

Symantec™ IT Management
Suite 8.0 HF2 powered by
Altiris™ technology Release
Notes



Symantec™ IT Management Suite 8.0 HF2 powered by Altiris™ technology Release Notes

Documentation version: 8.0 HF2

Legal Notice

Copyright © 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and Altiris, and any Altiris trademarks are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT 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 HF2 Release Notes

This document includes the following topics:

- [About IT Management Suite](#)
- [What's new in this release](#)
- [System requirements and supported platforms](#)
- [General installation and upgrade information](#)
- [Performing post installation tasks for Deployment Solution](#)
- [Fixed issues](#)
- [Known Issues](#)
- [Where to get more information](#)

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 HF2, the following new features are introduced:

Table 1-1 New features

Feature	Description
New features in SIM.	<p>SIM introduces the following new features:</p> <ul style="list-style-type: none"> On the Installed Products page, you have the option to reconfigure each installed product. Reconfiguration respects the dependency of products and order of installation. On the Product Licensing page, in the Licenses table, the new AUP column is introduced. The AUP column displays the Annual Upgrade Protection expiration date. Note that AUP is only applicable to Full License types.
New predefined schedule.	<p>The new predefined SMP schedule performs the defragmentation of SQL indexes.</p> <p>Note that this schedule is disabled by default. To set up the defragmentation of SQL indexes, you must enable the schedule and configure it according to your needs.</p>
Possibility to select multiple tasks.	When adding tasks to a job, you can now select multiple tasks at once by holding down the Ctrl key.
Improvements of the navigation tree on the Site Server Management page.	Navigation tree on the Site Server Management page is now faster and more reliable. When opening larger lists within the tree, a progress indicator is displayed.
Adjustable scoping of the target.	On the resource target edit page, it is now possible to adjust its scoping. Scoping for targets means that if currently logged in user is member of all the roles that are set in the scope, then such user has write permissions for this target. If the user is not member of all the roles, then such user has read-only permissions for target.
New command lines for Symantec Management Agent.	<p>The following new command lines are introduced for Package Server:</p> <ul style="list-style-type: none"> <code>aexagentutil.exe /psrefreshall</code> - refreshes all packages <code>aexagentutil.exe /psresendall</code> - resends all statuses
Possibility to control primary user type for Symantec Management Agent for Unix, Linux and Mac.	A Report only AD users as primary option is added to the Targeted Agent Settings page. This option lets you control the primary user type. If the checkbox is checked, the agent reports only Active Directory users. If the checkbox is unchecked, both local and Active Directory users are used to calculate the primary user.
WinPE 10 support	<p>Deployment Solution now supports WinPE 10 preboot configuration. For more information, refer to the following article:</p> <p>info3561</p>

Table 1-1 New features (*continued*)

Feature	Description
Support for 4K	<p>Deployment Solution now supports external 4K USB hard drives for the following scenarios:</p> <ul style="list-style-type: none"> ■ Storing image of a computer on a 4k drive. ■ Deploying a computer image from a 4K drive. <p>Note: Scripted OS install is not supported for a 4K drive.</p>
Workspace Virtualization components are upgraded to the version 7.6 HF4 (7.6.196).	<p>In Software Management Solution 8.0 HF2, the following Workspace Virtualization components are upgraded to the version 7.6 HF4 (7.6.196):</p> <ul style="list-style-type: none"> ■ Symantec Workspace Virtualization Agent (SWV Agent) (32/64 bit) ■ Virtual Composer (32/64 bit) ■ Streaming Agent (32/64 bit) <p>The correct version of SWV Agent appears in the list of plug-in versions for the selected client computer.</p> <p>After the 8.0 HF2 upgrade, the following changes occur in the custom policies that use the old version of the SWV Agent:</p> <ul style="list-style-type: none"> ■ The SWV Agent is upgraded to the latest version. ■ The policies stay enabled. ■ The policies deliver the latest version of the SWV Agent. <p>For SWV 7.6 HF4 Release Notes, please see the following link: http://www.symantec.com/docs/HOWTO124722</p>
OpenSSL is upgraded.	OpenSSL is now upgraded to version 1.0.1t.

