Dell EMC OpenManage Enterprise 3.6

Security Configuration Guide

September 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

Figures

Tables

1

PREFACE

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Some functions that are described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features.

Contact your Dell EMC technical support professional if a product does not function properly or does not function as described in this document. This document was accurate at publication time. To ensure that you are using the latest version of this document, go to https://www.dell.com/support.

Legal disclaimers

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.

The Security Configuration Guide intends to be a reference. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of this Security Configuration Guide are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

Scope of the document

This document includes information about security features and capabilities of Dell EMC OpenManage Enterprise. Also, use this document to:

- Understand the security features and capabilities of the product.
- Know how to modify the configuration of the product to maximize the security posture in your environment.
- Be aware of the capabilities Dell EMC has available for secure remote and on-site serviceability.
- Be informed of the expectations Dell EMC has of the environment in which the product is deployed.

Document references

In addition to this guide, you can access other documents of OpenManage Enterprise available at **https://www.dell.com/support**.

- *OpenManage Enterprise User's Guide*
- *OpenManage Enterprise Release Notes*
- *OpenManage Enterprise Support Matrix*

Getting help

The Support website **https://www.dell.com/support** provides access to product licensing, documentation, advisories, downloads, and troubleshooting information. The information can enable you to resolve a product issue before you contact support.

1. Go to **https://www.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.

Reporting security vulnerabilities

Dell EMC takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell EMC immediately.

For the latest on how to report a security issue to Dell, please see the Dell Vulnerability Response Policy on the Dell.com site.

2

Security quick reference

Topics:

Deployment models

Dell EMC OpenManage Enterprise is designed to be deployed as a virtual appliance for a variety of supported hypervisors (VMware, Hyper-V, and KVM). In general, it can be used in environments that support loading the VMDK or VHD formats.

For more information about deploying OME, see the deployment whitepaper at Deploy Dell EMC OpenManage Enterprise Virtual Appliance on Different Hypervisors.

Security profiles

Dell EMC OpenManage Enterprise is configured by default to ensure secure user interactions with the appliance. Customers need to configure the 'admin' user password through the TUI (Text User Interface) to access the OME User Interface(GUI) or rest APIs.

By default, the SSH service is disabled (not user configurable) and interaction with the appliance is limited to using the web UI or REST APIs. Also, OME redirects all HTTP requests to HTTPS and ensures that only secure encrypted connections are established with the OME appliance.

Enabling HTTPS Redirection

HTTP to HTTPS redirection redirects web server communication from HTTP port (default is 80) to HTTPS port (default is 443). This ensures that only secure encrypted connections are established when clients connect to OME. HTTPS redirection is enabled by default and is not user configurable.

3

Product and subsystem security

Topics:

Security controls map

OpenManage Enterprise is a systems management and monitoring application that provides a comprehensive view of the Dell EMC servers, chassis, storage, and network switches on the enterprise network.

The following figure displays the OpenManage Enterprise security controls map:

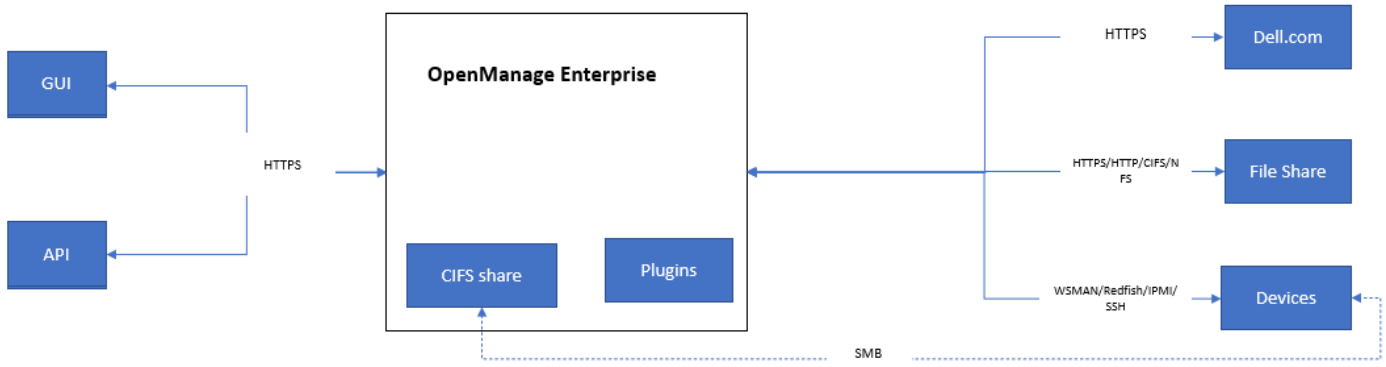

Figure 1. OME security control map

Authentication

OpenManage Enterprise supports session and basic authentication to allow local users to access the application. By default, only admin user is configured on the newly installed appliances. The password for the built-in admin user must be changed via text user interface on first login. The built-in admin can create other users with different roles (Administrators, Device Managers, and Viewers). Administrators can configure to support AD/LDAP and/or OpenID Connect User authentication(s).

