Symantec™ Client Management Suite 8.5 Release Notes

Symantec™ Client Management Suite 8.5 Release Notes

Legal Notice

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

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.

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:

www.symantec.com/business/support/

Client Management Suite

This document includes the following topics:

- About Client Management Suite
- Components of Client Management Suite 8.5
- What's new in this release
- System requirements and supported platforms
- General installation and upgrade information
- Fixed Issues
- Known Issues
- Other things to know about Client Management Suite 8.5 solutions and components:
- Where to get more information

About Client Management Suite

Client Management Suite combines the tools that help you deploy, manage, secure, and troubleshoot your desktop and laptop client computers.

Client Management Suite is a collection of solutions that run on the Symantec Management Platform. The platform and solutions of the Client Management Suite provide the following key features:

- Discovery and inventory

  The suite lets you gather inventory of all hardware and software on your client computers.
- Imaging and deployment

  The suite lets you deploy standardized and hardware-independent images on your client computers.

- Software distribution and patch management

  The suite lets you control the software configurations of your client computers. The automated policies for software and patch management help you distribute the latest software and operating system updates. You can ensure that the required software remains installed, is in a working state, and is correctly configured on the client computers.
- Remote Management

See "Components of Client Management Suite 8.5" on page 5.

See "Where to get more information" on page 83.

Components of Client Management Suite 8.5

Client Management Suite is a collection of solutions that run on the Symantec Management Platform. The following table lists all the solutions in Client Management Suite.

See "About Client Management Suite" on page 4.

Table 1-1 Components of Client Management Suite

Component	Link to User Guide
Symantec Management Platform	DOC11091
Deployment Solution	DOC11083
Inventory Solution	DOC11109
Inventory for Network Devices	DOC11110
IT Analytics	■ Client Server Management Pack for ITA DOC11099 ■ ServiceDesk Pack for ITA DOC11167
Patch Management Solution	■ Patch Management Solution for Linux: DOC11111 ■ Patch Management Solution for Mac: DOC11112 ■ Patch Management Solution for Windows: DOC11113
Real-Time System Manager	DOC11105
Software Management Solution	DOC11114
Symantec Workflow Solution	DOC11087

What's new in this release

In Client Management Suite 8.5, new features for the following solutions and components are introduced:

- Symantec Management Platform
  See "What's new in Symantec Management Platform" on page 6.
- Deployment Solution
  See "What's new in Deployment Solution" on page 14.
- Inventory Solution
  See "What's new in Inventory Solution" on page 15.
- IT Management Suite integrations
  See "What's new in IT Management Suite integrations" on page 17.
- IT Management Suite Views
  See "What's new in ITMS Management Views" on page 18.
- Patch Management Solution
  See "What's new in Patch Management Solution" on page 18.
- Software Management Solution
  See "What's new in Software Management Solution" on page 20.
- Symantec Endpoint Management Workspaces
  See "What's new in Symantec Endpoint Management Workspaces" on page 24.
- Workflow Solution
  See "What's new in Workflow Solution" on page 25.

What's new in Symantec Management Platform

In the Symantec Management Platform 8.5, the following new features are introduced.

Note that the list also includes features that have been introduced in Symantec Management Platform 8.1 release updates (RU).

Table 1-2 Time Critical Management

Feature	Description
Time Critical Management portal	The **Time Critical Management** portal lets you gather inventory on endpoints in real time so that you can perform immediate hardware and software state analysis. You can also perform various actions on endpoints in real time. About Time Critical Management

Table 1-2 Time Critical Management *(continued)*

Feature	Description
Symantec Management Agent can use persistent connection to communicate with Notification Server and site servers.	Persistent connection enables real time data transfer from and to Symantec Management Agent and lets you perform tasks on client computers in real time. Real time communication is also possible with the agents that are connected to Notification Server over CEM. About persistent connection
Pushing policies to client computers in real time.	In addition to real time tasks that you can perform in **Time Critical Management** portal, you can push policies to client computers in real time in the Symantec Management Console. Pushing a policy in real time

Table 1-3 List of new features

Feature	Description
Expanded list of supported platforms for CMDB.	The following version of Microsoft SQL Server are now supported for the Configuration Management Database (CMDB): ■ SQL Server 2016 SP1 ■ SQL Server 2016 SP2 **Note:** The following versions of Microsoft SQL Server are no longer supported for CMDB: SQL Server 2008 (SP2, SP3) and SQL Server 2008 R2 (SP1, SP2, SP3).

Table 1-3 List of new features *(continued)*

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: ■ Ubuntu (versions (14.04 LTS Trusty Tahr, 16.04 LTS Xenial Xerus and 17.04 Zesty Zapus) http://www.symantec.com/docs/HOWTO127014 ■ Windows 10 Creators Update (version 1703) http://www.symantec.com/docs/HOWTO127016 ■ Windows 10 Fall Creators Update http://www.symantec.com/docs/HOWTO127802 ■ Windows 10 April 2018 Update http://www.symantec.com/docs/HOWTO128230 ■ Windows Server 2016 http://www.symantec.com/docs/HOWTO125454 ■ SUSE Linux Enterprise Server 12 SP2 and SUSE Linux Enterprise Desktop 12 SP2 http://www.symantec.com/docs/HOWTO127018 ■ SUSE Linux Enterprise Server 12 SP3 and SUSE Linux Enterprise Desktop 12 SP3 http://www.symantec.com/docs/HOWTO127910 ■ Red Hat Enterprise Linux 6.9 and CentOS 6.9 http://www.symantec.com/docs/DOC10575 ■ Red Hat Enterprise Linux 7.3 and CentOS 7.3 http://www.symantec.com/docs/HOWTO127035 ■ Red Hat Enterprise Linux 7.4 and CentOS 7.4 http://www.symantec.com/docs/HOWTO127907 ■ macOS High Sierra 10.13 http://www.symantec.com/docs/HOWTO127741 More information: Symantec IT Management Suite Platform Support Matrix
Expanded list of supported platforms for site servers.	Task service and package service are now supported on: ■ Windows 10 Creators Update (version 1703) ■ Windows 10 Fall Creators Update (version 1709) ■ Windows 10 April 2018 Update (version 1803) All site services are now supported on: ■ Windows Server 2016

Table 1-3 List of new features *(continued)*

Feature	Description
ITMS binaries for Mac are converted to 64-bit.	The Symantec Management Agent for Mac and all plug-ins for Mac are converted to 64-bit binaries. 64-bit transition on macOS
Enhancements of Internet gateway	The following enhancements of Internet gateway are introduced: ■ Internet gateway supports WebSocket protocol, allowing to perform real time management tasks on Cloud-enabled agents. ■ One instance now supports 15,000 concurrent client connections. ■ Dependency on Apache HTTP Server and OpenSSL has been removed. ■ Internet gateway can report to multiple Notification Servers. For more information, see the following knowledge base article: https://www.symantec.com/docs/DOC11227
New features and enhancements in SIM.	The following new features and enhancements are available in SIM: ■ Symantec Installation Manager now shows the installed products from all defined product listings. You can manage the products that belong to currently selected product listing. ■ You can now edit the credentials of the AppIdentity account in Symantec Installation Manager in case the access to Symantec Management Console is not possible due to lockout or expiration of AppIdentity. ■ To make the actual validity period of applied licenses more visible, it is no longer possible to apply the licenses that will be valid in the future. ■ A new **Recover NS Settings** option is displayed on the **Configure Notification Server** page when the **NsConfiguration** key is missing in the registry at: HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\AIM\Configuration This option lets you recover Notification Server settings and Configuration Management Database (CMDB) settings without fully reconfiguring your products.
Integrated page for managing certificates.	The **Certificate Management** page combines both existing capabilities, like replacement of Site Server certificates, and new capabilities like: ■ Renewal of CEM agent certificates ■ Replacement of root certificate ■ Replacement of website certificates ■ Viewing and managing communication profile certificates

Table 1-3 List of new features *(continued)*

Feature	Description
(Windows only) Ability to apply a Cloud-enabled Management offline package to multiple organizational groups.	During the creation of the Cloud-enabled Management offline package, you can select multiple organizational groups to which you want to apply the package.
Task Server communication profile.	A Task Server communication profile lets you configure how Task Server communicates with Notification Server. Configuring a Task Server communication profile
New reports added to ITMS providing better visibility over various management aspects.	The following reports are now available in the Symantec Management Console: ■ The **Agent Connection Status** report displays the list of all managed client computers and their connection status. In this report, you can check if an agent is ready to use cloud-enabled management and/or persistent connection. ■ The **ITMS Plug-in Status** report lists install, uninstall, and upgrade policies of all ITMS plug-ins. The report shows the status of each policy and the number of computers to which the policy is applied. The **Enable** option in the right-click menu lets you apply this policy from the report. ■ The **Subnet to Site assignments** report lists the subnets and the sites to which they are assigned. This report lets you make sure that each subnet is assigned to a site. ■ The **Packages Distribution by Download Type** report shows package information and download count across all subnets or specific subnet. Report provides a drill-down with additional information on exact source for package download along with transport used - HTTP, UNC, or P2P. ■ After initiating the replacement of **NS web site** certificate, you can use the **Computers having (or without) a Certificate** report to check how many computers have received the new certificate and how many computers are still missing it. ■ **Subnets with Affiliated Sites** and **Subnets with Affiliated Sites by Computer** provide information about the subnets.

Table 1-3 List of new features *(continued)*

Feature	Description
Enhancements in Task Management.	■ A new **Clean up Task Schedules** task lets you disable or delete the schedules that have no occurrence in the future. ■ In the advanced settings dialog box, on the **Task options** tab, the new **The task is succeeded if its return code is** option lets you override the default success return code by specifying a custom value. ■ The **Fail Job if this Task fails** option lets you fail the job if a specific sub-task or sub-job within this job fails. ■ When you schedule a task, you can now add a custom description to the task instance in the **Quick Run** section or in the **New Schedule** dialog box. ■ A new option is added to the **Restart Computer** task that lets you restart only the computers that are pending restart. ■ Added ability to export content of task-instance details into a XLS or HTML file. ■ The new **Update task settings** option allows to change **Run as** settings for a script task type. This option is only available for **Symantec Administrators** role. ■ In main task details dialogs, you can now press the **Esc** key to close the dialog.
Ability to use command line for applying Notification Server Communication Profile to a client computer.	You can now use command line to apply an Notification Server Communication Profile to the client computer. You can use the following options with `aexnsagent` command: ■ `/importprofile:<path>` - lets you specify the path to the XML file of the profile ■ `/profilepwd:<pwd>` - lets you specify the decryption password Note that you have to run the command on the client computer.
New options for configuring peer-to-peer downloading.	For peer-to-peer downloading, the following new options are available: ■ **Maximum upload bandwidth** and **Maximum download bandwidth** options replace the **Maximum bandwidth** option. The **Maximum download bandwidth** option lets you specify the throttling value for peer-to-peer downloading which is independent from general throttling value. ■ **Don't use peer-to-peer downloading** option lets you disable using the peer-to-peer downloading in certain cases. ■ The new **File block download progress on peer** option lets you configure how often a peer should notify other peers about the package download progress.

Table 1-3 List of new features *(continued)*

Feature	Description
Peer-to-peer downloading now supports Microsoft Office 365 updates.	The implemented file block downloading functionality allows storing the Office 365 update blocks on a peer computer and making them available for other peers to download using the peer-to-peer downloading feature.
A **Targeted Agent Settings** policy with initial settings.	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. For example, after a re-imaged client computer receives the **(Initial Settings)** policy with ACC, it can immediately connect to Task Server.
Symantec Management Console notifications.	The bell icon is displayed in the top right corner of the Symantec Management Console in following cases: ■ The IT Management Suite GA Product Listing changes ■ A certificate is about to expire in 60 days By default, these notifications are displayed only to **Administrator** role. The **View Console Notifications** privilege lets you configure if the notifications are displayed in the Symantec Management Console. **Note:** The notifications are informational only.
Ability to separately configure time periods for retiring and deleting the computers in CMDB.	The **Purging Maintenance** policy lets you now configure different time periods for retiring and deleting the computers in CMDB. For example, you can configure the computers to be retired when they have not reported data for 6 months and to be deleted when they have not reported data for 9 months.
UI option for managing Data Class Summary Generator to populate custom data classes.	The **Data Class Summary Generator** page in the Symantec Management Console lets you manage the **Altiris.NS.StandardItems.DataClassSummaryGenerator** class. This class lets you aggregate an extensive data set in Configuration Management Database (CMDB) into a smaller data class content. For more information, see: Creating Data Class Summary Generator
Enhancements for managing targets.	The following enhancements have been made for managing targets: ■ To avoid situations in which modifications to a re-used target impact previously created policies, you can now clone targets in the target editor. ■ New icon is added to the target selector. When the target icon has a small lock icon next to it, it indicates that the Security Role(s) to which the current account belongs to does not have enough rights for this resource target.

Table 1-3 List of new features *(continued)*

Feature	Description
(Windows only) Enhancements of package delivery.	The following enhancements are implemented in package delivery: - **Block by block downloading** Package delivery downloads all files block by block. Package delivery is aware of locally available and valid file blocks and is able to download only the missing file blocks. - **Block chain hash validation** Package delivery uses the block chain hash to validate the file integrity during the file download. Package delivery verifies each block hash as soon as it is received from the server and does not write the block if hash validation fails.
New default schedule for SQL defragmentation.	In previous releases, the **NS.SQL defragmentation schedule.{cdcd50e9-1c42-402b-921c-8ad6c9ff0d34}** task is set to run only once by default and does not repeat anymore. After upgrading to IT Management Suite 8.5, the **NS.SQL defragmentation schedule.{cdcd50e9-1c42-402b-921c-8ad6c9ff0d34}** task has a new default schedule and runs as follows: - If no custom schedule is specified, the task will run weekly **every Saturday at 12:00PM**. - If a custom schedule is specified, the task will run according to the specified schedule. You can configure the schedule for this task in Task Scheduler.
New hierarchy replication rule.	The new default hierarchy replication rule **AD import Replication** replicates data for users and computers that are imported from Active Directory. By default, this rule is disabled.
Ability to configure hierarchy replication mode.	The **Replication mode** option lets you configure what kind of data the hierarchy replication rule should replicate. 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.
Item tracking.	Item tracking feature lets you set up a function that saves a record each time when an action is performed on a specified item. Later you can view the history of all actions that are performed on this item. Configuring global settings for item tracking

Table 1-3 List of new features *(continued)*

Feature	Description
Editing core settings in Symantec Management Console.	Core settings in NS Configurator can now also be viewed and configured in the Symantec Management Console. To access the settings, in the Symantec Management Console, on the **Settings** menu, click **Notification Server > Core Settings**.
Added ability to specify language for Symantec Management Console.	You can now select a specific language that you want to use in the Symantec Management Console instead of the default browser language. **Note:** This option is available only if you have **Language Packs** installed.
The full version number of Symantec Management Platform is displayed.	The 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.
New features of ASDK.	The following enhancements are introduced in ASDK: ■ On a server side, ASDK is able to run tasks and policies over the WebSocket protocol. ASDK is extended with methods specific to Time Critical Management: **TaskManagement.ExecuteTCMTask**, **TaskManagement.GetTCMTaskStatus**, **TaskManagement.GetTCMTaskResults**, **TaskManagement.GetTCMTaskResult**, and **ResourceManagementLib.PushPolicy**. ■ **CreateResourceTarget** method can now create a target in a custom folder if the **parentFolderGuid** element with custom folder's Guid is in target's source XML. If the **parentFolderGuid** element is not in source XML, the target is created in the root target folder.

