM.

NOTE: When updating the network adapter settings on a Hyper-Visor VM that is bound to a VF on a network adapter, the properties in the Microsoft Synthetic Network Adapter on the VM should be changed first, followed by a corresponding change in the properties on the VF.

11.4 VMware SR-IOV Use Case Example

NOTE: For Windows guest operating systems, to obtain the maximum number of virtual functions per PF, disable **Virtual Switch RSS** and set the **Maximum Number of RSS Queues** to 1 from the driver advanced properties.

1. On ESXi, install the driver as shown in [Installing the VMware Driver](#).

2. Enable SR-IOV VFs:

Only the physical functions (PFs) are automatically enabled. If a PF supports SR-IOV, the PF (vmknicX) is part of the output of the command shown below.

```
esxcli network sriovnic list
```

To enable one or more virtual functions (VFs), the driver uses the module parameter `max_vfs` to enable the desired number of VFs per PF. For example, to enable four VFs on PF1:

```
esxcfg-module -s 'max_vfs=4' bnxtnet (reboot required)
```

To enable VFs on a set of PFs, use the command format shown below. For example, to enable four VFs on PF 0 and 2 VFs on PF 2:

```
esxcfg-module -s 'max_vfs=4,2' bnxtnet (reboot required)
```

The required VFs of each supported PF are enabled in order during the PF bring up. See the VMware documentation for information on how to map a VF to a VM.

NOTE: When using NPAR + SR-IOV, every NPAR function (PF) is assigned a maximum of eight VFs.

NOTE: For a VF to be in promiscuous mode, one of the following conditions must be true:

- The VF should be associated with a default VLAN.
- The VF should be a trusted VF.

If none of the above conditions are true, the VF will not be in promiscuous mode and, therefore, will not see packets received by the PF.

12 NPAR – Configuration and Use Case Example

12.1 Features and Requirements

- OS/BIOS Agnostic – The partitions are presented to the operating system as real network interfaces so no special BIOS or OS support is required like SR-IOV.
- Additional NIC functions without requiring additional switch ports, cabling, PCIe expansion slots.
- Traffic Shaping – The allocation of bandwidth per partition can be controlled to limit or reserve as needed.
- Can be used in a Switch Independent manner – The switch does not need any special configuration or knowledge of the NPAR enablement.
- Can be used in conjunction with RoCE and SR-IOV.
- Supports stateless offloads such as LSO, TPA, RSS/TSS, and RoCE (two PFs per port only).
- Alternative Routing-ID support for greater than eight functions per physical device.

NOTE: In the **UEFI HII Menu** page, the NXE adapters support up to 16 PFs per device on an ARI capable system. For a 2-port device, this means up to 8 PFs for each port.

12.2 Limitations

NOTE: An NPAR configuration where a team, virtual switch (simple or distributed), or a logical network switch (N-VDS) contains more than one partition from the same physical port is not supported.

- Shared settings must be suppressed to avoid contention. For example: Speed, Duplex, Flow Control, and similar physical settings are hidden by the device driver to avoid contention.
- Non-ARI systems enable only eight partitions per physical device.
- RoCE + SRIOV + NPAR combination is not supported.
- RoCE for BCM5741X adapters, is only supported on the first two partitions of each physical port, or a total of four partitions per physical device. BCM9575XX adapters can support RoCE on all partitions.
- NPAR + SR-IOV/MultiRSS is not supported with ESXi 7.0 for the BCM5741X.
- Teaming partitions within the same physical port are not supported.
- LACP teaming is not supported.

12.3 Configuration

NPAR can be configured using BIOS configuration HII menus on legacy boot systems. Some vendors also expose the configuration via additional proprietary interfaces.

To enable NPAR:

1. Select the target NIC from the BIOS HII Menu and set the Multi-Function Mode or Virtualization Mode option. The choice of options affects the whole NIC instead of the individual port.

Integrated NIC 1 Port 1: Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Main Configuration Page • Device Level Configuration

Broadcom Adv. Dual 25Gb Ethernet - B0:26:28:C4:06:7A

Virtualization Mode NPar

NParEP Mode None

Number of MSI-X Vectors per VF NPar

Maximum Number of PF MSI-X Vectors SR-IOV

Link FEC NPar + SR-IOV

Operational Link Speed Disabled

Firmware Link Speed Auto Negotiated

DCBX Mode Auto Negotiated

LLDP nearest bridge Disabled

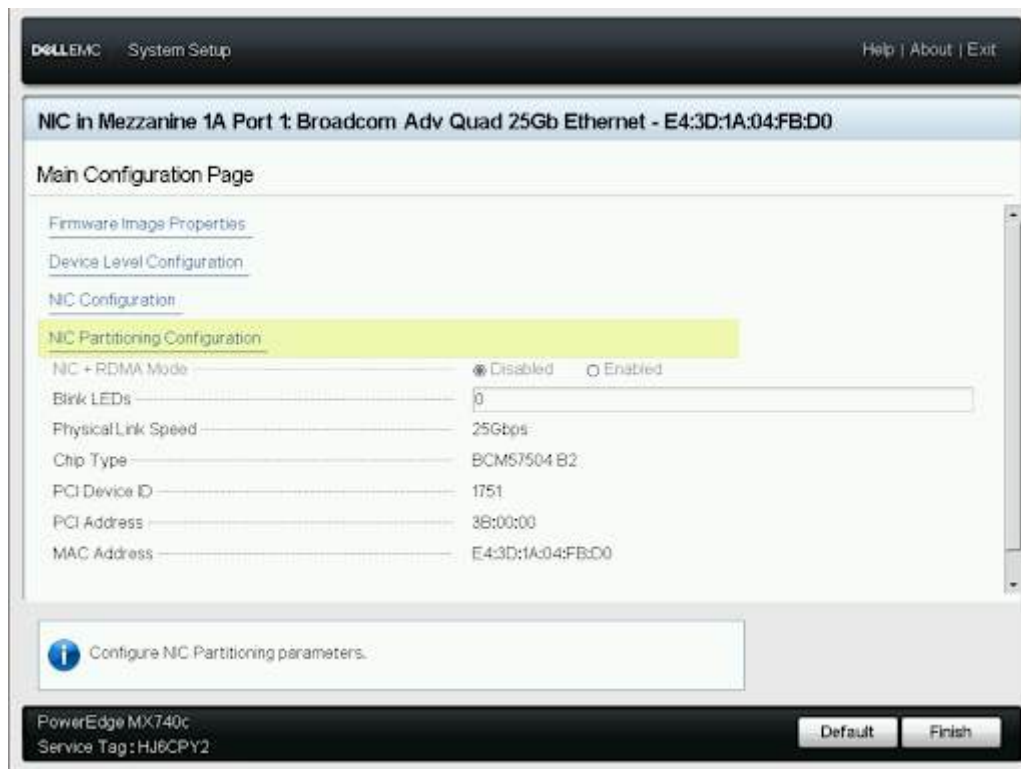
LLDP nearest non-TPMR bridge Enabled

Auto-negotiation Protocol Disabled

IEEE and Consortium

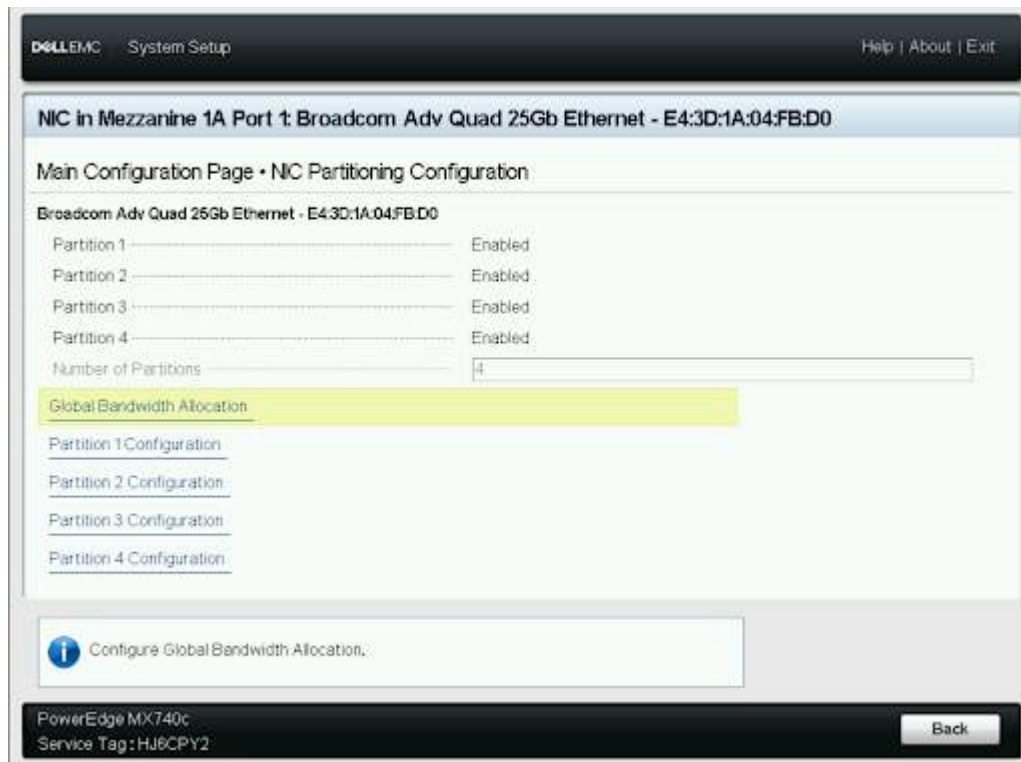
NOTE: For some ARI capable OEM systems, the **NParEP** button is available to explicitly allow the Broadcom Ethernet Network adapter to support up to 16 partitions. Switching from single function mode to multifunction mode, the device needs to be re-enumerated, therefore changes do not take effect until a system reboot occurs.

2. Once NPAR is enabled, the **NIC Partitioning Main Configuration** menu option is available from the main NIC Configuration Menu associated with each physical port.



3. The NIC Partition Configuration Menu (shown below) allows the user to choose the number of partitions that should be allocated from the selected physical port. Each Broadcom Ethernet Network adapter can support a maximum of 16 partitions on an ARI capable server. By default, dual-port adapters are configured for eight partitions per physical port.

Configuration options for each partition are also accessible from this menu. For some OEM systems, the HII menu also includes a Global Bandwidth Allocation page where the minimum (reserved) and maximum (limit) TX bandwidth for all partitions can be configured.



4. Set the NIC Partition Configuration parameters (see [Table 34](#)).



Table 34: NPAR Parameters

Parameter	Description	Valid Options
BW Limit	Maximum percentage of available bandwidth this partition is allowed.	Value 0 to 100
BW Limit Valid	Functions as an on/off switch for the BW Limit setting.	True/False
RDMA Support	Functions as an on/off switch for RDMA support on this partition. NOTE: Only two partitions per physical port can support RDMA. For a dual-port device, up to 4 NPAR partitions can support RDMA.	Enabled/Disabled

NOTE: The NPAR minimum bandwidth parameter cannot be changed on the BCM575XX. BCM5741X devices are permitted to change the NPAR minimum value.

12.4 Reducing NIC Memory Consumption with NPAR

The default value of receive buffers was selected to work well for typical configurations. If you have many NICs in a system, have enabled NPAR on multiple NICs, or you have only a small amount of RAM, you may see a Code 12 yellow bang in the Device Manager for some of the NICs. Code 12 means that the driver failed to load because there were not enough resources. In this case, the resource is a specific type of kernel memory called Non-Paged Pool (NPP) memory.

If you are getting a Code 12, or for other reasons wish to reduce the amount of NPP memory consumed by the NIC:

- Reduce the number of RSS queues from the default of 8 to 4 or 2. Each RSS queue has its own set of receive buffers allocated, so reducing the number of RSS queues reduces the allocated NPP memory. There can be performance implications from reducing the number of RSS queues, as fewer cores participate in processing receive packets from that NIC. Per processor CPU utilization should be monitored to ensure that there are no “hot” processors after this change.
- Reduce memory allocation by reducing the number of receive buffers allocated. The default value of 0 means the driver should automatically determine the number of receive buffers. For typical configurations, a setting of 0 (=auto) maps to XXXX receive buffers per queue. You can choose a smaller value such as 1500, 1000, or 500. (The value needs to be in multiples of 500 and between the range of 500 and 15000.) As mentioned above, a smaller number of receive buffers increases the risk of packet drop and a corresponding impact to packet retransmissions and decreased throughput.

The parameters “Maximum Number of RSS Queues” and “Receive Buffers (0=Auto)” can be modified using the **Advanced** properties tab for each NIC in the **Device Manager**. If you want to modify multiple NICs at the same time, it is faster to use the *Set-NetAdapterAdvancedProperty PowerShell cmdlet*. For example, to assign two RSS queues for all NICs in a system whose NIC name starts with “SI”, run the following command:

```
Set-NetAdapterAdvancedProperty SI* -RegistryKeyword *NumRSSQueues -RegistryValue 2
```

Similarly, to set the number of Receive buffers to 1500, run the following command:

```
Set-NetAdapterAdvancedProperty SI* -RegistryKeyword *ReceiveBuffers -RegistryValue 1500
```

For an overview of how to use PowerShell to modify NIC properties, see [Microsoft.com](https://www.microsoft.com).

12.5 Advanced NPAR

Advanced NPAR is known as switch dependent partitioning or Virtual Ethernet Port Aggregator (VEPA) Multi-Channel QinQ. The switch performs all switching between partitions and replication of broadcast and multicast packets.

Figure 42: S-Tag Frame

Destination MAC	Source MAC	802.1 Q Header (S-TAG)	802.1 Q Header (C-TAG)	IP Header	TCP Header	PayLoad

Figure 43: S-Tag Header

Tag Protocol ID (TPID) 2 bytes		PCP 3 bits	DEI 1 bit	C-VLAN ID 12 bits
0x88/0x91	0xa8/0x00			

Figure 44: C-Tag Header

Tag Protocol ID (TPID) 2 bytes		PCP 3 bits	DEI 1 bit	C-VLAN ID 12 bits
0x81	0x00			

Table 35: Advanced NPAR Terms

Term	Definition
TPID	Tag Protocol ID
S-VLAN	Stacked VLAN. Double VLAN tag structure allows service providers to add VLAN tags (S-Tag) to forward frame traffic across the network.
S-Tag	Service VLAN tag.
C-VLAN	The VLAN that a customer uses in double tag frames.
C-Tag	Customer VLAN tag. The inner VLAN tag in a double tag frame.
Intra-Partition Traffic	The traffic between the PF and VFs of a partition.
Inter-Partition Traffic	The traffic between PCIe functions on different partitions.
PF	NIC physical function.
VF	NIC virtual function.

12.5.1 Supported Broadcom Devices

- BCM57508-NGM2100D
- BCM57504-NGM425D

12.5.2 Supported Operating Systems

- VMware ESXi 7 u3 and higher, ESXi 8.0 and higher

12.5.3 Supported Features and Limitations

Supported Features:

- The OS driver via in-band utility or uEFI menu (Dell) can set features. Advanced NPAR related configuration is set through the BMC and UEFI drivers.
- RoCE v2 traffic inherits the S-VID from VF or PF.
- Stateless offloads on PF and VF levels are supported and independent of the NPAR mode.
- QoS is supported for the egress traffic on partition.

Limitations:

- OS-BMC is unsupported when Advanced NPAR is enabled.
- The options can only be set in HII menu for certain release (2.26).
- User tool, bnxtnvm, does not show the S-Tag options.
- When operating in Advanced NPAR mode, only the Ethernet adapter firmware can see the LLDP packets.
- NIC Teaming: Switch dependent teaming is not supported in the Advanced NPAR mode.

12.5.4 Supported Hardware Configurations

PF/VF (SR-IOV) Configuration:

- Number PFs/Adapter: Max 16 PFs.
- Number PFs/Port: 16/(number of ports). Example: 16/2 ports = 8 per port.
- Number VFs/Adapter: Max 128 VFs
- Number VFs/PF: Max 64 VFs. The number of VFs/PF shall be in multiples of 8.

12.5.5 Required Hardware Settings

Required hardware settings:

- Advanced NPAR mode enabled.
- DCBX = disabled
- Default EVB mode = VEPA (enabled)

NOTE: Ensure that EVB mode is set to VEPA (shown in [Figure 46](#)). No other mode is supported.

Figure 45: UEFI Menu for Advanced NPAR Mode

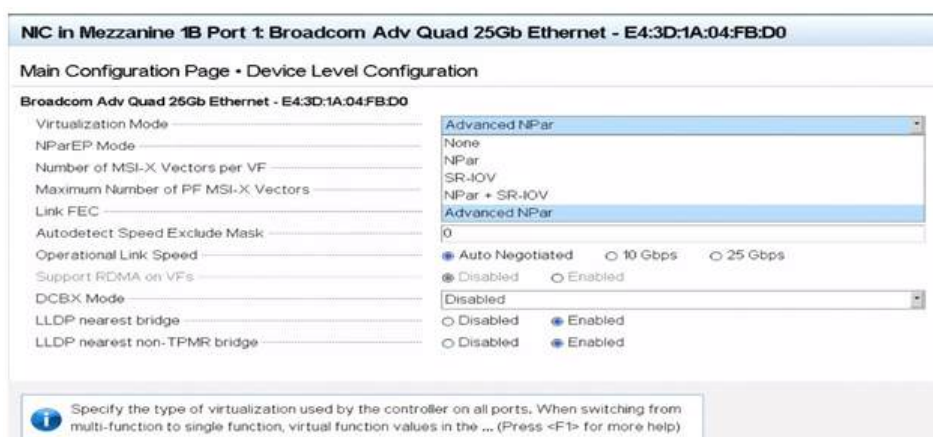


Figure 46: UEFI Menu for DCBX and EVB Modes

NIC in Mezzanine 1B Port 1: Broadcom Adv Quad 25Gb Ethernet - E4:3D:1A:04:FB:D0

Main Configuration Page • Device Level Configuration

Autodetect Speed Exclude Mask

0

Operational Link Speed

☒ Auto Negotiated ☐ 10 Gbps ☐ 25 Gbps

Support RDMA on VFs

☒ Disabled ☐ Enabled

DCBX Mode

Disabled

LLDP nearest bridge

☐ Disabled ☒ Enabled

LLDP nearest non-TPMR bridge

☐ Disabled ☒ Enabled

Auto-negotiation Protocol

IEEE 802.3by & Consortium

Media Auto Detect

☐ Disabled ☒ Enabled

Default EVB Mode

☐ VEB ☒ VEPA ☐ None

Flow Offload

☒ Disabled ☐ Enabled

Port Link Training

☒ Disabled ☐ Enabled

Adapter Error Recovery

☐ Disabled ☒ Enabled

Figure 47: UEFI Menu for S-Tag Ether Type

NIC in Mezzanine 1B Port 2: Broadcom Adv Quad 25Gb Ethernet - E4:3D:1A:04:FB:D1

Main Configuration Page • NIC Partitioning Configuration

Broadcom Adv Quad 25Gb Ethernet - E4:3D:1A:04:FB:D1

Partition 1

Enabled

Partition 2

Disabled

Partition 3

Disabled

Partition 4

Disabled

Number of Partitions

4

S-Tag Ether Type

☒ 0x88a8 ☐ 0x9100

Global Bandwidth Allocation

Partition 1 Configuration

Partition 2 Configuration

Partition 3 Configuration

Creating an S-VLAN requires the use of a second encapsulation tag, called S-Tag. The TPID of a S-Tag is set to 0x88a8 or 0x9100.

Figure 48: UEFI Menu for S-VLAN ID

NIC in Mezzanine 1B Port 2: Broadcom Adv Quad 25Gb Ethernet - E4:3D:1A:04:FB:D1

Main Configuration Page • NIC Partitioning Configuration • Partition 1 Configuration

Broadcom Adv Quad 25Gb Ethernet - E4:3D:1A:04:FB:D1

NIC + RDMA Mode

☒ Disabled ☐ Enabled

S-VLAN ID

3

MAC Address

E4:3D:1A:04:FB:D1

Virtual MAC Address

E4:3D:1A:04:FB:D1

PCI Device ID

1751

PCI Address

86:00:01

Specify the s-VLAN ID (s-Tag) to be used by the partition in Advanced NPar mode. The s-VLAN ID must be unique per partition and in the range from ... (Press <F1> for more help)

All partition S-VLAN IDs in the same physical port are unique in the range of 3-4094. The default S-VLAN ID for a partition numbered X is X+2.

Broadcom

EthernetNIC-User-Guide-UG316-2CS

104

12.6 Ethernet Adapter Operations

Ingress Traffic:

Determines the destination partition of each inbound frame by examining the S-VID in the S-tag of the frame and strips the frame of the S-tag prior to delivering the frame to the partition.

Egress Traffic:

Apply an S-tag, as described in IEEE 802.1Q, to each frame that is outbound from a partition as the frame traverses the Port-mapping S-VLAN component.

Intra-Partition and Inter-Partition Traffic:

The inter-partition switching is handled by the adjacent switch while the intra-partition switching is handled by the Ethernet adapter. The Ethernet adapter embedded switch supports switching of the traffic between the PF and its children VFs on the same partition. The traffic switched by the Ethernet adapter embedded switch can not be S-Tagged. Traffic is originated on a PF or VF of a partition that is going to a PF or VF the adjacent (external) switch shall use S-Tag to forward the frame traffic.

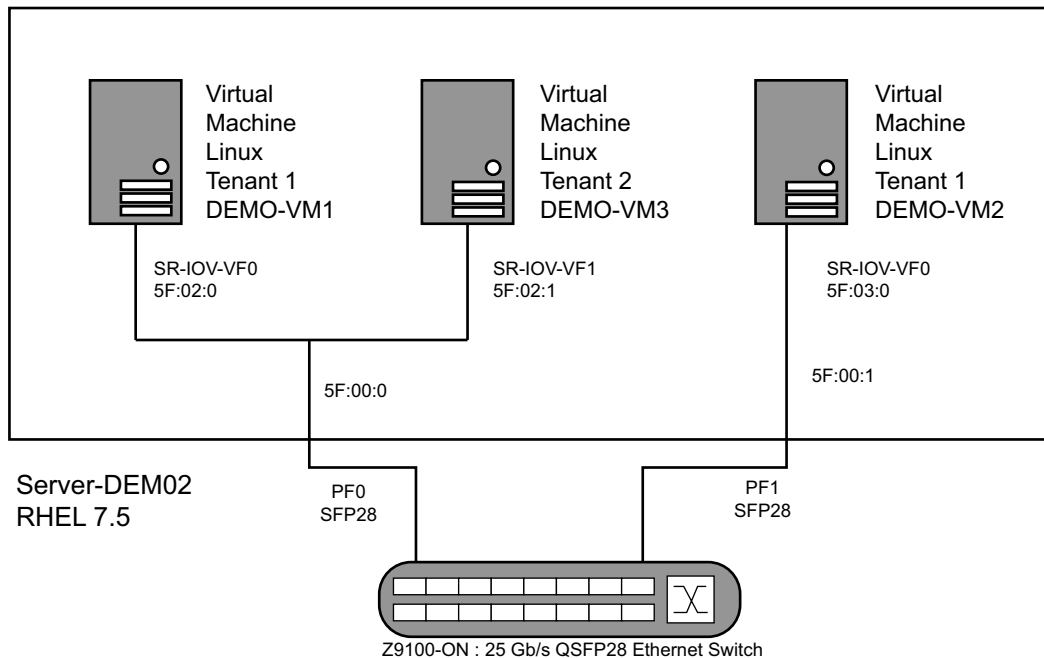
13 Tunneling Configuration Examples

Broadcom BCM5741X and BCM5751X devices support VXLAN, GRE, and IP-in-IP tunneling offloads. This section provides tunneling configuration examples.

13.1 Network Diagram

The test network shown in [Table 49](#) uses one Linux server with one two port Ethernet adapter. SR-IOV is enabled in the adapter and two VFs are instantiated on the first port. A VF from the second port is exposed to the third VM (see [SR-IOV – Configuration and Use Case Examples](#) for information on SR-IOV bring up).

Figure 49: Network Diagram



13.2 VEB and VEPA Modes

VEB (Virtual Ethernet Bridging) mode generates an internal bridge within the NIC for VM-to-VM communication. The Ethernet frames are traverses through the internal bridge. VEPA (Virtual Ethernet Port Aggregator) mode transports the frames to the external switch. The switch handles the frame transport between the ports. VEB and VEPA can be configured through UEFI HII.

13.2.1 VLAN Configuration

A VLAN can be configured on the Linux VF using:

NOTE: In this example physical function Port 1 (for example, eth2) VF 0 is configured to VLAN 2.

```
ip link set eth2 vf 0 vlan 2
```

When the VLAN is configured at the VF level, the Ethernet switch is configured as a VLAN.

13.3 VLAN Double Tagging

A VLAN can be configured at the PF level and another VLAN can be configured at the VF level inside the VM. Once the VF is exposed inside the VM, the Linux L2 driver can be installed to activate the interface. The following commands can be used to enable the VLAN inside the VM:

```
modprobe 802.1q;  
ip link add link <IntName> name <Vlan.2> type vlan id <vlan num>  
ip link set <IntName> up;  
ip addr add <IPAddr>/mask broadcast <Gateway Addr> dev <IntName>
```

13.4 GRE Tunnelling

An IP GRE is an IP inside an IP tunnel that can carry private network traffic between two heterogeneous networks. On the VM, use the following commands:

```
modprobe ip_gre;  
ip tunnel add gre45 mode gre local <public IP> remote <Private IP>  
ip link set dev gre45 up;  
ip addr add <private IP>/mask broadcast <broadcast ip> dev gre45
```

In this example, gre45 is the interface name.

13.5 IP-in-IP Tunnelling

Similar to GRE, IP-in-IP is another encapsulation that carries a private IP onto a public IP. Use the following commands:

```
modprobe ipip  
ip tunnel add ipip45 mode ipip remote <Peer IP> local <private ip> ttl 255 dev <VM Interface Name>  
ip link set dev ipip45 up  
ip addr add dev ipip45 <IP addr> peer <Peer IP>/mask  
ip link set dev ipip45 up
```

NOTE: In this example, ipip45 is the name of the newly created tunnel device.

13.6 VXLAN – Configuration and Use Case Examples

VXLAN encapsulation permits multiple virtual machines or containers residing on one server to be isolated from each other in virtual tunnels by encapsulating traffic with VXLAN headers. Broadcom Ethernet Network adapters accelerate this encapsulation and de-encapsulation in hardware.

This example discusses basic VXLAN connectivity between two Linux servers. Each server has one physical NIC enabled with outer IP address set to 1.1.1.4 and 1.1.1.2, respectively.

A VXLAN interface with ID 10 is created with multicast group 239.0.0.10 and is associated with physical network port eth1 on each server.

An IP address for the host is created on each server and associated with that VXLAN interface. Once the VXLAN interface is brought up, the VM present in system 1 can communicate with the VM present in system 2 using the VXLAN interfaces. The VLXAN format is shown in [Table 36](#).

Table 36: VXLAN Frame Format

MAC header	Outer IP header with proto = UDP	UDP header with Destination port= VXLAN	VXLAN header (Flags, VNI)	Original L2 Frame	FCS

[Table 37](#) provides VXLAN command and configuration examples.

Table 37: VXLAN Command and Configuration Examples

System 1	System 2
ifconfig eth1 1.1.1.4/24	ifconfig eth1 1.1.1.2/24
ip link add vxlan10 type vxlan id 10 group 239.0.0.10 dev eth1 dstport 4789	ip link add vxlan10 type vxlan id 10 group 239.0.0.10 dev eth1 dstport 4789
ifconfig vxlan10 192.168.1.5 mtu 1450	ifconfig vxlan10 192.168.1.10 mtu 1450
ip -d link show vxlan10	—
ping 192.168.1.10	—

14 RoCE – Configuration and Use Case Examples

This section provides configuration and use case examples for Remote Direct Memory Access over Converged Ethernet (RoCE).

NOTE: RoCE SR-IOV + NPAR is not a supported combination.

NOTE: RoCE SR-IOV is not supported on BCM5741X.

NOTE: RoCE SR-IOV is supported on the BCM5750X starting with the 2.19 release. The total number of VFs supported per device is up to 128 VFs.

14.1 Enabling RoCE

To enable RoCE for PFs or VFs, enable the RDMA selection in the HII menu in the BIOS before the RDMA option takes effect in the host or guest OS.

To enable RDMA in single function mode (if Virtualization Mode is None or SR-IOV):

1. During the system boot, access the **System Setup** → **NetXtreme-E NIC** → **Main Configuration Page** and set **NIC+ RMDA Mode** to **Enabled**.

To enable RDMA if Virtualization Mode is NPAR or NPAR + SR-IOV:

1. During the system boot, access the **System Setup** → **NetXtreme-E NIC** → **NIC Partitioning Configuration** → **Partition 1 (or 2) Configuration** and set **NIC+ RMDA Mode** to **Enabled**.

14.2 Disabling DCBx and LLDPs

To disable DCBx and LLDPs:

1. During the system boot, access the **System Setup** → **Device Settings** → **Broadcom Network Device** → **Device Level Configuration** and **disable** the following settings:
 - DCBX Mode
 - LLDP nearest bridge
 - LLDP nearest non-TPMR bridge

14.3 Linux Configuration and Use Case Examples

This section describes how to install the `bnxt_en` Linux L2 and/or `bnxt_re` RoCE driver and user space library for the Broadcom Ethernet Network adapter BCM95741X and BCM9575XX 10/20/25/40/50/100/200 Gb/s Ethernet Network Controllers (ENCs). RoCE is supported on the BCM9575XX and the BCM95741X Ethernet network controllers. See the [NetExtreme-E Linux RoCE Configuration Guide](#) for information on configuring RoCE for these network controllers.

14.3.1 Requirements

To configure RoCE in Linux, the following items are required:

- Linux L2 driver `bnxt_en`
- Linux RDMA RoCE driver `bnxt_re`
- Linux RoCE user space library `libbnxt_re`

14.3.1.1 BNXT_EN Driver Dependencies

If kernels older than 4.7 are used or if the `CONFIG_VLAN_MODULE` kernel option is set as a module option, the `vxlan.ko` module must be loaded before the `bnxt_en.ko` module.

14.3.1.2 BNXT_RE Driver Dependencies

The RoCE driver (`bnxt_re`) depends on the L2 Linux driver (`bnxt_en`) networking counterpart. The `bnxt_re` driver depends on the IB stack available with the Linux kernel or the OFED IB stack.

14.3.1.3 LIBBNXT_RE User Library Dependencies

The user space RoCE driver depends on the following:

- Ethernet driver for Broadcom Ethernet Network adapters (`bnxt_en`)
- RoCE driver for Broadcom Ethernet Network adapters (`bnxt_re`)
- uVerbs device interface, it is an IB-stack component (`ib_uverbs`)
- User space RDMA-CM, it is an IB-stack component (`rdma_ucm`)

14.3.2 Installing Drivers and the RoCE Library

The following sections provide information on how to install the RDMA stack, drivers, and RoCE library.

NOTE: Only one of either Native IB Stack or OFED must be installed. Unless a specific need for OFED is required, using the Linux native IB stack is recommended.

14.3.2.1 Installing the Native IB Stack

To install the native IB stack:

1. Use one of the following options:

```
- yum -y install libibverbs* infiniband-diags perftest qperf librdmacm-utils
- yum -y groupinstall "InfiniBand Support"
```

Using the yum commands requires a RedHat subscription. If a RedHat subscription is not available, locate the following RPM packages from the RedHat installation CD or ISO:

```
- infiniband-diag.x86_64
- libibverbs-devel.x86_64
- libibverbs-utils.x86_64
- libibverbs.x86_64
- librdmacm-utils.x86_64
- iperf3-devel.x86_64
- iperf3.x86_64
```

2. Install all of the RPM packages using the following yum command:

```
# yum -y install infiniband-diag.x86_64 libibverbs-devel.x86_64 libibverbs-utils.x86_64
libibverbs.x86_64 librdmacm-utils.x86_64 iperf3-devel.x86_64 iperf3.x86_64
```

NOTE: If Ubuntu 14.04 and above is used, use the following command:

```
sudo apt-get install perftest libibverbs* ibverbs-utils
```

NOTE: If SLES 12 SP2/SP3 and above is used, use the following command:

```
zypper install ofed* libibverbs* librdmacm* perftest
```

3. If yast2 must be used, the following command is used to install RoCE.

```
# yast2 --install libibverbs libipathverbs compat-dapl dapl libamso-rdmav2 libcxgb3-rdmav2 libcxgb4
-rdmav2 libmlx4-rdmav2 libmthca-rdmav2 libnes-rdmav2 librdmacm ib-bonding ibsim ibutils
ibvexdmtools infiniband-diags libibcm libibcommon1 libibmad5 libibumad3 libsdp ofed ofed-doc ofed-
kmp-default ofed-kmp-pae ofed-kmp-trace opensm mstflint rds-tools ibutils libibcommon libibcommon1
srptools
```

14.3.2.2 Installing the OFED IB Stack

To install the OFED IB stack:

1. See the OFED release notes provided in the following links and install OFED before compiling bnxt_re driver:

```
- http://downloads.openfabrics.org/downloads/OFED/release\_notes/OFED\_3.18-2\_release\_notes
- http://www.openfabrics.org/downloads/OFED/ofed-3.18-2/OFED-3.18-2.tgz
```

OFED requires several development packages to compile and install. Install the following packages using the SDK CD:

```
- zlib-devel
- libnl-devel
- tcl-devel
- glib2-devel
- libudev-devel
```

2. Retrieve the OFED file from the following link:

<http://www.openfabrics.org/downloads/OFED/ofed-3.18-2/OFED-3.18-2.tgz>

3. Install the file using the following commands:

```
tar xzf OFED-x.y.z3.18-2.tgz
cd OFED-x.y.z3.18-2
./install.pl
```

4. Select Option 2.

5. Select Option 3.

After the **OFED is installed completely** message is displayed, run the `ofed_info -s` command to verify that the correct version of OFED is installed. Then proceed to the L2 + ROCE driver installation.

NOTE: The OFED library installs only once on the system regardless of the number of kernels in the OS. It always overrides with latest. Ensure that OFED is compiling and installing for the correct kernel to install the RoCE driver.

14.3.2.3 Installing the Broadcom Ethernet Network adapter Drivers and RDMA Library

Install the `bnxt_en`, `bnxt_re` drivers, and `libbnxt_re` RDMA library as shown in [Installing the Linux Driver](#).

14.3.3 Verifying RoCE Functionality

To verify RoCE functionality:

1. Verify that the Broadcom NIC driver is loaded using the following command:

```
# modinfo bnxt_en
```

2. Verify that the Broadcom RoCE driver is loaded using the following command:

```
# modinfo bnxt_re
```

3. Verify that the RoCE kernel is loaded using the following commands:

```
# lsmod | grep ib_
ib_isert                50818  0
iscsi_target_mod       291713  1 ib_isert
ib_iser                 47861  0
libiscsi                57233  1 ib_iser
scsi_transport_iscsi    99909  2 ib_iser,libiscsi
ib_srpt                 43624  0
target_core_mod        340809  3 iscsi_target_mod,ib_srpt,ib_isert
ib_srp                  52589  0
scsi_transport_srp      20993  1 ib_srp
ib_ipoib                115042  0
ib_ucm                  22636  0
ib_uverbs               78543  2 ib_ucm,rdma_ucm
ib_umad                 22119  0
rdma_cm                 59529  4 rprdma,ib_iser,rdma_ucm,ib_isert
ib_cm                   51741  5 rdma_cm,ib_srp,ib_ucm,ib_srpt,ib_ipoib
ib_core                 236827  14
rdma_cm,ib_cm,iw_cm,rprdma,ib_srp,ib_ucm,ib_iser,ib_srpt,ib_umad,ib_uverbs,bnxt_re,rdma_ucm,ib_i
poib,ib_isert
```

4. Verify that the Broadcom RoCE devices are available using the following commands:

```
# ibv_devices
```

```
[root@dhcp-10-13-107-210 ~]# ibv_devices
device          node GUID
-----
bnxt_re1        021918ffffead1fa1
bnxt_re0        021018ffffead1fa0
```

5. Verify that the Broadcom RoCE device is enabled and can be accessed using the following commands:

```
# ibv_devinfo -d bnxt_re0
```

```
[root@dhcp-10-13-107-210 ~]# ibv_devinfo -d bnxt_re0
hca_id: bnxt_re0
  transport:                      Infini Band (0)
  node_guid:                      0210:18ff: fead:1fa0
  sys_image_guid:                 0210:18ff: fead:1fa0
  vendor_id:                      0x14e4
  vendor_part_id:                 5847
  hw_ver:                         0x1405
  phys_port_cnt:                  1
    port:                          1
      state:                       PORT_ACTIVE (4)
      max_mtu:                     4096 (5)
      active_mtu:                  1024 (3)
      sm_lid:                      0
      port_lid:                    0
      port_lmc:                    0x00
      link_layer:                   Ethernet
```

```
# ibv_devinfo -d bnxt_re1
```

```
[root@dhcp-10-13-107-210 ~]# ibv_devinfo -d bnxt_re1
hca_id: bnxt_re0
  transport:                      Infini Band (0)
  node_guid:                      0210:18ff: fead:1fa1
  sys_image_guid:                 0210:18ff: fead:1fa1
  vendor_id:                      0x14e4
  vendor_part_id:                 5847
  hw_ver:                         0x1405
  phys_port_cnt:                  1
    port:                          1
      state:                       PORT_ACTIVE (4)
      max_mtu:                     4096 (5)
      active_mtu:                  1024 (3)
      sm_lid:                      0
      port_lid:                    0
      port_lmc:                    0x00
      link_layer:                   Ethernet
```

14.3.4 RoCE Connectivity Tests

This section provides information on how to test basic RoCE connectivity using rping. The test utilities use a server and client model during RoCE testing.

1. Server side: `rping -s -a <ServerIP> -v`

```
[root@localhost ~]# rping -s -a 10.0.0.5 -v
server ping data: rdma-ping-1052: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1053: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1054: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1055: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1056: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1057: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1058: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1059: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1060: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1061: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1062: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1063: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
```

2. Client side: rping -c -a <ServerIP> -v

```
[root@localhost ~]# rping -c -a 10.0.0.5 -v
server ping data: rdma-ping-1035: FGHIJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1036: GHIJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1037: HIJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1038: IJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1039: JKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1040: KLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1041: LMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1042: MNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1043: NOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz
server ping data: rdma-ping-1044: OPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzA
server ping data: rdma-ping-1045: PQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzAB
server ping data: rdma-ping-1046: QRTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABC
server ping data: rdma-ping-1047: RSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCD
server ping data: rdma-ping-1048: STUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDE
server ping data: rdma-ping-1049: TUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEF
server ping data: rdma-ping-1050: UVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEFGF
server ping data: rdma-ping-1050: VWXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEFGH
server ping data: rdma-ping-1050: WXYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEFGHI
server ping data: rdma-ping-1050: XYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEFGHIJ
server ping data: rdma-ping-1051: XYZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEFGHIK
server ping data: rdma-ping-1051: YZ[\]^_'abcdefghijklmnopqrstuvwxyzABCDEFGHIKM
server ping data: rdma-ping-1051: Z[\]^_'
```

3. Basic ping pong test:

a. Server side: ibv_rc_pingpong -g 0 -d bnxt_re<x> -i 1

```
[root@dhcp-10-13-107-210 ~]# ibv_rc_pingpong -g0 -d bnxt_re0 -il
local address: LID 0x0000, QPN 0x000094, PSN 0x390112, GID fe80::210:18ff:fead:1fa0
remote address: LID 0x0000, QPN 0x000095, PSN 0xe00732, GID fe80::210:19ff:fead:1fa0
8192000 bytes in 0.01 seconds = 4410.53 Mbit/sec
1000 iters in 0.01 seconds = 14.86 usec/iter
```

b. Client side: ibv_rc_pingpong -g 0 -d bnxt_re<x> -i 1 <ServerIP>

```
[root@dhcp-10-13-107-210 ~]# ibv_rc_pingpong -g0 -d bnxt_re0 -il 10.0.0.50
local address: LID 0x0000, QPN 0x000095, PSN 0xe00732, GID fe80::210:18ff:fead:1fa0
remote address: LID 0x0000, QPN 0x000094, PSN 0x390112, GID fe80::210:19ff:fead:1fa0
8192000 bytes in 0.01 seconds = 4432.60 Mbit/sec
1000 iters in 0.01 seconds = 14.78 usec/iter
```

14.3.4.1 Performance Test (perftest) Package

The perftest package is a collection of tests written over uverbs intended for use as a performance micro-benchmark. The tests are used for tuning as well as for functional testing. The server-side IB server and the client-side IB client must be run.

