

Dell EMC OpenManage Essentials Version 2.5 Release Notes

This document describes the new features, enhancements, and known issues in Dell EMC OpenManage Essentials Version 2.5.

Topics:

- [Release type and definition](#)
- [Platforms affected](#)
- [What is supported](#)
- [New in this release](#)
- [Known issues](#)
- [Manage MIBs](#)
- [Troubleshooting](#)
- [Limitations](#)
- [Installation](#)
- [Installation instructions](#)
- [Upgrade](#)
- [Uninstallation](#)
- [Contacting Dell](#)

Release type and definition

Dell EMC OpenManage Essentials

Dell EMC OpenManage Essentials provides a central point of access to monitor and manage systems on a local area network (LAN). By allowing an administrator a comprehensive view across the enterprise, OpenManage Essentials can increase system uptime, reduce repetitive tasks, and prevent interruption in critical business operations.

Version

2.5

Release Date

October 2018

Previous Version

2.4

Importance

OPTIONAL: Dell EMC recommends the customer review specifics about the update to determine if it applies to your system. The update contains changes that impact only certain configurations, or provides new features that may/may not apply to your environment.

For the latest updates to the release notes, see DellTechCenter.com/OME.

Platforms affected

For a complete list of affected Dell EMC systems and supported operating systems, see the *Dell EMC OpenManage Essentials Version 2.5 Support Matrix* at DellTechCenter.com/OME or Dell.com/OpenManageManuals.

What is supported

For a complete list of supported devices, operating systems, and web browsers, see the *Dell EMC OpenManage Essentials Version 2.5 Support Matrix* at DellTechCenter.com/OME or Dell.com/OpenManageManuals.

New in this release

- Support for the following features of a MX7000 chassis—as a standalone chassis and as a lead chassis in an MCM group:
 - Discovery, inventory, monitoring, and status polling
 - Alerts recognition and traps classification
 - System updates
 - Configuration template creation and deployment
 - Configuration compliance and remediation
 - Configuring VLANs on MX7000 chassis by using the blade server template deployment feature
- Support for the following devices:
 - Latest 14th generation PowerEdge servers including new blade servers of MX7000 chassis
 - PowerEdge MX7000 modular enclosure
 - VxFlex Ready Nodes

For a complete list of supported device models, see the *Dell EMC OpenManage Essentials Support Matrix* at Dell.com/OpenManageManuals.

- Enhancements:
 - Enhanced view to display catalog baselines associated to the custom device groups

Known issues

System updates

NOTE: OpenManage Essentials does not support the software update task on the management station. This is because the task is interrupted and the final results of the update are not known. You can perform software updates by using other Dell EMC tools.

Before creating an update task for noncompliant systems, Dell EMC recommends that you update to the latest catalog from downloads.dell.com. Ensure that you have Internet connectivity to download the latest catalog.

Issue 1:

Description: When performing the system update task as a sudo user on a target that does not have OMSA installed, the Scheduled F/W & Driver Inventory task fails with the **sudo requires password** error.[48587]

Resolution: Edit the sudoers file using the `visudo` command, and add the following:

- For target systems running a 32-bit operating system:

```
Cmd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec, /tmp/LinuxPreInstallPackage/runbada,/tmp/LinuxPreInstallPackage/omexec, /tmp/invcol.bin <sudo_username>
ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```
- For target systems running a 64-bit operating system:

```
Cmd_Alias OMEUPDATE = /bin/tar,/opt/dell/srvadmin/bin/omexec, /tmp/LinuxPreInstallPackage64/runbada,/tmp/LinuxPreInstallPackage64/omexec, /tmp/invcol64.bin <sudo_username>
ALL=OMEUPDATE,NOPASSWD:OMEUPDATE
```

Issue 2:

Description: Simultaneously running the OMSA deployment task and in-band system update task on the same server is not supported. [44598]

Issue 3:

Description: In rare cases, inapplicable package may be listed in the compliance report, but the updates are not applied to the target node if the package is not applicable.

Issue 4:

Description: Intel PCI-E driver package information for a server that is seen in OpenManage Essentials might be different than the driver package information seen in SUU. Package name, Component name, Current Version, and Repository Version might be different. [473495]

Issue 5:

Description: Broadcom NetXtreme driver package information for a server that is seen in OpenManage Essentials might be different than the driver package information seen in SUU. Package name, Component name, Current Version, and Repository Version might be different. [473493]

Issue 6:

Description: For systems with a Trusted Computing Group (TCG) 1.2-compliant Trusted Platform Module (TPM) chip, software updates for the BIOS fail if all of the following are true:

- The Microsoft Windows BitLocker Drive Encryption feature is enabled.
- The TPM feature is set (using BIOS) to ON with Preboot Measurement.

For information about TPM security settings, see the *Dell OpenManage Server Administrator Online Help* or the *Dell OpenManage Server Administrator User's Guide* available at Dell.com/OpenManageManuals and on the appropriate media that are supplied by Dell. For software updates for BIOS to function, perform the following steps:

1. Disable the **Microsoft Windows BitLocker Drive Encryption** feature. For information on disabling this feature. See the *Microsoft documentation* at www.microsoft.com.
2. Update the BIOS.
3. Restart the system.
4. Re-enable the **Microsoft Windows BitLocker Drive Encryption** feature.

You can use OpenManage Essentials to view the TPM information in the **Device Details** page.

Issue 7:

Description: After creating a system update task to run immediately, it may take several minutes or more to see the task created, because the update packages are downloaded in the background before the task is registeredw.

Issue 8:

Description: When quota management is enabled on the management station and a user approaches the quota limit, system update tasks that are created by the user are not initiated. The **Task Execution History Status** displays the pause icon. [29773]

Resolution: Increase the quota assigned to the user and then rerun or re-create the system update task.

Issue 9:

Description: System Update task does not work if the security group policy called Admin Approval Mode for the built-in Administrator account is enabled on the system running OpenManage Essentials. [30884]

Resolution: OpenManage Essentials cannot elevate permissions to copy and run updates when Admin Approval Mode is enabled on the OpenManage Essentials system. Use the default settings to execute the System Update task.

Issue 10:

Description: OpenManage Essentials only supports system updates on PowerEdge systems. Sometimes PowerVault NX devices may display in the compliance report even though system updates on PowerVault NX devices are not supported by OpenManage Essentials.

Issue 11:

Description: System update task to upgrade Emulex LightPulse HBA — Storport Miniport driver (10 GbE Network Adapter) on Windows Server 2008 R2 or 2012 results in a time-out error. [61903]

Resolution: Installation of the Emulex NIC driver on Windows Server 2008 R2 and Windows Server 2012 results in an error message that states that a KB article from Microsoft needs to be installed, even if the indicated KB article (hot fix) is already installed. Therefore, ensure that the hot fix specified in Microsoft KB article 2846340 is applied on the server, and then run the system update task.

Issue 12:

Description: After updating the PSU firmware through OpenManage Essentials, the **Device Inventory** page continues to display the earlier PSU firmware version.

Issue 13:

Description: After the PSU firmware is updated through OpenManage Essentials, some PowerEdge servers may not turn on automatically after they shut down.

Resolution: Turn on the server manually.

Issue 14:

Description: During in-band system update for SAS HDD firmware, DUP is failing with "invalid image file" error. [63920]

Resolution: Use out-of-band method to update the SAS HDD firmware. Or, for a workaround to use in-band method of system update, see the *Device Buffer error when running Online HDD firmware DUP* article at www.dell.com/support/article/is/en/isdhs1/SLN155722/device-buffer-error-when-running-online-hdd-firmware-dup?lang=EN.

Issue 15:

Description: The Software Inventory table is not updated with the latest firmware version of the iDRAC if the firmware update is done using in-band method on servers with Linux operating system and OMSA (v8.2 to v8.5) installed. [78339]

Resolution: Restart the OMSA shared services on target server, or discover iDRAC using out-of-band method and update the firmware. Alternatively, change the SELinux settings value to "Permissive" from "Enforcing" on target server, and perform the inventory again. The SELinux config file is available at /etc/selinux/config.

Issue 16:

Description: In OpenManage Essentials 2.4, if common devices are present in more than one custom group, selecting the bar chart of a custom group (on the System Update page) displays noncompliant devices of that respective custom group. However, using the "Filter by" option to select a custom group displays noncompliant devices common to other custom groups also. [81438]

Issue 17:

Description: In OpenManage Essentials 2.4, OmeSiteAdministrators can view the devices including those for which they do not have access by clicking the Compliant or Noncompliant bars in the **All Devices** section of the bar chart. [81958]

Issue 18:

Description: In-band System Update task fails with an error: Unable to copy the file to the remote system. [82358]

Resolution: You must delete all the temporary files including the WindowsPreInstallPackage file from C:\Windows\Temp on the target system, and then rerun the in-band System Update task.

Issue 19:

Description: The **Task Execution History** tab displays the System Update Task state as Pending even when the task has failed due to the missing catalog files in the FTP location.

Issue 20:

Description: As a OmeSiteAdministrators, when you select the **View System Update** portal, the **Filtered by** option is not updated from the custom device group and pie chart is displayed instead of bar chart. [84782]

Resolution: Click the **Filtered by** option, and select the **All devices** check box.

Issue 21:

Description: As a SiteAdmin, when you select the **Non-Compliant Systems** tab under **Manage > System Update** for the first time, all the noncompliant devices are listed. [84802]

Resolution: Refresh the page, and select the noncompliant chart under Compliance Report.

Issue 22:

Description: If you select the **Enable Downgrades** option under **Manage > System Updates > Advanced Settings**, the devices are displayed as noncompliant. However, when you upgrade to OpenManage Essentials version 2.5, the systems and downgradable packages are not considered for compliance. [84897]

Resolution: After the upgrade, select **Disable Downgrades** and then select the **Enable Downgrades** option under **Advanced Settings**.

Issue 23:

Description: If ICMP ping is disabled in a OpenManage Essentials system configured with multiple IP addresses, and one or more subnets (IP addresses) of the system are accessible or reachable from iDRAC subnet, the firmware update on an iDRAC might fail with an error: Unable to download Update Package. MessageID: RED006. [PSE-4386]

Resolution: Allow ICMP packets through firewall and clear the **Skip ICMP ping during discovery** option under Discovery Settings, or use an OpenManage Essentials system configured with a single IP address.

Installation

It is recommended that you install OpenManage Essentials by using either the `Setup.exe` or `Autorun.exe` file.

Issue 1:

Description: An SQL ODBC Driver timeout error is displayed during the installation of OpenManage Essentials. [47759]

Resolution: This error may be seen invalidly if the host name cannot be resolved on the OpenManage Essentials server.

1. Ping the host name of the OpenManage Essentials server to confirm that name resolution works.
2. If the ping fails, fix the DNS issues before attempting to install or use OpenManage Essentials.

NOTE: Both the installer and application require proper name resolution to function properly.

3. If name resolution is successful, follow the instructions in the *Troubleshooting: Timeout Expired* knowledge base article at technet.microsoft.com.

Issue 2:

Description: After installing Essentials on a database retained from an earlier Essentials installation, the following are unsuccessful:

- Discovery/Inventory
- Remote task/Scheduled tasks
- Proxy connection
- Email alert action [40085]

Resolution: The following must be provided after the Essentials installation:

- Protocol-specific credentials for discovery and inventory.
- Credentials for remote/scheduled tasks.
- Proxy credentials.
- Email alert action credentials.
- Any other feature that requires credentials.

Issue 3:

Description: After installing OpenManage Essentials, if you reinstall the database application (which is used by OpenManage Essentials) the OpenManage Essentials database is detached from the database application.

Issue 4:

Description: OpenManage Essentials installation may stop after a system reboot.

Cause: This issue occurs because the files are extracted to the %temp% directory and the files get deleted after a system reboot.

Resolution: To resolve this issue, re-launch the OpenManage Essentials executable file again.

Issue 5:

Description: After the installation of a prerequisite for OpenManage Essential is completed, the system does not restart even after confirmation. [67806]

Resolution: Manually restart the system.

Migration

The following Tasks will not get migrated from ITA:

- Server Software Update
- Client Software Update
- IPMI Command Line
- Power Control Device (via ASF)
- Performance Management
- Import Dell EMC Catalog
- Server Administrator Deployment for Windows
- Server Administrator Deployment for Linux
- While migrating tasks from IT Assistant to OpenManage Essentials, all the **Run Now** tasks are migrated as disabled.
- While migrating tasks from IT Assistant to OpenManage Essentials, if **Run Once** tasks have the start schedule in the future they will start in the future. If the start schedule is in the past, they will not start.
- Migration of IT Assistant to OpenManage Essentials installation using local database, or OpenManage Essentials using remote database is not supported.
- While migrating Alerts from IT Assistant to OpenManage Essentials, Alert filters get migrated, but alert actions do not get migrated from ITA.
- While migrating from IT Assistant 8.x to OpenManage Essentials 1.0 to OpenManage Essentials 1.0.1, if you encounter a problem during OpenManage Essentials 1.0.1 repair, rename the folder containing OpenManage Essentials 1.0 installation and retry the repair.

- It is recommended that you ensure that all system update and remote tasks are completed before you upgrade OpenManage Essentials. If a system update folder migration error occurs during upgrade, you can copy the folder manually from the %temp% folder, or you can re-run the required tasks after upgrade.
- On a system where OpenManage Essentials version 2.1 and SupportAssist version 2.1 are installed, after upgrading OpenManage Essentials to version 2.2, you must manually start the SupportAssist service.

Issue 1:

Description: After upgrading from OpenManage Essentials version 2.1 to version 2.2, duplication of the PowerVault MD Series storage arrays is observed in the device tree. [68438]

Resolution: To eliminate the duplicate entries, ensure that you delete and rediscover the PowerVault MD Series storage arrays.

Issue 2:

Description: After upgrading from OpenManage Essentials version 1.1.1 to 2.2, or 1.1.1 to 1.2 to 1.3 to 2.0 to 2.0.1 to 2.1 to 2.2, the **Custom URL settings** page may display multiple custom URLs based on the classification of a device in the device tree.

For example, if a custom URL is created for the Servers device group and the servers in your environment are classified under the Servers, RAC, and VMware ESX Servers device groups in the device tree, after upgrading to OpenManage Essentials version 2.2, the **Custom URL settings** page displays three Custom URLs (one for each of the device groups under which the servers are classified in the device tree). [40774]

Issue 3:

Description: After upgrade to OpenManage Essentials version 2.2:

- The devices are not classified correctly.
- The devices that were reported in the **Non-Compliant Systems** tab are displayed in the **Compliant Systems** tab. [40445]

Resolution: After the upgrade, you must initiate the discovery and inventory for all ranges.

1. Click **Manage > Discovery and Inventory**.
2. Under Discovery Ranges, click **All Ranges**. The Discovery Range Summary is displayed.
3. Select all the discovery ranges, right-click and select **Perform Discovery and Inventory Now**.

Issue 4:

Description: After an upgrade from OME 1.0/1.0.1 or migration from ITA, RAC health status will be unknown if it was discovered using IPMI protocol and user or operator privileges.

Resolution: Provide the user account in the discovery wizard with IPMI admin privileges on the RAC and re-run discovery to get the health status.

Issue 5:

Description: Customizations to the Devices portal layout are deleted on upgrading to OpenManage Essentials 2.2. [18342]

Issue 6:

Description: While upgrading from OpenManage Essentials version 1.0.1 or 1.1 installed with remote SQL Server 2005 to OpenManage Essentials version 2.2, the following message is displayed:

SQL Server 2005 is detected on the target system. The minimum version of SQL Server supported by Essentials is SQL server 2008. [31161]

Resolution: In this case, you must manually migrate the data from SQL Server 2005 to other supported SQL Server versions, and then upgrade to OpenManage Essentials version 2.0. For more information, see the **Frequently Asked Questions** section in the *OpenManage Essentials version 2.0 User's Guide*.

Launching OpenManage Essentials

Issue 1:

Description: If the host name of the management station is changed after the installation of OpenManage Essentials, you will be prompted to provide the system credentials when OpenManage Essentials is launched. [38871]

Issue 2:

Description: OpenManage Essentials launches in Internet Explorer even if any other browser is set as the default browser. [35491]

Issue 3:

Description: OpenManage Essentials does not launch or displays an exception when the number of connections to the OpenManage Essentials website is limited in IIS.

