Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

BROADCOM®

DELL EMC

THE INTEGRATED DELL REMOTE ACCESS CONTROLLER 9 (IDRAC9) WITH LIFECYCLE CONTROLLER

COMPLETE AGENT-FREE MANAGEMENT OF POWEREDGE SERVERS

Dell iDRAC9 provides security and intelligent automation.

Modernize with the Dell EMC PowerEdge portfolio

The integrated Dell Remote Access Controller 9 (iDRAC9) delivers advanced, agent-free local and remote server administration. Embedded in every PowerEdge server, iDRAC9 provides a secure means to automate a multitude of common management tasks. Because iDRAC9 is embedded in every PowerEdge server, there's no additional software to install; just plug in power and network cables, and iDRAC9 is ready to go. Even before installing an operating system or hypervisor, IT administrators have a complete set of server management features at their fingertips: Maximize storage performance with up to 12 NVMe drives and ensure application performance scales easily.

- Configuration
- OS deployment
- Firmware updates
- Health monitoring
- Automation of other routine management activities

Scalable Architecture

With iDRAC9 in place across the PowerEdge portfolio, the same IT administration techniques and tools can be applied throughout This consistent management platform allows easy scaling of PowerEdge servers as an organization's infrastructure needs grow. Customers will be able to use the iDRAC RESTful API for the latest in scalable administration methods of PowerEdge servers. With this API, iDRAC9 enables support for the Redfish standard and enhances it with Dell EMC extensions to optimize at-scale management of PowerEdge servers. Regardless of size though, the entire OpenManage portfolio of systems management tools allows every customer to tailor an effective, affordable solution for their environment. This portfolio includes tools, consoles and integrations.

Each component leverages iDRAC9 to make management easy. By extending the reach of administrators to larger numbers of servers, that staff becomes more productive and drives down costs.

Intelligent Automation

Dell's agent-free management puts IT administrators in control. Once a PowerEdge server is connected to power and networking, that system can be monitored and fully managed, whether you're standing in front of the server or remotely over a network. In fact, with no need for software agents, an IT administrator can:

- Monitor
- Manage
- Update
- Troubleshoot and remediate Dell EMC servers

With features like zero-touch deployment and provisioning, iDRAC Group Manager, and System Lockdown, iDRAC9 is purpose-built to make server administration quick and easy. For those customers whose existing management platform utilizes in-band management, Dell EMC does provide iDRAC Service Module, a lightweight service that can interact with both iDRAC9 and the host operating system to support legacy management platforms.

Secure Local and Remote Management

Whether iDRAC9 is used via the updated, HTML5-based web interface, command line interface, or via a set of robust APIs such as the iDRAC RESTful API, security is ensured with HTTPS, SSL, Smart Card authentication, LDAP, and Active Directory integration. The iDRAC9 web interface, remote RACADM utility, and WS-MAN interfaces all support TLS 1.2. Every web page served by the iDRAC9 is delivered with TLS encryption at 256-bit strength (unless configured otherwise). Dell also supports encryption on the virtual KVM (virtual console redirection) and virtual media over TLS. The iDRAC9 virtual console and media also benefit from SSL encryption. Additionally, the iDRAC9 firmware is equipped with a default security certificate, which can be replaced by one of a customer's choosing. By providing secure access remote servers, administrators can carry out critical management functions while maintaining the integrity and security of their data.

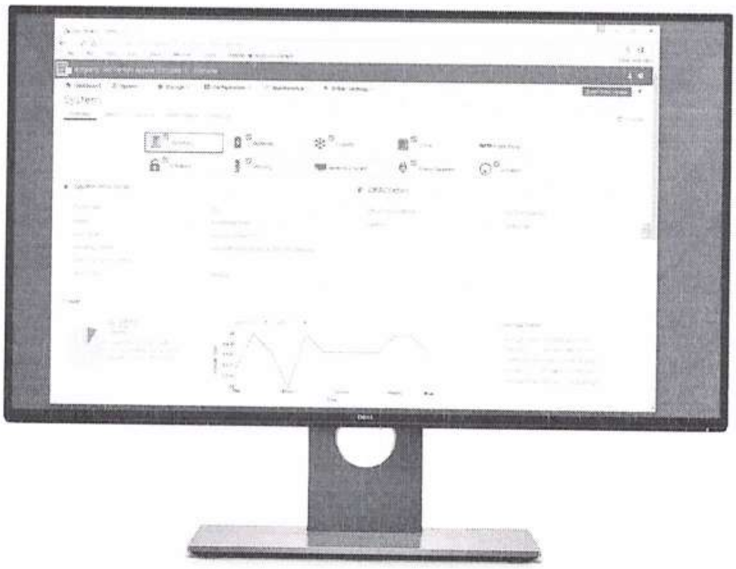
The Heart of PowerEdge Manageability

The iDRAC9 provides common, embedded management across the PowerEdge family of servers, automation that lets your organization grow, and ensure security for peace of mind. This is why iDRAC is the core of managing Dell EMC servers. From the variety of tools and technologies in the OpenManage portfolio, a customer can build a management solution that matches their needs, and by leveraging iDRAC9, ensures optimal server management.

Key iDRAC9 Features and Specifications

BIOS Recovery	Detect an invalid, untrusted BIOS image when a boot is attempted and recover to an authenticated, trusted BIOS image.
Connection View	Quickly check if server LOMs/NDCs and iDRAC are connected to the correct switches and ports via the GUI or by command line interface. This helps prevent costly remote dispatch of technicians to remediate cabling errors.
Full Power Cycle	By utilizing the iDRAC Service Module (iSM), DC power, including AUX power, can be temporarily removed via local or remote control to reset all power nodes in a server, saving time when troubleshooting.
iDRAC Direct	Secure front-panel USB connection to iDRAC web interface which eliminates the need for crash carts or a trip to the hot aisle of your data center. You can use the same port to insert a USB key to upload new system profile for secure, rapid system configuration.
iDRAC Group Manager	Provides built-in, one-to-many monitoring and inventory of local iDRAC9s with no software to install. Ideal for customers who don't want to install and maintain a separate monitoring console. This feature does require iDRAC Enterprise licenses.
iDRAC RESTful API	With this API, iDRAC enables support for the Redfish standard and enhances it with Dell extensions.
Multi Vector Cooling	Airflow for each PCIe slot can be fine-tuned to ensure proper cooling. This allows for greater power efficiency and more precise cooling within each server for accessory cards.
OpenManage Mobile and Quick Sync 2	Use the OpenManage Mobile 2.0 (or higher) app on your handheld device to securely retrieve critical health data and easily perform bare-metal server configuration tasks via BLE/Wi-Fi connectivity. Compatible with various iOS and Android devices.
System Erase	With proper authentication, administrators can securely erase data from local storage (HDDs, SSDs, NVMs) and embedded flash devices.
System Lockdown	Helps to prevent configuration or firmware changes to a server when using Dell tools. Requires iDRAC Enterprise License.
Zero touch deployment and provisioning	When ordered with DHCP enabled from the factory, PowerEdge servers can be automatically configured when they are initially powered up and connected to your network. This process uses profile-based configurations that ensure each server is configured per your specifications. This feature requires an iDRAC Enterprise license.

iDRAC Licenses / Server Model	200-500 Series Rack / Tower	600+ Rack/Tower	Modular
Basic	Standard	n/a	n/a
Express	Optional	Standard	n/a
Express for Blades	n/a	n/a	Standard
Enterprise	Upgrade	Upgrade	Upgrade



Learn more at dell.com/poweredge and delltechcenter.com/idrac

New features in yellow

iDRAC 9 License Levels and Features

License Type	Basic	Express	Express for Blades	Enterprise
		Interfaces / Standards		
Redfish	✓	✓	✓	✓
IPMI 2.0	✓	✓	✓	✓
DCMI 1.5	✓	✓	✓	✓
Web-based GUI	✓	✓	✓	✓
Racadm command line (local/remote)	✓	✓	✓	✓
SMASH-CLP (SSH-only)	✓	✓	✓	✓
Telnet	✓	✓	✓	✓
SSH	✓	✓	✓	✓
Serial Redirection	✓	✓	✓	✓
WSMAN	✓	✓	✓	✓
Network Time Protocol		✓	✓	✓
		Connectivity		
Shared NIC	✓	✓	N/A	✓[1]
Dedicated NIC	✓	✓	✓	✓[2]
VLAN tagging	✓	✓	✓	✓
IPv4	✓	✓	✓	✓
IPv6	✓	✓	✓	✓
DHCP (new default; not static IP)	✓	✓	✓	✓
DHCP with Zero Touch				✓
Dynamic DNS	✓	✓	✓	✓
OS pass-through	✓	✓	✓	✓
iDRAC Direct - Front panel USB	✓	✓	✓	✓
Connection View	✓	✓		✓
NFS v4	✓	✓	✓	✓
SMB3.0 with NTLMv1 and NTLMv2	✓	✓	✓	✓
		Security		
Role-based authority	✓	✓	✓	✓
Local users	✓	✓	✓	✓
SSL encryption	✓	✓	✓	✓
IP blocking		✓	✓	✓
Directory services (AD, LDAP)				✓
Two-factor authentication				✓
Single sign-on				✓
PK authentication		✓	✓	✓
Secure UEFI boot - certificate management	✓	✓	✓	✓
Lock down mode				✓
Unique iDRAC default password	✓	✓	✓	✓
FIPS 140-2	✓	✓	✓	✓
Customizable Security Policy Banner - login page	✓	✓	✓	✓

iDRAC 9 License Levels and Features

License Type	Basic	Express	Express for Blades	Enterprise
Quick Sync 2.0 - optional auth for read operations	✓	✓	✓	✓
Quick Sync 2.0 - add mobile device number to LCL	✓	✓	✓	✓
System Erase of internal storage devices	✓	✓	✓	✓
		Remote Presence		
Power control	✓	✓	✓	✓
Boot control	✓	✓	✓	✓
Serial-over-LAN	✓	✓	✓	✓
Virtual Media			✓	✓
Virtual Folders				✓
Remote File Share				✓
Virtual Console			✓	✓
HTML5 access to Virtual Console			✓	✓
VNC connection to OS				✓
Quality/bandwidth control				✓
Virtual Console collaboration (6 users)				✓
Virtual Console chat				✓
Virtual Flash partitions				✓
Group Manager				✓
HTTP / HTTPS support along with NFS/CIFS	✓	✓	✓	✓
		Power & Thermal		
Real-time power meter	✓	✓	✓	✓
Power thresholds & alerts		✓	✓	✓
Real-time power graphing		✓	✓	✓
Historical power counters		✓	✓	✓
Power Capping				✓
OpenManage Power Center integration (view only)		✓	✓	✓
Temperature monitoring	✓	✓	✓	✓
Temperature graphing		✓	✓	✓
		Health Monitoring		
Full agent-free monitoring	✓	✓	✓	✓
Predictive failure monitoring	✓	✓	✓	✓
SNMPv1, v2, and v3 (traps and gets)	✓	✓	✓	✓
Email Alerting		✓	✓	✓
Configurable thresholds	✓	✓	✓	✓
Fan monitoring	✓	✓	✓	✓
Power Supply monitoring	✓	✓	✓	✓
Memory monitoring	✓	✓	✓	✓
CPU monitoring	✓	✓	✓	✓
RAID monitoring	✓	✓	✓	✓
NIC monitoring	✓	✓	✓	✓
HD monitoring (enclosure)	✓	✓	✓	✓
Out of Band Performance Monitoring				✓
Alerts for excessive SSD wear	✓	✓	✓	✓

iDRAC 9 License Levels and Features

License Type	Basic	Express	Express for Blades	Enterprise
Customizable settings for Exhaust Temperature	✓	✓	✓	✓
Update				
Remote agent-free update	✓	✓	✓	✓
Embedded update tools	✓	✓	✓	✓
Sync with repository (scheduled updates)				✓
Auto-update				✓
Improved PSU firmware updates	✓	✓	✓	✓
Deployment & Configuration				
Local configuration via F10	✓	✓	✓	✓
Embedded OS deployment tools	✓	✓	✓	✓
Embedded configuration tools	✓	✓	✓	✓
Auto-Discovery		✓	✓	✓
Remote OS deployment		✓	✓	✓
Embedded driver pack	✓	✓	✓	✓
Full configuration inventory	✓	✓	✓	✓
Inventory export	✓	✓	✓	✓
Remote configuration	✓	✓	✓	✓
Zerotouch configuration				✓
System Retire/Repurpose	✓	✓	✓	✓
Server Configuration Profile in GUI	✓	✓	✓	✓
Diagnostics, Service & Logging				
Embedded diagnostic tools	✓	✓	✓	✓
Part Replacement		✓	✓	✓
Server Configuration Backup				✓
Server Configuration Restore	✓	✓	✓	✓
Easy Restore (system configuration)	✓	✓	✓	✓
Easy Restore Auto Timeout	✓	✓	✓	✓
Health LED / LCD (requires optional bezel)[5]	✓	✓	N/A	✓
Quick Sync (require NFC bezel, 13G only)				
Quick Sync 2.0 (requires optional BLE/WiFi hardware)	✓	✓	✓	✓
iDRAC Direct (front USB management port)	✓	✓	✓	✓
iDRAC Service Module (iSM) embedded	✓	✓	✓	✓
Alert forwarding via iSM to inband monitoring consoles	✓	✓	✓	✓
Crash screen capture		✓	✓	✓
Crash video capture [4]				✓
Boot capture				✓
Manual reset for iDRAC (LCD ID button)	✓	✓	✓	✓
Remote reset for iDRAC (requires iSM)	✓	✓	✓	✓

iDRAC 9 License Levels and Features

License Type	Basic	Express	Express for Blades	Enterprise
Virtual NMI	✓	✓	✓	✓
OS watchdog [4]	✓	✓	✓	✓
SupportAssist Report (embedded)	✓	✓	✓	✓
System Event Log	✓	✓	✓	✓
Lifecycle Log	✓	✓	✓	✓
Enhanced Logging in Lifecycle Controller Log	✓	✓	✓	✓
Work notes	✓	✓	✓	✓
Remote Syslog				✓
License management	✓	✓	✓	✓
Improved Customer Experience				
iDRAC -Faster processor. more memory	✓	✓	✓	✓
GUI rendered in HTML5	✓	✓	✓	✓
Add BIOS configuration to iDRAC GUI	✓	✓	✓	✓
iDRAC support for SW RAID licensing	✓	✓	✓	✓

footnotes

1 Not available with blade servers

2 500 series and lower rack and tower servers require a hardware card to enable this feature this hardware offered at additional cost.

3 Requires vFlash SD card media

4 Requires iDRAC Service Module (iSM) or OpenManage Server Administrator (OMSA).

5 Requires optional bezel

Dell EMC OpenManage Enterprise 3.8.3

User's Guide

February 2022
Rev. 1

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.**

Revision history

The following table shows the revision history of this document:

Revision	Date	Description
1	February 2022	Content updated for this release of OpenManage Enterprise.

Preface

As part of an effort to improve product lines, we periodically release revisions of software. Therefore, some functions described in this document might not be supported by all versions of the software currently in use. The product release notes provide the most up-to-date information on product features.

Contact your technical support professional if a product does not function properly or does not function as described in this document.

ⓘ **NOTE:** This document was accurate at publication time. Go to Online Support (https://www.dell.com/support) to ensure that you are using the latest version of this document.

Purpose

This document includes conceptual information on managing OpenManage Enterprise.

Audience

This document is intended for use by administrators, device managers, and viewers who use OpenManage Enterprise for systems management and monitoring.

Related documentation

The following publications provide additional information:

- *OpenManage Enterprise Support Matrix*
- *OpenManage Enterprise Release Notes*
- *OpenManage Enterprise Security Configuration Guide*
- *OpenManage Enterprise User's Guide*
- *OpenManage Enterprise RESTful API Guide*
- *OpenManage Enterprise RESTful API* at https://developer.dell.com/apis.
- *OpenManage Enterprise Modular Edition Release Notes*
- *OpenManage Enterprise Modular Edition RESTful API Guide*

In addition to the core documents, we also provide white papers, plugin documentation and demos on YouTube.

Typographical conventions

This document uses the following style conventions:

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Path names, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values

|	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Product documentation

ⓘ **NOTE:** For video demos and tutorials, search for the Dell EMC OpenManage Enterprise playlist on **YouTube**.

- For **OpenManage Enterprise**, go to https://www.dell.com/openmanagemanuals.

  To display the documentation of:

  - *Dell EMC OpenManage Enterprise*, click

    Dell OpenManage Enterprise > **Dell EMC OpenManage Enterprise** > **Documentation**.
  - *Dell EMC OpenManage Mobile*, click

    OpenManage Mobile > **Select the required version** > **Documentation**.
- For **OpenManage Enterprise plugins**, go to https://www.dell.com/openmanagemanuals.

  To display the documentation of:

  - *Dell EMC OpenManage Enterprise Services plugin*, click

    OpenManage Enterprise Connected Services > **OpenManage Enterprise Services** > **Documentation**.
  - *Dell EMC OpenManage Enterprise Power Manager plugin*, click

    OpenManage Enterprise Power Manager > **Dell EMC OpenManage Enterprise Power Manager** > **Documentation**.
  - *Dell EMC OpenManage Enterprise Update Manager plugin*, click

    OpenManage Enterprise Update Manager > **OpenManage Enterprise Update Manager** > **Documentation**.
  - *Dell EMC OpenManage Enterprise CloudIQ plugin*, click

    OpenManage Enterprise Connected Services > **OpenManage Enterprise CloudIQ** > **Documentation**.
- For **OpenManage Enterprise APIs**, go to https://developer.dell.com/products.

  To display the API documentation of:

  - *Dell EMC OpenManage Enterprise*, click **Servers** > **OpenManage Enterprise API**
  - *Dell EMC OpenManage Enterprise Modular Edition*, click **Servers** > **OpenManage Enterprise Modular API**
  - *Dell EMC OpenManage Enterprise Services plugin*, click **Servers** > **OpenManage Enterprise Services API**.
  - *Dell EMC OpenManage Enterprise Update Manager plugin*, click **Servers** > **OpenManage Enterprise Update Manager API**
  - *Dell EMC OpenManage Enterprise Power Manager plugin*, click **Servers** > **OpenManage Enterprise Power Manager API**
  - *Dell EMC OpenManage Enterprise CloudIQ plugin*, click **CloudIQ Public API**

Product information

For documentation, release notes, software updates, or information about products, go to **Online Support** at https://www.dell.com/support.

Where to get help

Go to **Online Support** at www.dell.com/support and click **Contact Support**. To open a service request, you must have a valid support agreement. Contact your sales representative for details about obtaining a valid support agreement or with questions about your account.

Where to find the support matrix

Consult the **Support Matrix** on **Dell OpenManage Enterprise** at https://www.dell.com/openmanagemanuals and click **Documentation**.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to https://contentfeedback.dell.com/s.

Contents

Tables

About Dell EMC OpenManage Enterprise

OpenManage Enterprise is a systems management and monitoring web application delivered as a virtual appliance. It provides a comprehensive view of the Dell EMC servers, chassis, storage, and network switches on the enterprise network. With OpenManage Enterprise, a web-based one-to-many systems management application, users can:

- Discover devices in a data center environment.
- View hardware inventory and monitor health of devices.
- View and manage alerts received by the appliance and configure alert policies.
- Monitor firmware / driver versions and Manage firmware / driver updates on devices with firmware baselines.
- Manage remote tasks (such as power control) on devices.
- Manage configuration settings across devices using deployment templates.
- Manage virtual identity settings across devices using intelligent identity pools.
- Detect and remediate configuration deviations across devices using configuration baselines.
- Retrieve and monitor warranty information for devices.
- Group devices into static or dynamic groups.
- Create and manage OpenManage Enterprise users.

> NOTE:
>
> - OpenManage Enterprise's system management and monitoring is best suited for enterprise LANs and is not recommended for usage over WANs.
> - For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.

Some of the security features of OpenManage Enterprise are:

- Role-based access that limits access to console settings and device actions.
- Scope based access control allows administrators to restrict the device groups that device managers can access and manage.
- Hardened appliance with Security-Enhanced Linux (SELinux) and an internal firewall.
- Encryption of sensitive data in an internal database.
- Use of encrypted communication outside the appliance (HTTPs).
- Create and enforce firmware and configuration-related policies.
- Provision for configuring and updating the bare-metal servers.

OpenManage Enterprise has a domain-task-based GUI, where the navigation is designed by considering the sequence of tasks that are predominately used by an administrator and device manager. When you add a device to an environment, OpenManage Enterprise automatically detects the device properties, places it under relevant device group, and enables you to manage the device. The typical sequence of tasks performed by OpenManage Enterprise users:

- Install OpenManage Enterprise on page 22
- Configure OpenManage Enterprise by using Text User Interface on page 29
- Discovering devices for monitoring or management on page 43
- Manage devices and device groups on page 58
- Monitor devices by using the OpenManage Enterprise dashboard on page 40
- Organize devices into groups on page 58
- Manage the device firmware and drivers on page 80
- View and configure individual devices on page 72
- Monitor and Manage device alerts on page 124
- View and renew device warranty on page 145
- Manage device deployment templates on page 90
- Managing the device configuration compliance on page 116
- Manage compliance templates on page 117
- Monitor audit logs on page 133
- Managing OpenManage Enterprise appliance settings on page 156
- Run an inventory job now on page 78

- Manage the device warranty on page 145
- Reports on page 147
- Managing MIB files on page 153
- Role and scope-based access control in OpenManage Enterprise on page 18
- Directory services integration in OpenManage Enterprise on page 165

Topics:

OpenManage Enterprise Advanced license

ⓘ **NOTE:** Installing and using OpenManage Enterprise does not require the *OpenManage Enterprise Advanced* license. Only the server configuration management feature—deploying device configurations and verifying configuration compliance on servers, requires that the *OpenManage Enterprise Advanced* license is installed on target servers. This license is not required for creating deployment templates from a server.

The *OpenManage Enterprise Advanced* license is a perpetual license that is valid for the life of a server, and can be bound to the Service Tag of only one server at a time. OpenManage Enterprise provides a built-in report to view the list of devices and their licenses. Select **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**, and then click **Run**. See Run reports on page 148.

ⓘ **NOTE:** Enabling the server configuration management feature in OpenManage Enterprise does not require any separate license. If the *OpenManage Enterprise Advanced* license is installed on a target server, you can use the server configuration management feature on that server.

OpenManage Enterprise Advanced license—Supported servers

You can deploy the *OpenManage Enterprise Advanced* license on the following PowerEdge servers:

- YX3X servers having the iDRAC8 2.50.50.50 or later firmware versions. The YX3X firmware versions are backward compatible and are installable on YX2X hardware. See Generic naming convention for Dell EMC PowerEdge servers on page 197.
- YX4X servers having the iDRAC9 3.10.10.10 or later firmware versions. See Generic naming convention for Dell EMC PowerEdge servers on page 197

Purchase OpenManage Enterprise Advanced license

You can purchase the *OpenManage Enterprise Advanced* license when you purchase a server or by contacting your sales representative. You can download the purchased license from the Software License Management Portal at Dell.com/support/retail/lkm.

Verify license information

OpenManage Enterprise provides a built-in report to view the list of devices monitored by OpenManage Enterprise, and their licenses. Click **OpenManage Enterprise** > **Monitor** > **Reports** > **License Report**. Click **Run**. See Run reports on page 148.

You can verify if the *OpenManage Enterprise Advanced* license is installed on a server by:

- On all pages of OpenManage Enterprise, in the upper-right corner, click the **i** symbol, and then click **Licenses**.
- In the **Licenses** dialog box, read through the message and click appropriate links to view and download OpenManage Enterprise related open-source files, or other open-source licenses.

License-based features in OpenManage Enterprise

The *OpenManage Enterprise Advanced* license is required to use the following features of OpenManage Enterprise:

- Server configuration deployment.
- Server configuration compliance baseline creation and remediation.
- Boot to ISO.
- Activate the available plugins, such as the Power Manager, to extend the capability of the appliance.

ⓘ **NOTE:** To access features of the OpenManage Enterprise such as the Virtual Console Support function, which depends on the iDRAC, you would need the iDRAC enterprise license. For more details, see the *iDRAC documentation* available on the support site.

2

Security features in OpenManage Enterprise

Some of the security features of OpenManage Enterprise are:

- Role-based access control allows different device management functionality for different user roles (Administrator, Device Manager, Viewer).
- Scope-based access control allows an administrator to determine the device groups that the device managers are expected to manage.
- Hardened appliance with Security-Enhanced Linux (SELinux) and an internal firewall.
- Encryption of sensitive data in an internal database.
- Use of encrypted communication outside the appliance (HTTPS).
- Only browsers with 256-bit encryption are supported. for more information refer, Minimum system requirements for deploying OpenManage Enterprise on page 23

WARNING: **Unauthorized users can obtain OS-level access to the OpenManage Enterprise appliance bypassing Dell EMC's security restrictions. One possibility is to attach the VMDK in another Linux VM as a secondary drive, and thus getting OS partition access, whereby OS-level login credentials can possibly be altered. Dell EMC recommends that customers encrypt the drive (image file) to make unauthorized access difficult. Customers must also ensure that for any encryption mechanism used, they can decrypt files later. Else, the device would not be bootable.**

NOTE:

- Any change to the user role takes effect immediately and the impacted user(s) will be logged out of their active session.
- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).
- Executing device management actions requires an account with appropriate privileges on the device.

Topics:

OpenManage Enterprise user role types

NOTE:

- AD and LDAP directory users can be imported and assigned one of the OpenManage Enterprise roles (Admin, DeviceManager, or Viewer).
- Actions run on the devices require a privileged account on the device.

Table 1. OpenManage Enterprise User role types

User with this role...	Has the following user privileges
Administrator	Has full access to all the tasks that can be performed on the console. • Full access (by using GUI and REST) to read, view, create, edit, delete, export, and remove information related to devices and groups monitored by OpenManage Enterprise. • Can create local, Microsoft Active Directory (AD), and LDAP users and assign suitable roles • Enable and disable users • Modify the roles of existing users • Delete the users

Table 1. OpenManage Enterprise User role types (continued)

User with this role...	Has the following user privileges
	• Change the user password
Device Manager (DM)	• Run tasks, policies, and other actions on the devices (scope) assigned by the Administrator. • Can only view and manage entities (jobs, firmware or configuration templates and baselines, alert policies, profiles, and so on) that they have created or have assigned ownership.
Viewer	• Can only view information displayed on OpenManage Enterprise and run reports. • By default, has read-only access to the console and all groups. • Cannot run tasks or create and manage policies.

ⓘ NOTE:

- If a Viewer or DM is changed to an Administrator, they get the full Administrator privileges. If a Viewer is changed to a DM, the Viewer gets the privileges of a DM.
- Any change to the user role takes effect immediately and the impacted user(s) will be logged out of their active session.
- An audit log is recorded when:
  - A group is assigned or access permission is changed.
  - User role is modified.

Related information

Role and scope-based access control in OpenManage Enterprise on page 18

Role and scope-based access control in OpenManage Enterprise

OpenManage Enterprise has Role Based Access Control (RBAC) that clearly defines the user privileges for the three built-in roles—Administrator, Device Manager, and Viewer. Additionally, using the Scope-Based Access Control (SBAC) an administrator can limit the device groups that a device manager has access to. The following topics further explain the RBAC and SBAC features.

Role-Based Access Control (RBAC) privileges in OpenManage Enterprise

Users are assigned roles which determine their level of access to the appliance settings and device management features. This feature is termed as Role-Based Access Control (RBAC). The console enforces the privilege required for a certain action before allowing the action. For more information about managing users on OpenManage Enterprise, see Manage OpenManage Enterprise users on page 157.

This table lists the various privileges that are enabled for each role.

