Symantec™ IT Management Suite 8.5 RU2 Release Notes

Symantec™ IT Management Suite 8.5 RU2 Release Notes

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

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

Knowledge Base Articles and Symantec Connect

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

https://support.symantec.com

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

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

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

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

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

To contact Symantec Support, see:

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

Symantec IT Management Suite 8.5 RU2

This document includes the following topics:

About Symantec IT Management Suite

Symantec IT Management Suite is a tool for managing corporate IT assets such as desktop computers, laptop computers and servers that have Windows, UNIX, Linux, or Mac operating systems.

IT Management Suite is a collection of solutions and components that run on the Symantec Management Platform.

What's new in this release

In IT Management Suite 8.5 RU2, the following new features are introduced:

Table 1-1 New features

Feature	Description
Expanded list of supported platforms for Symantec Management Agent.	The following operating systems are now supported for the installation of the Symantec Management Agent and solution plug-ins: ■ Windows Server 1809 and 2019 LTSC (Core installation) For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11329 ■ Red Hat Enterprise Linux (RHEL) 7.6 and CentOS 7.6 For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11324 ■ Solaris 11.4 For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11319 ■ VMware ESXi 6.7 For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11325
Patch Management Solution support for Microsoft Office 2019.	Patch Management Solution for Windows supports Microsoft Office 2019 Volume and Retail updates. The patch management metadata release version 7.3 contains the following Microsoft Office 2019 software products: ■ Microsoft Office Click to Run 2019 Volume ■ Microsoft Office Click to Run 2019 Retail For more information, see the knowledge base article DOC11334.
Patch Management Solution support for Windows 10 feature updates installation on endpoints with drive encryption.	You can use Patch Management Solution for Windows software update policies together with the upgrade scripts provided by Symantec to install Windows 10 feature updates on endpoints with Symantec encryption products without decrypting and re-encrypting your drives. The upgrade scripts provided by Symantec support Symantec Endpoint Encryption and Symantec Encryption Desktop by default. You can use additional customization options to address specifics of your environment. For more information, see the knowledge base article TECH252359.
Patch Management Solution support for Oracle Java SE 8 non-public updates.	Patch Management Solution supports deployment of non-public updates for Oracle Java SE Runtime Environment (JRE) starting from **JRE 8u211**. For more information, see the knowledge base article TECH252140.

Table 1-1 New features *(continued)*

Feature	Description
New patch management task for software update installation.	Patch Management Solution lets you create an **Install Software Updates** task for installation of single or multiple software updates. If you need to perform management operations immediately before and after the installation of the updates as part of a sequence of events, you can sequence the task in a single client job with other pre- and post-installation tasks according to your needs. For more information, see the knowledge base article DOC11414
Added ability to back up and restore critical Notification Server data.	In Symantec Installation Manager, you can now back up and restore the following items: ■ Notification Server root certificate and Site Server root certificate ■ Notification Server Web configuration ■ Notification Server core settings and registry ■ Software Library content You can also configure schedules to create backups regularly, in Symantec Management Console, on the **Notification Server Settings** page, on the **Critical Data Backup** tab, at **Settings > Notification Server > Notification Server Settings**.
Changes in peer-to-peer downloading.	The following changes are made in peer-to-peer downloading feature: ■ Peer-to-peer network can now also be created based on sites. ■ A new option is added for disabling peer-to-peer downloading when a Package Server is available in the peer-to-peer network.
New policies for configuring settings for a site.	New **Targeted Site Settings** policies let you limit the number of simultaneous outbound data transfers from an internal site or from an Internet site. This feature also introduces two new reports: ■ **Outbound Data Transfers by Site** ■ **Details of Outbound Data Transfers** The reports are located at **Reports > Notification Server Management > Server > Subnets and Sites Info > Data Transfers by Site**. Note that by default, these reports are visible only to **Symantec Administrators** role.
New throttling type for downloads.	In **Targeted Agent Settings**, you can configure a new throttling type **Range**. This throttling type regulates Symantec Management Agent traffic depending on the third-party application traffic while keeping the agent traffic within the specified range.

