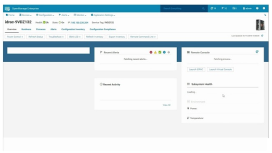
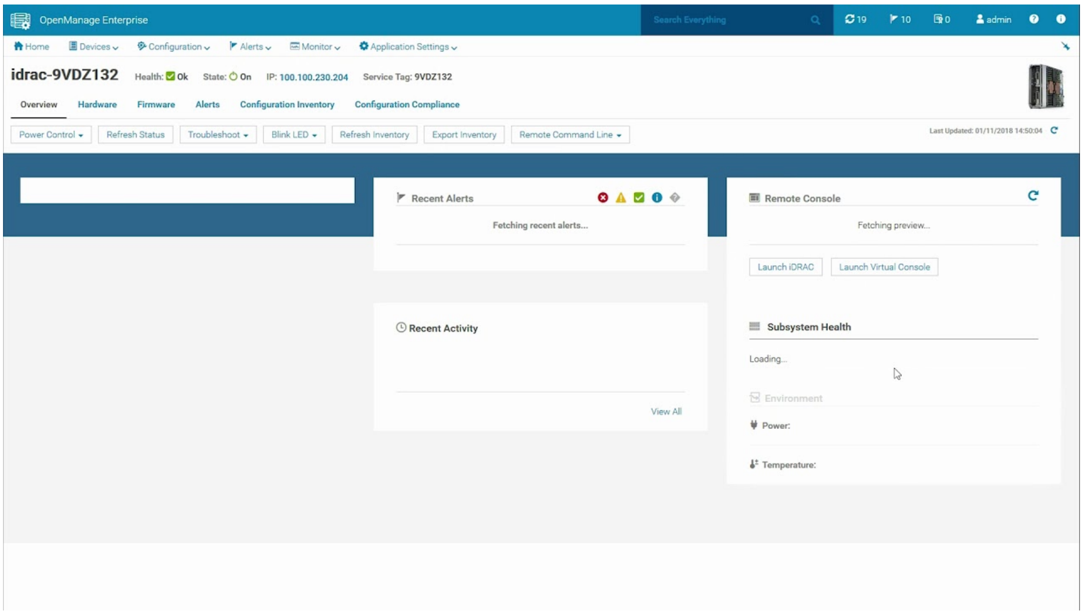


DELL 3.10 OpenManage Enterprise Security Configuration Owner’s Manual

Contents

1 DELL 3.10 OpenManage Enterprise Security Configuration
2 Product Information OpenManage Enterprise 3.10
3 Notes, Cautions, and Warnings
4 Product Usage Instructions
5 Preface
6 Security quick reference
7 Product and subsystem security
8 Authorization
9 Cryptography
10 Auditing and logging
11 Network vulnerability scanning
12 Documents / Resources
13 Related Posts

DELL 3.10 OpenManage Enterprise Security Configuration



idrac-9VDZ132 Health: Ok State: On IP: 100.100.230.204 Service Tag: 9VDZ132

Last Updated: 01/11/2018 14:50:04

Fetching recent alerts...

Fetching preview...

Loading...

Power:

Temperature:

Product Information OpenManage Enterprise 3.10

OpenManage Enterprise 3.10 is a software designed for systems management and monitoring. It includes various features such as security configurations, user guides, and RESTful API guides. The software is periodically updated to improve product lines and the release notes provide the most up-to-date information on product features. This software is intended for use by administrators, device managers, and viewers who use OpenManage Enterprise for systems management and monitoring. For documentation, release notes, software updates, or information about products, go to Online Support at **https://www.dell.com/support**

Notes, Cautions, and Warnings

The user manual includes notes, cautions, and warnings to alert users about important information, potential damage to hardware or loss of data, and potential for property damage, personal injury or death respectively.

- **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 revision history table in the user manual shows the latest revision of the document along with its release date and description of content updated for the release of OpenManage Enterprise. The following table shows the revision history of this document:

Revision	**Date**	**Description**
A01	January 2023	Content updated for this release of OpenManage Enterprise.

Related Documentation

The user manual lists several publications that provide additional information on OpenManage Enterprise including support matrix, release notes, security configuration guide, user’s guide, RESTful API guide, modular edition release notes, and modular edition RESTful API guide. In addition to these core documents, white papers, plugin documentation, and demos are also available on YouTube.

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

NOTE: For video demos and tutorials, search for the Dell OpenManage Enterprise playlist on YouTube, or see the following videos for demos of the OpenManage Enterprise Graphical User Interface (GUI) in action:

- OpenManage Enterprise overview (01:44 m)
- Creating a firmware baseline in OpenManage Enterprise (01:22 m)
- OpenManage Enterprise systems management console (02:02 m)
- For OpenManage Enterprise, go to **https://www.dell.com/openmanagemanuals**.

  To display the documentation of:

  - OpenManage Enterprise, click

    Dell OpenManage Enterprise > Dell OpenManage Enterprise > Documentation.
  - 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:
  - OpenManage Enterprise Services plugin, click

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

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

    OpenManage Enterprise Update Manager > OpenManage Enterprise Update Manager > Documentation.
  - 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:
  - OpenManage Enterprise, click Servers > OpenManage Enterprise API
  - OpenManage Enterprise Modular Edition, click Servers > OpenManage Enterprise Modular API
  - OpenManage Enterprise Services plugin, click Servers > OpenManage Enterprise Services API.
  - OpenManage Enterprise Update Manager plugin, click Servers > OpenManage Enterprise Update Manager API
  - OpenManage Enterprise Power Manager plugin, click Servers > OpenManage Enterprise Power Manager API
  - OpenManage Enterprise CloudIQ plugin, click CloudIQ Public API

Product Usage Instructions

1. Ensure that you are using the latest version of the user manual by visiting Online Support at **https://www.dell.com/support**.
2. Refer to the user manual for conceptual information on managing OpenManage Enterprise.
3. Follow the security configuration guide to configure security settings for OpenManage Enterprise.
4. Refer to the RESTful API guide to integrate OpenManage Enterprise with other systems.
5. For OpenManage Enterprise plugins, visit **https://www.dell.com/openmanagemanuals** and select the required plugin for documentation.
6. Contact technical support if the product does not function properly or as described in the user manual.