OpenManage Enterprise supports Roles and Privileges to restrict user access to certain features - for a full mapping of feature based access details, refer to the OpenManage Enterprise User Guide.

Login security settings

Dell EMC OpenManage Enterprise supports only secure connections to appliance over TLS v1.2 channel. OME redirects all HTTP requests to HTTPS and ensures that credentials are communicated through a secure channel.

OME security configuration settings are accessible in the Web UI using the **OpenManage Enterprise** > **Application Settings** > **Security** page. Incoming connections to the appliance can be restricted by providing network IP details in the **Restrict Allowed IP Range** option or by selecting the **Login Lockout Policy** and providing details such as :

- Select the **By Username** check box to prevent a specific username from logging in to OpenManage Enterprise.
- Select the **By IP Address** check box to prevent a specific IP address from logging in to OpenManage Enterprise.
- In the **Lockout Fail Count** box, enter the number of unsuccessful attempts after which OpenManage Enterprise must prevent the user from further logging in. The default value is three attempts.
- In the **Lockout Fail Window** box, enter the duration for which OpenManage Enterprise must display information about a failed attempt.
- In the **Lockout Penalty Time** box, enter the duration for which the user is prevented from making any login attempt after multiple unsuccessful attempts.

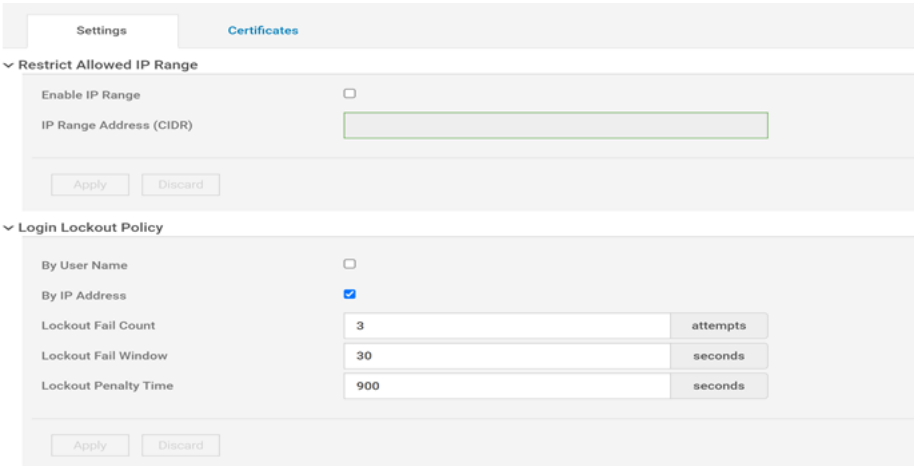

Figure 2. Security settings

Failed login behavior

For any Authentication failures, user can see the message `The username or password you entered is incorrect.`. When a user fails to successfully log in (and exceeds the Lockout Fail count on repeated login attempts), OME will lock the account in question for the period indicated by the Lockout Penalty Time.

Session configuration

Administrators can terminate any user sessions to limit the number of concurrent sessions. By default six concurrent GUI sessions and 100 API sessions are allowed, but, the administrator can change the number to limit the concurrent sessions and can configure up to 100 concurrent sessions. Administrators can terminate user sessions by going to **Application Settings** > **User Session** and by selecting one or more users. Administrators can also see how many users are logged in and can terminate the specific sessions under **Application Settings** > **User** tab. OME provides an option to restrict a specific IP address range to access the appliance.

