Dell EMC OpenManage Mobile

Version 4.1 User's Guide (Android)

October 2020
Rev. A00

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

About OpenManage Mobile (OMM)

By using the OpenManage Mobile (OMM) application, you can:

- Monitor and manage devices in data centers by using an Android mobile phone.
- Manages devices that are already monitored and managed by OpenManage Enterprise, OpenManage Essentials, and iDRAC7 and later versions.
- Add one or more OpenManage Essentials consoles, Integrated Dell Remote Access Controllers (iDRACs) 7 or later, OpenManage Enterprise consoles, or MX7000 chassis.
- Send alerts from the OpenManage Consoles to your mobile phone and enable troubleshoot hardware issues.

See the following videos about the OpenManage Mobile (OMM) features:

- Systems Management with OpenManage Mobile
- Dell EMC OpenManage Mobile 4.0
- Monitor and manage infrastructure with OpenManage Mobile
- Manage your PowerEdge MX7000 with Augmented Reality
- Introducing OpenManage Mobile with iDRAC Quick Sync 2
- To watch quick and short videos about handling the PowerEdge server components, go to QRL video website.

It is recommended that you upgrade to the latest version of OMM. To view information about the current version of OMM installed on your mobile phone, see View technical documentation, EULA, and version of OMM on page 57.

Hereafter, the term OpenManage Consoles implies OpenManage Essentials and OpenManage Enterprise.

Topics:

What is new in this release

Before upgrading OMM, review the new features and improvements available with OMM 4.1.

OpenManage Mobile version 4.1 is supported on Android versions 6.0 and later.

User Experience

- Added a filter option for storage devices—physical and virtual disks. See View storage devices on PowerEdge servers by using OMM on page 37.
- View OpenManage Enterprise or group chassis devices and alerts based on device health status. Tap the color symbols that indicate the device health. See View OpenManage Consoles dashboard on OMM on page 16 and View the chassis group overview on page 43.

Manage OpenManage Enterprise

- View the device warranty information managed by OpenManage Enterprise. See View warranty information of devices managed by OpenManage Enterprise on page 18.
- View the firmware compliance reports of devices managed by OpenManage Enterprise. See View firmware compliance report of device components managed by OpenManage Enterprise on page 18.
- Share server inventory information with OpenManage Enterprise by using OMM. See Share server inventory information with OpenManage Enterprise by using OMM on page 19.

Manage PowerEdge servers

- View the license information of YX4X and later PowerEdge servers. See View the OpenManage Consoles devices on OMM on page 17 and View the dashboard of individually managed servers on OMM on page 29.

Key features of OpenManage Mobile (OMM)

- Monitor and manage:
  - Devices that are already managed by OpenManage Consoles
  - An MX7000 chassis by using the AR feature
- Monitor, manage, and access:
  - Servers remotely or physically (at-the-server) by using the Quick Sync 2 module feature
  - By physically interacting with the MX7000 chassis (at-the-chassis)

Dell EMC OpenManage Consoles

The OpenManage consoles used for monitoring devices in a data center are:

- OpenManage Essentials—Hardware management application that provides a comprehensive view of systems, devices, and components in an enterprise network.
- OpenManage Enterprise—System management and monitoring application that provides a comprehensive view of the Dell EMC servers, chassis, storage, and network switches.

For more information about the OpenManage Consoles, see the respective User's Guides available at www.dell.com/openmanagemanuals.

On-device security—best practices for using OpenManage Mobile

To better secure the mobile phones used with OMM:

- Use OMM with a password. Recommended passwords must have at least 12 characters in length and use a combination of uppercase, lowercase, number, and special characters.
- Secure the device by using a password, pattern, or biometric lock. Locks are required when VPN information is cached. Enable the lock when the screen is off, or the device is inactive for more than 10 minutes.
- Enable internal-storage encryption on your mobile device. Encryption is enabled by default in Android 5, and iOS 8 or later.
- Download OMM and other applications only from trusted sources such as the Google Play Store or the Apple App Store. This includes applications that are started by OMM, including web browsers, VNC clients, and email clients. Some trusted apps are typically included with the device.
- Consider using an anti-malware app on the device.

For more information about the Quick Sync Security feature in OMM, see the Understanding OpenManage Mobile and Quick Sync Security (PowerEdge 14th Gen servers and MX Chassis) technical white paper available at www.dell.com/openmanagemobilemanuals.

2

Install and configure OpenManage Mobile

Topics:

Install OMM on your mobile phone

Before installing OMM on a mobile phone, ensure that the mobile has:

- Android version 6.0 or later.
- Access to the Google Play Store application.
- A registered Google account to receive alert notifications in OMM.

1. Start **Google Play Store** on your mobile.
2. Search for the **OpenManage Mobile** application and tap **install**.

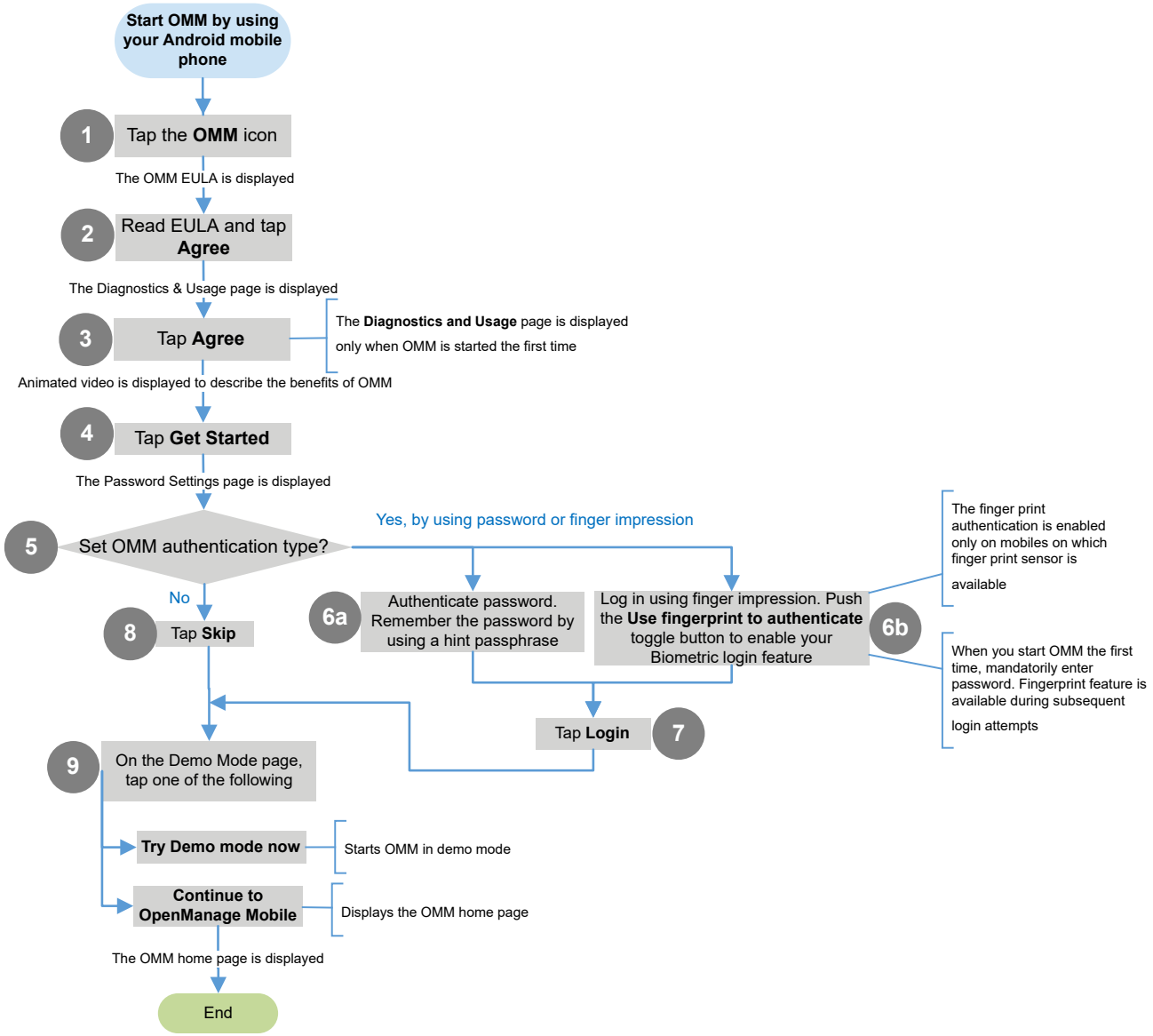
Start OpenManage Mobile (OMM)

An Internet connection is required when you start OMM for the first time.

The application tries to install a Google Cloud Messaging (GCM) token when the phone is connected to the Internet.

NOTE: To refresh the information that is displayed on any page in OMM, tap and swipe downwards.

NOTE: Data on the **OMM** page is updated every 15 minutes. The Last Poll section displays the number of minutes before which an OMM page was last updated.


Start OMM by using your Android mobile phone
1
Tap the OMM icon
The OMM EULA is displayed
2
Read EULA and tap Agree
The Diagnostics & Usage page is displayed
3
Tap Agree
The Diagnostics and Usage page is displayed only when OMM is started the first time
Animated video is displayed to describe the benefits of OMM
4
Tap Get Started
The Password Settings page is displayed
5
Set OMM authentication type?
Yes, by using password or finger impression
No
8
Tap Skip
6a
Authenticate password. Remember the password by using a hint passphrase
Log in using finger impression. Push the Use fingerprint to authenticate toggle button to enable your Biometric login feature
6b
The finger print authentication is enabled only on mobiles on which finger print sensor is available
When you start OMM the first time, mandatorily enter password. Fingerprint feature is available during subsequent login attempts
Tap Login
7
9
On the Demo Mode page, tap one of the following
Try Demo mode now
Starts OMM in demo mode
Continue to OpenManage Mobile
Displays the OMM home page
The OMM home page is displayed
End

Secure OMM by using password

You can enable password authentication using the **Enable Password** option in **Settings**.

- If an OMM password is:
  - Lost—OMM cannot recover it. You can provide a hint-phrase to remember the password. To view the hint, tap **Forgot Password**.
  - Set, and you do not use the application for more than 15 minutes—OMM is automatically logged off. The **login** page of OMM is displayed.
- To reset OMM, use the Forgot Password option on the OMM **login** page. For more information, see Reset OMM to factory default settings on page 13.

Change the OMM password

1. Do one of the following:
   - Start OMM > **Change password**.
   - On the OMM **home** page, tap  > **Settings** > **Change Password**.
2. Enter the current OMM password, new password, reenter the new password. Also, you can enter a hint-phrase to remember the password.
3. Tap **Change**.

Disable the OMM password

1. On the OMM **home** page, tap  > **Settings** > **Enable Password**.
2. Enter the current password and tap **Confirm**.

Log in to OMM by using your authenticated fingerprint

OMM provides fingerprint authentication access (biometric) to all the fingerprint registered users. The fingerprint option is not available on mobiles without a fingerprint reader.

NOTE: OMM permits five consecutive unsuccessful attempts after which the fingerprint authentication is disabled for approximately one minute. If necessary, you can enter the login password to access OMM.

You can enable fingerprint authenticated login through one of the following:

- After successful installation—See step 5 of Start OpenManage Mobile (OMM) on page 9.
- When you start OMM for the first time.
- On the Settings page—See Configure the fingerprint authentication from the settings page of OMM.

Configure the fingerprint authentication from the settings page of OMM

Ensure that you enable the fingerprint authentication on your mobile phone.

1. Tap  > **Settings**.
2. Enable the **Use fingerprint to authenticate** toggle button.
3. Tap **Yes**.

View the OMM home page

1. Start OMM.
2. If applicable, enter the OMM password and tap **Login**. The OMM **home** page is displayed.

- **RECENT**—Devices recently viewed on OMM.
- **INVENTORY**—The devices are listed based on the servers, chassis, and type of OpenManage Consoles.

3. To add new devices to OMM, tap **CONNECT**.
4. To view all the devices added in OMM, tap **VIEW ALL**.
5. To search for devices, on the **home** page or on the **VIEW ALL** >**INVENTORY** page, tap in the upper right corner. You can search for servers available on an OpenManage Enterprise console.
6. In the upper right corner of the **INVENTORY** page:
   - To view the filter options, tap .
     - Select an option from the list to filter the devices.
   - To add new devices, tap .

Navigate through the OMM features

On any OMM page, tap . A list of OMM features that enable you to manage devices is displayed:

- Home—See View the OMM home page on page 11.
- Templates—See Configure servers by using templates on OMM on page 33.
- IP pools—Specify a range of IP for template deployment.
- Task Manager—View the actions performed in OMM.
- Settings—Set and manage OMM properties.
- App log—See View the OMM application log on page 57.
- Inventory tool—See Collect server inventory using OMM on page 54 and Share server inventory information with OpenManage Enterprise by using OMM on page 19.
- Augmented Reality—See Monitor MX7000 chassis by using Augmented Reality (AR) on page 44.
- Share Feedback—See Share feedback about OMM on page 57.
- About—See Supporting information about OMM on page 57.

NOTE: Data on the **OMM** page is updated every 15 minutes. The Last Poll section displays the number of minutes before which an OMM page was last updated.

OpenManage Mobile (OMM) demo mode

By using the demo mode, you can explore the basic features of OMM—view alerts, create, and delete hosts.

Features that require data center network connection do not work in demo mode. Enabling demo mode does not delete the information that you save on OMM. When you disable the demo mode, the information you saved is restored to OMM.

1. Tap > **Settings**.
   The **Settings** page is displayed.
2. Enable the **Enable Demo Mode** toggle button.

Configure analytics settings on OMM

The analytics setting in OMM collects information about the actions you perform in OMM. OMM sends it to the Dell EMC technical support teams that use the information to enhance the functionality of the application.

You can opt to enable or disable sharing the analytics data.

NOTE:

- The analytics data that is collected does not contain any Personally Identifiable Information (PII). The collected data is treated in accordance with the Dell Privacy Policy available for review at Dell.com/ privacy.
- You are prompted to configure the analytics settings when you start OMM for the first time after an installation or upgrade.

1. Tap > **Settings**.
   The **Settings** page is displayed.
2. Enable **Share Diagnostics and Usage Data**.

Reset OMM to factory default settings

If the OMM password cannot be retrieved, you can use the reset option.

1. Do one of the following:
   - On the OMM **home** page, tap > **Settings** > **Reset OpenManage Mobile**.
   - On the **login** page, tap **Forgot Password** > **Reset OpenManage Mobile**.
2. When prompted to reset, tap **Yes**.
   The **Confirm Reset** message is displayed.
3. Tap **Reset**.
   The OMM End User License Agreement (EULA) page is displayed.
4. Start OMM. Go to step-2 of Start OpenManage Mobile (OMM) on page 9.

Uninstall OMM

WARNING: All the existing data is lost when OMM is uninstalled.

Ensure that the mobile phone is connected to the Internet.

1. On your mobile phone, press and hold the OMM icon.
   - Tap **Uninstall** > **OK**.
2. Open **Google Play Store** and tap the menu icon > **My apps and games** > **OMM** > **Uninstall**.

3

Manage OpenManage Consoles on OMM

You can manage devices monitored by OpenManage Consoles by associating them to OMM. See the *OpenManage Enterprise integration with OpenManage Mobile* technical white paper available at www.dell.com/openamanagemobilemanuals.

