

Symantec™ IT Management
Suite 8.1 RU5 powered by
Altiris™ technology Release
Notes



Symantec™ IT Management Suite 8.1 RU5 powered by Altiris™ technology Release Notes

Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

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

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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 RU5

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 RU5, the following new features are introduced:

Table 1-1 New features

Feature	Description
Enhanced user interface of the Software Portal.	<p>RU5 introduces the enhanced UI of the Software Portal that improves the user experience.</p> <p>The Software Portal Administrator can configure whether the legacy UI or the enhanced UI is displayed to the users. Note that the legacy UI is enabled by default.</p> <p>The enhanced UI has the following features:</p> <ul style="list-style-type: none"> ■ Users can access the Software Portal only from Windows and Mac client computers that 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. ■ The computers are present in the Software Portal Client Access Policy target and the policy is enabled. <p>Note: The enhanced user interface requires an HTML5-compatible browser.</p> <ul style="list-style-type: none"> ■ End users can also open the Software Portal on Windows computers with Cloud-enabled Management enabled. ■ End users can view and request only the applications that are compatible with the software platform of the device they use to open the Software Portal. ■ End users can request Windows and Mac applications that are listed or not listed in the Software Portal. ■ In the user profile, end users can enable the following notification options: <ul style="list-style-type: none"> ■ View notifications when the requested application is installed on the user's device. ■ Receive emails when someone comments on or changes the status of the user's application request. The emails contain the link to the Software Portal, where the user can manage the application request. The user can use the Software Portal credentials to open the link from any device. ■ Software Portal managers can specify the users whose software requests they process. They can review, approve, or deny application requests. ■ End users and managers can search for the applications by name, vendor, and version. ■ End users can filter the applications by category, type, and approval. Managers can filter user requests by request status and application type. Managers can also use the Requests filter to view only the requests from the users who report directly to them. ■ The Software Portal Administrator can customize the Software Portal header with company-branded background and logo images. ■ When the Software Portal Administrator publishes the software resource or a Managed Software Delivery policy that delivers the software resource to the Software Portal, the enhanced UI displays the predefined or custom icon for the software resource.

Table 1-1 New features (*continued*)

Feature	Description
Enhanced software resource management experience.	<p>When you edit a software resource in the Software Catalog, you can add or edit a custom icon for the software resource.</p> <p>When you manage the software resource in the Software Management view or in the Software Catalog, you can view these custom icons.</p>
Ability to configure access to the Software Portal from Mac client computers.	<p>The Software Portal Administrator can configure the Software Portal Client Access Policy that defines how end users access the Software Portal from client computers.</p> <p>The following options are available for Mac client computers:</p> <ul style="list-style-type: none"> ■ Show the Software Portal icon in the Symantec Management Agent user interface. ■ Show the link to the Software Portal in the Symantec Management Agent context menu.
Support for Windows 10 Fall Creators Update.	<p>Symantec Management Agent and solution plug-ins can be installed on Windows 10 Fall Creators Update 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/HOWTO127802</p>
New hierarchy replication rule.	<p>The new default hierarchy replication rule AD import Replication replicates data for users and computers that are imported from Active Directory.</p> <p>By default, this rule is disabled.</p>
Ability to configure hierarchy replication mode.	<p>The Replication mode option lets you configure what kind of data the hierarchy replication rule should replicate.</p> <p>For example, if you replicate Active Directory (AD) import data from parent Notification Server to its children, you can either replicate missing data for the resources that exist on child Notification Servers or replicate the resources that are not present on child Notification Servers.</p>
A Targeted Agent Settings policy with initial settings is enabled by default.	<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.</p> <p>The (Initial Settings) policy is now enabled by default.</p>
A full version number of Symantec Management Platform is displayed.	<p>A full version number of Symantec Management Platform is displayed in the dialog box that opens when you click Help > About Symantec Management Console... in the Symantec Management Console.</p> <p>Now the number also shows the release update version.</p>

Table 1-1 New features (*continued*)

Feature	Description
Workflow support for Symantec Endpoint Protection 14	From this release onwards, Workflow provides limited support for Symantec Endpoint Protection 14 components. For more information refer to the following article: DOC10748
Support for WinPE 10 1709 (Redstone 3)	From this release onwards, Deployment Solution supports WinPE 10 version 1709 (Redstone 3). For more information, refer to the following article: HOWTO126076

System requirements and supported platforms

Before you install IT Management Suite 8.1 RU5, 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 RU5 involves installation of Symantec Management Platform (SMP) 8.1 RU5 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 RU5

After you install this release update (8.1 RU5), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.1 RU5 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 RU5 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 RU5, 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 RU5 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU5

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.1.5844	8.1.5817
Altiris Client Task Agent	8.1.5844	8.1.5817
Altiris Client Task Server Agent	8.1.5860	N/A
Altiris Pluggable Protocols Architecture Agent	8.1.5419	N/A
Inventory Agent	8.1.5832	8.1.5832
Application Metering Agent	8.1.5636	8.1.5072 (Mac only)
Server Inventory Agent	8.1.5636	8.1.5636
Inventory Rule Agent	8.1.5844	8.1.5817
Monitor Plug-in	8.1.5412	8.1.5412
Package Server	8.1.5844	8.1.5817
Power Scheme Task Plug-in	8.1.4504	N/A
Software Update Plug-in	8.1.5620	8.1.5836
Software Management Framework Agent	8.1.5844	8.1.5817
Software Management Solution Agent	8.1.5889	8.1.5889

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU5 (*continued*)

Agent or plug-in	Windows	UNIX/Linux/Mac
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)	8.1.5845	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	8.1.5845	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 RU5:

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 RU5	Yes	Yes	Yes
Upgrade from 8.1 RU4 to 8.1 RU5	Yes	No	Yes

Post installation tasks for Deployment Solution

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

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

To recreate the automation folders

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

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

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

- PEInstall_x86

```
<install_dir>\Notification  
Server\NSCap\bin\Win32\X86\Deployment\Automation\PEInstall_X86
```

- PEInstall_X64

```
<install_dir>\Notification  
Server\NSCap\bin\Win64\X64\Deployment\Automation\PEInstall_x64
```

- LinInstall

```
<install_dir>\Notification  
Server\NSCap\bin\UNIX\Deployment\Linux\x86\Automation\LinInstall_x86
```

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

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

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

To deploy the automation folders on the Windows client computers

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

To deploy the automation folders on the Linux client computers

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

To deploy the automation folders on the Linux or Mac client computers

- 1 Run the following automation folder uninstall policies:
 - **Deployment Automation Folder for Linux-Uninstall**
 - **Deployment Automation Folder for Mac-Uninstall**

After you enable the **Deployment Automation folder for Mac-Uninstall** policy, you must manually delete the DSAutomation partition that is present in the unmounted and unallocated state.

If you do not want to run the uninstall policy to uninstall the automation folder from the client computer, you must manually erase the disk and the volume of the client computer. If you manually erase the disk and the volume of the client computer, ensure that you clean the Non-volatile random-access memory (NVRAM) of the client computer. For information on how to clean the NVRAM of a client computer, see the following article:
<https://support.apple.com/en-us/HT204063>
- 2 Run the following automation folder installation policies:
 - **Deployment Automation Folder for Linux-Install**
 - **Deployment Automation Folder for Mac-Install**

Fixed issues

IT Management Suite 8.1 RU5 contains fixed issues for the following solutions and components:

- Symantec Management Platform
See [“Symantec Management Platform Fixed Issues”](#) on page 16.
- 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.
- ITMS Management Views
See [“ITMS Management Views Fixed Issues”](#) on page 20.

- Patch Management Solution
See [“Patch Management Solution Fixed Issues”](#) on page 20.
- Software Management Solution
See [“Software Management Solution Fixed Issues”](#) on page 21.
- Workflow Solution
See [“Workflow Solution Fixed Issues”](#) on page 22.

Symantec Management Platform Fixed Issues

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

This release contains fixed issues for the following components:

- Symantec Installation Manager
See [Table 1-5](#) on page 16.
- Notification Server
See [Table 1-6](#) on page 16.
- Task Server
See [Table 1-7](#) on page 17.
- Symantec Management Agent
See [Table 1-8](#) on page 17.
- Network Discovery
See [Table 1-9](#) on page 17.

Table 1-5 Fixed issues for Symantec Installation Manager

Issue	Article link
When you try to open SIM while logged on with credentials other than Notification Server credentials, the SIM is not launched, and the following generic error is displayed in SIM logs: "Uncaught Exception in Application. One or more errors occurred."	N/A

Table 1-6 Fixed issues for Notification Server

Issue	Article link
NS.Hidden Purging Maintenance disregards the configured purging rules. For example, even if you configure the Evt_AeX_Client_LogOn data to be kept 60 days without a size limit, the NS.Hidden Purging Maintenance deletes this data daily.	N/A

