OpenManage Mobile Best Practices

OME Engineering Team
David Warden
Sean Kim

February 2014

A Dell Best Practices

Revisions

Date	Description
February 2014	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

Revisions 2

Executive Summary 4

1 Configuring Notification Alert Filter Settings 5

2 Mobile Device Security 7

3 Configuring VPN Settings 8

4 Configuring Wireless Networks 10

5 Configuring OME Proxy Settings 11

6 Power Control Requirements 12

Executive Summary

OpenManage Mobile (OMM) provides a subset of Dell's system monitoring and management capabilities on mobile devices. This document describes best practices for deploying OMM in an enterprise environment. It is assumed the reader has a basic understanding of OpenManage Mobile (OMM), OpenManage Essentials (OME), the Integrated Dell Remote Access Controller (iDRAC), and is also familiar with the OS on their mobile device. More information on Dell products is available at the Dell Tech Center at: http://www.DellTechCenter.com.

1 Configuring Notification Alert Filter Settings

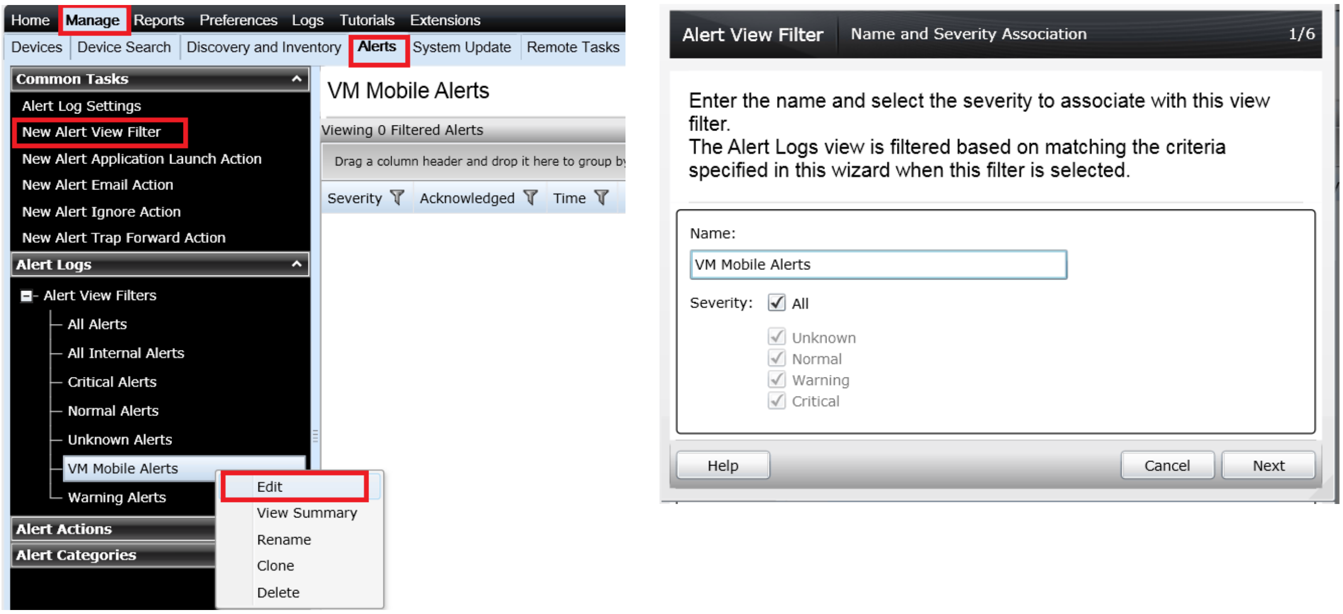
OpenManage Mobile allows a user monitoring OME servers to receive alert notifications on their phone. When the alert reaches the OpenManage Essentials server it gets pushed to the user's mobile phone through the Google Cloud Messaging service.

OME allows alerts to be filtered by severity, category, device/device group, date/time, and acknowledgement status. Pre-defined filters exist for each severity level.

In order to minimize unwanted disruptions, it is recommended that each mobile administrator use a filter customized to their role:

- Severity and category filters should be used to exclude unimportant alerts, such as those with lower severity levels.
- Device filters should be used to limit alerts to those systems for which an administrator is responsible for, such as servers in a particular VM farm.
- Alerts should be filtered by time so they are received only on those days/times when the administrator is "on call" or assigned to duty.
- If acknowledgements are used to indicate that a task has been or is being resolved, acknowledged alerts may be filtered.

