Dell EMC OpenManage Port Information Guide

Version 10.2.0.0

June 2021
Rev. A00

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

Introduction

The Dell EMC OpenManage Port Information document helps system administrators and technicians to identify the ports usage in Dell EMC OpenManage systems management software, standard operating system services, and other agent applications.

NOTE: This document includes sections or data that is not applicable to the PowerEdge MX740x and PowerEdge MX840c.

Topics:

Accessing support content from the Dell EMC support site

Access supporting content related to an array of systems management tools using direct links, going to the Dell EMC support site, or using a search engine.

- Direct links:
  - For Dell EMC Enterprise Systems Management and Dell EMC Remote Enterprise Systems Management—https://www.dell.com/esmmanuals
  - For Dell EMC Virtualization Solutions—www.dell.com/virtualizationsolutions
  - For Dell EMC OpenManage—https://www.dell.com/openmanagemanuals
  - For iDRAC—https://www.dell.com/idracmanuals
  - For Dell EMC OpenManage Connections Enterprise Systems Management—https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - For Dell EMC Serviceability Tools—https://www.dell.com/serviceabilitytools
- Dell EMC support site:
  1. Go to https://www.dell.com/support.
  2. Click **Browse all products**.
  3. From the **All products** page, click **Software**, and then click the required link.
  4. Click the required product and then click the required version.

Using search engines, type the name and version of the document in the search box.

Other Documents You May Need

In addition to this guide, you can access the following guides available at **www.dell.com/Support/Home**.

- The *Dell EMC Systems Software Support Matrix* provides information about the various Dell systems, the operating systems supported by these systems, and the Dell EMC OpenManage components that can be installed on these systems.
- The *Dell EMC OpenManage Server Administrator Installation Guide* contains instructions to help you install Dell EMC OpenManage Server Administrator.
- The *Dell EMC OpenManage Management Station Software Installation Guide* contains instructions to help you install Dell EMC OpenManage management station software that includes Baseboard Management Utility, DRAC Tools, and Active Directory Snap-In.
- The *Dell EMC OpenManage Server Administrator SNMP Reference Guide* documents the Simple Network Management Protocol (SNMP) management information base (MIB). The SNMP MIB defines variables that extend the standard MIB to cover the capabilities of systems management agents.

- The *Dell EMC OpenManage Server Administrator CIM Reference Guide* documents the Common Information Model (CIM) provider, an extension of the standard management object format (MOF) file. The CIM provider MOF documents supported classes of management objects.
- The *Dell EMC OpenManage Server Administrator Messages Reference Guide* lists the messages that are displayed in your **Server Administrator** home page Alert log or on your operating system's event viewer. This guide explains the text, severity, and causes of each Instrumentation Service Alert message that Server Administrator issues.
- The *Dell EMC OpenManage Server Administrator Command Line Interface User's Guide* documents the complete command-line interface for Server Administrator, including an explanation of CLI commands to view system status, access logs, create reports, configure various component parameters, and set critical thresholds.
- The *Integrated Dell Remote Access Controller User's Guide* provides detailed information on configuring and using the iDRAC.
- The *Dell Chassis Management Controller User's Guide* provides detailed information on installing, configuring and using CMC.
- The *Dell Online Diagnostics User's Guide* provides complete information on installing and using Online Diagnostics on your system.
- The *Dell EMC OpenManage Baseboard Management Controller Utilities User Guide* provides additional information about using Server Administrator to configure and manage your system's BMC.
- The *Dell EMC OpenManage Server Administrator Storage Management User's Guide* is a comprehensive reference guide for configuring and managing local and remote storage attached to a system.
- The *Dell Remote Access Controller RACADM User's Guide* provides information about using the RACADM command-line utility.
- The *Dell Remote Access Controller 5 User's Guide* provides complete information about installing and configuring a DRAC 5 controller and using DRAC 5 to remotely access an inoperable system.
- The *Dell Update Packages User's Guide* provides information about obtaining and using Dell Update Packages as part of your system update strategy.
- The *Dell EMC OpenManage Server Update Utility User's Guide* provides information about obtaining and using the Server Update Utility (SUU) to update your Dell systems or to view the updates available for any systems listed in the Repository.
- The *Dell Management Console User's Guide* has information about installing, configuring, and using Dell Management Console. Dell Management Console is a Web-based systems management software that enables you to discover and inventory devices on your network. It also provides advanced functions, such as health and performance monitoring of networked devices and patch management capabilities for Dell systems.
- The *Dell EMC OpenManage Essentials User's Guide* has information about installing, configuring, and using Dell EMC OpenManage Essentials. OpenManage Essentials is a hardware management application that provides a comprehensive view of Dell systems, devices, and components in the enterprise's network.
- The *Dell Lifecycle Controller User Guide* provides information on setting up and using the Unified Server Configurator to perform systems and storage management tasks throughout your system's lifecycle. You can use the Unified Server Configurator to deploy an operating system, configure a Redundant Array of Independent Disks (RAID), and run diagnostics to validate the system and attached hardware. Remote Services capabilities enable automated system platform discovery by management consoles and enhance remote operating system deployment capabilities. These capabilities are exposed through the web services based hardware management interface provided by the Lifecycle Controller firmware.