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

Issue	Article link
When you define a schedule for a policy or task in the Symantec Management Console on a computer on which the Time Zone settings are different than on the Notification Server computer, the scheduled time is not saved as expected.	N/A
Notification Server Events (NSEs) are saved under C:\windows\system32\inetsvr folder.	TECH248162
When you specify a schedule in the Symantec Management Console, the first day of the week is not Monday in calendar.	N/A

Table 1-7 Fixed issues for Task Server

Issue	Article link
Saving the Call Web Service task that is configured with WSDL URL for ServiceDesk server fails with the following error: "Unexpected exception saving new task. Requested value '%!RequestChannel!%' was not found."	N/A

Table 1-8 Fixed issues for Symantec Management Agent

Issue	Article link
A Package Server that runs on Windows 2008 R2 SP1 constantly gets the following error: "Package Server is configured to publish HTTP(s) codebases, but could not access it's own Web site."	N/A
Image packages that are uploaded to Package Server remain in Pending download state after the upgrade to IT Management Suite 8.1 RU4.	N/A

Table 1-9 Fixed issues for Network Discovery

Issue	Article link
Network Discovery task that is configured to scan specific IP address discovers a non-existing device if no actual device is found at the specified IP address.	TECH248213

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 item and add data to a custom data class which has one of the attributes defined as Integer to a configuration item type, a following error occurs: An error occurred saving changes. Unable to save changes. There is a problem with the value for column 'Integer' at row 1., This issue appears when the custom data class types that have one of the attributes defined as Integer and the Required parameter is checked.	N/A
You can create a Cost Center without specifying the Cost Center Code , although it is a mandatory field.	N/A
In the Software view, when you edit a software license in in the Software Product dialog box, the Description of that license is cleared.	N/A
When you create or edit a Monitor configuration item, and on the editing/creating page, search for the Model information, the results appear at the bottom of the page, although they should appear directly beneath the Model search field.	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
For DeployAnywhere the password length is only 10 characters.	N/A
If you clone and modify the Install Windows OS task, the unattended.xml file is overwritten and the task fails.	N/A
If computers with MAC address pass through feature are booted into PXE or automation folder, recognize the MAC address of the docking station instead of the computer.	N/A
The custom unattend.xml file of an Install Windows OS task does not get replicated from parent Notification Server to child Notification Server.	N/A
Cannot import predefined computers using a CSV file in Deployment Solution 8.1 RU4.	N/A
The Driver Database Manager fails and no message is displayed when you try to add a driver to the preboot driver database if the previous driver import is in progress.	N/A
Jobs fail to run if you configure the Agent Registration Policy - Allow to anything other than Host name = *.	TECH247822

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

Issue	Article link
For Windows 10, the Prepare for Image capture task fails if the User Account Control (UAC) is turned on.	N/A
For Windows 10 Redstone 3, and Windows Redstone 2 after the Scripted OS Install task completes, you have to manually select and set the Region.	N/A
For Deployment Solution 8.1 RU2, custom compiled drivers are not added to LinPE.	N/A
Unable to upload Cab files to Sysprep Imaging Configuration .	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

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
When you open software summary in the Resource Manager, you may experience such performance issues as slow loading or timeout.	N/A
Inventory tasks may hang on SUSE client computers.	N/A
Standalone inventory incorrectly reports basic inventory data for OSBuildVersion on the target Windows 8.1/10 computers.	N/A
Software component remains associated with its software product when the component does not match the product filter criteria anymore because of the following changes: <ul style="list-style-type: none"> ■ The software product filter criteria are changed. ■ The software component name, company, or version is changed. Starting from 8.1 RU5, the predefined nightly task NS.Nightly schedule to associate Software component to software product breaks such association and moves the unassociated software component to Discovered Unreviewed Software .	N/A
Inventory Solution provides the predefined software product Adobe Acrobat DC that incorrectly includes the software component Adobe Acrobat Reader DC .	N/A
The predefined nightly task NS.Nightly schedule to associate Software component to software product runs very slowly in the environments that have numerous client computers.	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 1-13 Fixed issues for ITMS Management Views

Issue	Article link
<p>In the Software view, when you select a software product with one or more Managed Software Delivery policies applied, the policies are not displayed in the Policies installing this software section.</p> <p>This happens when the Managed Software Delivery policies contain software resources that are part of this software product.</p>	N/A
<p>When you scroll down the Managed Software Delivery Policies page, the page becomes blank and does not show any results.</p> <p>This issue appears in the Computers view, on the Managed Delivery Policies page of the filter summary view flipbook</p>	N/A
<p>In the Software view when you add a key program file to the software component, click Add Program, and then in the Add Program dialog box, check Show all program files, the dialog box stops responding and times out.</p>	N/A
<p>Inventory data is not displayed in the Computers view, if it is gathered using the standalone-alone packages.</p>	N/A
<p>In the Software view, when you edit a software release, the Software resource page opens in the bottom of the screen. As a result, the options on the Software Publishing tab are not fully displayed.</p>	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
<p>Patch Management Solution for Linux incorrectly handles 3rd party <code>.repo</code> files that may appear in the location where the software update plug-in keeps its temporary <code>.repo</code> files for the client-based dependency resolving.</p>	N/A
<p>Windows system assessment scan fails to run on child Notification Server computers.</p>	N/A

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

Issue	Article link
CentOS patches that are published in non-standard format in The CentOS-announce Archives are not imported to Patch Management Solution.	N/A
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.	HOWTO127741

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 publish a Managed Software Delivery policy or a software resource to the Software Portal and change the target on the Software Publishing tab, the Select a resource target dialog box is small and not re-sizable. As a result, the dialog box does not display full target names.	N/A
While publishing a software resource or a Managed Software Delivery policy to the Software Portal, you can target devices and users for software publishing. However, when you edit the existing targets on the Software Publishing tab, the following issues occur: <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
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.	N/A
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.	N/A

Table 1-15 Fixed issues for Software Management Solution (*continued*)

Issue	Article link
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 .	N/A
You may experience slow loading or timeout when you add tasks to a Managed Software Delivery policy.	N/A
You cannot import a ZIP or DMG installation file into the Software Library or an existing UNC to create a software resource for macOS High Sierra 10.13.2.	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
Value of the variable is not displayed in the output when the Generated script component - Script Generator (C#) uses multiple output paths.	N/A
Mobile devices do not support emails that are sent from Automation using the UTF-16 encoding.	N/A
Secure attribute is not set for Process Manager login.	N/A
Digital gauge Component disappears after page postback.	N/A
The Process Action Send Email does not allow attachments.	N/A
The Send Email Action does not display the applied template properly. The description of the incident does not include line breaks.	N/A
In Workflow Designer, the Rectangle component does not allow selection by single click.	N/A
In the Workflow Designer, an error is displayed if you select a component empty configuration field and then try to select or change fields.	N/A
Line graphs and Point graphs of the Report Viewer do not show the definition for the value when you hover the mouse pointer on any of the data points.	N/A
The Radial gauge value is set to the middle of the default value after page postback.	N/A

Known Issues

IT Management Suite 8.1 RU5 contains known issues for the following solutions and components:

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

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 23.

Table 1-17 Known issues for Symantec Management Agent

Issue	Article link
<p>A Package Server that is set to publish CEM/HTTPs codebases fails to access its own site and serve its client computers after upgrading this Package Server to Windows 10 Redstone 3.</p> <p>This is an OS-specific issue: HTTP Error 503 and WAS event 5189 on Windows 10</p> <p>Workaround: Apply the newest updates of Windows 10 Redstone 3.</p>	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
<p>Failed to update preboot configuration packages on package servers. An error is logged in the Deployment Solution: reloadPackage.</p> <p>Workaround:</p> <p>If you add drivers to the preboot database or import a new WinPE, you must manually run the package refresh task.</p>	N/A
<p>The Install Windows OS task fails if you use the default setting for the configuration option.</p> <p>Workaround:</p> <p>Select another option from the drop down list for the Configuration option and then select the Use inventory data to reconfigure computer.</p>	N/A
<p>For WinPE 10, the Partition Disk task is unable to create required partitions.</p>	N/A
<p>Automation folder is no longer functional after you deploy a BIOS-based image to a UEFI computer.</p>	N/A
<p>Sometimes, package upload from Symantec Management Console fails for OS Files and Drivers upload.</p>	N/A
<p>For macOS Sierra 10.13 NetInstall (SOI) is not currently supported.</p>	N/A
<p>For macOS Sierra 10.13 sometimes the Deploy Image task of Apple file system containers fails with following error:</p> <p>Could not mark APFS container as new/unique.</p>	N/A
<p>Deploy Image task fails to deploy an image of a computer with RHEL 7.2 operating system and XFS file system.</p>	N/A
<p>For macOS Sierra 10.13 clients, you cannot create image of volumes of Apple File System containers.</p>	N/A
<p>Computers that imported from the Active Directory are listed in Predefined Computers.</p>	N/A

Software Management Solution Known Issues

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

Table 1-19 Known issues for Software Management Solution

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

Where to get more information

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

Table 1-20 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 1-20 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 1-21 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 1-21 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.	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