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.

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

Where to get help

Go to Online Support at **https://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.

NOTE:
For quick access to the content of the OpenManage Enterprise User’s Guide, open the OpenManage Enterprise Online Help by clicking the ? icon in the upper-right corner of a screen in the product GUI.

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**.

Security quick reference

Topics:

- Deployment models
- Security profiles

Deployment models

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 OpenManage Enterprise Deployment.

Security profiles

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.

Product and subsystem security

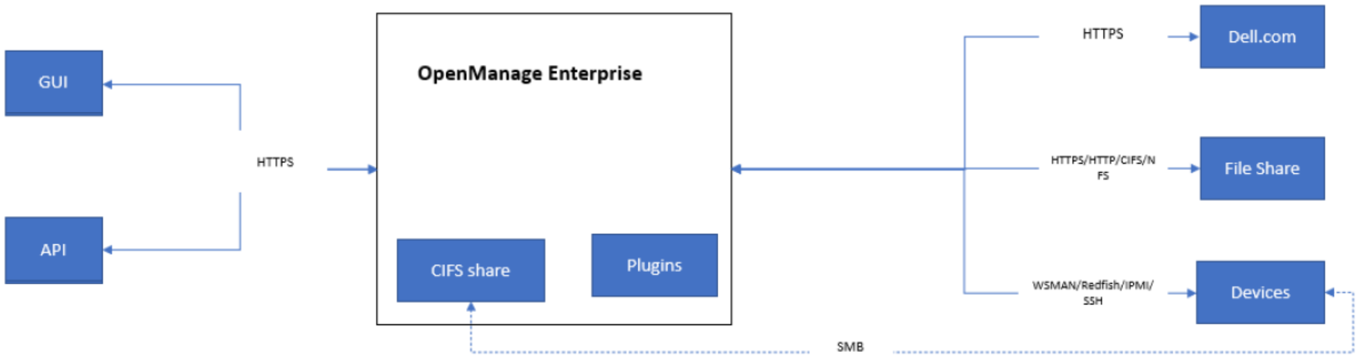
Topics:

- Security controls map
- Authentication
- Login security settings
- Authentication types and setup considerations
- Authorization

- Data security
- Cryptography

Security controls map

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



NOTE: OME now allows users to disable all versions of CIFS.

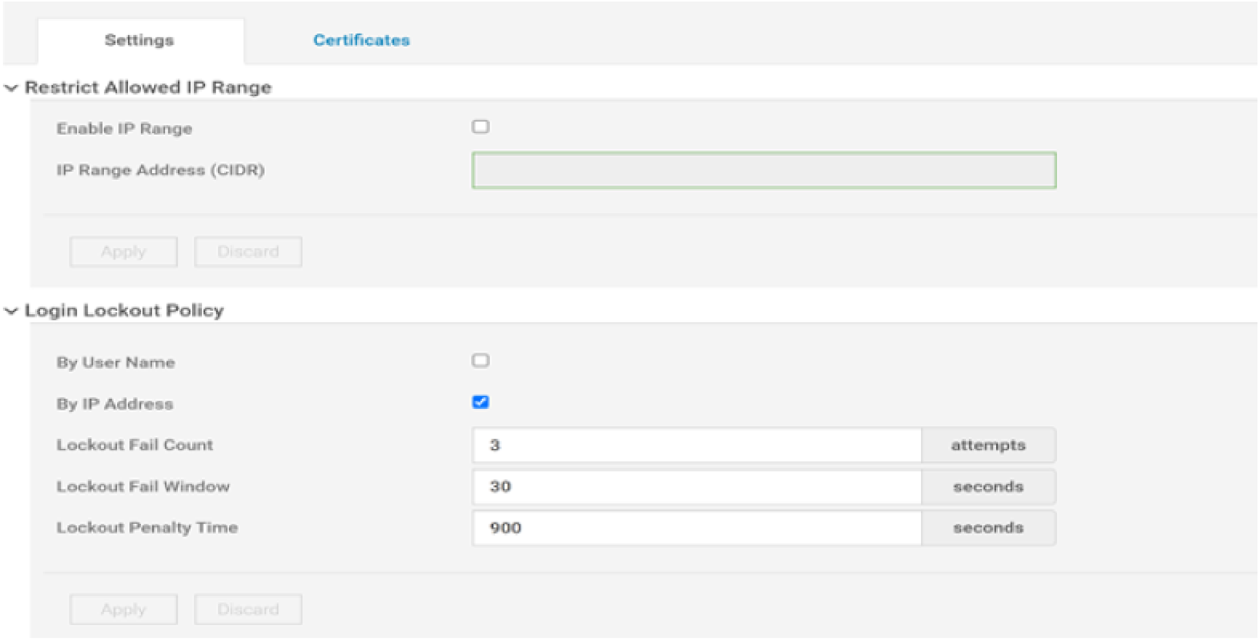
Authentication

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

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 (Users are allowed to input multiple IP ranges in this field) 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.



Restrict Allowed IP Range

Enable IP Range ☐

IP Range Address (CIDR)