Resolution: The OpenManage Essentials console requires constant communication with the web server to ensure that the data is up-to-date always. The communication between the console and the web server is performed utilizing web method calls in a multi-threaded environment. As such, multiple, simultaneous connections to the web server are required in order for OpenManage Essentials to operate properly. As a general rule, ensure that your web server is configured for a minimum of 50 active connections.

Issue 4:

Description: OpenManage Essentials does not launch when the IP address of the remote database is changed. [31801]

Resolution: Reinstall OpenManage Essentials and target the existing remote database with the new IP address.

Discovery and inventory

The processor count in OpenManage Essentials differs for managed systems that contain processors with multiple cores or HyperThreading enabled. The count differs based on whether the managed system is discovered using the CIM or SNMP protocol. The systems discovered using SNMP report physical processors, and the systems discovered using CIM report logical processors.

Issue 2:

Description: An EqualLogic storage array is displayed even after excluding the EqualLogic discovery range.

Resolution: If the EqualLogic Group Management, EqualLogic Storage Group, and all the EqualLogic member IP addresses are included in a single discovery range configuration, excluding that range will exclude the entire group in the device tree.

If these IP addresses are distributed among multiple discovery range configurations, to exclude the EqualLogic group, all the associated discovery ranges must be excluded.

Issue 2:

Description: For Dell EMC PowerVault MD storage arrays with thin virtual disks, the **Virtual Disk Information** table in the OpenManage Essentials device inventory displays the name of the repository for thin provisioning instead of the thin virtual disk name. [42606]

Issue 3:

Description: For Dell EMC PowerVault MD storage arrays, OpenManage Essentials displays critical health status, even if the device is in a warning state. [42607]

Issue 4:

Description: The model number for both Dell EMC Force10/Networking C150 and C7004 Ethernet switches is displayed as C150/C7004 switch in the device inventory. The model number for both Dell EMC Force10/Networking C300 and C7008 Ethernet switches is displayed as C300/C7008 switch in the device inventory. [43443]

Issue 5:

Description: OEM devices discovered using the SNMP or WS-Man protocol are classified under **Modular Systems** in the device tree. [40572]

Issue 6:

Description: When a PowerEdge FX2s chassis is discovered using WS-Man protocol, the hostname of the corresponding mapped sled is not displayed in the **PCIe Slot Information** table in the device inventory. [37351]

Issue 7:

Description: When a PowerEdge FM120x4 sled is discovered in-band using SSH protocol, the **Embedded Device Information** table is not displayed in the device inventory. [39312]

Issue 8:

Description: When a PowerEdge FM120x4 sled is discovered using SNMP+WMI protocol, the **Software Inventory Table** displays multiple entries for the iDRAC version. [39428]

Issue 9:

Description: If a device is not configured with the system contact details, the **Contact Information** table is not displayed in the device inventory information. [36733]

Issue 10:

Description: If the PowerEdge RAID Controllers (PERC) in a PowerEdge VRTX chassis have different versions of firmware installed, the **Software Inventory Information** table displays only the PERC with the main controller firmware version. [39761]

Resolution: Make sure you update the firmware version of the PERC manually in the Chassis Management Controller console.

Issue 11:

Description: Dell EMC EqualLogic FS7500 NAS device discovered using the management member IP is displayed as **Unknown** in the device tree. [39618]

Resolution: Discover the Dell EMC EqualLogic FS7500 NAS device using the group manager IP.

Issue 12:

Description: If a PowerEdge VRTX chassis is discovered using SNMP protocol and NetBIOS name resolution setting, the instrumentation (NetBIOS) name is not resolved. [27327]

Issue 13:

Description: When a monolithic Dell EMC 11th or 12th Generation PowerEdge server with iDRAC6/7 is discovered using the IPMI protocol only (iDRAC out-of-band discovery), the overall health status of the server is not reported correctly in OpenManage Essentials. This issue occurs due to a known limitation in iDRAC. [21599]

Resolution: Discover the server's iDRAC (out-of-band) using either WS-Man or SNMP protocol.

Issue 14:

Description: When only the EqualLogic storage array in a PowerEdge chassis is discovered, the EqualLogic storage array is not classified under **Modular Systems > PowerEdge chassis > Storage** in the device tree. [38654]

Resolution: Make sure that the PowerEdge chassis is also discovered.

Issue 15:

Description: Dell EMC Fibre Channel switches (modular) are classified under **Network Devices > Switches** and not under **Modular Systems** in the device tree. [36990]

Issue 16:

Description: When the name resolution on an IP address to a host name fails using DNS, OpenManage Essentials attempts to resolve the name using the NetBIOS name query. This action may cause the device to appear in Essentials with the NetBIOS name even if it does not have a DNS entry. [138013]

Issue 17:

Description: In case of SNMP discovery, when the name resolution on an IP address to a host name fails using DNS, Essentials attempts to resolve the name using the MIB2 name query. If the MIB2 name query also fails, then Essentials displays the IP address of the device as the device name.

Issue 18:

Description: For Remote Access Controllers (RACs) that have instrumentation installed and that are running on the host operating system, the RAC IP addresses are shown in the **RAC Device** table. [134365]

Issue 19:

Description: For NIC information on systems, Essentials uses the operating system's provider(s) to retrieve data rather than Server Administrator. This behavior can result in discrepancies in reporting NIC information between Essentials and Server Administrator. For example:

- On Linux systems, adapters may be named differently between OpenManage Essentials and Server Administrator. For example, OpenManage Essentials may report a NIC adapter as **eth0**, while Server Administrator shows the actual manufacturer name of the NIC.
- If more than one NIC card is not configured with an IP address, OpenManage Essentials may show only one of the cards with an IP address of 0.0.0.0.
- OpenManage Essentials may not report disabled NIC adapters.

Issue 20:

Description: While performing discovery, if a device is discovered using **host name**, and if its IP address changes at a later time, OpenManage Essentials displays two devices after the next discovery cycle. One device displays the old IP address and status as **Power Down**, while the other displays the new IP address. This problem is likely to affect systems that have DNS-DHCP IP addressing and for which the IP addresses frequently change. [148069]

Resolution: A workaround to eliminate duplicate device is to delete the device with the old IP address.

Issue 21:

Description: NIC information is not displayed in the device details screen for Dell EMC arrays. Use **Navisphere Manager** to view these details.

Issue 22:

Description: If you are managing a Dell EMC storage array, enter the IP address for only one of the storage processors (that is, either SPA or SPB, and not both) in the discovery range. The storage processors are redundant and return the same inventory data to OpenManage Essentials. If you enter both SPs in the discovery range, only one SP will be displayed in the device tree.

Issue 23:

Description: It is not recommended to provide an IP address in multiple ranges, especially when you are using the IPMI protocol. This could result in duplicate devices being displayed in the device tree. [78710]

Issue 24:

Description: For IPMI-based discovery or inventory, the maximum length for the host operating system name is 62 characters. Any character beyond that limit will be truncated. [91210]

Issue 25:

Description: SNMP connectivity from Essentials may fail if the SNMP ports on the management station and managed system are different. If some management applications change the default SNMP port, it could lead to SNMP connectivity failure from Essentials. [175442]

Issue 26:

Description: If you manually change the host name of the server which has already been discovered in OpenManage Essentials, then duplicate entries appear in the device list corresponding to the IP address of the device whose host name has been changed. The new host name also corresponds to same IP address and the duplicate entry of the earlier host name is not automatically deleted. OpenManage Essentials displays both the new and the old host names. [247879]

Issue 27:

Description: If a server is discovered using both SNMP and IPMI (in-band and out-of-band IP addresses respectively), Essentials will correlate the two and display a single device under the **Servers** group in the devices view. If IPMI is then disabled, a new device would appear under the **Unknown** group, corresponding to the out-of-band interface. The device details under the **Servers** group continues to display the out-of-band IP address as well. After you re-enable IPMI, the device under **Unknown** group can be removed by right-clicking it and selecting **Remove**. [262869]

Issue 28:

Description: When a **Power Monitoring Capable** Server is discovered through the CIM protocol, on the **Device Details** screen, Essentials may display **No** under the **Power Management** column in the **Power Supply Information** section. To display the correct information, discover the server using either SNMP, or both SNMP and CIM protocols. [300080]

Issue 29:

Description: Even after performing inventory on the discovered Linux servers **N** number of times, the Linux servers are still listed under **Non-Inventoried systems**.

Resolution: To resolve this issue perform the following steps:

For Red Hat Enterprise Linux 5.5, SUSE Linux Enterprise Server 10, SUSE Linux Enterprise Server 11

1. Mount the OpenManage Server Administrator DVD in the Linux server.
2. Install **'srvadmin-cm'** rpm.
3. Restart the OpenManage Server Administrator services.
4. Ensure that the OpenManage Server Administrator inventory collector is working fine (Run `./invcol -outc=/home/inv.xml` from `/opt/dell/srvadmin/sbin/invcol` location)
5. Re-inventory the Linux server in OpenManage Essentials.
6. Now the Linux server will be either listed under **Compliant systems** or **Non-Compliant systems**.

Issue 30:

Description: An exception might be seen in the OpenManage Essentials Console, when a discovered virtual machine of a VMware Classic ESX server is selected from the **Unknown** node in the **All Devices** tree. [516274]

Issue 31:

Description: The RAC Console application launch point is available when SNMP protocol is used to discover the DRAC (Dell Remote Access Controller) devices. [515308]

Issue 32:

Description: To properly discover, inventory and classify a Dell EMC server running ESXi 5.0, you must install the OpenManage Offline Bundle and VIB 6.5 A02 available at support.dell.com. For more information, see delltechcenter.com/ome.

Issue 33:

Description: When you create a custom group, you have the ability to select a pre-defined device search query or the ability to select individual devices and groups to form your newly created custom group.

If you select a device search query as your basis for your custom group content and you subsequently decide to modify the device search query, the results of the modified device search query is not reflected in the custom group. You will have to delete the custom group and recreate it using the newly modified device search query group.

If you create a custom group using a device search query, you subsequently modify the device search query and then attempt to edit the custom group that used the device search query in question, the original device search query group gets deleted. So, once you create a custom group based on a device search query, do not edit it. If you need to modify it, delete it first and then re-create it.

Issue 34:

Description: When a PowerConnect 8100 series switch is discovered, the MAC address associated with the management IP in the **NIC Information** table will be displayed as **N/A** in OpenManage Essentials.

Issue 35:

Description: Discovery and Inventory of servers that have virtual network adapters are not displayed in the **NIC Information** table of the server. This occurs when discovering and inventorying Microsoft Windows servers with SNMP, WMI, or both along with Hyper-V role configured with virtual networks adapters.

Resolution: OpenManage Essentials displays only the IP of the network adapter it was discovered on. If it is a virtual network adapter, it displays **Host NIC Adapter**. OpenManage Essentials displays only the physical network adapters in the **NIC Information** table of the server.

Issue 36:

Description: When discovering and inventorying 12G servers using SNMP, there may be some instances where the device is removed from the device tree and replaced with another 12G server. This issue is known to occur with the initial release of the iDRAC7 firmware 1.06.06.

Resolution: It is recommended that the iDRAC7 firmware is updated to version 1.20.20 or later.

Issue 37:

Description: If you import more than 1,500 discovery ranges (each range can have one or more IP addresses) using the Discovery **import CSV** feature, the first time you navigate to the **Manage | Discovery and Inventory** page, you may see a delay of 10-15 seconds until the page loads. After that, subsequent visits to that page will load normally.

Resolution: Do one of the following:

1. Allow the console to complete loading for up to 15 seconds.
2. Do not import individual IP addresses, instead import the IP ranges.

Issue 38:

Description: While discovering ESXi 5.0 and ESXi 5.0 U1 using WS-Man you may observe that the discovery task may take about 6 minutes. This issue is due to the enhanced information OpenManage Essentials is gathering from the ESXi 5 host and the increased storage and software calls being sent to the OMSA ESXi 5 VIB.

Resolution: Do one of the following:

1. Perform discovery and inventory of ESXi 5 when the servers are not busy.
2. Review the *Performance and Scalability white paper* at delltechcenter.com/ome for other recommendations.

Issue 39:

Description: When OpenManage Essentials is used to discover and inventory devices of the same category having same name (for example, servers) in different subnets (for example, my_server), then

- The device tree displays the information of the device that was discovered last.
- The device information portal (Details tab) displays the merged data from all devices.

Resolution:

1. Ensure that the correct FQDN is defined for each target device.
