Symantec™ IT Management Suite 8.0 HF1 powered by Altiris™ technology Release Notes

Symantec™ IT Management Suite 8.0 HF1 powered by Altiris™ technology Release Notes

Documentation version: 8.0 HF1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

support.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

IT Management Suite 8.0 HF1 Release Notes

This document includes the following topics:

About IT Management Suite

IT Management Suite is a tool for managing corporate IT assets such as desktop computers, laptop computers and servers that have Windows, UNIX, Linux or Mac operating systems.

IT Management Suite is a collection of solutions and components that run on the Symantec Management Platform.

What's new in this release

In IT Management Suite 8.0 HF1, the following new features are introduced:

Table 1-1 New features

Feature	Description
Enhanced Help system.	In ITMS 8.0 HF1 Help system, enhancements in the user interface and improvements of the search process have been introduced. Also, localization is now supported for the standard ITMS locales.
OpenSSL is upgraded.	OpenSSL is upgraded to version 1.0.1s.
Improvements of the AD import user interface.	The following improvements of the AD import user interface are introduced: ■ The status of the AD import rules is added. ■ Different filtering and sorting options are added. ■ List of import rules now provides more information about each rule. For more information, see the Connect article.
The defer dialog box for the tasks is redesigned.	After you enable the **Allow the user to defer execution of this task** option in the Symantec Management Console, a defer dialog box is displayed on the client computer that allows the user to postpone the task. This defer dialog box is now redesigned. The redesign addresses multiple stability and usability issues.
New configuration option is added to the **Cleanup Task Data** task.	In the environment with high task load, the **Cleanup Task Data** task may remove the task instances of the recently executed tasks. As a result, some task instances might be missing and the summary information for that task may be incorrect. To avoid this problem, you can now enable the **Minimum time period to keep the task instances/summaries** option. If you enable this option, the **Clean-up Task Data** task will not remove the task records that are newer than the defined time period.
Support for RHEL 6.7	Symantec Management Agent and solution plug-ins can be installed on RHEL 6.7. For the list of supported solutions and limitations refer to the following article: http://www.symantec.com/docs/DOC9268
Support for SQL 2012 SP3	Starting from ITMS 8.0 HF1, SQL Server 2012 Service Pack 3 is supported.
New API-s added to the **ResourceModel** web service.	New API-s are added to the **ResourceModel** web service: **SaveDataClassLight**, **SaveDataClassRowsLight**.
Redirecting 7.6 Agents to 8.0 Notification Servers on Mac	On Mac computers, starting from ITMS 8.0 HF1, you can redirect 7.6 Agents that have no direct connection with Notification Server to 8.0 Notification Servers after an off-box upgrade. For more information about restoring Cloud-enabled Management communication on Mac computers after an off-box upgrade, see the *IT Management Suite 8.0 Installation and Upgrade Guide*: http://www.symantec.com/docs/DOC8650

Table 1-2 New features in Deployment Solution

Feature	Description
Enhanced Resource Import tool.	The Resource Import tool now lets you import an image as an external package to remote site servers. **Note:** Currently, the tool cannot cycle through different drives when there is no disk space.

System requirements and supported platforms

Before you install IT Management Suite 8.0 HF1, read the section Hardware recommendation in the *IT Management Suite 8.0 Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC8631

For information about the supported operating systems in Symantec Management Platform 8.0 and the IT Management Suite 8.0 solutions, see the article at the following URL:

http://www.symantec.com/docs/HOWTO9965

General installation and upgrade information

The installation of IT Management Suite (ITMS) 8.0 HF1 involves installation of Symantec Management Platform (SMP) 8.0 HF1 and solutions using Symantec Installation Manager.

For more information on how to install and configure the product, see the *Installing the IT Management Suite solutions* chapter in the *IT Management Suite Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC8650

Upgrade to IT Management Suite 8.0 HF1

After you install this hotfix (8.0 HF1), you cannot uninstall it or roll back to the previous version of ITMS. Therefore, install this Hotfix only if you require the fixes. If you decide to install ITMS 8.0 HF1 for Symantec Management Platform, you need to enable the Symantec Management Agent and remote Task Servers upgrade policies.