Login Lockout Policy

By User Name ☐

By IP Address ☑

Lockout Fail Count: 3 attempts

Lockout Fail Window: 30 seconds

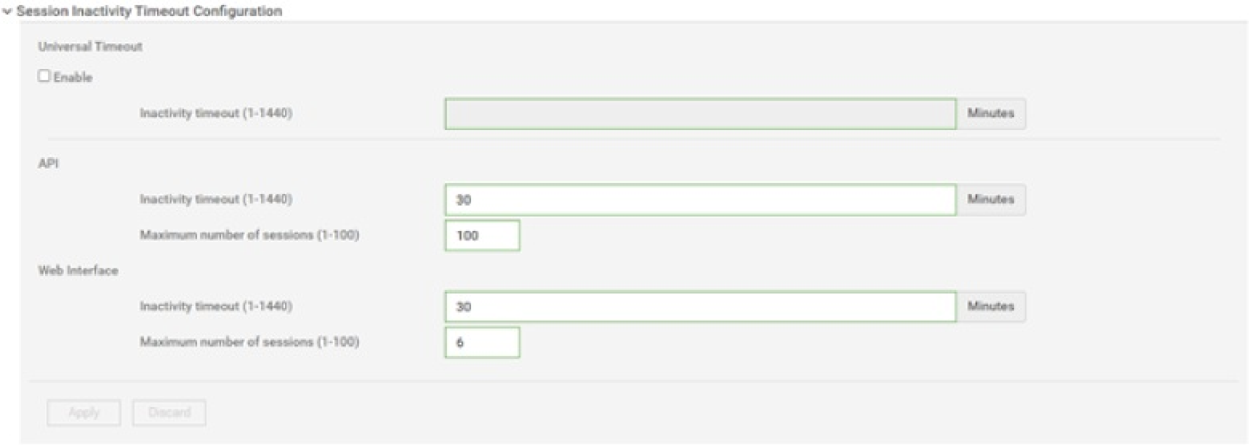
Lockout Penalty Time: 900 seconds

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.



Session Inactivity Timeout Configuration

Universal Timeout

☐ Enable

Inactivity timeout (1-1440): Minutes

API

Inactivity timeout (1-1440): 30 Minutes

Maximum number of sessions (1-100): 100

Web Interface

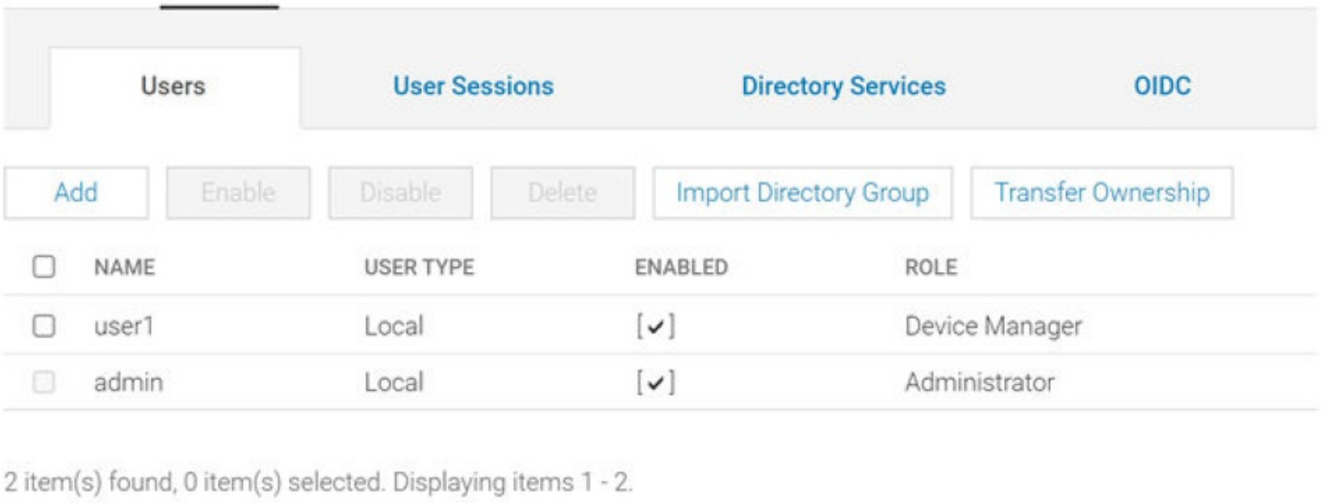
Inactivity timeout (1-1440): 30 Minutes

Maximum number of sessions (1-100): 6

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.