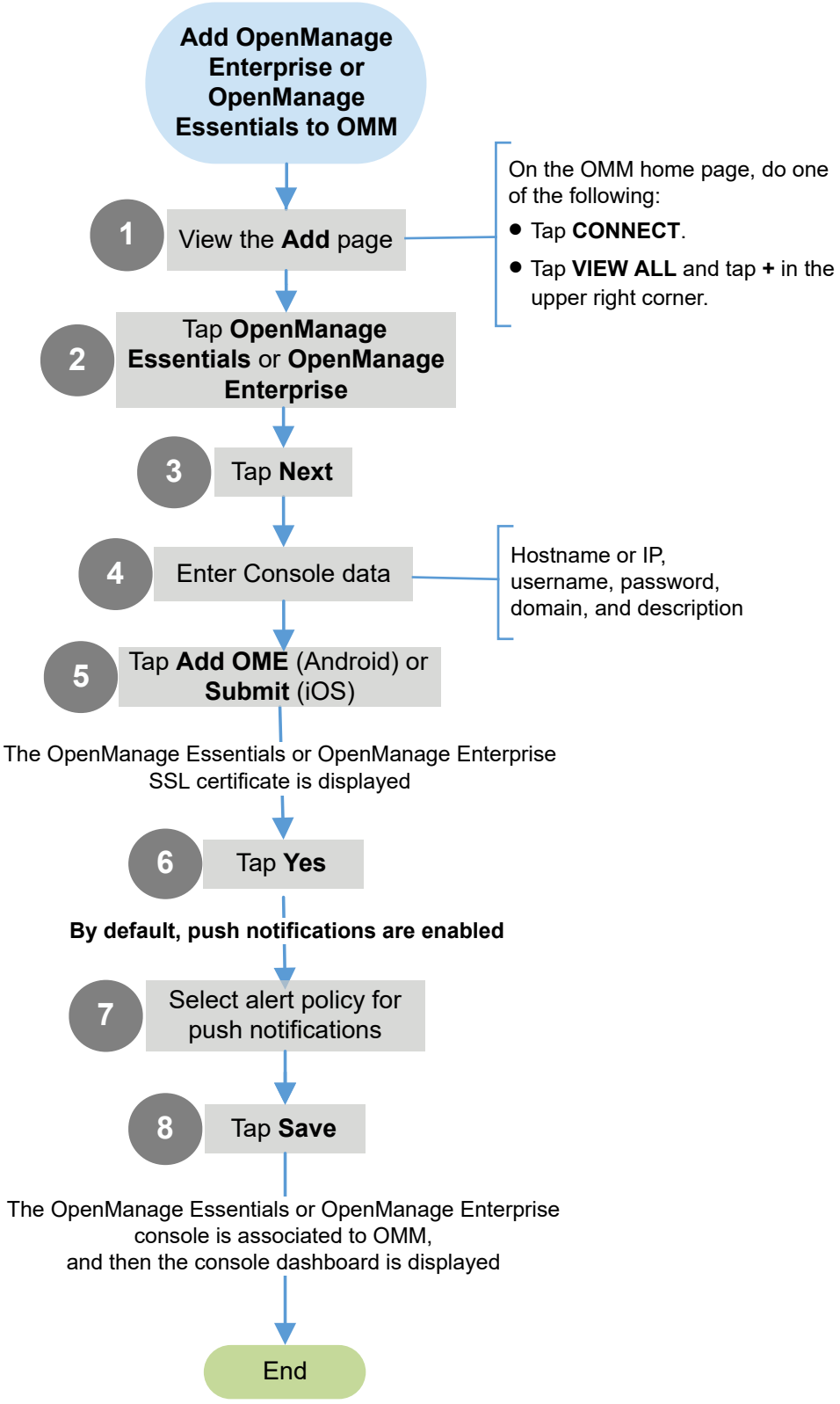
Topics:

Add OpenManage Consoles to OMM

Before adding an OpenManage Console to OMM, ensure that:

- The latest version of OpenManage Consoles is installed.
- You have VPN or internal WiFi access to the OpenManage Consoles network on mobile phone.

NOTE: To refresh the information displayed on any OMM page, tap and swipe downwards.


Add OpenManage Enterprise or OpenManage Essentials to OMM
1
View the Add page
On the OMM home page, do one of the following:
Tap CONNECT.
Tap VIEW ALL and tap + in the upper right corner.
2
Tap OpenManage Essentials or OpenManage Enterprise
3
Tap Next
4
Enter Console data
Hostname or IP, username, password, domain, and description
5
Tap Add OME (Android) or Submit (iOS)
The OpenManage Essentials or OpenManage Enterprise SSL certificate is displayed
6
Tap Yes
By default, push notifications are enabled
7
Select alert policy for push notifications
8
Tap Save
The OpenManage Essentials or OpenManage Enterprise console is associated to OMM, and then the console dashboard is displayed
End

NOTE:

- To customize your alert filters, see the respective User's Guides of OpenManage Consoles available at www.dell.com/OpenManageManuals.
- Sometimes, there might be a delay in receiving push notifications on OMM. For more information about push notifications, see Troubleshoot OMM issues.

View the Add page

On the OMM home page, do one of the following:

- Tap **CONNECT**.
- Tap **VIEW ALL**, and then tap + in the upper right corner.

Discover servers in OpenManage Enterprise console by using OMM

You can add single or multiple servers to one OpenManage Enterprise console at a time by using OMM.

Ensure that the server is added to OMM. For more information, see Add servers to be monitored by OMM without a Dell EMC console.

Discover a server in OpenManage Enterprise console by using OMM

To discover one server at a time, do the following:

1. On the OMM **home** page, tap the appropriate server.
   The **Server** dashboard is displayed.
2. Tap ⋮ > **Add Server to OME**.
   The list of OpenManage Enterprise consoles available in OMM is displayed.
3. Tap the OpenManage Enterprise console > **DONE**.
   The discovery task is initiated successfully, and then the device is added to the OpenManage Enterprise console.

Discover multiple servers in OpenManage Enterprise console

1. On the OMM **home** page, do one of the following:
   - Go to the OpenManage Enterprise console dashboard.
     - Tap ⋮ > **Import Servers**.
   - Tap **VIEW ALL** > ⋮ > **Add to OME(s)**.
     - Tap the OpenManage Enterprise console > **NEXT**.
2. Select the servers and tap **DONE**.
   The discovery task is initiated successfully, and the device is added to the OpenManage Enterprise console.

View OpenManage Consoles dashboard on OMM

1. View device data by using OMM on page 17.

   The OpenManage Consoles dashboard is displayed. For more information about the color symbols, see Colors indicating the health status of devices managed by OMM on page 67.

   - To view the devices or alerts based on the health status, on the OpenManage Enterprise dashboard, tap the color symbols that indicate the health of devices.

2. To view information about:
   - Devices or device groups in OpenManage Enterprise, tap **Devices**.
   - Alerts, tap **Alerts**.
   - Certificates, tap , and then tap **View Certificate**.
3. To view information about warranty and firmware compliance reports of devices monitored by OpenManage Enterprise:
   - Tap **Warranty Status** and **Compliance Reports**.

   NOTE: Data on the OMM page is updated every 15 minutes. The Last Poll section displays the number of minutes before which an OMM page was last updated.

View the OpenManage Consoles devices on OMM

1. View device data by using OMM on page 17.
2. On the OpenManage Consoles dashboard page, tap **Devices**.
3. Tap the appropriate device category (for example, RAC), and then tap a device to select the device you want to view. The inventory information of the device is displayed. When the warranty or license of a device is going to expire, then the information about the number of days remaining is displayed.
4. Device data that is commonly displayed on OpenManage Consoles are:
   - Software—Tap **Software Details**.
   - Hardware logs—Tap **Hardware Log**.
   - Alerts—Tap **Alerts**.
   - Warranty—Tap **Warranty**.

   However, the OpenManage Enterprise console also displays Hardware configuration data of server managed by OMM on page 30 and the following:
   - **Licenses**—View information about licenses of YX4X and later PowerEdge servers added by using network. You can also view the description, status, license type, and expiration date.
5. To access the Dell Quick Resource Locator (QRL) website, tap , and then tap **Support**. The Dell QRL website is displayed on a new web browser page.

View device alerts—generated by OpenManage Consoles—by using OMM

1. View device data by using OMM on page 17.
2. Tap **Alerts** or tap the color symbols that indicate the health status of devices.

   To filter alerts, tap the box in the upper pane of the **Alerts** page. For more information about multiple alerts, see Manage multiple alerts of devices monitored by OpenManage Consoles by using OMM.
3. Tap the alert that you want to the view. The **Alert Details** page is displayed.

   You can share, acknowledge, unacknowledge, or delete an alert.

View device data by using OMM

In the INVENTORY section of the OMM **home** page, do one of the following:

- Tap the appropriate console, chassis, or server.
- Tap **VIEW ALL**, and then tap an appropriate console, chassis, or server.

Manage multiple alerts of devices monitored by OpenManage Consoles by using OMM

1. On the OpenManage Consoles dashboard, tap **Alerts**.
   The **Alerts** page is displayed.
2. Select multiple alerts by selecting the corresponding check boxes.
3. To delete, acknowledge, unacknowledge, or share alerts, tap  , and then tap the required option.

Device warranty information

You can view the warranty information of all devices managed by OpenManage Enterprise and:

- The status of the device warranty. For more information about the color symbols, see Colors indicating the health status of devices managed by OMM on page 67.
- The option to filter the warranty information based on the days remaining to expire, Service Tag, or model.
- Information as a list or a card, tap **List** or **Cards**.
- In the **List** list, the Service Tag, server model information, and the number of days remaining for the warranty to expire is displayed. Tap the Service Tag number to view more information about the warranty of a device.
- In the **Cards** list, information about the warranty of a device is displayed.

View warranty information of devices managed by OpenManage Enterprise

1. On the OpenManage Enterprise dashboard, tap **Warranty Status**.
   The **Warranty Status** page displays all server warranty information.
2. To view information of a device, tap **View Device**.
3. To renew a device warranty, tap **Dell Warranty Renewal for Device** > **View Warranty Details Renew** > **Renew**.
   The warranty information is displayed on the Dell EMC support site page.

View firmware compliance report of device components managed by OpenManage Enterprise

1. On the OpenManage Enterprise dashboard, tap **Compliance Reports**.
   The compliance baselines are displayed.

   To view information as a list or a card, tap **List** or **Cards**.
2. From the **Cards** list, tap **View Report**.
   The devices that are associated with the baseline are displayed.
3. To view the health status and firmware compliance information of the device components, tap a device name.
   The overview of the device and the components are displayed.
   a. To view the components, tap **View Components**.
   b. To view the firmware information on the Dell EMC support site page, tap the baseline of a component.

Share server inventory information with OpenManage Enterprise by using OMM

You can share server inventory information of all servers in OMM with OpenManage Enterprise console for discovery of servers.

Ensure that you add servers to the **Inventory Tool** page. For more information, see Add servers to the inventory page by using OMM on page 54.

1. Tap > **Inventory Tool**.
2. On the **Inventory Tool** page, tap **Send** > **Send to OME** > **NEXT**.
3. To save the server inventory information in a CSV file, tap **Send** > **Export to CSV** > **NEXT**.
   Provide the encryption password and share the file by using any application available on your mobile. Use the file to import the server credentials to OpenManage Enterprise console.
4. Select the OpenManage Enterprise console and tap **SEND**.
   The servers are exported from OMM to OpenManage Enterprise.

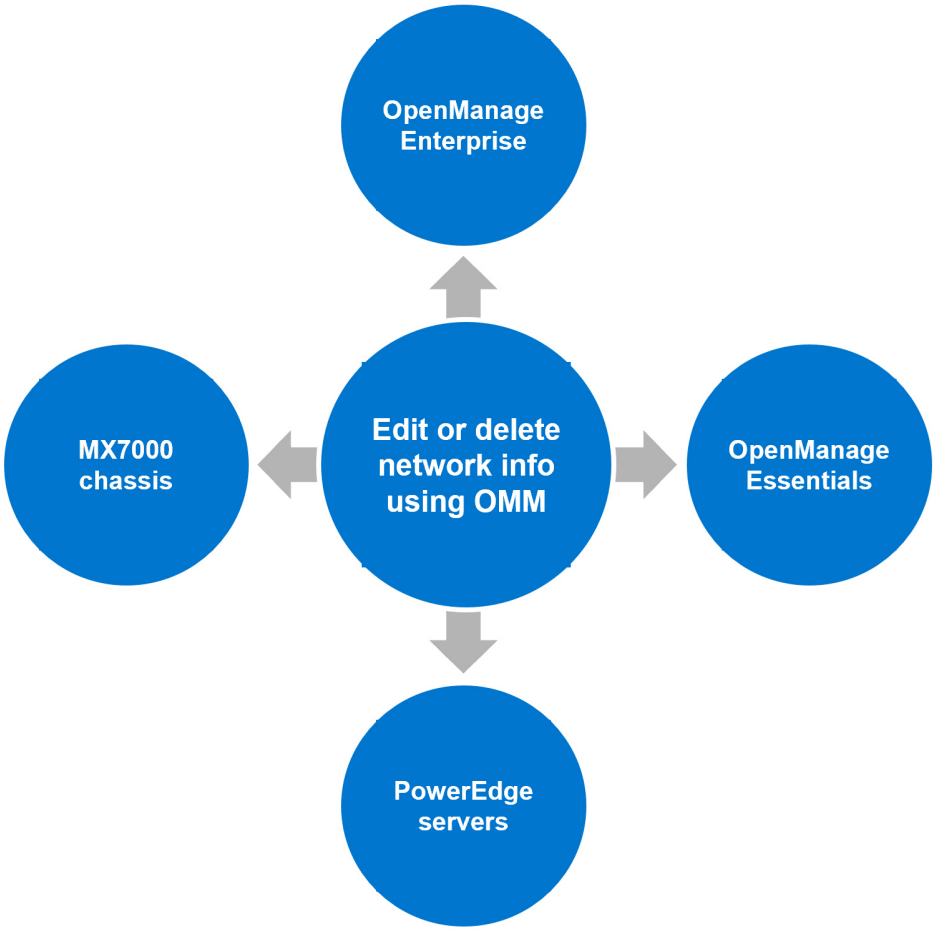
Manage power operations on devices monitored by OpenManage Consoles by using OMM

Ensure that the server and iDRAC are discovered to perform all the power operations.

For devices managed by OpenManage Consoles, the power-control operations are supported only on iDRAC and servers.

1. View device data by using OMM on page 17.
2. On the OpenManage Consoles dashboard, tap **Devices**.
3. Tap the appropriate device category (for example, RAC), and then tap to select the device.
   The inventory information of the device is displayed.
4. Tap > **Reboot**.
   Options to power cycle, shut down the operating system, power on, or power off are displayed.
5. Select the power-control operation that you want to perform.
6. Tap **Submit**.

Edit or delete the network connection information by using OMM



1. In the INVENTORY section of the OMM **home** page, tap **VIEW ALL**.
   A list of devices monitored by the OpenManage Consoles, chassis, and servers available in OMM are displayed.
2. Do one of the following:
   - Press and hold the device name (IP address), and then tap **Edit Connection**.
     - To delete the device, tap **Delete**.
   - Swipe the device name (IP address) to the left, and then tap **Edit** or **Delete**.
3. Edit the hostname or IP, username, password, domain, and description.
4. For OpenManage Consoles, do the following:
   a. Tap **Next**.
   b. Edit the alert policy for alert subscription.
5. Tap **Save**.

   NOTE: If OMM is unable to contact the OpenManage Consoles server when the console is deleted or edited, the latter retains the device in its mobile subscriber list until it is manually deleted. For more information about deleting a mobile subscriber', see the respective User's Guide of *OpenManage Essentials* or *OpenManage Enterprise* available at www.dell.com/openmanagemanuals.

6. To view the updated information of a chassis, manually reconnect OMM to the chassis.
   - On the chassis dashboard, swipe downwards to view the updated status of the device.

   The chassis is reconnected.

View reports of devices managed by OpenManage Enterprise

You can view the reports of devices managed by OpenManage Enterprise and OpenManage Enterprise Power Manager.

To view Power Manager reports, ensure that:

- The Power Manager plug-in is installed on the OpenManage Enterprise appliance.
- There is sufficient disk space on your mobile phone to download and save the reports.

For more information about Power Manager reports, see the OpenManage Enterprise Power Manager User's Guide available at www.dell.com/powermanager.

1. On the OMM **home** page, go to the OpenManage Enterprise dashboard.
2. Tap  > **View Reports**.
3. Tap any device, and tap any report.
4. Tap **Generate New Report** > **TASK MANAGER**.
   You can monitor this action in Task Manager.
5. To view the report, perform step 3 and tap **VIEW**.
6. To refresh the report, tap **Refresh Report**.

4

Manage OpenManage Enterprise Power Manager

You can view the Power Manager reports and perform an Emergency Power Reduction (EPR) on devices and groups managed by Power Manager by using OMM.

Topics:

Enable Emergency Power Reduction (EPR) feature on devices or groups by using OMM

By using OMM, you can enable EPR on a device or on devices that are part of a group.

