

Symantec™ IT Management  
Suite 8.1 RU6 powered by  
Altiris™ technology Release  
Notes



# Symantec™ IT Management Suite 8.1 RU6 powered by Altiris™ technology Release Notes

## Legal Notice

Copyright © 2018 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@symantec.com](mailto:customercare@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)

# Symantec IT Management Suite 8.1 RU6

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 8.1 RU6, the following new features are introduced:

Table 1-1 New features

Feature	Description
Expanded list of supported platforms for Symantec Management Agent.	<p>The following operating systems are now supported for the installation of the Symantec Management Agent and solution plug-ins:</p> <ul style="list-style-type: none"> <li>■ Red Hat Enterprise Linux 7.4 and CentOS 7.4 For the list of supported solutions and limitations refer to the following knowledge base article: <a href="http://www.symantec.com/docs/HOWTO127907">http://www.symantec.com/docs/HOWTO127907</a></li> <li>■ SUSE Linux Enterprise Server 12 SP3 and SUSE Linux Enterprise Desktop 12 SP3 For the list of supported solutions and limitations refer to the following knowledge base article: <a href="http://www.symantec.com/docs/HOWTO127910">http://www.symantec.com/docs/HOWTO127910</a></li> </ul>
<p>Extended health information for the Symantec Endpoint Protection clients.</p> <p>(Windows and Mac only)</p>	<p>The Symantec IT Management Suite RU6 enables you to report on the Symantec Endpoint Protection client (SEP agent) health and start the SEP service on client computers with SEP agent installed.</p> <ul style="list-style-type: none"> <li>■ Inventory Solution provides extended information for the SEP agents that are installed on client computers in your environment. To gather this information, ensure that the <b>SEP Agent</b> data class is enabled on an inventory policy or task page, at <b>Advanced Options &gt; Data Classes &gt; Software &gt; Common</b>.</li> <li>■ New pages are added to view the SEP agent health information: <ul style="list-style-type: none"> <li>■ On the <b>SEP Agent Health</b> summary page you can view the SEP Agent health information for all SEP agents installed on client computers in your environment.</li> <li>■ On the <b>SEP Agent Health</b> page in the <b>Computer Details</b> flipbook you can view the SEP Agent health information for a selected client computer.</li> </ul> </li> <li>■ The <b>SEP Agent Health Evaluation Settings</b> page lets you choose how the SEP Agent health is evaluated and then displayed on the <b>SEP Agent Health</b> summary page and on the <b>SEP Agent Health</b> page.</li> <li>■ The <b>Control SEP Service State</b> task lets you control the state of the SEP service on endpoints. Note that in RU6, you can only start the SEP service.</li> </ul> <p>For more information about extended health information for the Symantec Endpoint Protection clients, see the following knowledge base article: <a href="http://www.symantec.com/docs/DOC10947">http://www.symantec.com/docs/DOC10947</a></p>

**Table 1-1** New features (*continued*)

Feature	Description
Minor version displayed for Microsoft Windows 10 and Microsoft Windows 2016.	<p>The minor version for Microsoft Windows 10 and Microsoft Windows 2016 operating system is now displayed for a computer in Resource Manager and on the <b>General</b> page of the computer details flipbook in ITMS Management Views.</p> <p>The minor version is also displayed in the following reports:</p> <ul style="list-style-type: none"> <li>■ <b>Computers with Agent Installed</b></li> <li>■ <b>Computer last information update time</b></li> <li>■ <b>All Windows 2000/XP/2003/Vista/2008/7/8/2012/10/2016 Computers with no Agent</b></li> </ul> <p><b>Note:</b> This information becomes available only after you upgrade the Symantec Management Agent on the client computers to 8.1 RU6.</p>
Ability to access the Software Portal over the Internet on Cloud-enabled Mac computers.	<p>Users can securely access the enhanced user interface of the Software Portal over the Internet on Mac OS X or later computers that are in Cloud-enabled mode.</p> <p>For more information about using the enhanced user interface of the Software Portal, see the Mind Map <i>Making on-demand software available in the Software Portal</i> that is listed in the following knowledge base article:</p> <p><a href="http://www.symantec.com/docs/DOC9706">http://www.symantec.com/docs/DOC9706</a></p>
New reports to provide information about the subnets.	<p>The following new reports are introduced:</p> <ul style="list-style-type: none"> <li>■ <b>Subnets with Affiliated Sites</b></li> <li>■ <b>Subnets with Affiliated Sites by Computer</b></li> </ul> <p>Both reports have a drill-down report <b>View Computers in this subnet</b>.</p> <p>The reports are available in the Symantec Management Console, at <b>Reports &gt; Notification Server Management &gt; Server &gt; Subnets and Sites Info</b>.</p>
Added ability to download and use <b>ScreenCapture Utility</b> .	<p>From this release onwards, you can download and use the <b>ScreenCapture Utility</b> from a remote computer on which Workflow Solution is not installed.</p> <p>For more information, refer to the following knowledge base article:</p> <p><a href="http://www.symantec.com/docs/DOC10956">http://www.symantec.com/docs/DOC10956</a></p>



**Table 1-1** New features (*continued*)

Feature	Description
Workspace Virtualization components are upgraded to the version 7.6 HF10.	<p>In Software Management Solution 8.1 RU6, the following Workspace Virtualization components are upgraded to the version 7.6 HF10:</p> <ul style="list-style-type: none"> <li>■ Symantec Workspace Virtualization Agent (SWV Agent) (32/64 bit, 7.6.269.0)</li> <li>■ Virtual Composer (32/64 bit, 7.6.0.269)</li> <li>■ Streaming Agent (32/64 bit, 7.6.0.269)</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 8.1 RU6 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 HF10 Release Notes, please see the following link:  <a href="http://www.symantec.com/docs/DOC10725">http://www.symantec.com/docs/DOC10725</a></p>

## System requirements and supported platforms

Before you install IT Management Suite 8.1 RU6, read the section Hardware recommendation in the *IT Management Suite Planning for Implementation Guide* at the following URL:

<http://www.symantec.com/docs/DOC9470>

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

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

## General installation and upgrade information

The installation of IT Management Suite (ITMS) 8.1 RU6 involves installation of Symantec Management Platform (SMP) 8.1 RU6 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/DOC9500>

## Upgrade to IT Management Suite 8.1 RU6

After you install this release update (8.1 RU6), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.1 RU6 for Symantec Management Platform, you need to enable upgrade policies for all plug-ins and the Symantec Management Agent to upgrade the client computers.

To avoid issues with cross-dependencies, Symantec recommends to install all available RU6 components at once.

---

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

---

In ITMS 8.1 RU6, Symantec Installation Manager (SIM) automatically creates a registry backup in the support folder before starting the installation, upgrade, or release update 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 knowledge base article:  
<http://www.symantec.com/docs/TECH183086>

For more information about creating a support package, see the following knowledge base 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 8.1 to this release update, 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.
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.	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.

**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 <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/DOC9500>

## 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 8.1 RU6 are as follows:

**Table 1-3** Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU6

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.1.6049	8.1.6023
Altiris Client Task Agent	8.1.6049	8.1.6023
Altiris Client Task Server Agent	8.1.6060	N/A
Altiris Pluggable Protocols Architecture Agent	8.1.6029	N/A
Inventory Agent	8.1.6101	8.1.6101
Application Metering Agent	8.1.5636	8.1.5072 (Mac only)
Server Inventory Agent	8.1.5636	8.1.6101
Inventory Rule Agent	8.1.6049	8.1.6023
Monitor Plug-in	8.1.6039	8.1.6039
Package Server	8.1.5844	8.1.6023
Power Scheme Task Plug-in	8.1.4504	N/A
Software Update Plug-in	8.1.5620	8.1.5836
Software Management Framework Agent	8.1.6049	8.1.6023
Software Management Solution Agent	8.1.6065	8.1.6065
Virtual Machine Management Task Handler	8.1.5613	N/A
Deployment Task Server Handler	8.1.5622	N/A
Deployment Package Server	8.1.5622	N/A
Deployment Plug-in for Windows (x64/x86)	8.1.6034	N/A
Deployment Plug-in for Linux (x64)	N/A	8.1.4536
Deployment Plug-in for Linux (x86)	N/A	8.1.4536
Deployment Plug-in for Mac	N/A	8.1.4536
Deployment NBS plug-in	8.1.6034	N/A
Symantec Workspace Streaming Agent	7.6.0.269	N/A
Symantec Workspace Virtualization Agent	7.6.269	N/A

**Table 1-3** Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU6 (*continued*)

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Workspace Virtual Composer	7.6.0.269	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 8.1 RU6:

**Table 1-4** Post installation tasks for Deployment Solution

Upgrade	Windows automation folder	Mac automation volume	Linux automation folder
Upgrade from 8.1 to 8.1 RU6	Yes	Yes	Yes
Upgrade from 8.1 RU5 to 8.1 RU6	Yes	No	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 client computers

- 1 Run the **Deployment Automation Folder for Linux-Uninstall** automation folder uninstall policy.
- 2 Run the **Deployment Automation Folder for Linux-Install** automation folder install policy.

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 8.1 RU6 contains fixed issues for the following solutions and components:

- Symantec Management Platform  
See [“Symantec Management Platform Fixed Issues”](#) on page 16.
- Deployment Solution  
See [“Deployment Solution 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 19.
- Monitor Solution  
See [“Monitor Solution Fixed Issues”](#) on page 20.
- Patch Management Solution  
See [“Patch Management Solution Fixed Issues”](#) on page 20.
- 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:

- Symantec Installation Manager  
See [Table 1-5](#) on page 17.



- Notification Server  
See [Table 1-6](#) on page 17.
- Task Server  
See [Table 1-7](#) on page 18.
- Symantec Management Agent  
See [Table 1-8](#) on page 18.
- UNIX/Linux/Mac  
See [Table 1-9](#) on page 18.
- Network Discovery  
See [Table 1-10](#) on page 18.
- Data Connector  
See [Table 1-11](#) on page 18.

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

Issue	Article link
After changing the App Identity password in SIM, both SIM and Symantec Management Console will not load and the " <b>Symantec Management Server Error</b> " is displayed. The issue occurs when SIM detects that CMDB cannot be accessed after App Identity password change and performs configuration incorrectly.	N/A

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

Issue	Article link
Package Server fails to download a package from the Notification Server folder that has spaces in its name. The following error occurs: <b>"Error while downloading package: HTTP status 400: The server cannot process the request because the syntax is not valid."</b>	N/A
Active Directory Import tasks stay in a " <b>Starting Import rule ....</b> " state without performing any actual tasks. It is not possible to restart or stop the task.	<a href="#">TECH240407</a>
Internally merged computers cause Deployment Solution tasks to drop or fail.	<a href="#">TECH247228</a>
In specific conditions, the computers that are deleted from Active Directory are not being deleted from the database after an AD Import.	<a href="#">TECH233402</a>
After upgrading to IT Management Suite 8.1 RU5, the run time of Package Refresh task increased remarkably.	N/A
Package Servers and client computers send excessive Config Requests while trying to get their Agent Communication Profiles.	<a href="#">TECH249292</a>

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

Issue	Article link
The text of Task Server requirements message in the <b>Add/Remove Services</b> dialog box is updated to mention Microsoft .NET Framework 4.7 instead of Microsoft .NET Framework 4.6.	N/A

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

Issue	Article link
Client Task Agent registration issue in case authenticated connection fails by the server with unauthenticated error.	N/A
When you disable the <b>Cloud-enabled Management Settings</b> policy and apply it to the client computer, the CEM mode is turned off, but the CEM certificates are not completely removed from the client computer.	N/A
Symantec Management Agent stops responding during the connection speed test that uses SMB protocol. This issue occurs in rare cases and only when SMB v1 is disabled.	N/A

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

Issue	Article link
If distribution points update fails during product configuration, the ULM filters get broken and also target Windows computers.	N/A

**Table 1-10** Fixed issues for Network Discovery

Issue	Article link
Sometimes Network Discovery does not detect SNMP v1/v2 enabled devices with the default timeout values that are defined in Connection Profile.	N/A

**Table 1-11** Fixed issues for Data Connector

Issue	Article link
A CMDB rule that is set to use SQL Query with a large data set fails to perform the <b>Retrieve column names</b> operation.	N/A
Even if the <b>Report Export Rule</b> is configured not to add column headings to the data file (the option <b>CVS file contains column headings</b> is not checked), the export rule creates the file with column headings.	N/A
Data Connector export rule does not export data if the column names are present in the file data source without column data.	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 1-12** Fixed issues for Deployment Solution

Issue	Article link
A delay of 30 seconds in restarting a computer is observed after you run the <b>Apply System Configuration</b> task in a job, thus the remaining tasks of the job fail to run.	N/A
For Non-English languages, Deployment Solution fails to install automation folder on client computers.	N/A
For RHEL 6.9, Symantec Management Agent is not registered with the Task Server during the <b>Boot to Production</b> task in a <b>Scripted OS Install</b> job.	N/A
Computers that are imported from Active Directory are included in the predefined computer filter.	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 1-13** Fixed issues for Inventory Solution

Issue	Article link
The <b>Manage Custom Data classes</b> page times out due to long execution time for large custom data class tables.	<a href="#">TECH249335</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
When you add a user to a security role without the permission to view specific default filters in the <b>Favorites</b> folders on the <b>Software</b> and <b>Computers</b> view pages, this user can still see all the default filters.	N/A
When you edit a software component and upload a new icon, the changes are not immediately visible. The new icon is displayed only after you refresh the page.	N/A

**Table 1-14** Fixed issues for ITMS Management Views (*continued*)

Issue	Article link
When you create a computer filter or a report from the <b>Computers with software installed</b> list on the <b>Software Product Summary</b> flipbook, the results provided in the filter or the report may be different from those in the list.	N/A
In the <b>Software Product</b> dialog box, on the <b>Identify inventory</b> tab, the software <b>Installs</b> count includes client computers that have a custom asset status applied and are no longer <b>Active</b> .	N/A

## Monitor Solution Fixed Issues

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

**Table 1-15** Fixed issues for Monitor Solution

Issue	Article link
In some cases the Monitor Agent service (AexMetricProv.exe) may experience excessive memory usage.	N/A

## Patch Management Solution Fixed Issues

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

**Table 1-16** Fixed issues for Patch Management Solution

Issue	Article link
<p>During Red Hat metadata import, removal of obsolete channels fails because other items reference the channels.</p> <p>To properly remove excluded channels and their updates, perform the following steps:</p> <ol style="list-style-type: none"> <li>1. In the Symantec Management Console, on the <b>Home</b> menu, click <b>Patch Management</b>.</li> <li>2. On the Patch Management home page, expand <b>Red Hat Linux</b>, and then under <b>Settings</b>, click <b>MetaData Import Task</b>.</li> <li>3. On the <b>Import Patch Data for Red Hat</b> task page, under <b>Select software channels for import</b>, click <b>Import channels</b> to download the list of available software channels.</li> <li>4. Under <b>Import Options</b>, enable the option <b>Delete data for excluded software channels</b>, and then click <b>Save changes</b>.</li> <li>5. Run the <b>Import Patch Data for Red Hat</b> task.</li> </ol>	N/A
<p>When a remote server closes the connection unexpectedly and some physical files are partially downloaded, the re-download of the missing files starts but does not stop.</p>	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
<p>Quick Delivery tasks, Package Delivery tasks, and Managed Software Delivery policies stop running and fail because of timeout on Windows client computers. To resume running the tasks or policies, you need to restart the Symantec Management Agent.</p> <p><b>Note:</b> After the upgrade to 8.1 RU6, the stopped policies or tasks fail. You need to re-schedule the failed policies or tasks with non-repeat schedule.</p> <p><b>Note:</b> In the unlikely event that the issue repeats, restart the Symantec Management Agent to resume running the policies or tasks older than 8.1 RU6. You need to create new policies or tasks to resolve the issue for the future.</p>	N/A
<p>You cannot access the Software Portal Help Center and context-sensitive help when you open the enhanced UI on Windows computers with Cloud-enabled Management enabled.</p>	N/A

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

Issue	Article link
When you customize the Software Portal header with your company-branded background image, you cannot upload an image file with the name that contains a space.	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
Symantec Endpoint Protection (SEP) Workflow Component do not connect to a SEP 14 Server.	N/A
Incorrect time is displayed when you manually set time zone to UTC.	N/A
If a DNS alias is configured, you cannot expand the list of project names.	N/A
The Process Action <b>Send Email</b> to a group of recipients is not sorted alphabetically.	N/A
Set SLA component does not work with the following Start Date Variables: <ul style="list-style-type: none"> <li>■ UseProcessStart</li> <li>■ UseCurrentDate</li> </ul>	N/A
A validation error is displayed if you use a Dynamic Model as source for Grid element with Dropbox with some components in the model.	N/A
The <b>WebChart</b> component does not show data from the Process Variables or the Dynamic Model.	N/A
Errors are logged when you save a knowledge base article with images.	N/A
The <b>Send Email</b> windows of the <b>Process Action</b> does not close automatically after a confirmation email is sent.	N/A
When you try to access some project links in the <b>Process Manager</b> portal, following error is displayed:  Generic PM Error	N/A
An error is displayed if you create an Administrator account in a ServiceDesk environment with an email address of more than 36 characters.	N/A

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

Issue	Article link
When you use a variable to represent date and time or if you use a dynamic model to generate a variable for date and time in PauseSLA or CompleteSLA components, an error is logged.	N/A
The Symantec Data Loss Prevention (DLP) Workflow Components of Symantec.Components.DLP.Reporting.dll are not compatible with DLP 15.0 Authentication method.	N/A
If you select to use Angular JS Capability at project and component level, the data is not displayed in grids.	N/A
You can edit cell data even if Angular JS Grid component Grid Mode is configured for <b>Select Items</b> mode.	N/A
When you schedule a report in the Report Scheduler, the email account used to send and run the report is admin@symantec.com even if you have set another user name and email address.	N/A
The SLA Status Update causes an error if the email address is longer than 36 characters.	N/A
When you try to close the Form Builder, it also tries to close the browser window.	N/A
Time data is not included in the Excel reports if you export reports with Date.	N/A
The Date and the Time references are not set to UTC for LogicBase.Ensemble.WorkflowTasks.TaskResponsePage and TaskResponsePage.Asp.cs.	N/A

## Known Issues

IT Management Suite 8.1 RU6 contains known issues for the following solutions and components:

- Deployment Solution  
See [“Deployment Solution Known Issues”](#) on page 24.
- Inventory Solution  
See [“Inventory Solution Known Issues”](#) on page 25.
- Software Management Solution  
See [“Software Management Solution Known Issues”](#) on page 25.

## 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 1-19** Known issues for Deployment Solution

Issue	Article Link
<p>For SUSE 12 SP3 Desktop edition, the <b>Scripted OS Install</b> task fails and displays the following error:</p> <pre>Packages could not be found. .</pre> <p>Workaround:</p> <p>Click <b>OK</b> in the dialog box that appears on the client computer.</p>	N/A
<p>Failed to update preboot configuration packages on package servers. An error is logged in the Deployment Solution: reloadPackage.</p> <p>Workaround:</p> <p>If you add drivers to the preboot database or import a new WinPE, you must manually run the package refresh task.</p>	N/A
<p>The <b>Install Windows OS</b> task fails if you use the default setting for the configuration option.</p> <p>Workaround:</p> <p>Select another option from the drop-down list for the <b>Configuration</b> option and then select the <b>Use inventory data to reconfigure computer</b>.</p>	N/A
<p>For WinPE 10, the <b>Partition Disk</b> task is unable to create required partitions.</p>	N/A
<p>Automation folder is no longer functional after you deploy a BIOS-based image to a UEFI computer.</p>	N/A
<p>Sometimes, package upload from Symantec Management Console fails for OS Files and Drivers upload.</p>	N/A
<p>For macOS Sierra 10.13 NetInstall (SOI) is not currently supported.</p>	N/A
<p>For macOS Sierra 10.13 sometimes the <b>Deploy Image</b> task of Apple file system containers fails with following error:</p> <p>Could not mark APFS container as new/unique.</p>	N/A
<p><b>Deploy Image</b> task fails to deploy an image of a computer with RHEL 7.2 operating system and XFS file system.</p>	N/A
<p>For macOS Sierra 10.13 clients, you cannot create image of volumes of Apple File System containers.</p>	N/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 1-20** Known issues for Inventory Solution

Issue	Article link
The <b>Control SEP Service State</b> task fails to start the Symantec Endpoint Protection service and the return code 4 is reported when the startup type of the service on a client computer is set to <b>Disabled</b> .	N/A
<p>The status of an unmanaged Symantec Endpoint Protection (SEP) agent is incorrectly reported on the <b>SEP Agent Health</b> page in the <b>Computer Details</b> flipbook.</p> <p>After the inventory data is gathered for the SEP agent that is not centrally managed by a management server, the <b>SEP Manager Server</b> status is displayed as <b>No data available</b>.</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 1-21** Known issues for Software Management Solution

Issue	Article link
<p>The Software Portal user can configure a user profile so that the <b>Installation Succeeded</b> notification appears when the application that the user has requested in the Software Portal is installed on the user's device.</p> <p>However, on Windows devices, the notification may be displayed for too short time (less than 30 seconds), and the user may overlook it.</p>	N/A
The non-working link to the Software Portal appears in the Symantec Management Agent context menu on a Mac computer that has no access to the Software Portal if you enable the <b>Software Portal Client Access Policy</b> , check the corresponding option, and then target the policy to the Mac computer without Software Management plug-in installed.	N/A
<p>Enhanced user interface of the Software Portal (enhanced UI) is not supported in Safari 8 that is included with Mac OS X 10.10.</p> <p>Workaround:</p> <p>You can open the enhanced UI after you upgrade to Mac OS X 10.10.5 and Safari 10.</p>	N/A

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

Issue	Article link
Even if you apply the legacy UI to the Software Portal, the enhanced UI opens on client computers with Cloud-enabled Management enabled.	N/A

## Where to get more information

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

**Table 1-22** Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	<p>The <b>Supported Products A-Z</b> page, which is available at the following URL:</p> <p><a href="https://www.symantec.com/products/products-az">https://www.symantec.com/products/products-az</a></p> <p>Open your product's support page, and then under <b>Common Topics</b>, click <b>Release Notes</b>.</p>
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></li> </ul> <p>Open your product's support page, and then under <b>Common Topics</b>, click <b>Documentation</b>.</p>
Help	<p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p>	<p>The Documentation Library, which is available in the Symantec Management Console on the <b>Help</b> menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <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 1-23** Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	<a href="#">Knowledge Base</a>
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.	The links to various groups on Connect are as follows: <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>