Symantec™ Management Platform 8.1 Release Notes

Symantec™ Management Platform 8.1 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

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

support.symantec.com

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Symantec Management Platform 8.1 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 8.1, the following new features are introduced:

Table 1-1 List of new features

Feature	Description
Expanded list of supported platforms for CMDB.	The following version(s) of Microsoft® SQL Server® are now supported for the Configuration Management Database (CMDB): ▪ SQL Server® 2012 SP3 ▪ SQL Server® 2014 SP2 ▪ SQL Server® 2016

Table 1-1 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: ■ CentOS 6.0 - 6.8 and CentOS 7.0 - 7.2 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/DOC9725 ■ AIX 7.1 TL4 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125360 ■ macOS 10.12 Sierra For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125347 ■ RHEL 6.7 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/DOC9268 ■ RHEL 6.8 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125430 ■ RHEL 7.2 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO124979 ■ Solaris 11.3 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO124985 ■ SUSE Linux Enterprise 12 SP1 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO124980 ■ Windows 10 Anniversary Update 1 (Windows 10, version 1607) For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125345 ■ Windows Server 2016 For the list of supported solutions and limitations, refer to: http://www.symantec.com/docs/HOWTO125454

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

Feature	Description
Peer-to-peer downloading.	The peer-to-peer downloading feature lets you download and distribute the software delivery and patch packages to Windows computers. It minimizes the software delivery time and provides you with a reliable software delivery to all endpoints. The peer-to-peer downloading feature significantly reduces the load on the network and the IT Management Suite infrastructure. For more information about peer-to-peer downloading, see the knowledge base article at the following URL: http://www.symantec.com/docs/DOC9473
Data migration between different versions of Symantec Management Platform.	Standalone replication and data export/import is now supported between Notification Servers that have different versions of IT Management Suite installed. Note that you can only replicate or export/import data from IT Management Suite version 7.6 HF7 or version 8.0 HF6 to IT Management Suite 8.1. For more information about data migration, see the knowledge base article at the following URL: http://www.symantec.com/docs/DOC9586
The licenses in SLIC format are now supported.	The licensing for ITMS functions now as follows: ■ The licenses in SLIC format are only supported for ITMS version 8.1. The import of SLIC license files for ITMS versions earlier than 8.1 is rejected. ■ Applying new SLIC license overwrites the existing legacy licenses. Note that even valid legacy licenses get overwritten. If you need to extend the node count for current legacy license for 8.1 product, Symantec issues a replacing SLIC license with new extending licenses. For example, if you want to extend license from 300 to 400 nodes - you get replacing SLIC license for 300 nodes and additional license for 100 nodes. ■ If multiple license files are applied for a single solution, each SLIC license is displayed in a separate row. ■ Adding new SLIC license on top of existing valid SLIC license adds nodes to the sum of allowed nodes. If you have any questions about SLIC licenses, contact the Symantec Customer Care.

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

Feature	Description
Mac OS Profile Management.	Mac OS Profile Management feature lets you import Mac configuration profiles and enforce them by implementing policies. Configuration profiles let you configure settings such as email settings, network settings, or distribute certificates to Mac computers. **Note:** This feature is only available if you install Client Management Suite 8.1 For more information about Mac OS Profile Management, see the knowledge base article at the following URL: http://www.symantec.com/docs/HOWTO125782
New features in SIM.	SIM introduces the following new features: ■ To increase security, XML signing for PL is implemented. Note that no limitations to functionality apply, only warning is displayed. ■ Database configuration has been moved from Symantec Management Console to SIM. This helps to troubleshoot database issues even when the Console is inaccessible. ■ Performing full repair is implemented. Full repair verifies the connection to the CMDB, repairs the installation errors, and reconfigures the installed solutions and components. ■ Repairing MSI-s and reconfiguring installed solutions is moved to separate pages to simplify the user interface.
Enhancements of target selector for policies and tasks.	■ From the **Apply to** menu, you can access to the recently used targets. ■ Saved targets are re-usable and editable by users with the same scope of access. ■ It is possible to view and edit the target scoping. ■ For computers target, you can include or exclude the unmanaged computers.
Prerequisites displayed for Task Service and Package Service.	In the **Add/Remove Services** dialog box, you can now right-click the service and view the list of prerequisites for installing this service.
UI enhancements on the **Site Server Settings** page.	The following changes have been made on the **Site Server Settings** page: ■ Task Server with version older than the version of Task Management installed on Notification Server has now status **Warning/Required Upgrade**. ■ Major information about the Task Server is now displayed under **Task Service** section. ■ Right-click menu now works similarly to other Symantec Management Console pages.

