

Symantec™ IT Management Suite 8.5 RU1 Release Notes



Symantec™ IT Management Suite 8.5 RU1 Release Notes

Legal Notice

Copyright © 2019 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

<https://www.symantec.com>

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

<https://support.symantec.com>

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

<https://www.symantec.com/connect>

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

<https://entced.symantec.com/default/ent/supportref>

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Symantec IT Management Suite 8.5 RU1

This document includes the following topics:

- [About Symantec 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 Symantec IT Management Suite

Symantec 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 8.5 RU1, 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"> ■ Red Hat Enterprise Linux 7.5 and CentOS 7.5 For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/HOWTO128504 ■ Red Hat Enterprise Linux 6.10 and CentOS 6.10 For the list of supported solutions and limitations refer to the following knowledge base article: https://www.symantec.com/docs/DOC11247 ■ Windows 10 October 2018 Update (1809) and Windows 10 Enterprise LTSC 2019 https://www.symantec.com/docs/HOWTO128718 ■ SUSE Linux Enterprise Server 15 and SUSE Linux Enterprise Desktop 15 https://www.symantec.com/docs/DOC11248 ■ Windows Server 2019 https://www.symantec.com/docs/DOC11249 ■ Core installation of Windows Server 2016 LTSC, 1709, and 1803 https://www.symantec.com/docs/DOC11250 ■ macOS 10.14 Mojave https://www.symantec.com/docs/HOWTO128948 ■ Ubuntu 18.04 LTS https://www.symantec.com/docs/HOWTO128508
Support for SQL Server 2012 SP4	Support for SQL Server 2012 SP4 is added for 8.1 RU7 and 8.5 RU1.
Expanded list of supported platforms for Internet gateway.	<p>The following operating system is now supported for the installation of Internet gateway:</p> <ul style="list-style-type: none"> ■ Windows Server 2019
Expanded list of supported platforms for Site Servers.	<p>The following operating systems are now supported for the installation of Task Server, Package Server, and Monitor Server:</p> <ul style="list-style-type: none"> ■ Windows Server 2019 ■ Core installations of Windows Server 2016 LTSC, 1709, and 1803
Added support for Windows 10 Build 1809 ADK	<p>Support for Windows 10 Build 1809 ADK is added with known issues. See “Deployment Solution Known Issues” on page 27. For more information, refer to the following article: Info3561</p>

Table 1-1 New features (*continued*)

Feature	Description
Ability to deploy software in real time with Time Critical Management.	<p>In the Time Critical Management workspace, you can deploy patches or software packages to your endpoints in real time to protect your environment as quickly as possible.</p> <p>Deploying software to an endpoint in real time</p>
Reports quick task in Endpoint Management Workspaces	<p>The Reports quick task enables users to run and view Notification Server reports in the Symantec Endpoint Management Workspaces.</p> <p>Setting up the Reports quick task</p>
Change Asset Status quick task in Endpoint Management Workspaces	<p>The Change Asset Status quick task enables users to update asset statuses in the Symantec Endpoint Management Workspaces.</p> <p>Setting up the Change Asset Status quick task</p>
Patch Management Solution support for Windows 10 compact update packages.	<p>Starting from the patch management metadata for Windows release 7.3.194, Patch Management Solution supports new compact update packages introduced in Microsoft Windows 10 1809.</p> <p>Windows 10 compact updates replace delta and cumulative updates for Windows 10 versions starting from 1809. The compact update package is a smaller file that contains all required fixes and provides better installation performance.</p> <p>For more information about compact updates support, see the knowledge base article TECH251853</p> <p>Note: Windows 10 monthly delta and cumulative updates continue to service Windows 10 versions earlier than 1809 until February 2019.</p> <p>For more information about delta and cumulative updates support, see the knowledge base article DOC9705</p>
Enhanced superseded update clean-up process.	<p>The following options extend the existing ability to disable the rollout of superseded software updates:</p> <ul style="list-style-type: none"> ■ Disable rollout of superseded updates if policies with the corresponding superseding updates exist ■ Delete superseded updates from software update policies ■ Delete superseded updates from software update policies if policies with the corresponding superseding updates exist
Digital signature verification of the software update catalog files.	<p>The Import Patch Data task validates the digital signature of software update catalog files before importing software management resources from the files into the Configuration Management Database.</p>

Table 1-1 New features (*continued*)

Feature	Description
New vendors support in Patch Management Solution.	<p>As of 10/31/2018, Patch Management Solution for Windows lets you install software updates for software from new vendors, for example, Gimp.org and TortoiseSVN.</p> <p>For the complete list of the vendors that Patch Management Solution for Windows supports, see the following knowledge base article: https://www.symantec.com/docs/HOWTO79563</p>
New statuses of software updates in Patch Management Solution.	<p>On the Patch Remediation Center page and in the Bulletins and Updates report, the Status column lets you view the download status of software updates for a bulletin.</p> <p>The status is Disabled if you have disabled the bulletin.</p> <p>The status is Enabled if you have created a policy for this bulletin and included all its updates.</p> <p>The status is Partial if you have created a policy for this bulletin but included only part of its updates.</p> <p>Otherwise no status is provided. For example, in case of a newly added bulletin or an enabled bulletin for which you have deleted a policy.</p>
Automation policies support for Windows Update patching.	<p>Patch Management Solution for Windows automation policies support reporting for software update policies that contain Windows Update Agent updates.</p> <p>For more information about Windows Update patching, see the following knowledge base article: http://www.symantec.com/docs/DOC11127</p>
Improved performance of Task Servers.	Each Task Server can now manage up to 15,000 endpoints.
Service recovery options for Internet gateway service.	Service recovery options are added for Internet gateway service in cases of accidental service shutdown.
More options for configuring throttling.	<p>The following new options are added for configuring throttling periods for Symantec Management Agent:</p> <ul style="list-style-type: none"> ■ You can select specific days when throttling should be used. ■ You can choose new throttling type Range for a throttling period.
Extended information about package servers available on the Symantec Management Agent UI.	The Package Server tab in the Symantec Management Agent UI now displays if the package server is constrained. It also displays the site for which this package server serves the packages.

Table 1-1 New features (continued)

Feature	Description
Changes in the reports of sites and subnets.	The following changes are done in the reports of sites and subnets: <ul style="list-style-type: none"> All reports of sites and subnets are moved under Reports > Notification Server Management > Server > Subnets and Sites Info. Two new reports are created: Site Servers and Subnet by IP. New parameters and pickers are added to the reports.
TCM Task Started message is added to the list of NS Messages for Automation Policies.	TCM Task Started message allows to trigger Automation Policy every time you start inventory update, software deployment, or any other task in the Time Critical Management portal.
Reporting the last agent communication time for computers with outdated inventory data.	A new column Last Agent Communication is added to the Inventory Solution report Computers that have not reported inventory in last N days to provide the information about the last time the Symantec Management Agent installed on the client computer has communicated with the Notification Server.
Improved UI of the report builder.	On the New Report page, under Formatting Style , an example is now added that provides guidelines of the acceptable content.
Added IMAP4 email components in Workflow Solution.	In Workflow Solution, the following IMAP4 email components are added using the ASPOSE library: <ul style="list-style-type: none"> IMAP4 Get Folder List New IMAP4 Get Message Count New IMAP4 List New IMAP4 Mark Message New <p>The Old Quicksoft library email components are kept as is. The ASPOSE library components are added with the "New" keyword.</p> <p>All the ASPOSE library components are added under the Process Components > Section of the components list.</p>

System requirements and supported platforms

Before you install Symantec IT Management Suite 8.5 RU1, read the section Hardware recommendation in the *IT Management Suite Planning for Implementation Guide* at the following URL:

<http://www.symantec.com/docs/DOC11101>

For information about the supported operating systems in Symantec Management Platform and the Symantec 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) 8.5 RU1 involves installation of Symantec Management Platform (SMP) 8.5 RU1 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/DOC11093>

Warning: Before you run any repair or reconfigure Deployment Solution from Symantec Installation Manager, read the following article:

[TECH250873](#).

Upgrade to IT Management Suite 8.5 RU1

The following on-box and off-box upgrade scenario is supported:

- From IT Management Suite 8.5 to IT Management Suite 8.5 RU1

After you install this release update (8.5 RU1), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.5 RU1 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 RU1 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 8.5 RU1, 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 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 Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins . Then, in the left pane, under Symantec Management Agent , locate and turn on the policies that upgrade the Symantec Management Agent on site servers.

Table 1-2 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 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> <p>Note: Ensure that all operating system updates and antivirus software updates are installed on the site server before starting the upgrade of Symantec Management Agent and Site Server services. Unfinished updates may interfere with the upgrade process.</p>
Step 3	Upgrade the Symantec Management Agent on client computers.	<p>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.</p>

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.

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/DOC11093>

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 8.5 RU1 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.5 RU1

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.5.3643	8.5.3639
Altiris Client Task Agent	8.5.3643	8.5.3633
Altiris Client Task Server Agent	8.5.3624	N/A
Altiris Pluggable Protocols Architecture Agent	8.5.3610	N/A
Inventory Agent	8.5.3687	8.5.3687
Application Metering Agent	8.5.3687	8.5.3041 (Mac only)
Server Inventory Agent	8.5.3687	8.5.3687
Inventory Rule Agent	8.5.3643	8.5.3633
Monitor Plug-in	8.5.3615	8.5.3615
Package Server	8.5.3643	8.5.3633
Power Scheme Task Plug-in	8.5.3006	N/A
Software Update Plug-in	8.5.3622	8.5.3049
Software Management Framework Agent	8.5.3643	8.5.3633
Software Management Solution Agent	8.5.3627	8.5.3627
Virtual Machine Management Task Handler	8.5.3603	N/A
Deployment Task Server Handler	8.5.3663	N/A
Deployment Package Server	8.5.3663	N/A
Deployment Plug-in for Windows (x64/x86)	8.5.3663	N/A
Deployment Plug-in for Linux (x64)	N/A	8.5.3663
Deployment Plug-in for Linux (x86)	N/A	8.5.3663
Deployment Plug-in for Mac	N/A	8.5.3663
Deployment NBS plug-in	8.5.3663	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 8.5 RU1 (*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 8.5 RU1:

Table 1-4 Post installation tasks for Deployment Solution

Upgrade	Windows automation folder	Mac automation volume	Linux automation folder
Upgrade from 8.5 to 8.5 RU1	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 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

Note: This document includes only the fixed issues resolved within the IT Management Suite version 8.5 RU1. For more information about the fixed issues in IT Management Suite 8.5, see the following release notes:

<http://www.symantec.com/docs/DOC11102>

IT Management Suite 8.5 RU1 contains fixed issues for the following solutions and components:

- Symantec Management Platform
See “[Symantec Management Platform Fixed Issues](#)” on page 17.
- Asset Management Solution
See “[Asset Management Solution Fixed Issues](#)” on page 19.
- Deployment Solution
See “[Deployment Solution Fixed Issues](#)” on page 20.
- Inventory Solution
See “[Inventory Solution Fixed Issues](#)” on page 21.
- Inventory Pack for Servers
See “[Inventory Pack for Servers Fixed Issues](#)” on page 21.
- IT Management Suite integrations
See “[Fixed issues of IT Management Suite integrations](#)” on page 21.
- Monitor Solution
See “[Monitor Solution Fixed Issues](#)” on page 22.
- Patch Management Solution
See “[Patch Management Solution Fixed Issues](#)” on page 22.
- Software Management Solution
See “[Software Management Solution Fixed Issues](#)” on page 23.

- Workflow Solution
See [“Workflow Solution Fixed Issues”](#) on page 25.

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 17.
- Task Server
See [Table 1-6](#) on page 18.
- Symantec Management Agent
See [Table 1-7](#) on page 18.
- Network Discovery
See [Table 1-8](#) on page 19.
- Pluggable Protocol Architecture (PPA)
See [Table 1-9](#) on page 19.
- Data Connector
See [Table 1-10](#) on page 19.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
<p>Off-box upgrade may take very long time because of the low performance of task-schedule handling during the upgrade process.</p> <p>Note that the problem lies within standard Windows API calls that are used to re-create the schedules. As a workaround, the re-creation of schedules has been moved to post-upgrade activities.</p>	N/A
<p>If the Symantec Management Agent uses persistent connection in CEM mode, it does not connect to proper Internet Site Servers.</p>	N/A
<p>In a hierarchy setup, the Replicate Now action may hang the console if destination server is not available.</p>	N/A
<p>After the upgrade or re-installation of Internet gateway, the Windows Firewall rule for Internet gateway does not function properly before system reboot and CEM agents are not able to connect to Notification Server via Internet gateway.</p>	TECH251954

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

Issue	Article link
Upgrade to ITMS 8.5 hangs with errors of ANONYMOUS user trying to access SQL database: "SQL connection failed, current user=Domain\User - Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'"	N/A
Very long SQL queries for Filter definition may cause issues with delta Filter membership updates.	N/A
Network devices, such as load balancers, may keep excessive WebSocket connections, causing memory leak in Symantec Management Agent.	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
ITMS installation or upgrade may fail in Symantec Installation Manager if IIS is stopped. For example, IIS is temporarily stopped during Task Server installation.	N/A

Table 1-7 Fixed issues for Symantec Management Agent

Issue	Article link
The import of a package that has spaces in its folder name or file name fails with the following error: "Error while downloading package: HTTP status 400: The server cannot process the request because the syntax is not valid."	TECH249435
Basic inventory send incorrect operating system type (OS type). For example, the OS Type for Windows 7 Professional is reported as Business .	N/A
When package download from a Package Server fails and the download retries also fail, the client is not redirected to download the package from Notification Server and package download fails.	N/A
After upgrading to IT Management Suite 8.5, the following problems occur on package servers: <ul style="list-style-type: none"> ■ A lot of packages are in Pending state and download very slowly (or do not download at all, remaining in Pending state). ■ After triggering Package Refresh on package server, some packages are not fully downloaded and remain in retry loop. For some packages, the download does not even start. 	TECH252298
After resume system events (sleep, hibernate) and also after Symantec Management Agent start, the package delivery does not reset the timers that are used for GetPackageInfo.aspx requests.	TECH251875

Table 1-7 Fixed issues for Symantec Management Agent (*continued*)

Issue	Article link
The Package Server tab in the Symantec Management Agent UI shows duplicate records for all packages when several users are logged in to the same site server.	N/A
Parsing long (more than 50 characters) operating system data from AD Import does not function properly.	N/A
Peer-to-peer communication between Symantec Management Agents fails in case Windows network adapter remains in Identifying... state.	TECH252171

Table 1-8 Fixed issues for Network Discovery

Issue	Article link
Network Discovery is not able to discover active and accessible devices that are outside of the subnet where the Notification Server is.	N/A
Network Discovery task discovers incorrect MAC address of a device and causes incorrect resource merging.	N/A
Network Discovery task discovers correct MAC address of a device but then assigns an incorrect MAC address to it. This issue occurs only for Weidmueller switches.	N/A
In the Topology View , incorrect number of linked devices is shown for the root device. The Network Discovery task gets connectivity information only for 33 devices, even when there are more devices connected.	N/A

Table 1-9 Fixed issues for Pluggable Protocol Architecture (PPA)

Issue	Article link
PluggableProtocols assembly installation may fail on the Microsoft Windows Server 2012 R2 operating system.	TECH251784

Table 1-10 Fixed issues for Data Connector

Issue	Article link
Data import with pre-processing script does not display the import results correctly until you click Refresh button.	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
Bulk edit option fails when you try to edit Computer or Virtual Machine resource types.	TECH251799

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
The Apply System Configuration task fails on Mac OSx after you upgrade to Deployment Solution 8.1 RU7.	TECH251154
The extract SSL policy fails to extract certificate on a Windows 2016 site server with domain certificate.	N/A
SUSE 15 server and desktop options are not supported for Linux SOI task.	N/A
The Copy File task fails in Software Delivery Policy. The following error is displayed: <code>copyFilePkgGuid is null</code>	N/A
The Install Windows OS task fails as Altiris.Deployment.OSFlavors throws exception.	N/A
Deploy Image job with DeployAnywhere fails as there are no drivers download.	TECH251608
The Default column of the Initial Deployment Settings page is large and cannot be resized.	TECH251744
Automation folder installation fails with a return code of 2.	N/A
In the Restore Image task, an error message is displayed when you try to select an image from the drop-down list.	N/A
iPXE does not auto-select PXE Boot image that is set on the NBS General Settings page for unknown, predefined, or managed computers.	TECH251431
DeployAnywhere logs are not copied to the logs directory at the following path: <code>x:\program files\symantec\deployment\logs</code>	TECH251139
When you add a predefined computer, an error is displayed on the PredefinedComputerEditor.aspx page.	TECH251491
The Scripted OS Install (SOI) task Fails in automation environment.	TECH250575

Table 1-12 Fixed issues for Deployment Solution (*continued*)

Issue	Article link
For Deployment Solution 8.5, it takes more than 10 minutes for the SBS server to get the Imaging package for a clean install.	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
Inventory Solution incorrectly reports the last start up time on AIX and HP-UX server computers.	N/A
Inventory Solution gathers data for all discovered USB devices but the data class USB Devices contains inventory data only for USB storage devices.	N/A

Inventory Pack for Servers 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 Pack for Servers

Issue	Article link
Server inventory incorrectly reports database name for Oracle 11g Express Edition as 10g.	N/A

Fixed issues of IT Management Suite integrations

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 of IT Management Suite integrations

Issue	Article link
If you try to add the Symantec Endpoint Protection Manager Server in the Symantec Management Console that is running on German language, the following error occurs: Error: Authentication failed. Provide valid Server details....	N/A

Table 1-15 Fixed issues of IT Management Suite integrations (*continued*)

Issue	Article link
SEP host integrity feature creates too many logs and slows down the event queue processing.	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 1-16 Fixed issues for Monitor Solution

Issue	Article link
In the Rule Library , when you create a new metric rule and try to add any metric to it, a dialog box with an error message appears.	N/A
In the Metric Library , when you try to edit a Compound or Command type metric, and error message is displayed: The data could not be loaded.	N/A

Patch Management Solution Fixed Issues

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

Table 1-17 Fixed issues for Patch Management Solution

Issue	Article link
After you perform an upgrade from ITMS 8.0 HF6 to 8.5, the upgraded software update policies and newly created after the upgrade policies do not work properly on the Linux client computers that have the software update plug-in less than 8.1 installed.	N/A
Automation policy report Software Update Policy Failed does not return any results for a failed software update policy that contains Windows Update Agent updates.	N/A
Client computers of the child Notification Server re-download the assessment package after each replication job even if no change occurs in the catalog file with information about the software updates selected for vulnerability assessment on the parent Notification Server.	N/A
If an assessment package is not ready during the software update policies evaluation process, the Notification Server gets multiple requests for the assessment package information.	N/A

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

Issue	Article link
The Import Patch Data for CentOS task fails to import updates for the CentOS 7 Updates channel.	N/A
<p>If you have the source Notification Server that has IT Management Suite (ITMS) version 8.0 or later with a custom installation directory, and the migration wizard is installed to this custom directory, the following issue occurs:</p> <ul style="list-style-type: none"> ■ Patch Management Solution is not listed in the Symantec Notification Server Migration Wizard, on the Exporter Configuration page, because Patch Management Solution components are installed into the default location C:\Program Files\Altiris\Upgrade\... <p>Workaround:</p> <p>Move Patch Management Solution components from the default location to the custom location.</p>	N/A
<p>Bulletin data for CentOS is incomplete because announcements for CR repository are not tracked.</p> <p>Note: To include newly added errata, run CentOS patch data import in full mode after upgrading to ITMS 8.5 RU1.</p>	N/A
<p>It is not possible to create a new folder under Patch Management > Software Update Policies > Windows. The following error is displayed in logs:</p> <p>"Failed to get list of Item actions"</p> <p>This problem occurs if there are already many items created under this folder.</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 1-18 Fixed issues for Software Management Solution

Issue	Article link
Each Managed Software Delivery compliance check on client computers generates and sends to Notification Server an event (NSE) even if no data has changed since the last check. An excessive number of NSEs can overload Notification Server and increase network traffic.	N/A
When you configure a Managed Software Delivery policy to run once and delete the unused packages, and the policy fails to run, the downloaded packages are not deleted from the client computer in the specified amount of time.	N/A

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

Issue	Article link
In the Symantec Management Agent UI, the Software Delivery tab incorrectly reports the last package status as disabled for an active delivery policy that is scheduled to run in future.	N/A
<p>In the Symantec Management Agent UI, the Software Delivery tab does not display detailed information about the last download and execution status of an execution task in a managed delivery policy.</p> <p>Starting from 8.5 RU1, you can view the following statuses of an execution task:</p> <ul style="list-style-type: none"> ■ Package Download pending ■ Downloading package ■ Command line start pending ■ Running command line 	N/A
If you have 2 software resources with the same name and want to edit one of them, not all categories are visible on the Manage Publications page, in the Edit Publication dialog box.	TECH251679
The report Software Compliance Detailed Summary displays duplicate rows for a computer that is targeted in a scheduled but not yet applied delivery policy.	N/A
When you use the Import Software wizard to create a software resource for a package and source the package from the Software Library, the process is slow and times out.	N/A
When you import an MSI installation file into the Software Library, the import fails because the upgrade code data cannot be retrieved from the file.	N/A
In environments with hierarchy, if you modify a Package Delivery task on the parent Notification Server, and then replicate it down, the corresponding task on the child Notification Server loses the previously completed task instance from the UI.	N/A
<p>An incorrect installation command line is generated during the import of SEP installation package for Mac. As the result, SEP agent is not installed properly and cannot communicate with SEP Manager.</p> <p>Note: The fix for this issue works only after you upgrade Symantec Management Agent to 8.5 RU1 on client computers, and then create a new SEP delivery policy for Mac.</p>	N/A
In the API, if you use the value Windows Batch Installation File for the parameter InstallationFileType , the method fails with an error. The issue occurs when you have the German OS or the English OS with the German language selected in the Symantec Management Console.	N/A
Software Delivery reports appear to be slow.	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 1-19 Fixed issues for Workflow Solution

Issue	Article link
During upgrade, the Install Readiness Check did not check for database mirroring.	N/A
<p>The following fields are not localized:</p> <ul style="list-style-type: none"> ■ Allow Add new Row ■ Allow Delete Row 	N/A
The drop-down list items in the Dynamic Model load several times when the page reloads.	N/A
Credentials are cached for web service caller components.	N/A
Some reports are not locked for editing and allow the users to modify out of the box reports.	N/A
<p>Following error is displayed if the password type application property includes the tilde symbol:</p> <p>Unable to access Ensemble to get the Application Property Profile Values.</p>	N/A
When you use a localized version of Workflow, the Process View Page does not display properly.	N/A
Sorting on Report Column does not work.	N/A
Modifying parameters at run-time for 'SQL Query with Parameters' removes line breaks from the query.	N/A
The <code>localserversetup.xml</code> file which is present at <code>\Program Files\Symantec\Workflow\Server Extensions</code> stores passwords in clear text.	N/A
Variables are displayed in the left pane only till the 'Iterate Text File Lines' component on the 'Next Line' path exits.	TECH251163
Merge text component does not handle <code><</code> , and <code>></code> in a variable.	N/A
<p>No error or warning is displayed when Password type application property includes special characters.</p> <p>The Password type application property is encrypted and saved with incorrect value.</p>	N/A

Table 1-19 Fixed issues for Workflow Solution (*continued*)

Issue	Article link
When you use Create From Request or Create From Sample form in the REST Generator to create the Response Content the generator crashes.	TECH251643
Cannot group a report by a column when a space is included in the title.	TECH251302

Known Issues

Note: This document includes only the issues that were found within the IT Management Suite version 8.5 RU1. For more information about the known issues in IT Management Suite 8.5, see the following release notes:

<http://www.symantec.com/docs/DOC11102>

IT Management Suite 8.5 RU1 contains known issues for the following solutions and components:

- Symantec Management Platform
See “[Symantec Management Platform Known Issues](#)” on page 26.
- Deployment Solution
[Deployment Solution Known Issues](#)

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:

- Package Server
See [Table 1-20](#) on page 27.
- UNIX/Linux/Mac
See [Table 1-20](#) on page 27.

Table 1-20 Known issues for Package Server

Issue	Article link
<p>When you create a new site server with Package Server service on Windows Core operating system where the latest Microsoft .NET updates are not installed, the Package Server setup will not be able to add .NET Extensibility 3.5 and ASP.NET 3.5 role services automatically during the installation.</p> <p>After installing Package Server, the following errors appear in the log from Package Server Agent source:</p> <ul style="list-style-type: none"> ■ "Web Server (IIS) role is installed, but the next required Role Services are missing: .NET Extensibility 3.5, ASP.NET 3.5." ■ "Not all required features of IIS are installed. IIS will not be used and Package Server's virtual directories will be deleted." ■ "Package Server is in the state that it can neither publish UNC codebases nor Web codebases." <p>Workaround: Perform the following steps:</p> <ol style="list-style-type: none"> 1 Install all available operating system updates. 2 Install .NET Extensibility 3.5 and ASP.NET 3.5 role services manually. <p>Symantec recommends to install Package Server to the freshly installed core operating system with the following steps:</p> <ol style="list-style-type: none"> 1 Add Web Server IIS server role. 2 Install all available operating system updates. 3 Install Symantec Management Agent. 4 Install Package Server. 	N/A

Table 1-21 Known issues for UNIX/Linux/Mac

Issue	Article link
<p>After configuring Apache Web Server, the Symantec Management Agent does not send httpd server role to Notification Server and cannot become a package server. This issue appears on SUSE Linux Enterprise 15 and CentOS 7.</p>	Help

Deployment Solution Known Issues

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

Table 1-22 Known issues for Deployment Solution

Issue	Article Link
Scripted OS Install task fails for Windows 7 if the computer is booted with WinPE 10 1809.	N/A
When you deploy an image of Windows 2019 or Windows 10 LTSC, the computer name is set to random as the operating systems are recognized as Windows XP.	N/A
When you upgrade to Deployment Solution 8.5, all the custom files that are present at <code>\Program Files\Altiris\Notification Server\NSCap\Bin\Deployment\BDC\bootwiz\Platforms\WinPE</code> are deleted and replaced with the default files.	N/A
You cannot log on to the client computer after you install RHEL 7.6 server edition using the scripted OS Install task.	N/A
After you deploy the disk image of SUSE Linux Enterprise Server 15, the host name does not change.	N/A
You cannot convert an EFI image with multiple partitions from GPT partition type when deployed on a BIOS-based client computer.	N/A
Surface Pro 4 computers using docking stations do not match the record when you use a USB device for imaging.	N/A
The Copy file task fails to copy files or folders using the UNC path when FIPS mode is enabled on a Linux client computer. Workaround: Disable the FIPS mode and run the task again.	N/A
The Boot To task fails to boot a Mac client computer as the System Integrity Protection feature is introduced in Mac OS X 10.11. Workaround: Run the <code>csrutil disable</code> command in the Recovery Mode.	N/A
For macOS Sierra 10.13 and higher NetInstall (SOI) is not currently supported.	N/A
For macOS Sierra 10.13 and higher sometimes the Deploy Image task of Apple file system containers fails with following error: Could not mark APFS container as new or unique.	N/A
Automation folder is no longer functional after you deploy a BIOS-based image to a UEFI computer.	N/A
For macOS Sierra 10.13 and higher clients, you cannot create image of volumes of Apple File System containers.	N/A

Where to get more information

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

Table 1-23 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The Supported Products A-Z page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under Common Topics , click Release Notes .
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	<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	<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 Help 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"> ■ Click the page and then press the F1 key. ■ Use the Context command, which is available in the Symantec Management Console on the Help menu.

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

Table 1-24 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	Knowledge Base
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	Unified Help System
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">■ 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