To create a custom alert filter in OME, navigate to the Alerts portal (**Manage**→ **Alerts**) and under the **Common Tasks** header, click **New Alert View Filter** and complete the wizard-driven process. To edit an existing user-created custom filter, select and right-click the filter name under the **Alert Logs** header, and then select **Edit** from the right-click menu option (See Figure 1). The pre-defined filters can be cloned, but not edited.



Enter the name and select the severity to associate with this view filter.
The Alert Logs view is filtered based on matching the criteria specified in this wizard when this filter is selected.

Name: VM Mobile Alerts

Severity: ☑ All

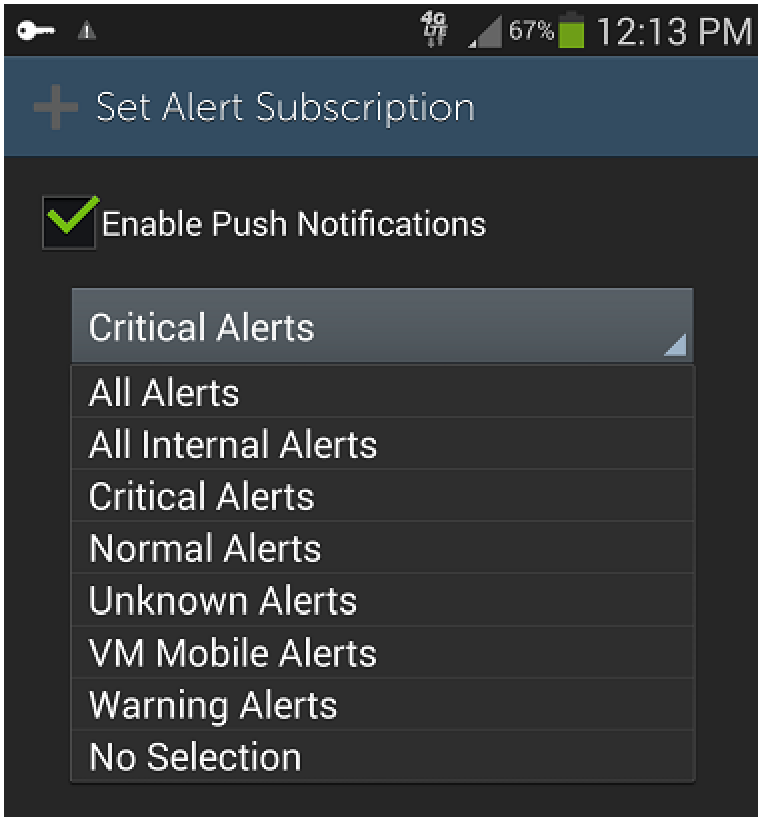
☑ Unknown
☑ Normal
☑ Warning
☑ Critical

Figure 1 Alert View Filters

All Alert View Filters that are seen in OME's Alert portal are available as push notification subscription filters when the OME connection is initially created or edited in OMM. If administrators in your organization periodically rotate roles, it may be easier to reassign filters among administrators, rather than edit the filters.

To change alert filters in OMM:

1. Verify network connectivity between the mobile device and the OME management system exists (i.e., secure Wi-Fi or VPN).
2. From the home screen in OMM, long press on the OME instance and select **Edit Instance**.
3. Click **Next** to go to the **Set Alert Subscription** page.
4. Select the alert filter from the drop-down list (Figure 2).



Set Alert Subscription

☑ Enable Push Notifications

Critical Alerts

- All Alerts
- All Internal Alerts
- Critical Alerts
- Normal Alerts
- Unknown Alerts
- VM Mobile Alerts
- Warning Alerts
- No Selection

Figure 2 OMM Alert Subscription Settings

Notifications can be disabled from OMM, OME, or the Android device settings. It may be useful to temporarily disable notifications at certain times, such as when on vacation. To disable notifications from within OMM, uncheck the **Enable Push Notifications** box from within the **Set Alert Subscription** page.

If an alert filter used by OMM includes more than 100 alerts/day, notifications may be throttled by Google and not received until after a delay of up to several hours.

2 Mobile Device Security

It is recommended that OMM be used with a PIN to protect access to the OMM app, particularly if the device does not have a screen lock configured. OMM uses encryption to protect connection information including credentials.

