Symantec™ IT Management Suite 8.0 HF6 powered by Altiris™ technology Release Notes

Symantec

Symantec™ IT Management Suite 8.0 HF6 powered by Altiris™ technology Release Notes

Documentation version: 8.0 HF6

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

ITMS 8.0 HF6

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 HF6, the following new features are introduced:

Table 1-1 New features

Feature	Description
Support for Microsoft Office 365 installations that include Office 2016	Patch Management Solution for Windows supports Microsoft Office 365 installations that include Office 2016 dependent on the availability of the corresponding bulletins in patch data. Subscribe to the KB article DOC9673 to get the latest information about the availability of Microsoft Office 365 bulletins in patch data.
Possibility to prevent computer from going into sleep mode while task runs.	If a computer goes to sleep mode while a task runs on it, the task will fail. To fix this issue, you can now prevent the computer from going to sleep mode by enabling the **Prevent the computer from going into sleep mode while the tasks run** option at the following locations: ■ On the **Task Agent Settings** page (global settings) ■ In the advanced options dialog box, on the **Task options** tab, of a client task. Note that for **Defragment Computer** task, this option is enabled by default.
Added possibility to perform actions on multiple items in the search results list.	In the Symantec Management Console, you can now select multiple items in the search results list and perform actions on them. For example, you can select multiple policies in the search results list, and then enable or disable them at once.
The **Maximum log file size** has been changed.	Previously, the **Maximum log file size** limited the size on one log file. Now, this option controls the total size of HTTP log files. The size of a single log file is 1 MB. The **Maximum log file size** option is located on the **Targeted Agent Settings** page, on the **Downloads** tab, under **Peer-to-peer Downloading Configuration Settings**.
The search in the **Select Users or Groups** dialog box has been extended.	In the **Select Users or Groups** dialog box, the search for specific groups within Active Directory import has been extended as follows: ■ Search supports special symbols. (For example, '&') ■ Search parameters are extended with **Contains** option.

Table 1-1 New features *(continued)*

Feature	Description
Workspace Virtualization components are upgraded to the version 7.6 HF8 (7.6.247)	In Software Management Solution 8.0 HF6, the following Workspace Virtualization components are upgraded to the version 7.6 HF8 (7.6.247): ■ Symantec Workspace Virtualization Agent (SWV Agent) (32/64 bit) ■ Virtual Composer (32/64 bit) ■ Streaming Agent (32/64 bit) The correct version of SWV Agent appears in the list of plug-in versions for the selected client computer. After the 8.0 HF6 upgrade, the following changes occur in the custom policies that use the old version of the SWV Agent: ■ The SWV Agent is upgraded to the latest version. ■ The policies stay enabled. ■ The policies deliver the latest version of the SWV Agent. For SWV 7.6 HF8 Release Notes, please see the following link: http://www.symantec.com/docs/DOC9670
Workspace Virtualization is supported on Windows 2016 Server and Windows 10 with the update 1607 or higher.	Symantec Workspace Virtualization Agent successfully installs on the computers with these operations systems. These operations systems are included into the following default filters for the predefined Symantec Workspace Virtualization installation and upgrade policies: ■ Computers are available for Software Workspace Virtualization agent installation ■ Computers are available for Software Workspace Virtualization agent upgrade
Improved performance while accessing packages from console.	Improved performance while accessing BDC, DriversDB, Imaging, and PCT packages from the console.
OpenSSL has been updated.	OpenSSL is updated to version 1.0.2k in the Pluggable Protocols Architecture.

System requirements and supported platforms

Before you install IT Management Suite 8.0 HF6, 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 HF6 involves installation of Symantec Management Platform (SMP) 8.0 HF6 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 HF6

After you install this hotfix (8.0 HF6), 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 HF6 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 HF6, 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:

`<installation_path>\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 1-2 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.
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.

Table 1-2 Process to upgrade Symantec Management Agent, site servers and solution plug-ins *(continued)*

Step	Action	Description
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.

