

Symantec™ IT Management
Suite 8.1 RU2 powered by
Altiris™ technology Release
Notes



Symantec™ IT Management Suite 8.1 RU2 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 RU2

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](#)
- [Other things to know](#)
- [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 RU2, the following new features are introduced:

Table 1-1 New features

Feature	Description
New page for managing certificates.	<p>The Certificate Management page combines both existing capabilities, like replacement of Site Server certificates, and new capabilities like:</p> <ul style="list-style-type: none"> ■ renewal of CEM agent certificates ■ replacement of root certificate ■ replacement of website certificates, etc. <p>Depending on the certificate type, the UI guides you through the required replacement process. Another benefit of the Certificate Management page is the ability to easily see and fix the issues with current certificates. For example, a certificate has a weak cipher suite or it expires soon.</p> <p>The Certificate Management page is located at Settings > Notification Server.</p>
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:</p> <ul style="list-style-type: none"> ■ Ubuntu (versions (14.04 LTS Trusty Tahr, 16.04 LTS Xenial Xerus and 17.04 Zesty Zapus) For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO127014 ■ Windows 10 Creators Update (Windows 10 version 1703) For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO127016 ■ SUSE Linux Enterprise Server 12 SP2 and SUSE Linux Enterprise Desktop 12 SP2 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO127018 ■ Red Hat Enterprise Linux 7.3 and CentOS 7.3 http://www.symantec.com/docs/HOWTO127035
Support for SQL Server 2016 SP1	Starting from 8.1 RU2, SQL Server 2016 Service Pack 1 is supported.
Support for Windows Server 2016	<p>Network Boot Service is supported on Windows Server 2016 operating system.</p> <p>For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125454</p>
New task for removing expired schedules.	<p>A new Clean up Task Schedules task lets you disable or delete schedules that have no occurrence in the future. The cleanup task removes these task schedules from the Windows Task Scheduler.</p> <p>The Clean up Task Schedules task is located at Settings > Notification Server > Task Settings.</p>

Table 1-1 New features (*continued*)

Feature	Description
<p>Ability to resume Software Management Framework activities on a computer pending a restart or a logoff.</p>	<p>Software Management Solution 8.1 RU2 introduces the functionality to resume Software Management Framework activities and allow other software delivery policies and tasks to execute on a computer pending a restart or a logoff that a Managed Software Delivery policy requires.</p> <p>This functionality is not available out of the box. You can enable it manually on the required client computer by creating the following non-default registry key value:</p> <pre>"DWORD: HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\SMFAgent\Delivery\Options\DisregardPostRunAction" = 1</pre> <p>When the value DisregardPostRunAction is absent or equals zero, the functionality is disabled.</p> <p>For more information about the functionality and its limitations, see the knowledge base article DOC10551.</p>
<p>Workspace Virtualization components are upgraded to the version 7.6 HF9.</p>	<p>In Software Management Solution 8.1 RU2, the following Workspace Virtualization components are upgraded to the version 7.6 HF9:</p> <ul style="list-style-type: none"> ■ Symantec Workspace Virtualization Agent (SWV Agent) (32/64 bit, 7.6.254.0) ■ Virtual Composer (32/64 bit, 7.6.0.254) ■ Streaming Agent (32/64 bit, 7.6.0.254) <p>The correct version of SWV Agent appears in the list of plug-in versions for the selected client computer.</p> <p>After the 8.1 RU2 upgrade, the following changes occur in the custom policies that use the old version of the SWV Agent:</p> <ul style="list-style-type: none"> ■ The SWV Agent is upgraded to the latest version. ■ The policies stay enabled. ■ The policies deliver the latest version of the SWV Agent. <p>For SWV 7.6 HF8 Release Notes, please see the following link: http://www.symantec.com/docs/DOC10534</p>
<p>Support for SNMPv3.</p>	<p>With the SNMPv3 support, you can perform the following tasks on SNMPv3-enabled Cisco switches and the devices connected to them (for example, VMs, Desktops, etc.):</p> <ul style="list-style-type: none"> ■ Discover the devices using Network Discovery. ■ Gather agentless inventory on the devices using Inventory for Network Devices. <p>Note that SNMPv3 support is limited to Cisco switches only.</p>

Table 1-1 New features (*continued*)

Feature	Description
Improved usability of peer-to-peer downloading reports.	<p>The usability of the following peer-to-peer downloading reports is improved:</p> <ul style="list-style-type: none"> ■ The Packages Distribution by Download Type report ■ The Downloads by Computers and Download Types report ■ The Computers TCP/IP Info report
Enhancements of Symantec Management Console Search.	<p>The search progress is now displayed in percentage to provide an estimate when the process will be finished.</p> <p>The search results now contain additional information and are divided by manageable sections for easier navigation.</p>
Improved support for cab archive.	Support for drivers upload in .cab archive for Deployment Solution is improved.