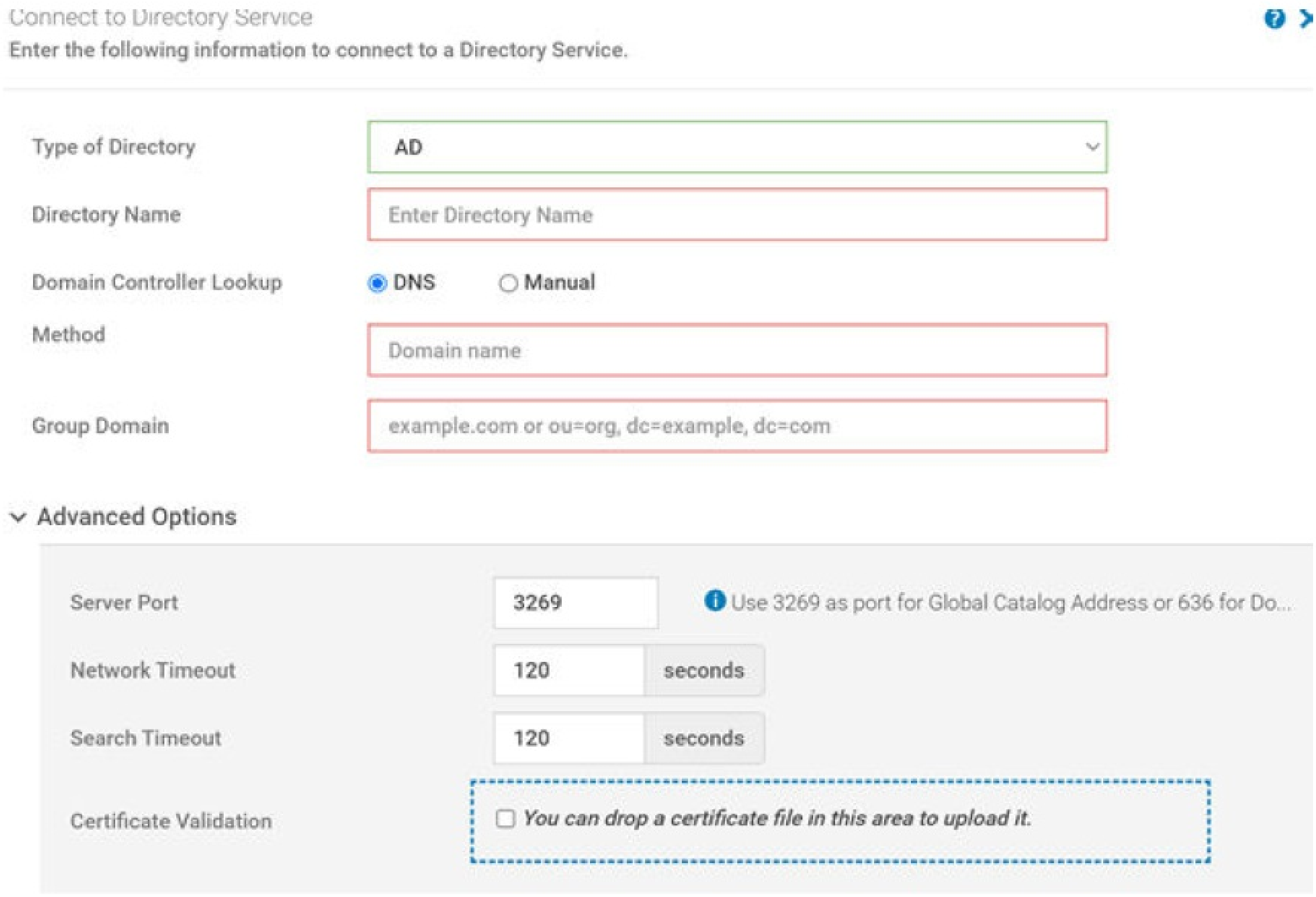


☐	NAME	USER TYPE	ENABLED	ROLE
☐	user1	Local	[✓]	Device Manager
☐	admin	Local	[✓]	Administrator

2 item(s) found, 0 item(s) selected. Displaying items 1 - 2.

Configuring active directory

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



Connect to Directory Service

Enter the following information to connect to a Directory Service.

Type of Directory: AD

Directory Name: Enter Directory Name

Domain Controller Lookup Method: ● DNS ○ Manual

Domain name

Group Domain: example.com or ou=org, dc=example, dc=com

Advanced Options

Server Port: 3269 — Use 3269 as port for Global Catalog Address or 636 for Do...

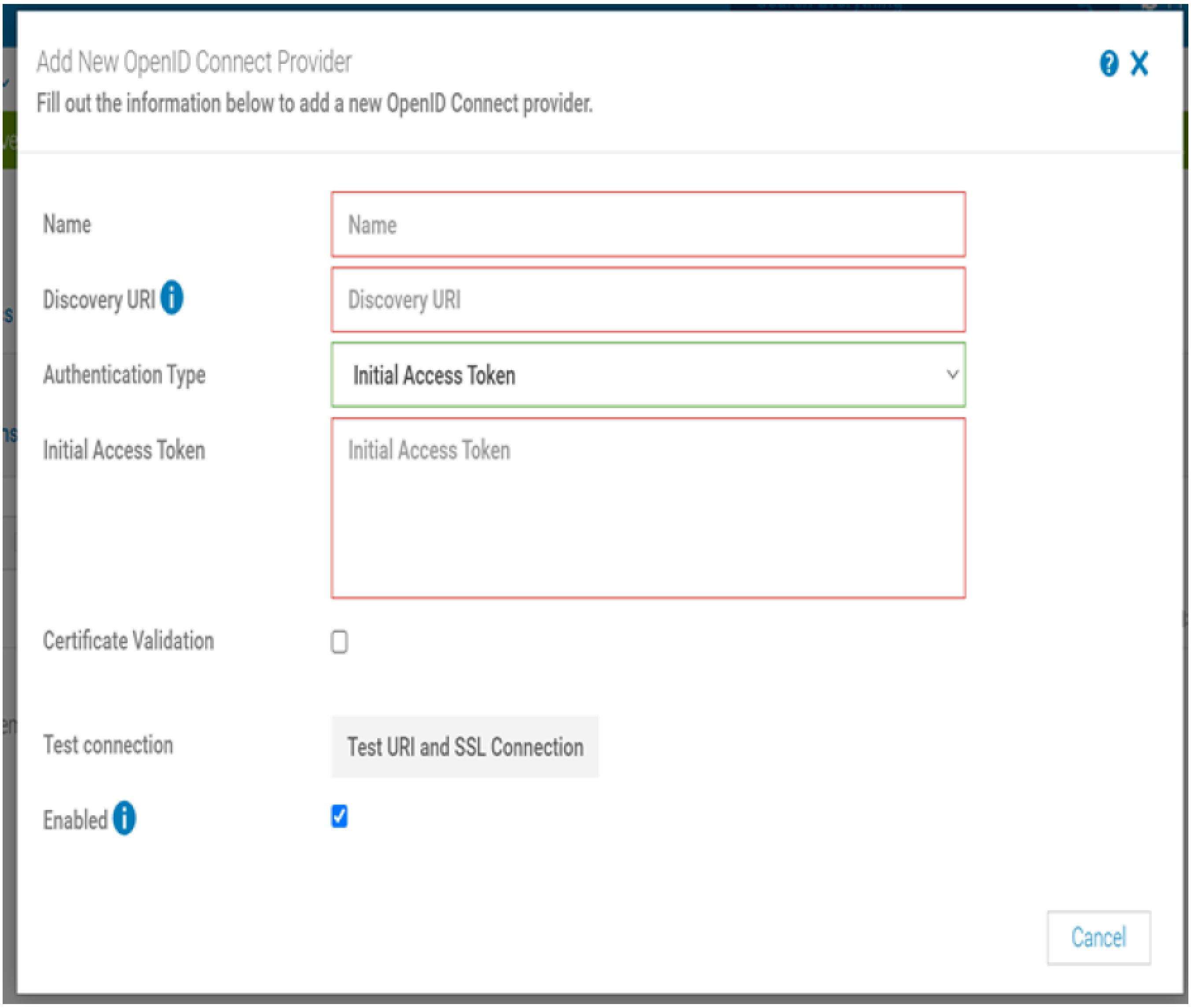
Network Timeout: 120 seconds

Search Timeout: 120 seconds

Certificate Validation: ☐ *You can drop a certificate file in this area to upload it.*

OIDC authentication

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



Add New OpenID Connect Provider

Fill out the information below to add a new OpenID Connect provider.

