Symantec™ IT Management Suite 8.5 RU3 Release Notes

Symantec™ IT Management Suite 8.5 RU3 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 RU3

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 RU3, 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 10 (version 1903) and Windows Server (version 1903) For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11328 ■ Windows 10 Enterprise 2016 LTSB For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11464 ■ Windows 10 (version 1909) and Windows Server (version 1909) For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11462 ■ macOS 10.15 For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11459 ■ SUSE Linux Enterprise Server 12 SP4 and SUSE Linux Enterprise Desktop 12 SP4 For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/DOC11463
Support for SQL Server 2017	Support for SQL Server 2017 is added.
Google Chrome browser support	Starting IT Management Suite 8.5 RU3 you can use Google Chrome browser to access Symantec Management Console on Windows computers.
Support for Windows 10 Build ADK.	Starting with 8.5 RU3, for WinPE 10, you can import any version of Windows 10 Build ADK. For more information, refer to the following article: Info3561
Ability to access cloud help without installing on-premise documentation.	You can now open Symantec Management Console help topics even if you do not install documentation on your Notification Server computer. Note that since the help is located on cloud, your Notification Server (or the computer from which you access the Symantec Management Console) must have Internet access. When you upgrade from previous versions of IT Management Suite to a version 8.5 RU3, you have an option in Symantec Installation Manager (SIM) to uninstall documentation during the upgrade.

Table 1-1 New features *(continued)*

Feature	Description
Enhanced overall user experience due to Microsoft Silverlight requirement removal.	■ Microsoft Silverlight is no longer required and replaced by HTML5 for the following IT Management Suite Views: ■ **Software View** ■ **Computers View** Opens by default after you install IT Management Suite 8.5 RU3, and then open Symantec Management Console for the first time. ■ **Policies View** ■ **Jobs and Tasks View** ■ Microsoft Silverlight IRC is removed from Symantec Installation Manager (SIM). **Note:** Client Management Suite users can uninstall Microsoft Silverlight after upgrade to 8.5 RU3. In Server Management Suite and IT Management Suite, Event Console still requires Microsoft Silverlight.
Enhancements of software and computer management.	The following new features are introduced in the IT Management Suite **Software View**: ■ All **Software Catalog** management activities and functionalities are moved to the **Software View**. ■ New **Add Software** icon/button lets you quickly perform one of the following actions: - Import a package - Create a software product - Create a software resource (Software Release, Service Pack or Software Update) ■ The **Software Product** dialog box is replaced by the **Software Product** flipbook. The following new features are introduced in the IT Management Suite **Computers View**: ■ A new folder in the targets tree **Time Critical Management** contains targets that you create in the **Time Critical Management** workspace. ■ When you create or edit a computer view or group, a new option **Include child groups** lets you include into a resource filter all resources in sub-groups hierarchy of a selected organizational view or group.

Table 1-1 New features *(continued)*

Feature	Description
Enhancements of jobs and tasks management.	Jobs and tasks management introduces the following new features: ■ The new **Running and Recently Completed Tasks** portal lets you check the status of the tasks in real time and perform various task management actions. ■ Auto refresh option is added to the **Task Instance Details** page.
Enhancements of the **Targeted Site Settings** policy.	**Targeted Site Settings** policy lets you now limit the outbound package download bandwidth and the sources from which the agents can download packages.
Enhancements of the download settings in Software Management Solution and Symantec Management Agent.	Now you can configure the download settings in Software Management Solution and Symantec Management Agent to perform the following actions even if the bandwidth is not greater than the connection speed: ■ Run the package directly from the Notification Server computer. ■ Download the package or the command line and run it locally.
Ability to manually create Symantec Management Agent support package.	In the Symantec Management Agent user interface, you can now manually create an agent support package that contains logs and other files useful for troubleshooting.
Enhancements of the Symantec Administrator Software Development Kit (ASDK) application programming interface (API).	The Symantec ASDK provides APIs that you can use to automate and customize the Symantec Management Platform. You can call APIs through Web services, COM, and the Windows command line (CLI). In 8.5 RU3, the following new API methods for interfacing with Task Management are introduced: ■ CreateClientJob ■ CreateServerJob ■ AddTaskFirstToJob ■ AddTaskLastToJob ■ CreateJobCondition ■ AddJobConditionRules ■ AddTaskToJobConditionThenGroup ■ AddTaskToJobConditionElseGroup ■ RemoveJobCondition ■ RemoveNodeFromJob ■ RemoveAllNodesFromJob ■ ConfirmJobChanges For more information, see the Symantec ASDK Help at `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Symantec\ASDK`

