Technical White Paper

# Understanding OpenManage Mobile (OMM) and Quick Sync Security (PowerEdge 14th Gen servers and MX Chassis)


## Abstract

This technical white paper helps you understand mobile management security features and optimize your environment for maximum security on Dell EMC PowerEdge servers.



October 2019

# Revisions

| Date | Description |
|---|---|
| March 2016 | Initial release |
| June 2017 | Revised for Quick Sync 2, OMM 2.0 |
| Aug 2018 | Added security for MX Chassis |
| Feb 2019 | Revisions for VNC clients and MX Chassis |
| Oct 2019 | Added more details of certificate verification in OMM 3.3 |

# Acknowledgements

This paper was produced by the following:

Author:

Manoj Malhotra — Product Consultant

Saurabh Kishore — Software Principal Engineer

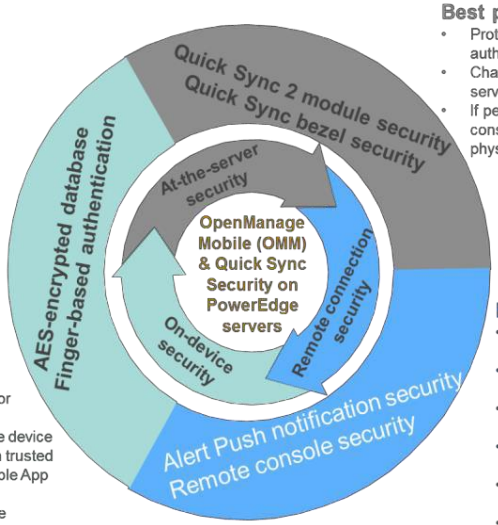
Alex Rote — Software Senior Engineer

# Table of contents

# Executive summary

Dell OpenManage Mobile (OMM) enables monitoring, provisioning, and troubleshooting of Dell PowerEdge servers as well as MX7000 chassis and associated sleds. In 2014, Dell EMC pioneered wireless at-the-server management with the NFC-based Quick Sync bezel. The latest generation of servers from Dell EMC support the Quick Sync 2 module that enables higher bandwidth Bluetooth Low Energy (BLE), and Wi-Fi connections. OpenManage Mobile also supports remote management.

Wireless and mobile security are critically important. By understanding the security features of OpenManage Mobile, organizations can embrace mobile management with confidence, that they can do so while performing their duties to keep systems secure. This document describes the security controls used by OpenManage Mobile to while at-the-server, when remote, and on the mobile device itself.




**Best practices**

- Protect your servers by limiting physical access to authorized personnel only
- Change the default credentials when provisioning a new server
- If personal devices are not permitted in the data center, consider using a dedicated mobile device which is always physically kept in the data center

**Best practices**

- Use OMM with a password
- Secure the device by using a password, pattern, or biometric lock
- Enable internal-storage encryption on your mobile device
- Download OMM and other applications only from trusted sources such as the Google Play Store or the Apple App Store
- Consider using an anti-malware app on the device

**Best practices**

- Use a VPN to secure access to the management network from remote sites
- Avoid connecting iDRAC and OME systems directly to the internet
- When making a management network available by using Wi-Fi, use the best available security configuration
- Use VNC over SSH or VNC clients with TLS encryption enabled
- Change the iDRAC root credentials to something other than the default
- Consider using a proxy server to control outbound internet access from the OME or OMM

# 1 OpenManage Mobile at-the-server and at-the-chassis security

OpenManage Mobile (OMM) can:

- Communicate directly with an iDRAC while at-the-server by using the Quick Sync 2 module and Quick Sync bezel technology. It can also communicate with MX7000 chassis using Quick Sync 2 module.
- Read server or MX chassis health, inventory, and configuration information including the Lifecycle Controller logs.
- Provision iDRAC settings such as the network configuration, root credentials, first boot device, and location information.

Administrators may power-cycle a system by using Quick Sync 2 or Quick Sync. Administrators who use Quick Sync 2 to run RACADM commands have access to all the iDRAC troubleshooting capabilities.

## 1.1 Quick Sync 2 module security

On the latest generation of PowerEdge servers and MX chassis equipped with the Quick Sync 2 module, OMM uses BLE and Wi-Fi technology to communicate. Quick Sync 2 modules support both Android and iOS.