Name	Name
Discovery URI	Discovery URI
Authentication Type	Initial Access Token
Initial Access Token	Initial Access Token
Certificate Validation	□
Test connection	Test URI and SSL Connection
Enabled	☑

Cancel

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
- ‘
- –
- !

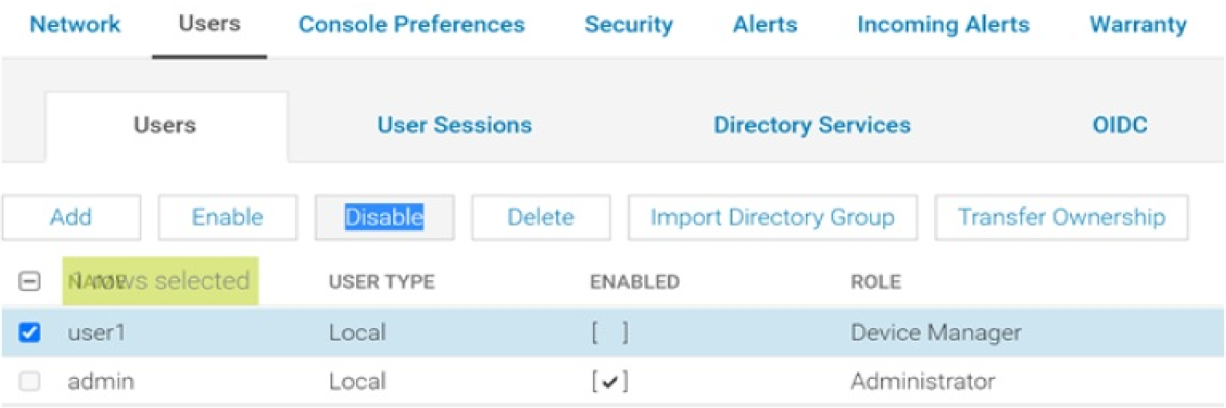
- “
- #
- $
- %
- &
- ( )
- *
- ,
- .
- /
- :
- ;
- ?
- @
- [
- \
-]
- ^
- _
- `
- {
- |
- }
- ~
- +
- <
- =
- >

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. The internal Admin account password needs to be configured immediately after deploying the appliance for the first time.

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.

NOTE: The Admin user account, which is created by default, cannot be deleted or disabled.

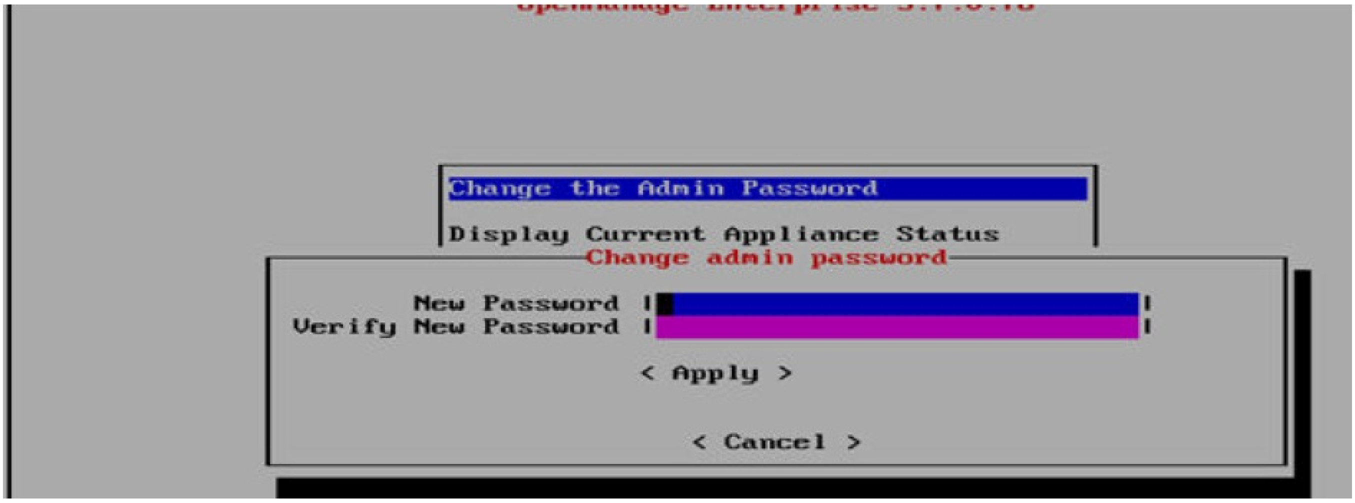


	NAME	USER TYPE	ENABLED	ROLE
☑	user1	Local	[ ]	Device Manager
□	admin	Local	[✓]	Administrator

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 > Userspage.

Changing admin password from Text User Interface



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 numerals (0-9), upper case letters (A-Z), lower case letters (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 OpenManage Enterprise version 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 o n the console ● Full access (by using GUI and REST) to read, view , create, edit, delete, export, and remove information r elated to devices and groups monitored by OpenMana ge 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

OpenManage Enterprise Supported protocols and ports on management stations

Port N umber	**Protoc ol**	**Port Type**	**Maximum Encryptio n 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 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.
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

Port Number	**Protocol**	**Port Type**	**Maximum Encryption Level**	**Source**	**Direction**	**Destination**	**Usage**

							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	UDP	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
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.
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.

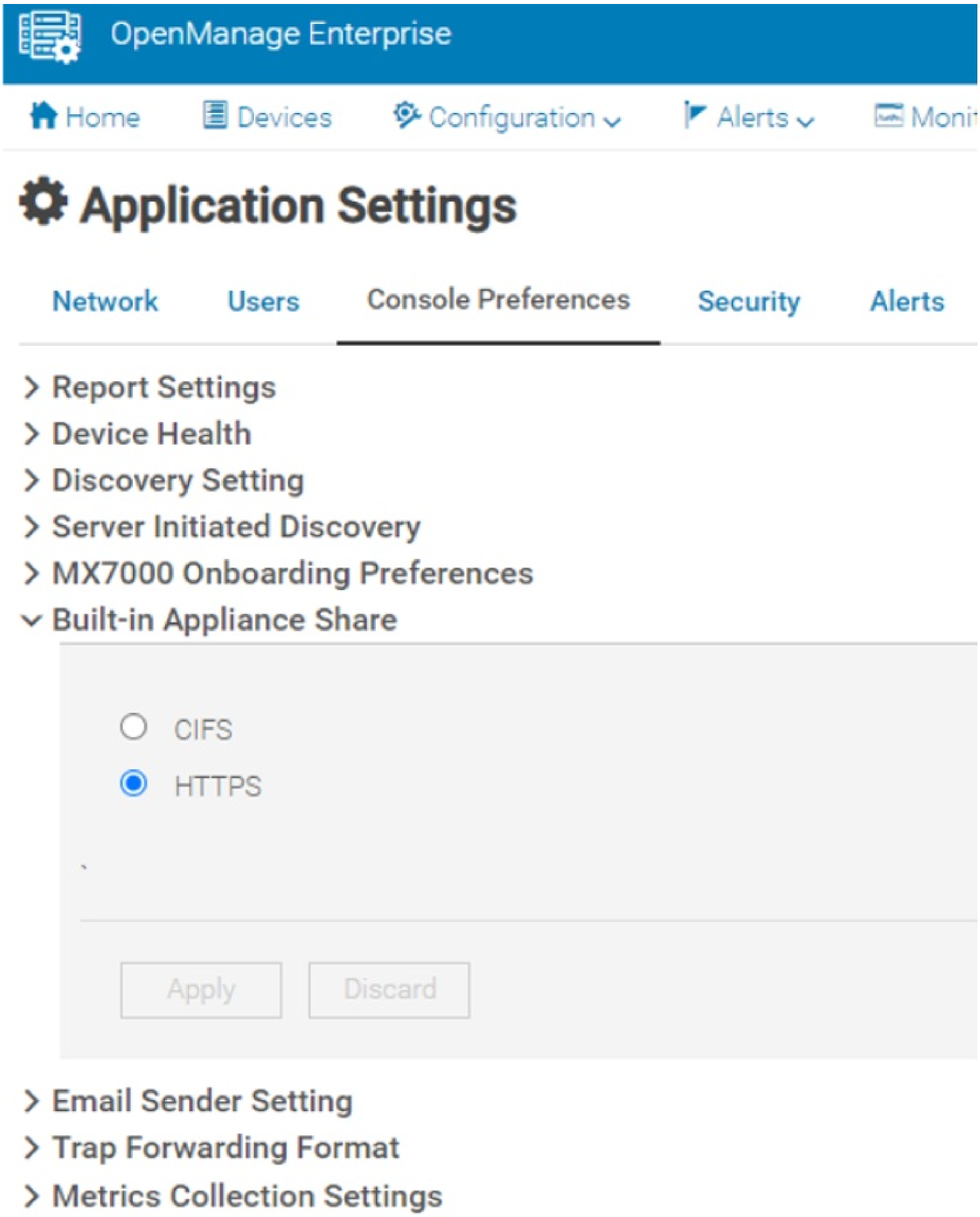
Port Number	**Protocol**	**Port Type**	**Maximum Encryption Level**	**Source**	**Direction**	**Destination**	**Usage**
443	Proprietary/ WS- Man/ Redfish	TCP	256-bit	OpenManage Enterprise appliance	Out	Managed node	● Discovery and inventory of iDRAC7 and later versions. ● For the CMC management.
623	IPMI/ 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 share

Many server operations such as Firmware Update, Template Extraction and Deployment, obtaining the Diagnostics or TechSupport Report from a server require access to an external network share (NFS / CIFS / HTTPS). Typically, it's the user's responsibility to set up and provide access to the network share. OpenManage Enterprise includes a built-in appliance file share, to reduce the work required to set up an external network share and thus improves customer experience. Access to the network share is further protected by credentials, that are rotated periodically. By default, the appliance file share is made available through CIFS (v2) and is made available to the devices that need to access it per operation. By default, a running OpenManage Enteprise instance will have smbd (samba daemon) listening on ports 139/445. With OpenManage Enterprise 3.8.x, the administrator has a choice of using HTTPS as the protocol to make the internal file share available. This can be done using the Application Settings page as follows:



Built-in Appliance Share

○ CIFS

● HTTPS

Once the switch to use HTTPS for the internal file share is made, smbd is shutdown, and the OME appliance no longer functions as a CIFS server. OME supports 12-15G servers, but only the later versions of server firmware support all operations via HTTPS shares. The table below identifies if the operation can be supported for servers, and the minimum FW version required to support it.

Use Case / Operation	**YX2X (12G) or YX3X (13G) servers**	**YX4X (14G) and above servers**
Firmware Update	Supported using: HTTPS URI 2.70.70.70 (October 2019)	Supported using: HTTPS URI 3.00.00.00
Driver Update	DSU 1.9.1	DSU 1.9.1
Server Configuration Profile (SCP) for template capture, deployment, configuration inventory, and remediation)	2.70.70.70	3.00.00.00
Technical Support Report (TSR)	N/A	3.21.21.21 (December 2018)
Remote Diagnostics	N/A	3.00.00.00

- Windows Driver update is effected over the DSU / DUEC / IC (D3 deliverables) that OME carries. DSU 1.9.1 offers HTTPS support.
- Template extraction and Profile Deployment is also supported on Chassis and IOAs. NPS Chassis does not support HTTPS (per Dev team interlocks) and will only work with NFS or CIFS shares. NGM supports HTTPS / NFS / CIFS shares.

Regardless of protocol choice (CIFS or HTTPS), access to the built-in network share is controlled by credentials, that are periodically rotated every 6 hours. This interval is not configurable. The share location and credentials are provided to the devices that need them within the context of each OME workflow. This share is used only for internal communication to the devices and there is no external method to get the share details

Field service debug (FSD)
By default, the OpenManage Enterprise appliance has SSH access disabled. Field Service Debug (FSD) enables root level access to the appliance via SSH, and can only be authorized through Dell Support services. For more information, check out the Field Service Debug sections in the Open Manage Enterprise User 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.