System requirements and supported platforms

Before you install IT Management Suite 8.0 HF2, 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 HF2 involves installation of Symantec Management Platform (SMP) 8.0 HF2 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 HF2

After you install this hotfix (8.0 HF2), 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 HF2 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 HF2, 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 1-2 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.	<p>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.</p> <p>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.</p> <p>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.</p>
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.	<p>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.</p> <p>To upgrade the solution-specific plug-ins to the latest version, do the following:</p> <ul style="list-style-type: none"> ■ 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, 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 HF2 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF2

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.0.2548	8.0.2516
Altiris Client Task Agent	8.0.2548	8.0.2516
Altiris Client Task Server Agent	8.0.2532	N/A
Altiris Base Task Handlers	8.0.2548	8.0.2516
Altiris Pluggable Protocols Architecture Agent	8.0.2516	N/A
Inventory Agent	8.0.2328	8.0.2259
Application Metering Agent	8.0.2526	N/A
Server Inventory Agent	8.0.2221	8.0.2221
Inventory Rule Agent	8.0.2548	8.0.2516
Monitor Plug-in	8.0.2518	8.0.2326
Package Server	8.0.2365	8.0.2516
Power Scheme Task Plug-in	7.6.1395	N/A
Software Update Plug-in	8.0.2531	8.0.2229
Software Management Framework Agent	8.0.2548	8.0.2516
Software Management Solution Agent	8.0.2225	8.0.2225
Virtual Machine Management Task Handler	8.0.2206	N/A
Deployment Task Server Handler	8.0.2571	N/A

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF2 (*continued*)

Agent or plug-in	Windows	UNIX/Linux/Mac
Deployment Package Server	8.0.2571	N/A
Deployment Plug-in for Windows (x64/x86)	8.0.2571	N/A
Deployment Plug-in for Linux (x64)	N/A	8.0.2571
Deployment Plug-in for Linux (x86)	N/A	8.0.2571
Deployment Plug-in for Mac	N/A	8.0.2246
Deployment NBS plug-in	8.0.2571	N/A
Symantec Workspace Streaming Agent	7.6.0.196	N/A
Symantec Workspace Virtualization Agent	7.6.196	N/A
Workspace Virtual Composer	7.6.0.196	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 HF2:

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 HF2	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-volatile random-access memory (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 HF2 contains fixed issues for the following solutions and components:

- Symantec Management Platform
See “[Symantec Management Platform Fixed Issues](#)” on page 16.
- CMDB Solution
See “[CMDB Solution Fixed Issues](#)” on page 18.
- Deployment Solution
See “[Deployment Solution Fixed Issues](#)” on page 18.
- First Time Setup Portal
See “[First Time Setup Portal Fixed Issues](#)” on page 19.
- Inventory Solution
See “[Inventory Solution Fixed Issues](#)” on page 19.
- ITMS Management Views
See “[ITMS Management Views Fixed Issues](#)” on page 20.
- Patch Management Solution
See “[Patch Management Solution Fixed Issues](#)” on page 21.
- Real-Time System Manager

See [“Real-Time System Manager Fixed Issues”](#) on page 21.

- Software Management Solution
See [“Software Management Solution Fixed Issues”](#) on page 21.
- Workflow Solution
See [“Workflow Solution Fixed Issues”](#) on page 22.

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 22.
- Task Server
See [Table 1-6](#) on page 17.
- Symantec Management Agent
See [Table 1-7](#) on page 17.
- Symantec UNIX/Linux/Mac
See [Table 1-7](#) on page 17.
- Data Connector
See [Table 1-9](#) on page 18.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
If you remove an organization unit from Active Directory import rule and later add it back to the import rule, it only adds 30% of computers into designated organizational group.	TECH234772
spResourceAssociationsDelete causes blocking and slows down the Event Queue processing.	N/A
The Cloud-enabled agent gets the following error when trying to connect over CEM: "InitializeSecurityContext error while client handshake: The specified data could not be decrypted. (0x80090330) on the client."	N/A
Delivery and execution of tasks is not reliable in an environment with low bandwidth connection between Notification Server and agents.	N/A
Saving Active Directory import rule fails with the following error: "The system cannot find the path specified. (Exception from HRESULT: 0x80070003)"	N/A

Table 1-5 Fixed issues for Notification Server (*continued*)

Issue	Article link
The Symantec Management Platform performance counters are functional and extended. They are available in Performance Monitor with "Altiris" prefix.	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
In an environment with a large amount of subnets, the log gets sometimes flooded with the Unable to load subnets and getclienttaskservers errors.	N/A
After resizing the columns in the Symantec Management Console, the following error appears: "An error occurred while refreshing. Check the Altiris log for more information."	TECH234818
When searching for a computer under Quick Run , it might take more than a minute to load the search result. Also, when drilling down to any of the already executed tasks, it takes a long time to populate the computers list under the Task Status .	TECH234756
After installing ITMS 8.0 HF1, the task server that was previously assigned to child Notification Server now tries to register on parent Notification Server. This issue occurs only when you define preferred NS Host on parent Notification Server.	TECH234779
Reboot to production fails randomly.	N/A
The message "Task instance details are not available. Only summary data exists" is not shown for the task instances that are processed by the clean-up task.	N/A

