Symantec™ Management Platform 8.5 Release Notes

Symantec™ Management Platform 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.

Knowledge Base Articles and Symantec Connect

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

https://support.symantec.com

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

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

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

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

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

To contact Symantec Support, see:

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

Symantec Management Platform 8.5 Release Notes

This document includes the following topics:

About Symantec Management Platform

The Symantec Management Platform provides a set of services that IT-related solutions can leverage. Solutions plug into the platform and take advantage of the platform services, such as security, reporting, communications, package deployment, and Configuration Management Database (CMDB) data. Because solutions share the same platform, they can share platform services as well as data. Shared data is more useful than data that is only available to a single solution.

For example, one solution collects data about the software that is installed on company computers and another solution uses the data to manage software licenses. A third solution can also use this data to help you update software. This close integration of solutions and the platform makes it easier for you to use the different solutions because they work in a common environment and are administered through a common interface.

The platform provides the following services:

- Role-based security
- Client communications and management
- Execution of scheduled or event-triggered tasks and policies
- Package deployment and installation
- Reporting
- Centralized management through a single, common interface
- Configuration Management Database (CMDB)
- Software Management Framework

When you install a solution or suite, the platform is also installed if it is not already installed.

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 1-1 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
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

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

Feature	Description
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 1-2 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 1-2 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 (incl. Core) 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 1-2 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 1-2 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 1-2 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 1-2 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 1-2 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 1-2 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.

System requirements and supported platforms

Before you install Symantec Management Platform 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 Symantec Management Platform 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 Symantec Management Platform 8.5

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 Symantec Management Platform 8.5

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

The following upgrade scenarios are supported:

- From Symantec Management Platform 8.0 HF6 to Symantec Management Platform 8.5
- From Symantec Management Platform 8.1 RU7 to Symantec Management Platform 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 Symantec Management Platform 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 Symantec Management Platform 7.5
2. Apply Symantec Management Platform 7.5 HF6
3. Upgrade to Symantec Management Platform 7.5 SP1
4. Apply Symantec Management Platform 7.5 SP1 HF5
5. Upgrade to Symantec Management Platform 8.0
6. Apply Symantec Management Platform 8.0 HF6
7. Upgrade to Symantec Management Platform 8.5

For detailed instructions on migrating to Symantec Management Platform 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 Symantec Management Platform 7.5 SP1 HF5 to Symantec Management Platform 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

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 1-3 on page 16.
- Task Server
  See Table 1-4 on page 16.
- Symantec Management Agent
  See Table 1-5 on page 16.
- ASDK
  See Table 1-6 on page 16.
- Security Cloud Connector
  See Table 1-7 on page 16.

Note: The issues that were fixed within release updates 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

Table 1-3 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 1-4 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 1-5 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 1-6 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 1-7 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

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 1-8 on page 17.
- Notification Server
  See Table 1-9 on page 18.
- Task server
  See Table 1-10 on page 19.
- Symantec Management Agent
  See Table 1-11 on page 23.
- UNIX/Linux/Mac
  See Table 1-12 on page 25.
- Network Discovery
  See Table 1-13 on page 26.
- Pluggable Protocol Architecture (PPA)
  See Table 1-14 on page 27.
- ASDK
  See Table 1-15 on page 28.
- Security Cloud Connector
  See Table 1-16 on page 28.

Table 1-8 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 1-9 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 1-9 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 1-10 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 1-10 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 1-10 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 1-10 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 1-10 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 1-11 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 1-11 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 1-12 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 1-12 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 1-13 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 1-13 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 1-14 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 1-15 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 1-16 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

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 1-17 on page 29.
- Task server
  See Table 1-18 on page 30.

- UNIX/Linux/Mac
  See Table 1-19 on page 31.
- Network Discovery
  See Table 1-20 on page 32.
- Data Connector
  See Table 1-21 on page 32.
- SymHelp
  See Table 1-22 on page 32.

Table 1-17 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

Table 1-17 Things to know about Notification Server *(continued)*

Information	Article link
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
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 1-18 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

Table 1-18 Things to know about Task Server *(continued)*

Information	Article Link
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
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 1-19 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 1-20 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 1-21 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 1-22 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

Where to get more information

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

Table 1-23 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	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 1-24 Symantec product information resources

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

Table 1-24 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