Note: To upgrade to the latest hotfix, log on to the Notification Server computer with the SMP application identity credentials.

In ITMS 8.0 HF1, Symantec Installation Manager (SIM) automatically creates a registry backup in the support folder before starting the installation, upgrade, or hotfix installation of SIM and ITMS solutions. The registry backup is available at the following location:

```
C:\Program Files\Altiris\Symantec Installation Manager\Support
```

If you encounter any errors because of missing registry entries or corrupted registry file, you can do one of the following:

- Restore the previous registry entries, and then run the installation or upgrade. To restore the previous registry entries, navigate to the registry backup, and then double-click the `AIMRoot.reg` file.
- Uninstall a solution, and then reinstall it, so that the registry entries are recreated. When you encounter the same error, repair the solution using SIM.
  For more information, see the following KB article:
  http://www.symantec.com/docs/TECH183086

For more information about creating a support package, see the following article:

http://www.symantec.com/docs/HOWTO93142

Upgrading Symantec Management Agent, site servers and solution level plug-ins

After you upgrade IT Management Suite from version 8.0 to this hotfix, upgrade the Symantec Management Agent, the site servers, and the solution plug-ins.

Table 1-3 Process to upgrade Symantec Management Agent, site servers and solution plug-ins

Step	Action	Description
Step 1	Upgrade the Symantec Management Agent on site servers.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the policies that upgrade the Symantec Management Agent on site servers.

Table 1-3 Process to upgrade Symantec Management Agent, site servers and solution plug-ins *(continued)*

Step	Action	Description
Step 2	Upgrade the site servers.	In the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins. To upgrade a remote task server, in the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings > Notification Server > Task Service > Advanced**, and then locate and turn on the upgrade policies for the remote task servers. To upgrade a remote package server, in the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings > Notification Server > Package Service > Advanced > Windows**, and then locate and turn on the **Windows Package Server Agent Upgrade** policy.
Step 3	Upgrade the Symantec Management Agent on client computers.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the policies that upgrade the Symantec Management Agent on client computers.
Step 4	Upgrade solution-specific agents and plug-ins.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the plug-in upgrade policies. To upgrade the solution-specific plug-ins to the latest version, do the following: ■ In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent. ■ In the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for the site server plug-ins. ■ In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the plug-in upgrade policies.

Symantec recommends that you configure a schedule for the upgrade policies. The default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. To speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

If the upgrade policy is set to **Run once ASAP**, the policy is rolled out just once.

You can also clone the upgrade policies instead of creating additional schedules.

http://www.symantec.com/docs/DOC8650

For more information on the post-upgrade tasks, see the chapter *Performing post-upgrade tasks* in the *IT Management Suite Installation and Upgrade Guide* at the following URL:

Enabling imaging after the upgrade in non-domain environment

In Deployment Solution 8.0 HF1, the basic authentication has been replaced with NTLM authentication for non-domain environment. For imaging to work, after the upgrade, you need to do the following:

To enable imaging

1. Run the Deployment Package Server Components – Upgrade policy.
2. Recreate all Windows and Linux preboot configurations.
3. Upgrade all the Windows and Linux automation folders on the client computers.

Post-upgrade versions of Symantec Management Agent and solution plug-ins

The Symantec Management Agent and its plug-in versions after you upgrade to ITMS 8.0 HF1 are as follows:

Table 1-4 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF1

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.0.2365	8.0.2315
Altiris Client Task Agent	8.0.2365	8.0.2315
Altiris Client Task Server Agent	8.0.2356	N/A
Altiris Base Task Handlers	8.0.2365	8.0.2315
Altiris Pluggable Protocols Architecture Agent	8.0.2354	N/A
Inventory Agent	8.0.2328	8.0.2259

