

# Symantec™ IT Management Suite 8.5 powered by Altiris™ technology Release Notes



# Symantec™ IT Management Suite 8.5 powered by Altiris™ technology Release Notes

## Legal Notice

Copyright © 2018 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and Altiris are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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](https://support.symantec.com/en_US/contact-support.html)

# IT Management Suite 8.5

This document includes the following topics:

- [About IT Management Suite](#)
- [What's new in this release](#)
- [System requirements and supported platforms](#)
- [General installation and upgrade information](#)
- [Known issues and fixed issues](#)
- [Where to get more information](#)

## About IT Management Suite

IT Management Suite from Symantec is a comprehensive, integrated suite. It promotes effective service delivery by reducing the cost and complexity of owning and managing corporate IT assets such as desktops, laptops, thin clients, and servers on heterogeneous platforms such as Windows, UNIX, Linux, and Mac.

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

## What's new in this release

In IT Management Suite 8.5 release, new features can be categorized into general enhancements in Symantec Management Platform and enhancements in the IT Management Suite solutions.

General enhancements and new features of Symantec Management Platform and the solutions of IT Management Suite 8.5 are as follows:

- Symantec Management Platform

- See [“What's new in Symantec Management Platform”](#) on page 5.
- Deployment Solution  
See [“What's new in Deployment Solution”](#) on page 13.
- Inventory Solution  
See [“What's new in Inventory Solution”](#) on page 14.
- IT Management Suite integrations  
See [“What's new in IT Management Suite integrations”](#) on page 16.
- ITMS Management Views  
See [“What's new in ITMS Management Views”](#) on page 17.
- Patch Management Solution  
See [“What's new in Patch Management Solution”](#) on page 17.
- Software Management Solution  
See [“What's new in Software Management Solution”](#) on page 19.
- Symantec Endpoint Management Workspaces  
See [“What's new in Symantec Endpoint Management Workspaces”](#) on page 23.
- Virtual Machine Management  
See [“What's new in Virtual Machine Management”](#) on page 24.
- Workflow Solution  
See [“What's new in Workflow Solution”](#) on page 24.

## 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	<p>The <b>Time Critical Management</b> 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.</p> <p><a href="#">About Time Critical Management</a></p>

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

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

**Table 1-2** List of new features

Feature	Description
Expanded list of supported platforms for CMDB.	<p>The following version of Microsoft SQL Server are now supported for the Configuration Management Database (CMDB):</p> <ul style="list-style-type: none"> <li>■ SQL Server 2016 SP1</li> <li>■ SQL Server 2016 SP2</li> </ul> <p><b>Note:</b> 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).</p>

**Table 1-2** List of new features (*continued*)

Feature	Description
Expanded list of supported platforms for Symantec Management Agent.	<p>The following operating systems are now supported for the installation of the Symantec Management Agent and solution plug-ins:</p> <ul style="list-style-type: none"> <li>■ Ubuntu (versions (14.04 LTS Trusty Tahr, 16.04 LTS Xenial Xerus and 17.04 Zesty Zapus) <a href="http://www.symantec.com/docs/HOWTO127014">http://www.symantec.com/docs/HOWTO127014</a></li> <li>■ Windows 10 Creators Update (version 1703) <a href="http://www.symantec.com/docs/HOWTO127016">http://www.symantec.com/docs/HOWTO127016</a></li> <li>■ Windows 10 Fall Creators Update <a href="http://www.symantec.com/docs/HOWTO127802">http://www.symantec.com/docs/HOWTO127802</a></li> <li>■ Windows 10 April 2018 Update <a href="http://www.symantec.com/docs/HOWTO128230">http://www.symantec.com/docs/HOWTO128230</a></li> <li>■ Windows Server 2016 (incl. Core) <a href="http://www.symantec.com/docs/HOWTO125454">http://www.symantec.com/docs/HOWTO125454</a></li> <li>■ SUSE Linux Enterprise Server 12 SP2 and SUSE Linux Enterprise Desktop 12 SP2 <a href="http://www.symantec.com/docs/HOWTO127018">http://www.symantec.com/docs/HOWTO127018</a></li> <li>■ SUSE Linux Enterprise Server 12 SP3 and SUSE Linux Enterprise Desktop 12 SP3 <a href="http://www.symantec.com/docs/HOWTO127910">http://www.symantec.com/docs/HOWTO127910</a></li> <li>■ Red Hat Enterprise Linux 6.9 and CentOS 6.9 <a href="http://www.symantec.com/docs/DOC10575">http://www.symantec.com/docs/DOC10575</a></li> <li>■ Red Hat Enterprise Linux 7.3 and CentOS 7.3 <a href="http://www.symantec.com/docs/HOWTO127035">http://www.symantec.com/docs/HOWTO127035</a></li> <li>■ Red Hat Enterprise Linux 7.4 and CentOS 7.4 <a href="http://www.symantec.com/docs/HOWTO127907">http://www.symantec.com/docs/HOWTO127907</a></li> <li>■ macOS High Sierra 10.13 <a href="http://www.symantec.com/docs/HOWTO127741">http://www.symantec.com/docs/HOWTO127741</a></li> </ul> <p>More information: <a href="#">Symantec IT Management Suite Platform Support Matrix</a></p>
Expanded list of supported platforms for site servers.	<p>Task service and package service are now supported on:</p> <ul style="list-style-type: none"> <li>■ Windows 10 Creators Update (version 1703)</li> <li>■ Windows 10 Fall Creators Update (version 1709)</li> <li>■ Windows 10 April 2018 Update (version 1803)</li> </ul> <p>All site services are now supported on:</p> <ul style="list-style-type: none"> <li>■ Windows Server 2016</li> </ul>