Table 2. Role-based user privileges in OpenManage Enterprise

OpenManage Enterprise features	Privilege Description	User levels for accessing OpenManage Enterprise		
		Admin	Device Manager	Viewer
Appliance setup	Global appliance settings involving setting up of the appliance.	**Y**	N	N
Security setup	Appliance security settings	**Y**	N	N

Table 2. Role-based user privileges in OpenManage Enterprise (continued)

OpenManage Enterprise features	Privilege Description	User levels for accessing OpenManage Enterprise		
		Admin	Device Manager	Viewer
Alert management	Alerts actions / management	Y	N	N
Fabric management	Fabric actions / management	Y	N	N
Network management	Network actions / management	Y	N	N
Group management	Create, read, update and delete (CRUD) for static and dynamic groups	Y	N	N
Discovery management	CRUD for discovery tasks, run discovery tasks	Y	N	N
Inventory management	CRUD for inventory tasks, run inventory tasks	Y	N	N
Trap management	Import MIB, Edit trap	Y	N	N
Auto-deploy management	Manage auto-deploy configuration operations	Y	N	N
Monitoring setup	Alerting policies, forwarding, Services (formerly SupportAssist), and so on.	Y	Y	N
Power control	Reboot / cycle device power	Y	Y	N
Device configuration	Device configuration, application of templates, manage/migrate IO identity, storage mapping (for storage devices), and so on.	Y	Y	N
Operating system deployment	Deploy operating system, map to LUN, and so on.	Y	Y	N
Device update	Device firmware update, application of updated baselines, and so on.	Y	Y	N
Template management	Create / manage templates	Y	Y	N
Baseline management	Create / manage firmware / configuration baseline policies	Y	Y	N
Power management	Set power budgets	Y	Y	N
Job management	Job execution / management	Y	Y	N
Report management	CRUD operations on reports	Y	Y	N
Report run	Run reports	Y	Y	Y
View	View all data, report execution / management, and so on.	Y	Y	Y

Scope-Based Access Control (SBAC) in OpenManage Enterprise

With the use of Role-Based Access Control (RBAC) feature, administrators can assign roles while creating users. Roles determine their level of access to the appliance settings and device management features. Scope-based Access Control (SBAC) is an extension of the RBAC feature that allows an administrator to restrict a Device Manager role to a subset of device groups called scope.

While creating or updating a Device Manager (DM) user, administrators can assign scope to restrict operational access of DM to one or more system groups, custom groups, and / or plugin groups.

Administrator and Viewer roles have unrestricted scope. That means they have operational access as specified by RBAC privileges to all devices and groups entities.

Scope can be implemented as follows:

1. Create or Edit User
2. Assign DM role
3. Assign scope to restrict operational access

For more information about managing users, see Manage OpenManage Enterprise users on page 157.

A natural outcome of the SBAC functionality is the Restricted View feature. With Restricted View, particularly the Device Managers will see only the following:

- Groups (therefore, the devices in those groups) in their scope.
- Entities that they own (such as jobs, firmware or configuration templates and baselines, alert policies, profiles, and so on).
- Community entities such as Identity Pools and VLANs which are not restricted to specific users and can be used by everyone accessing the console.
- Built-in entities of any kind.

It should be noted that if the scope of a Device Manager is 'unrestricted', then that Device Manager can view all the devices and groups, however, would only be able to see the entities owned by him/her such as jobs, alert policies, baselines, and so on along with the community and built-in entities of any kind.

When a Device Manager (DM) user with an assigned scope logs in, the DM can see and manage scoped devices only. Also, the DM can see and manage entities such as jobs, firmware or configuration templates and baselines, alert policies, profiles and so on associated with scoped devices, only if the DM owns the entity (DM has created that entity or is assigned ownership of that entity). For more information about the entities a DM can create, see *Role-Based Access Control (RBAC) privileges in OpenManage Enterprise*.

For example, by clicking **Configuration** > **Templates**, a DM user can view the default and custom templates owned by the DM user. Also, the DM user can perform other tasks as privileged by RBAC on owned templates.

By clicking **Configuration** > **Identity Pools**, a DM user can see all the identities created by an administrator or the DM user. The DM can also perform actions on those identities specified by RBAC privilege. However, the DM can only see the usage of those identities that are associated to the devices under the DM's scope.

Similarly, by clicking **Configuration** > **VLANs Pools**, the DM can see all the VLANs created by the admin and export them. The DM cannot perform any other operations. If the DM has a template, it can edit the template to use the VLAN networks, but it cannot edit the VLAN network.

In OpenManage Enterprise, scope can be assigned while creating a local or importing AD/LDAP user. Scope assignment for OIDC users can be done only on Open ID Connect (OIDC) providers.

SBAC for Local users:

While creating or editing a local user with DM role, admin can select one or more device groups that defines the scope for the DM.

For example, you (as an administrator) create a DM user named dm1 and assign group *g1* present under custom groups. Then dm1 will have operational access to all devices in *g1* only. The user dm1 will not be able to access any other groups or entities related to any other devices.

Furthermore, with SBAC, dm1 will also not be able to see the entities created by other DMs (let's say dm2) on the same group *g1*. That means a DM user will only be able to see the entities owned by the user.

For example, you (as an administrator) create another DM user named dm2 and assign the same group *g1* present under custom groups. If dm2 creates configuration template, configuration baselines, or profiles for the devices in *g1*, then dm1 will not have access to those entities and vice versa.

A DM with scope to All Devices has operational access as specified by RBAC privileges to all devices and group entities owned by the DM.

SBAC for AD/LDAP users:

While importing or editing AD/LDAP groups, administrators can assign scopes to user groups with DM role. If a user is a member of multiple AD groups, each with a DM role, and each AD group has distinct scope assignments, then the scope of the user is the union of the scopes of those AD groups.

For example,

- User dm1 is a member of two AD groups (*RR5-Floor1-LabAdmins* and *RR5-Floor3-LabAdmins*). Both AD groups have been assigned the DM role, with scope assignments for the AD groups are as follows: *RR5-Floor1-LabAdmins* gets *ptlab-servers* and *RR5-Floor3-LabAdmins* gets *smdlab-servers*. Now the scope of the DM dm1 is the union of *ptlab-servers* and *smdlab-servers*.

- User dm1 is a member of two AD groups (*adg1* and *adg2*). Both AD groups have been assigned the DM role, with scope assignments for the AD groups as follows: *adg1* is given access to *g1* and *adg2* is given access to *g2*. If *g1* is the superset of *g2*, then the scope of dm1 is the larger scope (*g1*, all its child groups, and all leaf devices).

When a user is a member of multiple AD groups that have different roles, the higher-functionality role takes precedence (in the order Administrator, DM, Viewer).

A DM with unrestricted scope has operational access as specified by RBAC privileges to all device and group entities.

SBAC for OIDC users:

Scope assignment for OIDC users does not happen within the OME console. You can assign scopes for OIDC users at an OIDC provider during user configuration. When the user logs in with OIDC provider credentials, the role and scope assignment will be available to OME. For more information about configuring user roles and scopes, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 170.

ⓘ **NOTE:** If PingFederate is being used as the OIDC provider, then only administrator roles can be used. For more information, see Configure an OpenID Connect provider policy in PingFederate for role-based access to OpenManage Enterprise on page 170 and the Release Notes at https://www.dell.com/support/home/en-yu/product-support/product/dell-openmanage-enterprise/docs.

Transfer ownership : The administrator can transfer owned resources from a device manager (source) to another device manager. For example, an administrator can transfer all the resources assigned from a source dm1 to dm2. A device manager with owned entities such as firmware and/or configuration baselines, configuration templates, alert policies, and profiles is considered an eligible source user. Transfer of ownership transfers only the entities and not the device groups (scope) owned by a device manager to another. For more information see, Transfer of ownership of Device Manager entities on page 164.

Related references

OpenManage Enterprise user role types on page 17

3

Install OpenManage Enterprise

Dell EMC OpenManage Enterprise is provided as an appliance that you can install on a hypervisor and manage resources to minimize downtime. The virtual appliance can be configured from the application web console after initial network provisioning in the Text User Interface (TUI). For steps to view and update the console version, see Check and update the version of the OpenManage Enterprise and the available plugins on page 178. This chapter describes the installation prerequisites and minimum requirements.

ⓘ NOTE: For information about supported browsers, see the *OpenManage Enterprise Support Matrix* available on the support site.

Topics:

Installation prerequisites and minimum requirements

For a list of supported platforms, operating systems, and browsers, see the *Dell EMC OpenManage Enterprise Support Matrix* on the support site and Dell TechCenter.

To install OpenManage Enterprise, you require local system administrator rights and the system you are using must meet the criteria mentioned in the Minimum recommended hardware and Minimum system requirements for installing OpenManange Enterprise.

Hardware requirements

Lists the minimum hardware requirements for the OpenManage Enterprise appliance.

Table 3. Hardware requirements

Hardware configuration	Large deployments	Small deployments
Number of devices that can be managed by the appliance	Up to 8000	1000
RAM	32 GB	16 GB
Processors	8 cores total	4 cores total
Hard drive	400 GB	400 GB

Minimum system requirements for deploying OpenManage Enterprise

Table 4. Minimum requirements

Particulars	Minimum requirements
Supported hypervisors	• VMware vSphere versions: ○ vSphere ESXi 5.5 onwards • Microsoft Hyper-V supported on: ○ Windows Server 2012 R2 onwards • KVM supported on: ○ Red Hat Enterprise Linux 6.5 onwards
Network	Available virtual NIC which has access to the management networks of all the devices which is managed from OpenManage Enterprise.
Supported browsers	• Internet Explorer (64-bit) 11 and later • Mozilla Firefox 52 and later • Google Chrome 58 and later • Microsoft Edge version 41.16299 and later
User interface	HTML 5, JS based

> ⓘ **NOTE:** For the latest update about the minimum requirements for OpenManage Enterprise, see the *Dell EMC OpenManage Enterprise Support Matrix* on the support site.

Deploy OpenManage Enterprise on VMware vSphere

Prerequisites

> ⓘ **NOTE:** To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18.

> ⓘ **NOTE:** If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.

Steps

1. Download the `openmanage_enterprise_ovf_format.zip` file from the support site and extract the file to a location accessible by VMware vSphere Client. It is recommended to use a local drive or CD/DVD, because installing from a network location can take up to 30 minutes.
2. Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select Deploy OVF Template.
3. On the **Select an OVF template** page, specify the location of the source OVF template and click **Next**.

   > ⓘ **NOTE:** If you are using VMware vSphere v6.0 or the earlier versions, you must install the Client Integration plug-in before you deploy an OVF template. Then, in vSphere Client select **File** > **Deploy OVF Template**.

   The **Deploy OVF Template** wizard is displayed.
4. On the **Source** page, click **Browse**, and then select the OVF package. Click **Next**.
5. On the **OVF Template Details** page, review the information that is displayed. Click **Next**.
6. On the **End User License Agreement** page, read the license agreement and click **Accept**. To continue, click **Next**.
7. On the **Name and Location** page, enter a name with up to 80 characters, and then select an inventory location where the template will be stored. Click **Next**.
8. Depending on the vCenter configuration, one of the following options is displayed:

- **If resource pools are configured** — On the **Resource Pool** page, select the pool of virtual servers to deploy the appliance VM.
- **If resource pools are NOT configured** — On the **Hosts/Clusters** page, select the host or cluster on which you want to deploy the appliance VM.

9. If there are more than one datastores available on the host, the **Datastore** page displays such datastores. Select the location to store virtual machine (VM) files, and then click **Next**.
10. On the **Disk Format** page, click **Thick provision** to pre-allocate physical storage space to VMs at the time a drive is created.
11. On the **Ready to Complete** page, review the options you selected on previous pages and click **Finish** to run the deployment job.
    A completion status window displays where you can track job progress.

Deploy OpenManage Enterprise on Hyper-V 2012 R2 and earlier host

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

Steps

1. Download the `openmanage_enterprise_vhd_format.zip` file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows Server 2012 R2 or an earlier version. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
    - provide the **Virtual machine name.**
    - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

    ⓘ NOTE: If the check box is not selected, the VM is stored in the default folder.
6. Click **Next**
7. On the **Specify Generation** page, select **Generation 1** and click **Next**.

    ⓘ NOTE: OpenManage Enterprise does not support Generation 2.
8. On the **Assign Memory** page, enter the startup memory in the **Startup memory** field and click **Next**.

    ⓘ NOTE: Ensure that a minimum of 16,000 MB (16 GB) is assigned.
9. On the **Configure Networking** page, select the network adapter in the **Connection** drop-down list. Ensure that the **virtual switch** is connected to the network. Click **Next**.

    ⓘ NOTE: If set to '**Not Connected**', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
10. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then browse to the location where the VHD file is copied as mentioned in **step 1**. Click **Next**.
11. Complete the on-screen instructions.

NOTE: Make sure to have a minimum storage size of 20 GB

12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise on Hyper-V 2016 host

Prerequisites

NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

Steps

1. Download the **openmanage_enterprise_vhd_format.zip** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager** in the Windows server 2016. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
    - provide the **Virtual machine name.**
    - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

    NOTE: If the check box is not selected, the VM is stored in the default folder.
6. Click **Next**
7. On the **Specify Generation** page, select **Generation 1** and click **Next**.

    NOTE: OpenManage Enterprise does not support Generation 2.
8. On the **Assign Memory** page, enter the startup memory in the **Startup memory** field and click **Next**.

    NOTE: Ensure that a minimum of 16,000 MB (16 GB) is assigned.
9. On the **Configure Networking** page, select the network adapter in the **Connection** drop-down list. Ensure that the **virtual switch** is connected to the network. Click **Next**.

    NOTE: If set to '**Not Connected**', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
10. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then browse to the location where the VHD file is copied as mentioned in **step 1**. Click **Next**.
11. Complete the on-screen instructions.

    NOTE: Make sure to have a minimum storage size of 20 GB
12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise on Hyper-V 2019 or Windows 2022 host

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.
- After installing or upgrading the appliance on Hyper-V, power off the appliance, remove the standard network adapter and add a legacy network adapter, and then power on the appliance.

Steps

1. Download the **openmanage_enterprise_vhd_format.zip** file from the support site. Extract the file and then move or copy the enclosed VHD file into an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
2. Start the **Hyper-V Manager**. The Windows Hyper-V should be displayed under the Hyper-V Manager. If not, right-click **Hyper-V Manager**, and then select **Connect to Server**.
3. Click **Actions** > **New** > **Virtual Machine** to start the **New Virtual Machine Wizard**.
4. Click **Next** on the initial **Before You Begin** page.
5. On the **Specify Name and Location page**
   - provide the **Virtual machine name.**
   - (Optional) Select the **Store the virtual machine in a different location** check box to activate the **Location** field, and then browse and navigate to capture a folder location where the VM would be stored.

   ⓘ NOTE: If the check box is not selected, the VM is stored in the default folder.
6. Click **Next**
7. On the **Specify Generation** page, select **Generation 1** and click **Next**.

   ⓘ NOTE: OpenManage Enterprise does not support Generation 2.
8. On the **Assign Memory** page, enter the startup memory in the **Startup memory** field and click **Next**.

   ⓘ NOTE: Ensure that a minimum of 16,000 MB (16 GB) is assigned.
9. On the **Configure Networking** page, select the network adapter in the **Connection** drop-down list. Ensure that the **virtual switch** is connected to the network. Click **Next**.

   ⓘ NOTE: If set to '**Not Connected**', OME will not function properly during the first reboot, and requires redeployment if this situation recurs.
10. On the **Connect Virtual Hard Disk** page, select **Use an existing virtual disk drive**, and then browse to the location where the VHD file is copied as mentioned in **step 1**. Click **Next**.
11. Complete the on-screen instructions.

    ⓘ NOTE: Make sure to have a minimum storage size of 20 GB
12. Open the **Settings** of the newly created VM and power on the VM.
13. On the TUI screen, accept the EULA and when prompted, change the password of the appliance and set network parameters to the IP of the appliance.

Deploy OpenManage Enterprise by using Kernel-based Virtual Machine

Prerequisites

ⓘ NOTE:

- To perform any tasks on OpenManage Enterprise, you must have necessary user privileges. See Role and scope-based access control in OpenManage Enterprise on page 18
- If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.

Steps

1. Install the required virtualization packages while installing the operating system.
2. Download the `openmanage_enterprise_kvm_format.zip` file from the support site. Extract the file to an appropriate location on your system where you want to store the OpenManage Enterprise virtual drive.
3. Start the virtual manager and select **File** > **Properties**.
4. On the **Network Interfaces** page, click **Add**.
5. Select **Bridge** as the interface type and click **Forward**.
6. Set the start mode to **onboot** and select the **Activate now** check box.
7. Select the interface to bridge from the list and ensure the properties match with the host device, and then click **Finish**.
   A virtual interface is now created, and you can configure the firewall settings by using the terminal.
8. On the Virtual Machine Manager, click **File** > **New**.
9. Enter a name for the VM and select the **Import existing disk image** option, and then click **Forward**.
10. Navigate the file system and select the QCOW2 file that is downloaded in step 1, and then click **Forward**.
11. Assign 16 GB as the memory and select two processor cores, and then click **Forward**.
12. Assign the required disk space for the VM and click **Forward**.
13. Under **Advanced options**, ensure that the bridged host device network is selected and KVM is selected as the Virt Type.
14. Click **Finish**.
    OpenManage Enterprise appliance is now deployed by using the KVM. To get started with OpenManage Enterprise, see Log in to OpenManage Enterprise on page 29.

Deploy OpenManage Enterprise programmatically

OpenManage Enterprise can be deployed programmatically (using a script) on VMWare ESXi version 6.5 or later.

Prerequisites

ⓘ NOTE: Programmatic/scripted deployment is only supported using the primary interface.

ⓘ NOTE: If a secondary adapter is added before powering on the appliance for the first time, the adapter will be configured with IPv4 and IPv6 disabled. Upon login to the TUI, and after accepting the EULA and changing the admin password, the adapter will show up as **DISABLED** and must be configured by the user.

ⓘ NOTE: You must use the latest versions of OVF Tool and Python 3.0 or later for the programmatic deployment.

To programmatically deploy OpenManage Enterprise, do the following:

Steps

1. Download and extract the `openmanage_enterprise_ovf_format.zip` file or download the following OVF files individually from the support site:
   - `openmanage_enterprise.x86_64-0.0.1-disk1.vmdk`
   - `openmanage_enterprise.x86_64-0.0.1.mf`

- openmanage_enterprise.x86_64-0.0.1.ovf
- openmanage_enterprise.x86_64-0.0.1.vmx
- ovf_properties.config
- update_ovf_property.py

2. Open the ovf_properties.config and set the following parameters:

   Table 5. Parameters used in ovf_properties.config

Parameter	Accepted Values	Description
bEULATxt	true or false	By setting this value to true, you agree to the terms and conditions in the End-User License Agreement (EULA). The EULA is available at the bottom of the ovf_properties.config file.
adminPassword	Must contain at least one character in: uppercase, lowercase, digit, and special character. For example, Dell123$	Type a new administrator password for the OpenManage Enterprise.
bEnableDHCP	true or false	Set to true if you want the appliance to enable IPv4 DHCP and to ignore the static IPv4.
bEnableIpv6AutoConfig	true or false	Set to true if you want the appliance to enable IPv6 auto configuration and to ignore the static IPv6.
staticIP	static IP in CIDR format	Can be IPv4 or IPv6. (You cannot set both the IPv4 and IPv6 types at a time.)
gateway	IPv4 or IPv6	You cannot set static Gateway as IPv4 and IPv6 types at a time.

3. Run the update_ovf_property.py script.

   This script modifies the openmanage_enterprise.x86_64-0.0.1.ovf file for deployment in accordance with the values set in the ovf_properties.config file. When the script finishes execution, a sample ovftool command is displayed. It contains tags such as <DATASTORE>, <user>, <password>, <IP address>, and so on, that you must replace as per your deployment environment. These settings define the resources that are used on the target ESXi system and also the credentials and IP address of the target system.

   NOTE: Remember to replace the entire tag including the < and > symbols.

4. Run the modified ovftool command from the previous step.

   NOTE: The ovftool command must be run with the --X:injectOvfEnv and --powerOn flags because they are required for programmatic deployment.

After the ovftool command is run, the manifest validates and the deployment begins.

4

Get started with OpenManage Enterprise

Topics:

Log in to OpenManage Enterprise

About this task

When you boot the system for the first time from the Text User Interface (TUI), you are prompted to accept the EULA, and then change the administrator password. If you are logging in to OpenManage Enterprise for the first time, you must set the user credentials through the TUI. See Configure OpenManage Enterprise by using Text User Interface on page 29.

△ CAUTION: **If you forget the administrator password, it cannot be recovered from the OpenManage Enterprise appliance.**

Steps

1. Start the supported browser.
2. In the **Address** box, enter the OpenManage Enterprise appliance IP address.

   On the login page, OpenManage Enterprise logo and a security notice stating 'By accessing the computer, you confirm that such access complies with your organization's security policy,' is displayed. The security notice can be customized by the administrators using API. For more information, see the OpenManage Enterprise API Guide.
3. Type the login credentials, and then click **Log in**.

   ⓘ **NOTE:** The default user name is `admin`.

Next steps

If you are logging in to OpenManage Enterprise for the first time, the **Welcome to OpenManage Enterprise** page is displayed. Click **Initial Settings**, and complete the basic configuration setup. See Configure OpenManage Enterprise on page 33. To discover the devices, click **Discover Devices**.

ⓘ **NOTE:** By default, after three failed login attempts, your OpenManage Enterprise account gets locked and you cannot log in until the account lockout duration is over. The account lockout duration is 900 seconds by default. To change this duration, see Set the login security properties on page 175.

