Dell OpenManage Essentials
Version 1.0

Release Notes
Dell 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, Essentials can increase system uptime, reduce repetitive tasks, and prevent interruption in critical business operations.

**Hardware and Software Requirements**

**Recommended Minimum Hardware Configuration for Essentials**

Small (up to 500 Managed Systems):

- Processor: 2 - 4 cores (1.8 GHz minimum)
- Memory: 4 GB
- Disk Space: at least 4 GB

Large (500+ Managed Systems):

- Processor: 4 or more cores (1.8 GHz minimum)
- Memory: 6 GB
- Disk Space: as much as 10 GB

**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

**Operating System (Standard and Enterprise Editions)**

- Microsoft Windows 2008 Server R2
- Microsoft Windows 2008 Server R2 SP1
- Microsoft Windows 2008 Server (x86/x64)

**NOTE:** Essentials is a 32 bit application and therefore requires the Wow64 component to be enabled on R2/x64 bit Operating System.

**Database (Microsoft SQL Server - Local or Remote)**

- SQL Server 2008 Express R2 SP1 (Bundled with Essentials Installer media).

Also supports:

- SQL Server 2005 Express SP3/SP4
- SQL Server 2005 SP3/SP4
- SQL Server 2008 SP1
- SQL Server 2008 R2

**Notes:**

- It is recommended that you install the latest SQL Server Service pack. SQL Server 2005 SP2 and lower are not supported.
- OME Supports 32 bit and 64 bit SQL Server. 64 bit is recommended.

**Other Minimum Requirement (Many of these can be installed from the prerequisites window)**
Internet Explorer 7, Internet Explorer 8, Internet Explorer 9 (32 bit instances)
- IIS 7.x
- Microsoft SilverLight 4.0
- Microsoft .Net Framework 3.5 SP1
- Microsoft ASP.NET
- Dell OpenManage DRAC Tools
- Dell OpenManage IPMI Utilities

Additional Software Required to Run Some Features of Essentials

- For Dell/EMC storage arrays inventory, ensure that your array is FLARE(R) version 19 or above. You should also install Navisphere(R) Secure CLI (version 19 or above) on your management station.

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

Installation

(A) First-time Installation of Essentials 1.0

See the Dell OpenManage Essentials Version 1.0 User's Guide for instructions on setting up Essentials for the first time on a system.

(B) Upgrade from IT Assistant 8.x to Essentials 1.0

IT Assistant 8.x can be upgraded to Essentials 1.0. IT Assistant user data will be consumed during upgrade. After upgrade IT Assistant will be removed from the system.

The followings data/tasks are not migrated during the upgrade to Essentials:

1) System Update: Essentials provides new functionality on the System Update (Software Repository), and OpenManage Server Administrator deployment so your existing packages and tasks in ITA will not be migrated to Essentials after upgrade. You have to reimport those packages and re-create those tasks.

2) Performance and Power Monitoring Tasks: Essentials 1.0 does not provide Performance and Power monitoring.

NOTE: If you used the CIM protocol before an upgrade, then after an upgrade, it is important to verify the CIM credentials. CIM credentials should be qualified with a domain or local host if no trusted domain is configured (for example, domain\administrator or local host\administrator). You can view the CIM credentials by editing the imported discovery ranges in the "CIM Configuration Pane." If the CIM credentials are not qualified with a domain or local host, devices are not discovered through the CIM protocol.

Prerequisites

For more information on Operating system, Browser & Consoles, and Minimum Hardware Configuration see the Dell Systems Software Support Matrix on support.dell.com/manuals

Operating System (Standard and Enterprise Editions)

- Microsoft Windows 2008 Server R2
- Microsoft Windows 2008 Server R2 SP1
- Microsoft Windows 2008 Server (x86/x64)
NOTE: Essentials is a 32 bit application and therefore requires the Wow64 component to be enabled on R2/x64 bit Operating System.

Database (Microsoft SQL Server - Local or Remote)

- SQL Server 2008 Express R2 SP1 (Bundled with Essentials Installer media).

Also supports:
- SQL Server 2005 Express SP3/SP4
- SQL Server 2005 SP3/SP4
- SQL Server 2008 SP1
- SQL Server 2008 R2

Notes:
- It is recommended that you install the latest SQL Server Service pack. SQL Server 2005 SP2 and lower are not supported.
- OME Supports 32 bit and 64 bit SQL Server. 64 bit is recommended.

