

Symantec™ IT Management  
Suite 8.0 HF5 powered by  
Altiris™ technology Release  
Notes



# Symantec™ IT Management Suite 8.0 HF5 powered by Altiris™ technology Release Notes

Documentation version: 8.0 HF5

## 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/](http://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/](http://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](http://support.symantec.com)

## Customer service

Customer service information is available at the following URL:

[www.symantec.com/business/support/](http://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](mailto:customercare_apj@symantec.com)

Europe, Middle-East, and Africa [semea@symantec.com](mailto:semea@symantec.com)

North America and Latin America [supportsolutions@symantec.com](mailto:supportsolutions@symantec.com)

# IT Management Suite 8.0 HF5 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 HF5, the following new features are introduced:

Table 1-1 New features

Feature	Description
Peer-to-peer downloading	<p>The peer-to-peer downloading feature lets you download and distribute the software delivery and patch packages to Windows computers. It minimizes the software delivery time and provides you with a reliable software delivery to all endpoints. The peer-to-peer downloading feature significantly reduces the load on the network and the IT Management Suite infrastructure.</p> <p>For more information about peer-to-peer downloading, see the knowledge base article at the following URL:</p> <p><a href="http://www.symantec.com/docs/DOC9473">http://www.symantec.com/docs/DOC9473</a></p>
Support for Microsoft Windows Server 2016	<p>Symantec Management Agent and solution plug-ins can be installed on Windows Server 2016.</p> <p>For the list of supported solutions and limitations refer to the following article:</p> <p><a href="http://www.symantec.com/docs/HOWTO125454">http://www.symantec.com/docs/HOWTO125454</a></p>
Deployment Solution updated security	<p>For Deployment Solution components, security is enhanced with an updated OpenSSL.</p>
Workspace Virtualization components are upgraded to the version 7.6 HF7 (7.6.0.233)	<p>In Software Management Solution 8.0 HF5, the following Workspace Virtualization components are upgraded to the version 7.6 HF7 (7.6.0.233):</p> <ul style="list-style-type: none"> <li>■ Symantec Workspace Virtualization Agent (SWV Agent) (32/64 bit)</li> <li>■ Virtual Composer (32/64 bit)</li> <li>■ Streaming Agent (32/64 bit)</li> </ul> <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 HF5 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"> <li>■ The SWV Agent is upgraded to the latest version.</li> <li>■ The policies stay enabled.</li> <li>■ The policies deliver the latest version of the SWV Agent.</li> </ul> <p>For SWV 7.6 HF7 Release Notes, please see the following link:</p> <p><a href="http://www.symantec.com/docs/HOWTO125403">http://www.symantec.com/docs/HOWTO125403</a></p>
It is now possible to generate bootstrap files using the custom configuration XML	<p>You can now also apply custom settings to ULM agent pull installation packages and to ULM agent Cloud-enabled installation packages using the custom configuration XML.</p>
Search in <b>Create New Task</b> and <b>Select Task</b> dialog box	<p>In the <b>Create New Task</b> dialog box and <b>Select Task</b> dialog box, it is now possible to use search.</p>

Table 1-1 New features (*continued*)

Feature	Description
Support for XFS file system	Deployment Solution now supports provisioning RHEL 7 computers with XFS file system.

## System requirements and supported platforms

Before you install IT Management Suite 8.0 HF5, 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 HF5 involves installation of Symantec Management Platform (SMP) 8.0 HF5 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 HF5

After you install this hotfix (8.0 HF5), 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 HF5 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 HF5, 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 <b>Actions</b> menu, click <b>Agents/Plug-ins &gt; Rollout Agents/Plug-ins</b> . Then, in the left pane, under <b>Symantec Management Agent</b> , locate and turn on the policies that upgrade the Symantec Management Agent on site servers.