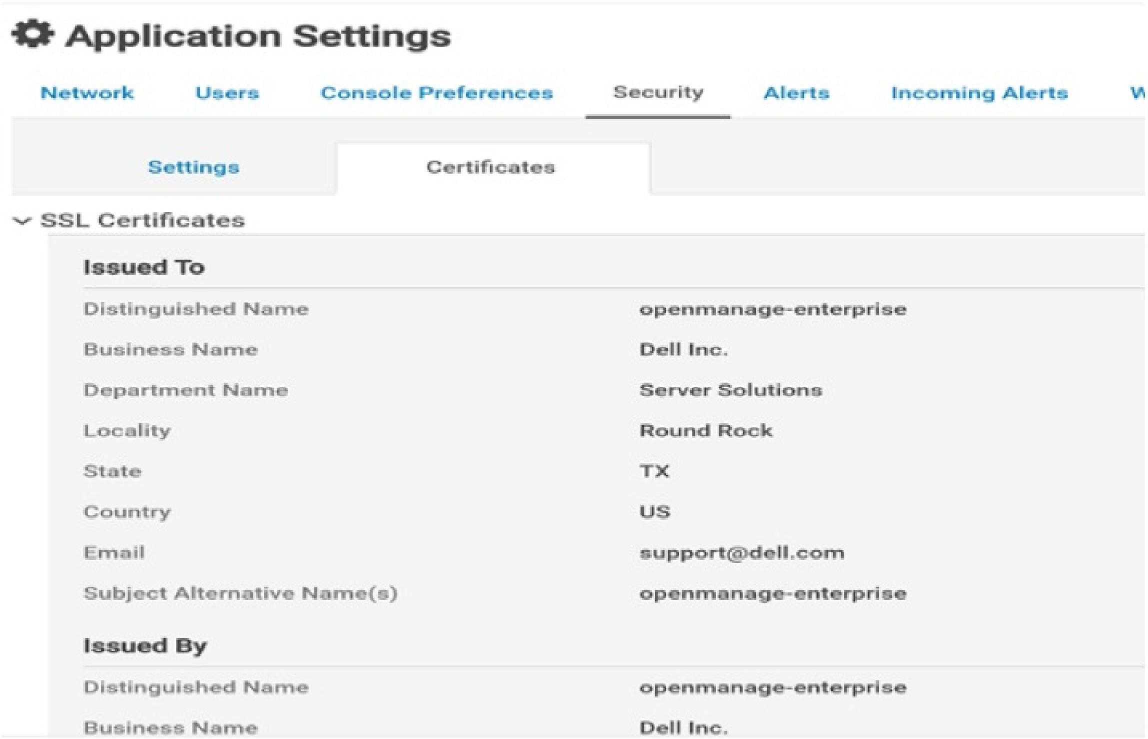
Cryptography

Internal services are configured with specific Access Control Lists (ACL) that ensure only required services can have access . OpenManage Enterprise supports industry-proven crypto algorithms for client communication. OME only allows communication via TLS v1.2 with clients. Clients can negotiate communication with OME using the below ciphers:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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.



SSL Certificates

Issued To

Distinguished Name	openmanage-enterprise
Business Name	Dell Inc.
Department Name	Server Solutions
Locality	Round Rock
State	TX
Country	US
Email	support@dell.com
Subject Alternative Name(s)	openmanage-enterprise

Issued By

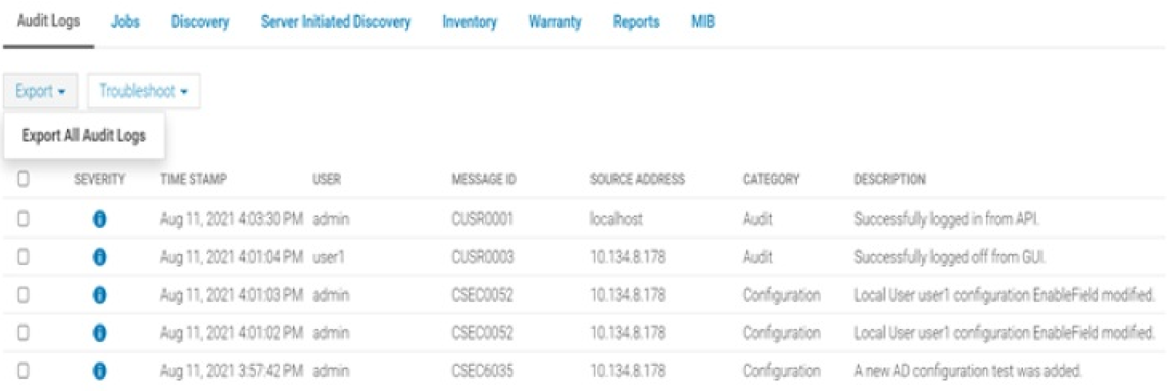
Distinguished Name	openmanage-enterprise
Business Name	Dell Inc.

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 Support teams in troubleshooting and analysis. An audit log is recorded when:

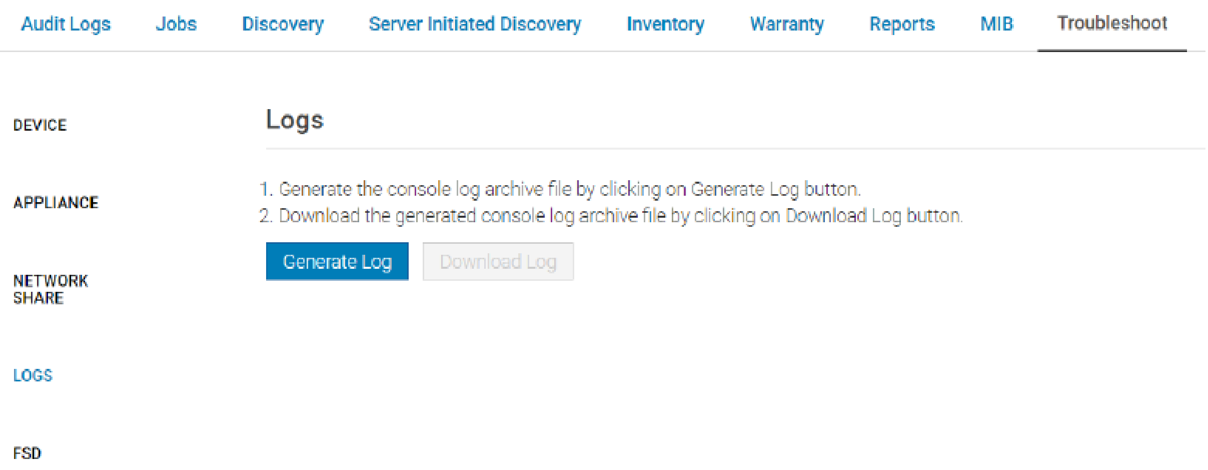
- A group is assigned, or access permission is changed.
- User role is modified.
- Actions that were performed on the devices monitored by OpenManage Enterprise. The audit log files can be exported to the CSV file format