Quick Sync 2 module technology provides a level of physical security. To activate a Quick Sync 2 module, an administrator must be physically present at the server to press the activation button. Activation button is a physical button on servers and a virtual button on MX Chassis LCD. Until Quick Sync 2 is activated, no information can be exchanged or observed.

Before authenticating the server or chassis, Quick Sync 2 BLE communications are attenuated to about 1 meter in range for typical devices. After authentication, the range is extended; the typical range is 5 meters but may vary based on the RF environment. The range of the Quick Sync Wi-Fi after activation is about 5 meters.

Quick Sync 2 BLE connections are limited to one mobile device per server at a time, and repeated attempts to access a system with invalid credentials will trigger a lockout, thus requiring a manual reactivation (by pressing the button) of the Quick Sync 2.

After connecting to a server by using Quick Sync 2 BLE, a specifically adapted version of the industry standard TLS 1.2 protocol is used to communicate with the server. Diffie-Hellman key exchange is performed by using 2048-bit or larger primes, and 128-bit symmetric AES keys are used to encrypt all subsequently exchanged BLE data. The GCM Authenticated Encryption with Associated Data cipher mode is used with unique sequence numbers to protect against tampering, information disclosure, and replay attacks.

Quick Sync 2 Wi-Fi is activated only when required for communications that require higher bandwidth or IP-based communications. Whenever Quick Sync 2 Wi-Fi is activated, a new random WPA2PSK key is generated and exchanged with OMM over the BLE connection. The relatively short key lifetime helps protect Wi-Fi level communications. Diagnostics information, RACADM commands, and iDRAC GUI access are further protected by HTTPS in the same manner as remote connections. Remote desktop connections may be protected by using the VNC over SSH or VNC over TLS.

By default, Quick Sync 2 module users are authenticated to iDRAC by using the iDRAC credentials (same goes for MX chassis). The 14th generation PowerEdge servers generally ship with a randomized secure default password. If a legacy default password (root/calvin) is specifically requested, Quick Sync 2 requires

that the unique iDRAC MAC address be supplied. Therefore, each out-of-the-box Quick Sync 2 connection is authenticated with system specific information.

When connecting to servers by using Quick Sync 2, each server is identified by an x509 format PKI certificate identical to that used by the iDRAC web server or auto-discovery feature. Also, the Service Tag of each system is displayed while connecting. To ensure that the connection occurs with the correct system, administrators may activate the ID LED option.

Users can access all sleds and other components information on MX Chassis. The data is retrieved on chassis by using a proxy BLE service. For this proxy service the highly secure TLS 1.2 protocol along with 128 bit-AES is used for encryption. The data used internally on an MX Chassis is retrieved by using an internal VLAN on MX Chassis. The connection in internal VLAN is secure and not accessible outside the MX Chassis box.

## 1.2 Quick Sync bezel security

Figure 1 An administrator using iDRAC Quick Sync

Quick Sync bezels are available on selected 13th generation PowerEdge servers equipped with a Quick Sync bezel. OMM Android uses Near-Field Communication (NFC) technology to communicate with the Quick Sync bezel which is secured using encryption and authentication.

Because of its security properties, NFC technology is often selected for use in mobile payment solutions.

The Quick Sync bezel must be activated by an administrator physically present at the server. NFC communications are limited to within a few centimeters of the bezel, precluding observation from outside the data center or even from another area within the data center. Use of the iDRAC Quick Sync bezel is logged within iDRAC.

An administrator applying a configuration by using the Quick Sync bezel must authenticate themselves by using the iDRAC credentials. Configuration information sent to the Quick Sync bezel is cryptographically protected. Configuration data is digitally signed and encrypted by using the industry standard AES algorithm with 128-bit keys. Keys are dynamically generated for each configuration write-transaction and exchanged by using the Diffie-Hellman key exchange algorithm. Unique sequence numbers prevent re- application of the same configuration request. Therefore, Quick Sync bezel configuration information is protected against tampering, information disclosure, and replay attacks.

## 1.3 Best practices for at-the-server security

To help maximize security, Dell EMC recommends the following:

- Protect your servers and chassis by limiting physical access to authorized personnel only.
- Always change the default credentials when provisioning a new server.
- If personal devices are not permitted in the data center, consider using a dedicated mobile device which is always physically kept in the data center.