Table 1-1 New features *(continued)*

Feature	Description
New task for sending notifications to end users.	The **End User Notification Task** lets administrators create and configure notifications that are displayed to the end users on their devices. You can use default or custom token(s) in **Title** and **Body** of the tasks with **Plain text** or **HTML**. By default, only **Symantec Administrators** role can schedule this task.
Enhancements of jobs and tasks management.	Jobs and tasks management introduces the following enhancements: ■ When you schedule a job or task, you can now allow end users to postpone running this job or task for a specified period of time. ■ Rerun task functionality is extended with the ability to rerun some other task on the computers where the previous task failed. ■ The **Prevent the computer from going into sleep mode** option can now be enabled for the job. ■ The **Non-elevated user** option lets you launch task processes with restricted security settings. ■ **Job/Task Status Details** report provides more detailed information with its three new columns: **Start Date**, **End Date**, and **Started By**. Its drill-down report **Client Task Status Details** also has three new columns: **Start Date**, **End Date**, and **Task Server**.
Added ability to select **Targets** in Endpoint Management Workspaces.	The user can now select **Targets** when performing **Run Task** and **Deliver Software** quick tasks in Endpoint Management Workspaces. Configuring access to Targets in Endpoint Management Workspaces Viewing target details
Added ability to select scoping for targets in the **Computers** view content pane.	You can now prepare the targets and share them with the users with different roles in the **Computers** view content pane.
Tasks in Endpoint Management Workspaces override maintenance windows.	The tasks in Endpoint Management Workspaces override all maintenance windows that are specified in Notification Server configuration policies. When the user selects a task in the **Deliver Software** or **Run Task** widget, the task runs ASAP.
Improved speed of Red Hat Linux and SUSE Linux computer patching.	Client-based dependency resolving now speeds up the download of dependent software update packages to the Notification Server. As soon as the package download completes, the package distribution to the package servers starts immediately. For more information about limitations in the client-based dependency resolving, see the KB article DOC9722.

Table 1-1 New features *(continued)*

Feature	Description
Enhanced Patch Management Solution for Linux compliance reports.	New right-click menu items in Patch compliance reports for Red Hat Linux, SUSE Linux, and CentOS let you view the following data: ■ Applicable updates for a computer ■ Applicable computers by update ■ Applicable computers by erratum ■ Applicable computers by announcement
Software publishing enhancement.	On the **Software Portal Settings** page, the Software Portal Administrator can use a new setting to publish software for the users and groups in the specified list of domains trusted by the Notification Server domain. **Note:** If you have trusted domains defined in the registry for pre-8.5 RU2 versions, and then you upgrade to 8.5 RU2, the corresponding settings will be automatically configured on the **Software Portal Settings** page after upgrade. Starting from 8.5 RU2, maintenance of the registry values for trusted domains is no longer supported.
Removal of the Software Portal legacy user interface support.	The Software Portal deprecates support of the legacy user interface. Starting from 8.5 RU2, the enhanced user interface is the only UI of the Software Portal.
Enhanced Software Portal notifications.	Users can get detailed notifications about the installation of requested applications if users enable the notification option **Display notification when requested application is installed on my device**. In the Software Portal, users can also check the installation statuses of requested applications.
Immediate software delivery from approved software requests.	After a Software Portal user requests an application and the request is approved, the download and installation of the application starts within 1 minute.
Enhancements of ASDK.	The following enhancements are introduced in ASDK: ■ Added **GrantRoleItemPermissions** and **RemoveRoleItemPermissions** methods to add or remove item permission for a Role. ■ New method **SetAssetOwner** added to **ResourceManagementLib** class. This method lets you assign a state to a particular asset resource. ■ **TaskManagement.ExecuteTask** method lets you run client job with option **Allow the user to defer execution of this task**.