The perftest package contains the following bandwidth and latency benchmarks:

- `ib_send_bw`
- `ib_send_lat`
- `ib_write_bw`
- `ib_write_lat`
- `ib_read_bw`
- `ib_read_lat`

1. The IB test tool help commands are viewed using the following `-h` parameter in the command:

```
# ib_send_bw -h
```

2. Verify that the IP and RoCE node is up on both sides with the following command:

```
ifconfig InterfaceName ; ibv_devices;
```

The Interface Name is the name of the Ethernet interface.

```
[root@localhost ~]# ifconfig ens2f0 ; ibv_devices
ens2f0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fc80::9dc:71ff:fec8:c18 prefixlen 64 scopeid 0x20<link>
    ether 9c:dc:71:c8:8c:18 txqueuelen 1000 (Ethernet)
    RX packets 249 bytes 41586 (40.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 439 bytes 51150 (49.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

    device            node GUID
    -----
    bnxt_re1          9cdc71ffffec88c18
    bnxt_re0          9cdc71ffffec88c18
```

3. Run `ib_send_bw` on both sides with the following commands:

- a. Server Side: `ib_send_bw -d <RoCE Node> --report_gbits`

```
[root@localhost ~]# ib_send_bw -d bnxt_re0 --report_gbits
=====
* Waiting for client to connect... *
=====
-----
Send BW Test
Dual-port      : OFF          Device      : bnxt_re0
Number of qps  : 1           Transport type : IB
Connection type : RC         Using SRQ    : OFF
RX depth       : 512
CQ Moderation  : 100
MTU            : 1024[B]
Link type      : Ethernet
GID index      : 2
Max inline data : 0[B]
rdma_cm QPs    : OFF
Data cx. method : Ethernet
-----
local address: LID 0000 QPN 0x000d PSN 0x6ec690
GID: 00:00:00:00:00:00:00:00:00:00:255:255:192:168:01:01
remote address: LID 0000 QPN 0x000d PSN 0x2dbda2
GID: 00:00:00:00:00:00:00:00:00:00:255:255:192:168:01:02
-----
Bbytes      iterations      BW peak[Gb/sec]      BW average[Gb/sec]      MsgRate[Mpps]
65536       1000              0.00                22.98                   0.043825
-----
```

b. Client Side: `ib_send_bw -d <RoCE Node> --report_gbits <Server IP>`

```

root@localhost ~# ib_send_bw -d bnxt_re0 --report_gbits 192.168.1.1
-----
Send BW Test
Dual-port      : OFF      Device      : bnxt_re0
Number of qps  : 1        Transport type : IB
Connection type: RC        Using SRQ    : OFF
TX depth       : 128
CQ Moderation  : 1000
MTU            : 10241B
Link type      : Ethernet
GID index      : 2
Max inline data: 81B
rdma_cm QPs    : OFF
Data ex. method: Ethernet
-----
local address: LID 0000 QPN 0x000d PSN 0x2dbda2
GID: 00:00:00:00:00:00:00:00:255:255:192:168:01:02
remote address: LID 0000 QPN 0x000d PSN 0x2dbda2
GID: 00:00:00:00:00:00:00:00:255:255:192:168:01:01
-----
#bytes      #iterations    BW peak1Gb/sec    BW average1Gb/sec    MsgRate1Mpps1
65536       1000              22.91              22.91                0.843689
-----

```

NOTE: With dual-port NICs, if both ports are on the same subnet, RDMA perftest commands may fail. This is caused by an arp flux issue in Linux. Use multiple subnets for testing or bringing the other interface down.

14.3.5 RoCE Congestion Control

Broadcom Ethernet Network adapter Congestion Control (NCC) is a standards-based congestion control mechanism for RDMA over Ethernet v2 (RoCEv2), which utilizes Explicit Congestion Notification (RFC 3168) to signal to RoCE transmitting stations the congestion status of the network, which is used by Broadcom Ethernet Network adapters to control transmit rate, thereby reducing congestion, reducing packet drops, and minimizing network latency by keeping switch transmit queues minimally loaded.

NCC can work in conjunction with Flow Control including pause frames and Priority Flow Control to guarantee a lossless network, or NCC can operate alone.

14.3.5.1 Using the Section

This section is intended to provide information on the process of configuring a new server for RoCE use with RoCEv2 enabled, Congestion Control enabled, and optionally, PFC enabled and configured.

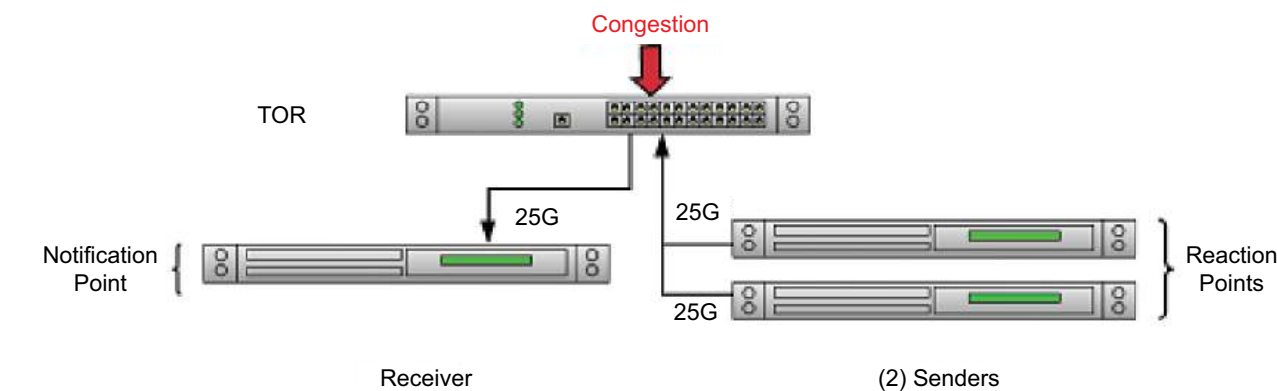
Any installation of other vendor's proprietary Infiniband software stack should be removed before proceeding with this section.

14.3.5.2 Understanding Congestion Control

14.3.5.2.1 Basic Topology

Congestion control topology provides a basic topology of how to test congestion control. In this topology, there are two senders transmitting packets at 25G to a receiver that can only receive at 25G.

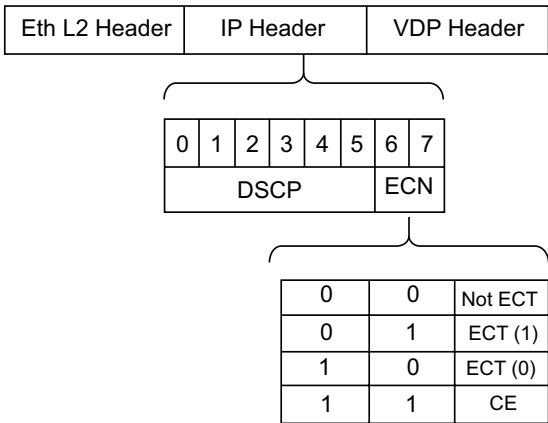
Figure 50: Congestion Control Topology



14.3.5.2.2 Background

Congestion control flow provides a simple overview of ECN congestion management.

1. After ECN has been configured and enabled, the ECN bits in the IP header of RoCEv2 packets are either ECT1(01b) or ECT0 (10b) based on the user configuration.

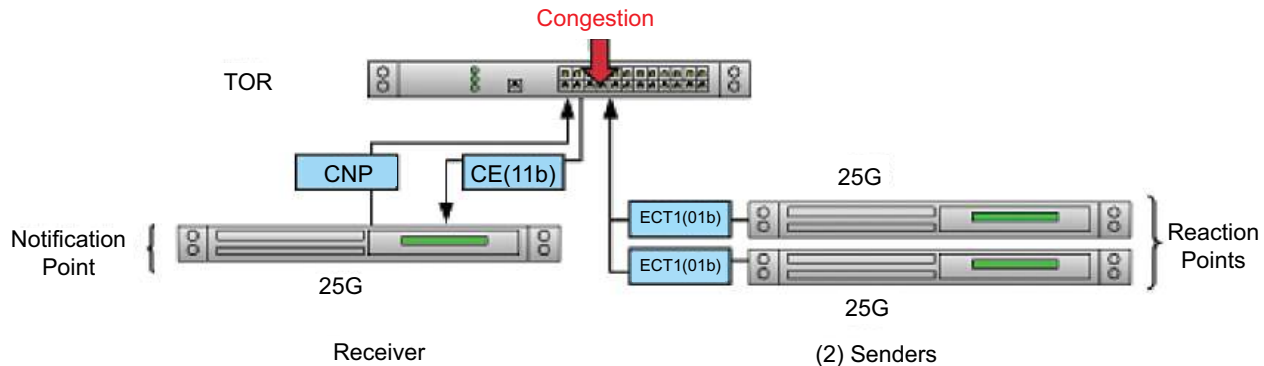


2. As the Egress Queue of the switch reaches the congestion marking threshold as defined by the user, the switch starts marking the ECN bits to CE(11b) to notify to the notification point that congestion has been detected for that port.
3. Once the CE bit is detected, the notification point transmits Congestion Notification Packet (CNP) packet(s) to the reaction points(s) to signify congestion.
4. Upon the reception of the CNP(s), the reaction point reduces its transmit rate based on a certain algorithm so that the congestion can be mitigated.

5. The reaction point continues to react to rate limit requests until Congestion Notification Packet (CNP) packets are no longer received.
6. At times when CNPs are not received by the transmitter, the transmitter attempt to gradually increase its transmission rate.

NOTE: Both reduction in rate and increase in rate are to be accomplished per QP

Figure 51: Congestion Control Flow



14.3.5.3 NIC Configuration

To configure the NIC to be lossless for RoCE, the correct traffic class is required to be used as the default traffic class is currently set to lossy. There are two available methods to configure the traffic classes and other QoS settings:

- LLDP Agent
- BnxtQoS

14.3.5.4 LLDP Agent

The LLDP agent is used to set QoS mappings (user priority, Linux TC, or NIC CoS queue) and configure Enhanced Transmission Selection (ETS) to configure bandwidth allocation if required. It is required to install the LLDP agent to properly configure QoS, which is necessary for maximum performance.

14.3.5.4.1 Debian/Ubuntu

To install the LLDP agent using Debian/Ubuntu, use the following commands:

```
sudo apt install libconfig9 libnl-3-200
wget http://ftp.us.debian.org/debian/pool/main/l/lldpad/lldpad_0.9.46-3.1_amd64.deb
sudo dpkg -i lldpad_0.9.46-3.1_amd64.deb
sudo systemctl enable lldpad
sudo systemctl start lldpad
```

14.3.5.4.2 Red Hat/CentOS

To install the LLDP agent using RedHat/CentOS, use the following commands:

```
sudo yum install lldpad
sudo systemctl enable lldpad
sudo systemctl start lldpad
```

14.3.5.5 BnxtQoS

Similar to the LLDP Agent, the Broadcom QoS configuration utility is used to set QoS mappings, priority flow control, and to configure Enhanced Transmission Selection (ETS). BnxtQoS only configures settings on the NIC side and requires the following:

- Switch configuration to match that of the NIC QoS settings.
- Disablement of the LLDPAD on the host and in the firmware (if enabled).

Table 38: Usage: bnxtqos -dev=<interface name> <command> [-options [...]]

Commands	
version	Display program version details.
set_ets	This command is used to configure the priority to tc and Bandwidths. This command is also used to configure TSA and Bandwidths. Syntax: bnxtqos -dev=<interface name> set_ets tsa=<tc[0-7]:tc_type[ets/strict]> [priority2tc=<priority[0-7]:tc>] tcbw=<bandwidths> with comma separated and in units of percentage (%). Example: bnxtqos -dev=p7p1 set_ets tsa=0:ets,1:ets,2:strict,3:strict,4:strict,5:strict,6:strict,7:strict priority2tc=0:0,1:0,2:0,3:0,4:0,5:1,6:0,7:0 tcbw=70,30
set_pfc	To enable PFC on given priority. Valid values are from 0 to 7. Syntax: bnxtqos -dev=<interface name> set_pfc enabled=<0-7> the values should be with comma separated Example: bnxtqos -dev=p7p1 set_pfc enabled=5,6
set_apptlv	This parameter is used to configure the priority of the APPTLV. Syntax: bnxtqos -dev=<interfac name> set_apptlv app=<priority,selector,protocol> Syntax: bnxtqos -dev=<interfac name> set_apptlv -d app=<priority,selector,protocol> Example: bnxtqos -dev=p7p1 set_apptlv app=5,1,35093 Example: bnxtqos -dev=p7p1 set_apptlv -d app=5,1,35093
get_qos	This command is used to get the configured priorities and bandwidth parameters.
ratelimit	This command is used to set the rate limit for each TC in units of percentage (%). Example: bnxtqos -dev=p7p1 ratelimit 80,60,70
dump	This command is used to dump the supported dump strings. The supported dump string is pri2cos. Syntax: bnxtqos -dev=<device name> dump <dump string> Example: bnxtqos -dev=p7p1 dump pri2cos
Options	
-v[v][v]	Enable extra console output (increase verbosity).
-V	Enable maximum verbosity of console output.
-d	Removes the application TLV.

14.3.5.6 DSCP vs. VLAN Mode

NCC has two operational modes: VLAN and DSCP. If your network uses VLAN tagging for traffic, the VLAN header is used to track traffic priority values, necessary to separate RoCE traffic from other traffic for congestion control. If your network uses DSCP tagging for traffic, the proper DSCP mapping is required to be set. In either case, the corresponding switch must be configured correctly to ensure the priority (VLAN or DSCP) map to a specific traffic class priority on the switch that has the ECN enabled and configured for the specified marking thresholds.

Determine the interface name of the NIC with the following command:

```
ifconfig -a
```

Create a boot-time configuration file for the interface.

14.3.5.6.1 Debian/Ubuntu

Add to `/etc/network/interfaces`:

```
auto <iface>
iface <iface> inet static
    address w.x.y.z
    netmask a.b.c.d
    gateway e.f.g.h
<iface> must be in the form of <iface>.<vlan id> to use VLANs
```

14.3.5.6.2 RedHat/CentOS

1. Add to `/etc/sysconfig/network-scripts/ifcfg-<iface>`:

```
DEVICE=<iface>
ONBOOT=yes
BOOTPROTO=static
NM_CONTROLLED=no
NETMASK=a.b.c.d
IPADDR=w.x.y.z
# Uncomment below for VLAN
#VLAN=yes
#VLAN_EGRESS_PRIORITY_MAP=0:0,1:1,2:1,3:1,4:1,5:1,6:1,7:1
*<iface> must be in the form of <iface>.<vlan id> to use VLANs
```

2. Create an `/etc/ifup-roce-<IFACE>` script to allow boot-time RoCE configuration:

```
#!/bin/sh
sleep 2

/sbin/modprobe bnxt_re
sleep 5

/sbin/ethtool -A $IFACE autoneg off rx off tx off
sleep 2

#Using bnxtqos
bnxtqos -dev=$IFACE set_apptlv app=1,5,34
bnxtqos -dev=$IFACE set_apptlv app=1,1,35093
bnxtqos -dev=$IFACE set_apptlv app=1,3,4791
```

```

bnxtqos -dev=$IFACE set_apptlv set_ets
tsa=0:ets,1:ets,2:strict,3:strict,4:strict,5:strict,6:strict,7:strict
up2tc=0:0,1:1,2:0,3:0,4:0,5:0,6:0,7:0 tcbw=10,90
bnxtqos -dev=$IFACE set_pfc enabled=1

#Uncomment if using LLDP Agent
#/usr/sbin/lldptool -T -i $IFACE -V APP app=1,5,34*
#/usr/sbin/lldptool -T -i $IFACE -V APP app=1,1,35093
#/usr/sbin/lldptool -T -i $IFACE -V APP app=1,3,4791
#/usr/sbin/lldptool -T -i $IFACE -V ETS-CFG
tsa=0:ets,1:ets,2:strict,3:strict,4:strict,5:strict,6:st
#rict,7:strict up2tc=0:0,1:1,2:0,3:0,4:0,5:0,6:0,7:0 tcbw=10,90
#/usr/sbin/lldptool -T -i $IFACE -V PFC enabled=1
#systemctl restart lldpad
sleep 10

/sbin/modprobe bnxt_re
sleep 5

mkdir -p /sys/kernel/config/rdma_cm/bnxt_re0
echo RoCE v2 > /sys/kernel/config/rdma_cm/bnxt_re0/ports/1/default_roce_mode

mkdir -p /sys/kernel/config/bnxt_re/bnxt_re0
cd /sys/kernel/config/bnxt_re/bnxt_re0/ports/1/cc/

# Uncomment below for DSCP Mode
#echo -n 0x22 > roce_dscp          # DSCP RoCE packets
#echo -n 0x6 > cnp_prio           # Priority for CNP Packets
#echo -n 0x23 > cnp_dscp          # DSCP for CNP packets
#echo -n 0x1 > vlan_tx_disable   # Set DSCP mode

# Uncomment below for VLAN mode
#echo -n 0x0 > vlan_tx_disable # Set VLAN mode
#echo -n 0x6 > cnp_prio       # Priority for CNP Packets

```

The support for DSCP tagging through lldptool is supported on a newer kernel.

3. Set the script to be executable with the following command:

```
sudo chmod 755 /etc/ifup-roce-<IFACE>
```

14.3.5.6.3 Debian

To configure a boot-time RoCE configuration, create the following `/etc/network/if-up.d/roce` script with the following commands:

```

#!/bin/sh

if [ -x /etc/ifup-roce-${IFACE} ]; then
    /etc/ifup-roce-${IFACE}
fi

```

Set the script to be executable with the following command:

```
sudo chmod 755 /etc/network/if-up.d/roce
```

14.3.5.6.4 Red Hat

1. Create an `/sbin/ifup-local` script to allow boot-time RoCE configuration with the following commands:

```
#!/bin/sh

export IFACE=$1

if [ -x /etc/ifup-roce-${IFACE} ]; then
    . /etc/ifup-roce-${IFACE}
fi
```

- Set the script to be executable with the following commands:

```
sudo chmod 755 /sbin/ifup-local
```

- Reconfigure the interface with the following commands:

```
sudo ifdown <IFACE>
sudo ifup <IFACE>
```

14.3.5.7 Congestion Control Settings

Different topologies may require different tunings. See [Performance](#) for additional information.

14.3.5.7.1 Congestion Control Parameters

Table 39: Congestion Control Parameters

CC Parameter ^a	Description
inact_cp	Inactivity time after which the CC parameters of a QP are re-initialized.
nph_per_state	Number of phases per state. 0 to 7. How many RTTs in Fast Recovery state.
cnp_dscp	DSCP value for RoCE Congestion Notification Packets.
roce_dscp	DSCP value for RoCE Packets.
cc_mode	0 for DCTCP algorithm, 1 for TCP. Default 0.
cnp_prio	Priority for RoCE Congestion Notification Packets.
ecn_enable	Enable congestion control.
ecn_marking	Specifies which ECN bit to set. 0x1 for 01b or 0x2 for 10b.
g	Running average weight in computing cp (Congestion Probability). The weight is 2 ^g , g between 1 and 7, default 4.
init_cr	Current rate after on QP creation and after QP has not transmitted for more than inctivity_th. Value between 0 and 1023 as fraction of full link BW.
int_tr	Target rate after on QP creation and after QP has not transmitted for more than inctivity_th. Value between 0 and 1023 as fraction of full link BW.
roce_prio	Priority for RoCE Packets.
rtt	Time period [us] over which cnp and transmitted packets counts accumulate. At the end of Rtt ratio between CNPs and TxPkts computed and cp is updated.
tcp_cp	The reduction level on reception of CNP when cc_mode is 1 (TCP mode). Value between 0 and 1023, representing 0-1.0.
vlan_tx_disable	Disables the VLAN headers (required if using DSCP).
apply	Applies the settings.

a. Releases prior to 20.8 have slightly different naming conventions.

The following is an example of setting congestion control parameters:

```
mkdir -p /sys/kernel/config/rdma_cm/bnxt_re0
echo RoCE v2 > /sys/kernel/config/rdma_cm/bnxt_re0/ports/1/default_roce_mode

mkdir -p /sys/kernel/config/bnxt_re/bnxt_re0
cd /sys/kernel/config/bnxt_re/bnxt_re0/ports/1/cc/

# DSCP configuration
echo -n 0x1 > roce_dscp
echo -n 0x1 > roce_prio
echo -n 0x1 > vlan_tx_disable

# Set CC parameters for and enable
echo -n 0x1 > ecn_enable
echo -n 0x1 > ecn_marking
echo -n 0xc8 > tcp_cp
echo -n 0x3 > nph_per_state
echo -n 0x28 > rtt
echo -n 0x4 > g
echo -n 0x1f4 > init_cr
echo -n 0x3ff > init_tr
echo -n 0x1f40 > inact_cp
echo -n 0x1 > apply
```

14.3.5.7.2 Setup Script

A setup script is provided as part of the release to configure the priority, DSCP, and congestion control parameters. The script does not load the drivers, bring up the interface, or setup the addresses.

Usage: `bnxt_setupcc.sh [OPTION]...`

```
-d - RoCE Device Name (e.g. bnxt_re0, bnxt_re_bond)
-i - Ethernet Interface Name (example: plp1 or for bond, specify slave interfaces like -i p6p1 -i p6p2)
-r [0-7] - RoCE Packet Priority
-s VALUE - RoCE Packet DSCP Value
-c [0-7] - RoCE CNP Packet Priority
-p VALUE - RoCE CNP Packet DSCP Value
-h - Display help
```

NOTE: In SIT release 212.1.x, the cosq used for CNPs has been removed from the user scope. Only two traffic classes are available to the user. Previous versions of the script were still configuring the 3rd traffic to be used for CNPs which results in unexpected behaviors (ensure that traffic class 2 is not set in the prio2tc).

The following is an example of running the setup script:

```
cd $REL_DIR/Linux/netxtreme-bnxt_en-x.y.z/bnxt_re
./bnxt_setupcc.sh -d bnxt_re0 -i plp1 -r 5 -s 0x22 -c 6 -p 0x23
```

14.3.5.8 Switch Configuration

NCC uses ECN to react to marked packets within the network switch infrastructure during times of congestion. The correct ECN threshold value is specific to each switch port, and is dependent on the link speed of that port. The following table shows which values are to be used for deterministic marking (cc_mode=0).

Link Speed	ECN Min./Max. Threshold (kilobytes)
10 Gb/s	12/12
25 Gb/s	16/16
50 Gb/s	22/22
100 Gb/s	33/33

Each switch port participating in NCC must be configured with the above ECN threshold for the class of service associated with RoCEv2 traffic. Different vendors have different naming conventions that specify the minimum and maximum marking threshold as well as the marking percentage. The following sections provide examples of setting such parameters aforementioned.

14.3.5.8.1 Operation

With the switches, servers, and NICs configured, RDMA applications can be deployed to run over the RoCE network. Any libverbs-linked application can be used with appropriate changes for using IP addresses rather than GUIDs for end-point addressing.

When using NCC, it is important to specify a RoCEv2 GUID. RoCEv1 does not support NCC.

1. To see a list of GUIDs supported by the device, use the following `ibv_devinfo -vvvv`:

```
[root@Host1 ~]# ibv_devinfo -vvvv
hca_id:bnxt_re1
transport:InfiniBand (0)
fw_ver:      212.1.93.0
node_guid:020a:f7ff:fea6:9cf1
sys_image_guid:020a:f7ff:fea6:9cf1
vendor_id:0x14e4
vendor_part_id:5847
hw_ver:      0x1406
phys_port_cnt:1
max_mr_size:0x8000000000
page_size_cap:0x201000
...
    active_width:1X (1)
    active_speed:25.0 Gb/s (32)
    phys_state:DISABLED (3)

    GUID[ 0]:fe80:0000:0000:0000:020a:f7ff:fea6:9cf0, RoCE V1 (IPV6)
    GUID[ 1]:fe80:0000:0000:0000:020a:f7ff:fea6:9cf0, RoCE V2 (IPV6)
    GUID[ 2]:0000:0000:0000:0000:0000:ffff:ac10:0102, RoCE V1 (IPV4)
    GUID[ 3]:0000:0000:0000:0000:0000:ffff:ac10:0102, RoCE V2 (IPV4)
```

2. Odd-numbered GUIDs are used for RoCEv2 and this can be verified with the following command:

```
# cat /sys/class/infiniband/bnxt_re0/ports/1/gid_attrs/types/1
```

NOTE: If the above directory does not exist, this indicates the installed kernel/OFED version does not support RoCE version 2.

A typical application of exercising the RoCE interface would be to use rping or perftest. Perftest can be obtained from GitHub or via most Linux package repositories such as:

```
RHEL/CentOS: yum install perftest
Ubuntu: apt install perftest
```

For example, the perftest tools can be run as:

```
# ib_write_bw -d bnxt_re0 -x 3 -F --report_gbits -p 1800 -s <message_size> -q <num of qps> -D <duration>
192.168.30.3
```

```
# ib_write_lat -d bnxt_re0 -x 3 -F --report_gbits -p 1800 -s 2 192.168.30.3
```

For a complete explanation of the parameters used by ib_write_bw/lat and other IB utilities, see GitHub as previously described.

14.3.5.8.2 Analytics

RoCE and congestion control statistics can be viewed from the sysfs files using the following commands:

```
# cat /sys/kernel/debug/<device name>/info (for example, /sys/kernel/debug/bnxt_re0/info)
bnxt_re debug info:
Adapter count: 1
===== [ IBDEV bnxt_re_bond0 ] =====
    link state: UP
    Max QP: 0xff80
    Max SRQ: 0x7fff
    Max CQ: 0xffff
    Max MR: 0x3ffff
    Max MW: 0x8000c
    Active QP: 2
    Active SRQ: 0
    Active CQ: 1
    Active MR: 0
    Active MW: 1
    Recoverable Errors: 0
    Active QPs P0: 0
    Active QPs P1: 2
    Rx Pkts: 42907336148
    Rx Bytes: 2664310290076
    Tx Pkts: 229562600627
    Tx Bytes: 248444124528782
    CNP Tx Pkts: 0
    CNP Tx Bytes: 0
    CNP Rx Pkts: 338012327
    CNP Rx Bytes: 25012912198
```


14.3.5.9 Counter Definitions

The following tables provide counter definitions.

Table 40: Device Resource Limits

Counters	Description
Max QP	Max number of QP limit
Max SRQ	Max number of SRQ limit
Max CQ	Max number of CQs limit
Max MR	Max number of memory region limit
Max MW	Max number of memory window limit

Table 41: Active Resources

Counters	Description
Active QP	Number of active QPs.
Active SRQ	Number of active SRQs.
Active CQ	Number of active CQs.
Active MR	Number of active Memory Regions.
Active MW	Number of active Memory Windows.

Table 42: Bytes and Packet Counters

Counters	Description
RX Pkts	Number of RoCE (v1/v2) packets received.
RX Bytes	Number of RoCE (v1/v2) bytes received.
TX Pkts	Number of RoCE (v1/v2) packets transmitted.
TX Bytes	Number of RoCE (v1/v2) bytes transmitted.

Table 43: Congestion Notification Counters

Counters	Description
CNP TX Pkts	Number of RoCE CNP packets received.
CNP TX Bytes	Number of RoCE CNP bytes received.
CNP RX Pkts	Number of RoCE CNP packets transmitted.
CNP RX Bytes	Number of RoCE CNP bytes transmitted.

Table 44: Recoverable Errors

Counters	Description
Recoverable Errors	Number of recoverable errors detected. Recoverable errors are detected by the HW. HW instructs FW to initiate the recovery process. RC connection does not teardown as a result of these errors.
to_retransmits	Number of retransmission requests.
rnr_naks_rcvd	Number of RNR (Receiver-Not-Ready) NAKs received.
dup_req	Number of duplicated requests detected.
missing_resp	Number of responses missing.

Table 45: Fatal Errors

Counters	Description
seq_err_naks_rcvd	Number of PSN sequencing error NAKs received.
max_retry_exceeded	Number of retransmission requests exceeded the maximum.
unrecoverable_err	Number of unrecoverable errors detected.
bad_resp_err	Number of bad response errors detected.
local_qp_op_err	Number of QP local operation errors detected.
local_protection_err	Number of local protection errors detected.
mem_mgmt_op_err	Number of times HW detected an error because of illegal bind/fast register/invalidate attempted by the driver.
remote_invalid_req_err	Number of invalid request received from the remote rdma initiator.
remote_access_err	Number of times H/W received a REMOTE ACCESS ERROR NAK from the peer.
remote_op_err	Number of times HW received a REMOTE OPERATIONAL ERROR NAK from the peer.

Table 46: Responder Errors

Counters	Description
res_exceed_max	Number of times HW detected incoming Send, RDMA write or RDMA read messages which exceed the maximum transfer length.
res_length_mismatch	Number of times HW detected incoming RDMA write message payload size does not match write length in the RETH.
res_exceeds_wqe	Number of times HW detected Send payload exceeds RQ/SRQ RQE buffer capacity.
res_opcode_err	Number of times HW detected First, Only, Middle, Last packets for incoming requests are improperly ordered with respect to the previous packet.
res_rx_invalid_rkey	Number of times HW detected an incoming request with an R_KEY that did not reference a valid MR/MW.
res_rx_domain_err	Number of times HW detected an incoming request with an R_KEY that referenced a MR/MW that was not in the same PD as the QP on which the request arrived.
res_rx_no_perm	Number of times HW detected an incoming RDMA write request with an R_KEY that referenced a MR/MW which did not have the access permission needed for the operation.
res_rx_range_err	Number of times HW detected an incoming RDMA write request that had a combination of R_KEY, VA and length that was out of bounds of the associated MR/MW.
res_tx_invalid_rkey	Number of times HW detected a R_KEY that did not reference a valid MR/MW while processing incoming read request.
res_tx_domain_err	Number of times HW detected an incoming request with an R_KEY that referenced a MR/MW that was not in the same PD as the QP on which the RDMA read request is received.
res_tx_no_perm	Number of times HW detected an incoming RDMA read request with an R_KEY that referenced a MR/MW which did not have the access permission needed for the operation.
res_tx_range_err	Number of times HW detected an incoming RDMA read request that had a combination of R_KEY, VA and length that was out of bounds of the associated MR/MW.
res_irq_oflow	Number of times HW detected that peer sent us more RDMA read or atomic requests than the negotiated maximum.
res_unsup_opcode	Number of times HW detected that peer sent us a request with an opcode for a request type that is not supported on this QP.
res_unaligned_atomic	Number of times HW detected that VA of an atomic request is on a memory boundary that prevents atomic execution.
res_rem_inv_err	Number of times HW detected an incoming send with invalidate request in which the R_KEY to invalidate did not MR/MW which could be invalidated.

Table 46: Responder Errors (Continued)

Counters	Description
res_mem_error64	Number of times HW detected a RQ/SRQ SGE which points to an inaccessible memory.
res_srq_err	Number of times HW detected a QP moving to error state because the associated SRQ is in error.
res_cmp_err	Number of time HW detected that there is no CQE space available on CQ or CQ is not in valid state.
res_invalid_dup_rkey	Number of times HW detected invalid R_KEY while re-sending responses to duplicate read requests.
res_wqe_format_err	Number of times HW detected error in the format of the WQE in the RQ/SRQ.
res_cq_load_err	Number of times HW detected error while attempting to load the CQ context.
res_srq_load_err	Number of times HW detected error while attempting to load the SRQ context.

Table 47: PCI Errors

Counters	Description
res_tx_pci_err	Number of responder transmit PCI errors detected.
res_rx_pci_err	Number of responder receive PCI errors detected.

14.3.5.10 Applications

14.3.5.10.1 OpenMPI

If OpenMPI is used, the OpenMPI source and configuration must be patched using the following commands:

```
$ cd openmpi-x.y.z
$ cat > openmpi.patch << EOF
diff --git a/opal/mca/common/verbs/common_verbs_port.c b/opal/mca/common/verbs/common_verbs_port.c
index 831ba3f..7eb30 100644
--- a/opal/mca/common/verbs/common_verbs_port.c
+++ b/opal/mca/common/verbs/common_verbs_port.c
@@ -68,6 +68,10 @@ int opal_common_verbs_port_bw(struct ibv_port_attr *port_attr,
    /* EDR: 25.78125 Gb/s * 64/66, in megabits */
    *bandwidth = 25000;
    break;
+ case 64:
+     /* ODR: 50 Gb/s * 64/66, in megabits */
+     *bandwidth = 50000;
+     break;
+ case 128:
+     /* ODR: 100 Gb/s * 64/66, in megabits */
+     *bandwidth = 100000;
+     break;
    default:
        /* Who knows? */
        return OPAL_ERR_NOT_FOUND;
EOF
$ patch -p1 < openmpi.patch
$ make
$ sudo make install
```

A device configuration section must also be added using the following commands:

```
$ sudo cat >> /usr/local/share/openmpi/mca-btl-openib-device-params.ini << EOF
[Broadcom Netxtreme]
```

```

vendor_id = 0x14e4
vendor_part_id =
5637,5638,5652,5824,5825,5838,5839,5846,5847,5848,5849,5855,5858,5859,5861,5867,5869,5871,5872,5873
use_eager_rdma = 1
mtu = 1024
receive_queues = P,128,256,192,128:S,65536,256,192,128
max_inline_data = 96
EOF

```

14.3.5.11 Performance

NCC is a comprehensive solution used for congestion management that can help reduce packet losses and congestion spreading as well as improve latency by keeping switch queue levels low.

Congestion control performance is measured by these network traffic performance metrics during periods of congestion:

- Fairness of bandwidth allocation between qp
- Link utilization
- Latency

Under heavy congestion, NCC can enforce fairness at a per-QP level, with low variation between streams. Streams not crossing the point of network contention are not affected.

Performance may vary depending on the topology, number of flows, traffic types, and the application used. Careful consideration and understanding should be used when adjusting the different NCC parameters. As a default, deterministic marking with DCTCP is recommended and can be configured using the setup script provided.

14.3.5.11.1 Priority Flow Control

Although Priority Flow Control (PFC) is not required, it is recommended to enable PFC to ensure that packets are not dropped in bursty or transient scenarios. In cases where PFC is not being utilized, adjustments of the cc tunables are required to ensure the ramp up and ramp down is appropriate based on the user's scenario.

14.3.5.11.2 CNP Traffic Classes

It is recommended that CNPs are classified onto a different traffic class on both the NIC and the switch for optimal performance to ensure CNP are not utilizing the same buffer as the RoCE packets.

14.3.5.11.3 Disable CPU Power Saving

Intel CPU power saving technology can cause packet RoCE drops with bursty traffic. It is highly recommended to set BIOS power saving mode to maximum performance, and disable c-states and p-states with kernel options by editing the `/etc/default/grub` file, and appending the following to `GRUB_CMDLINE_LINUX_DEFAULT`:

```
intel_pstate=disable processor.max_cstate=1 intel_idle.max_cstate=0
```

Rebuild the grub configuration using the following command:

```
sudo /usr/sbin/grub-mkconfig* -o /boot/grub/grub.cfg
```

14.3.5.12 Limitations

In dual-port NICs, if both ports are on same subnet, RDMA perftest commands may fail. The possible cause is due to an arp flux issue in the Linux OS. To work around this limitation, use multiple subnets for testing or bring the second port/interface down.

14.3.5.13 Known Issues

`Bnxt_en` and `Bnxt_re` are designed to function as a pair. Older `Bnxt_en` drivers prior to version 1.7.x do not support RDMA and cannot be loaded at the same time as the `Bnxt_re` (RDMA) driver. The user may experience a system crash and reboot if `Bnxt_re` is loaded with older `Bnxt_en` drivers. It is recommended that the user load the `Bnxt_en` and `Bnxt_re` module from the same `netxtreme-bnxt_en-<1.7.x>.tar.gz` bundle.

To prevent mismatching a combination of `bnxt_en` and `bnxt_re` from being loaded, the following is required:

- If RedHat/CentOS 7.2 OS was installed to the target system using PXEboot with `bnxt_en` DUD or a kernel module RPM, delete the file `bnxt_en.ko` found in `/lib/modules/$(uname -r)/extra/bnxt_en/bnxt_en.ko` or edit `/etc/depmmod.d/`.
- `bnxt_en.conf` to override to use updated version. Users can also erase the current Broadcom Ethernet Network adapter Linux kernel driver using the `rpm -e kmod-bnxt_en` command. RHEL 7.3/SLES 12 Sp2 has `bnxt_en` inbox driver (older than v1.7.x). This driver must be removed and the latest `bnxt_en` be added before applying the `bnxt_re` (RoCE drivers).

14.4 Windows and Use Case Examples

14.4.1 SMB Direct

Windows Server 2012 includes a new feature called SMB Multichannel, part of the SMB 3.0 protocol, which increases the network performance and availability for file servers.

SMB Multichannel allows file servers to use multiple network connections simultaneously and provides the following capabilities:

- Increased Throughput – The file server can simultaneously transmit more data using multiple connections for high speed network adapters or multiple network adapters.
- Network Fault Tolerance – When using multiple network connections at the same time, the clients can continue to work uninterrupted despite the loss of a network connection.
- Automatic Configuration – SMB Multichannel automatically discovers the existence of multiple available network paths and dynamically adds connections as required.

SMB Multichannel is the feature responsible for detecting the RDMA capabilities of NICs to enable the SMB Direct feature (SMB over RDMA). Without SMB Multichannel, SMB uses regular TCP/IP with these RDMA-capable NICs (all provide a TCP/IP stack side-by-side with the new RDMA stack).

With SMB Multichannel, SMB detects the RDMA capability and create multiple RDMA connections for that single session (two per interface). This allows SMB to use the high throughput, low latency, and low CPU utilization offered by these RDMA NICs. It also offers fault tolerance if multiple RDMA interfaces are used.

14.4.1.1 Kernel Mode

Windows Server 2012 and beyond invokes the RDMA capability in the NIC for SMB file traffic if both ends are enabled for RDMA. Broadcom NDIS miniport bnxtd.sys v20.6.2 and beyond support RoCEv1 and RoCEv2 via the NDKPI interface. The default setting is RoCEv1.

