

Software Change Management

Using Dell OpenManage IT Assistant

Dell™ OpenManage™ IT Assistant 7 enables organizations to significantly enhance management of the software life-cycle process, allowing administrators to inventory software asset information (BIOS, firmware, and drivers) in a centralized database; compare that asset information with a certified Dell Update Package or System Update Set; and schedule software updates for remote systems. This article outlines the IT Assistant 7 software change-management architecture and feature set.

BY SUDHIR SHETTY, STEVE HERACLEOUS, AND ROHIT SHARMA

Related Categories:

Asset management

Change management

Dell OpenManage

Dell PowerEdge servers

Inventory management

Systems management

Visit www.dell.com/powersolutions for the complete category index.

Dell OpenManage IT Assistant (ITA) 7 provides several key features that enable IT administrators to streamline management of the software life-cycle process. This feature set includes capabilities that enhance software inventory, software release management, compliance reporting, and software update processes. This article explains these features and provides step-by-step instructions for implementing software updates with ITA 7.

Figure 1 represents the Dell OpenManage IT Assistant change-management architecture. ITA requires the appropriate agent to be installed on the remote Dell PowerEdge™ server to enable the change-management infrastructure. The minimum supported agent is Dell OpenManage Server Administrator 2.0 (available on the Dell OpenManage 4.3 CD) running on a Microsoft® Windows® or Red Hat® Enterprise Linux® OS.

Software inventory

ITA collects software asset data from remote agents via Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI). This information is gathered from Dell OpenManage Server Administrator agents (version 4.3 or later) and centrally

stored in the ITA database. This capability enables administrators to run software inventory reports via either ITA or third-party enterprise reporting tools.

ITA collects the software inventory information during an inventory cycle scheduled by the network monitoring service. The inventory cycle can be scheduled within ITA. Alternatively, the inventory cycle can run on demand for a specific device or for a specific range.

Software release management

ITA enables administrators to view the Dell Update Packages and System Update Sets that reside on the Dell PowerEdge Updates CD, which is available as part of the Dell OpenManage Subscription Service. A System Update Set is a certified aggregate of Dell Update Packages that are specific to a hardware platform. Dell Update Packages are also available on the Dell support Web site at support.dell.com.

In ITA, administrators can open a software repository via the Software Updates View. To open the repository located on the Dell PowerEdge Updates CD, administrators should right-click on the Software Update Repositories node in the tree and select “Open Repository (Update CD).”

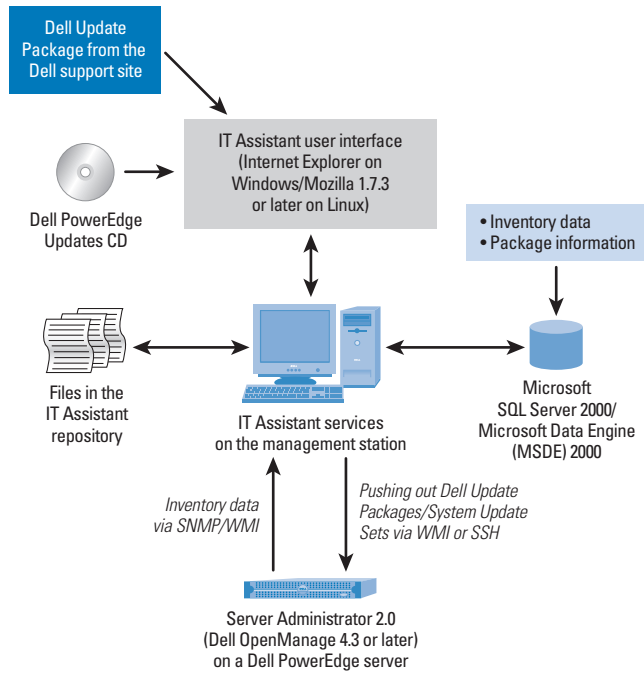


Figure 1. Overview of the IT Assistant change-management architecture

Administrators can then locate and select the catalog.xml file in the repository directory.

After the repository is opened, specific packages or System Update Sets can be imported into the ITA repository by right-clicking on those packages and selecting “Import.” Packages can also be added directly to the ITA repository by right-clicking on “IT Assistant Repository” in the tree and selecting “Add.” This operation can be used for Dell Update Packages that have been downloaded individually from the Dell support Web site.