2. Set the UI discovery to use the DNS for name resolution.
3. Go to C:\Program Files (x86)\Dell\SysMgt\Essentials\configuration or the path where OpenManage Essentials is installed.
4. Open the **dconfig.ini** file, and add the following under **[DISCOVERY_PARAM]: NAME_CORRELATION_MODE=value**

The possible values are:

- 0 = Default (OpenManage Essentials works as described in this issue).
- 1 = Matches device names based on the name resolution method set in the UI.

- 2 = Matches device names based on the name resolution method set in the UI, but also uses the alternate name if it gives a more optimal match. Setting the NAME_CORRELATION_MODE to 2 helps when you do not want a preferred name resolution method for correlation.

Issue 40:

Description: When a Dell EMC Compellent device discovered using the management IP (virtual IP) address or master controller IP address is rediscovered using a non-master controller IP address, the management IP (virtual IP) address will not be displayed in the NIC Information report. [30191]

Issue 41:

Description: The Service Tag may not be populated in OpenManage Essentials for devices with certain firmware versions. The device list may also display multiple entries for these devices if the hostname of these devices are changed. [29823]

Resolution: To ensure that the Service Tag is populated, upgrade the firmware of the managed nodes to the latest version.

Issue 42:

Description: When a Dell client device such as Dell OptiPlex, Dell Latitude, or Dell Precision with OMCI 8.x installed is discovered using the WMI protocol, the Agents table in device details page displayed the OMCI version as N/A. [16891]

Issue 43:

Description: When a XenServer is discovered using SSH, the MAC address is not displayed in the same column for the IP address.

Issue 44:

Description: HA Clusters can be discovered using SNMP only. The discovery task that is intended to discover HA Clusters must have SNMP enabled and the associated credentials must be correct for the target devices.

In order for the members to be discovered, the IP address of each cluster member must be included in the list of addresses to be discovered by the discovery task.

When discovering HA Clusters, the cluster name may replace the name of the active cluster node. To avoid this, do not include the cluster IP address in the discovery range.

If the cluster IP address is the only IP address in the discovery task that is related to the HA Cluster, the currently active cluster node will be discovered and its name will be the same as that of the cluster itself. This results in the cluster name appearing in several places under the All Devices organizational view.

Another option which helps with cluster discovery is setting the name resolution to NetBIOS instead of DNS names and running the discovery.

Issue 45:

Description: For Dell EMC PowerEdge servers discovered using out-of-band method, the system uptime displayed in OpenManage Essentials may not match with the actual system uptime. [51626]

Issue 46:

Description: OpenManage Essentials may not display the appropriate version in the inventory for OpenManage Storage Services (OMSS) version 8.0.2. [51149]

Issue 47:

Description: After replacing a server (source) with another server (target) from a compute pool, if the operating system IP address is discovered again, drill-down of the IP address on the **Discovery and Inventory** page displays both the source and target servers. [61513]

Resolution: Delete both the servers and then discover the servers again.

Issue 48:

Description: In OpenManage Essentials version 2.2, when the iDRAC and the server with the iDRAC are correlated:

- Deleting the discovery range of the iDRAC removes the iDRAC details in the **NIC Information** table of the server. However, the iDRAC is not removed from the device tree.
- Deleting the discovery range of the server removes the server details in the **NIC Information** table of the iDRAC. However, the server is not removed from the device tree. [61985]

Issue 49:

Description: For EqualLogic PS4210 storage arrays with EqualLogic firmware version 8.0.4, the **Application Launch** option is disabled. [62421]

Issue 50:

Description: When a server is discovered with the SNMP protocol, the RAC name of the server is not displayed in the device tree, portals, and wizards. [64443]

Resolution: Ensure that the iDRAC of the server is discovered with the WS-Man protocol. Otherwise, the system name is displayed in the device tree, portals, and wizards instead of the RAC name.

Issue 51:

Description: The location of a server is not displayed in the **Device Summary** table when the server is discovered out-of-band with either the WS-Man or SNMP protocol. [62819]

Resolution: The location of the server is displayed in the **Device Summary** table only if the server has OMSA installed and is discovered in-band. If the server is discovered out-of-band with either the WS-Man or SNMP protocol, the device location is displayed only in the **Data Center Location Information** table.

Issue 52:

Description: The Service Tag is not displayed for the PowerEdge FN IOAs that were manufactured prior to February 1, 2016. [63831]

Issue 53:

Description: For PowerEdge chassis, the **Enclosure Slot Information** table displays a slot as available, even though the slot may be occupied by quarter-width sleds. [65732]

Issue 54:

Description: For Dell's 11th or earlier generation of PowerEdge blade servers, the NIC and NIC Port details are not displayed in the VLAN configuration inventory, if the blade servers are discovered out-of-band with SNMP protocol. [69306]

Issue 55:

Description: For PowerVault MD Series storage arrays that are daisy chained, the Service Tag may not be displayed or displayed incorrectly in the device inventory. [64070, 18069]

Issue 56:

Description: For a Dell 11th generation PowerEdge modular server having iDRAC firmware version 3.75 installed, the health status displayed in OpenManage Essentials may not match with health status displayed in the RAC console. [61951]

Issue 57:

Description: For PowerVault MD Series storage arrays that are daisy chained, the enclosure ID displayed in the OpenManage Essentials Firmware Information inventory does not match with the enclosure ID displayed in PowerVault Modular Disk Storage Manager if default Enclosure ID values are changed. [67086]

Issue 58:

Description: Thin provisioned virtual disks of a PowerVault MD 38xxi storage array are displayed with REPOSITORY NAME & current size and not the actual disk name & maximum size in the Virtual Disks inventory information. [42606]

Issue 59:

Description: For PowerVault MD 38xxi storage arrays, the health status displayed in OpenManage Essentials may not match with the health status displayed in PowerVault Modular Disk Storage Manager. [42607]

Issue 60:

Description: The Service Tag of a PowerVault MD 38xx Series storage array displayed in OpenManage Essentials does not match with the Service Tag displayed in PowerVault Modular Disk Storage Manager. [64059]

Issue 61:

Description: The power supply information displays zero watts during discovery of devices having ESXi 6.0 and 6.5 operating system without OMSA. [78535]

Resolution: Discover the iDRAC of the devices having ESXi 6.0 and 6.5 operating system, or install OMSA.

Issue 62:

Description: When discovered using Ws-MAN protocol, PowerEdge C6420 servers running with firmware version 3.15.15.15 are not classified under Modular Systems group in the device tree. [80935]

Issue 63:

Description: When Windows or Linux systems with OMSA 9.1.1 is discovered by using SNMP, the Inventory Collector Agent version is not displayed under Data Sources. [82928]

Issue 64:

Description: If the mode of the IOAs in a chassis is changed from Standalone or VLT to PMUX, the IOAs of a chassis are not discovered when using the Chassis (CMC) Discovery — All Components filter. [65026]

Resolution: Do one of the following:

- Update the SNMP Community string of the IOA in the corresponding CMC console.
- Discover the IOAs separately in OpenManage Essentials.

Issue 65:

Description: Sometimes, when a F/W & Driver Inventory Task is run from **System Update > Non-Inventoried Systems**, an error is displayed: Select at least one server. [84764]

Resolution: Rerun the F/W & Driver Inventory Task.

Alerts

OpenManage Essentials can receive and process alerts from systems with an IPv4 address format.

Issue 1:

Description: Some of the alerts received in OpenManage Essentials from Dell EMC Networking C-Series devices may not indicate the actual cause of error or problem on the device.

Issue 2:

Description: FluidFS alerts received from the controller or management member IP are not associated with the corresponding Dell EMC EqualLogic FS7500 NAS device. [39667]

Issue 3:

Description: If the intensity of an alert storm increases beyond 5 traps per second, it could take OpenManage Essentials several minutes to process all the alerts. New alerts that are received in the interim are not displayed on the console until all the alerts in the storm are processed.

Issue 4:

Description: Alert Actions: Application Launch alert actions do not show the application in interactive mode if the Microsoft Windows **Interactive Service Detection** service is stopped. To see the applications, you have to start the service.

Issue 5:

Description: Alerts are not received when the **SNMP Trap** service is stopped and started. To resolve the issue, restart the **DSM Essentials Network Monitor** service.

Issue 6:

Description: For large number of alerts, two auto refreshes are required to show the total alerts and count on the home page. If the alert count is large, the first refresh fetches and shows only a subset of alerts. The second refresh displays the entire list.

Issue 7:

Description: If you edited sample alert actions in OpenManage Essentials version 1.0, you must manually clone them before migration. Those will get overwritten with default sample actions.

Issue 8:

Description: The test trap from PowerVault MD 32xx/32xxi is received in OpenManage Essentials system with IP 0.0.0.0. This is an expected behavior in OpenManage Essentials and any other trap listener.

Issue 9:

Description: While upgrading OpenManage Essentials from version 1.0.1 to 1.2 or above, all the existing Dell EMC Force10 traps are deleted because OpenManage Essentials version 1.2 installs the tested and verified Dell EMC Force10 trap definitions. Also, the Dell EMC Force10 traps from the MIB Import Utility are also removed and the severity of the traps are set as defined in OpenManage Essentials version 1.2. After upgrading to OpenManage Essentials version 1.2, make sure that you update the associated Event view/action filters for these Dell EMC Force10 trap definitions, because the previous OpenManage Essentials version 1.0.1 event filters may not work after the upgrade.

Issue 10:

Description: When creating an alert action for an application launch, OpenManage Essentials system path variables which contain % signs are not supported. Examples of unsupported variables are: %WINDIR%, %SystemRoot%, %APPDATA%, %HOMEPATH%, %PATH%, and so on.

Resolution: Avoid using the system path variables with % sign and use the full absolute path to the executable file.

Issue 11:

Description: SNMPv3 traps are received as "Unknown" alerts with severity for following CMC firmware versions: 5.20/5.21 (M1000E), 1.30/1.32 (FX2/FX2S), 2.20/2.22 (VRTX).

Remote tasks

- OpenManage Essentials supports iDRAC Service Module (iSM) deployment on servers running Community Enterprise Operating System (CentOS).

Issue 1:

Description: The task targets tree is not expandable when iDRAC Service Module Deployment task is opened in view mode. [51128]

Resolution: Open the corresponding task in edit mode to view the selected targets.

Issue 2:

Description: Target selection changes made to a remote task are applied to other remote tasks, if the tasks are created in quick succession. [49249]

Resolution: Right-click and delete the affected remote tasks, and re-create the required remote tasks.

Issue 3:

Description: While deploying iSM on servers running Linux with OMSA version 7.4 or earlier, the deployment task may display a success message, even though the task actually failed because of dependency issues. To confirm if the task was successful or failed, you can see the task details.[48523]

Issue 4:

Description: The iSM deployment task is unsuccessful when deploying iSM version 1.0 on a target device running Linux operating system.

Resolution: Ensure that the dependency packages/executables required for iSM deployment are installed on the target device, and then run the task again. For information on the dependency files, see the **Linux Install Dependency** section in the *iDRAC Service Module Version 1.0 Installation Guide* at www.dell.com/support/manuals. [47177]

Issue 5:

Description: After deployment of iSM by using a .rpm package, the iSM service (dsm_ism_srvmgrd) is not started. [43476]

Resolution: Start the iSM service manually on the server running Linux.

Issue 6:

Description: Only the OMSA web server component can be installed on a virtual machine. If you deploy the server administrator component using the OMSA Deploy Task on a virtual machine, the Task Status displays success. However, OMSA is not installed on the virtual machine. [26652]

Issue 7:

Description: If a user from the OmeAdministrators group executes a command that requires system Administrator privileges for tasks such as a command to stop a service, the task status is not displayed correctly. To view the correct status of the task, click the task under **Task Execution History**.

Issue 8:

Description: When OpenManage Essentials is installed with a remote database server, the database connection may be lost (due to local network failures, database server reboot, and so on). If this happens, the tasks may no longer run as scheduled. When observed, normal operation can be restored by restarting the OpenManage Essentials Windows services: **DSM Essentials Network Monitor** and **DSM Essentials Task Manager**. [498134]

Issue 9:

Description: Remote Server Administrator command line task may not respond for Server Administrator running on Microsoft Windows Server 2008 and Microsoft Windows Server 2008 R2.

To enable the successful functioning of remote Server Administrator CLI and software updates/deploy features, ensure the following (applicable to Microsoft Windows only):

- The managed system and the management station must be on the same domain or there should be a trust relationship between the two domains.
- If you have a Windows Firewall configured on the management station or the managed system, make the following configuration changes to enable remote Server Administrator CLI and software updates to work successfully.

Management Station:

1. Open TCP port 135.
2. Add the application **omremote.exe** (located in `Essentials\bin`) to the Firewall exception list.

Managed System:

- If you have the Windows firewall configured, enable remote administration by running the following command in the command prompt:

```
· "netsh firewall set service RemoteAdmin"
```

For more information on connecting through the Windows firewall, see *Microsoft's MSDN website* for **Platform SDK: Windows Management Instrumentation (Connecting through Windows Firewall)** at:

- [http://msdn.microsoft.com/en-us/library/aa389286\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx)
- <http://support.microsoft.com/kb/875605>

For Windows Server 2008 onwards, see the following link: [http://msdn.microsoft.com/en-us/library/aa822854\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx). [312918]

Issue 10:

Description: When creating or updating a task, the stamp for the creation or update time is that of the OpenManage Essentials UI. The **Last Run Time** displayed on the summary report, however, is the time of the Essentials Services system. If there is a significant variation in the UI and Services system time, it is possible that a scheduled task may not execute or show that it was executed before it was created. [137997]

Issue 11:

Description: If you set the task start or end time to a time in Daylight Saving Time (DST) shift period, OpenManage Essentials changes the task start or end time to the closest valid time. [165393]

Resolution: A workaround to eliminate the changing of start or end time is to set a valid start/end time.

Issue 12:

Description: By default, root login through SSH is not enabled on VMware ESX Servers. As a result, all the OpenManage Essentials tasks that use the root account fail. To enable the SSH root login on the ESX Server, set the option **PermitRootLogin=YES** in **/etc/ssh/sshd_conf** file. [174023]

Issue 13:

Description: The Server Administrator Deployment task requires dependent components (example libc++) to be installed on the target systems running the Linux operating system. If these components are not installed, the task fails with the following error message:

- omexec must be installed on the remote node for the task. See the help and ensure that the remote node requirements are met before executing the task.

Issue 14:

Description: If the **Log On** account of **DSM Essentials Task Manager** or **DSM Essentials Network Monitor** services is changed, the following user rights must be assigned for the **Log On** account:

- **Adjust memory quotas for a process**
- **Replace a process level token**

If the **Log On** account is missing the above user rights, the Essentials task fails to execute.

Resolution: To assign user rights to an account on the local computer:

1. From the **Start** menu, point to **Administrative Tools** and then click **Local Security Policy**.
2. In the **Local Security Settings** dialog box, double-click **Local Policies**, and then double-click **User Rights Assignment**.
3. In the details pane, double-click **Adjust memory quotas for a Process**.
4. Click **Add User or Group**, and in the **Enter the object names to select** box, type the user or group name to which you want to assign the user right and click **OK**.
5. Click **OK** again and double-click **Replace a process level token** in the **Details** pane.
6. Click **Add User or Group** and in the **Enter the object names to select** box, type the user or group name to which you want to assign the user right and click **OK**. [239550]

 **NOTE:** Changing Log On accounts of DA and Host Services is not supported. If changed, it will lead to errors. For these services, use Local System account for Log On.

Issue 15:

Description: While creating a **Generic Command Line** task, the **Application requires interaction with desktop** check box does not work and the executable window is not visible when Essentials is installed on the Microsoft Windows Server 2008 R2 system. The task runs the executable in the background. If Windows requires input, the task may hang and you may need to kill the process for the task to continue.

Issue 16:

Description: After successfully running the **Deploy Server Administrator** task on the Linux server, if discovery still classifies the server as **Unknown**, restart the Linux server and run the discovery again. The Linux server should start showing up under the device tree.

Issue 17:

Description: When trying to run a remote server administrator command against some Linux targets, the **Task Execution History** pane may show the task as complete even though, when the **Execution Details** pane is examined, the **Execution Summary** states: The task is not supported for the target device.

This occurs when the Dell OpenManage Server Administrator on the target devices does not properly report the information needed for OpenManage Essentials to determine if the Remote Server Administrator command can run on the system(s). This may mean that OMSA is not properly configured, is in an unknown state, or needs to be upgraded.

Issue 18:

Description: If you are a super-user on a system, and you do not have full permissions to this path: `~\InstallPath\SysMgt\Essentials\SystemUpdate\Packages`, you must give the super-user full access to that path before running the OM-Deploy task.

Issue 19:

Description: If a remote task is scheduled to run periodically and system time is changed to a future time, an exception may be seen in the console.

Resolution: To resolve this issue, disable all periodic tasks, stop the **DSM Essentials Task Manager** service, then change the system time. After time has been changed, start the **DSM Essentials Task Manager** service, and edit each period task schedule.

Issue 20:

Description: If the Remote task is running, it cannot be deleted from **Task Execution History** pane, though it can be deleted by right-clicking the task from **Task Tree** pane.

Issue 21:

Description: For Deploy Server Administrator Task, after the task is created, the task status may say **pending** while the task icon shows the **Task complete**. This means that the Deploy Server Administrator package i.e msi or msp has been downloaded successfully though the task execution is still pending. Once the task starts execution the 'task complete' icon will change accordingly.

Issue 22:

Description: For **Remote Task** and **System Update** multiple selections of task is not supported.

Issue 23:

Description: Even though a task is **Run Now** task, or if the task does not have a valid schedule associated with it, right-clicking the task in the left side task pane shows the **Activate Task Schedule** option. Though, activating the schedule will not do anything as there is no schedule associated with the task.

Issue 24:

Description: If you activate schedule for cloned sample tasks without adding targets, it may display a message for entering credentials for targets since the schedule cannot be activated without valid targets. To avoid this message, add valid targets for the cloned task before activating the task schedule

Issue 25:

Description: In view mode of the Task, you are able to see the Task Targets. You can also expand the tree to view sub-targets. Though, any selection made here is not saved, this has been made viewable so that you know all the targets associated with the task.

Issue 26:

Description: Sometimes when editing the remote task the target selection is not seen. To see the targets, cancel or close the edit window and re-edit the task to see the target selection.

Issue 27:

Description: Users can select the type of OpenManage Server Administrator packages depending on whether they want to perform an upgrade (major or minor) or clean install of OpenManage Server Administrator using OpenManage Essentials.

- Use .msi package for clean install /major upgrade/minor upgrade of OpenManage Server Administrator
- Use .msp package for minor upgrade
- Use .exe package for major/minor upgrade

Issue 28:

Description: OpenManage Server Administrator deployment on XenServer: OpenManage Server Administrator cannot be deployed on XenServer from OpenManage Essentials. OpenManage Server Administrator needs to be installed manually on the managed node. Dell OpenManage is available for XenServer as a Supplemental Pack. The supplemental pack can be downloaded from **support.dell.com**.

Issue 29:

Description: OpenManage Server Administrator deployment on ESXi server: OMSA cannot be deployed on ESXi server using OpenManage Essentials. For more information, see the *How to set up and configure ESXi 5 for use in OpenManage Essentials white paper* and the *Installing OpenManage Server Administrator on ESXi4 with OpenManage Essentials video* at **delltechcenter.com**.

Issue 30:

Description: To install OpenManage Server Administrator on a 64-bit Linux system, install the following 32-bit rpms and their dependent packages before running OpenManage Server Administrator Deploy task from OpenManage Essentials.

- compat-libstdc++-33.i686
- libxml2.i686
- pam.i686
- glibc.i686
- zlib.i686
- libgcc.i686

Issue 31:

Description: While creating an OpenManage Server Administrator update deployment task; the task may remain in the **In-progress** state for 6 hours. This occurs in certain scenarios where OpenManage Server Administrator was not properly uninstalled prior to running the update deployment task. This may also occur if the task was interrupted during the deployment process.

Resolution: Before running the update deployment task, make sure that OpenManage Server Administrator is uninstalled from the target server and then create an OpenManage Server Administrator deployment task.

Issue 32:

Description: Creating a Remote Server command task with the command `omreport system alertlog` may take longer than expected to complete. This occurs if the alert logged on the target system is unusually large, the task may fail to complete.

Resolution: Review the alert log on the system to determine if the log can be cleared.

Issue 33:

Description: When Server Administrator deployment task is performed on more than 20 Linux targets, the task may fail. This issue is due to the limitation on the number of simultaneous Server Administrator deployments task OpenManage Essentials is capable of.

Resolution: It is recommended to deploy Server Administrator on up to 20 targets with each task.

Issue 34:

Description: When creating a Command Line task and selecting Remote Server Administrator command for a Linux target using a command other than `omreport` and `omconfig`, the task status indicates the task as completed and displays a green status. This occurs because the Remote Server Administrator command supports `omreport` and `omconfig` commands.

Resolution: While creating a Remote Server Administrator command, make sure to use only `omreport` and `omconfig` commands for the task to return correct data. You can get the complete list of these commands at support.dell.com.

Issue 35:

Description: If you select an MSP package to update major versions of OpenManage Server Administrator, (for example, version 6.x to version 7.x) the task displays the status as successful and the details indicate that the software update is complete. However, you can notice that the update was never completed. This occurs because the MSP is only supported while updating minor versions. For example, 6.3 to 6.5 or 7.0 to 7.1. For more information about the valid packages that can be used to update OpenManage Server Administrator, see *OpenManage Server Administrator User's Guide* at dell.com/support/manuals.

Resolution: While updating major versions of OpenManage Server Administrator make sure that the MSI package is used.

Issue 36:

Description: The Deploy Server Administrator task runs forever.

Resolution: Make sure that the install arguments are valid for Deploy Server Administrator task. For more information about the Deploy Server Administrator task and install arguments refer to the *OpenManage Essentials User's Guide* or the *Deploy Server Administrator white paper* at http://en.community.dell.com/techcenter/extras/m/white_papers/20069180/download.aspx. If the arguments are invalid, stop the task and create a task with valid arguments.

Issue 37:

Description: If OpenManage Essentials is added to a domain, the Generic Command Line task fails when the username is provided as `localhost\.`

Resolution: Provide the username in one of the following formats:

`<Username>`

`<Hostname>\<Username>`

`.\<Username>`

`\<Username>`

Issue 38:

Description: The Sample — Linux OMSA Uninstall command line task does not support the uninstallation of OMSA version 6.1 or earlier. [30243]

Issue 39:

Description: The Total Targets in the Task Execution History retains the count of the previously executed targets and also the execution history. [29583]

Issue 40:

Description: OpenManage Essentials allow editing and rerun of OMSA deployment tasks. It is recommended that the editing and rerun options are selected only for tasks that have finished execution. [29525]

Issue 41:

Description: After the successful execution of the Sample — Windows OMSA Uninstall command line task, no details are displayed in the Task Execution History. [30535]

Issue 42:

Description: The Schedule View calendar allows you to select a date prior to the current date for launching the task creation wizard. OpenManage Essentials validates the date only during the task creation, and displays an error message if the task is scheduled on a date prior to the current date. [27551]

Issue 43:

Description: The Sample — Windows OMSA Uninstall and Sample — Linux OMSA Uninstall command line tasks do not verify if OMSA is installed on the target. After execution of the task, the Task Status displays Successful, even if OMSA is not installed on the target system. [30244, 30533]

Issue 44:

Description: When using a single OMSA deploy task on multiple targets, if one or more task targets are not updated, OpenManage Essentials displays `The task was cancelled for the target device`. The Task Execution History displays the `Stop` status.

Resolution: Rerun the task:

1. In the **Task Execution History**, right-click the task and click **Edit**.
2. Deselect all the targets that were successfully updated.
3. Provide the credentials and click Finish. [16585]

Issue 45:

Description: An existing remote task may be replaced by a newly created remote task. [31534]

Resolution: Restart the DSM Essentials Task Manager service.

Issue 46:

Description: Deploying OpenManage Server Administrator (OMSA) as a sudo user does not work on a system running SLES 11.

Resolution: Ensure that the directory for the sudo user exists in the `/home` directory on SLES 11, and then deploy OMSA. If the directory does not exist under `/home`, create the sudo user using the `useradd -m` option. The `-m` option ensures that the directory for the sudo user is created in `/home` directory.

Issue 47:

Description: If a device group is selected as a task target, the task runs on all devices in the group, including devices that were added to the group after the task creation. [55466]

Resolution: Before the task runs, edit the task and ensure that the task target only includes the required devices.

Issue 48:

Description: While accessing OpenManage Essentials remotely as an `OMESiteAdministrator`, creating a remote task displays an insufficient permission error. [61746]

Resolution: Close the web browser and open OpenManage Essentials again.

Issue 49:

Description: The **Task Target** page does not display all device groups for the `OMESiteAdministrator`. [61821]

Issue 50:

Description: A cloned task may not display all the task targets immediately after the task is cloned. [55462]

Resolution: Wait until the cloned task is displayed in both the **Remote Tasks** tree and the **Remote Tasks** grid, and then verify the task targets.

Configuration management

Issue 1:

Description: The device configuration **Inventory** and **Compliance** tabs in the **Devices Portal** display inventory and compliance information only after the corresponding tab is manually refreshed. [48567]

Issue 2:

Description: For device configuration inventory tasks, the **Task Execution History** displays the user who ran the task as System. [48738]

Issue 3:

Description: If a device on which a configuration template was deployed, is deleted and then rediscovered, the last template deployed on the device is not displayed in the **Repurpose and Bare Metal Devices** tab.

Issue 4:

Description: Auto deployment tasks created in OpenManage Essentials version 2.0 do not run successfully after upgrade to version 2.0.1 or version 2.2. [61955]

Resolution: Recreate the auto deployment task after the upgrade.

Issue 5:

Description: When CMC deployment fails on the target chassis (firmware M1000e 5.x, VRTX 2.x, FX2/FX2s 1.x) due to invalid or unsupported values in the template attributes, the status is displayed as "Unknown" instead of "Failed" in the **Task Execution History** window under **Details** tab. [75135]

Resolution: See the description in task details to determine the issue.

Issue 6:

Description: If the deployment template is captured from a server with configurations like DELL PERC S130/S140 with Single Disk based volumes, then the deployment of those templates on the target devices fail with "RAID Level not supported" error. [77419]

Resolution: The deployment of single disk-based volumes is not supported by iDRAC server configuration feature. After deploying the template, manually configure the single disk-based volumes using PERC configuration utility.

Issue 7:

Description: When the create template task is modified, junk characters are displayed in the template name which has non-English characters. [79180]

Resolution: Avoid using non-English characters in the template name. If the template name has non-English characters, then edit the template name in the edit wizard to remove them.

Issue 8:

Description: Compliance report is not generated when a configuration baseline is associated with more than 500 devices and is timed out after an interval of 30 minutes. [81748]

Resolution: As a workaround, associate the baseline with 500 devices at a time. For generating compliance report for more than 500 devices, clone the existing baseline and separately associate the other set of 500 devices.

Issue 9:

Description: After creating a system profile template from a server and setting TFTP as an option in the ShareType attribute of the AutoUpdate section, or setting TFTP as an option in the AutoUpdate section in iDRAC and exporting the profile template, the deployment of the template in both the scenarios always fails on any target server. [81956]

Issue 10:

Description: The Quick Deploy Settings cannot be configured for MX7000 Chassis by using the MX Chassis configuration template. [83592]

Issue 11:

Description: While deploying a MX Chassis configuration template, the device specific attributes are not listed under the **Edit Attributes > Device Specific Attributes** tab in the Deployment wizard. [83469]

Issue 12:

Description: If you associate devices with a different configuration baseline while the Make Device(s) Complaint task is running, the latest baseline is considered by the task for remediation of these devices.

Issue 13:

Description: When a remediation task is run for a noncomplaint MX7000 chassis which differs in the Power Cap value with the associated compliance baseline, and with Power Capping disabled, the task completes successfully. However, the device remains noncompliant as the Power Cap value will not be remediated by OpenManage Essentials. [84766]

Resolution: You must change the Power Cap value with Power Capping enabled on the chassis.

Issue 14:

Description: The compliance chart for individual device groups display incorrect data when **Enable Downgrades** is selected under **Advanced Settings** and the compliance of the groups are updated. [84767]

Resolution: Click the **Summary** tab and click the noncompliant section.

Issue 15:

Description: When a REST API is called to query noncompliant devices in a custom device group, incorrect noncompliance details are displayed if the devices are present in more than one custom group. [84801]

Issue 16:

Description: If the SNMP alert destinations are not configured in MX7000 chassis, in OpenManage Essentials, drop-down list is not available for the SNMP version attribute under **Attributes > SNMPAlerts** for MX7000 chassis configuration baselines and templates. [84844]

Resolution: Manually configure the SNMP version—SNMPV1 or SNMPV2 in MX7000 chassis templates and baselines.

Issue 17:

Description: When you import a device configuration template or baseline, the previously selected attributes before exporting the template or baseline are not retained.

Resolution: Before deploying the imported configuration template or baseline, manually select or clear the attributes from the template.

Issue 18:

Description: Device configuration templates that are captured from a server with BOSS-S1 AHCI controller connected displays invalid values of stripe size and LUN size under the **AHCI** attributes section. Do not edit the attributes of the template, and deploy the template as-is. [84888]

Issue 19:

Description: In OpenManage Essentials version 2.5, the server, chassis and MX chassis configuration baselines and templates will not group the new attributes introduced in newer firmware versions of iDRAC, Chassis Management Controller and OpenManage Enterprise —Modular. [141855]

Issue 20:

Description: When an MX7000 chassis is configured with a non-default web server port, the chassis configuration template creation and deployment will fail in OpenManage Essentials version 2.5. [142466]

Resolution: Configure the MX7000 chassis with default web server port and create the chassis configuration template and redeploy the template.

Issue 21:

Description: For 14th generation of PowerEdge servers with iDRAC firmware versions 3.30.30.30 and later, creating server configuration templates and baselines will fail. [144250]

Resolution: Configure deployment file share for 14th generation of PowerEdge servers with iDRAC firmware versions 3.30.30.30 and later.

Security

To prevent security issues due to cross frame scripting (XFS) in Internet Explorer, you must disable web frames across different domains:

1. Click **Tools > Internet Options**.
2. Click **Security**.
3. Under **Select a zone to view or change security settings**, select **Local intranet**.
4. Under **Security level for this zone**, click **Custom** level.
5. Under **Miscellaneous > Navigate windows and frames across domains**, select either **Prompt** or **Disable**.

Reports

Issue 1:

Description: In the Agent and Alert Summary report, if the devices are filtered by any Group other than **All Devices**, the **Agent Summary** table does not display the correct information. [49510]

Resolution:

Issue 2:

Description: **Device Name** is a default field and is present in all reports. [134260]

Issue 3:

Description: The time displayed in the reports generated by Essentials and the **Device Summary/Details** page are in the time zone corresponding to the management station. [75603]

Issue 4:

Description: Software Components report does not show entries for ESXi servers.

Issue 5:

Description: To populate **Modular enclosure reports**, CMC should have firmware version 4.0 and above.

Issue 6:

Description: Windows Server 2008 R2 and Windows 7 will not let you add the **Administrators and Users** group to the **OmeUsers** and **OmeAdministrators** groups using computer management. If you want to add the **Administrators and Users** group use the command prompt or delete the OME groups to have them reset.

Command to list your local groups: `net localgroup`

Command to add Users to OmeUsers: `net localgroup "OmeUsers" Users /add`

Command to add Administrators to OmeAdministrators: `net localgroup "OmeAdministrators" Administrators /add`

Command line interface

Issue 1:

Description: OpenManage Essentials Command Line Interface (CLI) functionality will not work when a non-default Console Launch port is used for installing OpenManage Essentials. If you want to use the CLI functionality, make sure that the default Console Launch port 2607 is used during installation.

Issue 2:

Description: OpenManage Essentials CLI does not support deleting nested custom groups. While deleting a child custom group using CLI, OpenManage Essentials deletes the parent custom group as well. You can delete the child custom group using the right-click option in the GUI.

Issue 3:

Description: On management systems with TLS 1.1 and TLS 1.2 enabled, OpenManage Essentials CLI-based commands fail with an exception error: "An error occurred while receiving the HTTP response". [84922]

Resolution: Set registry settings to allow .Net framework to use highest security protocol for communication. See docs.microsoft.com/en-us/dotnet/framework/network-programming/tls.

Miscellaneous

Issue 1:

Description: SupportAssist version 1.3 is not compliant with the Federal Information Processing Standard (FIPS). [40254]

Issue 2:

Description: If the system locale is set to English (India), clicking the **Help** icon in OpenManage Essentials displays an error.

Resolution: Copy the help file folder and rename it. For example, copy the EN-US help file folder and rename it as EN-IN.

Issue 3:

Description: If the system locale setting does not match with any of the following, clicking the **Help** icon in the Troubleshooting Tool displays an error:

- English (United States)
- German (Germany)
- Spanish (Spain)
- French (France)
- Japanese (Japan)
- Chinese (Simplified, PRC)

Issue 4:

Description: OpenManage Essentials does not display the Controller Information, Enclosure Information, and Physical Disk Information for Dell Compellent devices with firmware version 6.4.1. However, this issue is not observed for Compellent devices with firmware version 6.3.

Issue 5:

Description: You may not get appropriate privileges in the OpenManage Essentials GUI if:

- You are part of an Active Directory group, which is in turn part of another group.
- You launch Server Administrator using the desktop icon and Single Sign-on is enabled. [167801]

Issue 6:

Description: If the CPU throttles, the following message is displayed in the Hardware System Event Log (SEL) with an unknown severity:

- System Board Power Optimized: Performance status sensor for System Board, unknown event. This would be displayed in the **Hardware Logs** tab when you select the system in the Devices view. [175331]

Issue 7:

Description: If after reboot, **DSM Essentials Network Monitor** or **DSM Essentials Task Manager** services do not start automatically, you have to manually start those.

Issue 8:

Description: The **Contact Information** for a device may display the firmware version instead of the technical support contact information.

Issue 9:

Description: Dell EMC Force10 devices display MAC address for ports that are not configured under **NIC Information** instead of **N/A**.

Issue 10:

Description: OpenManage Essentials may not display the correct warranty date and time of the device. It displays the warranty date and time based on:

- The warranty start time.
- The location of the managed server or the request originator.

Issue 11:

Description: The warranty information (including expired and renewed) displayed in OpenManage Essentials for a particular Service Tag, may not match with the warranty record displayed at **support.dell.com**. The service level code and model name of a warranty record displayed at **support.dell.com** may not exactly match with the OpenManage Essentials warranty report. [44410]

Issue 12:

Description: If OpenManage Essentials uses the WMI protocol to discover a server, the RAC information table is not displayed.

Issue 13:

Description: Warranty information will not be displayed for all devices that do not display the Service Tag in the OpenManage Essentials console.

Issue 14:

Description: OpenManage Essentials displays power supply health as Normal when a redundant power supply has lost AC power source.

Resolution: This is the issue with Server Administrator version 6.x. To avoid this issue, install/upgrade to Server Administrator version 7.0 or higher.

Issue 15:

Description: After the SNMP feature is installed on Windows Server 2008 R2 or Windows Server 2012, the Windows Event Viewer logs an Error with Source: SNMP and Event ID: 1500, under Windows Logs-> System. This SNMP error is also logged whenever the SNMP Service is started. This SNMP error has been determined not to have any influence on the operation of SNMP or the system, and can be ignored. For more information, see the *Microsoft knowledgebase article 200203* at **support.microsoft.com**. [28951]