To enable RDMA:

1. The goal is to exercise as many RDMA connections per network interface as possible using a simple server to client relationship. To achieve that, following registry key needs to be added and set its value to 16:
 - a. HKLM\System\CurrentControlSet\Services\LanmanWorkstation\Parameters\ConnectionCountPerRdmaNetworkInterface
 - b. The default is 2; with a valid range from 1 to 16.
 - c. This allows 16 RDMA connections per Network share. In order to scale up from here with a single interface, additional alias IP address must be created with different subnets.
2. Upgrade the NIC NVRAM using the appropriate board packages. In the UEFI HII, enable support for RDMA.
3. Go to the adapter Advanced Properties page and set NetworkDirect Functionality to Enabled for each Broadcom Ethernet Network adapter miniport, or using PowerShell window, run the following command:

```
Set-NetAdapterAdvancedProperty -RegistryKeyword *NetworkDirect -RegistryValue 1
```

4. The following Powershell commands return true if NetworkDirect is enabled.

```
Get-NetOffLoadGlobalSetting  
Get-NetAdapterRDMA
```

14.4.1.2 User Mode

Before running a user mode application written to NDSPI, copy and install the bxndspi.dll user mode driver. To copy and install the user mode driver:

1. Copy bxndspi.dll to C:\Windows\System32.
2. Install the driver by running the following command:

```
rundll32.exe .\bxndspi.dll,Config install|more
```

14.4.1.3 Verifying that NIC is Enabled for RDMA

To verify that the NIC is enabled for RDMA:

1. Verify that NetworkDirect Functionality is enabled for each interface under the **Advance Tab**.
2. Using PowerShell, issue the following commands and ensure it returns True:

```
Get-NetAdapterRDMA
```

14.4.1.4 Verifying SMB Multichannel is Enabled

To verify that SMB multichannel is enabled:

1. Issue the following command and ensure Client RDMA Capable is True:

```
Get-SmbMultiChannelConnection
```

2. SMB multichannel is enabled by defaults. To enable or disable SMB multichannel, use the following commands:

Server Side:

- Enable – `Set-SmbServerConfiguration -EnableMultiChannel $true`
- Disable – `Set-SmbServerConfiguration -EnableMultiChannel $false`

Client Side:

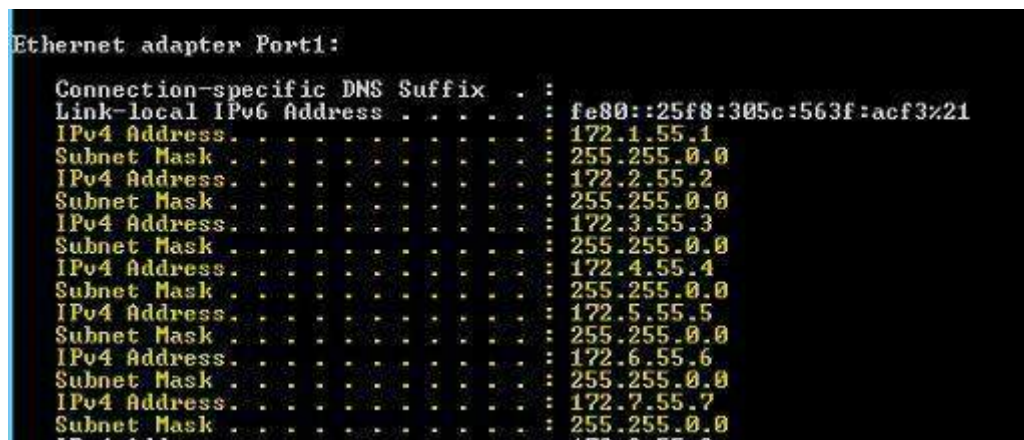
- Enable – `Set-SmbClientConfiguration -EnableMultiChannel $true`
- Disable – `Set-SmbClientConfiguration -EnableMultiChannel $false`

14.4.1.5 Setting Up the System

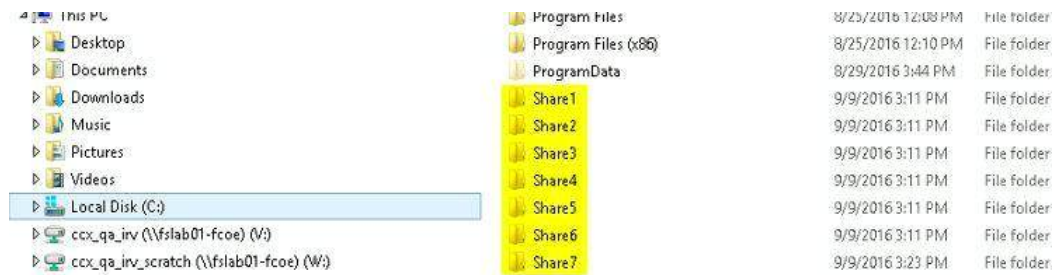
To setup the system:

1. Configure the server by creating seven or more IP address with different subnets. For example:
 - 172.1.55.1
 - 172.2.55.2
 - 172.3.55.3
 - 172.4.55.4
 - 172.5.55.5
 - 172.6.55.6
 - 172.7.55.7

Figure 52: Server/Target Configuration



2. Create seven folders named Share1 to Share7 and individually share them.

Figure 53: Shared Folders

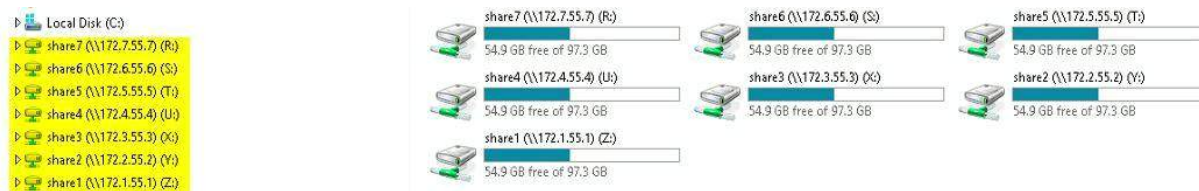
3. Configure the client by creating seven or more IP Address with different subnets that are accessible by the server system.

For example:

- 172.1.54.1
- 172.2.54.2
- 172.3.54.3
- 172.4.54.4
- 172.5.54.5
- 172.6.54.6
- 172.7.54.7

4. Map a network drive to the server as follows:

- Drive letter: \\172.1.55.1\Share1
- Drive letter: \\172.2.55.2\Share2
- Drive letter: \\172.3.55.3\Share3
- Drive letter: \\172.4.55.4\Share4
- Drive letter: \\172.5.55.5\Share5
- Drive letter: \\172.6.55.6\Share6
- Drive letter: \\172.7.55.7\Share7

Figure 54: Drive Mapping

Each of the network drives generated 16 RDMA connections for a total of 112 with seven drives.

14.4.1.6 Traffic Generation

To exercise all 16 RDMA connections simultaneously using a different traffic generation tool:

- If MLTT (License Software) is being used:
 - Change the number of thread counts from 1 to 16. This ensures that all 16 channels have traffic running.
- If Diskspd (freeware and successor to SQLIO) is being used:
 - Use a combination of the following two parameters which produce a product of 16, for example:

```
-o2 -t8, -o4 -t4, or -o1 -t16
-o: Outstanding I/O request. This is your queue depth.
-t: Number of threads per file.
```

14.4.1.7 Verifying RDMA

To verify RDMA:

Create a file share on the remote system and open that share using Windows Explorer. To avoid a hard disk read/write speed bottleneck, a RAM disk is recommended as the network share under test.

1. From PowerShell, run the following commands:

```
Get-SmbMultichannelConnection | fl *RDMA*
ClientRdmaCapable : True
ServerRdmaCapable : True
```

2. If both client and server show True, then any file transfers over this SMB connection use SMB.

3. The following commands can be used to enable/disable SMB Multichannel:

Server Side:

- Enable – `Set-SmbServerConfiguration -EnableMultiChannel $true`
- Disable – `Set-SmbServerConfiguration -EnableMultiChannel $false`

Client Side:

- Enable – `Set-SmbClientConfiguration -EnableMultiChannel $true`
- Disable – `Set-SmbClientConfiguration -EnableMultiChannel $false`

By default, the driver sets up two RDMA connections for each network share per IP address (on a unique subnet). Scale up the number of RDMA connections by adding multiple IP addresses, each with different a subnet, for the same physical port under test. Multiple network shares can be created and mapped to each link partner using the unique IP addresses created.

Example:

- On Server 1, create the following IP addresses for Network Port1:
 - 172.1.10.1
 - 172.2.10.2
 - 172.3.10.3
- On the same Server 1, create three shares:
 - Share1
 - Share2
 - Share3
- On the network link partners:
 - Connect to \\172.1.10.1\share1
 - Connect to \\172.2.10.2\share2
 - Connect to \\172.3.10.3\share3
 - And so forth.

14.4.1.8 Verification

14.4.1.8.1 How to Verify RDMA Connections

Verification can be performed using either Performance Monitor or Power Shell.

14.4.1.8.2 Perfmon

Using Perfmon, the total number of active RDMA connections can be verified using the RDMA Activity counter. Verification for which of the 16 channels are being exercised can also be done by using the SMB direct connection counters.

NOTE: Ensure that traffic is running to see the counters.

Figure 55: Perfmon for Verification (Part 1)

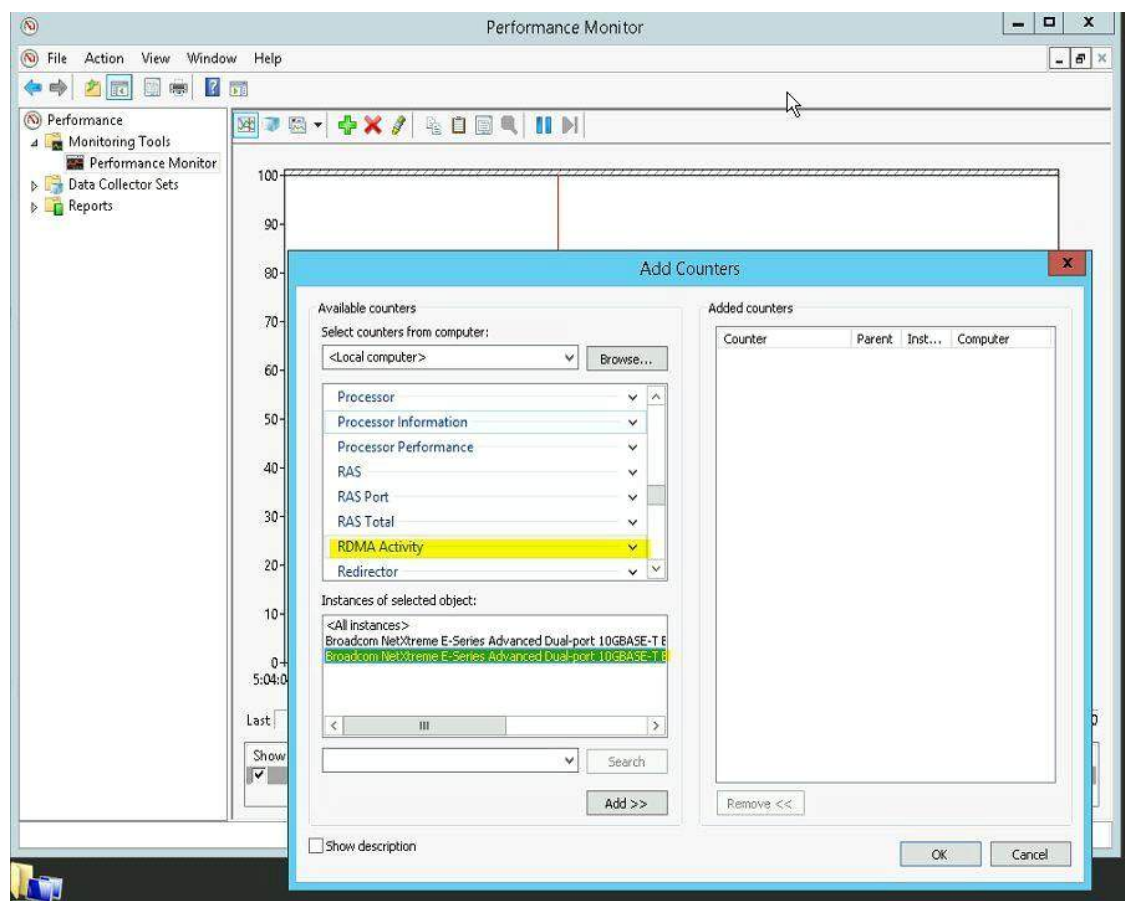


Figure 56: Perfmon for Verification (Part 2)

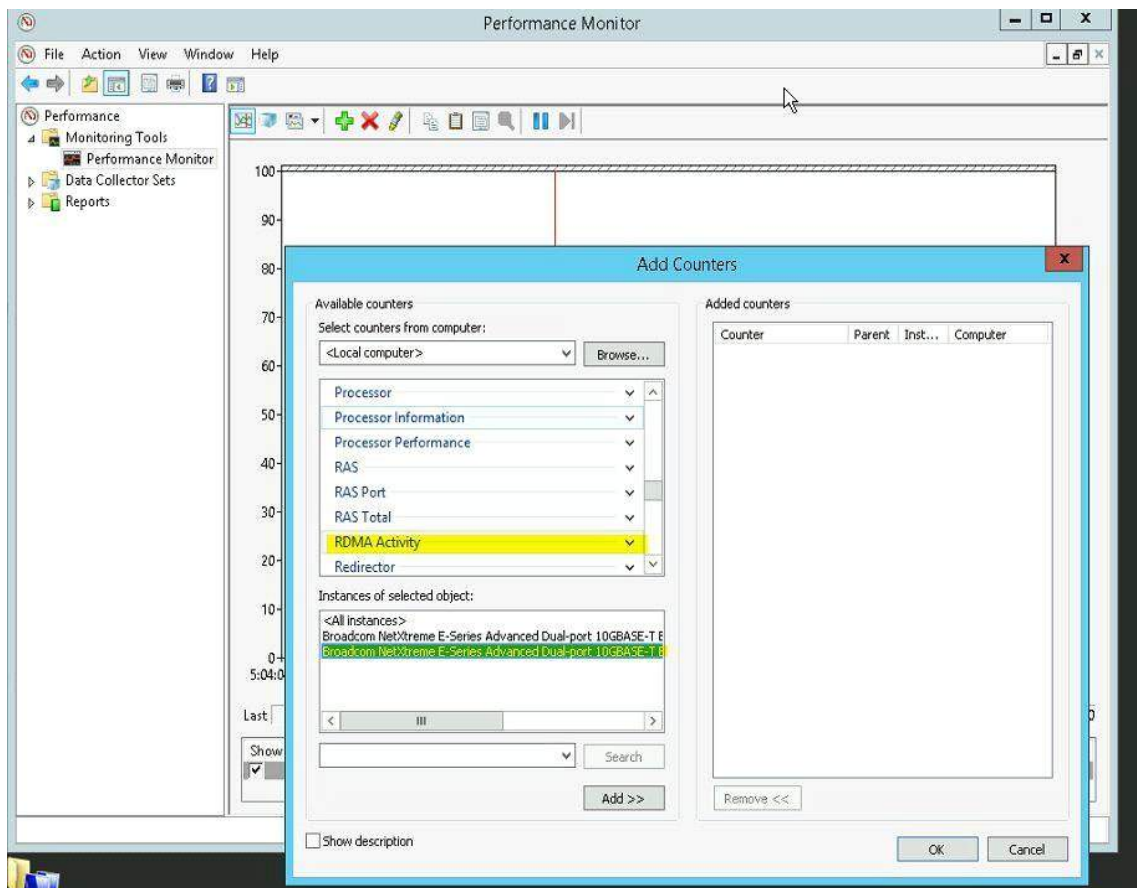
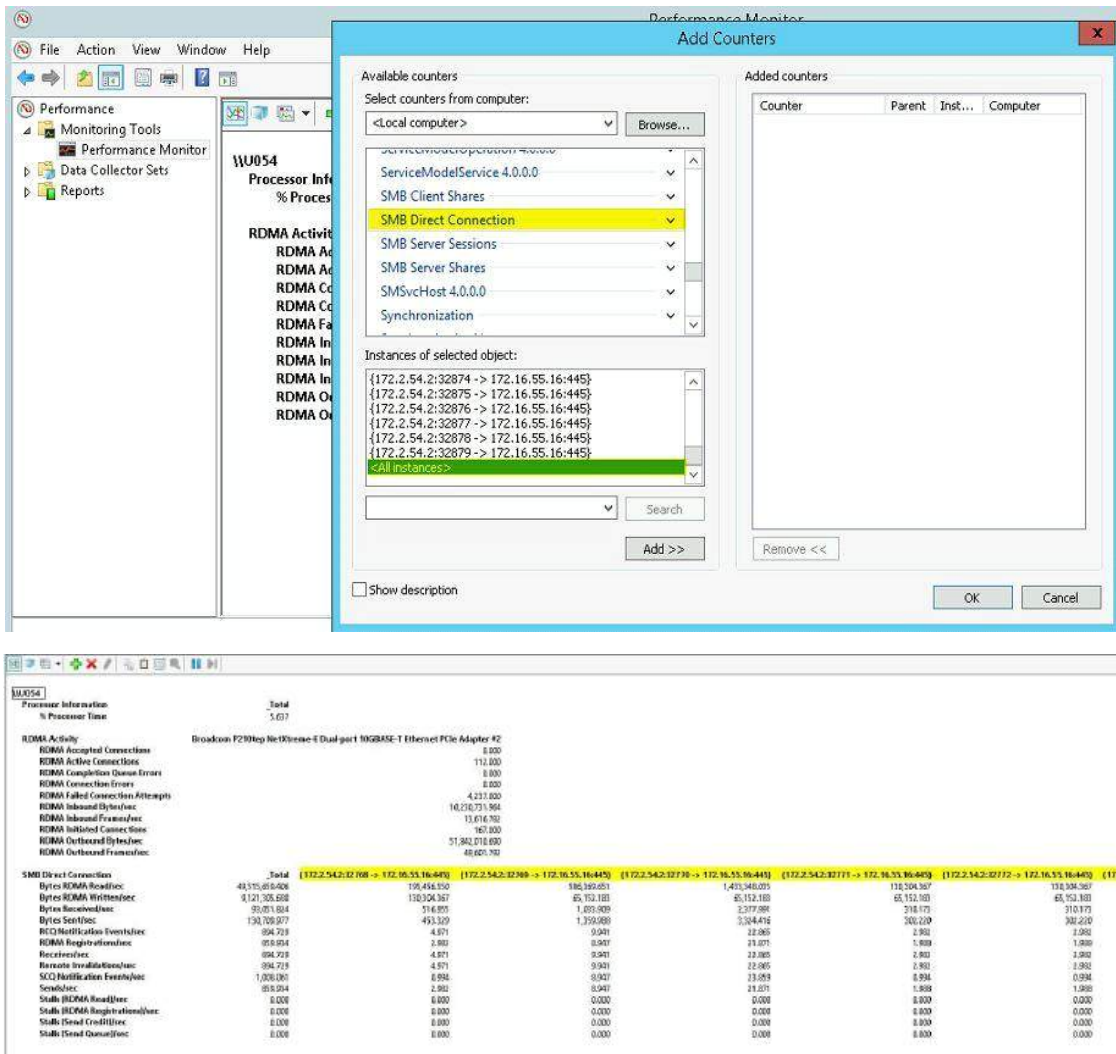


Figure 57: Perfmon for Verification (Part 3)

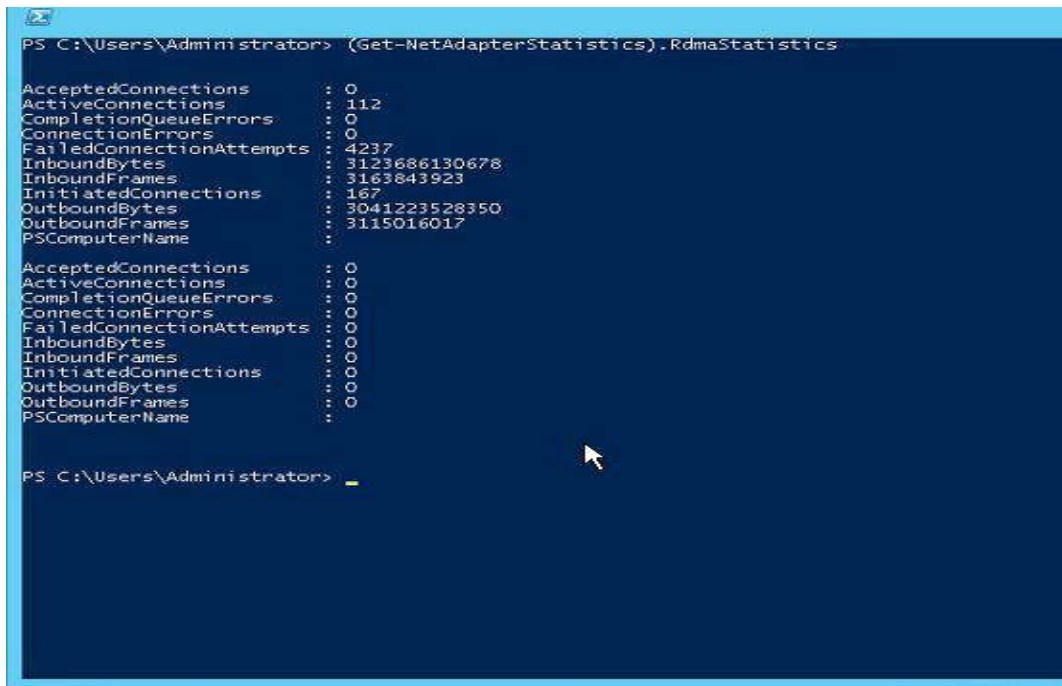


14.4.1.8.3 Powershell

PowerShell can be used for verification. Use the following commands at the Powershell prompt. There are connections listed if using RDMA. Otherwise, it defaults to TCP.

- Netstat -xan – Shows RDMA Connections
- Netstat -an – Shows TCP Connections
- (Get-NetAdapterStatistics).RdmaStatistics – Lists RDMA Activity Connections

Figure 58: Powershell for Verification



```

PS C:\Users\Administrator> (Get-NetAdapterStatistics).RdmaStatistics

AcceptedConnections      : 0
ActiveConnections        : 112
CompletionQueueErrors    : 0
ConnectionErrors         : 0
FailedConnectionAttempts : 4237
InboundBytes              : 3123686130678
InboundFrames            : 3163843923
InitiatedConnections     : 167
OutboundBytes             : 3041223528350
OutboundFrames           : 3115016017
PSComputerName           :

AcceptedConnections      : 0
ActiveConnections        : 0
CompletionQueueErrors    : 0
ConnectionErrors         : 0
FailedConnectionAttempts : 0
InboundBytes             : 0
InboundFrames            : 0
InitiatedConnections     : 0
OutboundBytes            : 0
OutboundFrames           : 0
PSComputerName           :

PS C:\Users\Administrator>
  
```

14.5 VMware ESX and Use Case Examples

14.5.1 Limitations

The current version of the RoCE supported driver requires ESXi-6.5.0 GA build 4564106 or above.

14.5.2 BNXT RoCE Driver Requirements

The BNXTNET L2 driver must be installed with the `disable_roce=0` module parameter before installing the driver.

To set the module parameter, use the following command:

```
esxcfg-module -s "disable_roce=0" bnxtnet
```

Use ESX6.5 L2 driver version 20.6.9.0 (RoCE supported L2 driver) or above.

14.5.3 Installation

To install the RoCE driver:

1. Copy the <bnxtroce>-<driver version>.vib file in /var/log/vmware using the following commands:

```
$ cd /var/log/vmware
$ esxcli software vib install --no-sig-check -v <bnxtroce>-<driver version>.vib
```

2. Reboot the machine.
3. Verify that the drivers are correctly installed using the following command:

```
esxcli software vib list | grep bnxtroce
```

To disable ECN (enabled by default) for RoCE traffic use the `tos_ecn=0` module parameter for bnxtroce.

14.5.4 Configuring Paravirtualized RDMA Network Adapters

See [Vmware.com](https://www.vmware.com) for additional information on setting up and using Paravirtualized RDMA (PVRDMA) network adapters.

14.5.4.1 Configuring a Virtual Center for PVRDMA

To configure a Virtual Center for PVRDMA:

1. Create DVS (requires a Distributed Virtual Switch for PVRDMA).
2. Add the host to the DVS.

14.5.4.2 Tagging vmknics for PVRDMA on ESX Hosts

To tag a vmknics for PVRDMA to use on ESX hosts:

1. Select the host and right-click on **Settings** to switch to the settings page of the **Manage** tabs.
2. In the **Settings** page, expand **System** and click **Advanced System Settings** to show the **Advanced System Settings** key-pair value and its summary.
3. Click **Edit** to bring up the **Edit Advanced System Settings**.
Filter on **PVRDMA** to narrow all the settings to just `Net.PVRDMAVmknics`.
4. Set the `Net.PVRDMAVmknics` value to `vmknics`, as in example `vmk0`.

14.5.4.3 Setting the Firewall Rule for PVRDMA

To set the firewall rule for PVRDMA:

1. Select the host and right-click on **Settings** to switch to the settings page of the **Manage** tabs.
2. In the **Settings** page, expand **System** and click **Security Profile** to show the firewall summary.
3. Click **Edit** to bring up the **Edit Security Profile**.
4. Scroll down to find `pvrmda` and check the box to set the firewall.

14.5.4.4 Adding a PVRDMA Device to the VM

To add a PVRDMA device to the VM:

1. Select the VM and right-click on **Edit Settings**.
2. Add a new Network Adapter.
3. Select the network as a **Distributed Virtual Switch** and **Port Group**.
4. For the **Adapter Type**, select **PVRDMA** and click **OK**.

14.5.5 Configuring the VM on Linux Guest OS

NOTE: The user must install the appropriate development tools including git before proceeding with the configuration steps below.

1. Download the PVRDMA driver and library using the following commands:

```
git clone git://git.openfabrics.org/~aditr/pvrdma_driver.git
git clone git://git.openfabrics.org/~aditr/libpvrdma.git
```

2. Compile and install the PVRDMA guest driver and library.
3. To install the driver, execute `make && sudo insmod pvrdma.ko` in the directory of the driver.
The driver must be loaded after the paired vmxnet3 driver is loaded.

NOTE: The installed RDMA kernel modules may not be compatible with the PVRDMA driver. If so, remove the current installation and restart. Then follow the installation instructions. See the README in the driver's directory for more information about the different RDMA stacks.

4. To install the library, execute `./autogen.sh && ./configure --sysconfdir=/etc && make && sudo make install` in the directory of the library.

NOTE: The installation path of the library needs to be in the shared library cache. Follow the instructions in the INSTALL file in the library's directory.

NOTE: The firewall settings may need to be modified to allow RDMA traffic. Ensure the proper firewall settings are in place.

5. Add the `/usr/lib` in the `/etc/ld.so.conf` file and reload the `ldconf` by running `ldconfig`
6. Load IB modules using `modprobe rdma_ucm`.
7. Load the PVRDMA kernel module using `insmod pvrdma.ko`.
8. Assign an IP address to the PVRDMA interface.
9. Verify whether the IB device is created by running the `ibv_devinfo -v` command.

15 DCBX – Data Center Bridging

Broadcom Ethernet Network adapters support IEEE 802.1Qaz DCBX as well as the older CEE DCBX specification. DCB configuration is obtained by exchanging the locally configured settings with the link peer. Since the two ends of a link may be configured differently, DCBX uses a concept of *willing* to indicate which end of the link is ready to accept parameters from the other end. This is indicated in the DCBX protocol using a single bit in the ETS Configuration and PFC TLV, this bit is not used with ETS Recommendation and Application Priority TLV. By Default, the Broadcom Ethernet Network adapter is in *willing* mode while the link partner network switch is in *non-willing* mode. This ensures the same DCBX setting on the Switch propagates to the entire network.

Users can manually set Broadcom Ethernet Network adapters to *non-willing* mode and perform various PFC, Strict Priority, ETS, and APP configurations from the host side. See the driver readme.txt for additional details on available configurations. This section provides an example of how such a setting can be done in Windows with Windows PowerShell. Additional information on DCBX, QoS, and associated use cases are described in additional details in a separate white paper, beyond the scope of this user manual.

The following settings in the UEFI HII menu are required to enable DCBX support:

System Setup→Device Settings→NetXtreme-E NIC→Device Configuration Menu

15.1 QoS Profile – Default QoS Queue Profile

NOTE: This section does not apply to BCM95750X devices.

Quality of Server (QoS) resources configuration is necessary to support various PFC and ETS requirements where finer tuning beyond bandwidth allocation is needed. Broadcom Ethernet Network adapters allow the administrator to select between devoting NIC hardware resources to support Jumbo Frames and/or combinations of lossy and lossless Class of Service queues (CoS queues). Many combinations of configuration are possible and therefore can be complicated to compute. This option allows a user to select from a list of precomputed QoS Queue Profiles. These precomputed profiles are designed to optimize support for PFC and ETS requirements in typical customer deployments.

The following is a summary description of each QoS Profile.

Table 48: QoS Profiles

Profile No.	Jumbo Frame Support	No. of Lossy CoS Queues/Port	No. of Lossless CoS Queues/Port	Support for 2-Port SKU
Profile #1	Yes	0	1 (PFC Supported)	Yes (25 Gb/s)
Profile #2	Yes	4	2 (PFC Supported)	No
Profile #3	No. (MTU <= 2 KB)	6	2 (PFC Supported)	Yes (25 Gb/s)
Profile #4	Yes	1	2 (PFC Supported)	Yes (25 Gb/s)
Profile #5	Yes	1	0 (No PFC Support)	Yes (25 Gb/s)
Profile #6	Yes	8	0 (No PFC Support)	Yes (25 Gb/s)
Profile #7	This configuration maximizes packet-buffer allocations to two lossless CoS Queues to maximize RoCE performance while trading off flexibility.			
	Yes	0	2	Yes (25 Gb/s)
Default	Yes	Same as Profile #4		Yes

15.2 DCBX Mode – Enable (IEEE only)

This option allows a user to enable/disable DCBX with the indicated specification. IEEE only indicates that IEEE 802.1Qaz DCBX is selected.

Windows Driver setting:

After enabling the indicated options in the UEFI HII menu to set firmware level settings, perform the following selection in the Windows driver advanced properties.

Open **Windows Manager** → **Broadcom NetXtreme E Series adapter** → **Advanced Properties** → **Advanced tab**

Quality of Service = Enabled

Priority & VLAN = Priority& VLAN enabled

VLAN = <ID>

Set desired VLAN id

To exercise the DCB related command in Windows PowerShell, install the appropriate DCB Windows feature.

1. In the **Task Bar**, right-click the Windows PowerShell icon and then click **Run as Administrator**. Windows PowerShell opens in elevated mode.
2. In the Windows PowerShell console, type:

```
Install-WindowsFeature "data-center-bridging"
```

15.3 DCBX Willing Bit

The DCBX willing bit is specified in the DCB specification. If the willing bit on a device is true, the device is willing to accept configurations from a remote device through DCBX. If the willing bit on a device is false, the device rejects any configuration from a remote device and enforces only the local configurations.

Use the following to set the willing bit to True or False. 1 for enabled, 0 for disabled.

Example `set-netQoSdcbxSetting -Willing 1`

Use the following to create a Traffic Class.

```
C:\> New-NetQoSTrafficClass -name "SMB class" -priority 4 -bandwidthPercentage 30 -Algorithm ETS
```

NOTE: By default, all IEEE 802.1p values are mapped to a default traffic class, which has 100% of the bandwidth of the physical link. The command shown above creates a new traffic class to which any packet tagged with eight IEEE 802.1p value 4 is mapped, and its Transmission Selection Algorithm (TSA) is ETS and has 30% of the bandwidth. It is possible to create up to seven new traffic classes. In addition to the default traffic class, there are at most eight traffic classes in the system.

Use the following in displaying the created Traffic Class:

```
C:\> Get-NetQoSSTrafficClass
```

Name	Algorithm	Bandwidth(%)	Priority
[Default]	ETS	70	0-3, 5-7
SMB class	ETS	30	4

Use the following in modifying the Traffic Class:

```
PS C:\> Set-NetQoSTrafficClass -Name "SMB class" -BandwidthPercentage 40
PS C:\> get-NetQoSTrafficClass
Name Algorithm Bandwidth(%) Priority
-----
[Default] ETS          60 0-3,5-7
SMB class ETS          40      4
```

Use the following to remove the Traffic Class:

```
PS C:\> Remove-NetQoSTrafficClass -Name "SMB class"
PS C:\> Get-NetQoSTrafficClass
Name Algorithm Bandwidth(%) Priority
-----
[Default] ETS          100      0-7
```

Use the following to create Traffic Class (Strict Priority):

```
C:\> New-NetQoSTrafficClass -name "SMB class" -priority 4 -bandwidthPercentage 30-Algorithm Strict
```

Enabling PFC:

```
PS C:\> Enable-NetQoSFlowControl -priority 4
PS C:\> Get-NetQoSFlowControl -priority 4
Priority Enabled
-----
4 True
```

```
PS C:\> Get-NetQoSFlowControl
```

Disabling PFC:

```
PS C:\> disable-NetQoSflowControl -priority 4
PS C:\> get-NetQoSFlowControl -priority 4
Priority Enabled
-----
4 False
```

Use the following to create QoS Policy:

```
PS C:\> New-NetQoSPolicy -Name "SMB policy" -SMB -PriorityValue8021Action 4

Name : SMB policy
Owner : Group Policy (Machine)
NetworkProfile : All
Precedence : 127
```

NOTE: The previous command creates a new policy for SMB. SMB is an inbox filter that matches TCP port 445 (reserved for SMB). If a packet is sent to TCP port 445 it is tagged by the operating system with IEEE 802.1p value of 4 before the packet is passed to a network miniport driver. In addition to SMB, other default filters include iSCSI (matching TCP port 3260), NFS (matching TCP port 2049), LiveMigration (matching TCP port 6600), FCOE (matching EtherType 0x8906) and NetworkDirect. NetworkDirect is an abstract layer created on top of any RDMA implementation on a network adapter. NetworkDirect must be followed by a Network Direct port. In addition to the default filters, a user can classify traffic by application's executable name (as in the first example below), or by IP address, port, or protocol.

Use the following to create QoS Policy based on the Source/Destination Address:

```
PS C:\> New-NetQosPolicy "Network Management" -IPDstPrefixMatchCondition 10.240.1.0/24 -
IPProtocolMatchCondition both -NetworkProfile all -PriorityValue8021Action 7
Name : Network Management
Owner : Group Policy (Machine)
Network Profile : All
Precedence : 127
IPProtocol : Both
IPDstPrefix : 10.240.1.0/24
PriorityValue : 7
```

Use the following to display QoS Policy:

```
PS C:\> Get-NetQosPolicy
Name : Network Management
Owner : (382ACFAD-1E73-46BD-A0A-6-4EE0E587B95)
NetworkProfile : All
Precedence : 127
IPProtocol : Both
IPDstPrefix : 10.240.1.0/24
PriorityValue : 7
Name : SMB policy
Owner : (382AFAD-1E73-46BD-A0A-6-4EE0E587B95)
NetworkProfile : All
Precedence : 127
Template : SMB
PriorityValue : 4
```

Use the following to modify the QoS Policy:

```
PS C:\> Set-NetqosPolicy -Name "Network Management" -IPSrcPrefixMatchCondition 10.235.2.0/24 -
IPProtocolMatchCondition both -PriorityValue802.1Action 7
PS C:\> Get-NetQosPolicy -name "network management"
Name : Network Management
Owner : {382ACFD-1E73-46BD-A0A0-4EE0E587B95}
NetworkProfile : All
Precedence : 127
IPProtocol : Both
IPSrcPrefix : 10.235.2.0/24
IPDstPrefix : 10.240.1.0/24
PriorityValue : 7
```

Use the following to remove QoS Policy:

```
PS C:\> Remove-NetQosPolicy -Name "Network Management"
```

16 DPDK – Configuration and Use Case Examples

The testpmd application can be used to test the DPDK in a packet forwarding mode and also to access NIC hardware features such as Flow Director. It also serves as an example of how to build a more fully-featured application using the DPDK SDK. The following chapters show how to build and run the testpmd application and how to configure the application from the command line and the run-time environment.

16.1 Compiling the Application

To compile the application:

1. Set the required environmental variables and go to the source code with the following commands:

```
cd /Linux/Linux_DPDK
tar zxvf dpdk-*.gz
cd dpdk-*
make config T=x86_64-native-linuxapp-gcc && make
```

2. Allocate system resources and attach the UIO module with the following commands:

```
mkdir -p /mnt/huge
mount -t hugetlbfs nodev /mnt/huge
echo 2048 > /sys/devices/system/node/node0/hugepages/hugepages-2048kB/nr_hugepages
echo 2048 > /sys/devices/system/node/node1/hugepages/hugepages-2048kB/nr_hugepages
modprobe uio
insmod ./build/kmod/igb_uio.ko
```

3. Bind the device with the following command:

```
usertools/dpdk-devbind.py -b igb_uio <PCI Device ID>
```

Example: ./usertools/dpdk-devbind.py -b igb_uio 3b:00.0

4. The PCI device information is displayed by lspci with the following commands:

```
[root@localhost /]# lspci |grep Eth
3b:00.0 Ethernet controller: Broadcom Limited BCM57414 NetXtreme-E 10Gb/25Gb RDMA Ethernet
Controller (rev 01)
3b:00.1 Ethernet controller: Broadcom Limited BCM57414 NetXtreme-E 10Gb/25Gb RDMA Ethernet
Controller (rev 01)
```

16.2 Running the Application

To run the application, execute the following command:

```
build/app/testpmd -l 0,1,2,3,4,5,6,7,8 -- -i --nb-ports=1 --nb-cores=8 --txq=2 --rxq=2
```

Options for this example:

- -l – CORELIST List of cores to run.
- -i – Interactive Run testpmd in interactive mode.
- --nb-cores=N – Sets the number of forwarding cores.
- --nb-ports=N – Sets the number of forwarding ports.
- --rxq=N – Sets the number of RX queues per port to N.
- --txq=N – Sets the number of TX queues per port to N.

16.3 Testpmd Runtime Functions

When the testpmd application is started in interactive mode, (-i|--interactive), it displays a prompt that can be used to start and stop forwarding, configure the application, display statistics (including the extended NIC statistics aka xstats), set the Flow Director, and other tasks.

```
testpmd>
```

16.4 Control Functions

This section contains the control functions.

start

Starts packet forwarding with current configuration:

```
testpmd> start
```

start tx_first

Starts packet forwarding with current configuration after sending specified number of bursts of packets:

```
testpmd> start tx_first (""|burst_num)
```

The default burst number is 1 when burst_num not presented.

stop

Stops packet forwarding and display accumulated statistics:

```
testpmd> stop
```

quit

Quits to prompt:

```
testpmd> quit
```

16.5 Display Functions

The functions in this section are used to display information about the testpmd configuration or the NIC status.

- show port – Displays information for a given port or all ports.
- show port rss reta – Displays the RSS redirection table entry indicated by masks on port X.
- show port rss-hash – Displays the RSS hash functions and RSS hash key of a port.
- show (rxq|txq) – Displays information for a given port's RX/TX queue.
- show config – Displays the configuration of the application. The configuration comes from the command-line.
- set fwd – Sets the packet forwarding mode.
- read rxd – Displays an RX descriptor for a port RX queue.
- read txd – Displays a TX descriptor for a port TX queue.