Compliance reports

ITA compliance reporting enables administrators to compare the software inventory of remote systems with a Dell Update Package or a System Update Set. After the import process is complete, administrators can perform a compliance check and determine which components on the remote target device are not compliant with the Dell Update Package or System Update Set.

Figure 2 displays an example compliance report that has been executed with a Dell PowerEdge 2800 System Update Set. The compliance has been executed against all devices in the enterprise. Administrators can pick specific devices in the device tree for the compliance report, or they can run the report against devices that meet certain query criteria. A system also must meet the following prerequisites to be listed in the compliance report:

- Running the appropriate Server Administrator agent (Dell OpenManage 4.3 or later).
- Containing inventory data in the ITA database.

- Complying with the update criteria for the specified Dell Update Package or System Update Set. ITA uses the prerequisite information in the Dell Update Package or System Update Set to determine applicability to a particular remote target system. Only the PowerEdge 2800 servers will show up in the example compliance report shown in Figure 2.

In the example compliance report, the system named bransom2800 is compliant with the System Update Set. Green checkmark icons in the compliance report indicate that components have the correct versions of the BIOS, baseboard management controller (BMC) firmware, Intel® connection driver, and backplane firmware. Note that the compliance report will not list components that are not present on the system. Hence, even if the System Update Set has packages corresponding to Broadcom network interface card (NIC) drivers, these packages will not be listed in the compliance report if a Broadcom NIC is not installed in the target system. Figure 3 explains the icons that appear in a compliance report.

Software update process

ITA can schedule remote software updates by deploying packages via WMI to a Microsoft Windows-based system or via Secure Shell (SSH) to a Linux-based system. The Server Administrator agent at the remote system applies the packages and performs the necessary reboots, if required.

After a compliance report is generated as described in the preceding section, administrators can proceed with updating devices that are not compliant with the Dell Update Package or System Update Set. If a target device is selected in the compliance report, the Update button in that panel becomes enabled (see Figure 4). After pressing the Update button, the administrator is guided by the Task Creation Wizard to create a software update task.

The wizard-guided process is similar to the process for creating a software update task via the task panel in ITA (invoked by going

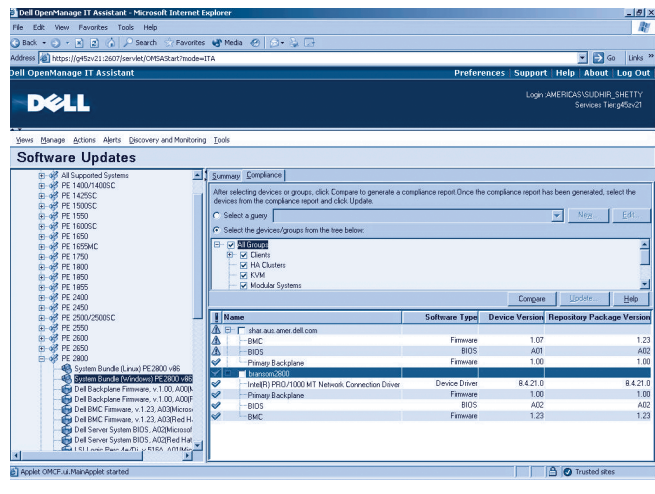


Figure 2. Example compliance report executed against all systems in an enterprise

Compliance report icons	
	The version of the software component on the remote target system is the same as the version of the component within the selected Dell Update Package or System Update Set
	The version of the software component on the remote target system is older than the version within the selected Dell Update Package or System Update Set and thus the component needs to be updated.
	The version of the software component on the remote target system is newer than the version within the selected Dell Update Package or System Update Set. (Note: These components will not be altered unless the administrator forces a downgrade or selects the re-apply option when creating the software update task.)
	The version of the software component on the remote target system does not meet the minimum prerequisites to be remotely updated via ITA. This typically occurs because the software component is too old or requires a floppy-based mechanism to perform the software update. In this scenario, the option to perform a remote software update is disabled for that system.
Task execution status icons	
	The update was successful.
	The target system must be rebooted for the update to take effect.
	The update task failed.
	The update task is in progress.
Individual package summary icons	
	The package applied successfully or was not applicable for this device.
	The package requires a reboot to take effect.
	The package failed to apply. To resolve this issue, administrators should try another method (such as a floppy-based image) to update this component.