Contacting Dell EMC

NOTE: If you do not have an active Internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell EMC product catalog.

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell EMC for sales, technical support, or customer service issues:

1. Go to **Dell.com/support.**
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.

2

Ports

The following tables list the ports used by the OpenManage systems management software, standard operating system services and other agent applications.

NOTE: Ports with the correct configuration are necessary to allow OpenManage systems management software to connect to a remote device through firewalls.

NOTE: The systems management software version mentioned indicates the minimum version of the product required to use that port.

NOTE: CIM ports are dynamic. See the Microsoft knowledge base at `support.microsoft.com` for information on CIM port usage.

NOTE: If you are using a firewall, you must open all ports listed in the following tables to ensure that OpenManage applications function correctly.

Topics:

OpenManage Essentials

Management Stations

Table 1. Supported Protocols and Ports on Management Stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
25	SMTP	TCP	None	In/Out	Optional email alert action
162	SNMP	UDP	None	In	Event reception through SNMP
1433	Proprietary	TCP	None	In/Out	Optional remote SQL server access
2607	HTTPS	TCP	128-bit SSL	In/Out	Web GUI
1278	HTTP	TCP	None	In/Out	To launch OME console over HTTP

Managed Nodes

Table 2. Supported Protocols and Ports on Managed Nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
22	SSH	TCP	128 – bit	In/Out	Contextual application launch — SSH client Remote software updates to Server Administrator— for systems supporting Linux operating systems Performance monitoring in Linux systems
80	HTTP	TCP	None	In/Out	Contextual application launch — PowerConnect console
135	RPC	TCP/ UDP	None	In/Out	Remote software update transfer to Server Administrator—for systems supporting Windows operating systems Remote Command Line — for systems supporting Windows operating systems
139	NetBIOS	TCP	None	In/Out	Remote Software Update (for Windows operating systems)
161	SNMP	UDP	None	In/Out	SNMP query management

Table 2. Supported Protocols and Ports on Managed Nodes (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
443*	Proprietary/ WSMAN	TCP	None	In/Out	iDRAC/OMSA communication
623*	RMCP	UDP	None	In/Out	IPMI access through LAN
1433	Proprietary	TCP	None	In/Out	Optional remote SQL server access
3389	RDP	TCP	128 - bit SSL	In/Out	Contextual application launch —Remote desktop to Windows terminal services
6389	Proprietary	TCP	None	In/out	EMC storage discovery and inventory. Enables communication between a host system (through NaviCLI/NaviSec CLI or Navisphere host agent) and a Navisphere Array Agent on a Storage system

* — If ports 443 and 623 are changed in iDRAC, ensure that you change these ports in the OME discovery wizard as well, so that OME can communicate with iDRAC on the new ports.

Chassis Management Controller

Table 3. Supported Protocols and Ports

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
20	FTP	TCP	None	Out	FTP data client	No
21	FTP	TCP	None	Out	FTP command client	No
22	SSH	TCP	128-bit	In	SSH server	Yes
23	Telnet	TCP	None	In	Telnet server	Yes
25	SMTP	TCP	None	Out	SMTP client	No
53	DNS	TCP	None	Out	DNS client	No
67*	DHCP	UDP	None	Out	DHCP client	No
68*	DHCP	UDP	None	In	DHCP client	No
69	TFTP	UDP	None	Out	TFTP client	No
80	HTTP	TCP	None	In	HTTP server	Yes
161	SNMP	UDP	None	In	SNMP Agent (server)	No
162	SNMP	UDP	None	Out	SNMP trap client	No
443	HTTPS	TCP	128–bit	In	HTTPS server	Yes
514	Syslog	TCP	None	Out	Syslog client	Yes

Table 3. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
636	LDAP	TCP	SSL	Out	LDAPS, Active Directory client	Yes
3269	LDAP	TCP	None	Out	Active Directory client	No
8081	HTTP	TCP	None	Out	Link and Launch to FN-IOA, MXL-IOA	No

* — When a DHCP client connects to a DHCP server, the source port is 68 and the destination port is 67. When the DHCP server responds to the DHCP client, the source port is 67 and destination port is 68. The CMC acts as a DHCP client.