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

Feature	Description
UI enhancements in **Security Role Manager** and on the **Automation Policies** page.	The following changes have been made in **Security Role Manager**: ■ Enhanced **View** and **Search** options to simplify finding the required item. ■ Extended layout to provide more information for the selected item. The following changes have been made on the **Automation Policies** page: ■ The state of each automation policy is indicated more clearly. ■ New system messages available. ■ New override and filtering options for system messages.
Added possibility to select multiple tasks when creating a job.	When you create a job and add tasks to it, you can now select multiple tasks at once by holding down the **Ctrl** key.
Possibility to prevent computer from going into sleep mode while task runs.	If a computer goes to sleep mode while a task runs on it, the task will fail. To fix this issue, you can now prevent the computer from going to sleep mode by enabling the **Prevent the computer from going into sleep mode while the tasks run** option at the following locations: ■ On the **Task Agent Settings** page (global settings) ■ In the advanced options dialog box, on the **Task options** tab, of a client task. Note that for **Defragment Computer** task, this option is enabled by default.
Non-English job's conditions now work with localized **True/False**.	It is now possible to use localized **True/False** strings in job’s conditions and they function as expected. Note that the change affects only the jobs that are created after the upgrade. The jobs that are created before the upgrade will function as previously.
Search in **Create New Task** and **Select Task** dialog box.	In the **Create New Task** dialog box and **Select Task** dialog box, it is now possible to use search.
New configuration option is added to the **Cleanup Task Data** task.	In the environment with high task load, the **Cleanup Task Data** task may remove the task instances of the recently executed tasks. As a result, some task instances might be missing and the summary information for that task may be incorrect. To avoid this problem, you can now enable the **Minimum time period to keep the task instances/summaries** option. If you enable this option, the **Cleanup Task Data** task will not remove the task records that are newer than the defined time period.

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

Feature	Description
The defer dialog box for the tasks is redesigned.	After you enable the option **Allow the user to defer execution of this task** in the Symantec Management Console, a defer dialog box is displayed on the client computer that allows the user to postpone the task. This defer dialog box is now redesigned. The redesign addresses multiple stability and usability issues.
Added ability to assign multiple packages to specific Package Servers.	On the **Packages** page, you can select multiple packages and assign these packages simultaneously to all Package Servers or to specific Package Servers.
Altiris Client Task Server Agent plug-in has been optimized.	As a result of optimization, the 32-bit version of the `CTServerAgent.dll` is not installed on a 64-bit operating system. In the Symantec Management Agent UI, on the **Agent Settings** tab, under **Agents/Plug-ins**, only one record is displayed for the Altiris Client Task Server Agent plug-in.
New **Client Task Status Details** report is available.	The new **Client Task Status Details** report displays details of a specific task or job. For example, you can view the list of computers on which this task or job was launched. To access the report, double-click any task or job item in the **Job/Task Status Detail** report. The **Job/Task Status Detail** report is located in the Symantec Management Console, at **Reports > Task Server > Status > Job/Task Status Detail**.
New reports are introduced on internal health indication.	The following new reports are available: ▪ **Notification Server Processes Statistics** report This report shows the statistics of the Altiris processes for this Notification Server. You can drill down each record to see the detailed resource usage data of an Altiris process within certain time range. ▪ **Client Configuration Policy Statistics** report This report shows the history of the policies requests that the managed computers have made on this Notification Server.
Added possibility to generate bootstrap files using the custom configuration XML.	You can now also apply custom settings to ULM agent pull installation packages and to ULM agent Cloud-enabled installation packages using the custom configuration XML.
Added possibility to perform actions on multiple items in the search results list.	In the Symantec Management Console, you can now select multiple items in the search results list and perform actions on them. For example, you can select multiple policies in the search results list, and then enable or disable them at once.

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

Feature	Description
Redirecting 8.0 HF1 Mac agents to 8.1 Notification Server.	Starting from ITMS version 8.0HF1, you can use Communication Profiles to redirect cloud-enabled Mac agents to Notification Server 8.1. For more information about restoring Cloud-enabled Management communication on Mac computers after an off-box upgrade, see the *IT Management Suite 8.1 Installation and Upgrade Guide*: http://www.symantec.com/docs/DOC9500
Smart Card Authentication for Symantec Management Console.	For more information about how to configure Smart Card Authentication for Symantec Management Console, see the following knowledge base article: http://www.symantec.com/docs/DOC9334

System requirements and supported platforms

Before you install Symantec Management Platform 8.1, read the **Hardware recommendation** chapter in the *IT Management Suite 8.1 Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC9470

For information about the supported operating systems in Symantec Management Platform 8.1 and the Symantec Management Platform 8.1 solutions, 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 8.1

For more information on how to install and configure the product, see the *IT Management Suite 8.1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC9500

Upgrade to Symantec Management Platform 8.1

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 7.6 HF7 to Symantec Management Platform 8.1

- From Symantec Management Platform 8.0 HF6 to Symantec Management Platform 8.1

For more information on how to upgrade the product, see the *IT Management Suite 8.1 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC9500

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 8.1

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 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:

- Notification Server

See Table 1-2 on page 15.