16.6 Configuration Functions

The testpmd application can be configured from the runtime as well as from the command line. This section describes the available configuration functions that are available.

csum set – Selects the hardware or software calculation of the checksum when transmitting a packet using the csum forwarding engine: `testpmd> csum set (ip|udp|tcp|sctp|outer-ip) (hw|sw) (port_id).`

17 Collecting Support Data

This section provides information on installing and using the Broadcom SOS reporting tool.

17.1 Introduction

The Broadcom SOS reporting tool builds on the open source `bcm_sosreport` tool to collect system information for support purposes. The following sections describe how to create the `bcm_sosreport` package and how to install and run the tool. The report that is generated can be sent to a Broadcom support representative for analysis.

17.2 Features

In addition to the default data collection plugins that come with `sosreport`, the package also includes the following:

- AMD and Nvidia GPU topology reports if `clinfo` or `nvidia-smi` utilities are installed.
- Broadcom NIC coredumps
- Broadcom sysfs files for RoCE statistics and tuning
- `lldptool` QoS configuration if installed
- `niccli` QoS configuration if installed

17.3 Installing the SOS Reporting Tool Automatically

The `bcm_sosreport` tool is prepackaged as an RPM and DEB package within the `utils/bcm_sosreport` folder of the software release archive. Install this package using the following command:

```
RPM: yum install /utils/bcm_sosreport/bcm_sosreport-<version>.noarch.rpm  
DEB: apt-get install /utils/bcm_sosreport/bcm_sosreport-<version>.deb
```

17.4 Installing the SOS Reporting Tool Manually

To install the SOS Reporting Tool manually, see the following sections:

17.4.1 Installing the sosreport from pip

The `bcm_sosreport` package is dependent on the `sosreport` tool. If the system does not have an `sosreport` package (such as SUSE), manually install `sosreport` and `bcm_sosreport`.

1. Install the pip utility package (`python3-pip`) per the project documentation located [here](#).
2. Install `sosreport` using pip: `pip3 install sosreport`

17.4.2 Installing the bcm_sosreport Package

After the `sosreport` package is installed with `pip`, the `bcm_sosreport` package can be installed with `yum` or `apt-get` as follows:

```
RPM: yum install /utils/bcm_sosreport/bcm_sosreport-<version>.noarch.rpm
DEB: apt-get install /utils/bcm_sosreport/bcm_sosreport-<version>.deb
```

17.4.3 Installing bcm_sosreport Manually

If it is not possible to install the `bcm_sosreport .deb` or `.rpm` package, manually extract the tar file and install each file as follows:

```
tar xf bcm_sosreport-<VERSION>.tar.gz
cd bcm_sosreport-<VERSION>
cp etc/sos/extras.d/*/etc/sos/extras.d/
cp opt/bcm_sosreport/* /opt/bcm_sosreport/
cp usr/bin/bcm_sosreport /usr/bin/
chmod +x /usr/bin/bcm_sosreport
```

17.5 Running the Report

After `bcm_sosreport` is installed, run a report using the following command:

```
bcm_sosreport
```

To view additional options, use the following command:

```
bcm_sosreport -h
```

17.6 Using the Report

The `bcm_sosreport` collects system data and then generates a `.tar.gz` file. The name of this file is shown by `bcm_sosreport` at the end of the collection. If working with a Broadcom support engineer, make this file available to them.

17.6.1 Viewing the File Contents

To view the contents of the file, copy it to a convenient system and then extract it with the following command:

```
tar xf <FILE>
```

A directory is created with the same name as the file (minus `.tar.gz`) with a partial copy of the target server's file system, plus additional log files, and collected device logs in the `"tmp"` directory.

Revision History

EthernetNIC-User-Guide-UG316-2CS; September 26, 2024

Updated:

- [Table 21, Host Interface Features](#) – Updated Wake On LAN description.
- [Table 27, Supported Operating Systems](#) – Updated supported operating systems.
- [Installing the Linux Driver](#) – Removed install.sh script.
- [Linux](#) – Removed install.sh script.

EthernetNIC-User-Guide-UG315-2CS; July 19, 2024

Added:

- Collecting Support Data

EthernetNIC-User-Guide-UG314-2CS; April 1, 2024

Updated:

- Table 21, Host Interface Features – Added note on BCM57454.
- RDMA over Converged Ethernet – RoCE – Added note on BCM57454.

NetXtreme-E-UG313-2CS; August 30, 2023

Updated:

- Configuring 200G Link Speeds
- VMware SR-IOV Use Case Example
- Generic Receive Offload (GRO) and Large Receive Offload (LRO)

NetXtreme-E-UG312-2CS; June 22, 2023

Updated:

- Table 18, LED Functions – added 200 Gb/s support.
- Table 21, Host Interface Features – updated PTP description.
- Table 26, Validated Cables and Modules
- SFP28 – Updated description.

Added:

- Configuring 200G Link Speeds

NetXtreme-E-UG311-2CS; June 1, 2023

Updated:

- Removed CCM support.

Added:

- Advanced NPAR

NetXtreme-E-UG310-2CS; November 15, 2022

Updated:

- Limitations – Added note on NPAR configuration support.

NetXtreme-E-UG309-2CS; August 31, 2022

Updated:

- Limitations – Added note on NPAR configuration support.

NetXtreme-E-UG308-2CS; February 1, 2022

Updated:

- Device Configuration Menu – Updated number of MS-X Vectors per PF section.

NetXtreme-E-UG307-2CS; November 2, 2021

Updated:

- Device Configuration Menu

NetXtreme-E-UG306-2CS; July 30, 2021

Updated:

- Table 29, Validated Cables and Modules

NetXtreme-E-UG305-2CS; June 10, 2021

Updated:

- Supported Operating Systems
- Device Configuration Menu

NetXtreme-E-UG304-2CS; March 23, 2021

Updated:

- Figure 45, Device Configuration Menu

NetXtreme-E-UG303-2CS; February 10, 2021

Updated:

- Supported Operating Systems
- Added BCM957504-NGM250 to the functional description table.
- System-Level Configuration
- Auto-Negotiation Configuration

Added:

- VMWare Enhanced Networking Stack (ENS)

NetXtreme-E-UG302-2CS; July 28, 2020

Updated:

- Supported Operating Systems

NetXtreme-E-UG301-2CS; June 8, 2020

Updated:

- Supported Operating Systems
- Host Interface Features
- Hardware Requirements
- Installing the VMware Driver
- Limitations

NetXtreme-E-UG300-2CS; February 20, 2020

Initial release



ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
RECEITA ESTADUAL

Nome: **COMPETHICS IT SOLUCOES EM TECNO DA INFORM LTDA**

CNPJ base: **28.452.362/**

Obs.: A presente certidão é válida para toda a empresa, representada pelo CNPJ base composto pelos 8 primeiros dígitos. Todos os estabelecimentos da empresa foram avaliados na pesquisa de regularidade fiscal.

Certificamos que, aos **11 dias do mês de JULHO do ano de 2025**, revendo os bancos de dados da Secretaria da Fazenda do Estado do Rio Grande Sul, não elidido o direito de a Fazenda proceder a posteriores verificações e, a qualquer tempo, vir a cobrar crédito apurado, o titular do CNPJ base acima se enquadra na seguinte situação:

CERTIDAO NEGATIVA

Constitui-se esta certidão em meio de prova de existência ou não, em nome do interessado, de débitos ou pendências relacionados na Instrução Normativa DRP nº 45/98, Título IV, Capítulo V, 1.1.

Débitos protestados e posteriormente regularizados perante a Receita Estadual do Rio Grande do Sul não impedem a emissão de "Certidão Negativa", porém, caso não sejam pagas as taxas cartoriais, o débito permanece protestado pelo cartório, podendo ser a causa de restrições em entidades de proteção ao crédito. Nesses casos, regularize as taxas diretamente no cartório.

Esta certidão **NÃO** comprova a quitação:

- a) de tributos devidos mensalmente e declarados na Declaração Anual de Simples Nacional (DASN) e no Programa Gerador do Documento de Arrecadação do Simples Nacional (PGDAS-D) pelos contribuintes optantes pelo Simples Nacional;
- b) de ITCD e de ITBI (nas hipóteses em que este imposto seja de competência estadual - Lei nº 7.608/81) em procedimentos judiciais e extrajudiciais de inventário, arrolamento, separação, divórcio, dissolução de união estável ou partilha de bens.

Esta certidão é válida até 8/9/2025.

Certidão expedida gratuitamente e com base na IN/DRP nº 45/98, Título IV, Capítulo V.

A autenticidade deste documento deverá ser confirmada em
<https://www.sefaz.rs.gov.br/SAT/CertidaoSitFiscalConsulta.aspx>
com o preenchimento apenas dos dois campos a seguir:

Certidão nº: **35838417**
Autenticação: **46209945**





ESTADO DO RIO GRANDE DO SUL
SECRETARIA DA FAZENDA
RECEITA ESTADUAL

Nome: **COMPETHICS IT SOLUCOES EM TECNO DA INFORM LTDA**

CNPJ base: **28.452.362/**

Obs.: A presente certidão é válida para toda a empresa, representada pelo CNPJ base composto pelos 8 primeiros dígitos. Todos os estabelecimentos da empresa foram avaliados na pesquisa de regularidade fiscal.

Certificamos que, aos **02 dias do mês de SETEMBRO do ano de 2025**, revendo os bancos de dados da Secretaria da Fazenda do Estado do Rio Grande Sul, não elidido o direito de a Fazenda proceder a posteriores verificações e, a qualquer tempo, vir a cobrar crédito apurado, o titular do CNPJ base acima se enquadra na seguinte situação:

CERTIDAO NEGATIVA

Constitui-se esta certidão em meio de prova de existência ou não, em nome do interessado, de débitos ou pendências relacionados na Instrução Normativa DRP nº 45/98, Título IV, Capítulo V, 1.1.

Débitos protestados e posteriormente regularizados perante a Receita Estadual do Rio Grande do Sul não impedem a emissão de "Certidão Negativa", porém, caso não sejam pagas as taxas cartoriais, o débito permanece protestado pelo cartório, podendo ser a causa de restrições em entidades de proteção ao crédito. Nesses casos, regularize as taxas diretamente no cartório.

Esta certidão **NÃO** comprova a quitação:

- a) de tributos devidos mensalmente e declarados na Declaração Anual de Simples Nacional (DASN) e no Programa Gerador do Documento de Arrecadação do Simples Nacional (PGDAS-D) pelos contribuintes optantes pelo Simples Nacional;
- b) de ITCD e de ITBI (nas hipóteses em que este imposto seja de competência estadual - Lei nº 7.608/81) em procedimentos judiciais e extrajudiciais de inventário, arrolamento, separação, divórcio, dissolução de união estável ou partilha de bens.

Esta certidão é válida até 31/10/2025.

Certidão expedida gratuitamente e com base na IN/DRP nº 45/98, Título IV, Capítulo V.

A autenticidade deste documento deverá ser confirmada em
<https://www.sefaz.rs.gov.br/SAT/CertidaoSitFiscalConsulta.aspx>
com o preenchimento apenas dos dois campos a seguir:

Certidão nº: **36841574**
Autenticação: **47228802**





ESTADO DO RIO GRANDE DO SUL
PODER JUDICIÁRIO

CERTIDÃO JUDICIAL CÍVEL NEGATIVA

À vista dos registros constantes nos sistemas de Informática do Poder Judiciário do Estado do Rio Grande do Sul é expedida a presente certidão por não constar distribuição de ação falimentar, concordatária, recuperação judicial e extrajudicial em tramitação contra a seguinte parte interessada:

COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, CNPJ 28452362000132, Endereço - AV. IPIRANGA, 2642, SANTA CECILIA, PORTO ALEGRE/RS, CEP: 90.610-000.

24 de junho de 2025, às 11:20:08

OBSERVAÇÕES:

A aceitação desta certidão está condicionada à conferência dos dados da parte interessada contra aqueles constantes no seu documento de identificação, bem como à verificação de sua validade no site do Tribunal de Justiça do Estado do Rio Grande do Sul na Internet, endereço <http://www.tjrs.jus.br>, menu Processos e Serviços / Serviços Processuais / Emissão de Antecedentes e Certidões, informando o seguinte código de controle: **0cc2f6c44be2e944f5fd50a0d4ecac68**

Importante: Esta certidão possui validade de 90 dias a partir da data de sua emissão.



ESTADO DO RIO GRANDE DO SUL
PODER JUDICIÁRIO

CERTIDÃO JUDICIAL CÍVEL NEGATIVA

À vista dos registros constantes nos sistemas de Informática do Poder Judiciário do Estado do Rio Grande do Sul é expedida a presente certidão por não constar distribuição de ação de execução patrimonial em tramitação contra a seguinte parte interessada:

COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, CNPJ 28452362000132, Endereço - AV. IPIRANGA, 2642, SANTA CECILIA, PORTO ALEGRE/RS, CEP: 90.610-000.

24 de junho de 2025, às 11:21:06

OBSERVAÇÕES:

A aceitação desta certidão está condicionada à conferência dos dados da parte interessada contra aqueles constantes no seu documento de identificação, bem como à verificação de sua validade no site do Tribunal de Justiça do Estado do Rio Grande do Sul na Internet, endereço <http://www.tjrs.jus.br>, menu Processos e Serviços / Serviços Processuais / Emissão de Antecedentes e Certidões, informando o seguinte código de controle: **341266012db5822a920441d7d8ea2d41**

Importante: Esta certidão possui validade de 90 dias a partir da data de sua emissão.



TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO GRANDE DO SUL
Praça Mal Deodoro, 55 - Bairro Centro - CEP 90010-908 - Porto Alegre - RS - 3º andar
www.tjrs.jus.br

CERTIDÃO - SERVIÇO DE CADASTRO DA CORREGEDORIA-GERAL DA JUSTIÇA

CERTIFICO, atendendo pedido formulado pela parte interessada, que na comarca de Porto Alegre, neste Estado, há:

1. No FORO CENTRAL (Prédios I e II): um (01) Cartório da Direção do Foro; dezoito (18) Cartórios Cíveis, nominados do primeiro ao décimo oitavo; quinze (15) Cartórios Criminais (1º, 2º, 3º, 4º, 5º, 6º, 7º, 8º, 9º, 10º, 11º, 12º, 13º, 14º e Juizado do Torcedor e Grandes Eventos e 16º); um (01) Cartório de Execução das Penas e Medidas Alternativas; três (03) Cartórios de Execuções Criminais (1º, 2º, 3º); quatro (04) Cartórios do Júri (1º, 2º, 3º, 4º); nove (09) Cartórios da Fazenda Pública (1º, 2º, 3º, 4º, 5º, 6º, 7º, 8º, 12º); cinco (05) Cartórios de Família (1º, 4º, 5º, 6º, 8º); um (01) Cartório das Curatelas; três (03) Cartórios exclusivos de Sucessões (1º, 2º, 3º); um (01) Cartório de Delitos de Trânsito; um (01) Cartório dos Registros Públicos; dois (02) Cartórios do Juizado da Violência Doméstica e Familiar Contra a Mulher (1º, 2º); quatro (04) Juizados Especiais Cíveis (2º, 3º, 4º, 5º); três (03) Juizados Especiais Criminais (1º, 2º, 3º); três (03) Juizados Especiais da Fazenda Pública (1º, 2º, 3º); quatro (04) Cartórios do Juizado Regional da Infância e Juventude (1º, 2º, 3º, 4º); um (01) Cartório Regional Empresarial; dois (02) Cartórios Estaduais de Processo e Julgamento dos Crimes de Organização Criminosa e Lavagem de Dinheiro (1º, 2º); um (01) Cartório Estadual de Improbidade Administrativa; um (01) Cartório Estadual de Execuções Fiscais de Tributos Estaduais; um (01) Cartório Estadual da Saúde Pública; um (01) Cartório Estadual de Acidente do Trabalho; um (01) Cartório Regional do Meio Ambiente; dois (02) Cartórios Regionais de Garantias (1º e 2º); dois (02) Cartórios da Contadoria (1º, 2º); e um (01) Cartório da Distribuição (incumbe a distribuição das causas Cíveis, Comerciais, dos feitos da Fazenda Pública, Direito Empresarial, Recuperação de Empresas e Falências, Criminais, das causas de Família e Sucessões e a de outras que lhe sejam dependentes).

2. Nos FOROS REGIONAIS*: um (01) Cartório Cível e um (01) Cartório de Família no Alto Petrópolis, no Partenon e na Restinga; dois (02) Cartórios Cíveis no Quarto Distrito (1º, 2º) e no Sarandi (1º Cartório Cível especializado em Família e Cartas Precatórias Cíveis e 2º Cartório Cível); um (01) Cartório Cível na Tristeza; um (01) Juizado Especial Cível e Criminal no Alto Petrópolis (7º), no Partenon (10º), na Restinga (8º), no Sarandi (1º), na Tristeza (6º); e um (01) Cartório da Distribuição e Contadoria em cada um dos Foros Regionais (Alto Petrópolis, Partenon, Restinga, Sarandi, Tristeza e Quarto Distrito), com as mesmas atribuições do Distribuidor do Foro Centralizado da comarca de Porto Alegre, excluídos os feitos de Direito Empresarial, Recuperação de Empresas e Falências, Registros Públicos e Acidentes do Trabalho. Qualquer certidão fornecida pelo Cartório da Distribuição do Foro Central abrange informações de todos os demais Foros, e vice-versa, pois é baseada em um único Banco de Dados. *Provisoriamente os Cartórios do Foro Regional do Quarto Distrito estão alocados no Foro Central (Prédios I e II) da comarca de Porto Alegre.

3. Três (03) Tabelionatos de Protesto de Títulos (1º, 2º, 3º) onde são processados os apontamentos e protestos das letras e títulos comerciais, distribuídos pela CENTRAL DE DISTRIBUIÇÃO DE TÍTULOS; três (03) Serviços de Registro de Títulos e Documentos e Registro

Civil das Pessoas Jurídicas (1º, 2º, 3º); catorze (14) Tabelionatos de Notas (1º ao 14º); seis (06) Serviços de Registro de Imóveis (1ª até a 6ª Zona); oito (08) Serviços de Registro Civil das Pessoas Naturais (1ª até a 8ª Zona).

Observações:

A presente certidão é confeccionada apenas com base nos registros informatizados desta Corregedoria-Geral da Justiça; somente registros consolidados até a presente data.

A conferência dos dados do(a) solicitante é de responsabilidade exclusiva da autoridade recebedora.

A expedição é gratuita.



ESTADO DO RIO GRANDE DO SUL
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

DOCUMENTO ASSINADO POR

RIO GRANDE DO SUL PODER JUDICIARIO

DATA

24/06/2025 11h21min



Este é um documento eletrônico assinado digitalmente conforme Lei Federal nº 11.419/2006 de 19/12/2006, art. 1º, parágrafo 2º, inciso III.

Para conferência do conteúdo deste documento, acesse, na internet, o endereço <https://www.tjrs.jus.br/verificadocs> e digite o seguinte

número verificador: 0001587238642





Certidão Simplificada

Certificamos que as informações abaixo constam dos documentos arquivados nesta Junta Comercial e são vigentes na data de sua expedição.

Nome Empresarial:		COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA	
Natureza Jurídica:		SOCIEDADE EMPRESARIA LIMITADA	
Número de Identificação do Registro de Empresas - NIRE	CNPJ	Data de Arquivamento do Ato Constitutivo	Data de Início de Atividade
4360028195-2	28.452.362/0001-32	17/08/2017	26/07/2017
Endereço Completo:			
AVENIDA IPIRANGA 2642 - BAIRRO SANTA CECILIA CEP 90610-000 - PORTO ALEGRE/RS			
Objeto Social:			
A) COMERCIO, DISTRIBUICAO, REPRESENTACAO, IMPORTACAO, EXPORTACAO E LOCACAO DE EQUIPAMENTOS, PECAS E ACESSORIOS DE INFORMATICA, TELECOMUNICACOES E CONVERGENCIA, SISTEMAS E APLICATIVOS B) COMERCIO DISTRIBUICAO, IMPORTACAO, LOCACAO E MANUTENCAO DE CIRCUITOS FECHADOS DE TELEVISAO, EQUIPAMENTOS E SERVICOS DE SEGURANCA PATRIMONIAL E PESSOAL C) PRESTACAO DE SERVICOS TECNICOS, TERCEIRIZACAO DE MANUTENCAO, PROGRAMACAO, GERENCIAMENTO, ADMINISTRACAO DE EQUIPAMENTOS, SISTEMAS E APLICATIVOS DE INFORMATICA, TELECOMUNICACOES E CONVERGENCIA, BEM COMO, DESENVOLVER TREINAMENTOS SOBRE OS PRODUTOS QUE COMERCIALIZA D) REPRESENTACAO E CESSAO DE LICENCAS DE PROGRAMAS DE COMPUTADOR NAO-CUSTOMIZAVEIS			
Capital Social:	R\$ 500.000,00	Microempresa ou Empresa de Pequeno Porte	Prazo de Duração
QUINHENTOS MIL REAIS		MICRO EMPRESA (Lei Complementar nº123/06)	INDETERMINADO
Capital Integralizado:	R\$ 500.000,00		
QUINHENTOS MIL REAIS			
Sócio(s)/Administrador(es)			
CPF/NIRE	Nome	Tér. Mandato	Participação
017.921.220-63	RAFAELLA TAVARES BARCELOS	xxxxxxx	R\$ 500.000,00
			Função
			SÓCIO / ADMINISTRADOR
Status:	CADASTRADA	Situação:	ATIVA
Último Arquivamento:	07/03/2024	Número:	10272119
Ato	002 - ALTERACAO		
Evento(s)	2211 - ALTERACAO DE ENDERECO DENTRO DO MESMO MUNICIPIO		
	2221 - ALTERACAO DO TITULO DO ESTABELECIMENTO (NOME DE FANTASIA)		
	051 - CONSOLIDACAO DE CONTRATO/ESTATUTO		
Empresa(s) Antecessora(s)			
Nome Anterior	Nire	Número Aprovação	UF
COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO EIRELI - ME	xxxxxxx	8600687	
			Tipo Movimentação
			ALTERAÇÃO DE NOME EMPRESARIAL
Filial(ais) nesta Unidade da Federação ou fora dela			
Nire	CNPJ	Endereço	

Certidão Simplificada Digital emitida pela JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL e certificada digitalmente. Se desejar confirmar a autenticidade desta certidão, acesse o site da JUCISRS (Rio Grande Do Sul) e clique em validar certidão. A certidão pode ser validada de duas formas:

- 1) Validação por envio de arquivo (upload)
- 2) Validação visual (digite o nº C250004791629 e visualize a certidão)



25/284.318-5



Sistema Nacional de Registro de Empresas Mercantil - SINREM
Governador do Estado do Rio Grande do Sul
Secretaria de Desenvolvimento Econômico e Turismo
Junta Comercial, Industrial e Serviços do Rio Grande do Sul

Certidão Simplificada

Certificamos que as informações abaixo constam dos documentos arquivados nesta Junta Comercial e são vigentes na data de sua expedição.

Nome Empresarial: COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA

Natureza Jurídica: SOCIEDADE EMPRESARIA LIMITADA

NADA MAIS#

Porto Alegre, 07 de Agosto de 2025 14:42


JOSÉ TADEU JACOBY
SECRETÁRIO GERAL

A empresa foi transformada automaticamente para sociedade limitada, nos termos do artigo 41 da Lei n.º 14.195, de 26 de agosto de 2021.

Certidão Simplificada Digital emitida pela JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL e certificada digitalmente. Se desejar confirmar a autenticidade desta certidão, acesse o site da JUCISRS (Rio Grande do Sul) e clique em validar certidão. A certidão pode ser validada de duas formas:

- 1) Validação por envio de arquivo (upload)
- 2) Validação visual (digite o nº C250004791629 e visualize a certidão)



25/284.318-5



PREFEITURA DE PORTO ALEGRE
SECRETARIA MUNICIPAL DA FAZENDA

CERTIDÃO GERAL NEGATIVA DE DÉBITOS

Esta certidão é válida até: **28/09/2025**

Nome: COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA

CNPJ: 28.452.362/0001-32

Ressalvado o direito de a Fazenda Pública Municipal cobrar quaisquer créditos que vierem a ser apurados, é certificado que, para o contribuinte acima especificado não constam débitos vencidos, lançados até 26 de agosto de 2025.

Certidão emitida em 29/08/2025 às 09:30:39, conforme Decreto 14.560 e Instruções Normativas SMF 04/2003 e 07/2024.

A autenticidade desta certidão deverá ser verificada no sítio da Secretaria Municipal da Fazenda (<http://www.portoalegre.rs.gov.br/smf>), informando **CNPJ: 28.452.362/0001-32** e o código de autenticidade **3F7BF8D35BFF**

O presente documento não certifica inexistência de débitos do Imposto sobre Serviços de Qualquer Natureza declarados pelo contribuinte no âmbito do Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte - Simples Nacional. Caso o contribuinte seja ou tenha sido optante pelo Simples Nacional nos últimos 5 (cinco) anos, a presente certidão deverá ser complementada por Certidão de Situação Fiscal fornecida pela Receita Federal do Brasil.



PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA
(MATRIZ E FILIAIS)

CNPJ: 28.452.362/0001-32

Certidão nº: 26778098/2025

Expedição: 15/05/2025, às 10:07:27

Validade: 11/11/2025 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **28.452.362/0001-32**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.

Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.º 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022. Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.

No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.

A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (<http://www.tst.jus.br>).

Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE

Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.



REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO 28.452.362/0001-32 MATRIZ	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA 17/08/2017
NOME EMPRESARIAL COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA		
TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA) COMPETHICS PROVEDORA DE SOLUCOES		PORTE ME
CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL 47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática		
CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS 46.15-0-00 - Representantes comerciais e agentes do comércio de eletrodomésticos, móveis e artigos de uso doméstico 46.51-6-01 - Comércio atacadista de equipamentos de informática 46.51-6-02 - Comércio atacadista de suprimentos para informática 46.52-4-00 - Comércio atacadista de componentes eletrônicos e equipamentos de telefonia e comunicação 47.52-1-00 - Comércio varejista especializado de equipamentos de telefonia e comunicação 61.90-6-99 - Outras atividades de telecomunicações não especificadas anteriormente 62.01-5-01 - Desenvolvimento de programas de computador sob encomenda 62.03-1-00 - Desenvolvimento e licenciamento de programas de computador não-customizáveis 62.04-0-00 - Consultoria em tecnologia da informação 62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação 77.39-0-99 - Aluguel de outras máquinas e equipamentos comerciais e industriais não especificados anteriormente, sem operador 80.20-0-01 - Atividades de monitoramento de sistemas de segurança eletrônico 80.20-0-02 - Outras atividades de serviços de segurança 82.99-7-99 - Outras atividades de serviços prestados principalmente às empresas não especificadas anteriormente 85.99-6-04 - Treinamento em desenvolvimento profissional e gerencial 95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos 95.12-6-00 - Reparação e manutenção de equipamentos de comunicação		
CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA 206-2 - Sociedade Empresária Limitada		
LOGRADOURO AV IPIRANGA	NÚMERO 2642	COMPLEMENTO *****
CEP 90.610-000	BAIRRO/DISTRITO SANTA CECILIA	MUNICÍPIO PORTO ALEGRE
UF RS		
ENDEREÇO ELETRÔNICO NFE@COMPETHICS.COM.BR		TELEFONE (51) 3342-3732/ (51) 9626-9055

ENTE FEDERATIVO RESPONSÁVEL (EFR) *****	
SITUAÇÃO CADASTRAL ATIVA	DATA DA SITUAÇÃO CADASTRAL 17/08/2017
MOTIVO DE SITUAÇÃO CADASTRAL	
SITUAÇÃO ESPECIAL *****	DATA DA SITUAÇÃO ESPECIAL *****

Aprovado pela Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022.

Emitido no dia **05/06/2025** às **15:35:19** (data e hora de Brasília).

Página: **1/1**

 Ministério do Empreendedorismo, da Microempresa e da Empresa de Pequeno Porte Secretaria Nacional de Microempresa e Empresa de Pequeno Porte Diretoria Nacional de Registro Empresarial e Integração Secretaria de Desenvolvimento Econômico e Turismo			Nº DO PROTOCOLO (Uso da Junta Comercial)		
NIRE (da sede ou filial, quando a sede for em outra UF) 43600281952		Código da Natureza Jurídica 2062	Nº de Matrícula do Agente Auxiliar do Comércio		
1 - REQUERIMENTO					
ILMO(A). SR.(A) PRESIDENTE DA Junta Comercial, Industrial e Serviços do Rio Grande do Sul					
Nome: <u>COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA</u>					
(da Empresa ou do Agente Auxiliar do Comércio)					
requer a V.Sª o deferimento do seguinte ato:					
Nº FCN/REMP  RSP2400076559					
Nº DE VIAS	CÓDIGO DO ATO	CÓDIGO DO EVENTO	QTDE	DESCRIÇÃO DO ATO / EVENTO	
1	002			ALTERACAO	
		051	1	CONSOLIDACAO DE CONTRATO/ESTATUTO	
		2221	1	ALTERACAO DO TITULO DO ESTABELECIMENTO (NOME DE FANTASIA)	
		2211	1	ALTERACAO DE ENDERECO DENTRO DO MESMO MUNICIPIO	
PORTO ALEGRE Local			Representante Legal da Empresa / Agente Auxiliar do Comércio:		
7 Março 2024 Data			Nome: _____		
			Assinatura: _____		
			Telefone de Contato: _____		
2 - USO DA JUNTA COMERCIAL					
☐ DECISÃO SINGULAR ☐ DECISÃO COLEGIADA					
Nome(s) Empresarial(ais) igual(ais) ou semelhante(s): ☐ SIM ☐ SIM ☐ NÃO ☐ NÃO _____/_____/_____ Data _____ Responsável _____/_____/_____ Data _____ Responsável				Processo em Ordem À decisão _____/_____/_____ Data _____ Responsável	
DECISÃO SINGULAR					
☐ Processo em exigência. (Vide despacho em folha anexa)	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência	
☐ Processo deferido. Publique-se e archive-se.	☐	☐	☐	☐	
☐ Processo indeferido. Publique-se.					
			_____/_____/_____ Data	_____ Responsável	
DECISÃO COLEGIADA					
☐ Processo em exigência. (Vide despacho em folha anexa)	2ª Exigência	3ª Exigência	4ª Exigência	5ª Exigência	
☐ Processo deferido. Publique-se e archive-se.	☐	☐	☐	☐	
☐ Processo indeferido. Publique-se.					
_____/_____/_____ Data	_____ Vogal	_____ Vogal	_____ Vogal		
Presidente da _____ Turma					
OBSERVAÇÕES					





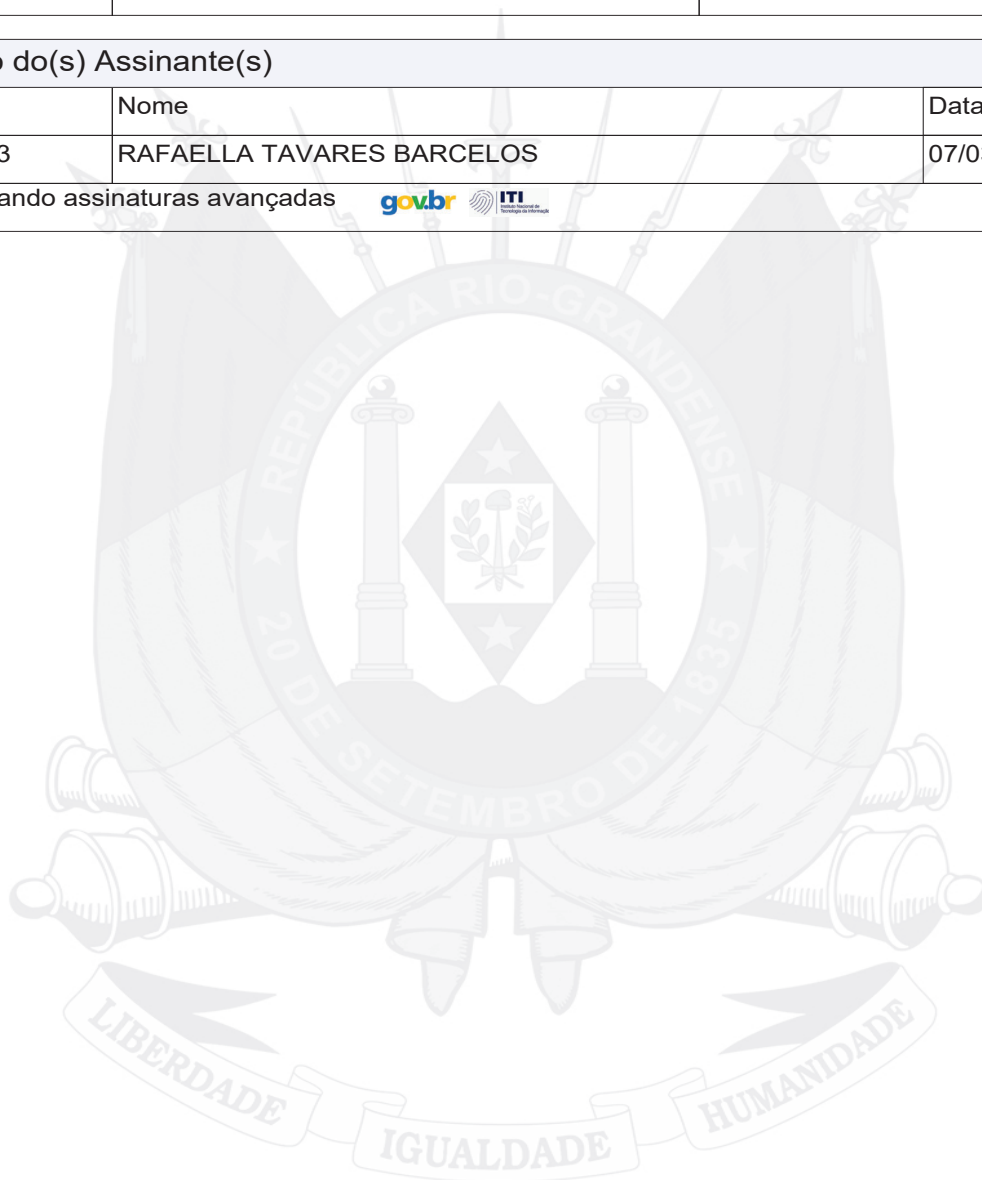
JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL

Registro Digital

Capa de Processo

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
24/067.156-2	RSP2400076559	27/02/2024

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
017.921.220-63	RAFAELLA TAVARES BARCELOS	07/03/2024
Assinado utilizando assinaturas avançadas  		



Junta Comercial, Industrial e Serviços do Rio Grande do Sul

Certifico registro sob o nº 10272119 em 07/03/2024 da Empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, CNPJ 28452362000132 e protocolo 240671562 - 27/02/2024. Autenticação: D7255244BCD83A57202CB2E816265D2C3CEC11FE. José Tadeu Jacoby - Secretário-Geral. Para validar este documento, acesse <http://jucisrs.rs.gov.br/validacao> e informe nº do protocolo 24/067.156-2 e o código de segurança nJ1H Esta cópia foi autenticada digitalmente e assinada em 07/03/2024 por José Tadeu Jacoby Secretário-Geral.


JOSÉ TADEU JACOBY
SECRETÁRIO-GERAL

**SEGUNDA ALTERAÇÃO DE ATO CONSTITUTIVO DE
COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO EIRELI ME
CNPJ 28.452.362/0001-32
NIRE Nº43600281952**

RAFAELLA TAVARES BARCELOS, brasileira, solteira, maior, empresária, portadora de cédula de identidade nº 2115897908, emitida pela SSP/RS, inscrita no CPF sob nº 017.921.220-63, residente e domiciliada na Rua Farnese nº 110, apto 1301, Bairro Bela Vista, Porto Alegre/RS CEP: 90.450-180, por esse instrumento constitui **EMPRESA INDIVIDUAL DE RESPONSABILIDADE LIMITADA**, que girará sob o nome empresarial de **COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO EIRELI ME**, e tem sede e domicílio na Avenida Ipiranga nº 2626 apto 401, Petrópolis, Porto Alegre/RS, CEP 90.610-000, registrada na Junta Comercial do Rio Grande do Sul sob NIRE 43600281952, em 17/08/2017, registrada no CNPJ sob nº 28.452.362/0001-32, com primeira Alteração contratual registrada sob o nº 5269874 em 18/01/2020.

1. A titular resolve alterar o endereço e sede da empresa que passa a ser na Avenida Ipiranga nº 2642, Bairro Petrópolis, Porto Alegre/RS, CEP 90610-000.
2. A alteração da natureza jurídica da presente sociedade operou-se por meio de transformação automática da EIRELI para Sociedade Limitada, conforme disposição contida no art 41 da Lei n.14.195, de 26 de agosto de 2021.
3. De acordo com a cláusula segunda o nome empresarial passa a ser **COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA- ME**.
4. A titular resolve alterar o nome fantasia da empresa para COMPETHICS PROVEDORA DE SOLUÇÕES.
5. Em razão da alteração do tipo societário a titular resolve dividir o capital social total em de R\$ 500.000,00 (quinhentos mil reais), dividindo em 500(quinhentas) mil quotas no valor de R\$ 1,00 (hum real) cada quota, sendo 100% de titularidade de **RAFAELLA TAVARES BARCELOS**, totalmente integralizadas em moeda corrente do País.
6. As demais cláusulas e condições do contrato social original não modificadas no presente Instrumento permanecem inalteradas.
7. A titular resolve consolidar o Contrato Social que passa a ter a seguinte redação:

CONSOLIDAÇÃO DO CONTRATO SOCIAL



1- A empresa possui a denominação de **COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA- ME**. O endereço e sede da empresa é na Avenida Ipiranga nº 2642, Bairro Petrópolis, Porto Alegre/RS, CEP 90610-000.

2. O capital social total é de R\$ 500.000,00 (quinhentos mil reais), dividido em 500(quinhentas) mil quotas no valor de R\$ 1,00 (hum real) cada quota, sendo 100% de titularidade de **RAFAELLA TAVARES BARCELOS**, totalmente integralizadas em moeda corrente do País.

3. A empresa possui o nome fantasia de “COMPETHICS PROVEDORA DE SOLUÇÕES”.

4. A sociedade tem por objeto : a) comércio, distribuição, representação, importação, exportação e locação de equipamentos, peças e acessórios de informática, telecomunicações e convergência, sistemas e aplicativos; b) comércio distribuição, importação, locação e manutenção de circuitos fechados de televisão, equipamentos e serviços de segurança patrimonial e pessoal; c) prestação de serviços técnicos, terceirização de manutenção, programação, gerenciamento, administração de equipamentos, sistemas e aplicativos de informática, telecomunicações e convergência, bem como, desenvolver treinamentos sobre os produtos que comercializa; e) representação e cessão de licenças de programas de computador não customizáveis .

5. A presente empresa se constitui por prazo indeterminado.

6. O titular desta empresa declara que está enquadrada como Microempresa nos termos da legislação vigente.

7. A administração da empresa caberá a **RAFAELLA TAVARES BARCELOS**, já qualificada, com os poderes e atribuições de administrador titular, autorizando o uso do nome empresarial, vedado, no entanto, em atividades estranhas aos interesses da empresa.

8. A responsabilidade do empresário é restrita ao valor de seu capital e responde exclusivamente pela integralização do capital.

9. Ao término de cada exercício, em 31 de dezembro, o administrador prestará contas justificadas de sua administração, procedendo à elaboração do inventário, do balanço patrimonial e do balanço de resultado econômico, cabendo ao empresário, os lucros ou prejuízos apurados.