OpenManage Integration for VMware vCenter

NOTE: When deploying the Server Administrator agent using the Fix non-compliant vSphere hosts link available from the Compliance window in the Dell Management Center, the OpenManage Integration for VMware vCenter starts the http Client service and enables port 8080 on and releases after ESXi 5.0 to download OMSA VIB and install it. Once the OMSA installation is completed, the service automatically stops and the port is closed.

Virtual Appliance

Table 4. Supported Protocols and Ports on Virtual Appliance

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
53	DNS	TCP	None	Out	OMIVV appliance to DNS server	DNS client	Connectivity to the DNS server or resolving the host names.
69	TFTP	UDP	None	Out	OMIVV appliance to TFTP server	TFTP Client	Used for firmware update on 11G servers with old firmware.
80/443	HTTP/ HTTPS	TCP	None	Out	OMIVV appliance to internet	Dell Online Data Access	Connectivity to the online (Internet) warranty, firmware, and latest RPM information.
80	HTTP	TCP	None	In	ESXi server to OMIVV appliance	HTTP server	Used in operating system deployment flow for post installation scripts to communicate with the OMIVV appliance.

Table 4. Supported Protocols and Ports on Virtual Appliance (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
162	SNMP Agent	UDP	None	In	iDRAC/ESXi to OMIVV appliance	SNMP Agent (server)	To receive SNMP traps from managed nodes.
443	HTTPS	TCP	128-bit	In	OMIVV UI to OMIVV appliance	HTTPS server	Web services offered by OMIVV. These Web services are consumed by vCenter Web Client and Dell Admin portal.
443	WSMan	TCP	128-bit	In/Out	OMIVV appliance to/ from iDRAC/ OMSA	iDRAC/OMSA communicatio n	iDRAC, OMSA, and CMC or Management Module communicatio n, used to manage and monitor the managed nodes.
445	SMB	TCP	128-bit	Out	OMIVV appliance to CIFS	CIFS communicatio n	To communicate with Windows share.
4433	HTTPS	TCP	128-bit	In	iDRAC to OMIVV appliance	Auto Discovery	Provisioning server that is used for auto discovering managed nodes.
2049	NFS	UDP/TCP	None	In/Out	OMIVV appliance to NFS	Public Share	NFS public share that is exposed by OMIVV appliance to the managed nodes and used in firmware update and operating system deployment flows.
4001 to 4004	NFS	UDP/TCP	None	In/Out	OMIVV appliance to NFS	Public Share	These ports must be kept open to run the statd, quotd, lockd,

Table 4. Supported Protocols and Ports on Virtual Appliance (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
							and mountd services by the V2 and V3 protocols of the NFS server.
11620	SNMP Agent	UDP	None	In	iDRAC to OMIVV appliance	SNMP Agent (server)	Port used to receive the standard SNMP alerts by using UDP: 162. Data from iDRAC, OMSA, and CMC or Management Module are received to manage and monitor the managed nodes.
User-defined	Any	UDP/TCP	None	Out	OMIVV appliance to proxy server	Proxy	To communicate with the proxy server.

Managed Nodes (ESXi)

Table 5. Supported Protocols and Ports on Managed Nodes

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
162, 11620	SNMP	UDP	None	Out	ESXi to OMIVV appliance	Hardware Events	Asynchronous SNMP traps sent from ESXi. This port has to open from ESXi.
443	WSMan	TCP	128-bit	In	OMIVV appliance to ESXi(OMSA)	iDRAC/ OMSA communicatio n	Used to provide information to the management station. This port has to open from ESXi.
443	HTTPS	TCP	128-bit	In	OMIVV appliance to ESXi	HTTPS server	Used to provide information to the management

Table 5. Supported Protocols and Ports on Managed Nodes (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
							station. This port has to open from ESXi.
8080	HTTP	TCP	128-bit	Out	ESXi to OMIVV appliance	HTTP server; downloads the OMSA VIB and fixes non-compliant vSphere hosts.	Helps ESXi to download the OMSA/driver VIB.

Managed Nodes (iDRAC or CMC or Management Module)

Table 6. Supported Protocols and Ports on Managed Nodes

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
443	WSMan/ HTTPS, REST/HTTPS	TCP	128-bit	In	OMIVV appliance to iDRAC or CMC or Management Module	iDRAC communicatio n	Used to provide information to the management station and communicate to MX chassis by using REST or HTTPS protocols. This port has to open from iDRAC and CMC or Management Module.
4433	HTTPS	TCP	128-bit	Out	iDRAC to OMIVV appliance	Auto Discovery	For auto discovering iDRAC (managed nodes) in the management station.
2049	NFS	UDP	None	In/Out	iDRAC to/from OMIVV	Public Share	For iDRAC to access NFS public share that is exposed by OMIVV appliance. That is used for operating system deployment

Table 6. Supported Protocols and Ports on Managed Nodes (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Destination	Usage	Description
							and firmware update. To access the iDRAC configuration s from the OMIVV used in deployment flow.
4001 to 4004	NFS	UDP	None	In/Out	iDRAC to/from OMIVV	Public Share	For iDRAC to access NFS public share that is exposed by OMIVV appliance. This is used for operating system deployment and firmware update. To access the iDRAC configuration s from the OMIVV used in deployment flow.
69	TFTP	UDP	128-bit	In/Out	iDRAC to/from OMIVV	Trivial File Transfer	Used for managing the iDRAC successfully from the management station.

