Dell PowerEdge XR4000w

Installation and Service Manual

Regulatory Model: E05X
Regulatory Type: E05X001
June 2023
Rev. A01

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.**

Contents

1

About this document

This document provides an overview about the system, information about installing and replacing components, diagnostic tools, and guidelines to be followed while installing certain components.

2

Dell PowerEdge XR4000w system configurations and features

The PowerEdge XR4000w system is a Witness sled with a chassis fan that is managed by the chassis manager and that supports:

- One Intel Atom C3508 processor with 4 cores
- 16 GB DDR4 1866 MT/s ECC RAM (soldered down)
- 1 x M.2 NVMe SSD (2280)

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Topics:

System configurations - front view for PowerEdge XR4000w

Figure 1. Front view of the witness sled

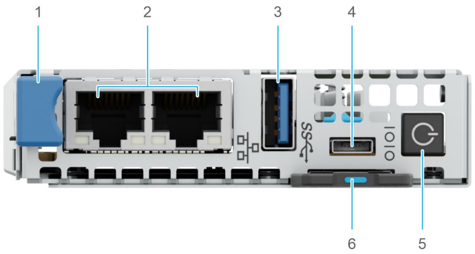


Table 1. Front view of the witness sled

Item	Ports, panels, or slots	Icon	Description
1	Pull handle	N/A	Enables you to remove the witness sled from the chassis.
2	Network Interface Controller (NIC) ports	🖧	The NIC ports that are integrated on the system board provide network connectivity.
3	USB 3.0 port	SS⭠	This port is USB 3.0-compliant.
4	Micro-USB connector	N/A	The micro-USB connector for the system console.
5	Sled power button	N/A	Enables you to power on the sled.

Table 1. Front view of the witness sled (continued)

Item	Ports, panels, or slots	Icon	Description
6	Information tag	N/A	The Information tag is a slide-out label panel that contains one MAC address and EST.

System configurations - inside view for PowerEdge XR4000w

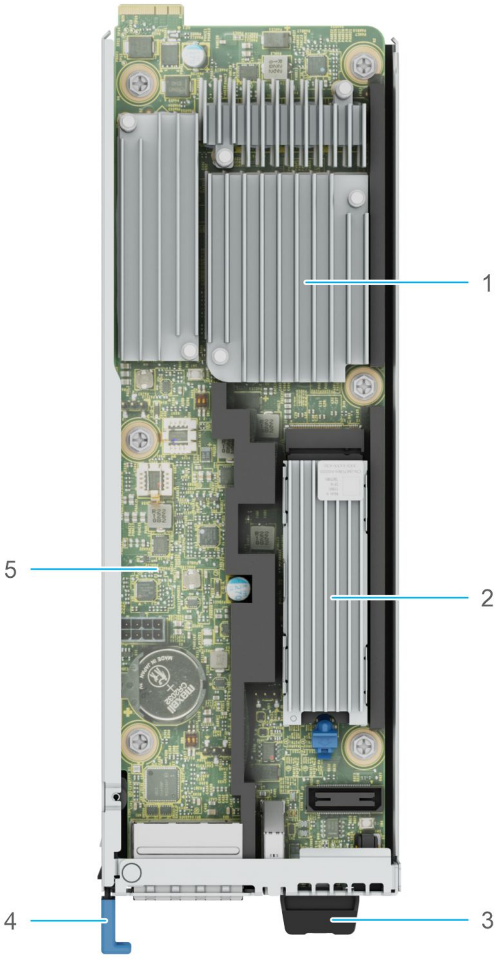


Figure 2. Inside the system -XR4000w

1. Processor and heat sink
2. M.2 SSD module
3. Information tag
4. Pull handle
5. System board

Locating the Express Service Code and Service Tag

The unique Express Service Code and Service Tag are used to identify the system.

The information tag is on the rear of the system that includes system information such as MAC address, Express Service Tag label.

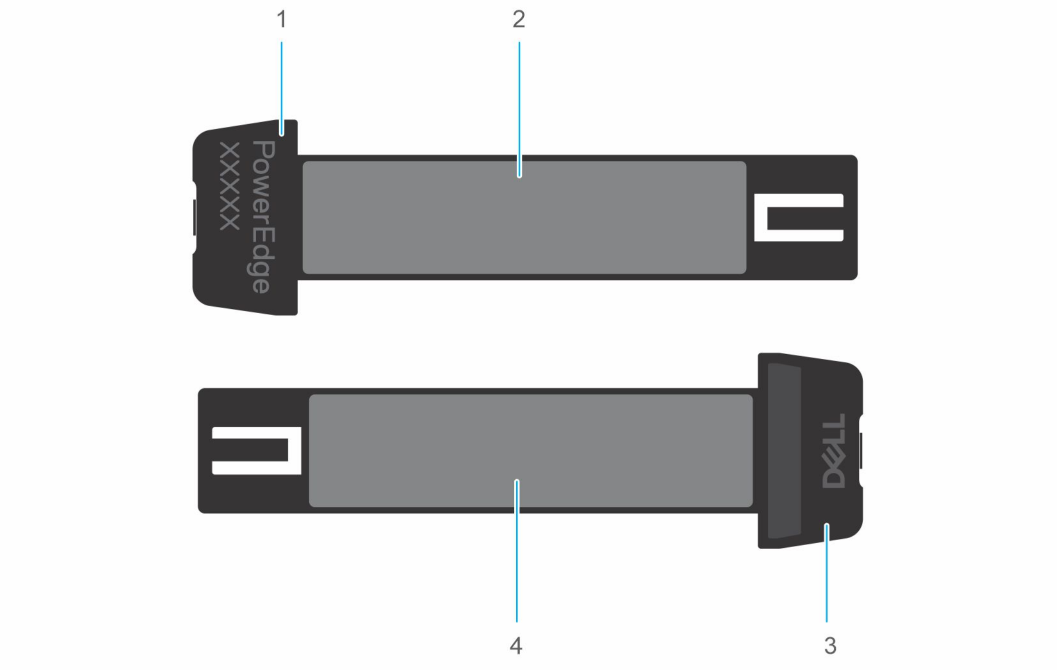


Figure 3. Locating the Service Tag of your system

1. Information tag (bottom view)
2. MAC address information label
3. Information tag (top view)
4. Express Service Tag label

Technical specifications

The technical and environmental specifications of your system are outlined in this section.

Topics:

Sled dimensions

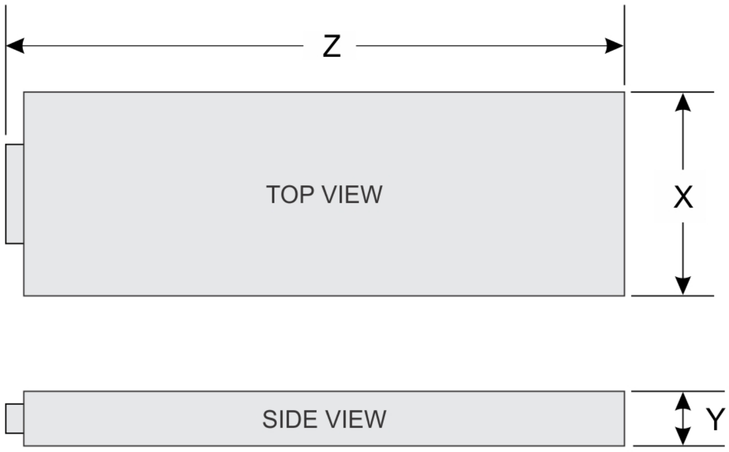


Figure 4. Sled dimensions

Table 2. PowerEdge XR4000w sled dimensions

X	Y	Z
83.25 mm (3.27 inches)	21.60 mm (0.85 inches)	250.79 mm (9.87 inches)

System weight

Table 3. PowerEdge XR4000w system weight

System configuration	Maximum weight
1 x M.2 SSD (2280)	0.44 kg (0.97 pound)

Processor specifications

Table 4. PowerEdge XR4000w processor specifications

Supported processor	Number of processors supported
Intel Atom C3508 processor with 4 cores	One

Supported operating systems

The PowerEdge XR4000w system supports the following operating systems:

- VMware ESXi

For more information, go to www.dell.com/ossupport.

Memory specifications

The PowerEdge XR4000w system supports 16 GB DDR4 ECC RAM (soldered down).

Storage specifications

The PowerEdge XR4000w system supports 1 x M.2 SSD of 960 GB (2280) storage pre-installed with ESXi boot image and application data.

Ports and connectors specifications

USB ports specifications

The PowerEdge XR4000w system supports one USB 3.0-compliant port on the front of the system.

NIC port specifications

The PowerEdge XR4000w system supports 1 GbE x 2 (intel I210), RJ45 ports with LEDs on the front of the system.

Serial connector specifications

The PowerEdge XR4000w system supports one Micro-USB connector for RS232 serial port, which is a Micro USB on the front of the system.

Environmental specifications

NOTE: For additional information about environmental certifications, refer to the *Product Environmental Datasheet* located with the *Documentation* on www.dell.com/support/home.

Table 5. Operating and non-operating temperature considerations

Description	Temperature range
Operating temperature range for rear air-flow (RAF) configuration	-5 to <55°C with a startup temperature of 0°C

Table 5. Operating and non-operating temperature considerations (continued)

Description	Temperature range
Ambient temperature for rear air-fllow (RAF) and normal air-flow (NAF) with GPU	45°C
Non-operating temperature range	-40 to 85°C

Environmental Considerations

The PowerEdge XR4000w system is targeted for edge deployments and it meets all the additional standards for thermal, shock, vibration parameters.

Table 6. Environmental considerations

Industry	Configuration	Description
Telco	GR-1089-CORE	Electromagnetic Compatibility and Electrical Safety – Generic Criteria for Network Telecommunications Equipment
	GR-63-CORE	NEBS Requirements: Physical Protection
	SR-3580 (NEBS Level 3)	NEBS Criteria Levels
	GR-3108-CORE (Class 1)	Network Equipment in the Outside Plant (OSP). An exception is made for cold boot at 0C instead of -5C.
Military	MILSTD 810H	Environmental engineering considerations and laboratory test
	MILSTD 461G///	Requirements for the control of electromagnetic interference characteristic of subsystems and equipment
	MILSTD 901E	High impact shock test – Shipboard
	MILSTD 1474E	Department of Defense Design Criteria Standard Noise Limits
Marine	IEC-60945	Maritime navigation and radiocommunication equipment and systems – General requirements
	DNV-GL	Environmental Test Specification for Instrumentation and Automation Equipment
Power Industry	IEEE 1613	Environmental and testing requirements for communications networking devices in electric power substations
	IEC – 61850-3	Communication networks and systems for power utility automation
Safety	NA	LDV, IEC/EN, CFR, CSA
EMC	NA	EN, CISPR, ES, DTAG, CFR, ICES, VCCI
EMV	NA	RoHS, WEEE, EN, ECE

Thermal restriction matrix

Table 7. M.2 Support Thermal Limitation for XR4000r Chassis (RAF Configurations)

M.2 Type	M.2 Module (Witness Sled)		
	Edge 2 (Max 55°C)	Edge 1 (Max 50°C)	ASHRAE A4 (Max 45°C)
Micron 480GB	No	No	No
Micron 800GB	No	No	No
Micron 960GB	Yes	Yes	Yes
Micron 1.92TB	No	No	No
Micron 3.84TB	No	No	No
Hynix 480GB	No	No	No
Hynix 800GB	No	No	No
Hynix 960GB	Yes	Yes	Yes
Hynix 1.92TB	No	No	No
Hynix 3.84BT	No	No	No

Table 8. M.2 Support Thermal Limitation for XR4000z Chassis (RAF Configurations)

M.2 Type	M.2 Module (Witness Sled)		
	Edge 2 (Max 55°C)	Edge 1 (Max 50°C)	ASHRAE A4 (Max 45°C)
Micron 480GB	No	No	No
Micron 800GB	No	No	No
Micron 960GB	Yes	Yes	Yes
Micron 1.92TB	No	No	No
Micron 3.84TB	No	No	No
Hynix 480GB	No	No	No
Hynix 800GB	No	No	No
Hynix 960GB	Yes	Yes	Yes
Hynix 1.92TB	No	No	No
Hynix 3.84BT	No	No	No

Table 9. XR4000w Processor Support Thermal Limitation for XR4000r chassis (RAF Configurations)

Processor Type	HSK type	Fan type	XR4000 RAF Configurations		
			Edge 2 (Max 55°C)	Edge 1 (Max 50°C)	ASHRAE A4 (Max 45°C)
Intel Atom C3508, 4 cores, 11.5W	Aluminum extrusion	Fan	Yes	Yes	Yes

Table 10. XR4000w Processor Support Thermal Limitation for XR4000z chassis (RAF Configurations)

Processor Type	HSK type	Fan type	XR4000 RAF Configurations		
			Edge 2 (Max 55°C)	Edge 1 (Max 50°C)	ASHRAE A4 (Max 45°C)
Intel Atom C3508, 4 cores, 11.5W	Aluminum extrusion	Fan	Yes	Yes	Yes

Table 11. M.2 Support Thermal Limitation for XR4000z Chassis (NAF Configurations)

M.2 Type	M.2 Module (Witness Sled)		
	Edge 2 (Max 55°C)	Edge 1 (Max 50°C)	ASHRAE A4 (Max 45°C)
Micron 480GB	No	No	No
Micron 800GB	No	No	No
Micron 960GB	Not Supported	Not Supported	Yes
Micron 1.92TB	No	No	No
Micron 3.84TB	No	No	No
Hynix 480GB	No	No	No
Hynix 800GB	No	No	No
Hynix 960GB	Not Supported	Not Supported	Yes
Hynix 1.92TB	No	No	No
Hynix 3.84BT	No	No	No

Table 12. XR4000w Processor Support Thermal Limitation for XR4000r chassis (NAF Configurations)

Processor Type	HSK type	Fan type	NAF Configurations		
			Edge 2 (Max 55°C)	Edge 1 (Max 50°C)	ASHRAE A4 (Max 45°C)
Intel Atom C3508, 4 cores, 11.5W	Aluminum extrusion	Fan	Not Supported		Yes

Thermal Restrictions

ASHRAE A4 Support Restriction for RAF (Reverse Air Flow Direction) Configurations

- In redundant mode, two power supplies are required. A single power supply failure is not supported.

Edge1 Support Restriction RAF (Reverse Air Flow Direction) Configurations

- In redundant mode, two power supplies are required. A single power supply failure is not supported.

Edge2 Support Restriction RAF (Reverse Air Flow Direction) Configurations

- In redundant mode, two power supplies are required. A single power supply failure is not supported.

ASHRAE A4 Support Restriction NAF (Normal Air Flow Direction) Configurations

- In redundant mode, two power supplies are required. A single power supply failure is not supported.

4

Initial system setup and configuration

This section describes the tasks for initial setup and configuration of the Dell system. The section also provides general steps to set up the system and the reference guides for detailed information.

Topics:

Pre-operating system management applications

Perform the following steps to set up the system:

Steps

1. Unpack the system.
2. Install the system in the chassis.
3. Power on the chassis.

   > ⓘ **NOTE:** The Witness node does not support any pre-operating system management applications (such as BIOS or iDRAC configuration).

Witness BIOS POST codes

Witness BIOS POST values are reported through the Chassis Manager (CM) and displayed by iDRAC interface that is located on any of the installed XR4510c or XR4520c compute sleds. The XR4000w does not have its own dedicated iDRAC. iDRAC presents these codes in its front-end interfaces such as:

- iDRAC GUI
- Redfish
- RACADM

Other interfaces that provide Witness data:

- CPLD
- IPMI

Table 13. Witness BIOS POST codes

Phase	POST codes	DESCRIPTION
PEI	0x11	Pre-memory CPU initialization is started
PEI	0x15	Pre-memory North Bridge initialization is started
PEI	0x19	Pre-memory South Bridge initialization is started
PEI	0x32	CPU post-memory initialization is started
PEI	0x37	Post-Memory North Bridge initialization is started
PEI	0x3B	Post-Memory South Bridge initialization is started

Table 13. Witness BIOS POST codes (continued)

Phase	POST codes	DESCRIPTION
PEI	0x4F	DXE IPL is started
PEI	0x60	DXE Core is started
DXE	0x61	NVRAM initialization
DXE	0x62	Installation of the South Bridge Runtime Services
DXE	0x68	PCI host bridge initialization
DXE	0x69	North Bridge DXE initialization is started
DXE	0x6A	North Bridge DXE SMM initialization is started
DXE	0x70	South Bridge DXE initialization is started
DXE	0x71	South Bridge DXE SMM initialization is started
DXE	0x78	ACPI module initialization
DXE	0x79	CSM initialization
DXE	0x90	Boot Device Selection (BDS) phase is started
DXE	0x91	Driver connecting is started
DXE	0x92	PCI Bus initialization is started
DXE	0x94	PCI Bus Enumeration
DXE	0x95	PCI Bus Request Resources
DXE	0x96	PCI Bus Assign Resources
DXE	0x97	Console Output devices connect
DXE	0x9A	USB initialization is started
DXE	0x9C	USB Detect
DXE	0x9D	USB Enable
DXE	0XA0	IDE initialization is started
DXE	0xA2	IDE Detect
DXE	0XAD	Ready to Boot event
DXE	0xB4	USB hot plug
DXE	0xC0	No NVMe (M.2) bootable device
DXE	0xD9	Error loading Boot Option (Boot Image failure)

Using the system

Witness serial communication

The Witness server uses a USB to UART method of serial communication accessible using a micro-USB form-factor port on the front panel.

Connecting to Witness using serial

The Witness serial interface can be connected with a USB to micro-USB cable.

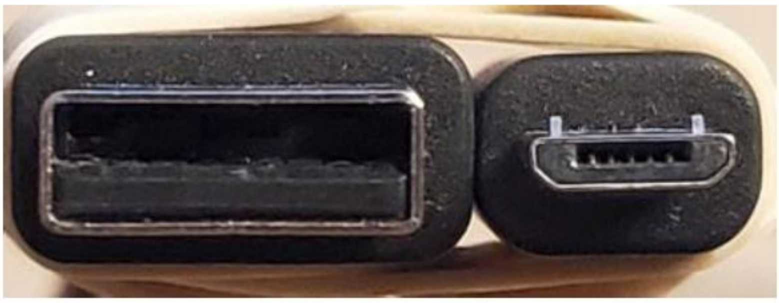


Figure 5. USB (left) to Micro-USB (right) cable

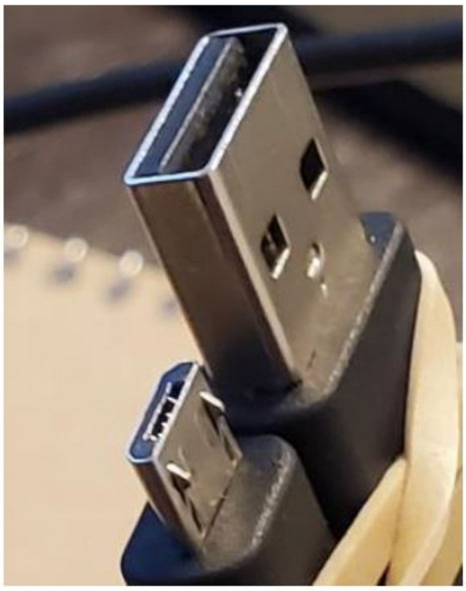


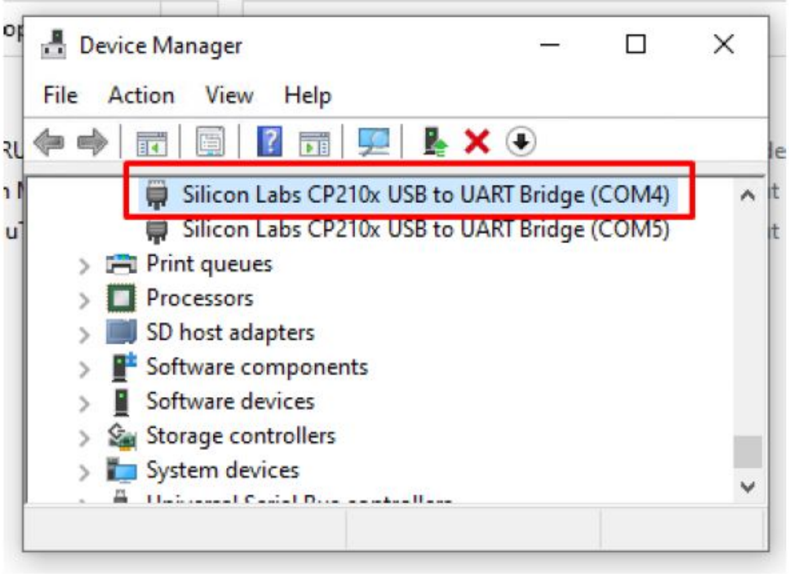
Figure 6. USB (top) to Micro-USB (bottom) cable

The micro-USB end of the cable plugs in to the micro-USB port on the front panel of the Witness. The USB end of the cable plugs into a USB port on the external system that will be communicating with the Witness.

If connecting from a Windows operating system, additional drivers are required to access the UART interface.

- CP210x USB -> UART Bridge VCP Drivers: https://www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers
- Download the CP210x Universal Windows Driver directly: https://www.silabs.com/documents/public/software/CP210x_Universal_Windows_Driver.zip

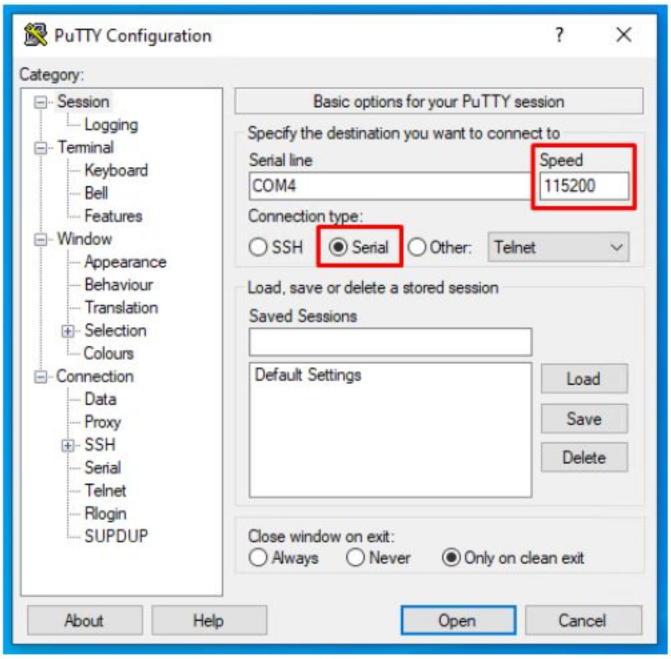
After driver installation, the Witness UART interface should appear to the connecting system once the Witness is powered on.



Silicon Labs CP210x USB to UART Bridge (COM4)
Silicon Labs CP210x USB to UART Bridge (COM5)
Print queues
Processors
SD host adapters
Software components
Software devices
Storage controllers
System devices

Figure 7. USB to UART Bridge device appears when Witness is powered on

The serial interface should then be accessible using serial TTY consoles such as PuTTY. Serial configuration baud rate must be set to 115200. Other settings can be left at their default value.



Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM4

Speed: 115200

Connection type: ○ SSH ● Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 8. PuTTY configuration for Witness serial connection

Witness serial interface

The Witness serial interface allows interaction with the Witness BIOS. See: Pre-operating system management applications for some additional information.

User interfaces: iDRAC

ⓘ **NOTE:** A valid Service Tag must be programmed to the Witness, and the CM must have backed up this tag as part of the Witness Easy Restore (FRU recovery) process. Without a valid Service Tag, the iDRAC will not report all Witness information.

The iDRAC of a compute sled that is connected to the same CM as a Witness node has several methods of interacting with or collecting information from the Witness.