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:

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

Enabling imaging after the upgrade in non-domain environment

In Deployment Solution, 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 HF6 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF6

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.0.3769	8.0.3504
Altiris Client Task Agent	8.0.3769	8.0.3504
Altiris Client Task Server Agent	8.0.3745	N/A
Altiris Base Task Handlers	8.0.3769	8.0.3504
Altiris Pluggable Protocols Architecture Agent	8.0.3708	N/A
Inventory Agent	8.0.3521	8.0.3521
Application Metering Agent	8.0.3338	N/A
Server Inventory Agent	8.0.3543	8.0.3543
Inventory Rule Agent	8.0.3769	8.0.3504
Monitor Plug-in	8.0.3512	8.0.3512
Package Server	8.0.3171	8.0.3504
Power Scheme Task Plug-in	7.6.1395	N/A
Software Update Plug-in	8.0.3323	8.0.2229
Software Management Framework Agent	8.0.3504	8.0.3504
Software Management Solution Agent	8.0.2225	8.0.2225
Virtual Machine Management Task Handler	8.0.2206	N/A
Deployment Task Server Handler	8.0.3740	N/A

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF6 *(continued)*

Agent or plug-in	Windows	UNIX/Linux/Mac
Deployment Package Server	8.0.3740	N/A
Deployment Plug-in for Windows (x64/x86)	8.0.3740	N/A
Deployment Plug-in for Linux (x64)	N/A	8.0.3740
Deployment Plug-in for Linux (x86)	N/A	8.0.3740
Deployment Plug-in for Mac	N/A	8.0.2246
Deployment NBS plug-in	8.0.3740	N/A
Symantec Workspace Streaming Agent	7.6.0.247	N/A
Symantec Workspace Virtualization Agent	7.6.247.0	N/A
Symantec Workspace Virtualization Agent	7.6.247	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 HF6:

Table 1-4 Post installation tasks for Deployment Solution

Upgrade	Windows automation folder	Mac automation volume	Linux automation folder
Upgrade from 8.0 to 8.0 HF6	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:
  https://support.apple.com/en-us/HT204063

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 HF6 contains fixed issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Fixed Issues" on page 15.
- Deployment Solution
  See "Deployment Solution Fixed Issues" on page 17.
- Workflow Solution
  See "Workflow Solution Fixed Issues" on page 18.
- Patch Management Solution
  See "Patch Management Solution Fixed Issues" on page 18.
- Software Management Solution
  See "Software Management Solution Fixed Issues" on page 19.

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
  See Table 1-5 on page 16.
- Symantec Task Server
  See Table 1-6 on page 16.
- Symantec Management Agent
  See Table 1-7 on page 17.
- Data Connector
  See Table 1-8 on page 17.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
The **AD Import Users** task times out because of the redundant rows in the **DirectoryImportRuleTree** table.	N/A
During the AD Import of Users, the following error appears in the Notification Server logs: "**Failed to process NSE. Invalid resource ref was looked up, corrupt Xml document!**" This issue occurs if vAssetView is missing data for the user.	N/A
After upgrading to IT Management Suite version 8.0 HF5, the scrollbar does not appear in the **Create New Task** dialog box. This issue occurs only if the Internet Explorer temporary files are not cleaned after the upgrade.	N/A
A report that is based on an SQL query fails to save if it contains the word "Create".	TECH236831
Inv_Aex_AC_InternetGatewayDetails table stores the **Last Failure** and **Last Success** times in UTC time. This causes problems with **Computers by Gateway** and **Internet Gateway communication problems (details)** reports.	N/A
If you mark a computer as **Retired** and run **Inventory Clean Up** task on it, the installation of Symantec Management Agent using manual push fails on such computer.	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
Deployment Solution job that contains several tasks might stop responding in WinPE environment because the agent fails to get a task from the Notification Server.	N/A
Sometimes, after you remove the **Cloud-enabled Management Agent IIS Website**, the Symantec Management Agents fail to register with Task Server.	N/A

Table 1-6 Fixed issues for Task Server *(continued)*

Issue	Article link
If the **Run Script** task has the option **Save Script Output with Task Status** enabled, and the generated output contains special characters, the processing of such output fails on Notification Server with errors. In this situation, the Client Task Agent loses the registration and goes into registration loop.	N/A
In some cases, upgrading the Symantec Management Agent on a site server with Task Service enabled might fail with the following error: **"Failed to start service, error 0x00000422"**	N/A

