

Symantec™ IT Management
Suite 8.1 RU3 powered by
Altiris™ technology Release
Notes



Symantec™ IT Management Suite 8.1 RU3 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 |

ITMS 8.1 RU3

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 RU3, the following new features are introduced:

Table 1-1 New features

| Feature | Description |
|---|--|
| Support for RHEL 6.9 and CentOS 6.9 | <p>Symantec Management Agent and solution plug-ins can be installed on RHEL 6.9 and CentOS 6.9 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/DOC10575</p> |
| Ability to change the Appliance account in Symantec Installation Manager. | <p>You can now edit the credentials of the Appliance account in Symantec Installation Manager in case the access to Symantec Management Console is not possible due to lockout or expiration of Appliance. The Appliance account is needed to run Notification Server.</p> <p>Note that you must enter a user name that has Administrator rights on this computer.</p> |
| Notification in case of changes to the IT Management Suite GA Product Listing. | <p>If the IT Management Suite GA Product Listing changes, the bell icon appears in the top right corner of the Symantec Management Console page.</p> <p>You can postpone the notification for selected period of time. Postponing works per account, so if a user logged on with one account postpones the update, then the user who logs on to the console with another account will still see the notification.</p> <p>Note: This notification is informational only. Actual update of product is performed in SIM.</p> |
| More flexibility for configuring the jobs. | <p>Fail Job if this Task fails option is added to server and client jobs.</p> <p>This option lets you fail the job if a specific sub-task or sub-job within this job fails.</p> <p>Note: Note that the Fail Job if any Task within this Job fails option is now disabled by default.</p> |
| Ability to add custom description to a task instance. | <p>When you schedule a task, you can now add a custom description to the task instance in the Quick Run section or in the New Schedule dialog box.</p> <p>This description is displayed under Task Status, in the Description column.</p> |
| In Task Management functionality, new option to restart only the computers that are pending reboot. | <p>A new option is added to the Restart Computer task that lets you restart only computers that are pending reboot.</p> |
| UI option for managing Data Class Summary Generator to populate custom data classes. | <p>The Data Class Summary Generator page in the Symantec Management Console lets you manage the Altiris.NS.StandardItems.DataClassSummaryGenerator class. This class lets you aggregate an extensive data set in Configuration Management Database (CMDB) into a smaller data class content.</p> <p>For more information, see:</p> <p>Creating Data Class Summary Generator</p> |

Table 1-1 New features (*continued*)

| Feature | Description |
|--|---|
| Ability to select specific Microsoft Office 365 channels for patching. | <p>With the patch management metadata for Windows release 7.2.73, you can select specific Microsoft Office 365 channels for patching from the following list:</p> <ul style="list-style-type: none"> ■ Microsoft Office Click to Run 2016 (Current) ■ Microsoft Office Click to Run 2016 (Deferred) ■ Microsoft Office Click to Run 2016 (First Release for Deferred) <p>For more information, see the following knowledge base article: http://www.symantec.com/docs/DOC9673</p> |
| Enhancements for managing targets. | <p>The following enhancements have been made for managing targets:</p> <ul style="list-style-type: none"> ■ You can now clone the target in the target editor to not impact other policies referencing the current target. ■ New icon is added to the target selector. When the target icon has a small lock icon next to it, it indicates that the Security Role(s) to which the current account belongs to does not have enough rights for this resource target. |
| Enhancements for certificate management. | <p>The following enhancements have been made on the Certificate Management page:</p> <ul style="list-style-type: none"> ■ Revocation of CEM Agent certificate triggers revocation of CEM certificates for client computer. ■ Warning is displayed if the replacement of specific certificate is not possible because it is reported from a CEM agent that is not upgraded. ■ Warning is displayed during the replacement of CEM site server certificate if the common name of this certificate does not match the host name of the computer to which it is applied. |
| Imaging support for 4K native drives. | <p>You can now create an image of a computer with 4K native drive that has GPT partition and NTFS file system and deploy it on a computer with 4K native drive.</p> <p>Note: The following scenarios are not supported:</p> <ul style="list-style-type: none"> Deploying an image that is created from a 4k drive to a drive with 512 sector size. Deploying an image that is created from a drive with 512 sector size to a 4k drive. |
| Improved performance of Boot Disk Creator. | <p>Improved performance of the Boot Disk Creator by reducing the time required to add preboot drivers and other packages while creating preboot packages for WinPE 5 and WinPE 10.</p> |

System requirements and supported platforms

Before you install IT Management Suite 8.1 RU3, 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 RU3 involves installation of Symantec Management Platform (SMP) 8.1 RU3 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 RU3