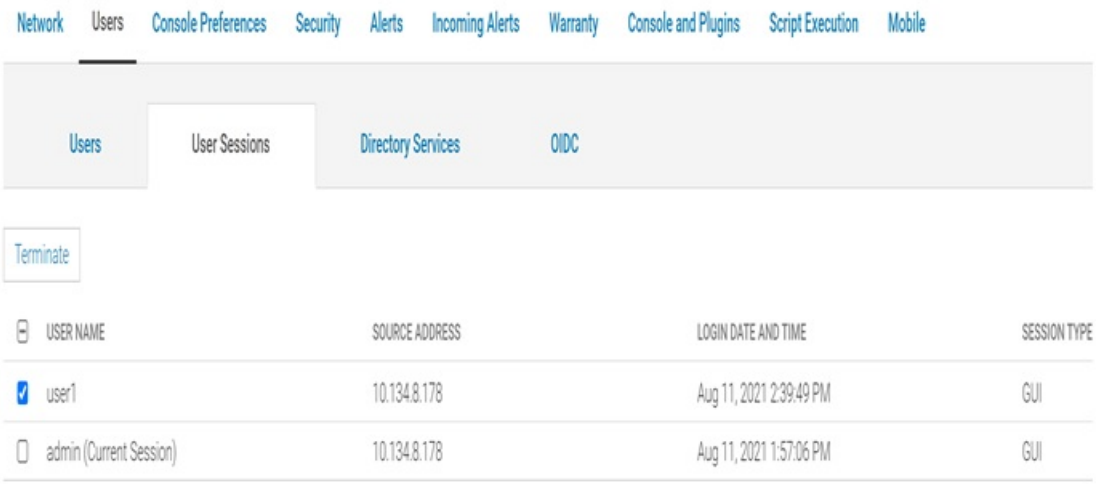

Figure 3. Application settings

Figure 4. Configuration settings for timeouts/max concurrent sessions

Inactive sessions are deleted when the admin configured inactivity timeout expires, and the user is logged out of the console.

Authentication types and setup considerations

OpenManage Enterprise supports local user authentication and authentication via AD/LDAP or OpenID Connect providers.

OpenManage Enterprise supports basic and session based (X-Auth) authentication types for Local users. For Directory and OpenID Connection users, OpenManage Enterprise depends on the customer infrastructure. Administrator can configure customer AD/LDAP and OpenID connect in the OpenManage Enterprise and delegate the responsibility to these infrastructures.

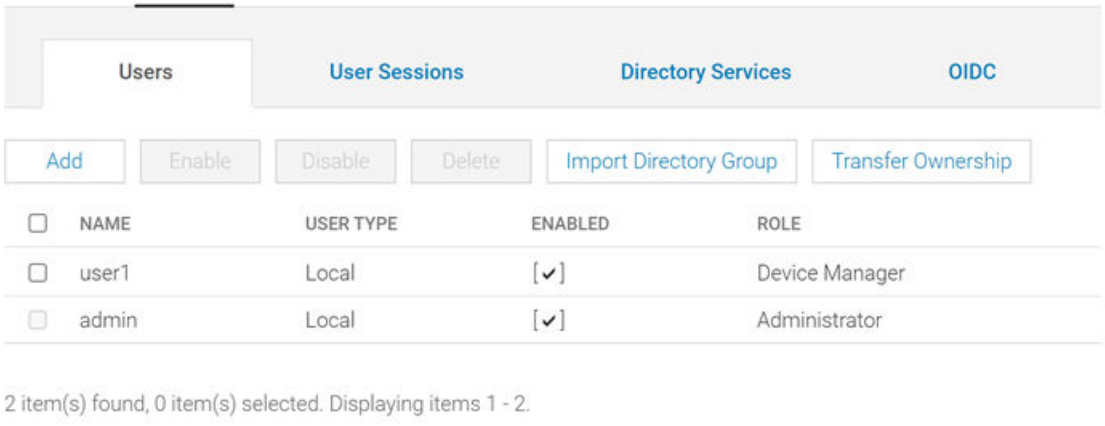

Figure 5. User types

Configuring active directory

User can configure active directory by navigating to **Application Setting** > **Directory Service**.

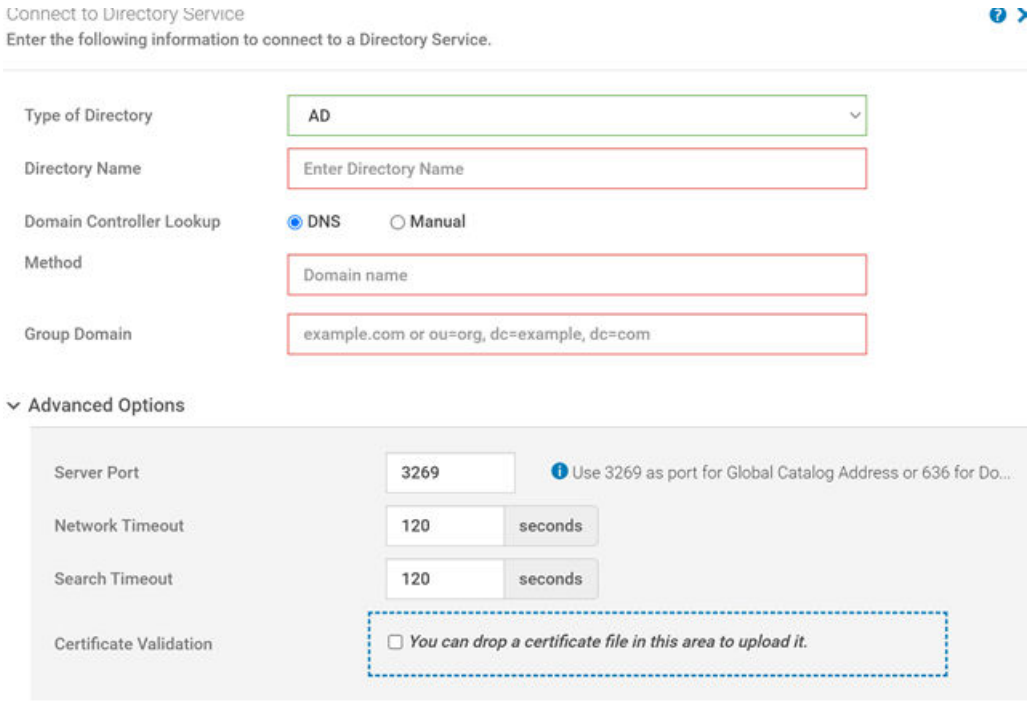

Figure 6. Configuring active directory

OIDC authentication

User can configure OpenID Connect providers by navigating to **Application Setting** > **OIDC**.

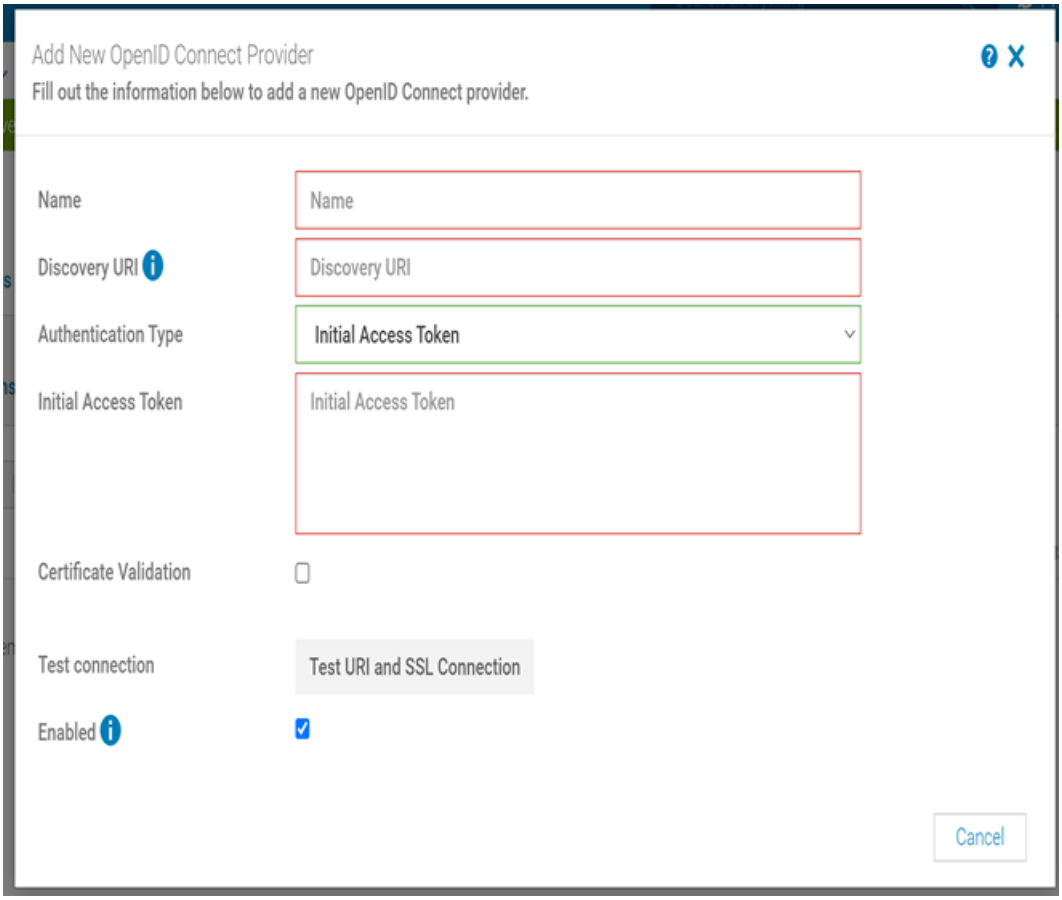

Figure 7. OIDC authentication

User and credential management

Administrator can create and manage users accounts from the Users page by navigating to **Application Settings** > **Users** in OpenManage Enterprise. Administrator can perform following tasks in this wizard:

- View add, enable, edit, disable, or delete the OpenManage Enterprise users (local users imported from AD and OIDC accounts).
- Assign OpenManage Enterprise roles to Active Directory users by importing the directory groups. For the device manager role, admin may limit the scope for the members of the imported directory group.
- View, add, enable, edit, disable, or delete OpenID connect providers (PingFederate and/or Key Cloak).

Local user passwords are encrypted and stored in local database. The recommended characters for passwords are as follows:

- 0-9
- A-Z
- a-z
- '
- -
- !
- "
- #
- $
- %
- &
- ( )
- *
- ,
- .
- /

- :
- ;
- ?
- @
- [
- \
-]
- ^
- _
- `
- {
- |
- }
- ~
- +
- <
- =
- >

Pre-loaded accounts

OpenManage Enterprise has **admin** as the default user. On first boot, after the EULA has been accepted, the password for the default admin account has to configured.

Default credentials

No default credentials are configured on Open Manage Enterprise. Admin need to configure the credentials on the TUI.

How to disable local accounts

Local users can be disabled from the user page which is accessible in OpenManage Enterprise through **Application Settings** > **Users** by selecting the user and clicking disable.

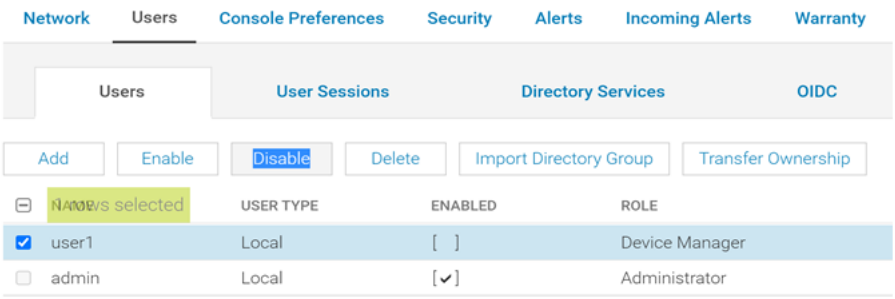

Figure 8. Disable local user accounts

Managing credentials

After first boot, the system prompts the user to accept the EULA and forces the user to set the credentials via Text User Interface (TUI). Default admin user can change the administrator password from the same Text User Interface (TUI) in the future. Other user accounts can be managed from **Application settings** > **Users**page.

Changing admin password from Text User Interface

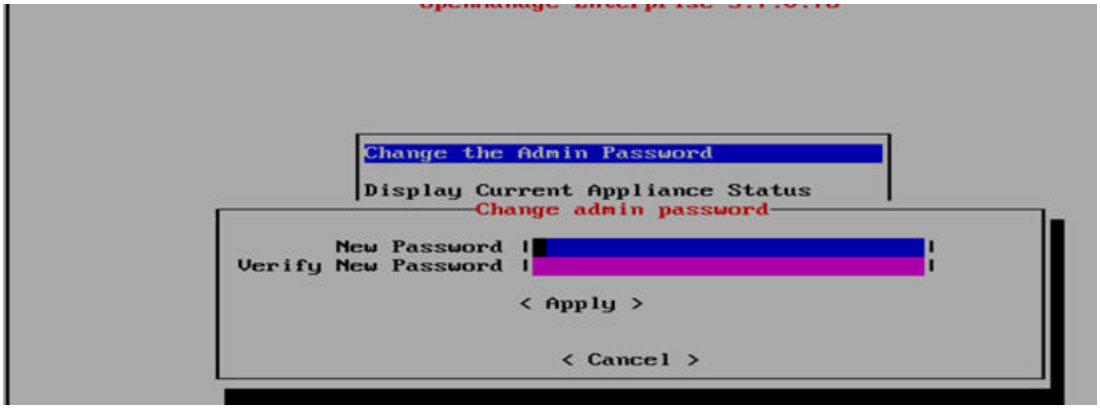

Figure 9. Admin password change from TUI

Securing credentials

User credentials are one-way hashed using the OpenBSD bcrypt scheme and stored in the database.