# 2 OpenManage Mobile remote connection security

OpenManage Mobile retrieves data remotely from the Dell OpenManage Enterprise or OpenManage Essentials one-to-many systems management console, and iDRAC server management controllers.

The information retrieved includes device inventory, health status information, alerts, log entries, and configuration information. OMM can configure servers by using an iDRAC connection. OMM sends power control operations and other commands by using the same OME or iDRAC connections. The devices that subscribe to OME alerts receive them by using OpenManage Mobile Cloud Services (OMCS) and vendor-specific push notification services. OMM also retrieves warranty data from Dell Services. OMM can start external applications such as remote-desktop clients and web browsers.

In general, OMM communications are protected by the standard HTTPS protocol, which provides protection against tampering and information disclosure. Remote hosts are identified by using the x509 PKI certificates. OMM users are authenticated by using the systems management or iDRAC credentials.

## 2.1 General remote connection security

Dell EMC recommends that OMM connect to management networks by using VPN or encrypted Wi-Fi. This connection layer security provides an extra layer of protection.

OMM connects to systems management console or iDRAC by using HTTPS which tunnels HTTP over the TLS protocol. TLS signs and encrypts data, preventing tampering, information disclosure, and replay attacks. Connections to the iDRAC GUI from OMM also use HTTPS.

Each systems management console or iDRAC is identified by using an x509 format PKI certificate. Because consoles and iDRAC often have self-signed certificates, OMM displays the certificate information when it first connects to a system for the user to review the details of the certificate. OMM attempts to automatically verify the certificate based on its chain of trust, using the root certificates stored in the mobile phone. Verifiable identities are highlighted green, whereas identities that contain a security fault or an expired trust are highlighted red, and any non-verifiable, non-faulted certificate is highlighted yellow.

The user always has the choice of accepting or rejecting any presented certificate. When the user first accepts the certificate, OMM records the certificate thumbprint for future use. Users are alerted if the thumbprint changes during subsequent communication attempts. Rejecting a certificate terminates the connection before any authentication or application data is shared.

Systems Management consoles and iDRAC users are authenticated by their OME (Windows) or iDRAC credentials, which may be associated with an Active Directory Domain or other LDAP server. Connections to iDRAC are logged.

While Warranty status and online (QRL) resources present publicly available information, OMM communications with the Dell Warranty and QRL sites are also encrypted by using HTTPS. The information cannot be tampered with, and an unauthorized observer would not be able to determine what information is being exchanged with OMM. Dell EMC sites are identified by standard PKI certificates issued from a trusted authority.

Most information within OMM may be forwarded by using email. While email clients are outside the scope of OMM, many email clients will encrypt email message contents or transmit email over encrypted connections.

Users may voluntarily share information with Dell on how the app is used, including which features are used and which devices it is used with. Information shared with Dell is sent via HTTPS. Dell does not store or use

any information that would personally identify an individual OMM user or information on customer networks, with the exception that the OMM client IP is logged temporarily for security purposes. The IP is not stored with analytics data and is discarded after a reasonable period of time.

## 2.2 Alert Push notification security

Alerts sent by using push notifications pass through several systems before reaching a mobile device. However, each step is secured as shown in Figure 2.