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

Step	Action	Description
Step 2	Upgrade the site servers.	<p>In the Symantec Management Console, on the <b>Settings</b> menu, click <b>All Settings</b>. In the left pane, expand <b>Notification Server &gt; Site Server Settings</b>, 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 <b>Settings</b> menu, click <b>All Settings</b>. In the left pane, expand <b>Notification Server &gt; Site Server Settings &gt; Notification Server &gt; Task Service &gt; Advanced</b>, 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 <b>Settings</b> menu, click <b>All Settings</b>. In the left pane, expand <b>Notification Server &gt; Site Server Settings &gt; Notification Server &gt; Package Service &gt; Advanced &gt; Windows</b>, and then locate and turn on the <b>Windows Package Server Agent Upgrade</b> policy.</p>
Step 3	Upgrade the Symantec Management Agent on client computers.	<p>In the Symantec Management Console, on the <b>Actions</b> menu, click <b>Agents/Plug-ins &gt; Rollout Agents/Plug-ins</b>. Then, in the left pane, under <b>Symantec Management Agent</b>, locate and turn on the policies that upgrade the Symantec Management Agent on client computers.</p>
Step 4	Upgrade solution-specific agents and plug-ins.	<p>In the Symantec Management Console, on the <b>Actions</b> menu, click <b>Agents/Plug-ins &gt; Rollout Agents/Plug-ins</b>. 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"> <li>■ In the Symantec Management Console, on the <b>Actions</b> menu, click <b>Agents/Plug-ins &gt; Rollout Agents/Plug-ins</b>. Then, in the left pane, under <b>Symantec Management Agent</b>, locate and turn on the upgrade policies for the Symantec Management Agent.</li> <li>■ In the Symantec Management Console, on the <b>Settings</b> menu, click <b>All Settings</b>. In the left pane, expand <b>Notification Server &gt; Site Server Settings</b>, and then locate and turn on the upgrade policies for the site server plug-ins.</li> <li>■ In the Symantec Management Console, on the <b>Actions</b> menu, click <b>Agents/Plug-ins &gt; Rollout Agents/Plug-ins</b>. Then, in the left pane, locate and turn on the plug-in upgrade policies.</li> </ul>

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 HF5 are as follows:

**Table 1-3** Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF5

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.0.3577	8.0.3504
Altiris Client Task Agent	8.0.3577	8.0.3504
Altiris Client Task Server Agent	8.0.3558	N/A
Altiris Base Task Handlers	8.0.3577	8.0.3504
Altiris Pluggable Protocols Architecture Agent	8.0.3110	N/A
Inventory Agent	8.0.3521	8.0.3521

**Table 1-3** Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.0 HF5 (*continued*)

Agent or plug-in	Windows	UNIX/Linux/Mac
Application Metering Agent	8.0.3338	N/A
Server Inventory Agent	8.0.3543	8.0.3543
Inventory Rule Agent	8.0.3558	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	8.0.3558	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	8.0.3583	N/A
Deployment Package Server	8.0.3583	N /A
Deployment Plug-in for Windows (x64/x86)	8.0.3583	N/A
Deployment Plug-in for Linux (x64)	N/A	8.0.3583
Deployment Plug-in for Linux (x86)	N/A	8.0.3583
Deployment Plug-in for Mac	N/A	8.0.2246
Deployment NBS plug-in	8.0.3583	N/A
Symantec Workspace Streaming Agent	7.6.0.233	N/A
Symantec Workspace Virtualization Agent	7.6.233.0	N/A
Symantec Workspace Virtual Composer	7.6.0.233	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 HF5:

**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 HF5	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:

<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 HF5 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.

- Asset Management Solution  
See [“Asset Management Solution Fixed Issues”](#) on page 18.
- ITMS Management Views  
See [“ITMS Management Views Fixed Issues”](#) on page 19.
- Software Management Solution  
See [“Software Management Solution Fixed Issues”](#) on page 20.
- Inventory Solution  
See [“Inventory Solution Fixed Issues”](#) on page 21.
- Patch Management Solution  
See [“Patch Management Solution Fixed Issues”](#) on page 22.
- First Time Setup Portal  
See [“First Time Setup Portal Fixed Issues”](#) on page 22.
- 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:

- Symantec Installation Manager  
See [Table 1-5](#) on page 16.
- Notification Server  
See [Table 1-6](#) on page 16.
- Symantec Task Server  
See [Table 1-7](#) on page 17.
- Symantec Management Agent  
See [Table 1-8](#) on page 17.
- UNIX/Linux/Mac  
See [Table 1-9](#) on page 17.