System requirements and supported platforms

Before you install IT Management Suite 8.1 RU2, 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 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 RU2 involves installation of Symantec Management Platform (SMP) 8.1 RU2 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 RU2

After you install this release update (8.1 RU2), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.1 RU2 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 RU2 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 RU2, 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 KB article:
<http://www.symantec.com/docs/TECH183086>

For more information about creating a support package, see the following article:

<http://www.symantec.com/docs/HOWTO93142>

Upgrading Symantec Management Agent, site servers and solution level plug-ins

After you upgrade IT Management Suite from version 8.1 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>
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 RU2 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU2

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.1.5276	8.1.5223
Altiris Client Task Agent	8.1.5276	8.1.5223
Altiris Client Task Server Agent	8.1.5237	N/A
Altiris Pluggable Protocols Architecture Agent	8.1.5243	N/A
Inventory Agent	8.1.5267	8.1.5267
Application Metering Agent	8.1.5072	8.1.5072 (Mac only)
Server Inventory Agent	8.1.5267	8.1.5267
Inventory Rule Agent	8.1.5223	8.1.5223
Monitor Plug-in	8.1.5207	8.1.5207
Package Server	8.1.5276	8.1.5223
Power Scheme Task Plug-in	8.1.4504	N/A
Software Update Plug-in	8.1.5256	8.1.4538
Software Management Framework Agent	8.1.5276	8.1.5223
Software Management Solution Agent	8.1.4504	8.1.4504
Virtual Machine Management Task Handler	8.1.5201	N/A
Deployment Task Server Handler	8.1.5051	N/A
Deployment Package Server	8.1.5051	N/A
Deployment Plug-in for Windows (x64/x86)	8.1.5231	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	8.1.5231	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 RU2 (*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 RU2:

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 RU2	Yes	No	No

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**

Fixed issues

IT Management Suite 8.1 RU2 contains fixed issues for the following solutions and components:

- Symantec Management Platform
See [“Symantec Management Platform Fixed Issues”](#) on page 16.
- Deployment Solution
See [“Deployment Solution Fixed Issues”](#) on page 18.
- IT Analytics Solution
See [“IT Analytics Solution Fixed Issues”](#) on page 18.
- ITMS Management Views
See [“ITMS Management Views Fixed Issues”](#) on page 19.
- Inventory Solution

- See “[Inventory Solution Fixed Issues](#)” on page 19.
- Patch Management Solution
See “[Patch Management Solution Fixed Issues](#)” on page 19.
- Software Management Solution
See “[Software 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:

- Notification Server
See [Table 1-5](#) on page 16.
- Task Server
See [Table 1-6](#) on page 17.
- Symantec Management Agent
See [Table 1-7](#) on page 17.
- UNIX/Linux/Mac
See [Table 1-9](#) on page 18.
- ASDK
See [Table 1-9](#) on page 18.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
In the Symantec Management Agent Settings dialog box, incorrect number of selected computers is displayed for Symantec Management Agent push installation. This issue appears if French (Canada) is set as the preferred language in Internet Explorer 11.	N/A
Editing the input parameters of Assign computers discovered in the last day to Organizational Group automation policy fails with “ HTTP Error 404.13 - Not Found ” error.	TECH246579
When you dispose a computer and change its name after disposing, the Purging Maintenance reverts the computer's name back to what it was before disposing.	N/A

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

Issue	Article link
When you create a custom report, the values that you configure for some options are not saved. For example, you cannot add or remove values under Manually add/edit Dropdown values .	N/A
When you add computers from a computer list to a new filter, the computers get included into the filter but the filter membership is not updated.	N/A
No default filter for the Microsoft Windows Server 2012 R2 computers.	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
Task Client does not handle PowerShell command " SetShouldExit " correctly. A failed task can return success without error code.	TECH239692

Table 1-7 Fixed issues for Symantec Management Agent

Issue	Article link
Symantec Management Agent on desktop operating system fails to upgrade from 7.6 HF7 to 8.1 with the following error message: " Failed to run action: InstallCoreAgentExe "	TECH201068
The agent's reboot notification window has keyboard focus on Reboot Now button by default. This can cause undesired restarts of the client computers.	N/A
Symantec Management Agent generates a Site Server certificate with no FQDN in the Subject Alternative Name .	TECH246994