Figure 3. Icon legend for Dell OpenManage IT Assistant 7

to Manage > Tasks on the menu bar). However, when creating a task via the task panel, administrators must select the specific Dell Update Package or System Update Set and also explicitly select the devices to be updated. To benefit from a compliance check before applying an update package, best practices recommend that administrators create update tasks using the Software Updates view.

Step 1: Create task

The first pane for creating a software update task enables administrators to enter a name and a description for the task. Context-sensitive help is available by clicking the Help button in each pane. If the administrator clicks the Cancel button, the task creation operation is canceled.

Step 2: Select options

The second pane for creating a software update task enables administrators to pick configuration options such as forcing a downgrade or re-apply, allowing a reboot, and generating a trusted key.

Force downgrade or re-apply. If applicable, this option will downgrade or re-apply the same version of the software package on the target device. If the component software on the target system is the same version or later of the package being

installed, the default behavior is that the component software will not be updated.

Allow reboot. This option enables the software update task to reboot the system if necessary. Otherwise, a message will be added to the task execution log, indicating that a reboot may be required for the update to be successfully applied.

Generate trusted key. For software updates on Linux target systems, ITA uses SSH to communicate with the remote Linux device. During the SSH connection, if the host key or device identifier is not recognized, then the SSH client software issues a warning. This warning may also be issued if administrators connect to a device for the first time. To trust the host key automatically and ignore the warning, administrators should enable this option. If working from within a company network and protected from the Internet by a firewall, administrator may choose to trust the host key without checking it.¹

Step 3: Select schedule

The third pane for creating a software update task enables administrators to schedule tasks at a specific time or on an hourly, daily, weekly, or monthly basis. For a software update task, administrators typically select the Run Now radio button to immediately execute the task, or they select “Run once” to pick the specific start date and time for running the task.

Step 4: Enter credentials

The fourth pane for creating a software update task enables administrators to specify the credentials required for task execution. Administrators must enter credentials that have administrative privileges on the target system. Windows OS user IDs should be specified as *domain\username* or *localhost\username*. On Linux target systems, the user ID is an administrative username for that system.

Step 5: Review task creation summary

Figure 5 displays the summary pane for the software update task, presenting pertinent information supplied during the task creation

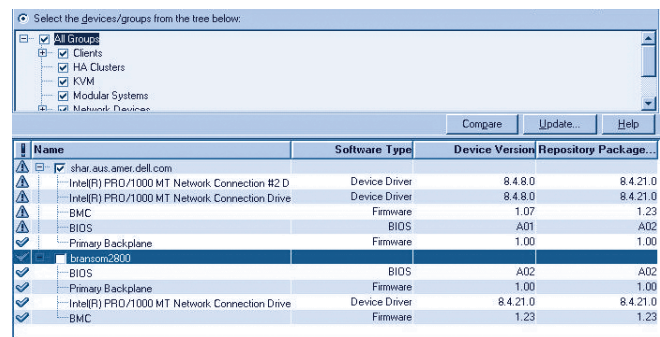


Figure 4. Software update task creation for a device listed in the compliance report

¹For additional information about configuring keys for SSH communication to a remote target Linux system, administrators should view the ITA readme.txt file in the IT Assistant folder of the installation directory.