Table 1-1 New features *(continued)*

Feature	Description
ITMS Help System no longer requires Java 8 to be installed on Notification Server.	In Symantec Installation Manager, Java 8 requirement is removed from **Installation Readiness Check**. ITMS Help System uses now Java 11. For more information regarding Java support, refer to the following article: INFO5397

System requirements and supported platforms

Before you install Symantec IT Management Suite 8.5 RU2, read the section Hardware recommendation in the *IT Management Suite Planning for Implementation Guide* at the following URL:

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

For information about the supported operating systems in Symantec Management Platform and the Symantec IT Management Suite solutions, see the knowledge base article at the following URL:

http://www.symantec.com/docs/HOWTO9965

General installation and upgrade information

The installation of IT Management Suite (ITMS) 8.5 RU2 involves installation of Symantec Management Platform (SMP) 8.5 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/DOC11093

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

TECH250873.

Upgrade to IT Management Suite 8.5 RU2

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

- From IT Management Suite 8.5 to IT Management Suite 8.5 RU2

- From IT Management Suite 8.5 RU1 to IT Management Suite 8.5 RU2

After you install this release update (8.5 RU2), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.5 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.

Note: To upgrade to the latest release update, log on to the Notification Server computer with the SMP application identity credentials.

In ITMS 8.5 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 knowledge base article:
  http://www.symantec.com/docs/TECH183086

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

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

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

After you upgrade IT Management Suite to this release update, upgrade the Symantec Management Agent, the site servers, and the solution plug-ins.

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

Step	Action	Description
Step 1	Upgrade the Symantec Management Agent on site servers.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the policies that upgrade the Symantec Management Agent on site servers.
Step 2	Upgrade the site servers.	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. 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. 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. **Note:** Ensure that all operating system updates and antivirus software updates are installed on the site server before starting the upgrade of Symantec Management Agent and Site Server services. Unfinished updates may interfere with the upgrade process.
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.	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. To upgrade the solution-specific plug-ins to the latest version, do the following: ■ In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent. ■ In the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for the site server plug-ins. ■ In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the plug-in upgrade policies.

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

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

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

For more information on the post-upgrade tasks, see the chapter *Performing post-upgrade tasks* in the *IT Management Suite Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC11093

Post-upgrade versions of Symantec Management Agent and solution plug-ins

The Symantec Management Agent and its plug-in versions after you upgrade to ITMS 8.5 RU2 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.5 RU2

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.5.4249	8.5.4235
Altiris Client Task Agent	8.5.4249	8.5.4235
Altiris Client Task Server Agent	8.5.4242	N/A
Altiris Pluggable Protocols Architecture Agent	8.5.4215	N/A
Inventory Agent	8.5.4273	8.5.4273
Application Metering Agent	8.5.4273	8.5.3041 (Mac only)
Server Inventory Agent	8.5.4273	8.5.3687
Inventory Rule Agent	8.5.4249	8.5.4235
Monitor Plug-in	8.5.3615	8.5.3615
Package Server	8.5.4249	8.5.4235
Power Scheme Task Plug-in	8.5.3006	N/A
Software Update Plug-in	8.5.4276	8.5.3049
Software Management Framework Agent	8.5.4249	8.5.4235
Software Management Solution Agent	8.5.4222	8.5.4222
Virtual Machine Management Task Handler	8.5.4203	N/A
Deployment Task Server Handler	8.5.4252	N/A
Deployment Package Server	8.5.4252	N/A
Deployment Plug-in for Windows (x64/x86)	8.5.4252	N/A
Deployment Plug-in for Linux (x64)	N/A	8.5.4252
Deployment Plug-in for Linux (x86)	N/A	8.5.4252
Deployment Plug-in for Mac	N/A	8.5.4252
Deployment NBS plug-in	8.5.4252	N/A

Performing post installation tasks for Deployment Solution

The following table lists the upgrade scenarios for which you must recreate the automation folders after you install the ITMS 8.5 RU2:

Table 1-4 Post installation tasks for Deployment Solution

Upgrade	Windows automation folder	Mac automation volume	Linux automation folder
Upgrade from 8.5 to 8.5 RU2	Yes	Yes	Yes

Post installation tasks for Deployment Solution

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

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

To recreate the automation folders

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

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

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

   - PEInstall_x86

     `<install_dir>\Notification Server\NSCap\bin\Win32\X86\Deployment\Automation\PEInstall_X86`
   - PEInstall_X64

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

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

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

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

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

To deploy the automation folders on the Windows client computers

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

To deploy the automation folders on the Linux client computers

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

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

1. Run the following automation folder uninstall policies:
   - **Deployment Automation Folder for Linux-Uninstall**
   - **Deployment Automation Folder for Mac-Uninstall**
     After you enable the **Deployment Automation folder for Mac-Uninstall** policy, you must manually delete the DSAutomation partition that is present in the unmounted and unallocated state.
     If you do not want to run the uninstall policy to uninstall the automation folder from the client computer, you must manually erase the disk and the volume of the client computer. If you manually erase the disk and the volume of the client computer, ensure that you clean the Non-volatilerandom-accessmemory (NVRAM) of the client computer.
     For information on how to clean the NVRAM of a client computer, see the following article:
     https://support.apple.com/en-us/HT204063
2. Run the following automation folder installation policies:
   - **Deployment Automation Folder for Linux-Install**

- **Deployment Automation Folder for Mac-Install**

Fixed issues

Note: This document includes only the fixed issues resolved within the IT Management Suite version 8.5 RU2. For more information about the fixed issues in IT Management Suite 8.5, see the following release notes:

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

IT Management Suite 8.5 RU2 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 18.
- Deployment Solution
  See "Deployment Solution Fixed Issues" on page 19.
- Inventory Solution
  See "Inventory Solution Fixed Issues" on page 20.
- IT Analytics
  See "IT Analytics Solution Fixed Issues" on page 21.
- IT Management Suite Views
  See "ITMS Management Views Fixed Issues" on page 21.
- Patch Management Solution
  See "Patch Management Solution Fixed Issues" on page 22.
- Software Management Solution
  See "Software Management Solution Fixed Issues" on page 22.
- Workflow Solution
  See "Workflow Solution Fixed Issues" on page 24.

Symantec Management Platform Fixed Issues

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

This release contains fixed issues for the following components:

- Notification Server

See Table 1-5 on page 17.

- Task Server
  See Table 1-6 on page 18.
- Symantec Management Agent
  See Table 1-7 on page 18.
- Network Discovery
  See Table 1-8 on page 18.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
After upgrading to IT Management Suite 8.5 or 8.5 RU1, horizontal scrollbar at the bottom of the reports is not showing up.	TECH253199
When you edit report parameters and leave the cursor in the text box, pressing **Enter** does not run the report but opens it for editing.	N/A
When you save a report as a CSV file, a leading comma is added to all data rows.	N/A
A user with non-administrative privileges gets "**No resources are added to organizational group**" error while trying to assign computers to an Organizational Group.	N/A
Replicating resources using standalone replication changes resource ownership even when **ReplicationOverwriteSourceNS** is set to **false**.	N/A
When you try to edit MSI command line, the following error occurs: "**ctrlAccordion: ReferenceError: 'ctrlAccordion_expdUninstallOptions' is undefined**"	N/A
In the **Client Task Status Details** report, question marks are displayed instead of non-Unicode characters.	N/A
Problems with stalled handshakes and queue overflow cause high memory and processor usage on Internet Gateway.	N/A
The less than (**<**) character in a token is replaced with **#%cLt#%** after you save this token.	N/A
When you edit a token, the text that you type does not appear where you have placed the cursor.	N/A
After upgrading to Symantec Management Platform version 8.5 RU1, software filters cannot be edited in Basic Query Mode.	TECH254025