Table 1-1 New features *(continued)*

Feature	Description
New patch management task for software update assessment.	Patch Management Solution lets you use a **Windows Software Update Assessment** task to assess applicability of selected software updates and detect if the updates are already installed on client computers. You can create a separate **Windows Software Update Assessment** task, and then manually sequence the task before a **Windows Software Update Installation** task in a single client job. Patch management reports also let you use a wizard to create one or both software update tasks together with a client job that contains the tasks. For more information, see the knowledge base article DOC11578
Enhancements of Patch Management Workflow Web Service application programming interface (API).	Patch Management Workflow Web Service is installed with Patch Management Solution. The service contains API that accesses the functionality of Notification Server (NS) and lets you perform various patch management actions. You can access the service at http:///*localhost*/Altiris/patchmanagementcore/patchworkflowsvc.asmx In 8.5 RU3, the following enhancements are introduced: ■ HTML Help page The page includes list of available methods, detailed method descriptions, and usage examples for some methods. You can access the page at http:///*localhost*/Altiris/patchmanagementcore/patchworkflowsvc.html ■ New API methods: - CreateWindowsUpdateAssessmentTask - CreateWindowsUpdateInstallationTask - EditWindowsUpdateAssessmentTask - EditWindowsUpdateInstallationTask For more information, see the knowledge base article DOC11543.
Enhanced superseded update clean-up process.	When you configure the **Import Patch Data** task, you can set the time period to define the superseded software updates that you want to stop rolling out or delete from software update policies. Only the updates that are older than the specified time period get automatically disabled or removed from the policies. This setting lets you prolong rollout of superseded updates for ring-based deployment or testing.

Table 1-1 New features *(continued)*

Feature	Description
Enhanced software usage tracking experience.	Inventory Solution simplifies software usage tracking on Windows computers. You can use usage tracking rules where you define the names and versions of the software program files that you want to track on the software product level. You can enter custom file data or use the predefined data that software inventory provides. You can use wildcards ('*') for file versions to broaden the scope of the rule. For simplified software usage tracking, no inventory of file properties is needed. Also, now you can enable tracking usage of a newly created managed software product before the inventory data for this product is gathered in your environment.
Linux OS kernel update to 4.19.69.	In Deployment Solution, kernel version has been updated to 4.19.69 in LinuxPE image.
Notification Server communication profile support in Windows preboot environment.	Deployment Solution lets you use Notification Server communication profiles to specify the following connection settings for Windows preboot environment (WinPE) to be used for connection to Notification Server: ■ TLS settings ■ Notification Server web certificates ■ Notification Server URLs ■ Proxy information ■ Credentials When you create WinPE on the **Preboot Configuration** page, under **Settings**, you can select a communication profile from the list of available Notification Server communication profiles and specify HTTP or HTTPs connection protocol. **Note:** If you edit the configured communication profile, you need to reapply the profile settings and rebuild the WinPE images on PXE server. You do not need to rebuild any automation folders for Windows.
Ability to specify or edit custom Object IDs in SNMP data mapping tables.	When you create custom SNMP data mapping tables, Inventory for Network Devices lets you benefit from new ways of specifying Object ID of the Management Information Base (MIB) data objects. In addition to using an Object ID from an available MIB as is, you can now select and edit the provided Object ID, or specify a custom Object ID.