**Table 1-5** Fixed issues for Symantec Installation Manager

Issue	Article link
After you apply Inventory Solution license in SIM, the SIM UI displays one license for Inventory for Network Devices instead of displaying this license for Inventory Solution.	N/A

**Table 1-6** Fixed issues for Notification Server

Issue	Article link
The <b>DriversDB</b> package that is larger than 30 GB fails to load in the Symantec Management Console.	N/A
The subfolders under the <b>Policies</b> and <b>Backup and Recovery</b> folders disappear if a role-based user clicks on them.	N/A
Generating a Package Snapshot fails if the Event Queue path is on a different drive than the drive where the final destination of the Snapshots is.	N/A
When you replicate <b>Server URL</b> with a copy of <b>Targeted Agent Settings</b> and HEP enabled from parent Notification Server to its children, the <b>Server URL</b> contains the URL of the parent server, and redirects the client computers of the child Notification Server to the parent Notification Server.	N/A
When you merge two computers that are located in different Organizational Groups, the resulting computer remains in both Organizational Groups after merging.	N/A
Internal hidden folder is not visible in Security Role Manager.	N/A
The newly imported computers that have Windows 10 Pro Anniversary Edition installed, are not displayed in the <b>Windows Computers with no Symantec Management Agent Installed</b> filter for agent push.	<a href="#">TECH236434</a>
After installing the IT Management Suite 8.0 HF4, the <b>Computer</b> resources are replicated down to the children in hierarchy, in case these <b>Computer</b> resources are included in the <b>Filters</b> that are replicated down.	N/A
In hierarchy, the HEP is not propagated to shadow policies which may lead to policies being disabled after the replication.	N/A
The reports that the automation policies deliver as attachments may contain non-readable symbols. This issue occurs only if the attachment is in CSV format.	N/A



**Table 1-7** Fixed issues for Task Server

Issue	Article link
UI issues of the <b>Tokens</b> dialog box: <ul style="list-style-type: none"> <li>Impossible to change the <b>Base Token Name</b> of a token.</li> <li>The <b>Base Token Name</b> is not properly displayed in Internet Explorer 10.</li> </ul>	N/A
In some circumstances, the <b>Altiris Object Host Service</b> cannot access its communication port because it is in use.	N/A
The <b>Restart Computer</b> task with <b>Shut down</b> option selected does not work unless you also check the <b>Force applications to close without prompting</b> option.	N/A

**Table 1-8** Fixed issues for Symantec Management Agent

Issue	Article link
On a computer that has Microsoft Windows 2012 R2 installed, the IIS binding certificate searches for a master certificate in an incorrect certificate store.	N/A
" <b>Package server could not access own Web Site using HTTPS</b> " appears in Package Server logs. Despite the error message, the packages are accessible.	N/A

**Table 1-9** Fixed issues for UNIX/Linux/Mac

Issue	Article link
If the computer gets merged, the Symantec Management Agent does not request a new GUID from Notification Server.	N/A
If the Symantec Management Agent receives an error for invalid resource ID in response to a policy request, it will not try to re-register on Notification Server.	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 1-10** Fixed issues for Deployment Solution

Issue	Article link
Software Delivery tasks fail after an image is deployed due to an old AexSWDPolicy.xml file.	<a href="#">TECH236051</a>
Deployment Solution fails to run a task on a client computer when booted in automation if the client computer status is <b>Retired</b> .	N/A

**Table 1-10** Fixed issues for Deployment Solution (*continued*)

Issue	Article link
DeployAnywhere copies tagged drivers at multiple places on a client computer.	N/A
If you add a new preboot driver in the <b>Driver Management</b> , it is not available in the <b>Preboot</b> drivers page.	N/A
After ITMS 8.0 HF3 installation, predefined computers and managed UEFI computers do not receive PXE menu if SQL is case-sensitive even if the following options are selected in the <b>NBS General Settings</b> page: <ul style="list-style-type: none"><li>■ <b>Respond to Predefined computers</b></li><li>■ <b>Respond to Managed computers</b></li></ul>	N/A
The name of the predefined computer is not retained when you deploy a Sysprep image in Linux preboot.	N/A
After you install IT Management Suite 8.0 HF2, Driver Manager may crash when you try to import drivers with some missing files.	N/A
For Linux computers, the domain account may get locked if the <b>Create Image</b> task attempts exceed the permissible number of attempts set for the Active Directory lockout policy.	N/A