For maximum security, it is recommended that you encrypt your device and use a screen lock with strong security such a strong password or PIN and screen lock timeout no longer than 15 minutes. It is also recommended that you do not use a "rooted" phone.

OMM relies on the same OME and iDRAC roles as the consoles normally use. Any task that can be performed via OMM could also be performed via the web browser. Therefore, there is no need to have separate mobile credentials.

OMM does not store device-specific credentials for devices connected via OME when performing actions. However, when performing actions on an iDRAC, the credentials used for the connection are pre-populated.

3 Configuring VPN Settings

It is highly recommended that your OME servers and iDRACs be protected by firewalls and only accessible to OMM through a secured Wi-Fi network or a Virtual Private Network. VPNs may be used with cellular or Wi-Fi connections.

Android has built-in support for a number of VPN protocols including:

Andriod VPN Protocols:

- PPTP
- L2TP/IPSec PSK
- L2TP/IPSec RSA
- IPSec Xauth PSK
- IPSec Xauth RSA
- IPSec Hybrid RSA

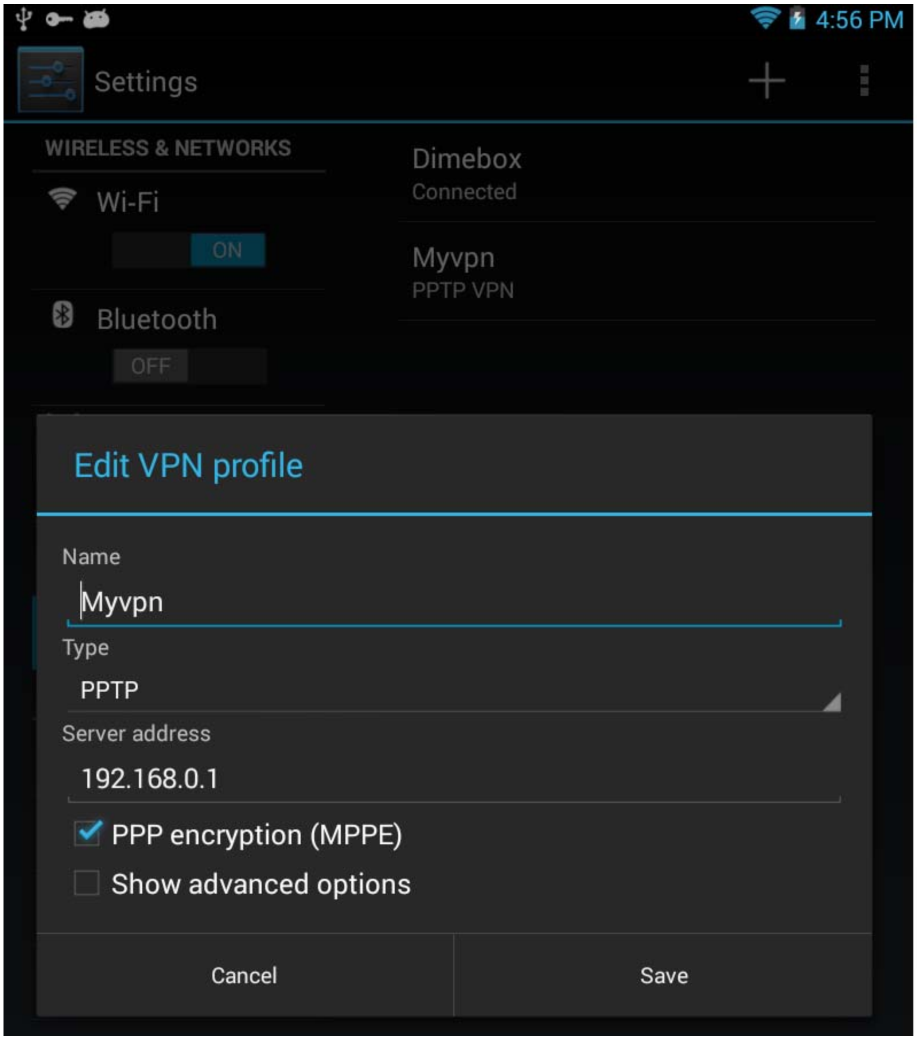
Standard VPN protocols are secured by some combination of username/password, certificate, or secret key. It is recommended that VPN usernames be associated with directory accounts so that the user accessing the network is known.