Configure OpenManage Enterprise by using Text User Interface

The Text User Interface (TUI) tool provides a text interface to change the Administrator password, view appliance status and network configuration, configure networking parameters, enable field service debug request, select the primary network, and to configure the appliance for automatic discovery of the servers in your network.

When you boot the system for the first time from the TUI, you are prompted to accept the End User License Agreement (EULA). Next, change the administrator password and configure network parameters for the appliance and load the web console in a supported browser to get started. Only users with OpenManage Administrator privileges can configure OpenManage Enterprise.

On the TUI interface, use the arrow keys or press **Tab** to go to the next option on the TUI, and press **Shift + Tab** to go back to the previous options. Press **Enter** to select an option. The **Space** bar switch the status of a check box.

> NOTE:
>
> - To configure IPv6, ensure that it is already configured by a vCenter server.
> - By default, the last discovered IP of a device is used by OpenManage Enterprise for performing all operations. To make any IP change effective, you must rediscover the device.

You can configure OpenManage Enterprise by using the TUI. The TUI screen has the following options:

Table 6. Text User Interface options

Options	Descriptions
Change the Admin Password	Select **Change the Admin Password** screen to enter a new password and confirm the password. For the first time, you must change the password by using the TUI screen.
Display Current Appliance Status	Select **Display Current Appliance Status** to view the URL and the status of the appliance. You can also view statuses of the Task Execution, Event Processing, Tomcat, Database, and Monitoring services.
Display Current Network Configuration	Select **Display Current Network Configuration** to view the IP configuration details. **Choose Network Adapter** menu lists all the available network adapters. Clicking on a network adapter will display its current settings.
Set Appliance Hostname	Select **Set Appliance Hostname** to configure the appliance hostname on the DNS. This field supports the following valid characters for host names: alphanumeric (a-z, A-Z, 0-9), periods (.), and dashes (-). NOTE: Using periods will designate domain name information. If the appliance DNS information is configured statically rather than getting domain details from DHCP, you must configure the hostname using the fully qualified domain name (FQDN) so that the domain search information can be populated.
Set Networking Parameters	Select **Set Networking Parameters** to reconfigure the network adapters. **Choose Network Adapter** menu lists all the available networks adapters. Select a network adapter, reconfigure its network parameters, and select **Apply** to save the changes to the appropriate interface. By default, only IPv4 is enabled on primary network interface with a private static IP in the appliance. However, if a new network interface is added, both IPv4 and IPv6 are enabled for multihoming. If the OpenManage Enterprise appliance fails to acquire a IPv6 address, check if the environment is configured for router advertisements to have the managed bit (M) turned on. Network Manager from current Linux distributions causes a link failure when this bit is on, but DHCPv6 is not available. Ensure that DHCPv6 is enabled on the network or disable the managed flag for router advertisements. NOTE:

Table 6. Text User Interface options (continued)

Options	Descriptions
	• DNS configuration is only available on the primary network interface. If DNS resolution is wanted on this interface, all host names must be resolvable by the DNS server configured on the primary interface. • For more information about multihoming, see the *Multihoming on OpenManage Enterprise* technical whitepaper on the Dell OpenManage Enterprise support site.
Select Primary Network Interface	**Select Primary Network Interface** allows you to designate a primary network. Primary interface selection gives priority to the selected interface in terms of routing and is used as the default route. This interface will have the routing priority if there is any ambiguity. The primary interface is also expected to be the 'public facing' interface which allows for corporate network/ internet connectivity. Different firewall rules are applied to the primary interface, which allow for tighter access control such as access restriction by IP range. ⓘ NOTE: If multihoming is enabled, the appliance can be accessed from two networks. In this case, the primary interface is used by the appliance for all external communication and when proxy settings are used. For more information about multihoming, see the *Multihoming on OpenManage Enterprise* technical whitepaper on the Dell OpenManage Enterprise support site.
Configure Static Routes	Select **Configure Static Routes** if the networks require a static route to be configured to reach a specific subnet over the IPv4 and IPv6 networks. ⓘ NOTE: A maximum of 20 static routes per interface is supported.
Configure Server Initiated Discovery	Select **Configure Server Initiated Discovery** to allow the appliance to automatically register the required records with the configured DNS server. ⓘ NOTE: • Ensure that the appliance is registered with DNS, and can dynamically update records. • The target systems must be configured to request registration details from DNS. • To change the DNS Domain Name, ensure Dynamic DNS registration is enabled on the DNS server. Also, for appliance to be registered on the DNS server, select the **Nonsecure and secure** option under Dynamic updates.
Configure Appliance Disk Size	Select **Configure Appliance Disk Size** to scan for the availability of disk space or new disk(s) and then allocate the additional disk space or disk(s) for the appliance if required. ⓘ NOTE: • It is highly recommended to take a VM snapshot of the console as a backup before applying any disk configuration changes. • Post addition of the disk space, deletion or reduction of the expanded disk space is not supported. To

Table 6. Text User Interface options (continued)

Options	Descriptions
	remove a newly added disk or to reverse the increase in size of an existing disk you must revert to prior VM snapshot. • If the initial scan detects no unallocated space, then allocate additional disk space or disks to the console on your hypervisor and rescan. • Scanning and allocation of disk space is limited to a maximum of four disks.
Enable Field Service Debug (FSD) Mode	Select **Enable Field Service Debug (FSD) Mode** (default) for console debugging using HTTPS. For more information, see Field service debug workflow on page 194.
Restart Services	Select **Restart Services** with the following options to restart the services and networking: • **Restart All Services** • **Restart Networking**
Setup Debug Logging	Select **Setup Debug Logging** using the following options : • **Enable All Debug Logs** ○ to collect the Debug logs of the all the application monitoring tasks, events, the task execution history, and installed plugins. • **Disable All Debug Logs** ○ to disable all the Debug logs. • **Configure Debug Logging** ○ To selectively enable debug logging for appliance and plugin services. ○ Use the **Options** menu to select all services, clear all selections or restore state prior to making any modifications. • **Enable SCP Retention**—to collect the template .XML files. ⓘ **NOTE:** SCP file retention is not applicable for MX7000 chassis templates. • **Disable SCP Retention**—to disable the SCP retention. You can create a console log archive from the **Monitor** > **Audit Logs** page by clicking **Troubleshoot** > **Create Console Log Archive**. To download the archived console log, click **Troubleshoot** > **Download Archived Console Logs**.
Enable CIFS share for FSD (emergency use only)	Select **Enable CIFS share for FSD (emergency use only)** for console debugging using CIFS share. For more information, see Field service debug workflow on page 194.
Change keyboard layout	Select **Change keyboard layout** to change the keyboard layout if needed.
Reboot the Appliance	Select **Reboot the Appliance** to restart the appliance. ⓘ **NOTE:** After running a command to restart the services, the TUI may display the following message: `NMI watchdog: BUG: soft lockup - CPU#0 stuck for 36s! [java:14439]`. The soft lockup issue likely occurs as a result of the hypervisor being overloaded. In such situations, it is recommended to have at least 16 GB of RAM and CPU of 8000 MHz reserved to the OpenManage Enterprise appliance. It is also recommended that the OpenManage