□	SEVERITY	TIME STAMP	USER	MESSAGE ID	SOURCE ADDRESS	CATEGORY	DESCRIPTION
□	●	Aug 11, 2021 4:03:30 PM	admin	CUSR0001	localhost	Audit	Successfully logged in from API.
□	●	Aug 11, 2021 4:01:04 PM	user1	CUSR0003	10.134.8.178	Audit	Successfully logged off from GUI.
□	●	Aug 11, 2021 4:01:03 PM	admin	CSEC0052	10.134.8.178	Configuration	Local User user1 configuration EnableField modified.
□	●	Aug 11, 2021 4:01:02 PM	admin	CSEC0052	10.134.8.178	Configuration	Local User user1 configuration EnableField modified.
□	●	Aug 11, 2021 3:57:42 PM	admin	CSEC6035	10.134.8.178	Configuration	A new AD configuration test was added.

Logs

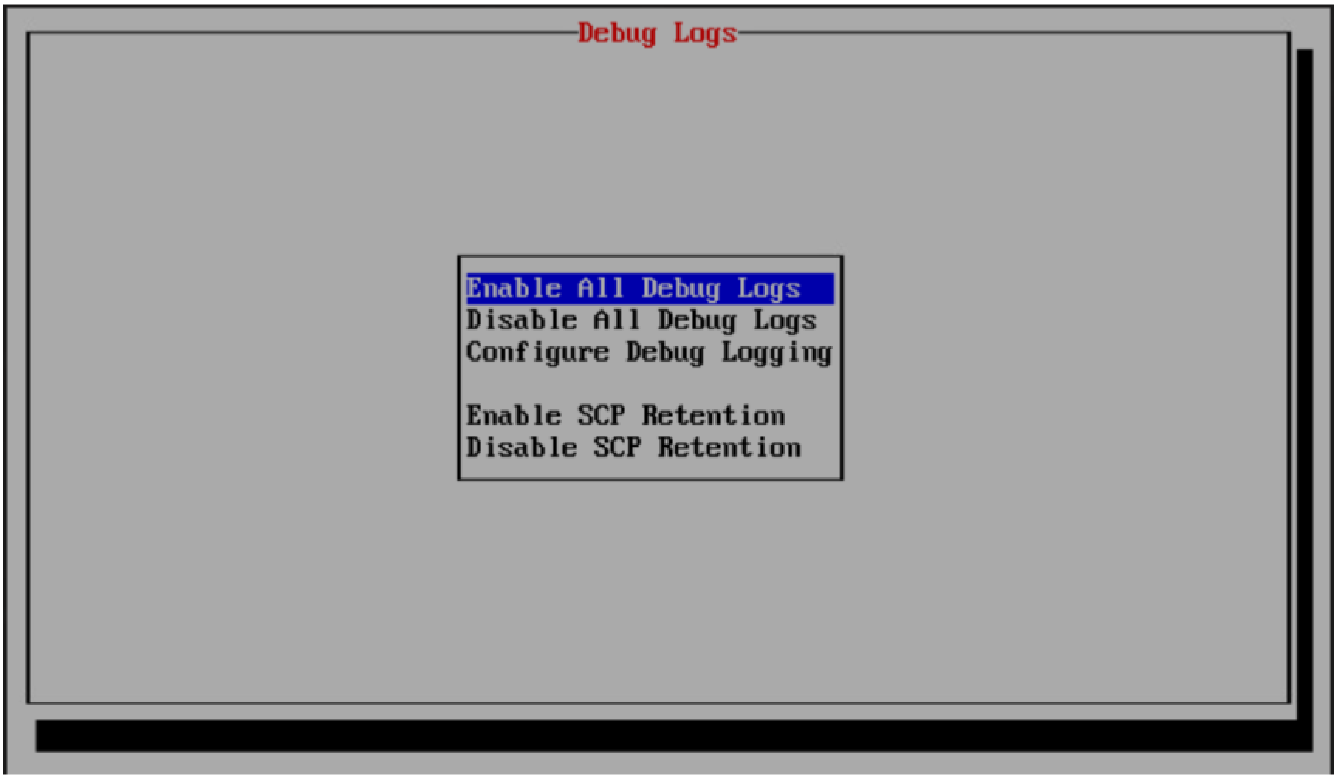
User can access all OME services logs and audit logs from the UI. Navigate to Monitor > Troubleshooting > Logs. Support can use these logs for analyzing the customer issues. By default, these logs are at INFO (or above) level.



Logs

1. Generate the console log archive file by clicking on Generate Log button.
2. Download the generated console log archive file by clicking on Download Log button.

Administrator can change log levels from Text User Interface.



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.
When using DHE-RSA ciphers, **httpd**/**mod_ssl** uses the 1024 bit key with commonly used prime numbers.	While iDRAC has removed support for DHE ciphers to fix this issue, for further protection, OME has mitigated by performing the following security measures by disabling DHE_RSA cipher support.

Documents / Resources

OpenManage Enterprise 3.10 Security Configuration Guide	**DELL 3.10 OpenManage Enterprise Security Configuration** [pdf] Owner's Manual 3.10, 3.10 OpenManage Enterprise Security Configuration, OpenManage Enterprise Security Configuration, Enterprise Security Configuration, Security Configuration