**Table 1-2** List of new features (*continued*)

Feature	Description
ITMS binaries for Mac are converted to 64-bit.	<p>The Symantec Management Agent for Mac and all plug-ins for Mac are converted to 64-bit binaries.</p> <p><a href="#">64-bit transition on macOS</a></p>
Enhancements of Internet gateway	<p>The following enhancements of Internet gateway are introduced:</p> <ul style="list-style-type: none"> <li>■ Internet gateway supports WebSocket protocol, allowing to perform real time management tasks on Cloud-enabled agents.</li> <li>■ One instance now supports 15,000 concurrent client connections.</li> <li>■ Dependency on Apache HTTP Server and OpenSSL has been removed.</li> <li>■ Internet gateway can report to multiple Notification Servers.</li> </ul> <p>For more information, see the following knowledge base article: <a href="https://www.symantec.com/docs/DOC11227">https://www.symantec.com/docs/DOC11227</a></p>
New features and enhancements in SIM.	<p>The following new features and enhancements are available in SIM:</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ You can now edit the credentials of the Apptidentity account in Symantec Installation Manager in case the access to Symantec Management Console is not possible due to lockout or expiration of Apptidentity.</li> <li>■ 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.</li> <li>■ A new <b>Recover NS Settings</b> option is displayed on the <b>Configure Notification Server</b> page when the <b>NsConfiguration</b> 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.</li> </ul>
Integrated page for managing certificates.	<p>The <b>Certificate Management</b> page combines both existing capabilities, like replacement of Site Server certificates, and new capabilities like:</p> <ul style="list-style-type: none"> <li>■ Renewal of CEM agent certificates</li> <li>■ Replacement of root certificate</li> <li>■ Replacement of website certificates</li> <li>■ Viewing and managing communication profile certificates</li> </ul>



**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.	<p>A Task Server communication profile lets you configure how Task Server communicates with Notification Server.</p> <p><a href="#">Configuring a Task Server communication profile</a></p>
New reports added to ITMS providing better visibility over various management aspects.	<p>The following reports are now available in the Symantec Management Console:</p> <ul style="list-style-type: none"> <li>■ The <b>Agent Connection Status</b> 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.</li> <li>■ The <b>ITMS Plug-in Status</b> 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 <b>Enable</b> option in the right-click menu lets you apply this policy from the report.</li> <li>■ The <b>Subnet to Site assignments</b> 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.</li> <li>■ The <b>Packages Distribution by Download Type</b> 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.</li> <li>■ After initiating the replacement of <b>NS web site</b> certificate, you can use the <b>Computers having (or without) a Certificate</b> report to check how many computers have received the new certificate and how many computers are still missing it.</li> <li>■ <b>Subnets with Affiliated Sites</b> and <b>Subnets with Affiliated Sites by Computer</b> provide information about the subnets.</li> </ul>