System requirements and supported platforms

Before you install Symantec IT Management Suite 8.5 RU3, 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 RU3 involves installation of Symantec Management Platform (SMP) 8.5 RU3 and solutions using Symantec Installation Manager.

For more information on how to install and configure the product, see the *Installing the IT Management Suite solutions* chapter in the *IT Management Suite Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/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 RU3

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

- From IT Management Suite 8.5 to IT Management Suite 8.5 RU3
- From IT Management Suite 8.5 RU1 to IT Management Suite 8.5 RU3
- From IT Management Suite 8.5 RU2 to IT Management Suite 8.5 RU3

After you install this release update (8.5 RU3), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.5 RU3 for Symantec Management Platform, you need to enable upgrade policies for all plug-ins and the Symantec Management Agent to upgrade the client computers.

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 RU3, Symantec Installation Manager (SIM) automatically creates a registry backup in the support folder before starting the installation, upgrade, or release update installation of SIM and ITMS solutions. The registry backup is available at the following location:

`<installation_path>\Altiris\Symantec Installation Manager\Support`

If you encounter any errors because of missing registry entries or corrupted registry file, you can do one of the following:

- Restore the previous registry entries, and then run the installation or upgrade. To restore the previous registry entries, navigate to the registry backup, and then double-click the `AIMRoot.reg` file.
- Uninstall a solution, and then reinstall it, so that the registry entries are recreated. When you encounter the same error, repair the solution using SIM.
  For more information, see the following knowledge base article:
  http://www.symantec.com/docs/TECH183086

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

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

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

After you upgrade IT Management Suite 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.	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.
Step 4	Upgrade solution-specific agents and plug-ins to the latest version.	Perform this step after you have already turned on the upgrade policies for the Symantec Management Agent and 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.

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

Symantec recommends that you configure a schedule for the upgrade policies.

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.

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 RU3 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.5 RU3

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.5.5032	8.5.5017
Altiris Client Task Agent	8.5.5032	8.5.5017
Altiris Client Task Server Agent	8.5.5030	N/A
Altiris Pluggable Protocols Architecture Agent	8.5.4215	N/A
Inventory Agent	8.5.5013	8.5.5013
Application Metering Agent	8.5.5013	8.5.3041 (Mac only)
Server Inventory Agent	8.5.5013	8.5.3687
Inventory Rule Agent	8.5.5032	8.5.5017
Monitor Plug-in	8.5.5009	8.5.5009
Package Server	8.5.5032	8.5.5017
Power Scheme Task Plug-in	8.5.3006	N/A
Software Update Plug-in	8.5.5009	8.5.3049
Software Management Framework Agent	8.5.5032	8.5.5017
Software Management Solution Agent	8.5.5007	8.5.5007
Virtual Machine Management Task Handler	8.5.5008	N/A
Deployment Task Server Handler	8.5.5077	N/A
Deployment Package Server	8.5.5077	N/A
Deployment Plug-in for Windows (x64/x86)	8.5.5077	N/A

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.5 RU3 *(continued)*

Agent or plug-in	Windows	UNIX/Linux/Mac
Deployment Plug-in for Linux (x64)	N/A	8.5.5077
Deployment Plug-in for Linux (x86)	N/A	8.5.5077
Deployment Plug-in for Mac	N/A	8.5.5077
Deployment NBS plug-in	8.5.5077	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 RU3:

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 RU3	Yes	Yes	Yes
Upgrade from 8.5 RU1 to 8.5 RU3	Yes	No	Yes
Upgrade from 8.5 RU2 to 8.5 RU3	Yes	No	Yes

Post installation tasks for Deployment Solution

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

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

To recreate the automation folders

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

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

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

   - PEInstall_x86

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

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

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

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

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

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

To deploy the automation folders on the Windows client computers

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

To deploy the automation folders on the Linux client computers

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

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 RU3. 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 RU3 contains fixed issues for the following solutions and components:

- Symantec Management Platform
  See “Symantec Management Platform Fixed Issues” on page 17.
- Inventory Solution
  See “Inventory Solution Fixed Issues” on page 19.