Witness node information, status, and power control interfaces are available through the following compute node interfaces:

- iDRAC GUI
- Redfish
- RACADM

More interfaces that provide some Witness data:

- CPLD
- IPMI

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

User interfaces: iDRAC GUI

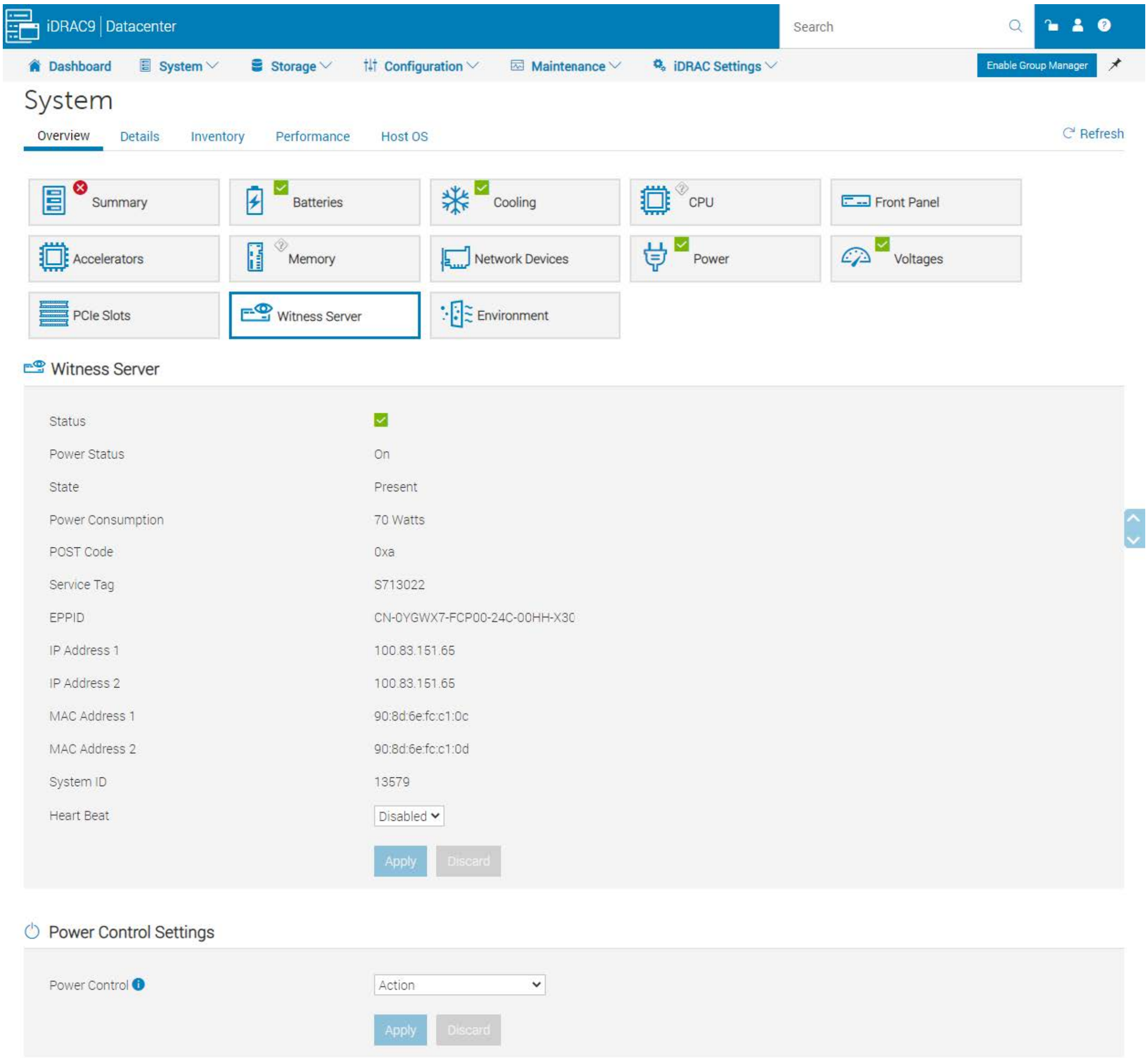
The Witness landing page under System Overview contains the data fields and available options that are gathered from the Chassis Manager (CM) and displayed by iDRAC interface that is located on any of the installed XR4510c or XR4520c compute sleds. The XR4000w does not have its own dedicated iDRAC.

For Witness power operation through the iDRAC user interface, see Witness power operations: iDRAC GUI.

For Witness heartbeat operation through the iDRAC user interface, see Using the Witness Heart Beat function.

The iDRAC user interface Witness Server page:

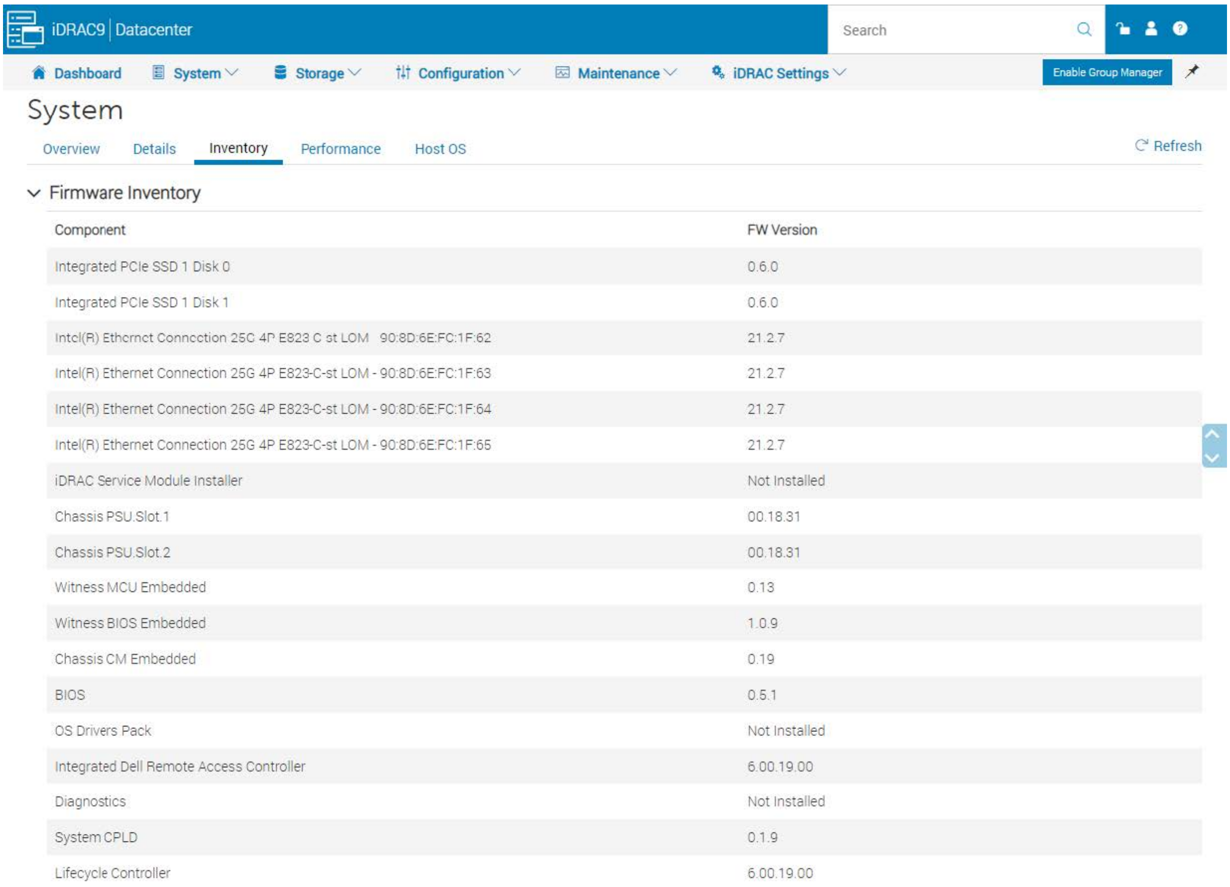
ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.



Status	✓
Power Status	On
State	Present
Power Consumption	70 Watts
POST Code	0xa
Service Tag	S713022
EPPID	CN-0YGWX7-FCP00-24C-00HH-X30
IP Address 1	100.83.151.65
IP Address 2	100.83.151.65
MAC Address 1	90:8d:6e:fc:c1:0c
MAC Address 2	90:8d:6e:fc:c1:0d
System ID	13579
Heart Beat	Disabled

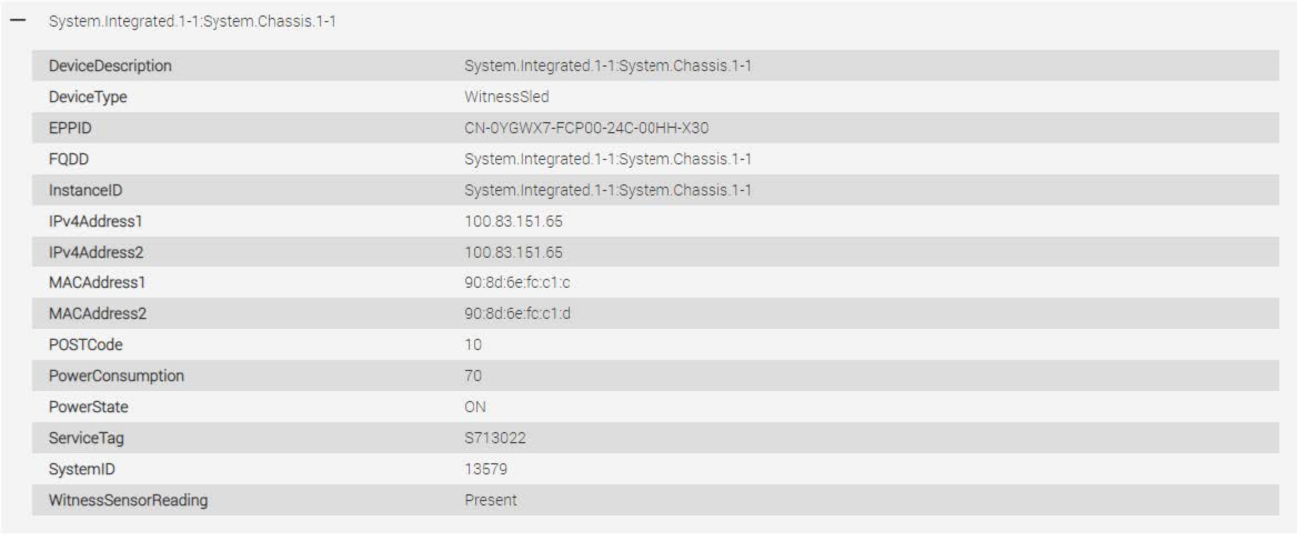
Power Control	Action

Figure 9. iDRAC Witness landing page



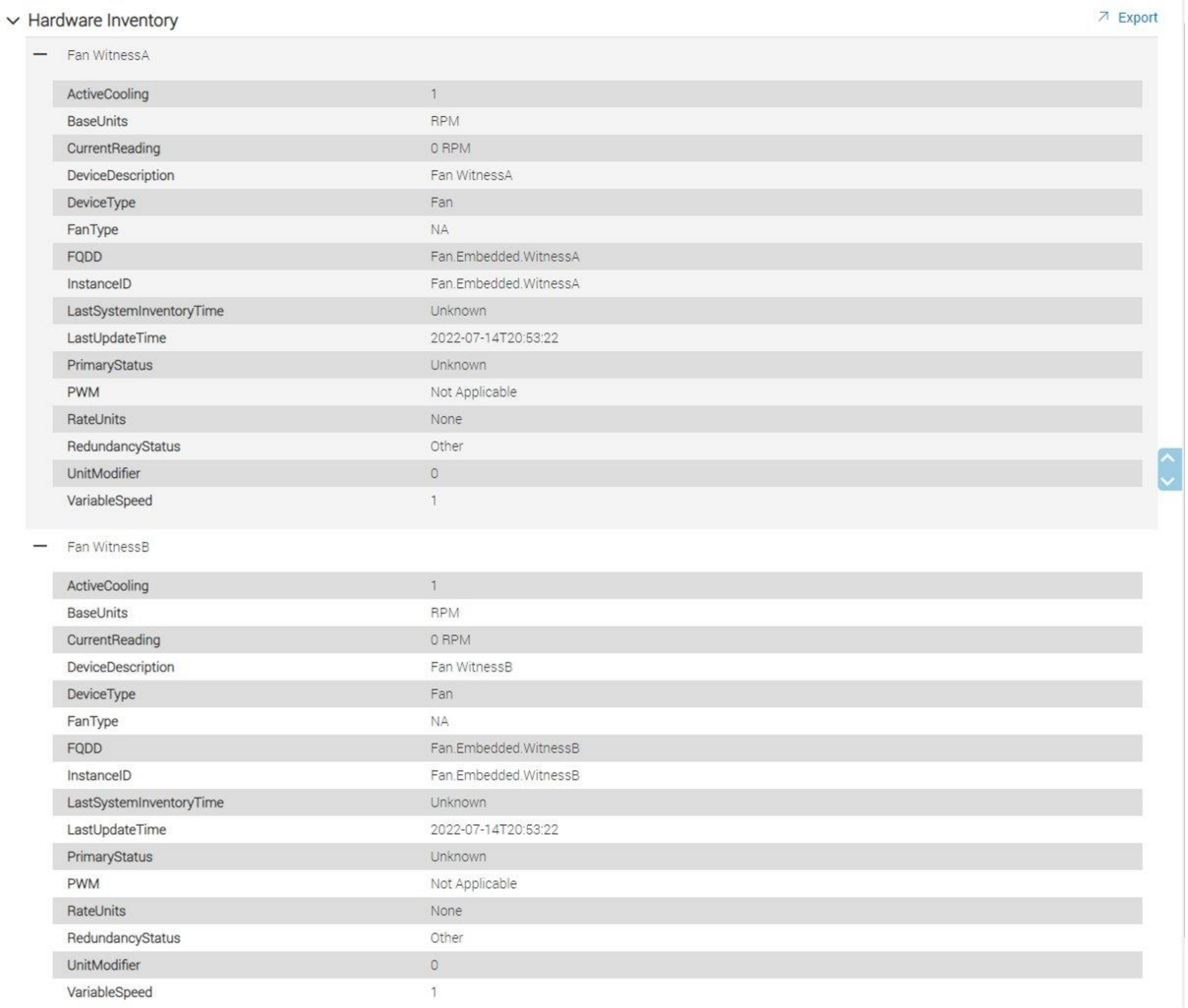
Component	FW Version
Integrated PCIe SSD 1 Disk 0	0.6.0
Integrated PCIe SSD 1 Disk 1	0.6.0
Intcl(R) Ethcrnct Conncction 25C 4P E823 C st LOM 90:8D:6E:FC:1F:62	21.2.7
Intel(R) Ethernet Connection 25G 4P E823-C-st LOM - 90:8D:6E:FC:1F:63	21.2.7
Intel(R) Ethernet Connection 25G 4P E823-C-st LOM - 90:8D:6E:FC:1F:64	21.2.7
Intel(R) Ethernet Connection 25G 4P E823-C-st LOM - 90:8D:6E:FC:1F:65	21.2.7
iDRAC Service Module Installer	Not Installed
Chassis PSU.Slot.1	00.18.31
Chassis PSU.Slot.2	00.18.31
Witness MCU Embedded	0.13
Witness BIOS Embedded	1.0.9
Chassis CM Embedded	0.19
BIOS	0.5.1
OS Drivers Pack	Not Installed
Integrated Dell Remote Access Controller	6.00.19.00
Diagnostics	Not Installed
System CPLD	0.1.9
Lifecycle Controller	6.00.19.00

Figure 10. iDRAC system firmware inventory


System.Integrated.1-1:System.Chassis.1-1

DeviceDescription	System.Integrated.1-1:System.Chassis.1-1
DeviceType	WitnessSled
EPPID	CN-0YGWX7-FCP00-24C-00HH-X30
FQDD	System.Integrated.1-1:System.Chassis.1-1
InstanceID	System.Integrated.1-1:System.Chassis.1-1
IPv4Address1	100.83.151.65
IPv4Address2	100.83.151.65
MACAddress1	90:8d:6e:fc:c1:c
MACAddress2	90:8d:6e:fc:c1:d
POSTCode	10
PowerConsumption	70
PowerState	ON
ServiceTag	S713022
SystemID	13579
WitnessSensorReading	Present

Figure 11. iDRAC system hardware inventory for Witness



Hardware Inventory

Export

Fan WitnessA

ActiveCooling	1
BaseUnits	RPM
CurrentReading	0 RPM
DeviceDescription	Fan WitnessA
DeviceType	Fan
FanType	NA
FQDD	Fan.Embedded.WitnessA
InstanceID	Fan.Embedded.WitnessA
LastSystemInventoryTime	Unknown
LastUpdateTime	2022-07-14T20:53:22
PrimaryStatus	Unknown
PWM	Not Applicable
RateUnits	None
RedundancyStatus	Other
UnitModifier	0
VariableSpeed	1

Fan WitnessB

ActiveCooling	1
BaseUnits	RPM
CurrentReading	0 RPM
DeviceDescription	Fan WitnessB
DeviceType	Fan
FanType	NA
FQDD	Fan.Embedded.WitnessB
InstanceID	Fan.Embedded.WitnessB
LastSystemInventoryTime	Unknown
LastUpdateTime	2022-07-14T20:53:22
PrimaryStatus	Unknown
PWM	Not Applicable
RateUnits	None
RedundancyStatus	Other
UnitModifier	0
VariableSpeed	1

Figure 12. iDRAC hardware inventory for Witness fans

User interfaces: Redfish

For Redfish methods of Witness power control, see: Witness power operations: Redfish.

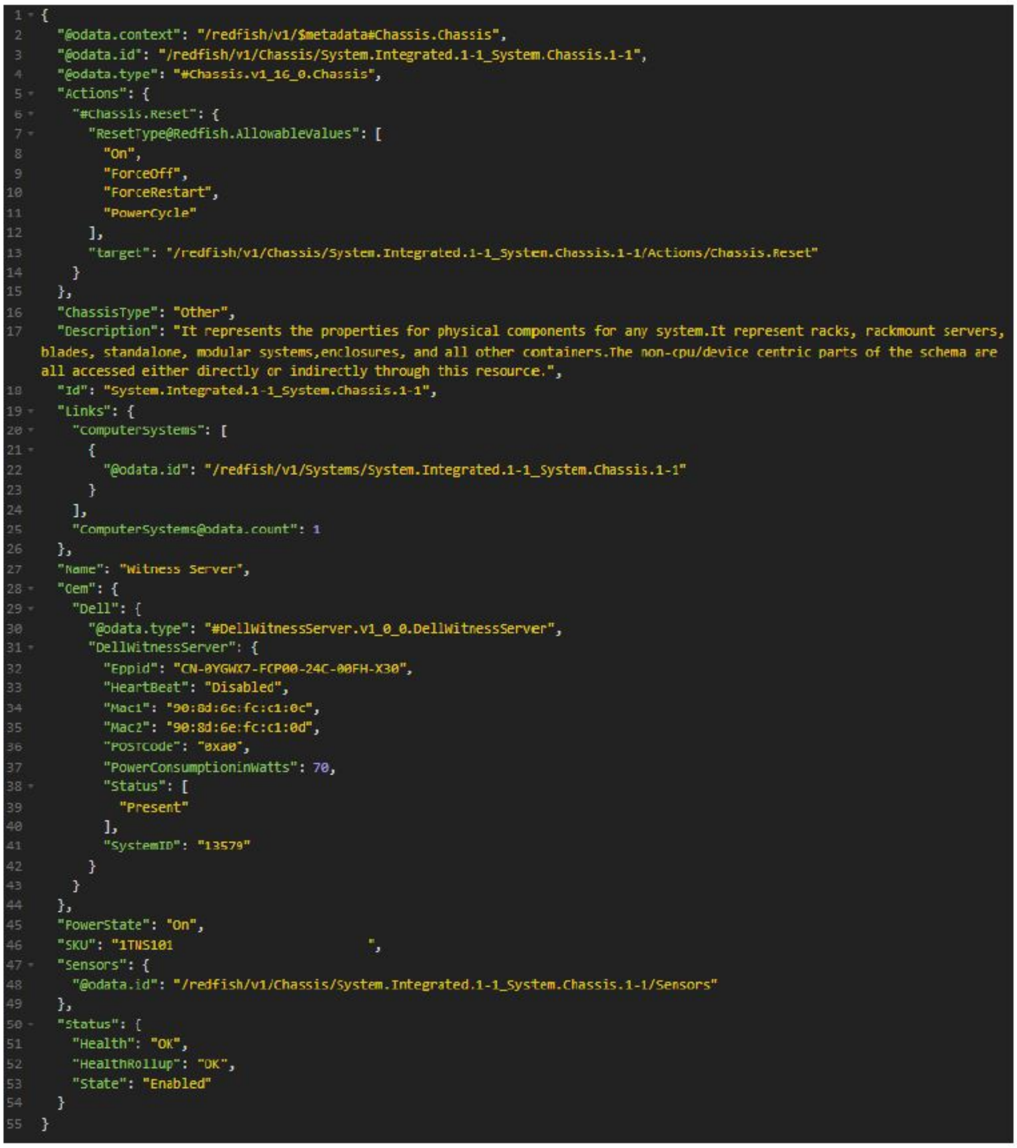
Witness information can be collected through the following URI:

- /redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1

An example of data gathered through this URI.

NOTE: The variables “BMC,” “USER,” and “PASS” are set in this example.

```
root@ubuntu:~# curl --request GET \

--url https://${BMC}/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1 \

--user ${USER}:${PASS}\

--header 'Content-Type: application/json' \

--insecure
```



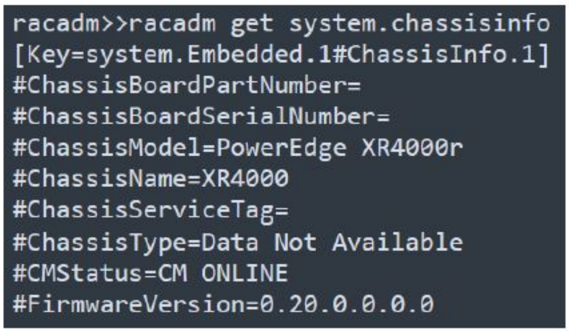
```
{
  "@odata.context": "/redfish/v1/$metadata#Chassis.Chassis",
  "@odata.id": "/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1",
  "@odata.type": "#Chassis.v1_16_0.Chassis",
  "Actions": {
    "#Chassis.Reset": {
      "ResetType@Redfish.AllowableValues": [
        "On",
        "ForceOff",
        "ForceRestart",
        "PowerCycle"
      ],
      "target": "/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1/Actions/Chassis.Reset"
    }
  },
  "ChassisType": "Other",
  "Description": "It represents the properties for physical components for any system.It represent racks, rackmount servers,
blades, standalone, modular systems,enclosures, and all other containers.The non-cpu/device centric parts of the schema are
all accessed either directly or indirectly through this resource.",
  "Id": "System.Integrated.1-1_System.Chassis.1-1",
  "Links": {
    "ComputerSystems": [
      {
        "@odata.id": "/redfish/v1/Systems/System.Integrated.1-1_System.Chassis.1-1"
      }
    ],
    "ComputerSystems@odata.count": 1
  },
  "Name": "Witness Server",
  "Oem": {
    "Dell": {
      "@odata.type": "#DellWitnessServer.v1_0_0.DellWitnessServer",
      "DellWitnessServer": {
        "Eppid": "CN-0YGWX7-FCP00-24C-00FH-X30",
        "HeartBeat": "Disabled",
        "Mac1": "90:8d:6e:fc:c1:0c",
        "Mac2": "90:8d:6e:fc:c1:0d",
        "POSTCode": "0xa0",
        "PowerConsumptioninWatts": 70,
        "Status": [
          "Present"
        ],
        "SystemID": "13579"
      }
    }
  },
  "PowerState": "On",
  "SKU": "1TNS101                         ",
  "Sensors": {
    "@odata.id": "/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1/Sensors"
  },
  "Status": {
    "Health": "OK",
    "HealthRollup": "OK",
    "State": "Enabled"
  }
}
```

Figure 13. Redfish Witness information

User interfaces: RACADM

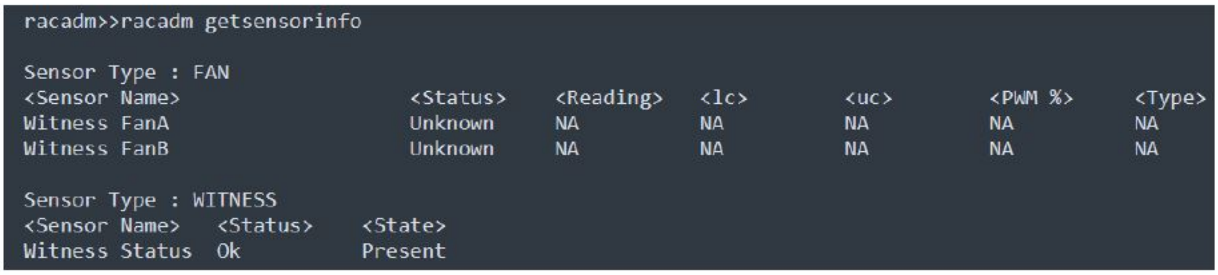
For RACADM methods of Witness power control, see: Witness power operations: RACADM.

Witness and some Chassis Manager information can be found through SW and HW operations with RACADM.