Issue 16:

Description: On a domain controller (DC) or a system that is part of a domain, only **The Administrator** user can repair Essentials using the **Repair** option available in the Uninstall or change a program window. Domain Admins or Enterprise Admins cannot repair Essentials using the **Repair** option. However, they can repair Essentials by launching the Essentials installer, and then selecting the **Repair** option. [31061]

Issue 17:

Description: REST API call to Dell's 11th generation of PowerEdge servers discovered in OpenManage Essentials using SNMP protocol does not provide the System ID attribute. [61502]

Resolution: It is recommended to discover the iDRAC of the 11th generation PowerEdge server using WS-Man protocol.

Issue 18:

Description: During discovery and inventory of more than 1000 devices, navigating to **Schedule View** page displays the loading icon and later causes the browser to become unresponsive. [74346]

Resolution: It is recommended to wait till the **Schedule View** page loads completely.

Issue 19:

Description: The displayed model name of VxFlex Ready Nodes is incorrect on the Troubleshooting Tool when an IPMI protocol test is run. [83826]

Manage MIBs

The following are some of the MIB(s) that have been verified.

- ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB, rmon-mib, rfc1213, Accord-mibs,Entity-mib, If-mib, ripv2-mib, snmpv2-mib, ADTRAN-DS1-MIB, ADTRAN-MIB, AS-2000, WaveLAN-MIB, AILUXCONNECT-MIB, AISPY-MIB, HHMSAGENT-MIB, HHMSSMALL-MIB, ALCATEL-IND1-CHASSIS-MIB, BGP4-MIB (IETF_BGP4.mib), MTSALLSTREAM-MIB, ADMIN-AUTH-STATS-MIB, ALTIGA-GENERAL-STATS-MIB, ALTIGA-MIB, ALTIGA-VERSION-STATS-MIB, ACC-NC-ALARM-MIB, ACC-NOTIFICATION-MIB, ANDOVER-CONTROLS-MIB, APPIAN-LPORT-DS1-MIB, APPIAN-PPORT-SONET-TRAP-MIB, APPIAN-SYSTEM-MIB, FLOWMGREXT-MIB, BRIDGEEXT-MIB, IPV4INTERFACE-MIB, BOOTEXT-MIB, ASANTE-HUB1012-MIB, ATI-MIB, NETSERVER-MIB, APPLTALK-PRIVATE-MIB, IPX, AXIS-MIB, BAS-TRAPS-MIB, BAS-PBRF-OSPF-MIB, BAS-CARD-INFO-MIB, BAS-CHASSIS-MIB, BESTPOWER-MIB, BIANCA-BOX-ISDN-MIB, BIANCA-BRICK-MIB, BLUEARC-SERVER-MIB, BLUEARC-TITAN-MIB, BASP-Config-MIB, BASP-Statistics-MIB, Brcm-BSAPTrap-MIB, Bull, cabletron-mib, CT-ELS10-27-MIB, CT-ELS10-MIB, CTRON-IGMP-MIB, CAIMIB, CA-W2KOS-MIB, CAYMAN-MIB, Fastpath-MIB, CHECKPOINT-MIB, SNMPv2-M2M-MIB, ATMPrivate-Mib, ChrComIfOpticsOMS-SNK-MIB, ChrComPmAtmATM-CELL-Day-MIB, ChrComPmEthETH-Day-MIB, ChrComPmSonetsSNT-PFE-Current-MIB, ChrComProtectionVpNextPeerSetVp-MIB, Citrix common mib, Mfagnet mib, COPPER-MOUNTAIN-NETWORKS-DSL-MIB, RBUC-MIB, CODAN-MIB, CODIMA-BUILTIN-CAP, CODIMA-EXPRESS-MIB, CODIMA-GLOBAL-REG, COM21-NMAPS-MIB, mau mib, OPTIMUX-MIB, CXR-CFIP-MIB, BASEBRDD_MIB-MIB, SanAppliance-MIB, DL5400-MIB (dl5400.mib), DL-NEW-DSX1-MIB, DL-SLA-MIB, DMTF-DMI-MIB, DMTF-LAN-ADAPTER-MIB, EFDATA-MIB, EFDATA-SPECTRACAST-DR5000-MIB, ECLAPBEXT-MIB, RFC1315-MIB, ENTERASYS-MAC-LOCKING-MIB, ENTERASYS-PWA-MIB, ENTERASYS-RADIUS-AUTH-CLIENT-ENCRYPT-MIB, EQUIPE-TRAP-MIB, EQUIPE-SYSTEM-MIB, EQUIPE-SONET-MIB, EQUIPE-ATM-MIB, EQUIPE-ACAC-MIB, ESSENTIAL-COMMUNICATIONS-GLOBAL-REG, ESSENTIAL-COMMUNICATIONS-HIPPI-SWITCH, ESSENTIAL-ODS-ESS2000-HIPPI-SWITCH-MIB, EXTREME-ENTITY-MIB, NETOPIA-MIB, fx8210-private, ESM-snmp (fibr_GigaHUB.mib), EDB-snmp (fibr_MultiHUB.mib, Hub-rptr-prvt (fibr_NM349_rptr.mib), Fore-Apsgroup-MIB, Fore-DSX3-Ext-MIB, Fore-PLCP-MIB, POWERHUB-ATM-MIB, FOUNDRY-CAR-MIB, FOUNDRY-SN-SW-L4-SWITCH-GROUP-MIB, FOUNDRY-SN-AGENT-MIB, FOUNDRY-SN-ROOT-MIB, GDSFrameRelay-MIB, HARMONIC-INC-NSG9000-MIB, HJ-PNNI-MIB, HUAWEI-LOAD-BACKUP-MIB, HUAWEINE80DEVICE-MIB, HW-IMAPV1NORTHBOUND-TRAP-MIB, Iana Charset mib, IanaIfType mib, INKTOMI-GLOBAL-REG, INTEL-ES480-MIB, INTEL-EXPRESS110-MIB, INTEL-GEN-MIB, PRAROUTERMIB, KBRIDGE-MIB, LC-ENTITY-MIB, LC-PHYSICAL-ENTITIES-MIB, ELSA-MIB, SMARTD-MIB, APPLIC-MIB, XSWITCH-MIB, LANPLEX-SYSTEMS-MIB-1-2-2 (lp.mib), LEFTHAND-NETWORKS-NUS-COMMON-NOTIFICATION-MIB, LEFTHAND-NETWORKS-GLOBAL-REG, LEFTHAND-NETWORKS-NUS-COMMON-CLUSTERING-MIB, LEFTHAND-NETWORKS-NUS-COMMON-DNS-MIB, LEFTHAND-NETWORKS-NUS-COMMON-SECURITY-MIB, LEFTHAND-NETWORKS-NUS-COMMON-STORAGE-MIB, LEFTHAND-NETWORKS-NUS-COMMON-STATUS-MIB, LEXMARK-PVT-MIB, LINKSYS-MODEL-MIB, LINKSYS-MIB, RAID-Adapter-MIB, SYMTRAP-MIB, LUMINOUS-PROVISIONING-MIB, LUMINOUS-ROUTING-MIB, LUMINOUS-SHELF-MIB, AVAYA-MPOA-MIB, DS3-MIB, ES-1000-MIB, ES1200-MIB, ED-1032-MIB, ED-5000-MIB, EF-6000-MIB, ES-1000-MIB, CXAsync-MIB, MICOM-NAC-MIB, MICOM-SYS-MIB, MICOM-MPANL-SIGNALING-MIB, MICOM-GCM-MIB, MICOM-4400-VOICE-NETWORK-MIB, MC2350-MIB, OSPF-TRAP-MIB, ISG-NSD-COMMON-TRAPS, ANTIVIRUS-MIB, NAI-MIB, TVD-MIB, CORE-MIB, MSCR-MIB, XYPLEX-SYSTEM-MIB, NBASE-G1-MIB, ALRM-01-PCALARMS-MIB, DGV_-01-PCMPEG-MIB, DOC_-01-PCTHERMAL-MIB, ISI_-01-PCINSERVICEINDICATOR-MIB, NETBOTZ-DEVICE-MIB, NETBOTZ-MIB, NETBOTZ-MIB, NETBOTZ-PRD-BOT-MIB, NETBOTZV2-MIB, NETCOR-MIB, LINK_PROBE-MIB, NSLDAP-MIB, NSMAIL-MIB,

NETSTAR-MIB, GRF-ATMP-MIB, CONTIVITY-TRAPS-V1-MIB, CONTIVITY-INFO-V1-MIB, ALTEON-ISD-PLATFORM-MIB, ALTEON-TRAP-MIB, CRMCONNECTION-MIB, CRMMISC-MIB, CRMPKGCONF-MIB, CRMPORTCONF-MIB, CRMSVC-MIB, CRMTRAFFICCOLLECTION-MIB, OKIDATA-MIB, LX-10-MIB, ORACLE-AGENT-MIB, ORACLE-ENTERPRISE-MANAGER-4-MIB, ORADB-MIB, ORAINTERCHANGE-MIB, ORALISTENER-MIB, ORANAMES-MIB, COSINE-GLOBAL-REG, PACKETEER-MIB (PACKETEER-MIB.mib), PACKETEER-RTM-MIB, ADSL-LINE-EXT-MIB, ADSL-LINE-MIB, DIAGNOSTICS-MIB, PBC-CMTS-MIB, PBC-ENT-MIB, PBC-GENERIC-MIB, PBC-KODIAK-M-G10-MIB, PENRIL-MIB, PERIPHONICS, PERIPHONICS-VRU-NETWORK-MIB, PICTURETEL-VCS-MIB, PICTURETEL-VCS-CONFIG-MIB, PICTURETEL-VCS-H320-MIB, PICTURETEL-VCS-H323-MIB, PICTURETEL-VCS-SYSSTAT-MIB, LSF-SNMP-MIB (LSF-AGENT-MIB)

The following MIB(s) that can be parsed to view the details, but cannot be imported. The trap details of these MIB(s) are already present in OpenManage Essentials.

- MIB-Dell-10900, DELL-SNMP-UPS-MIB, Printer-MIB, DELL-RAC-MIB, UPS-MIB, MIB-Dell-10892, MIB-Dell-10909, ArrayManager-MIB, CLARIION-MIB, DELL-ASF-MIB, DCS3RMT-MIB, StorageManagement-MIB, FluidFS-MIB, DELL-SHADOW-MIB, DellrPDU-MIB, INTEL-LAN-ADAPTERS-MIB, Dell-LAN-TRAP-MIB, MIB-Dell-CM,DS2-MIB, DellMDStorageArray, DELLPV132T-MIB, DELLPV136T-MIB, POWERCONNECT3024-MIB, SWITCHMGT-MIB, FCEOS-MIB, DELL-POWEREDGE-C-MIB, PowerConnect3248-MIB, PowerConnect5224-MIB, Brcm-BSAPTrap-MIB, BASP-Statistics-MIB, BASP-Config-MIB, ADIC-TAPE-LIBRARY-MIB, ADIC-MANAGEMENT-MIB, ADIC-INTELLIGENT-STORAGE-MIB, Brcm-adapterInfo-MIB, SW-MIB, ADIC-SANMGR-PROXY-MIB, Dell-Vendor-MIB, POWERCONNECT5012-MIB, POWERCONNECT3048-MIB, powerConnect4-MIB, SNMPv2-MIB, RAID-Adapter-MIB, EQLDISK-MIB, EQLMEMBER-MIB, IDRAC-MIB, DELL-AIM-MIB, MIB-Dell-OME, PowerCenter-MIB, FCMGMT-MIB, COMPELLENT-MIB, EXANET-MIB, DELL-MD-SS-06-MIB, DELL-STORAGE-SC-MIB, DELL-PV-SEM-MIB
- BRIDGE-MIB, NET-SNMP-MIB, ENTITY-MIB, PIM-MIB, PIM-BSR-MIB, PIM-STD-MIB, VRRP-MIB, DIAL-CONTROL-MIB, POWER-ETHERNET-MIB, OSPF-TRAP-MIB, SNMP-REPEATER-MIB, BCCUSTOM-OPR-MIB, BD-MIB, FA-EXT-MIB FASTPATH-BOXSERVICES-PRIVATE-MIB, FASTPATH-AUTHENTICATION-MANAGER-MIB, FASTPATH-CAPTIVE-PORTAL-MIB, FASTPATH-PORTSECURITY-PRIVATE-MIB, FASTPATH-INVENTORY-MIB, FASTPATH-LOGGING-MIB, FASTPATH-QOS-ACL-MIB, BGP4-MIB, IEEE8021-AS-MIB, DNOS-BGP-MIB, DNOS-MMRP-MIB, DNOS-MRP-MIB, DNOS-MSRP-MIB, DNOS-MVRP-MIB, DNOS-BOXSERVICES-PRIVATE-MIB, DNOS-AUTHENTICATION-MANAGER-MIB, DNOS-CAPTIVE-PORTAL-MIB, DNOS-PORTSECURITY-PRIVATE-MIB, DNOS-INVENTORY-MIB, DNOS-LOGGING-MIB, DNOS-QOS-ACL-MIB, GEN-MIB, RND-MIB, DS-MIB, PET-MIB, CIOMIB, CLARIION1-MIB, RMON-MIB, ED-1032-MIB, iDRAC-Server-MIB, DELLRCSG2-TRAP-MIB
- VMWARE-ROOT-MIB, VMWARE-VMKERNEL-MIB, VMWARE-ESX-MIB, VMWARE-ENV-MIB, VMWARE-CIMOM-MIB, VMWARE-VMINFO-MIB
- LINK-INCIDENT-MIB, HA-MIB, Brocade-TC, Brocade-REG-MIB, BROCADE-MAPS-MIB, FOUNDRY-SN-ROUTER-TRAP-MIB, FOUNDRY-SN-TRAP-MIB
- CISCO-IETF-ISIS-MIB, CISCO-IPMROUTE-MIB, CISCO-RHINO-MIB, CISCO-FLASH-MIB, CISCO-HSRP-MIB, CISCO-PROCESS-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-ENVMON-MIB, CISCO-CLUSTER-MIB, CISCO-PING-MIB, CISCO-SLB-MIB, CISCO-RF-MIB, CISCO-MAC-NOTIFICATION-MIB, CISCO-PAE-MIB, CISCO-L2-TUNNEL-CONFIG-MIB, CISCO-IF-EXTENSION-MIB, CISCO-PORT-SECURITY-MIB, CISCO-PORT-STORM-CONTROL-MIB, CISCO-POWER-ETHERNET-EXT-MIB, CISCO-SYSLOG-MIB, CISCO-RTTMON-MIB, CISCO-CONFIG-MAN-MIB, CISCO-VTP-MIB, CISCO-ERR-DISABLE-MIB, CISCO-ACCESS-ENVMON-MIB, CISCO-VLAN-MEMBERSHIP-MIB, CISCO-BULK-FILE-MIB, CISCO-ENTITY-SENSOR-MIB, CISCO-CONFIG-COPY-MIB
- JUNIPER-COLLECTOR-MIB, JUNIPER-CFGMGMT-MIB, JUNIPER-BFD-MIB, BGP4-V2-MIB-JUNIPER, BFD-STD-MIB, APS-MIB, OSPFV3-MIB-JUNIPER, MPLS-MIB, JUNIPER-VPN-MIB, JUNIPER-VIRTUALCHASSIS-MIB, JUNIPER-USER-AAA-MIB, JUNIPER-SYSLOG-MIB, JUNIPER-SP-MI, JUNIPER-SONET-MIB, JUNIPER-RMON-MIB, JUNIPER-PMon-MIB, JUNIPER-PING-MIB, JUNIPER-MPLS-LDP-MIB, JUNIPER-MIMSTP-MIB, JUNIPER-MIB, JUNIPER-LDP-MIB, JUNIPER-L2ALD-MIB, JUNIPER-JS-SCREENING-MIB, JUNIPER-JS-NAT-MIB, JUNIPER-JS-IDP-MIB, JUNIPER-JS-AUTH-MIB, JUNIPER-EVENT-MIB, JUNIPER-DFC-MIB
- F10-ISIS-MIB, FORCE10-BGP4-V2-MIB, F10-VIRTUAL-LINK-TRUNK-MIB, F10-CHASSIS-MIB FORCE10-COPY-CONFIG-MIB, FORCE10-SYSTEM-COMPONENT-MIB, F10-S-SERIES-CHASSIS-MIB FORCE10-MSTP-MIB, F10-LINK-AGGREGATION-MIB, DF10-DCB-MIB, F10-FIPSNOOPING-MIB, F10-M-SERIES-CHASSIS-MIB, F10-OPENFLOW-MIB
- SONICWALL-FIREWALL-TRAP-MIB
- WLSR-AP-MIB, WLSX-SWITCH-MIB, WLSX-TRAP-MIB, WLSX-WLAN-MIB
- LLDP-MIB, LLDP-V2-MIB, LLDP-EXT-MED-MIB, DVMRP-STD-MIB, MAU-MIB, DISMAN-TRACEROUTE-MIB, HC-ALARM-MIB, AI-AP-MIB

Issue 1:

Description: The following MIB(s) may not be parsed by the MIB Import Utility. You can verify if these MIB(s) compile properly with any standard MIB compiler tool.

- ORINOCO-MIB, AIBADGER-MIB, ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB, ALCATEL-IND1-STACK-MANAGER-MIB, MPLS-LDP-MIB, APTIS-TRAPS-MIB, APTIS-V2TRAPS-MIB, ASANTE-AH1012-MIB, SWITCH-VLAN-MIB, BEA-WEBLOGIC-MIB (BEA-WEBLOGIC-MIB.asn1.mib), Patrol, CAIOPSMIB, CAISECMIB, CAIUXOS, CA-NTOS-MIB, CASCADE-MIB, DHCP-MIB, COM21-HCXOC3-MIB, COM21-HCXTX-MIB, COM21-HCXTOP-MIB, COMPUTERM-COMMON-MIB, DMTF-SYSTEMS-MIB, SYMBIOSDMI20MIFDEFINITION-MIB, EICON-MIB-SERVER, EICON-MIB-PORT, EICON-MIB-CARD, EXTREME-CABLE-MIB, FUJITSU-EXTENDED-NONOS-AWN-MIB-V06, GANDALF-ENTERPRISE-MIB, XPRESS-MIB, INKTOMI-TS-MIB, INTELCORPORATIONBASEBOARD-MIB, ELSA-MIB, MERITAGE-MIB, SWITCHING-SYSTEMS-MIB, LUMINOUS-SYSTEM-MIB, LUMINOUS-TRAP-MIB, CXAsyncl-MIB, CXDDS-MIB, CXX25-MIB, CXLapBD-MIB, MICROSENS-CWDM8-MIB, FRX-MIB, NEWOAK-MIB, SQUID-MIB, OLIVETTI-MIB

NOTE: If you notice any errors while parsing the MIB file and the specific MIB line number is mentioned, fix the error in the MIB file and try again. Example: Parsing of MIBs that have special characters in the OBJECT-TYPE/TRAP-TYPE/NOTIFICATION-TYPE names may fail.

Issue 2:

Description: Re-importing does not remove traps that are already imported in OpenManage Essentials. Existing traps are updated (as long as the same EOID and Specific TrapId is present in the MIB) and new traps are added.

Issue 3:

Description: Removing a MIB does not remove the Event Category name from OpenManage Essentials. This is to support the following use case.

In following scenario category name is not removed:

- Import MIB **A** with the default category name **A**.
- Import another MIB **B** with the same category name selected for previous MIB **A**.
- Remove MIB **A**. Category Name **A** is not removed as it is used by MIB **B** traps. If you remove **B**, category **A** will still be present.

Issue 4:

Description: All the received traps (MIB imported trap definitions) in OpenManage Essentials are removed when you remove a specific MIB using the MIB Import Utility.

Example: Import a device **A** MIB having some traps definitions. After importing, assume OpenManage Essentials receives 10 traps from device **A**. If you remove the imported MIB from OpenManage Essentials, the 10 received traps in OpenManage Essentials are also removed.

Issue 5:

Description: **Search Unknown Traps** lists traps even after the trap is added using MIB Import Utility, as previous events received are still categorized in OpenManage Essentials as unknown.

Issue 6:

Description: The data displayed in the **Edit Trap(s)** grid is invalid if you delete or revert that same trap definitions and then navigate to the **Edit Trap** menu.

Issue 7:

Description: All the received traps (manually added trap definitions) in OpenManage Essentials are removed when you remove the specific trap definition using the **Delete Trap** functionality.

Issue 8:

Description: The data displayed in **Edited Trap(s) in OpenManage Essentials** indicates the original definition of the built-in traps that are edited using **Edit Trap** functionality.

Troubleshooting

Installation

- Ensure that the latest SQL server service packs are installed on the system. You can run the following command on the command prompt to verify the SQL version.
 - `sqlcmd -Q "print @@version"`
- For typical install, ensure that the current user has sysAdmin rights to the SQL Server. For custom install, ensure that the provided authentication credentials have sysAdmin rights.
- Try to use the custom install with different authentication methods if typical install fails.

- Collect the logs from the temp folder. Search for the latest MgmtSt_*.log and InstallUtil_Install.log files. Try to quickly analyze (if possible) InstallUtil_Install.log.

Launching OpenManage Essentials

- When an internet proxy server is configured on the system, the site must be added to the exception list to bypass the proxy. This should be configured with GPO's by a domain administrator.
- If you are using certificates, ensure that you use the domain certificates and those are added in IIS manager for the **DellSystemsEssentials** website.
- If you are viewing an unauthorized user message on the console, ensure that the user receiving the error has been added to the **omeAdministrators** or **omeUsers** Windows user groups.
- If shortcuts to launch OpenManage Essentials are not working, try to use the IP/hostname/localhost directly (replace XXXXXX) in the following URL to launch the Essentials.
 - **https://XXXXXX:2607/Web/Default.aspx**

Services

- Ensure that the OpenManage Essentials database is present and accessible by running the following command on the database server command prompt.
