Understanding OpenManage Mobile Security

Understand mobile management security features and optimize your environment for maximum security.

Dell Engineering
March 2016

A Dell Technical White Paper

Revisions

Date	Description
March 2016	Initial release

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Table of contents

Executive Summary

Dell OpenManage Mobile (OMM) enables remote system monitoring and remediation capabilities while simplifying at-the-server provisioning. As with any systems management technology, security is critically important. OMM includes a number of controls to ensure that system information is kept safe.

This document, *Understanding OpenManage Mobile Security*, provides an overview of the security features used by OMM to protect customer systems and data remotely, at-the-server, and on the mobile device itself. After understanding the security technologies used, administrators and executives can be confident in embracing mobile management capabilities.

This document also reviews current best practices so that administrators can configure their environment for maximum security. Following best practices provides in-depth protection against unauthorized access.

1 OpenManage Mobile Remote Connection Security

OpenManage Mobile retrieves data remotely from the Dell OpenManage Essentials (OME) one-to-many systems management console, as well as Dell iDRAC server management controllers.

The information retrieved includes device inventory, health status information, alerts, log entries, and configuration information. OMM sends power-control and other commands through the same OME/iDRAC connections. Devices that subscribe to OME alerts receive them via OpenManage Mobile Cloud Services (OMCS) and vendor-specific push-notification services. OMM also retrieves warranty data from Dell Services. OMM can launch external apps including 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 via x509 PKI certificates. OMM users are authenticated using standard OME or iDRAC credentials.

1.1 General Remote Connection Security

It is recommended that OMM be connected to management networks via VPN or encrypted Wi-Fi. This connection layer security provides an additional layer of protection.

OMM connects to OME and iDRAC via HTTPS which tunnels HTTP over the TLS protocol. TLS signs and encrypts data, preventing tampering, information disclosure, and replay attacks. Each OME or iDRAC is identified via a certificate. Since OMEs and iDRACs often have self-signed certificates, OMM displays the certificate info when it first connects to a system and records the certificate thumbprint. Users are alerted if the thumbprint changes on subsequent communication attempts. Connections to the iDRAC GUI launched from OMM also use HTTPS.

OME 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 via 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 sites are identified by standard PKI certificates issued from a trusted authority.

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

If users opt-in to client use analytics data collection, that information is sent to Dell 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.

1.2 Alert Push Notification Security

Alerts sent via push notifications pass through several systems before reaching a mobile device, however, each step is secured as shown in Figure 1.

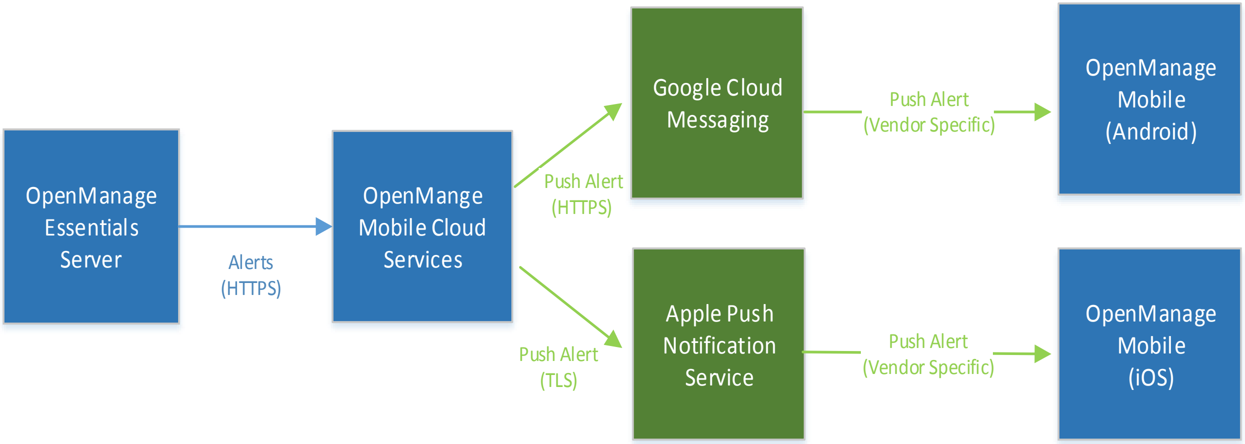
OpenManage Essentials Server
Alerts (HTTPS)
OpenMange Mobile Cloud Services
Push Alert (HTTPS)
Push Alert (TLS)
Google Cloud Messaging
Apple Push Notification Service
Push Alert (Vendor Specific)
Push Alert (Vendor Specific)
OpenManage Mobile (Android)
OpenManage Mobile (iOS)

Figure 1 Alert Push Notification Security

1. OME transmits alerts to Dell OpenManage Mobile Cloud Services (OMCS) via HTTPS as identified via a PKI certificate.
2. Depending on the platform, alerts are sent via HTTPS to Google Cloud Messaging (GCM) or via 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 of the OMM app. 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 app 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 via API key. OMM tracks which 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 does not persist the contents of alerts within OMCS.