**Table 1-2** List of new features (*continued*)

Feature	Description
Enhancements in Task Management.	<ul style="list-style-type: none"> <li>■ A new <b>Clean up Task Schedules</b> task lets you disable or delete the schedules that have no occurrence in the future.</li> <li>■ In the advanced settings dialog box, on the <b>Task options</b> tab, the new <b>The task is succeeded if its return code is</b> option lets you override the default success return code by specifying a custom value.</li> <li>■ The <b>Fail Job if this Task fails</b> option lets you fail the job if a specific sub-task or sub-job within this job fails.</li> <li>■ When you schedule a task, you can now add a custom description to the task instance in the <b>Quick Run</b> section or in the <b>New Schedule</b> dialog box.</li> <li>■ A new option is added to the <b>Restart Computer</b> task that lets you restart only the computers that are pending restart.</li> <li>■ Added ability to export content of task-instance details into a XLS or HTML file.</li> <li>■ The new <b>Update task settings</b> option allows to change <b>Run as</b> settings for a script task type. This option is only available for <b>Symantec Administrators</b> role.</li> <li>■ In main task details dialogs, you can now press the <b>Esc</b> key to close the dialog.</li> </ul>
Ability to use command line for applying Notification Server Communication Profile to a client computer.	<p>You can now use command line to apply an Notification Server Communication Profile to the client computer.</p> <p>You can use the following options with <code>aexnsagent</code> command:</p> <ul style="list-style-type: none"> <li>■ <code>/importprofile:&lt;path&gt;</code> - lets you specify the path to the XML file of the profile</li> <li>■ <code>/profilepwd:&lt;pwd&gt;</code> - lets you specify the decryption password</li> </ul> <p>Note that you have to run the command on the client computer.</p>
New options for configuring peer-to-peer downloading.	<p>For peer-to-peer downloading, the following new options are available:</p> <ul style="list-style-type: none"> <li>■ <b>Maximum upload bandwidth</b> and <b>Maximum download bandwidth</b> options replace the <b>Maximum bandwidth</b> option. The <b>Maximum download bandwidth</b> option lets you specify the throttling value for peer-to-peer downloading which is independent from general throttling value.</li> <li>■ <b>Don't use peer-to-peer downloading</b> option lets you disable using the peer-to-peer downloading in certain cases.</li> <li>■ The new <b>File block download progress on peer</b> option lets you configure how often a peer should notify other peers about the package download progress.</li> </ul>

**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 <b>Targeted Agent Settings</b> policy with initial settings.	The ( <b>Initial Settings</b> ) 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 <b>Targeted Agent Settings</b> policy. For example, after a re-imaged client computer receives the ( <b>Initial Settings</b> ) policy with ACC, it can immediately connect to Task Server.
Symantec Management Console notifications.	<p>The bell icon is displayed in the top right corner of the Symantec Management Console in following cases:</p> <ul style="list-style-type: none"> <li>■ The IT Management Suite GA Product Listing changes</li> <li>■ A certificate is about to expire in 60 days</li> </ul> <p>By default, these notifications are displayed only to <b>Administrator</b> role.</p> <p>The <b>View Console Notifications</b> privilege lets you configure if the notifications are displayed in the Symantec Management Console.</p> <p><b>Note:</b> The notifications are informational only.</p>
Ability to separately configure time periods for retiring and deleting the computers in CMDB.	The <b>Purging Maintenance</b> 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.	<p>The <b>Data Class Summary Generator</b> page in the Symantec Management Console lets you manage the <b>Altiris.NS.StandardItems.DataClassSummaryGenerator</b> class. This class lets you aggregate an extensive data set in Configuration Management Database (CMDB) into a smaller data class content.</p> <p>For more information, see:</p> <p><a href="#">Creating Data Class Summary Generator</a></p>
Enhancements for managing targets.	<p>The following enhancements have been made for managing targets:</p> <ul style="list-style-type: none"> <li>■ To avoid situations in which modifications to a re-used target impact previously created policies, you can now clone targets in the target editor.</li> <li>■ 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.</li> </ul>

**Table 1-2** List of new features (*continued*)

Feature	Description
(Windows only) Enhancements of package delivery.	<p>The following enhancements are implemented in package delivery:</p> <ul style="list-style-type: none"> <li>■ <b>Block by block downloading</b> 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.</li> <li>■ <b>Block chain hash validation</b> 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.</li> </ul>
New default schedule for SQL defragmentation.	<p>In previous releases, the <b>NS.SQL defragmentation schedule.{cdcd50e9-1c42-402b-921c-8ad6c9ff0d34}</b> task is set to run only once by default and does not repeat anymore.</p> <p>After upgrading to IT Management Suite 8.5, the <b>NS.SQL defragmentation schedule.{cdcd50e9-1c42-402b-921c-8ad6c9ff0d34}</b> task has a new default schedule and runs as follows:</p> <ul style="list-style-type: none"> <li>■ If no custom schedule is specified, the task will run weekly <b>every Saturday at 12:00PM</b>.</li> <li>■ If a custom schedule is specified, the task will run according to the specified schedule.</li> </ul> <p>You can configure the schedule for this task in Task Scheduler.</p>
New hierarchy replication rule.	<p>The new default hierarchy replication rule <b>AD import Replication</b> replicates data for users and computers that are imported from Active Directory.</p> <p>By default, this rule is disabled.</p>
Ability to configure hierarchy replication mode.	<p>The <b>Replication mode</b> option lets you configure what kind of data the hierarchy replication rule should replicate.</p> <p>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.</p>
Item tracking.	<p>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.</p> <p><a href="#">Configuring global settings for item tracking</a></p>