 - `sqlcmd -E -d OMEssentials -Q sqlcmd -E -d OMEssentials -Q "select * from sys.databases where name = 'OMEssentials'"`
- If the above command works, enable the logs using the `dconfig.ini` file and collect the logs from the specified folder location.

Issue:

Description: OpenManage Essentials services do not start automatically on the OME host if the Windows license is activated after a system reboot.

Resolution: If Windows is not activated, activate the Windows license, run Windows update and reboot the system. On inactivated systems, OpenManage Essentials services will not start up automatically. On such a system, the services must be restarted manually.

Protocol Specific Discovery Issues:

- Use Dell Troubleshooting Tool (gets installed with Essentials) to verify the specific protocol test.
- Ensure that the services are working, and protocol-specific ports are not blocked by the firewall.
- Manually restart the services.

Microsoft Internet Explorer

Issue:

Description:

- Unable to open OpenManage Essentials using Internet Explorer.
- Internet Explorer displays certificate errors.
- Internet Explorer displays a message to approve the certificate.
- Unable to browse the file system to deploy Server Administrator and system update.
- Unable to display the Device tree for devices.
- Unable to install active components.

Resolution:

1. Open OpenManage Essentials on the client server using Internet Explorer.
2. Click **Tools > Internet Options > Security**.
3. Enter **Local Intranet** and click **Sites**.
4. Click **Advanced**.
5. Enter the fully qualified name of the server where OpenManage Essentials is installed.
6. Click **Add**.

If the issue persists, there may be an issue with the DNS server resolving the name of the OpenManage Essentials server. To resolve the DNS server issue:

1. Contact your system administrator and add the OpenManage Essentials system name added to the DNS server.

2. Edit your host file to resolve the IP of the OpenManage Essentials server. The host file is located at %windir%\System32\drivers\etc\hosts.
3. Add the IP of the OpenManage Essentials server to the Local intranet sites in Internet Explorer.

NOTE: You cannot remove the certificate errors unless you use the fully qualified name of the OpenManage Essentials server.

If a certificate error is displayed:

- Contact your system administrator to add the OpenManage Essentials certificate published to the **Trusted Root Certificate Authorities** and **Trusted Publishers** on domain systems.
- Add the OpenManage Essentials certificate manually to your **Trusted Root Certificate Authorities** and **Trusted Publishers** certificate stores using Internet Explorer.

Exporting data from a grid in OpenManage Essentials using Internet Explorer 10: Under certain circumstances, when you attempt to export data from OpenManage Essentials by right-clicking and selecting the **Export** menu item from any grid control, if you select the `.csv` format, the exported data is actually saved in `html` format, even though the file generated is a `.csv` suffixed file. This behavior seems to be related to the security settings associated with Internet Explorer 10. If you reset the security settings to the default set, this behavior is no longer observable. [31647]

Limitations

- The server configuration template created using OpenManage Essentials may not include some of the RAID encryption attributes that are available in the configuration template that is generated using the `winRM` and `RACADM` commands. [47566]
- During upgrade of SupportAssist, you must uninstall Dell System E-Support Tool (DSET) version 3.3 to continue. Upgrade from DSET version 3.3 to version 3.4.1 is not possible. [46490]
- Windows Server 2012 and Windows Server 2012 R2 in a virtualization environment are only classified as **Servers** and not under **Microsoft Virtualization Servers** group.
- If you are launching OpenManage Essentials installer from an UNC/shared path, you will not be able to install prerequisites from the **OpenManage Essentials Prerequisites** window. You must copy the installer files to the system or mount the shared folder path to assign a drive to it.
- Alert Actions: Application Launch alert actions will not show the application in interactive mode if the Microsoft Window's **Interactive Service Detection** service is stopped. To see the applications, you have to start the service. Disadvantage is, each time action is executed, you would be prompted with an **Interactive Service Detection** dialog box pop-up.
- A 32-bit system with OpenManage Essentials may display an error message while applying system updates using iDRAC. To resolve this issue, make sure that you update the version of Windows Remote Management (WinRM) currently installed on the system to version 2.0 using the Windows updates.
- If you are unable to schedule system update tasks using iDRAC, check your credentials and access rights. You must have Administrator rights to update a system using iDRAC.
- For Dell EqualLogic devices, the model information is displayed as N/A in the **Details** tab. [30478]
- The **Warranty notification scoreboard** icon does not appear in the OpenManage Essentials heading banner until the browser is refreshed. [30126]
- For Dell PowerEdge M I/O Aggregator, the **Application Launch** option does not open the web console. [31059]
- Multiple simultaneous logins are not supported in OpenManage Essentials version 1.2 and above. Multiple users cannot log in using the **Sign in as Different User** feature on the same browser. [31131, 31132]
- The health status of disks displayed in the iDRAC7 console does not match with the health status of disks displayed in the OMSA console. [31383]
- On a domain controller only domain administrators are automatically added to **OmeAdministrators** and **OmeUsers** roles. Enterprise administrators must be manually added to the OpenManage Essentials roles. [31506]
- When running OpenManage Essentials using the Google Chrome browser, even if **Preferences > Console Settings > Security Settings (ActiveX)** are enabled in OpenManage Essentials:
 - The MIB Import Utility cannot be launched from the **Extensions** tab.
 - The remote desktop cannot be launched using the **Application Launch > Open Remote Desktop** option. [40290]
- When an HP iLO server is discovered with the IPMI protocol, the firmware name and type are displayed as Remote Access Controller in the Firmware Information table. [64315]
- When the VLAN configuration inventory of a chassis that has multiple IOAs is exported, the exported file does not contain the name, model, and status of all IOAs. [70374]

Installation

Prerequisites

Recommended minimum hardware configuration for OpenManage Essentials:

Small (up to 100 Managed Systems):

- Processor: 2 cores (1.8 GHz minimum)
- Memory (RAM): 6 GB
- Disk Space: at least 10 GB
- Database: SQL Server Express
- Database location: Local
- Database size: 1 GB

Medium (up to 500 Managed Systems):

- Processor: 4 cores (1.8 GHz minimum)
- Memory (RAM): 6 GB
- Disk Space: at least 10 GB
- Database: SQL Server Express
- Database location: Local
- Database size: 2 GB

Large (up to 2000 Managed Systems):

- Processor: 8 cores (1.8 GHz minimum)
- Memory (RAM): 8 GB
- Disk Space: at least 10 GB
- Database: SQL Server Enterprise or Standard
- Database location: Supports Remote SQL installation
- Database size: 6 GB

Large (up to 5500 Managed Systems):

- Processor: 8 cores (1.8 GHz minimum)
- Memory (RAM): 8 GB
- Disk Space: at least 20 GB
- Database: SQL Server Enterprise or Standard
- Database location: Supports Remote SQL installation
- Database size: 10 GB

Large (up to 8000 Managed Systems):

- Processor: 16 cores (1.8 GHz minimum)
- Memory (RAM): 16 GB
- Disk Space: at least 30 GB
- Database: SQL Server Enterprise or Standard
- Database location: Supports Remote SQL installation
- Database size: 14 GB

NOTE: The recommended minimum hardware requirements for OpenManage Essentials on a domain controller are 8 GB RAM, 8 cores processor, and a remote database.

NOTE: When accessing the OpenManage Essentials console via a remote browser, you will experience better performance in the console user interface by using a (remote) system that has a well-equipped processor. For small and medium configurations, a system with an Intel multi-core processor or equivalent is typically sufficient. For larger configurations, an Intel i3 (or better) processor or equivalent is recommended. The RAM and graphic capability of the system will not affect the performance as much as the processor. A virtual machine may also be used for launching OpenManage Essentials remotely. As with a physical system, a virtual machine with a better equipped processor will provide better performance in the remote console.

NOTE:

- The disk space needed may increase based on the:
 - Number of Dell Update Packages you import for software update.
 - Number of MSI files you import for software deployment.
- If SupportAssist Enterprise is installed along with OpenManage Essentials, you require 2 GB RAM, Dual core processors in addition to the minimum requirements described in the above table. If you are using SQL Server Standard or Enterprise Editions, the maximum SQL Server memory must be configured within SQL Server to prevent it from using the entire system memory. It is recommended that you use a maximum of 4 GB for a 6 GB RAM configuration.
- For large number of managed systems, see the *Dell EMC OpenManage Essentials User's Guide*.

Operating system

- Microsoft Windows Server 2016 Standard and Datacenter Editions
- Microsoft Windows Server 2012 R2 Standard and Datacenter Editions
- Microsoft Windows Server 2012 Standard and Enterprise Editions
- Microsoft Windows Server 2008 R2 SP1 Standard and Enterprise Editions

NOTE: OpenManage Essentials is supported only on 64-bit operating systems.

NOTE: The Wow64 component is required to run on a 64-bit operating system.

NOTE: OpenManage Essentials is also supported on virtual machines.

NOTE: Ensure that KB2919355 update is installed on Windows 2012 R2 systems to run OpenManage Essentials 2.5. To install KB2919355 update manually, see the Microsoft Knowledge Base article ID 2919355 at www.support.microsoft.com.

Database-Microsoft SQL Server–Local or Remote

NOTE: Only case-insensitive instance of SQL Server is supported. It is recommended that you install the latest SQL Server Service pack.

- Microsoft SQL Server 2016 Standard, Enterprise, and Express Editions
- SQL Server 2014 Standard, Enterprise, and Express Editions
- SQL Server 2012 Standard, Enterprise, and Express Editions
- SQL Server 2008 R2 SP1 Standard, Enterprise, and Express Editions

NOTE: If you choose to install OpenManage Essentials on a local database, Microsoft SQL Server 2014 SP2 Express edition is installed on the system. For large deployments, you must use SQL Standard.

NOTE: While installing OpenManage Essentials on a local database, ensure that Microsoft SQL Server Express editions are configured with 'SQLEXPRESSOME' named instance. For more information about the local database instances supported, see the *Installing OpenManage Essentials* technical white paper on the Dell TechCenter.

NOTE: Both 32-bit and 64-bit versions of Microsoft SQL Server are supported. However, it is recommended to use a 64-bit version of Microsoft SQL Server.

NOTE: OpenManage Essentials database does not support the 'Always On Availability Groups' feature of Microsoft SQL Servers.

Other minimum requirements

Many of these applications can be installed from the prerequisites window.

- Microsoft Internet Explorer 10 and 11; Mozilla Firefox 50 and 51
- IIS 7.x/8
- Microsoft SilverLight 5.1.50907
- Microsoft .NET Framework 4.6.2
- Microsoft ASP.NET

- Dell OpenManage DRAC Tools
- Dell OpenManage IPMI Utilities
- Microsoft Visual C++ 2015 Runtime 14.0

Additional software required to run some features of OpenManage Essentials: For Dell EMC storage arrays inventory, ensure that your array is FLARE(R) version 19 or above. You must also install Navisphere(R) Secure CLI (version 19 or above) on your management station.

NOTE: This CLI software is part of the OpenManage Essentials installer media and can be installed from the prerequisites window.

Installation instructions

First-time Installation of OpenManage Essentials version 2.5:

- See the *Dell EMC OpenManage Essentials Version 2.5 User's Guide* for instructions on setting up OpenManage Essentials for the first time on a system.

Migrating IT Assistant to OpenManage Essentials:

- Direct migration from IT Assistant to OpenManage Essentials version 2.5 is not supported. However, you can migrate IT Assistant to an earlier version of OpenManage Essentials (version 1.3), and then upgrade to OpenManage Essentials version 2.5.
- For information about migrating IT Assistant to an earlier version of OpenManage Essentials, see the appropriate *Dell EMC OpenManage Essentials User's Guide* at www.dell.com/support/manuals.

NOTE: The OpenManage Install dialog box displays a notification if the latest version of OpenManage Essentials or SupportAssist Enterprise is already installed on the system. For Dell EMC Repository Manager and Dell EMC License Manager, this notification may not be displayed, even if the latest versions are already installed. [28109]

Upgrade

See the *Dell EMC OpenManage Essentials Version 2.5 User's Guide* for instructions on upgrading to OpenManage Essentials version 2.5.

Uninstallation

NOTE: Before uninstalling OpenManage Essentials, you must uninstall Dell EMC OpenManage Essentials MIB Import Utility and Dell EMC SupportAssist Enterprise (if installed).

1. Click **Start > Control Panel > Programs and Features**.
2. In Uninstall or change a program, select **Dell EMC OpenManage Essentials** and click **Uninstall**.
3. In the message *Are you sure you want to uninstall OpenManage Essentials?*, click **Yes**.
4. In the message *Uninstalling OpenManage Essentials removes the OpenManage Essentials database. Do you want to retain the database?*, click **Yes** to retain the database, or click **No** to remove it.

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. Visit www.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 page.
4. Select the appropriate service or support link based on your need.