1.3 Remote Console Security

OMM can launch 3rd party remote console (VNC) apps based on the RFB protocol. OMM Android integrates with bVNC, while OMM iOS integrates with RealVNC. On Android, these connections can be channeled over TLS. The connection is also secured via a dedicated VNC password.

Note: Currently, no iOS VNC clients can communicate with iDRAC over TLS. Only use VNC on iOS if you are confident in the security of your management Wi-Fi or VPN network.

1.4 Remote Connection Security Best Practices

To help secure an environment using OMM for remote management:

- 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 via Wi-Fi, use the best available security configuration, such as WPA2 with a random key.
- Use 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 OME or OMM.

2 OpenManage Mobile At-The-Server Security

OpenManage Mobile on Android devices can communicate directly with a server while at-the-server using iDRAC Quick Sync. Quick Sync is available on select 13th generation Dell PowerEdge servers equipped with a Quick Sync bezel. Quick Sync is built on Near-Field Communication (NFC) technology.

Note: OMM on iOS does not currently support Quick Sync NFC communication.

Using Quick Sync OMM can read server health and inventory information. OMM can provision iDRAC network settings, root credentials, and the first boot device. Additionally, OMM may reboot the server or turn it on or off via NFC.

Quick Sync is protected by the physical security afforded by NFC, and configuration information is additionally protected by authentication and encryption. Given its security properties, NFC technology is often selected for use in mobile payment solutions.

2.1 General At-the-Server Protection

The nature of Quick Sync technology provides a level of effective physical security. In order to activate Quick Sync, an administrator must be physically present at the server to press the activation button. Until Quick Sync is activated, no information can be exchanged or observed.

An administrator using iDRAC Quick Sync.

A critical element of Quick Sync security is the limited communication range of NFC technology. 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. The mobile device must be held adjacent to the server bezel, providing a positive indication of which devices are communicating. By physically identifying the server, the administrator knows they are communicating with the system they expect.

The data available via Quick Sync read is intentionally limited to the type of general health and configuration data typically offered via LCD display or other at-the-server readouts. As such, it provides at least a level of security equivalent to those displays.

Use of iDRAC Quick Sync is logged within iDRAC.

2.2 At-The-Server Configuration Security

Server configuration information is protected by additional security. Configuration data is digitally signed and encrypted using the industry standard AES algorithm with 128-bit keys. Keys are dynamically generated for each configuration write transaction and exchanged via the Diffie-Hellman key exchange algorithm. Unique sequence numbers prevent re-application of the same configuration request. As such, configuration information is protected against tampering, information disclosure, and replay attacks.

All configuration commands must be issued by an authorized user using their standard iDRAC credentials. Unauthorized configuration attempts will not be accepted.

2.3 At-The-Server Security Best Practices

To help maximize mobile security, Dell recommends the following:

- 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 within the datacenter, consider using a dedicated mobile device which is always physically kept within the datacenter.

3 OpenManage Mobile On-Device Security

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

To protect this information, data is encrypted with a device-specific key, including an optional password.

3.1 On-Device Security Controls

OpenManage Mobile is protected by an optional password. The password prevents an unauthorized user from logging in to the app. 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 within 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 if 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. 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 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.
- Only download OMM and other applications from trusted sources such as the Google Play Store or the Apple App Store. This includes apps 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 Additional resources

For more information see:

- Dell OpenManage Mobile User's Guide (Android)
  http://www.dell.com/support/manuals/us/en/19/dell-omm-v1.3/OMMANDUG-v3/Notes-cautions-and-warnings?guid=GUID-5B8DE7B7-879F-45A4-88E0-732155904029&lang=en-us

- Dell OpenManage Mobile User's Guide (iOS)
  http://www.dell.com/support/manuals/us/en/19/dell-openmanage-mobile-v1.4/OMMiOSUG/Notes-cautions-and-warnings?guid=GUID-5B8DE7B7-879F-45A4-88E0-732155904029&lang=en-us

- FAQ: iDRAC Quick Sync & OpenManage Mobile – October 2014
  http://en.community.dell.com/techcenter/extras/m/white_papers/20440554