Table 1-4 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF1 *(continued)*

Agent or plug-in	Windows	UNIX/Linux/Mac
Application Metering Agent	8.0.2328	N/A
Server Inventory Agent	8.0.2221	8.0.2221
Inventory Rule Agent	8.0.2365	8.0.2315
Monitor Plug-in	8.0.2326	8.0.2326
Package Server	8.0.2365	8.0.2315
Software Update Plug-in	8.0.2321	8.0.2229
Software Management Framework Agent	8.0.2365	8.0.2315
Software Management Solution Agent	8.0.2225	8.0.2225
Virtual Machine Management Task Handler	N/A	N/A
Deployment Task Server Handler	8.0.2396	N/A
Deployment Package Server	8.0.2396	N/A
Deployment Plug-in for Windows (x64/x86)	8.0.2396	N/A
Deployment Plug-in for Linux (x64)	N/A	8.0.2396
Deployment Plug-in for Linux (x86)	N/A	8.0.2396
Deployment Plug-in for Mac	N/A	8.0.2246
Deployment NBS plug-in	8.0.2396	N/A
Symantec Workspace Streaming Agent	7.6.0.180	N/A
Symantec Workspace Virtualization Agent	7.6.181	N/A
Symantec Virtual Composer	7.6.0.180	N/A

Performing post installation tasks for Deployment Solution

The following table lists the upgrade scenarios for which you must recreate the automation folders after you install the ITMS 8.0 HF1:

Table 1-5 Post installation tasks for Deployment Solution

Upgrade	Windows automation folder	Mac automation volume	Linux automation folder
Upgrade from 8.0 to 8.0 HF1	Yes	Yes	Yes

Post installation tasks for Deployment Solution

- Recreate the automation folders.
- Deploy automation folders on client computers.

Note: Symantec recommends that you clear the Internet browser cache before running deployment tasks.

To recreate the automation folders

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Manage Preboot Configurations**.
2. On the **Manage Preboot Configurations** page, in the preboot configurations list, select the configuration that you want to recreate and click **Recreate Preboot Environment**.

   For Mac, you must recreate all the NetBoot images and the automation folders and create new preboot configurations.

   Symantec recommends that you wait for at least half an hour before running any deployment tasks. To see if the automation folder is updated, check the timestamp for the automation folders that are created at the following locations:

   - PEInstall_x86

     `<install_dir>\Notification Server\NSCap\bin\Win32\X86\Deployment\Automation\PEInstall_X86`
   - PEInstall_X64

     `<install_dir>\Notification Server\NSCap\bin\Win64\X64\Deployment\Automation\PEInstall_x64`
   - LinInstall

     `<install_dir>\Notification Server\NSCap\bin\UNIX\Deployment\Linux\x86\Automation\LinInstall_x86`

   To verify if the automation folder has been recreated, in the task manager, check if the Bootwiz.exe application has completed recreating the preboot configuration.

After recreating the automation folders, run the following tasks from the Task Scheduler to update the packages on Notification Server:

- NS.Delta Resource Membership Update
- NS.Package Distribution Point Update Schedule
- NS.Package Refresh

To deploy the automation folders on the Windows client computers

- Run the following automation folder upgrade policies:
  - **Deployment Automation Folder for Windows (x64) - Upgrade**
  - **Deployment Automation Folder for Windows (x86) - Upgrade**

To deploy the automation folders on the Linux or Mac client computers

1. Run the following automation folder uninstall policies:
   - **Deployment Automation Folder for Linux-Uninstall**
   - **Deployment Automation Folder for Mac-Uninstall**
     After you enable the **Deployment Automation folder for Mac-Uninstall** policy, you must manually delete the DSAutomation partition that is present in the unmounted and unallocated state.
     If you do not want to run the uninstall policy to uninstall the automation folder from the client computer, you must manually erase the disk and the volume of the client computer. If you manually erase the disk and the volume of the client computer, ensure that you clean the Non-volatilerandom-accessmemory (NVRAM) of the client computer.
     For information on how to clean the NVRAM of a client computer, see the following article:
     http://support.apple.com/kb/HT1533
2. Run the following automation folder installation policies:
   - **Deployment Automation Folder for Linux-Install**
   - **Deployment Automation Folder for Mac-Install**

Fixed issues

IT Management Suite 8.0 HF1 contains fixed issues for the following solutions and components:

- CMDB Solution
  See "CMDB Solution Fixed Issues" on page 17.
- Deployment Solution

See "Deployment Solution Fixed Issues" on page 18.