Table 1-7 Fixed issues for Symantec Management Agent

Issue	Article link
If no user is logged on, the computer should be restarted automatically after the execution of Managed Software Delivery policy. The automatic restart should be performed even if the Notify user about action or Allow user to defer action options are enabled.	N/A
Inability to decrypt credentials and AppID account lockout in case of accidental SMA storage corruption.	N/A

Table 1-8 Fixed issues for UNIX/Linux/Mac

Issue	Article link
In some cases, <code>getadinfo.sh</code> script incorrectly calculates the Active Directory user name field.	N/A

Table 1-9 Fixed issues for Data Connector

Issue	Article link
If the source column of the data class has a different name than its own column name, you get a Symantec Management Server Error after clicking Refresh Data Source on Data Connector import rule page.	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 1-10 Fixed issues for CMDB Solution

Issue	Article link
The task Update Network Resource Location deletes associations for the resources that cannot be associated to a location via an IP.	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 1-11 Fixed issues for Deployment Solution

Issue	Article link
Windows environment variables are not resolved by the Deploy Image Client Task Handler in automation.	N/A
If a Package Server is configured to UNC path only, then DeployAnywhere fails to download the <code>drivers.manifest.txt</code> .	N/A
Computer continuously reboots to PXE if Boot To PXE task is sent to a system already in PXE.	N/A
Driver Manager fails to import compressed drivers into the DeployAnywhere driver database.	N/A

Table 1-11 Fixed issues for Deployment Solution (*continued*)

Issue	Article link
The Install Windows OS task may fail to install Windows Server 2012 and Windows Server 2012 R2 operating system in any of the following scenarios: <ul style="list-style-type: none"> ■ Custom configuration option is selected. ■ The unattended default configuration files are modified. ■ The unattended inventory configuration files are modified. 	N/A
The Prepare for Image Capture task stops and displays the following error as the BCD Edit returns large amount of data for the recovery partition: Deployment Solution: The task has been stopped on user's request.	N/A
The password for Ghost user is not complex.	N/A
After upgrade to 8.0, the Install Deployment Solution PS component fails, if few files are not deleted from the <code>Altiris\Altiris Agent\Agents\Deployment\PSComponent</code> folder during the upgrade.	N/A
Following error occurs while importing OS files: Error occurred while uploading the files.	TECH235041
The Deployment Solution PS component install, uninstall and upgrade scripts fail in the following scenarios: <ul style="list-style-type: none"> ■ No IIS is installed. ■ http/https codebase are temporarily disabled. 	N/A

First Time Setup Portal 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 First Time Setup Portal

Issue	Article link
The Expires column on the Product Licensing page shows "N/A" instead of the number of days.	INFO3608

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 1-13 Fixed issues for Inventory Solution

Issue	Article link
After you install the Application Metering Plug-in 8.0 or 8.0 HF1 on Windows 7 or 10 client computers, a blue screen occurs with the error SYSTEM_SERVICE_EXCEPTION (Bug check code 0x0000003b) caused by SAMDriver.sys	N/A
The predefined task NS.Nightly schedule to associate Software component to software product times out and does not associate software components to appropriate software products.	N/A
Application metering is complicated in hierarchy environment, if a software product contains a software component that has no association with a program file resource. The software component loses the association with its file resource in the following scenario: <ul style="list-style-type: none"> You relocate the software component from child Notification Server to parent Notification Server. The same file resource has been present on parent Notification Server before the relocation the software component. 	N/A

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 1-14 Fixed issues for ITMS Management Views

Issue	Article link
After an upgrade from ITMS 7.5 to ITMS 7.6 HF7, the Software Catalog page does not load.	N/A
If the client computer data has "9999" in it, a filter, target or organizational group that contains this client computer does not load.	TECH234639
When, in ITMS Management Views, you try to import an item (right-click an item, and then click Import), an error occurs.	N/A
When, on the Software view page, you save the list of Computers with software installed as a report and check the Open report in new window after saving , an error occurs, and the list of computers is not shown in the dialog box that opens.	TECH234774
If you try to add new products using the Software Catalog, only the last added product is saved. All the previously created software products are deleted.	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 1-15 Fixed issues for Patch Management Solution

Issue	Article link
When you use the File Transfer Protocol to download updates, Patch Management Solution does not honor the specified proxy settings. Known limitation of the fix: with active proxy, when downloading updates, Patch Management Solution always re-downloads the files that are located on the File Transfer Protocol server.	N/A
A software update policy does not download a software update package immediately and stays in pending state until a maintenance window opens.	N/A

Real-Time System 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 1-16 Fixed issues for Real-Time System Manager

Issue	Article link
In ITMS 7.6 HF7, Boot redirection fails on AMT 9.1 client computers.	N/A
In ITMS 7.6 HF7, getting Out of Band inventory fails on AMT 9.1 client computers.	TECH234702
In ITMS 7.6 HF7, the power management task fails if only AMT and WSMAN protocols are enabled.	N/A
The current power state of a client computer is defined as "unknown" if any other protocol than WMI is used for the power management task.	N/A
Redirection options do not work if the reboot transaction is enabled.	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
All Managed Software Delivery policies with tasks execute at the time when one of the policies is scheduled to execute.	N/A
<p>Software import fails with the error <i>Exception has been thrown by the target of an invocation</i>, and an unconfigured package appears in the Software library under the following conditions:</p> <ul style="list-style-type: none"> ■ Notification Server uses Windows Authentication to connect to the database. ■ Specified Agent Connectivity Credentials have access to the package location but not the database. ■ You use the Import Software wizard to import a package, to create a new software resource, or to add a package association to an existing software resource. 	N/A
Client tasks in a software delivery policy ignore the enabled Max retries setting and fail.	N/A
<p>Predefined Software Management Solution compliance reports may show different computer counts.</p> <p>The Software Compliance By Managed Delivery Policy report shows results only for the computers that have SMA installed.</p> <p>Other software compliance reports include data for all computers, that have ever received a Managed Software Delivery policy or have sent a compliance data to a Notification Server, regardless of inclusion of such computer into the target for a corresponding Managed Software Delivery policy.</p>	N/A
In Managed Software Delivery policies, you cannot change the timeout of a wake-up server task. The wake-up server task takes a lot of time to process all target computers. The queue of server tasks appears and affects the performance of a task 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 1-18 Fixed issues for Workflow Solution

Issue	Article link
Unable to reset the Repeat Task option in Report Schedule, after setting up the option.	TECH233186
Incorrect UI strings are displayed after logging in as a Problem Analyst in Process Manager, opening My Task List and expanding SD.ProblemManagement.	N/A

Table 1-18 Fixed issues for Workflow Solution (*continued*)

Issue	Article link
Unable to compile the ASDK integration library Symantec.Components.Generated7.Altiris.ASDKTask.dll.	N/A
HTML tags for line breaks are displayed in the ticket description section of the Process View page.	N/A
In the Report Builder, the Process Columns for Age Description and Age display the start date of the process or task instead of the actual information.	N/A
Unable to upload files because the default file upload size is set to 0 MB.	N/A
Error occurs while trying to resolve an incident in ServiceDesk 8.0. Incorrect SLAGetProcessToComplete procedure is stored in the database.	N/A
The ReferralURL column in the ReportProcess table is not wide enough and truncates the URLs.	N/A

Known Issues

IT Management Suite 8.0 HF2 contains known issues for the following solutions and components:

- Symantec Management Platform
See [“Symantec Management Platform Known Issues”](#) on page 23.
- Deployment Solution
See [“Deployment Solution Known Issues”](#) on page 24.
- Inventory Solution
See [“Inventory Solution Known Issues”](#) on page 25.
- IT Analytics
See [“IT Analytics Solution Known Issues”](#) on page 24.

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 1-19](#) on page 24.

Table 1-19 Known issues for Task server

Issue	Article link
<p>During the configuration of Task Management 8.0 HF2, the following error appears in the Notification Server log: "Failed to start hosted object: config=C:\Program Files\Altiris\Altiris Agent\Client Task Server\TaskServer.config"</p> <p>Note that this error does not affect the task server functionality.</p>	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 1-20 Known issues for Deployment Solution

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

IT Analytics 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 1-21 Known issues for IT Analytics

Issue	Article link
In ITMS 8.0, IT Analytics reports and dashboards may have issues with loading on the SMP console.	TECH234703

Inventory 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 Inventory Solution

Issue	Article link
After the reconfiguration of Inventory Solution 8.0 HF2, the predefined Application Metering Plug-in for Windows Upgrade policy loses the translation of its name and description.	N/A

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 1-23 Known issues for Patch Management Solution

Issue	Article link
<p>During the upgrade from 8.0 HF1 to 8.0 HF2 and configuration of Patch Management Solution, the following error appears in the Notification Server log:</p> <p>"Item Update aborted. Unable to locate item with guid 368a5e6d-be26-41c4-a274-a0b9f11d555b. Continue with the remaining installation process."</p> <p>The issue does not affect the overall functionality of the solution.</p>	N/A

Where to get more information

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

Table 1-24 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.	<ul style="list-style-type: none"> ■ 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.
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: <ul style="list-style-type: none"> ■ 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 1-25 Symantec product information resources

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

Table 1-25 Symantec product information resources (*continued*)

Resource	Description	Location
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
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	<p>The links to various groups on Connect are as follows:</p> <ul style="list-style-type: none"> ■ 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