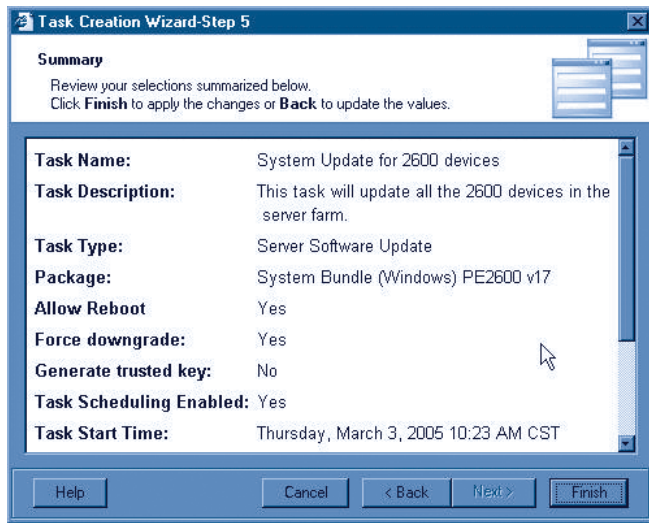


Figure 5. Summary of the task creation process

process. At this stage, administrators can cancel the task, use the Back button to update data that was entered in previous panes, or click the Finish button to complete the task creation process.

Task execution

Once the task creation process is completed, ITA will attempt to persist the task information in the database. Errors are reported to the administrator. If the task was successfully created, the administrator’s context is switched to the task panel and the summary information is displayed. The execution log can be viewed by clicking the Execution Log tab.

The task execution log provides detailed information about each run of a task. The bottom panel displays the overall task execution status for a particular target system as well as the individual execution log for each Dell Update Package in the System Update Set. The overall status is represented by the task execution icons explained in Figure 3.

Typically, a task will fail for one of the following reasons:

- **Improper credentials:** The credentials must have administrative privileges on the remote target system.
- **Networking problems:** ITA must be able to communicate with the remote target system. The troubleshooting tool can help diagnose network connectivity issues; the Ping Connectivity and CIM (Common Information Model) Connectivity tests can verify a successful connection to a target device.
- **Dell Update Package failures:** The detailed task execution log contains additional information about why an individual package failed to apply. The individual package summary icons are detailed in Figure 3.

Figure 6 describes additional troubleshooting issues.

Problem	Resolution
Administrator is unable to view the software inventory in the device details panel for a system in the device tree view.	<ul style="list-style-type: none"> • Verify that Server Administrator 2.0 (or later) is installed on the managed system. • Right-click on the device name in the device tree and select “Troubleshoot.” Run the SNMP Connectivity or CIM Connectivity test, and verify that the system is connected. Via SNMP, verify that ITA can successfully connect to the cminventorysnmp agent on the target device. • Right-click on the device name and select “Refresh Inventory” or “Perform Inventory Now” from the ranges view. Note that the agent can take up to five minutes to successfully inventory all the software on the device.
Compliance report for a Dell Update Package or System Update Set indicates that no devices can be updated by the selected package.	<ul style="list-style-type: none"> • Follow the preceding steps to help ensure that ITA can successfully retrieve the inventory for a specific system. • Note that the package contains prerequisite information that helps determine which PowerEdge systems or target operating systems can be updated. (For example, if the administrator is implementing a PowerEdge 2800 Linux System Update Set, devices will appear in the compliance report only if a PowerEdge 2800 server is running Red Hat Enterprise Linux within that environment.)
Software update task failed to execute and has an ❌ icon in the task execution log.	<ul style="list-style-type: none"> • View the task execution results to obtain a description of the failure. • View the detailed package log for more information about why the task execution failed.

Figure 6. Resolution of common troubleshooting issues

Effective change management using IT Assistant 7

Dell OpenManage IT Assistant 7 includes powerful features that are designed to enable administrators to streamline management of the enterprise software life-cycle process. ITA provides a centralized console for viewing software asset inventory, checking version compliance, and scheduling remote software updates. These capabilities allow administrators to keep their enterprises updated with the latest certified software and to manage distributed environments from a central console.

Sudhir Shetty works in the Dell Systems Management Consoles Group responsible for defining IT Assistant software functionality. He has an M.S. in Computer Science from The University of Texas at Austin.

Steve Heracleous works in the Dell Systems Management Consoles Group responsible for developing the IT Assistant user interface. He has a bachelor’s degree and a master’s degree in Electrical Engineering from The University of Texas at Austin.

Rohit Sharma is a test engineer in the Dell OpenManage software development and test organization. He has a bachelor’s degree in Computer Engineering from the University of Mumbai in India and a master’s degree in Computer Science from North Carolina State University.

FOR MORE INFORMATION

Dell OpenManage:
www.dell.com/openmanage