10. Nos quatro meses seguintes ao término do exercício, o empresário deliberará sobre as contas e designará o administrador quando for o caso.

11. A empresa poderá a qualquer tempo, abrir ou fechar filial ou outra dependência, mediante alteração do ato constitutivo, devidamente assinada pelo titular da empresa.

12. Falecendo o empresário, a empresa continuará suas atividades com os herdeiros, sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes, o valor de



seus haveres será apurado e liquidado com base na situação patrimonial da empresa, à data da resolução, verificada em balanço especialmente levantado.

13. O Administrador declara, sob as penas da lei, de que não está impedido de exercer a administração da empresa por lei especial, ou em virtude de condenação criminal, ou por se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato, ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

14. Fica eleito o foro de Porto Alegre para o exercício e o cumprimento dos direitos e obrigações resultantes deste ato constitutivo.

Porto Alegre, 26 de fevereiro de 2024.





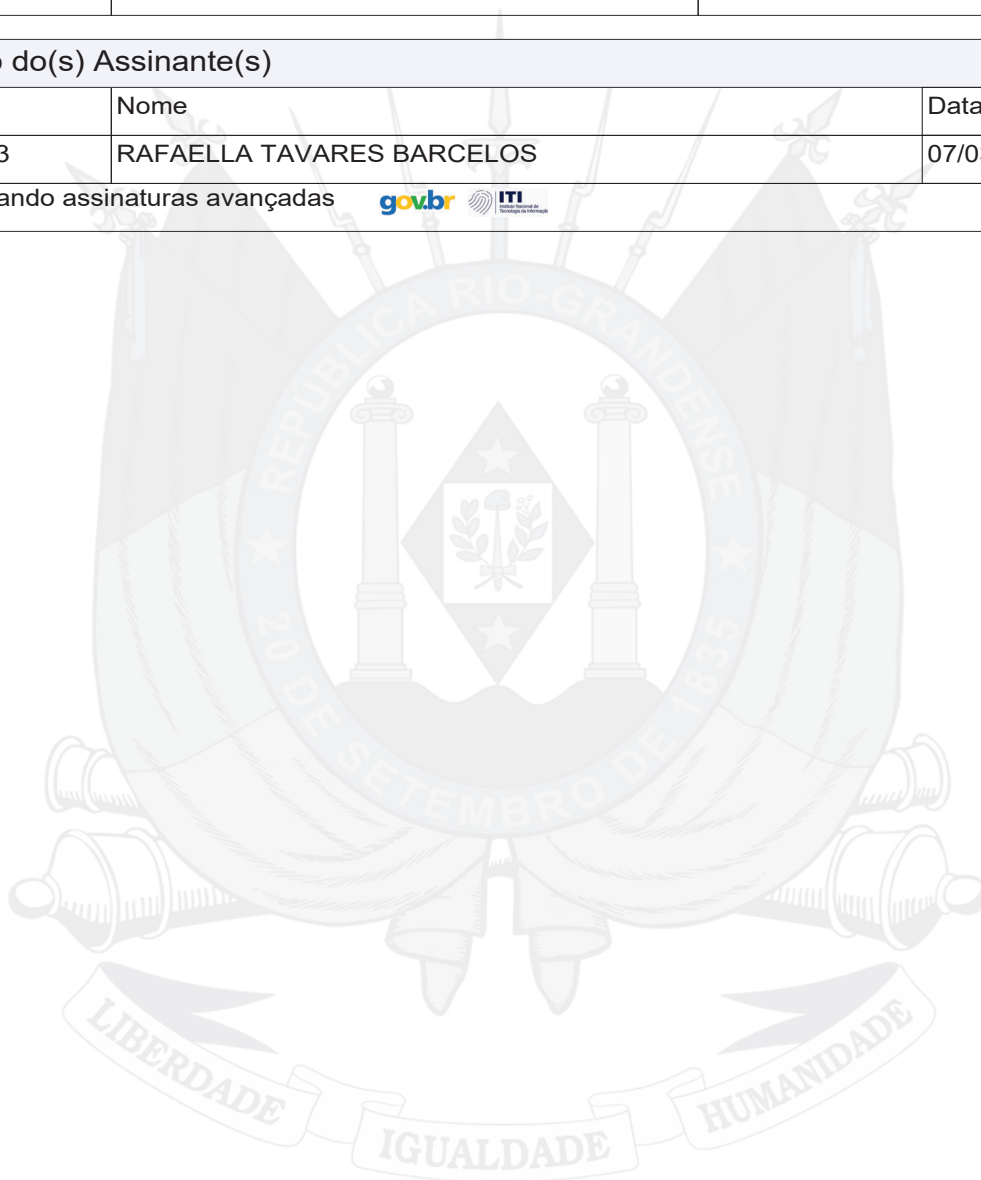
JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL

Registro Digital

Documento Principal

Identificação do Processo		
Número do Protocolo	Número do Processo Módulo Integrador	Data
24/067.156-2	RSP2400076559	27/02/2024

Identificação do(s) Assinante(s)		
CPF	Nome	Data Assinatura
017.921.220-63	RAFAELLA TAVARES BARCELOS	07/03/2024
Assinado utilizando assinaturas avançadas  		



Junta Comercial, Industrial e Serviços do Rio Grande do Sul

Certifico registro sob o nº 10272119 em 07/03/2024 da Empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, CNPJ 28452362000132 e protocolo 240671562 - 27/02/2024. Autenticação: D7255244BCD83A57202CB2E816265D2C3CEC11FE. José Tadeu Jacoby - Secretário-Geral. Para validar este documento, acesse <http://jucisrs.rs.gov.br/validacao> e informe nº do protocolo 24/067.156-2 e o código de segurança nJ1H Esta cópia foi autenticada digitalmente e assinada em 07/03/2024 por José Tadeu Jacoby Secretário-Geral.


JOSÉ TADEU JACOBY
SECRETÁRIO-GERAL



Sistema Nacional de Registro de Empresas Mercantil - SINREM
Governo do Estado do Rio Grande do Sul
Secretaria de Desenvolvimento Econômico e Turismo
Junta Comercial, Industrial e Serviços do Rio Grande do Sul

TERMO DE AUTENTICAÇÃO - REGISTRO DIGITAL

Certifico que o ato, assinado digitalmente, da empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, de CNPJ 28.452.362/0001-32 e protocolado sob o número 24/067.156-2 em 27/02/2024, encontra-se registrado na Junta Comercial sob o número 10272119, em 07/03/2024. O ato foi deferido eletronicamente pelo examinador Leander Belizário da Silva.

Certifica o registro, o Secretário-Geral, José Tadeu Jacoby. Para sua validação, deverá ser acessado o sítio eletrônico do Portal de Serviços / Validar Documentos (<https://portalservicos.jucisrs.rs.gov.br/Portal/pages/imagemProcesso/viaUnica.jsf>) e informar o número de protocolo e chave de segurança.

Capa de Processo

Assinante(s)		
CPF	Nome	Data Assinatura
017.921.220-63	RAFAELLA TAVARES BARCELOS	07/03/2024
Assinado utilizando assinaturas avançadas  		

Documento Principal

Assinante(s)		
CPF	Nome	Data Assinatura
017.921.220-63	RAFAELLA TAVARES BARCELOS	07/03/2024
Assinado utilizando assinaturas avançadas  		

Data de início dos efeitos do registro (art. 36, Lei 8.934/1994): 26/02/2024



Documento assinado eletronicamente por Leander Belizário da Silva, Servidor(a) Público(a), em 07/03/2024, às 12:00.



A autenticidade desse documento pode ser conferida no [portal de serviços da jucisrs](http://portalservicos.jucisrs.rs.gov.br/validacao) informando o número do protocolo 24/067.156-2.



Junta Comercial, Industrial e Serviços do Rio Grande do Sul

Certifico registro sob o nº 10272119 em 07/03/2024 da Empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, CNPJ 28452362000132 e protocolo 240671562 - 27/02/2024. Autenticação: D7255244BCD83A57202CB2E816265D2C3CEC11FE. José Tadeu Jacoby - Secretário-Geral. Para validar este documento, acesse <http://jucisrs.rs.gov.br/validacao> e informe nº do protocolo 24/067.156-2 e o código de segurança nJ1H Esta cópia foi autenticada digitalmente e assinada em 07/03/2024 por José Tadeu Jacoby Secretário-Geral.


JOSÉ TADEU JACOBY
SECRETÁRIO-GERAL

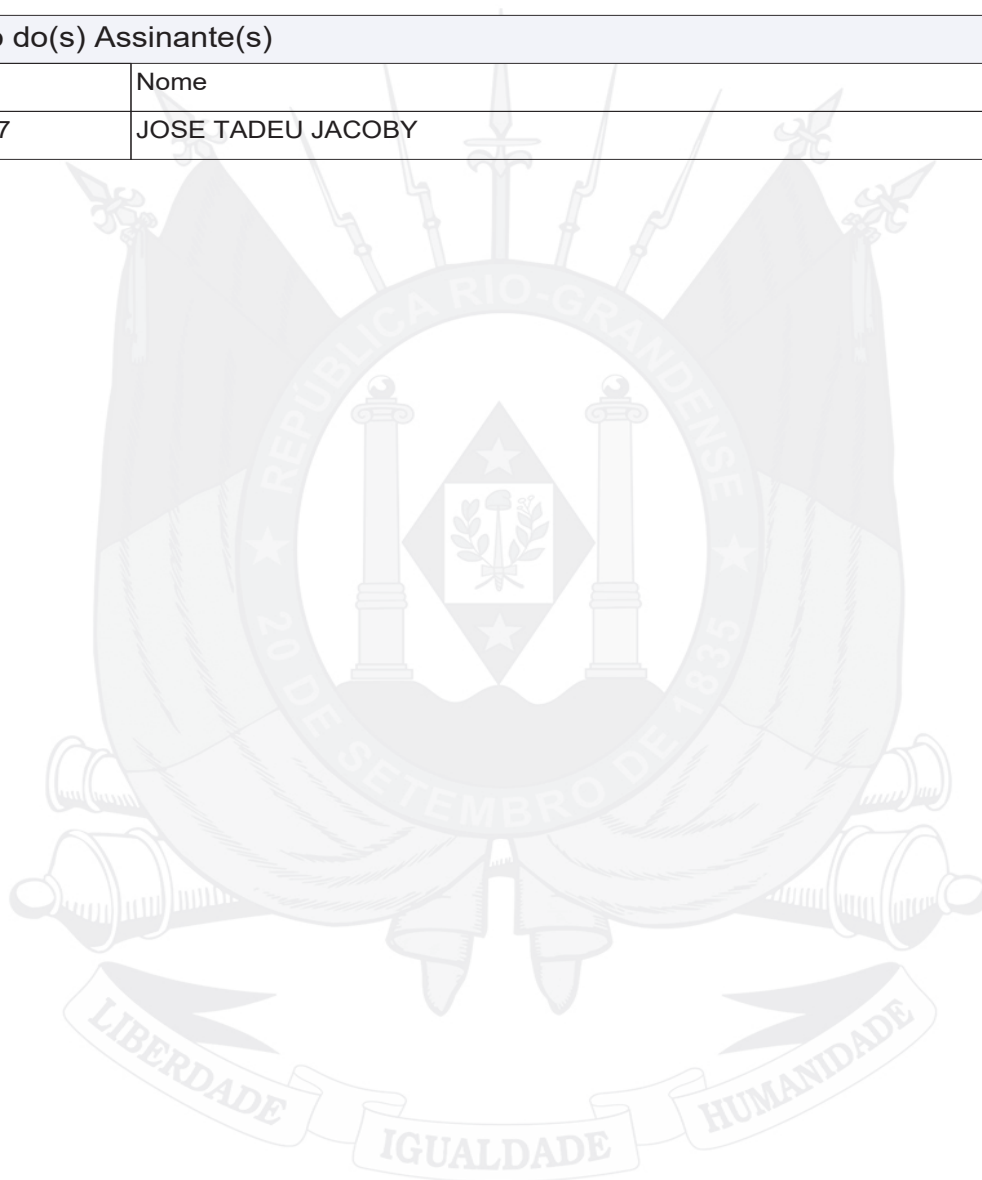


JUNTA COMERCIAL, INDUSTRIAL E SERVIÇOS DO RIO GRANDE DO SUL

Registro Digital

O ato foi assinado digitalmente por :

Identificação do(s) Assinante(s)	
CPF	Nome
054.744.500-87	JOSE TADEU JACOBY



Porto Alegre. quinta-feira, 07 de março de 2024



Junta Comercial, Industrial e Serviços do Rio Grande do Sul

Certifico registro sob o nº 10272119 em 07/03/2024 da Empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, CNPJ 28452362000132 e protocolo 240671562 - 27/02/2024. Autenticação: D7255244BCD83A57202CB2E816265D2C3CEC11FE. José Tadeu Jacoby - Secretário-Geral. Para validar este documento, acesse <http://jucisrs.rs.gov.br/validacao> e informe nº do protocolo 24/067.156-2 e o código de segurança nJ1H Esta cópia foi autenticada digitalmente e assinada em 07/03/2024 por José Tadeu Jacoby Secretário-Geral.


JOSE TADEU JACOBY
SECRETÁRIO-GERAL



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

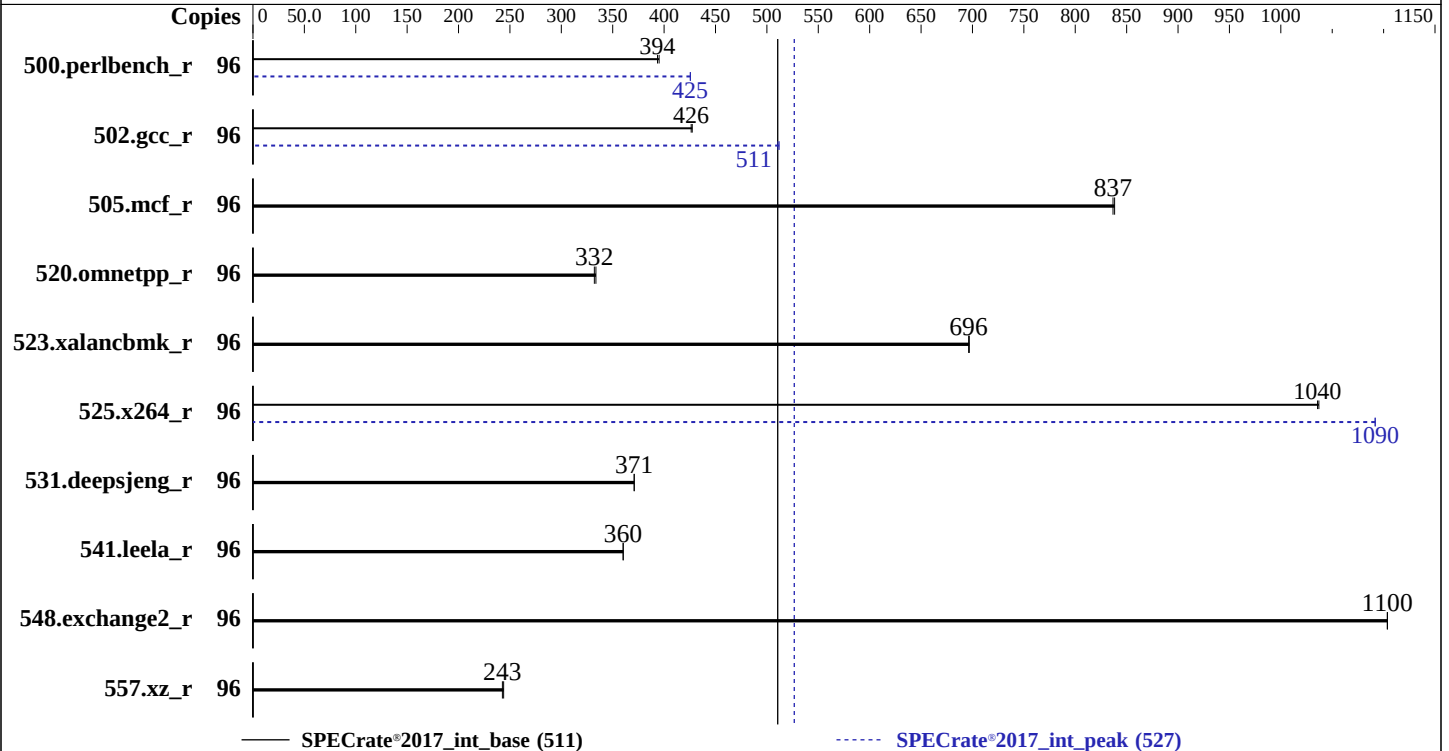
Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023



Hardware

CPU Name: Intel Xeon Gold 6542Y
Max MHz: 4100
Nominal: 2900
Enabled: 48 cores, 2 chips, 2 threads/core
Orderable: 1,2 chips
Cache L1: 32 KB I + 48 KB D on chip per core
L2: 2 MB I+D on chip per core
L3: 60 MB I+D on chip per chip
Other: None
Memory: 512 GB (16 x 32 GB 2Rx8 PC5-5600B-R, running at 5200)
Storage: 70 GB on tmpfs
Other: CPU Cooling: Air

Software

OS: SUSE Linux Enterprise Server 15 SP5
5.14.21-150500.53-default
Compiler: C/C++: Version 2023.2.3 of Intel oneAPI DPC++/C++
Compiler for Linux;
Fortran: Version 2023.2.3 of Intel Fortran
Compiler for Linux;
Parallel: No
Firmware: Version 1.9.12 released Nov-2023
File System: tmpfs
System State: Run level 3 (multi-user)
Base Pointers: 64-bit
Peak Pointers: 32/64-bit
Other: jemalloc memory allocator V5.0.1
Power Management: BIOS and OS set to prefer performance
at the cost of additional power usage.



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Results Table

Benchmark	Base							Peak						
	Copies	Seconds	Ratio	Seconds	Ratio	Seconds	Ratio	Copies	Seconds	Ratio	Seconds	Ratio	Seconds	Ratio
500.perlbench_r	96	387	395	<u>388</u>	<u>394</u>			96	359	426	<u>359</u>	<u>425</u>		
502.gcc_r	96	<u>319</u>	<u>426</u>	318	427			96	266	512	<u>266</u>	<u>511</u>		
505.mcf_r	96	<u>185</u>	<u>837</u>	185	838			96	<u>185</u>	<u>837</u>	185	838		
520.omnetpp_r	96	377	334	<u>379</u>	<u>332</u>			96	377	334	<u>379</u>	<u>332</u>		
523.xalancbmk_r	96	<u>146</u>	<u>696</u>	145	697			96	<u>146</u>	<u>696</u>	145	697		
525.x264_r	96	<u>162</u>	<u>1040</u>	162	1040			96	154	1090	<u>154</u>	<u>1090</u>		
531.deepsjeng_r	96	<u>297</u>	<u>371</u>	297	371			96	<u>297</u>	<u>371</u>	297	371		
541.leela_r	96	441	360	<u>441</u>	<u>360</u>			96	441	360	<u>441</u>	<u>360</u>		
548.exchange2_r	96	<u>228</u>	<u>1100</u>	228	1100			96	<u>228</u>	<u>1100</u>	228	1100		
557.xz_r	96	425	244	<u>427</u>	<u>243</u>			96	425	244	<u>427</u>	<u>243</u>		

SPECrate®2017_int_base = 511

SPECrate®2017_int_peak = 527

Results appear in the order in which they were run. Bold underlined text indicates a median measurement.

Submit Notes

The numactl mechanism was used to bind copies to processors. The config file option 'submit' was used to generate numactl commands to bind each copy to a specific processor. For details, please see the config file.

Operating System Notes

Stack size set to unlimited using "ulimit -s unlimited"

Environment Variables Notes

Environment variables set by runcpu before the start of the run:

LD_LIBRARY_PATH =

"/mnt/ramdisk/cpu2017-1.1.9-ic2023.2.3/lib/intel64:/mnt/ramdisk/cpu2017-1.1.9-ic2023.2.3/lib/ia32:/mnt

/ramdisk/cpu2017-1.1.9-ic2023.2.3/je5.0.1-32"

MALLOC_CONF = "retain:true"

General Notes

Binaries compiled on a system with 2x Intel Xeon Platinum 8280M CPU + 384GB RAM

memory using Red Hat Enterprise Linux 8.4

Transparent Huge Pages enabled by default

Prior to runcpu invocation

Filesystem page cache synced and cleared with:

sync; echo 3> /proc/sys/vm/drop_caches

runcpu command invoked through numactl i.e.:

numactl --interleave=all runcpu <etc>

jemalloc, a general purpose malloc implementation

built with the RedHat Enterprise 7.5, and the system compiler gcc 4.8.5

sources available from jemalloc.net or <https://github.com/jemalloc/jemalloc/releases>

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

General Notes (Continued)

NA: The test sponsor attests, as of date of publication, that CVE-2017-5754 (Meltdown) is mitigated in the system as tested and documented.
Yes: The test sponsor attests, as of date of publication, that CVE-2017-5753 (Spectre variant 1) is mitigated in the system as tested and documented.
Yes: The test sponsor attests, as of date of publication, that CVE-2017-5715 (Spectre variant 2) is mitigated in the system as tested and documented.

Benchmark run from a 70 GB ramdisk created with the cmd: "mount -t tmpfs -o size=70G tmpfs /mnt/ramdisk"

Platform Notes

BIOS settings:

ADDDC Setting : Disabled
DIMM Self Healing on
Uncorrectable Memory Error : Disabled

Virtualization Technology : Disabled
DCU Streamer Prefetcher : Disabled
Sub NUMA Cluster : 2-way Clustering
LLC Prefetch : Disabled
Dead Line LLC Alloc : Disabled

System Profile : Custom
CPU Power Management : Maximum Performance
C1E : Disabled
C States : Autonomous
Memory Patrol Scrub : Disabled
Energy Efficiency Policy : Performance
PCI ASPM L1 Link
Power Management : Disabled
Optimizer Mode : Enabled

Sysinfo program /mnt/ramdisk/cpu2017-1.1.9-ic2023.2.3/bin/sysinfo
Rev: r6732 of 2022-11-07 fe91c89b7ed5c36ae2c92cc097bec197
running on localhost Fri Mar 29 07:16:49 2024

SUT (System Under Test) info as seen by some common utilities.

Table of contents

1. uname -a
2. w
3. Username
4. ulimit -a
5. sysinfo process ancestry
6. /proc/cpuinfo
7. lscpu
8. numactl --hardware
9. /proc/meminfo
10. who -r
11. Systemd service manager version: systemd 249 (249.16+suse.171.gdad0071f15)
12. Services, from systemctl list-unit-files
13. Linux kernel boot-time arguments, from /proc/cmdline
14. sysctl
15. /sys/kernel/mm/transparent_hugepage
16. /sys/kernel/mm/transparent_hugepage/khugepaged
17. OS release

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Platform Notes (Continued)

18. Disk information

19. /sys/devices/virtual/dmi/id

20. dmidecode

21. BIOS

1. uname -a

```
Linux localhost 5.14.21-150500.53-default #1 SMP PREEMPT_DYNAMIC Wed May 10 07:56:26 UTC 2023 (b630043)
x86_64 x86_64 x86_64 GNU/Linux
```

2. w

```
07:16:49 up 3 min, 1 user, load average: 0.06, 0.03, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
root      tty1      -              07:16   22.00s 0.85s  0.00s /bin/bash
/home/DellFiles/bin/Intel/dell-run-speccpu.sh rate --define DL-BIOSinc=Dell-BIOS_Xeon-5.inc --define
DL-BIOS-LogProc=1 --define DL-BIOS-adddcD=1 --define DL-VERS=5.1 --output_format html,pdf,txt
```

3. Username

From environment variable \$USER: root

4. ulimit -a

```
core file size          (blocks, -c) unlimited
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size                (blocks, -f) unlimited
pending signals         (-i) 2059949
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files               (-n) 1024
pipe size                (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
real-time priority      (-r) 0
stack size              (kbytes, -s) unlimited
cpu time                 (seconds, -t) unlimited
max user processes      (-u) 2059949
virtual memory           (kbytes, -v) unlimited
file locks               (-x) unlimited
```

5. sysinfo process ancestry

```
/usr/lib/systemd/systemd --switched-root --system --deserialize 29
login -- root
-bash
/bin/bash ./DELL_rate.sh
/bin/bash /home/DellFiles/bin/dell-run-main.sh rate
/bin/bash /home/DellFiles/bin/dell-run-main.sh rate
/bin/bash /home/DellFiles/bin/Intel/dell-run-speccpu.sh rate --define DL-BIOSinc=Dell-BIOS_Xeon-5.inc
--define DL-BIOS-LogProc=1 --define DL-BIOS-adddcD=1 --define DL-VERS=5.1 --output_format html,pdf,txt
/bin/bash /home/DellFiles/bin/Intel/dell-run-speccpu.sh rate --define DL-BIOSinc=Dell-BIOS_Xeon-5.inc
--define DL-BIOS-LogProc=1 --define DL-BIOS-adddcD=1 --define DL-VERS=5.1 --output_format html,pdf,txt
runcpu --nobuild --action validate --define default-platform-flags --define numcopies=96 -c
ic2023.2.3-lin-sapphirerapids-rate-20231121.cfg --define smt-on --define cores=48 --define physicalfirst
--define invoke_with_interleave --define drop_caches --tune base,peak -o all --define DL-BIOS-SNC=2
--iterations 2 --define DL-BIOSinc=Dell-BIOS_Xeon-5.inc --define DL-BIOS-LogProc=1 --define
DL-BIOS-adddcD=1 --define DL-VERS=5.1 --output_format html,pdf,txt intrate
runcpu --nobuild --action validate --define default-platform-flags --define numcopies=96 --configfile
```

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Platform Notes (Continued)

```
ic2023.2.3-lin-sapphirerapids-rate-20231121.cfg --define smt-on --define cores=48 --define physicalfirst
--define invoke_with_interleave --define drop_caches --tune base,peak --output_format all --define
DL-BIOS-SNC=2 --iterations 2 --define DL-BIOSinc=Dell-BIOS-Xeon-5.inc --define DL-BIOS-LogProc=1 --define
DL-BIOS-adddcD=1 --define DL-VERS=5.1 --output_format html,pdf,txt --nopower --runmode rate --tune
base:peak --size refrate intrate --nopreenv --note-preenv --logfile
$SPEC/tmp/CPU2017.001/temlogs/preenv.intrate.001.0.log --lognum 001.0 --from_runcpu 2
specperl $SPEC/bin/sysinfo
$SPEC = /mnt/ramdisk/cpu2017-1.1.9-ic2023.2.3
```

6. /proc/cpuinfo

```
model name      : INTEL(R) XEON(R) GOLD 6542Y
vendor_id       : GenuineIntel
cpu family      : 6
model           : 207
stepping        : 2
microcode       : 0x210001b0
bugs            : spectre_v1 spectre_v2 spec_store_bypass swapgs eibrs_pbrsb
cpu cores       : 24
siblings        : 48
2 physical ids (chips)
96 processors (hardware threads)
physical id 0:  core ids 0-23
physical id 1:  core ids 0-23
physical id 0:  apicids 0-47
physical id 1:  apicids 128-175
```

Caution: /proc/cpuinfo data regarding chips, cores, and threads is not necessarily reliable, especially for virtualized systems. Use the above data carefully.

7. lscpu

From lscpu from util-linux 2.37.4:

```
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Address sizes:         46 bits physical, 57 bits virtual
Byte Order:            Little Endian
CPU(s):                96
On-line CPU(s) list:   0-95
Vendor ID:             GenuineIntel
Model name:            INTEL(R) XEON(R) GOLD 6542Y
CPU family:            6
Model:                207
Thread(s) per core:    2
Core(s) per socket:    24
Socket(s):             2
Stepping:              2
BogoMIPS:              5800.00
Flags:                 fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
                        clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdtscp
                        lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology
                        nonstop_tsc cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes64 monitor
                        ds_cpl smx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid dca sse4_1 sse4_2
                        x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm
                        abm 3dnowprefetch cpuid_fault epb cat_l3 cat_l2 cdp_l3 invpcid_single
                        cdp_l2 ssbd mba ibrs ibpb stibp ibrs_enhanced fsgsbase tsc_adjust bmi1 hle
                        avx2 smep bmi2 erms invpcid rtm cqm rdt_a avx512f avx512dq rdseed adx smap
                        avx512ifma clflushopt clwb intel_pt avx512cd sha_ni avx512bw avx512vl
                        xsaveopt xsavec xgetbv1 xsaves cqm_llc cqm_occup_llc cqm_mbm_total
                        cqm_mbm_local avx_vnni avx512_bf16 wbnoinvd dtherm ida arat pln pts hfi
```

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Platform Notes (Continued)

avx512vbmi umip pku ospke waitpkg avx512_vbmi2 gfni vaes vpcmlulqdd
avx512_vnni avx512_bitalg tme avx512_vpopcntdq la57 rdpid bus_lock_detect
cldemote movdiri movdir64b enqcmd fsrm md_clear serialize tsxldtrk pconfig
arch_lbr avx512_fp16 amx_tile flush_l1d arch_capabilities

L1d cache: 2.3 MiB (48 instances)
L1i cache: 1.5 MiB (48 instances)
L2 cache: 96 MiB (48 instances)
L3 cache: 120 MiB (2 instances)
NUMA node(s): 4
NUMA node0 CPU(s): 0, 6, 8, 12, 16, 20, 24, 26, 28, 32, 36, 44, 48, 54, 56, 60, 64, 68, 72, 74, 76, 80, 84, 92
NUMA node1 CPU(s): 2, 4, 10, 14, 18, 22, 30, 34, 38, 40, 42, 46, 50, 52, 58, 62, 66, 70, 78, 82, 86, 88, 90, 94
NUMA node2 CPU(s): 1, 9, 13, 19, 21, 25, 29, 33, 35, 39, 43, 45, 49, 57, 61, 67, 69, 73, 77, 81, 83, 87, 91, 93
NUMA node3 CPU(s): 3, 5, 7, 11, 15, 17, 23, 27, 31, 37, 41, 47, 51, 53, 55, 59, 63, 65, 71, 75, 79, 85, 89, 95
Vulnerability Itlb multihit: Not affected
Vulnerability L1tf: Not affected
Vulnerability Mds: Not affected
Vulnerability Meltdown: Not affected
Vulnerability Mmio stale data: Not affected
Vulnerability Retbleed: Not affected
Vulnerability Spec store bypass: Mitigation; Speculative Store Bypass disabled via prctl and seccomp
Vulnerability Spectre v1: Mitigation; usercopy/swapgs barriers and __user pointer sanitization
Vulnerability Spectre v2: Mitigation; Enhanced IBRS, IBPB conditional, RSB filling, PBRSE-eIBRS SW sequence
Vulnerability Srbds: Not affected
Vulnerability Tsx async abort: Not affected

From lscpu --cache:

NAME	ONE-SIZE	ALL-SIZE	WAYS	TYPE	LEVEL	SETS	PHY-LINE	COHERENCY-SIZE
L1d	48K	2.3M	12	Data	1	64	1	64
L1i	32K	1.5M	8	Instruction	1	64	1	64
L2	2M	96M	16	Unified	2	2048	1	64
L3	60M	120M	15	Unified	3	65536	1	64

8. numactl --hardware

NOTE: a numactl 'node' might or might not correspond to a physical chip.

available: 4 nodes (0-3)
node 0 cpus: 0, 6, 8, 12, 16, 20, 24, 26, 28, 32, 36, 44, 48, 54, 56, 60, 64, 68, 72, 74, 76, 80, 84, 92
node 0 size: 128398 MB
node 0 free: 119577 MB
node 1 cpus: 2, 4, 10, 14, 18, 22, 30, 34, 38, 40, 42, 46, 50, 52, 58, 62, 66, 70, 78, 82, 86, 88, 90, 94
node 1 size: 129017 MB
node 1 free: 128647 MB
node 2 cpus: 1, 9, 13, 19, 21, 25, 29, 33, 35, 39, 43, 45, 49, 57, 61, 67, 69, 73, 77, 81, 83, 87, 91, 93
node 2 size: 129017 MB
node 2 free: 128560 MB
node 3 cpus: 3, 5, 7, 11, 15, 17, 23, 27, 31, 37, 41, 47, 51, 53, 55, 59, 63, 65, 71, 75, 79, 85, 89, 95
node 3 size: 128576 MB
node 3 free: 128197 MB
node distances:
node 0 1 2 3
0: 10 12 21 21
1: 12 10 21 21
2: 21 21 10 12
3: 21 21 12 10

9. /proc/meminfo

MemTotal: 527370992 kB

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Platform Notes (Continued)

10. who -r
run-level 3 Mar 29 07:13

11. Systemd service manager version: systemd 249 (249.16+suse.171.gdad0071f15)
Default Target Status
multi-user running

12. Services, from systemctl list-unit-files

STATE	UNIT FILES
enabled	apparmor auditd cron firewalld getty@ irqbalance issue-generator kbdsettings kdump kdump-early nvme-fc-boot-connections postfix purge-kernels rollback sshd systemd-pstore wicked wickedd-auto4 wickedd-dhcp4 wickedd-dhcp6 wickedd-nanny
enabled-runtime	systemd-remount-fs
disabled	boot-sysctl ca-certificates chrony-wait chronyd console-getty debug-shell ebtables grub2-once haveged haveged-switch-root issue-add-ssh-keys kexec-load lunmask nfs nfs-blkmap nvme-fc-autoconnect rpcbind rpmconfigcheck rsyncd serial-getty@ systemd-boot-check-no-failures systemd-network-generator systemd-sysext systemd-time-wait-sync systemd-timesyncd
indirect	wickedd

13. Linux kernel boot-time arguments, from /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-5.14.21-150500.53-default
root=UUID=b8c6d51c-250a-4d03-852b-82b1db828fe3
splash=silent
mitigations=auto
quiet
security=apparmor
crashkernel=386M,high
crashkernel=72M,low

14. sysctl

kernel.numa_balancing	1
kernel.randomize_va_space	2
vm.compaction_proactiveness	20
vm.dirty_background_bytes	0
vm.dirty_background_ratio	10
vm.dirty_bytes	0
vm.dirty_expire_centisecs	3000
vm.dirty_ratio	20
vm.dirty_writeback_centisecs	500
vm.dirtytime_expire_seconds	43200
vm.extfrag_threshold	500
vm.min_unmapped_ratio	1
vm.nr_hugepages	0
vm.nr_hugepages_mempolicy	0
vm.nr_overcommit_hugepages	0
vm.swappiness	60
vm.watermark_boost_factor	15000
vm.watermark_scale_factor	10
vm.zone_reclaim_mode	0

15. /sys/kernel/mm/transparent_hugepage
defrag always defer defer+madvice [madvice] never
enabled [always] madvice never

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Platform Notes (Continued)

hpage_pmd_size 2097152
shmem_enabled always within_size advise [never] deny force

16. /sys/kernel/mm/transparent_hugepage/khugepaged
alloc_sleep_millisecs 60000
defrag 1
max_ptes_none 511
max_ptes_shared 256
max_ptes_swap 64
pages_to_scan 4096
scan_sleep_millisecs 10000

17. OS release
From /etc/*-release /etc/*-version
os-release SUSE Linux Enterprise Server 15 SP5

18. Disk information
SPEC is set to: /mnt/ramdisk/cpu2017-1.1.9-ic2023.2.3
Filesystem Type Size Used Avail Use% Mounted on
tmpfs tmpfs 70G 4.1G 66G 6% /mnt/ramdisk

19. /sys/devices/virtual/dmi/id
Vendor: Dell Inc.
Product: PowerEdge R760
Product Family: PowerEdge
Serial: SLR7601

20. dmidecode
Additional information from dmidecode 3.4 follows. WARNING: Use caution when you interpret this section.
The 'dmidecode' program reads system data which is "intended to allow hardware to be accurately
determined", but the intent may not be met, as there are frequent changes to hardware, firmware, and the
"DMTF SMBIOS" standard.
Memory:
16x 00AD063200AD HMC88AGBRA188N 32 GB 2 rank 5600, configured at 5200

21. BIOS
(This section combines info from /sys/devices and dmidecode.)
BIOS Vendor: Dell Inc.
BIOS Version: 1.9.12
BIOS Date: 11/10/2023
BIOS Revision: 1.9

Compiler Version Notes

=====

C	502.gcc_r(peak)

Intel(R) oneAPI DPC++/C++ Compiler for applications running on IA-32, Version 2023.2.3 Build x
Copyright (C) 1985-2023 Intel Corporation. All rights reserved.

=====

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Compiler Version Notes (Continued)

C | 500.perlbench_r(base, peak) 502.gcc_r(base) 505.mcf_r(base, peak) 525.x264_r(base, peak)
| 557.xz_r(base, peak)

Intel(R) oneAPI DPC++/C++ Compiler for applications running on Intel(R) 64, Version 2023.2.3 Build x
Copyright (C) 1985-2023 Intel Corporation. All rights reserved.

C | 502.gcc_r(peak)

Intel(R) oneAPI DPC++/C++ Compiler for applications running on IA-32, Version 2023.2.3 Build x
Copyright (C) 1985-2023 Intel Corporation. All rights reserved.

C | 500.perlbench_r(base, peak) 502.gcc_r(base) 505.mcf_r(base, peak) 525.x264_r(base, peak)
| 557.xz_r(base, peak)

Intel(R) oneAPI DPC++/C++ Compiler for applications running on Intel(R) 64, Version 2023.2.3 Build x
Copyright (C) 1985-2023 Intel Corporation. All rights reserved.

C++ | 520.omnetpp_r(base, peak) 523.xalancbmk_r(base, peak) 531.deepsjeng_r(base, peak)
| 541.leela_r(base, peak)

Intel(R) oneAPI DPC++/C++ Compiler for applications running on Intel(R) 64, Version 2023.2.3 Build x
Copyright (C) 1985-2023 Intel Corporation. All rights reserved.

Fortran | 548.exchange2_r(base, peak)

Intel(R) Fortran Compiler for applications running on Intel(R) 64, Version 2023.2.3 Build x
Copyright (C) 1985-2023 Intel Corporation. All rights reserved.

Base Compiler Invocation

C benchmarks:

icx

C++ benchmarks:

icpx

Fortran benchmarks:

ifx



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Base Portability Flags

500.perlbench_r: -DSPEC_LP64 -DSPEC_LINUX_X64
502.gcc_r: -DSPEC_LP64
505.mcf_r: -DSPEC_LP64
520.omnetpp_r: -DSPEC_LP64
523.xalancbmk_r: -DSPEC_LP64 -DSPEC_LINUX
525.x264_r: -DSPEC_LP64
531.deepsjeng_r: -DSPEC_LP64
541.leela_r: -DSPEC_LP64
548.exchange2_r: -DSPEC_LP64
557.xz_r: -DSPEC_LP64

Base Optimization Flags

C benchmarks:

-w -std=c11 -m64 -Wl,-z,muldefs -xsapphirerapids -O3 -ffast-math
-flto -mfpmath=sse -funroll-loops -qopt-mem-layout-trans=4
-L/home/specdev/new_compilers/ic2023.2.3/compiler/lib/intel64_lin
-lqkmallo

C++ benchmarks:

-w -std=c++14 -m64 -Wl,-z,muldefs -xsapphirerapids -O3 -ffast-math
-flto -mfpmath=sse -funroll-loops -qopt-mem-layout-trans=4
-L/home/specdev/new_compilers/ic2023.2.3/compiler/lib/intel64_lin
-lqkmallo

Fortran benchmarks:

-w -m64 -Wl,-z,muldefs -xsapphirerapids -O3 -ffast-math -flto
-mfpmath=sse -funroll-loops -qopt-mem-layout-trans=4
-nostandard-realloc-lhs -align array32byte -auto
-L/home/specdev/new_compilers/ic2023.2.3/compiler/lib/intel64_lin
-lqkmallo

Peak Compiler Invocation

C benchmarks:

icx

C++ benchmarks:

icpx

Fortran benchmarks:

ifx



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Peak Portability Flags

500.perlbench_r: -DSPEC_LP64 -DSPEC_LINUX_X64
502.gcc_r: -D_FILE_OFFSET_BITS=64
505.mcf_r: -DSPEC_LP64
520.omnetpp_r: -DSPEC_LP64
523.xalancbmk_r: -DSPEC_LP64 -DSPEC_LINUX
525.x264_r: -DSPEC_LP64
531.deepsjeng_r: -DSPEC_LP64
541.leela_r: -DSPEC_LP64
548.exchange2_r: -DSPEC_LP64
557.xz_r: -DSPEC_LP64

Peak Optimization Flags

C benchmarks:

500.perlbench_r: -w -std=c11 -m64 -Wl, -z,muldefs
-fprofile-generate(pass 1)
-fprofile-use=default.profddata(pass 2) -xCORE-AVX2(pass 1)
-flto -Ofast -xCORE-AVX512 -ffast-math -mfpmath=sse
-funroll-loops -qopt-mem-layout-trans=4
-fno-strict-overflow
-L/home/specdev/new_compilers/ic2023.2.3/compiler/lib/intel64_lin
-lqkmallo

502.gcc_r: -m32
-L/home/specdev/new_compilers/ic2023.2.3/compiler/lib/ia32_lin
-std=gnu89 -Wl, -z,muldefs -fprofile-generate(pass 1)
-fprofile-use=default.profddata(pass 2) -xCORE-AVX2(pass 1)
-flto -Ofast -xCORE-AVX512 -ffast-math -mfpmath=sse
-funroll-loops -qopt-mem-layout-trans=4
-L/usr/local/jemalloc32-5.0.1/lib -ljemalloc

505.mcf_r: basepeak = yes

525.x264_r: -w -std=c11 -m64 -Wl, -z,muldefs -xsapphirerapids -Ofast
-ffast-math -flto -mfpmath=sse -funroll-loops
-qopt-mem-layout-trans=4 -fno-alias
-L/home/specdev/new_compilers/ic2023.2.3/compiler/lib/intel64_lin
-lqkmallo

557.xz_r: basepeak = yes

C++ benchmarks:

(Continued on next page)



SPEC CPU®2017 Integer Rate Result

Copyright 2017-2024 Standard Performance Evaluation Corporation

Dell Inc.

SPECrate®2017_int_base = 511

PowerEdge R760 (Intel Xeon Gold 6542Y)

SPECrate®2017_int_peak = 527

CPU2017 License: 6573

Test Sponsor: Dell Inc.

Tested by: Dell Inc.

Test Date: Mar-2024

Hardware Availability: Feb-2024

Software Availability: Dec-2023

Peak Optimization Flags (Continued)

520.omnetpp_r: basepeak = yes

523.xalancbmk_r: basepeak = yes

531.deepsjeng_r: basepeak = yes

541.leela_r: basepeak = yes

Fortran benchmarks:

548.exchange2_r: basepeak = yes

The flags files that were used to format this result can be browsed at

<http://www.spec.org/cpu2017/flags/Intel-ic2023p2-official-linux64.html>

<http://www.spec.org/cpu2017/flags/Dell-Platform-Flags-PowerEdge-Intel-Xeon-v1.6.html>

You can also download the XML flags sources by saving the following links:

<http://www.spec.org/cpu2017/flags/Intel-ic2023p2-official-linux64.xml>

<http://www.spec.org/cpu2017/flags/Dell-Platform-Flags-PowerEdge-Intel-Xeon-v1.6.xml>

SPEC CPU and SPECrate are registered trademarks of the Standard Performance Evaluation Corporation. All other brand and product names appearing in this result are trademarks or registered trademarks of their respective holders.

For questions about this result, please contact the tester. For other inquiries, please contact info@spec.org.

Tested with SPEC CPU®2017 v1.1.9 on 2024-03-29 07:16:48-0400.

Report generated on 2024-05-07 22:15:45 by CPU2017 PDF formatter v6716.

Originally published on 2024-05-07.

Cyber Resilient Security in Dell PowerEdge Servers

October 2023

H19738.1

White Paper

Abstract

This white paper highlights the Dell PowerEdge Cyber Resilient Architecture and describes the server life cycle for implementing zero - trust principles for your infrastructure. Dell PowerEdge security controls provide a comprehensive security solution that ensures resiliency while enforcing a zero-trust posture.

Copyright

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2023 Dell Inc. or its subsidiaries. Published in the USA October 2023 H19738.1.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Contents

Executive summary.....	5
Overview	5
Revisions.....	5
We value your feedback	5
Introduction	6
Digital infrastructure complexity	6
Sophistication and complexity of threats	6
Regulatory landscape and internal mandates	6
Zero Trust strategy for the modern world	6
Core principles of Zero Trust	7
Seven pillars of Zero Trust.....	8
The Dell advantage	9
Security journey across the server life cycle	10
First stage – Choosing the server.....	10
Challenges	10
PowerEdge solutions.....	10
Dell Secure Development Lifecycle	11
Compliance advantage.....	11
Rapid response to new vulnerabilities	12
Bug Bounty Program.....	12
Solutions covering threat vectors for every layer of the server.....	13
Second stage – Supply chain security	14
Challenges	14
PowerEdge solutions.....	14
End-to-end supply chain assurance	14
Secured Component Verification.....	16
Software Bill of Materials.....	16
Third stage – Efficient deployment and configuration at-scale	17
Challenges	17
PowerEdge solution.....	17
System integrity.....	17
Hardware security	20
Protecting data at rest	21
Protecting Data in Flight.....	23
Protecting data in use	26
Identity Access Management	28
Capabilities and automation for efficient at-scale deployment	30

- Fourth Stage – Security management and monitoring.....31**
 - Challenges 31
 - PowerEdge Solutions 31
 - Visibility, logging, and alerts 31
 - SELinux framework 33
 - Real-time detection – BIOS Live scan 33
 - Silicon-based Root of Trust 34
 - Automated and manual recovery.....36
 - Updating 38
 - Restoring server configuration after hardware servicing 38
 - CloudIQ.....39
 - Managed detection and response services 39
- Fifth stage – Secure decommissioning and repurposing 40**
 - Challenge 40
 - PowerEdge solutions.....40
 - Secure Erase 41
 - Secure erase – physical disk.....41
 - Data sanitization and destruction services.....42
- Summary.....42**
- References.....44**
 - Dell Technologies documentation 44

Executive summary

Overview

The Dell Technologies approach to security is intrinsic in nature – it is built-in, not bolted-on later, and it is integrated into every step of Dell's Secure Development Lifecycle. We continuously strive to evolve our Dell PowerEdge security controls, features, and solutions to meet the ever-changing threat landscape and to help customers accelerate Zero Trust adoption.

Securing your infrastructure is not a one-time investment, but a mindset and overall approach. This white paper uses this journey perspective to describe the PowerEdge advantages across the server life cycle. In each of the life cycle phases, from deployment through maintenance to decommissioning, we highlight how Dell's PowerEdge Cyber Resilient Architecture security features work together to provide both resiliency and a zero-trust approach. The Dell Remote Access Controller (iDRAC9) enables many of these features.

We continue to anchor security with a Silicon-based Root-of-Trust (RoT). Since the previous PowerEdge cyber resilient security whitepaper, many new features have been added that span from access control to data encryption to supply chain assurance. All features make extensive use of intelligence and automation to help you stay ahead of the threat curve, and to enable the scaling demanded by ever-expanding use models. Dell's Cyber Resilient Architecture, enhanced over many years, is the foundation for the critical elements of a Zero Trust environment.

Revisions

Date	Part number/ revision	Description
November 2022	H19738	Initial release
October 2023	H19738.1	Updated to include the 16 th generation of PowerEdge servers

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by [email](#).

Authors: Deepak Rangaraj, Kim Kinahan

Contributors: Marshal Savage

Note: For links to other documentation for this topic, the [Dell Technologies Info Hub for PowerEdge](#).

Introduction

Digital infrastructure complexity

Modern IT environments have changed drastically in the past few years with servers being deployed in various use cases such as on-premises, multicloud, Edge, Telco, and so on. The server platforms are becoming more complex with an ever-increasing number of components that require firmware for configuration and management. We are generating data at a speed and volume higher than ever and this data is often generated and stored at numerous locations distributed geographically. This increasing complexity necessitates effective management of security controls to mitigate the expansion of the attack surface.

Sophistication and complexity of threats

The Dell Technologies Digital Transformation Index found that data privacy and cybersecurity concerns are the leading barriers to digital transformation¹. The complexity, sophistication, and frequency of cyberattacks are increasing, and the damage caused by attacks is becoming more costly. Complicating matters further, today's threat actors are taking advantage of technological advancements, such as AI and a lower cost of entry. Malicious actors are continuously searching for vulnerabilities to exploit. With the assistance of advanced AI systems, they can carry out nefarious activities at an unprecedented scale and manipulate systems in innovative and harmful ways beyond human capabilities. Global damages related to cybercrime are predicted to reach \$10.5 trillion by 2025.²

Regulatory landscape and internal mandates

As global threats increase, governments worldwide are developing regulatory guidance in response to cyber threats. As a result, private institutions are creating stronger policies and mandates to mitigate advanced persistent threats. Also, there are more mandates for security requirements that are needed to work with the government. These requirements impact suppliers, vendors, and any organization that partners with the government. In addition, regulations are carrying over to the critical infrastructure sectors, such as healthcare, transport, and finance. Outside of government regulations, many customers want to harden their infrastructure and are developing their own internal mandates or security policies.

Zero Trust strategy for the modern world

The increasing infrastructure complexity and threat landscape are driving a critical need to secure not only infrastructure hardware, but also the firmware and the supply chain itself. When applying a Zero Trust strategy, customers focus on business controls, the control plane, and applications and data. However, there is a critical need to secure what is below these items, including infrastructure hardware and firmware, supply chain for the infrastructure, and design and processes used to build the infrastructure. Zero Trust principles must be applied to all these aspects for more comprehensive cyber resilience.

Dell Technologies has security built into our industry-leading servers, storage, HCI, and data protection appliances to help protect data wherever it is stored, managed, or used. As a foundation for securing our PowerEdge server products, they are foremost cyber resilient – capable of anticipating, withstanding, and recovering from cyber threats.

¹ Dell Technologies 2020 Digital Transformation Index

² www.cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Simultaneously, the process of designing PowerEdge security controls and tools incorporates Zero Trust principles. By anticipating how customers want to use these capabilities while they are setting up their Zero Trust deployments, we have adapted our approach. We made it easier to work with us no matter where customers are on their journey towards Zero Trust adoption.

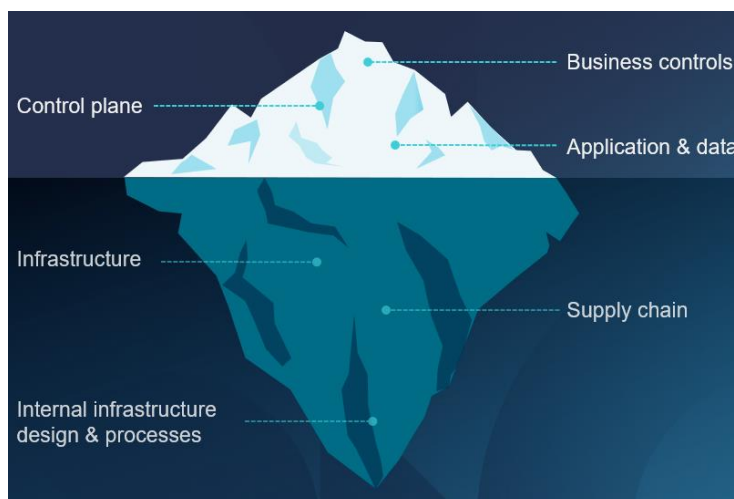


Figure 1. Infrastructure security and Zero Trust

The Dell infrastructure security approach is integral to Dell products and accelerates Zero Trust adoption because it is:

- Designed and built using Zero Trust principles
- Provides Zero Trust capabilities and features
- Provides common, consistent behavior

Core principles of Zero Trust

The tenets of Zero Trust architecture are built on a set of principles that presume that the *network is always vulnerable to compromise* and sets out to safeguard access to critical data and resources. Unlike trust-then-verify frameworks, a zero-trust approach eliminates implicit trust. Every user, device, and application must be continuously *authenticated and explicitly authorized* based on a range of factors such as identity, device status, location, and behavior.

Identity plays a crucial role in Zero Trust. Identification pertains not only to people but to applications, communication paths, network devices, and the data itself. When an IT asset is identified, authenticated, and explicitly authorized, the principle of *least privilege* is applied. This approach ensures that only authorized entities are given a minimum level of access required to perform their specific task. The data-centric security model constantly limits access while also looking for anomalous or malicious activity. The Zero Trust approach reduces the granularity of validation at key intersections for verified trust, optimizing least privilege without impacting workload efficiency. The goal is to deter attacks and reject them at point of entry. However, if a breach occurs, the amount of damage is minimized, along with an enhanced ability to detect and remediate immediately.

Adopting the Zero Trust mindset and using Zero Trust principles enables systems administrators to control how users, processes, and devices engage with data. These

principles can prevent the abuse of compromised user credentials, remote exploitation, insider threats, and even mitigate the effects of malicious supply chain activity.

Seven pillars of Zero Trust

The Zero Trust model, defined by the National Institute of Standards and Technology (NIST)³, identifies seven interrelated pillars that work together to provide a comprehensive and holistic approach to infrastructure and data security. Each pillar represents a specific functional or key focus area for implementation of Zero Trust security controls. When combined, these seven pillars provide a multifaceted, layered, and integrated security framework.

Dell's Zero Trust approach integrates a broad set of security controls and automation capabilities for the management of the infrastructure and the applications running on it. The following table highlights Dell's capabilities across the seven pillars as outlined by NIST:

Table 1. Dell Zero Trust approach across the seven pillars

Zero Trust pillar	NIST description ³	PowerEdge highlights
User	User identification, authentication, and access control: - Only validated and authorized users can access data and resources. - The principle of <i>least privilege</i> is applied where users are granted the minimum level of access required to perform their specific tasks.	- Identity and Access Management - Multi-Factor Authentication—RSA Secure ID - Active Directory or LDAP integration with single sign-on (SSO) support - Role-based access control and auditing
Device	Monitoring and enforcement of device health, compliance, and device posture assessment: - Monitoring - looking for anomalies and suspicious read/write activity. - Health – confirming the latest version of the firmware. - All devices are identified, inventoried, authorized, authenticated, and updated.	- Silicon Root-of-Trust (ROT) with complementary Intel Boot Guard and AMD Platform Secure Boot (AMD PSB) - Secure supply chain with Secured Component Verification (SCV) - Chassis locks and intrusion detection - Dynamic USB port enable/disable - Trusted Platform Module (TPM) - Device attestation with SPDM (Security Protocol Data Model from DMTF)
Data	Ensure data transparency and visibility by using enterprise infrastructure, applications, standards, solid end-to-end encryption, and data tagging.	Data-at-rest protection: - Drive encryption with local (LKM) or Secure Enterprise Key Management (SEKM) with direct-attached NVMe drive support - Baseboard Management Controller (BMC)-based Local Key Management (iLKM) Data-in-use protection:

³ National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Zero Trust Architecture

Zero Trust pillar	NIST description ³	PowerEdge highlights
		Confidential compute—Intel SGX, Intel MKTME, AMD Secure Memory Encryption (SME) AMD SME, AMD Secure Encrypted Virtualization (SEV) SEV, AMD persistent memory encryption
Application and Workload	Secure applications and workloads, and protect containers and VMs.	- Secure Development Lifecycle - Cryptographically signed BIOS and firmware updates - Secure end-to-end boot and Unified Extensible Firmware Interface (UEFI) boot capabilities - Drift detection - Rapid Response and mitigations for CVEs
Network and Environment	Encrypt, monitor, and analyze network. Logically and physically segment, isolate, and control the network and the environment (on-premises and off-premises) using granular access and policy restrictions.	- Dedicated BMC (iDRAC) network module - SSH/TLS communication options - TLS 1.3 support - DPU/SmartNIC
Visibility and Analytics	Monitor activities and behaviors across the infrastructure (user, device, data, network, and application) to identify patterns and anomalies. Use analytics to detect and respond to security threats.	- Persistent event logging and auditing - Real-time and boot time firmware scanning - Security alerts - CloudIQ
Automation and Orchestration	Automate manual security and other applicable processes to take policy-based actions across the enterprise with speed and at scale.	- OpenManage Enterprise drift detection - Firmware rollback - Automatic BIOS and operating system recovery - Centralized updates - Automatic SSL certificate renewal

The Dell advantage

Security is in our DNA, and we are committed to making our products secure by design and secure by default. PowerEdge servers are built using Zero Trust principles internally and have capabilities that enable customers to set up a Zero Trust IT environment and operations. Our products also strive to provide common and consistent behavior and controls across our portfolio.

PowerEdge servers with iDRAC9 have an integrated immutable silicon-based platform Root-of-Trust (RoT) that is used to establish a verified chain of trust that extends throughout the server life cycle, from deployment through maintenance to decommissioning. This RoT combined with security controls and comprehensive management tools provides robust layers of security across the PowerEdge hardware and firmware.

First stage – Choosing the server

These PowerEdge capabilities not only ensure cyber resiliency to protect, detect, and recover from attacks, they also maintain a locked-down posture for a Zero Trust approach of least privilege. Least privilege ensures that users and devices are only given access to what they need to perform their tasks. Our goal is to make Zero Trust a reality for our customers and accelerate its speed of adoption.

Security journey across the server life cycle

Implementing security across your infrastructure requires a series of ongoing efforts and measures to protect underlying systems, networks, and resources. Transitioning to a mature security model is not a one-time investment and cannot be accomplished overnight. It is an ongoing journey and approach of implementing stringent security policies. As your Zero Trust implementation matures over time, enhanced visibility and extensive controls allow you to keep pace with the threat landscape. We have organized this journey into five stages.

- **Stage 1: Choosing the server**—Customers want assurance that security is a top priority and is built into every aspect of design.
- **Stage 2: Ensuring supply chain security**—Customers face the real risk of malicious offenders replacing original components with counterfeits, implants, or malware.
- **Stage 3: Efficient deployment and configuration at scale**—How a server is deployed has a direct impact on its performance, stability, and security. Proper planning and configuration are essential to ensure that the server is set up correctly and that all necessary components are in place.
- **Stage 4: Security management and monitoring**— Because attacks happen quickly, faster than a human can detect, customers must proactively monitor their environment to take quick action. The lack of skills and training can also exacerbate the problem.
- **Stage 5: Secure repurposing and decommissioning**—Data security is a key consideration when the server is repurposed or retired. IT best-practices recommend removing all data from the server to ensure that confidential information is not inadvertently shared or compromised.

First stage – Choosing the server

Challenges

Customers want to be confident that their server is secure in its entirety and does not introduce any vulnerabilities into their environment. They want assurances from server vendors addressing every aspect of design, the entire supply chain, including hardware, software, and firmware. This level of assurance differentiates on-premises infrastructure when compared to cloud service providers who might only offer a black box infrastructure, leaving customers uncertain about the security of the underlying components of their cloud-based system.

PowerEdge solutions

The first step of the Zero Trust journey with Dell Technologies starts before you receive your PowerEdge server. Intrinsic security practices are incorporated into hardware product design and software or firmware code development. These practices include processes and policies that ensure security features are implemented at the time of product inception and continue throughout the development cycle. In essence, security is

'built' in. To perform this practice effectively, our engineers are required to take mandatory security training before handling the code. Security champions are assigned to each development team to drive a security culture in the organization.

Dell Secure Development Lifecycle

Delivering the Cyber Resilient Architecture requires security awareness and discipline at each stage of development. The Secure Development Lifecycle (SDL) model is used to make security an integral part of the overall server design process. Some key aspects of this process include:

- Features that are conceived, designed, prototyped, implemented, set into production, deployed, and maintained with security as a key priority
- Server firmware that is designed to obstruct, oppose, and counter the injection of malicious code during all phases of the product development life cycle:
 - Threat modeling and penetration testing provide coverage during the design process.
 - Secure coding practices are applied at each stage of firmware development.
- For critical technologies, external audits that supplement the internal SDL process to ensure that firmware adheres to known security best practices
- On-going testing and evaluation of new potential vulnerabilities using the latest security assessment tools
- Rapid response to critical Common Vulnerabilities and Exposures (CVEs) including recommended remediation measures if warranted



Figure 2. Dell Secure Development Lifecycle

Compliance advantage

Dell Technologies has received the certifications that are needed to comply with major United States Federal and other global governmental requirements as well as industry standards such as from NIST, as described in the following table:

Table 2. Certification descriptions

Certification	Description
Common Criteria	Certain configurations of PowerEdge Servers include components with common criteria certifications. (For example, iDRAC and TPM)
FIPS 140	Certain configurations of PowerEdge Servers include FIPS 140-certified cryptographic modules (For example, TPM, iDRAC9, Chassis Management Controller (CMC), Self-Encrypting Drives (SEDs), and SSDs)
IPv6	• PowerEdge Servers are fully USGv6r1 and IPv6 Ready Logo-compliant and certified with IPv6-only capabilities while running operating systems such as Red Hat Enterprise Linux 8.4 and the applicable versions of Windows 2019 or Windows 2022 Server. • Dell PowerEdge iDRAC9 (with 5.1x firmware) is USGv6r1 and IPv6 Ready Logo-compliant and certified with IPv6-only capabilities.

Rapid response to new vulnerabilities

CVEs are newly discovered attack vectors that compromise software and hardware products. Timely responses to CVEs are critical to most companies so they can swiftly assess their exposure and take appropriate action.

Dell Technologies works aggressively to respond quickly to new CVEs in our PowerEdge servers and provide timely information including the following:

- The products that are affected
- Remediation steps
- If needed, availability of updates to address the CVEs

Bug Bounty Program

Dell Technologies recognizes the value of the security research community to broaden visibility into potential vulnerabilities and threats and welcomes the opportunity to collaborate with community members who share this common goal.

Dell's Bug Bounty Program applies to security vulnerabilities identified in Dell-branded or currently supported products.

Solutions covering threat vectors for every layer of the server

There are many threat vectors in today's changing landscape. The following tables summarize the Dell approach to managing critical threats in each of the server layers.

Table 3. Dell solution for common server platform layer threat vectors

Server platform layers		
Security layer	Threat vector	Dell solution
Physical server	Server/component tampering or theft of component	- Secured Component Verification (SCV) - Chassis Intrusion Detection - Secure Enterprise Key Management - Intel TME - SPDM
Firmware and software	- Firmware corruption - Malware injection	- Silicon-based Root-of-Trust - Intel Boot Guard - AMD Secure Root-of-Trust - UEFI Secure Boot Customization - Cryptographically signed and validated firmware
	Software	- CVE reporting - Patching as required
Attestation trust features	Server identity spoofing	- TPM - Intel TXT - Chain of trust 802.1x features - SPDM
Server management	- Rogue configuration and updates - Unauthorized open-port attacks	iDRAC9 Remote attestation

Table 4. Dell solution for common server environment layer threat vectors

Server environment layers		
Security layer	Threat vector	Dell Technologies solution
Data	Data breach	• Self-Encrypting Drives (SED) – FIPS or Opal/TCG • Secure Enterprise Key Management ISE-only (Instant Secure Erase) drives • Secure User Authentication
Supply Chain Integrity	• Counterfeit components • Malware threats	• ISO9001 certification for all global server manufacturing sites • Secured Component Verification • Proof of possession • Software Bill of Materials (SBOM) • Security measures implemented as part of the Secure Development Lifecycle
Supply Chain Security	• Physical security in manufacturing sites • Theft and tempering during transport	• Transported Asset Protection Association (TAPA) facility security requirements • Customs-Trade Partnership Against Terrorism (C-TPAT) • Secured Component Verification

Second stage – Supply chain security

Challenges

Modern server platforms are becoming more complex with hundreds of components that require firmware for configuration and management. As a result, the server supply chain is also becoming increasingly complex with hundreds of third-party vendors supplying components as well as the use of open-source software. This complex supply chain contributes to an increase in the attack surface available for threat actors if not managed properly. Customers face the risk of vulnerabilities and threats being introduced into their environments if the supply chain integrity is not assured. The two main aspects of supply chain integrity include:

- **Maintaining hardware integrity**—Ensuring that there is no product tampering or the insertion of counterfeit components or malicious implants before the product is shipped to customers.
- **Maintaining software integrity**—Ensuring that no malware is inserted in firmware or device drivers before shipping the product to customers and preventing code with known vulnerabilities from being introduced into the environment.

PowerEdge solutions

End-to-end supply chain assurance

Dell Technologies employs a multifaceted approach to protect its supply chain and delivers solutions that customers can trust in an increased threat environment. Our supply chain security consists of prevention and detection controls that protect physical assets, inventory, information, intellectual property, and people. These security measures provide

supply chain assurance and ensure integrity by reducing opportunities for the malicious or negligent introduction of malware and counterfeit components into the supply chain.

Dell supply chain controls span supplier selection, sourcing, production processes, and governance through auditing and testing. When a supplier has been selected, the new product introduction process verifies that all materials used during all build stages are sourced from the approved vendor list and match the bill of materials as appropriate. Material inspections during production help identify components that are mismarked, deviate from normal performance parameters, or contain an incorrect electronic identifier.

Parts are procured directly from the Original Design Manufacturer (ODM) or Original Component Manufacturer (OCM) when possible. The material inspection that occurs during the new product introduction process provides multiple opportunities to identify counterfeit or corrupted components that might have entered the supply chain.

Additionally, Dell Technologies maintains ISO 9001 certification for all global manufacturing sites. Strict adherence to these processes and controls helps minimize the risk of counterfeit components being embedded among the Dell products or malware being inserted into firmware or device drivers. As part of SDL, Dell Technologies has several long-standing, key practices that establish and maintain security in manufacturing facilities and logistical networks.

Facilities used to design, build, customize, or fulfill Dell products must demonstrate compliance with several internationally recognized physical security standards such as those defined by the Transported Asset Protection Association (TAPA), American Society for Industrial Security (ASIS), International Standards Organization (ISO), and the Business Alliance for Secure Commerce (BASC).

Protective measures have also been put in place to guard products against theft and tampering during transport as part of an industry-leading logistics program. This program provides a continuously staffed command center to monitor select inbound and outbound shipments across the globe to ensure that shipments make it from one destination to another without disruption.

Dell Technologies audits suppliers and facilities, addressing various factors, including the use of digital closed-circuit TV cameras, access control systems, intrusion detection, and guard service protocols. Other controls are applied to protect Dell cargo during the shipping and logistics process, including tamper-evident packaging, cargo locks and seals, and threat intelligence monitoring of key freight lanes. Internet of Things (IoT) tracking devices are also deployed on select shipments to enable real-time telemetry data monitoring to escalate any security noncompliance events observed during transit.

Dell Technologies also maintains certifications in multiple secure trade and commerce programs such as Tier 3 status with the United States Customs and Border Protection's Customs Trade Partnership Against Terrorism (C-TPAT), Canada's Partners in Protection (PIP), Singapore's Secure Trade Partnership, and Authorized Economic Operator (AEO) status in several other nations. These programs are internationally recognized by member states of the World Customs Organization and demonstrate "best in class" supply chain security standards in the private sector. These programs focus on supplier accountability, security management policies, counter smuggling, trafficking controls, and tamper prevention – all intended to secure trade across international borders.

Supply chain integrity ensures that customers' products are safely delivered and when received, operate as intended. An important feature of supply chain integrity is the development of hardware and software baseline specifications that are preserved securely and later used as a reference to verify that no unauthorized modifications have been made.

Secured Component Verification

Dell Technologies' Secured Component Verification (SCV) for PowerEdge is a supply chain assurance offering that verifies that the server received by a customer matches the configuration that was shipped from the factory. The factory generates a certificate that contains unique component IDs for a specific server. This certificate is stored in a cryptographically secure vault in iDRAC. On receiving the server, the customer runs the SCV application on the host to generate an inventory of the current system, including unique component IDs, and then validates it against the golden factory inventory in the SCV certificate stored in iDRAC.

The SCV application generates a report that identifies any component mismatches from what was installed in the factory. It also verifies the certificate and Chain of Trust along with the Proof of Possession of the SCV Private key for iDRAC. The current implementation supports direct ship customers and does not include Value Added Reseller (VAR) or Part Replacement scenarios.

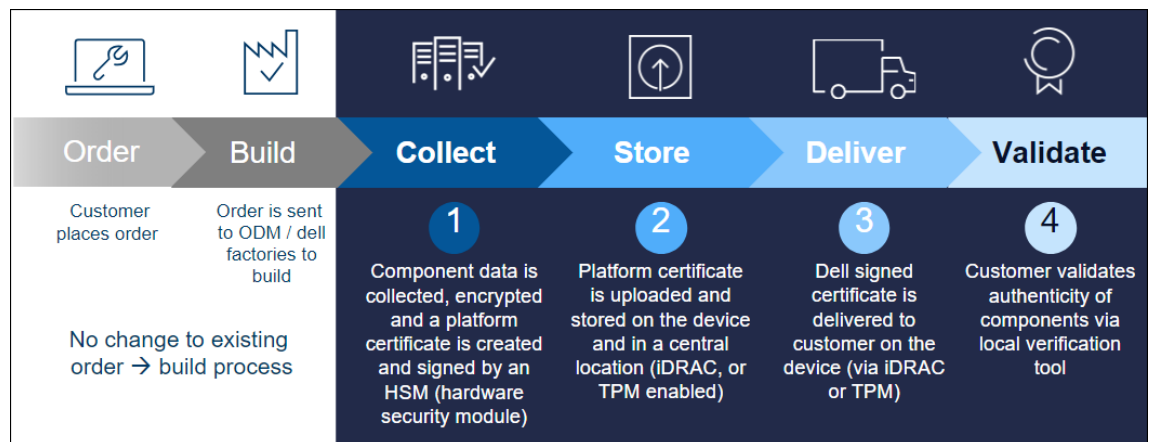


Figure 3. Dell Secured Component Verification

Software Bill of Materials

As part of Dell's software supply chain security controls, NIST standards, and in alignment with the President's Executive Order (EO) 14028, a Software Bill of Materials (SBOM) is available for a limited number of products across our portfolio. Dell SBOM data adheres to the Software Package Data Exchange (SPDX) standard and is provided in JSON format. SBOM data provides software supply chain transparency and can be used in vulnerability scanning and asset tracking tools on the customer side.

SBOM enables customers to gain a clearer understanding of the software components, versions, licenses, and any open-source software used on the platform. It can facilitate faster detection of known security vulnerabilities in the software components, ultimately enhancing security.

Third stage – Efficient deployment and configuration at-scale

Challenges

Cyber resilient configuration and deployment of the servers is a critical step in the server life cycle. Any mistakes or oversights during this process can result in poor server performance, downtime, or even security breaches. The right set of controls and gates must be in place to ensure system and data integrity throughout the server operation. This configuration and deployment must be performed for hundreds or thousands of servers while ensuring consistency and minimizing any manual errors.

PowerEdge solution

System integrity

Ensuring system integrity is foundational for securing the server and establishing a lockdown posture for Zero Trust operations. This integrity starts with ensuring that server hardware and components are genuine, and from a trusted and authorized source. Then, the firmware and software must be verified to ensure that a bad actor has not tampered with them. For PowerEdge, this process of ensuring system integrity starts with a silicon-based platform RoT. This RoT anchors the other security controls on the server platform and establishes a chain of trust for cryptographic verification of hardware and software components on the server.

RoT as the anchor for cryptographically verified trusted booting

One of the most critical aspects of server security is ensuring that the boot process can be verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an operating system or updating firmware.

All PowerEdge servers have an immutable, silicon-based RoT burnt into them from the factory. The RoT has one-time programmable, read-only public keys that can be used for cryptographic verification and attestation of integrity.

The BIOS boot process uses Intel Boot Guard technology or AMD PSB technology that cryptographically verifies the BIOS code to be loaded. A verification failure results in a server shutdown and the Lifecycle Controller Log includes a notification. The IT administrator can then initiate the BIOS recovery. If Boot Guard validates successfully, a chain of trust procedure validates the remaining BIOS modules until control is handed off to the operating system or hypervisor.

In addition to Boot Guard's verification mechanism, iDRAC9 4.10.10.10 or higher provides a RoT mechanism to verify the BIOS image at the host boot time. The host can boot only after the BIOS image is successfully validated. iDRAC9 also provides a mechanism to validate the BIOS image at run time, on demand, or at user-scheduled intervals.

Cryptographically verified Trusted Booting

One of the most critical aspects of server security is ensuring that the boot process can be verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an operating system or updating firmware.

PowerEdge servers have used silicon-based security for several generations for features such as iDRAC Credential Vault, an encrypted secure memory in iDRAC for storing sensitive data. The boot process is verified using a silicon-based RoT to meet recommendations in NIST SP 800-147B (*BIOS Protection Guidelines for Servers*) and NIST SP 800-155 (*BIOS Integrity Measurement Guidelines*).

Security Protocol Data Model for component attestation

The Distributed Management Task Force (DMTF), of which Dell Technologies is a leading member, defines the Security Protocol Data Model (SPDM). SPDM defines a consistent, open-standard method of communicating in the server to gather information about server components. This component information is protected by encrypting it and using authenticated key exchange to integrity-protect all communications between components. iDRAC SPDM implementation provides visibility into the PERC12 and certain NIC components. As part of the hardware inventory, iDRAC verifies the authenticity and integrity of PERC12 and NIC devices by cryptographically verifying the identity, firmware, and configuration.

TPM Support

PowerEdge servers support two versions of TPM:

- TPM 2.0 FIPS + Common Criteria + TCG certified (Nuvoton)
- TPM 2.0 China (NationZ)

TPM can be used to perform public key cryptographic functions, compute cryptographic hash functions, generate, manage, and securely store keys, and perform attestation. Intel's Trusted Execution Technology (TXT) functionality and Microsoft's Platform Assurance feature in Windows Server 2016 is also supported. TPM can also be used to enable the BitLocker hard drive encryption feature in Windows Server 2012, Windows Server 2016, and Windows Server 2022.

Attestation and remote attestation solutions can use TPM to take measurements at boot time of a server's hardware, hypervisor, BIOS, and operating system, and compare them in a cryptographically secure manner against "golden" or "base" measurements. These measurements are commonly stored outside the TPM on a remote attestation server solution. The TPM PCR measurements stored in the TPM are recalculated on every boot. If they are not identical, the server system might have been compromised and system administrators can disable and disconnect the server either locally or remotely.

Servers can be ordered with or without TPM, but for many operating systems and other security provisions, it is becoming a standard. TPM is enabled through a BIOS option. It is a Plug-In Module solution; the planar has a connector for this plug-in module.

UEFI Secure boot for firmware

PowerEdge servers also support industry-standard UEFI Secure Boot that checks the cryptographic signatures of UEFI drivers and other code loaded before the operating system is running. Secure Boot represents an industry-wide standard for security in the preboot environment. Computer system vendors, expansion card vendors, and operating system providers collaborate on this specification to promote interoperability.

When enabled, UEFI Secure Boot prevents unsigned (that is, untrusted) UEFI device drivers from being loaded, displays an error message, and does not allow the device to function. You must disable Secure Boot to load unsigned device drivers.

In addition, the 14th, 15th, and 16th generations of PowerEdge servers offer the unique flexibility of using a customized boot loader certificate. This certificate is primarily a feature for administrators of Linux environments that want to sign their own operating system boot loaders instead of relying on the default signing certificate provided by Microsoft's UEFI Certificate Authority (CA). Custom certificates can be uploaded by using the preferred

iDRAC API to authenticate the customer's specific operating system boot loader. The NSA cites this PowerEdge UEFI customization method for mitigating Grub 2 vulnerabilities in servers.⁴ PowerEdge supports complete customization of Secure Boot, including removal of all industry-standard certificates provided by Microsoft, VMware, or the UEFI CA.

Intel Boot Guard and AMD PSB

Intel Boot Guard and AMD PSB are host processor features that provide strong firmware integrity guarantees, by preventing firmware that is not authorized by the Dell OEM from running on the system. By enabling these features as additional defense-in-depth measures, certain classes of physical attacks are mitigated, such as flash memory replacement or reprogramming, and Time-of-Check-Time-of-Use (TOCTOU) race conditions. All combined, the RoT features in the system make compromise of the trusted computing base (TCB) difficult.

iDRAC/BMC

The Integrated Dell Remote Access Controller (iDRAC) is a Baseboard Management Controller (BMC) that is integrated in Dell PowerEdge servers. iDRAC provides secure and remote server access for many common management functions; administrators can deploy, manage, monitor, update, troubleshoot, and remediate Dell servers from any location without the use of agents and out of band.

iDRAC offers industry-leading security features that adhere to and are certified against well-known NIST standards, Common Criteria, and FIPS 140-2. It is through iDRAC9 that the end user can configure security features to maximize the security posture of the system.

iDRAC credential vault

The iDRAC service processor provides a secure storage memory that protects sensitive data such as iDRAC user credentials and private keys for self-signed SSL certificates. Another example of silicon-based security, this memory is encrypted with a unique immutable root key that is programmed into each iDRAC chip at the time of manufacture. This memory protects against physical attacks where the attacker desolders the chip to gain access to the data.

SELinux framework

SELinux operates at the core kernel level on iDRAC and does not require user input or configuration. SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to enrolled customers. In future iDRAC releases, these logs will be available in the Lifecycle Controller Logs.

Factory-generated default passwords

By default, all 14th, 15th, and 16th generations of PowerEdge servers ship with a unique, factory-generated iDRAC password to provide additional security. This password is on the pull-out Service Tag on the front of the chassis, next to the server asset label. If you choose this default option, use this password to log in to iDRAC for the first time, rather than using a universal default password. For security purposes, Dell Technologies strongly recommends changing the default password.

⁴ [CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF \(defense.gov\)](#)

Hardware security

Hardware security is an integral part of any comprehensive security solution. Some customers want to limit access to external ports, such as USB. Generally, a server chassis does not need to be opened after it has been put into production. At a minimum, customers always want to track and log any such activities. The overall goal is to discourage and limit any physical intrusion.

Chassis intrusion detection and alert

PowerEdge servers provide hardware intrusion detection and logging, with detection working even when no AC power is available. Sensors on the chassis detect when anyone opens or tampers with the chassis, even during transit. Servers that have been opened while in transit generate an entry in the iDRAC Lifecycle log after power is supplied.

Dynamic USB port management

For more security, you can completely disable USB ports. You also have the option of disabling only the USB ports on the front. For example, USB ports can be disabled for production use and then temporarily enabled to grant access to a crash cart for debugging purposes.

iDRAC Direct

iDRAC Direct is a special USB port that is hardwired to the iDRAC service processor for at-the-server debugging and management from the front of the server (cold aisle). It allows you to attach a standard Micro-AB USB cable to this port and the other end of the cable (Type A) to a laptop. A standard web browser can then access the iDRAC UI for extensive debugging and management of the server. If the iDRAC Enterprise license is installed, you can access the operating system desktop using the iDRAC's Virtual Console.

Because you use iDRAC credentials for logging in, iDRAC Direct works as a secure crash cart with the additional advantage of extensive hardware management and service diagnostics. This method is an attractive option for securing physical access to the server in remote locations (host USB ports and VGA outputs can be disabled in this case).

iDRAC Connection View with Geolocation

Connection View enables iDRAC to report the external switches and ports connected to Server I/O.

It is a feature on select networking devices and requires the Link Layer Discovery Protocol (LLDP) to be enabled on connected switches.

Some of the benefits of Connection View enable you to:

- Remotely and quickly check if server I/O modules (LOMs, NDCs, and add-in PCIe cards) are connected to the correct switches and ports
- Avoid costly remote dispatch of technicians to remediate wiring errors
- Avoid tracing cables in the server room hot aisles
- Retrieve information for all connections by accessing the UI or by using RACADM commands

Beyond the obvious time and monetary savings, Connection View provides an additional benefit – real-time geolocation of a physical server or VM. Using iDRAC Connection View, administrators can pinpoint a server to see to which switch and port the server is connected. This information helps secure servers from being connected to networks and devices that do not comply with corporate security guidelines or best practices.

Connection View validates the location of the server indirectly by reporting the switch identities to which it is connected. The switch identity helps to determine the geolocation and to assure that the server is not a rogue server in a nonauthorized site, providing another layer of physical security. This information also provides validation that an application or VM has not “crossed” country borders, and that it is running in an approved, secure environment.

Protecting data at rest

Data at rest protection ensures that sensitive data that resides in storage is protected from unauthorized access through encryption and external key management.

Dell Technologies provides:

- Software-based encryption (for example, virtual devices)
- Enterprise key management (for example, SED devices and key management)
- Hardware drive encryption (for example, SED devices)

Whether it is due to internal policies or external compliance, securing data continues to be a high priority for organizations of all sizes.

The 14th, 15th, and 16th generations of PowerEdge servers offer several storage drive options for securing data, as shown in the following figure:

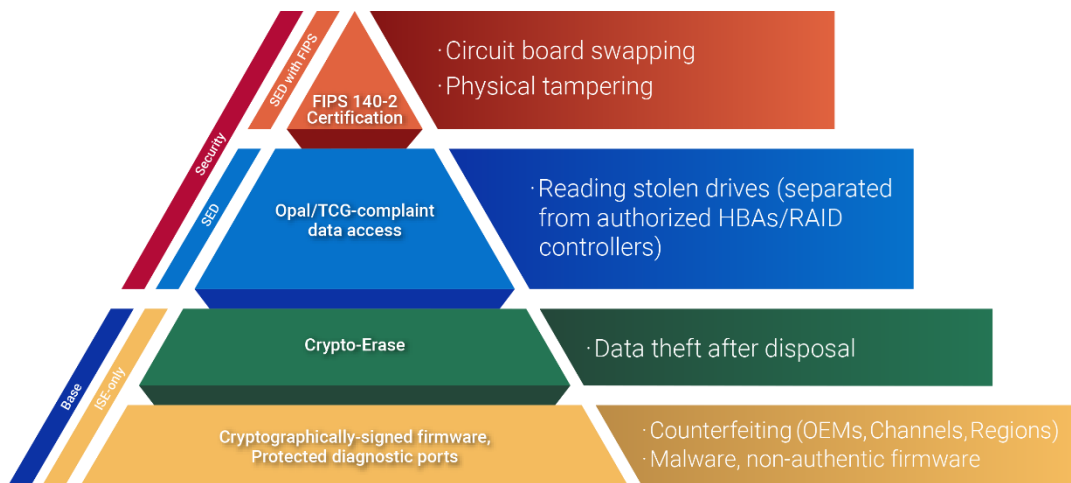


Figure 1. Storage drive options

The options start with drives that support Instant Secure Erase (ISE), a new technology to erase user data instantly and securely. The 14th, 15th, and 16th generations of PowerEdge servers offer ISE-capable drives as a default. This white paper describes ISE in more detail later as part of the System Erase feature description.

The next higher security option is Self-Encrypting Drives (SEDs), which offer locking protection that binds the storage drive to the server and RAID card used. This method protects against so-called “smash and grab” theft of drives and the subsequent loss of sensitive user data. When thieves try to use the drive, they do not know the required locking key passphrase and are thwarted from accessing the encrypted drive data. Customers can protect against theft of the entire server by using Secured Enterprise Key Manager (SEKM), which is described in the following section.

NIST FIPS 140-2 certified SEDs offer the highest level of protection. Testing laboratories have accredited drives conforming to this standard. Tamper-resistant stickers are applied to the drive. Dell SED drives have FIPS 140-2 certification by default.

Secured Enterprise Key Manager

OpenManage Secured Enterprise Key Manager (SEKM) delivers a central key management solution to manage data at rest across the organization. It enables you to use an external Key Management Server (KMS) to manage keys that iDRAC can use to lock and unlock storage devices on a PowerEdge server. Using embedded code that is activated with a special license, iDRAC requests that the KMS creates a key for each storage controller, which iDRAC fetches and provides to the storage controller on every host boot so that the storage controller can unlock the SEDs.

The advantages of SEKM over Local Key Management (LKM) include:

- Protection against “Theft of a server” because the keys are not stored on the server and are stored externally and retrieved by connected PowerEdge server nodes (using iDRAC)
- Centralized and scalable key management for encrypted devices with high availability
- Support for the industry-standard Key Management Interoperability Protocol (KMIP), which enables the use of other KMIP-compatible devices
- Protection of data at rest when drives or the entire server are compromised
- On-drive encryption performance scales with drive count

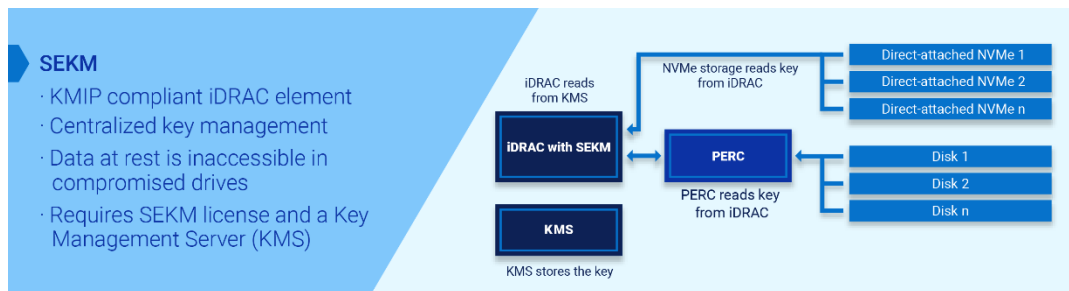


Figure 2. Secure Enterprise Key Manager (SEKM)

Local Key Management

PowerEdge servers provide the ability to secure SED drives connected to a PERC controller using Local Key Management (LKM).

To ensure user data protection if a drive is stolen, the SED must be locked with a separate key so that it does not decrypt user data unless that key is provided. This key is

referred to as the Key Encryption Key (KEK). The KEK is stored in the PERC, not on an external server.

Set a keyId/passphrase on the PERC controller to which the SED is connected. Then, the PERC controller generates a KEK using the passphrase and uses it to lock the SED. When the drive is powered on, it comes up as a locked SED and encrypts or decrypts user data only when the PERC provides the KEK to unlock it. If a locked drive is stolen, an attacker cannot provide the KEK, and the user data is protected.

The following figure shows the LKM solution:

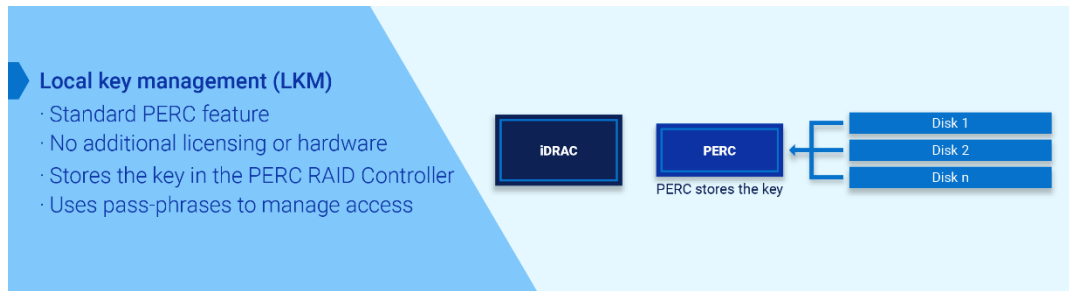


Figure 3. Local Key Management (LKM)

iLKM

For direct attach NVMe configurations where a PERC RAID controller is not available, iDRAC can be used as the key manager. This solution called OpenManage iLKM, is iDRAC-based and enables key exchange locally. iDRAC acts as a key manager and generates authentication keys that can then be used to secure storage devices. You can transition from iDRAC-based iLKM to iDRAC-based SEKM to upgrade to external key management.

The following figure shows the iLKM solution:

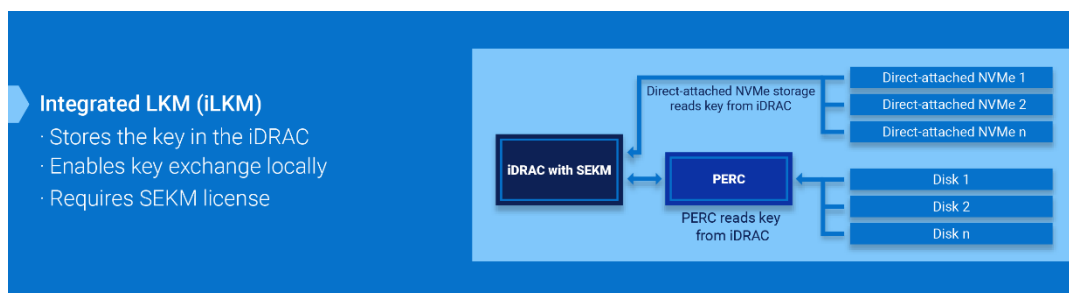


Figure 4. Integrated Local Key Management (iLKM)

Protecting Data in Flight

Data-in-flight protection ensures that data is protected from unauthorized disclosure or interception as it travels across networks or between systems. Sensitive data can be intercepted, stolen, or modified in transit, leading to data breaches, loss of intellectual property, and other security risks.

Distributed and cloud environments where data is constantly moving between systems and across networks, protecting your data through encryption and access controls are important components for data-in-flight protection in a Zero Trust environment.

TLS 1.3

The iDRAC web server uses a TLS/SSL certificate to establish and maintain secure communications with remote clients. Web browsers and command-line utilities, such as RACADM and WS-Man, use this TLS/SSL certificate for server authentication and establishing an encrypted connection.

There are several options available to secure the network connection using a TLS/SSL certificate. iDRAC's web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Whichever method you choose, when iDRAC is configured and the TLS/SSL certificate is installed on the management stations, TLS/SSL-enabled clients can access iDRAC securely and without certificate warnings.

SSH

iDRAC provides user control over the cryptographic settings for the SSH daemon such that you can determine the ideal settings for your environment. The control given to you is not a relaxation of the settings. Instead, the feature enables you to modify the value set for each option to achieve a narrower and stringent cryptographic policy. That is, you can only remove values from the options but cannot add any values other than those values that have been defined and allowed in the default value-set.

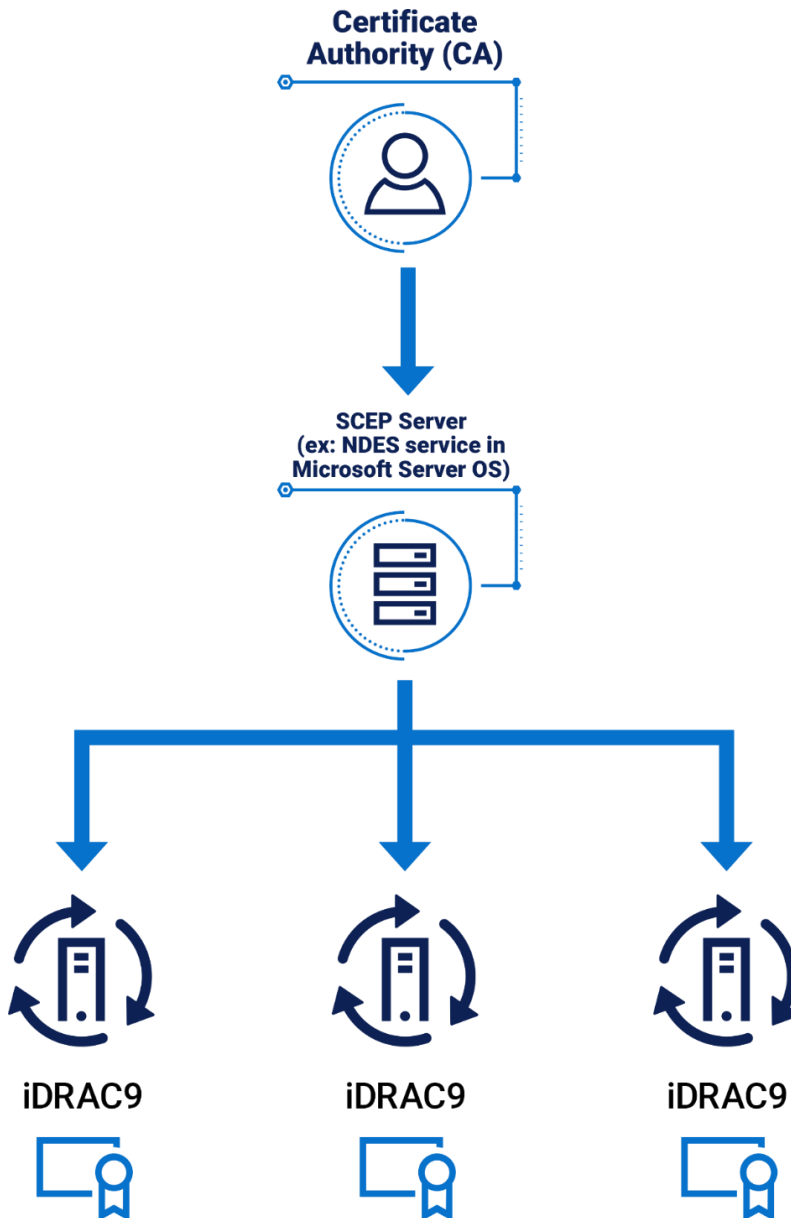
The cryptographic policies are configured using the following options:

- Ciphers — Ciphers
- Host-Key-Algorithms — HostKeyAlgorithms
- Key-Exchange Algorithms — KeyExchangeAlgorithms
- MACs — MACs

Typically, the values for each of these options are set to prudent settings that reflect the best security practices that cater to a wide variety of environments. As such, the iDRAC default settings for these options are the same as those options assigned by the SSH package open-source community. These settings can be configured using the RACADM command-line interface. See the *iDRAC RACADM CLI User's Guide*.

Automatic certificate renewal

iDRAC9 v4.0 and later has added a client for Simple Certificate Enrollment Protocol (SCEP) support and requires a Datacenter License. SCEP is a protocol standard used for managing certificates for large numbers of network devices using an automatic enrollment process. iDRAC can now integrate with SCEP-compatible servers such as the Microsoft ServerNDES service to maintain SSL/TLS Certificates automatically. This feature can be used to enroll and refresh a soon-to-be-expired web server certificate. You can use Server Configuration Profile to set the certificates on a one-to-one basis in the iDRAC UI. Also, you can provide scripts using tools such as RACADM.

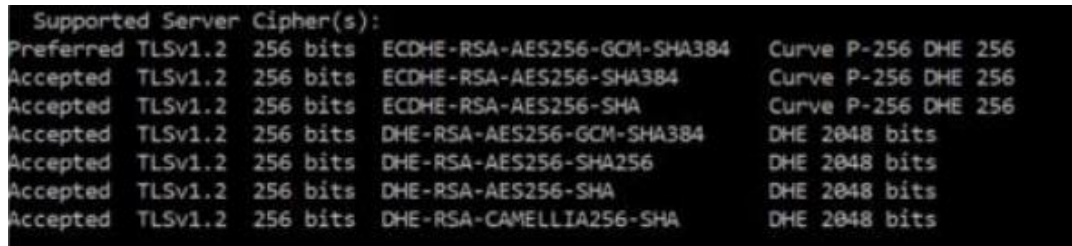


iDRAC Cipher Select

The Cipher Suite Selection can be used to limit the ciphers that the web browser can use to communicate with iDRAC. Also, it can determine the security of the connection. These settings can be configured through the iDRAC web interface, RACADM, and Redfish. This functionality is available across several iDRAC releases – iDRAC7, iDRAC8 (2.60.60.60 and higher), and the current iDRAC9 (3.30.30.30 and higher).

Commercial National Security Algorithm (CNSA) support

The supported ciphers available in iDRAC9 with TLS1.3 Bit and 256 Bit Encryption are shown in the following figure. The ciphers available are inclusive of the ciphers in the CNSA-approved set.

A screenshot of a terminal window showing the 'Supported Server Cipher(s):' list. The list includes a 'Preferred' cipher and several 'Accepted' ciphers, each with its TLS version, key size, and algorithm details.

Label	TLS Version	Key Size	Algorithm	Curve
Preferred	TLSv1.2	256 bits	ECDHE-RSA-AES256-GCM-SHA384	P-256 DHE 256
Accepted	TLSv1.2	256 bits	ECDHE-RSA-AES256-SHA384	P-256 DHE 256
Accepted	TLSv1.2	256 bits	ECDHE-RSA-AES256-SHA	P-256 DHE 256
Accepted	TLSv1.2	256 bits	DHE-RSA-AES256-GCM-SHA384	DHE 2048 bits
Accepted	TLSv1.2	256 bits	DHE-RSA-AES256-SHA256	DHE 2048 bits
Accepted	TLSv1.2	256 bits	DHE-RSA-AES256-SHA	DHE 2048 bits
Accepted	TLSv1.2	256 bits	DHE-RSA-CAMELLIA256-SHA	DHE 2048 bits

Tips for securing iDRAC connection

The most secure network connection is the iDRAC's Dedicated NIC because it can be connected to a network that is physically separated from the production network. This method physically separates the iDRAC management traffic from the production network traffic.

If use of the iDRAC's Dedicated NIC is not feasible, iDRAC can be run in Shared LOM mode with a VLAN enabled. However, the iDRAC's management traffic is sent across the same connection as the production network. Alternatively, if the use of a VLAN is not possible while in Shared LOM mode, access to iDRAC must be secured using strong passwords and other security measures.

For further information, see the [iDRAC Security Configuration Guide](#).

IEEE.802.1x

The network standard IEEE 802.1x has been enabled on PowerEdge servers. This network protocol provides port-based network authentication. Devices requesting access to the LAN or WLAN must be authenticated and validated before authorization for access.

Domain isolation

The 14th, 15th, and 16th generations of PowerEdge servers provide additional security by using domain isolation, an important feature for multitenant hosting environments. To secure the server's hardware configuration, hosting providers might want to block any reconfiguration by tenants. Domain isolation is a configuration option that ensures that management applications in the host operating system have no access to the out-of-band iDRAC or to Intel chipset functions, such as Management Engine (ME) or Innovation Engine (IE).

Protecting data in use

Protecting application data that is being used in memory has become increasingly important. Whether data in use is a machine learning dataset or relates to keeping a secret in memory such as in multitenant environments, data in-use can be vulnerable to

threat vectors that can intrude on the contents of memory or the access bus. Data in use protection is necessary to secure computations that are increasingly operating on large datasets in memory. Additionally, code running on the data must be trusted and tamper-free. There must be facilities to separate trusted and nontrusted code execution environments for data in use.

New developments in CPU technology for confidential computing allow secure enclaves to protect application data at the hardware layer, enabling a more comprehensive data protection strategy. Starting with the 15th generation of server offerings, Dell Technologies enables these CPU technologies, including Intel SGX/TME and AMD SEV/SME.

AMD confidential compute features

AMD introduced Secure Encrypted Virtualization (SEV) with the first generation of AMD EPYC processors. It encrypts full system memory and individual virtual machine (VM) memory isolating the VM memory from the hypervisor. With each generation of AMD EPYC processors, AMD has enhanced SEV with additional features to safeguard privacy and integrity by encrypting each VM with one of up to 509 unique encryption keys known only to the processor. The keys are used to encrypt memory using 128-bit AES encryption engines in the memory controller. The hypervisor manages the keys in the memory controller with the help of AMD's Secure processor. The key AMD SEV technologies that are part of the Infinity Guard technology solution suite from AMD that address different use cases, deployments, and threat models include:

- AMD's SME technology refers to using a single key to encrypt system memory.
- AMD SEV uses one key per VM to isolate guests and the hypervisor from one another.
- AMD SEV-ES encrypts all CPU register contents when a VM stops running to prevent leakage of information from CPU registers to the hypervisor.
- AMD SEV-SNP adds strong memory integrity protection to help prevent hypervisor-based attacks like data replay, memory remapping, and so on.

Intel confidential computing features

Starting with the 3rd Generation Intel Xeon platform, Intel introduced several key security innovations. Total Memory Encryption (TME) is available to ensure memory accessed from the CPU is encrypted. By encrypting all memory, existing software applications run unmodified while simultaneously providing greater protection for system memory.

Intel TME helps ensure that all memory accessed from the Intel CPU is encrypted, including customer credentials, encryption keys, and other intellectual property or personal information about the external memory bus. Intel developed this feature to provide greater protection for system memory against hardware attacks, such as removing and reading the dual inline memory module (DIMM) after spraying it with liquid nitrogen or installing purpose-built attack hardware. Using the NIST storage encryption standard, AES XTS, an encryption key is generated using a hardened random number generator in the processor without exposure to software. This method allows existing software to run unmodified while better protecting memory.

Identity Access Management

Identity and Access Management (IAM) is a set of security controls to manage digital identities and provide authentication and authorization by controlling the requestor's access to information and resources, at the right level, and at the right time to limit unauthorized access. IAM frameworks provide advantages over simple passwords, such as:

- **Enhanced security**—Includes various tools such as single sign-on (SSO) services, multifactor authentication (MFA), and privileged access management for stronger security and to avoid risks from vulnerable passwords. IAM plays a critical role in protecting organizations against phishing and social engineering attacks by implementing strong authentication, access control, monitoring, and user education. It helps organizations reduce their attack surface and respond effectively to threats.
- **Reduction of compromised passwords**—Deters credential theft from phishing, social engineering, and brute-force attacks by using MFA and additional security layers.
- **Granular access control**— Enables fine-grained control over user access permissions by using role-based access control (RBAC) and attribute-based access control (ABAC) to ensure that users only have access to necessary resources and data.
- **Centralized management**—Controls user accounts and access policies, which provides easier management of users as they join, move within, or leave the organization.
- **Auditing and logging**—Monitors user activities to identify and remediate suspicious access attempts.
- **Scalability**—Adapts to the need for a growing number of users and resources
- **Regulatory compliance**—Adheres to regulatory requirements to avoid legal consequences.
- **User experience**—Provides SSO services and password management to enable users to access multiple applications and services by using one set of credentials.
- **Adaptive authentication**—Applies additional security measures by assessing risk factors.
- **Emergency access and recovery**—Grants temporary emergency access for critical situations while maintain security controls.
- **Integration**—Integrates with various systems, applications, and cloud services for seamless access management across the entire IT ecosystem.

As a broad IT issue spanning technological and regulatory requirements, IAM is a strategic business imperative for all organizations to enhance security and resiliency. Zero Trust Architecture (ZTA) has emerged as the standard choice for securing all levels of infrastructure and is a foundational part of ZTA. The unofficial mantra of Zero Trust is “never trust, always verify” and if you cannot verify then you cannot trust. IAM provides that verification.

The foundation to a strong cybersecurity framework and the adoption and implementation of Zero Trust principles is identity. Identification of not only people but of applications, communication paths, network devices, and the data itself. If an organization does not have a strong Identity Credentialing and Access Management (ICAM) practice, then the underlying security practices are at risk. An effective identity and access solution must include necessary tools and controls that can capture and store user login details, facilitate the assignment and revocation of user access credentials, and oversee the central enterprise database of user roles, levels, and access privileges. At a minimum, access must only be allowed to facilitate the necessary functions that the organization has defined. As an example, users must only have access and permission to data, applications, and services to do what is defined in their job. Practices and tools must be implemented to ensure that this role is maintained and that even in that role, a user must be monitored to ensure that they are not doing anything that violates the organization's goals for data utilization.

MFA –Smartcards (CAC/PIV)

MFA for Smartcards (CAC/PIV) is a general-purpose certificate authentication that includes Common Access Card (CAC) and Personal Identification Verification (PIV) cards. Certificate authentication uses the client identity certificate to authenticate the user. It is used primarily in government or organizations that work with the federal industry.

MFA – RSA SecurID

RSA SecurID is another means of authenticating a user on a system. As another two-factor authentication, iDRAC9 supports RSA SecurID with the Datacenter license and starting with firmware 4.40.00.00 and later, as another two-factor authentication.

Directory integration for authorization

For centralized user and domain management, iDRAC supports integration into privileged management tools such as Lightweight Directory Access Protocol (LDAP) and Active Directory. Using a directory service provides a central location for easier user inventory management and assigning user account access controls and settings.

You can use LDAP to authenticate users and groups in iDRAC. To configure the LDAP directory service, you can use the objects in the `cfgLdap` and `cfgLdapRoleGroup` groups with the `config` command. You can also use the objects in the `iDRAC.LDAP` and `iDRAC.LDAPRole` groups with the `set` command 12.

For Active Directory integration, you can configure LDAP over SSL (LDAPS) on iDRAC to communicate with Active Directory domain controllers. After a valid certificate is installed on the domain controller and the connection to the DC using SSL over port 636 is verified, you can use the directory service integration test on iDRAC/OME to communicate with the domain controller.

SSO

iDRAC supports SSO, which provides the ability to share validated credentials and identifications across multiple domains without having to rechallenge or reauthenticate the user. SSO enables an authenticated operating system administrator to directly access the iDRAC web interface without requiring login using separate iDRAC administrator credentials. iDRAC supports the following SSO protocols:

- **OpenID connect** is an open standard and is a decentralized authentication protocol that is typically used for machine-to-machine-like RestAPIs.

- Open-standards **Security Assertion Markup Language (SAML)** is typically used for UI SSO.

Role-based access controls

Role-based access control (RBAC) is the most popularly used form of access control. Permissions are grouped in roles and are typically assigned to a group. Assigning authorization capabilities to users and groups is managed in Active Directory.

You can set up user accounts with specific privileges (role-based authority to manage your system using iDRAC and maintain system security). By default, iDRAC is configured with a local administrator account. The default iDRAC username and password are provided with the system badge. As an administrator, you can set up user accounts to allow other users to access iDRAC. For more information, see the documentation for the server.

You can set up local users or use directory services such as Microsoft Active Directory or LDAP to set up user accounts. Using a directory service provides a central location for managing authorized user accounts.

iDRAC supports role-based access to users with a set of associated privileges. The roles are administrator, operator, read-only, or none. The role defines the maximum privileges available.

Time-based access controls

Time-based access control is another valuable tool for enhancing security and managing access to sensitive data, facilities, or systems in a tightly controlled and monitored environment. For instance, if a technician needs physical access to the USB port on the server, the iDRAC administrator can enable/disable specific access times for USB port access.

Scope-based access control

Scope-based access control provides more granular control than user- and role-based access control. It allows the administrator to apply a policy with a set of permissions that are evaluated when an entity tries to access the resource. For instance, access can be restricted, based on resource location, IP address range, and so on.

Capabilities and automation for efficient at-scale deployment

Zero-touch automation with iDRAC – Server configuration profiles

Zero Touch provisioning is available with iDRAC Enterprise or Datacenter licenses. Zero Touch provisioning automates all hardware configuration, certificate installation, repository firmware updates, and operating system deployment. The IT Admin can preconfigure security settings and ensure uniform server images. Zero Touch provisioning is available through the iDRAC Server Configuration Profile feature and with OpenManage Enterprise.

CloudIQ

CloudIQ monitors the health and cybersecurity of your enterprise-wide servers and predicts their performance so that you can proactively address issues before they impact your business.

CloudIQ offers a simple and intuitive solution to collect firmware details from PowerEdge servers including BIOS, iDRAC, NICs, PERC, drives, and supported peripherals. A recent

feature from both OpenManage Enterprise and CloudIQ identifies BIOS and firmware that requires an update. CloudIQ can report the current installed version, compare it to the latest Dell release available, and schedule updates. This information is collected from each server using the agent-free iDRAC, consolidated by OpenManage Enterprise, and then transferred to CloudIQ to be processed. This powerful feature includes user rights integrated in both OpenManage Enterprise and CloudIQ to allow only authorized users to run these commands. Also, CloudIQ can consolidate multiple OpenManage Enterprise instances into one server fleet management view.

Fourth Stage – Security management and monitoring

Challenges

You cannot defend what you cannot see. Attacks happen quickly, faster than a human can detect and respond. Protecting your critical assets in real-time within a dynamic and complex threat environment is a challenge. Lack of skills and resources exacerbates the problem. As IT administrators face ongoing challenges in their environments, more easily managing the infrastructure—through more automation, fewer task steps, and more intuitive interactions—is key to administration productivity.

It is critical that your business remains resilient and unaffected by adverse outcomes. The business must stay nimble to be aware, respond, and recover:

- Observability and transparency enable effective security event awareness and timely remediation.
- Lack of skills and resources increases problems. Monitor activity across infrastructure (user, device, data, network, and application) to identify patterns and anomalies. Analytics can be used to detect and respond to security threats.
- Automation is important.
- Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve models that improve detection and reaction time in making real-time access decisions. Simplification is foundational and fundamental to a resilient infrastructure.

PowerEdge Solutions

The Dell management portfolio simplifies administrator tasks. It improves security and health monitoring to scale security confidently by using automation and intelligence. Monitoring and logging are a key part of a zero-trust implementation.

Visibility, logging, and alerts

It is critical to have a detection capability that provides complete visibility into the configuration, health status, and change events in a server system. This visibility must also detect malicious or other changes to BIOS, firmware, and option ROMs in the boot and operating system runtime process. Proactive polling must be coupled with the ability to send alerts for any events in the system. Logs must provide complete information about access and changes to the server. Most importantly, the server must extend these capabilities to all components.

Dell OpenManage Enterprise enables users to set up alert policies once and then automatically assign them for future alerts. Also, OpenManage Enterprise can apply a template to many servers at once. The OpenManage Enterprise solution ultimately saves time and effort by automating actions based on alerts after administrators have created a policy.

Telemetry

Beginning with iDRAC9 v4.00.00.00 firmware and a Datacenter license, IT managers can integrate advanced server hardware operation telemetry into their existing analytics solutions. Telemetry is provided as granular, timeseries data that is streamed or pushed. The advanced agent-free architecture in iDRAC9 provides over 180 data metrics that are related to server and peripheral operations. Metrics are precisely timestamped and internally buffered to allow highly efficient data stream collection and processing with minimal network loading. This comprehensive telemetry can be fed into analytics tools to predict failure events, optimize server operations, and enhance cyber resiliency. The iDRAC9 Telemetry Streaming collects and streams live system data from one or more PowerEdge servers to a centralized collector.

iDRAC Lifecycle Logs

The Lifecycle Logs are a collection of events that occur in a server over time. They provide a description of events with timestamps, severity, user ID or source, and recommended actions. This technical information helps with security tracking and other hardware alerts.

The various types of information that is recorded in the Lifecycle Controller Log (LCL) include:

- Configuration changes on the system hardware components
- iDRAC, BIOS, NIC, and RAID configuration changes
- Logs of all the remote operations
- Firmware update history based on device, version, and date
- Information about replaced parts
- Information about failed parts
- Event and error message IDs
- Host power-related events
- POST errors
- User login events
- Sensor state change events

Alerts

iDRAC provides the capability to configure different event alerts and actions to be performed when a Lifecycle Logs event occurs. When an event is generated, it is forwarded to the configured destinations by using the selected alert type mechanisms. Users can enable or disable alerts through the iDRAC web interface, RACADM, or with the iDRAC settings utility.

iDRAC supports several types of alerts such as:

- Email or IPMI alert
- SNMP trap
- Operating system and Remote System logs
- Redfish event

Alerts are categorized by severity – Critical, Warning, or Informational. The following filters can be applied to alerts:

- **System health**—For example, temperature, voltage, or device errors
- **Storage health**—For example, controller errors, physical or virtual disk errors
- **Configuration changes**—For example, change in RAID configuration, PCIe card removal
- **Audit logs**—For example, password authentication failure
- **Firmware**—For example, upgrades or downgrade

The IT administrator can set different actions for alerts – Reboot, Power Cycle, Power Off, or No action.

TLS for Remote Syslog

The iDRAC Remote Syslog feature allows you to write the RAC log and the System Event Log (SEL) remotely to an external syslog server. You can read all logs from the entire server farm from a central log. The Remote Syslog protocol does not require user authentication. For the logs to be entered in the Remote Syslog server, ensure that there is proper network connectivity between iDRAC and the Remote Syslog server and that the Remote Syslog server is running on the same network as iDRAC.

The iDRAC's web server has a self-signed TLS/SSL certificate by default. The self-signed certificate can be replaced with a custom certificate, a custom signing certificate, or a certificate signed by a well-known Certificate Authority (CA). Redfish scripts can perform automated certificate uploads. When a link has been established between the two servers, TLS encryption and SSL decryption enable secure data transport.

SELinux framework

SELinux operates at the core kernel level on iDRAC and does not require user input or configuration. SELinux logs security messages when an attack is detected. These log messages indicate when and how an attacker tried to break into the system. These logs are available through SupportAssist to customers enrolled in this new feature. In future releases of iDRAC, these logs will be available in the Lifecycle Controller Logs.

Real-time detection – BIOS Live scan

BIOS live scanning verifies the integrity and authenticity of the BIOS image in the primary ROM when the host is powered on. BIOS live scanning is not in the POST process. This feature is available only with the iDRAC9 4.10.10.10 (supported AMD platforms) and iDRAC9 4.40.20.00 (supported Intel platforms) Datacenter licenses. You must have administrator privileges or operator privileges with the "Execute Debug Commands" debug privilege to perform this operation.

You can initiate BIOS image scanning either on demand or by scheduling the scan through the iDRAC UI, RACADM, and Redfish interfaces. The BIOS live scan feature is available starting with 15th generation of PowerEdge servers with AMD “Rome”-based processors or Intel “Ice Lake”-based processors.

Boot time and run time BIOS scanning

A critical aspect of server security is ensuring that the boot process is verified as secure. This process provides a trusted anchor for all subsequent operations such as booting an operating system or updating firmware. PowerEdge servers have used silicon-based security for several generations for features such as iDRAC Credential Vault, an encrypted secure memory in iDRAC for storing sensitive data. The boot process is verified using a silicon-based RoT to meet the following recommendations:

- NIST SP 800-147B, BIOS Protection Guidelines for Servers
- NIST SP 800-155, BIOS Integrity Measurement Guidelines

On the Dell PowerEdge servers with iDRAC9, iDRAC first boots with chain of trust authentication, and then verifies BIOS integrity. iDRAC assumes the role of hardware-based root of trust. For AMD platforms, iDRAC accesses the primary BIOS ROM through SPI and the AMD fusion controller hub (FCH), and performs the RoT process. For Intel platforms, iDRAC accesses the primary BIOS ROM through SPI and the Intel Platform Controller Hub (PCH), and performs the RoT process.

iDRAC9 directly accesses the BIOS primary ROM to perform a RoT operation on the processor on both the security block and the host Initial Boot Block.

Silicon-based Root of Trust

PowerEdge servers use an immutable, silicon-based RoT to attest to the integrity of BIOS and iDRAC9 firmware cryptographically. This RoT is based on one-time programmable, read-only public keys that provide protection against malware tampering. The BIOS boot process uses Intel Boot Guard technology or AMD Platform Secure Boot technology. This technology verifies that the digital signature of the cryptographic hash of the boot image matches the signature stored in silicon by Dell Technologies in the factory. A verification failure results in a server shutdown and user notification in the Lifecycle Controller Log. The user can initiate the BIOS recovery process. If Boot Guard validates successfully, the other BIOS modules are validated by using a chain of trust procedure. Then, control is given to the operating system or hypervisor. In addition to Boot Guard, iDRAC9 4.10.10.10 or later provides a RoT mechanism that verifies the BIOS image at the host boot time. The host can boot only after the BIOS image is successfully validated. iDRAC9 also provides a mechanism to validate the BIOS image at run time, on demand, or at user-scheduled intervals.

For the chain of trust, each BIOS module contains a hash of the next module in the chain. The key modules in the BIOS include:

- Technical support and resources ID 483
- Initial Boot Block (IBB)
- Security (SEC)
- Pre-EFI Initialization (PEI)
- Memory Reference Code (MRC) o Driver Execution Environment (DXE)

- **Boot Device Selection (BDS)**

If Intel Boot Guard authenticates the IBB module, the IBB module validates the SEC and PEI modules before handing control to it. The SEC and PEI modules then validate the PEI and MRC modules, which further validates the DXE and BDS modules. Next, control is handed over to UEFI Secure Boot. Similarly, for PowerEdge AMD EPYC-based servers, AMD Secure Root of Trust technology ensures that servers boot only from trusted firmware images. AMD Secure Run Technology encrypts the main memory, keeping it private from malicious intruders accessing the hardware. There are no required application modifications to use this feature, and the security processor never exposes the encryption keys outside of the processor. iDRAC takes on the role of hardware-based security technology and accesses the primary BIOS ROM through SPI. iDRAC, along with the AMD fusion controller hub (FCH) performs the RoT process.

Under the following conditions, iDRAC9 recovers the BIOS:

- BIOS integrity check failed
- BIOS self-check failed

Note: Use the RACADM command to recover the BIOS setup.

The iDRAC boot process uses its own independent silicon-based RoT that verifies the iDRAC firmware image. The iDRAC RoT also provides a critical trust anchor for authenticating the signatures of Dell firmware update packages (DUPs).

System lockdown

iDRAC9 offers a feature that ‘locks down’ the server hardware and firmware configuration and requires an Enterprise or Datacenter license. You can enable this mode by using the UI, the RACADM CLI, or the Server Configuration Profile. Users with administrative privileges can set System Lockdown mode, which prevents users with lesser privileges from changing the server. The IT administrator can enable or disable this feature. Any changes made when System Lockdown is disabled are tracked in the Lifecycle Controller Log. By enabling lockdown mode, you can prevent configuration drift in your data center when using Dell tools and agents and protect against malicious attacks against embedded firmware when using Dell Update Packages. Lockdown mode can be enabled dynamically, without requiring a system reboot. iDRAC9 v4.40 introduced enhancements where in addition to the current System Lockdown which only controls the updates using Dell Update Package (DUP), this lockdown functionality is extended to select NICs.

Note: Enhanced Lockdown for NICs only includes firmware lockdown to prevent firmware updates.

Configuration (x-UEFI) lockdown is not supported. When the customer sets the system in lockdown mode by enabling or setting attributes from any of the supported interfaces, iDRAC will take additional actions depending on the system configuration. These actions depend on the third-party devices detected as part of the iDRAC discovery process.

Drift detection

By enforcing standardized configurations and adopting a “zero tolerance” policy for any changes, organizations can reduce the potential for exploitation. Dell OpenManage

Enterprise Console allows you to define your own server configuration baselines and then monitor the drift of your production servers from those baselines. The baseline can be built based on different criteria to fit different production enforcement, such as security and performance.

OpenManage Enterprise can report any deviations from the baseline and optionally repair the drift with a simple workflow to stage the changes on iDRAC out of band. The changes can then take place at the next maintenance window while servers reboot to make the production environment compliant again. This staged process enables you to deploy configuration changes to production without any server downtime during nonmaintenance hours. It increases the server availability without compromising the serviceability or security.

Chassis intrusion detection

PowerEdge servers provide hardware intrusion detection and logging, with detection working even when no AC power is available. Sensors on the chassis detect when anyone opens or tampers with the chassis, even during transit. Servers that have been opened while in transit generate an entry in the iDRAC Lifecycle Logs after power is supplied.

Automated and manual recovery

BIOS and operating system recovery

The 14th, 15th, and 16th generations of PowerEdge servers include two types of recovery: BIOS Recovery and Rapid Operating System (OS) Recovery. These features enable rapid recovery from corrupted BIOS or operating system images. In both cases, a special storage area is hidden from run-time software (BIOS, operating system, device firmware, and so on). These storage areas contain pristine images that can be used as alternatives to the compromised primary software.

Rapid Operating System (OS) Recovery enables rapid recovery from a corrupted operating system image (or an operating system image suspected of malicious tampering). The recovery media can be accessed using an internal SD card, SATA ports, M.2 drives, or internal USB. The selected device can be exposed to the boot list and the operating system to install the recovery image. It can then be disabled and hidden from the boot list and operating system. In the hidden state, the BIOS disables the device so that the operating system cannot access it. If there is a corrupted operating system image, the recovery location can then be enabled for the boot process. These settings can be accessed through BIOS or the iDRAC interface.

In extreme cases, if the BIOS is corrupted (either by a malicious attack, a power loss during the update process, or any other unforeseen event), it is important to provide a way to recover the BIOS to its original state. A backup BIOS image is stored in iDRAC so it can be used to recover the BIOS image if needed. iDRAC orchestrates the entire end-to-end recovery process.

- BIOS itself initiates automatic BIOS recovery.
- Users using the RACADM CLI command can initiate on-demand BIOS recovery.

FW rollback

We recommend that you update the firmware to ensure you have the latest features and security updates. However, you may need to rollback an update or install an earlier

version if you encounter issues after an update. If you roll back to the previous version, it is also verified against its signature.

Firmware Rollback from existing production version “N” to a previous version “N-1” is supported for the following firmware images:

- BIOS
- iDRAC with Lifecycle Controller
- Network Interface Card (NIC)
- PowerEdge RAID Controller (PERC)
- Power Supply Unit (PSU)
- Backplane

You can roll back the firmware to the previously installed version (N-1) using any of the following methods:

- iDRAC web interface
- CMC web interface
- RACADM CLI for iDRAC and CMC
- Lifecycle Controller UI
- Lifecycle Controller remote services

You can roll back the firmware for iDRAC or any device that Lifecycle Controller supports, even if the upgrade was previously performed using another interface. For example, if the firmware was upgraded using the Lifecycle Controller UI, you can roll back the firmware using the iDRAC web interface. You can perform firmware rollback for multiple devices with one system reboot.

On 14th, 15th, and 16th generations of PowerEdge servers that have a single iDRAC and Lifecycle Controller firmware, rolling back the iDRAC firmware also rolls back the Lifecycle Controller firmware.

Firmware rollback protection

If the firmware has a known vulnerability which would expose your server to attack, the BIOS itself can prevent downgrade to a previous version. The firmware release notes state that you cannot rollback when performing an update.

Full Power Cycle

In a Full Power Cycle, the server and all its components are rebooted. It drains main and auxiliary power from the server and all components. All data in volatile memory is also erased.

A physical Full Power Cycle requires removing the AC power cable, waiting for 30 seconds, and then putting the cable back. This method poses a challenge when working with a remote system. A feature in the 14th, 15th, and 16th generations of PowerEdge servers enables you to perform an effective full power cycle from the iDRAC Service Module (iSM), iDRAC UI, BIOS, or a script. A full power cycle takes effect at the next power cycle.

The Full Power Cycle feature eliminates the need for anyone to be physically present in the data center, thus reducing time to troubleshoot. It can eliminate, for example, any malware that is still memory-resident.

Updating

Dell Technologies provides a rich set of tools to make it easier to keep your server's firmware and BIOS up-to-date and update quickly. Ensuring firmware is up to date is a vital task to keep production servers secure and operating efficiently. Tracking and implementing these updates can be burdensome for administrators. iDRAC9 provides automatic updates with the ability to schedule firmware updates as wanted.

Many companies schedule monthly maintenance windows to handle operating system, application, and firmware updates. With OpenManage Enterprise, systems administrators can stage firmware updates for the next time the system is rebooted or for a scheduled deployment. This method ensures that nobody must be physically present to run the updates.

PowerEdge provides patches to security vulnerabilities with Dell security advisories. The advisories provide timely information, guidance, and mitigation options to minimize risks associated with security vulnerabilities.

Restoring server configuration after hardware servicing

Remediating service events is a critical part of any IT operation. The ability to meet recovery time objectives and recovery point objectives has direct implications on the security of the solution. Restoring server configuration and firmware assures that security policies for server operation are automatically met.

PowerEdge servers provide functionality that quickly restores server configuration in the following situations:

- Individual part replacement
- Motherboard replacement (full server profile backup and restore)
- Motherboard replacement (easy restore)

Parts replacement

iDRAC automatically saves the firmware image and configuration settings for NIC cards, RAID controllers, and Power Supply Units (PSUs). If there is a field replacement of these parts, iDRAC automatically detects the new card and restores the firmware and configuration to the replaced card. This functionality saves critical time and ensures a consistent configuration and security policy. The update occurs automatically on system reboot after replacing the supported part.

Easy Restore (for motherboard replacement)

Easy Restore is an integrated storage component that maintains critical configuration information. The Easy Restore feature allows you to restore your system's service tag, all licenses, UEFI configuration, system configuration settings (BIOS, iDRAC and NIC), and the OEM ID (Personality Module) after replacing the system board. All data is backed up to a backup flash device automatically. If the BIOS detects a new system board and the service tag in the backup flash device, the BIOS prompts you to restore the backup information. You can still choose to perform the full system backup with iDRAC8 as you do with iDRAC6 and iDRAC7. This solution backs up and restores the actual firmware

versions in addition to the hardware settings. Easy Restore does not copy the firmware drivers due to size limitations.

CloudIQ

Misconfigurations of infrastructure systems can open your organization to cyber intrusion and are a leading threat to data security. The CloudIQ cybersecurity feature proactively monitors infrastructure security configurations for Dell PowerStore and PowerMax storage systems and PowerEdge servers, and notifies users of security risks. A risk level is assigned to each system, placing the system into one of four categories, depending on the number and severity of the issues: Normal, Low, Medium, or High.

By using CloudIQ Cybersecurity policy templates, users can quickly set up security configuration evaluation tests and assign them to large numbers of systems with just a few clicks. Once assigned, the test plan is evaluated against each associated system, and the system administrator is notified in minutes of any unwanted configuration settings.

When a security risk is found, remediation instructions are provided to help you address the issue quickly. CloudIQ evaluates outgoing Dell Security Advisories (DSAs) and intelligently notifies users when those advisories are applicable to their specific Dell system models with specific system software and firmware versions. This notification eliminates the need for users to investigate if a Security Advisory applies to their systems and allows them to focus on remediation immediately.

Managed detection and response services

Dell Technologies Managed Detection and Response services is a cloud-based offering that helps organizations quickly and significantly improve their security posture—while reducing the burden on IT. This fully managed, end-to-end, 24/7 service monitors, detects, investigates, and responds to threats across the entire IT environment.

Designed for organizations with 50 endpoints or more, this unique service uses two key capabilities:

- The power of the open Secureworks Taegis XDR security analytics software, built on more than 20 years of SecOps expertise including real-world threat intelligence and research, and experience detecting and responding to advanced threats
- The expertise of Dell Technologies security analysts, gained through years of experience helping organizations worldwide to better protect their business

[Dell Technologies Managed Detection and Response](#) provides around-the-clock access to security experts. They provide end-to-end visibility and protection from endpoint to cloud, covering every aspect of advanced threat detection and response supported by Taegis XDR's database of 52,000 unique threat indicators that are managed and updated daily. Taegis XDR also ingests data from existing security solutions to use any previous security investments.

Dell Technologies security analysts assist with initial setup, monitoring, detection, remediation, and response—all for one predictable price. They work closely with your IT team to understand the environment. They provide advice about improvements to the security posture and help you set up and deploy the Taegis XDR software agent to endpoints. Then, using the Taegis XDR application, they monitor and review alerts 24/7.

Fifth stage – Secure decommissioning and repurposing

If an alert merits investigation, analysts determine and perform the appropriate response. If a threat is malicious or requires your action, you are informed and, if necessary, provided with step-by-step instructions. As part of the service, Dell Technologies also provides up to 40 hours per quarter of [remote remediation assistance](#), such as helping with troubleshooting, issue resolution, software deployments, patch and asset assessment, and configuration of IT environments.

If there is a security incident, Dell Technologies initiates the process to get your business up and running and provides up to 40 hours of remote incident response assistance a year.

Fifth stage – Secure decommissioning and repurposing

Challenge

Data security is a key consideration throughout the life cycle of a server, including when the server is repurposed or retired. Many servers are repurposed as they are transitioned from workload to workload, or as they change ownership from one organization to another. All servers are retired when they reach the end of their useful life. When such transitions occur, IT best practices recommend removing all data from the server to ensure that confidential information is not inadvertently shared.

PowerEdge solutions

Beyond best practices, in many cases government regulations about privacy rights also necessitate complete data elimination when IT resources are transitioned. Data erasure is a key capability encompassed in the Dell Secure Development Lifecycle (SDL). The SDL and secure server management tools ensure that PowerEdge servers are secure at every stage in the server life cycle, from server conception, design and manufacturing, to operation and decommissioning.

At this final stage (decommissioning/retirement), or when a server is repurposed due to change of workload or ownership, a capability starting with the PowerEdge 14th generation of servers, can simplify data erase.

System Erase, with iDRAC9 and the 14th, 15th, and 16th generations of PowerEdge servers, simplifies the process of erasing server storage devices and server nonvolatile stores such as caches and logs. To meet varying Systems Administrator needs for interactive and programmable operations, the following methods can perform System Erase:

- Lifecycle Controller UI
- WS-Man API
- RACADM CLI

Using one of these methods, an administrator can selectively reset a PowerEdge server to its original state (factory settings), removing data from internal server nonvolatile stores and from storage devices within the server.

System Erase can discover server-attached storage including hard disk drives (HDDs), SEDs, ISE, and nonvolatile memory drives (NVMe). Data stored on ISE, SED, and NVMe devices can be made inaccessible using cryptographic erase while devices such as non-ISE SATA HDDs can be erased using data overwrite.

Secure Erase

Through the life cycle controller, customers can repurpose or retire a system. All drives now shipping on PowerEdge systems can be securely erased. On an older platform that might not have encryption-capable drives, there is a “standard disks (overwrite data)” option. Unrecoverable processes generate warning messages. The server is powered off after a retire or repurpose operation. You can view the Lifecycle Logs in iDRAC to confirm that the operation was successful.

At the end of a system life cycle, it can either be retired or repurposed. For either scenario, System Erase removes sensitive data and settings from the server. Secure Erase wipes storage devices and server nonvolatile stores such as caches and logs so that no confidential information unintentionally leaks. It is a utility in Lifecycle Controller (F10) that erases logs, configuration data, storage data, and cache.

The System Erase feature can erase the following devices, configuration settings, and applications:

- iDRAC is reset to default settings, erasing all data and settings.
- Lifecycle Controller (F10) data is cleared.
- BIOS and NVRAM are reset to default settings.
- Embedded diagnostics and operating system driver packs are cleared.
- iDRAC Service Module (iSM) are cleared.
- SupportAssist Collection reports are cleared.

The following components can also be erased:

- Hardware Cache (clear PERC NVCache)
- vFlash SD Card (initialize card)

Note: vFlash not available on 15th generation of PowerEdge servers or later.

System Erase cryptographically disposes of data on the following components:

- Self-Encrypting Drives (SED)
- ISE drives
- NVM devices such as Intel Apache Pass and NVDIMMs

Secure erase – physical disk

Reset the drive to the factory settings. All data on the SSD is permanently removed and cannot be recovered. To sanitize the drive, the mapping table is deleted and all blocks to which data has been written are erased. Not all SSDs support the sanitize feature.

Overwrite erase

Overwrite-erase is a software-based method that overwrites data with zeros and ones. Data overwrite can erase non-ISE SATA hard drives.

Summary

Crypto erase

ISE destroys the internal encryption key that is used in the 14th, 15th, and 16th generations of PowerEdge drives and renders the user data unrecoverable. Used on self-encrypting drives, the encryption key is erased. The data remains on the drive but is inaccessible without the key. ISE is a recognized method of data erasure on storage drives as seen in NIST Special Publication 800-88 “Guidelines for Media Sanitization.”

Advantages of the new ISE feature with System Erase include:

- **Speed**—ISE is faster than data overwriting techniques like DoD 5220.22-M (seconds compare with hours)
- **Effectiveness**—ISE renders all the data on the drive, including reserved blocks, unreadable.
- **Better TCO**—Storage devices can be reused instead of being physically destroyed.

The following methods can perform System Erase procedure:

- Lifecycle Controller interface (F10)
- RACADM CLI
- Redfish

Data sanitization and destruction services

Data continues to grow and drive strategic advantage. Meanwhile, national security issues and data privacy regulations are escalating. As organizations navigate technology changes, they are further challenged with data security and compliance.

The end of the product life cycle is an aspect of data security that is increasingly important. Data Sanitization for Enterprise is a software-based method of securely overwriting data to render it unrecoverable. The various options include:

- **Data Sanitization for Enterprise Onsite**—An option for customers looking to refresh or redeploy assets. This service performs sanitization at the business' location, securing data while assets remain in the environment.
- **Data Sanitization for Enterprise Offsite with Asset Resale and Recycle**—A service that removes assets from the business' environment, sanitizes them at a secure location, and evaluates them for resale or reuse. The customer is compensated if value is found. If no value is found, assets are recycled according to local regulatory guidelines.

Data Destruction for Enterprise—A process that renders data inaccessible through the process of physical shredding. It is available for all Dell infrastructure solutions and similar third-party non-Dell branded assets. This process does not require systems to be operational.

Summary

Data center security is paramount to business success, and the security of the underlying server infrastructure is critical. Cyberattacks have the potential for extended system and business downtime, lost revenue and customers, legal damages and tarnished corporate

reputation. To protect, detect, and recover from hardware-targeted cyberattacks, security must be built into server hardware design, not added on later.

Dell Technologies has been a leader in using silicon-based security to secure firmware and protect sensitive user data in PowerEdge servers for the past two generations. The 14th, 15th, and 16th generations of PowerEdge product lines feature an enhanced Cyber Resilient Architecture that uses silicon-based Root-of-Trust to further harden server security including the following features:

- Cryptographically verified Trusted Booting that anchors end-to-end server and overall data center security. It includes features like silicon-based Root-of-Trust, digitally signed firmware, and automatic BIOS recovery.
- Secure Boot, which checks the cryptographic signatures of UEFI drivers and other code loaded before the operating system runs.
- iDRAC Credential Vault, a secure storage space for credentials, certificates, and other sensitive data that is encrypted with a silicon-based key that is unique for every server.
- Dynamic System Lockdown, a capability unique to PowerEdge servers, helps secure any system configuration and firmware from malicious or unintended changes while alerting users to any attempted system changes.
- Enterprise Key Management delivers a central key management solution to manage data-at-rest across the organization.
- System Erase, which allows users to easily retire or repurpose their 14th, 15th, and 16th generations of PowerEdge servers by securely and quickly wiping data from storage drives and other embedded nonvolatile memory.
- Supply Chain Security provides supply chain assurance by ensuring there is no product tampering or counterfeit components before shipping products to the customers.

The 14th, 15th, and 16th generations of PowerEdge servers, with their industry-leading security, form a trusted foundation for IT transformation on which customers can securely run their IT operations and workloads, and accelerate to Zero Trust adoption. Dell Technologies stops at nothing to help our customers build their breakthrough deployments. Our modern security approach ensures that an organization's environment is secure and resilient so that customers can focus on their core competencies, introduce their innovations, and advance human progress.

References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- [iDRAC9 Security Configuration Guide](#)
- [Dell EMC Secured Component Verification Reference Guide for Servers](#)
- [Understanding Confidential Computing with Trusted Execution Environments and Trusted Computing Base models](#)
- [iDRAC9 System Lockdown: Preventing Unintended Server Changes](#)
- [Next Generation Dell PowerEdge Servers: Transition to Modern UEFI](#)
- [Dell EMC PowerEdge UEFI Secure Boot Customization: Reduce Attack Surface with Complete Control of Certificates](#)
- [Dell Technologies Supply Chain Security: Secured Component Verification for PowerEdge](#)
- [Dell PowerEdge: iDRAC Automatic Certificate Enrollment](#)
- [Improved iDRAC9 Security using TLS 1.3 over HTTPS on Dell PowerEdge Servers](#)
- [A Partnership of Trust: Dell Supply Chain Security](#)
- [PowerEdge Advantages in your Zero Trust Journey – Video](#)
- [AMD on PE - Extending Data Protection to Data in Use - Video](#)
- [AMD on PE – Extended Boot Protection - Video](#)
- [Zero Trust Architecture - Video](#)
- [Cyber Resilient Architecture - Video](#)
- [Secured Component Verification - Video](#)
- [SEKM – Video](#)
- [IPv6 – Direct from Development](#)
- [iDRAC9 Virtual Power Cycle: Remotely power cycle Dell EMC PowerEdge Servers -Direct from Development](#)
- [Transform Datacenter Analytics with iDRAC9 Telemetry Streaming](#)
- [Configure iDRAC to use Active Directory Authentication \(dell.com\)](#)
- [Securing 14th Generation Dell EMC PowerEdge Servers with System Erase](#)
- [\(Direct from Development\) Security in Server Design](#)
- [\(Direct from Development\) Cyber-Resiliency Starts At The Chipset And Bios](#)
- [Factory Generated Default Password for iDRAC9 for Dell EMC 14th Generation \(14G\) PowerEdge Servers](#)

- [Dell EMC iDRAC Response to Common Vulnerabilities and Exposures \(CVE\) CVE-2017- 1000251 “BlueBorne”](#)
- [\(Video\) Secure Boot Configuration And Certificatemanagement Using RACADM- Video](#)
- [Secure Boot Management on Dell EMC PowerEdge Servers](#)
- [Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers](#)
- [Rapid Operating System Recovery](#)
- [Managing iDRAC9 Event Alerts on 14th generation \(14G\) Dell EMC PowerEdge Servers](#)
- [UEFI Secure Boot Customization](#)
- [iDRAC Overview](#)
- [OpenManage Console Overview](#)
- [OpenManage Mobile Overview](#)
- [Motherboard Replacement](#)

Eldorado do Sul, 28 de agosto de 2025

À

COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA
A/C Sr. Rafaella Tavares Barcelos

Ref.: COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE –
PROCEMPA - LICITAÇÃO ELETRÔNICA Nº 046/2025

ASSISTÊNCIAS TÉCNICAS

A **DELL COMPUTADORES DO BRASIL LTDA. (“Dell”)**, inscrita no CNPJ/MF sob o nº 72.381.189/0001-10, com sede na Av. Industrial Belgraf, 400 – Medianeira – Cep 92990-000, Eldorado do Sul/RS, vem, através da presente, informar as suas assistências técnicas autorizadas:

Nome	UF	Cidade	Razão Social	CNPJ	Endereços	CEP	Gerente Logístico
Porto Alegre	RS	Porto Alegre	Proxxi Tecnologia Ltda	47379565000438	RUA BEIRUTE, 340 - NAVEGANTES - PORTO ALEGRE - CEP 90240-080	90240-080	Nicolly Ribeiro Pereira - (48) 98841-4694

Atenciosamente,

DELL COMPUTADORES DO BRASIL
LTDA:72381189000110

Digitally signed by DELL
COMPUTADORES DO BRASIL
LTDA:72381189000110
Date: 2025.08.29 14:48:31 -03'00'

Dell Computadores do Brasil Ltda
Juliane Casagrande Rodrigues – Gerente de Vendas

Esta declaração é válida pelo prazo de 90 (noventa dias) da sua emissão.

DELL Computadores do Brasil Ltda.
Av. Industrial Belgraf , 400 . Eldorado do Sul / RS . Geral : 51 3481 5500 Fax : 51 3481 5458

Declaração do Fabricante

A **DELL COMPUTADORES DO BRASIL LTDA.** ("Dell"), inscrita no CNPJ sob o n. 72.381.189/0001-10, na qualidade de fabricante do(s) equipamento(s) de marca Dell (abaixo identificado(s)), ofertado(s) pela empresa **COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA**, no certame licitatório **LICITAÇÃO ELETRÔNICA Nº 046/2025**, promovido pela **COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE - PROCempa**, vem, através desta, declarar que:

- o(s) modelo(s) **Servidor Dell PowerEdge R760** possui(em) garantia de 60 meses, on-site, com atendimento telefônico 24 horas por dia, 7 dias na semana.

Declaramos, ainda, que:

- Os equipamentos por nós fabricados serão novos, sem uso e não são produtos descontinuados.
- A **COMPETHICS IT SOLUÇÕES EM TECNOLOGIA DA INFORMAÇÃO LTDA** está autorizada a comercializar os equipamentos propostos para esse certame.

Eldorado do Sul, 28 de agosto de 2025

DELL COMPUTADORES DO BRASIL
LTDA:72381189000110

Digitally signed by DELL
COMPUTADORES DO BRASIL
LTDA:72381189000110
Date: 2025.08.28 16:39:46 -03'00'

Dell Computadores do Brasil Ltda
Juliane Casagrande Rodrigues – Gerente de Vendas

Esta declaração é válida pelo prazo de 90 (noventa dias) da sua emissão.

DELL Computadores do Brasil Ltda.
Av. Industrial Belgraf, 400 . Eldorado do Sul / RS . Geral : 51 3481 5500 Fax : 51 3481 5458

ANEXO VII – DECLARAÇÃO DE QUALIFICAÇÃO TÉCNICA

A

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

REF.: PREGÃO ELETRÔNICO Nº 46/2025

PROPOSTA N.º 242/25

Declaro, sob as penas da lei, para fins de participação na LICITAÇÃO ELETRÔNICA 46/25, que a empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA dispõe do aparelhamento técnico adequado e necessário para a realização do objeto a que se refere esta licitação, e que tomei conhecimento de todas as informações e das condições para o cumprimento das obrigações objeto da licitação, bem como comunicarei qualquer fato ou evento superveniente à entrega dos documentos de habilitação, que venha alterar a atual situação da empresa relativamente à sua capacidade técnica.

Porto Alegre, 29 de agosto de 2025.

RAFAELLA TAVARES
BARCELOS:0179212
2063

Assinado de forma
digital por RAFAELLA
TAVARES
BARCELOS:01792122063

RAFAELLA TAVARES BARCELOS
CPF: 017.921.220-63 | RG: 2115897908



Eldorado do Sul, 28 de agosto de 2025

À

COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA
A/C Sr. RAFAELLA TAVARES BARCELOS

Ref.: COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE –
PROCEMPA – LICITAÇÃO ELETRÔNICA Nº 046/2025

DECLARAÇÃO TÉCNICA

DELL COMPUTADORES DO BRASIL LTDA. (“Dell”), inscrita no CNPJ/MF sob o nº 72.381.189/0001-10, com sede na Av. Industrial Belgraf, 400 – Medianeira – CEP 92990-000, Eldorado do Sul/RS, com o objetivo de complementar as informações que não constam no Catálogo Técnico Oficial do(s) produto(s) abaixo ofertado(s), vem, através da presente, declarar o que segue:

Objeto: **Servidor Dell PowerEdge R760**

- Os equipamentos fornecidos são novos, integrados de fábrica, projetado para uso corporativo, sendo modelo disponível em linha de fabricação do fabricante Dell;
- O equipamento possui BIOS (UEFI) do mesmo fabricante, o qual detém direitos de copyright sobre essa BIOS.

DELL COMPUTADORES DO BRASIL
LTDA:72381189000110

Digitally signed by DELL
COMPUTADORES DO BRASIL
LTDA:72381189000110
Date: 2025.08.28 16:40:36 -03'00'

Dell Computadores do Brasil Ltda

Juliane Casagrande Rodrigues – Gerente de Vendas

Esta declaração é válida pelo prazo de 90 (noventa dias) da sua emissão.

DELL Computadores do Brasil Ltda.
Av. Industrial Belgraf, 400 . Eldorado do Sul / RS . Geral : 51 3481 5500 Fax : 51 3481 5458



Declaração de Informações Socioeconômicas e Fiscais(DEFIS)

Declaração Original

Exercício 2025

Ano-Calendário 2024

Período abrangido pela Declaração: 01/01/2024 a 31/12/2024

1. Identificação do Contribuinte

CNPJ Matriz: 28.452.362/0001-32
Nome empresarial: COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA
Data de abertura no CNPJ: 17/08/2017
Regime de Apuração: competência
Optante pelo Simples Nacional: Sim

1.1 CNPJ das Filiais Presentes nesta declaração:

Nenhuma.

2. Informações Econômico-Fiscais da Pessoa Jurídica

Ganhos de capital	R\$ 0,00
Quantidade de empregados no início do período abrangido pela declaração	0
Quantidade de empregados no final do período abrangido pela declaração	0
Receita proveniente de exportação direta	R\$ 0,00
Lucro superior ao limite de que trata o § 1º do art. 6º da resolução CGSN nº 4 de 30/05/2007, no período abrangido por esta declaração	R\$ 0,00
Total de ganhos líquidos auferidos em operações de renda variável	R\$ 36.405,24

2.1 Receita proveniente de exportação por meio de comercial exportadora

CNPJ da comercial exportadora	Valor
-	-

2.2 Identificação e Rendimentos dos Sócios

CPF do sócio: 017.921.220-63

Nome: RAFAELLA TAVARES BARCELOS

Rendimentos isentos pagos ao sócio pela empresa	R\$ 0,00
Rendimentos tributáveis pagos ao sócio pela empresa	R\$ 16.944,00
Percentual de participação do sócio no capital social da empresa no	100,00%

último dia do período abrangido pela declaração

Imposto de renda retido na fonte sobre os rendimentos pagos ao sócio
pela ME/EPP R\$ 0,00

2.3 Percentual de participação em cotas em tesouraria no capital social da empresa (%) 0,00%

2.4 Doações à Campanha Eleitoral

CNPJ do Beneficiário	Nome do Beneficiário	Tipo de Beneficiário	Forma de Doação	Valor
-	-	-	-	-

3. Informações Econômicas e Fiscais dos Estabelecimentos

Estabelecimento: 28.452.362/0001-32 UF: RS

Estoque inicial do período abrangido pela declaração	R\$ 0,00
Estoque final do período abrangido pela declaração	R\$ 46.346,56
Saldo em caixa/banco no início do período abrangido pela declaração	R\$ 412.011,98
Saldo em caixa/banco no final do período abrangido pela declaração	R\$ 593.296,66
Total de aquisições de mercadorias para comercialização ou industrialização no período abrangido pela declaração	R\$ 187.967,63
Aquisições no mercado interno	R\$ 187.967,63
Importações	R\$ 0,00
Total de entradas de mercadorias por transferência para comercialização ou industrialização no período abrangido pela declaração	R\$ 0,00
Total de saídas de mercadorias por transferência para comercialização ou industrialização no período abrangido pela declaração	R\$ 242.012,00
Total de devoluções de vendas de mercadorias para comercialização ou industrialização no período abrangido pela declaração	R\$ 0,00
Total de devoluções de compras de mercadorias para comercialização ou industrialização no período abrangido pela declaração	R\$ 0,00
Total de entradas no período abrangido pela declaração	R\$ 187.967,63
Total de despesas no período abrangido pela declaração	R\$ 30.095,56

Total de entradas interestaduais por UF

UF	Valor
SP	R\$ 187.126,03
DF	R\$ 841,60

Total de saídas interestaduais por UF

UF	Valor
-	-

Valor do ISS retido na fonte no ano-calendário, por Município

UF	Município	Valor
-	-	-

Prestações de Serviços de Comunicação

UF onde o serviço foi prestado	Município onde o serviço foi prestado	Valor
-	-	-

Informações sobre prestação de serviços de transporte de cargas interestadual e/ou intermunicipal, e de transporte intermunicipal e interestadual de passageiros autorizados no inciso VI do art. 17 da LC 123 com e sem substituição tributária

Valor total do frete:	-	
UF de origem	Município onde se iniciou a prestação do serviço	Valor da Prestação (R\$)
-	-	-

4. Informações da Recepção da Declaração

Data e Horário da transmissão da Declaração: 17/03/2025 10:08:22

Número do Recibo: 02.07.25076.0146694-0

Autenticação: 28178.45018.23358.62430

ANEXO III – DECLARAÇÃO CONJUNTA

A

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

REF.: PREGÃO ELETRÔNICO Nº 46/2025

PROPOSTA N.º 242/25

Prezados,

A Proponente DECLARA, de acordo com o art. 38, I a VIII, da Lei 13.303/2016 e, sob as penas da Lei, para fins de participação na LICITAÇÃO ELETRÔNICA 46/25, que:

1. Não possui administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social que seja diretor ou empregado da empresa pública ou sociedade de economia mista contratante;

2. Não se encontra suspensa pela empresa pública ou sociedade de economia mista;

3. Não foi declarada inidônea pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada a empresa pública ou sociedade de economia mista, enquanto perdurarem os efeitos da sanção;

4. Não é constituída por sócio de empresa suspensa, impedida ou declarada inidônea;

5. Não possui administrador que seja sócio de empresa suspensa, impedida ou declarada inidônea;

6. Não é constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

7. Não possui administrador que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

8. Não possui, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

9. Não possui, nos seus quadros de diretoria, pessoa que tenha relação de parentesco, até o terceiro grau civil, com:

a) dirigente ou empregado da PROCEMPA cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

b) autoridade do ente público a que a PROCEMPA esteja vinculada.

10. Não é constituída por sócio ou administrador que tenha terminado seu prazo de gestão ou rompido seu vínculo com a PROCEMPA há menos de 6 (seis) meses.

DECLARA que não realizou doação em dinheiro, ou bem estimável em dinheiro, para partido político ou campanha eleitoral de candidato a cargo eletivo, a contar do dia 02 de outubro de 2015.

DECLARA que não está sob efeito de uma Declaração de Inidoneidade para contratar com a Administração Direta ou Indireta do Município, bem como que comunicará qualquer fato ou evento superveniente à entrega dos documentos da habilitação que venha alterar a atual situação quanto à capacidade jurídica, técnica, regularidade fiscal e idoneidade econômico-financeira.

DECLARA, cumprindo o disposto no inciso XXXIII, art. 7º, da Constituição Federal, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos, assim como assume o compromisso de declarar a superveniência de qualquer fato impeditivo à sua habilitação.

Por ser a expressão da verdade, assumindo inteira responsabilidade pela declaração acima sob as penas da lei, assino para que produza seus efeitos legais.

Porto Alegre, 29 de agosto de 2025.

RAFAELLA TAVARES
BARCELOS:0179212
2063

Assinado de forma
digital por RAFAELLA
TAVARES
BARCELOS:01792122063

RAFAELLA TAVARES BARCELOS

CPF: 017.921.220-63 | RG: 2115897908

comercial@compethics.com.br

Av. Ipiranga, 2642 | Petrópolis | Porto Alegre | RS | Brasil | CEP 90610-000 | (51) 3342-3732

ANEXO IV – DECLARAÇÃO DE VERACIDADE DOS DOCUMENTOS JUNTADOS

A

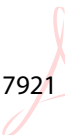
COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

REF.: PREGÃO ELETRÔNICO Nº 46/2025

PROPOSTA N.º 242/25

Eu, RAFAELLA TAVARES BARCELOS, inscrito no CPF sob o nº 017.921.220-63, representante legal da empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, declaro, sob as penas da lei, para fins de participação na LICITAÇÃO ELETRÔNICA 46/25, que todos os documentos apresentados são verdadeiros e que as cópias reproduzem fielmente os originais, responsabilizando-me pessoalmente, nas esferas cível, administrativa e criminal, pela veracidade desta declaração.

Porto Alegre, 29 de agosto de 2025.

RAFAELLA		Assinado de forma
TAVARES		digital por RAFAELLA
BARCELOS:017921		TAVARES
22063		BARCELOS:0179212206 3

RAFAELLA TAVARES BARCELOS

CPF: 017.921.220-63 | RG: 2115897908

ANEXO V – DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

A

COMPANHIA DE PROCESSAMENTO DE DADOS DO MUNICÍPIO DE PORTO ALEGRE – PROCEMPA

REF.: PREGÃO ELETRÔNICO Nº 46/2025

PROPOSTA N.º 242/25

A empresa COMPETHICS IT SOLUCOES EM TECNOLOGIA DA INFORMACAO LTDA, inscrita no CNPJ sob o nº 28.452.362/0001-32, por intermédio de seu representante legal, RAFAELLA TAVARES BARCELOS, CPF nº 017.921.220-63, Carteira de Identidade nº 2115897908, declara, sob as penas da lei, para fins de participação na LICITAÇÃO ELETRÔNICA 46/25, que é considerada:

(X) microempresa, conforme o artigo 3º, I, da Lei Complementar nº 123/2006 e o regulamento consubstanciado no Decreto nº 8.538/2015.

() empresa de pequeno porte, conforme o artigo 3º, II, da Lei Complementar nº 123/2006 e o regulamento consubstanciado no Decreto nº 8.538/2015.

Declara, ainda, que a empresa está excluída das vedações constantes no artigo 3º, § 4º, da Lei Complementar nº 123/2006 e no Decreto nº 8.538/2015.

Por fim, a empresa declara que, na hipótese de ser proclamada vencedora do certame, promoverá a regularização de eventuais defeitos ou restrições existentes na documentação exigida para efeito de regularidade fiscal.

Porto Alegre, 29 de agosto de 2025.

RAFAELLA TAVARES Assinado de forma
BARCELOS:0179212 digital por RAFAELLA
2063 TAVARES
BARCELOS:01792122063

RAFAELLA TAVARES BARCELOS

CPF: 017.921.220-63 | RG: 2115897908



Dell PowerEdge R760

The Dell PowerEdge R760 offers powerful performance in a purpose- built, cyber resilient, mainstream server.

Overview

Certifications

Learn about Red Hat Certification



Compare	Product	Level	
☐	Red Hat OpenStack Services on OpenShift 18.0 - 18.x Base OS: Red Hat Enterprise Linux 9.0 Architecture: x86_64	Certified	View features
☐	Red Hat OpenStack Platform 17.0 - 17.x Base OS: Red Hat Enterprise Linux 9.0 Architecture: x86_64	Certified	View features
☐	Red Hat Enterprise Linux 10.0 - 10.x Architecture: x86_64	Certified	View features
☐	Red Hat Enterprise Linux 9.0 - 9.x Architecture: x86_64	Certified	View features
☐	Red Hat Enterprise Linux for Real Time 9.0 - 9.x Architecture: x86_64	Certified	View features
☐	Red Hat Enterprise Linux for Real Time 8.6 - 8.x Base OS: Red Hat Enterprise Linux 8.6 Architecture: x86_64	Certified	View features
☐	Red Hat Enterprise Linux 8.6 - 8.x Architecture: x86_64	Certified	View features

Compare	Product	Level
☐	Red Hat OpenShift Container Platform 4.13 - 4.x Base OS: Red Hat Enterprise Linux 9.0 Architecture: x86_64	Certified View features
☐	Red Hat OpenShift Container Platform 4.11 - 4.12 Base OS: Red Hat Enterprise Linux 8.6 Architecture: x86_64	Certified View features
☐	Red Hat Virtualization 4.4 - 4.x Base OS: Red Hat Enterprise Linux 8.6	Certified View features
Provided by Dell Technologies Type System Form factor Server Works with Red Hat OpenShift Container Platform Red Hat OpenStack Services on OpenShift Red Hat Enterprise Linux Red Hat OpenStack Platform		

Contact

Product specs



in

Platforms

Products & services

Try, buy, sell

Help

About Red Hat Ecosystem Catalog

The Red Hat Ecosystem Catalog is the official source for discovering and learning more about the Red Hat Ecosystem of both Red Hat and certified third-party products and services.

We're the world's leading provider of enterprise open source solutions—including Linux, cloud, container, and Kubernetes. We deliver hardened solutions that make it easier for enterprises to work across platforms and environments, from the core datacenter to the network edge.



- [Jobs](#)
- [Events](#)
- [Locations](#)
- [Contact Red Hat](#)
- [Red Hat Blog](#)
- [Inclusion at Red Hat](#)
- [Cool Stuff Store](#)
- [Red Hat Summit](#)

-
- [© 2025 Red Hat, Inc.](#)
 - [Privacy statement](#)
 - [Terms of use](#)
 - [All Policies and guidelines](#)
 - [Digital accessibility](#)
 - [Cookie preferences](#)

Your submission was sent successfully! [Close](#)

Thank you for contacting us. A member of our team will be in touch shortly. [Close](#)

You have successfully unsubscribed! [Close](#)

Thank you for signing up for our newsletter!

In these regular emails you will find the latest updates about Ubuntu and upcoming events where you can meet our team. [Close](#)

Your preferences have been successfully updated. [Close notification](#)

Please try again or [file a bug report](#).

https://github.com/canonical/ubuntu.com/issues/new?template=ISSUE_TEMPLATE.yaml > [Close](#)

[servers](#) > [PowerEdge R760](#) > **PowerEdge R760 (Emerald Rapids)**

Dell Technologies PowerEdge R760 (Emerald Rapids)

Server system certified with Ubuntu

Ubuntu 22.04 LTS

The Dell Technologies PowerEdge R760 (Emerald Rapids) with the components described below has been awarded the status of certified for Ubuntu.

[Download](#) <<https://ubuntu.com/download/server/>>

Kernel	5.15.0-89-generic

BIOS	Dell Inc.: 2.0.0 (UEFI)

Hardware

Processor	• Intel Corp. INTEL(R) XEON(R) PLATINUM 8592+ • Intel Corp. INTEL(R) XEON(R) PLATINUM 8592+
Network	• Broadcom Corp. NetXtreme BCM5720 2-port Gigabit Ethernet PCIe pci (14e4:165f 1028:0a6b) • Broadcom Corp. NetXtreme BCM5720 2-port Gigabit Ethernet PCIe pci (14e4:165f 1028:0a6b)
Video	• Matrox Electronics Systems Ltd. Integrated Matrox G200eW3 Graphics Controller pci (102b:0536 1028:0a6b)

[All hardware details >](#)

[1 more certified configuration in the PowerEdge R760 platform >](#)

Issues? Let us know

If there is an issue with the information for this system, [please let us know](https://answers.launchpad.net/ubuntu-certification/+addquestion?field.title=Feedback+on+the+Dell+Technologies+PowerEdge+R760+(Emerald+Rapids).+202312-33292) [<https://answers.launchpad.net/ubuntu-certification/+addquestion?field.title=Feedback on the Dell Technologies PowerEdge R760 \(Emerald Rapids\) \(202312-33292\)>](https://answers.launchpad.net/ubuntu-certification/+addquestion?field.title=Feedback+on+the+Dell+Technologies+PowerEdge+R760+(Emerald+Rapids).+202312-33292).