Table 1-7 Fixed issues for Symantec Management Agent

Issue	Article link
When you specify the reboot as the results-based action for a Managed Delivery Policy, the reboot does not restart the client computer immediately when the user clicks **Reboot now**. The actual restart happens in 5 minutes without a warning.	N/A
VPN computers with throttling enabled are unable to download packages over HTTP.	N/A
The Symantec Management Agent pop-up message that displays alert about an occurring reboot is misleading.	N/A

Table 1-8 Fixed issues for Data Connector

Issue	Article link
Data Connector rule that exports report results generates invalid CSV file if null data is present at the end of the row.	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 1-9 Fixed issues for Deployment Solution

Issue	Article link
NBS general policies for site servers do not clone properly.	N/A
EFI computers that are hosted on ESXi 6.0 cannot boot into PXE.	N/A

Table 1-9 Fixed issues for Deployment Solution *(continued)*

Issue	Article link
Sometimes, BootWiz.exe fails to create Windows preboot configurations. **Note:** Ensure that the Authenticated users group for BootWiz.exe has Read & execute permissions.	N/A
Sometimes, computers fail to boot into preboot environment if some details, such as computer name disappear from computer details after Active Directory Import.	N/A
For Windows version later than Windows 8, the **Deploy Image** task with DeployAnywhere fails to install drivers on client computers.	N/A
The Symantec Management Agent of images that are captured with a CEM certificate fail to connect to Notification Server.	N/A

Workflow 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 1-10 Fixed issues for Workflow Solution

Issue	Article link
While using the Workflow HF5 installer to upgrade ServiceDesk installation, a warning appears for ServiceDesk compatibility.	N/A
SymQ Configuration does not connect to the SQL server using native SQL accounts.	N/A
In an SSL setup, the Workflow project cookies are not set to secure in the IIS settings.	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 1-11 Fixed issues for Patch Management Solution

Issue	Article link
In a hierarchy environment, on the child Notification Server, the user cannot configure the language setting on the **Windows Patch Remediation Settings** page.	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 1-12 Fixed issues for Software Management Solution

Issue	Article link
A managed software delivery policy runs on a client computer once, and then after the user logs on, the subsequent policies fail to run until the user logs off. This issue occurs if you configure the two options on the policy page, in the **Advanced Options** dialog box, as follows: ■ On the **Results-based actions** tab, for the **Action** option, you select the condition **Log off user**. ■ On the **Run** tab, for the **Task can run** option, you select the condition **Whether or not the user is logged on**.	N/A
A managed software delivery policy or quick delivery task fail to run with the error **Unable to locate the specified file** if you configure the policy or task settings as follows: ■ On the policy or task page, in the **Advanced Options** dialog box, on the **Download** tab, you enable the option **Use the following settings to download and run**, and then you do not check the option **Run from the server if bandwidth is above**.	N/A
Multiple versions of execution tasks are being generated for a managed software delivery policy or task and cause slow and unstable performance.	N/A

Known Issues

IT Management Suite 8.0 HF6 contains known issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Known Issues" on page 19.
- Deployment Solution
  See "Deployment Solution Known Issues" on page 20.
- Patch Management Solution
  See "Patch Management Solution Known Issues" on page 21.

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:

- Notification Server
  See Table 1-13 on page 20.

Table 1-13 Known issues for Notification Server

Issue	Article link
In the Security Role Manager, the items that have special characters in their names (for example, "", |, or !) are not displayed properly.	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 1-14 Known issues for Deployment Solution

Issue	Article link
Sometimes, a predefined virtual computer with XFS partition fails to restart into production.	N/A
A computer fails to boot to production after deploying a Windows 10 Redstone (x86) Sysprep image.	N/A
When you deploy an image of RHEL 7.2, the **Partition** tab shows all partitions of LinuxSwap type.	N/A
Sometimes the **Deploy Image** task may fail to remove AexSWDPolicy.xml file after an image is deployed on Windows XP and Windows 2003 computer.	N/A
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
Boot Disk creator fails to create an X86 WinPE 3.1 preboot configuration.	N/A
IP address is not reassigned by DHCP server after you deploy a syspreped image of RHEL 6.7 on a client computer that has single NIC. Workaround: Delete the file `70-persistent-net.rules` from /etc/udev/rules.d/ and restart the client computer.	N/A