A number of VPN solutions are available which can provide additional security, including authentication of particular devices and scanning of traffic for malware. For information on Dell SonicWALL VPN solutions for Android see: SonicWALL Mobile Connect for Google Android.

Android requires devices having a VPN connection configured remain protected by a PIN or other lock mechanism with a timeout of not more than 30 minutes.

Exact configuration steps vary by device. To configure VPN settings on a Dell Venue 8 running Android 4.3 (Figure 3):

1. From the settings app, select **More** under the **Wireless and Networks** header.
2. Select **VPN** to go to the VPN connection list.
3. If prompted, configure the lock screen.
4. Touch the **+** icon to create a new VPN connection
5. Enter a **Name** for the connection.
6. Select the **Type** of connection from the drop-down list.
7. Enter the **Server address**.
8. If necessary, configure Proxy and DNS details by tapping the **Show advanced options** check box and completing the associated fields. Proxy information may be required in order to receive push notifications while connected to your VPN. DNS information may be required to resolve hostnames.
9. Complete any other required fields.
10. Touch **Save**.



Name
Myvpn

Type
PPTP

Server address
192.168.0.1

☑ PPP encryption (MPPE)

□ Show advanced options

Figure 3 Dell Venue 8 VPN Settings

To connect to the VPN:

1. Select the VPN from the VPN connection list.
2. Enter the **Username** and **Password**, if required.
3. Touch **Connect**.

4 Configuring Wireless Networks

Android also supports a number of wireless security protocols based on a passphrase or certificate which may vary by device. Protocols commonly include:

Common Android Wireless Security Protocols

- None
- WEP
- WPA/WPA2
- 802.1x EAP

Running a Wi-Fi network with no security or with WEP security is not recommended. Use of 802.1x EAP with MS_CHAPv2 secondary authentication is also not recommended due to security vulnerabilities in the protocol.

As with VPN solutions, Wi-Fi security solutions are available which authenticate a particular user and/or device and can help protect against malware. It is possible to use a VPN in combination with a Wi-Fi network.

Android devices do not require a PIN lock to protect access to a Wi-Fi network.

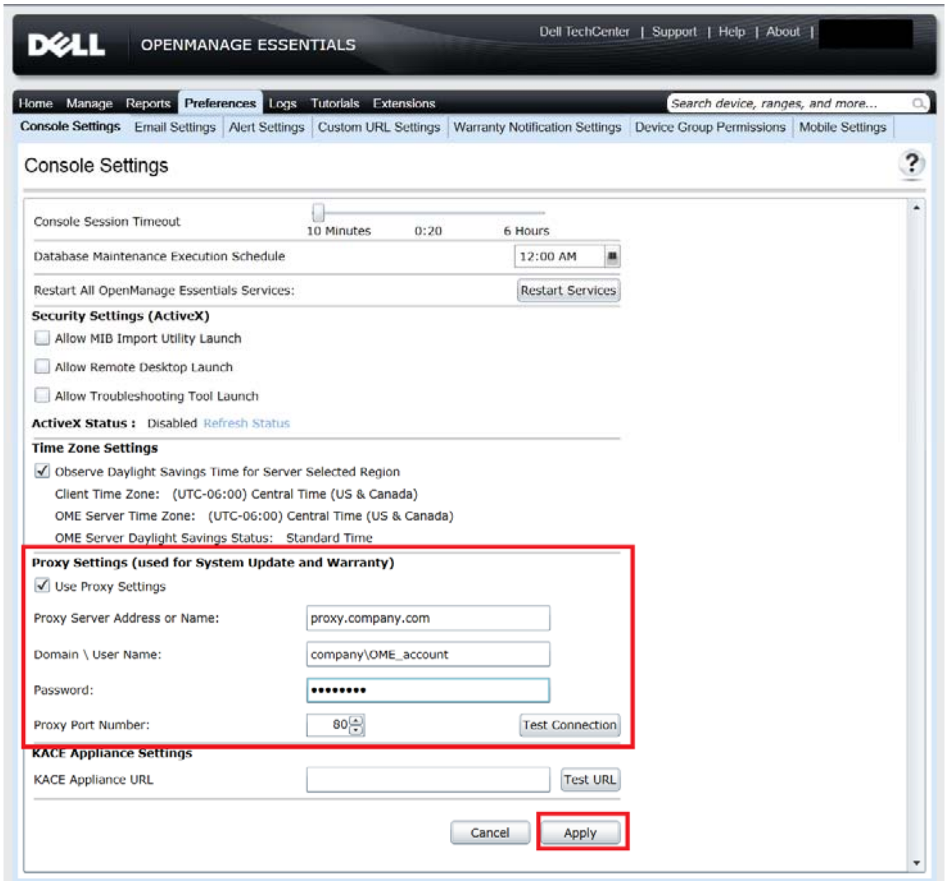
5 Configuring OME Proxy Settings

To support alert push notifications, OME requires outbound Internet access. For security, it is recommended that outbound Internet access be controlled via firewall or proxy authentication.

If your organization uses a password authenticated proxy, it is recommended that a dedicated OME proxy account be created with a password that does not expire. The account password will need to be updated in OME each time it is changed in order to ensure that the delivery of push notifications, sent from OME, are not interrupted.

To configure proxy settings in OME:

1. From the OME console navigate to **Preferences→ Console Settings**.
2. Enter the proxy server **Address**, **Domain\Username**, **Password**, and **Port Number** as required.
3. Ensure that the **Use Proxy Settings** box is checked.
4. Click **Apply**.
5. The system will test the connection by attempting to connect to **dell.com** and report the results.


DELL
OPENMANAGE ESSENTIALS
Dell TechCenter | Support | Help | About |
[redacted]
Home Manage Reports Preferences Logs Tutorials Extensions
Search device, ranges, and more...
Console Settings Email Settings Alert Settings Custom URL Settings Warranty Notification Settings Device Group Permissions Mobile Settings
?

Console Settings

Console Session Timeout: 10 Minutes 0:20 6 Hours

Database Maintenance Execution Schedule: 12:00 AM

Restart All OpenManage Essentials Services: Restart Services

Security Settings (ActiveX)

□ Allow MIB Import Utility Launch

□ Allow Remote Desktop Launch

□ Allow Troubleshooting Tool Launch

ActiveX Status : Disabled Refresh Status

Time Zone Settings

☑ Observe Daylight Savings Time for Server Selected Region

Client Time Zone: (UTC-06:00) Central Time (US & Canada)

OME Server Time Zone: (UTC-06:00) Central Time (US & Canada)

OME Server Daylight Savings Status: Standard Time

Proxy Settings (used for System Update and Warranty)

☑ Use Proxy Settings

Proxy Server Address or Name: proxy.company.com

Domain \ User Name: company\OME_account

Password: ••••••••

Proxy Port Number: 80 Test Connection

KACE Appliance Settings

KACE Appliance URL: Test URL

Cancel Apply

Figure 4 OME Proxy Settings

If you attempt to use OME with a database created by another instance of OME (other than an upgrade), proxy credentials will need to be re-entered.

6 Power Control Requirements

To ensure successful completion of remote remediation power tasks using OMM, managed servers must meet protocol requirements. Some power tasks may not run successfully if these requirements are not met. Please refer to the *Device Capability Matrix* in the *Managing Remote Tasks* section in the OME Help documentation for more details.

The following guidelines are recommended to ensure successful power task operations using OME and OMM.

- **Power On** task:
  - OME should have network connectivity to the out-of-band IP/host name of the managed DRAC.
  - IPMI-over-LAN must be enabled and configured on the DRAC device.
  - The DRAC IP/hostname should be discovered and inventoried using IPMI protocol in OME.
- **Power Off, Reboot, Shutdown** tasks:
  - OME should have network connectivity to the in-band IP/host name of the server host OS.
  - OpenManage System Administrator (OMSA) should be installed on the server.

Power task commands performed on an iDRAC, managed by OMM, are sent from OMM directly to the iDRAC, in contrast to power task commands performed on a system managed by OME, which are sent from OMM to OME to be processed.

The **Enable All** option, available in the Power Options GUI in OMM, is an alternative way of performing power tasks if the managed node is not properly discovered and inventoried in OME or the device details of the managed node are not up-to-date in OME.

The **Enable All** option is useful in the following scenarios:

- OMSA has been recently installed on a managed node, however the inventory update task has not subsequently completed within OME and the power options are not shown as available. Selecting the **Enable All** option will allow power tasks to be completed on the server.
- The managed node has OMSA installed and the DRAC is properly configured for the IPMI-over-LAN feature, but the iDRAC IP/host name has not been discovered and inventoried using the IPMI protocol in OME and the system is powered off. Selecting the **Enable All** option will allow the system to be powered on.