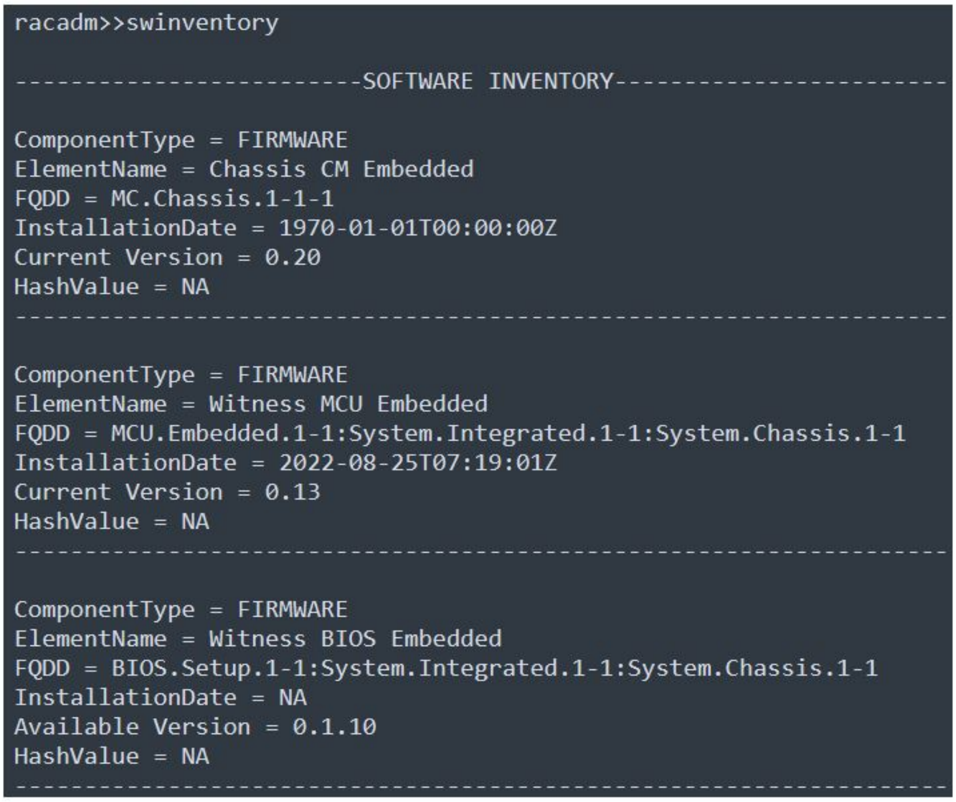
```
racadm>>racadm get system.chassisinfo
[Key=system.Embedded.1#ChassisInfo.1]
#ChassisBoardPartNumber=
#ChassisBoardSerialNumber=
#ChassisModel=PowerEdge XR4000r
#ChassisName=XR4000
#ChassisServiceTag=
#ChassisType=Data Not Available
#CMStatus=CM ONLINE
#FirmwareVersion=0.20.0.0.0.0
```

Figure 14. RACADM system chassis info



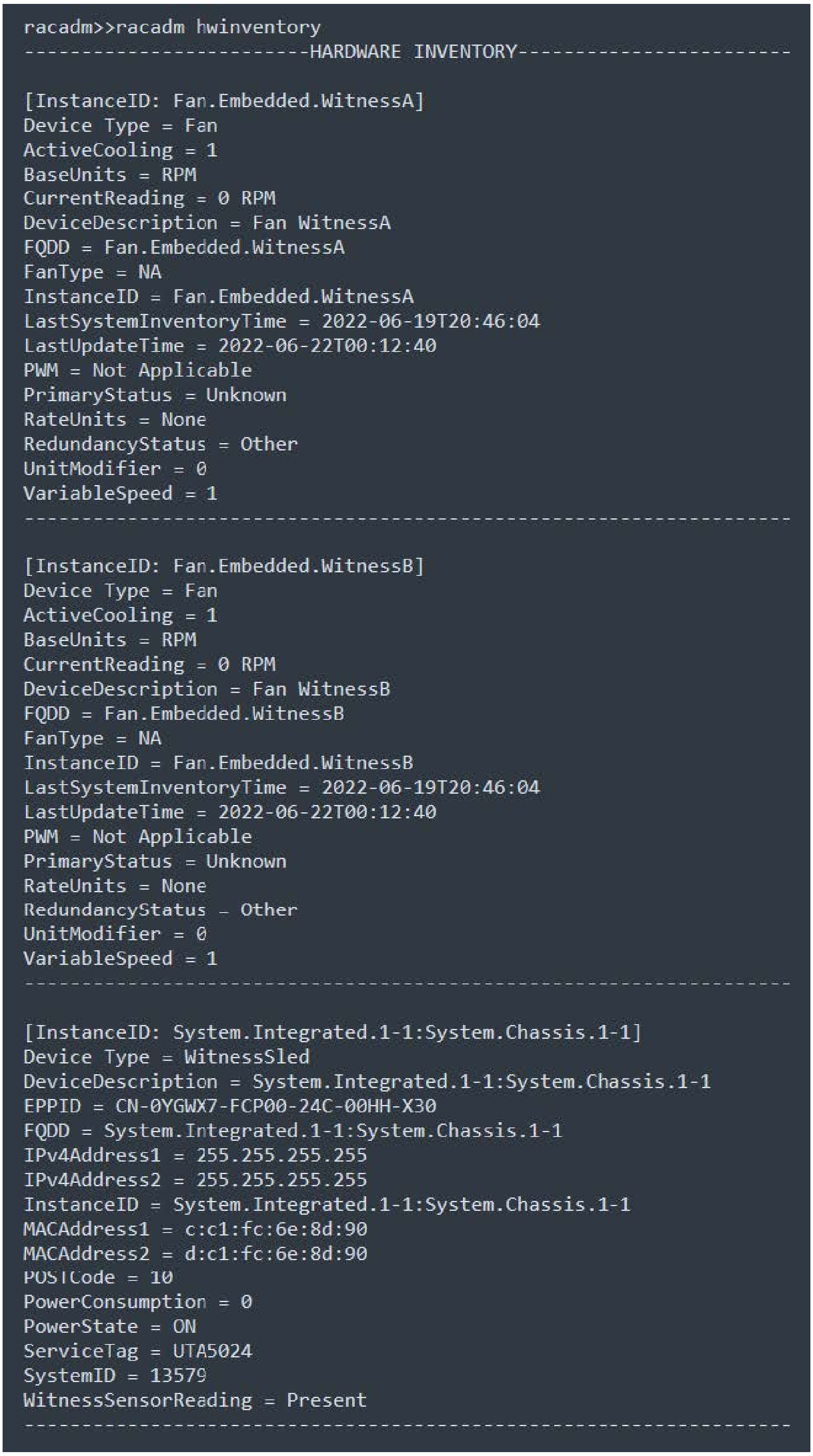
```
racadm>>racadm getsensorinfo

Sensor Type : FAN
<Sensor Name>                   <Status>    <Reading>   <lc>        <uc>        <PWM %>     <Type>
Witness FanA                    Unknown     NA          NA          NA          NA          NA
Witness FanB                    Unknown     NA          NA          NA          NA          NA

Sensor Type : WITNESS
<Sensor Name>   <Status>    <State>
Witness Status  Ok          Present
```

Figure 15. RACADM Witness sensor information



```
racadm>>swinventory

-------------------------SOFTWARE INVENTORY------------------------

ComponentType = FIRMWARE
ElementName = Chassis CM Embedded
FQDD = MC.Chassis.1-1-1
InstallationDate = 1970-01-01T00:00:00Z
Current Version = 0.20
HashValue = NA
-------------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Witness MCU Embedded
FQDD = MCU.Embedded.1-1:System.Integrated.1-1:System.Chassis.1-1
InstallationDate = 2022-08-25T07:19:01Z
Current Version = 0.13
HashValue = NA
-------------------------------------------------------------------

ComponentType = FIRMWARE
ElementName = Witness BIOS Embedded
FQDD = BIOS.Setup.1-1:System.Integrated.1-1:System.Chassis.1-1
InstallationDate = NA
Available Version = 0.1.10
HashValue = NA
-------------------------------------------------------------------
```

Figure 16. RACADM Witness software information



```
racadm>>racadm hwinventory
-------------------------HARDWARE INVENTORY------------------------

[InstanceID: Fan.Embedded.WitnessA]
Device Type = Fan
ActiveCooling = 1
BaseUnits = RPM
CurrentReading = 0 RPM
DeviceDescription = Fan WitnessA
FQDD = Fan.Embedded.WitnessA
FanType = NA
InstanceID = Fan.Embedded.WitnessA
LastSystemInventoryTime = 2022-06-19T20:46:04
LastUpdateTime = 2022-06-22T00:12:40
PWM = Not Applicable
PrimaryStatus = Unknown
RateUnits = None
RedundancyStatus = Other
UnitModifier = 0
VariableSpeed = 1
-------------------------------------------------------------------

[InstanceID: Fan.Embedded.WitnessB]
Device Type = Fan
ActiveCooling = 1
BaseUnits = RPM
CurrentReading = 0 RPM
DeviceDescription = Fan WitnessB
FQDD = Fan.Embedded.WitnessB
FanType = NA
InstanceID = Fan.Embedded.WitnessB
LastSystemInventoryTime = 2022-06-19T20:46:04
LastUpdateTime = 2022-06-22T00:12:40
PWM = Not Applicable
PrimaryStatus = Unknown
RateUnits = None
RedundancyStatus = Other
UnitModifier = 0
VariableSpeed = 1
-------------------------------------------------------------------

[InstanceID: System.Integrated.1-1:System.Chassis.1-1]
Device Type = WitnessSled
DeviceDescription = System.Integrated.1-1:System.Chassis.1-1
EPPID = CN-0YGWX7-FCP00-24C-00HH-X30
FQDD = System.Integrated.1-1:System.Chassis.1-1
IPv4Address1 = 255.255.255.255
IPv4Address2 = 255.255.255.255
InstanceID = System.Integrated.1-1:System.Chassis.1-1
MACAddress1 = c:c1:fc:6e:8d:90
MACAddress2 = d:c1:fc:6e:8d:90
POSTCode = 10
PowerConsumption = 0
PowerState = ON
ServiceTag = UTA5024
SystemID = 13579
WitnessSensorReading = Present
-------------------------------------------------------------------
```

Figure 17. RACADM Witness hardware information

Witness host

Witness host interfaces are dependent on the installed host.

Interfaces for the Witness host include:

- A network-accessible host interface
- Witness serial connection to the host

Documentation should be found online for the installed Witness host capabilities.

Witness host: ESXi

ⓘ **NOTE:** The default VMware login for the Witness ESXi factory image is: root / @witness123!

The ESXi host on the Witness node supports standard ESXi and vCenter interface methods.

The ESXi serial console is also accessible through serial communication with the Witness.

ⓘ **NOTE:** Accessing Witness serial connection:

1. Access the Witness OS interface by using the Witness IP captured from the serial connection. Refer screenshot.
2. Go to "Actions," select "Services," Enable Secure Shell (SSH).
3. Go to "Actions," select "Services," Enable ESXi Shell.
4. Access Witness with SSH connection by using Witness IP address.

Witness power operations

The Witness node must be installed into a properly configured chassis. See Installing the Witness for details.

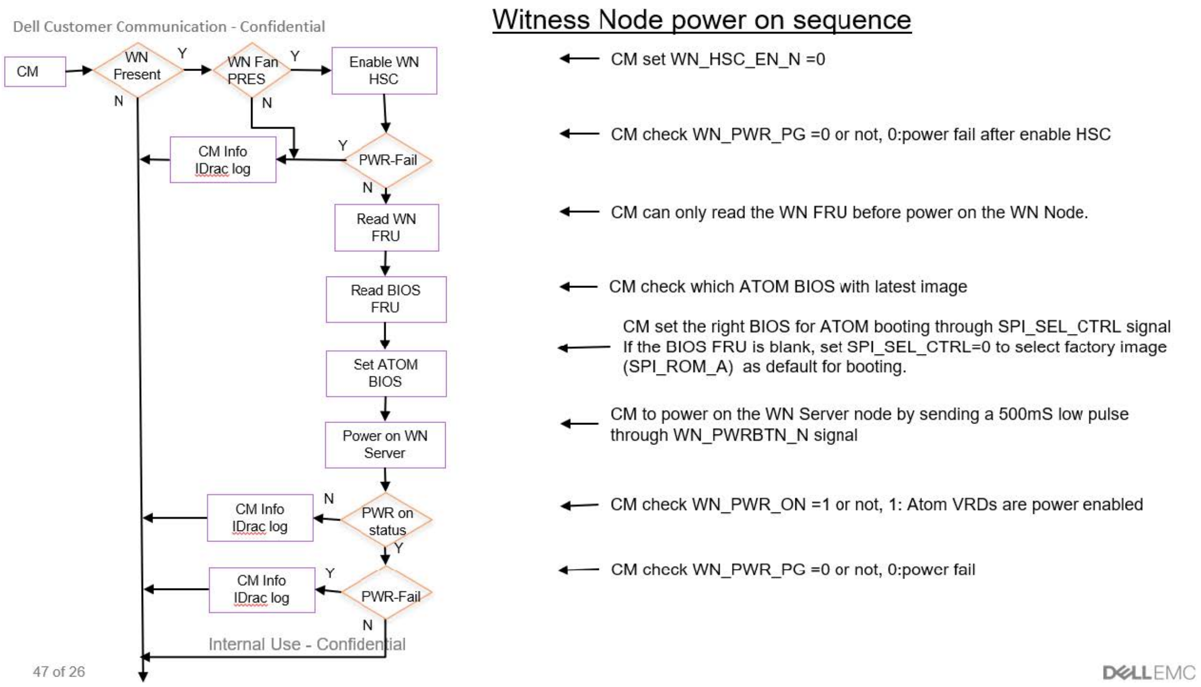
Witness power operations are accessible through:

- Witness front panel power button
- iDRAC
  1. User interface
  2. Redfish
  3. RACADM
  4. IPMI
  5. CPLD
- Witness host interfaces
- Chassis manager serial connection

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

The CM controls power to the Witness. Auto power-on for the Witness is enabled by default in the CM and will power on the Witness once its presence is detected. As previously mentioned in installation requirements, the CM runs several checks to ensure that various system fans are following expected behavior. If these checks fail, then the CM will not supply the Witness with power.

The below block and state diagrams add additional detail to the Witness power behavior as seen by the CM.



Witness Node power on sequence

CM set WN_HSC_EN_N =0

CM check WN_PWR_PG =0 or not, 0:power fail after enable HSC

CM can only read the WN FRU before power on the WN Node.

CM check which ATOM BIOS with latest image

CM set the right BIOS for ATOM booting through SPI_SEL_CTRL signal
If the BIOS FRU is blank, set SPI_SEL_CTRL=0 to select factory image (SPI_ROM_A) as default for booting.

CM to power on the WN Server node by sending a 500mS low pulse through WN_PWRBTN_N signal

CM check WN_PWR_ON =1 or not, 1: Atom VRDs are power enabled

CM chcck WN_PWR_PG =0 or not, 0:powcr fail

Figure 18. Witness Node power on sequence

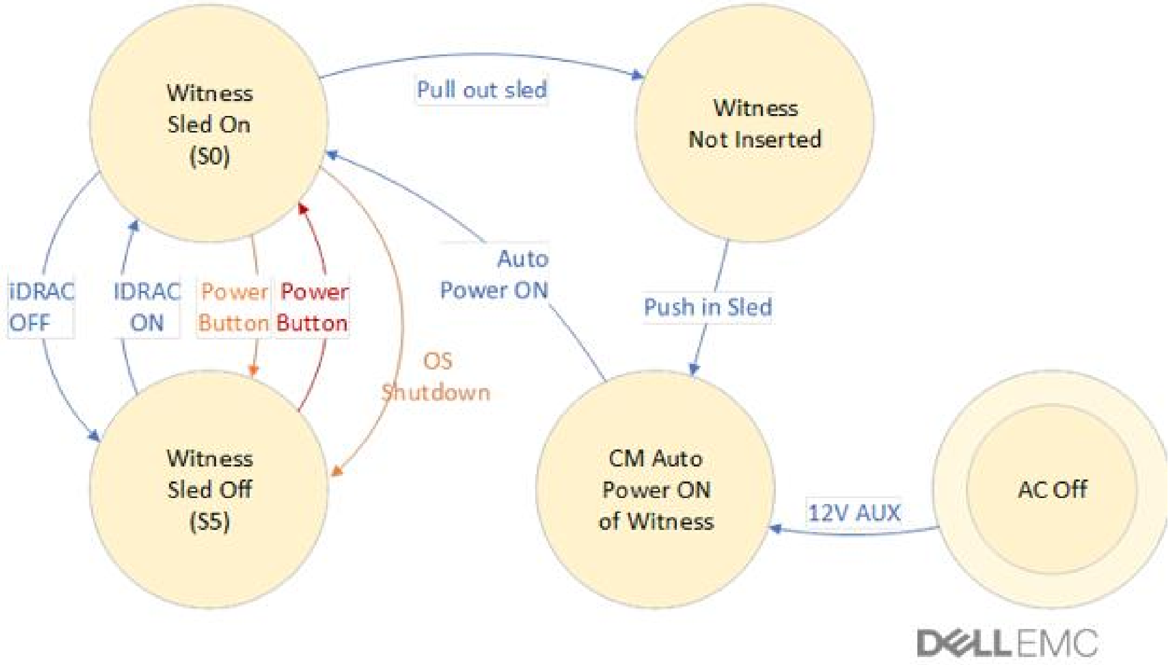


Figure 19. Witness Node power state machine

Witness power operations: Witness power button

The Witness Manager supports basic power button control for power-on and power-off from iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds. The XR4000w does not have its own dedicated iDRAC.

Witness power button LED behavior

The Witness power LED is a bicolor LED consisting of AMBER and GREEN. The LED communicates Witness status during both runtime and BIOS updates.

Witness power LED during runtime behavior is shown in the below table.

Table 14. Witness power button LED behavior

State	Amber	Green
BIOS no POST or failure	Blink @1hz	OFF
POST Progressing	OFF	Blink @1hz
BIOS POST complete	OFF	ON
S5 power state	OFF	OFF

During Witness BIOS updating, the Chassis Manager sets a “WM SPI image updating” bit in register map. This sets the Witness LED behavior as:

- Amber ON one second, Green OFF
- Green ON one second, Amber OFF

Once the CM clears the “WM SPI image updating bit” normal Witness LED runtime behavior resumes.

Witness power operations: iDRAC

iDRAC supports the following Witness operations:

- Power Off/On
- Hard Reset
- Power Cycle (Reseat Node)

These can be performed through iDRAC interfaces that are mentioned below:

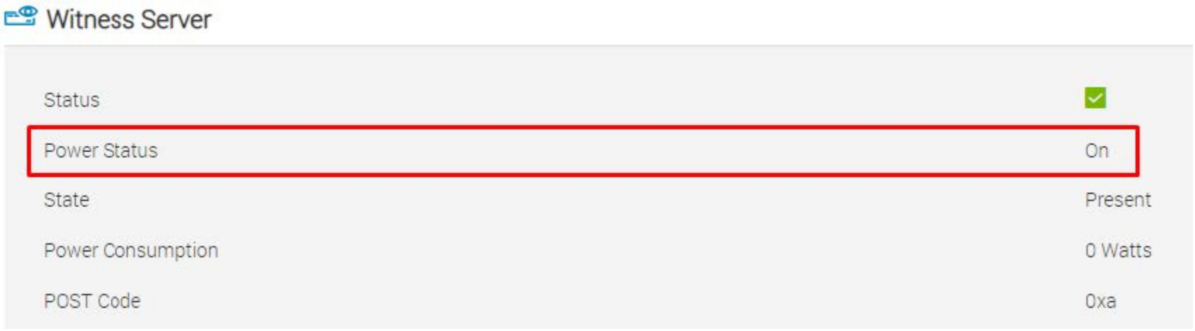
- iDRAC GUI
- Redfish
- RACADM
- CPLD

NOTE: The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Witness server power status is identified in GUI:

The iDRAC GUI Witness Page displays can be used to view Witness power items and manipulate witness power.

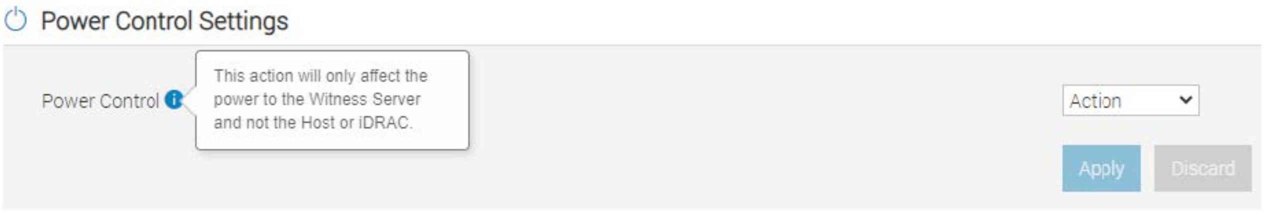
Witness server power status is identified in GUI:



Witness Server

Status	✓
Power Status	On
State	Present
Power Consumption	0 Watts
POST Code	0xa

Figure 20. iDRAC GUI Witness power status



This action will only affect the power to the Witness Server and not the Host or iDRAC.

Figure 21. iDRAC GUI Witness power control 1

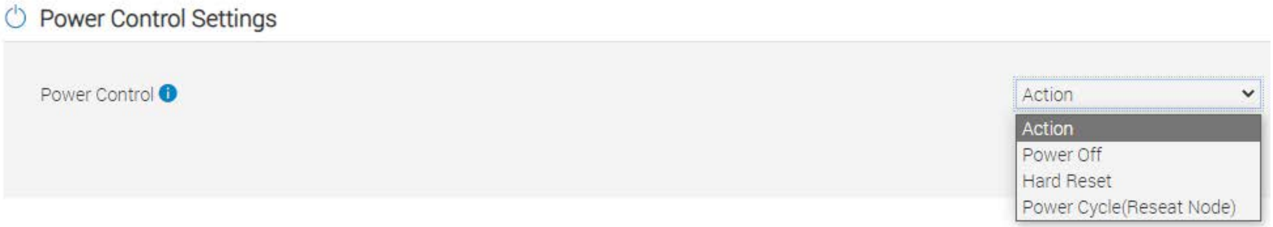


Figure 22. iDRAC GUI Witness power control 2

Witness power operations: Redfish

Witness power operations can be performed through the FQDN:

/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1/Actions/Chassis.Reset

With valid actions being:

- "On"
- "ForceOff"
- "ForceRestart"
- "PowerCycle"

Example of successfully requesting a power-off of the Witness.

The variables “BMC,” “USER,” and “PASS” are set in this example.

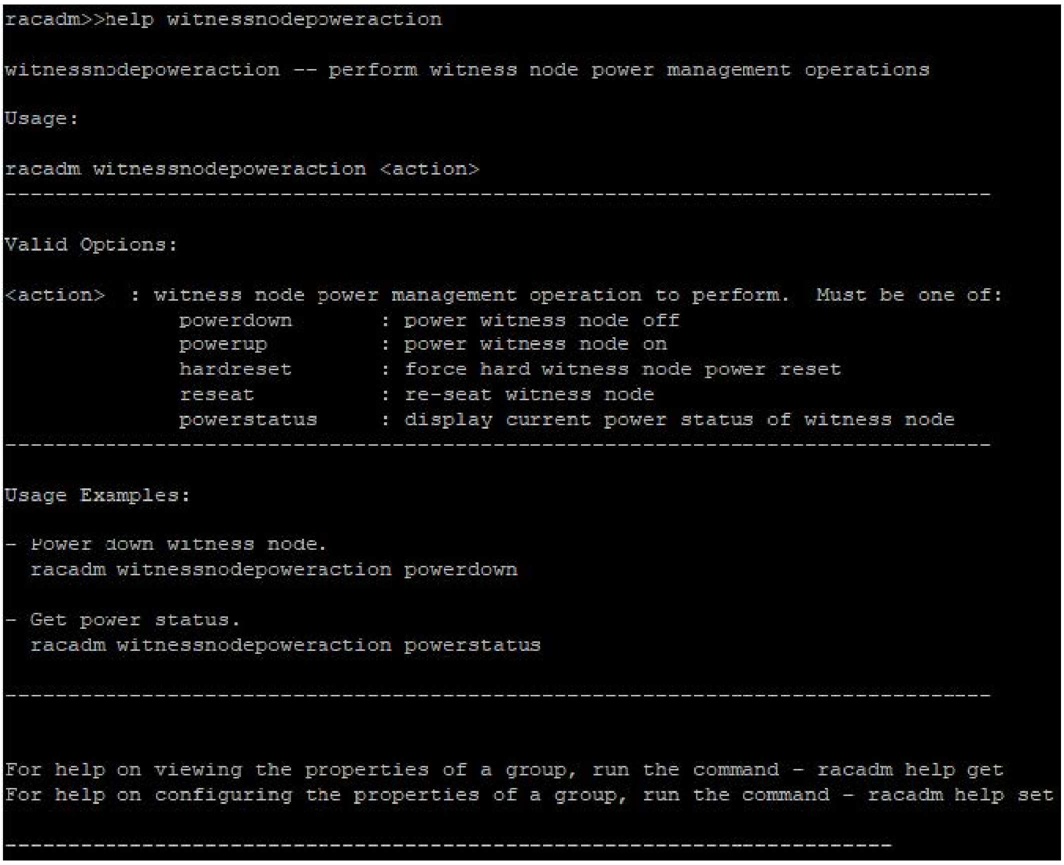
```
root@ubuntu:~# curl --request POST \
--url https://${BMC}/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-
1/Actions/Chassis.Reset \
--user ${USER}:${PASS} \
--header 'Content-Type: application/json' \
--insecure \
-i \
--data '{
"ResetType": "ForceOff"
}'
HTTP/1.1 204 No Content
```

Witness power operations: RACADM

RACADM supports the following power operations for Witness:

- powerdown
- powerup
- hardreset

- reseat
- powerstatus



```
racadm>>help witnessnodepoweraction

witnessnodepoweraction -- perform witness node power management operations

Usage:

racadm witnessnodepoweraction <action>
-------------------------------------------------------------------------------

Valid Options:

<action>  : witness node power management operation to perform.  Must be one of:
              powerdown        : power witness node off
              powerup          : power witness node on
              hardreset        : force hard witness node power reset
              reseat           : re-seat witness node
              powerstatus      : display current power status of witness node
-------------------------------------------------------------------------------

Usage Examples:

- Power down witness node.
  racadm witnessnodepoweraction powerdown

- Get power status.
  racadm witnessnodepoweraction powerstatus

-------------------------------------------------------------------------------


For help on viewing the properties of a group, run the command - racadm help get
For help on configuring the properties of a group, run the command - racadm help set

-----------------------------------------------------------------------
```

Figure 23. Help output for RACADM witnessnodepoweraction

Witness power operations: host

Witness host power control capabilities are dependent on the installed host.

Possible interfaces for the Witness host include:

- A network-accessible host interface
- Witness serial connection to the host

Witness power operations: ESXi

The ESXi host on the Witness node supports standard ESXi and vCenter interface methods. Documentation is available online for these.

The ESXi serial console is also accessible through serial communication with the Witness.

Getting Witness host network information

Once a valid network connection is applied to the Witness, host IPv4 and MAC address information are accessible over typical iDRAC interfaces of any compute node that is connected to the same CM. This data is sent by the host OS agent to the CM. The CM stores and provide this data to any connected iDRAC through a shared CPLD memory-map.