- Inventory Solution
  See "Inventory Solution Fixed Issues" on page 19.
- ITMS Management Views
  See "ITMS Management Views Fixed Issues" on page 19.
- Monitor Solution
  See "Monitor Solution Fixed Issues" on page 21.
- Patch Management Solution
  See "Patch Management Solution Fixed Issues" on page 20.
- Software Management Solution
  See "Software Management Solution Fixed Issues" on page 21.
- Symantec Installation Manager
  See "Symantec Installation Manager Fixed Issues" on page 15.
- Symantec Management Platform
- Virtual Machine Management
  See "Virtual Machine Management Fixed Issues " on page 21.

Symantec Installation Manager Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-6 Fixed issues for Symantec Installation Manager

Issue	Article link
When the SIM is closed and re-launched, it incorrectly shows that the products are installed but not configured.	TECH234519
During the upgrade the SIM **Install Readiness Check** states that IIS script maps for ASP.NET 4.5.1 are missing or misconfigured.	N/A
The SIM **Install Readiness Check** only looks for x86 version of Java.	N/A
SIM does not correctly detect the status of the hierarchy environment.	N/A

Symantec Management Platform Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

This release contains fixed issues for the following components:

- Notification Server
- Task Server
- Symantec Management Agent
- UNIX/Linux/Mac
- Data Connector
  See Table 1-11 on page 17.

Table 1-7 Fixed issues for Notification Server

Issue	Article link
The Active Directory import does not function correctly for the users that are members of multiple security groups.	N/A
If the Symantec Management Agent reports a new subnet with its inventory data, the subnet is automatically created in database. It is not possible to specify the subnets that should be ignored and not automatically created.	TECH234718
The Agent Communication Profile does not allow to use a DNS alias as the **HTTPS communication host**.	N/A
When you edit a report and under the **Report Parameters** you try to add a **New Parameter**, then in the **Editing Parameter** dialog box, under **Add Dropdown Values From A Report**, the **Select a Value** function does not work.	TECH234632
Hierarchy editable properties (HEP) for role members are applicable for the standalone security replication rules.	N/A
Changing the URL ports in the hierarchy breaks the hierarchy. The fix for HF1 release allows changing the URL and server name in the **Servers** grid under **Settings > Notification Server > Hierarchy and Replication**.	N/A
If you want to import from all groups in AD and use the * in the **Starts with** field, in the **Select Security Groups** dialog box, the AD import will not work.	N/A

Table 1-8 Fixed issues for Task Server

Issue	Article link
When you create a run script task and want to select a computer name token from the **Insert Token** drop-down list, then any token past the first 25 tokens cannot be found in this drop-down list.	N/A
When the task fails because of time-out, no meaningful error message is displayed under the detailed information of the task instance.	N/A

Table 1-9 Fixed issues for Symantec Management Agent

Issue	Article link
In some cases, the following error appears in the Package Server Agent logs: "**Error while obtaining IIS installed features: IDispatch error #3607 (0x80041017)**"	N/A
Internal activities, such as package download, are not reflected in the Symantec Management Agent UI.	N/A
In some cases, the import of chained 3rd party certificates can fail.	N/A

Table 1-10 Fixed issues for UNIX/Linux/Mac

Issue	Article link
After installing a specific package through managed delivery, the agent on Mac OS may not correctly recognize the compliance status and leave the managed delivery state as not compliant.	N/A
The Symantec Management Agent that uses a profile with only one FQDN specified, cannot connect to a web resource that prohibits anonymous authentication.	N/A
The agent calculates the primary user based on logins count and not based on the login duration.	N/A

Table 1-11 Fixed issues for Data Connector

Issue	Article link
Connector import into a standard data class fails because the connector does not recognize the numeric(16,0) column type.	N/A

CMDB Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-12 Fixed issues for CMDB Solution

Issue	Article link
The **Update Network Resource Location** task deletes associations for resources that cannot be associated to a location via IP.	N/A
Merging client computers fails with the following error: *Conversion failed when converting from a character string to uniqueidentifier*.	N/A

Deployment Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-13 Fixed issues for Deployment Solution