**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 <b>Settings</b> menu, click <b>Notification Server &gt; Core Settings</b> .
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. <b>Note:</b> This option is available only if you have <b>Language Packs</b> 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 <b>Help &gt; About Symantec Management Console...</b> in the Symantec Management Console.
New features of ASDK.	The following enhancements are introduced in ASDK: <ul style="list-style-type: none"> <li>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: <b>TaskManagement.ExecuteTCMTask</b>, <b>TaskManagement.GetTCMTaskStatus</b>, <b>TaskManagement.GetTCMTaskResults</b>, <b>TaskManagement.GetTCMTaskResult</b>, and <b>ResourceManagementLib.PushPolicy</b>.</li> <li><b>CreateResourceTarget</b> method can now create a target in a custom folder if the <b>parentFolderGuid</b> element with custom folder's Guid is in target's source XML. If the <b>parentFolderGuid</b> element is not in source XML, the target is created in the root target folder.</li> </ul>

## What's new in Deployment Solution

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

**Table 1-3** List of new features

Feature	Description
WinPE support for Windows 10 1703, 1709, and 1803 versions.	Deployment Solution now supports WinPE for Windows 10 1703, 1709, and 1803 versions with limitations. For more details, refer to the following article. <a href="#">HOWTO126076</a>

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

Feature	Description
Driver Manager lets you upload.CAB archives	<p>Deployment Solution lets you upload drivers as .CAB archives. The following procedure lists the steps that you must follow to add drivers to the driver database:</p> <ul style="list-style-type: none"> <li>■ In the Symantec Management Console, navigate to Settings &gt; Deployment &gt; Driver Manager.</li> <li>■ In the <b>Driver Database Management</b> dialog box click the <b>Preboot</b> tab or <b>DeployAnywhere</b> tab.</li> <li>■ Click <b>Add</b>.</li> </ul> <p>For the complete procedure, refer to the following URL: <a href="http://help.symantec.com">http://help.symantec.com</a></p>
Improved support for cab archive.	Support for drivers upload in .cab archive for Deployment Solution is improved.
Imaging support for 4K native drives.	<p>You can now create an image of a computer with 4K native drive that has GPT partition and NTFS file system and deploy it on a computer with 4K native drive.</p> <p><b>Note:</b> The following scenarios are not supported:</p> <p>Deploying an image that is created from a 4k drive to a drive with 512 sector size.</p> <p>Deploying an image that is created from a drive with 512 sector size to a 4k drive.</p>
Improved performance of Boot Disk Creator.	The performance of the Boot Disk Creator is improved by reducing the time required to add preboot drivers and other packages while creating preboot packages for WinPE 5 and WinPE 10.
Support for iPXE	<p>Deployment Solution supports creating pre-boot configurations that can be deployed over HTTP.</p> <p><a href="#">TECH250831</a></p>
Support for Smart raw imaging	<p>Deployment Solution supports raw imaging for RHEL 7.2 and RHEL7.4 with XFS file system. When you capture an image, all the sectors are copied along with their offset on the disk.</p> <p>To capture an image using the Smart raw imaging feature, use the <code>-isr</code> switch in the <b>Create Image</b> task.</p>