Host network information can be found through the following methods:

- iDRAC
  1. iDRAC GUI
  2. Redfish

3. RACADM
4. IPMI
5. CPLD

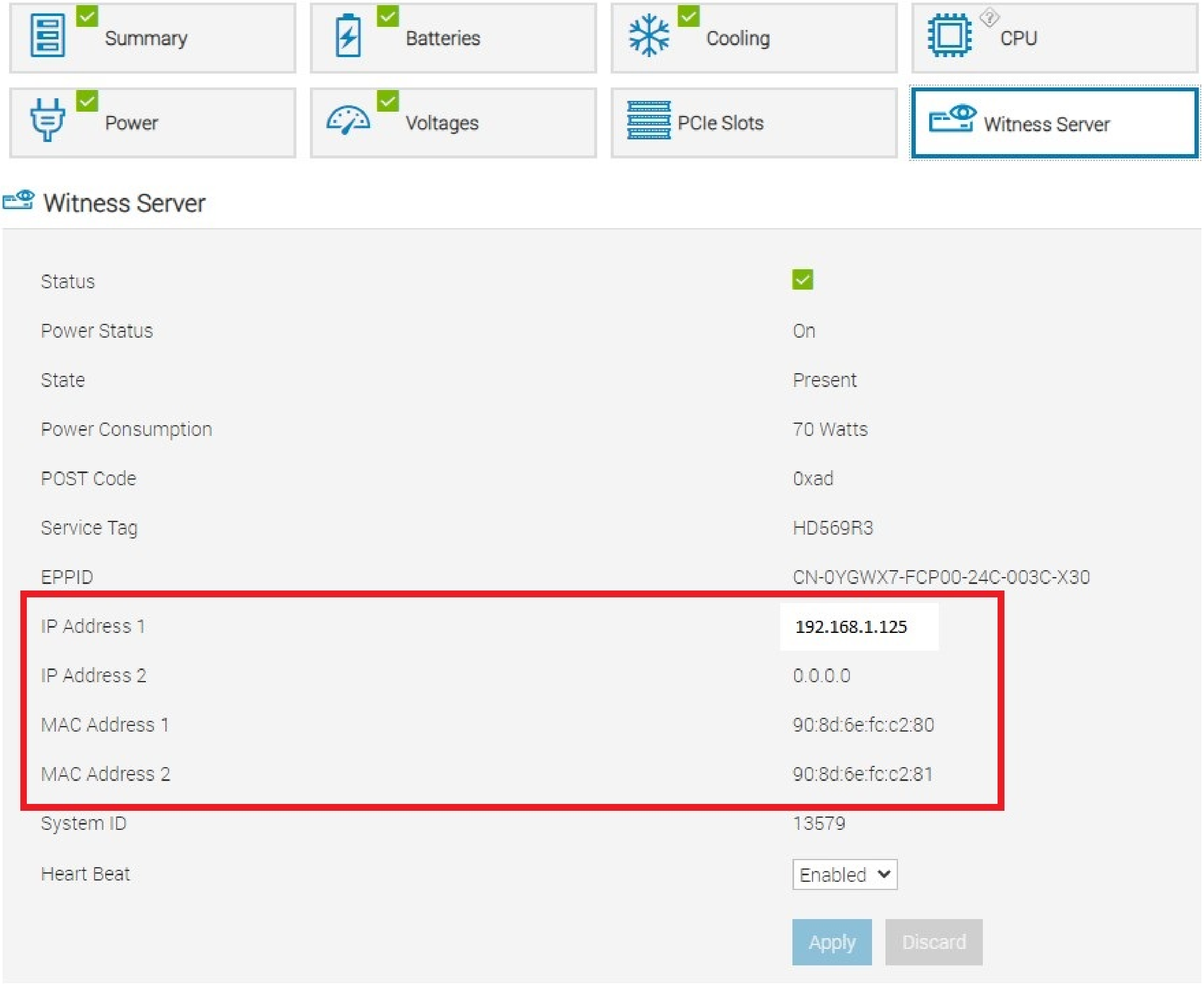
- Witness serial connection
- Chassis manager serial connection

Witness host network: iDRAC

NOTE: A valid Dell OS Agent for Witness (DOSA-W) must be installed on the Witness host for a compute sled to receive host networking information. See Witness DOSA-W deployment for more information.

Witness host network: iDRAC GUI

Using the iDRAC of a connected compute sled, the Witness Server page displays the Witness host networking information:



Status	✓
Power Status	On
State	Present
Power Consumption	70 Watts
POST Code	0xad
Service Tag	HD569R3
EPPID	CN-0YGWX7-FCP00-24C-003C-X30
IP Address 1	192.168.1.125
IP Address 2	0.0.0.0
MAC Address 1	90:8d:6e:fc:c2:80
MAC Address 2	90:8d:6e:fc:c2:81
System ID	13579
Heart Beat	Enabled

Figure 24. iDRAC GUI Witness network information

Witness host network: Redfish

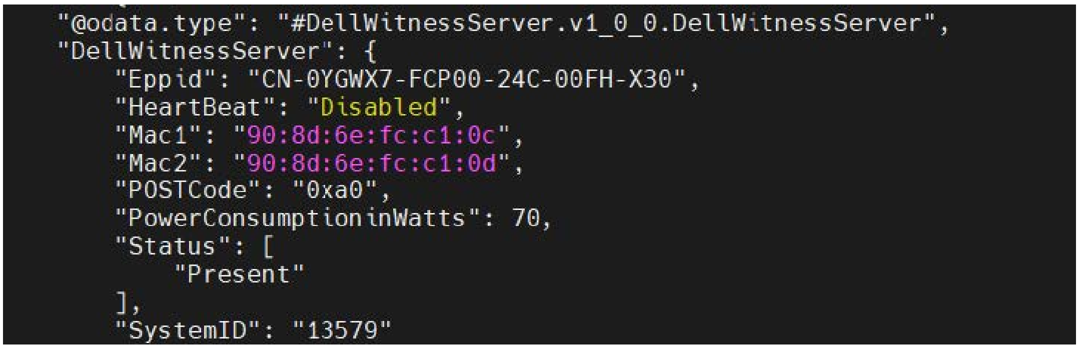
Witness network information can be found from the following URI:

redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1

Example of collecting data from the above URI.

The variables “BMC”, “USER”, and “PASS” are set in this example.

```
root@ubuntu:~# curl --request GET \

--url https://${BMC}/redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1 \

--user ${USER}:${PASS}\

--header 'Content-Type: application/json' \

--insecure
```

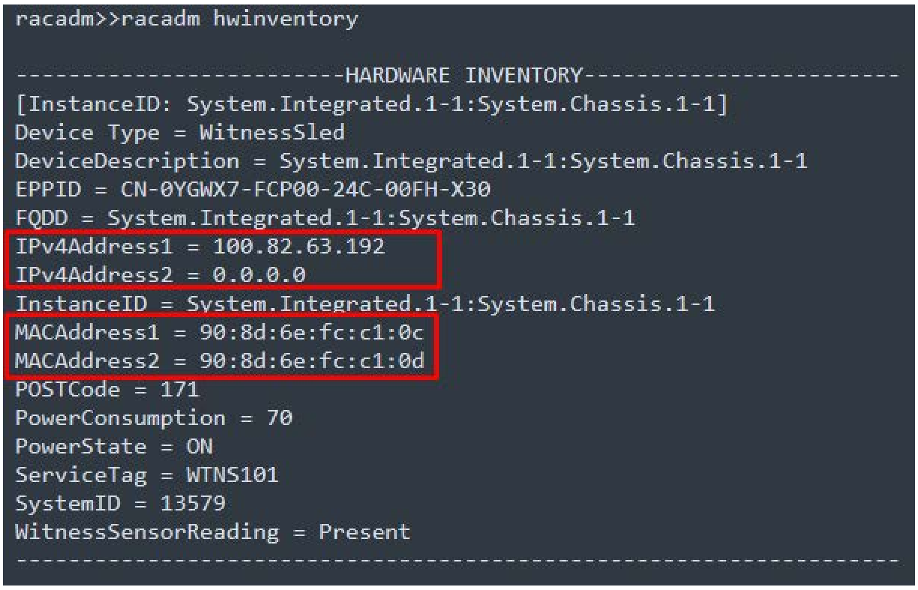


```
    "@odata.type": "#DellWitnessServer.v1_0_0.DellWitnessServer",
    "DellWitnessServer": {
        "Eppid": "CN-0YGWX7-FCP00-24C-00FH-X30",
        "HeartBeat": "Disabled",
        "Mac1": "90:8d:6e:fc:c1:0c",
        "Mac2": "90:8d:6e:fc:c1:0d",
        "POSTCode": "0xa0",
        "PowerConsumptioninWatts": 70,
        "Status": [
            "Present"
        ],
        "SystemID": "13579"
```

Figure 25. Witness Mac1, Mac2 provided from a GET on redfish/v1/Chassis/System.Integrated.1-1_System.Chassis.1-1

Witness host network: RACADM

Witness host network information through RACADM is found with the `racadm hwinventory` command.



```
racadm>>racadm hwinventory

-------------------------HARDWARE INVENTORY------------------------
[InstanceID: System.Integrated.1-1:System.Chassis.1-1]
Device Type = WitnessSled
DeviceDescription = System.Integrated.1-1:System.Chassis.1-1
EPPID = CN-0YGWX7-FCP00-24C-00FH-X30
FQDD = System.Integrated.1-1:System.Chassis.1-1
IPv4Address1 = 100.82.63.192
IPv4Address2 = 0.0.0.0
InstanceID = System.Integrated.1-1:System.Chassis.1-1
MACAddress1 = 90:8d:6e:fc:c1:0c
MACAddress2 = 90:8d:6e:fc:c1:0d
POSTCode = 171
PowerConsumption = 70
PowerState = ON
ServiceTag = WTNS101
SystemID = 13579
WitnessSensorReading = Present
-------------------------------------------------------------------
```

Figure 26. Witness host information through RACADM

Witness host network: Witness host OS

See Witness serial communication for details on serial connection to the Witness.

Limited interaction with the Witness host is possible depending on the headless capabilities of the installed host. See external host-specific documentation to identify headless-mode capabilities.

This section also assumes that the Witness host installed has been properly configured for network access. For additional information, see Witness host deployment.

Witness host network: ESXi

The ESXi Witness host supports multiple methods of getting the Witness IP address including:

- Witness serial connection
- ESXi shell
- ESXi GUI
- vCenter/vSphere

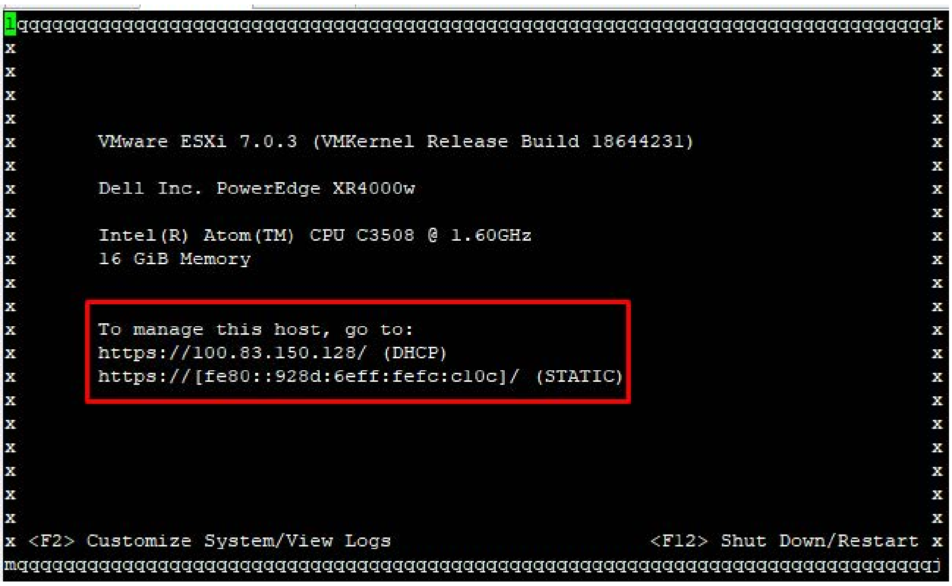
Only the serial connection is detailed here, please see host-specific documentation available online for alternative methods.

The ESXi host uses the Witness NIC 1 port as a management network internally designated as vmnic0. The IPv4 and IPv6 addresses for this management connection are displayed in the Witness serial interface after the ESXi host boots.

The displayed IPv4 management address can be used to access the host ESXi interface (Witness host: ESXi).

NOTE: IP Address information may not be displayed until the default password is changed.

An example of the ESXi serial management console with network information:



```
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x                                                                              x
x                                                                              x
x                                                                              x
x                                                                              x
x       VMware ESXi 7.0.3 (VMKernel Release Build 18644231)                    x
x                                                                              x
x       Dell Inc. PowerEdge XR4000w                                            x
x                                                                              x
x       Intel(R) Atom(TM) CPU C3508 @ 1.60GHz                                  x
x       16 GiB Memory                                                          x
x                                                                              x
x                                                                              x
x       To manage this host, go to:                                            x
x       https://100.83.150.128/ (DHCP)                                         x
x       https://[fe80::928d:6eff:fefc:c10c]/ (STATIC)                          x
x                                                                              x
x                                                                              x
x                                                                              x
x                                                                              x
x                                                                              x
x                                                                              x
x <F2> Customize System/View Logs                      <F12> Shut Down/Restart x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Figure 27. Witness host ESXi serial interface

Using the Witness Heart Beat function

The Witness “Heart Beat” is a feature that is enabled through the Dell OS Agent for Witness (DOSA-W) which resides on the Witness host. Usage of the Heart Beat requires a properly deployed DOSA-W driver to the Witness host (Witness DOSA-W deployment for deployment information).

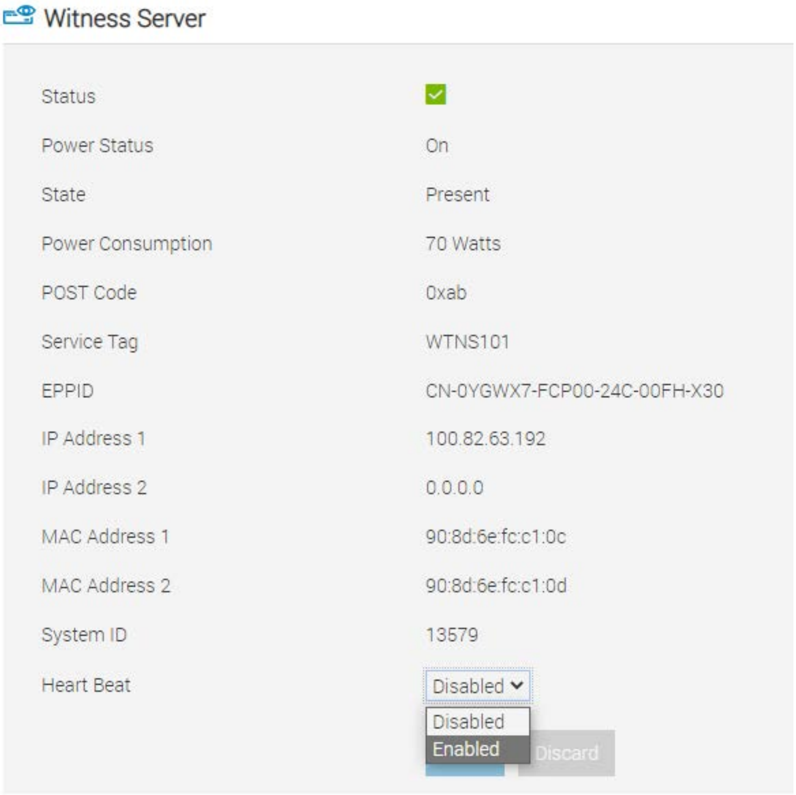
The Witness Heart Beat is a regular pulse that the CM receives from the Witness OS every 60 seconds. The iDRAC of connected compute sleds supports a Heart Beat monitor feature which is disabled by default. If there are no compute sleds in the chassis, the Chassis Manager disables this feature by default as well.

- Script Adapted from: Solved: Re: How to discover the ESXi node in given IP rang... - VMware Technology Network VMTN

When the Heart Beat functionality is enabled through iDRAC, the CM behavior is as follows:

- After Witness power-on, CM waits five minutes for BIOS load and Witness OS boot.
- After five minutes (or if heartbeat monitoring is switched to “Enabled” through iDRAC during this period), a three minute watchdog timer starts.
- Every 60 seconds, the heartbeat pulse send from the Witness host will reset the watchdog timer.
- If the watchdog timer expires, the CM will cold-reboot the Witness.

NOTE: This cold-reboot cannot occur more than three times in a 24-hour period; any additional expiry of the watchdog timer will only log an error in iDRAC.



Witness Server

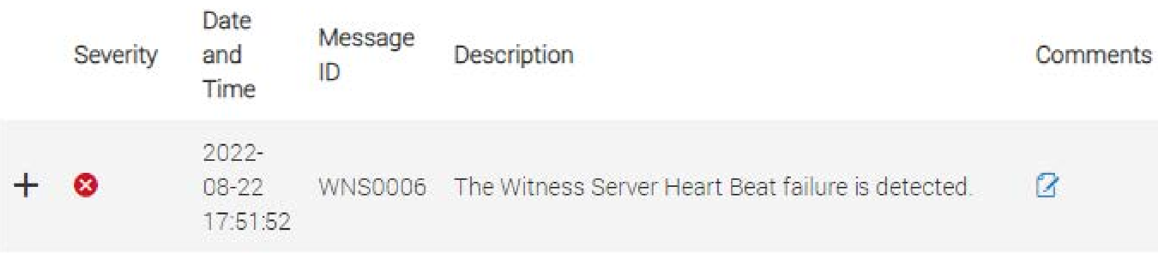
Status	✓
Power Status	On
State	Present
Power Consumption	70 Watts
POST Code	0xab
Service Tag	WTNS101
EPPID	CN-0YGWX7-FCP00-24C-00FH-X30
IP Address 1	100.82.63.192
IP Address 2	0.0.0.0
MAC Address 1	90:8d:6e:fc:c1:0c
MAC Address 2	90:8d:6e:fc:c1:0d
System ID	13579
Heart Beat	Disabled

Figure 28. Enabling the Witness Heart Beat in iDRAC

The logging follows the Telco WM iDRAC behavior Spec:

Table 15. Telco WM iDRAC behavior Spec

Message ID	Message	RRA	DD	Severity
WNS0006	The Witness Server Heart Beat failure is detected.	Ensure that Witness server host is booted to OS. If not, make sure it boots to OS successfully by restarting it. Use “RACADM WitnessServerPowerAction reset” command to restart the Witness server. Similarly iDRAC GUI or Redfish option can also be used to restart the Witness Server.	The Witness Server OS is not responding to Heart Beat sent from Chassis Manager.	Severity -1 (Critical)



	Severity	Date and Time	Message ID	Description	Comments
+	⊗	2022-08-22 17:51:52	WNS0006	The Witness Server Heart Beat failure is detected.	✎

Figure 29. LC log for Witness Heart Beat failure

Getting system component versions

Most system component versions are accessible through examples that are given in User interfaces: iDRAC.

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Getting component version: Witness BIOS

The Witness BIOS version can be found through:

- iDRAC
  1. GUI
  2. Redfish
  3. RACADM
  4. CPLD
- Witness ESXi OS interface

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Getting component version: Witness manager (MCU)

The Witness MCU version can be found through:

- iDRAC
  1. GUI
  2. Redfish
  3. RACADM
  4. CPLD
- Chassis manager serial connection

ⓘ **NOTE:**

The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

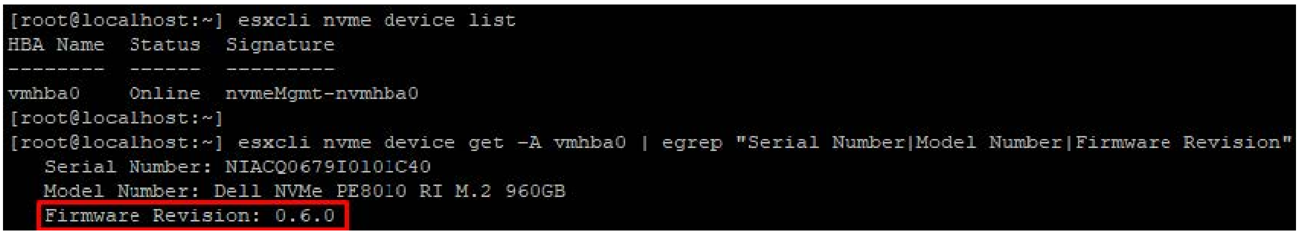
Getting component version: Witness i210 NIC

The Witness i210 NIC FW can only be found through potential host interfaces or vendor tools that are run on the host. Please see Updating Witness i210: Witness host for some information pertaining to vendor tools.

Getting component version: Witness M.2 FW

The Witness M.2 card firmware versions can be found through the Witness host through standard operations. Documentation for the specific Witness host should be located online.

Examples provided for ESXi shell only:



```
[root@localhost:~] esxcli nvme device list
HBA Name  Status  Signature
--------  ------  ---------
vmhba0    Online  nvmeMgmt-nvmhba0
[root@localhost:~]
[root@localhost:~] esxcli nvme device get -A vmhba0 | egrep "Serial Number|Model Number|Firmware Revision"
   Serial Number: NIACQ0679I0101C40
   Model Number: Dell NVMe PE8010 RI M.2 960GB
   Firmware Revision: 0.6.0
```

Figure 30. ESXi M.2 card firmware version

Getting component version: Witness host

See host-specific documentation available online to determine the Witness host version.

Getting component version: DOSA-W

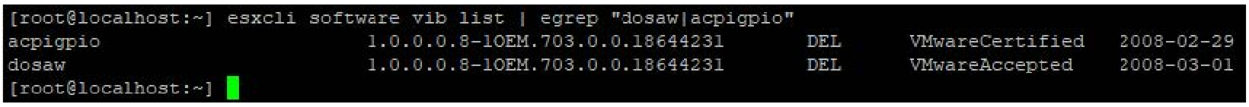
Additional host-level enhancement packages potentially have their firmware reported through host-level interfaces.

Getting component version: Witness host

See host-specific documentation available online to determine the Witness host version.

DOSA-W version: ESXi

The DOSA package can be found through standard ESXi interfaces.