Other Minimum Requirement (Many of these can be installed from the prerequisites window)
- Internet Explorer 7, Internet Explorer 8, Internet Explorer 9 (32 bit instances)
- IIS 7.x
- Microsoft SilverLight 4.0
- Microsoft .Net Framework 3.5 SP1
- Microsoft ASP.Net
- Dell OpenManage DRAC Tools
- Dell OpenManage IPMI Utilities

Additional Software Required to Run Some Features of Essentials

- For Dell/EMC storage arrays inventory, ensure that your array is FLARE(R) version 19 or above. You should also install Navisphere(R) Secure CLI (version 19 or above) on your management station.

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

Recommended Minimum Hardware Configuration for Essentials

Small (up to 500 Managed Systems):
- Processor: 2 - 4 cores (1.8 GHz minimum)
- Memory: 4 GB
- Disk Space: at least 4 GB

Large (500+ Managed Systems):
- Processor: 4 or more cores (1.8 GHz minimum)
- Memory: 6 GB
- Disk Space: as much as 10 GB
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

Open Issues and Resolutions

System Updates

NOTE: Essentials does not support the software update task on the management station itself. This is because the Software Update task is interrupted and the final results of the update will not be known. You can perform software updates using the other Dell Tools.

- In rare cases, inapplicable package may be listed in compliance report but the update are not be applied to target node if the package is not applicable.
- Intel PCI-E driver package information for a server seen in OME might be different than driver package information seen in SUU. Package name, Component name, Current Version and Repository Version might be different.[473495]
- Broadcom NetXtreme driver package information for a Server seen in OME might be different than driver package information seen in SUU. Package name, Component name, Current Version and Repository Version might be different.[473493]

Resolution:

- Before creating an update task for the Non-Compliant systems it is recommended that you Update to the latest catalog from ftp.dell.com by clicking the “Get the latest” button under the System Update tab. Ensure that you have Internet connectivity to get the latest catalog.

For systems with a Trusted Computing Group (TCG) 1.2-compliant Trusted Platform Module (TPM) chip, software updates for BIOS fails 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 “support.dell.com” and on the appropriate media supplied by Dell.

For software updates for BIOS to function, perform the following steps:

- Enable the Microsoft Windows BitLocker Drive Encryption feature for information on disabling this feature, see the Microsoft documentation at “www.microsoft.com.”
- Update the BIOS.
- Re-start the system.
- Re-enable the Microsoft Windows BitLocker Drive Encryption feature.

You can use Essentials to view the TPM information in the Device Details page.
• If after successfully running the Software Update Task on Windows HyperV server, the server is still shown under "Non-Compliant" tab, wait for 30-45 minutes. The server should start showing under "Compliant" Tab.

• While updating PERC using Essentials two Firmware packages may show up for PERC 4e/Di RAID Controller if you use the 6.5 SUU DVD. You can use either package to update your PERC.

• To perform remote Linux software update, Essentials uses Plink for SSH communication. By default, Essentials passes your password as a command-line parameter to Plink.

  NOTE: This occurs only on the Essentials management station. Passwords are always encrypted when transferred to the managed system.

If passing passwords through the command line on the Essentials management station is of concern, you can configure the updates to use RSA keys instead of passwords. A blank password in Essentials will trigger SSH authentication using the RSA keys.

To create RSA keys, perform the following steps:

  NOTE: It is assumed that you are running an SSH2 server and are using the RSA2 keys.

1. Run PuTTYgen (or your preferred mechanism) for generating public/private key pairs. You can save your private keys (".ppk" files) to any location on your system. The following is a sample public key that you would put in a file that you create called "authorized_keys2 for RSA2 keys."

   ssh-rsa
   AAAAB3NzaC1yc2EAAAABJQAAAIEAxfMzTwS4Cwnua61h7kia9l3Hvl
   SeFIYPsZOryCMyuA++

   9mPRralEtKNkwdAPKqPnc2/JFHyaOu31j/fUgQqgM2Cswqdr7fuowjseVVPtUG
   5jzM1RwUAX/1K
   Hy1BM+jmkHMuNg0TrN/gUxcmIA0lHFaFNRJ+veM15upJsk= rsa-key-20050209

Linux ships with other utilities for creating public/private key pairs. You can download PuTTYgen from the following Web address: "http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html"

The public keys are saved in the following configuration file on the Linux system.