## Asset 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 Asset Management Solution

Issue	Article link
<p>The following <b>Service and Asset Management</b> tasks fail:</p> <ul style="list-style-type: none"> <li>■ Add to Filter</li> <li>■ Assign Asset to Cost Center</li> <li>■ Assign Asset to Location</li> <li>■ Assign Computers Ownership to be the Primary User</li> <li>■ Assign Owner</li> <li>■ Assign Owner Percentages</li> <li>■ Assign User to Department</li> <li>■ Assign User to Company</li> <li>■ Assign User to Contract</li> <li>■ Cleanup Ownership</li> <li>■ Duplicate Computer Merge</li> <li>■ Duplicate User Merge</li> <li>■ Inventory Cleanup</li> <li>■ Inventory to Asset Synchronization</li> <li>■ Set Asset Status</li> </ul> <p>The following errors occur in Altiris Log Viewer:</p> <pre>Failed to check permission for item. Unexpected exception creating new task schedule.</pre>	N/A
<p>In the <b>Resource Change History</b> dialog box, the <b>Save</b> and <b>Save As</b> buttons do not save the changes that you do under <b>Filter Settings</b>.</p>	N/A
<p>When you run the <b>Generate Purchase Order Task</b> task, the following error appears in the log: <b>System.MissingMethodException: Method 'Altiris.Receiving.ReceivingHelpers.OperationHelper.GeneratePurchaseOrders' not found.</b></p>	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 1-12** Fixed issues for ITMS Management Views

Issue	Article link
The <b>Managed Software Delivery Policies</b> compliance filter runs incorrect parameter in the background.	<a href="#">TECH236147</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 1-13** Fixed issues for Software Management Solution

Issue	Article link
If a user manually turns on a Managed Software Delivery policy that contains a power management computer restart task, the policy behaves as follows: <ul style="list-style-type: none"> <li>Only the first task in the policy and the restart task run.</li> <li>After the computer restart, the policy runs according to its defined schedule.</li> </ul>	N/A
Software Discovery scan works incorrectly for the software product that has an apostrophe in the path of the software installation folder from uninstall string in the registry. The following error occurs:  An error occurred when running Software discovery by SMFAgent. Reregister SMFAgent.dll and try again.	N/A
Notification Server Events (NSE) are generated for every detection check on repeated policy executions.	N/A
Incorrect language is used on some of the Software Management Solution and Software Portal pages.	N/A
Windows 2016 Server and Windows 10 with the update 1607 should be removed from the following filters for the predefined Symantec Workspace Virtualization installation and upgrade policies: <ul style="list-style-type: none"> <li>Computers are available for Software Workspace Virtualization agent installation</li> <li>Computers are available for Software Workspace Virtualization agent upgrade</li> </ul> As Workspace Virtualization is not supported on these operations systems, the BSoD error is displayed after the installation of Symantec Workspace Virtualization Agent on the computers with these operations systems and the restart of such computers.	<a href="#">HOWTO125403</a> <a href="#">TECH235603</a>
Software package download on client computers loops when many Managed Software Delivery policies use the same package and download it from different custom locations at the same time.	N/A

**Table 1-13** Fixed issues for Software Management Solution (*continued*)

Issue	Article link
The package name in the <b>Evt_AeX_SWD_Package</b> data class is reported incorrectly.	N/A
The supersedence settings of a Managed Software Delivery policy work inconsistently if a software resource has multiple superseding or superseded software.	N/A
When a peer computer restarts during the peer-to-peer downloading of a software delivery package, the package status is reported incorrectly.	N/A