- Task server
  See Table 1-3 on page 17.
- Symantec Management Agent
  See Table 1-4 on page 22.
- UNIX/Linux/Mac
  See Table 1-5 on page 23.
- Network Discovery
  See Table 1-6 on page 25.
- Pluggable Protocol Architecture (PPA)
  See Table 1-7 on page 26.
- ASDK
  See Table 1-8 on page 27.
- ITMS Management Views
  See Table 1-9 on page 27.
- Security Cloud Connector
  See Table 1-10 on page 27.

Table 1-2 Known 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. **Workaround:** Manually apply the custom site server certificate newly after the upgrade. Take the following steps: 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**. 2 In the left pane, expand **Notification Server > Site Server Settings**, and then click **Global Site Server Settings**. 3 On the **Global Site Server Settings** page, under **Certificates Rollout**, click the master certificate. 4 In the **Select Certificate** dialog box, click the custom certificate that was applied to the site servers before the upgrade, and then click **OK**.	N/A
When you replicate custom task with custom password from ITMS 7.6 HF7 v10 server to ITMS 8.1 server with FIPS enabled, the replication fails with the following error in the log: "**Unable to decrypt credentials, in case of migration please check that KMS keys were also migrated from old NS.**" **Workaround:** Disable FIPS on ITMS 8.1 server and replicate the required data.	N/A

Table 1-2 Known issues for Notification Server *(continued)*

Issue	Article link
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
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

Table 1-2 Known issues for Notification Server *(continued)*

Issue	Article link
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 1-3 Known issues for Task Server

Issue	Article link
The information on the right pane of the **Task Version History** dialog box is not displayed properly. Note that this problem appears after installing the Microsoft security update KB4012216.	
During the upgrade to ITMS 8.1, 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
User-based targets are visible and can be added to the tasks that do not support these targets.	N/A

Table 1-3 Known issues for Task Server *(continued)*

Issue	Article link
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
In 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 4.6 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 8.1.	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 8.0 and enable FIPS, the task that contains encrypted data fails on the clients that are not upgraded to 8.0. 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 1-3 Known issues for Task Server *(continued)*

Issue	Article link

When you upgrade your remote task server, Windows installs multiple updates for Microsoft Framework. Installation of the Framework updates may cause the remote task server to become non-functional and the clients are not able to register to that server.
Workaround: To resolve this issue, run the following command:
`aspnet_regiis.exe /iru`
The `aspnet_regiis.exe` file can be found at one of the following locations:
`%windir%\Microsoft.NET\Framework\v4.0.30319`
`%windir%\Microsoft.NET\Framework64\v4.0.30319` (on a 64-bit computer)
	N/A

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

Table 1-3 Known issues for Task Server *(continued)*

Issue	Article link
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
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

Table 1-3 Known issues for Task Server *(continued)*

Issue	Article link
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
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 1-4 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
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

Table 1-4 Known issues for Symantec Management Agent *(continued)*

Issue	Article link
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
On client computers with Internet Explorer 10 installed, Symantec Management Agent help might not be properly formatted. For example, images are not displayed.	HOWTO95650
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 1-5 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

Table 1-5 Known issues for UNIX/Linux/Mac *(continued)*

Issue	Article link
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

A custom command metric with the following command line returns an incorrect value on SLES 10:
`ps -ef | grep -v 'grep' | grep -c -i -w "chssrvInfoServerapp01mgtNode01Cell"`
The value that is returned when executed within the OS shell is "1," but the metric returns a value of "0." This value is to monitor if a process is running, but something interferes with the command execution of the metric. The cause is a character limitation of 32 characters of the desired process name (not a character limitation of the entire command-line syntax).
The command returns either a "1" or a "0"; therefore, the character length of the process name should not be an issue, but it is.
If you configure the command line of the metric as follows, it returns the correct value:
`ps -ef | grep -v 'grep' | grep -c -i -w "chssrvInfoServerapp01mgtNode01Ce"`
Note: This issue does not appear to exist on RHEL computers.
	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 after you restart the client system.	N/A

Table 1-5 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 1-6 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 1-6 Known issues in Network Discovery *(continued)*