   ~/.ssh/authorized_keys2

2. Create this file, if it is not present.

3. You can store the private keys in the directory of your choice. For security reasons, it is recommended that you set the appropriate permissions for your private key files. This is a sample "sshconfig.pro" file where you can configure the names and location of your private keys:

   #server[.user]=<path-to-file>
   #A server-name of global would be appropriate to accommodate a network where all or most systems are set up using the same key.
   #global[.user]=<path-to-file>
   global.root=C:\SSH Private Keys\root\global_root_privatekey.ppk
   global.fred=C:\SSH Private Keys\fred\global_fred_privatekey.ppk
   192.168.157.149.root=C:\SSH Private Keys\root\system1_root_privatekey.ppk
4. Copy "sshconfig.pro" to the bin folder of Essentials. By default, this folder is located at:
"C:\Program Files\Dell\SysMgt\Essentials\bin directory"

NOTE: A blank password in Essentials triggers SSH authentication using the RSA keys instead of using passwords. Essentials then attempts to find the entry in the "sshconfig.pro" file. If Essentials finds the system and user or global key in "sshconfig.pro", it uses the " .ppk" file for establishing an SSH connection to the server. However, if Essentials cannot find this information, it assumes that you meant to enter a blank password.

It is recommended that you use SSH version 2 or above be used on the managed system for better security.

For more information on the usage of public keys for SSH authentication, see
"http://www.tartarus.org/~simon/puttydoc/Chapter8.html"

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

- After installing Essentials, if you reinstall the database application (which is used by Essentials) the Essentials database will be detached from the database application.

- If you are installing Essentials using "Administrators" group user, and UAC is enabled, Prerequisites installer window is blocked after the reboot. You have to allow setup to proceed with rest of the prerequisites installation using the System tray icon.

- If using prerequisites link, SQL Server 2008 R2 SP1 is not installing on the specific OS version and service pack, verify the SQL Server 2008 R2 SP1 support matrix. You need Windows Server 2008 x86 (SP2) to install SQL Server 2008 R2 SP1.

- When OME is used to install SQL Server Express OME must be installed by the same user. Other users are not given the 'sysadmin' role by OME for SQL Server Express. The easiest way for a user to fix this is to uninstall SQL Server Express and try again. The user can also be added using 'sqlcmd.exe' command line interface.

- 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 Catalog
  - Server Administrator Deployment for Windows
  - Server Administrator Deployment for Linux

- While migrating tasks from ITA to OME, all the 'Run Now' tasks are migrated as disabled.
• While migrating tasks from ITA to OME, if 'Run Once' tasks have 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 ITA installation using local database to OME using remote database is not supported.

---

**Discovery and Inventory**

• The processor count in 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 reports physical processors, and the systems discovered using CIM reports logical processors.

• When the name resolution on an IP address to a host name fails using DNS, 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]

• 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 'RACDevice' table. [134365]

• 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:

  1. On Linux systems, adapters may be named differently between Essentials and Server Administrator. For example, Essentials may report a NIC adapter as 'eth0,' while Server Administrator shows the actual manufacturer name of the NIC.

  2. If more than one NIC card is not configured with an IP address, Essentials may show only one of the cards with an IP address of 0.0.0.0.

  3. Essentials may not report disabled NIC adapters.

• While performing discovery, if a device is discovered using "host name," and if its IP Address changes at a later time, 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. A workaround to eliminate duplicate device is to delete the device with the old IP address. [148069]

• The choice of protocols specified for discovering and managing the devices can result in varying levels of manageability. For instance, if you choose to manage devices in your network using only WMI, the devices with only SNMP agent (example DRAC) are classified under the "Unknown" group and consequently, you may not get application launch (example RAC console) functionality for the device. To avoid such issues, make a careful choice of the protocols while configuring discovery ranges, keeping in mind the devices (and protocols supported by agents running on those devices) that you are going to manage. [153729]

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

• If you are managing a Dell/EMC storage array, note that you need to 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 Essentials. If you enter both SPs in the discovery range, only one SP will be displayed in the device tree.

• 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 on the device tree. [78710]
• 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]

• 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]

• If user manually changes the hostname of the server which has already been discovered in Essentials, then duplicate entries appear in the device list corresponding to the IP address of the device whose hostname has been changed. The new hostname also corresponds to same IP address and the duplicate entry of the earlier hostname is not automatically deleted. Essentials displays both the new and the old hostnames.[247879]

• 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 continue 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]

• 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 "Power Supply Information" section. To display the correct information, discover the server with either SNMP, or both SNMP and CIM protocols. [300080]

• Even after performing inventory on the discovered Linux servers 'N' number of times, the Linux servers are still listed under Non-Inventoried systems'. To resolve this issue perform the following steps:

   For RHEL 5.5, SLES10, SLES11
   1. Mount OMSA6.5 dvd in the Linux server
   2. Install 'srvadmin-cm' rpm.
   3. Restart OMSA services.
   4. Ensure OMSA inventory collector is working fine
      (Run ./invcol -outc=/home/inv.xml from /opt/dell/srvadmin/sbin/invcol location)
   5. Reinventory the linux server in OME.
   6. Now your the Linux server will be either listed under 'Compliant systems' or 'Non-Compliant systems'.