Table 1-14 Known issues for Deployment Solution *(continued)*

Issue	Article link
For Windows 10 (1607) Anniversary update, the imaging task fails. For details of the workaround, refer to the following article: HOWTO125161	HOWTO125161

Patch Management 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 1-15 Known issues for Patch Management Solution

Issue	Article link
If you have downloaded Windows software updates catalog, and then you uncheck some vendors, software and/or languages on the Import Patch Data for Windows page, the data for the unchecked items will not be automatically deleted for Microsoft Office 365 Click-to-Run installations. **Workaround**: To save disk space, you need to open the directory `C:\Program Files\Altiris\Patch Management\Packages\Updates\` and remove the folder(s) with name of Office 365 bulletin, for which you want to delete the data. Then you need to manually recreate the packages for the bulletin as follows: 1 In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**. 2 In the right pane, in the **Show** drop-down box, click **All Software Bulletins**, and then click the **Refresh** symbol. 3 Select the bulletins that you want to revise. You can select multiple items while holding down the **Shift** or **Ctrl** key. 4 Right-click the selected bulletin(s), and then click **Recreate Packages**. 5 On the **Download Software Update Package** page, click **Close**.	DOC9673

Table 1-15 Known issues for Patch Management Solution *(continued)*

Issue	Article link
On the **Import Patch Data for Windows** page, the enabled option **Automatically revise Software Update policies after importing patch data** does not work in the software update policies for Microsoft Office 365 Click-to-Run installations. **Workaround**: You need to manually recreate the packages for the bulletins that you want to revise as follows: 1 In the Symantec Management Console, on the **Actions** menu, click **Software > Patch Remediation Center**. 2 In the right pane, in the **Show** drop-down box, click **All Software Bulletins**, and then click the **Refresh** symbol. 3 Select the bulletins that you want to revise. You can select multiple items while holding down the **Shift** or **Ctrl** key. 4 Right-click the selected bulletin(s), and then click **Recreate Packages**. 5 On the **Download Software Update Package** page, click **Close**.	DOC9673
After an off-box upgrade of Patch Management Solution for Windows 7.6 post-HF7 point fix to the 8.0 HF6 version, Microsoft Office 365 software update package files are exported from the source Notification Server incorrectly. From all Microsoft Office 365 software update package files, only 2 files in the **Experiment** folder get imported to the target Notification Server. **Workaround:** 1 Manually transfer all Microsoft Office 365 software update package files from the source Notification Server to the new software update files location on the target Notification Server. 2 On the target Notification Server, run the task "Check Software Update Package Integrity" with the enabled option "Relocate existing packages if default Software Update package location on Core Services page has changed". **Warning:** Do not change the "Software Update Package Location" value on the "Core Services" page. 3 Manually recreate the packages for each Microsoft Office 365 bulletin. 4 Download the Windows software updates catalog to download the Windows Assessment and Patch Install Tools packages.	DOC9673

Table 1-15 Known issues for Patch Management Solution *(continued)*

Issue	Article link
After an upgrade of Patch Management Solution for Windows 7.6 post-HF7 point fix to the 8.0 version that does not support Microsoft Office 365 installations (8.0 HF5 or earlier), the Microsoft Office 365 software updates get transferred to the client computers of the upgraded Notification Server. To eliminate incorrect behaviour, Microsoft Office 365 updates are configured as follows: ■ Microsoft Office 365 updates are disabled in Patch Management Solution. You cannot download them or create new software update policies using them. ■ Microsoft Office 365 updates that have been previously included into software update policies are disabled for distribution. ■ New Microsoft Office 365 updates will not be imported on subsequent imports of patch data. After an upgrade to Patch Management Solution for Windows 8.0 HF6, Microsoft Office 365 updates will be enabled for download, distribution, and use in software update policies.	DOC9673

Where to get more information

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

Table 1-16 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 1-16 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 1-17 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	Knowledge Base
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.	Unified Help System

Table 1-17 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 ■ Discovery and Inventory ■ ITMS Administrator ■ Mac Management ■ Monitor Solution and Server Health ■ Patch Management ■ Reporting ■ ServiceDesk and Workflow ■ Software Management ■ Server Management ■ Workspace Virtualization and Streaming