Password complexity

The recommended characters for passwords are as follows:

- 0-9
- A-Z
- a-z
- '
- -
- !
- "
- #
- $
- %
- &
- ( )
- *
- ,
- .
- /
- :
- ;
- ?
- @
- [
- \
-]
- ^
- _
- `
- {
- |
- }
- ~
- +

- <
- =
- >

Authentication to external systems

OpenManage Enterprise saves device credentials encrypted with AES encryption with a 128-bit key size using encryption key generated on Open Manage Enterprise. Device credentials are used to communicate with devices by using multiple supported protocols such as Redfish, WSMan, SSH, IPMI, and SNMP protocols.

Authorization

OpenManage Enterprise has Role Based Access Control 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.

RBAC privileges

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. OpenManage Enterprise comes with three built-in roles - Administrator, Device Manager, and Viewer.

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 introduced in 3.6.0 that allows an administrator to restrict a Device Manager role to a subset of device groups called scope

Role mapping

User with role	Has the following user privilege
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 ● Change the user password
Device Manager (DM)	Run tasks, policies, and other actions on the devices (scope) assigned by the Administrator
Viewer	● Can only view information displayed on OpenManage Enterprise and run reports ● y default, has read-only access to the console and all groups ● Cannot run tasks or create and manage policies

Network security

Supported protocols and ports on management stations

Table 1. OpenManage Enterprise Supported protocols and ports on management stations

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	Management station	In	OpenManage Enterprise appliance	• Required for incoming only if FSD is used. OpenManage Enterprise administrator must enable only if interacting with the Dell EMC support staff.
25	SMTP	TCP	None	OpenManage Enterprise appliance	Out	Management station	• To receive email alerts from OpenManage Enterprise.
53	DNS	UDP/TCP	None	OpenManage Enterprise appliance	Out	Management station	• For DNS queries.
68 / 546 (IPv6)	DHCP	UDP/TCP	None	OpenManage Enterprise appliance	Out	Management station	• Network configuration.
80*	HTTP	TCP	None	Management station	In	OpenManage Enterprise appliance	• The Web GUI landing page. This will redirect a user to HTTPS (Port 443).
123	NTP	TCP	None	OpenManage Enterprise appliance	Out	NTP Server	• Time synchronization (if enabled).
137, 138, 139, 445	CIFS	UDP/TCP	None	iDRAC/ CMC	In	OpenManage Enterprise appliance	• To upload or download deployment templates. • To upload TSR and diagnostic logs. • To download firmware/driver DUPs, and FSD process. • Boot to network ISO.
				OpenManage Enterprise appliance	Out	CIFS share	• To import firmware/driver catalogs from CIFS share.

Table 1. OpenManage Enterprise Supported protocols and ports on management stations (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
111, 2049 (default)	NFS	UDP/TCP	None	OpenManage Enterprise appliance	Out	External NFS share	• To download catalog and DUPs from the NFS share for firmware updates. • For manual console upgrade from network share.
162*	SNMP	UDP	None	Management station	In/Out	OpenManage Enterprise appliance	• Event reception through SNMP. The direction is 'outgoing' only if using the Trap forward policy.
443 (default)	HTTPS	TCP	128-bit SSL	Management station	In/Out	OpenManage Enterprise appliance	• Web GUI. • To download updates and warranty information from Dell.com. 256-bit encryption is allowed when communicating with the OpenManage Enterprise by using HTTPS for the web GUI. • Server-initiated discovery.
514	Syslog	TCP	None	OpenManage Enterprise appliance	Out	Syslog server	• To send alert and audit log information to Syslog server.
3269	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	• AD/ LDAP login for Global Catalog.
636	LDAPS	TCP	None	OpenManage Enterprise appliance	Out	Management station	• AD/ LDAP login for Domain Controller.

*Port can be configured up to 499 excluding the port numbers that are already allocated.

Supported protocols and ports on managed nodes

Table 2. OpenManage Enterprise supported protocols and ports on the managed nodes

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
22	SSH	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	• For the Linux OS, Windows, and Hyper-V discovery.

Table 2. OpenManage Enterprise supported protocols and ports on the managed nodes (continued)

Port Number	Protocol	Port Type	Maximum Encryption Level	Source	Direction	Destination	Usage
161	SNMP	UDP	None	OpenManage Enterprise appliance	Out	Managed node	• For SNMP queries.
162*	SNMP	UDP	None	OpenManage Enterprise appliance	In/ Out	Managed node	• Send and receive SNMP traps.
443	Proprietary/ WS-Man/ Redfish	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	• Discovery and inventory of iDRAC7 and later versions. • For the CMC management.
623	IPMI/ RMCP	UDP	None	OpenManage Enterprise appliance	Out	Managed node	• IPMI access through LAN.
69	TFTP	UDP	None	CMC	In	Management station	• For updating CMC firmware.

* Port can be configured up to 499 excluding the port numbers that are already allocated.

NOTE: In an IPv6 environment, you must enable IPv6 and disable IPv4 in the OpenManage Enterprise appliance to ensure all the features work as expected.

Internal network (CIFS) share

Some device functionality such as firmware update, server configuration profile capture and deployment, tech support and diagnostic report extraction require access to an external network share (that is external to the server) to complete the operation. OME has included a built-in CIFS share to reduce the work required to set up an external network share and improve customer experience. That means OME includes smbd (www.samba.org) and a running OME instance will have smbd listening on ports 139 / 445. The CIFS share in OME is available after the appliance is powered on. However, access is protected with credentials and SMB protocol version defaults to SMBv2 (this can be altered using the Appliance Settings). OME rotates the credentials on a periodic basis (every six hours, this is not externally configurable) and stores encrypted passwords in a database. The share location and credentials are provided to the devices that need to access them, within the context of each such OME workflow. This share is used only through internal communication to the devices and there is no external method to get the share details.

Field service debug (FSD)

In OpenManage Enterprise, you can authorize console debugging by using the Field Service Debug (FSD) option. FSD enables root level access to appliance via SSH. This process can only be authorized through Dell-EMC Support services. For more information, see *Field service debug workflow* section in the user's guide.

OpenManage Enterprise update

Users can upgrade to the next version of OpenManage Enterprise by downloading the latest bundle from dell.com. For more information, see *Update OpenManage Enterprise* section in the user's guide.

Data security

OME stores all sensitive data encrypted with the OME generated encryption key. All user credentials are stored with a one-way hash and cannot be decrypted.

All Device credentials are encrypted with AES 128 bit key encryption. All other data on the appliance is protected by privileges and provides access based on the privileges. Also, OME pre-configured SeLinux policies ensure data protection and access to the OME workflows.

Cryptography

Internal services are configured with specific Access Control Lists (ACL) and ensures only required services can have access .

OpenManage Enterprise supports industry-proven crypto algorithms for client communication. OME only allows communication via the TLS v1.2 protocol with clients. Clients can negotiate to communicate with OME using the below cipher:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

NOTE: Selection of ciphers is NOT user configurable.

Certificate management

By default, OME is configured to use self-signed certificates. Admins can configure the CA signed certificate under **Application Settings** > **Security** > **Certificates**.

Users can view all view information about the currently available SSL certificate for the device by navigating to **Application Settings** > **Security** > **Certificates**. By default, OpenManage Enterprise comes with self-signed certificates.

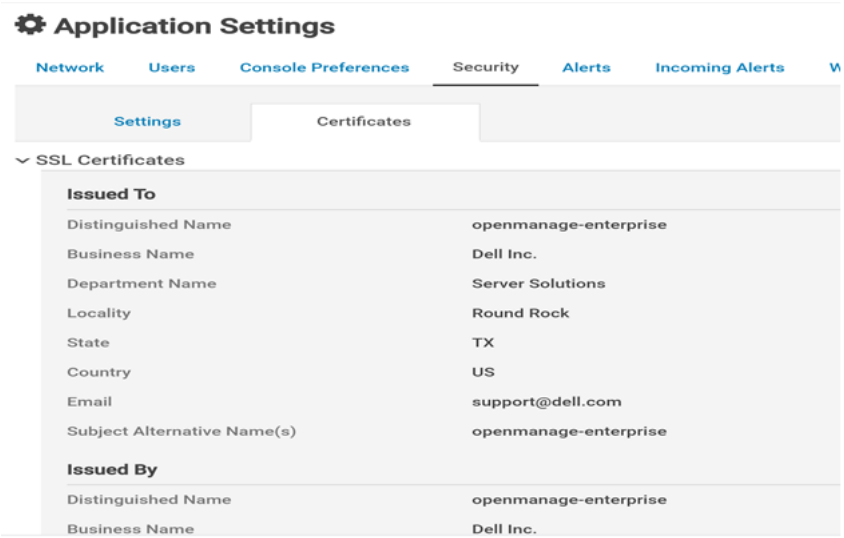

Figure 10. Certificate management

User can also generate CSR, get it signed, and then upload the signed certificate to OpenManage Enterprise console.