## What's new in Inventory Solution

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

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

**Table 1-4** List of new features in Inventory Solution

Feature	Description
<p>New <b>Collect Time-Critical Inventory</b> policy.</p>	<p>Inventory Solution provides the <b>Collect Time-Critical Inventory</b> policy that gathers the most important hardware and software inventory data on client computers frequently during a day according to a schedule.</p> <p>You can also enable the policy option <b>Real-Time Inventory</b> that monitors the current software state and runs software inventory scan on client Windows computers in real time on certain events.</p>
<p>Ability to gather inventory data for Microsoft Application Virtualization (App-V) virtual applications and Microsoft Windows store applications.</p>	<p>You can now gather information about the following software:</p> <ul style="list-style-type: none"> <li>■ Microsoft Application Virtualization (App-V) virtual applications</li> <li>■ Microsoft Windows store applications</li> </ul>
<p>Enhanced delta inventory scan and data inconsistency detection.</p>	<p>Inventory Solution automatically detects the computers with data discrepancies and maintains the inventory data consistency.</p>
<p>Enhanced software identification process.</p>	<p>When Inventory Solution runs the software inventory scan on managed computers, it implements intelligent identification of software components and key program files. Now the software identification process is simplified and runs faster.</p>
<p>Enhanced stand-alone inventory. (Windows only)</p>	<p>Inventory Solution lets you run stand-alone inventory packages on Windows computers with Symantec Management Agent and Inventory Plug-in installed.</p>
<p>Support for SNMPv3.</p>	<p>With the SNMPv3 support, you can perform the following tasks on SNMPv3-enabled Cisco switches and the devices connected to them (for example, VMs, Desktops, etc.):</p> <ul style="list-style-type: none"> <li>■ Discover the devices using Network Discovery.</li> <li>■ Gather agentless inventory on the devices using Inventory for Network Devices.</li> </ul> <p>Note that SNMPv3 support is limited to Cisco switches only.</p>
<p>Inventory Solution gathers the software-based usage tracking data on Mac computers.</p>	<p>Inventory Solution lets you track usage of the managed software at the software product level on your managed Mac OS X 10.10 and above computers.</p> <p>To store the gathered usage tracking data, the new data class <b>Product Monthly Summary</b> is introduced.</p>

## What's new in IT Management Suite integrations

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

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

**Table 1-5** New features

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



**Table 1-5** New features (*continued*)

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

## What's new in ITMS Management Views

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

**Table 1-6** List of new features

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

## What's new in Patch Management Solution

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

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

**Table 1-7** List of new features

Feature	Description
Express Updates support.	<p>Patch Management Solution for Windows supports the Express Updates technology that is built into Windows Update service and optimizes distribution of some updates for Microsoft products by only downloading the incremental changes that each computer requires.</p> <p>For more information about Express Updates support, see the following knowledge base article:  <a href="http://www.symantec.com/docs/DOC11127">http://www.symantec.com/docs/DOC11127</a></p>
Enhanced Windows system assessment scan and assessment data inconsistency detection.  (Windows only)	<p>Windows system assessment scan in delta mode reduces the network load by only reporting data that has changed since the last full scan.</p> <p>Patch Management Solution automatically ensures that the system assessment scan data known to the Notification Server is consistent with the data on each endpoint.</p>
Ability to remove disabled bulletins from the software update policies, and then delete unused Windows and Linux packages.	<p>When you disable software bulletins, you can also remove the software bulletins from software update policies.</p> <p>You can then run the <b>Check Software Update Package Integrity</b> task to automatically delete unused Windows and Linux packages. This may be helpful to free up disk space consumed by large update packages that are no longer being distributed.</p>
Ability to distribute only selected updates for a particular software bulletin.	<p>You can create a software update policy that downloads and distributes only selected updates for a particular software bulletin. You can edit the policy later to download additional updates in the bulletin.</p> <p>If you revise software update policies to download additional updates associated with a bulletin included in the policy, distribution of the newly downloaded updates will be disabled by default.</p>
Filter for compliance reports that shows superseded updates or the software bulletins that contain superseded updates.	<p>The <b>(All)</b> filtering option of the <b>Supersedence Status</b> parameter lets you view and distribute superseded updates or the software bulletins that contain superseded updates on the <b>Patch Remediation Center</b> page or in the following enhanced patch management compliance reports:</p> <ul style="list-style-type: none"> <li>■ Software Bulletin Details</li> <li>■ Compliance by Bulletin</li> <li>■ Compliance by Update</li> <li>■ Compliance by Computer</li> <li>■ Software Update Delivery Summary</li> </ul>