```
[root@localhost:~] esxcli software vib list | egrep "dosaw|acpigpio"
acpigpio                    1.0.0.0.8-1OEM.703.0.0.18644231      DEL      VMwareCertified   2008-02-29
dosaw                       1.0.0.0.8-1OEM.703.0.0.18644231      DEL      VMwareAccepted    2008-03-01
[root@localhost:~]
```

Figure 31. ESXi DOSA-W and GPIO driver versions

Updating system components

Not all Witness DUPs are supported currently; DUP support is indicated on SWBs where it is available. Other methods of updating is indicated where relevant.

Although this document is highly focused on the Witness node, the Chassis Manager update process is also included as part of the Witness solution.

Updating the Witness BIOS

For BIOS recovery methods, see Recovering the Witness BIOS.

Although this document is highly focused on the Witness node, the Chassis Manager update process is also included as part of the Witness solution.

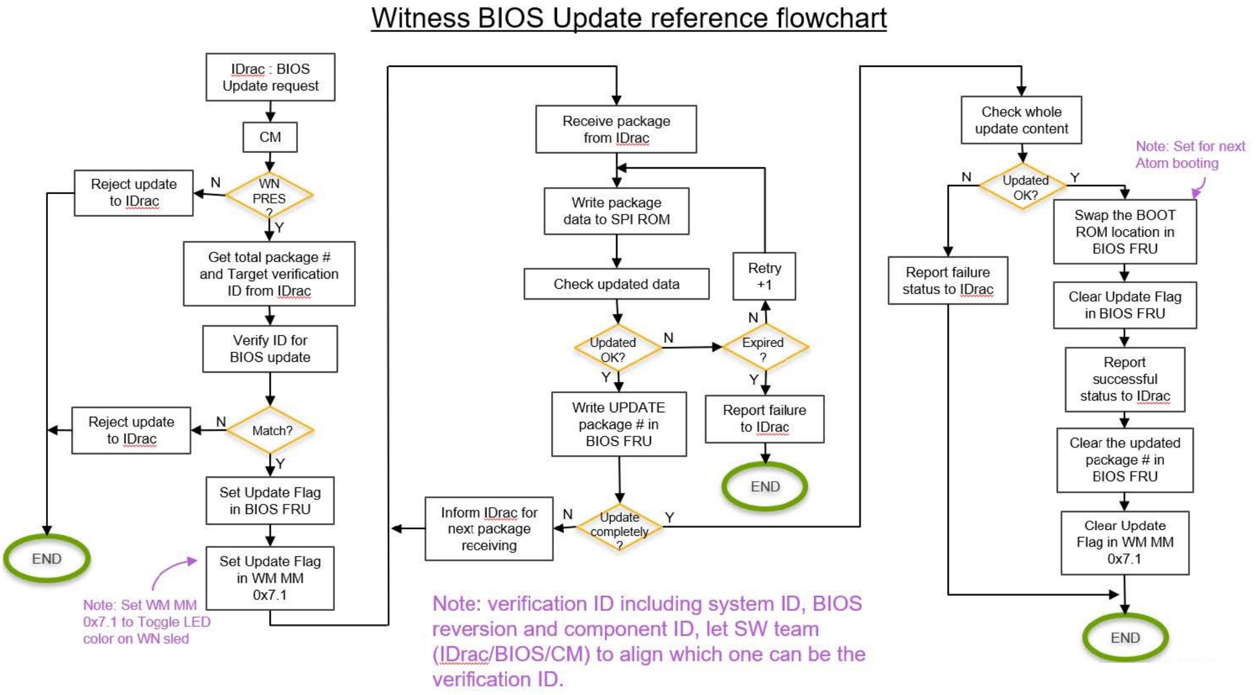
The Witness BIOS supports updates using:

- DUP
  1. iDRAC GUI
  2. RACADM
  3. UEFI Shell

Witness BIOS updates are handled by the Chassis Manager.

- iDRAC sends package data to the CM.

- Chassis Manager writes the data to the Witness SPI ROM.
- On completion, boot ROM locations are swapped in Witness BIOS FRU.


Witness BIOS Update reference flowchart
IDrac : BIOS Update request
CM
WN PRES ?
N
Reject update to IDrac
Y
Get total package # and Target verification ID from IDrac
Verify ID for BIOS update
Match?
N
Reject update to IDrac
Y
Set Update Flag in BIOS FRU
Set Update Flag in WM MM 0x7.1
END
Receive package from IDrac
Write package data to SPI ROM
Check updated data
Updated OK?
N
Expired ?
N
Retry +1
Y
Report failure to IDrac
END
Y
Write UPDATE package # in BIOS FRU
Update completely ?
N
Inform IDrac for next package receiving
Y
Check whole update content
Updated OK?
N
Report failure status to IDrac
Y
Swap the BOOT ROM location in BIOS FRU
Clear Update Flag in BIOS FRU
Report successful status to IDrac
Clear the updated package # in BIOS FRU
Clear Update Flag in WM MM 0x7.1
END

Note: Set WM MM 0x7.1 to Toggle LED color on WN sled

Note: verification ID including system ID, BIOS reversion and component ID, let SW team (IDrac/BIOS/CM) to align which one can be the verification ID.

Note: Set for next Atom booting

Figure 32. Witness BIOS update flow

Updating Witness manager: MCU

The Witness MCU supports updates using:

- DUP through only iDRAC or RACADM of a valid compute sled that is connected to the same CM as the Witness.
- Development binaries through only iDRAC or RACADM of a valid compute sled that is connected to the same CM as the Witness.

Witness Manager (MCU) updating is handled by the CM.

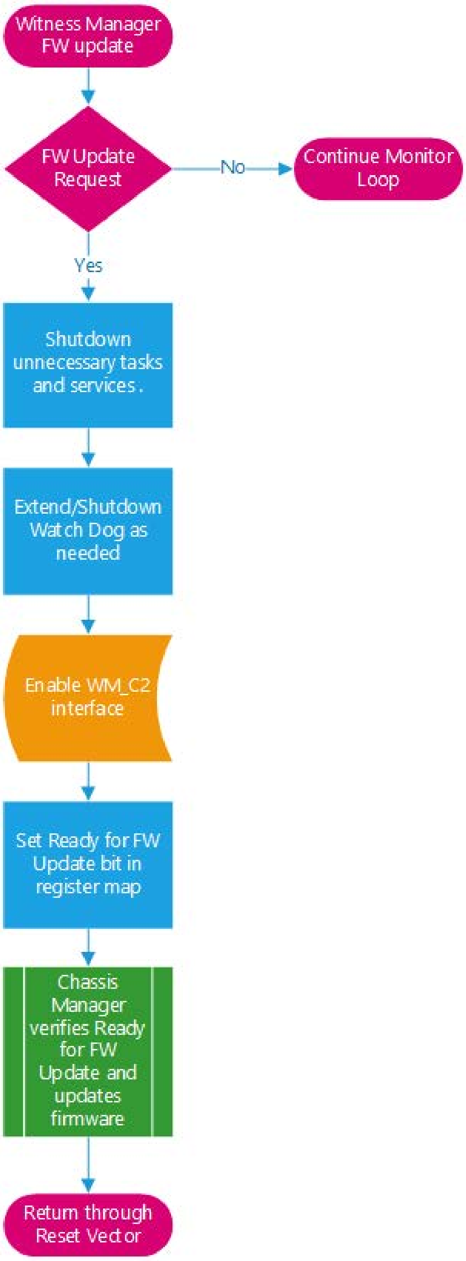

Witness Manager FW update
FW Update Request
No
Continue Monitor Loop
Yes
Shutdown unnecessary tasks and services.
Extend/Shutdown Watch Dog as needed
Enable WM_C2 interface
Set Ready for FW Update bit in register map
Chassis Manager verifies Ready for FW Update and updates firmware
Return through Reset Vector

Figure 33. Witness MCU update flow

Updating Witness BIOS: DUP (Dell Update Package)

Witness BIOS DUPs are only supported through the iDRAC GUI or RACADM interfaces. Follow standard iDRAC and RACADM procedures for this method.

NOTE: The Witness BIOS update with DUP takes 40 to 80 minutes.

NOTE: The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Updating Witness MCU: DUP

Witness MCU BIOS DUPs are only supported through the iDRAC GUI or RACADM interfaces. Follow standard iDRAC procedures for this method.

Updating the Chassis manager

The chassis manager (CM) supports updates using:

- DUP only through iDRAC or RACADM of a valid compute sled that is connected to the same chassis manager (CM) as the Witness.
- Development binaries

Updating Chassis Manager: DUP

Chassis Manager (CM) DUPs are only supported through the iDRAC GUI or RACADM interfaces. Follow standard iDRAC procedures for this method.

> **NOTE:**
>
> The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Updating Witness host: ESXi

There are two methods to perform upgrade apart from ISO-based upgrade.

1. Using esxcli profile update
    a. Upgrade or Update a Host with Image Profiles (vmware.com)
2. Using vLCM(vSphere Life Cycle Manager)
    - https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere-lifecycle-manager.doc/GUID-74295A37-E8BB-4EB9-BFBA-47B78F0C570D.html

Updating Witness i210: Witness host

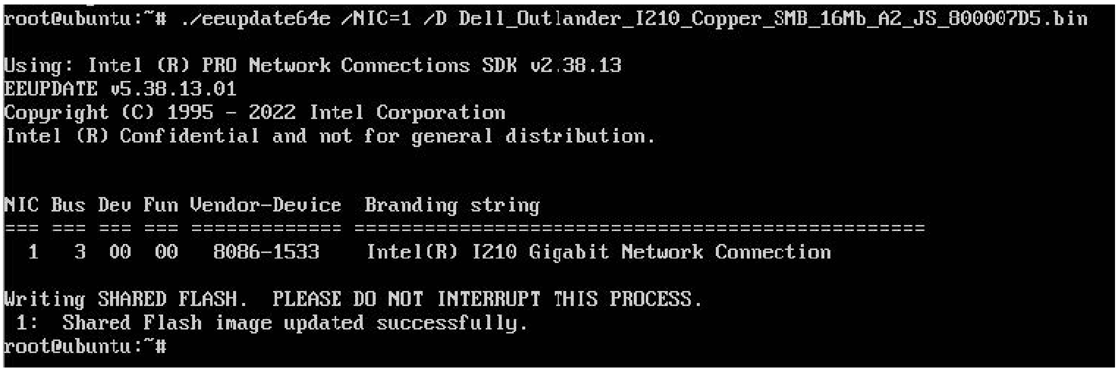
Updating the i210 NICs on the Witness host can be done using the eeupdate tool from the UEFI update section. Instead of using the UEFI version, the Linux_x64 version should be copied to the host OS. An ESXi VM running Ubuntu 20.04 is used in this section.

The i210 NIC to be updated must be in Passthrough mode for the host to update properly.

If the desired NIC is set up as an uplink to the Virtual Switch, passthrough mode will not work. Set the other i210 as the Virtual Switch uplink, disconnect the desired NIC from the Virtual Switch, and then assign this newly disconnected NIC as Passthrough to the VM. i210 drivers must be downloaded and compiled from www.intel.com

Once the iq drivers are installed, i210 update can be performed with:

./eeupdate64e /NIC=XX /D <imagefile>



```
root@ubuntu:~# ./eeupdate64e /NIC=1 /D Dell_Outlander_I210_Copper_SMB_16Mb_A2_JS_800007D5.bin

Using: Intel (R) PRO Network Connections SDK v2.38.13
EEUPDATE v5.38.13.01
Copyright (C) 1995 - 2022 Intel Corporation
Intel (R) Confidential and not for general distribution.


NIC Bus Dev Fun Vendor-Device  Branding string
=== === === === ============= =================================================
  1   3  00  00   8086-1533    Intel(R) I210 Gigabit Network Connection

Writing SHARED FLASH.  PLEASE DO NOT INTERRUPT THIS PROCESS.
 1:  Shared Flash image updated successfully.
root@ubuntu:~#
```

Figure 34. Updating Witness i210: Witness host

Updating Witness DOSA-W

The Dell OS Agent for Witness supports updates using:

- In-band host-specific updates

Updating Witness DOSA-W: ESXi

The DOSA-W update packages are provided as ESXi VIB files.

Deployment of the DOSA-W on ESXi requires installation of both the DOSA-W daemon and the ACPI GPIO drivers.

> **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

1. Copy both the VIB packages (daemon and driver) to the Witness ESXi host under the following directory:

   /var/log/vmware/
2. Package installation is performed with the following command in the ESXi shell:

   esxcli software vib install -d /var/log/vmware/<package.zip>

   Load the GPIO package first, then load the DOSA package
3. In ESXi host's /bootbank/boot.cfg:

   kernelopt=autoPartition=FALSE text nofb com2_baud=115200 com2_Port=0xe030 tty3Port=com2 gdbPort=none logPort=none
4. Reboot the witness host.

   > **NOTE:** The witness host must be rebooted after these steps to enable the display of IP addresses in iDRAC interfaces of the sleds.
5. Repeat the above steps and confirm the parameter from /bookbank/boot.cfg

   > **NOTE:** If the parameter is not saved as mentioned in the steps above, copy the parameter again and save the file, and then reboot the Witness sled.
6. Repeat the above steps and double check the parameter from /bookbank/boot.cfg
7. If the parameter saved shows as expected, then check the Witness IP from iDrac GUI, system, Witness sled and Witness IP should be available.

5

Witness host deployment

Host deployment of the Witness should involve a supported host OS packaged with additional drivers or software that is required for a successful deployment of all Witness features.

When a bootable USB is inserted into the Witness node and the Witness is rebooted, the USB is booted to by default. Serial access to the Witness is required to deploy a host through this method (see: Witness serial communication). The supported methods of host deployment in this manner are:

- RASR

6

Witness host installation: RASR

The RASR tool developed by the FEAR (Factory Enablement And Recovery) team can reimage a Witness host operating system along with any required drivers or packages. These packages include:

- Dell OS-Agent for Witness (DOSA-W)
  - More GPIO driver support packages
- Virtual Machine - VMware vSAN Witness Appliance

ⓘ **NOTE:** The default password for the VMware vSAN Witness Appliance is @witness123!

For XR4000w Witness sled this tool is limited to ESXi.

For this process, two items are required:

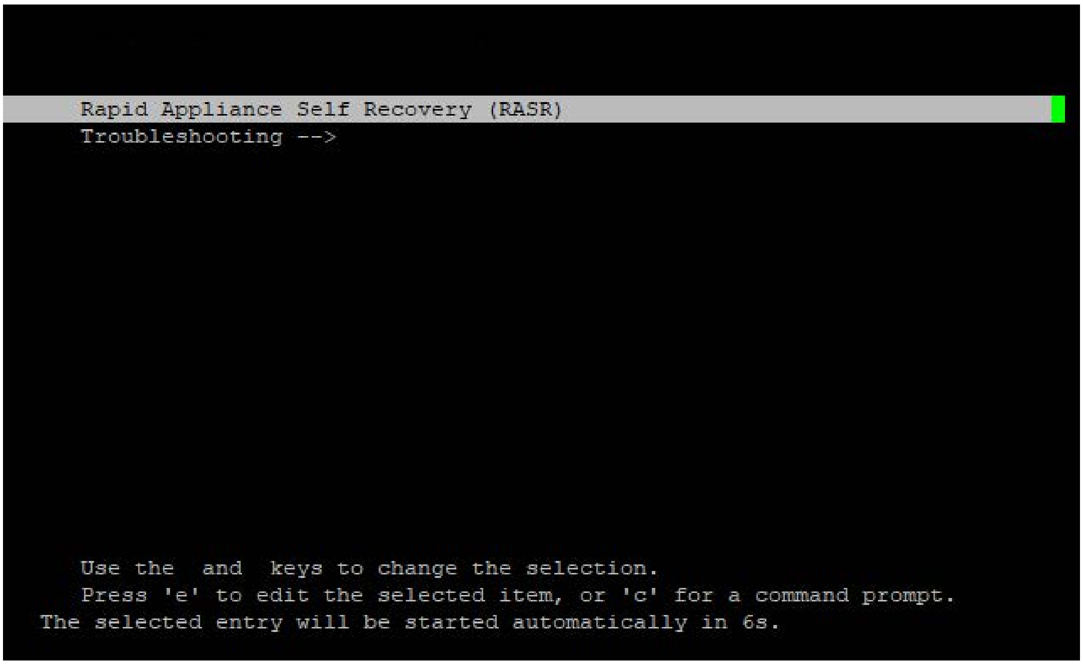
- An ISO created specifically for the RASR process
- An additional tool RASRISO-to-RASRUSB to create the bootable RASRUSB key

RASRUSB key is required since the XR4000w Witness sled does not have an iDRAC that can use virtual media functionality.

ⓘ **NOTE:** Follow the instructions for using the RASRISO-to-RASRUSB tool to create a bootable RASRUSB key.

To perform the RASR installation process, the Witness sled must be powered off and the created RASRUSB key that is inserted. A serial connection to the Witness is required to interact with the RASR process. See Connecting to Witness via serial for details.

Upon powering the Witness back on, it should boot to the inserted USB. Once booted to the RASR drive, the only options available are to perform a Factory Reset or Quit. Selecting the Factory Reset option prompts the user for confirmation before beginning. During the reset process, the system reboots multiple times to facilitate the installation of the operating system and its packages or dependencies.



```
    Rapid Appliance Self Recovery (RASR)
    Troubleshooting -->




    Use the  and  keys to change the selection.
    Press 'e' to edit the selected item, or 'c' for a command prompt.
  The selected entry will be started automatically in 6s.
```

7

Additional host deployment items

Topics:

Witness serial interface

ⓘ **NOTE:** This section is for engineering and development use only.

OVA deployment is performed as part of the FEAR RASR process: Witness host installation: RASR. If performing manually, documentation is available online detailing OVA deployment for ESXi systems.

8

Witness DOSA-W deployment

The Witness node supports enhanced functionality for BMC-level management in the form of a host-specific package that is developed by Dell. This package, which is known as the Dell Operating System Agent for Witness (DOSA-W), was implemented to support both the heartbeat functionality defined in the Witness OS Agent HLD Spec (Witness specs) and the reporting of certain Witness host data back to the Chassis Manager. This data is then available to be used by a compute node as shown in Getting Witness host network information.

ESXi OS agent

NOTE: Only the ESXi shell interface is shown here, for ESXi GUI operations please locate external documentation.

To check the DOSA-W or ACPI GPIO versions, see: Getting component version: DOSA-W.

To check the DOSA-W daemon status:

```
[root@localhost:~] esxcli daemon info get -s dosaw

Daemon Name Is Running Up or Down Time Restarts

----------- ---------- --------------- -------- --------------- ----------------------- ----------------------- --------

dosaw true up 00:45:15 0
```

To start DOSA-W daemon:

```
[root@localhost:~] esxcli daemon control start -s dosaw
```

To stop DOSA-W daemon:

```
[root@localhost:~] esxcli daemon control stop -s dosaw
```

To restart DOSA-W daemon:

```
[root@localhost:~] esxcli daemon control restart -s dosaw
```

10

Minimum configuration to POST

The components listed below are the minimum configuration to POST:

- One XR4000w sled installed in XR4000r or XR4000z chassis
- One power supply unit

11

Installing and removing system components

Topics:

Safety instructions

△ **CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.**

ⓘ **NOTE:** It is recommended that you always use an antistatic mat and antistatic strap while working on components inside the system.

ⓘ **NOTE:** Please wait for 10 minutes between AC cycles (Power off and Power on cycles) for graceful shutdown to occur when XR4000r and XR4000z chassis has XR4000w installed. This ensures graceful shutdown of underlying hardware and software components in the system.

Before working inside your system

Prerequisites

Follow the safety guidelines listed in the Safety instructions.

Steps

1. Power off the sled.
2. Remove the sled from the enclosure.

After working inside your system

Prerequisites

Follow the safety guidelines listed in Safety instructions.

Steps

Reconnect the peripherals and connect the system to the electrical outlet, and then power on the system.

Recommended tools

You may need any or combination of the following tools to perform the removal and installation procedures:

- Phillips 1 screwdriver
- Wrist grounding strap connected to the ground
- ESD mat

You need the following tools to assemble the cables for a DC power supply unit:

- AMP 90871-1 hand-crimping tool or equivalent
- Tyco Electronics 58433-3 or equivalent
- Wire-stripper pliers to remove insulation from size 10 AWG solid or stranded, insulated copper wire

  NOTE: Use alpha wire part number 3080 or equivalent (65/30 stranding).

XR4000w sled

Removing a witness sled blank

Prerequisites

Follow the safety guidelines listed in Safety Instructions.

Steps

1. Pull the plunger on the witness sled blank.
2. Remove the blank.

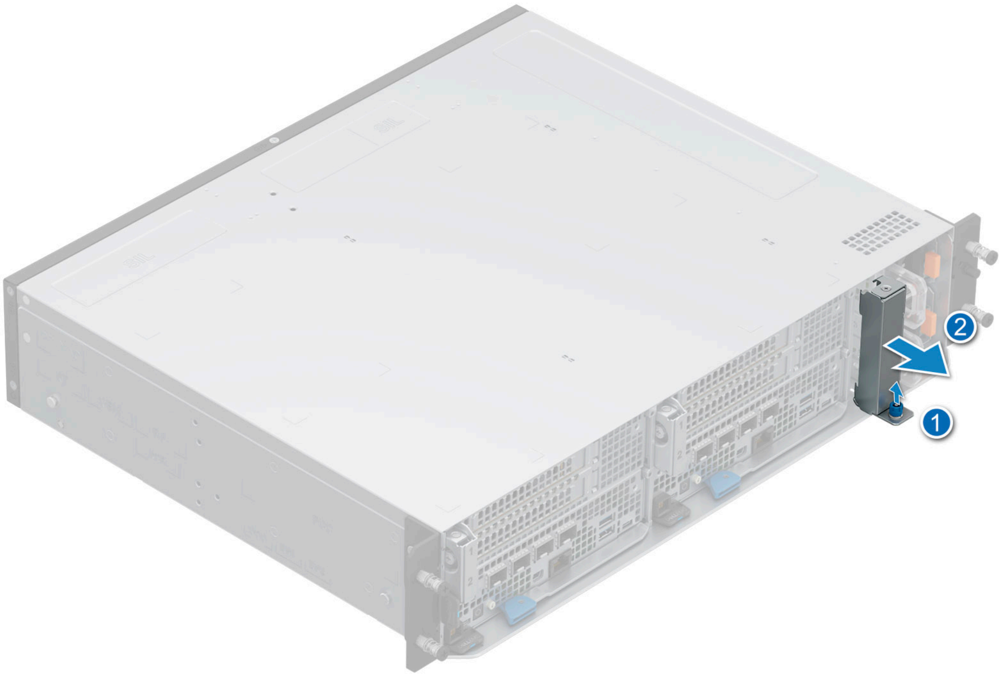


Figure 35. Removing the witness sled blank from XR4000r

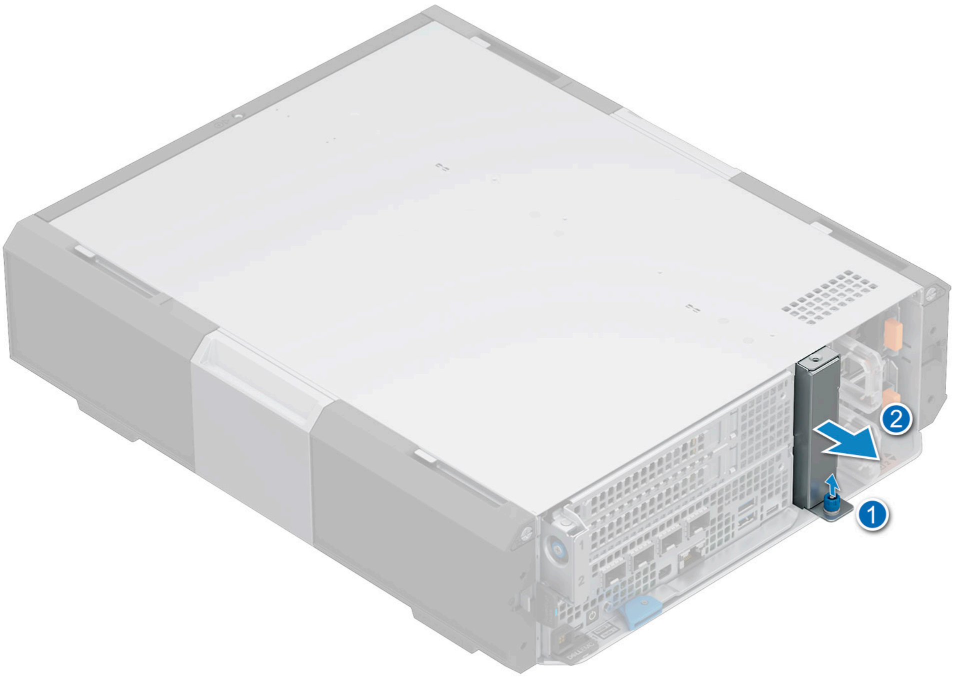


Figure 36. Removing the witness sled blank from XR4000z

Next steps

Install a sled or sled blank.

Removing the witness sled

Prerequisites

1. Follow the safety guidelines listed in the Safety instructions.
2. Disconnect all the peripherals and the cables from the witness sled.

Steps

Pull the blue tag to slide the witness sled from the chassis.

> **NOTE:** The XR4000w (witness) sled is not hot pluggable and the chassis has to be powered off before removing the witness sled.

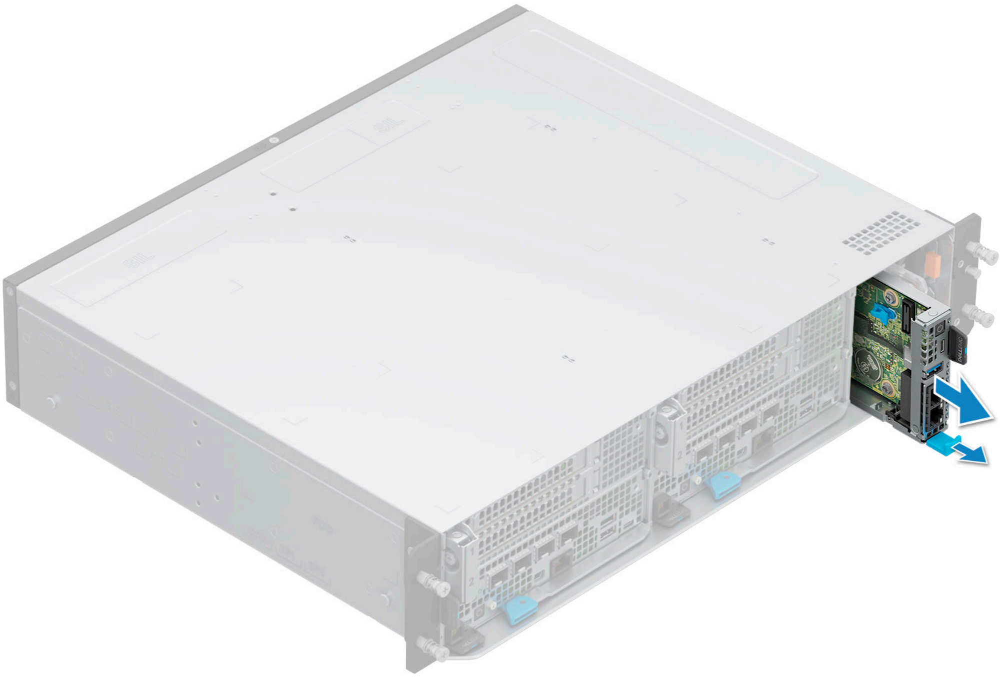


Figure 37. Removing the witness sled from XR4000r chassis

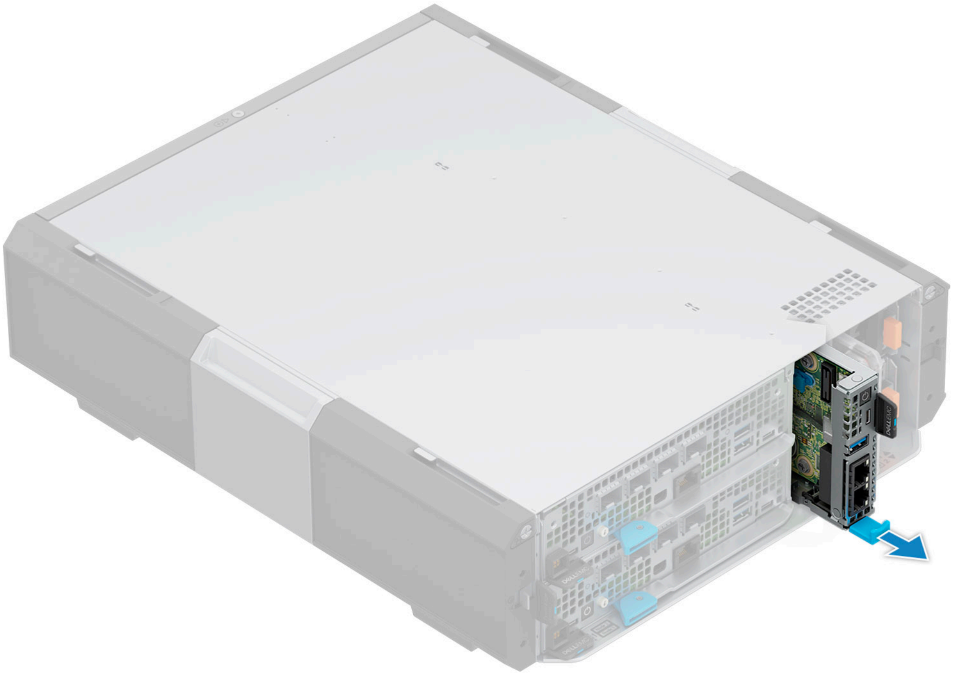


Figure 38. Removing the witness sled from XR4000z chassis

Next steps

Replace witness sled.

Installing the witness sled

Prerequisites

Follow the safety guidelines listed in the Safety instructions.

Steps

1. Align and insert the witness sled into the chassis.
2. Using the witness sled handle, slide the sled until it locks into place.

   NOTE: The XR4000w (witness) sled in not hot pluggable and the chassis has to be powered off before removing the witness sled. Once power is reapplied to the chassis, the Witness sled must be allowed time to boot. This boot time should be around 5 minutes.

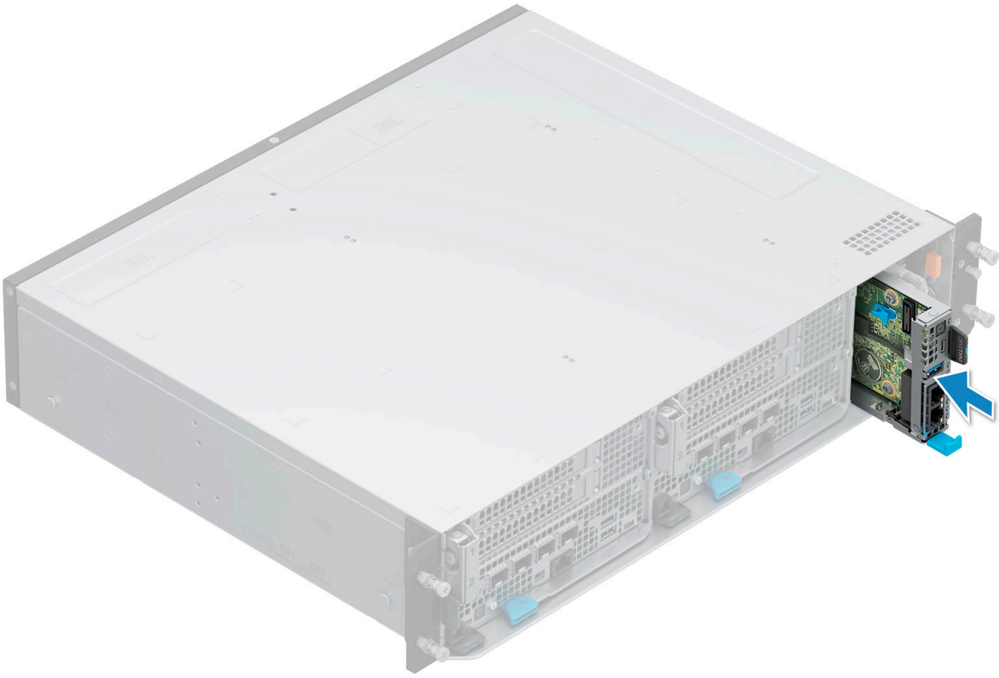


Figure 39. Installing the witness sled into XR4000r

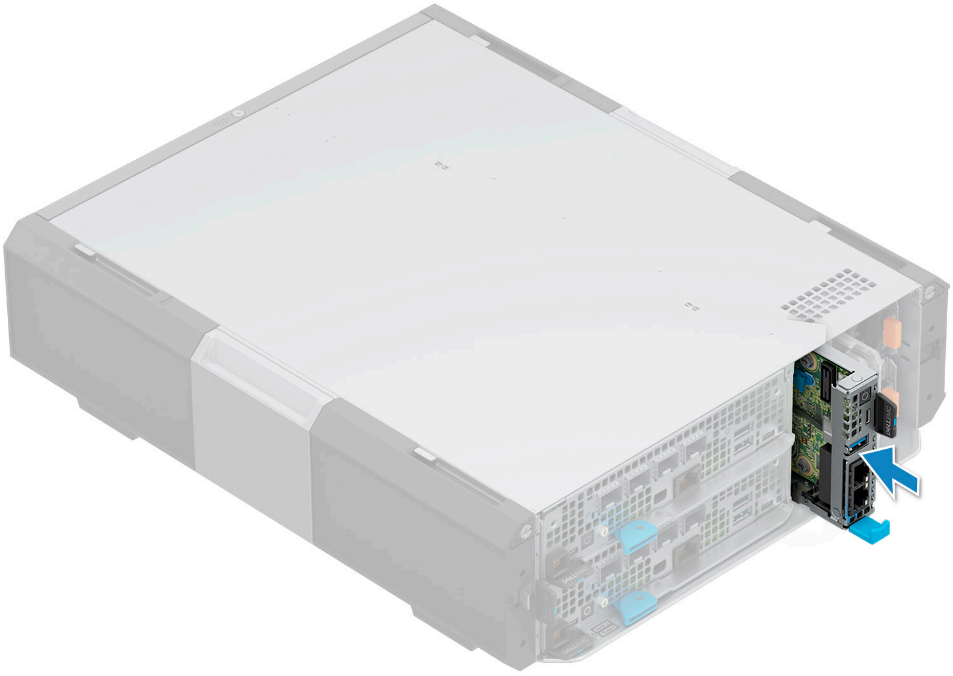


Figure 40. Installing the witness sled into XR4000z

Next steps

Connect all the cables and peripherals.

Installing a sled blank

Prerequisites

Follow the safety guidelines listed in Safety Instructions.

Steps

1. Align the sled blank with the bay of the enclosure.
2. Insert and push the sled blank until the plunger locks into place.

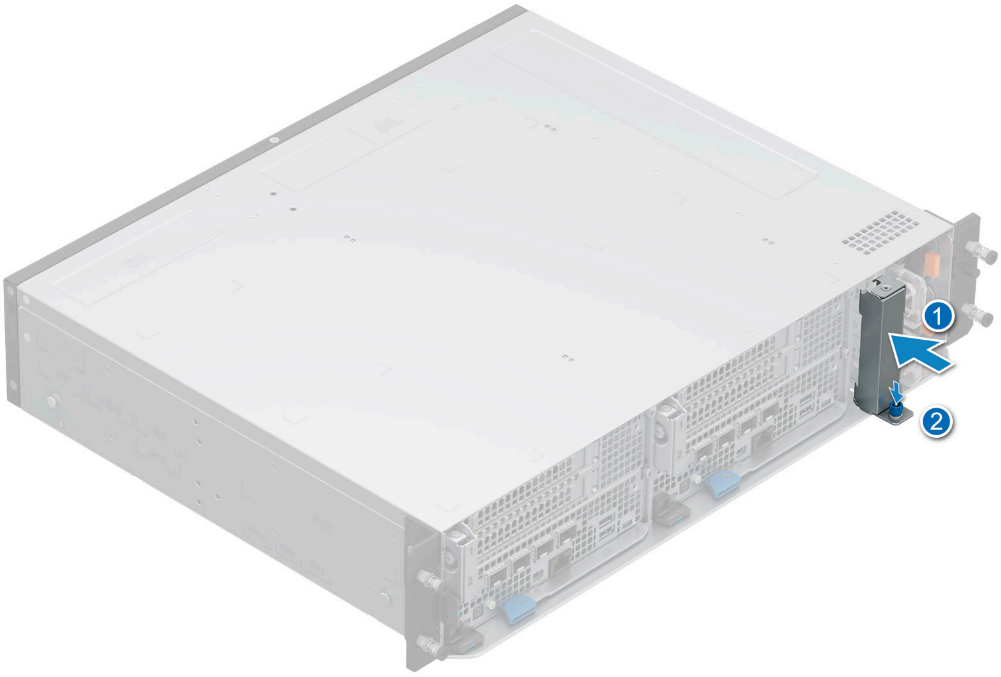


Figure 41. Installing the witness sled blank on XR4000r

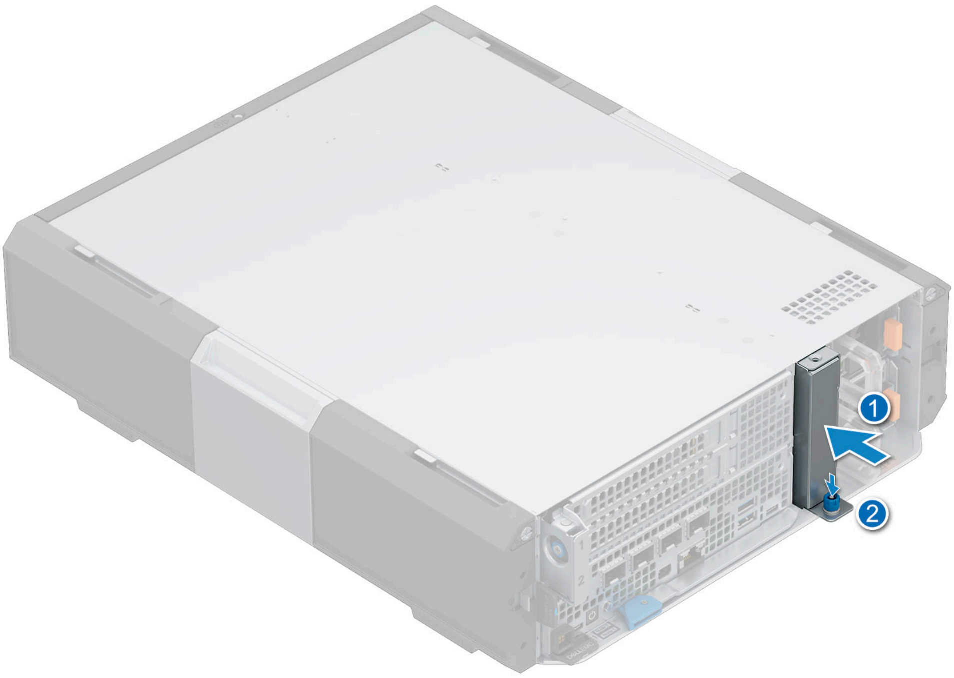


Figure 42. Installing the witness sled blank on XR4000z

M.2 SSD module

Removing the M.2 SSD module

Prerequisites

1. Follow the safety guidelines listed in the Safety instructions.
2. Follow the procedure listed in the Before working inside your system.

Steps

1. Slide the blue release latch that secures the M.2 SSD module.
2. Pull the M.2 SSD module away from the M.2 connector on system board.

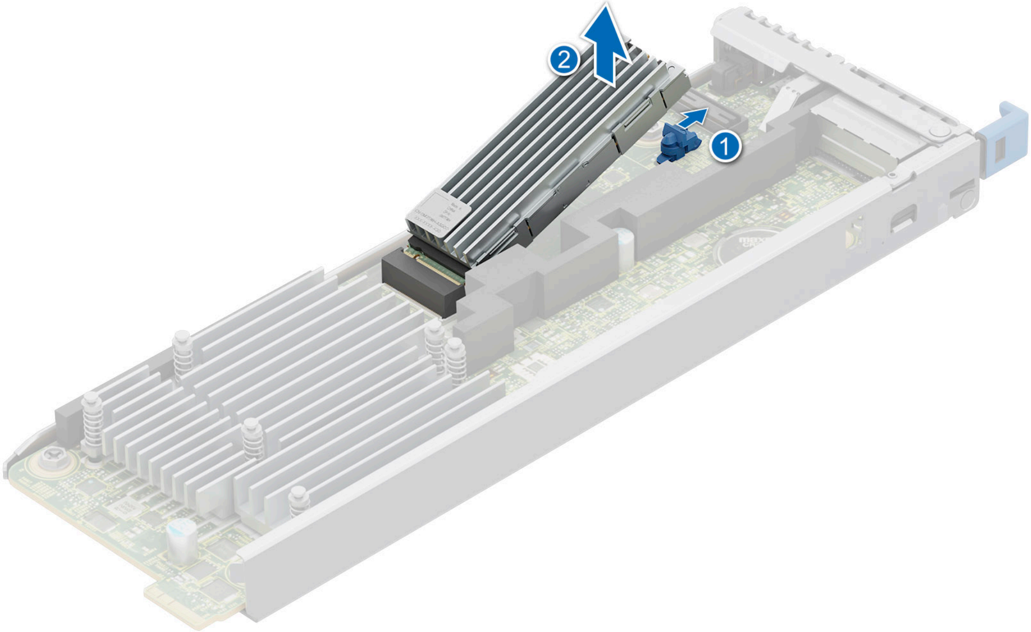


Figure 43. Removing the M.2 SSD module

Next steps

Replace the M.2 SSD module.

Installing the M.2 SSD module

Prerequisites

1. Follow the safety guidelines listed in the Safety instructions.
2. Follow the procedure listed in the Before working inside your system.

Steps

1. Align the M.2 SSD module at an angle with the M.2 connector on the system board.
2. Insert the M.2 SSD module until it is firmly seated in M.2 connector.

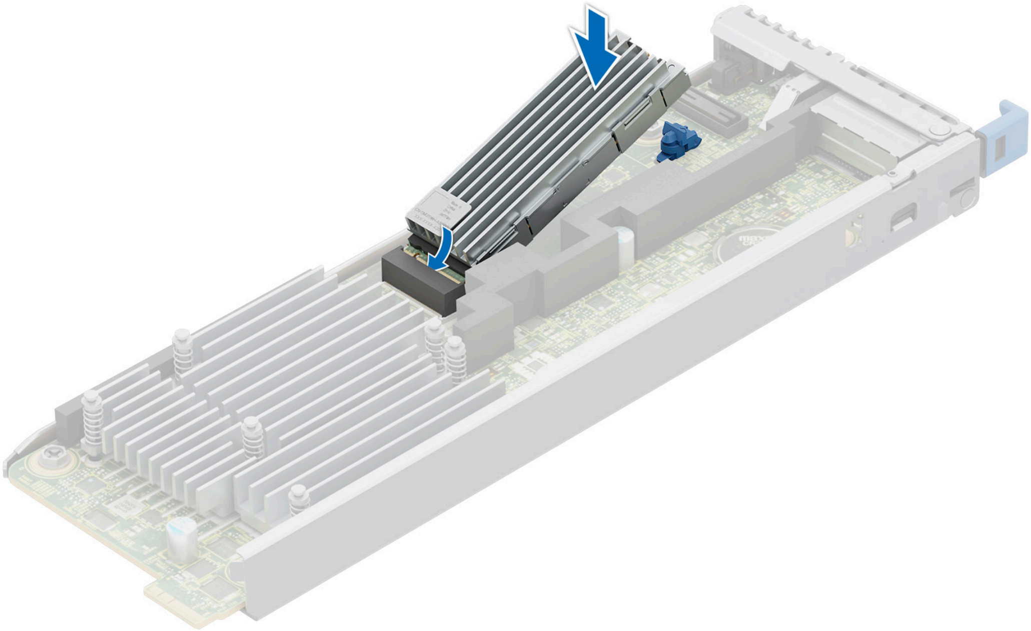


Figure 44. Installing the M.2 SSD module

Next steps

Follow the procedure listed in After working inside your system.

System battery

This is a service technician replaceable part only.

Replacing the system battery

Prerequisites

⚠ **WARNING: There is a danger of a new battery exploding if it is incorrectly installed. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions. See the Safety instructions that came with your system for more information.**

1. Follow the safety guidelines listed in the Safety instructions.
2. Follow the procedure listed in the Before working inside your system.

Steps

1. To remove the battery:
   a. Use a plastic scribe to pry out the system battery.

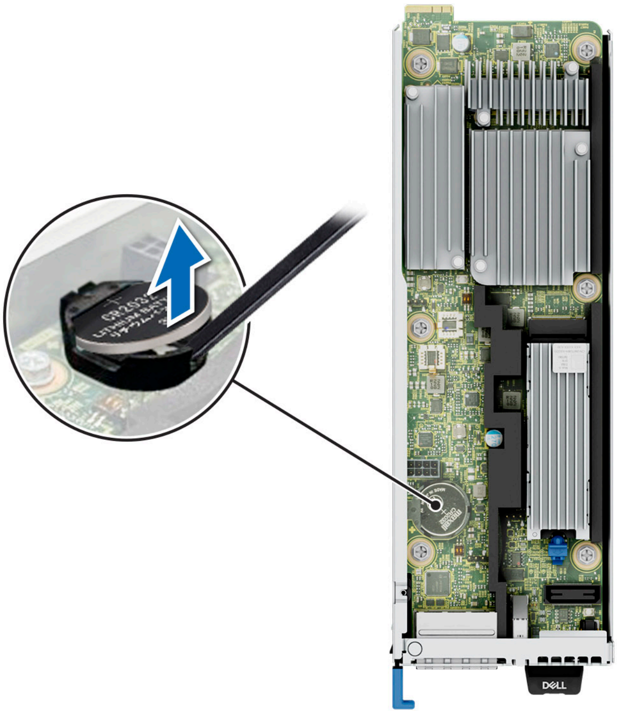


Figure 45. Removing the system battery

⚠ **CAUTION: To avoid damage to the battery connector, you must firmly support the connector while installing or removing a battery.**

2. To install a new system battery:
    a. Hold the battery with the positive side facing up and slide it under the securing tabs.
    b. Press the battery into the connector until it snaps into place.

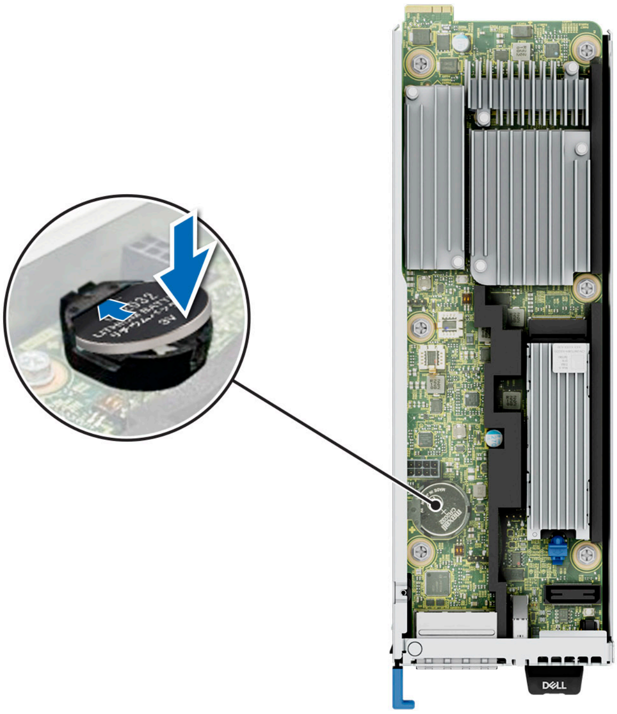


Figure 46. Installing the system battery

System board

This is a service technician replaceable part only.

Removing the system board

Prerequisites

1. Follow the safety guidelines listed in the Safety instructions.
2. Follow the procedure listed in the Before working inside your system.
3. Remove the following components:
    a. Witness sled
    b. M.2 module

Steps

1. Using a Phillips 2 screwdriver, remove the screws that secure the witness sled system board to the system.
2. Hold the witness sled system board by the edges and slide it towards the rear. Lift the system board out of the system.

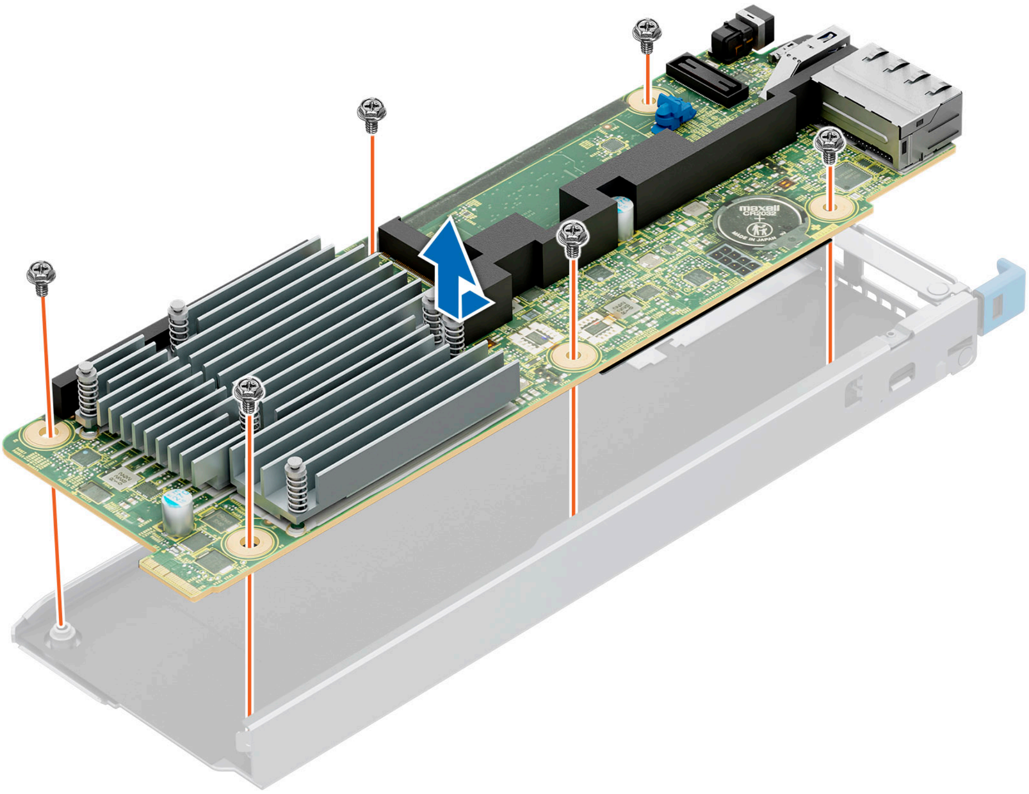


Figure 47. Removing the system board

Next steps

Install the system board.

Installing system board

Prerequisites

1. Follow the safety guidelines listed in the Safety instructions.
2. Follow the procedure listed in the Before working inside your system.
3. If you are replacing the system board, remove all the components that are listed in the removing the system board section.

Steps

1. Unpack the new system board assembly.
2. Holding the system board by the edges, lower the witness sled system board it into the system.
3. Align the connectors on the witness sled system board with the slots on the front of the system until the connectors are firmly seated in the slots.

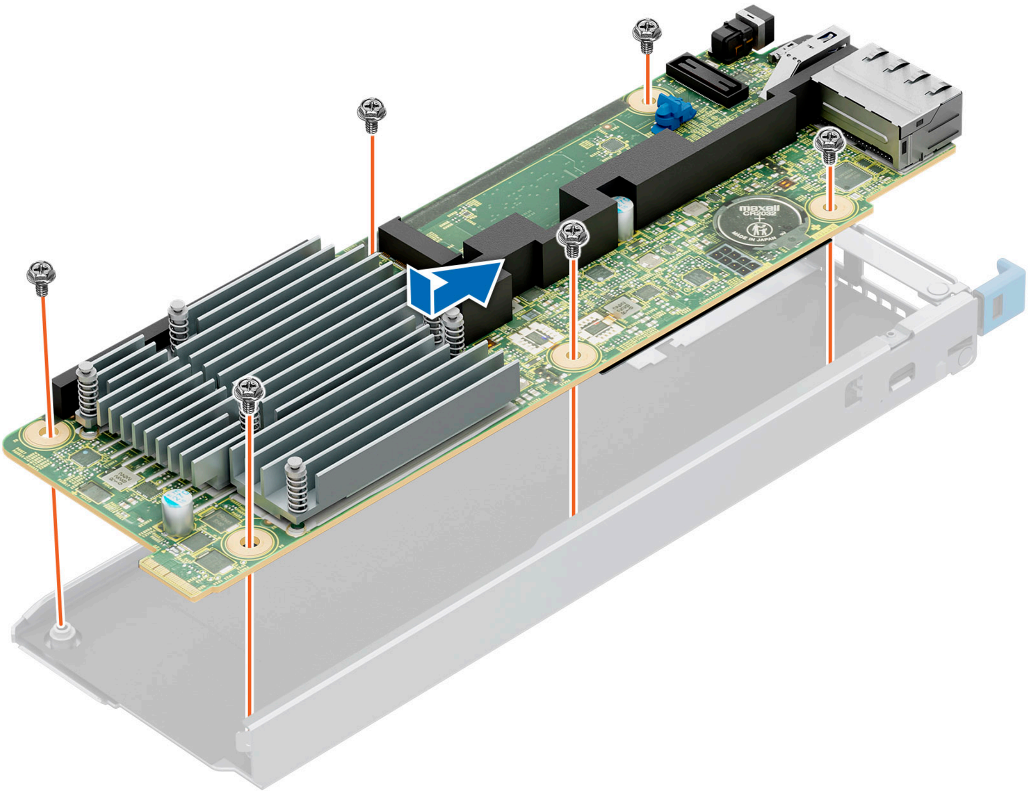


Figure 48. Installing the system board

Next steps

1. Replace the M.2 SSD module.

12

Recovery procedures

This section describes the different recovery methods for XR4000w system.

Topics:

Witness host deployment

Host deployment of the Witness should involve a supported host OS packaged with additional drivers or software that is required for a successful deployment of all Witness features.

When a bootable USB is inserted into the Witness node and the Witness is rebooted, the USB is booted to by default. Serial access to the Witness is required to deploy a host through this method (see: Witness serial communication). The supported methods of host deployment in this manner are:

- RASR

Recovering the Witness BIOS

Witness BIOS can be recovered using:

- Witness BIOS DUP flash
- SPI flashing the EEPROM chips

Witness BIOS does not have any software-based recovery procedures. As the Witness platform has two BIOS EEPROMs, failure to flash a BIOS to one EEPROM results in that ROM not being activated by the CM – thus preventing entry into a corrupt-BIOS scenario.

Recovering Witness BIOS: DUP flashing

As the Witness board contains two SPI EEPROM BIOS chips that are mixed by the chassis manager (CM), a corrupt BIOS on the active chip should be a recoverable situation.

The assumptions here are that:

1. The chassis manager (CM) is functional.
2. The Witness MCU is functional.
3. The Witness board is detectable by the chassis manager (CM).

Given these, applying a standard Witness BIOS DUP should:

1. Tell the chassis manager (CM) to start flashing the inactive BIOS EEPROM.
2. Once BIOS flash is complete chassis manager (CM) toggles the EEPROM mux. This sets the currently active, corrupt BIOS as “Inactive” and the newly flashed BIOS chip as “Active”.
3. The Witness should boot successfully from the now active EEPROM.

Recovering the Witness host OS

For recovering the Witness host, follow the RASR process under Witness host deployment.

Witness host installation: RASR

The RASR tool developed by the FEAR (Factory Enablement And Recovery) team can reimage a Witness host operating system along with any required drivers or packages. These packages include:

- Dell OS-Agent for Witness (DOSA-W)
  - More GPIO driver support packages
- Virtual Machine - VMware vSAN Witness Appliance

NOTE: The default password for the VMware vSAN Witness Appliance is @witness123!

For XR4000w Witness sled this tool is limited to ESXi.

For this process, two items are required:

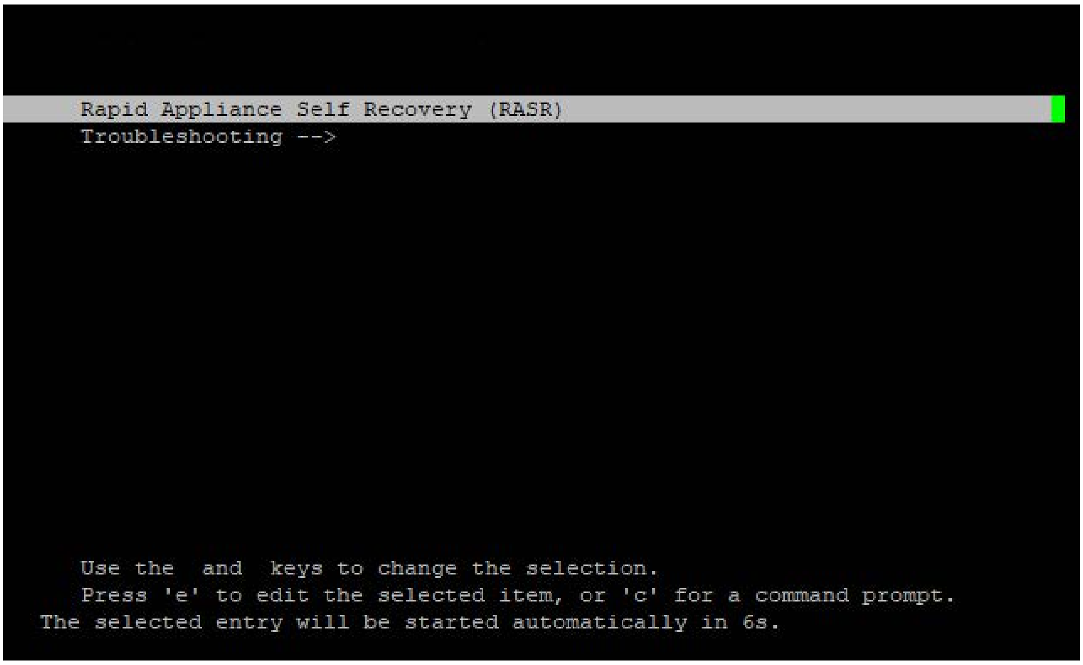
- An ISO created specifically for the RASR process
- An additional tool RASRISO-to-RASRUSB to create the bootable RASRUSB key

RASRUSB key is required since the XR4000w Witness sled does not have an iDRAC that can use virtual media functionality.

NOTE: Follow the instructions for using the RASRISO-to-RASRUSB tool to create a bootable RASRUSB key.

To perform the RASR installation process, the Witness sled must be powered off and the created RASRUSB key that is inserted. A serial connection to the Witness is required to interact with the RASR process. See Connecting to Witness via serial for details.

Upon powering the Witness back on, it should boot to the inserted USB. Once booted to the RASR drive, the only options available are to perform a Factory Reset or Quit. Selecting the Factory Reset option prompts the user for confirmation before beginning. During the reset process, the system reboots multiple times to facilitate the installation of the operating system and its packages or dependencies.



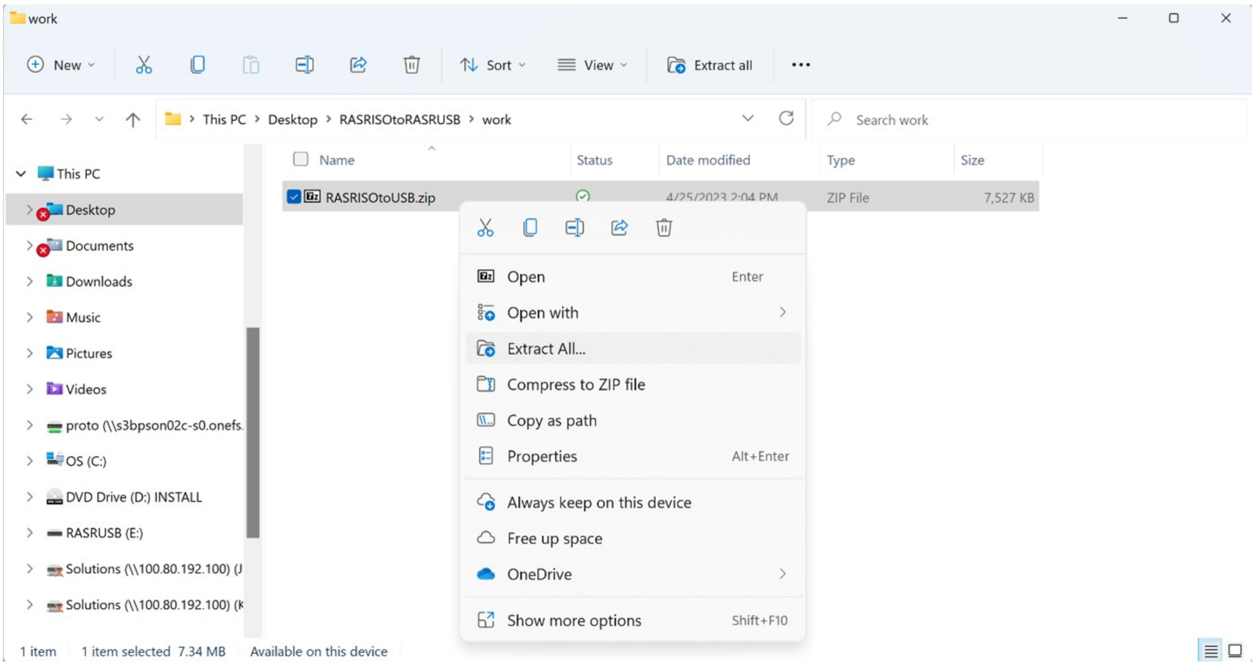
```
    Rapid Appliance Self Recovery (RASR)
    Troubleshooting -->