Ensure that:

- The Power Manager plug-in is installed on the OpenManage Enterprise appliance.
- You have the necessary user privileges.

1. On the OMM **home** page, open the OpenManage Enterprise dashboard.
2. Tap **Devices** and select a device or a group.
   The **Device Inventory** page is displayed.
3. Tap > **Enable EPR**.
4. Tap one of the following options:
   - **Throttle**—All the selected devices or groups consume extremely less power and have an impact on performance.
     NOTE: This feature is supported on devices that have an OpenManage Enterprise Advance license and iDRAC Enterprise license.
   - **Shut down**—All the selected devices or groups are shut down gracefully.
     NOTE: In a group consisting of servers and chassis, this feature is supported only for servers. This feature is supported on devices that have an OpenManage Enterprise Advance license and iDRAC Enterprise or Express license.

   EPR is enabled on the selected device or group. A yellow bar indicator is displayed on the OpenManage Enterprise dashboard indicating the number of EPR-enabled devices.

Disable EPR on devices or groups by using OMM

Ensure that:

- The Power Manager plug-in is installed on the OpenManage Enterprise console.
- You have the necessary user privileges.

1. On the OMM **home** page, open the OpenManage Enterprise dashboard.
2. Tap **Devices** and select a device or a group.
3. Do one of the following:
   - On the yellow bar indicator, tap **Disable EPR**.
   - Tap > **Disable EPR**.

EPR is successfully disabled.

View EPR-enabled devices or groups by using OMM

Ensure that EPR is enabled on devices or groups. For more information, see Enable Emergency Power Reduction (EPR) feature on devices by using OMM.

1. From the OMM **home** page, open the OpenManage Enterprise dashboard.
2. Do one of the following:
   - On the yellow bar indicator, tap **View Devices**.
   - Tap **Devices** > **EPR**.

   The list of devices that are EPR-enabled is displayed.

5

Individually manage PowerEdge servers by using OMM

OpenManage Mobile enables you to monitor your data center devices that are not associated with OpenManage Consoles. You can directly access the iDRAC of a PowerEdge server by using this unique feature in OMM.

Topics:

Features available for different series of PowerEdge servers

For more information about the naming conventions of servers, see Identifying the series of your Dell EMC PowerEdge servers on page 68.

Devices—YX2X and YX3X servers added by using network

- Hardware logs—System event and Lifecycle logs
- Firmware details—Yes
- Network details—Yes
- Storage—Not applicable
- Hardware inventory—Yes
- Health status—Yes
- Warranty information—Yes
- SupportAssist collection—Not applicable
- Location—Yes

Devices—YX2X and YX3X servers added by using iDRAC Quick Sync Read

- Hardware logs—System event and Lifecycle logs
- Firmware details—Yes
- Network details—Yes
- Storage—Not applicable
- Hardware inventory—Not applicable
- Health status—Yes
- Warranty information—Yes
- SupportAssist collection—Not applicable
- Location—Yes

Devices—YX4X servers added by using network

- Hardware logs—Yes
- Firmware details—Yes
- Network details—Yes
- Storage—Yes
- Hardware inventory—Yes
- Health status—Yes
- Warranty information—Yes
- SupportAssist collection—Yes
- Location—Yes

Devices—YX4X servers added by using Quick Sync 2

- Hardware logs—System event and Lifecycle logs
- Firmware details—Yes
- Network details—Yes
- Storage—Not applicable
- Hardware inventory—Yes
- Health status—Yes
- Warranty information—Yes
- SupportAssist collection—Yes
- Location—Yes

Add servers to be monitored by OMM without a Dell EMC console

Before adding servers to OMM, ensure that you have:

- iDRAC7 or later with Enterprise or Express edition license. Or, iDRAC9 with Datacenter license.
- VPN or internal WiFi access to the iDRAC network from your mobile phone.

You can add servers to OMM by using a network, Quick Sync Read, or Quick Sync 2.

NOTE: To refresh the information displayed on any page in OMM, tap and swipe downwards.

Add servers to OMM without a Dell EMC console by using a network

If the username and password are the same, you can add multiple servers. Ensure to add all the servers in the range by using a + or * for the last octet. For example, 192.168.0. Or, enter the start and end IP numbers of the server in the last octet and use a dash to separate it. For example, `192.168.0.50-100`.

1. View the Add page on page 16.
2. Add a device by using a network on page 25.

Add a device by using a network

1. Tap **Server or MX Chassis** > **NEXT** > **Add via Network** > **NEXT**.
2. Enter the hostname or IP, username, password, and domain of the device.
3. To save data you entered, tap **Add iDRAC** or **Add MX Chassis**.
   The server or chassis is added to OMM and the updated server or chassis dashboard is displayed.

Add servers to OMM without Dell EMC console by using iDRAC Quick Sync Read feature

Ensure that the Near-Field Communication (NFC) chip inside the mobile phone must be in contact with the iDRAC Quick Sync activation switch. To identify the NFC chip in your mobile phone, see the respective mobile phone documentation.

This feature is applicable only for YX3X PowerEdge servers with iDRAC Quick Sync bezel.

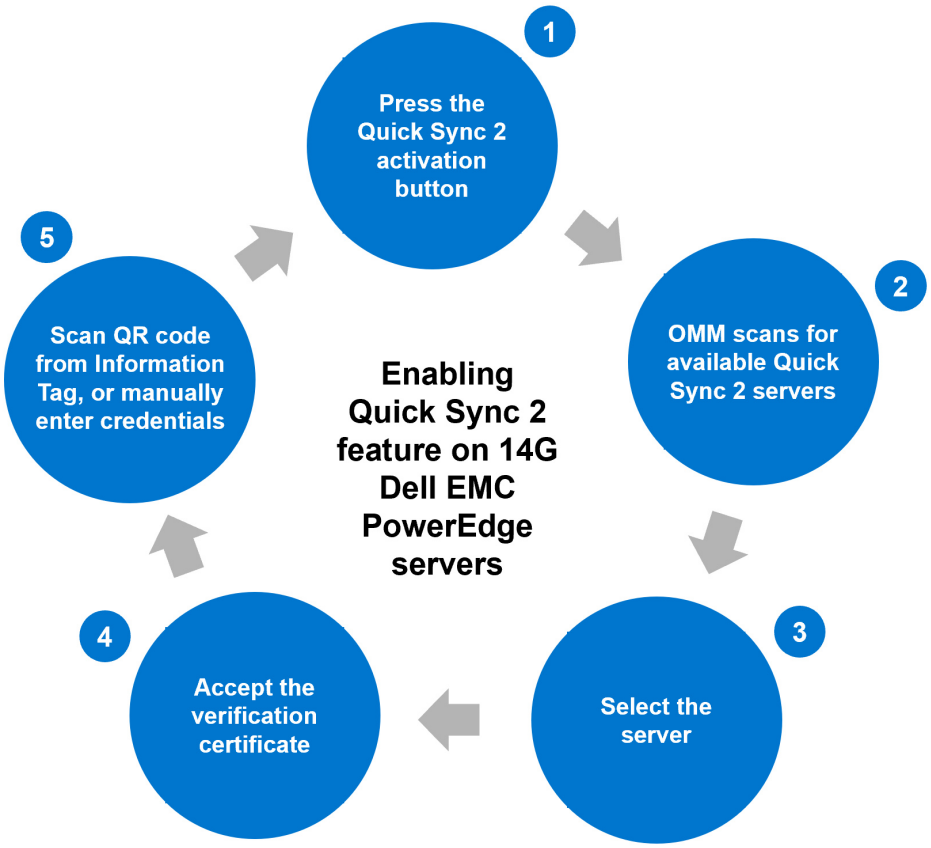
For more information about the naming conventions of servers, see Identifying the series of your Dell EMC PowerEdge servers on page 68.

To watch quick and short videos about handling the PowerEdge server components, go to the QRL video website.

1. View the Add page on page 16.
2. Tap **Server** > **NEXT** > **Add via Quick Sync** > **NEXT** > **Launch iDRAC Quick Sync**.
3. Enable iDRAC Quick Sync bezel on the server.
4. Hold your mobile phone close to the activation switch of the iDRAC Quick Sync bezel on your server. Ensure to hold your mobile for at least three seconds.

   NOTE: The iDRAC Quick Sync bezel remains activated for about 30 seconds. If you do not add the server within 30 seconds, reactivate the iDRAC Quick Sync Bezel and retry step 3.

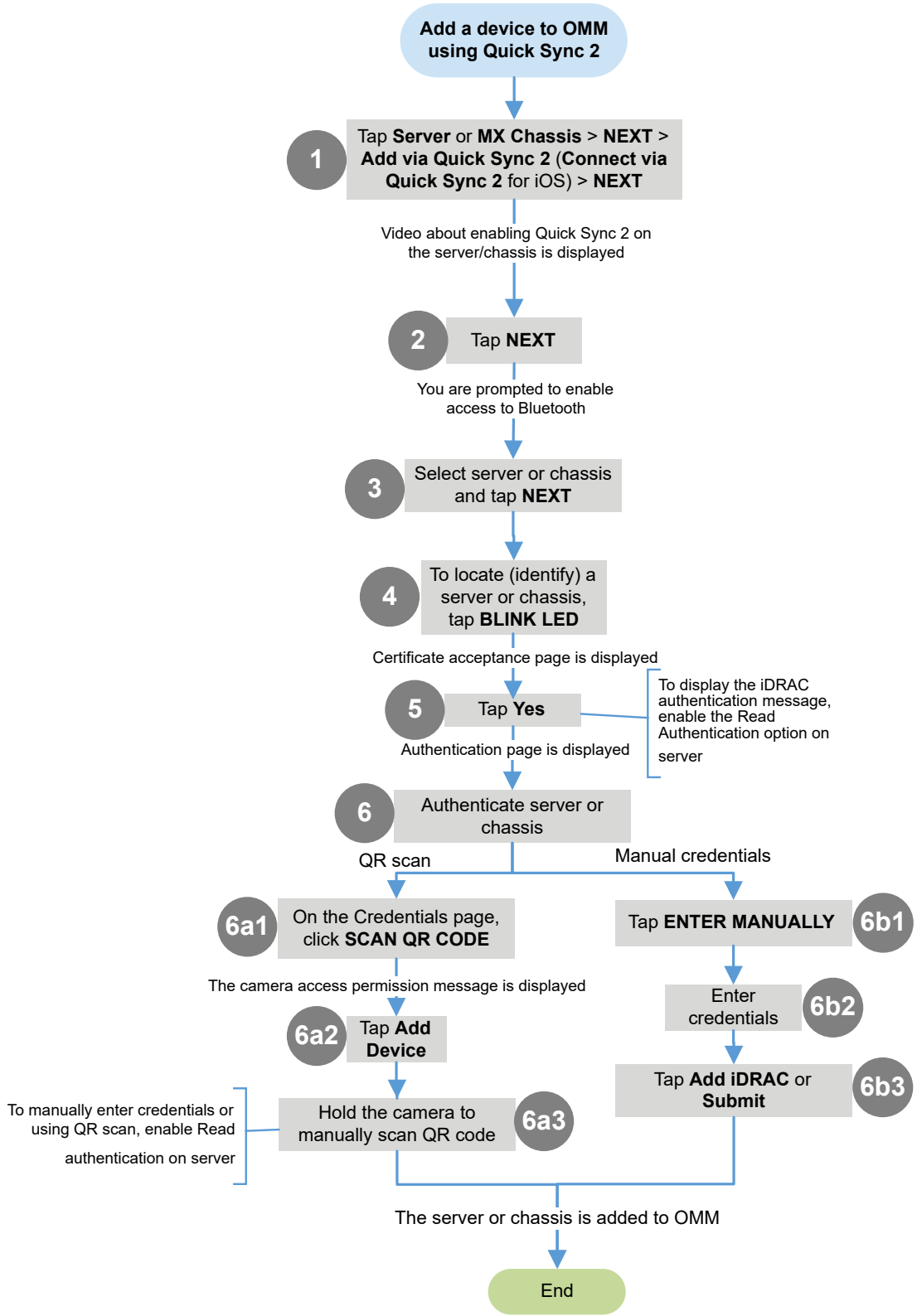
Enable Quick Sync 2 on PowerEdge servers



Add servers to OMM without Dell EMC console by using Quick Sync 2

1. View the Add page on page 16.
2. Add a device by using Quick Sync 2.

Add a device by using Quick Sync 2



View the dashboard of individually managed servers on OMM

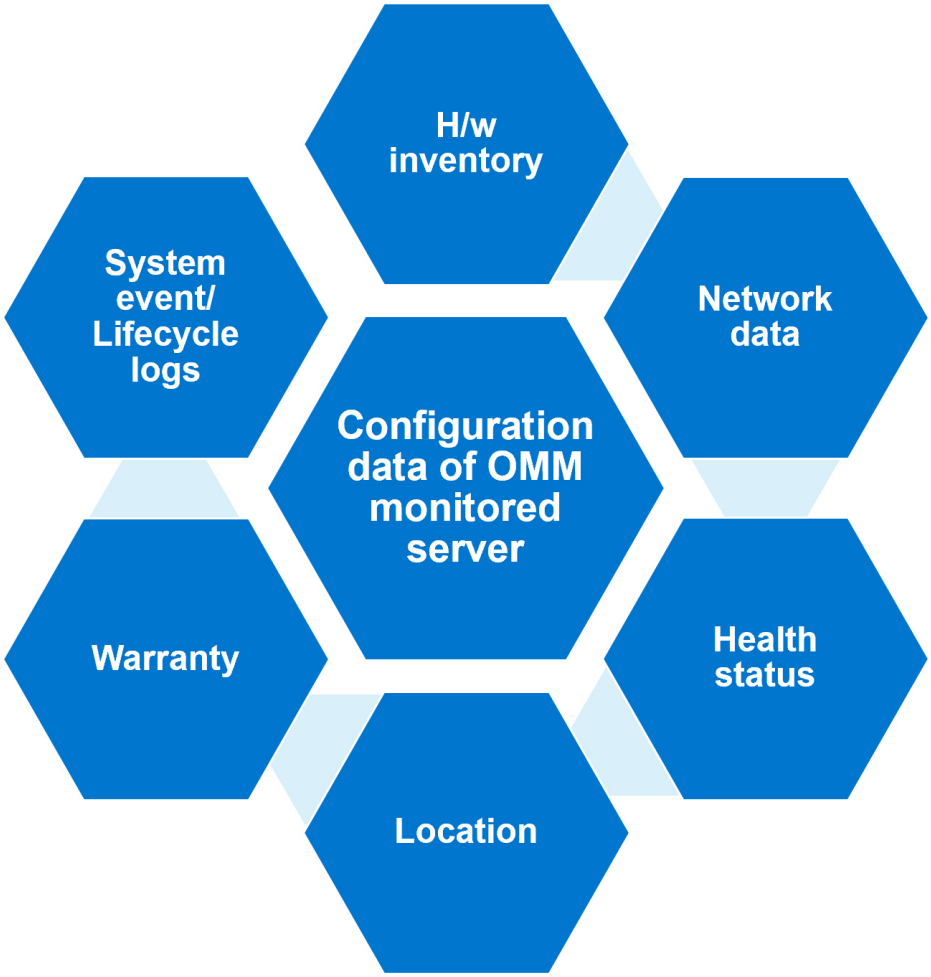
Ensure to accept all the storage permissions while downloading a SupportAssist report.

1. View device data by using OMM on page 17.
2. You can view the Hardware configuration data of server managed by OMM on page 30 and the following information:
   - **Firmware Details**—View information about the firmware versions of BIOS, CPLD, iDRAC, and Lifecycle Controller running on the server.
   - **SupportAssist Collection**—Create a SupportAssist report of the storage and debug logs, operating system, and application data.
   - **Licenses**—View information about licenses of YX4X and later PowerEdge servers added by using network. You can also view the description, status, license type, and expiration date.
   - To view the Dell Technologies QRL website, tap , and then tap **Support**.

   To share information using an application available on your phone, tap , and then tap **Share**.

   NOTE: Data on the OMM page is updated every 15 minutes. The **Last Poll** section displays the number of minutes before which an OMM page was last updated.

Hardware configuration data of server managed by OMM



View information about individually managed servers on OMM

1. View device data by using OMM on page 17.
2. Tap .
3. Select one of the following:
   - **Launch Virtual Console**—Start the virtual console by using OMM on page 31.
   - **Configure**—PowerEdge server properties by using OMM:
     - See Configure server power operations by using OMM on page 31.
     - See Configure servers manually by using OMM on page 31.
     - See Configure servers automatically by using WS-Man on OMM on page 33.
     - See Configure servers by using templates on OMM on page 33.
   - **Enable Network**—See Edit or delete the network connection information by using OMM.
   - **Report**—Generate a comprehensive report about the information of servers—system overview, CPU, memory, and location information, health status, network details, warranty, and logs.
   - **Share**—Share information about servers—IP address, health status, power state, CPU information, and memory.

- **Power Options**—See Configure server power operations by using OMM on page 31.
- **Blink LED**—Blink the server LED to locate a server.
- **Launch iDRAC GUI**—View information about iDRAC on a web browser page.
- **Diagnostics**—See Diagnose servers by using Quick Sync 2 on page 36.
- **Run RACADM command**—See Run RACADM commands by using OMM on page 36.
- **Support**—View the Dell QRL website: QRL video website.
- **View Certificate**—View the warranty status of OMM installed on the mobile phone.

NOTE: To refresh the information displayed on any page in OMM, tap and swipe downwards.

Start the virtual console by using OMM

To view the remote desktop, ensure that the bVNC Viewer is installed on your mobile phone.

For more information about accessing Remote Desktop using VNC on PowerEdge servers and MX7000 chassis, see the Accessing Remote Desktop using VNC on Dell PowerEdge Servers and MX7000 Modular Infrastructure technical white paper available at www.dell.com/openmanagemobilemanuals.

1. View device data by using OMM on page 17.
2. Tap > **Launch Virtual Console**.
   The **Launch Remote Desktop** page is displayed.
3. Enter the remote desktop password, and then tap **Launch**. The password is the VNC password that is configured in iDRAC settings. For more information about the VNC password, see the iDRAC User's Guide available at www.dell.com/idracmanuals.
   The bVNC Viewer starts, and the remote desktop is displayed.

   In iDRAC, if the encryption is set to 128-bit or more, select the **Use Secure Tunnel** check box.

   NOTE: The bVNC application displays a message indicating that connection cannot be started with remote desktop when:

   - The iDRAC does not support remote desktop.
   - A remote desktop password is not set.

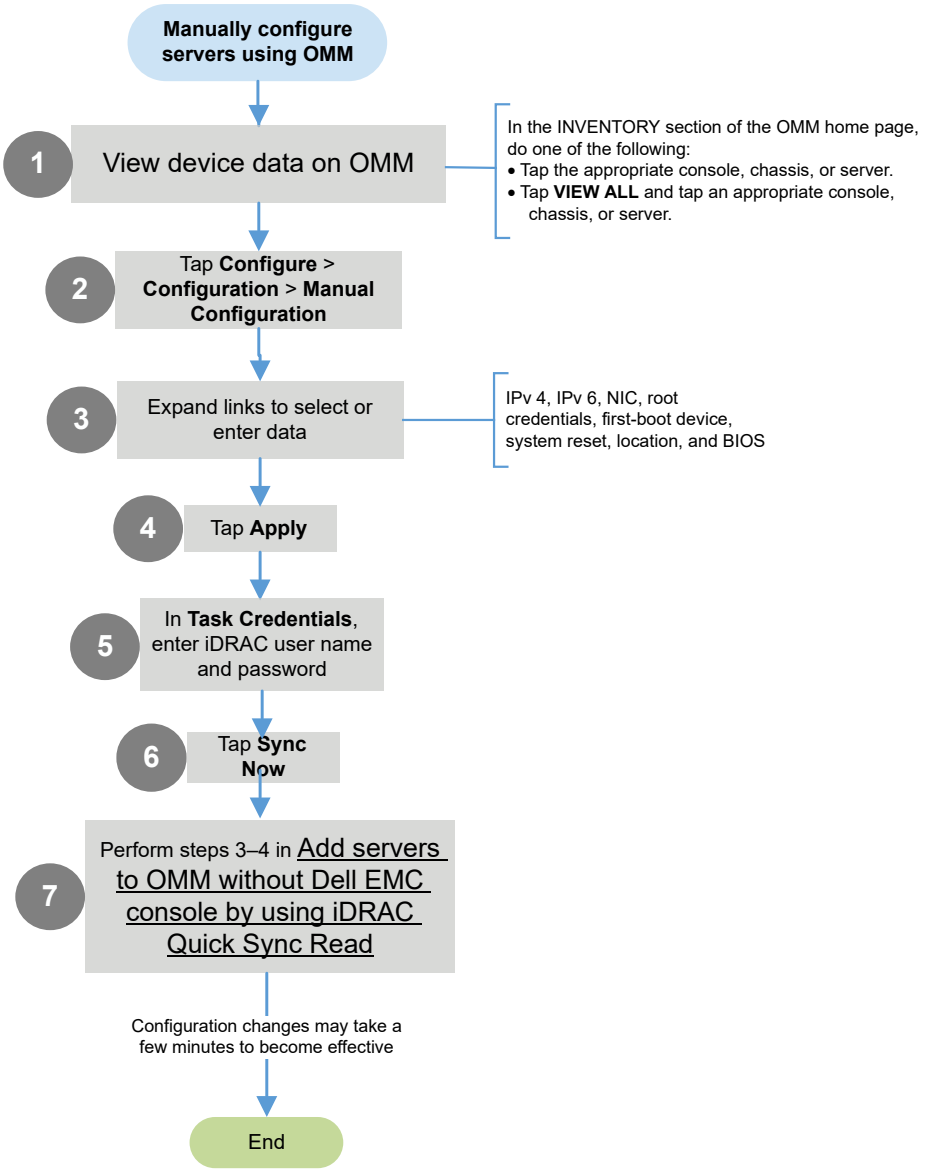
Configure server power operations by using OMM

1. View device data by using OMM on page 17.
2. Tap > **Power Options**.
   Options to power cycle, shut down the operating system, or full power-cycle are displayed.
   NOTE: The full power-cycle operation can be performed only on individually managed servers.
3. Select the power-control operation that you want to perform and tap **Submit**.
   OpenManage Mobile performs the requested power-control operation.
   NOTE: The Shutdown OS First feature is supported only for those power-control operations that support a normal shutdown of the operating system.

   NOTE: On the Power Options page, credentials that are used when adding a server are displayed. You can change the username and password, if necessary.

Configure servers manually by using OMM

The server configuration can be changed only on YX3X servers that have the iDRAC Quick Sync bezel. For more information about the naming conventions of servers, see Identifying the series of your Dell EMC PowerEdge servers on page 68.

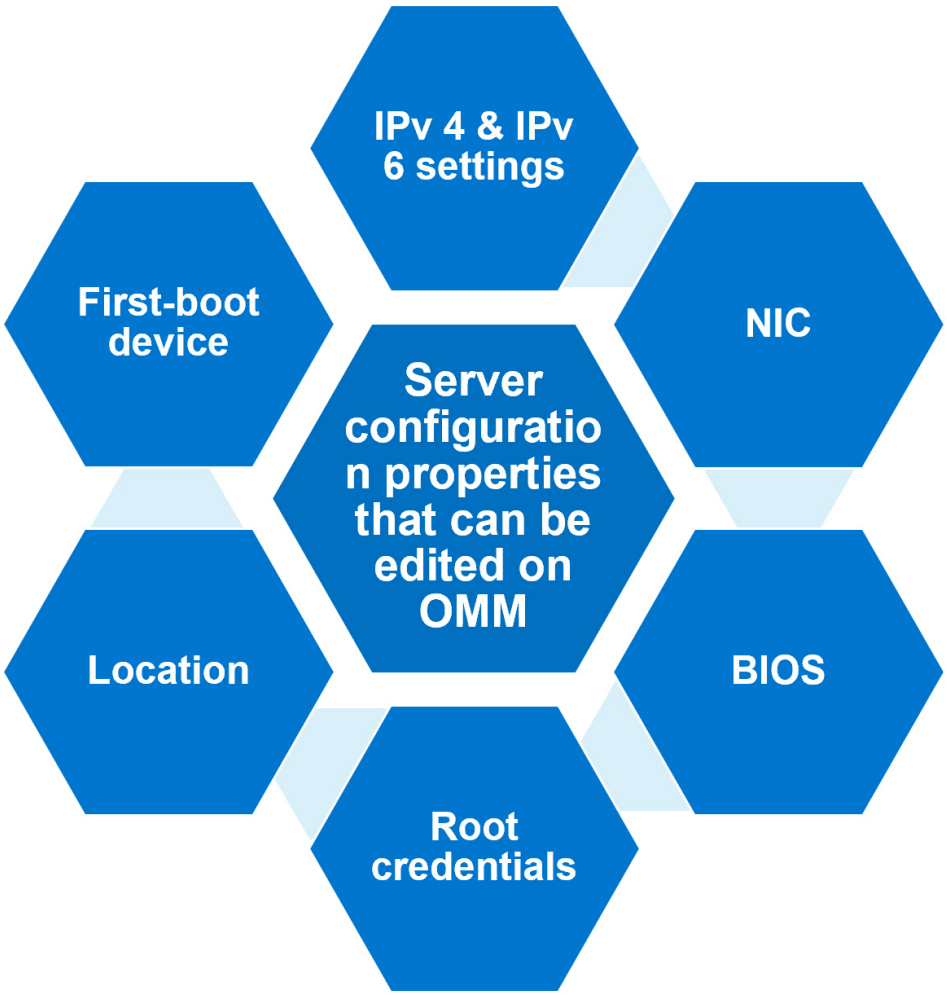

Manually configure servers using OMM
1
View device data on OMM
In the INVENTORY section of the OMM home page, do one of the following:
• Tap the appropriate console, chassis, or server.
• Tap VIEW ALL and tap an appropriate console, chassis, or server.
2
Tap Configure > Configuration > Manual Configuration
3
Expand links to select or enter data
IPv 4, IPv 6, NIC, root credentials, first-boot device, system reset, location, and BIOS
4
Tap Apply
5
In Task Credentials, enter iDRAC user name and password
6
Tap Sync Now
7
Perform steps 3–4 in Add servers to OMM without Dell EMC console by using iDRAC Quick Sync Read
Configuration changes may take a few minutes to become effective
End

Configure servers automatically by using WS-Man on OMM

This option is available only on servers that have an iDRAC Enterprise or Datacenter licenses.

1. View device data by using OMM on page 17.
2. Tap ⋮ > **Configure** > **Configuration**.
3. Enable **Auto Config**.
   The **Select DHCP Provisioning** dialog box is displayed.
4. Tap **DHCP Provisioning**, tap the appropriate option, and then tap **Next**.
   The configuration information is saved.

Configure servers by using templates on OMM



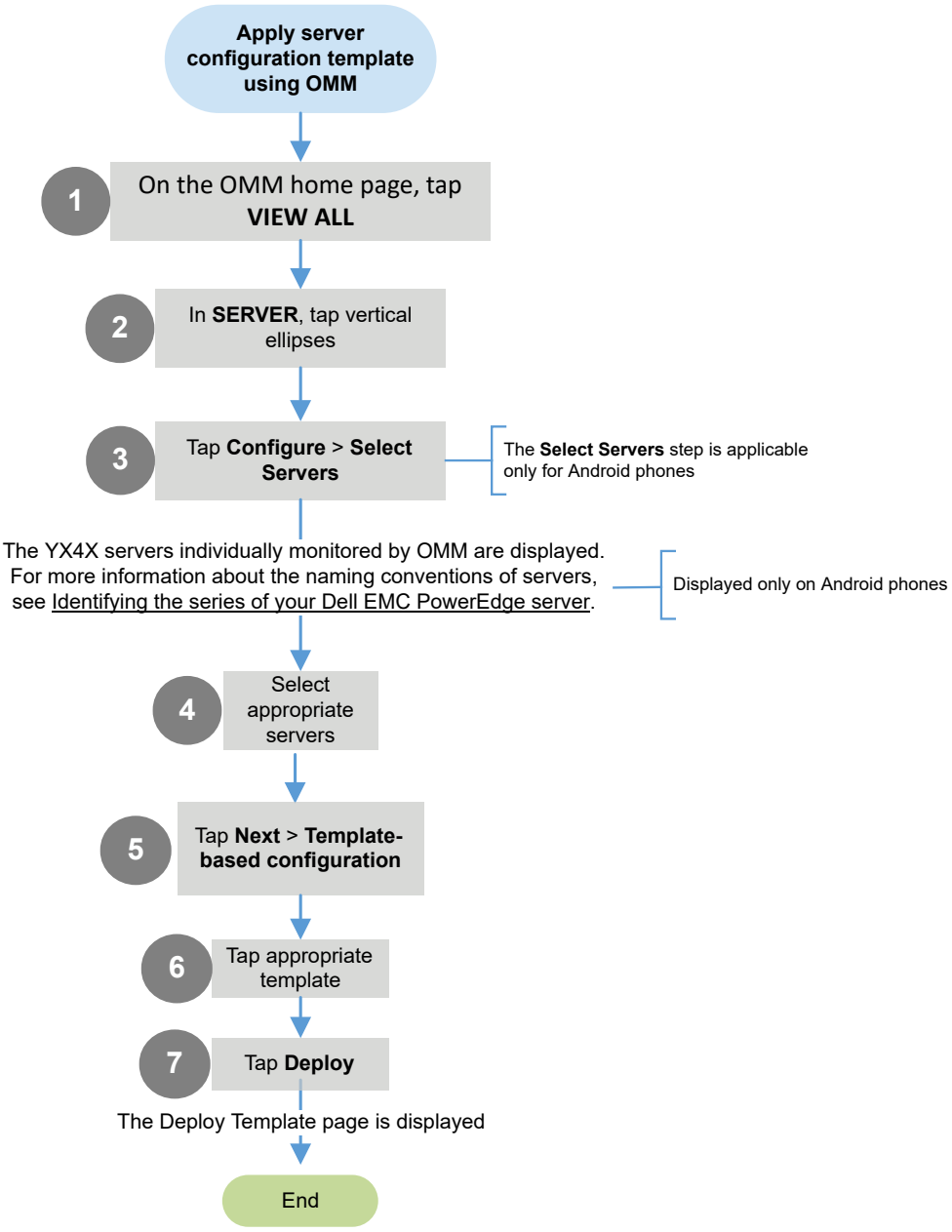
Create server configuration template by using OMM

You can create a server configuration template only for the YX4X servers. For more information about the naming conventions of servers, see Identifying the series of your Dell EMC PowerEdge servers on page 68.

1. Tap  > **Templates**.
   The **Manage Template** page is displayed.
2. Tap **Add**.
3. Enter a template name and description.
4. Expand the links to enter or select properties—IPv 6, IPv 4, NIC, BIOS, root credentials, location, and first-boot device.
5. Enter the appropriate configuration, and tap **Save**.
   The template is created and displayed on the **Manage Template** page.

Apply a server configuration template by using OMM

- Ensure that the Quick Sync 2 feature is enabled, and the access is set to read/write.
- To successfully deploy a template, ensure that you are working in the Bluetooth Low Energy (BLE) signal.


Apply server configuration template using OMM
1
On the OMM home page, tap VIEW ALL
2
In SERVER, tap vertical ellipses
3
Tap Configure > Select Servers
The Select Servers step is applicable only for Android phones
The YX4X servers individually monitored by OMM are displayed. For more information about the naming conventions of servers, see Identifying the series of your Dell EMC PowerEdge server.
Displayed only on Android phones
4
Select appropriate servers
5
Tap Next > Template-based configuration
6
Tap appropriate template
7
Tap Deploy
The Deploy Template page is displayed
End

Diagnose servers by using Quick Sync 2

Before running the diagnostics report by using Quick Sync 2, ensure that:

- The mobile phone is connected to the server. For more information about enabling the Quick Sync 2 feature on the server, tap **CONNECT** > **Server** > **Add via Quick Sync 2**.
- Storage permissions are accepted while downloading a diagnostic report.

1. View device data by using OMM on page 17.
2. Tap > **Diagnostics**.
3. To view the real-time status, tap one of the visual diagnostics options.

   NOTE: If the diagnostics report file takes a long time to download because of the size of the file, cancel the job and view the progress in Task Manager.

   NOTE: Else, the reports can be generated by using the WS-Man protocol or Quick Sync over WiFi features.

   For more assistance, email the downloaded attachment to Dell EMC technical support teams.

Run RACADM commands by using OMM

Ensure that the device is connected to an appropriate server and network.

Alternatively, the RACADM commands can be run by using the WS-Man or Quick Sync over WiFi features.

1. View device data by using OMM on page 17.
2. Tap > **Run RACADM command**.
   The RACADM Commands page is displayed.
3. Tap one of the commands displayed on the screen. For example, to view hardware inventory of a server, tap **Hardware Inventory**.

   - `Custom Command`—You can manually enter a RACADM command to perform any server operation.

   Data about the selected properties are displayed.

6

Monitor storage devices on PowerEdge servers

You can view information about the storage controllers, hard drives, virtual drives, and enclosures of a server by using OMM.

For more information about storage devices on Dell EMC PowerEdge servers, see the iDRAC User's Guide available at www.dell.com/idracmanuals.

Topics:

View storage devices on PowerEdge servers by using OMM

This feature is available:

- For servers added by using a network.
- On YX4X and later PowerEdge servers.

1. On the OMM **home** page, tap the appropriate server.
   The **server** dashboard is displayed.
2. Tap **Storage**.
   The **Storage Summary** page lists the supported storage devices and components.
   - To view information about the controllers, hard drives, virtual drives, and enclosures, tap **Controllers**, **Physical Disks**, **Virtual Disks**, and **Enclosures**.
   - To view more information about a controller, hard drives, virtual drives, or enclosures, tap **Advanced Properties**.
   - To view the filter options to filter the physical and virtual disks, tap the box in the upper pane of the page. If the filtering of storage devices does not render the required result, then ensure that iDRAC is upgraded to the latest version.
   - To locate a drive on the server, tap **Blink LED**. To use this feature, you must have appropriate user privileges.
   - To view log information about the storage devices, tap **View Logs**.

7

Manage MX7000 chassis

You can manage MX000 chassis by associating them to OMM. A Chassis is a combination of sleds, storage enclosures, cooling fans, and PSUs. You can monitor MX7000 chassis by using the AR feature.

Topics:

Add MX7000 Chassis to OMM using Quick Sync 2

Before adding an MX7000 chassis to OMM, ensure that a Quick Sync module is installed on the chassis or the chassis is accessible on the network.

NOTE: You cannot add a chassis by using the Internet connection of your mobile phone.

NOTE: To refresh the information displayed on any page in OMM, tap and swipe downwards.

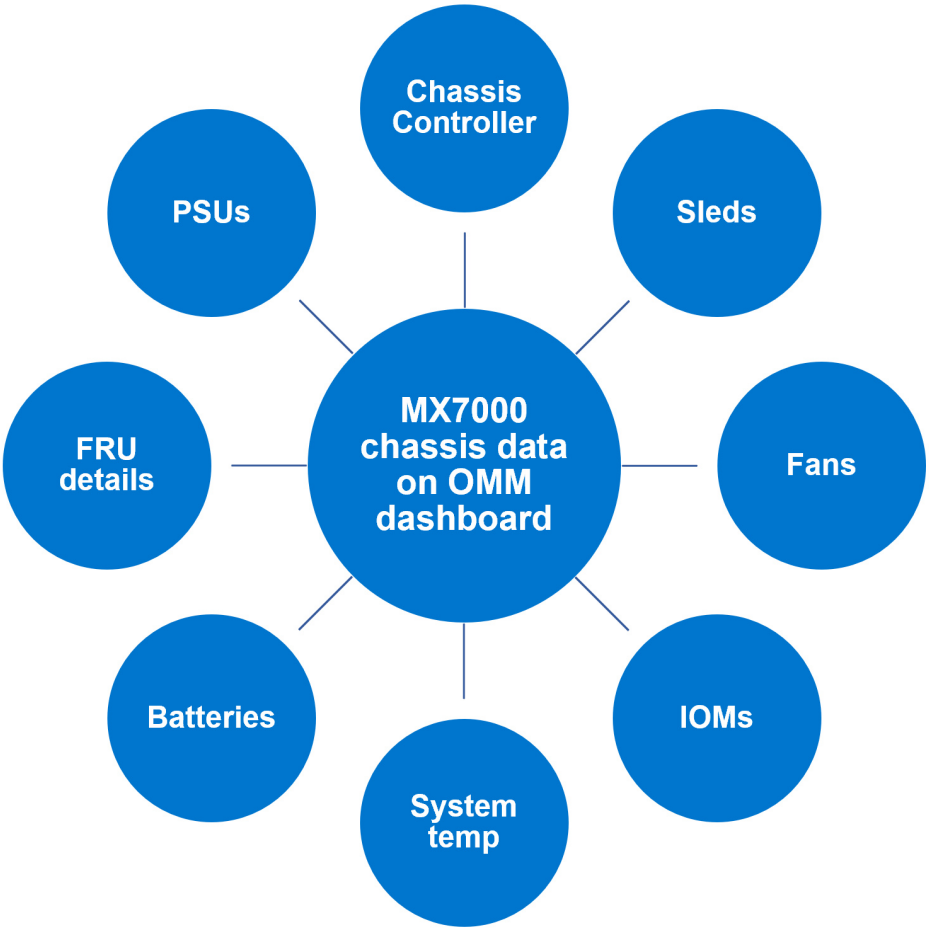
1. View the Add page on page 16.
2. Add a device by using Quick Sync 2.

Add MX7000 Chassis to OMM using a network

1. View the Add page on page 16.
2. Add a device by using a network on page 25.

View MX7000 Chassis dashboard on OMM

1. View device data by using OMM on page 17.
2. You can view the Hardware configuration data of server managed by OMM on page 30 and the following information:



To share information using an application available on your mobile, tap , and then tap **Share**.

NOTE: Data on the OMM page is updated every 15 minutes. The Last Poll section displays the number of minutes before which an OMM page was last updated.

View additional MX7000 chassis options

NOTE: To refresh the information displayed on any page in OMM, tap and swipe downwards.

1. On the chassis dashboard, tap .
2. You can view information about configuration, report, power options, support, share, view certificate, and LEDs that blink to identify devices.

   See View information about individually managed servers on OMM on page 30 and Configure a chassis group on OMM on page 40.

   - **Quick Deploy**—Configure the sleds manually, automatically, or by using templates. This feature is available only on YX4X PowerEdge servers.
   - See Configure servers manually by using OMM on page 31.
   - See Configure servers automatically by using WS-Man on OMM on page 33.
   - See Configure servers by using templates on OMM on page 33.
3. To edit or delete the chassis network connection information, see Edit or delete the network connection information by using OMM on page 20.

Configure a chassis group on OMM

All the chassis group features in OMM can be configured by using Quick Sync 2 and network. Also, you can do the following:

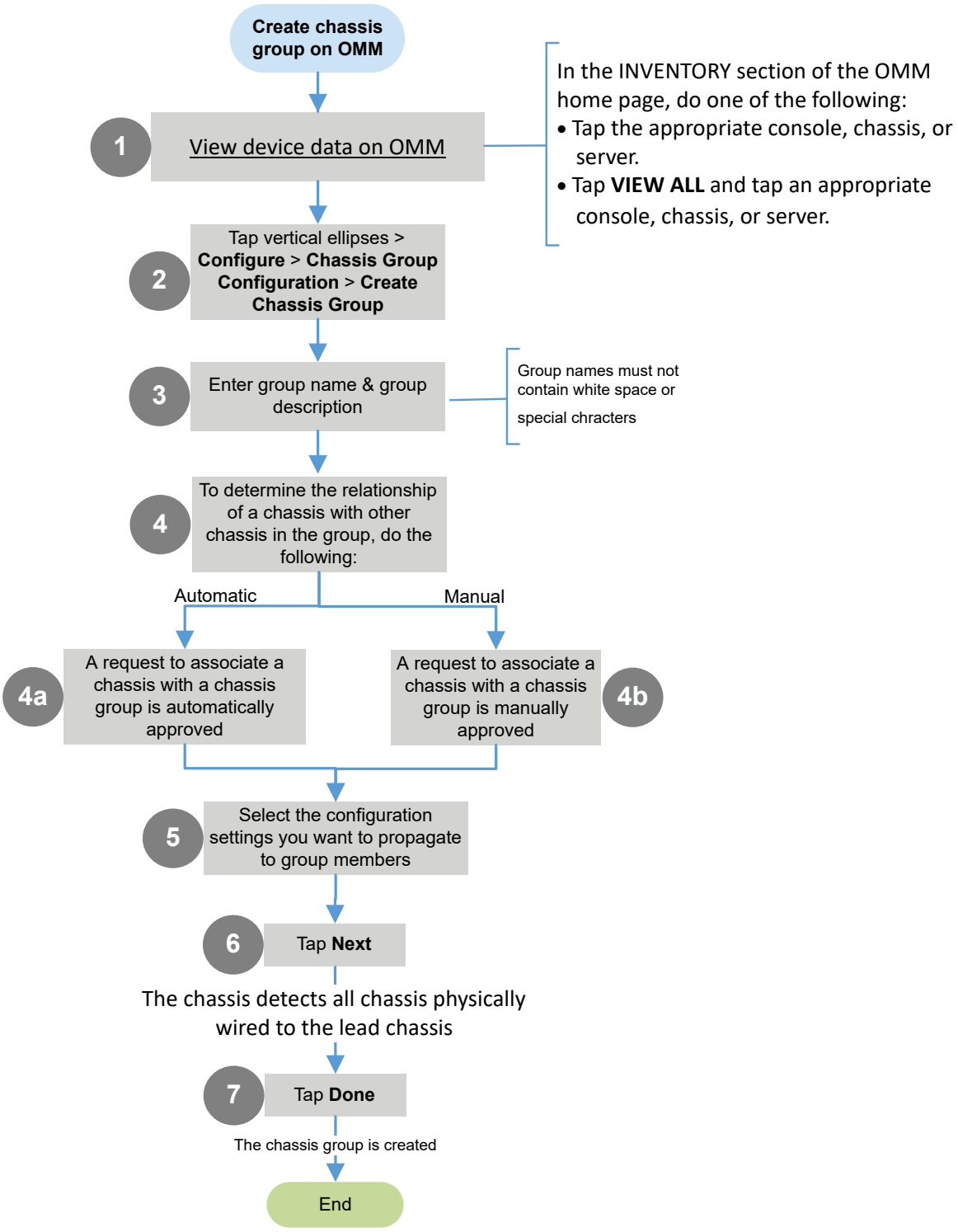
- View the health status of lead and members of a chassis group.
- A stand-alone chassis in OMM can:
  - Be associated to an existing chassis group.
  - Create a chassis group.
- Delete a chassis group that is associated to the lead chassis.
- Exit a member chassis from a chassis group.

Create a chassis group on OMM

You can create a chassis group by making a chassis as the lead chassis of a group. You can also add the settings to the group and add other stand-alone chassis to the group.

Before creating a chassis group, ensure that:

- The chassis is a stand-alone chassis.
- The defined Prerequisites for configuring a chassis group on page 42 are fulfilled.


Create chassis group on OMM
1
View device data on OMM
In the INVENTORY section of the OMM home page, do one of the following:
• Tap the appropriate console, chassis, or server.
• Tap VIEW ALL and tap an appropriate console, chassis, or server.
2
Tap vertical ellipses > Configure > Chassis Group Configuration > Create Chassis Group
3
Enter group name & group description
Group names must not contain white space or special chracters
4
To determine the relationship of a chassis with other chassis in the group, do the following:
Automatic
Manual
4a
A request to associate a chassis with a chassis group is automatically approved
A request to associate a chassis with a chassis group is manually approved
4b
5
Select the configuration settings you want to propagate to group members
6
Tap Next
The chassis detects all chassis physically wired to the lead chassis
7
Tap Done
The chassis group is created
End

Associate a chassis to a chassis group by using OMM

Before associating a chassis to a chassis group, ensure that:

- The chassis is a stand-alone chassis.
- The defined Prerequisites for configuring a chassis group on page 42 are fulfilled.

1. View device data by using OMM on page 17.
2. Tap > **Configure** > **Chassis Group Configuration** > **Join Chassis Group**.
3. Select the appropriate group and tap **Done**.
   The chassis becomes the member of the group.

Leave a chassis group using OMM

Before leaving a chassis group, ensure that:

- The chassis is a member of a group.
- The defined Prerequisites for configuring a chassis group on page 42 are fulfilled.

1. View device data by using OMM on page 17.
2. Tap > **Configure** > **Chassis Group Configuration** > **Next** > **Leave Chassis Group** > **Next**.
   A message is displayed to confirm the successful exit.
3. Tap **Done**.
   The chassis is now a stand-alone chassis.

Delete a chassis group from OMM

When you delete a chassis group, its member chassis becomes a stand-alone chassis. Before deleting a chassis group, ensure that:

- The chassis is a lead chassis.
- The defined Prerequisites for configuring a chassis group on page 42 are fulfilled.

1. View device data by using OMM on page 17.
2. Tap **Chassis**.
   The **Chassis Group** page is displayed.
3. Select the lead chassis from the list.
   The **Chassis Dashboard** of the lead chassis is displayed.
4. Tap > **Configure** > **Chassis Group Configuration** > **Delete Chassis Group**.
   The delete confirmation message is displayed.
5. Tap **Done**.
   The chassis group is deleted.

Prerequisites for configuring a chassis group

- The chassis is accessible on the network.
- The chassis is authenticated with proper user privileges.

Configure backup chassis of a group

Configure a member chassis to be the backup lead chassis of the group. All the chassis group features in OMM can be configured by using Quick Sync 2 and network.

1. View device data by using OMM on page 17.
2. Go to the lead chassis dashboard.
3. Tap > **Configure** > **Chassis group configuration** > **Assign Backup Chassis**.

4. Select the chassis from the list and tap **Done**.

Chassis group overview

You can view the group summary of a lead chassis, including the health status of the group and the member chassis of the group.

View the chassis group overview

Before viewing a chassis group information, ensure that:

- The chassis is accessible on the network.
- The chassis is a lead chassis.

The following constraints are observed while viewing the member chassis data on OMM:

- The network information (LAN, IPv 4, and IPv 6) of the chassis cannot be configured or displayed.
- The root credentials of the chassis cannot be configured.

1. View device data by using OMM on page 17.
   The Chassis Group Dashboard is displayed. You can view the health status and alerts of the members in a chassis group. For more information about the color symbols, see Colors indicating the health status of devices managed by OMM on page 67.
   - To view the devices or alerts based on the health status, tap the color symbol that indicate the status of devices or alerts.
2. Tap the **Chassis** summary.
   You can view the health status of each chassis. The color symbols to the left of each chassis indicate the health status.
3. Select the lead chassis from the list to view the group information. Select the member chassis to view the information of that chassis.

View the chassis group topology on OpenManage Enterprise-Modular application

1. View device data by using OMM on page 17.
2. Do one of the following:
   - Tap **Chassis** > **Show Topology**.
   - In the **CHASSIS** section, tap **Show Topology**.

   The OpenManage Enterprise-Modular application displays the topology of the chassis group.

   NOTE: The group topology supports troubleshooting, and the port wiring connections are dynamically traced. It may take several minutes to display the topology when there are multiple chassis, with each having multiple port connections.

8

Monitor MX7000 chassis by using Augmented Reality (AR)

To provide a touchless and robust method to manage your MX7000 chassis, OMM provides the Augmented Reality (AR) feature. By using this feature, you can manage and monitor the Dell EMC MX7000 chassis. See the Understanding Augmented Reality Monitoring in OpenManage Mobile technical white paper available at www.dell.com/openmanagemobilemanuals.

Topics:

Start Augmented Reality (AR) on OpenManage Mobile (OMM)

Before you start AR, ensure that:

- Your mobile has an Android version 7 and later.
  NOTE: AR feature is now supported on tablet devices.
- OMM has access permission to the camera, Bluetooth, and location of your mobile phone.
- The ARCore application by Google is installed from Google Play Store.

1. On the OMM **home** page, tap  .

   If the AR feature has not been used before, a red-color-filled circle is displayed on  and the Augmented Reality icon. The circle is not displayed when you have used the AR mode at least once.
2. Tap **Augmented Reality**. If the ARCore application by Google is not installed, you are prompted to install from Google Play Store.
   The **Augmented Reality** page is displayed. A video about the functioning of the AR mode is displayed.
3. Tap **Start**. If OMM does not have access permission to the camera, Bluetooth, and location of your mobile phone, you are prompted to provide access.
   The mobile phone camera is activated.

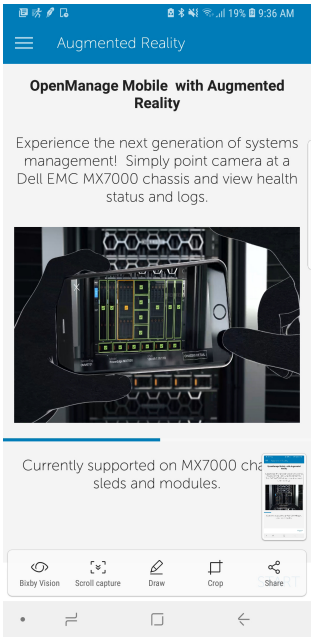


Figure 1. Start Augmented Reality on OMM

Monitor MX7000 chassis by using Augmented Reality (AR)

By using AR, you can:

- Monitor an MX7000 chassis which is identified by using the mobile phone camera.
- Connect to the chassis and view information about the chassis by using Quick Sync 2.

After a successful connection, the health status is displayed on the camera. Before monitoring an MX7000 chassis, ensure that:

- The chassis:
  - Is Quick Sync 2 compatible
  - Is clearly visible to the camera
  - Is powered on
  - Does not move
  - Has unmoved objects around it. An object larger than chassis must not move.
- If the ambient illumination is unclear, then the mobile light is powered on.
- If there are multiple chassis, only one chassis is visible to the camera. Initiate Quick Sync 2 only on that chassis.
- Sixty percent or more of the camera view is directed towards the chassis.
- The mobile phone is moving but not more than 2 feet per second.
- The mobile phone does not rotate more than 180^0 per second.

Related Links—Add a device by using Quick Sync 2 on page 28

See a micro video about AR:
Manage your PowerEdge MX7000 with Augmented Reality

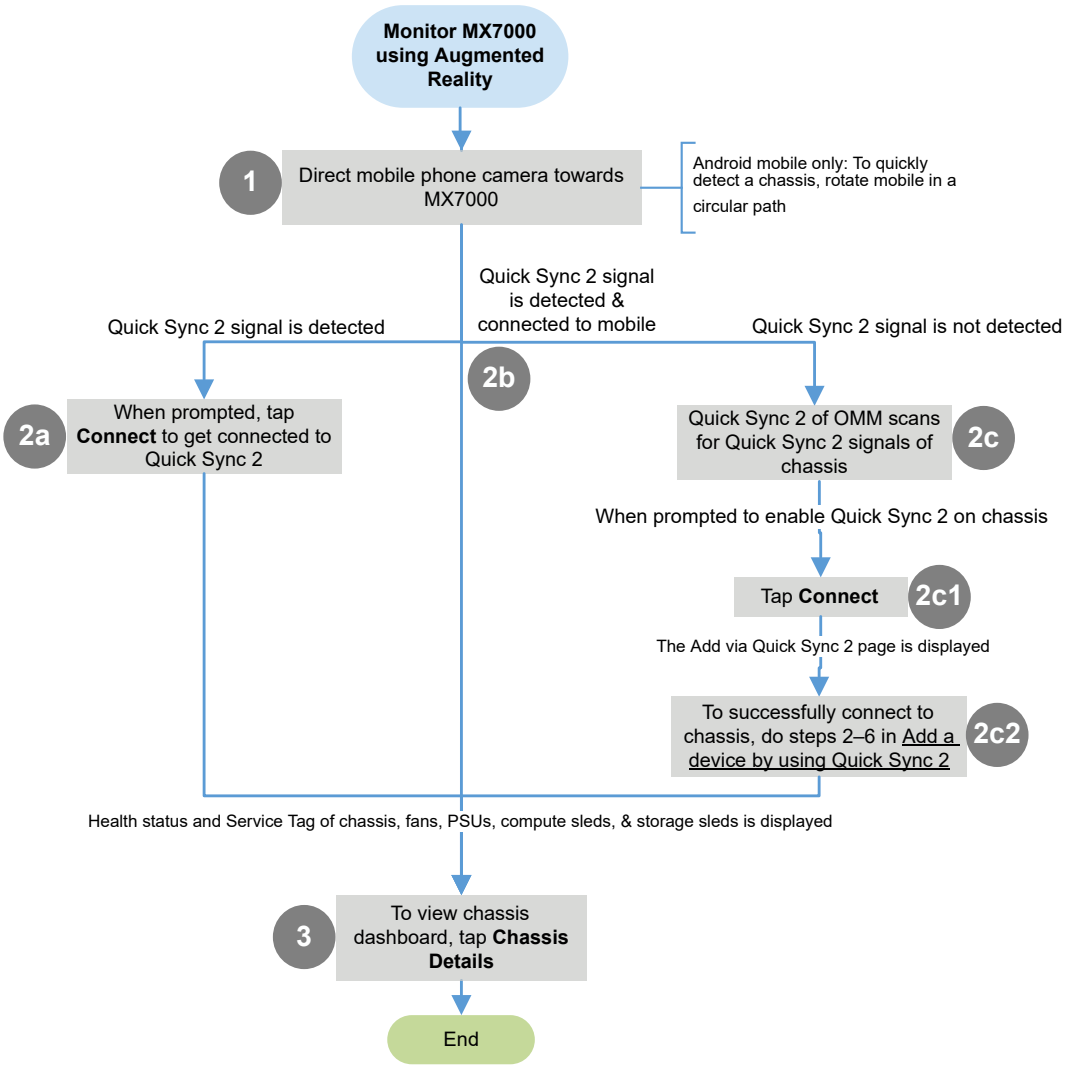

Monitor MX7000 using Augmented Reality
1
Direct mobile phone camera towards MX7000
Android mobile only: To quickly detect a chassis, rotate mobile in a circular path
Quick Sync 2 signal is detected & connected to mobile
Quick Sync 2 signal is detected
Quick Sync 2 signal is not detected
2b
2a
When prompted, tap Connect to get connected to Quick Sync 2
Quick Sync 2 of OMM scans for Quick Sync 2 signals of chassis
2c
When prompted to enable Quick Sync 2 on chassis
Tap Connect
2c1
The Add via Quick Sync 2 page is displayed
To successfully connect to chassis, do steps 2–6 in Add a device by using Quick Sync 2
2c2
Health status and Service Tag of chassis, fans, PSUs, compute sleds, & storage sleds is displayed
3
To view chassis dashboard, tap Chassis Details
End

Figure 2. Monitor MX7000 chassis by using AR

View the front-end of MX7000 chassis in AR mode

1. View MX7000 chassis information in AR mode on page 49.

   See the micro video here:
   Manage your PowerEdge MX7000 with Augmented Reality
2. To view information about the components in the front end of an MX7000 chassis, tap Sleds, Fans, or PSUs. The information is displayed in a new window that opens next to the main window of the AR mode.

Sleds	• Name, health status, slot name, power state, model, and Service Tag
Fans	• Health status, slot name, PWM, and speed
PSUs	• Health status, slot name, power state, capacity, and input voltage

3. View MX7000 chassis log information in AR mode on page 49.

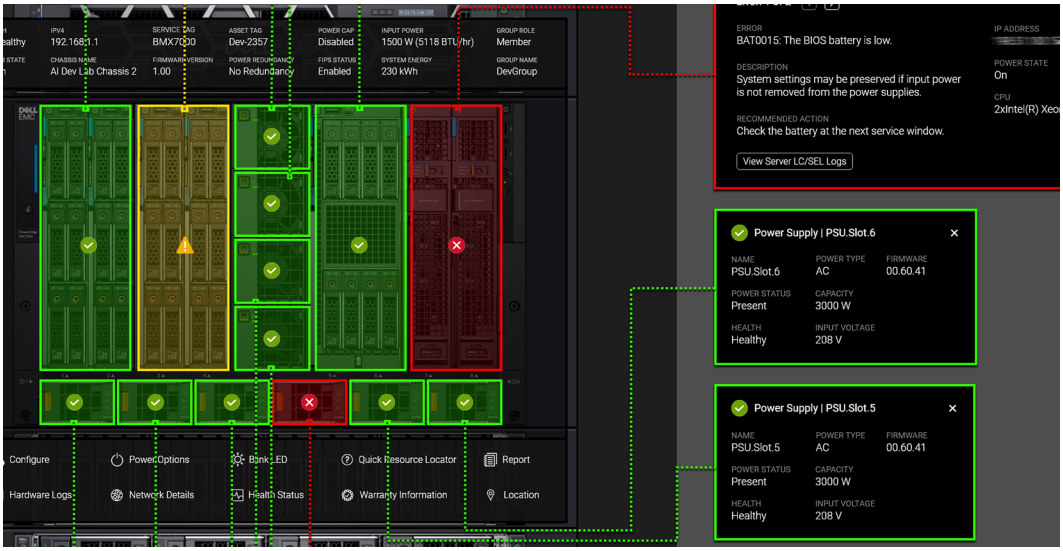


Figure 3. View the log information of the front-end chassis components

View the back-end of MX7000 chassis in AR mode

1. View MX7000 chassis information in AR mode on page 49.
2. Tap  in the upper right corner.
   The back-end of the chassis is displayed.
3. To view information about the components in the back-end of a chassis, tap IOMS, Fans, or Management Modules:

IOMs	• Name, type, health status, power state, model, Service Tag, fabric type, and firmware version
Fans	• Name, type, health status, PWM, and speed
Management Modules	• Name, type, health status, MSM state, and firmware version

4. View MX7000 chassis log information in AR mode on page 49.

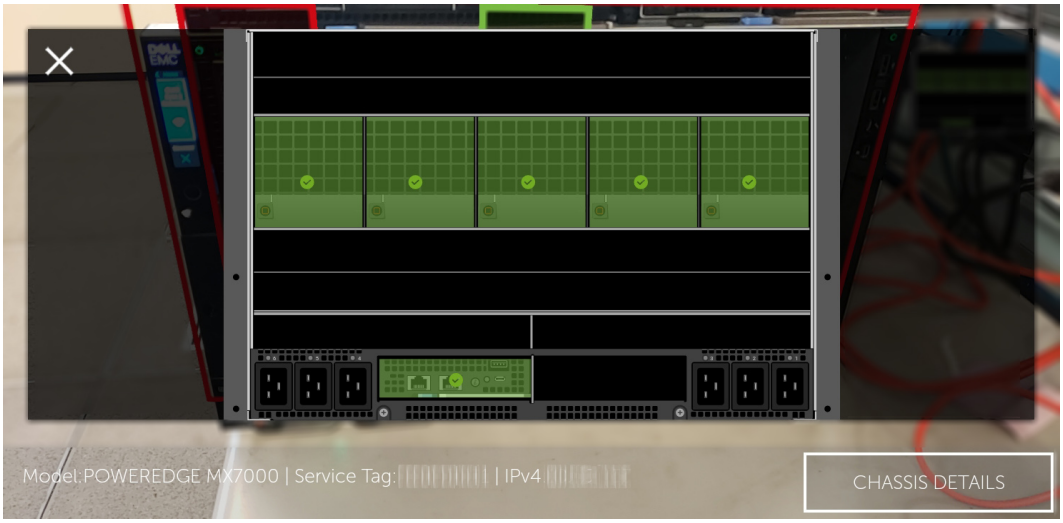


Figure 4. Back end view of MX 7000 chassis

View MX7000 chassis information in AR mode

You can view the health status and log information of each component in the chassis.

Before viewing the front- or back-end of a chassis, ensure that:

- OpenManage Mobile is connected to the chassis in the AR mode. For more information, see Monitor MX7000 chassis by using Augmented Reality (AR) on page 45.
- The chassis and mobile phone are connected by using Quick Sync 2.

See the micro video here:
Manage your PowerEdge MX7000 with Augmented Reality

NOTE: See the Understanding Quick Sync 2 for Dell EMC PowerEdge 14th Gen Servers and MX7000 Chassis and Understanding Augmented Reality Monitoring in OpenManage Mobile technical white paper available at www.dell.com/openmanagemobilemanuals.

View MX7000 chassis log information in AR mode

You can:

- Tap **Hardware Logs** and **Power Options** of the components.
- View the recommended action for the errors that occur in the back chassis components.

Close the AR mode

Tap the exit button in the upper left corner. You can also use **<** button on your mobile.

The OpenManage Mobile **home** page is displayed.

9

Manage SupportAssist Enterprise (SAE) by using OMM

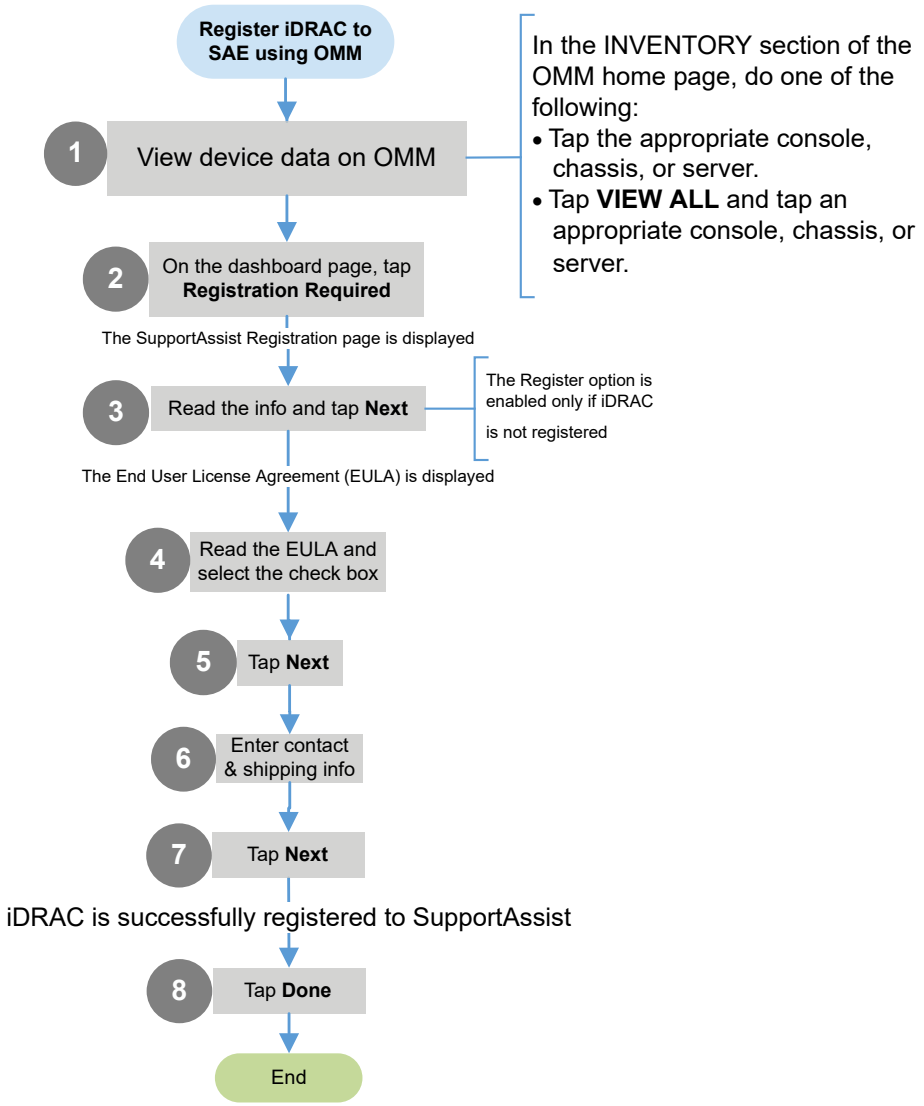
SupportAssist enables you to identify hardware issues and upload this data to Dell EMC technical support teams. The support teams manually create a case for the uploaded SupportAssist data, and then contacts you, if necessary.