**Table 1-7** List of new features (*continued*)

Feature	Description
Ability to select specific Microsoft Office 365 channels for patching.	<p>The patch management metadata release version 7.3 contains separate entries for the following Microsoft Office 365 channels enabling you to just download and distribute the updates associated with the channels required:</p> <ul style="list-style-type: none"> <li>■ Microsoft Office Click to Run 2016 (Office 365 Deferred Channel)</li> <li>■ Microsoft Office Click to Run 2016 (Office 365 Monthly Channel)</li> <li>■ Microsoft Office Click to Run 2016 (Office 365 Semi-Annual Channel)</li> <li>■ Microsoft Office Click to Run 2016 (Office 365 Semi-Annual Targeted Channel)</li> </ul> <p>For more information, see the following knowledge base article:  <a href="http://www.symantec.com/docs/DOC9673">http://www.symantec.com/docs/DOC9673</a></p>
Lists of Windows and Linux policies are available on the <b>Patch Management</b> home page.	<p>You can access the lists of software update policies for Windows and Linux that you have created on the <b>Patch Management</b> home page:</p> <ul style="list-style-type: none"> <li>■ Windows Policies</li> <li>■ SUSE Linux Policies</li> <li>■ Red Hat Linux Policies</li> <li>■ CentOS Linux Policies</li> </ul> <p>You can select a policy from the list and view the details of the policy or edit its settings if necessary on the corresponding policy page.</p>

## What's new in Software Management Solution

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

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

**Table 1-8** List of new features

Feature	Description
Enhanced Software Portal administration.	<p>Software Management Solution introduces the following enhancements of the Software Portal administration:</p> <ul style="list-style-type: none"> <li>■ The <b>Manage Publications</b> page provides a consolidated view of all software that has been published to the Software Portal. You can use this page to quickly publish additional software to the Software Portal, temporarily or permanently remove software from the portal, or edit the attributes of published items rather than performing these actions on the pages related to individual software resources or Managed Software Delivery policies.</li> <li>■ You can configure access to the Software Portal from Mac client computers by using the <b>Software Portal Client Access Policy</b>. The following options are available: <ul style="list-style-type: none"> <li>■ Show the Software Portal icon in the Symantec Management Agent user interface.</li> <li>■ Show the link to the Software Portal in the Symantec Management Agent context menu.</li> </ul> </li> <li>■ You can categorize software published to the Software Portal so that end users can more quickly locate the software they require.</li> <li>■ To limit end users to only being able to request software published for them in the Software Portal, you can use the new <b>Prevent end users from requesting unlisted software</b> on the <b>Software Portal Settings</b> page.</li> <li>■ While publishing a software resource or a Managed Software Delivery policy to the Software Portal, the Software Portal Administrator can target devices or groups of devices for software publishing. If the administrator targets both devices (or groups of devices) and users (or groups of users) for software publishing, only the selected users on the specified devices will have permission to request the software.</li> <li>■ The default number of open software requests per user is increased to 1000. Note that a Managed Software Delivery policy that contains dependencies or multiple tasks counts as one request.</li> </ul>

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

Feature	Description
<p>Enhanced user interface of the Software Portal.</p> <p>(Windows and Mac only)</p>	<p>Software Management Solution 8.1 RU5 has introduced the enhanced UI of the Software Portal that provides an app store-like user experience.</p> <p>The Software Portal Administrator can configure whether the legacy UI or the enhanced UI is displayed to the users.</p> <p><b>Note:</b> After the first-time installation, the enhanced UI is enabled by default. After the upgrade from the previous version, the UI setting remains in the same state as before the upgrade.</p> <p>The enhanced UI has the following new features:</p> <ul style="list-style-type: none"> <li>■ The Software Portal Administrator can customize the Software Portal header with company-branded background image.</li> <li>■ When the Software Portal Administrator publishes the software resource or a Managed Software Delivery policy that delivers the software resource to the Software Portal, the enhanced UI displays the predefined or custom icon for the software resource.</li> <li>■ End users can also open the Software Portal on Windows and Mac computers with Cloud-enabled Management enabled.</li> <li>■ End users can only see the software that is compatible with the platform of the computer from which they launch the Software Portal.</li> <li>■ In the user profile, end users can enable the option to view notifications when the requested application is installed on the user's device.</li> <li>■ End users and managers can search for the applications by vendor, and version.</li> <li>■ End users can filter the applications by category, type, and approval.</li> </ul> <p>For more information about using the enhanced user interface of the Software Portal, see the Mind Map <i>Making on-demand software available in the Software Portal</i> that is listed in the following knowledge base article:</p> <p><a href="http://www.symantec.com/docs/DOC9706">http://www.symantec.com/docs/DOC9706</a></p>
<p>Enhanced Software Discovery scan in Software Management Framework.</p>	<p>Speed of Software Discovery scan is improved.</p>
<p>Ability to perform software import and managed delivery at once.</p>	<p>You can create a software resource in the Software Catalog, import the associated package, and create a Managed Software Delivery policy to install the package as part of a single sequence of actions from within the Symantec Management Console or by using the Administrator Software Development Kit (ASDK). The ASDK Help can be found at</p> <p>C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Symantec\ASDK</p>

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

Feature	Description
Enhanced expressions for standard and smart rules.	<ul style="list-style-type: none"> <li>■ Support for the <b>MSI Upgrade Code</b> expression is added for standard and smart rules to check the client computer for the MSI upgrade code that you specify. For example, this may help you to determine that no newer versions of a software application are installed.</li> <li>■ Wildcard support is added for the <b>Static File Expression</b> and <b>Registry Key Exists</b> expressions.</li> <li>■ You can specify the registry entry for the expression <b>Registry Key Exists</b>.</li> </ul>
New results-based action setting for Managed Delivery.	<p>Software Management Solution introduces new results-based action setting <b>Continue job if component is not applicable</b> that you can use as the default global setting for all new Managed Software Delivery policies or as an override setting for a specific software resource that a Managed Software Delivery policy contains.</p> <p>When you enable this setting for the policy that is set to abort upon failure, the policy continues to run if it includes some components that the applicability rules define as not applicable.</p>
Enhanced software resource management experience	<p>A predefined icon identifies each software resource in the Software Catalog. By default, the icon corresponds to the type of the resource: <b>Software Update</b>, <b>Software Component</b>, <b>Service Pack</b>, or <b>Software Release</b>.</p> <p>You can add or edit a custom icon for a software resource when you edit the software resource in the Software Catalog.</p> <p>When you manage the software resource in the <b>Software</b> Management view or in the Software Catalog, you can view the custom icon.</p> <p>When you add the software resource to a Managed Software Delivery policy, the predefined or custom icon is displayed on the policy page.</p>
Running software delivery policies and tasks on a computer pending a restart or a logoff.	<p>Enable software delivery policies and tasks to execute when there is a pending restart or logoff required by Managed Software Delivery policy.</p> <p>This functionality is not available out of the box. You can enable it manually in the registry on the required client computer.</p> <p>For more information about the functionality and its limitations, see the following knowledge base article:  <a href="http://www.symantec.com/docs/DOC10551">http://www.symantec.com/docs/DOC10551</a>.</p>

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

Feature	Description
Removal of Symantec Workspace Virtualization support	<p>Software Management Solution 8.5 does not support the management of the Symantec Workspace Virtualization Agent (SWV Agent). The installation of Software Management Solution 8.5 will not copy SWV Agent to the Notification Server, nor will it create predefined policies to install or upgrade SWV Agent.</p> <p>If you upgrade from the solution version 8.0 HF6 or 8.1 RU7 to 8.5, you can use the software virtualization technology as follows:</p> <ul style="list-style-type: none"> <li>■ Your upgraded Managed Software Delivery policies with the enabled virtual layer option will continue to install software into virtual layer for the client computers with SWV Agent installed.</li> <li>■ Your upgraded Managed Software Delivery policies with the enabled virtual layer option will install software in a non-virtualized state for the client computers without SWV Agent installed.</li> <li>■ You will be able to create new Managed Software Delivery policies with the enabled virtual layer option.</li> </ul> <p>If you migrate Managed Software Delivery policies with the enabled virtual layer option from the solution version 8.0 HF6 or later to 8.5, the policies lose virtualization and install software in a non-virtualized state on the client computers.</p> <p>For more information about the End of Life of Symantec Workspace Virtualization and Symantec Workspace, see the following knowledge base article:</p> <p><a href="https://www.symantec.com/docs/INFO4060">https://www.symantec.com/docs/INFO4060</a></p>

## What's new in Symantec Endpoint Management Workspaces

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

**Table 1-9** List of new features

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

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

Feature	Description
<b>Search</b> workspace	The <b>Search</b> workspace enables users to search for resources and view inventory details for the selected resource (endpoint).
<b>Quick Tasks</b> workspace	The <b>Quick Tasks</b> workspace enables help desk users to deliver software and run tasks
<b>Endpoint Management Workspaces Users</b> role	Specifically for help desk workers, Symantec introduces a new role - <b>Endpoint Management Workspaces Users</b> .  By default, the new role gives the permission to the user to perform the following actions in the Symantec Endpoint Management Workspaces: <ul style="list-style-type: none"> <li>■ Search for resources (endpoints).</li> <li>■ View selected endpoint inventory and health information.</li> <li>■ Use <b>Quick Tasks</b> workspace to deliver software and run tasks.</li> </ul>

## What's new in Virtual Machine Management

In Virtual Machine Management 8.5, the following new features are introduced:

**Table 1-10** List of new features

Feature	Description
Added new OS Support	The following operating systems are now supported: <ul style="list-style-type: none"> <li>■ Windows10 Redstone 4</li> <li>■ Mac OS X 10.11</li> <li>■ Mac OS X 10.12</li> </ul>
Support for ESXi 6.5 and vSphere 6.5.	Virtual Machine Management now supports ESXi 6.5 and vSphere 6.5.

## What's new in Workflow Solution

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



**Table 1-11** List of new features

Feature	Description
Added support for Aspose.Email library	<p>A new component is added that supports all the existing functions in all the types of SSL environments.</p> <p>The new components are developed with the Aspose.Email library.</p> <p>Currently, the new components are listed with the suffix, "New" and are added in the <b>Process Components &gt; Email</b> category of the component list.</p> <p>For more information, refer to the following article: <a href="#">DOC11187</a></p>
Localized uninstaller of Process Manager and Workflow Designer	The uninstaller for <b>Process Manager</b> and <b>Workflow Designer</b> are now localized.
Improved UI of Process Manager.	The application menu and UI for <b>Calendar</b> , <b>Scheduler</b> , <b>Knowledge Base</b> , and <b>Documents</b> of the <b>Process Manager</b> of Workflow Solution are updated.
Workflow support for Symantec Endpoint Protection 14	<p>From this release onwards, Workflow provides limited support for Symantec Endpoint Protection 14 components.</p> <p>For more information refer to the following article: <a href="#">DOC10748</a></p>
Changes in Workflow Solution	Password hint field is removed from the modify User Account page.
Added the option to insert image.	From this release, the insert image option is added to the HTML Editor toolbar, Add Article dialog FAQ, Bulletins, and Discussions.

## System requirements and supported platforms

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

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

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

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

# General installation and upgrade information

## Installation of IT Management Suite 8.5

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

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

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

## Upgrade to IT Management Suite 8.5

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

The following upgrade scenarios are supported:

- From IT Management Suite 8.0 HF6 to IT Management Suite 8.5
- From IT Management Suite 8.1 RU7 to IT Management Suite 8.5

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

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

## Migration of Symantec Management Platform and the IT Management Suite solutions

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

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

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

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

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

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

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

## Known issues and fixed issues

For information about the known issues and fixed issues of the solutions and components of IT Management Suite 8.5, refer to the corresponding chapters in the following suite's Release Notes:

- Symantec Management Platform Release Notes  
<http://www.symantec.com/docs/DOC11103>
- Asset Management Suite Release Notes  
<http://www.symantec.com/docs/DOC11096>
- Client Management Suite Release Notes  
<http://www.symantec.com/docs/DOC11107>
- Server Management Suite Release Notes  
<http://www.symantec.com/docs/DOC11104>
- Deployment Solution Release Notes  
<http://www.symantec.com/docs/DOC11089>
- Workflow Solution Release Notes  
<http://www.symantec.com/docs/DOC11090>

## Where to get more information

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

Table 1-12 Documentation resources

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

**Table 1-12** Documentation resources (*continued*)

Document	Description	Location
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	<ul style="list-style-type: none"> <li>The Documentation Library, which is available in the Symantec Management Console on the <b>Help</b> menu.</li> <li>The <b>Supported Products A-Z</b> page, which is available at the following URL: <a href="https://www.symantec.com/products/products-az">https://www.symantec.com/products/products-az</a> Open your product's support page, and then under <b>Common Topics</b>, click <b>Documentation</b>.</li> </ul>
Help	<p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p>	<p>The Documentation Library, which is available in the Symantec Management Console on the <b>Help</b> menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <ul style="list-style-type: none"> <li>Click the page and then press the F1 key.</li> <li>Use the Context command, which is available in the Symantec Management Console on the <b>Help</b> menu.</li> </ul>

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

**Table 1-13** Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	<a href="#">Knowledge Base</a>
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.	<a href="#">Unified Help System</a>

**Table 1-13** Symantec product information resources (*continued*)

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	The links to various groups on Connect are as follows: <ul style="list-style-type: none"><li>■ <a href="#">Deployment and Imaging</a></li><li>■ <a href="#">Discovery and Inventory</a></li><li>■ <a href="#">ITMS Administrator</a></li><li>■ <a href="#">Mac Management</a></li><li>■ <a href="#">Monitor Solution and Server Health</a></li><li>■ <a href="#">Patch Management</a></li><li>■ <a href="#">Reporting</a></li><li>■ <a href="#">ServiceDesk and Workflow</a></li><li>■ <a href="#">Software Management</a></li><li>■ <a href="#">Server Management</a></li><li>■ <a href="#">Workspace Virtualization and Streaming</a></li></ul>