Issue	Article link
If the **Prepare for Image Capture** task is not run for the deployed image, the client computer fails to boot into production after a **Deploy Image** task that uses DeployAnywhere is ran.	TECH234725
Incorrect status is logged in the PectAgent.log for installation of PFX certificate.	TECH234726
SBSservice.exe service stops unexpectedly.	TECH234727
Computer fails to boot in EFI mode from a WinPE ISO image that is created by BootWiz.exe	TECH234728
The PectAgent version number is missing from the PectAgent logs of a computer that is booted into the preboot environment.	TECH234729
Driver Manager fails to add drivers without hardware ID.	TECH234730
DeployAnywhere fails to install USB 3.0 drivers from the driver database to the client computer.	TECH205253
The **Create Image** task fails and the client computer stops receiving tasks from Notification Server after the computer is booted in the preboot environment using a WinPE X86 configuration.	TECH234731
Deploy Image task fails to list all the stored images if the SQL database is case-sensitive.	TECH234487
The Resource Import tool fails to import images into the remote site servers' package shares as an external package.	TECH234735
An exception is thrown by DeployAnywhere during driver retargeting operations if the **DevicePath** registry variable located under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion contains empty paths (";;").	TECH234732
Initial deployment job fails if the name or the description includes a special character.	TECH234733
Prepare for Image Capture task runs sysprep on systems containing the `HKLM\SYSTEM\Setup\Upgrade` registry key.	TECH234068
PECTAgent posts 169 IPs in **GetClientTaskServers** request.	TECH234734

Inventory Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-14 Fixed issues for Inventory Solution

Issue	Article link
If a user profile on Windows client computer contains symbolic links or junction points which create loops within the structure of the directories, the Inventory task hangs with high cpu usage when collecting the **User Account Windows** dataclass information. To work around the issue, you need to either change the links, or exclude **User Account Windows** from the inventory.	N/A
When you plug a USB Storage with no serial number into a client computer, and then collect hardware inventory on the computer, the work of Symantec Management Agent is terminated.	N/A
A file scan reports numerous instances of same files that are located in the directories generated by junction and symbolic links. As a result, inventory task execution time increases. If a junction exists in the user profile folder, a file scan execution time is increased even if this folder is excluded in the **File Properties scan** settings.	TECH234351
When **Application Metering Plug-in** starts, a blue screen may occur with the kernel error 0x00000050 (PAGE_FAULT_IN_NONPAGED_AREA).	N/A
The report **Count of Computers by Manufacturer and Model** times out.	N/A
After an upgrade to 8.0, a standalone inventory package is not created, because StandAlonePackager.exe is removed from `\Altiris\Inventory\Standalone\bin` folder during the upgrade process.	TECH234291

ITMS Management Views Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-15 Fixed issues for ITMS Management Views

Issue	Article link
When you select multiple computers under **Manage > Computers**, and then select only one computer, the **Computer Summary Multiple** blade doesn't turn back to **General** blade.	TECH234249

Table 1-15 Fixed issues for ITMS Management Views *(continued)*

Issue	Article link
On child servers, in the **Computers Views and Groups** View, the lists of computers from the selected groups are not loaded.	N/A

Patch Management Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-16 Fixed issues for Patch Management Solution

Issue	Article link
The task **Import Patch Data for Windows** fails to complete if you enable the option **Delete previously downloaded data for vendors, software and languages that are now excluded**.	TECH234411
On the **Windows Compliance** Dashboard, in the **Windows Patch Configuration Summary** Web Part, the report **Computers with Software Update Plug-in** excludes client computers redirected from another Notification Servers. The report shows only the computers with the **Software Update Plug-in** rolled out from the same Notification Server.	N/A
Target computers do not restart in the following scenario: 1 You specify a maintenance window in Notification Server configuration policies. 2 You configure the **Default Software Update Plug-in Policy** to run after the maintenance window closure or at the end of software update cycle. 3 You enable the option **Override Maintenance Windows settings** for the policy, and then distribute the policy to the target computers. 4 Software update installation finishes after the maintenance window closure.	N/A

FTP download of software update packages uses active FTP mode only.
To download software update packages in passive FTP mode, use the following registry setting:
`Registry key : HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Patch Management`
`Registry value [DWORD]:UseFTPPassiveMode`
`Value: 0=OFF(Use Active Mode), 1=ON(Use Passive mode), default value is OFF`
	INFO3604