- Software Management Solution
  See "Software Management Solution Fixed Issues" on page 19.
- Patch Management Solution
  See "Patch Management Solution Fixed Issues" on page 20.
- Deployment Solution
  See "Deployment Solution Fixed Issues" on page 21.
- Asset Management Solution
  See "Asset Management Solution Fixed Issues" on page 22.
- CMDB Solution
  See "CMDB Solution Fixed Issues" on page 23.
- Monitor Solution
  See "Monitor Solution Fixed Issues" on page 23.
- Workflow Solution
  See "Workflow Solution Fixed Issues" on page 23.

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 19.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
Adding computers to a filter using a CSV file fails if the user does not belong to **Symantec Administrators** security role.	TECH254500
Repeat settings of a shared schedule are saved incorrectly. If you set **Monthly**, **The Last**, and **Wednesday**, the saved schedule has **First**, or **Third** instead of **Last**.	TECH254985
A task runs everyday even if you set the task to run on a shared schedule weekly on specific days.	N/A

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

Issue	Article link
The Altiris Service stops working during check for updates if proxy is configured and proxy authentication fails.	N/A
After upgrade to 8.5 RU2, the following right-click menu options are not available for users that are not part of the **Symantec Administrators** and **Symantec Supervisors** roles: ■ Delete computers ■ Edit location	TECH254681
After upgrade to 8.5 RU2, the **Edit configuration item** page loads slowly.	N/A
After upgrade to 8.5 RU2, all user roles are unable to add a new rule to an existing policy target.	N/A
After you edit a software update policy on the parent Notification Server, and then replicate the policy to the child Notification Server, the following issues occur: ■ The state of update packages from the replicated policy becomes **Not ready**. ■ The packages are re-downloaded from the parent Notification Server.	N/A
When you install the 8.5 MSI file representing the Administrator SDK (ASDK) COM components on remote computers, the installation command fails with errors.	N/A
IIS and Notification Server application pool stop working after you click **Advanced** on the **Targeted Agent Settings** page.	N/A
Import of computers from Microsoft Active Directory fails due to mishandling of one or more characters in the generated XML.	TECH256585
Notification Server replication and event processing constantly update same SQL resources and cause poor performance.	N/A
When you click **Replicate Now** to replicate some data (eg., a folder or an item) from the parent Notification Server to the child Notification Server, the replication fails and the following error appears in the log: "The local credential username could not connect to the local server."	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
When a user initiates a task in Endpoint Management Workspaces, reports do not display the correct user who has run the task.	N/A
Tokens do not work in HTML mode in the body of the **End User Notification Task**.	N/A

Table 1-7 Fixed issues for Symantec Management Agent

Issue	Article link
In certain cases, peer computers fail to download a package from a peer that has downloaded this package and marked it as available.	N/A
Symantec Management Agent does not use % bandwidth throttling if threshold is not set.	N/A
Symantec Management Agent stops working on Site Servers and leaves the Site Servers in the stopped state.	N/A
Symantec Management Agent takes long time to load to start functioning properly.	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 1-8 Fixed issues for Inventory Solution

Issue	Article link
The **Underutilized Software** report displays incorrect data if you configure the report to show all software and filter the results by application name.	N/A

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 1-9 Fixed issues for Software Management Solution

Issue	Article link
The vendor name **Microsoft** changes if you add an Active Directory user that has **MS** in the **Company** properties.	N/A
The stored procedure **spSWP_GetCategoryGuidsPerUserPublishedSoftwares** increases the loading time of the Software Portal.	N/A
After upgrade, the ASDK method **SetPackageSource** with the **PackageSourceType** value set to **5** (Library) does not work.	N/A