Issue	Article link
In the Symantec Management Console, when you enter into **Maximum number of threads per discovery task** field different value than 1-99, a warning message is displayed. Regardless of the Symantec Management Console language, that warning message is always in English.	N/A
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 1-7 Known issues in Pluggable Protocol Architecture (PPA)

Issue	Article link
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 1-8 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 1-9 Known issues in ITMS Management Views

Issue	Article link
When you navigate from the **Manage** menu to **Computers**, **Software**, **Policies**, or **Jobs/Tasks**, the section doesn't open if the name of Notification Server that you are connecting to contains non-alphanumeric characters.	N/A

Table 1-10 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

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:

- Symantec Installation Manager
  See Table 1-11 on page 28.
- Task Server
  See Table 1-12 on page 28.

Note: The issues that were fixed within hot fix releases for ITMS version 8.0 are not included in this document.

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

- ITMS 8.0 HF1
- ITMS 8.0 HF2
- ITMS 8.0 HF3
- ITMS 8.0 HF4
- ITMS 8.0 HF5
- ITMS 8.0 HF6

Table 1-11 Fixed issues for Symantec Installation Manager

Issue	Article Link
It is not possible to install Migration Wizard 8.0 using Symantec Installation Manager 8.1.	N/A

Table 1-12 Fixed issues for Task Server

Issue	Article Link
Client Task Agent causes GPF (Global Protection Fault) in Symantec Management Agent during the intensive processing of tasks and policies. The agent gets restarted automatically and usually the problem does not re-occur”.	N/A

If a task fails by timeout, in the **Task Instance Details** window, the following message appears:
`An unknown exception was thrown.`
When you click the **Show raw exception message** link, the following status appears:
`An unknown exception was thrown.`
`Task was cancelled.`
This issue does not affect any functionality.
	N/A

Table 1-12 Fixed issues for Task Server *(continued)*

Issue	Article Link
The following issues have been fixed on the **Tokens** page: ▪ Token queries are not saved if the token name contains space. ▪ If you click **Cancel** on the **Tokens** page, the SQL statement and the Token name are cleared. ▪ Existing token queries do not pass the SQL validation. ▪ It is not possible to delete a token or rename a token with an empty name. ▪ In token dialog box, the description of the token is not displayed. The **Tokens** page is available in the Symantec Management Console, at **Settings > Notification Server > Task Settings > Tokens**.	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 1-13 on page 30.
- Task server
  See Table 1-14 on page 31.
- UNIX/Linux/Mac
  See Table 1-15 on page 31.
- Network Discovery
  See Table 1-16 on page 32.
- Data Connector
  See Table 1-17 on page 33.
- SymHelp
  See Table 1-18 on page 33.

Table 1-13 Things to know about Notification Server

Information	Article link
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
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 1-14 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
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 1-15 Things to know about UNIX/Linux/Mac

Information	Article Link
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

Table 1-15 Things to know about UNIX/Linux/Mac *(continued)*

Information	Article Link
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
This issue is a system limitation that is caused by Mac OS 10.6 operating system design, and it cannot be overridden. This limitation may affect the commands that SWD/SMF tasks execute, or it may affect Script tasks.	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 1-16 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 1-17 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 1-18 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, do the following: ■ Go to browser security settings and customize it to 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 1-19 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: http://www.symantec.com/business/support/index?page=products 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: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.

Table 1-19 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ▪ Click the page and then press the F1 key. ▪ Use the Context command, which is available in the Symantec Management Console on the **Help** menu.

In addition to the product documentation, you can use the following resources to learn about Symantec products.

Table 1-20 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	https://support.symantec.com/en_US.html
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.	http://help.symantec.com/Welcome?context=ITMS8.1

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

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management/forums/endpoint-management-documentation The links to various groups on Connect are as follows: - Deployment and Imaging http://www.symantec.com/connect/groups/deployment-and-imaging - Discovery and Inventory http://www.symantec.com/connect/groups/discovery-and-inventory - ITMS Administrator http://www.symantec.com/connect/groups/itms-administrator - Mac Management http://www.symantec.com/connect/groups/mac-management - Monitor Solution and Server Health http://www.symantec.com/connect/groups/monitor-solution-and-server-health - Patch Management http://www.symantec.com/connect/groups/patch-management - Reporting http://www.symantec.com/connect/groups/reporting - ServiceDesk and Workflow http://www.symantec.com/connect/workflow-servicedesk - Software Management http://www.symantec.com/connect/groups/software-management - Server Management http://www.symantec.com/connect/groups/server-management - Workspace Virtualization and Streaming http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming