

Symantec™ IT Management
Suite 8.1 RU4 powered by
Altiris™ technology Release
Notes



Symantec™ IT Management Suite 8.1 RU4 powered by Altiris™ technology Release Notes

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information

- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

support.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan

customercare@symantec.com

Europe, Middle-East, and Africa

semea@symantec.com

North America and Latin America

supportsolutions@symantec.com

Symantec IT Management Suite 8.1 RU 4

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 RU4, the following new features are introduced:

Table 1-1 New features

| Feature | Description |
|---|---|
| Support for Mac OS High Sierra 10.13 | <p>Symantec Management Agent and solution plug-ins can be installed on Mac OS High Sierra 10.13 client computers.</p> <p>For the list of supported solutions and limitations refer to the following knowledge base article:</p> <p>http://www.symantec.com/docs/HOWTO127741</p> |
| Ability to configure the update notification icon in Symantec Management Console. | <p>The View Update Notifications privilege lets you configure if the update notification icon is displayed in the Symantec Management Console.</p> <p>Note that you cannot disable this privilege for default Symantec Administrators role.</p> |
| Changes and enhancements in SIM. | <p>RU4 introduces the following changes and enhancements in SIM:</p> <ul style="list-style-type: none"> ■ To make the actual validity period of applied licenses more visible, it is no longer possible to apply the licenses that will be valid in the future. ■ A new Recover NS Settings option is displayed on the Configure Notification Server page when the following key is missing in the Registry: [HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\AIM\Notification\NsConfiguration] This option lets you recover Notification Server settings and Configuration Management Database (CMDB) settings without fully reconfiguring your products. |
| Enhancements of package delivery. | <p>The following enhancements are implemented in package delivery:</p> <ul style="list-style-type: none"> ■ Block by block downloading Package delivery downloads all files block by block. Package delivery is aware of locally available and valid file blocks and is able to download only the missing file blocks. The download is performed using GET requests with file block range specified. If peer-to-peer downloading is enabled, package delivery periodically updates package value in DHT with the latest package blocks bitmask while downloading the package block by block. ■ Block chain hash validation Package delivery uses the block chain hash to validate the file integrity during the file download. Package delivery verifies each block hash as soon as it is received from the server and does not write the block if hash validation fails. |

Table 1-1 New features (continued)

| Feature | Description |
|---|---|
| A Targeted Agent Settings policy with initial settings. | <p>The (Initial Settings) policy lets you send the initial set of settings to the agents of client computers that have successfully registered but not yet appeared in the target of any regular Targeted Agent Settings policy. For example, after a re-imaged client computer receives the (Initial Settings) policy with ACC, it can immediately connect to Task Server.</p> <p>The (Initial Settings) policy has no specific target because it is automatically applied to the registered agents that are not found in the target of any other Targeted Agent Settings policy. After the agent appears in the target of a regular Targeted Agent Settings policy, it receives the settings of the regular policy.</p> <p>Note that if you clone the (Initial Settings) policy, it will become a regular policy and is applied based on the configured target.</p> <p>The (Initial Settings) policy is disabled by default. You can find it in the list of regular Targeted Agent Settings policies.</p> <p>Note: You must enable the Initial Settings policy for Deployment Solution.</p> |
| Ability to configure how often a peer notifies other peers about the package download progress. | <p>The new File block download progress on peer option lets you configure how often a peer should notify other peers about the package download progress. Peer computer downloads a file block by block (2MB blocks by default) and notifies other peers about its progress periodically. If download of one block is completed, other peers can start downloading it from that peer.</p> |
| New report for checking the state of the NS web site certificate replacement. | <p>After initiating the replacement of NS web site certificate, you can use the Computers having (or without) a Certificate report to check how many computers have received the new certificate and how many computers are still missing it.</p> <p>During the replacement, the report is listed on the Certificate Management page, under Reports. You can also access the report at Reports > Notification Server Management > Agent.</p> |
| (Windows only) Ability to apply a Cloud-enabled Management offline package to multiple organizational groups. | <p>During the creation of the Cloud-enabled Management offline package, you can select multiple organizational groups to which you want to apply the package.</p> <p>If an offline package contains more than one organizational group, the end user must select the group during manual setup. Depending on the selected organizational group, appropriate communication profile with Cloud-enabled Management information is applied.</p> |

Table 1-1 New features (continued)

| Feature | Description |
|-------------------------------------|--|
| Enhancements of the Software Portal | <p>RU4 introduces the following enhancements of the Software Portal:</p> <ul style="list-style-type: none"> ■ Users can access the Software Portal only from the computers that are licensed for Software Management Solution and meet the following requirements: <ul style="list-style-type: none"> ■ The Symantec Management Agent and Software Management Solution Plug-in are installed on the computers. ■ (Windows only) The computers are present in the Software Portal Plug-in Policy target. ■ The Software Portal Administrator can select a category for the published software while performing the following tasks: <ul style="list-style-type: none"> ■ Editing a software resource before publishing it to the Software Portal. ■ Creating or editing a Managed Software Delivery policy before publishing it to the Software Portal. ■ End users can search for software applications by vendor or category in the Software Portal. ■ The Software Portal Administrator can use the new option Prevent end users from requesting unlisted software on the Software Portal Settings page to hide the functionality that lets end users request the software that is not published for them in the Software Portal. ■ While publishing a software resource or a Managed Software Delivery policy to the Software Portal, the Software Portal Administrator can target devices or groups of devices for software publishing. <p>If the administrator targets both devices (or groups of devices) and users (or groups of users) for software publishing, only the selected users on the specified devices will have permission to request the software.</p> ■ The default number of open software requests per user is increased to 1000. The Software Portal Administrator can change this number in the NS Configurator tool as follows: <ol style="list-style-type: none"> 1. Run the NS Configurator tool that is located at <code>Program Files\Altiris\Notification Server\Bin\Tools</code>. 2. In the NSConfigurator dialog box, navigate to Core Settings > Software Portal > SoftwarePortalMaxOpenRequestsPerUser. 3. In the Value field, type the number of requests that a user can have open simultaneously, and then click Save. <p>Note that a Managed Software Delivery policy that contains dependencies or multiple tasks counts as one request.</p> |

Table 1-1 New features (continued)

| Feature | Description |
|---|--|
| Ability to add or edit a custom icon for a software resource. | <p>A predefined icon identifies each software resource in the Software Catalog. By default, the icon corresponds to the type of the resource: Software Update, Software Component, Service Pack, or Software Release.</p> <p>Starting from 8.1 RU4, you can add or edit a custom icon for a software resource when you edit the software resource in the Software Catalog.</p> <p>When you add the software resource to a Managed Software Delivery policy, the predefined or custom icon is displayed on the policy page.</p> |
| New default schedule for SQL defragmentation. | <p>In previous releases, the NS.SQL defragmentation schedule.{cdcd50e9-1c42-402b-921c-8ad6c9ff0d34} task is set to run only once by default and does not repeat anymore.</p> <p>After upgrading to IT Management Suite 8.1 RU4, the NS.SQL defragmentation schedule.{cdcd50e9-1c42-402b-921c-8ad6c9ff0d34} task has a new default schedule and runs as follows:</p> <ul style="list-style-type: none"> ■ If no custom schedule is specified, the task will run weekly every Saturday at 12:00PM. ■ If a custom schedule is specified, the task will run according to the specified schedule. <p>You can configure the schedule for this task in Task Scheduler.</p> |
| Improved UI of Process Manager. | The application menu and UI for Calendar , Scheduler , Knowledge Base , and Documents of the Process Manager of Workflow Solution are updated. |

System requirements and supported platforms

Before you install IT Management Suite 8.1 RU4, 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 RU4 involves installation of Symantec Management Platform (SMP) 8.1 RU4 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 RU4

After you install this release update (8.1 RU4), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.1 RU4 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 RU4 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 RU4, 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 Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins . Then, in the left pane, under Symantec Management Agent , locate and turn on the policies that upgrade the Symantec Management Agent on site servers. |
| Step 2 | Upgrade the site servers. | <p>In the Symantec Management Console, on the Settings menu, click All Settings. In the left pane, expand Notification Server > Site Server Settings, and then locate and turn on the upgrade policies for various site server plug-ins.</p> <p>To upgrade a remote task server, in the Symantec Management Console, on the Settings menu, click All Settings. In the left pane, expand Notification Server > Site Server Settings > Notification Server > Task Service > Advanced, and then locate and turn on the upgrade policies for the remote task servers.</p> <p>To upgrade a remote package server, in the Symantec Management Console, on the Settings menu, click All Settings. In the left pane, expand Notification Server > Site Server Settings > Notification Server > Package Service > Advanced > Windows, and then locate and turn on the Windows Package Server Agent Upgrade policy.</p> <p>Note: For Symantec IT Management Suite 8.1 RU4 the package server service upgrade is not required, as it has not changed and contains RU3 package.</p> |
| Step 3 | Upgrade the Symantec Management Agent on client computers. | In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins . Then, in the left pane, under Symantec Management Agent , locate and turn on the policies that upgrade the Symantec Management Agent on client computers. |

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

| Step | Action | Description |
|--------|--|--|
| Step 4 | Upgrade solution-specific agents and plug-ins. | <p>In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins. Then, in the left pane, locate and turn on the plug-in upgrade policies.</p> <p>To upgrade the solution-specific plug-ins to the latest version, do the following:</p> <ul style="list-style-type: none"> ■ In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins. Then, in the left pane, under Symantec Management Agent, locate and turn on the upgrade policies for the Symantec Management Agent. ■ In the Symantec Management Console, on the Settings menu, click All Settings. In the left pane, expand Notification Server > Site Server Settings, and then locate and turn on the upgrade policies for the site server plug-ins. ■ In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins. Then, in the left pane, locate and turn on the plug-in upgrade policies. |

Symantec recommends that you configure a schedule for the upgrade policies. The default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. To speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

If the upgrade policy is set to **Run once ASAP**, the policy is rolled out just once.

You can also clone the upgrade policies instead of creating additional schedules.

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 RU4 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU4

| Agent or plug-in | Windows | UNIX/Linux/Mac |
|--|-----------|---------------------|
| Symantec Management Agent | 8.1.5641 | 8.1.5618 |
| Altiris Client Task Agent | 8.1.5641 | 8.1.5618 |
| Altiris Client Task Server Agent | 8.1.5623 | N/A |
| Altiris Pluggable Protocols Architecture Agent | 8.1.5419 | N/A |
| Inventory Agent | 8.1.5636 | 8.1.5636 |
| Application Metering Agent | 8.1.5636 | 8.1.5072 (Mac only) |
| Server Inventory Agent | 8.1.5636 | 8.1.5636 |
| Inventory Rule Agent | 8.1.5641 | 8.1.5618 |
| Monitor Plug-in | 8.1.5412 | 8.1.5412 |
| Package Server | 8.1.5484 | 8.1.5618 |
| Power Scheme Task Plug-in | 8.1.4504 | N/A |
| Software Update Plug-in | 8.1.5620 | 8.1.5620 |
| Software Management Framework Agent | 8.1.5641 | 8.1.5618 |
| Software Management Solution Agent | 8.1.4504 | 8.1.4504 |
| 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) | 8.1.5622 | 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 | 8.1.5622 | N/A |
| Symantec Workspace Streaming Agent | 7.6.0.254 | N/A |
| Symantec Workspace Virtualization Agent | 7.6.254 | N/A |

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU4 (*continued*)

| Agent or plug-in | Windows | UNIX/Linux/Mac |
|-------------------------------------|-----------|----------------|
| Symantec Workspace Virtual Composer | 7.6.0.254 | 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 RU4:

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 RU4 | Yes | Yes | Yes |

Note: Refer to the following article for instructions to download and install the Deployment Solution point fix that addresses the Pending Download error of Package Servers.

[TECH248528](#)

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 RU4 contains fixed issues for the following solutions and components:

- Symantec Management Platform
See “[Symantec Management Platform Fixed Issues](#)” on page 18.
- Asset Management Solution
See “[Asset Management Solution Fixed Issues](#)” on page 19.
- CMDB Solution
See “[CMDB Solution Fixed Issues](#)” on page 19.
- Deployment Solution
See “[Deployment Solution Fixed Issues](#)” on page 19.
- Inventory Solution
See “[Inventory Solution Fixed Issues](#)” on page 20.
- Patch Management Solution
See “[Patch Management Solution Fixed Issues](#)” on page 21.
- Software Management Solution
See “[Software Management Solution Fixed Issues](#)” on page 22.
- Workflow Solution
See “[Workflow Solution Fixed Issues](#)” on page 22.

Symantec Management Platform Fixed Issues

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

This release contains fixed issues for the following components:

- Notification Server
See [Table 1-5](#) on page 18.
- UNIX/Linux/Mac
See [Table 1-6](#) on page 18.

Table 1-5 Fixed issues for Notification Server

| Issue | Article link |
|---|----------------------------|
| The " Contracts expiring in the next 30 days " automation policy fails with the following error: " An unexpected error occurred. Please check the logs for details. Parameter value can not be null. " | TECH247893 |
| Symantec Management Console times out when you try to add computers to a filter from a CSV file. | N/A |
| Client Task Agents cannot get the list of Task Servers with the following errors: " The handler 'GetClientTaskServers' is failed to process request " and " All pooled connections were in use and max pool size was reached ". | TECH247922 |
| If you delete a filter that is currently being used by a report, you cannot select a new filter for the report that used the deleted filter as a parameter. | TECH248018 |
| It is allowed to create Agent Communication Profiles with duplicate host names and Web application paths although having non-unique communication profiles can lead to unexpected behaviour. | N/A |
| Update notification icon in Symantec Management Console is displayed for all Security Roles and there is no option to make it visible only for appropriate role(s). | N/A |
| If the name of an Organizational Unit (or multiple names together) in AD are longer than 255 characters, the following error occurs during the AD import: " Failed to generate import data. Insufficient memory to continue the execution of the program. [System.OutOfMemoryException @ mscorlib] " | TECH248164 |

Table 1-6 Fixed issues for UNIX/Linux/Mac

| Issue | Article link |
|---|----------------------------|
| During package import with extract option, some packages get corrupted and their size is displayed as 0 KB. | TECH247698 |

Table 1-6 Fixed issues for UNIX/Linux/Mac (continued)

| Issue | Article link |
|--|--------------|
| The Restart Computer job returns 34603009 from SUSE Linux operating system. The expected return value is 0. | 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 1-7 Fixed issues for Asset Management Solution

| Issue | Article link |
|--|----------------------------|
| The Assets by Type, Status, Department, Cost Center and Location report does not return a list of assets if Asset Status is set to Active . | TECH247590 |
| When you create a purchase request in the Symantec Management Console and do not specify an owner that is assigned to a Department and Cost Center , the system does not automatically set the requestor as the owner of all line items. | N/A |

CMDB Solution Fixed Issues

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

Table 1-8 Fixed issues for CMDB Solution

| Issue | Article link |
|---|--------------|
| When you associate an Asset or a User to a Service on the Datacenter Types page, the Picker Reports performance is slow. | N/A |

Deployment Solution Fixed Issues

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

Table 1-9 Fixed issues for Deployment Solution

| Issue | Article link |
|---|--------------|
| Client computers fail to boot to preboot environment using Windows PXE and automation folder tasks when you enable only the TLS 1.2 protocol. | N/A |

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

| Issue | Article link |
|---|----------------------------|
| <p>Blank folders are created for an Install Windows OS task that uses an unattended.XML file in the following scenarios:</p> <ul style="list-style-type: none"> ■ If you leave the Install Windows OS task window and resume editing the task. ■ If you switch between two Install Windows OS task windows. | N/A |
| <p>The Create Image task fails to capture an image if the option Primary file storage location on a Windows OS: is changed.</p> | TECH247266 |
| <p>Custom unattend.XML file of the Deploy Image task does not get replicated from the parent Notification Server to the child Notification Server.</p> | N/A |
| <p>Failed to deploy a BIOS-based image to an EFI-based computer.</p> <p>More information related to this fix:</p> <p>Following changes are made when you deploy a BIOS-based image to a EFI-based computer:</p> <ul style="list-style-type: none"> ■ System partition and Microsoft Reserve partition are inserted before the normal Windows partition. ■ Old system partition of the BIOS-based image is preserved as a normal NTFS partition. | N/A |
| <p>Sometimes after you deploy a Sysprep image on a computer, the AeXAgentUtil fails to set new Notification Server name after the client computer boots into production for the first time.</p> | N/A |
| <p>In the template builder of PC Transplant the Advanced option does not work.</p> | 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 1-10 Fixed issues for Inventory Solution

| Issue | Article link |
|---|--------------|
| <p>When you gather inventory on Windows computers where paging file is disabled, the paging file data is not reported. As a result, an error appears in the Notification Server logs.</p> <p>Starting from 8.1 RU4, in such cases, the paging file data will be reported as not applicable.</p> | N/A |

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

| Issue | Article link |
|---|----------------------------|
| Two scroll bars appear on the Blacklisted Applications policy page, on the Options tab. | N/A |
| Inventory Solution provides the predefined software product Adobe Acrobat DC that incorrectly includes the software component Adobe Acrobat Reader DC . | N/A |
| Inventory Solution does not gather the provider data for mapped network drives on client computers. | TECH248036 |
| Basic inventory incorrectly reports the following 64-bit plug-ins as 32-bit plug-ins: <ul style="list-style-type: none"> ■ Inventory Plug-in ■ Inventory Pack for Servers Plug-in ■ Application Metering Plug-in | N/A |
| Server inventory tries to gather SQL cluster data from Windows non-SQL clusters. As a result, a warning appears in the Notification Server logs. Starting from 8.1 RU4, server inventory will not consider Windows non-SQL clusters as SQL clusters. | N/A |

Patch Management Solution Fixed Issues

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

Table 1-11 Fixed issues for Patch Management Solution

| Issue | Article link |
|--|----------------------------|
| A software update policy runs successfully but the software update package is partially downloaded because the remote server has closed the connection unexpectedly. In RU4, such partially downloaded files will be re-downloaded to ensure that the downloaded file size equals the expected size defined by the remote server. For example, this fix lets you ensure that all your files for Microsoft Office 365 (Office 2016 version) Click-to-Run installations are downloaded properly. | TECH248141 |
| Software updates fail to install if Patch Install Tools are updated during the software update cycle. | N/A |
| The task Import Patch Data for Red Hat fails with the following error: Failed to repair certificates, please check that valid RHN userName/password are specified. | TECH247935 |

Software Management Solution Fixed Issues

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

Table 1-12 Fixed issues for Software Management Solution

| Issue | Article link |
|---|----------------------------|
| When you edit a software resource, the store procedure is very slow and causes a timeout of <code>dlgResourceSelector.aspx</code> . | TECH239540 |
| The Software Portal Managers receive the notification This request is not assigned to you when they edit requests from the users who are assigned to them. | N/A |
| When you import a package to create or edit a software resource, and choose the package sourcing option Access package from an existing UNC , an empty GUID folder appears in the Software Library location. | 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 1-13 Fixed issues for Workflow Solution

| Issue | Article link |
|---|--------------|
| The tasks Reassign Ticket , Set Ownership , and Work Incident are disabled as the task's Leased Until values are set to time in future. | N/A |
| The Linear Gauge value is reset to the middle after page postback. | N/A |
| In the Workflow Designer, you cannot select the Rectangle component with a single click. | N/A |
| The Number (integer) type input parameters does not work with no value/NULL value even if the Null Allowed is checked. | N/A |
| The Menu Select Component does not re-evaluate the Root Node Label on a form post. | N/A |
| In Reports , when you click on a bar of a Bar graph, it does not display the details of the data. | N/A |
| If you export a project from Workflow 7.5 SP1 to 7.6, then following exception is displayed: <code>CostItems datatype exception</code> | N/A |

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

| Issue | Article link |
|---|--------------|
| The Form overflow behavior changes from 7.6 to 8.0 and you cannot configure it. | N/A |
| Ruleset menu is misplaced off the screen to the right. | N/A |
| The Date and the Time fields of ORM datatypes are saved in local server time instead of the UTC time. | N/A |

Known Issues

IT Management Suite 8.1 RU4 contains known issues for the following solutions and components:

- Deployment Solution
See [“Deployment Solution Known Issues”](#) on page 23.
- Patch Management Solution
See [“Patch Management Solution Known Issues”](#) on page 24.
- Software Management Solution
See [“Software Management Solution Known Issues”](#) on page 24.

Deployment Solution Known Issues

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

Table 1-14 Known issues for Deployment Solution

| Issue | Article Link |
|---|--------------|
| UEFI-based computers that require the bootx64.efi or the bootia32.efi files fail to boot to production after you deploy a BIOS-based image. | N/A |
| Deployment Solution fails to deploy a BIOS-based image to a UEFI-based computer if the image is modified. | N/A |
| Automation folder is no longer functional after you deploy a BIOS-based image to a UEFI computer. | N/A |
| Sometimes, package upload from Symantec Management Console fails for OS Files and Drivers upload. | N/A |
| For Windows 10 Redstone2 and Windows 10 Redstone3, after the Scripted OS Install task completes, you have to manually select and set the Region . | N/A |

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

| Issue | Article Link |
|---|--------------|
| Deploy Image task fails to deploy an image of a computer with RHEL 7.2 operating system and XFS file system. | N/A |
| The Create Image task fails for mac High Sierra 10.13 client computers with Apple File System. | N/A |
| Windows 10 predefined computers that boot into production environment after you deploy an image are not able to connect to a Task Server. | N/A |
| An error is displayed in the console when you upload a .cab file in the Sysprep Imaging Configuration. | N/A |
| Computers that imported from the Active Directory are listed in Predefined Computers. | N/A |

Patch Management Solution Known Issues

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

Table 1-15 Known issues for Patch Management Solution

| Issue | Article link |
|--|-----------------------------|
| <p>Patch Management Solution for Mac has a limited support of macOS 10.13 High Sierra.</p> <p>When you run Install All Updates Requiring Restart or other similar job to install the update MacOS 10.13.1 Update-10.13.1 on Mac client computers, the job fails with the following error details:</p> <pre>Failure message: command finished with error code: (2) no such file or directory</pre> <p>Package download status: package downloaded successfully, but failed to launch the program</p> <p>The update is installed but the installation result is handled incorrectly.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1 Restart the client computer. 2 Run the task Run System Assessment Scan on Mac Computers. | HOWTO127741 |

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 1-16 Known issues for Software Management Solution

| Issue | Article link |
|---|--------------|
| <p>While publishing a software resource or a Managed Software Delivery policy to the Software Portal, you can target devices and users for software publishing.</p> <p>However, when you edit the existing targets on the Software Publishing tab, the following issues occur:</p> <ul style="list-style-type: none">■ When you click Change User or Change Target, the Select Users or Groups or Select a resource target dialog boxes do not display the current targets.■ When you click Change User and Change Target to edit the already customised target, select a new user and device target, and then click OK, the user target may not be changed.■ When you click the already customised target, click the Delete icon, click OK, and then continue with editing the targets, the deleted target may reappear in the Software availability list.■ When you click Change User to edit the already customised user target, select a new user target, and then click OK, no users get targeted. | N/A |
| <p>When you edit multiple command lines for publishing on the software resource edit page, on the Software Publishing tab, the new configuration may be incorrectly saved.</p> <p>Workaround:</p> <ol style="list-style-type: none">1 Open a software resource for editing.2 On the software resource edit page, on the Software Publishing tab, select one command line, type a description, select a category, and then click OK.3 Open a software resource for editing again and repeat the step 2 for each command line that you want to edit. | N/A |

Table 1-16 Known issues for Software Management Solution (*continued*)

| Issue | Article link |
|---|--------------|
| <p>After you upgrade to 8.1 RU4, and then import the XML file for the Managed Software Delivery policy with the custom user target created in 8.1, no target and user settings are preserved for the policy under the Policy Rules/Actions section, on the Software Publishing tab.</p> <p>Workaround: Before you import the exported XML file, add the Device Target node to the file in the following way:</p> <pre><softwarePublishingInformation> <softwarePublishing> <PublishingItemGuid>94751e0f-09e6-49ab-a4e7- c4c15ea35ac6</PublishingItemGuid> <TrusteeId>S-1-5-21-560673693-1856947920-1706538875-500</TrusteeId> <Settings>IsApproved</Settings> <value>1</value> <DeviceTarget/> </softwarePublishing> <softwarePublishing> <softwarePublishing> <PublishingItemGuid>94751e0f-09e6-49ab-a4e7- c4c15ea35ac6</PublishingItemGuid> <TrusteeId>S-1-5-32-544</TrusteeId> <Settings>IsRequiringApproval</Settings> <value>1</value> <DeviceTarget/> </softwarePublishing> </softwarePublishingInformation></pre> | N/A |
| <p>When you edit a software resource that already has a customised target for software publishing, it is possible to add duplicate target entries that contain All Users and All Computers.</p> | N/A |

Where to get more information

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

Table 1-17 Documentation resources

| Document | Description | Location |
|---------------|--|--|
| Release Notes | Information about new features and important issues. | The Supported Products A-Z page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under Common Topics , click Release Notes . |
| User Guide | Information about how to use this product, including detailed technical information and instructions for performing common tasks. | <ul style="list-style-type: none"> ■ The Documentation Library, which is available in the Symantec Management Console on the Help menu. ■ The Supported Products A-Z page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under Common Topics , click Documentation . |
| Help | Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format. | The Documentation Library, which is available in the Symantec Management Console on the Help menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: <ul style="list-style-type: none"> ■ Click the page and then press the F1 key. ■ Use the Context command, which is available in the Symantec Management Console on the Help menu. |

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

Table 1-18 Symantec product information resources

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

Table 1-18 Symantec product information resources (*continued*)

| Resource | Description | Location |
|---------------------------|--|---|
| Cloud Unified Help System | All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud. | Unified Help System |
| Symantec Connect | An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products. | 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 |