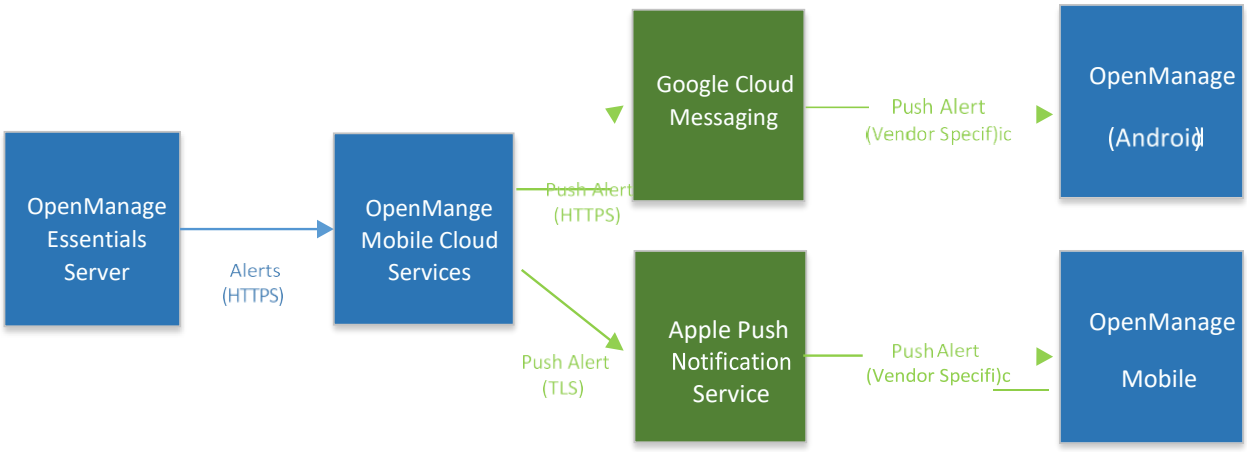



Figure 2 Alert Push Notification Security

1. OME transmits alerts to Dell OpenManage Mobile Cloud Services (OMCS) via HTTPS as identified by using a PKI certificate.
2. Based on the platform, 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.
3. 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 OME 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/or API keys to identify OMCS as being associated with the OMM app. Similarly, OMCS identifies OME instances by using API key. OMM tracks the OME instances 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 ensures that all alert messages are stored in volatile memory in order to create the push notification payload. They are erased from OMCS as soon as the push notifications are sent.

## 2.3 Remote console security

OMM can start third party remote console (VNC) applications based on the RFB protocol. OMM Android integrates with bVNC, while OMM iOS integrates with RealVNC and Remotix.

When connecting to the latest generations of PowerEdge servers, these connections can be channeled over SSH by using standard iDRAC credentials. On iOS, this requires the paid Remotix app.

On Android, connections to the earlier generation of PowerEdge servers can be channeled over TLS. The connection is secured by using a dedicated VNC password.

---

**Note**: Currently, no iOS VNC clients can communicate with iDRAC 8 and earlier over TLS. If you are confident of the security of your management Wi-Fi or VPN network, use unencrypted VNC connections.

---

## 2.4 Remote Connection Security — best practices

To help secure an environment by using OMM for remote management:

- Use a VPN to secure access to the management network from remote sites. Avoid connecting to iDRAC and OME systems directly to the internet.
- When making a management network available by using Wi-Fi, use the best available security configuration, such as WPA2 with a random key.
- Use VNC over SSH or VNC clients with TLS encryption enabled.
- Change the iDRAC root credentials to something other than the default.
- Acquire a verifiable signing certificate and generate unique identities for each systems management console or iDRAC. Install the signing certificate into the mobile devices to be able to automatically verify the identity of all remotely-accessed systems.
- Consider using a proxy server to control outbound internet access from the OME or OMM.

# 3 OpenManage Mobile on-device security

OMM stores a variety of information on the mobile device, such as credentials, host address information, and settings. When used with iDRAC Quick Sync, server health, inventory, and configuration information are also cached.

To protect this information, data is encrypted with a device-specific key, such as an optional password. When used with biometric fingerprint authentication, a fingerprint may be used to quickly access information protected by the key.

## 3.1 On-Device security controls

OpenManage Mobile is protected by an optional password and optional fingerprint-based authentication. These controls prevent an unauthorized user from logging in to the application. A fifteen-minute inactivity timeout helps protect the app if the device is laid aside for some time. This password is in addition to any device password.

Information stored within OMM is protected in an AES encrypted database and user preference files. The encryption key includes a device-specific component, so the data cannot be accessed from OMM on another device, when the data is moved (even when a password is not used). If the password is used, the password forms part of the encryption key, preventing access by anyone without the password. If fingerprint authentication is used, the device stores an encrypted copy of the password with a key derived from the fingerprint on behalf of the application. This security is in addition to any platform-specific encryption.

## 3.2 On-device security—best practices

To better secure mobile devices used with OMM:

- Use OMM with a password. Recommended passwords are at least 12 characters in length and use a combination of uppercase, lowercase, number, and symbol characters.
- Secure the device by using a password, pattern, or biometric lock. Locks are generally 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 launched 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.

# A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

## A.1 Related resources

Dell OpenManage Mobile v3.3 User's Guide (Android and iOS):
https://www.dell.com/support/home/us/en/04/product-support/product/openmanage-mobile-v3.3/manuals