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

Issue	Article link
A Managed Delivery Policy fails to keep the configured service packs order after you do the following: Create a Managed Delivery Policy to deliver a software resource with service packs, configure the service packs order, and then save the policy.	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 1-10 Fixed 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.	N/A
If you have limited visibility on resources scope, the following Windows patch management reports display incorrect data after you open a report, click the **Computer** parameter, change an organizational view, and then run the report: ■ **Compliance by Bulletin** ■ **Compliance by Update** ■ **Compliance by Computer** ■ **Missing Software Update Plug-In**	N/A
The **Windows Compliance by Update** report displays incorrect data under **Applicable(Count)** and **Install(Count)** after you open the report, click the **Filtered by** parameter, select only one computer, and then run the report.	N/A
Software updates that are configured to install with a default schedule fail to install on client computers if the computers receive a **Software Update Plug-in Policy** without any defined schedule. Such a policy can be created using Patch Management Workflow Web Service.	N/A
The date value is inconsistent in the following reports: ■ **Linux Software Update Delivery Summary** ■ **Linux Software Update Delivery - Details** that opens when you drill down on any line in the **Linux Software Update Delivery Summary** report	N/A

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

Issue	Article link
When you drill down on a client computer in the Linux patch management **Compliance by Computer** report, the drill-down report displays different count of **Applicable** and **Installed** updates. The issue occurs if the update belongs to several errata or announcements.	N/A
The Linux patch management report **Compliance by Computer** times out in the Symantec Management Console, and later the report times out when you try to run it via SQL studio.	N/A
After the rule **Patch Management Import Data Replication for Windows** replicates the data from the parent Notification Server (NS) to child NS's, child NS's recreate all updates and can cause system overload. The issue occurs if the option **Automatically revise software update policies after importing patch data** is not enabled on the parent NS.	TECH251651

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
In some cases, after import of OS files, two separate GUID folders are created on the Notification Server computer, in the **SOI** folder. One folder contains the Source > OEM subfolders. The other folder contains the rest of the Windows files.	TECH250575
Sometimes the SBS Server service attempts to stop unexpectedly. While attempting to stop, the service ceases to respond.	TECH256690
The PECTAgent version 8.5 RU2 fails to run properly when you run it from an ISO image or a USB flash drive.	TECH256689
In larger environments, the Deployment Plug-in and Symantec boot services can cause unnecessary traffic while gathering the plug-in information on client computers through the TCP port 415, and then sending the data to Notification Server.	N/A
If you use a proxy server in your environment, the call to get a resource GUID for a Windows or Linux computer can fail with the error message: "The get package settings request XML is invalid."	N/A
In some cases when you deploy an image, the deployment task fails when DeployAnywhere generates Unattend_DeployAnywhere.xml.	TECH256691

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

Issue	Article link
In 8.5 RU2, the Notification Server creates a duplicate record of a managed client computer if **DSUniqueID** cannot be read from the hard drive after booting to automation from production.	N/A
In some cases after migration or backup, iPXE fails to build proper request if Symantec Management Agent has multiple server records stored in registry.	N/A
The PECTAgent version 8.5 RU2 stops running or fails to detect whether a computer is unknown or predefined after you do the following: Turn off Symantec Management Agent on a client computer, delete the computer from the Symantec Management Console, and then boot to automation.	TECH255082
In 8.5 RU2, the Notification Server creates a duplicate computer record after using **Scripted OS Install** task or deploying an image with no Symantec Management Agent installed.	TECH251140
When you configure the **Deploy Image** task and select for deployment the Windows OS images imported in French and English OS, Windows 10 OS product keys are missing from the drop-down menu in the French and English Symantec Management Console.	N/A
After you import WinPE on the parent Notification Server (NS) only, and then run the **Replication** schedule, the following issue occur: Child NS client computers receive the replicated WinPE **Deployment Automation folder-Install** policy, and the policy stops responding in the running state.	N/A
Driver Database Management fails to correctly import all the drivers that the Driver Package Installer (DPInst) requires for installation of Intel Video Drivers.	N/A
When you create a copy file task, the task does not create a package on the package server until the package server configuration gets updated. As a result of such a package creation delay, the task fails immediately on client computers in Windows preboot environments if the associated package is not yet ready on the package server.	TECH255904
Unstable performance of the tasks that handle personality packages (PCT packages).	N/A
Complex drivers where an .inf file points to some other .inf file are incorrectly imported into the DeployAnywhere database.	DOC11601