• The RAC Console application launch point will not be available when SNMP protocol is used to discover the DRAC (Dell Remote Access Controller) devices.[515308]

• To properly discover, inventory and classify a Dell Server running ESXi 5.0 you must install OpenManage Offline Bundle and VIB 6.5 A02 from support.dell.com.

• Deleting large number of discovery ranges e.g. 1500, might result in 'Unhandled Error in the Application' error. To avoid this error, delete subset of ranges at a time.

--------------------------------------------------------------------------------
Alerts--------------------------------------------------------------------------------

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

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

• Alerts are not received when "SNMP services" are stopped and started. To resolve this issue, restart the “DSM Essentials Network Monitor” service.

• For large number of alerts, two auto refreshes are required to show the total alerts & 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.

• In Alert Filter window once some values are entered in the text box, to remove the values use 'Clear Filter' button. Using 'Backspace' or 'Delete' key to remove the text can result in clearing all the Alerts in UI.

---

Remote Tasks

---

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

• 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://support.microsoft.com/kb/875605"


• When creating or updating a task, the stamp for the creation or update time is that of the 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]

- If you set the task start or end time to a time in Daylight Saving Time (DST) shift period, Essentials changes the task start or end time to the closest valid time. A workaround to eliminate the changing of start or end time is to set a valid start/end time. [165393]

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

- 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." [175296]

- If "Log On" account of "DSM Essentials Task Manager" or "DSM Essentials Network Monitor" services are 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 tasks fails to execute.

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

From the "Start" menu, point to "Administrative Tools," and then click "Local Security Policy."

In the "Local Security Settings" dialog box, double-click "Local Policies", and then double-click "User Rights Assignment."

In the details pane, double-click "Adjust memory quotas for a Process."

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."

Click "Ok" again and double-click "Replace a process level token" in the "Details" pane.

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]

- When you launch Dell OpenManage Server Administrator for managed systems with Server Administrator agent only installations, a remote web server is used; you must provide the user name and password of the managed system. [390431]

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

- 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.
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 OME to determine if the Remote Server Administrator command can run on the system(s). This may mean OMSA is not properly configured, is in an unknown state, or needs to be upgraded.

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

If a remote task is scheduled to run periodically and system time is changed to the future time, exception may be seen in the console. To resolve this issue, disable all period 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.

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

In task device selection, device capabilities are not taken into account. Hence, if the target node is not capable of running the task, the task might fail.

Deploy Server Administrator task is not supported for Windows Server 2008 Core 64-bit operating system.

Deploy Server Administrator task might fail when run against multiple targets.

---------------------------------------------------------------
Security
---------------------------------------------------------------

---------------------------------------------------------------
Reports
---------------------------------------------------------------

“Device Name” is a default field and is present in all reports. [134260]

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]

Software Components report does not show entries for ESXi servers

---------------------------------------------------------------
Miscellaneous
---------------------------------------------------------------

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

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

If the CPU throttles, the following message in the Hardware System Event Log (SEL) is displayed 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]

- If after reboot, “DSM Essentials Network Monitor” or “DSM Essentials Task Manager” services are not up automatically, you have to manually start those.

Troubleshooting

-------------------------------

Install:

- Ensure 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 method 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:

- 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 seeing unauthorized messages on the console, ensure that the user with the error has been added to the “omeAdministrators” or “omeUsers” windows user groups.

- If shortcuts to launch the Essentials are not working, try to use the IP/hostname/localhost directly (replace XXXXXX) in the following URL to launch the Essentials.

Services:

- Ensure that the “OMEEssentials” database is present and accessible by running the following command on the database server command prompt.
  - sqlcmd -E -d OMEEssentials -Q sqlcmd -E -d OMEEssentials -Q "select * from sys.databases where name = 'OMEEssentials'"

- If the above command works, enable the logs using the dconfig.ini file and collect the logs from the specified folder location.

Protocol Specific Discovery Issues:

- Use Dell troubleshooting tool (gets installed with Essentials) to verify the specific protocol test.

- Ensure services are working, and protocol specific ports are not blocked by firewall.

- Manually restart the services
Miscellaneous:

- If OME is installed using domain user and if discovery/inventory fails after install, verify the domain controller is responsive, a slow domain controller might cause discovery/inventory to fail.

Known Limitations and Workarounds

- If you are launching Essentials installer from an UNC/shared path, you will not be able to install prerequisites from the Essentials Prerequisites window. You must copy the installer files to the system or mount the shared folder path to assign a drive to it.

Global Support

For information on technical support, visit www.dell.com/contactus.

For information on documentation support, visit support.dell.com/manuals. On the Manuals page, click Software ‒ Systems Management. Click the specific product on the right-side to access the documents.