What's new in Deployment Solution

Following new features are added in this release:

Table 1-4 List of new features

Feature	Description
WinPE support for Windows 10 1703, 1709, and 1803 versions.	Deployment Solution now supports WinPE for Windows 10 1703, 1709, and 1803 versions with limitations. For more details, refer to the following article. HOWTO126076

Table 1-4 List of new features *(continued)*

Feature	Description
Driver Manager lets you upload.CAB archives	Deployment Solution lets you upload drivers as .CAB archives. The following procedure lists the steps that you must follow to add drivers to the driver database: ■ In the Symantec Management Console, navigate to Settings > Deployment > Driver Manager. ■ In the **Driver Database Management** dialog box click the **Preboot** tab or **DeployAnywhere** tab. ■ Click **Add**. For the complete procedure, refer to the following URL: http://help.symantec.com
Improved support for cab archive.	Support for drivers upload in .cab archive for Deployment Solution is improved.
Imaging support for 4K native drives.	Yyou can now create an image of a computer with 4K native drive that has GPT partition and NTFS file system and deploy it on a computer with 4K native drive. **Note:** The following scenarios are not supported: Deploying an image that is created from a 4k drive to a drive with 512 sector size. Deploying an image that is created from a drive with 512 sector size to a 4k drive.
Improved performance of Boot Disk Creator.	The performance of the Boot Disk Creator is improved by reducing the time required to add preboot drivers and other packages while creating preboot packages for WinPE 5 and WinPE 10.
Support for iPXE	Deployment Solution supports creating pre-boot configurations that can be deployed over HTTP. TECH250831
Support for Smart raw imaging	Deployment Solution supports raw imaging for RHEL 7.2 and RHEL7.4 with XFS file system. When you capture an image, all the sectors are copied along with their offset on the disk. To capture an image using the Smart raw imaging feature, use the `-isr` switch in the **Create Image** task.

What's new in Inventory Solution

In Inventory Solution 8.5, the following new features are introduced.

Note that the table also includes features that have been introduced in Inventory Solution 8.1 release updates (RU).

Table 1-5 List of new features in Inventory Solution

Feature	Description
New **Collect Time-Critical Inventory** policy.	Inventory Solution provides the **Collect Time-Critical Inventory** policy that gathers the most important hardware and software inventory data on client computers frequently during a day according to a schedule. You can also enable the policy option **Real-Time Inventory** that monitors the current software state and runs software inventory scan on client Windows computers in real time on certain events.
Ability to gather inventory data for Microsoft Application Virtualization (App-V) virtual applications and Microsoft Windows store applications.	You can now gather information about the following software: ■ Microsoft Application Virtualization (App-V) virtual applications ■ Microsoft Windows store applications
Enhanced delta inventory scan and data inconsistency detection.	Inventory Solution automatically detects the computers with data discrepancies and maintains the inventory data consistency.
Enhanced software identification process.	When Inventory Solution runs the software inventory scan on managed computers, it implements intelligent identification of software components and key program files. Now the software identification process is simplified and runs faster.
Enhanced stand-alone inventory. (Windows only)	Inventory Solution lets you run stand-alone inventory packages on Windows computers with Symantec Management Agent and Inventory Plug-in installed.
Support for SNMPv3.	With the SNMPv3 support, you can perform the following tasks on SNMPv3-enabled Cisco switches and the devices connected to them (for example, VMs, Desktops, etc.): ■ Discover the devices using Network Discovery. ■ Gather agentless inventory on the devices using Inventory for Network Devices. Note that SNMPv3 support is limited to Cisco switches only.
Inventory Solution gathers the software-based usage tracking data on Mac computers.	Inventory Solution lets you track usage of the managed software at the software product level on your managed Mac OS X 10.11 and above computers. To store the gathered usage tracking data, the new data class **Product Monthly Summary** is introduced.

What's new in IT Management Suite integrations

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

Note that the table also includes features that have been introduced in IT Management Suite 8.1 release updates (RU).

Table 1-6 New features

Feature	Description
Extended health information for the Symantec Endpoint Protection clients. (Windows and Mac only)	The IT Management Suite enables you to report on the Symantec Endpoint Protection client (SEP agent) health and start the SEP service on client computers with SEP agent installed. For more information about extended health information for the Symantec Endpoint Protection clients, see the following knowledge base article: http://www.symantec.com/docs/DOC10947
Ability to deliver the Symantec Endpoint Protection clients (SEP agents) to client computers.	Software Management Solution provides the predefined **Symantec Endpoint Protection Delivery** policy. The policy delivers a SEP installation package to Windows and Mac client computers, installs SEP agent, and makes sure it remains installed. The policy also upgrades the existing SEP agent if necessary. The **Conflicting SEP Delivery Policies** report presents the enabled **Symantec Endpoint Protection Delivery** policies that are targeted to the same computers. Running such policies may result in double installation of the SEP agent on the computers. The report lets you detect conflicting policies and resolve them to ensure that only one instance of SEP agent is installed on the computers. You can view this report in the Symantec Management Console, on the **Reports** menu, at **All Reports > Software > Delivery**. For more information about SEP management tasks, see the *Whitepaper* at the following URL: https://www.symantec.com/docs/DOC11174
Quarantine computers without required patches.	IT Management Suite (ITMS) lets you check if the computer is compliant with respect to the software updates that need to be installed on it. If patches associated with CVE-ID specified in ITMS are found not to be installed on targeted computers, such computers will be quarantined until the patches are installed. For more information about checking patch compliance and taking quarantine action on client computers, see the *Whitepaper* at the following URL: https://www.symantec.com/docs/DOC11174

Table 1-6 New features *(continued)*

Feature	Description
Automated remediation of vulnerabilities detected by Symantec Conrtol Compliance Suite Vulnerability Manager.	Use the Patch Management Solution to automatically remediate vulnerabilities detected by Symantec Control Compliance Suite Vulnerability Manager. For more information about Automated Vulnerability Remediation, see the *Whitepaper* at the following URL: https://www.symantec.com/docs/DOC11174
Automated remediation of vulnerabilities in response to service requests (Symantec Control Compliance Suite integration).	Automatically remediate vulnerabilities in response to service requests created in ticketing systems such as ServiceNow by products such as Symantec Control Compliance Suite. Currently, IT Management Suite supports remediation management for Windows clients. For more information, refer to the following article: http://www.symantec.com/docs/DOC9752

What's new in ITMS Management Views

In ITMS Management Views 8.5, the following new feature is introduced:

Table 1-7 List of new features

Feature	Description
Number of entries in the **Computers with software installed** list.	You can now view the total number of client computer entries on which a selected software product is installed. The number is shown in the bottom row of the **Computers with software installed** list.
New filter criterion is added in the **Software** view.	A new filter criterion is added for software products, software components, and software releases. The new **IsPublished** criterion filters the software depending on whether it is published to the Software Portal or not.
New folder in the **Software Filters** tree in the **Software** view.	The new **Published Software** folder contains the **Published Software Releases** filter for software releases published to the Software Portal.

What's new in Patch Management Solution

In Patch Management Solution 8.5, the following new features are introduced.

Note that the table also includes features that have been introduced in Patch Management Solution 8.1 release updates (RU).

Table 1-8 List of new features

Feature	Description
Express Updates support.	Patch Management Solution for Windows supports the Express Updates technology that is built into Windows Update service and optimizes distribution of some updates for Microsoft products by only downloading the incremental changes that each computer requires. For more information about Express Updates support, see the following knowledge base article: http://www.symantec.com/docs/DOC11127
Enhanced Windows system assessment scan and assessment data inconsistency detection. (Windows only)	Windows system assessment scan in delta mode reduces the network load by only reporting data that has changed since the last full scan. Patch Management Solution automatically ensures that the system assessment scan data known to the Notification Server is consistent with the data on each endpoint.
Ability to remove disabled bulletins from the software update policies, and then delete unused Windows and Linux packages.	When you disable software bulletins, you can also remove the software bulletins from software update policies. You can then run the **Check Software Update Package Integrity** task to automatically delete unused Windows and Linux packages. This may be helpful to free up disk space consumed by large update packages that are no longer being distributed.
Ability to distribute only selected updates for a particular software bulletin.	You can create a software update policy that downloads and distributes only selected updates for a particular software bulletin. You can edit the policy later to download additional updates in the bulletin. If you revise software update policies to download additional updates associated with a bulletin included in the policy, distribution of the newly downloaded updates will be disabled by default.
Filter for compliance reports that shows superseded updates or the software bulletins that contain superseded updates.	The **(All)** filtering option of the **Supersedence Status** parameter lets you view and distribute superseded updates or the software bulletins that contain superseded updates on the **Patch Remediation Center** page or in the following enhanced patch management compliance reports: ▪ Software Bulletin Details ▪ Compliance by Bulletin ▪ Compliance by Update ▪ Compliance by Computer ▪ Software Update Delivery Summary

Table 1-8 List of new features *(continued)*

Feature	Description
Ability to select specific Microsoft Office 365 channels for patching.	The patch management metadata release version 7.3 contains separate entries for the following Microsoft Office 365 channels enabling you to just download and distribute the updates associated with the channels required: ■ Microsoft Office Click to Run 2016 (Office 365 Deferred Channel) ■ Microsoft Office Click to Run 2016 (Office 365 Monthly Channel) ■ Microsoft Office Click to Run 2016 (Office 365 Semi-Annual Channel) ■ Microsoft Office Click to Run 2016 (Office 365 Semi-Annual Targeted Channel) For more information, see the following knowledge base article: http://www.symantec.com/docs/DOC9673
Lists of Windows and Linux policies are available on the **Patch Management** home page.	You can access the lists of software update policies for Windows and Linux that you have created on the **Patch Management** home page: ■ Windows Policies ■ SUSE Linux Policies ■ Red Hat Linux Policies ■ CentOS Linux Policies You can select a policy from the list and view the details of the policy or edit its settings if necessary on the corresponding policy page.

What's new in Software Management Solution

In Software Management Solution 8.5, the following new features are introduced.

Note that the table also includes features that have been introduced in Software Management Solution 8.1 release updates (RU).

Table 1-9 List of new features

Feature	Description
Enhanced Software Portal administration.	Software Management Solution introduces the following enhancements of the Software Portal administration: ■ The **Manage Publications** page provides a consolidated view of all software that has been published to the Software Portal. You can use this page to quickly publish additional software to the Software Portal, temporarily or permanently remove software from the portal, or edit the attributes of published items rather than performing these actions on the pages related to individual software resources or Managed Software Delivery policies. ■ You can configure access to the Software Portal from Mac client computers by using the **Software Portal Client Access Policy**. The following options are available: ■ 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. ■ You can categorize software published to the Software Portal so that end users can more quickly locate the software they require. ■ To limit end users to only being able to request software published for them in the Software Portal, you can use the new **Prevent end users from requesting unlisted software** on the **Software Portal Settings** page. ■ While publishing a software resource or a Managed Software Delivery policy to the Software Portal, the Software Portal Administrator can target devices or groups of devices for software publishing. If the administrator targets both devices (or groups of devices) and users (or groups of users) for software publishing, only the selected users on the specified devices will have permission to request the software. ■ The default number of open software requests per user is increased to 1000. Note that a Managed Software Delivery policy that contains dependencies or multiple tasks counts as one request.

Table 1-9 List of new features *(continued)*

Feature	Description
Enhanced user interface of the Software Portal. (Windows and Mac only)	Software Management Solution 8.1 RU5 has introduced the enhanced UI of the Software Portal that provides an app store-like user experience. The Software Portal Administrator can configure whether the legacy UI or the enhanced UI is displayed to the users. **Note:** After the first-time installation, the enhanced UI is enabled by default. After the upgrade from the previous version, the UI setting remains in the same state as before the upgrade. The enhanced UI has the following new features: ■ The Software Portal Administrator can customize the Software Portal header with company-branded background image. ■ 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. ■ End users can also open the Software Portal on Windows and Mac computers with Cloud-enabled Management enabled. ■ End users can only see the software that is compatible with the platform of the computer from which they launch the Software Portal. ■ In the user profile, end users can enable the option to view notifications when the requested application is installed on the user's device. ■ End users and managers can search for the applications by vendor, and version. ■ End users can filter the applications by category, type, and approval. For more information about using the enhanced user interface of the Software Portal, see the Mind Map *Making on-demand software available in the Software Portal* that is listed in the following knowledge base article: http://www.symantec.com/docs/DOC9706
Enhanced Software Discovery scan in Software Management Framework.	Speed of Software Discovery scan is improved.
Ability to perform software import and managed delivery at once.	You can create a software resource in the Software Catalog, import the associated package, and create a Managed Software Delivery policy to install the package as part of a single sequence of actions from within the Symantec Management Console or by using the Administrator Software Development Kit (ASDK). The ASDK Help can be found at `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Symantec\ASDK`

Table 1-9 List of new features *(continued)*

Feature	Description
Enhanced expressions for standard and smart rules.	■ Support for the **MSI Upgrade Code** expression is added for standard and smart rules to check the client computer for the MSI upgrade code that you specify. For example, this may help you to determine that no newer versions of a software application are installed. ■ Wildcard support is added for the **Static File Expression** and **Registry Key Exists** expressions. ■ You can specify the registry entry for the expression **Registry Key Exists**.
New results-based action setting for Managed Delivery.	Software Management Solution introduces new results-based action setting **Continue job if component is not applicable** that you can use as the default global setting for all new Managed Software Delivery policies or as an override setting for a specific software resource that a Managed Software Delivery policy contains. When you enable this setting for the policy that is set to abort upon failure, the policy continues to run if it includes some components that the applicability rules define as not applicable.
Enhanced software resource management experience	A predefined icon identifies each software resource in the Software Catalog. By default, the icon corresponds to the type of the resource: **Software Update**, **Software Component**, **Service Pack,** or **Software Release**. You can add or edit a custom icon for a software resource when you edit the software resource in the Software Catalog. When you manage the software resource in the **Software** Management view or in the Software Catalog, you can view the custom icon. When you add the software resource to a Managed Software Delivery policy, the predefined or custom icon is displayed on the policy page.
Running software delivery policies and tasks on a computer pending a restart or a logoff.	Enable software delivery policies and tasks to execute when there is a pending restart or logoff required by Managed Software Delivery policy. This functionality is not available out of the box. You can enable it manually in the registry on the required client computer. For more information about the functionality and its limitations, see the following knowledge base article: http://www.symantec.com/docs/DOC10551.