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

Issue	Article link
Symantec Management Agent on Mac ignores the Warning Countdown Duration setting and only uses 5 minutes. This issue appears with Managed Software Delivery only.	N/A
Symantec Management Agent Push installation to a Mac computer fails with " Invalid Hostname " error.	N/A
The push installation of Symantec Management Agent for UNIX/Linux/Mac fails because the push installation requests the agent download using the server name and not the FQDN that is specified in the Communication Profile.	N/A

Table 1-9 Fixed issues for ASDK

Issue	Article link
Core Altiris.ASDK.NS.SoftwareDelivery API fails if the Software license is expired or not present.	N/A

Deployment Solution Fixed Issues

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

Table 1-10 Fixed issues for Deployment Solution

Issue	Article link
PC Transplant Distribute Personality does not work in Deployment Solution 8.0.	N/A
Microsoft Office files that are placed on the Desktop are not transferred using the PC Transplant.	N/A
Client computer fails to download certificates if the setting Client certificate is set to Accept .	N/A
Client computer fails to receive PXE Boot menu if the SSL setting on Notification Server is set to Accept.	N/A
Cannot save an Apply System Configuration task if the name of task starts with a number.	N/A
Recently added predefined computers are not available for scheduling through Quick Run and Quick Add drop-down menus.	N/A
If you uninstall the Deployment Solution Package Server component, a few entries remain in the web.config file.	N/A
The UI label on Add Driver > Location does not indicate if you can add CAB files.	N/A

IT Analytics 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 IT Analytics Solution

Issue	Article link
The search functionality in the Manage Filters window has been modified from Exact Text Search to Contains Text Search and now allows the use of wild cards.	N/A
You cannot view all the content in IT Analytics Reports , as the vertical and horizontal scroll bars are missing.	N/A

ITMS Management Views Fixed Issues

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

Table 1-12 Fixed issues for ITMS Management Views

Issue	Article link
Software products with enabled metering and tracking and one or more Mac software components, appear in the Missing program associations filter.	N/A

Inventory Solution Fixed Issues

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

Table 1-13 Fixed issues for Inventory Solution

Issue	Article link
Some capital Russian letters and double-byte characters (for example, Japanese and Chinese) are omitted from the collected inventory fields.	N/A
When you gather software application file inventory and configure an inventory task or policy to scan the two folders, where the path to the first folder is a substring of the path to the second folder (for example, <code>C:\qwerty123</code> and <code>C:\qwerty</code>), file properties data is gathered only from the second folder.	N/A
After an inventory task or policy gathers hardware data on a client computer, the task or policy can remove previous records related to this computer from the SW Patch Windows data class in the CMDB.	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 1-14 Fixed issues for Patch Management Solution

Issue	Article link
Patch Management Solution has a functionality to clean up folders with expired packages in default and custom locations. The software update plug-in gets notifications from Symantec Management Agent about the deletion of an expired Patch or Software package, identifies the package location, and deletes the contents of the corresponding folder. If the folder <code>C:\Windows</code> is configured as the package location folder, it gets deleted during this process.	TECH246634
Undesired additional software bulletins get listed in the Distribute Software Updates wizard if you start the wizard for the multi-selected bulletins in the report sorted by a column with a space in the header name (i.e. Applies To).	TECH246808

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 1-15 Fixed issues for Software Management Solution

Issue	Article link
When you configure the package server settings for the current package in the Add or Edit Package dialog box, on the Package Server tab, the option Assign package to: Package Servers individually displays a list of package servers and lets you select specific servers. However, the list goes back to the top after a server gets selected. So you have to scroll down each time you want to select more servers from the list.	N/A
When you configure the user run conditions settings of a Managed Software Delivery policy or a legacy delivery policy, the option Prompt user before running does not work if you do not check the option Allow user to defer up to a total of .	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 1-16 Fixed issues for Workflow Solution

Issue	Article link
Mapping an array to a parameter in the Code (Script) Component no longer works.	N/A

Table 1-16 Fixed issues for Workflow Solution (*continued*)

Issue	Article link
Text box and Multiline Text Box components generate following error: System.Web.HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (1b="<junk>")	N/A
Line breaks do not work properly in email template variables.	TECH217398
CommentAdded event Input Data creates a blank web service page.	N/A
An SQL Injected Vulnerability exists in a User-Generated version of Web services that is created using the List and Profiles generator.	N/A
In the Workflow form project, duplicate items are removed automatically.	N/A