## 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
The CPU information and processor count are reported incorrectly for HP-UX 11i v3 (PA-RISC and Itanium) server computers.	N/A
The installed date in the <b>Patch Windows</b> data class is reported incorrectly.	N/A
The file rule <b>FileName contains &lt;file name&gt;</b> collects no data for the files that match this rule if the file rule <b>FileType equals &lt;file type&gt;</b> for the corresponding files is not present in the software scan.	N/A
Collection of inventory data for the Apache data classes never ends and increases memory consumption.	N/A
The data classes for MySQL version 5.7.x are reported incorrectly.	N/A
Software inventory scan gathers no data for the software product that has an apostrophe in the path of the software installation folder from the uninstall string in the registry. The following error occurs: An exception caught in m_pSMFAgent->InventoryScan2(bQuickScan,bSendFullINSE)	N/A
After you install the Inventory Plug-in, you can gather inventory using the options /fi, /dhi, /dswi, /fsi and /dsi of the utility <code>InvSoln.exe</code> only after you successfully run the corresponding predefined inventory policy on your client computers.	N/A
Inventory data for Oracle instances is not reported correctly from the UNIX/Linux Oracle database servers if the oratab files located on a client computer have extra characters at the ends of the lines.	N/A

**Table 1-14** Fixed issues for Inventory Solution (*continued*)

Issue	Article link
The custom inventory data classes that are created on the target Notification Server or a child Notification Server are not visible and not available for editing on the <b>Manage Custom Data Classes</b> page after migration or standalone replication of the custom data classes from another Notification Server or parent Notification Server.	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
The updates for the RealVNC vendor cannot be downloaded due to the SSL error.	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 1-16** Fixed issues for First Time Setup Portal

Issue	Article link
The data is not displayed in the <b>Discovered Computers</b> list.	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 1-17** Fixed issues for Workflow Solution

Issue	Article link
If a second model is used as an invocation target with a single output data variable, you cannot publish a workflow.	N/A

**Table 1-17** Fixed issues for Workflow Solution (*continued*)

Issue	Article link
For ServiceDesk 8.0 HF3, if you do not have the SuperAdmin rights, the search function does not work for the following: <ul style="list-style-type: none"> <li>■ The KB on <b>Home</b> page.</li> <li>■ The Articles on <b>Knowledge Base</b> page.</li> </ul>	N/A
The categories <b>Recent Articles</b> and <b>Popular Articles KB</b> are inaccessible on the Russian portal.	N/A
The <b>ProcessStarted Date</b> changes when you update the <b>Title</b> or the <b>Description</b> of the <b>Processes</b> .	<a href="#">TECH235792</a>
The <b>ModifiedOn</b> Column of the <b>ReportProcess</b> table logs the local time and not the UTC time.	N/A
The <b>Application Property</b> profile breaks if you create or modify a Profile Value Definition that contains a dash (-).	N/A

## Known Issues

IT Management Suite 8.0 HF5 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.
- Software Management Solution  
See "[Software Management Solution Known Issues](#)" on page 26.
- Inventory Solution  
See "[Inventory Solution Known Issues](#)" on page 25.

## 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 1-18](#) on page 24.

- Network Discovery  
See [Table 1-19](#) on page 24.

**Table 1-18** Known issues for Notification Server

Issue	Article link
Symantec Installation Manager is unable to install HF release on Notification Server because modifying the <code>web.config</code> file fails. This problem occurs only if you have modified the security settings of the Default web site. <b>Workaround:</b> Before installing the IT Management Suite 8.0 HF5, remove the security setting of the Default web site from the <code>web.config</code> file. After completing the installation, add the security settings back.	N/A
If you are using peer-to-peer downloading feature in ITMS 7.6HF7 (enabled through a point-fix), you must save any customization that you have made to the settings and restore them manually after upgrading to ITMS 8.0HF5 release, because peer-to-peer downloading settings are reset to default during the upgrade.	N/A

**Table 1-19** Known issues for Network Discovery

Issue	Article link
When you perform Network Discovery using SNMP protocol, the incorrect operating system is shown for Windows Server 2016 computers.	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
For Windows version later than Windows 8, the <b>Deploy Image</b> task with DeployAnywhere fails to install drivers on client computers.	N/A
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 <b>Partition</b> tab shows all partitions of LinuxSwap type.	N/A



**Table 1-20** Known issues for Deployment Solution (*continued*)

Issue	Article link
Sometimes the <b>Deploy Image</b> 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 <b>Primary file storage location</b> is specified in the <b>Package Server Settings</b> 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 <code>70-persistent-net.rules</code> from <code>/etc/udev/rules.d/</code> and restart the client computer.	N/A
For Windows 10 (1607) Anniversary update, the imaging task fails.  For details of the workaround, refer to the following article:  <a href="#">HOWTO125161</a>	<a href="#">HOWTO125161</a>

## 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 1-21** Known issues for Inventory Solution

Issue	Article link
When you upgrade the 7.x Inventory Pack for Servers Plug-in to 8.0 HF5, inventory task configuration files for the following predefined server inventory policies are removed from the <code>InvTaskConfig</code> folder: <ul style="list-style-type: none"> <li>■ <b>Collect Full Server Inventory</b></li> <li>■ <b>Collect Delta Server Inventory</b></li> </ul> In such case, you can gather server inventory using <code>InvSoln.exe/fsi</code> or <code>InvSoln.exe/dsi</code> only after you successfully run the predefined server inventory policies on your client computers.	N/A

**Table 1-21** Known issues for Inventory Solution (*continued*)

Issue	Article link
<p>You cannot view the names for some software components previously discovered on Mac computers after the Inventory Plug-in is upgraded to 8.0 HF5 and software inventory is collected for the first time after the upgrade on these computers.</p> <p>The software component names get displayed on the user interface after the <b>NS.Daily</b> task successfully runs at 2:10 A.M. by default.</p>	N/A

## Software 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 1-22** Known issues for Software Management Solution

Issue	Article link
<p>The supersedence settings of a Managed Software Delivery policy work inconsistently in the following cases:</p> <ul style="list-style-type: none"> <li>■ A software resource has a dependency on some Software Update or Service Pack.</li> <li>■ A software resource has a loop in its supersedence dependency.</li> </ul>	N/A
<p>After you run standalone Item Replication Rule to migrate new Managed Software Delivery policies or software delivery tasks, software package source is not distributed on target client computers.</p> <p>You need to import the required software packages to the target Notification Server again using the <b>Software Resource Replicator</b> utility. Note that you must uncheck the option <b>Do not import resources which already exists in NS</b>.</p>	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 <b>Supported Products A-Z</b> page, which is available at the following URL: <a href="https://www.symantec.com/products/products-az">https://www.symantec.com/products/products-az</a> Open your product's support page, and then under <b>Common Topics</b> , click <b>Release Notes</b> .
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"> <li>■ The Documentation Library, which is available in the Symantec Management Console on the <b>Help</b> menu.</li> <li>■ The <b>Supported Products A-Z</b> page, which is available at the following URL:  <a href="https://www.symantec.com/products/products-az">https://www.symantec.com/products/products-az</a>                              Open your product's support page, and then under <b>Common Topics</b>, click <b>Documentation</b>.</li> </ul>
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 <b>Help</b> 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"> <li>■ Click the page and then press the F1 key.</li> <li>■ Use the Context command, which is available in the Symantec Management Console on the <b>Help</b> menu.</li> </ul>

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.	<a href="#">Knowledge Base</a>

**Table 1-24** 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.	<a href="#">Unified Help System</a>
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"> <li>■ <a href="#">Deployment and Imaging</a></li> <li>■ <a href="#">Discovery and Inventory</a></li> <li>■ <a href="#">ITMS Administrator</a></li> <li>■ <a href="#">Mac Management</a></li> <li>■ <a href="#">Monitor Solution and Server Health</a></li> <li>■ <a href="#">Patch Management</a></li> <li>■ <a href="#">Reporting</a></li> <li>■ <a href="#">ServiceDesk and Workflow</a></li> <li>■ <a href="#">Software Management</a></li> <li>■ <a href="#">Server Management</a></li> <li>■ <a href="#">Workspace Virtualization and Streaming</a></li> </ul>