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 1-12 Fixed issues for Asset Management Solution

Issue	Article link
When you create new editable association type, configure the **Enable Editing From** option, save the changes, and then reload the configuration item association type page, your picker selection is saved and displayed incorrectly.	N/A
When you configure the options **Users Company** or **Users Department**, the picker takes about 50 seconds to run.	N/A
When you run the **All Contracts** report and select the contract type **Contract**, the report displays all contract types.	N/A

CMDB Solution Fixed Issues

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

Table 1-13 Fixed issues for CMDB Solution

Issue	Article link
When you double-click a data class change on the **Resource Change History** page, under **Data Class History**, you cannot view the detailed information about the change on a separate page.	N/A

Monitor 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 Monitor Solution

Issue	Article link
After you import an exported monitor policies folder with some nested folders to the target Notification Server, the folder loses its parent-to-child folder association, and you cannot view the imported policies in the tree view.	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 1-15 Fixed issues for Workflow Solution

Issue	Article link
Generated LDAP/AD components correctly retrieve content for attributes with the **String** type only.	TECH254679
Active Directory synchronization works incorrectly for Active Directory sync profiles that have organizational units selected for synchronization.	TECH253583
In the Process Manager portal, the knowledge base search does not respect group permissions.	N/A
The **Document** page displays incorrectly when you click the attached document on the **Process View Page**.	N/A
Uninstalling a Workflow Server removes the entire Workflow folder with its contents. As a result, Workflow Solution files, projects and other possible custom data can be removed.	N/A
Scroll bars appear in feeder and incident forms because of an extra space on the top of the forms.	N/A

Known Issues

Note: This document includes only the issues that were found within the IT Management Suite version 8.5 RU3 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 RU3 contains known issues for the following solutions and components:

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

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:

- UNIX/Linux/Mac
  See Table 1-16 on page 25.

Table 1-16 Known issues for UNIX/Linux/Mac

Issue	Article link
The **Prevent Downloads** functionality of the **Targeted Site Settings** policy does not work in CEM mode.	N/A

Patch Management Solution Known Issues

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

Table 1-17 Known issues for Patch Management Solution

Issue	Article link
Newly initiated Microsoft Office 365 update process may fail in the following scenario: ■ The data blocks that the Office updater service (ClickToRunSvc) requires are not available on peers of the Symantec Management Agent and are only available on the Notification Server or Package Server in other site. ■ You have configured the targeted site settings policy to limit the number of outbound data transfers from a site to which the Symantec Management Agent belongs. ■ The number of outbound connections has exceeded the limit configured in the other site. The update installation process is as follows: 1 Click to Run performs 3 connection attempts in less than a minute, and then update installation fails. 2 Click to Run repeats update installation attempts 3 times with 1h intervals. 3 If the data blocks are still not accessible, Click to Run performs new update installation attempt only after the Symantec Management Agent restarts or a software update policy changes. **Remediation:** ■ Ensure that your sites have own site servers assigned so that download of the required data blocks occurs within site boundaries. ■ Increase limit of simultaneous data transfers between sites to match your actual usage pattern.	DOC9673
The **Windows Software Update Installation** task does not work on the Windows client computers that have the software update plug-in version older than 8.5 RU3.	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
Scripted OS Install task fails for Windows 7/2008r2 if the computer is booted with WinPE 10 1809 or newer version.	N/A

Where to get more information

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

Table 1-19 Documentation resources

Document	Description	Location
■ Release Notes ■ User Guides	■ Information about new features and important issues. ■ Information about how to use this product, including detailed technical information and instructions for performing common tasks.	IT Management Suite (ITMS) 8.5 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 1-20 Symantec product information resources

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

Table 1-20 Symantec product information resources *(continued)*

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