Known Issues

IT Management Suite 8.1 RU2 contains known issues for the following solutions and components:

- Symantec Management Platform
See “[Symantec Management Platform Known Issues](#)” on page 21.
- Deployment Solution
See “[Deployment Solution Known Issues](#)” on page 22.
- Inventory Pack for Servers
See “[Inventory Pack for Servers Known Issues](#)” on page 23.
- Inventory Solution
See “[Inventory Solution Known Issues](#)” on page 23.
- Software Management Solution
See “[Software Management Solution Known Issues](#)” on page 23.

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:

- Symantec Management Agent
See [Table 1-17](#) on page 22.

Table 1-17 Known issues for Symantec Management Agent

Issue	Article link
<p>If Symantec Management Agent 7.6 HF7 receives Agent Communication Profile from Notification Server 8.1 where 8.1 Cloud-enabled Management Settings are applied and Allow Windows agent to perform Cloud-Enabled registration on specified Notification Server option is enabled, the agent cannot register on Notification Server 8.1.</p> <p>This issue only occurs if Notification Server 8.1 runs on Windows 2012 R2 Server operating system.</p>	N/A
<p>The Symantec Management Agent fails to register on Notification Server (NS) in the following scenario:</p> <ol style="list-style-type: none"> 1. NS has a non-CA certificate in the Trusted Root Certification Authorities store. 2. You generate an offline Cloud-enabled Management package and install it on a client computer that has direct access to the network that hosts NS. <p>Use one of the workarounds below to resolve the issue:</p> <ul style="list-style-type: none"> ■ Perform the Symantec Management Agent registration outside the internal network. ■ Move the certificate to appropriate store. For example, the Intermediate Certificates have to be placed into Intermediate Certification Authorities store. ■ Temporarily remove the misplaced certificate from NS, and restore it after the Symantec Management Agent is successfully registered on NS. 	N/A

Deployment Solution Known Issues

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

Table 1-18 Known issues for Deployment Solution

Issue	Article Link
Sometimes, package upload from Symantec Management Console fails for OS Files and Drivers upload.	N/A
For Russian and Spanish languages, the Browse option on the Add Driver page of Driver Database Management does not work.	N/A
For Windows 10 Redstone2, after the Scripted OS Install task completes, you have to manually select and set the Region .	N/A
Deploy Image task fails to deploy an image of a computer with RHEL 7.2 operating system and XFS file system.	N/A

Inventory Pack for Servers Known Issues

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

Table 1-19 Known issues for Inventory Pack for Servers

Issue	Article link
Predefined Inventory Pack for Servers Plug-in install, uninstall, and upgrade policies are reset to the default state after applying Inventory Pack For Servers 8.1 RU2.	N/A
Server inventory data may not be properly gathered for Oracle server database on the client computers with Ubuntu operating system. The reason for this limitation is that Oracle Corporation does not officially support Ubuntu for Oracle database.	HOWTO127014

Inventory Solution Known Issues

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

Table 1-20 Known issues for Inventory Solution

Issue	Article link
The following predefined Inventory Solution policies are reset to the default state after applying Inventory Solution 8.1 RU2: <ul style="list-style-type: none"> Inventory Plug-in install, uninstall, and upgrade policies Application Metering Plug-in install, uninstall, and upgrade policies 	N/A
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

Software Management Solution Known Issues

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

Table 1-21 Known issues for Software Management Solution

Issue	Article link
The software installation into a virtual layer via Managed Delivery Policy does not work on the computers with Windows 10 Redstone 2 operation system. The activation of a layer fails with error code 1040.	N/A

Other things to know

The following are the things to know about this release. If additional information is available, the information has a corresponding article link.

Table 1-22 Things to know about IT Management Suite

Information	Article link
<p>The following changes are made in Symantec Product Improvement Program:</p> <ul style="list-style-type: none"> ■ Among other information, the Symantec Product Improvement Program now collects data about Microsoft Office 365 patching. ■ The options for enabling and disabling the participation in Product Improvement Program have been removed from Symantec Installation Manager and Symantec Management Console. 	HOWTO77301

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.	<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>

Table 1-23 Documentation resources (*continued*)

Document	Description	Location
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

Table 1-24 Symantec product information resources (*continued*)

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	<p>The links to various groups on Connect are as follows:</p> <ul style="list-style-type: none"> ■ 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