OpenManage Server Administrator

Table 7. Supported Protocols and Ports

Port Number	Protocols	Port Type	Direction	Usage	Configurable
22	SSH	TCP	In/Out	Remote Server Administrator Command Line (for OpenManage Essentials). Remote Software Update feature (for Linux operating systems).	Yes
25	SMTP	TCP	In/Out	Optional email alert messages from Server Administrator	No
135	RPC	TCP/	In/Out	CIM management queries	No
135	RPC	TCP/	In/Out	Remote Server Administrator Command Line (for OpenManage Essentials). Remote	No

Table 7. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Direction	Usage	Configurable
				software update feature (for Windows operating systems).	
161	SNMP	UDP	In/Out	SNMP query management	No
162	SNMP	UDP	Out	SNMP trap event	No
443	HTTPS	TCP	In/Out	Remote Management using Web Server to connect to OpenWSMAN/WinRM)	Yes
1311	HTTPS	TCP	In/Out	Server Administrator Web GUI	Yes
Random Port Number	Proprietary	TCP	In/Out	On localhost/127.0.0.1 only. Internal Java loopback port needed for performance and stability	No

OpenManage Storage Management

Table 8. Supported Protocols and Ports

Port Number	Protocol	Port Type	Direction	Usage	Configurable
5554	TCP	TCP	In/Out	Personal agent to transfer data between LSI IDE solution server and client	No

Dell Command Monitor OpenManage Client Instrumentation

Table 9. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
20	HTTP and FTP	TCP	7.x	None	In/Out	Flash BIOS communicatio n	No
21	HTTP and FTP	TCP	7.x	None	In/Out	Flash BIOS communicatio n	No
80	HTTP and FTP	TCP	7.x	None	In/Out	Flash BIOS communicatio n	No
135	DCOM	TCP/UDP	7.x, 8.x	None	In/Out	Monitoring and configuration through WMI	No
135	DCOM	TCP	7.x, 8.x	None	Out	Event transmission through WMI	No
161	SNMP	UDP	8.1	None	In/Out	SNMP query management	No

Table 9. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
162	SNMP	UDP	8.1	None	Out	SNMP trap event	No
1024-65535 (Dynamically assigned)	DCOM	TCP/UDP	7.x, 8.x	None	In/Out	Monitoring and configuration through WMI	N/A

OpenManage Baseboard Management Utility

Table 10. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
623	Telnet	TCP	1.x	None	In/Out	Accepts incoming Telnet connections	Yes
623	RMCP	UDP	1.x	None	In/Out	Basic BMC commands: server status, power up/ down, and so on.	No
623	RMCP	UDP	1.x	None	In/Out	Basic BMC commands and console redirection	No

Dell Management Console

Table 11. Supported Protocols and Ports

Port Number	Protocol	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSH	TCP	1.x – 2.0.3	128-bit	None	SSH client Remote software updates to Server Administrator —for systems supporting Linux operating systems Performance monitoring in Linux systems	Yes
23	Telnet	TCP	1.x – 2.0.3	None	In/Out	Telnet to Linux device.	No
25	SMTP	TCP	1.x – 2.0.3	None	In/Out	Optional email alert action from Dell Management Console	No
67, 68, 69, 4011	PXE	UDP	N/A	N/A	N/A	PXE and DHCP	N/A
68	UDP	UDP	1.x – 2.0.3	None	In/Out	Wake-on-LAN	Yes

Table 11. Supported Protocols and Ports (continued)