After you install this release update (8.1 RU3), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.1 RU3 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 RU3 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 RU3, 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. |

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> |
| 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> |
| 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 RU3 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU3

| Agent or plug-in | Windows | UNIX/Linux/Mac |
|--|----------|---------------------|
| Symantec Management Agent | 8.1.5484 | 8.1.5416 |
| Altiris Client Task Agent | 8.1.5484 | 8.1.5416 |
| Altiris Client Task Server Agent | 8.1.5454 | N/A |
| Altiris Pluggable Protocols Architecture Agent | 8.1.5419 | N/A |
| Inventory Agent | 8.1.5437 | 8.1.5437 |
| Application Metering Agent | 8.1.5072 | 8.1.5072 (Mac only) |
| Server Inventory Agent | 8.1.5437 | 8.1.5437 |
| Inventory Rule Agent | 8.1.5484 | 8.1.5416 |
| Monitor Plug-in | 8.1.5207 | 8.1.5207 |
| Package Server | 8.1.5484 | 8.1.5416 |
| Power Scheme Task Plug-in | 8.1.4504 | N/A |
| Software Update Plug-in | 8.1.5256 | 8.1.4538 |
| Software Management Framework Agent | 8.1.5484 | 8.1.5416 |

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU3 (*continued*)

| Agent or plug-in | Windows | UNIX/Linux/Mac |
|--|-----------|----------------|
| Software Management Solution Agent | 8.1.4504 | 8.1.4504 |
| Virtual Machine Management Task Handler | 8.1.5407 | N/A |
| Deployment Task Server Handler | 8.1.5433 | N/A |
| Deployment Package Server | 8.1.5433 | N/A |
| Deployment Plug-in for Windows (x64/x86) | 8.1.5433 | 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 | 8.1.5433 | N/A |
| Symantec Workspace Streaming Agent | 7.6.0.254 | N/A |
| Symantec Workspace Virtualization Agent | 7.6.254 | N/A |
| 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 RU3:

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 RU3 | Yes | No | Yes |

Post installation tasks for Deployment Solution

- Recreate the automation folders.
- Deploy automation folders on client computers.

Note: Symantec recommends that you clear the Internet browser cache before running deployment tasks.

To recreate the automation folders

- 1 In the Symantec Management Console, on the **Settings** menu, click **Deployment > Manage Preboot Configurations**.
- 2 On the **Manage Preboot Configurations** page, in the preboot configurations list, select the configuration that you want to recreate and click **Recreate Preboot Environment**.

For Mac, you must recreate all the NetBoot images and the automation folders and create new preboot configurations.

Symantec recommends that you wait for at least half an hour before running any deployment tasks. To see if the automation folder is updated, check the timestamp for the automation folders that are created at the following locations:

- PEInstall_x86
`<install_dir>\Notification
Server\NSCap\bin\Win32\X86\Deployment\Automation\PEInstall_X86`
- PEInstall_X64
`<install_dir>\Notification
Server\NSCap\bin\Win64\X64\Deployment\Automation\PEInstall_x64`
- LinInstall
`<install_dir>\Notification
Server\NSCap\bin\UNIX\Deployment\Linux\x86\Automation\LinInstall_x86`

To verify if the automation folder has been recreated, in the task manager, check if the Bootwiz.exe application has completed recreating the preboot configuration.

After recreating the automation folders, run the following tasks from the Task Scheduler to update the packages on Notification Server:

- NS.Delta Resource Membership Update
- NS.Package Distribution Point Update Schedule
- NS.Package Refresh

To deploy the automation folders on the Windows client computers

- ◆ Run the following automation folder upgrade policies:
 - **Deployment Automation Folder for Windows (x64) - Upgrade**
 - **Deployment Automation Folder for Windows (x86) - Upgrade**

To deploy the automation folders on the Linux client computers

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

Fixed issues

IT Management Suite 8.1 RU3 contains fixed issues for the following solutions and components:

- Symantec Management Platform
See [“Symantec Management Platform Fixed Issues”](#) on page 15.
- Asset Management Solution
See [“Asset Management Solution Fixed Issues”](#) on page 17.
- Deployment Solution
See [“Deployment Solution Fixed Issues”](#) on page 18.
- Inventory Solution
See [“Inventory Solution Fixed Issues”](#) on page 19.
- Patch Management Solution
See [“Patch Management Solution Fixed Issues”](#) on page 20.
- Workflow Solution
See [“Workflow Solution Fixed Issues”](#) on page 20.

Symantec Management Platform Fixed Issues

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

This release contains fixed issues for the following components:

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

- Data Connector
See [Table 1-9](#) on page 17.

Table 1-5 Fixed issues for Symantec Installation Manager

| Issue | Article link |
|---|-----------------------------------|
| <p>When you start the IT Management Suite upgrade from version 7.6 HF7 to version 8.0 by clicking the Begin Install button, the upgrade fails immediately with the following error: "Exception while packaging Symantec_Migration_Package_2017_06_02_111822_x64.exe migration wizard zip."</p> | <p>TECH246709</p> |
| <p>When in Symantec Installation Manager, on the Product Licensing page, you click Install licenses..., the Select License Files window does not show any available license files.</p> <p>This issue occurs only if under computer's Region and Language settings, the Format is set to Chinese (Simplified, PRC) and Location is set to China.</p> | <p>N/A</p> |

Table 1-6 Fixed issues for Notification Server

| Issue | Article link |
|---|--------------|
| <p>If you generate an offline Cloud-enabled Management package and install it on a client computer which has direct access to the network that hosts Notification Server, the Symantec Management Agent fails to register on Notification Server with the following error:</p> <p>"HTTP status 403: The client does not have sufficient access rights"</p> <p>This issue occurs only if you have placed a not self-signed certificate in Trusted Root store on Notification Server.</p> | <p>N/A</p> |
| <p>NS tools cannot be launched from <code>%NS Install Directory%\Notification Server\Bin\Tools\</code> when UAC is enabled on installed Notification Server computer.</p> <p>For this issue, three workarounds are available:</p> <ul style="list-style-type: none"> ■ Change security settings for profile and grant rights directly to the required user ■ Change UAC settings. ■ Copy Tools folder to drive C:\ and launch NS tools from there. | <p>N/A</p> |
| <p>Upgrading to IT Management Suite version 8.1 RU2 adds additional parameters to the external web links that are defined in Symantec Management Console.</p> | <p>N/A</p> |
| <p>After the upgrade to IT Management Suite version 8.1 RU2, some cloud-enabled client computers fail to re-establish communication with Notification Server because of the resource merge operations that occurred.</p> | <p>N/A</p> |

Table 1-6 Fixed issues for Notification Server (*continued*)

| Issue | Article link |
|---|--------------|
| When you edit the default time range of a Maintenance Window, save the changes, leave the page, and then view this Maintenance Window again, the default time range is displayed again. | N/A |
| When you open a report, it runs with default filter values and not with the filter values that were specified last time. | N/A |

Table 1-7 Fixed issues for Task Server

| Issue | Article link |
|---|----------------------------|
| When you run simultaneously Run Script tasks or same task instances with the same input token, the token value of the second task overwrites the token value of the first task. | N/A |
| During the upgrade from IT Management Suite 7.6 HF7 or 8.0 HF6 to IT Management Suite 8.1, <code>altiris_taskmanagement_8_1_x64.msi</code> fails with Install failure error. | TECH247328 |

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

| Issue | Article link |
|--|--------------|
| A software delivery script to install a profile that is set to run as the Current logged-on user , fails with an Exit code 1. | N/A |

Table 1-9 Fixed issues for Data Connector

| Issue | Article link |
|---|--------------|
| " Symantec Management Server Error " appears after clicking Show selected resources... on a CMDB rule page. | 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 1-10 Fixed issues for Asset Management Solution

| Issue | Article link |
|--|--------------|
| When you edit a resource by adding or editing a date in a Multi Rows data class, a Notification Server Error appears. This error occurs only when you use the localized Symantec Management Console with a non-English language. | N/A |
| You cannot edit a resource that has a reference to Multi Rows data class that contains SQL Query List type attribute. | N/A |
| When you create a new Invoice and add a Unit Cost value that contains a decimal point, it disappears after saving. For example, a Unit Cost value 12,35 becomes 1235 after you save the invoice. | N/A |
| When you add or edit a date in data classes, that are defined to use the Date data type, the acceptable date time range is from 1900/01/1 00:00:00 to 2029/12/30 23:59:59. Starting from 8.1 RU3 the acceptable date time range is from 1753/01/01 to 9999/12/31. | N/A |

Deployment Solution Fixed Issues

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

Table 1-11 Fixed issues for Deployment Solution

| Issue | Article link |
|--|--------------|
| The Prepare for Image Capture task fails when you upgrade to Windows 10 1607 and 1703 version. | N/A |
| The Extract SSL Certificate (x64) -Install policy fails if you install Notification Server and Symantec Management Agent on different drives. | N/A |
| Computers with Static IP address are not displayed on the Predefined Computers page. | N/A |
| PXE preboot configurations that are deleted from the console do not get deleted from the site servers. | N/A |
| On the Preboot Configuration status page, duplicate statuses are shown for a preboot configuration. | N/A |
| The ResourceImportTool.exe fails to launch and create the log file on a site server if the SIM installer is run at least once on the site server. | N/A |

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

| Issue | Article link |
|---|--------------|
| Incorrect status is displayed on the Preboot Configuration Status page even when the PXE configuration is recreated successfully. | N/A |
| On the Driver Management page and the Copy File task page, the Browse option and the Folder icons do not work properly. | N/A |
| The PCT restore closes while restoring a PCT package, if you use the user accounts option. | N/A |
| The Create Image task saves the image to UNC path even if the SSL Setting is set to Accept . | 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 1-12 Fixed issues for Inventory Solution

| Issue | Article link |
|---|----------------------------|
| The Operating System data class contains an incorrect installation date and operating system name on computers with Ubuntu Linux. | N/A |
| The following issues occur when you gather inventory on computers that run Ubuntu 14 with an old awk version (i. e. mawk 1.3.3 Nov 1996): <ul style="list-style-type: none"> Inventory scan does not gather network adapter information. SMBIOS provider script fails to run due to a syntax error. | N/A |
| After applying a release update, the right-click menu items for creation of the following new Inventory Solution policies become unavailable in the Symantec Management Console UI: <ul style="list-style-type: none"> Targeted Software Inventory Inventory Policy Application Metering Policy For more information on troubleshooting the issue that has already occurred before applying 8.1 RU3, see the KB article TECH164410 . | TECH164410 |
| Inventory Solution incorrectly reports the last start up time and installation date on AIX and HP-UX server computers. | N/A |
| Hardware inventory incorrectly reports the model name on Lenovo server computers (for example, NeXtScale and System x). | N/A |

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

| Issue | Article link |
|---|--------------|
| Members of the Symantec Level 1 Workers role can manage Inventory Solution policies despite having only read rights to the policies. | N/A |
| Standalone inventory does not gather basic inventory TCP/IP data. | N/A |
| Inventory for servers incorrectly reports MySQL 5.0.x database information on Red Hat Enterprise Linux 5.11 server computers. | 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 1-13 Fixed issues for Patch Management Solution

| Issue | Article link |
|--|----------------------------|
| A software update policy cannot be created for the Red Hat bulletin RHBA-2016:2516 after the import of the CentOS channels. | TECH247139 |
| SUSE patch management metadata cannot be downloaded for the software channels that have an extra dash in the channel name (ex.: <code>SLE-12-SP1-SAP-Updates</code>). | N/A |
| Red Hat Network (RHN) Entitlement Operations Authority certificate is incorrectly installed into the Trusted Root Certificate Authority store instead of the Intermediate Certification Authorities store. | N/A |
| The Import Patch Data for Windows task cannot detect partially downloaded files. As a result, the task fails during the import stage. | TECH217969 |

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 1-14 Fixed issues for Workflow Solution

| Issue | Article link |
|--|--------------|
| The Process Age column of My Open Tickets report does not report any values. | N/A |
| Setting the User time zone manually fails for the time zones that recognize daylight savings time. | N/A |

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

| Issue | Article link |
|---|--------------|
| The Filter option is missing from the Process History and the Process Comment Web Parts. | N/A |
| In the Report generator , the Graph tooltips are not readable. | N/A |

Known Issues

IT Management Suite 8.1 RU3 contains known issues for the following solutions and components:

- Symantec Management Platform
See "[Symantec Management Platform Known Issues](#)" on page 21.

Symantec Management Platform Known Issues

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

The known issues are listed for the following components:

- Task Server
See [Table 1-15](#) on page 21.

Table 1-15 Known issues for Task Server

| Issue | Article link |
|--|--------------|
| Because of Windows API limitation, the Clean up Task Schedules task is not able to delete all Windows schedules if the total number of schedules that you want to remove is bigger than 3800. Workaround: Remove the Windows schedules manually from the following location: C:\Windows\System32\Tasks | N/A |

Where to get more information

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

Table 1-16 Documentation resources

| Document | Description | Location |
|---------------|---|---|
| Release Notes | Information about new features and important issues. | <p>The Supported Products A-Z page, which is available at the following URL:</p> <p>https://www.symantec.com/products/products-az</p> <p>Open your product's support page, and then under Common Topics, click Release Notes.</p> |
| User Guide | Information about how to use this product, including detailed technical information and instructions for performing common tasks. | <ul style="list-style-type: none"> ■ 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 <p>Open your product's support page, and then under Common Topics, click Documentation.</p> |
| Help | <p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p> | <p>The Documentation Library, which is available in the Symantec Management Console on the 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 1-17 Symantec product information resources

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

Table 1-17 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 |