Auditing and logging

Auditing provides a historical view of the users and activity on the system. Audit logs page lists the log data to help you or the Dell EMC Support teams in troubleshooting and analysis. An audit log is recorded when:

- A group is assigned, or access permission is changed.
- User role is modified.
- Actions that were performed on the devices monitored by OpenManage Enterprise. The audit log files can be exported to the CSV file format.

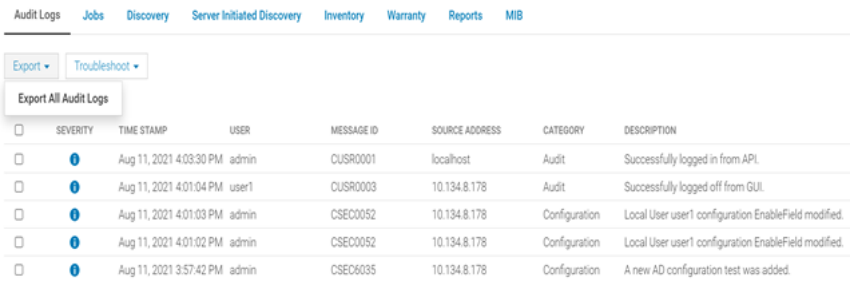

Figure 11. Audit log

Logs

User can access all OME services logs and audit logs from the UI. Navigate to **Monitor** > **Audit logs** > **Export Console logs/Audit logs**. Support can use these logs for analyzing the customer issues. By default, these logs are at INFO (or above) level.

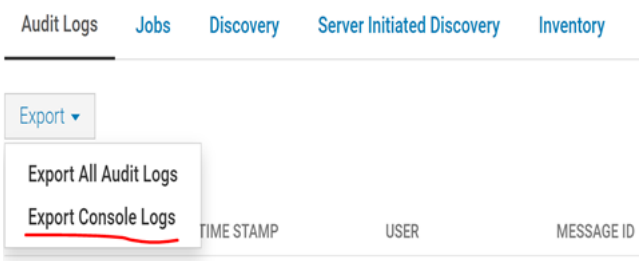

Figure 12. Export audit log

Administrator can change log levels from Text User Interface.

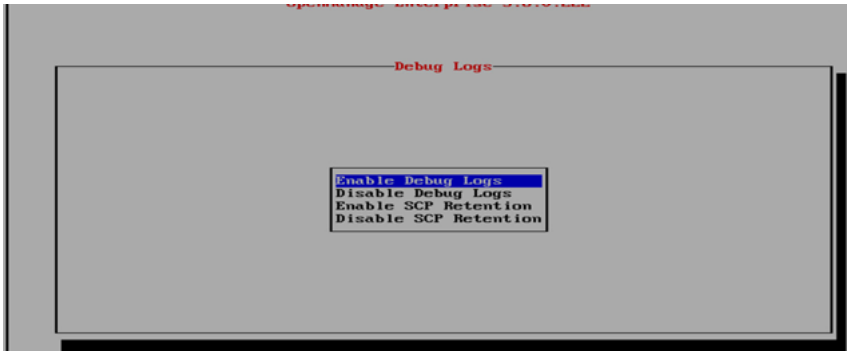

Figure 13. Debug log

OpenManage Enterprise has a size-based log roll-over policy. The maximum size of the log file can go up to 10 MB. Users can find up to 10 rollover log files for any service.

Network vulnerability scanning

Issues	Resolution

SSL certificate cannot be trusted	Security scans on OME may show the SSL certificate issues with the default certificate on OME. As a best practice, customers can choose to upload the CA trusted certificate to the production environment.
SSL certificate chain ends in an unrecognized self-signed certificate	
SSL certificate - Computer Name (CN) does not match FQDN	
SSL certificate - Invalid Maximum validity date detected	
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the target machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.	Security scans on OME may show the issue with ICMP configuration. Knowledge of OpenManage Enterprise's uptime is not considered a risk and its operating system is well-known and documented.
Unfiltered Ports on NMAP scans	Security scans may report some of the ports on OME as Unfiltered. All unfiltered ports are closed other than all documented ports.

4

Contacting Dell

Prerequisites

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

About this task

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 for sales, technical support, or customer service issues:

Steps

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.