Port Number	Protocol	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
53, 80, 135, 137, 139, 150, 1433, 2500	N/A	TCP	N/A	N/A	N/A	Symantec Console—Console using a remote computer	N/A
80	HTTP	TCP	1.x – 2.0.3	None	In/Out	Application launch—PowerConnect Console	No
135, 137, 139, 445	N/A	TCP/ UDP	N/A	N/A	N/A	Non-HTTP communications (for example, client package download using UNC)	N/A
135	RPC/ DCOM	TCP/ UDP	1.x – 2.0.3	None	In/Out	WMI/CIM management queries	No
138	N/A	UDP	N/A	N/A	N/A	NS client installation	N/A
161	SNMP	UDP	1.x – 2.0.3	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.x – 2.0.3	None	In/Out	SNMP Event Reception and Trap Forwarding	No
389	LDAP	TCP	1.x – 2.0.3	128-bit	In/Out	Domain authentication for IT Assistant log-on	No
401-402	N/A	TCP/ UDP	N/A	N/A	In/Out	Deployment Solution: is used to tickle the Aclient	N/A
443	Proprietary/ Symantec Agent, WSMan	TCP	1.x – 2.0.3	None	In/Out	EMC storage discovery and inventory, Symantec Agent after installation	No
445	N/A	UDP	N/A	N/A	N/A	Non-HTTP communications (for example, client package download using UNC)	N/A
623	RMCP	UDP	1.x – 2.0.3	None	In/Out	IPMI, WSMan, and ASF management	No
664	RMCP	UDP	N/A	N/A	In/Out	Secure ASF management	Yes
1010	PXE	TCP	N/A	N/A	N/A	Deployment Solution: PXE configuration to talk with PXE configuration Service.	N/A
1011	N/A	TCP	N/A	N/A	N/A	Monitor Solution.	N/A
2070-2073, 1758, 1759	PXE	UDP	N/A	N/A	N/A	Deployment Solution: PXE for TFPT and MTFTP transfer of PXE image	N/A
3389	RDP	TCP	1.x – 2.0.3	128-bit SSL	In/Out	Application launch—Remote desktop to Windows terminal services	Yes
3829, 4949, 4950, 4951	N/A	TCP	N/A	N/A	N/A	Used by Symantec Deployment Solutions and PCT Real Time to communicate between PCTWiz and RTDestAgent and to search for RTDestAgent.	N/A

Table 11. Supported Protocols and Ports (continued)

Port Number	Protocol	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
4952	N/A	TCP	N/A	N/A	N/A	Deployment Solutions communication that is used for managing the connection drops.	N/A
6389	Proprietary	TCP	1.x – 2.0.3	None	In/Out	Enables communication between a host system (through NaviCLI/ NaviSecCLI or Navisphere Host Agent) and a Navisphere Array Agent on a storage system	No
8080	N/A	N/A	N/A	N/A	N/A	Deployment Solutions Web Console	N/A
16992	N/A	N/A	N/A	N/A	Out	AMT management unsecure	No
16993	N/A	N/A	N/A	N/A	Out	AMT management secure	No
16994	N/A	N/A	N/A	N/A	Out	AMT management redirection service unsecure	No
16995	N/A	N/A	N/A	N/A	Out	AMT management redirection service secure	No
50120-50124	N/A	N/A	N/A	N/A	N/A	Task Server	N/A
52028, 52029	N/A	TCP	N/A	N/A	N/A	NS Client Multicast	N/A
1024–65535	DCOM	TCP/ UDP	Unknown	None	In/Out	WMI query management (random port)	OS -msdn.microsoft.com/enus/library/ms809327.aspx

OpenManage Power Center

Management Station

Table 12. Supported Protocols and Ports on Management Stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
25	SMTP	TCP	None	In/Out	Email alert action
162	SNMP Trap	UDP	None	In/Out	SNMP Event Reception and Trap Forwarding
6443	Postgres	TCP	None	All	PostgreSQL
8643	HTTPS	TCP	256-bit AES	In/Out	Web GUI

NOTE: The ports that are mentioned in the Management Station table are default ports in OpenManage Power Center. If required, you can change these default ports according to your requirements.

Managed Node

Table 13. Supported Protocols and Ports on Managed Nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Direction	Usage
22	SSH	TCP	256–bit AES	In/Out	Non-Dell chassis communication
161	SNMP Agent	UDP	56-bit DES	In/Out	SNMP query management
443	WSMan	TCP	256-bit AES	In/Out	Chassis communication
623	RMCP/RMCP+	UDP	128-bit AES	In/Out	IPMI access over LAN

Dell Lifecycle Controller Integration for System Center Configuration Manager

Table 14. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
21	FTP	TCP	None	Out	FTP command client	No
53/139	DNS	TCP	None	Out	DNS client for SCCM Console AD login	No
443	WSMan	TCP	128-bit	In/Out	iDRAC/DLCI communication	No
445	NetBIOS	TCP	None	In/Out	CIFS File Share	No
2049	NFS	UDP/TCP	None	All	Public Share	No
4433	HTTPS	TCP	128-bit	In	Auto Discovery	No
4434	HTTPS	TCP	None	In/Out	Non-Windows OSD	No

NOTE: All other ports are as per SCCM. For more information, go to `https://technet.microsoft.com/en-us/library/hh427328.aspx`