    Use the  and  keys to change the selection.
    Press 'e' to edit the selected item, or 'c' for a command prompt.
 The selected entry will be started automatically in 6s.
```

RASRISO to RASRUSB tool instructions

Follow the steps to create a RASRUSB key from RASR ISO file.

Extract the ISO image

1. Go to dell.com/support, enter XR4000w Witness sled service tag.
2. Download RASRISOtoUSB.zip from drivers and downloads section on the XR4000w support page.
3. Extract the RASRISOtoUSB.zip file.

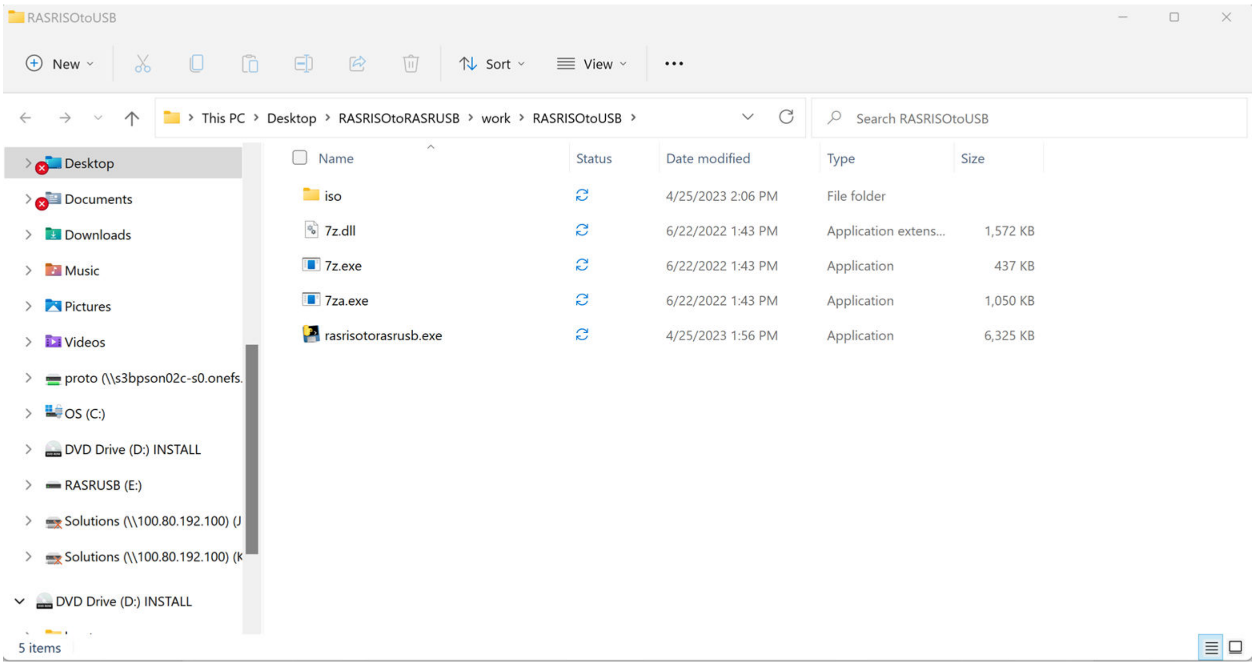

work
New
Sort
View
Extract all
This PC > Desktop > RASRISOtoRASRUSB > work
Search work
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
proto (\\s3bpson02c-s0.onefs.
OS (C:)
DVD Drive (D:) INSTALL
RASRUSB (E:)
Solutions (\\100.80.192.100) (J
Solutions (\\100.80.192.100) (K
Open Enter
Open with
Extract All...
Compress to ZIP file
Copy as path
Properties Alt+Enter
Always keep on this device
Free up space
OneDrive
Show more options Shift+F10
1 item 1 item selected 7.34 MB Available on this device

Name	Status	Date modified	Type	Size
☑ RASRISOtoUSB.zip	✓	4/25/2023 2:04 PM	ZIP File	7,527 KB

Figure 49. Extracting the ISO image

Check files

1. Confirm that the following files are visible after extracting.

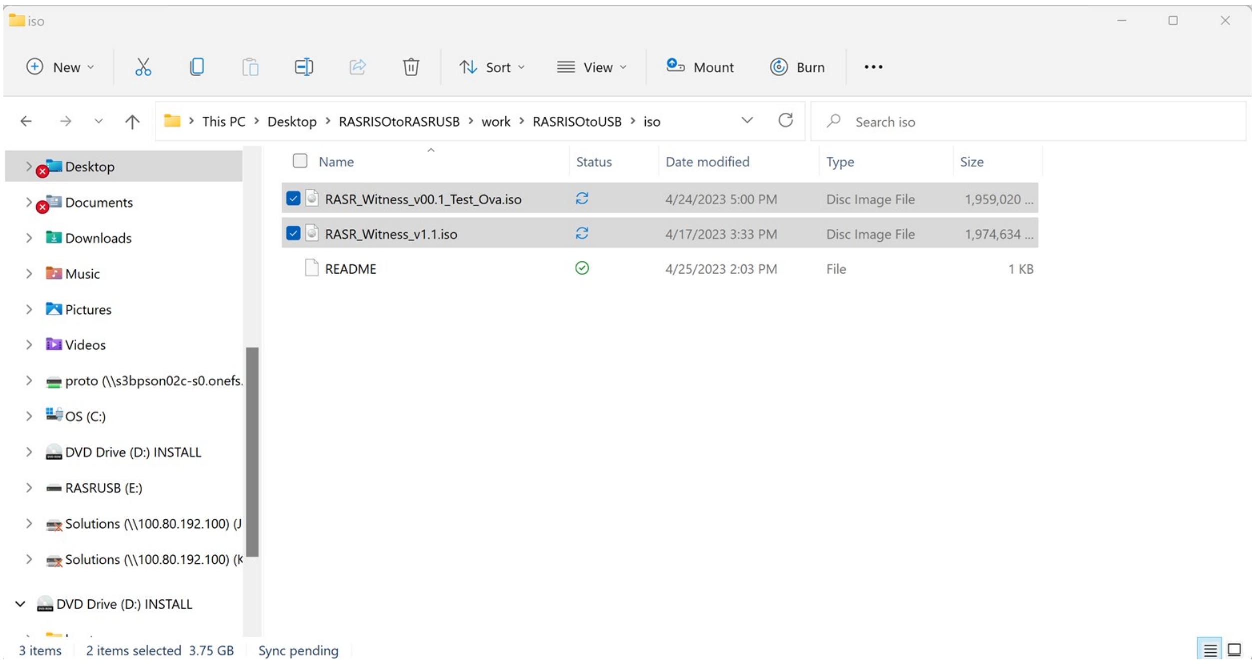


Name	Status	Date modified	Type	Size
iso	⟳	4/25/2023 2:06 PM	File folder	
7z.dll	⟳	6/22/2022 1:43 PM	Application extens...	1,572 KB
7z.exe	⟳	6/22/2022 1:43 PM	Application	437 KB
7za.exe	⟳	6/22/2022 1:43 PM	Application	1,050 KB
rasrisotorasrusb.exe	⟳	4/25/2023 1:56 PM	Application	6,325 KB

Figure 50. Extracted files

2. Copy RASR ISO file to the iso directory after extraction is complete.

   ⓘ **NOTE:** The RASR ISO file is copied to the iso directory after extracting the RASRISOtoUSB.zip file.

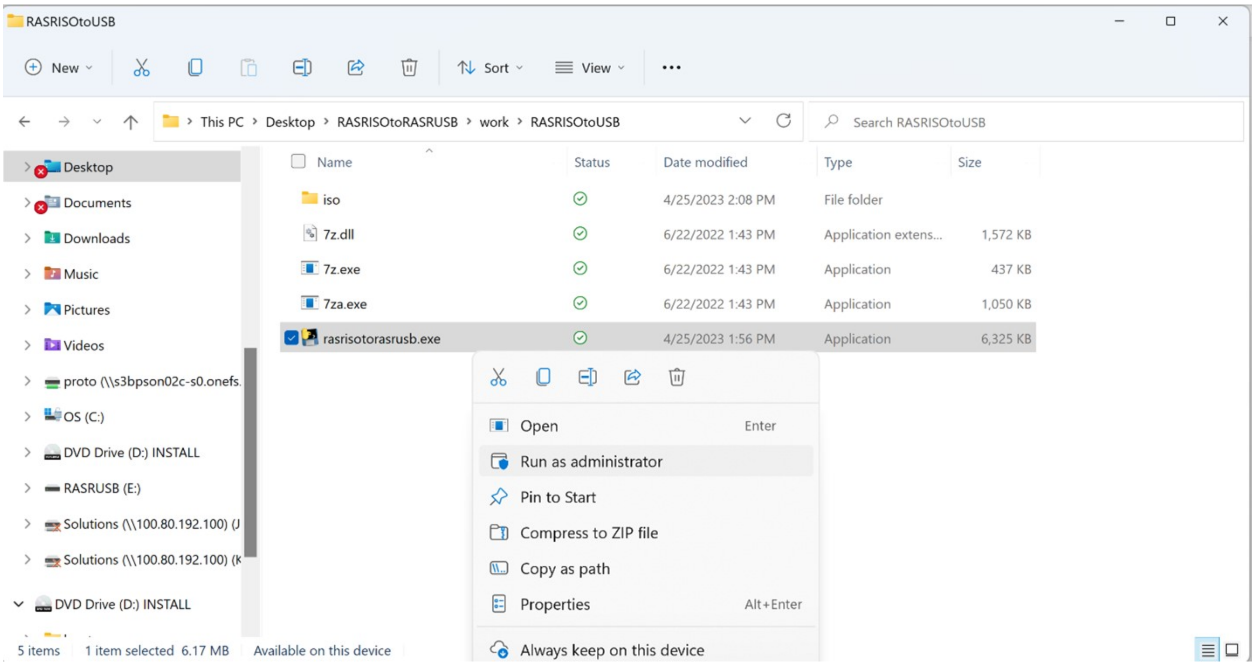

iso
New
Sort
View
Mount
Burn
This PC > Desktop > RASRISOtoRASRUSB > work > RASRISOtoUSB > iso
Search iso
Desktop
Documents
Downloads
Music
Pictures
Videos
proto (\\s3bpson02c-s0.onefs.
OS (C:)
DVD Drive (D:) INSTALL
RASRUSB (E:)
Solutions (\\100.80.192.100) (J
Solutions (\\100.80.192.100) (K
DVD Drive (D:) INSTALL
3 items 2 items selected 3.75 GB Sync pending

☐ Name	Status	Date modified	Type	Size
☑ RASR_Witness_v00.1_Test_Ova.iso		4/24/2023 5:00 PM	Disc Image File	1,959,020 ...
☑ RASR_Witness_v1.1.iso		4/17/2023 3:33 PM	Disc Image File	1,974,634 ...
README	✓	4/25/2023 2:03 PM	File	1 KB

Figure 51. RASRISO.iso files

Launch executable

Right click on "rasrisotorasrusb.exe" and run as administrator.

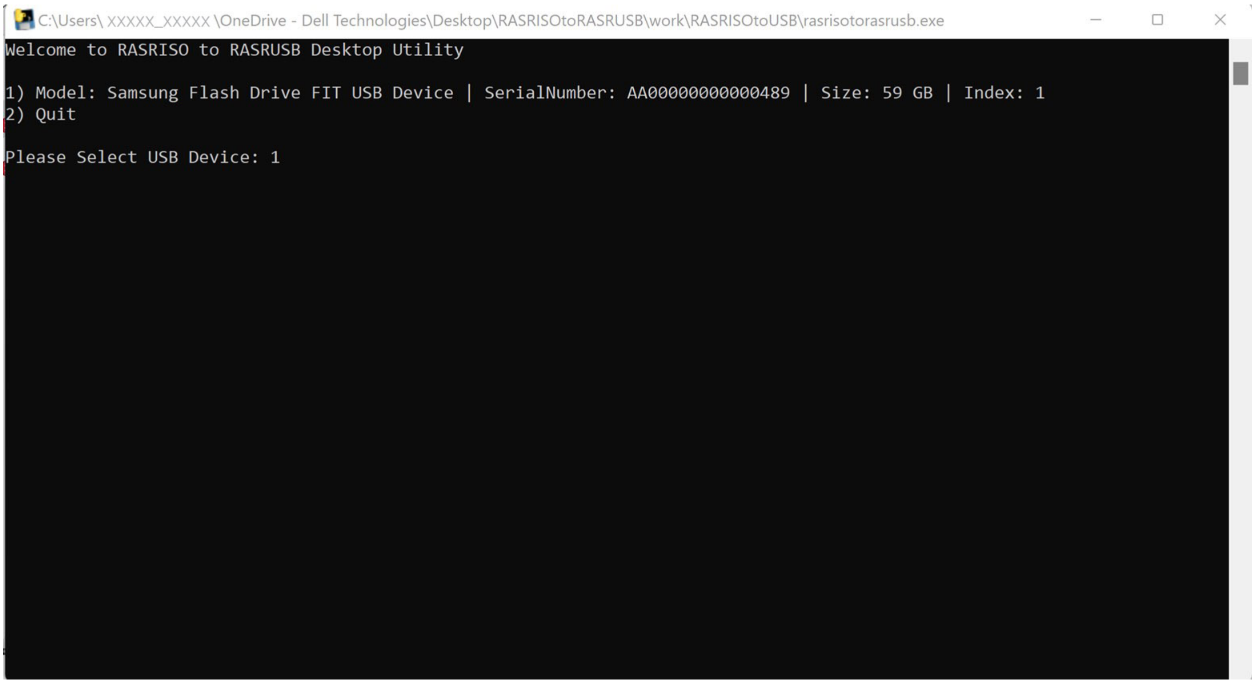


☐ Name	Status	Date modified	Type	Size
iso	✓	4/25/2023 2:08 PM	File folder	
7z.dll	✓	6/22/2022 1:43 PM	Application extens...	1,572 KB
7z.exe	✓	6/22/2022 1:43 PM	Application	437 KB
7za.exe	✓	6/22/2022 1:43 PM	Application	1,050 KB
☑ rasrisotorasrusb.exe	✓	4/25/2023 1:56 PM	Application	6,325 KB

Figure 52. Launch executable

Select USB device

1. Ensure that the USB device is plugged in. Select the USB device and press enter.



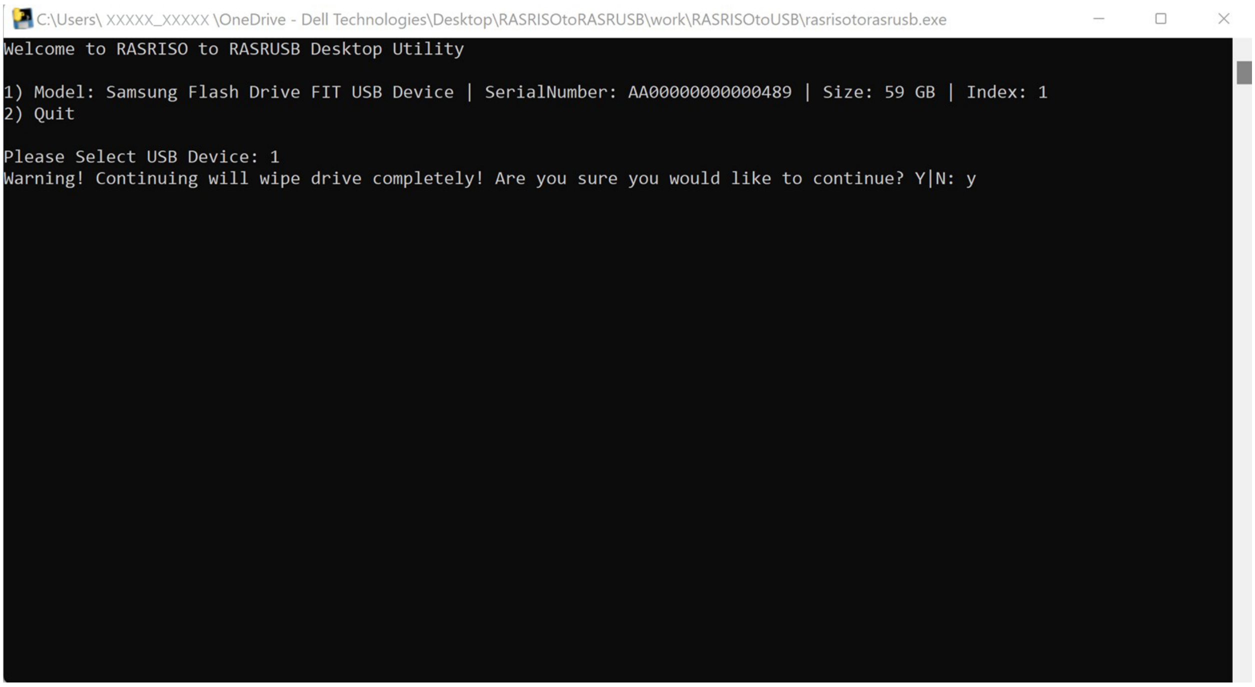
C:\Users\ XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISOtoUSB\rasrisotorasrusb.exe

```
Welcome to RASRISO to RASRUSB Desktop Utility

1) Model: Samsung Flash Drive FIT USB Device | SerialNumber: AA00000000000489 | Size: 59 GB | Index: 1
2) Quit

Please Select USB Device: 1
```

Figure 53. Selecting USB device

2. Confirm selection, and press enter.

ⓘ **NOTE:** USB device will be wiped after this step. Backup any important data in the USB before proceeding.

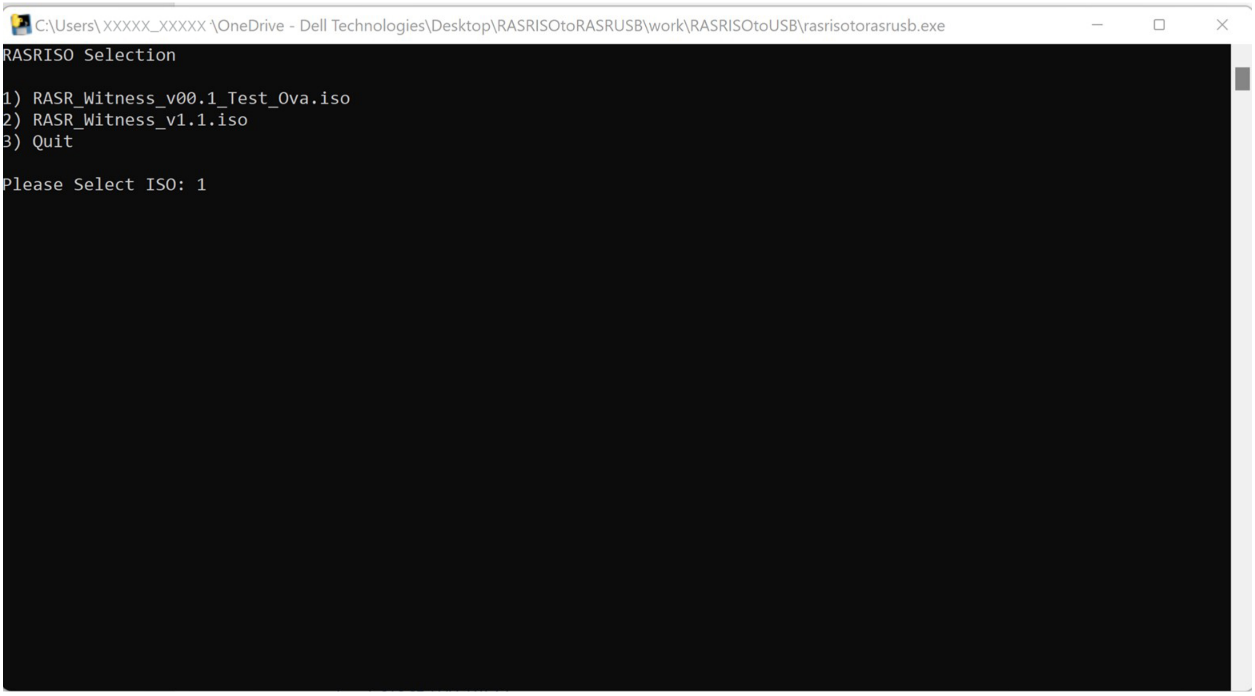


C:\Users\ XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISOtoUSB\rasrisotorasrusb.exe