Table 1-9 List of new features *(continued)*

Feature	Description
Removal of Symantec Workspace Virtualization support	Software Management Solution 8.5 does not support the management of the Symantec Workspace Virtualization Agent (SWV Agent). The installation of Software Management Solution 8.5 will not copy SWV Agent to the Notification Server, nor will it create predefined policies to install or upgrade SWV Agent. If you upgrade from the solution version 8.0 HF6 or 8.1 RU7 to 8.5, you can use the software virtualization technology as follows: ▪ Your upgraded Managed Software Delivery policies with the enabled virtual layer option will continue to install software into virtual layer for the client computers with SWV Agent installed. ▪ Your upgraded Managed Software Delivery policies with the enabled virtual layer option will install software in a non-virtualized state for the client computers without SWV Agent installed. ▪ You will be able to create new Managed Software Delivery policies with the enabled virtual layer option. If you migrate Managed Software Delivery policies with the enabled virtual layer option from the solution version 8.0 HF6 or later to 8.5, the policies lose virtualization and install software in a non-virtualized state on the client computers. For more information about the End of Life of Symantec Workspace Virtualization and Symantec Workspace, see the following knowledge base article: https://www.symantec.com/docs/INFO4060

What's new in Symantec Endpoint Management Workspaces

In Symantec Endpoint Management Workspaces, the following new feature is introduced:

Table 1-10 List of new features

Feature	Description
Symantec Endpoint Management Workspaces console	Symantec introduces a new console with dedicated pages (workspaces) and widgets that are designed to simplify and speed up the day-to-day endpoint management jobs. With the help of the Symantec Endpoint Management Workspaces, help desk workers can respond quickly to tickets and requests. About Symantec Endpoint Management Workspaces

Table 1-10 List of new features *(continued)*

Feature	Description
Search workspace	The **Search** workspace enables users to search for resources and view inventory details for the selected resource (endpoint).
Quick Tasks workspace	The **Quick Tasks** workspace enables help desk users to deliver software and run tasks
Endpoint Management Workspaces Users role	Specifically for help desk workers, Symantec introduces a new role - **Endpoint Management Workspaces Users**. By default, the new role gives the permission to the user to perform the following actions in the Symantec Endpoint Management Workspaces: ■ Search for resources (endpoints). ■ View selected endpoint inventory and health information. ■ Use **Quick Tasks** workspace to deliver software and run tasks.

What's new in Workflow Solution

In the Workflow Solution 8.5, the following new features are introduced. Note that the table also includes features that have been introduced in Workflow Solution 8.1 release updates (RU).

Table 1-11 List of new features

Feature	Description
Added support for Aspose.Email library	A new component is added that supports all the existing functions in all the types of SSL environments. The new components are developed with the Aspose.Email library. Currently, the new components are listed with the suffix, "New" and are added in the **Process Components > Email** category of the component list. For more information, refer to the following article: DOC11187
Localized uninstaller of Process Manager and Workflow Designer	The uninstaller for **Process Manager** and **Workflow Designer** are now localized.
Improved UI of Process Manager.	The application menu and UI for **Calendar**, **Scheduler**, **Knowledge Base**, and **Documents** of the **Process Manager** of Workflow Solution are updated.

Table 1-11 List of 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
Changes in Workflow Solution	Password hint field is removed from the modify User Account page.
Added the option to insert image.	From this release, the insert image option is added to the HTML Editor toolbar, Add Article dialog FAQ, Bulletins, and Discussions.

System requirements and supported platforms

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

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

For information about the supported operating systems in Client Management Suite 8.5, see the *Symantec IT Management Suite Platform Support Matrix* at the following URL:

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

General installation and upgrade information

Installation of Client Management Suite 8.5

The installation of Client Management Suite 8.5 involves installation of Symantec Management Platform (SMP) 8.5 along with the installation of suites and their solutions using the Symantec Installation Manager.

For more information on how to install and configure the product, see the *IT Management Suite 8.5 Installation and Upgrade Guide* at the following URL:

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

Upgrade to Client Management Suite 8.5

You can upgrade from the previous versions of Client Management Suite to the latest version using Symantec Installation Manager.

The following upgrade scenarios are supported:

- From Client Management Suite 8.0 HF6 to Client Management Suite 8.5

- From Client Management Suite 8.1 RU7 to Client Management Suite 8.5

For more information on how to upgrade the product, see the *IT Management Suite 8.5 Installation and Upgrade Guide* at the following URL:

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

Migration of Symantec Management Platform and the Client Management Suite solutions

If you want to migrate from older releases where direct upgrade to the latest version is not supported, do the following:

1. Migrate from older release to Client Management Suite 7.5
2. Apply Client Management Suite 7.5 HF6
3. Upgrade to Client Management Suite 7.5 SP1
4. Apply Client Management Suite 7.5 SP1 HF5
5. Upgrade to Client Management Suite 8.0
6. Apply Client Management Suite 8.0 HF6
7. Upgrade to Client Management Suite 8.5

For detailed instructions on migrating to Client Management Suite 7.5, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.5* at the following URL:
  http://www.symantec.com/docs/DOC5668
- *IT Management Suite Migration Guide version 7.0 to 7.5* at the following URL:
  http://www.symantec.com/docs/DOC5669

For detailed instructions on upgrading from Client Management Suite 7.5 SP1 HF5 to Client Management Suite 8.0, see the following documentation resource:

- *IT Management Suite 8.0 Installation and Upgrade Guide* at the following URL:
  http://www.symantec.com/docs/DOC8650

Fixed Issues

Client Management Suite 8.5 contains fixed issues for the following solutions and components:

- Symantec Management Platform
  See “Symantec Management Platform Fixed Issues” on page 28.
- Deployment Solution
  See “Deployment Solution Fixed Issues” on page 30.
- Inventory Solution

See “Inventory Solution Fixed Issues” on page 30.

- Patch Management Solution
  See “Patch Management Solution Fixed Issues” on page 31.
- Real-Time System Manager
  See “Real-Time System Manager Fixed Issues” on page 32.
- Software Management Solution
  See “Software Management Solution Fixed Issues” on page 33.
- Workflow Solution
  See “Workflow Solution Fixed Issues” on page 33.

Note: The issues that were fixed within release updates (RU) for ITMS version 8.1 are not included in this document.

For more information about the fixes in release updates, see the following release notes:

- ITMS 8.1 RU1
- ITMS 8.1 RU2
- ITMS 8.1 RU3
- ITMS 8.1 RU4
- ITMS 8.1 RU5
- ITMS 8.1 RU6
- ITMS 8.1 RU7

Symantec Management Platform Fixed Issues

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

The fixed issues are separated into the following components:

- Notification Server
  See Table 1-12 on page 29.
- Task Server
  See Table 1-13 on page 29.
- Symantec Management Agent
  See Table 1-14 on page 29.
- ASDK
  See Table 1-15 on page 29.

- Security Cloud Connector

  See Table 1-16 on page 30.

Table 1-12 Fixed issues for Notification Server

Issue	Article Link
During the upgrade to ITMS 8.1, the custom site server certificate is replaced with the default certificate.	N/A
Site Server Communication profile does not allow to force the clients to use only one particular port for communication.	N/A

Table 1-13 Fixed issues for Task Server

Issue	Article Link
Call Web Service Task does not properly respond to the Servicedesk Incident Management Web Service.	N/A
Task client does not properly pull the exit codes from PowerShell scripts.	N/A
If you have uninstalled Task Service on your Notification Server and then perform upgrade to IT Management Suite 8.1, the Task Service gets re-installed. To restore the previous state of your Notification Server, you must uninstall the Task Service again after the upgrade.	N/A

Table 1-14 Fixed issues for Symantec Management Agent

Issue	Article Link
AppID account seems to be used to authenticate external sites. Because the AppID account cannot be used outside of the internal network, the access to the external site is denied.	N/A

Table 1-15 Fixed issues for ASDK

Issue	Article Link
When you execute the **RunReportWithParameters** method for **Software Bulletins Details** report with parameter **Software Bulletins=(All)**, the following error occurs: **"An error occured executing the report Software Bulletin Details. Value given for parameter Software Bulletins is invalid: All."**	N/A

Table 1-16 Fixed issues for Security Cloud Connector

Issue	Article Link
There is no option to configure the **Bulk Resource Export Rule** to export the resources without GUIDs.	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.

For more information about the fixes in hot fix releases, see the following release notes:

- ITMS 8.1 RU1
- ITMS 8.1 RU2
- ITMS 8.1 RU3
- ITMS 8.1 RU4
- ITMS 8.1 RU5
- ITMS 8.1 RU6
- ITMS 8.1 RU7

Table 1-17 Fixed issues for Deployment Solution

Issue	Article link
DeployAnywhere doesn't run because no active Windows drive is detected.	TECH250967
The **Use iPXE** setting is not saved after you edit a preboot configuration.	TECH251329
The AexBasicInventory.dll fails to load in WinPE automation causing the PECTAgent.exe to crash. For more information and workaround, refer to the following article: TECH211409	TECH211409
During upgrade from Deployment Solution 8.0 to 8.1, the jobs that are assigned to the **Re-deployment (Managed Computer) Menu** in the **Settings > Deployment > Initial Deployment Settings** disappear.	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 1-18 Fixed issues for Inventory Solution

Issue	Article link
If you run a standalone inventory package on a managed client computer with installed NS Agent and the inventory execution is terminated unexpectedly, the NS Agent may be left in nonfunctional state. To resolve this issue, you need to register the original NS Agent .dlls manually using the following command lines: Regsvr32 "C:\Program Files\Altiris\Altiris Agent\AeXBasicInventory.dll" Regsvr32 "C:\Program Files\Altiris\Altiris Agent\Agents\SoftwareManagement\"SMFAgent.dll" Regsvr32 "C:\Program Files\Common Files\Altiris\AeXNetComms.dll" Regsvr32 "C:\Program Files\Common Files\Altiris\ AeXNSEvent.dll"	N/A
Inventory Solution automatically detects the computers with data discrepancies and maintains the inventory data consistency. This technology fixes the following issue within one day: After you run some inventory task with delta inventory enabled on one Notification Server computer, redirect Inventory Plug-in to another Notification Server computer, and run another inventory task with delta inventory enabled along with some other types of inventory, only delta inventory data is sent.	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 1-19 Fixed issues for Patch Management Solution

Issue	Article link
A box that you uncheck on page 1 in the **Distribute Software Updates** wizard does not stay unchecked when you switch to the page 2. Workaround: In the Symantec Management Console, on the **Manage** menu, click **Policies**. Create a software update policy, configure, and then enable it.	N/A
The **Windows Computers with Software Update Plug-in** counter works only for the client computers that have the Software Update plug-in originally rolled out from the same Notification Server.	N/A

Table 1-19 Fixed issues for Patch Management Solution *(continued)*

Issue	Article link
If you change the package location from default to **Alternative Location** with custom credentials and then back to default, you will not be able to perform **Vendors and Software** update. To complete the update, you need to select **Default Location** and complete the **Vendors and Software** update. You can then switch back to the **Alternative Location**.	N/A
An issue when using FTP as patch data alternative download location. If you want to use an FTP location as the alternative download location on the **Import Patch Data** page, on the Notification Server computer, add the `C:\Program Files\Altiris\Notification Server\Bin\AeXsvc.exe` service to the firewall Exception List.	N/A
The **Software Bulletin Details** report shows the computers that are out of the scope of the current console user.	N/A
If you change the settings of the **Advertisement Set** policy, and then run the Patch Management with the **Revise** option enabled, the modified update will not be re-downloaded.	N/A
The out-of-scope client computers are displayed in the **Compliance Summary** report.	N/A
A software update policy may fail to save. This issue may occur when anonymous access is enabled for the Altiris folder in IIS.	N/A
The **SUSE/Red Hat Compliance by Update** report can show an incorrect number of computers on which updates have been installed.	N/A

Real-Time System Manager 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 1-20 Fixed issues for Real-Time System Manager

Issue	Article link
After you apply newer Windows Updates (starting from June 30, 2018 and onwards), the Keyboard-Video-Mouse (KVM) functionality does not work in TLS mode.	TECH251378

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 1-21 Fixed issues for Software Management Solution

Issue	Article link
In the Symantec Management Agent UI, the **Software Delivery** tab can display outdated information about the last run time of the managed delivery policies and their tasks that have the option **Run for each user** enabled. If you clone such a policy, and then disable the original policy, the advertisements of the both policies are displayed in the UI.	N/A
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.	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 1-22 Fixed issues for Workflow Solution

Issue	Article link
In the Workflow Process Manager **Admin Portal > Master Setting**, text is displayed in English language for other languages.	N/A
In the Workflow **Process Manager > Process Automation > Add Email Template**, text is displayed in English language for other languages.	N/A
For languages other than English, some fields on the Home page of the **Process Manager portal** appear in English.	N/A
In the Process Manager, the **View Documents** option does not open the document in the browser.	N/A
You cannot drag and drop a Model from the project sub-window to create a linked Model.	N/A
The **Auto Start** project runs every 15 seconds in the debugger.	N/A
Libraries tab in the **Project Properties** does not reflect the correct library information.	N/A

Table 1-22 Fixed issues for Workflow Solution *(continued)*

Issue	Article link
When you process reports over a period of time that includes SLA data AND Incident or Process Data, incorrect result count is displayed.	N/A
You cannot select classification past Files & Directories.	N/A
When the Start date and End date of the Date Range are same, the report displays no results.	N/A
In report, based on SQL with parameters modifying DateTime parameters requires mm/dd/yyyy format instead of the parameter defined in the OS/browser and detected by Process Manager Portal.	N/A
The Reports Group by does not run properly if the data contains blank string and null values.	N/A
Workflow project installer does not properly replace the project when the project is already published with a different name.	N/A
In the Project Properties page, the `Ctrl+C` copies the data of the entire row.	N/A
Dropdown list displays an exception when you reload the page after a duplicate item is selected.	N/A
You cannot translate the component called Grid, Class: Logicbase.Components.FormBuilder.InfragisticsComponents.WebGrid.GridComponent.	N/A
In a project, the Script Generator (C#) components with multiple output paths does not generate the output variable value.	N/A
The emails that are sent from automation are sent using a UTF-16 encoding and conflicts with mobile device requirements for viewing email.	N/A
Secure attribute is not set on Process Manager login cookie.	N/A
Radial gauge defaults to middle when the value is configured with Dynamic Model after the page postback.	N/A
The **Digital gauge** component disappears after page postback.	N/A
The Process Action "Send Email" does not let you att any attachments.	N/A
In an Incident Email template, the description does not include line breaks.	N/A
In Workflow Designer, the initial creation of a Rectangle component does not allow resizing.	N/A
SEP Workflow Components are unable to connect to a SEP 14 Server.	N/A

Table 1-22 Fixed issues for Workflow Solution *(continued)*

Issue	Article link
In Workflow Designer, an error is displayed if you select a component empty configuration field and then choose to change the field.	N/A
The Line and the Point graphs in the Report Viewer do not show the definition for the value.	N/A
The time zone settings are incorrectly saved when you manually set the time zones for UTC and Eastern time.	N/A
You cannot expand the Process lists on specific pages when you use a Configured Server Alias to access Servicedesk.	N/A
The Group selection of the **Send Email** action is not alphabetically sorted.	N/A
Cannot upload screen captured with the Screen Capture Utility as it uses the localhost path instead of workflow host.	N/A
The Set SLA Component does not work with any of the following Start Date variables: ▪ UseProcessStart ▪ UseCurrentDate	N/A
A validation error is displayed when you use the Dynamic Model as source for Grid element with DropBox.	N/A
The WebChart component does not show data from the Process Variables or the Dynamic Model.	N/A
When you save a Knowledge Base article that includes images, error is displayed in the logs.	N/A
After you send an email, the window does not close automatically.	N/A
For Latin language, when you access links for certain projects in the ProcessManager Portal, an error is displayed.	N/A
If the email address is longer than 36 characters, the SLA is created with email address instead of the User GUIDs.	N/A
An error is displayed when you use a variable to represent date/time or if you use a dynamic model to generate a variable for date time in either the PauseSLA or CompleteSLA components.	N/A
The Grid component is not visible in the debug session when the **AngularJS** option is selected for the project and the component.	N/A

Table 1-22 Fixed issues for Workflow Solution *(continued)*

Issue	Article link
When the Angular JS Grid component is configured for the **Select Items** menu, you can edit the data in the cells.	N/A
The Report scheduling module only sends emails of the scheduled reports from the Admin@symantec.com account.	N/A
If the email address is longer than 36 characters, the SLA Status Update that marks the SLA as Late is populating the Audithistory.ModifiedBy column with the system Administrator email account, instead of the user GUID.	N/A
In Google Chrome and Mozilla Firefox, when you terminate the Form Builder component it also attempts to close the browser window.	N/A
When you export reports with Date Values, the .xlsx report is does not display the time data.	N/A
Incorrect date and time is used and an error is generated by LogicBase.Ensemble.WorkflowTasks.TaskResponsePage, TaskResponsePage.Aspx.cs.	N/A
Text is not displayed correctly on the Process View Page when you use the > symbol.	N/A
The component **Send Email with SSL over SMTP** does not work.	N/A
The following Value Datatypes that are configured as input parameters do not pass through default values configured in Debug to published web services: ■ Number - integer ■ Number - Decimal	N/A
The **Set SLA > For Milestone by Process Priority** rule action does not work with extended Incident data type.	N/A
Explicit permissions for Knowledge Base articles generate an error when accessing the Article Category.	N/A
If you search for a user by Last Name, no results are displayed if the Last Name is unique.	N/A
The Datetime.Kind error is displayed in three different instances.	N/A
The manually set time zone are not correctly saved for Central American and Canada users.	N/A
An error is displayed when you try to connect to a SMP resource and save the data after clearing the rows of the multi-row data class.	N/A
In Servicedesk Process View Pages does not auto-refresh after any change.	N/A

Table 1-22 Fixed issues for Workflow Solution *(continued)*

Issue	Article link
The Process History Webparts on the Process View Page display the date/time entries such that the date and time run together	N/A
If you upgrade from version 8.1.6030.2 point fix to 8.1 RU7 it does not replace the Logicbase*.DLL files found in the \Program Files\Symantec\Workflow\ProcessManager\bin	N/A

Known Issues

Client Management Suite 8.5 contains fixed issues for the following solutions and components:

- Symantec Management Platform
  See “Symantec Management Platform Known Issues” on page 38.
- Deployment Solution
  See “Deployment Solution Known Issues” on page 49.
- Inventory Solution
  See “Inventory Solution Known Issues” on page 50.
- IT Analytics
  See “IT Analytics Solution Known Issues” on page 53.
- IT Management Suite integrations
  See “Known issues of IT Management Suite integrations” on page 54.
- IT Management Suite Views
  See “ITMS Management Views Known Issues” on page 54.
- Patch Management Solution
  See “Patch Management Solution Known Issues” on page 55.
- Real-Time System Manager
  See “Real-Time System Manager Known Issues” on page 62.
- Software Management Solution
  See “Software Management Solution Known Issues” on page 66.
- Symantec Endpoint Management Workspaces
  See “Symantec Endpoint Management Workspaces Known Issues” on page 73.
- Workflow Solution
  See “Workflow Solution Known Issues” on page 74.

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 separated into the following components:

- Symantec Installation Manager
  See Table 1-23 on page 38.
- Notification Server
  See Table 1-24 on page 39.
- Task server
  See Table 1-25 on page 40.
- Symantec Management Agent
  See Table 1-26 on page 44.
- UNIX/Linux/Mac
  See Table 1-27 on page 46.
- Network Discovery
  See Table 1-28 on page 47.
- Pluggable Protocol Architecture (PPA)
  See Table 1-29 on page 48.
- ASDK
  See Table 1-30 on page 49.
- Security Cloud Connector
  See Table 1-31 on page 49.

Table 1-23 Known issues in Symantec Installation Manager

Issue	Article link
During the IT Management Suite upgrade from 8.1 RU7 to 8.5, SIM may display the following error message: "**UHS port 8080 is used by another application. Specify unused open port.**". At the same time, SIM does not allow to specify another port and the upgrade cannot proceed. **Workaround:** Before the upgrade, manually set **SOFTWARE\Altiris\UHSPort\Port** to **8080** or any other unused port that you want to set for UHS help.	N/A
Applying the services or features that the ITMS Installation Readiness Check requires might fail on Microsoft Windows 2012 R2 server.	TECH248455

Table 1-24 Known issues for Notification Server

Issue	Article link
The **Push Policy** feature assumes that all endpoints are able to receive the policy. For example, it does not check if the endpoints have the required plug-ins installed or if the license count is sufficient. In this situation, the Push Policy message can display an incorrect number of endpoints to which the policy is delivered.	N/A
On the **Domain Membership/WINS Import** page, it is not possible to find any domain in the network using **Browse** and not possible to add known domains. This issue occurs only when SMBv1 is disabled on your Notification Server.	N/A
The upgrade to the latest version of ITMS fails if you configure the IIS settings for the Default Web Site and enable HTTP redirection feature using your Notification Server hostname.	N/A
Setting the value of **VisiblePkgFiles** setting in **CoreSettings** to true and initiating package distribution points update removes the **Hidden** attribute from the files or folders inside the imported packages.	N/A
If you migrate the Configuration Management Database (CMDB) to a different server and then migrate other data with the Migration Wizard, some full licenses that were previously applied are not restored in the new Symantec Management Platform installation. Those are reverted to the trial or the extended trial licenses.	N/A

The aexconfig fails to reset service account if the password contains a ^ character, like in the following example:
`AeXConfig.exe /svcid user:altiris\SRVC_AeXNS_Dev password:pass^w"ord`
`AeXConfig.exe /svcid user:altiris\SRVC_AeXNS_Dev "password:pass^w"ord"`
	N/A

If package server is installed on a computer with host name that contains double byte or HIASCII characters, packages cannot be downloaded.	N/A
If you open the **Task Instance Details** window on a parent Notification Server, to check the details of a replicated task, the **Close** option does not let you close this window. This problem occurs because the **Task Instance Details** window is identified as in the Internet zone instead of in the Local intranet zone and the functions of the **Close** option are prevented. To avoid this issue, add the URL of child Notification Server to the list of trusted sites. For more information, read the Microsoft knowledge base article 303650. **Workaround:** Use the **X** symbol in the upper right corner of the window, to close the **Task Instance Details** window.	N/A

Table 1-24 Known issues for Notification Server *(continued)*

Issue	Article link
Occasionally the **www publishing** service `w3wp.exe` process causes very high CPU and Memory usage. It can cause the computer to stop responding. It is a problem on low-end Windows servers with single core processors. To work around this issue, restart the **www publishing** service.	TECH176493
If you have a hierarchy of Notification Servers, some reports display summary data for each Notification Server. These reports let you drill down into the results. To drill down you click the appropriate row in the results grid for detailed data about a particular Notification Server. However, if a Notification Server is installed to a non-default website and port, its summary data is displayed correctly in the summary report. Any attempt to drill down to display the detailed data fails. A new browser window opens to display the report results, but it contains a Server Error message saying that the resource cannot be found.	N/A
If the Symantec Management Console is set up to use a non-default port, you may see an exception error in the following situation: you try to add computers on the **Agent Push** page of the console by using the FQDN (non-localhost). The following error message is displayed: Data for the page you are currently viewing has expired. **Workaround:** Use the appropriate IP address in the console URL rather than using the FQDN.	N/A

Table 1-25 Known issues for Task Server

Issue	Article link
If before the off-box upgrade to 8.5, you have **Advanced Task Server Settings** enabled and **Alternate URL** specified for the Task Server to access the Notification Server, then after the upgrade a **Task Server Communication Profile** is created. However, this communication profile contains the host name that was used to connect to the old Notification Server. As a result, the Task Servers to which this communication profile is applied try to register on the old Notification Server. **Workaround:** After the off-box upgrade, go to **Task Server Communication Profile** and remove the **communication hosts** values that refer to old Notification Server.	N/A
In some situations, the child process of a Client Script Task may remain in running state, although the parent process is already closed.	N/A

Table 1-25 Known issues for Task Server *(continued)*

Issue	Article link
During the upgrade to ITMS 8.5, the following error may appear in the logs: "**Task execution engine failed Could not find stored procedure 'CtsGetMerges'.**" Note that this warning does not cause any functional problems.	N/A
Task Server notifies client computer if a new task is available for it. If there are too many of such notifications, the Symantec Endpoint Protection (SEP) might treat these notifications as port scan attack and block connections from Task Server for 10 minutes. **Workaround:** In SEP, add an allow rule for Task Server so that the SEP does not trigger.	N/A
Starting from ITMS 8.1, **Anonymous Authentication** is disabled for the **ClientTaskServer** website. That may lead to situation where client computer is not able to access Task Server. For example, if Notification Server and Task Server are in domain and configured under the domain user and the client computer is not in domain. You may need to set up the **Agent Connectivity Credentials** to let the client computers access the **ClientTaskServer** website.	N/A
You cannot install or upgrade Task Server if supported version of .NET Framework is not installed on the computer. One of the .NET Framework versions from 4.5.1 to 4.7 must be installed on the task server computer. Also, note that Windows XP, 2003 Server, and Windows Vista operating systems are not supported for the Task Server install in 8.5.	N/A
Issues with Task Server functionality after repair or upgrade if Task Server is installed on Notification Server.	TECH234031
When you install task server on a Windows 10 computer, multiple errors and warnings appear in windows application log. For example: "**Windows cannot copy file C:\Users\Default\NTUSER.DAT to location C:\Users\Classic .NET AppPool\NTUSER.DAT. This error may be caused by network problems or insufficient security rights**". Note that such errors and warnings are logged only once and do not cause any functional issues for the operating system or for the Task Server functionality.	N/A
After you upgrade to IT Management Suite 8.5 and enable FIPS, the task that contains encrypted data fails on the clients that are not upgraded to 8.5. If you then disable FIPS, and try to run the same task again on the same clients, the task still fails. **Workaround:** Re-saving the task updates the task version in database and requires the client to re-download the task instead of using the cached task.	N/A

Table 1-25 Known issues for Task Server *(continued)*

Issue	Article link
After the upgrade, you sometimes cannot select task or policy items in the left pane, and the right pane cannot display the contents of a task or policy. If the content of the task or policy is not loaded in the right pane, the wait sign is displayed or a blank page is loaded. **Workaround:** Open Internet Explorer options and delete **Temporary Internet files and website files**. Reload the Symantec Management Console.	N/A
If you create and run a **Run Script** task that contains incorrect JavaScript syntax, the task fails, but the status of this task is given as **Completed**.	N/A
If you run a Task Server task with the option **Now** or with a custom schedule with disabled **Override Maintenance Window** option, it ignores the active Maintenance Window and runs anyway.	N/A
The Symantec Management Agents that communicate with Notification Server via proxy are not able to connect to the tickle port.	N/A
When you install Symantec Management Agent on a new client computer, the following error message might appear in the logs: `Removed record for not allowed endpoint, because no such endpoint is registered on NS.` This issue does not affect any functionality.	N/A
The **Run Script** task can be created and saved, but if the syntax is incorrect the task fails. Following error is displayed: `An unknown exception was thrown. System.Data.SqlClient.SqlException: Incorrect syntax near '0'.` **Workaround:** Fix the incorrect syntax of the token. On the **Run Script** page, under **Script Details**, replace the *{0}* with the number of the actual NIC that is used: *1* or *2*.	HOWTO95510
If you create a Control Service State task with the Restart action and you use the full service name, the task fails. **Workaround:** Use the short service name in the task configuration.	N/A
When you install or upgrade task server on a remote client computer, warnings about firewall exceptions can be registered in Notification Server's and Symantec Management Agent's log files. The issue occurs when Windows Firewall service is disabled or stopped.	N/A

Table 1-25 Known issues for Task Server *(continued)*

Issue	Article link
When the data is replicated from the parent Notification Server, error messages regarding the performance counter for Task Server can be logged on the child Notification Server. The cause of this issue is the fact that the CTDataLoader service tries to update before they are initialized. This issue does not affect any functionality.	N/A
If you have uninstalled a solution, and there are some custom jobs that contain task using that solution, those jobs cause error messages to appear in the Symantec Management Console. For example, if you create a job with tasks from Patch Management Solution and then remove that solution, in the Symantec Management Console, an error message appears every time you click that job. Additionally, a detailed error message is visible in the Altiris Log Viewer. Jobs with recurring schedule produce an exception in the Altiris Log Viewer every time the schedule is executed. To stop the jobs with recurring schedule from producing errors every time the job is scheduled, do the following: ■ In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**. ■ In the left pane, right-click the task that produces an error, and then click **Properties**. Then, in the **Properties** window, find out what is the task GUID. For example, you can copy it to a text file. ■ On the Notification Server computer, open the Task Scheduler. To do that, you can press Windows + R, and then, in the **Run** dialog box, enter `taskschd.msc`. Then, click **OK**. ■ In the Task Scheduler, in the left pane, click **Task Scheduler Library**. Then, in the right pane, find the task that has the same Guid included in its name and right-click it. Then, click **Delete**.	N/A
For a task that is executed in hierarchy, if you use **Rerun Failed** on the parent Notification Server, the **Selected Devices** field is not populated with clients reporting to a child Notification Server. This problem occurs because task execution statuses are not replicated from the child Notification Server to the parent Notification Server. **Workaround:** When you use **Rerun Failed** on parent Notification Server, under **Selected Devices**, enter the missing targets manually.	N/A
If you create a task with a schedule on parent Notification Server, the schedule of the task can trigger the replication of this task. In this case, the Windows Task Scheduler on child Notification Server does not display the **Last Run Time** for this task after the task runs. **Workaround:** Replicate the task before its schedule triggers the replication. For example, you can use the **Replicate now** option to replicate the task.	N/A

Table 1-25 Known issues for Task Server *(continued)*

Issue	Article link
If you create a **Client Task Schedule** policy and apply it to a revoked or blocked client computer, the scheduled policy is not delivered to this computer and the task does not run. However, on Notification Server, on the **Client Task Schedule** page, the status of this policy is displayed **0% Started** instead of **Failed**.	N/A
In the **Task Instance Details** dialog box, two different data sources are used for the **Start time** value. In the left pane, the **Start time** data is taken from the managed computer. In the right pane, the data for both **Start Time** and **End Time** is taken from the Notification Server computer. The difference appears if the time data between the Notification Server computer and the managed computer is not synchronized.	N/A
The sample client task **Delete Temporary Files** does not delete any files on Windows Vista, 7, 8, 2008, or 2012 operating systems. The task does not delete files on these operating systems for all user profiles because it looks for the files in the wrong location.	TECH160710
The initial use of ".\username" causes any script tasks that are specified as Machinename\username to fail with the error 'Unable to open the file.' This error is due to a profile loading problem. This issue applies only to some operating systems, such as Window XP SP2 and Windows 2003. It does not apply to Windows 7 or to Windows Vista Ultimate SP2.	N/A

Table 1-26 Known issues for Symantec Management Agent

Issue	Article link
The Symantec Management Agent 7.6 HF7 fails to register on Notification Server 8.1, after receiving the following settings from the Notification Server 7.6 HF7: ■ **Agent Communication Profile** that has Cloud-enabled Management settings specified. This profile is exported from Notification Server 8.1 and imported to Notification Server 7.6 HF7. ■ Custom **Targeted Agent Settings** policy that has the option **Specify an alternate URL for the Symantec Management Agent to use to access the NS** enabled and communication profile imported from Notification Server 8.1 specified, and also the option **Allow Windows agent to perform Cloud-Enabled registration on specified Notification Server** enabled. This issue occurs only if the Notification Server 8.1 is running on Windows 2012 R2 Server. **Workaround:** On Notification Server 8.1, add registry DWORD **"ClientAuthTrustMode"=dword:00000002** at the following location: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]	N/A

Table 1-26 Known issues for Symantec Management Agent *(continued)*

Issue	Article link
In some cases, TLS 1.2 connection might not work between Symantec Management Agent and Notification Server. This issue was introduced by Microsoft and has been fixed now. Make sure that you get the latest updates for your Microsoft Windows Server 2012 R2.	N/A
Client computers that are installed from Cloud-enabled Management offline packages are not part of the default **Cloud-enabled Management Settings** policy targets and don't receive the changes in the default **Cloud-enabled Management Settings** policy. **Workaround:** Clone the **Cloud-enabled Management Settings** policy, and then manually add targets based on the CEM Agents installed from package `pkg_name` filter.	N/A
For Symantec Management Agent to start, permissions for SYSTEM user on `C:\Users\All Users\Microsoft\Crypto\` folder and its contents should be set to **Allow**. If those permissions are set to **Deny**, Symantec Management Agent does not start, and the following error message is logged: `Failed to initialize agent storage: Access is denied (0x00000005)`	N/A
In some cases, Windows XP and Server 2003 computers with Symantec Management Agent installed may show a delay on boot, at the Applying computer settings screen. The cause of this issue is Symantec Management Agent's startup type being set to **Automatic**. **Workaround:** Change the Symantec Management Agent service startup type to **Manual**.	TECH211289
If you have revoked the Symantec Management Agent of a package server, it can take up to three hours before clients assigned to that package server can download packages from Notification Server.	N/A
When you perform a push installation of Symantec Management Agent to a computer that has McAfee All Access 2012 installed, the installation fails.	N/A

Table 1-27 Known issues for UNIX/Linux/Mac

Issue	Article link
After performing an off-box upgrade of IT Management Suite from version 7.6 to 8.0 it is not possible to redirect the 7.6 CEM agents on OSX computers to communicate with 8.0 Notification Server in CEM mode. **Workaround 1:** Take the following steps: 1 Ensure that the 7.6 agents are able to communicate with the 8.0 Notification Server without using CEM. 2 On 7.6 Notification Server, disable the CEM policy to remove the old CEM settings from the agents and configure the **Targeted Agents Settings** to redirect the agents to 8.0 Notification Server.. 3 On the 8.0 Notification Server, enable the CEM policy. After the 7.6 agent registers on 8.0 Notification Server and receives the CEM policy, it receives the new CEM settings. **Workaround 2:** Re-install the agent using the Cloud-enabled Agent installation package.	N/A
Due to file system limitations, Package Server running on Linux-based operating system does not support more than 30000 packages for ext3 file system and not more 65000 for ext4 file system, leading to unavailability of packages in case the number of packages exceeds this limitation.	N/A
Mac OS X agent does not support the **Run As** options for the Managed Software Delivery policy and the Quick Delivery task. If you change the default **Run As** option from **Symantec Management Agent credential** to **Current logged-on user** or **Specific user**, the Managed Software Delivery policy or Quick Delivery task fails to run on your Mac client computer. This issue appears only when you install native packages in Silent or Interactive mode.	N/A
You cannot enable a package server password for Linux Package Server when **Publish HTTP codebase** is enabled. A certain security risk exists if you disable anonymous access to a Linux package server in HTTP mode. Linux package servers support only "basic authentication". Consequently, passwords are sent in plain text. Use either HTTPS or keep anonymous HTTP access for a Linux package server.	N/A
Known limitations exist on supported Apache configurations for the computer that is intended as a package server candidate. For example, HttpdIntegration does not properly parse Apache config file with SSL and custom. Please avoid using complex Apache configurations on such computers.	N/A
After you make a time zone change on a UNIX/Linux/Mac client, the change may not affect running services until you restart the client system.	N/A

Table 1-27 Known issues for UNIX/Linux/Mac *(continued)*

Issue	Article link
The AIX `inittab` service does not support any of the actions that are available in the **Service Action** drop-down list. When the AIX `inittab` service is checked, the **Service Action** field should be grayed out and not selectable. At present this field is (incorrectly) functional in the Symantec Management Console. To avoid errors in your Service Control task, set the **Service Action** field to **No action**. This action prevents any attempt to execute Start, Stop, Restart, or Get Status commands for AIX `inittab` services. Note that currently the No action setting is incorrectly processed and cannot be used for task creation. As a result, all Service Control tasks that are created for the `inittab` service control system are reported as failed. The error message “Missing or invalid service action” is displayed. This message appears regardless of whether the specified process or service was successfully modified.	N/A
Some basic inventory information, such as Time zone, OS language, Primary User, and host id, may not be reported for certain ULM systems (Solaris, HP-UX, and RedHat).	N/A

Table 1-28 Known issues in Network Discovery

Issue	Article link
When you perform Network Discovery using SNMP protocol, the incorrect operating system is shown for Windows 10, and for Windows Server 2016 computers. For Windows 10, Windows 8.1 is displayed. For Windows Server 2016, Windows Server 2012 is displayed.	N/A
When Network Discovery for Windows Embedded Standard 7 SP1 client computers is performed using WMI Connection profile and credentials, the results are displayed as Microsoft Windows Embedded Standard 6.1 65 instead of Windows Embedded Standard 7 SP1.	N/A
Discovery tasks do not identify duplicate identity values among discovered devices. While you run a discovery task, virtual machines with the same UUID are considered as one device. Accordingly, one CMDB resource is created for those devices.	N/A
When running the hierarchy differential replication schedule in certain upgrade scenarios, you may get exceptions such as: "Incompatible columns in DataClassAttribute. Error:Class Name: VM Guest" in the Notification Server computer log. Break the hierarchy before upgrading. Then, upgrade both parent and children before re-joining.	TECH154203

Table 1-28 Known issues in Network Discovery *(continued)*

Issue	Article link
In the Symantec Management Console, on the **Network Discovery** portal page, in the **Network Discovery Task Management** Web Part, on the **Task runs** tab, there is a stop icon that becomes active even when no tasks are selected.	N/A

Table 1-29 Known issues in Pluggable Protocol Architecture (PPA)

Issue	Article link
PPA installation may fail on the Microsoft Windows Server 2012 R2 operating system. **Workaround:** Before starting the installation of IT Management Suite or Remote Monitoring Service, install the Microsoft update KB2919355 on your server.	N/A
PPA plug-in requires .NET 4.5.1 to function properly, but .NET 4.5.1 installation is not supported on Windows 2003 computer. If you try to install PPA plug-in on a Windows 2003 computer, the installation fails.	N/A
After the server restart, the `AtrsHost` service might stop responding with an exception that references to PPA_x64. The root cause of this issue is incorrect practice of using the connection profiles. When the connection profile has some protocols enabled without credentials or when credentials are there but they are not selected, the service stops responding. **Workaround:** Create proper credentials for the connection profile, select them, and then enable the appropriate protocol.	N/A
Remote Monitoring Server (RMS) of Monitor Solution stops responding on computer having Windows Server 2012/2012 R2 and .NET Framework 4.0. .NET Framework 2.0 is a prerequisite for the Pluggable Protocol Architecture (PPA) agent installation. When you enable .NET Framework 3.5 from the **Add Roles and Features** wizard, .NET Framework 2.0 gets installed automatically. .NET Framework 2.0 does not get installed automatically on installing .NET Framework 4.0. Because .NET Framework 2.0 is not installed on the computer, the PPA agent installation is affected, which in turn affects RMS. **Workaround:** Enable .NET Framework 4.5.1 on the computer and then install PPA.	N/A
WMI, WSMAN, and other monitoring plug-ins become unavailable if multiple web-service identities are used. You must ensure that you remove multiple identities if you choose a custom website.	TECH142631

Table 1-30 Known issues in ASDK

Issue	Article link
To use the `ExecuteTask` ASDK method, you have to be a member of the Symantec Administrators security role.	N/A
SecurityManagement.AddRolePrivileges and SecurityManagement.RemoveRolePrivileges do not work on right-click privileges. An automated workaround using the ASDK currently does not exist. However, right-click privileges can be added to a role and removed from a role using the Symantec Management Platform item update process.	N/A
ItemManagement.SetItemsSchedule does not successfully set a schedule on a policy item. Currently a workaround using the ASDK does not exist.	N/A

Table 1-31 Known issues in Security Cloud Connector

Issue	Article link
When you import device data from Unified Endpoint Protection to the child Notification Server, the imported devices are replicated up to parent Notification Server. However, the organizational views and groups in which these devices reside, are not replicated up to parent. As a result, the imported devices only appear under the default **Computer** organizational group.	N/A
Not all user data that is imported from Unified Endpoint Protection to the child Notification Server, is replicated up to the parent Notification Server. Only device owners are replicated up.	N/A
The resources that are imported from Unified Endpoint Protection to Notification Server are not purged on Notification Server.	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 1-32 Known issues for Deployment Solution

Issue	Article Link
In the **Restore Image** task, an error message is displayed when you try to select an image from the drop-down list.	N/A
iPXE does not autoselect PXE boot image set on the **NBS General Settings** page for unknown, predefined, or managed computers.	TECH251431

Table 1-32 Known issues for Deployment Solution *(continued)*

Issue	Article Link
You cannot convert an EFI image with multiple partitions from GPT partition type when deployed on a BIOS-based client computer.	N/A
The extract SSL policy fails to extract certificate on a Windows 2016 site server with domain certificate.	N/A
DeployAnywhere logs are not copied to the logs directory at the following path: `x:\program files\symantec\deployment\logs`	N/A
Surface Pro 4 computers using docking stations do not match the record when you use a USB device for imaging.	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
A UEFI-based computer with secure boot mode enabled is unable to boot to production when you deploy a BIOS-based Windows 8 64-bit image.	N/A
For macOS Sierra 10.13 and higher NetInstall (SOI) is not currently supported.	N/A
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/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.	

Inventory Solution Known Issues

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

The known issues are separated into the following groups:

- Installation and upgrade issues.
  See Table 1-33 on page 51.
- Hierarchy and replication issues.
  See Table 1-34 on page 51.
- Other known issues that are common for all types of platforms.
  See Table 1-35 on page 51.
- Other known issues for Windows platforms.
  See Table 1-36 on page 52.
- Other known issues for UNIX, Linux, and Mac platforms.
  See Table 1-37 on page 53.

Table 1-33 Installation and upgrade issues

Issue	Article link
After you upgrade the Symantec Management Agent to the latest version, the old version Inventory Plug-in may experience troubles collecting some data. To avoid this problem, you should always upgrade Inventory plug-in to the latest version.	N/A

Table 1-34 Hierarchy and replication issues

Issue	Article link
If the parent Notification Server and child Notification Server have different region time format settings, the **Days Metered** count on the **Underutilized Software** report page displays incorrect value.	N/A
When you replicate an inventory task from a parent Notification Server to a child Notification Server in a hierarchy, you can edit the advanced options of the replicated task on the child NS computer. After you edit the advanced options of the replicated task on the child NS computer and click **Save changes**, the changes that you made are not saved. Normally, the advanced settings on the replicated task page should not be editable, and the Save changes and Cancel options should not be enabled.	N/A

Table 1-35 Other known issues that are common for all types of platforms

Issue	Article link
The **Control SEP Service State** task fails to start the Symantec Endpoint Protection service and the return code 4 is reported when the startup type of the service on a client computer is set to **Disabled**.	N/A

Table 1-35 Other known issues that are common for all types of platforms *(continued)*

Issue	Article link
Inventory scan does not report the information about file language when you enable the option **File properties - manufacturer, version, size, internal name, etc.** on an inventory policy or task page.	N/A
Inventory reports display incorrect **Install Date** for installed software products.	N/A
During full inventory scan, file inventory is not collected for the software components that are not .MSI based. You cannot view file inventory data when you right-click a non-MSI based software component, click **Actions > Edit Software Resource**, and then click the **File Inventory** tab. As a result, you cannot automatically meter the usage of this software component as it has no file inventory and is not associated with an executable file. To enable a non-MSI based software component for metering, you should manually add executable files to the software component.	N/A
A license is not reclaimed when the **Asset Status** is set to a custom asset status. Inventory Solution or Inventory Pack for Servers license should be reclaimed on setting the **Asset Status** to other than **Active**.	N/A

Table 1-36 Other known issues for Windows platforms

Issue	Article link
When Inventory Solution gathers information about Microsoft Windows store applications, the software component names are reported as provided by the vendor and may be unclear. For example, GUID may be reported as a component name.	N/A
SCDP Inventory task and software scan may overwrite the contents of the table dbo.Inv_InstalledSoftware with their own different results.	N/A
Software Catalog Data Provider Inventory task may incorrectly detect several languages of the same software component as several components that are installed on the same client computer.	N/A
An inventory policy that runs under the **System account** does not collect inventory information about Network Printers. To collect this information, you need to run the policy as a **Logged in user**.	TECH145268

Table 1-36 Other known issues for Windows platforms *(continued)*

Issue	Article link
When you use Internet Explorer 10 or 11 to download a stand-alone package, an error occurs. This issue occurs because of the **SmartScreen Filter** security feature by Microsoft. You can directly download the package exe from the `NSCap` folder on the server, and run it on unmanaged client computers.	N/A
After the NS.Nightly schedule task runs, the Yahoo! Messenger is displayed in the Software Catalog under **Newly Discovered Software** instead of under **Unmanaged Software**.	N/A
When you configure the advanced options for the Inventory policy and include a file scanning rule for a file type that is not in a default list, the files are not scanned if the file type is written in capital letters.	N/A

Table 1-37 Other known issues for UNIX, Linux, and Mac platforms

Issue	Article link
Errors related to invalid characters (like `hex 0x1F`) appear in the Notification Server's logs when processing the inventory data collected on UNIX, Linux, or Mac computers.	N/A
Inventory scan does not report Model ID for some Mac client computers.	N/A
Running three software inventory tasks simultaneously on UNIX, Linux, and Mac computers results in the system overload and long execution time because CPU usage increases to 100%. As a workaround, you can schedule the tasks to avoid running them simultaneously.	N/A
Inventory scan does not scan deeper than maximum length paths limitation.	N/A
HW_DiskPartition data class cannot be populated on AIX platforms.	N/A

IT Analytics 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 1-38 Known issues for IT Analytics

Issue	Article link
Optional Configuration is not displayed unless **Reporting Services** configuration is defined.	N/A

Table 1-38 Known issues for IT Analytics *(continued)*

Issue	Article link
Column headers are not localized properly in **Cube Browser**.	N/A
In some SQL Server 2008 **Reporting Services** configurations, Internet Explorer compatibility issue causes report controls to render incorrectly.	N/A
IT Analytics Event Reports and dashboards are not installed by default.	N/A
Starting from ITMS 8.0, IT Analytics reports and dashboards may have issues with loading on the SMP console.	TECH234703

Known issues of IT Management Suite integrations

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 1-39 Known issues of IT Management Suite integrations

Issue	Article link
An incorrect installation command line is generated during the import of SEP installation package for Mac if the imported package file has white spaces in the name. As the result, SEP agent is not installed properly, the execution status is failed. Workaround: You can rename the package before importing so that it does not contain white spaces. Another possibility is to edit the generated command line so that the package name is quoted.	N/A

ITMS Management Views 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 1-40 Known issues for ITMS Management Views

Issue	Article link
You can select **Hardware Summary** and **Operating System Summary** data classes in the Custom Criteria dialog box if the root Data Classes have been disabled for your particular user role.	N/A
A target cannot be saved to an empty root directory.	N/A

Table 1-40 Known issues for ITMS Management Views *(continued)*

Issue	Article link
If the version of the installed Server Inventory plug-in is earlier than 7.6, the expected plug-in version is displayed as N/A.	N/A
You may experience problems when downloading ITMS Management Views. In this case, Symantec recommends that you clear the browser cache.	N/A
When you navigate from the **Manage** menu to **Computers**, **Software**, **Policies** or **Jobs/Tasks**, the corresponding section doesn't open if the host name of Notification Server that you are connecting to contains underscore characters. To resolve this issue, you need to change the server host name or connect to the server using the IP address.	Domain names Session variables
Software products with enabled metering and tracking and one or more Mac software components, appear in the **Missing program associations** filter.	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.

The known issues are separated into the following groups:

- Patch Management for Windows installation, upgrade, and data migration issues
  See Table 1-41 on page 56.
- Patch Management for Windows hierarchy and replication issues
  See Table 1-42 on page 56.
- Patch Management for Windows software updates installation issues
  See Table 1-43 on page 57.
- Patch Management for Windows other known issues
  See Table 1-44 on page 58.
- Patch Management for Mac known issues
  See Table 1-45 on page 60.
- Patch Management for Linux installation and upgrade issues
  See Table 1-46 on page 60.
- Patch Management for Linux hierarchy and replication issues
  See Table 1-47 on page 61.
- Patch Management for Linux other known issues
  See Table 1-48 on page 61.

Table 1-41 Patch Management for Windows installation, upgrade, and data migration issues

Issue	Article link
If you have the source Notification Server that has IT Management Suite (ITMS) version 8.0 or later with a custom installation directory, and the migration wizard is installed to this custom directory, the following issue occurs: ■ Patch Management Solution is not listed in the **Symantec Notification Server Migration Wizard**, on the **Exporter Configuration** page, because Patch Management Solution components are installed into the default location `C:\Program Files\Altiris\Upgrade\...` Workaround: Move Patch Management Solution components from the default location to the custom location.	N/A
The **Symantec Notification Server Migration Wizard** does not migrate RPM Catalogs. Workaround: Manually transfer files from the directory `C:\Altiris\Patch Management\Packages\RPMCatalogs` on the source Notification Server to the target 8.5 Notification Server.	N/A
After the upgrade to 8.5, system assessment scan fails on client computers that have the Symantec Management Agent upgraded but the software update plug-in not yet upgraded.	N/A

Table 1-42 Patch Management for Windows hierarchy and replication issues

Issue	Article link
After an upgrade from the previous version for which you had to break the existing hierarchy, you need to run **Patch Management Import Data Replication for Windows** once with **Replication Mode = Complete** to ensure that items deleted on parent server are also properly deleted on the child servers (for example, Patch Data bulletins).	N/A
If you run complete replication but do not replicate the patch data, and then try to run the **Vulnerability Scan** task on a child server or a client computer from the Parent Notification Server, the scan fails.	N/A
Replicated policies get deleted on the child Notification Server, when Patch Management Import Data for Windows uses the **Standard Replication Schedule**.	TECH210370

Table 1-43 Patch Management for Windows software updates installation issues

Issue	Article link
Some updates do not support silent installation. Some dialog or progress windows may be visible to the user of the client computer.	N/A
Some updates may fail to install in certain conditions. The following updates are known to have issues: ▪ Flash Player All Mozilla Firefox browser windows and all instances of Flash Player must be closed before installation. Symantec recommends that you update Flash Player 7.x, 8.x, and 9.x to the latest version. ▪ Real Player Installation may fail if a limited user is logged in to the system. ▪ Mozilla Firefox version 1.5, 2.0 and 3.0 All Mozilla Firefox browser windows must be closed before installation. ▪ Opera Silent installation may fail on Windows XP. ▪ Adobe Reader version 7 and 8 All instances of Adobe Reader, including those opened inside of a browser, must be closed before installing updates. Symantec recommends that you install Adobe Reader updates shortly after a computer restart. ▪ ISA Server 2000 Security Patch for Web Proxy Service and H.323 ASN DLL (MS01-045) Installation of this hot fix requires user interaction on the target computer. The user must click **Yes** in the installation dialog box.	HOWTO54657
Some software updates are shown as not installed in the **Windows Update** dialog box. This issue occurs because the executable is a full software release, not a patch. Symantec recommends that you use Altiris Software Management Solution from Symantec to roll out this software. The following software updates are known to have this issue: ▪ KB982671 - Microsoft .NET Framework 4 ▪ KB968930 - Windows PowerShell 2.0 and WinRM 2.0 ▪ KB940157 - Windows Search 4.0 IE8 - Internet Explorer 8 ▪ KB2526954 - Microsoft Silverlight IE9 - Internet Explorer 9 ▪ KB2463332 - Windows Internal Database Service Pack 4	N/A

Table 1-43 Patch Management for Windows software updates installation issues *(continued)*

Issue	Article link
Some updates may require original installation media. The updates that are known to require one are as follows: ■ Microsoft Project 2003 SP3 ■ Microsoft Visio 2003 SP3 ■ Citrix Presentation Server If the product was installed from a CD/DVD, then the original CD/DVD must be inserted in the disk reader on the client computer.	N/A
Issues occur when various Microsoft Office components are having different Service Pack versions applied.	N/A
A removed vendor or software update is displayed in the **Vendors and Software** list. The removed vendor or software release will disappear from the list after the **Import Patch Data for Windows** task is completed.	N/A
When you deploy Microsoft updates that require the computer restart through Patch Management with the restart settings disabled, the operating system still forces the client computers to restart.	N/A

Table 1-44 Patch Management for Windows other known issues

Issue	Article link
Automation policy report **Software Update Policy Failed** does not return any results for a failed software update policy that contains Windows Update Agent updates.	N/A
A non-administrator cannot navigate to the AexPatchUtil.exe utility using the command prompt because of access restrictions to the `C:\Program Files\Altiris` folder. This issue occurs only on the Notification Server computer. Workaround: `cd` straight to the `C:\Program Files\Altiris\Altiris Agent\Agents` directory.	N/A
An issue occurs when you re-image or reinstall an operating system on a client computer. Software update plug-in cannot process the policies and install software updates. Workaround: Restart the Symantec Management Agent service or restart the computer.	N/A
Patching of software that is installed into a virtual layer is not supported.	N/A

Table 1-44 Patch Management for Windows other known issues *(continued)*

Issue	Article link
Packages are not always downloaded to managed computers at the correct time. This is due to a timing issue where the initial download is not triggered by Software Management and the status of the package is not updated. The packages will be downloaded when the update install schedule fires or when the next maintenance window opens.	N/A
When you click **Save Changes** in a policy, a confirmation message displays *Saved Changes* even though the policy is still being saved.	N/A
The Software Update Plug-in stays in the *Update Pending* state after the **Software Update Installation** dialog box closes. Occasionally, clicking **Install Now** in the **Software Update Installation** dialog box or waiting for the dialog box to close itself does not result in the immediate installation of a software update. The installation starts five minutes after the dialog box has closed, when the software update plug-in wakes up and checks its state.	N/A
When, on the **Import Patch Data for Windows** page, under **Package Location**, you select **Alternative Location**, you need to enter it in the following format: **<alternative location>/pmimport.cab** Otherwise, if you enter the path in the wrong format, the new location will still be saved successfully, but, the import will fail.	N/A
After the disaster recovery, you need to rerun the Patch Management import.	N/A

Table 1-45 Patch Management for Mac known issues

Issue	Article link

After upgrade of Patch Management Solution for Mac, the following tasks fail to run on the Mac client computers that still have the older version of Symantec Management Agent:
■ Run System Assessment Scan on Mac Computers
■ Install All Available Updates
■ Install All Recommended Updates
■ Install All Updates Not Requiring Restart
■ Install All Updates Requiring Restart
The error details are as follows:
`Failure message: command finished with error code: (133) unknown error.`
`Package download status: package downloaded successfully, but failed to launch the program.`
Workaround: Upgrade Symantec Management Agent to fix the issue.
	N/A

The Mac Software Update Helper Tool might not detect some firmware updates for Mac computers. Therefore, those updates do not appear in the **Available Mac Software Updates** report. Workaround: Manually download the update from the Apple Downloads site. If you are unsure whether your computer needs a particular update, download and open the update installer. The installer indicates whether the firmware update is already installed or is not needed.	N/A

Table 1-46 Patch Management for Linux installation and upgrade issues

Issue	Article Link
After you perform an upgrade from ITMS 8.0 HF6 to 8.5, the upgraded software update policies and newly created after the upgrade policies do not work properly on the Linux client computers that have the software update plug-in less then 8.1 installed.	N/A
On the client computers that have the software update plug-in less then 8.1 installed, the **Linux System Assessment Scan** does not report as applicable the Linux updates with the following characteristics: ■ The updates obsolete another installed update packages. ■ The updates have been imported by the **MetaData Import Task** running on the 8.1 Notification Server. As soon as the software update plug-in on the client computers is upgraded to 8.1, the **Linux System Assessment Scan** reports such updates as applicable.	N/A

Table 1-46 Patch Management for Linux installation and upgrade issues *(continued)*

Issue	Article Link
Software Update Plug-in 8.1 on Linux clients may be not functional with the state **Waiting for repository** if the task **Import Patch Data for SUSE/Red Hat** is not executed after the upgrade to 8.1.	N/A

Table 1-47 Patch Management for Linux hierarchy and replication issues

Issue	Article Link
Exporting software update policies from parent to child is not supported.	N/A
Replicating data between different versions of Patch Management Solution is not supported.	N/A

Table 1-48 Patch Management for Linux other known issues

Issue	Article Link
A user who belongs to the **Patch Management Administrators** role cannot edit default targets in the following policies: ■ Novell patch management configuration policy You access this policy from **Settings > Software > Patch Management > SuSE Settings > SuSE**. ■ Red Hat patch management configuration policy You access this policy from **Settings > Software > Patch Management > Red Hat Settings > Red Hat**. Workaround: On the configuration policy's page, delete the default targets, and then add the appropriate custom targets.	N/A
Task details do not show the cause of the **Import Patch Data for Red Hat** or the **Import Patch Data for SUSE** that fail due to lack of free space on the Notification Server computer.	N/A
Automation policy report **Maintain Retired Machine Historical Data** does not return any results.	N/A
Patch Management for Linux uses Linux native tools Yum and Zypper to resolve and install dependent software update packages. On Linux client computers, a software update policy attempts to install in a single transaction all the software updates that are included into the policy and their resolved dependent packages. If the native tool fails to install at least one of the packages, the policy fails to install the other packages too.	N/A

Real-Time System Manager 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 separated into the following groups:

- SOL/IDE-R issues
  See Table 1-49 on page 62.
- RTCI known issues
  See Table 1-50 on page 64.
- Other known issues
  See Table 1-51 on page 64.

Table 1-49 Known issues for SOL/IDE-R

Issue	Article link
SOL terminal window does not support double-byte characters (Japanese, Chinese).	N/A
The following options must be configured in the ME BIOS advanced settings for Intel AMT Serial-over-LAN to work correctly with HP computers: ■ SOL Terminal Emulation Mode: ANSI ■ Disabled echo char: ON	N/A
When the SOL/IDE-R session is used to remotely boot a Dell client computer from a physical floppy diskette that is inserted into a floppy drive on the Notification Server computer, or from a binary floppy image file, the client computer performs a restart but does not load the operating system. On the client computer's monitor, the message `Attempting remote IDE boot` appears, but the Real-Time System Manager's terminal window remains blank until the session is terminated. This is a known issue with Dell computers (tested on Dell OptiPlex 745c). Workaround: Start the client from other media (physical CD-ROM, DVD-ROM, or ISO image file).	N/A
If a SOL session window is already opened for a computer, you must close it before establishing a new remote SOL connection to the computer. Otherwise, following error message may appear: `SOL session terminated.`	N/A
When SOL and IDE-R are disabled in the target computer's BIOS, the controls for these options on the **Intel AMT Settings** page (**Task progress window and remote control** and **Redirect to optical/floppy drive or image on a server**) are not disabled.	N/A

Table 1-49 Known issues for SOL/IDE-R *(continued)*

Issue	Article link
IDE-R session to an MS-DOS boot image may not work correctly with the managed HP client computers that have BIOS versions earlier than 1.5. Workaround: Upgrade BIOS on the client computer.	N/A
When you use any Alt+<key> sequence on the keyboard during the Serial-over-LAN session, the controlled computer may not receive it.	N/A
Due to SOL emulation limitations, installation of a graphical operating system through IDE-R can lead to a BSOD on some Intel vPro implementations and is not fully supported by Intel AMT 2.x products. The problem affects HP Compaq Business Desktop System BIOS for Intel vPro Technology (786E1 BIOS). Workaround: Download and install the latest BIOS/firmware update from the vendor's website.	N/A
When you establish a SOL/IDE-R session with HP computers with Intel AMT 2.5, the first line of the terminal output is not displayed in the remote console.	N/A
Ctrl+Alt+Del key sequence does not work in the SOL session established with Intel AMT 2.5 devices.	N/A
Function keys do not work in the SOL session. Use use the <Esc>+1 - <Esc>+0 key sequence to emulate the function keys.	N/A
On some hardware (HP, Fujitsu), the SOL/IDE-R session initiated by wireless connection terminates after 1 minute. This is a hardware limitation. To work around this issue, do the following: **1** In the Notification Server computer's registry, set the following DWORD value to *1*: *HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Notification Server\ProductInstallation\{13987439-8929-48d2-aa30-ef4bf0eb26a6}\InstantAMTPing*. **2** Restart the IIS.	N/A
One-to-many server IDE-R task fails if the IDE-R session is left active from the one-to-one real-time task and vice versa.	N/A
Boot redirection options are not available for DASH computers.	N/A

Table 1-50 Known issues for RTCI/RTSM

Issue	Article link
If the redirection privileges are disabled, it is impossible to execute one-to-one power actions, such as power off or restart.	N/A
It is not possible to run one-to-many out-of-band tasks on IPMI computers. That is because the IP address of the IPMI management controller differs from the computers's IP address. Notification Server does not know the IPMI controller's IP.	N/A
The **Restore State** power action is not capable of putting computers into Stand-by (S3) or Hibernate (S4) states. Consequently, the **Restore State** power action turns off the computer (if needed) in an attempt to restore the Hibernate (S4) state and turns on the computer (if needed) to restore the Stand-by (S3) state.	N/A
The following Intel AMT inventory is not collected by the **Get Out-of-Band Inventory** task: ▪ RTCI AMT Battery Serial Number ▪ RTCI AMT Battery Manufacture Date	N/A

Table 1-51 Other known issues

Issue	Article link
Error while performing power management operation `Reboot` command. This problem is known for Dell Precision T3500 computers.	N/A
It is not possible to connect to Intel AMT 5.0 using secure WS-MAN connection. To solve this problem, you need to upgrade the Intel AMT 5.0 firmware to the latest Intel AMT 5.2.	N/A
You cannot connect to Intel DASH computer configured in mutual authentication mode.	N/A
IDE redirection does not work with "Kerberos" user.	N/A
Firewall settings prevent WMI connection to a computer running Windows XP Service Pack 2. If you provided valid WMI credentials, but cannot establish a WMI connection to a computer that is running Windows XP Service Pack 2 (WMI is not in the list of supported protocols on the Real-Time Consoles page), check the firewall settings on the target computer. The default configuration of the Windows Firewall program in Windows XP SP2 blocks incoming network traffic on Transmission Control Protocol (TCP) port 445. Configure the firewall to allow incoming network traffic on TCP port 445.	N/A

Table 1-51 Other known issues *(continued)*

Issue	Article link
When using Real-Time System Manager to remotely connect to Windows Vista, Windows 7, Windows 8, or Windows 8.1 client computers, you must make sure that Windows Firewall is configured to allow remote Windows Management Instrumentation (WMI) connections on the client computer. To enable WMI connections on Windows Vista, in the Control Panel, click **Windows Firewall > Change Settings > Exceptions**, and then check **Windows Management Instrumentation (WMI)**. Additionally, for standalone WWindows Vista, Windows 7, Windows 8, or Windows 8.1 clients (not in a domain), you must disable the User Account Control (UAC). For example, to do this for Windows Vista, in the Control Panel click **User Accounts > Turn User account control on or off** and then uncheck **Use User Account Control (UAC) to help protect your computer**. Optionally, you can disable the UAC for the built-in administrator account (if you want to use this account for remote connection). To do this, in the **Control Panel > Administrative Tools > Local Security Policy** MMC snap-in, click **Local Policies > Security Options** and disable the **User Account Control: Admin Approval mode for Built-in Administrator account** policy.	N/A
Connection capabilities limited when connecting to computers that have multiple network cards.	N/A
One-to-many tasks cannot manage resources by an IP address.	N/A
Some Intel ASF hardware does not support power off from the S3 state. You can try to turn on the computer and then run the turn off command again. Broadcom ASF does not have this problem.	N/A
PXE Boot does not work with some ASF hardware.	N/A
Both one-to-one and one-to-many tasks in the Real-Time System Manager software require a direct connection to the target computer that you want to manage. It is not possible to manage computers located behind NAT-enabled routers.	N/A
Graceful shutdown or restart returns an error on Microsoft Windows Vista, Windows 7, Windows 8, or Windows 8.1.	N/A
It is not possible to update properties on the **Operating System** page in the **Real-Time** view if the target computer is running Microsoft Windows Vista (32-bit and 64-bit editions).	N/A
Intel AMT computer management using CIRA is possible only with Intel AMT 4.0 and later computers that are configured to use TLS or TLS with mutual authentication.	N/A
It is impossible to connect to Intel DASH computer configured in mutual authentication mode.	N/A

Table 1-51 Other known issues *(continued)*

Issue	Article link
In the **Real-Time** view, on the **Intel AMT Configuration Mode** page, the setup and Configuration Server address is not shown for computers with Intel AMT version 2.6 and 4.0.	N/A
During upgrade, custom configuration of Network Filtering resets to default. To keep using the custom setting you need to do the following: - On your NS Server, from the *\RTSM\Web\UIData* folder, copy the `CBFilters.bak` file. - Rename the `CBFilters.bak` file to `CBFilters.xml`. - Replace the original xml with the one containing the custom configuration.	N/A
It is not possible to connect to a remote computer using local account. Whether you are connecting to a remote computer in a domain or in a workgroup determines whether User Account Control (UAC) filtering occurs. In a workgroup, the account connecting to the remote computer is a local user on that computer. Even if the account is in the Administrators group, UAC filtering means that a script runs as a standard user. Workaround: A best practice is to create a dedicated local user group or user account on the target computer specifically for remote connections.	https://msdn.microsoft.com/

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.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 1-52 on page 67.
- Managed software delivery issues
  See Table 1-53 on page 68.
- Software Portal issues
  See Table 1-54 on page 71.
- Hierarchy and replication issues
  See Table 1-55 on page 71.
- Non-Windows-specific issues
  See Table 1-56 on page 71.
- Software Management Framework issues

See Table 1-57 on page 71.

- Other issues
  See Table 1-58 on page 73.

Table 1-52 Installation and upgrade issues

Issue	Article link
A Managed Software Delivery policy with the compliance schedule window, which is set for a time period in the past, re-executes after the on-box upgrade from ITMS 7.5 SP1 HF5 to ITMS 8.0 and the upgrade of Symantec Management Agent and Software Management Solution Plug-in on the client computer.	N/A
If you import custom software resources to `\\<NS>\NSCAP` UNC share, and then upgrade Symantec Management Platform, the software is removed during the process.	N/A
After upgrade from IT Management Suite 7.0, previous versions of Symantec Management Agent and Software Management Plug-in may fail to run Managed Delivery Policies and Quick Delivery tasks under specific user credentials. Workaround: Upgrade Symantec Management Agent and Software Management Plug-in or run Managed Delivery Policies and Quick Delivery tasks using Symantec Management Agent credentials.	N/A
Managed Software Delivery policies stay in the detection check state after upgrade. If Managed Software Delivery policies stay in the detection check state on the client computer for a long time after upgrade, then they may not get executed. Workaround: To fix this issue, restart the affected client computer or the corresponding Symantec Management Agent.	N/A
Modified installation error code descriptions are reset to default values, after upgrading from Software Management Solution 7.0.	N/A
Migrated software components are not merged with newly discovered software components if those components have separate 32-bit and 64-bit versions. After upgrading to Software Management Solution 7.5, software component duplicates appear in Software Catalog, after running Software Discovery for those components which have 32-bit and 64-bit separate versions.	N/A
If you enable Legacy Agent Communication mode after you upgrade Notification Server, the "Windows computers with installed Software Management plug-in" filter along with the tasks and policies, based on this filter does not work, unless the Software Management plug-in is up-to-date.	N/A

Table 1-52 Installation and upgrade issues *(continued)*

Issue	Article link
The version of the Virtual Composer in the software resource package remains unchanged, after upgrading to the latest version of Software Management Solution. Detection and applicability rules, based on the Virtual Composer version must be updated manually.	N/A
If the Software Library is inaccessible during the upgrade to the latest version of Software Management Solution, software packages are not grouped properly on the IIS web server.	N/A

Table 1-53 Managed software delivery issues

Issue	Article link
The **Import and Deliver** method lets you import .exe files. However, the .exe files that do not contain file resource data (company name and/or version) are not supported.	N/A
You can use a **Symantec Endpoint Protection Delivery** policy to deliver Symantec Endpoint Protection client (SEP agent) to Windows and Mac client computers. However, SEP delivery supports only the following SEP installation package files: ■ Non-DMG based ZIP files for Mac ■ EXE files for Windows ■ EXE self-extracting (SFX) archive files for Windows Workaround: You can use Managed Software Delivery policies to deliver SEP agent that is installed with other types of installation package files.	N/A
When on the parent Notification Server computer, you right-click the **Symantec Endpoint Protection Delivery** policy, and then click **Replicate Now**, the Symantec Endpoint Protection (SEP) release that is associated with the policy is also replicated. However, the replicated SEP release is not listed on the child Notification Server computer, at **Manage > Software > Deliverable Software > SEP Releases**. Workaround: You can perform differential or complete replication to solve the issue.	N/A
The following issue may appear to a Managed Software Delivery policy that is scheduled to run during a maintenance window: The Symantec Management Agent user interface shows the **Restart is pending** status for the Managed Software Delivery policy if a required computer restart occurs during the maintenance window closure. During the next scheduled maintenance window, the status changes to **Compliant** or **Not compliant** depending on the detection check results.	N/A

Table 1-53 Managed software delivery issues *(continued)*

Issue	Article link
You can create a Managed Software Delivery policy and schedule compliance or remediation to start running at computer startup. If the policy is received approximately 20 minutes after the target computer startup, the policy runs as soon as the computer receives the policy.	N/A
When you schedule many Managed Software Delivery policies, and on the **Managed Delivery Settings** page, in the **Actions after success** section, select the advanced option **Log off user**, the other policies in the queue are postponed until the post-execution restart of the client computer occurs.	N/A
When you schedule a Managed Software Delivery policy and on the **Managed Delivery Settings** page, in the **Run As** section, select the advanced option **Symantec Management Agent credential** or **Current logged-on user**, and then in the **Task can run** section, select the advanced option **Only when user is logged on**, the policy does not respect the selected settings and runs at the scheduled time, even if the user is not logged on a client computer.	N/A
After you run a Managed Software Delivery policy on a managed client computer, SMA restart occurs during the policy execution, and then you cancel the software installation, the last status **Success** is incorrectly displayed for **Execute install command** on the client computer, on the **Symantec Management Agent** toolbar, in the **Software Delivery** tab. At the same time, the policy is correctly reported as not compliant on the client computer and in reports on Notification Server.	N/A
If Managed Software Delivery policy is created for a software, which has a dependency on another software, using **Managed Software Delivery** wizard, where on the **Specify dependencies and updates** page the **Verify dependencies** option is checked and the software resource option is unchecked for the corresponding software, the dependent software is not installed even if the dependency option is later checked in the policy settings. Workaround: To fix the issue, remove the software resource from the Managed Software Delivery policy and add it again.	N/A

Table 1-53 Managed software delivery issues *(continued)*

Issue	Article link
Managed Software Delivery policy or a Quick Delivery task fail to run from a directory on the Notification Server computer with a 1619 error code, if the following conditions are met: ■ Managed Software Delivery policies and Quick Delivery tasks fail to run from a directory on the Notification Server computer. ■ There are no package servers in an environment; ■ A software resource is imported from a Notification Server; ■ The **Use the following settings to download and run** option is checked; ■ The **Download and run locally if bandwidth is above** is unchecked; ■ The **Run from server if bandwidth is above any connection speed** is checked; ■ The **Current logged-in user** option is checked on the **Run Options** settings.	N/A
When running a Managed Software Delivery policy under **Currently logged in user**, the file version detection check fails to detect a file, which is located under the %user name% folder. Workaround: To fix the issue, in the file location path, use the %useprofile% environment variable, which points to the same folder.	N/A
When running a Managed Software Delivery policy under **Currently logged in user**, the **Registry Key/File Path to File Version** and the **Registry Key/File Path to Product Version** detection rules fail to detect a file, if the path is specified using environment variables.	N/A
If multiple users log in locally or remotely to the client computer, on which a software resource is installed by a Managed Software Delivery Policy, and specify different settings, when prompted to restart the computer after the software installation is complete, the following situations may occur: ■ If a client computer user snoozes the computer restart, after a software resource is installed by a Managed Software Delivery policy, computer can only restart, when this user is logged in again. If another user logs in to the same client computer and selects to restart the computer after the installation is complete, the computer does not restart. ■ If a user has accepted computer restart, but it was snoozed by another user, or the maintenance window has not started yet, the computer will then restart unexpectedly for the first user, when the snooze period, specified by another user expires or the maintenance windows starts.	N/A

Table 1-54 Software Portal issues

Issue	Article link
Even if you apply the legacy UI to the Software Portal, the enhanced UI opens on client computers with Cloud-enabled Management enabled.	N/A
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. However, on Windows devices, the notification may be displayed for too short time (less than 30 seconds), and the user may overlook it.	N/A
When migrating from Software Management Solution 6.x, the Software Portal publishing permissions for a software resource change their status from **Approved** to **Requesting Approval**.	N/A

Table 1-55 Hierarchy and replication issues

Issue	Article link
When you run **Differential Hierarchy update** from the Parent Notification Server to the Child Notification Server, a Managed Software Delivery policy gets replicated every differential replication, if you enable the option **Power on computers if necessary (using Wake-on-LAN, Intel AMT, ASF or DASH)** on the **Managed Delivery Settings** page or under the **Schedule** section that appears when you create or edit the policy.	N/A

Table 1-56 Non-Windows-specific issues

Issue	Article link
A false-positive status for a software package on a Mac client computer may be reported, if the user cancels the software interactive installation. If a user of a Mac client computer cancels a Quick Delivery task or a Managed Delivery task, which has an interactive install, the success execution event is sent to the Notification Server, leading to a false-positive status for this installation. At the same time, the software scan for the Quick Delivery task and the detection check for the Managed Delivery task provides the correct information.	N/A

Table 1-57 Software Management Framework issues

Issue	Article link
If you import computer resource information from an XML file, exported from another Notification Server, the computer resource information related to installed software in the Resource Manager is lost.	N/A

Table 1-57 Software Management Framework issues *(continued)*

Issue	Article link
Source Path Update and Windows Installer Repair tasks fail with error code -1073741515 on computers, running Windows Server 2012 R2 Core operating system.	N/A
The **Log off user** option in the **Managed Software Delivery** policy logs off only a single session rather than all sessions when multiple sessions are active. For more information, see topics on Results-based actions settings in Software Management Solution in the *IT Management Suite Administration Guide* at the following URL: http://www.symantec.com/docs/DOC7978 Workaround: Use the **Log off** option available with the **Restart Computer** task to successfully log off every session.	N/A
Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	N/A
If you create a Quick Delivery task and the task times out before the maintenance window is activated on the client, the task fails. By default, a task times out after 300 minutes. On the **Task options** tab of the Advanced settings, you can change when a task ends.	N/A
With a Managed Software Delivery policy or Quick Delivery task, applications with large installation paths fail to execute.	TECH133459
When creating a package by ASDK **AutoGenerateCommandLines** parameter set to **True**, no command lines are generated for the package.	N/A
If you add one large file or a very big number of small files, estimating around 2 GB in total, the procedure will fail with errors in the Notification Server computer log file, while editing a software resource.	N/A
Setting weak ACL, such as "Everyone", for a shared location, which is used for the Software Library, may lead to intentional or unintentional loss of Software Library data or lack of storage on the corresponding server. Workaround: To prevent the issues, set strong ACL for UNC path, which leads to the Software Library repository.	N/A
When importing software packages using Import Software wizard, package files can be read by an unauthorized party during data transfer from package store to the Notification Server computer. If package files contain sensitive information, such as passwords inside scripts, in unencrypted form, then such software import can be a subject to information disclosure threat.	N/A

Table 1-58 Other issues

Issue	Article link
The detection rule expressions **Registry Key Exists** and **Static File Expression** support wildcards in path. However, they work incorrectly in the following case: ■ Several keys or files are matching. ■ An additional condition is set (**Entry** for **Registry Key Exists** and **Version** for **Static File Expression**).	N/A
Detection rules do not detect the registry key **Binary Value** while determining whether a specific instance of a software application is installed on a client computer.	N/A
Applicability rule for a software resource does not work, when re-importing the software resource using the Replicator tool on a different Notification Server, after the initial rule is changed.	N/A
Unable to generate a command line for a package from a Software Library. If the Software Library is specified as a source for a package containing large files, while editing an existing software resource, the command lines are not generated for this software resource.	N/A
Software discovery creates second software resource for a software resource that is imported from MSI. If after running the Software Discovery task or gathering software inventory, Software Catalog duplicates previously imported software resources as newly discovered software resources, this means, that the corresponding imported MSI files contained different software keys. Workaround: To fix the issue, run the Merge Duplicate Resources scheduled task. If this task does not fix all issues, merge the software resources manually.	N/A
If you run a Detailed Export for a software resource, which has a "conflicts with" association, then this association is not displayed after importing the resource from the XML file.	N/A

Symantec Endpoint Management Workspaces 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 1-59 Known issues for Symantec Endpoint Management Workspaces

Issue	Article link
Internet Explorer security settings may prevent downloading the HTML fonts that are required for Symantec Endpoint Management Workspaces. As a result, the pages style (fonts and icons) may be displayed incorrectly in the Symantec Endpoint Management Workspaces console. To resolve the issue, enable the **Font download** option in Internet Explorer options.	

Workflow 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 1-60 Known issues for Workflow Solution

Issue	Article link
Workflow Service stops after upgrade from 8.0.HF6 to 8.5.	N/A
Microsoft Edge Reading view is not supported. Use the normal mode to view Process Manager and Workflow pages	N/A
Access denied error is displayed while opening project packages containing some DLL files that were created in the earlier build. Workflow Solution fails to copy or create the DLL files in the customlib directory. Workaround: For the logged in user, manually grant access to the Symantec install directory.	N/A
If the base URL contains hostname, the published web form does not open in the Microsoft Edge browser. Workaround: Open the URL in Internet Explorer 11 or use that fully qualified hostname, IP address, or localhost in the base URL.	N/A
After an off-box upgrade to Symantec Management Platform 8.5, the older projects cannot be republished from Workflow Designer. This is because the default **Local SMP** environment has information about the older SMP server. Workaround: To resolve this issue, delete the old SMP server from SMP, manually register the new Workflow Server, and add the new server to the **Local SMP** environment. Republish the project from Workflow Designer.	N/A

Table 1-60 Known issues for Workflow Solution *(continued)*

Issue	Article link
After an off-box upgrade to Process Manager 8.1, the existing AD synchronization might not run because the background server in the Process Manager master setting has information about the older Process Manager server. Workaround Delete the old background server and manually add the new server to the background server from the Process Manager settings and then restart IIS.	N/A

Other things to know about Client Management Suite 8.5 solutions and components:

- Symantec Management Platform
- IT Analytics
  See "Other things to know about IT Analytics" on page 79.
- Patch Management Solution
  See "Other things to know about Patch Management Solution" on page 80.
- Software Management Solution
  See "Other things to know about Software Management Solution" on page 80.

Other things to know about Symantec Management Platform

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

Things to know are separated into the following components:

- Notification Server
  See Table 1-61 on page 76.
- Task server
  See Table 1-62 on page 77.
- UNIX/Linux/Mac
  See Table 1-63 on page 78.
- Network Discovery
  See Table 1-64 on page 79.
- Data Connector
  See Table 1-65 on page 79.

- SymHelp
  See Table 1-66 on page 79.

Table 1-61 Things to know about Notification Server

Information	Article link
Check the allowed protocols on site server before disabling any in a communication profile. For example, if you disable TLS 1.0 in the communication profile but do not enable TLS 1.1 or TLS 1.2 on Notification Server or site servers, the agent loses connectivity.	N/A
If menu items in the Symantec Management Console are not shown or not clickable, make sure that the FQDN used in the console URL is not in the **Restricted sites** list in the Internet Explorer settings.	N/A
When you perform an off-box upgrade, the FQDN of the old server and the new server differs. To maintain the connectivity of the agents after the upgrade, Notification Server automatically updates the default communication profile of the old server with the FQDN of the new server. After this change, the communication profile of the old server will remain available, but all references to it are switched to the communication profile of the new server. The agent settings that point to the custom communication profile are not changed during the upgrade process.	N/A
Default times for differential replication and for the **NS.Daily** schedule do not allow to perform Differential or Complete replications within the same night. Default **NS.Daily** schedule, which collects summary data is set to run every day at 02:10 AM. By default, the differential replication is set to run every day at 01:00 AM, Complete replication runs at 2:00 AM. This means that the summary data for a given day is replicated on the next day. To replicate the summary data on the same day it is collected, change the time for the **NS.Daily** schedule to run before the replication starts.	N/A
In hierarchy, the **Source** field in **Resource Manager** always indicates Notification Server from which the client computer was replicated. Server field is used to indicate Notification Server that the client computer reports to.	N/A

Table 1-61 Things to know about Notification Server *(continued)*

Information	Article link
The package server uses ACLs to restrict access to the folders and files that it owns. Installation of the package server on a file system without ACLs implementation is supported, but not recommended. The following file systems do not include the ACL functionality: ▪ UFS ▪ FAT ▪ VFAT ▪ FAT32	N/A
If you attempt to upgrade across collations, the database reconfiguration fails with the following error message: Cannot resolve the collation conflict. The database and the database server collations must match. This function is by design: Symantec Management Platform does not support upgrading across different collations.	N/A
The user name for the Symantec Management Agent ACC cannot include any special characters	N/A

Table 1-62 Things to know about Task Server

Information	Article Link
If you replicate a task with **system** attribute from parent Notification Server to its child and run this task on a child Notification Server's client computer, the task will not run and its status will be marked as **Failed**.	N/A
When you create a **Client Task Schedule** policy on parent Notification Server and replicate it to a child Notification Server, the schedule of this policy is not always displayed on the **Client Task Schedule** policy page of the child Notification Server. The schedule of the policy is only displayed, when you open the default view of the **Client Task Schedule** policy page. After you make changes under **Policy Status**, in the **View** drop-down list, the schedule of the policy disappears. However, the policy runs successfully by schedule.	N/A
If a computer is in a workgroup environment then some tasks (for example **Delete Temporary Files**) advanced settings require the user name in full format, *computer_name\user_name*.	N/A
Installation of a Task Server on a Microsoft domain controller is not supported. Installation of a Package Server on a Microsoft domain controller is not supported.	HOWTO59071

Table 1-62 Things to know about Task Server *(continued)*

Information	Article Link
For Notification Server to run properly, you must be able to install (or be prompted to install) ActiveX objects. If your Internet Explorer settings prevent the ActiveX control from running, you see errors when you work with jobs and tasks. This function is by design.	N/A
This error occurs even though the **Show Script in a Normal Window** option is selected. The cause of this error may be a new Windows 2008 security feature called "Session isolation".	N/A

Table 1-63 Things to know about UNIX/Linux/Mac

Information	Article Link
Linux package servers do not support certificate management in the Symantec Management Console, on the **Certificate Management** page. You must manually manage the certificates on Linux package servers.	N/A
When you push-install the Unix/Linux/Mac agent onto the HP-UX computers that have CSH set as boot-shell for root, links to the agent's binaries location (commands) are created. However, on systems such as HP-UX ia64 11.23-11.31, these binaries or commands cannot be executed in user sessions. In this case, you must specify the absolute path.	N/A
If you attempt to push-install the Symantec Management Agent for UNIX, Linux, and Mac to a computer system that has a secondary shell that is configured in .profile, the installation may fail. The failure is due to a timeout error. The secondary shell is any shell other than the configured shell in `/etc/passwd` for user root in `/etc/profile`, `.profile`, or `.bash_profile`.	N/A
When you import a .bz2 package into a software component, the command line for installing this package is generated automatically. While this command line works on Linux and Mac computers, it may not work on some HP-UX systems. In this situation, you must manually adjust the command line.	N/A
A package server configuration has an **Alternate Download Location** option. With a Linux package server, you can set this option with a Windows-style path. The path is then converted to a UNIX-style path; for example, `C:\path\` becomes `/path/`. However, a trailing slash is required for proper conversion. If you omit the trailing slash as in `C:\path`, then the path is not converted correctly.	N/A

Table 1-64 Things to know about Network Discovery

Information	Article Link
Symantec Management Platform supports only **Universal Groups** for the cross-domain Active Directory import. Other group types are not supported.	N/A
Use connection profiles to configure the protocols that are used to communicate with network devices.	HOWTO9348
You can set up Symantec Management Platform Security Privileges.	DOC1740
If you schedule a Network Discovery task to run on a recurring basis, you cannot stop that task unless you perform one of the following actions: ■ Delete the task. ■ In the console, under **Manage > Jobs and Tasks**, delete the next scheduled occurrence of the task. This action cancels the schedule.	N/A

Table 1-65 Things to know about Data Connector

Information	Article link
When you import subnets or computers with Data Connector, make sure that you use the following resource lookup keys: ■ For subnets, use **Subnet/Subnet Mask** lookup key. ■ For computers, use **Computer Name/Domain** lookup key.	HOWTO95681 HOWTO95682

Table 1-66 Things to know about SymHelp

Information	Article link
When SymHelp contains the content that can be accessed through HTTP or HTTPS protocols, by default, the Internet Explorer displays only secured content, thereby blocking all unsecured content. To let Internet Explorer display the blocked SymHelp content, go to browser security settings and enable the mixed content display.	kb/2625928 ee264315

Other things to know about IT Analytics

The following are the things to know about this release.

Table 1-67 Other things to know about IT Analytics

Description
In Client Management Suite 8.5, IT Analytics (version is 8.1.3000) is released with minor bug fixes and performance improvements.

Table 1-67 Other things to know about IT Analytics *(continued)*

Description
An IT Analytics mind map is available online. To view the map, follow the link: Analysing your data using IT Analytics

Other things to know about Patch Management Solution

The following are the things to know about this release.

Table 1-68 Other things to know about Patch Management Solution

Issue	Description
The **Windows System Assessment Scan** package returns **1** in case of success.	In the Symantec Management Agent user interface, the successful exit code for the **Windows System Assessment Scan** package is **1**.
Download progress data location for a Windows update policy.	When you enable the software update policy that uses Windows Update Agent to perform the download and installation of a software update, the status dialog box can display the update in the **Downloading** state for a long time. You can view the download progress and other transaction information in the Windows Update Agent log file at `%`*`windir`*`%\Windowsupdate.log`
Restart and delivery data loss after the upgrade to the latest version of Notification Server.	When you re-target the client computers from the Notification Server version earlier that 8.0 to the latest version of Notification Server, the information about the restart and delivery status of the Symantec Management Agent is lost. For more information, see the KB article INFO3179.
Restart Required to Complete Installation automation policy.	This automation policy generates a report and sends an email if a client computer needs to be restarted to complete the software update installation. This policy only works with Symantec Management Agent 8.0 and later. Older Symantec Management Agent versions are not supported.

Other things to know about Software Management Solution

The following are the things to know about this release.

Table 1-69 Other things to know about Software Management Solution

Issue	Description
Replicating custom icons for software resources with Software Resource Replicator.	You can export a software resource and its metadata to a detailed XML file and replicate the software resource on another Notification Server computer by importing the XML file to that computer. However, you need to use the Software Resource Replicator utility to export the software resource together with its custom icon. The exported icons are stored in the subfolder of the root export folder **AppIcons**. The imported icons are stored at `C:\Program Files\Altiris\SoftwareManagement\Web\AppIcons`. For more information about replicating software resources with Software Resource Replicator, see the following knowledge base article: https://www.symantec.com/docs/TECH166711
The default number of open software requests per user is 1000.	The default number of open software requests per user is 1000. The Software Portal Administrator can change this number in the **NS Configurator** tool as follows: 1. Run the **NS Configurator** tool that is located at `Program Files\Altiris\Notification Server\Bin\Tools`. 2. In the **NSConfigurator** dialog box, navigate to **Core Settings > Software Portal > SoftwarePortalMaxOpenRequestsPerUser**. 3. In the **Value** field, type the number of requests that a user can have open simultaneously, and then click **Save**. Note that a Managed Software Delivery policy that contains dependencies or multiple tasks counts as one request.
Execution Status report has been modified to filter the tasks by name.	**Execution Status** report has been modified to filter the tasks by name if the **Only most recent for Computer** option is selected in the **Software Delivery Instances to Include** drop-down list.
Old **AddRemoveProgram** data class entries are displayed in the Resource Manager after the corresponding software is upgraded on the client computers.	If a client computer software, for which the data is already gathered by the **Collect full inventory** task, is upgraded, old entries in the AddRemoveProgram data class are visible in the Resource Manager, even after running the **Collect full inventory** task on this client computer. Workaround: To fix the issue, run the **Collect full inventory** task on this client computer once again.

Table 1-69 Other things to know about Software Management Solution *(continued)*

Issue	Description
Java Update software component is not added into the Software Catalog after running the Software Discovery task.	Java 6 Update software component, which is installed on the client computer, is not added into the Software Catalog after running the Software Discovery task. This happens, because Java 6 Update software component has association with Java(TM) 6 Unmanaged software product, which is added by the Inventory Solution.
If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails.	If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails. The reason the installation fails is that the software starts to install while a user logoff is still pending.
The support of **Run from server if bandwidth is above some speed** setting is limited in CEM mode.	The usage of this setting on Internet-managed client computers is limited as follows: ▪ If the setting is enabled for a Quick Delivery task or a Package Delivery task, these tasks will fail with timeout error, unless the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached. ▪ If the setting is enabled for a Managed Delivery policy, the policy will not run, until the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached.
Computers in CEM mode cannot be turned on if necessary.	The **Power on computers if necessary** compliance setting is not supported for Internet-managed client computers due to limitations of remote power management technology.
Managed Software Delivery policies and Quick Software Delivery tasks execution requires Symantec Management Agent upgrade.	Due to significant changes in this component, Symantec Management Agent has to be upgraded to version 7.5 in an environment with hierarchy, to execute Managed Software Delivery policies and Quick Software Delivery tasks
Source Path Update execution requires Symantec User credentials.	Source Path Update will only work under Symantec User Credentials.

Table 1-69 Other things to know about Software Management Solution *(continued)*

Issue	Description
The status of the Quick Delivery tasks for software resources with EXE files, which contain MSI packages, does not reflect the status of the embedded MSI package installation.	Tasks and policies allow you to use software packages with EXE executable files, which contain MSI components. The logic behind such tasks only monitors the execution of the initial EXE file, which calls the MSI component. Once the embedded MSI is triggered, the result of the task or policy is considered to be successful. This may lead to confusing situations, in case the embedded MSI file fails to complete, particularly, when you use Quick Delivery tasks, which do not utilize detection checks. For example, if you try to install an executable with Adobe Reader in silent mode, using a Quick Delivery task on a client computer running Windows 7 Embedded, the installation may fail, without returning an error code, while the Quick Delivery task status returns successful completion of the executable file. Symantec recommends you to use MSI software packages instead of EXE files and policies with detection checks instead of Quick Delivery tasks, where possible, to make sure receive accurate and detailed information about the software installation process.
Tasks and policies may fail to access UNC source locations in complex network environments..	Windows Installer Repair task, Quick Delivery task, Package Delivery task and Managed software delivery policy may fail to access the UNC source location, which contains the software package, in an environment, where Notification Server, package server and client computers do not reside in the same domain. To ensure access to such packages, use the agent connectivity credential to connect to download resources. For more information setting up access to the Package Server, see the *Enabling access to a package at a UNC source location* section in the *IT Management Suite Administration Guide*.

Where to get more information

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

Table 1-70 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**.
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 1-71 Symantec product information resources

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

Table 1-71 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