Table 15. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
443	WSMan	TCP	128-bit	In/Out	iDRAC/DLCI communication	No
445	NetBIOS	TCP	None	In/Out	CIFS File Share	No
2049	NFS	UDP/TCP	None	All	Public Share	No
4434	HTTPS	TCP	None	In/Out	Non-Windows OSD	No

Dell Lifecycle Controller Integration for System Center Virtualization Machine Manager

Table 16. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
21	FTP	TCP	None	Out	FTP command client	No
53	DNS	TCP	None	Out	DNS client	No
80	HTTP	TCP	None	Out	Dell Online Data Access	No
80	HTTP	TCP	None	In	Administration Console	No
443	HTTPS	TCP	128-bit	In	HTTPS server	No
443	WSMan	TCP	128-bit	In/Out	iDRAC/OMSA communication	
4433	HTTPS	TCP	128-bit	In	Auto Discovery	No
5432	Postgres	TCP	128-bit	All	PostgreSQL	No
135, 136, 137, 138, 139, 445	HTTPS	TCP	128-bit	All	These ports are enabled for iDRAC to access the CIFS share created by the Integration gateway.	No
8455	HTTPS	TCP	128-bit	In/Out	Integration Gateway	Yes
8543	HTTP	TCP	128-bit	In/Out	DCLM Communication	No
8544	HTTP	TCP	128-bit	In/Out	DCLM Web Server Console Launch	No

Table 17. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
21	FTP	TCP	None	Out	FTP command client	No
443	WSMan	TCP	128-bit	In/Out	iDRAC/OMSA communication	No
135, 136, 137, 138, 139, 445	HTTPS	TCP	128-bit	All	These ports are enabled for iDRAC to access the CIFS share created by the Integration gateway.	No

Dell Connections License Manager DCLM

Table 18. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
8543	HTTP	TCP	None	In/Out	DCLM Web Service UI	No
8544	HTTP	TCP	None	In/Out	DCLM Web Server	No

Dell EMC OpenManage Integration for Microsoft System Center for Operations Manager

Table 19. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
161	SNMP	UDP	None	In/Out	SNMP Query Management	No
162	SNMP	UDP	None	In	Event reception through SNMP	No
443	WSMan	TCP	128-bit	In/Out	ESX/iDRAC/Chassis Communication	No
8543	HTTP	TCP	None	Out	DCLM Communication	No
8544	HTTP	TCP	None	Out	DCLM Web Server Console Launch	No

NOTE: Other ports to be accessed or opened as per `https://technet.microsoft.com/en-in/library/jj656649.aspx#BKMK_Firewall`

Table 20. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
443	WSMan	TCP	128-bit	In/Out	ESX/iDRAC/Chassis Communication	No
443	HTTPS	TCP	128-bit	In	RACADM Communication	No
161	SNMP	UDP	None	In/Out	SNMP Query Management	No
162	SNMP	UDP	None	Out	Hardware SNMP Events	No
2463	SymbolSDK	TCP	None	In	PowerVault MD Array Communication	No
1311	HTTP/HTTPS	TCP	None	In/Out	OMSA Web Console	No

Dell Smart Plug-in(SPI) for HP Operations Manager for Microsoft Windows

Table 21. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
162	SNMP	UDP	None	In	Event reception through SNMP	No

Table 22. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
443	WSMan	TCP	128-bit	In/Out	ESXi Communication	No
161	SNMP	UDP	None	In/Out	SNMP Query Management	No

Table 22. Managed Node (continued)

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
162	SNMP	UDP	None	Out	Hardware SNMP Events	No
2463	SymbolSDK	TCP	None	In	PowerVault MD Array Communication	No
1311	HTTP/ HTTPS	TCP	None	In/Out	OMSA Web Console	No
8543	HTTP	TCP	None	Out	DCLM Communication	No
8544	HTTP	TCP	None	Out	DCLM Web Server Console Launch	No

OpenManage Connection for IBM Tivoli Network Manager

Table 23. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
162	SNMP	UDP	None	In	Event reception through SNMP	No

Table 24. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
443	WSMan	TCP	128-bit	In/Out	ESXi Communication	No
161	SNMP	UDP	None	In/Out	SNMP Query Management	No
162	SNMP	UDP	None	Out	Hardware SNMP Events	No
2463	SymbolSDK	TCP	None	In	PowerVault MD Array Communication	No
1311	HTTP/ HTTPS	TCP	None	In/Out	OMSA Web Console	No
8543	HTTP	TCP	None	Out	DCLM Communication	No
8544	HTTP	TCP	None	Out	DCLM Web Server Console Launch	No

Dell EMC OpenManage Connection for IBM Tivoli Netcool/OMNIbus

Table 25. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
162	SNMP	UDP	None	In	Event reception through SNMP	No

Table 26. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
443	WSMan	TCP	128-bit	In/Out	ESXi Communication	No
161	SNMP	UDP	None	In/Out	SNMP Query Management	No
162	SNMP	UDP	None	Out	Hardware SNMP Events	No
2463	SymbolSDK	TCP	None	In	PowerVault MD Array Communication	No
1311	HTTP/HTTPS	TCP	None	In/Out	OMSA Web Console	No

Dell EMC OpenManage Plug-in for Nagios

Table 27. Management Station

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
162	SNMP	UDP	None	In	Event reception through SNMP	No

Table 28. Managed Node

Port Number	Protocols	Port Type	Maximum Encryption Level	Direction	Usage	Configurable
443	WSMan	TCP	128-bit	In/Out	iDRAC Communication	No
161	SNMP	UDP	None	In/Out	SNMP Query Management	No
162	SNMP	UDP	None	Out	Hardware SNMP Events	No
2463	SymbolSDK	TCP	None	In	PowerVault MD Array Communication	No
1311	HTTP/HTTPS	TCP	None	In/Out	OMSA Web Console	No

Dell EMC iDRAC Service Module

Table 29. Supported Protocols and Ports

Port Number	Protocols	Port Type	Direction	Usage	Configurable
1266	WSMan, GUI, Redfish, and remote RACADM over HTTPS	TCP	In/Out	iDRAC Service Module's feature, iDRAC access through Host OS, uses the default port 1266 on Microsoft Windows and Linux operating systems to provide access to iDRAC interfaces (WSMan, GUI, Redfish, and remote RACADM) using https://hostname:1266 as the base URL.	Yes

iDRAC7 and iDRAC8

Table 30. Supported Protocols and Ports — Ports iDRAC Listens for Connections

Port Number	Protocols	Configurable
22	SSH	Yes
23	Telnet	Yes
80	HTTP	Yes
161	SNMP Agent	No
443	HTTPS	Yes
623	RMCP/ RMCP+	Yes
5900	Virtual Console Keyboard and mouse redirection, Virtual Media, Virtual Folders, Remote File Share	Yes
5901	Virtual Network Computing (VNC)	Yes

Table 31. Supported Protocols and Ports — Ports iDRAC Uses as Client

Port Number	Protocols	Configurable
25*	SMTP	Yes
53	DNS	No
68	DHCP-assigned IP address	No
69	TFTP	No
123	NTP	No
162*	SNMP trap	Yes
445	Common Internet File System (CIFS)	No
636	LDAP Over SSL (LDAPS)	No
2049	Network File System (NFS)	No
3269	LDAPS for Global Catalog (GC)	No

* — SNMP and SMTP ports can be configured, if the firmware version is 1.5x.5x or greater.

iDRAC6 for Rack and Tower Servers

Table 32. Supported Protocols and Ports

Port Number	Protocols	Configurable
22	SSH	Yes
23	Telnet	Yes
25	SMTP	No
53	DNS	No
68	DHCP-assigned IP address	No
69	TFTP	No
80	HTTP	Yes
161	SNMP Agent	No
162	SNMP Trap	No
443	HTTPS	Yes
623	RMCP/RMCP+	No
636	LDAPS	No
5900	Virtual Console/Virtual Media	Yes
3269	LDAPS for global catalog (GC)	No

iDRAC for Blade Servers

Table 33. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
22	Secure Shell (SSH)	TCP	1.30	128-bit SSL	In/Out	Secure CLI management	Yes
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet-based CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.0	None	In/Out	Dynamic DNS registration of host name assigned within DRAC	No
68	DHCP-assigned IP address	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update through Trivial FTP	No
80	HTTP	TCP	1.0	None	In/Out	Redirected to HTTPS	Yes
162	SNMP traps	UDP	1.0	None	Out	SNMP trap event	No

Table 33. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
443	HTTPS	TCP	1.0	128-bit SSL	In/Out	Web management GUI	Yes
623	RMCP/ RMCP+	UDP	1.0	128-bit SSL	In/Out	IPMI over LAN	No
636	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3269	LDAPS for global catalog (GC)	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3668, 3669	Virtual Media Service	TCP	1.0	None-SSL	In/Out	For the Virtual Media transfer	Yes
3670, 3671	Virtual Media Secure Service	TCP	1.0	SSL	In/Out	For Virutal Media redirection and transfer	Yes
5900	Console Redirection keyboard/ mouse	TCP	1.0	None-SSL	In/Out	For mouse and keyboard redirection	Yes
5901	Console Redirection video	TCP	1.0	None-SSL	In/Out	For video redirection	Yes

iDRAC6 Enterprise for Blade Servers

Table 34. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSH	TCP	1.30	128-bit SSL	In/Out	Secure CLI management	Yes
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet-based CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.0	None	In/Out	Dynamic DNS registration of host name assigned within DRAC	No
68	DHCP-assigned IP address	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update	No

Table 34. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
						through Trivial FTP	
80	HTTP	TCP	1.0	None	In/Out	Redirected to HTTPS	Yes
162	SNMP trap	UDP	1.0	None	Out	SNMP trap event	No
443	HTTPS	TCP	1.0	128-bit SSL	In/Out	Web management CLI	Yes
623	RMCP/ RMCP+	UDP	1.0	128-bit SSL	In/Out	IPMI over LAN	No
636	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3269	LDAPS for global catalog (GC)	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3668, 3669	Virtual Media Service	TCP	1.0	Non-SSL	In/Out	For Virtual Media transfer	No
3670, 3671	Virtual Media Secure Service	TCP	1.0	SSL	In/Out	For Virtual Media redirection and transfer	No
5900	Console Redirection keyboard/ mouse	TCP	1.0	Non-SSL	In/Out	For mouse and keyboard redirection	Yes
5901	Console Redirection video	TCP	1.0	Non-SSL	In/Out	For video redirection	Yes

Dell Remote Access Configuration Tool DRACT

Table 35. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
443	HTTPS	TCP	1.0	128-bit SSL	In/Out	Web management GUI and remote racadm CLI utility	No

Digital KVM

Table 36. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
2068	Proprietary	TCP	1.0	128-bit SSL	In/Out	Video redirection — keyboard/ mouse	No
3668	Proprietary	TCP	1.0	None	In/Out	Virtual Media	No
8192	Proprietary	TCP	1.0	None	In/Out	Video redirection to client viewer	No

DRAC 5

Table 37. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSHv2	TCP	1.30	128-bit SSL	In/Out	Optional Secure Shell (SSH) CLI management	Yes
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.0	None	In/Out	Dynamic DNS registration of host name assigned within DRAC	No
68	DHCP	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update through Trivial FTP	No
80	HTTP	TCP	1.0	None	In/Out	Web GUI redirected to HTTPS	Yes
161	SNMP	UDP	1.0	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.0	None	Out	SNMP trap event	No
443	HTTPS	TCP	1.0	128-bit SSL	In/Out	Web management	No

Table 37. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
						GUI and remote racadm CLI utility	
623	RMCP/ RMCP+	UDP	1.0	128-bit SSL	In/Out	IPMI over LAN	No
636	LDAPS	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3269	LDAPS for global catalog (GC)	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3668	Proprietary	TCP	1.0	None	In/Out	Virtual Media Service	Yes
3669	Proprietary	TCP	1.0	128-bit SSL	In/Out	Virtual Media Secure Service	Yes
5900	N/A	TCP	1.0	128-bit SSL	Out	Console Redirection: keyboard/ mouse	Yes
5901	N/A	TCP	1.0	128-bit SSL	In	Console Redirection: Video	Yes

DRAC 4

Table 38. Supported Protocols and Ports

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
22	SSHv2	TCP	1.30	128-bit	In/Out	Optional Secure Shell (SSH) CLI management	Yes
23	Telnet	TCP	1.0	None	In/Out	Optional Telnet CLI management	Yes
25	SMTP	TCP	1.0	None	In/Out	Optional e-mail alert messages	No
53	DNS	UDP	1.20	None	In/Out	Dynamic Domain name server (DNS) registration of the host name assigned within DRAC	No

Table 38. Supported Protocols and Ports (continued)

Port Number	Protocols	Port Type	Version	Maximum Encryption Level	Direction	Usage	Configurable
68	DHCP	UDP	1.0	None	In/Out	DHCP assigned IP address	No
69	TFTP	UDP	1.0	None	In/Out	Firmware update through Trivial FTP	No
80	HTTP	TCP	1.0	None	In/Out	Web GUI redirected to HTTPS	Yes
161	SNMP Agent	UDP	1.0	None	In/Out	SNMP query management	No
162	SNMP	UDP	1.0	None	Out	SNMP trap event	No
443	HTTPS	TCP	1.0	128-bit SSL	In/Out	Web management GUI and remote RACADM CLI utility	Yes
636	LDAP	TCP	1.0	128-bit SSL	In/Out	Optional Active Directory Services (ADS) authentication	No
3269	LDAP for global catalog (GC)	TCP	1.0	128-bit SSL	In/Out	Optional ADS authentication	No
3668	Proprietary	TCP	1.0	None	In/Out	CD or diskette virtual media service	Yes
5869	Proprietary	TCP	1.0	None	In/Out	Remote RACADM spcmp server	No
5900	Proprietary	TCP	1.0	128bit RC4, Keyboard/ mouse traffic only	In/Out	Console redirection	Yes