```
Welcome to RASRISO to RASRUSB Desktop Utility

1) Model: Samsung Flash Drive FIT USB Device | SerialNumber: AA00000000000489 | Size: 59 GB | Index: 1
2) Quit

Please Select USB Device: 1
Warning! Continuing will wipe drive completely! Are you sure you would like to continue? Y|N: y
```

Select RASRISO

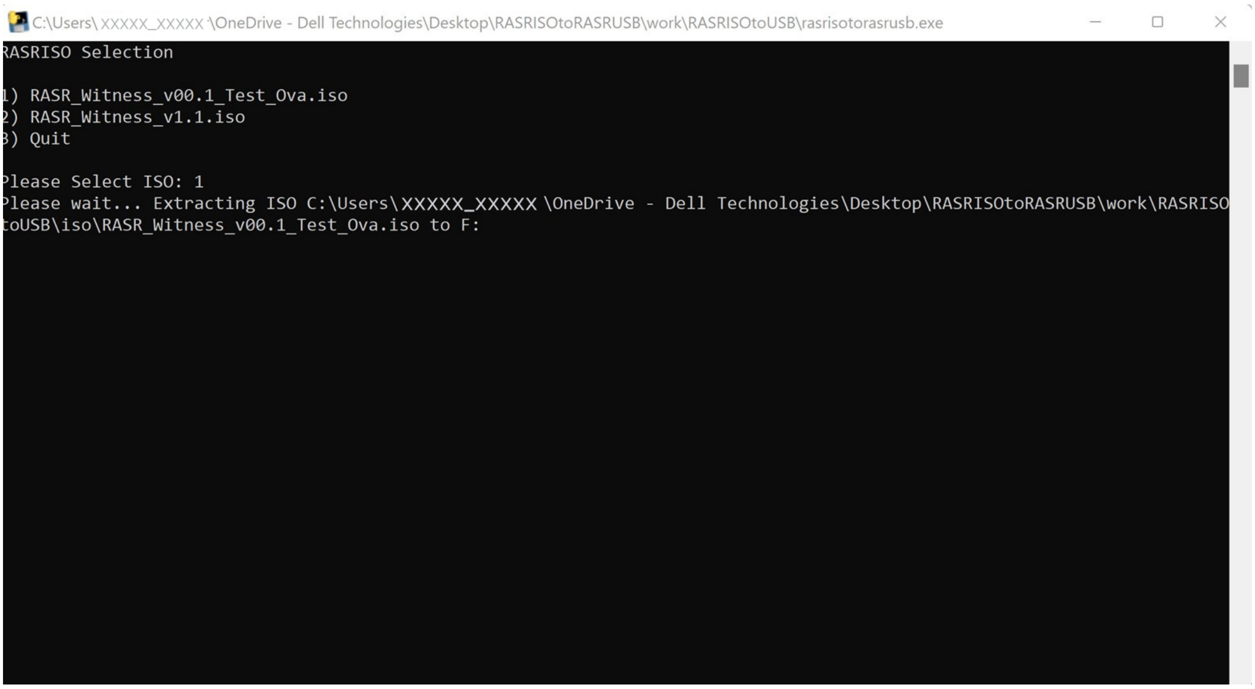
1. Select the RASRISO to use and press enter.


C:\Users\ XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISOtoUSB\rasrisotorasrusb.exe

```
RASRISO Selection

1) RASR_Witness_v00.1_Test_Ova.iso
2) RASR_Witness_v1.1.iso
3) Quit

Please Select ISO: 1
```

Figure 54. Selecting RASRISO

2. The contents of ISO are now being extracted to the USB device, this may take few minutes. Wait until extraction is complete.

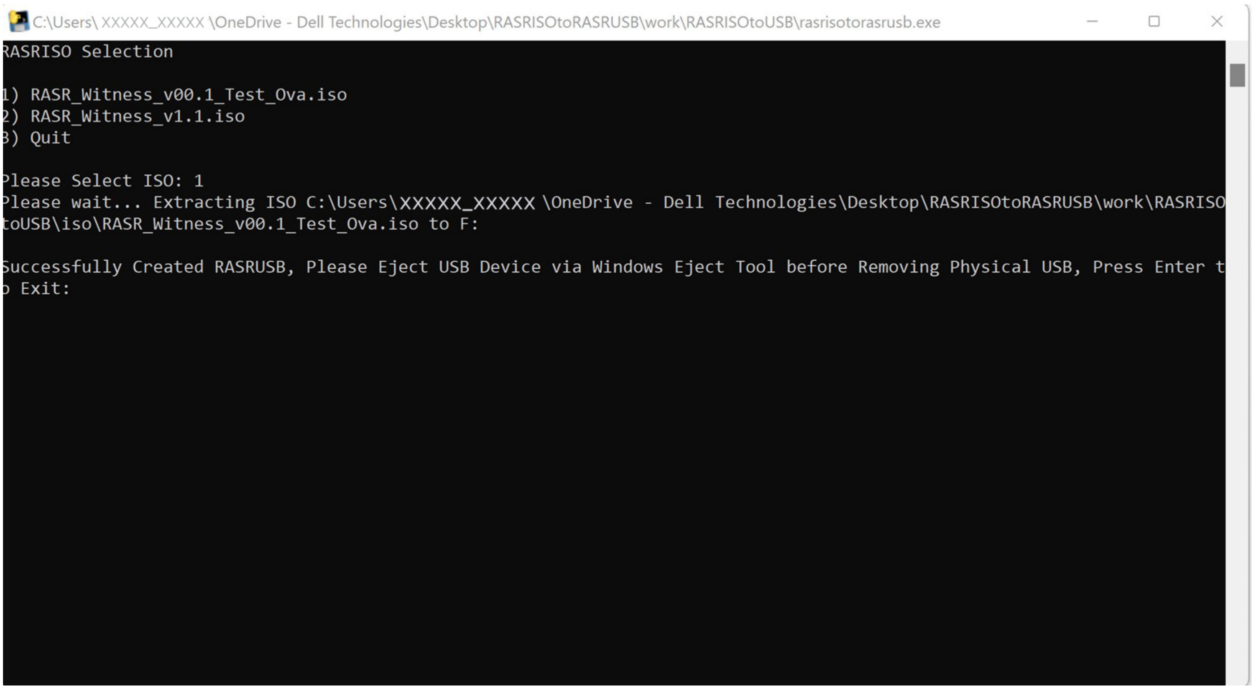

C:\Users\ XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISOtoUSB\rasrisotorasrusb.exe

```
RASRISO Selection

1) RASR_Witness_v00.1_Test_Ova.iso
2) RASR_Witness_v1.1.iso
3) Quit

Please Select ISO: 1
Please wait... Extracting ISO C:\Users\XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISO
toUSB\iso\RASR_Witness_v00.1_Test_Ova.iso to F:
```

Figure 55. Extracting iso contents to USB

Confirm completion

1. Once extraction is complete, the following message is displayed, "*Successfully created RASRUSB, please eject USB device visa Windows Eject Tool before removing physical USB, press enter to exit:*"



C:\Users\ XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISOtoUSB\rasrisotorasrusb.exe

```
RASRISO Selection

1) RASR_Witness_v00.1_Test_Ova.iso
2) RASR_Witness_v1.1.iso
3) Quit

Please Select ISO: 1
Please wait... Extracting ISO C:\Users\XXXXX_XXXXX \OneDrive - Dell Technologies\Desktop\RASRISOtoRASRUSB\work\RASRISO
toUSB\iso\RASR_Witness_v00.1_Test_Ova.iso to F:

Successfully Created RASRUSB, Please Eject USB Device via Windows Eject Tool before Removing Physical USB, Press Enter t
o Exit:
```

2. Rerun iso extraction if the process fails.

Eject USB

Eject USB device to ensure the files do not get corrupted before physically disconnecting USB.

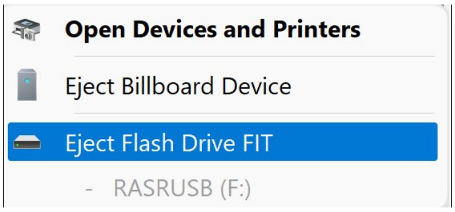


Figure 56. Ejecting USB

13

Reference and resolution guide

This section describes the common issues and resolutions for XR4000w system.

Topics:

Witness does not power on

Items to check:

1. Witness power LED does not turn on.
   a. Use Witness power control: CPLD to clear the CPLD power request byte.
   b. After clearing CPLD request byte, use Witness power operations to power on Witness.
2. Confirm that installation requirements are met.
3. Confirm that Witness BIOS is functional by Recovering the Witness BIOS.

Witness does not have serial output

Items to check:

1. Witness is not powered on.
   a. Use Witness power operations.
2. Improper serial connection.
   a. Use Connecting to Witness via serial.
3. Witness is booting.
   a. Serial output will appear to hang at several locations in the Witness boot process. Give the system enough time to fully boot.
4. Serial terminal is blank.
   a. Press a key (such as spacebar) to refresh the host OS serial output.

Witness information does not appear in iDRAC

Witness IP is not reported

NOTE: Witness IP does not require a valid Service Tag to populate in iDRAC front end.

Items to check:

1. Witness NIC 1 is improperly connected to a configured network.
   a. Ensure that all cables are securely plugged in.
2. Abnormal Witness NIC LED behavior.
   a. Link and Port LED do not illuminate.
   b. Link LED flickers once then stays dark.

      NOTE: This is most likely an issue with the Witness BIOS. See Recovering the Witness BIOS.
   c. Port activity LED lights up a steady yellow.

ⓘ **NOTE:** This means link is up but inactive. Connect to a properly configured network.

3. IP address does not appear in Witness host serial connection (Witness host network: Witness host OS).

   ⓘ **NOTE:** IP address does not appear in Witness host serial connection (Witness host network: Witness host OS).

4. DOSA-W package is not installed/DOSA-W package is not correctly deployed. Deploy or start the DOSA-W service. Witness DOSA-W deployment.
   a. As part of the above deployment, ensure that all host-specific steps have been followed. Example: Deployment on ESXi requires modification of kernel parameters through the "bootconfig" file.

If IP address still does not populate after the above steps, confirm that all firmware is up to date and that the connected network is configured properly. Finally, attempt an AC cycle of the chassis (with at least 30 seconds of AC OFF before AC ON).

Witness Service Tag, EPPID, MAC information not reported

Witness Service Tag, EPPID, and MAC information require a valid Witness Service Tag to populate in iDRAC front end.

Items to check:

1. Valid Service Tag in compute sled CPLD.
   a. Check for valid Service Tag in compute sled CPLD: User interfaces: CPLD, If no tag is found, move to step 2.
   b. If tag is found, allow time for CPLD to populate to iDRAC front end.
2. Valid Service Tag in Chassis Manager backup FRU/Witness FRUUse Witness Service Tag deployment to:
   - Check the CM backup FRU area for a valid Service Tag.
   - Check the Witness FRU for a valid Service Tag.
3. If CM does not have a valid tag, but the Witness does:
   a. Trigger the Easy Restore process by either rebooting the CM or physically reseating the Witness node.
   b. When CM is back up, repeat steps 1-2.
4. If neither CM nor Witness has a valid service tag:
   a. Use Witness Service Tag deployment to program a digital Service Tag that matches the physical Service Tag of the Witness.
   b. Trigger the Easy Restore Process by either rebooting the CM or physical reseating the Witness node.
   c. When CM is back up, repeat steps 1-2.

Chassis Manager, Witness MCU, or Witness BIOS DUPs failing

ⓘ **NOTE:** Witness BIOS DUPs should be expected to run anywhere from 45-90 minutes before completion.

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

1. Attempting to install incompatible firmware
2. iDRAC job queue task immediately “Failed” or stuck in “Scheduling (0%)”
   a. Clear iDRAC job queue with

      ```
      racadm jobqueue delete -i JID_CLEARALL_FORCE
      ```
   b. Reset the BMC
   c. Reattempt to install DUP

ⓘ **NOTE:** The XR4000w does not have a dedicated iDRAC interface. All references to iDRAC in this document are from the standpoint of the iDRAC interface that is on any of the installed XR4510c or XR4520c compute sleds.

Jumpers and connectors

This topic provides some basic and specific information about jumpers and switches. It also describes the connectors on the various boards in the system. Jumpers on the system board help to disable the system and reset the passwords. To install components and cables correctly, you must know the connectors on the system board.

Topics:

System board jumpers and connectors

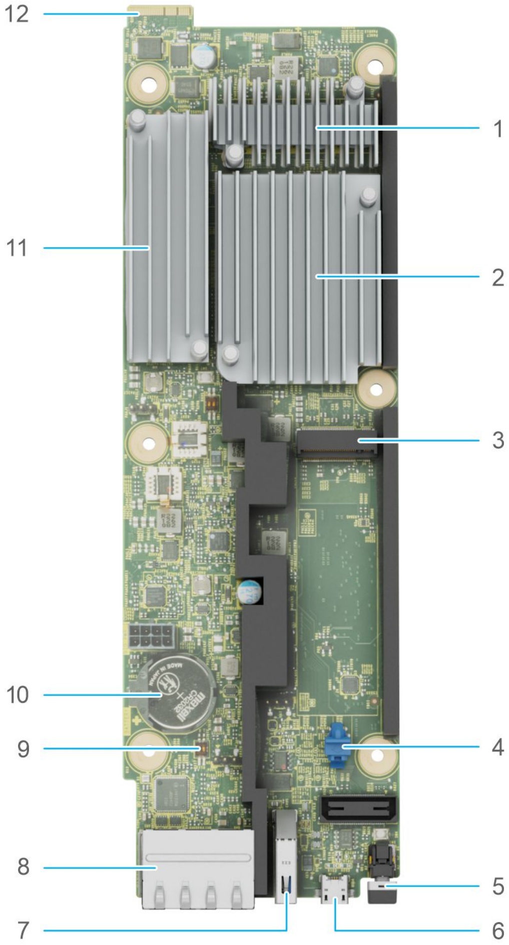


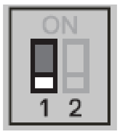
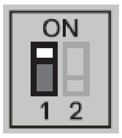
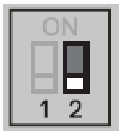
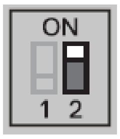
Figure 57. System board jumpers and connectors

1. Memory heat sink
2. Processor and heat sink
3. M.2 SSD card slot
4. M.2 SSD card latch
5. Power button
6. Micro USB connector for system console
7. USB 3.0 port
8. Network Interface Controller (NIC) ports
9. DIP switch
10. CMOS battery
11. Memory heat sink
12. PIB connector

DIP switch settings

For information about resetting the password using DIP switch, see the Disabling a forgotten password section.

Table 16. DIP switch settings

Jumper	Setting	Description
NVRAM_CLR	 (default)	The BIOS configuration settings are retained at system boot.
		The BIOS configuration settings are cleared at system boot.
PWRD_EN	 (default)	The BIOS password feature is enabled.
		The BIOS password feature is disabled.

⚠ **CAUTION: You should be cautious when changing the BIOS settings. The BIOS interface is designed for advanced users. Any changes in the setting might prevent your system from starting correctly and may even result in data loss.**

Disabling a forgotten password

The software security features of the system include a system password and a setup password. The password jumper enables or disables password features and clears any password(s) currently in use.

Prerequisites

⚠ **CAUTION: Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.**

Steps

1. Power off the compute sled and remove the compute sled from chassis.
2. Move the DIP switch on the system board from switches 1 and 2 to switches 2 and 3.

   ⓘ **NOTE:** Use a plastic scribe to change the DIP switch settings.

   ⓘ **NOTE:** The existing passwords are not disabled (erased) until the system boots with the DIP switch on switches 2 and 3. However, before you assign a new system and/or setup password, you must move the DIP switch back to switches 1 and 2.

   ⓘ **NOTE:** If you assign a new system and/or setup password with the DIP switch on switches 2 and 3, the system disables the new password(s) the next time it boots.

3. Insert compute sled into chassis and power on the compute sled.
4. Power off the compute sled and remove the compute sled from chassis.
5. Move the DIP switch on the system board from switches 2 and 3 to switches 1 and 2.
6. Insert compute sled into chassis and power on the compute sled.
7. Assign a new system and/or setup password.

15

Getting help

Topics:

Recycling or End-of-Life service information

Take back and recycling services are offered for this product in certain countries. If you want to dispose of system components, visit www.dell.com/recyclingworldwide and select the relevant country.

Contacting Dell Technologies

Dell provides online and telephone based support and service options. If you do not have an active internet connection, you can find Dell contact information on your purchase invoice, packing slip, bill or Dell product catalog. The availability of services varies depending on the country and product, and some services may not be available in your area. To contact Dell for sales, technical assistance, or customer service issues follow these steps:

Steps

1. Go to www.dell.com/support/home.
2. Select your country from the drop-down menu on the lower right corner of the page.
3. For customized support:
   a. Enter the system Service Tag in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field.
   b. Click **Search**.
      The support page that lists the various support categories is displayed.
4. For general support:
   a. Select your product category.
   b. Select your product segment.
   c. Select your product.
      The support page that lists the various support categories is displayed.
5. For contact details of Dell Global Technical Support:
   a. Click Contact Technical Support.
   b. The **Contact Technical Support** page is displayed with details to call, chat, or e-mail the Dell Global Technical Support team.

Accessing system information by using QRL

You can use the Quick Resource Locator (QRL) located on the information tag in the front of the XR4000w system, to access information about PowerEdge XR4000w. There is also another QRL for accessing product information located on the back of the system cover.

Prerequisites

Ensure that your smartphone or tablet has a QR code scanner installed.

The QRL includes the following information about your system:

- How-to videos
- Reference materials, including the Installation and Service Manual, and mechanical overview
- The system service tag to quickly access the specific hardware configuration and warranty information
- A direct link to Dell to contact technical assistance and sales teams

Steps

1. Go to www.dell.com/qrl, and navigate to your specific product or
2. Use your smart phone or tablet to scan the model-specific Quick Resource (QR) code on your system or in the Quick Resource Locator section.

Quick Resource Locator for PowerEdge XR4000w system

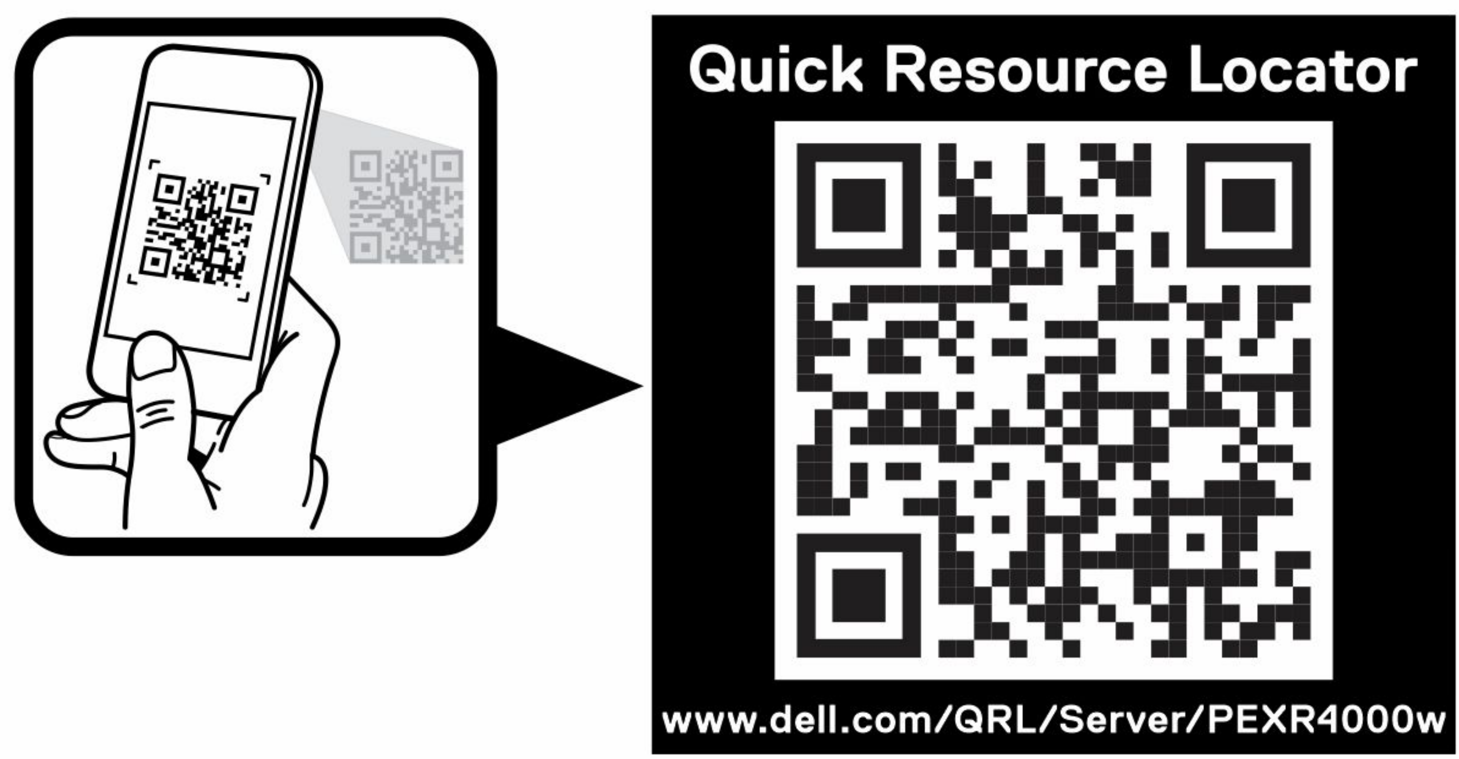


Figure 58. Quick Resource Locator for PowerEdge XR4000w system

Receiving automated support with SupportAssist

Dell SupportAssist is an optional Dell Services offering that automates technical support for your Dell server, storage, and networking devices. By installing and setting up a SupportAssist application in your IT environment, you can receive the following benefits:

- Automated issue detection — SupportAssist monitors your Dell devices and automatically detects hardware issues, both proactively and predictively.
- Automated case creation — When an issue is detected, SupportAssist automatically opens a support case with Dell Technical Support.
- Automated diagnostic collection — SupportAssist automatically collects system state information from your devices and uploads it securely to Dell. This information is used by Dell Technical Support to troubleshoot the issue.
- Proactive contact — A Dell Technical Support agent contacts you about the support case and helps you resolve the issue.

The available benefits vary depending on the Dell Service entitlement purchased for your device. For more information about SupportAssist, go to www.dell.com/supportassist.

16

Documentation resources

This section provides information about the documentation resources for your system.

To view the document that is listed in the documentation resources table:

- From the Dell support site:
  1. Click the documentation link that is provided in the Location column in the table.
  2. Click the required product or product version.

     ⓘ **NOTE:** To locate the model number, see the front of your system.
  3. On the Product Support page, click **Documentation**.
- Using search engines:
  - Type the name and version of the document in the search box.

Table 17. Additional documentation resources for your system

Task	Document	Location
Setting up your system	For information about setting up your system, see the *Getting Started Guide* document that is shipped with your system.	www.dell.com/poweredgemanuals
Configuring your system	For information about the iDRAC features, configuring and logging in to iDRAC, and managing your system remotely, see the Integrated Dell Remote Access Controller User's Guide. For information about understanding Remote Access Controller Admin (RACADM) subcommands and supported RACADM interfaces, see the RACADM CLI Guide for iDRAC. For information about Redfish and its protocol, supported schema, and Redfish Eventing implemented in iDRAC, see the Redfish API Guide. For information about iDRAC property database group and object descriptions, see the Attribute Registry Guide. For information about Intel QuickAssist Technology, see the Integrated Dell Remote Access Controller User's Guide.	www.dell.com/poweredgemanuals
	For information about earlier versions of the iDRAC documents. To identify the version of iDRAC available on your system, on the iDRAC web interface, click **?** > **About**.	www.dell.com/idracmanuals
	For information about installing the operating system, see the operating system documentation.	www.dell.com/operatingsystemmanuals
	For information about updating drivers and firmware, see the Methods to download firmware and drivers section in this document.	www.dell.com/support/drivers

Table 17. Additional documentation resources for your system (continued)

Task	Document	Location
Managing your system	For information about systems management software offered by Dell, see the Dell OpenManage Systems Management Overview Guide.	www.dell.com/poweredgemanuals
	For information about setting up, using, and troubleshooting OpenManage, see the Dell OpenManage Server Administrator User's Guide.	www.dell.com/openmanagemanuals > OpenManage Server Administrator
	For information about installing and using Dell Secure Connect Gateway, see the Dell Secure Connect Gateway Enterprise User's Guide.	https://www.dell.com/serviceabilitytools
	For information about partner programs enterprise systems management, see the OpenManage Connections Enterprise Systems Management documents.	www.dell.com/openmanagemanuals
Working with the Dell PowerEdge RAID controllers	For information about understanding the features of the Dell PowerEdge RAID controllers (PERC), Software RAID controllers, or BOSS card and deploying the cards, see the Storage controller documentation.	www.dell.com/storagecontrollermanuals
Understanding event and error messages	For information about the event and error messages generated by the system firmware and agents that monitor system components, go to qrl.dell.com > **Look Up** > **Error Code**, type the error code, and then click **Look it up**.	www.dell.com/qrl
Troubleshooting your system	For information about identifying and troubleshooting the PowerEdge server issues, see the Server Troubleshooting Guide.	www.dell.com/poweredgemanuals