Topics:

Register iDRAC to SupportAssist using OMM

Ensure that the:

- Setting for storing the registration information is enabled. For more information, see Store iDRAC-SupportAssist data on OMM on page 52.
- iDRAC Service Module (iSM) is installed on the server for a successful registration.


Register iDRAC to SAE using OMM
1
View device data on OMM
In the INVENTORY section of the OMM home page, do one of the following:
• Tap the appropriate console, chassis, or server.
• Tap VIEW ALL and tap an appropriate console, chassis, or server.
2
On the dashboard page, tap Registration Required
The SupportAssist Registration page is displayed
3
Read the info and tap Next
The Register option is enabled only if iDRAC is not registered
The End User License Agreement (EULA) is displayed
4
Read the EULA and select the check box
5
Tap Next
6
Enter contact & shipping info
7
Tap Next
iDRAC is successfully registered to SupportAssist
8
Tap Done
End

Related links: View device data by using OMM on page 17

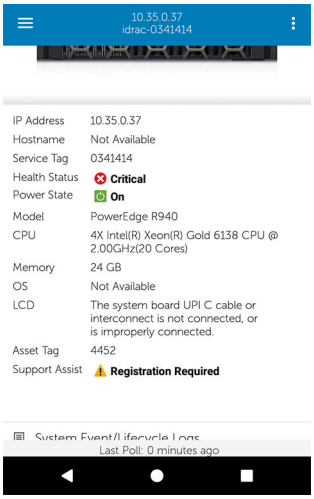


Figure 5. View—registration required—option on server dashboard

Store iDRAC-SupportAssist data on OMM

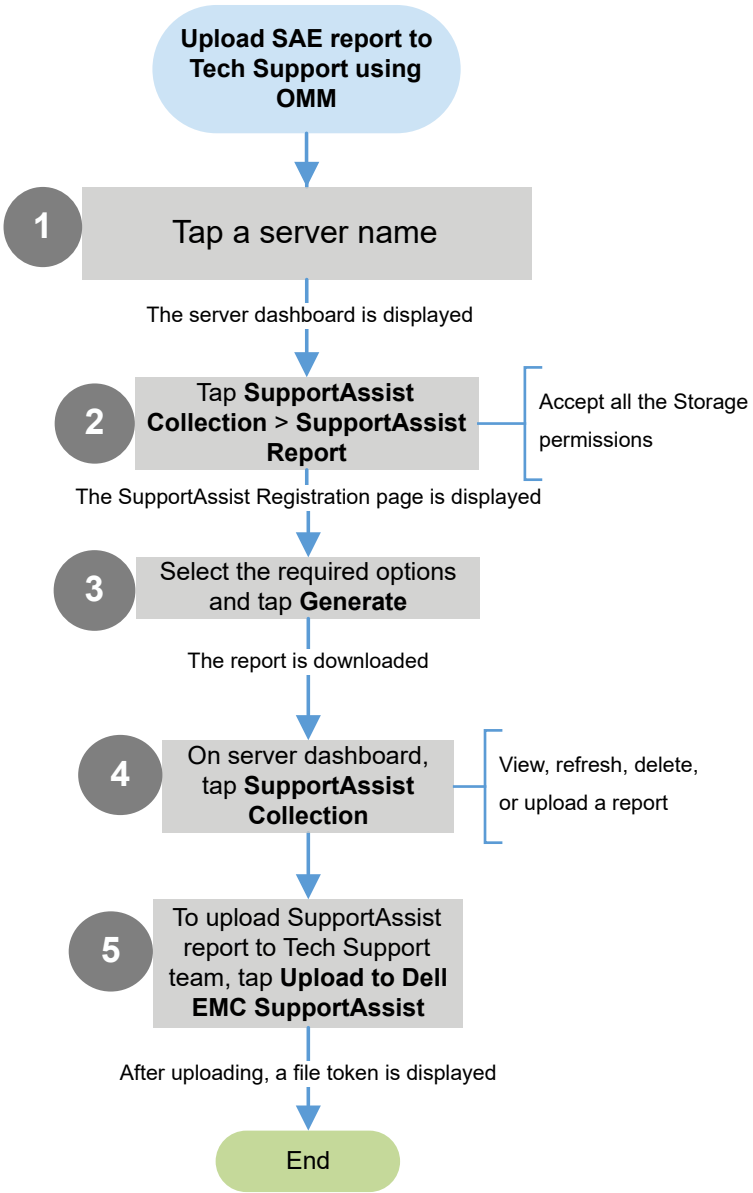
By default, this feature is enabled on OMM. The registration information is stored in OMM after a server is registered to SupportAssist.

Ensure that the chassis is accessible over the network.

1. Tap > **Settings**.
2. Enable or disable **Save Contact Registration Data**.

Upload SupportAssist report to Dell EMC technical support by using OMM

Ensure that the iDRAC is registered with SupportAssist.


Upload SAE report to Tech Support using OMM
1
Tap a server name
The server dashboard is displayed
2
Tap SupportAssist Collection > SupportAssist Report
Accept all the Storage permissions
The SupportAssist Registration page is displayed
3
Select the required options and tap Generate
The report is downloaded
4
On server dashboard, tap SupportAssist Collection
View, refresh, delete, or upload a report
5
To upload SupportAssist report to Tech Support team, tap Upload to Dell EMC SupportAssist
After uploading, a file token is displayed
End

10

Collect server inventory using OMM

The OMM inventory collection feature enables you to scan the QR codes to save the Service Tag and MAC address of devices. This inventory information can be shared to Dell License Manager to batch-update factory unique passwords of YX4X and later PowerEdge servers.

Topics:

Add servers to the inventory page by using OMM

- Ensure that you have pulled out the tag with the QR code information available on the server.
- This feature is applicable only for YX4X and later PowerEdge servers.
- You can import the servers to OpenManage Enterprise version 3.4 and later.

1. Tap  > **Inventory Tool**.
2. Tap **Start Adding** or  .
   The **Add Servers** page is displayed.
3. Add servers by using any of the following methods:
   - Tap **Scan QR code(s) (batch support)** > **NEXT**.

     You are prompted to enable access to the mobile camera.

     - Tap **Ok**. Scan the QR code available on the lower side of the pull-out tag.
   - Tap **Select servers you already have in OMM** > **NEXT**.
     - Select the servers and tap **IMPORT**.

   The server information is displayed on the **Inventory Tools** page.

Share the server inventory information to Dell License Manager by using OMM

Ensure that the device is connected to the Internet.

1. On the **Inventory Tool** page, tap **Export**.
2. Tap **Export file for DLM** > **EXPORT**.
3. Enter an encryption password, and tap **Submit**. You can share the file using the applications available on your phone.

11

Manage alert notifications by using OMM

Push-notifications notifies you when one of the subscribed OpenManage Consoles receives alerts from a monitored device. The notification is displayed in the status bar of your mobile phone—similar to the notifications that are displayed for messages, and downloads. OMM enables you to configure the type of push notification you want to receive.

Topics:

Configure alert notifications settings

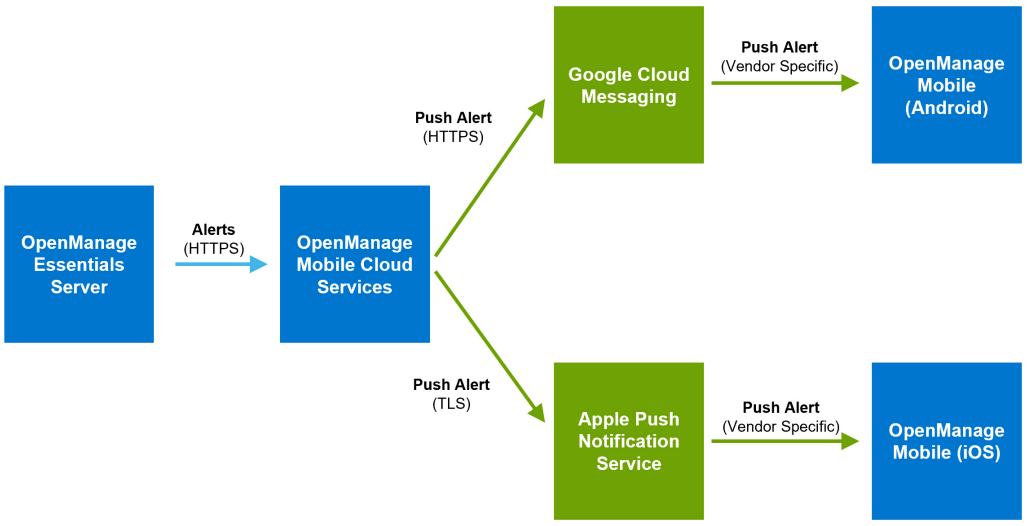
1. On the OpenManage Mobile **home** page, tap .
2. Tap **Settings** > **Notification Settings**.
   The **Notification Settings** page is displayed.
3. Select one or both of the following:
   - **Play Sound**—Enable your mobile phone to play a sound when an alert is received.
   - **Vibrate**—Enable your mobile phone to play a sound when an alert is received.

View alerts using push notifications

1. Tap the alert notification.
   The dashboard of OpenManage Consoles displays the newly received alert.
2. To view the alerts associated with a push notification, tap **New alerts**.

Alert Push notification security

Alerts that are sent by using push notifications pass through several systems before reaching a mobile phone.



- OpenManage Essentials transmit alerts to Dell OpenManage Mobile Cloud Services (OMCS) using HTTPS as identified by using a PKI certificate.
- Alerts are sent by using HTTPS to Google Cloud Messaging (GCM), or by using a binary protocol over TLS to the Apple Push Notification Service (APNS). Google and Apple servers are also identified by a certificate.
- Android and Apple devices connect to Google and Apple servers respectively over a secure channel and retrieve the alert push notifications.

Only limited information such as the number of new alerts is available outside the OMM application. Potentially-sensitive information such as alert message contents are not shown on the device notification bar, app icons, or other mobile display areas. Each mobile device supplies an application- and device-specific registration token to each OpenManage Essentials server when it subscribes for alerts. The token is sent to and used by OMCS to identify the device to GCM and APNS. Without that token, no other service can send push notifications to that OMM instance.

Apple and Google use certificates and API keys to identify OMCS as being associated with the OMM app. Similarly, OMCS identifies OpenManage Essentials instances by using API key. OMM tracks the OpenManage Essentials instances that it is subscribed to, so that it can discard alerts from subscriptions that have been removed. This helps prevent spurious or unwanted notifications. Dell EMC does not persist the contents of alerts within OMCS.

12

Supporting information about OMM

Describes information about viewing the OMM log, version, End User License Agreement (EULA), and manuals and documentation.

Topics:

View the OMM application log

1. On the **home** page, tap .
2. Tap **App Log**.
   The application log displays the following operations that are performed on the OMM pertaining to the OpenManage Consoles, chassis, or servers:
   - Add or remove devices.
   - Acknowledge, unacknowledge, share, or delete alerts.
   - Perform power-control operations.

View technical documentation, EULA, and version of OMM

- On the **home** page, tap > **About**.
  - The OpenManage Mobile product information and version is displayed.
- To view:
  - Manuals and documentation, tap **Manuals and Documentation**.
  - End User License Agreement, tap **View EULA**.
  - Open-source license, tap **View OpenSource Licenses**.

Share feedback about OMM

1. On the OMM **home** page, tap > **Send Feedback**.
   The default email application is displayed.
2. Enter your feedback and send the email.
   You can email your feedback also to om_mobile_feedback@dell.com.

13

Troubleshoot OMM issues

Topics:

Unable to view BLE-enabled servers on Android 7.0 and 7.1.1 mobile phones

Sometimes, on devices running Android version 7.0 or later, Quick Sync 2 does not detect the Bluetooth Low Energy (BLE) enabled servers.

Workaround:

- Restart BLE. Close and reopen the application.
- Restart the device, and retry the operation.

Unable to add individually managed servers to OMM by using iDRAC Quick Sync Read

Workarounds:

- Update the iDRAC firmware. For more information about updating the iDRAC firmware, see the *iDRAC User's Guide.*
- Update OMM to the latest available version.
- The Near-Field Communication (NFC) chip in the mobile phone must be in contact with the iDRAC Quick Sync activation switch. See the documentation of your mobile phone to find the location of the NFC chip.
- Remove the protective casing from the mobile phone, if any.

Unable to add OpenManage Consoles or individually managed servers to OpenManage Mobile (OMM)

The OpenManage Consoles (OpenManage Essentials and OpenManage Enterprise) or individually managed servers cannot be added to current OMM version. As applicable, do the following as workaround methods, and then retry the operation:

- Verify network configuration on page 59
- Verify credentials on page 59

- Verify OpenManage Essentials version on page 59
- Verify iDRAC version on page 59

Verify network configuration

To add OpenManage Consoles to OMM, the former must not be blocked by any firewall or other security modes. Ensure that VPN and wireless network is connected, enabled, and configured. Verify if you can connect to the OpenManage Consoles host from your device by using a web browser.

NOTE: Ensure to accurately enter the port number of the consoles in OMM when it is non-default.

NOTE: When adding individually managed servers, verify if you can connect to iDRAC host from your phone using a web browser. Ensure the port ID number in the iDRAC UI and the OMM application on the mobile phone are the same.

Verify credentials

To log in to the remote system, ensure that the username and password are correct. If you use domain credentials, ensure that the domain name is entered in the correct format that is supported by your directory server (such as companyname.com).

Verify OpenManage Essentials version

Only OpenManage Essentials version 2.5 and later are supported.

Verify iDRAC version

Only iDRAC7 and later versions, with Express, Enterprise, or datacenter licenses are supported (available on the YX2X and later PowerEdge servers).

Data from OpenManage Essentials is displayed with a latency of several minutes by OMM

Workaround:

Internet connection on your mobile phone may be slow. Use OMM on WiFi or 3G or later network. Operations such as viewing event logs through OpenManage Essentials require the latter to retrieve data from the managed nodes, and sometimes there is a delay of several minutes in retrieving data.

Updated information is not displayed in OMM

Information that is displayed in OMM does not match the information that is displayed in OpenManage Essentials or iDRAC.

Workaround

OpenManage Mobile uses a data cache to improve performance. Touch and swipe downwards on any page to view the updated data.

OMSA or OpenManage Essentials-managed device data displayed on OMM is not up to date

- The operating system name or hostname is not displayed.

Workaround: To receive the hostname or operating system name, install OpenManage Server Administrator (OMSA) on the managed node.

- Incomplete information is displayed for devices managed by OpenManage Essentials.

  Workaround: Ensure that data is correctly inventoried in OpenManage Essentials. For more information, see the *OpenManage Essentials User's Guide* available on the support site.

Unable to register OpenManage Essentials for push notifications

Workaround: Do the following:

1. Tap  > **Settings** > **Notifications**
2. On OMM, ensure **Allow Notifications** is enabled.

Delay in receiving push notifications

Either alert notification is not received, or there is a delay of several hours in receiving alerts. Workaround:

- Verify OpenManage Essentials operation—Ensure that OpenManage Essential is receiving alerts, and it is successfully forwarding alerts to the Dell Message Forwarding Service. For more information about transmitting alerts from OpenManage Essentials to the Dell Message Forwarding Service, see *OpenManage Essentials User's Guide*. During normal operation, it takes up to two minutes for the alerts to transmit from OpenManage Essentials to Dell Message Forwarding Service.
- Understand provider limitations—The Dell Message Forwarding Service uses provider notifications services including Google Cloud Messaging. Google imposes a notification limitation on a per-device and per-application basis. If your alert notifications are more than 100 a day, select specific filters to reduce the number of alerts that are transmitted to your mobile phone.
- Verify phone network connectivity—Push-notifications require an Internet connection on your phone or a wireless connection (that may not be available in remote locations and places with poor signal). If your mobile phone is inactive, carriers, Internet service providers, and networking equipment may end the connection to Google servers. Notifications cannot be received until the connection is restored. If the communication is unstable with specific devices because it is not registered, a message is displayed in OpenManage Essentials.

Workaround:

If OMM is backed up and restored on to your mobile phone, the GCM registration token must be refreshed. Go to the **Settings** page and tap **Refresh** to reinstall the GCM token. To do this, you must have Internet connection.

NOTE: If you refresh the GCM token, edit the connections of all the OpenManage Essentials added and resubscribe to the alert filters.

Unable to log in to OpenManage Mobile

You cannot log in when:

- The **Don't keep Activities** option is selected on the **Settings > Developer options** page.

  Workaround: Ensure that the **Don't keep Activities** option is not selected.

- You forget your OMM password.

  Workaround:

  - To retrieve your OMM password, tap **Forgot Password**. Your password hint-phrase is displayed.
  - If you are unable to retrieve your OMM password using the password hint, delete the OMM data, and then create a password. To delete the OMM data, go to **Settings > Apps > OMM**, and then tap **Clear data**.

NOTE: If application data is deleted or application is reinstalled, add the OpenManage Essentials and server instances again to OMM.

Unable to retrieve iDRAC data

If you refresh the **iDRAC Details** page multiple times to retrieve data, OMM displays a message that the connection was unsuccessful.

Workaround:

Refresh the **iDRAC Details** page after one minute. If incorrect credentials are entered while adding an iDRAC or while performing power operations on an iDRAC, the iDRAC might disable all incoming requests and appear disabled for some time. For more information about this behavior, see the *iDRAC User's Guide*. iDRAC will be enabled after some time. Wait until iDRAC is enabled, and then retry the operation by using the correct credentials.

Unable to start RDP session because the VNC connection failed on OMM

When you try to start an RDP session for an iDRAC, and if:

- The VNC RDP session is already running then the following message is displayed: `VNC connection failed`.
- Another active bVNC session is running on a different mobile phone for the same iDRAC because iDRAC VNC supports only one connection at a time. You cannot connect to the same iDRAC by using any instance of a VNC client, whether from the same mobile phone or a different device.

Workaround:

Reset iDRAC to start the network connection. For more information about accessing RDP session on OMM, see the *Accessing Remote Desktop using VNC on Dell PowerEdge Servers and MX 7000 blades* technical white paper available at www.dell.com/openmanagemobilemanuals.

Password inventory file is unavailable in the received email sent from OMM

Sometimes, when a password inventory file is shared from OMM using Gmail, the file may not be available in the received email in certain mobile phones.

Workarounds:

- Save the email as a draft and send again.
- You can use another email application. For example, use Outlook to send the file.

Known issues in OpenManage Mobile

- If the server WiFi frequency is set to 5.0 GHz, then OMM is unable to wirelessly connect using Quick Sync 2. iDRAC supports only 2.4 GHz frequency band for direct WiFi.
- OpenManage Mobile does not provide the appropriate output logs for the following RACADM commands:
  - `storage get controllers -o`
  - `storage get enclosures -o`
  - `raid get controller`
  - `raid get pdisks -o`
  - `lclog`

  The following message is displayed: `Command Successful`
- To receive alert notifications in OMM on your Android phone, you must have a registered Google account.
- If you are not connected to a network, then tap the **Network** button for a server added using Quick Sync. You are prompted to repeatedly check the certificate.
- Unsupported device: Sony Xperia Tablet Z (SGP321 TABLET Z)
- Issue: User is prompted to enter the wireless password for saved networks.

Workaround: To connect to the saved network, try one of the following steps:

  - Close and open the **Settings** page of your mobile phone. Try to connect to the wireless network.
  - Restart the WiFi on your device.
  - Close the password prompt and retry the connection until it gets connected.

- Issue: Unable to power on a server if the KG key value in the RAC GUI page is set to a nondefault value.

  For iDRAC shown in OpenManage Consoles, OMM does not perform the operation with nondefault values.

- If the **login** page is displayed again after you exit OMM, tap the Home button to minimize the application.
- If you have more than 100 devices in the **All Devices** group, the devices are sorted by health only on the first page.
- If the SSL encryption is changed, OMM prompts you to set the VNC password.
- Issue: The following message is displayed while performing manual configuration: `Quick Sync lost`

  This is because of an Android limitation. You see this message when the Bluetooth connection is ended. It connects automatically, and this does not interrupt the configuration process.

- Issue: When you delete a server that is added by using Quick Sync 2 and try to scan again on the same server, it is not displayed on the **Scan** page.

  Workaround: Exit the OpenManage Mobile application and restart it to view the deleted server on the Scan page.

- If you are connecting to a secured network, you are prompted to check the certificate every time.
- If the phone is restarted or is inactive for long periods, OMM offline data cache is lost.
- While powering off the server, ensure that Titan Quick Sync is active. If the latter is inactive, all the features are disabled. To enable, you must enable the Quick Sync button on the server.
- If your mobile phone has limited memory space, OMM offline cache can be lost.
- If OpenManage Essentials is reinstalled by retaining the same database as an earlier OpenManage Essentials installation, then Push Notifications are not received.
- Unable to acknowledge or delete an alert received by a user who is a member of the `OMEssentialsPowerUsers` group.
- Last successful remote desktop session is seen when multiple VNC sessions are running simultaneously because bVNC is an open-source component and its behavior is outside the scope and control of OMM. OMM has limited control over launch interactions and subsequent activity.
- Issue: OMM is unable to add servers using Quick Sync (NFC) in One Plus 5.

  This is because of a mobile phone limitation.

  Workaround: You can use other Android phones or add the servers by using network in One Plus 5.

- Issue: Unable to start iDRAC GUI for a server added in OMM by using Quick Sync 2 WiFi.

  Unable to open the page. The following message is displayed: `Webpage not available`. This issue can occur in any mobile phone running on early versions of Android 9.0, and can impact the functioning of RACADM, and SupportAssist file generation.

  Workaround: Update to Android 9 and try again.

14

Related documents and resources

Other documents you may need

You can find the following documents on the Dell EMC Support website at www.dell.com/OpenManageManuals:

- Dell EMC OpenManage Essentials version 2.5 User's Guide
- Integrated Dell Remote Access Controller 9 User's Guide
- Dell EMC OpenManage Enterprise Version 3.3.1 User's Guide
- Dell EMC PowerEdge MX7000 Enclosure Installation and Service Manual

Topics:

Contacting Dell

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.

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:

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.

Accessing documents from the Dell EMC support site

You can access the required documents in one of the following ways:

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

- **Mainframe**
- **Operating Systems**
- **Public Sector Solutions**
- **Serviceability Tools**
- **Support**
- **Utilities**
- **Virtualization Solutions**

4. To view a document, click the required product and then click the required version.

Using search engines:

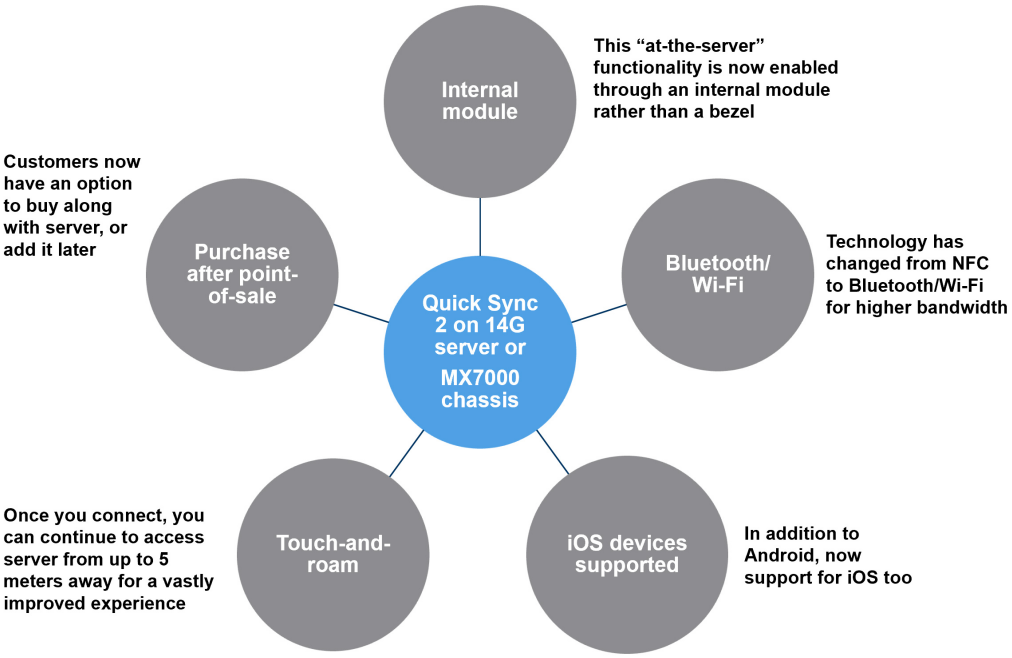
- Type the name and version of the document in the search box.

A

iDRAC Quick Sync Read feature in PowerEdge servers

The iDRAC Quick Sync Read feature enables a mobile phone to act as a proximity reader. It reads data from a server when the phone is in contact with the iDRAC Quick Sync bezel. See the *Understanding Quick Sync 2 for Dell EMC PowerEdge 14th Gen Servers and MX7000 Chassis* technical white paper available at www.dell.com/openmanagemobilemanuals.

- It is recommended to upgrade your iDRAC firmware to the latest version. For more information about upgrading the iDRAC firmware, see the *iDRAC User's Guide* available on the support site.
- This feature is applicable only for the YX3X PowerEdge servers that have an iDRAC Quick Sync bezel. For more information about the naming conventions of servers, see Identifying the series of your Dell EMC PowerEdge servers on page 68.
- Reading iDRAC information using Quick Sync is not password-protected. Making configuration changes using iDRAC Quick Sync requires iDRAC credentials.



Topics:

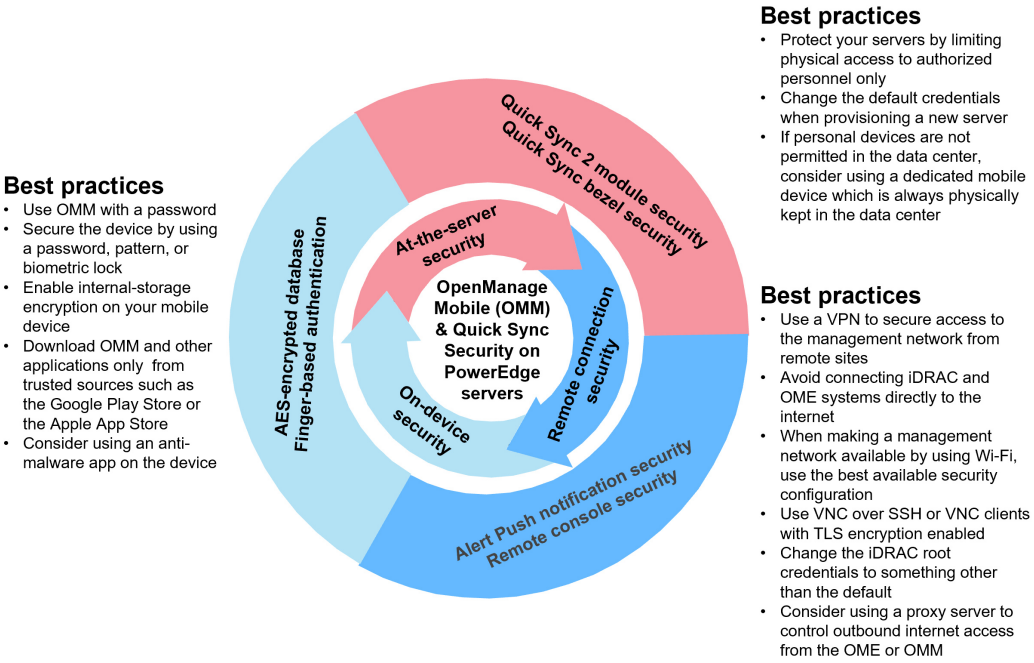
iDRAC Quick Sync 2 in PowerEdge servers and MX7000

With Dell OMM running on an Android or iOS mobile phones, you can access a server directly or through OpenManage Essentials or OpenManage Enterprise console. It enables you to review the server information and inventory and get automatic notifications on mobile phone from an OpenManage Essentials or OpenManage Enterprise console. Assign IP address and modify iDRAC password, configure key BIOS attributes, and take remediation actions as needed. You can also power-cycle a server, access system console, or access iDRAC GUI.

For more information about Quick Sync on PowerEdge servers, see the *iDRAC User's Guide* and *Installation and Service Manual* of your PowerEdge server available at www.dell.com/idrac9manuals.

Quick Sync 2 uses the integrated wireless capabilities of Quick Sync 2 equipped PowerEdge servers to directly manage those servers. Quick Sync 2 uses encrypted Bluetooth Low Energy (BLE) and dedicated WiFi connections. Quick Sync 2 is activated on the server using the connection button.

An infrastructure network uses WiFi base station or VPN to communicate with the iDRAC IP-based management network connected to the wired Ethernet port of the iDRAC. The connection uses the WS-Man protocol.



RACADM commands supported by OMM

NOTE: Only users with iDRAC configure privileges can modify the settings.

RACADM Commands enables you to run predefined commands. The generic GET and SET sub commands are used to configure and retrieve the objects. For a list of all the RACADM command supported by iDRAC, see the *RACADM CLI Reference Guide* available on the support site. The available RACADM commands are as follows:

- `System Information`
- `Hardware Inventory`
- `License Information`
- `Software Inventory`
- `Job Information`
- `Current NIC config`
- `Current NIC Statistics`
- `LC Log`

- Custom Commands

Autoconfiguration using XML configuration file

You can use the XML configuration file in OpenManage Mobile. The XML file can be accessed from the shared network folder. The XML files are configured uniquely using the DHCP server. The available DHCP Provisioning options are:

- Enable once
- Enable once after reset
- Enable always

NOTE: This option is available only for servers that have iDRAC Enterprise or Datacenter licenses.

Servers diagnostics by using Quick Sync 2

By using OpenManage Mobile as an administrator, you can:

- Perform at-the-box troubleshooting using Quick Sync 2.
- Download Tech Support Reports (TSR), screenshots, and crash screen videos to diagnose and identify the point of failure.

These actions are enabled on the PowerEdge servers and accessed remotely by using WS-Man.

Colors indicating the health status of devices managed by OMM

- —Indicates the number of devices or alerts that are in critical status.
- —Indicates the number of devices or alerts that are in warning status.
- —Indicates the number of devices or alerts that are in healthy status.
- —Indicates the number of devices or alerts that are unknown.
- —Indicates the available information about the devices or alerts.

Alert Push notification security

See Alert Push notification security on page 55.

View inventory information of a device

You can view one or more of the following device inventory information of a server (iDRAC connection), an OpenManage Essentials, or an OpenManage Enterprise—managed device.

- IP address—When individually added, indicates the IP address of servers that is used to connect to iDRAC. If this device is discovered through the OpenManage Consoles, there could be multiple IP addresses that are associated with the device.
- Operating System—This may require OpenManage Server Administrator (OMSA) to be installed on the system.

Identifying the series of your Dell EMC PowerEdge servers

The PowerEdge series of servers from Dell EMC are divided into different categories based on their configuration. They are referred as YX2X, YX3X, YX4X, YX4XX, or YX5XX series of servers. The structure of the naming convention is described below:

The letter Y denotes the character in the server model number. The character denotes the form factor of the server. The form factors are listed below:

- C- Cloud
- F- Flexible
- M or MX- Modular
- R- Rack
- T- Tower

The letter X denotes the numbers in the server model number. The number denotes multiple characteristics about the server. They are listed as follows:.

- The first digit (X) denotes the value stream or class of the server.
  - 1-5—iDRAC basic
  - 6-9—iDRAC Express
- The second digit denotes the series of the server. It is retained in the server naming convention and does not replace the letter X.
  - 0—series 10
  - 1—series 11
  - 2—series 12
  - 3—series 13
  - 4—series 14
  - 5—series 15
- The last digit (X) always denotes the make of the processor as described below:
  - 0-Intel
  - 5-AMD

NOTE: For servers that use an AMD processor, the model number is made up of four digits instead of three. The third digit (X) denotes the number of processor sockets that the series of server supports.

- 1–one socket server
- 2–two socket server

Table 1. PowerEdge servers naming convention and examples

YX3X servers	YX4X systems	YX4XX systems	YX5XX
PowerEdge M630	PowerEdge M640	PowerEdge R6415	PowerEdge R6515
PowerEdge M830	PowerEdge R440	PowerEdge R7415	PowerEdge R7515
PowerEdge T130	PowerEdge R540	PowerEdge R7425	PowerEdge R6525