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

Issue	Article link
When you select new certificate on **Command Line Right-Click Action Certificate** page and save it, the original Agent CA certificate gets selected and saved.	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
Communication errors between site server and Client Task Agent with the following error: **"Client Certificate is not trusted or not valid."**	N/A
When you create a Power Shell script with Unicode characters and run it in a Run Script task, the task converts the script to ASCII and replaces characters with question marks.	N/A
After you enable Websocket connection on Notification Server, Client Task Agent loses tickle connection to remote Task Server.	N/A

Table 1-7 Fixed issues for Symantec Management Agent

Issue	Article link
Certain configurations in Targeted Agent Settings and Communication Profile cause CEM agents to disconnect regularly.	N/A
Warning messages about terminated persistent connection are displayed on Agent UI and in logs even if persistent connection is not enabled.	N/A

Table 1-8 Fixed issues for Network Discovery

Issue	Article link
Network Discovery does not work with SNMP v2 protocol after you add multiple comma separated values as community names for this protocol.	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 1-9 Fixed issues for Asset Management Solution

Issue	Article link
Asset Management Solution fails to configure AssetControl.config during upgrade process from 8.1 RU7 to 8.5, and then to 8.5 RU1.	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
Sometimes it takes more than 10 minutes to download the PXE package from a remote PXE Server if the network download speed is slow.	N/A
The **Deploy Image** task **Image Name** field fails to filter the images.	N/A
When you deploy an image of Windows 2019 or Windows 10 LTSC, the computer name is set to random as the operating systems are recognized as Windows XP.	N/A
When you upgrade to Deployment Solution 8.5, all the custom files that are present at `\Program Files\Altiris\Notification Server\NSCap\Bin\Deployment\BDC\bootwiz\Platforms\WinPE` are deleted and replaced with the default files.	N/A
You cannot log on to the client computer after you install RHEL 7.6 server edition using the scripted OS Install task.	N/A
After you deploy the disk image of SUSE Linux Enterprise Server 15, the host name does not change.	N/A
Surface Pro 4 computers using docking stations do not match the record when you use a USB device for imaging.	N/A
Extract SSL Certificate policy keeps running on the sire server if DISM.exe scripts are not updated.	N/A
The Deployment Solution **Scripted OS Install** task fails when TLS 1.2 is the only protocol enabled.	N/A
Duplicate records are displayed when you boot a computer into automation mode using external NICs.	TECH251140
Deployment Solution fails to save an image over HTTP and https to the Package Server if the App ID password includes a '\' , ':" or "@" character.	TECH251929

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

Issue	Article link
Deployment Solution fails to work with the new **Custom Package Service Settings**.	TECH253092
For a predefined computer with name and serial number only, the Mac address inventory is not collected during the basic inventory collection.	N/A
The MTU package size that is set in the NBS General Settings is not respected you try to PXE Boot a client computer.	N/A
The following error is displayed when you deploy an image using https: `unexpected character following SZE parameter`	TECH252727
Duplicate records are created for Predefined computers when you run the Push Symantec Management Agent policy.	N/A
Client computer fails to join the domain that is specified in the **Install Windows OS** task.	N/A
When you import predefined computers, it times out displays an exception.	N/A
When you add predefined computers without hardware identifier, duplicate records are created.	N/A
The **Copy File** task fails to copy folder to the client computer.	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 1-11 Fixed issues for Inventory Solution

Issue	Article link
Software inventory data remains in reports for the software that is no longer installed on Mac or Linux client computers.	N/A
The following policies or tasks fail on client computers that have AppX software with corrupted `AppxManifest.xml` file. ■ **Software Discovery** policy ■ **Gather Inventory** task ■ **Collect Full Inventory** policy	N/A

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

Issue	Article link
Inventory Solution can incorrectly report Symantec Endpoint Protection (SEP) for Windows agent version after SEP upgrade if multiple entries for older SEP agent versions are present in the registry.	N/A
Only users with administrator privileges can run standalone inventory.	N/A
The Resource Manager presents incomplete software inventory data on the **Software Summary** page, under the **Add Remove Program**.	N/A
You can discover a network device using the Network Discovery task with a custom connection profile. However, you cannot gather inventory data about such network device because agentless inventory uses the default connection profile instead of the custom connection profile that you have specified.	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 1-12 Fixed issues for IT Analytics Solution

Issue	Article link
For some versions of SQL Server 2016, cube **Processing** task cannot be completed.	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
When you associate multiple program files with a software product, in the **Add Program** dialog box, under **Available programs**, only one file is listed. This issue occurs if the files have the same name and version.	N/A
After you delete a custom data class which is added as a **Filter Criteria** to a filter, the filter displays the following error: `An error has occurred that prevents the data displaying. Check server logs for details.`	N/A

Table 1-13 Fixed issues for ITMS Management Views *(continued)*

Issue	Article link
No data is displayed in the **First Time Setup** portal. This issue occurs if the user is a member of multiple security roles.	TECH253808

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
When software update packages are recreated on child Notification Server after the corresponding software update policy is replicated from the parent Notification Server to its child, the packages may lose their package servers assignment and get **Not Ready** status until availability information is resent from the package servers.	N/A
Patch management metadata for CentOS bulletins is incomplete because CentOS announcements regarding the CR repositories are not included.	N/A
You can enable the Hierarchy Editable Property feature for the **Default Software Update Plug-in Policy** to make the policy page editable on the child Notification Server. However, after you edit and save the policy installation schedule settings on the parent Notification Server, and replicate the policy down the hierarchy, the settings become disabled and non-editable on the child Notification Server.	N/A
You cannot save as a CSV file any of the following Windows Update-specific compliance reports: ■ Microsoft Updates ■ Windows (Microsoft Data) Compliance by Update ■ Windows (Microsoft Data) Compliance by Computer ■ Windows (Microsoft Data) Compliance Updates	TECH254241

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
Targets of the **Software Portal Client Access Policy** change automatically during upgrade.	N/A
An error occurs when you save a software package that contains a colon in the name.	TECH252498
Old software cache `.xml` files cause the Symantec Management Agent to stop responding.	N/A
You cannot submit more than one request for an unlisted application in the Software Portal.	N/A
The **Execution status** report fails to run or runs for too long time and then fails.	TECH253458
When you import a software package with multiple files to create a software resource, select the file that is not automatically defined as the installation file, and then click **Set Installation File**, two files appear in bold type as the installation files. Only the file that you have selected will be used to generate the command lines though.	N/A
When you import a software package and source the package file from the Software Library, the **Date Modified** of the file changes to the date and time of the file import.	N/A
The **Software Compliance** report presents no results for the Managed Software Delivery policy that has spaces at the beginning or end of the name.	N/A
When you change the order of **Service pack and Update Tasks** in a Managed Software Delivery policy, and then save the policy, the changes are not preserved.	N/A
When you create a new software release using an installation file larger than 5 GB, and then you create and run a Managed Software Delivery policy with this software release, the actual start of installation process occurs in 60 seconds or later after the reported policy execution.	N/A
When you use Azure Active Directory (Azure AD) and run a Managed Software Delivery policy with the option **Current logged-on user** enabled, the policy fails with the following error: `Failed to build interactive user SID. Error = 0`	N/A
When you apply a non-English language to the Symantec Management Console, and then run the ASDK method **Windows Batch Installation File** for the parameter **InstallationFileType** using English versions of the installation file names, the method fails with an error.	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
In a localized environment, If you add a rule set, the rule set engine does not properly interpret them, and following error is displayed: Requested value was not found.	N/A
DLP Workflow Components of Symantec.Components.DLP.Reporting.dll does not recognize the URL values that are set in the **Properties** of the Workflow Project.	N/A
Cannot remove or convert the Workflow project properties.	TECH253804
The **Edit Web Part** option does not work in Internet Explorer with Compatibility View enabled.	TECH236070
When you debug a web application project, the following error is displayed: System.NullReferenceException: Object reference not set to an instance of an object at LogicBase.Tool.UI.Debugging.DebugEngine.CheckEscalationThreadStart()	N/A
You cannot save after editing a knowledge base article that includes an HTML. Following error is displayed: Error Application 'LogicBase.Ensemble' System.Web.HttpUnhandledException (0x80004005): Exception of type 'System.Web.HttpUnhandledException' was thrown.	N/A
Only the first page of the report is exported when you generate a report based on Age and Description.	N/A
Failed to validate project as you cannot add default values to Global Data of type Integer and Decimal.	N/A
The **Web Chart Component** values are duplicated when you refresh the form page.	TECH252638
Failed to interpret localized Group Permissions.	N/A
The Report loader that runs on Process Manager startup fails to overwrite existing reports.	N/A
The Changelog Info-level messages are displayed with default or error level logging and are also copied to the event logs.	N/A

Known Issues

Note: This document includes only the issues that were found within the IT Management Suite version 8.5 RU2 For more information about the known issues in IT Management Suite 8.5, see the following release notes:

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

IT Management Suite 8.5 RU2 contains known issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Known Issues" on page 25.
- Deployment Solution
  See "Deployment Solution Known Issues" on page 26.
- Patch Management Solution
  See "Patch Management Solution Known Issues" on page 27.

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 25.
- Task Server
  See Table 1-18 on page 26.

Table 1-17 Known issues for Symantec Management Agent

Issue	Article link
End User Notification Task is not supported on Windows Core operating system. End user will see an empty dialog box with warning icon when **End User Notification Task** arrives on such client computer.	N/A

Table 1-18 Known issues for Task Server

Issue	Article link
In some cases, when you use a shared target for a task schedule, the following error may occur: "**An unexpected error occurred while saving this schedule. See the Altiris log for more information.**" **Workaround:** Re-save the target in target builder.	N/A
When you create an **End User Notification Task**, select **Binary**, specify location of a file, and then save the task, the specified file location disappears when you reopen this task. **Workaround:** Reopen the task and move the cursor over the **Browse** button.	N/A
Selecting **Binary** and specifying a file that is bigger than 25 MB for the **End User Notification Task** causes very high memory consumption by W3WP process.	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 1-19 Known issues for Deployment Solution

Issue	Article Link
Scripted OS Install task fails for Windows 7 if the computer is booted with WinPE 10 1809.	N/A
You cannot convert an EFI image with multiple partitions from GPT partition type when deployed on a BIOS-based client computer.	N/A
The **Copy file** task fails to copy files or folders using the UNC path when FIPS mode is enabled on a Linux client computer. Workaround: Disable the FIPS mode and run the task again.	N/A
The **Boot To** task fails to boot a Mac client computer as the System Integrity Protection feature is introduced in Mac OS X 10.11. Workaround: Run the csrutil disable command in the Recovery Mode.	N/A
For macOS Sierra 10.13 and higher NetInstall (SOI) is not currently supported.	N/A

Table 1-19 Known issues for Deployment Solution *(continued)*

Issue	Article Link
For macOS Sierra 10.13 and higher sometimes the **Deploy Image** task of Apple file system containers fails with following error: Could not mark APFS container as new or unique.	N/A
Automation folder is no longer functional after you deploy a BIOS-based image to a UEFI computer.	N/A
For macOS Sierra 10.13 and higher clients, you cannot create image of volumes of Apple File System containers.	

Patch Management Solution Known Issues

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

Table 1-20 Known issues for Patch Management Solution

Issue	Article link
The **Install Software Updates** task may fail with the error 87 if you configure the Windows patch remediation settings so that the software update program runs under the specified user account. Workaround: Re-run the task or change the remediation settings so that the program runs under the system account.	N/A

Where to get more information

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

Table 1-21 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Release Notes**.

Table 1-21 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.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Documentation**.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ 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 1-22 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 1-22 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: ■ 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