Patch severity reports show double rows with English and non-English severity strings.	N/A

Software Management Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-17 Fixed issues for Software Management Solution

Issue	Article link
Client computers cannot download software packages for **Managed Software Delivery** policies if you enable the download setting **Use the default Symantec Management Agent settings to download**, and disable the targeted agent setting **Download the package files as soon as possible**.	N/A
The Symantec Management Agent tries to download a package from the first Notification Server in the following scenario: 1 SMA receives a software delivery policy (**Managed Software Delivery**, **Quick Delivery**, or legacy software delivery) and downloads a package from the first Notification Server. 2 You redirect SMA to the second Notification Server. 3 The second Notification Server sends to SMA a software delivery policy with the package that is equal to the package received from the first Notification Server. Workaround: To fix the issue, stop SMA, delete the secure store contents from the location `C:\ProgramData\Symantec\Symantec Agent\Ldb`, and restart SMA.	TECH234647

Monitor Solution Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-18 Fixed issues for Monitor Solution

Issue	Article link
Monitor Solution Agent stops running on AIX 6.1 machines.	N/A

Virtual Machine Management Fixed Issues

The following are the fixed issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-19 List of fixed issues

Issue	Article link
The "Create VM and OS Installation" job randomly fails at the "DS Job Scheduling" task step and logs an error.	N/A

Known Issues

IT Management Suite 8.0 HF1 contains known issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Known Issues" on page 22.
- Deployment Solution
  See "Deployment Solution Known Issues" on page 23.

Symantec Installation Manager Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-20 Known issues for Symantec Installation Manager

Issue	Article Link
When you upgrade Symantec Installation Manager as a part of hotfix installation process, the SIM UI might open while the SIM upgrade is still in progress. Symantec recommends to wait until the SIM upgrade finishes, usually it takes 1-2 minutes.	N/A

Symantec Management Platform Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

The known issues are listed for the following components:

- Task server
  See Table 1-21 on page 22.

Table 1-21 Known issues for Task server

Issue	Article link
The "**Task instance details are not available. Only summary data exists.**" message is not shown for the task instances processed by the clean-up task.	N/A

Deployment Solution Known Issues

The following are the known issues for this release. If additional information about an issue is available, the issue has a corresponding article link.

Table 1-22 Known issues for Deployment Solution

Issue	Article link
Imaging tasks fail when the **Primary file storage location** is specified in the **Package Server Settings** page for Package Server with multiple hard disks. Following error is displayed: `Cannot find out web/unc path`	N/A
A **Create Image** task that is saving an image to a standalone https web server fails when ran from a Linux preboot.	N/A
Boot Disk creator fails to create an X86 WinPE 3.1 preboot configuration.	N/A
The Hostname of a Linux client computer is not displayed in Linux preboot environment.	N/A
Linux client computers are displayed as a single resource when booted into Linux preboot environment.	N/A

Where to get more information

Use the following documentation resources to learn about and use this product.

Table 1-23 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Release Notes**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-23 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ Click the page and then press the F1 key. ■ Use the Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-24 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	http://help.symantec.com/Welcome?context=ITMS8.0

Table 1-24 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	The links to various groups on Connect are as follows: ■ Deployment and Imaging http://www.symantec.com/connect/groups/deployment-and-imaging ■ Discovery and Inventory http://www.symantec.com/connect/groups/discovery-and-inventory ■ ITMS Administrator http://www.symantec.com/connect/groups/itms-administrator ■ Mac Management http://www.symantec.com/connect/groups/mac-management ■ Monitor Solution and Server Health http://www.symantec.com/connect/groups/monitor-solution-and-server-health ■ Patch Management http://www.symantec.com/connect/groups/patch-management ■ Reporting http://www.symantec.com/connect/groups/reporting ■ ServiceDesk and Workflow http://www.symantec.com/connect/workflow-servicedesk ■ Software Management http://www.symantec.com/connect/groups/software-management ■ Server Management http://www.symantec.com/connect/groups/server-management ■ Workspace Virtualization and Streaming http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming