Symantec™ Server Management Suite 7.5 powered by Altiris™ technology Release Notes

Symantec

Symantec™ Server Management Suite powered by Altiris™ technology Release Notes

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal 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:

www.symantec.com/business/support/

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_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Server Management Suite 7.5

This chapter includes the following topics:

About Server Management Suite

Server Management Suite combines the essential tools that help you effectively manage your physical servers and virtual servers, reduce service interruptions, and increase uptime.

Server Management Suite incorporates a variety of wizards and other features that let you automate configuration, stage tasks, and create policies to manage your servers. Various graphical reports let you quickly identify the health of your environment, pinpoint problems, and analyze trends. Expanded support for virtual technologies simplifies the management of multiple operating system environments.

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

- Discovery and inventory
  The suite automatically identifies the devices that are found in your network, and aggregates inventory data across your environment. Multi-platform support makes it easy to consolidate the discovery data of all your Windows, UNIX, and Linux assets within an integrated console. You can easily assess security vulnerabilities, prepare for software audits, and more accurately determine hardware availability and needs.
- Provisioning
  The suite lets you improve the consistency and increase the quality of server configurations. It delivers the comprehensive deployment capabilities that include image-based or scripted operating system installation and continuous provisioning. The suite helps you implement the standardized configurations, and provides you the tools for migration.
- Software distribution and patch management
  The suite lets you control server configurations through its software management capabilities. The automated policies for software and patch management help you keep the servers standardized and secure. You can modify similar configurations on multiple servers simultaneously. You can distribute applications, and security updates to target systems.
- Proactive monitoring and alerting
  The suite helps you proactively monitor the critical components of your network. You can increase the network uptime with the self-healing remediation tasks that are configured before the critical events occur. You can organize your servers into vital groups and quickly ascertain the current health of the whole network. The monitoring capabilities provide you also a summarized view of each single server performance over time.

See "Where to get more information" on page 20.

What has changed in the release notes

In the IT Management Suite 7.5 release, to make the release information easier to find and access, the release notes information of most solutions are now part of the following release notes:

- IT Management Suite 7.5
- Asset Management Suite 7.5
- Client Management Suite 7.5
- Server Management Suite 7.5
- Symantec Management Platform 7.5

For more information about the changes in the release notes see the following link:

http://www.symantec.com/docs/DOC5702

Components of Server Management Suite 7.5

Server Management Suite is a collection of solutions that run on the Symantec Management Platform. These solutions let you discover, inventory, monitor, and provision servers from a central console - the Symantec Management Console.

See "About Server Management Suite" on page 10.

Table 1-1 Components of Server Management Suite

Component	Link to User Guide
Symantec Management Platform	DOC5330
Deployment Solution 7.5	DOC5803
Enhanced console views	DOC5330
Inventory Solution	DOC5719
Inventory Pack for Servers	N/A
Inventory for Network Devices	DOC5717
Monitor Solution for Servers	DOC5767
Monitor Pack for Servers	DOC5767
Patch Management Solution	■ Patch Management Solution for Linux: DOC5772 ■ Patch Management Solution for Mac: DOC5776 ■ Patch Management Solution for Windows: DOC5768
Real-Time System Manager	DOC5709
Software Management Solution	DOC5446
Symantec Endpoint Protection Integration Component	DOC5671
Virtual Machine Management	DOC5667
Symantec Workflow Solution	DOC5941

Table 1-1 Components of Server Management Suite *(continued)*

Component	Link to User Guide
Topology viewer	N/A
Server Resource Manager view	N/A

What's new in this release

The new features in Server Management Suite 7.5 are categorized into the following:

- General enhancements in Symantec Management Platform 7.5
  See Table 1-2 on page 13.
- New features in solutions of Server Management Suite 7.5
  See Table 1-3 on page 16.

Table 1-2 List of general enhancements

Feature	Description

General enhancements	■ Symantec Management Console
	  ■ Administrators will notice console performance up to 15 times faster than in previous releases.
	  ■ New Task Rerun functionality lets you rerun tasks on computers that failed the task.
	  ■ New Software Delivery flipbook page lets you view and act on summary information about Quick Delivery tasks and Managed Delivery policies in your environment.
	■ New Log Viewer:
	  ■ Ability to load a large amount of log files without consuming too much of your server's resources
	  ■ Simplified filter mechanism
	  ■ Bookmarks
	  ■ Ability to search in log files without loading the log files into Log Viewer
	■ Reporting: New SuppressReportAutorun functionality
	■ Symantec Management Platform does not support a hierarchy that is more than 2 levels (a parent notification server with child Notification Servers) deep.
	■ Network Discovery supports Linux and Mac devices by SSH protocol.

Table 1-2 List of general enhancements *(continued)*

Feature	Description
Cloud-enabled Management (CEM)	Cloud-enabled Management (CEM) lets you manage remote endpoints even when those endpoints are not connected to the corporate network through VPN. This functionality helps to improve software and patch deployment coverage of your mobile workforce and telecommuting employees. CEM allows for fully secure communication between roaming endpoints and Notification Server(s) on the internal network. CEM is supported on Windows computers only. The following solutions and functionality is supported over CEM: ■ Task Management Task Management lets you run any task types in CEM mode. However, tickle connection to the Task Server is not established in CEM mode and immediate task execution is not available. The tasks can run with up to 60 minutes delay according to the default settings. Running a Task Server on a Cloud-enabled, Internet-managed client computer is not supported and can lead to undesirable behavior. ■ Inventory Solution Hardware inventory, software inventory, custom inventory, server inventory, and application metering features are supported. ■ Software Management Solution ■ Patch Management Solution
Agent registration	Along with the Cloud-enabled Management feature that lets you manage the devices that are outside the firewall, the agent registration feature was added in IT Management Suite 7.5 to ensure that only trusted endpoints can communicate with Notification Server. The agent registration feature requires an endpoint to be allowed to communicate with Notification Server before it can be managed.
Legacy Agent Communication (LAC) mode	The Legacy Agent Communication (LAC) mode lets you control whether the computers that use older versions of Symantec Management Agent can communicate with the upgraded 7.5 Notification Server. This option lets you upgrade the agents in your environment in phases and still maintain management capabilities for the legacy agents.

Table 1-2 List of general enhancements *(continued)*

Feature	Description
The list of supported platforms has been expanded.	The following operating system is now supported for the installation of Symantec Management Platform and its components: ■ Windows Server 2008 R2 SP1 (64-bit) The following versions of Microsoft SQL Server are now supported for the Configuration Management Database (CMDB): ■ Microsoft SQL Server 2008 R2 SP1 ■ Microsoft SQL Server 2008 SP3 ■ Microsoft SQL Server 2012 ■ Microsoft SQL Server 2012 SP1 ■ Microsoft SQL Server 2008 R2 SP2 The following operating systems are now supported or have improved support for the installation of the Symantec Management Agent: ■ Windows 7 SP1 ■ Windows 8 ■ Windows Server 2008 R2 SP1 ■ Windows Server 2012 ■ Red Hat Enterprise Linux 5.7, 5.8, 5.9, 6.2, 6.3, and 6.4 ■ Novell SUSE Linux 11 SP2 ■ Mac OS X 10.8 ■ IBM AIX 7.1
Support for Internet Explorer 10 (compatibility mode) in Software Portal	Software Management Solution's Software Portal now supports Internet Explorer 10 in compatibility mode.

Table 1-2 List of general enhancements *(continued)*

Feature	Description
Out of Band Management component	The Out of Band Management Component (OOB) is no longer bundled with ITMS. This component was required to define, apply, and maintain the configuration of Intel® Active Management Technology (AMT). Though the OOB Management Component is no longer bundled, existing Real-Time System Manager features continue to function on supported Intel AMT computers. When you perform an upgrade from earlier versions of IT Management Suite, the Out of Band Remover utility removes the Out of Band Management Component items from Notification Server and site servers. The Intel Setup and Configuration Software (SCS) database, commonly referred to as the IntelAMT database remains intact. The Out of Band Remover utility does not affect the Intel AMT firmware configuration settings on the client computers. If you have already installed a standalone Intel SCS server it is not affected by the OOBRemover utility. For more information on how to discover out-of-band capable computers along with guidance migrating your current IntelAMT database to the latest version of Intel SCS, see http://www.symantec.com/docs/DOC6628.

Table 1-3 List of new features in Server Management Suite solutions

Feature	Description

Inventory Solution	The following enhancements are added to Inventory Solution:
	■ In the Cloud-enabled Management environment, you can use the following methods for gathering inventory data:
	  ■ Basic inventory
	  ■ Standard inventory on target computers
	  ■ Custom inventory
	  ■ Server inventory
	  ■ Application metering
	■ Inventory Solution for Network Devices is now part of Inventory Solution. There is no longer a separate licence for Inventory for Network Devices. When agentless inventory is used to collect information from an SNMP-enabled device and the information is posted to the server, then a license of Inventory Solution will be consumed by that device.

Patch Management	The following enhancements are added to Patch Management: ■ Support for Cloud-enabled Management ■ Support for Agent Registration ■ New Patch Workflow

Table 1-3 List of new features in Server Management Suite solutions *(continued)*

Feature	Description
Monitor Solution	The following enhancements are added to Monitor Solution: ■ Monitor rule condition aggregation Monitor rules are designed to alert the administrator or execute certain client and server tasks, when the specific condition is reached. One rule can monitor multiple item instances for multiple conditions at the same time. The complicated logic of rule metrics and instances aggregation provides a high level of customization of the alerting frequency. ■ Support for Windows Server 2012 A new monitor pack for Windows Server 2012 provides the same monitoring capabilities as for Windows Server 2008. ■ ESX Monitor Packs were removed in the 7.5 release.
Software Management Solution	The following enhancements are added to Software Management: ■ Support for Cloud-enabled Management ■ Support for ASDK Lets you create custom scripts to automate and simplify complex procedures in IT Management Suite components. ■ OS Platform awareness in Software catalog: allows filtering of software resources by platform (Windows, UNIX, Linux, Mac) to which these software resources are applicable. ■ Support for IE10: Customers can now access the Software Portal on the client computers using Internet Explorer 10, which is a default browser for Windows 8 operating system.
Virtual Machine Management (VMM)	The following enhancements are added to Virtual Machine Management: ■ Create VM from VMware template You can clone a VM from an existing VM template directly from the SMP Console and through provided tasks. ■ Guest and host VMM tasks available through right-click option in the All Resources view. Lets you perform VMM tasks such as Create VM, Create VM Snapshot, Restart/Resume/Suspend VM from the All Resources view. ■ New Orphaned VMs report Reports on the VMs, which were deleted without VCenter's knowledge.

Table 1-3 List of new features in Server Management Suite solutions *(continued)*

Feature	Description
Deployment Solution	Deployment Solution contains the following enhancements: ■ Support for imaging Macintosh computers ■ Support for imaging Windows 8 computers and Windows Server 2012 computers ■ Support for SUSE Linux ES 11 SP1 ■ Support for ESX 4.0, 4.1 and ESXi 4.1, 5.1 ■ Support for Red Hat Enterprise Linux (RHEL) 6.0, 6.1, 6.2, and 6.3
Workflow	The following enhancements are added to Workflow Solution: ■ Web Application Project Type You can use the Workflow, Dialog, and Service Models in the same Project. You can use multiple entry points to control how the Web Application Project Type is consumed. You can use the Start Workflow component to invoke a Workflow Model from another Model Type. ■ Workflow Solution Center An online repository that contains the prebuilt Workflow templates and updated Workflow component packs for you to download. It also contains videos and documentation on how to implement the templates and the component packs. ■ Collaborative component wiki All component information is now stored on Symantec Connect in the collaborative component pages. Each component has its own wiki page. The collaborative component pages are community-based. You can also access these pages from inside Workflow Designer.

For more information about what has changed in each of the solutions and components, see the individual solution chapters in this document.

System requirements and supported platforms

Before you install Server Management Suite 7.5, read the section Hardware recommendation in the *IT Management Suite 7.5 Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC5670

For any additional solution and components system requirements, see the chapters for individual solutions in this document.

For information about the supported operating systems in Symantec Management Platform 7.5 and the IT Management Suite 7.5 solutions, see the article in the following URL:

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

General installation and upgrade information

You install the Symantec Management Platform (SMP) 7.5 and the Server Management Suite (SMS) 7.5 solutions using Symantec Installation Manager.

Installation of Symantec Management Platform 7.5 and the Server Management Suite 7.5 solutions

You can download the installation files directly to your server or you can create offline installation packages.

For more information on how to install and configure the product, see the *Installing the IT Management Suite solutions* chapter in the *IT Management Suite 7.5 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC5697

Before you install or upgrade to Server Management Suite, Symantec Management Platform, or IT Management Suite, ensure that you have reviewed the latest changes to the Symantec Management Platform of this release. For more information on what's new in Symantec Management Platform 7.5, see the *Symantec™ Management Platform 7.5 Release Notes* at http://www.symantec.com/docs/DOC6713.

Upgrade to Symantec Management Platform 7.5 and the Server Management Suite 7.5 solutions

You can upgrade from the previous versions of Symantec Management Platform and Server Management Suite solutions to the latest versions using Symantec Installation Manager.

The supported upgrade paths are as follows:

- 7.1
- 7.1 SP1
- 7.1 SP2

To perform an upgrade from version 7.1 or later, in the Symantec Installation Manager click **Upgrade installed products**, and then choose to install this product.

Symantec recommends that you upgrade all the installed products to the latest version. The easiest way to upgrade to 7.5 version is to choose to install a suite. If you use hierarchy, you must disable hierarchy replication and upgrade all products to the latest version on each of the Notification Server computers.

For more information on how to upgrade to Server Management Suite 7.5 solutions, see the *Upgrading to IT Management Suite 7.5* chapter in the *IT Management Suite 7.5 Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC5697

Upgrade to Symantec Management Agent 7.5

After upgrade to SMP 7.5 and SMS 7.5, you must upgrade the Symantec Management Agent (SMA) on client computers to SMA 7.5. Additionally, you must upgrade the SMA plug-ins, such as Altiris Client Task Agent and Deployment Solution Plug-in, to the latest versions that are available in SMP 7.5 and SMS 7.5. Different versions of the SMA and plug-ins are not supported in 7.5 release.

To upgrade to Symantec Management Agent 7.5, you can execute any one of the following tasks:

- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent.
- In the Symantec Management Console, click **Settings > All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins.
- In the Symantec Management Console, click **Actions > Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the upgrade policies for various plug-ins.

Symantec recommends that you configure a schedule for these policies; the default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. Also, to speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

For detailed instructions on migrating from 6.x or 7.0 to 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

Where to get more information

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

Table 1-4 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**.
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 1-5 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Table 1-5 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 Here is the list of links to various groups on Connect: ■ 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

Chapter 2

Deployment Solution

This chapter includes the following topics:

What's new in this release

In the Deployment Solution 7.5, the following new features are introduced:

Table 2-1 List of new features in Deployment Solution 7.5

Feature	Description
Support for Mac 10.6, 10.7, and 10.8 versions of operating system	Deployment Solution supports the following for the Mac OS computers ■ Imaging of Mac computers ■ Installing Mac OS on computers ■ Providing option to customize the background image of Mac computers when in the automation environment mode. ■ Providing option to install the Mac plug-ins and the automation folders from the **Actions > Deployment** menu of the console.
Class 2 type of UEFI/EFI computers that are installed with Windows operating system	Deployment Solution supports the following for the Windows UEFI/EFI client computers: ■ Booting the UEFI/EFI computers in the preboot environment using the WinPE 4.0 preboot package ■ Imaging the computers using the Ghost imaging tool ■ Installing the Windows OS on the UEFI/EFI computers using the **Install Windows OS** task of Deployment Solution. ■ Installing the automation folder for UEFI/EFI computers that are installed with Windows 8, and Windows 2012 operating system.

Table 2-1 List of new features in Deployment Solution 7.5 *(continued)*

Feature	Description
Support for LinuxPE v2.6	Deployment Solution supports LinuxPE v2.6.
SSL support in preboot environment	Deployment Solutions now supports SSL communication in the preboot environment.
Support for WinPE 4.0	Deployment Solution supports WinPE 4.0 preboot package for both x64 and x86 architecture computers.
Leverage Package Server	Deployment Solution now leverages the function of the Package Server for storing images and large amount of data thereby removing the dependency from the Task Server. The network share facility of the Task Server is removed and all data is stored on the Package Server.
PXE service changes and improvement	A new site service, Network Boot Service (NBS) is introduced in this release that runs on a site server. This service performs the combined tasks of the PXE server, TFTP server, Boot Disk Creator, and the preboot image creation policy. The NBS can be installed independent of the task service and the package service and can therefore be deployed on a site server as a standalone.
Predefined Computers	Deployment Solution provides provision to add predefined computer through the **Predefined Computers** dialog box of the console besides importing them. An already added predefined computer can be edited using the Edit option of the dialog box.
Support for Red Hat Enterprise Linux	Deployment Solution now supports execution of deployment tasks on client computers of RHEL 6.0 and RHEL 6.1 operating systems. Except for the SOI task, all other tasks can be executed on the RHEL 6.2 and RHEL 6.3 computers. For more information refer to the Symantec Management Platform and Altiris Solutions Support Matrix at http://www.symantec.com/docs/HOWTO9965.
Support for SUSE Linux ES 11 SP1	Deployment Solution now supports execution of deployment tasks on client computers of SLES 11 SP1 operating system.
Support for ESX 4.0, 4.1 and ESXi 4.1, 5.1	Deployment Solution now supports installation of ESX 4.0, ESX 4.1, and ESXi 4.1 and ESXi 5.1 operating systems on the client computers using the **Install Linux/ESX OS** task.
Support for Windows 8 and Windows Server 2012 computers	Deployment Solution now supports Windows 8 and Windows Server 2012 computers.

Table 2-1 List of new features in Deployment Solution 7.5 *(continued)*

Feature	Description
Manual job selection for managed computers in automation environment and boot image customization	Deployment Solution provides a new feature to manually select predefined jobs in the automation environment for a re-deployed managed computer. The predefined set of jobs are configured for the Initial Deployment job and are displayed after a managed computer boots in the automation environment. The boot image customization feature provides customization of the background screen that is displayed in the preboot environment. The provision to lock or unlock the preboot screen is also provided.

Known Issues

The following are the known issues for this release:

Table 2-2 Known Issues of Deployment Solution 7.5

Issue	Description
For Linux computers, the **Boot To** task when executed displayed incorrect status.	For Linux, client computers that are in the production environment, the **Boot To** task status displays as "Failed" even after the task completes successfully.
Multiple NIC entries cannot be added for a predefined computer.	You cannot specify multiple NIC entries when adding a predefined computer through the **Predefined Computers** dialog box of the console. The workaround to this issue is that you can add one NIC as DHCP and the other NICs as static.
In the **Deploy Image** task, the UNC path is displayed for the images that are created using the HTTP or HTTPS path.	The **Deploy Image** task displays a UNC path for the images that are created using the HTTP path or the HTTPS path.
An external hard disk that is connected to the package server computer is considered as a fixed drive and the package share is created on the connected external hard disk.	An external hard disk that is connected to the package server computer is considered as a fixed drive and the package share is created on the connected external hard disk.

Table 2-2 Known Issues of Deployment Solution 7.5 *(continued)*

Issue	Description
The **Capture Personality** task fails for Windows XP Professional x86 and Windows 7 SP1 x64 managed computers when they are moved from a CEM to Non-CEM environment.	When executing the **Capture Personality** task on Windows XP Professional x86 and Windows 7 SP1 x64 an error is displayed when Package Server and the client computer are moved from CEM environment to Non-CEM environment
For Mac computers, saved data for the Network Adapter is not displayed in the **Apply System Configuration** task.	For Mac computers, when you create a **Apply System Configuration** task, if you set the DNS1 address as "Leave existing" and provide only DNS2 address, then the DNS2 address is not saved and is not available in the **Edit configuration…** of the **Apply System Configuration** task for editing.
For Mac computers, the **Apply System Configuration** task is not able to restore the network details.	For Mac computers, you cannot restore the network details such as Domain suffix using the restore functionality of the **Apply System Configuration** task. You can modify only the host name using the **Apply System Configuration** task.
Partition information of HTTP image imported using Resource Import Tool is not displayed in the **Advanced** tab of the **Deploy Disk Image** task dialog box	For Linux client computers, the partition information of the HTTP image that you import using Resource Import Tool is not displayed in the **Advanced** tab of the **Deploy Disk Image** task dialog box.
The **Create Image** task fails when the default drive on package server is full	The **Create Image** task fails to create new images when the default drive on the package server is full. The workaround for the issue is as follows: In the Symantec Management Console, create a **Copy File** task that replicates a package that is created on Notification Server to the package server. This replication of the package creates a new net share on the package server if an additional drive is available on package server.
HTTP server's port of package server is different from that of the Symantec Management Platform (SMP)	As the HTTP server's port number for a package server is different from that of the SMP computer, all queries that are created for the package server contain the SMP's HTTP server's port number.

Table 2-2 Known Issues of Deployment Solution 7.5 *(continued)*

Issue	Description
Undefined error occurs on SMP and **Personality Capture** task fails if client computer moves to non-CEM mode	An undefined error occurs on the SMP and the **Personality Capture** task fails if CEM policy is enabled. After the CEM policy is enabled, the package servers that are in the non-CEM environment are also CEM enabled and the client computer of the non-CEM environment fails to communicate with the package servers The workaround to this issue is as follows: ■ Go to **Settings > Notification Server > Cloud-enabled Management** ■ Expand **Policy > Cloud-enabled Management Settings** ■ Select the **Applied To filter > Click Edit** (Pencil icon) ■ Click **Update results** ■ Right-click on the Package server which is expected to be in the **Non-CEM environment > Click Exclude > Click OK** ■ Click **Save Changes.** After the non-CEM package servers are removed from the CEM policy, the status on the package server changes to CEM disabled. The non-CEM client computers can then communicate with the non-CEM Package Server.
If Package Server is in HTTPS mode, then **Install Windows OS** task fails with error	The following error message is displayed and the **Install Windows OS** task fails if the package server is launched in HTTPS mode: `Package Path is Null`
New drivers do not replicate on package server computer if exception is thrown during addition of drivers	During addition of drivers through the **Driver Database Management** dialog box, if an exception is thrown, then the new drivers are not replicated on the package server computer. The workaround to this issue is that after you get an exception on the driver management console, import only a single driver which displays the result of the addition of driver in the console. Later, you can find the other drivers replicate on the Package server.
Copy File task does not execute successfully on client computers if path of package server is changed	The **Copy File** task does not execute successfully on the client computer if the path of the package server is changed through the dialog box.
For a Linux predefined computer, deployment of non-Sysprep image does not retain the predefined name	For a Linux predefined computer, deployment of a non-Sysprep image does not retain the name of the predefined computer.

Table 2-2 Known Issues of Deployment Solution 7.5 *(continued)*

Issue	Description
Deploy Image task using Deploy Anywhere does not insert a driver to Windows Server 2008 32-bit computer (DELL 960V)	A **Deploy Image** task that uses the DeployAnywhere database fails to insert a driver on a Windows Server 2008 32-bit Dell (960V) computer.
Drivers not displayed in the **DeployAnywhere** tab of the **Driver Database Management** dialog box when drivers are added simultaneously from command line and through the dialog box	If a driver is added through the **Driver Database Management** dialog box and through the command-line simultaneously, then the drivers are not displayed for the DeployAnywhere tab of the dialog box, even though the appropriate driver folder is created on the client computer.
If image creation operation stops in middle, Ghost tool re-launches and continues to create image over UNC path	While creating images using the Ghost imaging tool, image creation task stops in the middle, the Ghost tool launches again, and the image creation again continues over the UNC path.
Ghost imaging tool attempts multiple times to create image on web server even when the server is unavailable	Even when the web server is unavailable, the Ghost imaging tool attempts multiple times to create an image on the web server from the client computer.
Restore Backup Image task fails if image is stored in non-default path	The **Restore Backup Image** task fails if the image package is stored in the non-default location of the computer.
The deployment-related tasks fail when Notification Server is changed from HTTP to HTTPS	The deployment-related tasks fail when Notification Server is changed from HTTP to HTTPS.
A predefined computer with a space in the UUID hardware identifier boots as an unknown computer.	If the UUID hardware identifier of a predefined computer has a space separator, then it boots as an unknown computer after you add the computer into the network.
The **Apply System Configuration** task fails to change the host name for the SUSE Linux Enterprise SP1 client computers	You cannot change the host name for the SUSE Linux Enterprise SP1 client computers through the **Apply System Configuration** task.

Table 2-2 Known Issues of Deployment Solution 7.5 *(continued)*

Issue	Description
For Mac, the **Deploy Image** task fail that involves deploying image of a non-HFS or HFS type of disk partition when the DS Automation volume is located with the target volume on the same disk	For Mac, the **Deploy Image** task fail to deploy an image for the following if the DS Automation volume is located with the target volume on the same disk and the client computer is booted in the preboot environment using the DS Automation volume: ■ An image of a non- HFS type of disk partition is deployed on a disk that has HFS type of partition. ■ An image of an HFS type of disk partition is deployed on a disk that has non-HFS type of partition.
The **Install Linux/ESX OS** task is not supported for RHEL6.2 and RHEL 6.3 version.	The **Install Linux/ESX OS** task is not supported for RHEL 6.2 and RHEL 6.3 version.
The **Deploy Image** task cannot be stopped by using the stop option of the task status page of the Symantec Management Console.	You cannot stop the execution of the **Deploy Image** task on the client computer from the task status page of the Symantec Management Console.
Incorrect help opens when you click on the help icon of the **Partition Disk** task.	The help icon that is present on the **Partition Disk** task does not open relevant help when you use the Internet Explorer 9 browser to browse the console.
The 32-bit virtual machine or the ESX client computers cannot boot into preboot environment using WinPE4.0	You cannot boot a 32-bit virtual machine or an ESX client computer into preboot environment using WinPE4.0 For more information on this issue refer to the following: ■ VMWare Community ■ Microsoft TechNet
For Mac OS X 10.6 version, the running application icons are not displayed in the dock of the client computer that is booted into the automation environment	For Mac OS X 10.6 version, the running applications are not captured during automation partition creation. When the client computer is booted in the automation environment using the automation folder, the running application icons are not displayed.

Table 2-2 Known Issues of Deployment Solution 7.5 *(continued)*

Issue	Description
For Mac, the Automation folder install policy fails to download the automation folder on the client computer when the thumbs.db file is present in the Automation folder or the Agent folder	For Mac, the Automation folder install policy fails to download the automation folder on the client computer if the thumbs.db file is present as hidden in the Automation folder or the Agent folder A thumbs.db file is generated when you access the Automation folder or the Agent folder from the <Install_dir>\Program Files\Notification Server\NSCapBin\ UNIX\Deployment\Mac\universal\ path and change the view of the folder content to Thumbnails view. Following is the workaround for this issue: ■ Navigate to <Install_dir>\Program Files\Notification Server\NSCapBin\ UNIX\Deployment\Mac\universal\Automation folder ■ Select Show hidden files,folder, and drives. ■ Uncheck the Hide Protected operating system files(Recommended) check box ■ If the Thumbs.db file is present then run the following command in the command prompt for the location where the file is generated (with Administrator Privileges `ATTRIB -S -H Thumbs.db`
The **Install Windows OS** task fails in a Notification Server only set-up if the port 445 is blocked.	The **Install Windows OS** task fails in a Notification Server only set-up if the port 445 is blocked.
The Automation folder is not updated on the client computers after you recreate the preboot configuration	The automation folder is not updated on the client computers. After you update the preboot configuration the package distribution points are not updated after you recreate the preboot configuration. Following is the workaround for this issue: ■ In the Symantec Management Console, navigate to **Settings > All Settings > Deployment and Migration** and select the Automation folder upgrade policy. ■ Disable the appropriate automation folder upgrade policy. ■ From the **Settings > Deployment > Create Preboot Configurations** recreate the preboot configuration ■ From the Windows Task Scheduler, update the package server distribution points by updating the NS.Package Refresh task. ■ Check that the packages are updated on all the package servers. ■ After you ensure that the packages are updated on the package servers, **Settings > All Settings > Deployment and Migration** and enable the automation folder upgrade policy.

Table 2-2 Known Issues of Deployment Solution 7.5 *(continued)*

Issue	Description
The **Copy File** task fails and displays an error message when you copy a file on the client computer that is booted in the automation environment	The **Copy File** task fails when you copy a file of size that is equal to or greater than half the size of the RAM disk of the client computer that is booted in the automation environment when enough space is available on the X drive and displays the following error message Not enough space available on the destination drive. Following is the workaround for the issue: Use the **Run Script** task to map the drive on which the file is located and then use the file when the client computer is booted in the preboot environment.
The **Erase Disk** task status displays as failed in the console even when the task is executed successfully.	The **Erase Disk** task displays the status as failed even when the task is executed successfully. This issue occurs when you execute the task to erase a disk of a client computer that has multiple disks and different operating systems installed on the disks.
You cannot recreate the PEInstall and LinInstall configuration with the **Repair** option of the Symantec Installation Manager.	You cannot recreate the PEInstall and LinInstall configuration with the **Repair** option of the Symantec Installation Manager This issue occurs when you delete the configuration files from the following paths and recreate the PEInstall with the **Repair** option from the Symantec Installation Manager: ■ <Install_dir>:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\Automation\PEInstall_x86 ■ <Install_dir>\Program Files\Altiris\Notification Server\NSCap\bin\Win64\X64\Deployment\Automation\PEInstall_x64 ■ <Install_dir>:\Program Files\Altiris\Notification Server\NSCap\bin\UNIX\Deployment\Linux\x86\Automation\LinInstall_x86 Following is the workaround for this issue: In the Symantec Management Console, navigate to **Setting > Deployment > Create Preboot Configurations**, select the PEInstall or LinInstall, and click the **Recreate Preboot Environment.**.

Other things to know

The following are things to know about this release:

- From this release onwards, few of the drivers that were earlier available in the driver database have been removed. You can add the drivers to the driver database in the following ways:

  - If you are upgrading to the Deployment Solution 7.5 version, then you can import drivers to the driver database from the driver database that is installed from the previous version.
  - If you are installing Deployment Solution for the first time then you must add the drivers to the driver database.
    For information on adding drivers to the driver database please refer to the *Deployment Solution 7.5 User Guide* on http://www.symantec.com/DOC5678.

- Mac imaging, is not supported on HTTP/HTTPS and you must have the **Publish UNC codebase** check box checked in the **Package Server Settings** page.
- From this release onwards, the RapiDeploy tool is for legacy use only. Symantec recommends that you use the Ghost tool over RapiDeploy tool to execute imaging tasks on Windows and Linux client computers.
- Deployment Solution does not support the client computers that are managed with Cloud enabled Management.

Chapter 3

Inventory Solution

This chapter includes the following topics:

Known issues

The following are the known issues for this release.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

The known issues are separated into the following groups:

- Installation and upgrade issues.
  See Table 3-1 on page 34.
- Hierarchy and replication issues.
  See Table 3-2 on page 36.
- Other known issues that are common for all types of platforms.
  See Table 3-3 on page 36.
- Other known issues for Windows platforms.
  See Table 3-4 on page 37.
- Other known issues for UNIX, Linux, and Mac platforms.
  See Table 3-5 on page 38.

Table 3-1 Installation and upgrade issues

Issue	Description
Installation of the Inventory Plug-in for UNIX, Linux, and Mac fails after migration to Inventory Solution 7.5, to a custom location.	When you migrate Inventory Solution from version 7.0 to 7.5 and, instead of the default location `C:\Program Files\Altiris\...`, select some custom location, for example `C:\AdministratorTools\Altiris\...`, then the installation of Inventory Plug-in for UNIX, Linux, and Mac fails on the target Notification Server computer. You get the error message: "Failed to get package snapshot". The problem does not occur if you select the default location during the migration.
Some inventory automation policy settings are not preserved after an upgrade from Inventory Solution 7.x to 7.5.	The **On/Off** status of the following automation policies is not preserved after upgrade: ■ **Low Disk Space** ■ **Collection failed** ■ **New machine** ■ **Inactive machine** ■ **Machine changed identity** Enabled inventory automation policies send important alerts to an administrator. If the **On** status is not preserved, the administrator can miss important alerts.
Software components are not displayed in the Catalog after upgrade.	When you upgrade from SMP 7.1 SP 1 to SMP 7.5 and gather inventory, some software components may not be displayed in the Software Catalog. After you run the **NS.Nightly schedule to associate Software component to software product** task, these components are displayed on the **Software Catalog** page, under **Newly Discovered Software**.
Hidden software components are displayed in the Catalog after upgrade.	When you upgrade from SMP 7.1 SP 1 to SMP 7.5 and gather inventory, the software components that should be hidden are displayed in the software products lists on the Software page and Software Catalog dialog box After you run the **NS.Nightly schedule to associate Software component to software product** task, the hidden components will disappear from all software lists.
During the upgrade, Symantec Management Agent stops working on Windows 2008 R2 SP1 client computers.	When you upgrade the Symantec Management Agent from 7.0 or 7.1 to 7.5, it stops working on the Windows 2008 R2 SP1 client computers. On client computers with other operating systems the Agent is upgraded successfully. After you manually start the Symantec Management Agent on the client computer, it continues to function normally.

Table 3-1 Installation and upgrade issues *(continued)*

Issue	Description
During the Inventory Solution Plug-in upgrade, the Symantec Management Agent service can sometimes crash on the client computers.	After you upgrade or migrate to 7.5, during the Inventory Solution Plug-in upgrade, the Symantec Management Agent (SMA) service can sometimes crash on the client computers with the Application Metering Plug-in installed. On the client computer, the following error message is displayed: Agent Altiris.AppMeteringAgent has not stopped. (Stop time limit is 10 sec) Also, a fatal error occurs in modules “AMAgent.dll” and “AeXNSAgent.exe”. To work around this issue, do the following: ■ On the client computer, open the **Run** dialog box, type the Notification Server computer name, and then go to `NSCap`. ■ 2. Copy the AMAgentSetup MSI from the following location: NSCap\bin\Win32\X86\Inventory\Application Metering\Agent Package ■ 3. Double-click the AMAgentSetup or, in the command prompt, run the following command: `msiexec /i <path of msi> skipaim=1` The SMA will start functioning properly after the Application Metering Plug-in is upgraded to 7.5.

During the upgrade from 7.0 MR4, Altiris.AppMeteringAgent and Altiris.InvAgent cannot stop in 10 seconds.	When you upgrade from 7.0 MR4 to 7.5, during the solution plug-in upgrade, the Altiris.AppMeteringAgent and Altiris.InvAgent cannot stop in 10 seconds, and the errors appear in the log.
	To work around this issue, do the following:
	■ On the client computer, in the **Run** box, type the Notification Server computer name, and then go to NSCap.
	■ Copy the AMAgentSetup msi from the following location:
	`NSCap\bin\Win32\X86\Inventory\Application Metering\Agent Package`
	■ Double-click the AMAgentSetup or, in the command prompt, run the following command:
	`msiexec /i <path of msi> skipaim=1`
	After you upgrade Application Metering Plug-in to 7.5, the Symantec Management Agent starts working properly.

Table 3-2 Hierarchy and replication issues

Issue	Description
Replicated custom data class is editable on a child Notification Server computer.	When you create a custom data class, and then replicate the data class from the parent Notification Server computer to its child, the custom data class is editable on the child Notification Server computer A custom data class that is defined on the parent Notification Server computer should never be editable on a child Notification Server computer.
Different region time format settings on parent and child servers lead to incorrect **Days Metered** data display.	If the parent Notification Server and child Notification Server have different region time format settings, the **Days Metered** count on the **Underutilized Software** report page will display incorrect value.
When you replicate a task from parent to child NS, the task advance options can be edited.	When you replicate an inventory task from a parent Notification Server to a child Notification Server in a hierarchy, you can edit the advanced options of the replicated task on the child NS computer. After you edit the advanced options of the replicated task on the child NS computer and click **Save changes**, the changes that you made are not saved. Normally, the advanced settings on the replicated task page should not be editable, and the Save changes and Cancel buttons should not be enabled.

Table 3-3 Other known issues that are common for all types of platforms

Issue	Description
Inventory install, uninstall, and upgrade policies do not run once ASAP in the maintenance window only.	You can check **Run once ASAP** on a policy page to run inventory install, uninstall, and upgrade policies once as soon as possible. However, you cannot currently run the policies once ASAP in the maintenance window only.
Incorrect Install Date in inventory reports.	Inventory reports display incorrect Install Date for installed software products. TECH133481

Table 3-3 Other known issues that are common for all types of platforms *(continued)*

Issue	Description
File inventory is not collected for some software components. As a result, you cannot meter the usage of these software components.	During full inventory scan, file inventory is not collected for the software components that are not .MSI based. You cannot view file inventory data when you right-click a non-MSI based software component, click **Actions > Edit Software Resource**, and then click the **File Inventory** tab. As a result, you cannot automatically meter the usage of this software component as it has no file inventory and is not associated with an executable file. To enable a non-MSI based software component for metering, you should manually add executable files to the software component. For more information, see the topics about association of new program files to metered software components in the *Inventory Solution 7.5 User Guide*.
A license is not reclaimed when the **Asset Status** is set to a custom asset status.	A license is not reclaimed when the **Asset Status** is set to a custom asset status. Inventory Solution license should be reclaimed on setting the **Asset Status** to other than **Active**.
If you create several rules for the same type of files, the delta inventory information will not be sent for those files.	When you create an Inventory policy to gather the information about file properties and, in the **Advanced Options** dialog box, create several rules for the same file type, the S**end inventory changes (deltas)** only will not work for that type of files. Full information will be sent to the Notification Server computer after each inventory scan.

Table 3-4 Other known issues for Windows platforms

Issue	Description
After the NS.Nightly schedule task runs, the Yahoo! Messenger is displayed in the Software Catalog under **Newly Discovered Software** instead of under **Unmanaged Software**.	After you gather inventory, the data about Yahoo! Messenger is not displayed in the Software Catalog. This happens because Software Management Framework is unable to gather the information about the version of this product. After you run the NS.Nightly schedule task, the Yahoo! Messenger is displayed on the **Software Catalog** page, under **Newly Discovered Software** instead of under **Unmanaged Software**.
File scan unable to gather the data if the file type is written in capital letters.	When you configure the advanced options for the Inventory policy and include a file scanning rule for a file type that is not in a default list, the files are not scanned if the file type is written in capital letters.
Data class information is missing because Microsoft IIS version 8.0 drops some registry key.	When you view the data class information in the Resource Manager, on the **IIS Settings** page, the values for some fields are not populated. This happens because Microsoft IIS version 8.0 drops some registry keys and Inventory Solution cannot report inventory for these fields.

Table 3-4 Other known issues for Windows platforms *(continued)*

Issue	Description
A huge number of events is logged into the SMA log during software scan on Windows 8 computers.	When you run a software scan on a Windows 8 computer with trace level logging enabled, numerous events are logged into the Symantec Management Agent (SMA) log. As a result, the SMA log folder size can exceed 1GB. To avoid this issue, disable trace level logging before you run the software scan.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms

Issue	Description
`.Trash` directories must be excluded from a software inventory scan by default when you run the scan on Mac, UNIX, or Linux computers.	If an application is deleted, it is moved to the `<userhome>/.Trash` directory. `.Trash` directories must be excluded from a software scan by default; however currently they are presented in the software scan results. When you run a software inventory scan, you have to manually exclude the `.Trash` and `.Spotlight-V100` folders on the Mac platform and the `.Trash` folder if it exists on UNIX or Linux platforms.
On UNIX and Linux computers, an inventory task keeps running permanently during the software inventory scan on a directory with a large number of items.	When you run software inventory using the `filescan.rule` file on a directory with an extraordinary large number of items, the `swscan.bin` gets completed but the inventory task keeps running permanently and no NSE file is generated. As a workaround, you can use folder or file scanning limitations to reduce the number of scanned items.
The SoftwareScanner does not scan "~" (home directory).	The SoftwareScanner does not process the "~" home directory by the rule: `<folder status="include" scanSubFolders="true">~</folder><folderLimits />`
Inventory task execution on UNIX, Linux, and Mac computers.	When you run software inventory, it is possible to run three inventory tasks simultaneously on UNIX, Linux, and Mac computers. Running three software inventory tasks at the same time results in the system overload and long execution time because CPU usage increases to 100%. As a workaround, you can schedule the tasks to avoid running them simultaneously.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description
On UNIX, Linux, and Mac computers, inventory data is not sent after Inventory Plug-in is redirected to another Notification Server computer and delta inventory is enabled in an inventory task.	After you run some inventory task with delta inventory enabled on one Notification Server computer, redirect Inventory Plug-in to another Notification Server computer, and run another inventory task with delta inventory enabled along with some other types of inventory, only delta inventory data is sent
On UNIX, Linux, and Mac computers, **OS_NFSShare** gets incorrect results if `/etc/exports` contains invalid records.	According to the logic of script, **nfstat** lets you figure out active calls and `/etc/exports` provides you with share points. If `/etc/exports` contains an incorrect entry, the **OS_NFSShare** output gets incorrect results. The system utility `exportfs` controls incorrect entries and filters them when share points are created and listed.
The **UG_UserUsage** script does not detect local login on Solaris platforms.	The **UG_UserUsage** script does not detect entries for any local logins on Solaris platforms.
On UNIX, Linux, and Mac computers, NSE file contains unchanged data after software inventory scan, even if delta inventory is enabled.	When you collect software inventory using the filescan rules with delta inventory enabled for the second time, NSE file contains full inventory data. However, it should contain only the changes in the target directory such as changed number or size of files.
Some values of the **OS_Timezone** data class are reported incorrectly or not reported on HP-UX platforms.	If the time zone is not GMT, the values of the **OS_Timezone** data class are reported incorrectly or not reported on HP-UX platforms. The **StandardName, StandardCaption, StandardOffset** values are reported incorrectly. The **DaylightName, DaylightCaption, DaylightOffset** values are not reported.
Errors in the Notification Server computer log after an inventory policy is run on Linux computer.	When you complete running an inventory policy on Linux computer, you get multiple errors in the Notification Server computer log. The errors notify you that login session start time cannot be set.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description
"Unsupported file filter property" error occurs in the Notification Server computer log after software inventory is collected on UNIX, Linux, and Mac computers.	You can collect software inventory using the filescan rules with the acceptable date format for **LastModifiedDate** such as YYYY-MM-DD HH:MM:SS or YYYY-MM-DD. However, after software inventory is collected on UNIX, Linux, and Mac computers, you get the error "Unsupported file filter property: "LastModified". The filter will be ignored". As a result, the data for last modified date is not collected. To work around the problem, you can create a custom inventory task to collect the data for last modified date.
Some inventory scans may take a long time to complete.	The default inventory task includes several software rules for scanning that can take quite a long time depending on the platform. For example, on Solaris platforms, the **/opt** or **/Volumes** on Mac OS directories contain multiple subfolders and files. On less powerful computers, this can take more than one hour. To avoid this, you can exclude such rules and exactly define the directories that you want to scan.
Inventory scan does not scan deeper than system limitations.	Each operating system has a maximum length paths limitation (though not the file system). For example, for Solaris and Mac OS X, by default the limit is 1024 chars, and for Linux OS, it is 4096. As a result, an Inventory scan does not detect files allocated deeper than the system limitations.
The **Manufacturer** field of the **Storage** data class may be empty.	On UNIX/Linux/Mac OS clients that have IDE disks, the **Manufacturer** field of the **Storage** data class may be empty.
Some fields of the **HW Chassis** data class may be empty on Mac OS X platform.	The fields may be empty for the following reasons: ■ Information for the fields **PartNumber** and **AudibleAlarm** is not available on Mac OS X platform. ■ The availability of the fields **PartNumber** and **SecurityBreach** depends on the current model.
HW_DiskPartition data class cannot be populated on AIX platforms.	On AIX platforms, the logical volume manager (LVM) is used by default, and the current inventory data model is not capable of representing it. The Partition and Volume concept of AIX does not directly match with the fields of the **HW_DiskPartition** data class.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description
Not all inventory data is reported correctly on AIX platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** AIX | **DB_DatabaseStorageArea** | **FileSystemType** for Oracle AIX | **DB_Database** | **Vendor** for MySQL AIX | **HW_PhysicalMemory** | **DataWidth** and **TotalWidth** AIX | **HW_PhysicalMemory** | **Speed** AIX | **HW_PhysicalMemoryArray** | **MaxCapacity** AIX | **HW_Chassis** | **AudibleAlarm, LockPresent, PartNumber, SecurityBreach, SecurityStatus** AIX | **HW_Chassis** | **ChassisPackageType** AIX | **OS_OperatingSystem** | **MaxProcessMemorySize** AIX | **HW_USBDevice** | all fields AIX | **HW_DesktopMonitor** | **Manufacturer, Model, MonitorType, SerialNumber, ManufacturingDate, FeatureSupport** AIX | **SW_BIOSElement** | some firmware fields AIX | **HW_DisplayController** | **MaxMemorySupported, AdapterRAM, MaxRefreshRate** AIX | **HW_Printer** | **DefaultPaperType, HorizontalResolution, VerticalResolution** AIX | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** As a workaround, you can run custom inventory to collect required data on AIX platforms.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description
Not all inventory data is reported correctly on HP-UX and HP-UX IA64 platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** HP-UX | **HW_Baseboard** | some fields HP-UX | **HW_Chassis** | **Manufacturer, AudibleAlarm, LockPresent, PartNumber, SecurityBreach, SecurityStatus** HP-UX | **HW_Chassis** | **ChassisPackageType** HP-UX | **HW_USBDevice** | **USBVersion, SerialNumber, DeviceSpeed** HP-UX | **HW_PhysicalMemory** | **Manufacturer, Speed, DataWidth and TotalWidth** HP-UX | **HW_DesktopMonitor** | **MonitorType, VideoInputMode, ManufacturingDate, FeatureSupport** HP-UX | **HW_SCSIController** | **Index** HP-UX | **SW_BIOSElement** | some firmware fields HP-UX | **HW_DisplayController** | **MaxMemorySupported, AdapterRAM, MaxRefreshRate** HP-UX | **HW_Printer** | **DefaultPaperType, HorizontalResolution, VerticalResolution** HP-UX | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** HP-UX IA64 | **HW_SCSIController** | **MaxTransferRate, MaxDataWidth** As a workaround, you can run custom inventory to collect required data on HP-UX and HP-UX IA64 platforms.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description
Not all inventory data is reported correctly on Linux, Mac, and UNIX platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** RHEL3 | **HW_DesktopMonitor** | all fields for Linux with kernel 2.4 Linux | **HW_Keyboard-Linux** | **Manufacturer** Linux | **HW_PhysicalMemory** | **Model, Manufacturer** Linux | **HW_DesktopMonitor** | **VideoInputMode, SerialNumber, ManufacturingDate, FeatureSupport** Mac | **HW_PointingDevice** | **Type** Mac | **OS_OperatingSystem** | **OSArchitecture, InstallDate, RegisteredUser** Linux, Mac | **HW_Chassis** | **AudibleAlarm, PartNumber, Model** Linux, Mac | **HW_SCSIController** | **Index, MaxDataWidth, MaxTransferRate** Linux, Mac | **HW_DisplayController** | **MaxRefreshRate, VideoProcessor** Linux, Mac | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** Linux, Mac, UNIX | **HW_DesktopMonitor** | **MonitorType** As a workaround, you can run custom inventory to collect required data on Linux, Mac and UNIX platforms.

Table 3-5 Other known issues for UNIX, Linux, and Mac platforms *(continued)*

Issue	Description
Not all inventory data is reported correctly on Solaris platforms.	The inventory for the following data class fields is not correctly collected: **Platform | Data class | Field** Solaris | **OS_OperatingSystem** | **CountryCode, NumberOfLicensedUsers, RegisteredUser, SerialNumber** Solaris | **HW_DisplayController** | **MaxRefreshRate, VideoProcessor** Solaris | **HW_DiskPartition** | **Bootable** Solaris | **SW_BIOSElement** | **BuildNumber, IdentificationCode, Name** Solaris | **HW_DisplayController** | **MaxMemorySupported, VideoProcessor, AdapterRAM** Solaris | **HW_Battery, HW_USBDevice** | all fields Solaris | **HW_SCSIController** | **HardwareVersion, Index, MaxDataWidth, MaxTransferRate** Solaris | **HW_SCSIController** | **HardwareVersion** for **SCSI Fibre Channel Controller** Solaris | **OS_OperatingSystem** | **MaxProcessMemorySize** Solaris x86 | **HW_Chassis** | **Model, AudibleAlarm, PartNumber, SecurityBreach** Solaris SPARC | **HW_PhysicalMemory** | all fields As a workaround, you can run custom inventory to collect required data on Solaris platforms.

Fixed issues

The following are the fixed issues for this release:

Table 3-6 Fixed issues

Issue	Description
The **DMI Version** column in the **Hardware Inventory Search report** does not display any value.	The **Asset Tag** column is empty in the report that is located in **Symantec Management Console**, at **Reports > All reports > Discovery and Inventory > Inventory > Cross-platform > Hardware > Hardware Inventory Search report**. In 7.5 release, the **DMI Version** column has been removed from the report..

Table 3-6 Fixed issues *(continued)*

Issue	Description
On the parent Notification Server computer, no version is displayed for the key program file that is dynamically associated with a software component on a child Notification Server computer.	On a child Notification Server computer, you can collect full inventory and application metering information for the managed software product that has a software component with dynamically associated key program files. However, after replication, on the parent Notification Server computer, the versions are not displayed for the dynamically associated key program files at the following locations: ■ In the **Software Catalog**, when you open the managed software product and view the relevant software component. ■ In the **Executable Usage** report. In 7.5 release, this issue has been fixed.
The reports **Installed Software**, **Underutilized Software**, and **Executable Usage** can show different count of installed software.	If all your target computers have Inventory Plug-in installed, but only some of them have Application Metering Plug-in installed, then after you gather full inventory on all target computers and enable the software-based usage tracking option, the reports **Installed Software**, **Underutilized Software**, and **Executable Usage** show different count of installed software. ■ In the reports **Installed Software** and **Underutilized Software**, the columns **Count** and **Total Installed** respectively show the data for all target computers with Inventory Plug-in. ■ In the **Executable Usage** report, the column **Installed** shows the data for the target computers with Application Metering Plug-in. It is recommended to install Application Metering Plug-in on all the target computers on which you want to track software usage.

Other things to know

The following are the things to know about this release.

The other things to know are separated in the following groups:

- Other things to know
  See Table 3-7 on page 46.
- Changes in the filter description
  See Table 3-8 on page 47.

Table 3-7 Other things to know

<table>
<tr><th>Issue</th><th>Description</th></tr>
<tr><td>Windows 2000 Professional</td><td>This platform is supported only for gathering inventory with stand-alone packages.</td></tr>
<tr><td>Windows 2000 Datacenter Server</td><td>This platform is supported only for gathering inventory with stand-alone packages.</td></tr>
<tr><td>Requirements for UNIX, Linux, and Mac computers.</td><td>To be able to collect the inventory data, ensure that the following requirements are met on your UNIX, Linux, and Mac computers:
■ Perl version 5.6 or later is installed.
■ $PATH environment variable has correct reference to Perl location.
Otherwise you cannot collect all inventory data, and the errors appear in the log.</td></tr>
<tr><td>Process priority settings on UNIX, Linux, and Mac platform.</td><td>The priority of the executed inventory tasks is set to Normal by default. You can change the priority on the inventory policy page, at Advanced > Run Options. It is possible to set the following values: Very Low, Low, Normal, High, Very High.
Use the relevant command to specify the process priority settings accordingly:
<table>
<tr><th></th><th>Linux</th><th>UNIX</th><th>Mac</th></tr>
<tr><td>Very Low</td><td>19</td><td>39</td><td>20</td></tr>
<tr><td>Low</td><td>10</td><td>30</td><td>10</td></tr>
<tr><td>Normal</td><td>0</td><td>20</td><td>0</td></tr>
<tr><td>High</td><td>-10</td><td>10</td><td>-10</td></tr>
<tr><td>Very High</td><td>-20</td><td>0</td><td>-20</td></tr>
</table>
You can change these mapping values in the database, in the Inv_Task_Setting table.</td></tr>
<tr><td>Migrating data class from 6.x.</td><td>When you migrate inventory data from 6.x to 7.5, the data from the AeX AC Inventory Result data class gets migrated to the Inventory Results table.
To view the migrated data, do the following:
■ In the Resource Manager, on the toolbar, click View > Inventory.
■ In the navigation pane, expand Data Classes > Inventory > Operating System > Inventory Results.</td></tr>
<tr><td>On older Solaris SPARC computers, W_Baseboard and HW_Chassis data class information is not collected.</td><td>When you gather hardware inventory, on some older Solaris SPARC computers the HW_Baseboard and HW_Chassis data class information is not collected. These models are, for example, Ultra2, Ultra60, and Netra T1.
On more modern Solaris SPARC hardware, such as SunFire V210, V240 or newer models, regardless of version (9 or 10), this problem does not occur.</td></tr>
</table>

For 7.5 release, the description of several Agent and Plug-in filters has been changed. The changes in the filter descriptions are as follows:

Table 3-8 Changes in the filter description

Filter name	New description
Windows Computers without Application Metering Plug-in	All Windows client computers that do not have the Application Metering Plug-in installed.
Windows Computers Requiring Application Metering Plug-in Upgrade	All Windows client computers that have a version of the Application Metering Plug-in that is older than the version available on the Altiris Notification Server.
Windows Computers with Application Metering Plug-in	All Windows client computers that have the Application Metering Plug-in installed.

Chapter 4

Inventory Pack for Servers

This chapter includes the following topics:

Known issues

The following are the known issues for this release.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

Table 4-1 Known issues

Issue	Description
Server inventory policies report the incorrect database size for Microsoft SQL Server 2000.	You can gather the information about database size for Microsoft SQL Server 2000 with the **Full Server Inventory** and **Delta Server Inventory** policies. However, the policies report the database size as the size of the `.mdf` files (database files) only and do not include `.ldf` files (log files). For Microsoft SQL Server 2005 and 2008, the policies correctly report the sum of the `.mdf` and `.ldf` file sizes as the database size. The database size is presented in round numbers. For example, 2.4 MB are reported as 2 MB, and 2.7 MB are reported as 3 MB.
Full inventory for Microsoft SQL Server 2012 is not gathered when you run an inventory policy or task using the advanced option **System account**.	To gather full inventory for Microsoft SQL Server 2012 with the predefined policy or a custom inventory policy or task, you need to select the advanced option **Logged in user** on an inventory policy or task page, at **Advanced Options > Run Options**. If you run an inventory policy or task using the advanced option **System account**, the data is not gathered for all server inventory data classes and not all the database users are reported.

Table 4-1 Known issues *(continued)*

Issue	Description
A license is not reclaimed when the **Asset Status** is set to a custom asset status.	A license is not reclaimed when the **Asset Status** is set to a custom asset status. Inventory Pack for Servers license should be reclaimed on setting the **Asset Status** other than **Active**.
An inventory task with the disabled MySQL dataclass but with valid MySQL credentials collects MySQL data on Linux computers.	If you create an inventory task with the MySQL dataclass unchecked in the **Advanced** options, on the **Data Classes** tab, and then, on the **Run Options** tab, select valid MySQL credentials, the inventory task still collects MySQL data on target Linux computers. MySQL data must not be collected if no MySQL dataclass is checked in the inventory task.
The Inventory policy or task that runs with the root rights when collecting the inventory on SUSE Linux Enterprise Server or on AIX is not able to log into the Oracle database.	The Inventory policy or task, if not specified otherwise, runs with the root rights by default. However, on SUSE Linux Enterprise Server and on AIX it is not possible to access Oracle applications while you are logged in as a root user. Because of that, the Inventory policy or task that runs with the root user credentials is not able to log in to the Oracle database. This problem does not occur on Red Hat Enterprise Linux, Solaris, and HP-UX Oracle servers. As a workaround, you can create an inventory policy or task that collects inventory for Oracle data classes only and runs with non-root user credentials. To do so, perform the following steps: 1 In the **Symantec Management Console**, click **Manage**. 2 ■ To create the corresponding inventory policy, click **Policies > Discovery and Inventory > Inventory**. ■ To create the corresponding inventory task, click **Jobs and Tasks**. In the left pane, navigate to the folder where you want to create an inventory task, right-click the folder, and then click **New > Task**. 3 On the inventory policy or task page, click **Advanced**. 4 On the **Advanced Options** page, on the **Data Classes** tab, expand **Server Inventory data classes > Databases**, and then check the **Oracle** data class. 5 On the **Run Options** tab, under **UNIX**, specify non-root user credentials. 6 Click **OK**. 7 Click **Save changes**.

Table 4-1 Known issues *(continued)*

Issue	Description
Traces in the log files.	On the target computer, Inventory Pack for Servers tries to inventory the data classes for various supported server components, such as Microsoft Exchange Server, Microsoft IIS Server, and so on, irrespective of whether server components are present. This does not result in slowing down the inventory process. However, some traces, like “Could not collect the inventory information for xxxx”, “Failed to collect inventory for xxxx”, “Execution of query Failed”, or “Failed to inventory information from WMI. Error: … ” are added to the log files when you run an inventory task for gathering server data classes with the **Enable verbose client logging** option selected at **Advanced option > Run Options**.
The **DHCP Scopes** and **DHCP Options** data classes incorrectly report the values that have double quotes.	When you define the DHCP scopes and use double quotes in the description (for example, **DHCP Scope Configuration for “Altiris” company**), the **Description** column of the **DHCP Scopes** data class reports a value only up to the first double quotes. In the given example it returns only **DHCP Scope Configuration for**. This limitation also applies to the **Scope Id** and the **Super Scope** columns of the **DHCP Scopes** data class and the **Scope Id** column of the **DHCP Options** data class. The same limitation also applies to the `netsh exec filename` command provided by the DHCP Server. This command is used to import the DHCP configuration details from the text files.
The reported version of the DHCP server does not match with the DHCP version given in the **About** dialog of the DHCP server.	The **Version** column of the DHCP data class reports the DHCP version that is different from the version given in the **About** dialog of the DHCP server.
IIS Inventory.	■ The IIS inventory that is gathered for the **IIS Application Pools** data class automatically starts the IIS Admin service if it is in a stopped state. ■ The **Application Server Console Installed** and **Remote Admin Installed** fields from the **IIS Setting** data class are not reported on Windows Server 2008 for IIS 7.0. The Inventory plug-in gathers the IIS inventory using IIS metabase. IIS metabase is fully supported until IIS version 6.0. With IIS version 7.0, on Microsoft Windows Server 2008, IIS metabase has been replaced by XML configuration files. To gather the IIS 7.0 inventory, you need to install the Management Compatibility features by using “Server Manager” on Microsoft Windows Server 2008.

Table 4-1 Known issues *(continued)*

Issue	Description
IIS Inventory data classes are reported incorrectly.	With IIS 7.0 installed on Microsoft Windows Server 2008, some fields of the following IIS data classes are not populated correctly, even if the Management Compatibility features are installed. Fields of **IIS Http VirtualDir Setting Data** data class: ■ Content Location ■ Default Document Enabled ■ Default Document Name ■ Script Source Access Enabled ■ Access Read Enabled ■ Access Write Enabled ■ Directory Browsing Enabled ■ SSL Access Enabled ■ Content Expiration Enabled ■ Content Expiration Setting ■ Log Enabled ■ Execute Permission Fields of **IIS Http Host Setting Data** data class: ■ Content Location ■ Default Document Enabled ■ Default Document Name ■ Script Source Access Enabled ■ Access Read Enabled ■ Access Write Enabled ■ Directory Browsing Enabled ■ SSL Access Enabled ■ Content Expiration Enabled ■ Content Expiration Setting ■ Log Enabled ■ Execute Permission Fields of **IIS Http Server Setting Data** data class: ■ Central Binary Logging Enabled ■ Rapid Fail Protection Interval ■ Rapid Fail Protection Max Crashes

Table 4-1 Known issues *(continued)*

Issue	Description
Prerequisite for gathering the inventory of **Exchange Mailboxes** data class.	On a freshly installed operating system, before executing a server inventory standalone package or a server inventory task for gathering Microsoft Exchange Server data classes, you must explicitly install the Microsoft Visual C++ 2005 SP1 Redistributable Package (x86). Otherwise, the inventory for the data class **Exchange Mailboxes** is not gathered. The Microsoft Visual C++ 2005 SP1 Redistributable Package (x86) installs runtime components of Visual C++ Libraries that are required to run the applications that use these runtime components. Server Inventory plug-in depends upon these libraries and runtime components. You can download the package for free at http://www.microsoft.com/downloads/details.aspx?familyid=200b2fd9-ae1a-4a14-984d-389c36f85647&displaylang=en
Exchange Server Inventory.	■ On Windows 2003 operating system, inventory of the **Exchange Mailboxes** data class is only populated when you use “Logged In” user context. ■ On Windows 2000 Server Operating System, inventory of the **Exchange Mailboxes** data class are not populated. ■ Inventory for Microsoft Exchange Server 2007 is not supported. ■ Exchange Inventory does not return data from Exchange Server Clusters.
SQL Server Inventory.	■ The **License Type** and **Number of License** fields are not populated in the **SQL Server License** data class. ■ If multiple instances of SQL Server are installed on the target computer, the **Inv Srv SQL Database Service** data class reports the service name without including the prefix “MSSQL$”. Inventory reports incorrect SQL instance name if a user changes the name of target computer after installing Microsoft SQL Server on it. In this case the previous name of the computer would be reported as an SQL instance name in the SQL Server data classes.

Table 4-1 Known issues *(continued)*

Issue	Description
Oracle inventory.	Inventory Pack for Servers Plug-in for Windows does not implement the logic for populating the following fields: ■ The **Block Size** field of the **Oracle Database** data class. ■ The **Block Size** and **File System Size** fields of the **Database Storage Area** data class for Oracle 9i. ■ The **Users High Watermark** field of the **Oracle Database Service** data class. On Microsoft Windows Server 2008, the following data classes are not reported, or if reported, do not contain the inventory for Oracle: ■ **Oracle Database Service** ■ **Database System** ■ **Database Service** ■ **Associate Database System to Service**
MySQL inventory.	■ MySQL details for the **DB_Database Service** data class are not populated when MySQL service is stopped. ■ Inventory of installations of multiple instances of MySQL Server on a computer is not supported. If multiple instances are installed, the inventory is gathered for the first instance that is found.
Database inventory.	■ If you select any kind of database inventory (for example, Oracle, MySQL or MS SQL) from the data class treeview, Inventory will gather data for almost all the databases (Oracle, MySQL, and MS SQL) installed, irrespective of selection in the treeview because most of the data classes are common among them. ■ If you disconnect from the registered server running SQL Server through SQL Server Enterprise Manager by right-clicking the server name and clicking the **Disconnect** menu, then after gathering the inventory, the **Operational Status** property of the **Database Service** data class is not reported.
Running an inventory task in the **Specified User** context fails.	As a workaround, please execute the inventory task in the **System** user context or in a **Logged In** user context.

Table 4-1 Known issues *(continued)*

Issue	Description
Apache Web Server.	■ Only a single instance of Apache Server is supported. ■ Server Inventory Plug-in does not implement the logic for populating the **Host State** field of the **Http Host** data class for Apache Servers. This field is not populated in any scenarios with Apache Server. ■ If you tag some modules that are compiled statically, the properties under such a section are retrieved and displayed without checking the specific module condition. ■ (Windows only) If the value for the **KeepAliveTimeout** parameter is specified in the configuration file `httpd.conf` of Apache Web Server, then after gathering the inventory, NSE loading fails for the data class **Http Host Setting Data** on Notification Server.
Hardware inventory on Windows Server 2003 R2 SP2 (x86) computers reports incorrect processor count.	When you collect hardware inventory from Windows Server 2003 R2 SP2 (x86) computers, the number of physical processors is reported incorrectly. This happens when the client computer uses either hyperthreading-enabled processors or multicore processors because Windows Server 2003 cannot detect them. For more information on this issue and a hotfix, please see the following links: http://support.microsoft.com/kb/936235 http://support.microsoft.com/kb/932370

Other things to know

The following are the things to know about this release.

The other things to know are separated into the following groups:

- Other things to know
  See Table 4-2 on page 54.
- Changes in the filter description
  See Table 4-3 on page 56.

Table 4-2 Other things to know

Issue	Description
SQL Server inventory in Specified User or Logged-in User context.	Inventory Pack for Servers gathers inventory for SQL Server using the **Windows Authentication** method. When using the Specified User or Logged-in User context to gather inventory for SQL Server, the user must have access rights to connect to SQL Server, otherwise the inventory for SQL Server will not be gathered.

Table 4-2 Other things to know *(continued)*

Issue	Description
Disabled **Auto Growth** causes blank reports for some data classes.	**Data File Growth Mode** and **Data File Growth Size** fields from **MS SQL Server Databases** data class for a database will return blank whenever **Auto Growth** property for that database is disabled.

Accepted MySQL connection parameters for Inventory tasks.	To access the **MySQL Credentials** dialog box, perform the following steps in order:
	■ Open an inventory task.
	■ In the right pane, click **Advanced**.
	■ In the **Advanced Options** dialog box, on the **Run Options** tab, under **MySQL**, click the **Add** symbol.
	You must specify the user name and password to connect to the MySQL Server and collect the inventory data. Specify the other connection parameters only when they differ from the default values.
	On Windows, you can specify the following connection parameters:
	■ `--host=host:port`
	Default port is 3306
	On UNIX and Linux, you can specify the following connection parameters:
	■ `--protocol={TCP|SOCKET}`
	Default protocol is SOCKET
	■ `--port=port_num`
	Default port is 3306
	■ `--socket=path`
	Default socket file is `/tmp/mysql.sock`
	You can use the following examples:
	■ To specify TCP/IP connection with port 13306:
	`--protocol=TCP --port=13306`
	■ To specify UNIX socket file `/var/lib/mysql/mysql.sock`:
	`--protocol=SOCKET --socket=/var/lib/mysql/mysql.sock`
	For more information about connecting to the MySQL Server, please refer to the following URL:
	http://dev.mysql.com/doc/refman/5.0/en/connecting.html

Table 4-2 Other things to know *(continued)*

Issue	Description
Oracle Database (Windows only).	■ For gathering Oracle Database Inventory, inventory component establishes connection with the database. The user credentials provided to connect to the Oracle database must have SYS DBA privileges to gather the Oracle inventory successfully. ■ If multiple instances of Oracle are installed, and user wants to gather inventory from that computer, then each database instance entry should be present in all `tnsnames.ora` files. That means that all the `tnsnames.ora` files related to each Oracle instance should be identical. For that to happen, a user should replicate the database entries from one `tnsnames.ora` to another. The location for `tnsnames.ora` file is `OracleHome\Network\Admin`.

For 7.5 release, the description of several Agent and Plug-in filters has been changed. The changes in the filter descriptions are as follows:

Table 4-3 Changes in the filter description

Filter name	New description
Windows Computers Requiring Inventory Pack for Servers Plug-in Upgrade	All Windows Server computers that have a version of the Inventory Pack for Servers Plug-in that is older than the version available on the Altiris Notification Server.
Windows Computers with Inventory Pack for Servers Plug-in	All Windows Server computers that have the Inventory Pack for Servers Plug-in installed.

Chapter 5

Inventory for Network Devices

This chapter includes the following topics:

Known issues

The following are the known issues for this release.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

Table 5-1 Known issues

Issue	Description
Separate licenses for Inventory for Network Devices are displayed in the Symantec Management Console.	Inventory for Network Devices should share licenses with Inventory Solution. Currently the licenses for these two products are separately listed in the Symantec Management Console. However, the licenses are shared, and Inventory Solution license is consumed for every device that is inventoried by Inventory for Network Devices.
Custom SNMP data mapping tables are not displayed after migration to 7.1 SP2	Custom SNMP data mapping tables migrate from 6.x and 7.0 to 7.1 SP2 but are not displayed on the SNMP data mapping tables page.

Fixed issues

The following are the fixed issues for this release.

Table 5-2 Fixed issues

Issue	Description
The reports in the **Agentless Inventory** folder belong to Network Discovery.	The folder has been renamed. The Network Discovery reports are now located at **Symantec Management Console > Reports > All reports > Discovery and Inventory > Discovery**.

Other things to know

The following are the things to know about this release:

Table 5-3 Other things to know

Issue	Description
Hierarchy and replication support.	All discovered agentless inventory resources (computers, routers, switches, etc.) replicate up to the parent Notification Server. Predefined SNMP data mapping tables replicate down from the parent Notification Server to the child Notification Servers. Possible workaround: To manually replicate a custom SNMP data mapping table down from the parent Notification Server to child Notification Servers do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **All Settings**. ■ In the left pane, expand **Notification Server > Resource and Data Class Settings > Data Classes > Network Resource Data**. ■ In the left pane, under **Network Device Data**, right-click the custom SNMP data mapping table that you want to replicate, and then click **Hierarchy > Replicate Now**. ■ In the confirmation dialog box, click **OK**.

Table 5-3 Other things to know *(continued)*

Issue	Description
Security and permissions.	The Symantec Management Platform provides role-based security. The Administrator role has all rights to perform all agentless inventory tasks. For other users, you can assign rights to different roles. The following are the unique privileges for Inventory for Network Devices: ■ Read SNMP Table. Lets you access the SNMP Table Mappings page for initial viewing. ■ Import SNMP Table XML. Lets you import SNMP Table mapping definitions as .XML. ■ Manage SNMP Tables. Lets you create, delete, and edit existing SNMP user tables. **Note:** Predefined tables cannot be edited. ■ Test SNMP Table Mappings. Lets you use the test SNMP functionality on the SNMP Table Mappings page.

Chapter 6

Monitor Solution for Servers

This chapter includes the following topics:

What's new in this release

In Monitor Solution for Servers 7.5, the following new features are introduced:

Table 6-1 List of new features in Monitor Solution

Feature	Description
New rule and metrics aggregation logic.	New aggregation logic is introduced in Monitor Solution 7.5 to allow the following capabilities: ■ Monitor multiple instances for multiple metrics at the same time. For example, one rule can simultaneously monitor free space and usage metrics on multiple hard drives. ■ Bring down the amount of the alerts to a more easily managed number.
Event Console on Silverlight	Event Console is now running on Silverlight.

Known issues

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

The known issues are separated into the following groups:

- Monitor Solution
  Table 6-2
- Event Console
  Table 6-3

Table 6-2 Known issues for Monitor Solution

Issue	Description	Article Link
A client computer operating in Cloud-enabled Management (CEM) mode is available for Reset Monitored Resource task run.	In some cases, monitored resource that is managed in CEM mode is available as a target for Reset Monitored Resource task. This situation appears if you run the task using **Quick Run** or **New Schedule** run options.	N/A
Details of forwarded alerts are not displayed correctly on the Management Station console.	After you add and save a new rule, and then send alerts based on the rule, the categories Hostname, Definition, and Protocol are not displayed correctly on the Management Station console	N/A
Customized Monitor rollout policy targets are rewritten with default values during upgrade.	When you upgrade to Monitor Solution 7.1 from 7.0 SP4 HF1, all customized targets for the Monitor Plug-in rollout policies are rewritten with default values.	N/A
Incorrect heartbeat alert behavior on a virtual machine.	A heartbeat alert may be raised in Event Console from a monitored resource that runs on a virtual machine, even if it is online and the metric provider is running.	N/A
Monitor token values that include double quotes cause VBScript tasks to fail.	If you have a VBScript client side task that is associated with a rule and the output from a token produces double quotes, the VBScript fails.	TECH154599
The **Disk Paging Activity** report displays incomplete data.	The **Disk Paging Activity** report displays incomplete HP-UX and AIX data when it is viewed in the Chart View.	N/A

Table 6-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Agentless monitoring uses Pluggable Protocol Architecture (PPA) connection profiles.	The Remote Monitoring Server (RMS) agent leverages PPA to make connections to monitored remote resources to obtain metric data. PPA references the connection profiles used during Network Discovery. The Network Discovery connection profiles define which protocols are enabled and any applicable credentials and settings for each protocol. When the RMS agent attempts to monitor an agentless resource, it queries the database and uses the connection profile that was used during Network Discovery. If the RMS agent cannot find a reference to a connection profile, the Default connection profile is used. To select a different connection profile, run a new Network Discovery and select the desired connection profile for remote resources.	N/A
Unable to assign a connection profile to a resource.	On the **Manage Connection Profile** page, when you create connection profiles for different configured clients, the user is not able to assign (to map) connection profiles to the resources.	N/A
WS-Management service cannot process the request on Windows clients.	WS-Management service does not work on Windows clients because it cannot process the request. The service cannot find the resource that the resource URL and selector identify.	N/A
Time drifting issues occur when monitoring heartbeats on Linux computers that are hosted on VMware.	When monitoring heartbeats on Linux computers that are hosted on VMware, there are issues with time drifting. This issue can cause Notification Server to receive heartbeats after a very long delay and an alert to be raised in the Event Console. To avoid issues with unnecessary alerts in the Event Console, make sure that your heartbeat time settings are synchronized to account for possible time drifting.	N/A
The Poll Metric on Demand task cannot poll agent-based metrics on a computer that does not have the Monitor Plug-in.	The **Poll metric on demand** task can poll two different types of metrics: agent-based and agentless. It is supported on two different types of targets: with and without Monitor Plug-in. If the **Poll metric on demand** Task is executed on an agentless target without the Monitor Plug-in installed, then it can only poll agentless metrics on that computer. Agent-based metrics are not polled on an agentless client computer as agent-based metrics require the Monitor Plug-in to run.	N/A

Table 6-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Network Discovery found devices may not be listed in the targeted filters of the default agentless policy.	Agentless monitor policies target filters of computers and devices. By default, the target includes only unmanaged devices running Windows 2003 or 2008. When computers are discovered, the local operating system is a property of that computer resource. If during discovery, a computer's operating system cannot be determined, an operating system-specific filter does not recognize that computer. If an agentless monitor policy is not running on a computer as expected this issue is a possible cause. **Note:** The operating system version is correctly discovered for the target computers that have SNMP enabled.	N/A
A failed heartbeat may not raise an alert if the **Check for heartbeat every** option is less than the **Send heartbeat every** option with zero retry attempts.	A failed heartbeat may not raise an alert in the Event Console due to network latency when you have the following configuration: ■ The **Retry every** option on the **Heartbeat** tab of the **Monitor Server Settings** page has a value of "0". ■ The value of the **Check for heartbeats every** option is less than or equal to the **Send heartbeat every** option on the **Data Collection** tab of the **Monitor Plug-in Configuration Settings** page. In this case, a Monitor Plug-in may appear to occasionally go down only to come right back up again. However, the uptime data is not affected in this case.	N/A
Agentless monitoring is not available for the targets that have been discovered through an Active Directory Import.	You cannot apply agentless monitor policies to targets that have been discovered through an Active Directory Import. **Workaround:** Use a Network Discovery or a WINS import instead of an Active Directory Import.	N/A
You must reconnect the Real-time Performance Viewer if metric data becomes unavailable.	When you use the Real-time Performance Viewer, if a metric becomes unavailable and then becomes available again, updated data is not displayed. The viewer continues to display the data value that was last received before the metric became unavailable. The Real-time Performance Viewer must be re-connected to the target computer before updated data is reflected in the viewer.	N/A
Monitor RMS 7.0.2671 RMS cannot get information for HTTP metrics from password-protected resources.	In some cases Monitor RMS 7.0.2671 RMS cannot get information for HTTP metrics from password-protected resources.	N/A

Table 6-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
There is a delay in the Computers List for the Real-time Viewer and Historical Performance Viewer.	Computers are not populated in the Computers List for the Real-time Viewer and Historical Performance Viewer until data is received from the target computer by Notification Server.	N/A
When "Altiris" log type is selected, the Log Event metric only supports Windows platforms.	When the "Altiris" log type is selected, the Log Event metric uses Notification Server log file as source. This type of log is supported for Windows platforms only.	N/A
HTTP metrics do not support virtual hosts.	The HTTP metric cannot be used with virtual hosting. The HTTP metric only supports the use of the current host name of a physical computer that reports basic inventory to the Notification Server computer.	TECH40807
An error occurs when you export a monitor pack to Windows Vista and Windows Server 2008 with active IE protected mode.	The monitor pack's .XML file is copied to the \temp\ folder instead of the intended path. In this case, completing the import process from this location would fail. This error occurs when you export a monitor pack to a Windows Vista or a Windows Server 2008 computer with Internet Explorer protected mode ON.	N/A
WMI metrics read the data with the lowest polling interval.	If two WMI metrics are configured to parse the same command output and they both have different polling intervals, these metrics read the data with the lowest polling interval. The WMI metrics combine into a similar query for optimization. The query runs at the lowest interval setting.	N/A
Polling metric on-demand task fails.	If you add the **Poll metric on demand** task to a policy or to a rule, then the task fails to run when the rule is activated. The task completes successfully when manually executed.	N/A
False information about ESX in 7.5.	During the upgrade from 7.0 MR4 to 7.5 following error appears in the log during Monitor Solution configuration: "Item attributes (NoDelete, System) do not include deletion for: 'Monitor Agent for ESX – Upgrade". In 7.5 "Monitor Agent for ESX – Upgrade" policy is available in the console, but not functional, since VMware ESX is not supported in 7.5. These errors do not affect functionality and should be ignored.	N/A

Table 6-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Remote Monitor Service (RMS) is not supported for site servers with Windows Server 2102 in 7.5.	Windows Server 2012 is not supported as site server for RMS in 7.5. However, the installation is not blocked. Resources with Windows Server 2012 can be selected during RMS site server installation. Installation does not proceed, a "Pending/Not installed" status is displayed. The process of installing RMS cannot be carried out due to resource target limitation. In the **Add/Remove Services** dialog box, check **Monitor Service** to be installed on a Windows Server 2012 site server at your own risk. Symantec also recommends not to install RMS on Windows Server 2012 site servers manually, since that produces unstable results.	N/A
Exceptions appear during upgrade from version 7.0 to 7.5.	Exceptions that contain "You must either specify a resource key or a resource GUID when creating a resource" appear in the NS log. These exceptions are temporary, have no functional impact and disappear as soon as the agent creates the resources.	N/A
Manually created Monitor site servers disappear after disaster recovery.	Monitor site servers that are created manually disappear after disaster recovery. You need to manually create them again.	N/A
Custom resource collections are imported incorrectly during migration from 6.x to 7.5.	Data about custom resource collections exported during migration from 6.x to 7.5 does not contain full amount of information required to continue using custom targets. You need to manually create them again.	N/A
SQL metric default connection data must be provided to configure **All Windows Servers** policy.	It is possible to save the **All Windows Servers** policy configuration, without providing all information required under **SQL metric default connection**. To use SQL metrics you must provide information in all fields under **SQL metric default connection**. You do not have to provide all data, if you do not intend to use SQL metrics.	N/A
Log Event metric for FTP log file with "Unlimited file size" setting produces incorrect results	On Windows Server 2003 or Windows Server 2008, the **Log Event** metric for the FTP log file, with the "Unlimited file size" setting enabled, during the agent-based monitoring, triggers the rule incorrectly. When FTP log file size is set to unlimited, Monitor Agent functionality does not allow to determine when changes are made to the log and metric data in not parsed by the Agent from the FTP log file. **Workaround:** Set a constant file size (for example, 64K) for the FTP log file, instead of unlimited, when configuring **Log Event** metric.	N/A

Table 6-2 Known issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Aggregation can only evaluate metrics if they monitor an equal number of instances.	If one of the two metrics inside the rule monitors more instances, than the other one, the aggregation logic evaluation may produce unexpected results.	N/A
Policies may get overwritten, when creating multiple policies in a new window or from the Server Management Suite portal.	On the **Home** menu click **Monitoring and Alerting**. In the left pane expand **Monitor > Policies**, and then right-click the name of the policy, and click **Open in New Window**. If several policies are created in the same manner, every subsequent policy rewrites all the previous ones. When policies are turned on from the Server Resource Manager View of the Server Management Suite Portal, the same result is produced – last policy overwrites all previous ones. **Workaround:** To get back the overwritten policies, re-import the rewritten monitor packs manually. All monitor pack settings will also be reset to default in this case.	N/A

Table 6-3 Known issues for Event Console

Issue	Description	Article Link
It is not possible to export or import **Alert Rule Settings** from **Event Console**.	It is not possible to export and import **Alert Rule Settings** from the **Event Console** page. **Workaround:** On a source server, do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **Monitoring and Alerting**. ■ In the left pane, expand **Event Console**, and click **Alert Rule Settings**. ■ In the right pane, right-click each rule, and then click **Export**. ■ Save the rules. On a target server, do the following: ■ In the Symantec Management Console, on the **Settings** menu, click **Monitoring and Alerting**. ■ In the left pane, expand **Event Console**, and click **Alert Rule Settings**. ■ In the right pane, right-click on any item in the list, and then click **Import**. ■ Select the previously saved rules.	N/A

Table 6-3 Known issues for Event Console *(continued)*

Issue	Description	Article Link
The **Acknowledge** and **Resolve** options become disabled in some cases.	When you select multiple alerts holding down the Shift key, the **Acknowledge** and **Resolve** options on the toolbar become unavailable. **Workaround:** Right-click any of the selected items and click **Acknowledge** or **Resolve**.	N/A
In the **Event Console**, the **Select Filter** text box does not support Double-byte Character Sets (DBCS) input.	In the **Event Console**, the **Select Filter** text box has a limitation. The DBCS input is not supported from neither a physical keyboard, nor using the IME virtual keyboard. **Workaround:** You can copy DBSC text and paste it into the **Select Filter** text box.	N/A
Internet Explorer error message for "about:blank" pops up.	Internet Explorer error message for “about:blank” pops up: "Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration". **Workaround:** "about:blank" needs to be added into the **Trusted sites** list of the Internet Explorer.	N/A

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:

- Monitor Solution
  Table 6-4
- Event Console
  Table 6-5

Table 6-4 Fixed issues for Monitor Solution

Issue	Description	Article Link
After upgrade the Remote Monitor Server becomes uninstalled.	After completing the upgrade from IT Management Suite 7.1 MP1 to IT Management Suite 7.1 SP2 the Remote Monitor Server x86 and Remote Monitor Server x64 automatically become uninstalled.	N/A

Table 6-4 Fixed issues for Monitor Solution *(continued)*

Issue	Description	Article Link
Uninstalling Monitor Solution does not remove all its items.	When you uninstall Monitor Solution, some of the Monitor Solution related tasks (for example, Monitor License status and Monitor Purge item) remain on the server and continue working.	N/A
The **Create a monitor policy** wizard stops responding.	The **Create a monitor policy** wizard stops responding if, in the **Choose what to monitor** panel, you click **Next** or **Finish** without entering a name for the policy.	N/A
A customized view of a Monitor Solution report is not preserved after the report refreshes.	After you customize the view of a Monitor Solution report, the customizations to the view are lost when the report is refreshed. The report then displays the default view.	N/A

Table 6-5 Fixed issues for Event Console

Issue	Description	Article Link
Event Console page refreshes every hour.	When the Event Console page refreshes, it resets the filter to the default value. The Event Console page is refreshed every hour to prevent memory leak.	N/A
Event Console Web Part does not appear.	The Event Console Web Part should appear on the Resource Manager Portal page that is accessed from the Home menu of Resource Manager. However, the Event Console Web Part currently does not display. You must contact support for a point fix to resolve this issue.	N/A

Other things to know

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

The other things to know are separated into the following groups:

- Monitor Solution
  Table 6-6
- Event Console
  Table 6-7

Table 6-6 Other things to know about Monitor Solution

Items	Description	Article Link
You may need to install `sysstat` on your monitored Linux computers.	You must install `sysstat` on your targeted Linux computers to use the following monitor policies: ■ Processor ■ Disk I/O ■ Memory ■ Linux Server Health	N/A
The repeat count feature specifies the number of times the rule must trigger in a row before an action is taken.	After the repeat count specified in a rule has been reached, the rule resets to "normal" on the next value, even if that value crosses the threshold. If the value crosses the threshold, the rule restarts the repeat count for the next evaluation. Example: Rule count definition - if CPU > 10 for three times. If the values are 11, 12, 13, 11, the rule triggers on the third value and then resets to normal on the fourth value. **Note:** Repeat count for rule increases for each condition which is met instead of for the overall criteria for the rule.	N/A
Activated Monitor Policies Web Part only shows the policies that the Monitor Plug-in has activated.	The Monitor Plug-in must first activate a monitor policy before it is displayed in the **Activated Monitor Policies** Web Part of the **Monitoring and Alerting** home page. If you enabled a monitor policy but it is not yet displayed in the Web Part, it might be because the Web Part is populated from inventory data that is received from the plug-in	N/A
Purging log event and Syslog data.	Both log event and Syslog data purging is controlled with the single String metric data purging schedule. To schedule string metric data purging: 1 In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**. 2 In the left pane, click **Monitoring and Alerting > Monitor > Settings > Monitor Server Settings**. 3 On the **Monitor Server Settings** page, click the **Purge Maintenance** tab. 4 Under **Non-numeric Data**, set the value for **String metric data**. 5 On the **Monitor Server Settings** page, click **Save changes**.	N/A

Table 6-6 Other things to know about Monitor Solution *(continued)*

Items	Description	Article Link
The specific setup is required to enable Smart Metrics using SNMP.	To enable Smart Metrics using SNMP: ■ The SNMP service must be installed on the monitored computer. ■ The community name must be configured in the SNMP service on the monitored computer. The community name must match the community string in the SNMP protocol settings for your connection profile. ■ SNMP packets must be accepted from any host in the SNMP properties on the monitored computer.	N/A
How WMI Metric handles WMI property arrays.	In some cases WMI property values are stored as arrays of values. In this case, each property in the array is represented as a different instance\value pair for the metric. The name for instance is "Name of the instance (n)" where n is the index. For example, if % disk space had multiple properties for disk space: "C: (1)" = 23, "C: (2)" = 43, "D: (1)" = 54, "D: (2)" = 7	N/A

Table 6-7 Other things to know about Event Console

Items	Description	Article Link
Help is not available on the **Workflow rule** tab.	On the **Workflow rule** tab of the **Alert Rule Settings** page, the context-sensitive Help may not appear when you click F1. To display the context-sensitive Help for the **Workflow rule** tab, you must first create a workflow rule and click on the Web Part that contains the rule before clicking F1.	N/A

Chapter 7

Monitor Pack for Servers

This chapter includes the following topics:

What's new in Monitor Pack for Servers 7.5

In Monitor Solution 7.5, the following new features are introduced:

Table 7-1 List of new features in Monitor Solution

Feature	Description
A new Monitor Pack for Windows 2012.	A new Monitor Pack for Windows 2012 has been added.
No Monitor Pack for ESX	Monitor Pack for ESX has been removed.

Known issues

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

Table 7-2 Known issues

Issue	Description	Article link
After upgrade, all user modifications of the default policies, rules, and metrics are overwritten.	Any default rule or metric settings are reset to their default values after migration. If you modified a default monitor pack policy to include your custom metrics, the rules and metrics are not migrated. Instead, these settings are lost. Only monitor pack cloned policy settings, cloned rule settings, and cloned metric settings are migrated. To work around this issue, you can create clones of these policies. Your new custom monitor policies can then be migrated. For more information, see topics on monitor packs in the IT Management Suite Migration Guide version 7.0 to 7.5.	N/A

Fixed issues

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

Table 7-3 Fixed issues

Issues	Description	Article Link
The metric **ASP.NET % Processor Time (w3wp)** from **Windows 2003** pack goes to retry state even though the corresponding counter works on the client.	The metric **ASP.NET % Processor Time (w3wp)** from **Windows 2003** pack goes to retry state even though the corresponding counter works on the client. The metric works successfully on an IIS server with constant ASP.NET activity. The w3wp process is only started for a short time by ASP feature use. Some time after the use of ASP, if there are no requests, the w3wp process stops. On servers with occasional ASP.NET activity the metric goes to retry state as the w3wp process does not work constantly. While it waits for another polling try, it can miss the w3wp process activity. As a consequence, it never leaves the retry state even if the w3wp process is running.	N/A

Other things to know

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

Table 7-4 Other things to know

Issue	Description	Article link
You need to install **sysstat** on your targeted Linux computers.	You need to install **sysstat** on your targeted Linux computers to use the following monitor policies: ■ Processor ■ Disk I/O ■ Memory	N/A
Informational Rules are migrated from 7.0 to 7.1.	Informational Rules are migrated from 7.0 to 7.1. Informational rules are now removed from default monitor policies. As a consequence, all informational rules that are migrated from 7.0 to 7.1 have no reference to default policies. You can find them in the **Rule Library**. **Note:** Apache Server Log informational rules for AIX/Linux/Solaris stay because Apache Server policy contains only informational rules.	N/A
Platforms that Monitor Pack for Servers does not support.	Monitor Pack for Servers does not support the following platforms: ■ Windows 2000 Server. ■ RHEL 3. ■ SLES 9. ■ ESX ■ Windows 2008 Core (32- and 64-bit) agent-based. ■ Windows 2008 R2 Core agent-based.	N/A
Available memory dropped below 4 MB rules cannot be edited.	In the **Rule Library**, the **Available memory dropped below 4 MB** rules cannot be edited for agent-based and agentless monitoring. A warning appears: `This name is already in use by another item of the same type. Select a different name.` A solution is to save the rule with a different name.	N/A
Current bandwidth is not reported on VMware client systems running RHEL.	Current bandwidth is not reported on VMware client systems running Red Hat Enterprise Linux (RHEL). VMware Tools are required. After VMware Tools are installed and configured on the system, the command line or utility application querying for current bandwidth information returns results.	HOWTO10695

Table 7-4 Other things to know *(continued)*

Issue	Description	Article link
The command `mailq` should not be used in certain metrics. It can generate a heavy load.	In some situations the command `mailq` can generate a heavy load on Solaris computers. The following metrics may fail to execute in the specified timeout if you use the `mailq` command: ■ **SMTP Server - Mail Queue Size Solaris** ■ **SMTP Server - Number of Deferred Messages Solaris** The cause of the heavy load is suspected to be due to the wrong configuration of FQDN on the server.	N/A

Chapter 8

Patch Management Solution for Linux

This chapter includes the following topics:

What's new in this release

In Patch Management Solution for Linux 7.5, the following new features are introduced:

Table 8-1 List of new features

Feature	Description
New option **Delete data for Excluded software channels** added to Red Hat and Novell import pages.	A new **Delete data for excluded software channels** check box was added to make the behavior of the import tasks consistent with Windows import task.

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.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 8-2 on page 76.
- Hierarchy and replication issues
  See Table 8-3 on page 77.
- Other known issues
  See Table 8-4 on page 78.

Table 8-2 Installation and upgrade issues

Issue	Description	Article Link
Steps to do after migrating from 7.0.	■ Type the Novell Mirror Credentials on the **Novell Patch Remediation Settings** page. Starting from version 7.1, Patch Management Solution for Linux uses Novell Mirror Credentials to manage SUSE Linux updates. ■ Because of the changes in the architecture, it is not possible to migrate the selected software channels from 7.0 to 7.5 After you migrate the solution from 7.0 to 7.5, import the channels list and select the channels for which you want to download updates. ■ For Red Hat, after you upgrade the product, on the **Import Patch Data for Red Hat** page, select and import the same channels as you had in the 7.0 version of the product If you do not import these channels, it is not possible to distribute migrated Red Hat packages. For more information, see the *Symantec™ IT Management Suite Powered by Altiris™ technology Migration Guide version 7.0 to 7.5* at the following URL: http://www.symantec.com/docs/DOC5669	DOC4743
Steps to do after upgrading from 7.1 and 7.1 SP1.	Run the **Import Patch Data for Novell** and **Import Patch Data for Red Hat** tasks.	N/A
Breaking hierarchy before migrating to 7.1 SP2.	You must break the hierarchy if you are performing a migration from 7.0 to 7.5. After you break the hierarchy on the parent Notification Server computer, sometimes the child Notification Server computer retains its association with the parent server. Workaround: Also break the hierarchy on the child Notification Server computer.	N/A

Table 8-2 Installation and upgrade issues *(continued)*

Issue	Description	Article Link
Invalid custom severities are not removed from the bulletins.	Invalid custom severities are cleaned up during upgrade. However, bulletins keep the invalid severities assigned to them. To remove an invalid severity from a bulletin, change its severity by using the right-click menu.	N/A
Package server settings are not migrated from 7.0.	Package server settings on the **Policy and Package Settings** tab are not migrated from 7.0. Configure the settings after the migration.	N/A
SQL queries in automation policies are overwritten.	Parameters in the default automation policies can be migrated, but SQL queries are overwritten. Symantec recommends that if you want to customize an automation policy, you clone the policy, and then make changes to the clone.	N/A
Custom severity with non-Latin characters is not migrated after upgrade from 7.0.	Sometimes custom severity with non-Latin characters is not migrated.	N/A
RHEL3, RHEL4 and SLES9 are no longer supported.	The historical data is kept in the database, but you cannot download or install patches for RHEL3, RHEL4, and SLES9 after the migration.	N/A
The system_id for RHEL Server 5 x64 channel is not migrated after upgrade to 7.5.	After you upgrade the Patch Management Solution from 7.0 SP2 MR4 to 7.5, the system_id for RHEL Server 5 x64 channel is not migrated. After the upgrade, you need to check the Import tasks with at least the same channels to get the new System ID.	N/A

Table 8-3 Hierarchy and replication issues

Issue	Description	Article Link
Only two-level hierarchy is supported.	Although Symantec Management Platform lets you create multi-level hierarchies, Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another Notification Server computer.	HOWTO44217
Scheduled client tasks are not replicated to child immediately.	When you create a schedule for a client task (for example, **Run System Assessment Scan on Linux Computers**), and include managed computers from a child into the target, the schedule does not replicate to the child Notification Server computers immediately. Workaround: Use the **Run now** option.	N/A
Exporting software update policies from parent to child is not supported.	Do not attempt to export a software update policy on the parent Notification Server computer and import it on the child. Instead use the built-in replication functionality.	N/A

Table 8-3 Hierarchy and replication issues *(continued)*

Issue	Description	Article Link
An issue with **Allow Package Server Distribution with Manual Prestaging** setting.	The **Allow Package Server Distribution with Manual Prestaging** settings are replicated, but displayed incorrectly in the Symantec Management Console of the child Notification Server computer. The functionality is not affected, you can ignore this user interface issue.	N/A
Reports do not display any data from hierarchy.	With the exception of the **Compliance Summary** report, Patch Management Solution reports do not display any data from the child Notification Server computers. Only the data for the current Notification Server computer is displayed in patch reports.	N/A
Packages are not replicated to child.	Child Notification Server computers download packages from Novell and Red Hat servers after the Patch metadata is replicated down the hierarchy.	N/A
Replicating data between different versions of Patch Management Solution is not supported.	Although some items may replicate between different versions of Patch Management Solution that are installed on parent and child Notification Server computers, Symantec does not recommend this. If you want to use hierarchy and replication, Patch Management Solution versions must be the same on the parent and child.	N/A

Table 8-4 Other known issues

Issue	Description	Article Link
Relocating packages from an UNC location to another location does not work.	If on the **Core Services** page, you change the **To Location** value from an UNC path to another path, the packages will not be relocated. Workaround: Relocate the packages manually.	N/A
Software updates cannot be downloaded from an alternate download location on a non-IIS package server.	Only UNC paths can be used as an alternate download location on a non-IIS Windows package server. If you specify a local path on the server as the alternate download location, the software updates are not downloaded from a package server that does not have IIS installed.	N/A

Table 8-4 Other known issues *(continued)*

Issue	Description	Article Link
The Patch Administrator cannot edit the default targets in the patch management configuration policies.	A user who belongs to the **Patch Management Administrators** role cannot edit default targets in the following policies: ■ Novell patch management configuration policy You access this policy from **Settings > Software > Patch Management > Novell Settings > Novell**. ■ Red Hat patch management configuration policy You access this policy from **Settings > Software > Patch Management > Red Hat Settings > Red Hat**. Workaround: On the configuration policy's page, delete the default targets, and then add the appropriate custom targets.	N/A
Task details do not show the cause of the **Import Patch Data for Red Hat** or the **Import Patch Data for Novell** failing due to lack of free space on the Notification Server computer.	When there is no free space on the Notification Server computer, the **Import Patch Data for Red Hat** and **Import Patch Data for Novell** fail. When you open the task details in the **Task Status** table, no mention is made of the lack of free space causing the task to fail.	N/A
Reports can show incorrect data.	The **Novell/Red Hat Compliance by Update** report can show incorrect number of computers on which updates have been installed. For example, this happens when the same update belongs to two different channels. Such an update is displayed as if it was installed on two computers. To work around this issue, use the report's parameters section to filter the results by operating system or by software channel.	N/A
Sometimes a software update policy fails to save.	This issue may occur when anonymous access is enabled for the Altiris folder in IIS.	N/A
Automation policy report **Maintain Retired Machine Historical Data** does not return any result.	The automation policy creates a report, but it contains no data.	N/A
Steps to do if installation fails.	Sometimes bulletin can fail to install because of a conflicting bulletin included into the same software update policy. To work around this issue, Symantec recommends that you create a software update policy for this failing bulletin only. If it still fails, you can set the log level to DEVNOTE and examine the rpm output. You can also try to install the update and its dependencies manually.	N/A

Table 8-4 Other known issues *(continued)*

Issue	Description	Article Link
Duplicates are created if the MetaData Import task is run after software inventory is collected from Linux client computers.	Duplicates are created during the execution of the Red Hat or Suse Linux Patch Management Import task if Linux client computers have already sent in their first-time software inventory, before the MetaData Import task was run.	TECH210368
The **Delete data for excluded software channels** may fail to delete the corresponding data.	Checking the **Delete data for excluded software channels** does not delete the data that has already been downloaded for the previously selected channels. Workaround: To resolve this issue, uncheck all the channels associated with corresponding operating system, wait until the data will be deleted, and then check the required channels again.	N/A

Fixed issues

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

Table 8-5

Issue	Description	Article link
Old server name is displayed in the **Compliance summary** report after the upgrade.	After the migration from 7.0, the old Notification Server computer's name is displayed in the **Compliance summary** report.	N/A
Software Update Plug-in policies settings are not migrated.	The settings in the Software Update Plug-in Install, Uninstall, and Upgrade policies are not migrated from 7.x to this version of Patch Management Solution for Linux.	N/A
Software Update policy targets are not migrated from 7.0.	The targets in the **Applied to** section are reset after migration. The targets are reset to the target value that is indicated in the **Default Software Update Plug-in Settings** policy.	N/A
Software update policies on the child are not revised.	Software update policies that were created on child are not revised when you run the **Import Patch Data for Windows** task with the **Automatically revise Software Update policies after importing patch data** option checked on the parent Notification Server computer. Workaround: After the patch management import data replication is complete, recreate the policies on child using the same bulletins.	N/A

Table 8-5 *(continued)*

Issue	Description	Article link
Sometimes policy schedules work incorrectly across timezones.	Sometimes, when you create a schedule for a policy and select either **Use Agent time** or **Use Server time**, the policy does not run as planned on the endpoints that are located in a different time zone. Workaround: Use the **Coordinate using UTC** option.	N/A
The **Terminate after** setting on the **Novell** and **Red Hat** pages does not work.	On the **Programs** tab on the **Novell** and **Red Hat** pages, when you set a value in **Terminate after**, the setting does not work. The default value of 60 minutes is always used.	N/A
Staging Red Hat and Novell patches from an alternate location is not possible.	When you specify an alternate download location for Red Hat and Novell patches, the download fails. This setting is under **Settings > Software > Patch Management**, on the **Core Services** page, on the **Languages and Locations** tab.	N/A
Software updates import task status is incorrect.	When the **Import Patch Data for Red Hat** or the **Import Patch Data for Novell** task is running, the **Pending** status is displayed in the **Task Status** section of the task page. This status is not correct. To view the correct status of the task, click the task instance and open the task instance details.	N/A
Software update details page does not work.	In Resource Manager, the **Summaries > Software Bulletin Details or Summaries > Software Update Details** pages do not work.	N/A
The **Software Update Tasks Delivery Summary** Web Part shows executed tasks as incomplete.	In the **Red Hat/Novell Software Update Tasks Delivery Summary** Web Part, the tasks that were executed more than 30 days ago are shown as Incomplete.	N/A
Cannot save settings on **Red Hat** and **Novell** pages when credentials left empty.	The changes on the **Red Hat** and **Novell** pages cannot be saved if you leave the credentials fields empty. Workaround: Type the credentials; the credentials are critical for the solution to work. If you do not know the valid credentials at the time of editing the configuration settings, you can type fake credentials.	N/A
Sometimes policies with custom schedules can trigger other policies.	When you set a custom installation schedule for a policy, other policies with default schedules can also be triggered on the client computers and software updates will be installed. Other policies that have a custom schedule set are not affected by this issue. They will run on their scheduled time.	N/A

Table 8-5 *(continued)*

Issue	Description	Article link
The **Software Bulletin Details** report shows the computers that are out of scope of the current console user.	In the **Software Bulletin Details** report, **Applies To** column, the number of all applicable computers is shown, including those for which the current console user has access and those for which access is disabled.	N/A
Software update installations that require a computer restart are shown as complete.	The **Linux Software Update Delivery Summary** report shows software update installations that require computer restart as complete. You can use the **Restart Status** report to view if any computers are pending restart.	N/A

Other things to know

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

Table 8-6 Other things to know

Issue	Description	Article Link
You can use the First Time Setup portal to configure Patch Management Solution for the first time.	If you want, you can use the wizard on the **Home > Notification Server Management > First Time Setup** page to configure Patch Management Solution for the first use. Perform the following steps in order: 1 On the portal page, under **Step 5 - Schedule Patch Management**, click **Schedule Patch**. 2 In the wizard, configure the schedules for the patch metadata import tasks. If you want to enable more than one task, make sure the schedules are staggered to prevent the server from overloading. When you turn on the Linux tasks, you must type the Novell Mirror Credentials and the Red Hat Network access credentials. By default, all vendors and all channels are enabled. You can customize the settings later on the appropriate Import Patch Data pages. 3 (Optional) Configure the notification options. If you enable administrator notifications, you must also configure the SMTP server Settings. You can configure SMTP settings on the **Settings > Notification Server > Notification Server Settings** page. 4 On the next panel, configure the assessment scan and update installation schedules or leave the default ones. 5 Click **Schedule patch**.	N/A
Updates download URLs for Novell and Red Hat.	The software updates metadata is downloaded from the following URLs: ■ Red Hat — http://xmlrpc.rhn.redhat.com ■ Novell — https://nu.novell.com Make sure that your firewall and proxy configuration allows network communication to these URLs.	N/A
Entitlement check is removed from the product.	Patch Management Solution for Linux no longer checks for entitlement. For this reason, inventory policies and the Update Agent Discovery task are removed from the product.	N/A
Use mirror credentials for Novell.	In the previous versions of Patch Management Solution for Linux, you used Novell Customer Center credentials. Starting from version 7.1, you must type the Novell Mirror credentials on the **Novell** page, **Novell Customer Center** tab.	N/A

Table 8-6 Other things to know *(continued)*

Issue	Description	Article Link
Log file is created on the endpoint.	A log file is created on the endpoint that lets you troubleshoot patch installation issues for the particular computer. The log file location is `swuagent/var/InstallLog.txt`	N/A
Integrating Patch Management Solution with IT Analytics solution.	IT Analytics solution provides reports that display patch management data. By default, users with **Patch Administrator** role do not have access to these reports. To grant access, add the **IT Analytics Users** role to the users. For more information, see the IT Analytics documentation.	N/A
Patch Management Solution for Linux creates a new Software association type during Patch data import	This is done for binding Linux update channels with exact OS version. This is working as designed.	HOWTO65658

Chapter 9

Patch Management Solution for Mac

This chapter includes the following topics:

What's new in this release

In Patch Management Solution for Mac 7.5, the following new features are introduced:

Table 9-1 List of new features

Feature	Description
Enhance reporting for Mac OS Patching	In 7.5 relese, the following new reports have been added: ■ Mac System Assessment Scan Summary ■ Mac Compliance by Computer ■ Available Mac Software Updates for computers managed by this server ■ Not Installed Updates ■ Mac Software Update Delivery Summary ■ Mac Software Update Delivery Details ■ No Scan Data Reported

Known issues

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

Table 9-2 Other known issues

Issue	Description	Article link
The updates that require user interaction cannot be installed.	Patch Management Solution for Mac does not support installing updates that require user interaction.	N/A
Some firmware updates for Mac computers might not be displayed automatically in Patch Management Solution for Mac.	The Mac Software Update Helper Tool might not detect some firmware updates for Mac computers. Therefore, those updates do not appear in the **Available Mac Software Updates** report. Workaround: Manually download the update from the Apple Downloads site. If you are unsure whether your computer needs a particular update, download and open the update installer. The installer indicates whether the firmware update is already installed or is not needed.	N/A

Fixed issues

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

Table 9-3

Issue	Description	Article link
A manual update of the IIS configuration is required after upgrade from 7.0 to 7.1 or later.	After you perform the upgrade from 7.0 to 7.5, you must manually update the **Physical Path** value for the following node in the IIS Manager: `Default Web Site/Altiris/Packages /{3fb61de0-7af0-40b3-a40e-2f303410715d}` Set the **Physical Path** value to the actual location of the package. By default, the package location is as follows: C:\Program Files\Altiris\Patch Management\Mac\Packages\SoftwareUpdateHelper\	N/A

Other things to know

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

Table 9-4 Other things to know

Issue	Description	Article link
Hierarchy is not supported.	This product does not support hierarchy and replication.	N/A
Client Mac computers must have Internet access.	Client Mac computers download updates directly from the Apple website.	N/A
About Patch Management security roles.	You can assign the following security roles to Symantec Management Console users: ■ **Patch Management Administrators** ■ **Patch Management Rollout** Users with **Patch Management Administrators** role have full access to Patch Management Solution functionality, but no access to the rest of the Symantec Management Console. Users with **Patch Management Rollout** role have limited access to the following Patch Management Solution functionality: ■ Software Update policies ■ Reports ■ **Patch Remediation Center** page Users with **Patch Management Rollout** role can perform the following actions: ■ Enable/disable/change settings in the software update policies ■ View reports	N/A

Chapter 10

Patch Management Solution for Windows

This chapter includes the following topics:

What's new in this release

In Patch Management Solution for Windows 7.5, the following new features are introduced:

Table 10-1 List of new features

Feature	Description
New **Package Distribution** Hierarchy Editable Property (HEP) is introduced.	This feature allows to control the parent Notification Server, if the **Package Distribution** section on the Windows Patch Remediation Settings page is editable on the child Notification Server. This means that these settings can then be managed on the child Notification Servers independently from the parent Notification Server.
Increased performance for Patch Data import operations.	Multiple code optimizations and multithreading are implemented to speed up Patch Data Import operations.

Known issues

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

The known issues are separated into the following groups:

- Installation and upgrade issues
  See Table 10-2 on page 89.
- Hierarchy and replication issues
  See Table 10-3 on page 91.
- Software updates installation issues
  See Table 10-4 on page 92.
- Other known issues
  See Table 10-5 on page 95.

Table 10-2 Installation and upgrade issues

Issue	Description	Article link
Invalid custom severities are not removed from the bulletins.	Invalid custom severities are cleaned up during upgrade. However, bulletins keep the invalid severities assigned to them. To remove an invalid severity from a bulletin, change its severity by using the right-click menu.	N/A
An issue when breaking the hierarchy before migrating to 7.5.	You must break the hierarchy if you are performing a migration from 7.0 to 7.5. After you break the hierarchy on the parent Notification Server computer, sometimes the child Notification Server computer retains its association with the parent server. Workaround: Also break the hierarchy on the child Notification Server computer.	N/A
The **Download from staging location** setting is reset to default.	The **Download from staging location** setting on the **Core Services** page is reset to default after upgrade.	N/A
License count is reset after upgrade.	The count of licenses in use is reset after you upgrade from version 7.1 or earlier to 7.5. The count will increase after you upgrade the Software Update Plug-in on the client computers to version 7.5, and then run the system assessment scan	N/A

Table 10-2 Installation and upgrade issues *(continued)*

Issue	Description	Article link
SQL queries in automation policies are overwritten.	The query parameters in the automation policies (**Item Status Changed After PM Import**, **Maintain Retired Machine Historical data**, **Software Update Advertisement Disabled**, **Software Update Policy Failed**) are not migrated during an upgrade from 7.x to this version of Patch Management Solution. Parameters in the default automation policies can be migrated, but SQL queries are overwritten. Symantec recommends that if you want to customize an automation policy, you clone the policy, and then make changes to the clone.	N/A
Software update packages are not migrated to 7.5 in case of an off-box upgrade.	If you are performing an off-box upgrade to 7.5 (installing on a new computer) and using migration wizard to transfer data, the software update packages are not migrated. You must copy the packages manually or use a network location to store the packages.	N/A
The **Alternative Location** settings and credentials are not migrated from 7.1 SP2.	When you upgrade from 7.1 SP2 to 7.5 and run the **Import Patch Data for Windows** task, the **Alternative Location** settings and credentials are not migrated.	N/A
Windows Computers with Software Update Plug-in counter does not show the count of the agents with non-upgraded plug-ins.	When you upgrade to 7.5, the **Windows Computers with Software Update Plug-in** counter in the **Patch Configuration Summary** Web Part does not show the count of the agents with non-upgraded plug-ins. To obtain the correct data, you need to upgrade the Software Upgrade plug-in to the 7.5 version.	N/A
The **Delete packages after** value that is not available in the drop-down list in 7.5, will be set to **Never delete** after you migrate.	If, before you migrate from 6.x to 7.5, on the **Windows Patch Remediation Settings** page, you set **Delete packages after** to a value that is not available in the similar drop-down list in 7.5, the value will be set to **Never delete** after you migrate. However, the distributed updates will still use the custom value that you set.	N/A
The Software Update Plug-in cannot be uninstalled unless it is upgraded to 7.5.	You cannot uninstall the Software Update Plug-in with the **Software Update Plug-in Uninstall** policy unless you upgrade Symantec Management Agent and Software Update Plug-in to the 7.5 version.	N/A
The custom settings in the patch **Management Language Alerting** dialog box are not migrated.	When you upgrade from 7.0 Maintenance Release 4 to 7.5, most of the custom settings in the patch **Management Language Alertring** dialog box are not migrated.	N/A

Table 10-2 Installation and upgrade issues *(continued)*

Issue	Description	Article link
If any custom severities with the names containing at least 2 words have been created in 6.x and then migrated to 7.5, then, when you assign any of the existing custom severities to the bulletin, errors occur.	If any custom severities with the names containing at least 2 words have been created in 6.x and then migrated to 7.5, then, when you assign any of the existing custom severities (including the ones with the names consisting of only 1 word) to the bulletin, the following issues will occur: ■ When you try to assign the custom severity with the name containing at least 2 words that was migrated from 6.x to the bulletin, nothing will be assigned. ■ When you try to assign the custom severity with the name consisting of 1 word to the bulletin, one of the custom severities migrated from 6.x with a name containing at least 2 words will be assigned to the bulletin even though you did not select it. To work around this issue, after you migrate from 7.5, on the **Core Services** page, re-save the list of severities.	N/A

Table 10-3 Hierarchy and replication issues

Issue	Description	Article link
Only two-level hierarchy is supported.	Although Symantec Management Platform lets you create multi-level hierarchies, Patch Management Solution supports only two-level hierarchy. A child Notification Server computer cannot be a parent to another Notification Server computer.	HOWTO44217
An issue with the **Allow Package Server Distribution with Manual Prestaging** setting.	The **Allow Package Server Distribution with Manual Prestaging** settings are replicated, but displayed incorrectly in the Symantec Management Console of the child Notification Server computer. The functionality is not affected, you can ignore this user interface issue.	N/A
The **Check Software Update Package Integrity Task** cannot be run on the child.	The **New schedule** button on the **Check Software Update Package Integrity Task** page is disabled on the child Notification Server computer. Workaround: Schedule the task on the parent Notification Server computer. Then edit the schedule on the child.	N/A
Replicating data between different versions of Patch Management Solution is not supported.	Although some items may replicate between different versions of Patch Management Solution that are installed on parent and child Notification Server computers, Symantec does not recommend this. If you want to use hierarchy and replication, Patch Management Solution versions must be the same on the parent and child.	N/A

Table 10-3 Hierarchy and replication issues *(continued)*

Issue	Description	Article link
Errors occur when the plug-in requests configuration for replicated software update tasks before the associated packages have been re-created.	During software update policy replication, the policies are created before the packages have been downloaded to the child Notification Server computers. If a software update plug-in requests configuration during this time, errors appear in logs as the policies are incomplete until the packages are downloaded. After the packages are downloaded, the errors will no longer occur.	N/A
Notification Server Item replication deletes any task history on the child.	Replication of items down a hierarchy deletes any task history on the child for the Patch Management server tasks.	N/A
The **Vulnerability Scan** task fails if the patch data has not been replicated.	If you run complete replication but do not replicate the patch data, and then try to run the **Vulnerability Scan** task on a child server or a client computer from the Parent Notification Server, the scan will fail.	N/A
Replicated Policies Get Deleted on the Child Notification Server, when using **Standard Replication Schedule**.	Replicated policies get deleted on the Child Notification Server, when Patch Management Import Data for Windows uses the **Standard Replication Schedule**.	TECH210370

Table 10-4 Software updates installation issues

Issue	Description	Article link
Installation of some updates cannot be performed silently.	Some updates do not support silent installation. Some dialog or progress windows may be visible to the user of the managed computer. This issue does not affect the installation, and can be ignored.	N/A

Table 10-4 Software updates installation issues *(continued)*

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

Table 10-4 Software updates installation issues *(continued)*

Issue	Description	Article link
Some updates require original installation media.	Some updates may require original installation media. The updates that are known to require one are as follows: ■ Microsoft Project 2003 SP3 ■ Microsoft Visio 2003 SP3 ■ Citrix Presentation Server If the product was installed from a CD/DVD, then the original CD/DVD must be inserted in the disk reader on the client computer. If the product was installed from a network location, then anonymous access from the client computer to this location must be available to install the update	N/A

An issue occurs when installing Sun-Java updates.	When Java software is in use on the client computer, the update cannot be installed silently. A "Close applications" dialog box appears on the client that prevents the update process from proceeding.
	Workaround: You can add a 'tskill java /A' command into the installation script to terminate the Java processes:
	`...`
	`"cmd.exe" /C start /wait NET STOP "JAVA QUICK STARTER"`
	`tskill java /A`
	`"cmd.exe" /C start /wait %LSFN% /s "IEXPLORER=1 MOZILLA=1" /quiet /norestart`
	`"cmd.exe" /C start /wait NET START "JAVA QUICK STARTER"`
	`...`
		N/A

Sun-Java gets uninstalled if Internet Explorer is open at the time of installation.	If an Internet Explorer window is open on an endpoint at the time of Sun-Java update installation, Sun-Java gets completely uninstalled from the endpoint. The uninstall is performed silently and the status of software update installation is **Installed**. JAVA6-27 and JAVA6-29 are among the bulletins that are known to have this problem. Workaround: If possible, restart the endpoint or kill Internet Explorer before installing the update.	N/A
Microsoft Office components must be on the same Service Pack level.	Issues occur when various Microsoft Office components are having different Service Pack versions applied.	N/A

Table 10-4 Software updates installation issues *(continued)*

Issue	Description	Article link
A removed vendor or software update is displayed in the **Vendors and Software** list.	If a vendor or software release is removed from Patch Data, this vendor or software release is still displayed under **Vendors and Software** list on the **Import Patch Data for Windows** page after the **Vendors and Software** list is updated. The removed vendor or software release will disappear from the list after the **Import Patch Data for Windows** task is completed.	N/A
The **Windows Computers with Software Update Plug-in** counter works only for the client computers that have the Software Update plug-in originally rolled out from the same Notification Server.	The **Windows Computers with Software Update Plug-in** counter in the **Patch Configuration Summary** Web Part works only for those client computers that have the Software Update plug-in originally rolled out from the same Notification Server. The counter excludes the client computers clients that were redirected from another Notification Server after the Software Update plug-in rollout. It will include the redirected client computers only after they are reinstalled or upgraded.	N/A
If you change the package location from default to **Alternative Location** with custom credentials and then back to default, you will not be able to perform **Vendors and Software** update.	When, on the **Import Patch Data for Windows** page, you change the package location from default to **Alternative Location** with custom credentials and then back to default, you will not be able to perform **Vendors and Software** update. To complete the update, you need to select **Default Location** and complete the **Vendors and Software** update. You can then switch back to the **Alternative Location**.	N/A
When you deploy Microsoft updates through Patch Management with the restart settings disabled, the operating system still forces the client computers to restart.	When you deploy Microsoft updates through Patch Management with the restart settings disabled, after the installation is complete, the operating system still forces the client computers to restart. This does not happen if you have the Windows Update turned off. To turn off the Windows Updates, on the client computer, you need to enable the **Never check for updates (not recommended)** option. **Warning:** Do not disable Windows Update service because it is required for successful patching via .MSU files.	N/A

Table 10-5 Other known issues

Issue	Description	Article link
An issue when using FTP as patch data alternative download location.	If you want to use an FTP location as the alternative download location on the **Import Patch Data** page, on the Notification Server computer, add the C:\Program Files\Altiris\Notification Server\Bin\AeXsvc.exe service to the firewall Exception List.	N/A

Table 10-5 Other known issues *(continued)*

Issue	Description	Article link
An issue occurs when accessing the AexPatchUtil.exe utility.	A non-administrator cannot navigate to the AexPatchUtil.exe utility using the command prompt because of access restrictions to the C:\Program Files\Altiris folder. This issue occurs only on the Notification Server computer. Workaround: `cd` straight to the C:\Program Files\Altiris\Altiris Agent\Agents directory.	N/A
An issue with re-imaged endpoints.	An issue occurs when you re-image or reinstall an operating system on an endpoint. Software update plug-in is not able to process the policies and install software updates. Workaround: Restart the Symantec Management Agent service or restart the computer.	N/A
Patching of software that is installed into a virtual layer is not supported.	Patches that you apply to the software in a virtual layer might not be applied correctly and can corrupt the system.	N/A
Packages are not always downloaded to managed computers at the correct time.	Occasionally, software update packages may not be downloaded immediately to managed computers. This is due to a timing issue where the initial download is not triggered by Software Management and the status of the package is not updated. The packages will be downloaded when the update install schedule fires or when the next maintenance window opens.	N/A
When you click **Save Changes** in a policy, a confirmation message displays "Saved Changes" even though the policy is still being saved.	When you edit a Software Update policy, the screen is updated with the text "Saved Changes" even though the task that saves the changes made to the policy and underlying advertisements may still be running. If the changes that you made do not appear on the screen immediately, refresh the screen after a few seconds. Your changes should appear after the refresh.	N/A
The Software Update Plug-in stays in the "Update Pending" state after the dialog box closes.	Occasionally, clicking **Install Now** on the **Software Update Installation** dialog box or waiting for the dialog box to close itself does not result in the immediate installation of a software update. The installation starts five minutes after the dialog box has closed, when the Software Update Plug-in wakes up and checks its state.	N/A
The **Software Bulletin Details** report shows the computers that are out of the scope of the current console user.	In the **Software Bulletin Details** report, in the **Applies To** column, the number of all applicable computers is shown, including those for which the current console user has access and those for which access is disabled.	N/A

Table 10-5 Other known issues *(continued)*

Issue	Description	Article link
Update installations that require a computer restart are shown as complete.	The **Windows Software Update Delivery Summary** report shows update installations that require computer restart as complete. You can use the **Restart Status** report to view if any computers are pending restart.	N/A
Some system privileges on the **Roles** page can become unchecked after migration.	When you migrate from 6.x to ITMS 7.5, some system privileges on the **Roles** page become unchecked after migration. This may cause problems with saving Software Update policies under Patch Management Administrator role. If this problem occurs, you need to enable the **View Security** privilege.	N/A
The client computers are sometimes listed in the **Windows Computers Not Reporting System Assessment Scan Data** report, even though the **Vulnerability Scan** was successful.	The client computers are sometimes listed in the **Windows Computers Not Reporting System Assessment Scan Data** report, even when the **Vulnerability Scan** is executed successfully on them. This happens if the software releases that are installed on these computers are not selected in the **Windows Patch Data Import Task**.	N/A
The modified update will not be re-downloaded when the **Revise** option is enabled.	If you change the settings of the **Advertisement Set** policy, and then run the Patch Management with the **Revise** option enabled, the modified update will not be re-downloaded.	N/A
The out-of-scope client computers are displayed in the **Compliance Summary** report.	The **Compliance Summary** report displays the summary for the total number of Notification Server client computers, including the out-of-scope client computers. The drill-down report displays detailed information for the computers from the trusted scope only.	N/A
Moving or deleting a folder or a file takes too much time.	If, after you generate Patch data (at least 10000 packages), you move or delete a folder or a file, it takes about 3 minutes until the action is completed. This problem is connected with the performance of Windows Shell.	N/A
if you enter the **Alternative Location** path in the wrong format, the new location will still be saved successfully, but, the import will fail.	When, on the **Import Patch Data for Windows** page, under **Package Location**, you select **Alternative Location**, you need to enter it in the following format, as follows: **<alternative location>/pmimport.cab** Otherwise, if you enter the path in the wrong format, the new location will still be saved successfully, but, the import will fail.	N/A

Table 10-5 Other known issues *(continued)*

Issue	Description	Article link
After the disaster recovery, you need to rerun the Patch Management import.	After you have performed the disaster recovery, you need to rerun the Patch Management import.	N/A
Patch Management Solution version 6.x reports cannot be automatically saved in the version 7.5 format.	Patch Management Solution version 6.x reports must be converted for usage in Patch Management Solution 7.5.	TECH210366
Only UNC paths can be used as an alternate download location on a non-IIS Windows package server.	Only UNC paths can be used as an alternate download location on a non-IIS Windows package server. If you specify a local path on the server as the alternate download location, the software updates are not downloaded from a package server that does not have IIS installed.	N/A

Fixed issues

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

Table 10-6 Fixed issues

Issue	Description	Article link
Software update policies that were created on child are not revised when you run the **Import Patch Data for Windows** task.	Software update policies that were created on child are not revised when you run the **Import Patch Data for Windows** task with the **Automatically revise Software Update policies after importing patch data** option checked on the parent Notification Server computer.	N/A
The schedule for a client task that includes managed computers from a child into the target does not replicate to the child Notification Server computers immediately.	When you create a schedule for a client task (for example, **Run System Assessment Scan on Windows Computers**), and include managed computers from a child into the target, the schedule does not replicate to the child Notification Server computers immediately.	N/A
Software update status does not get updated on the **Software Updates** tab.	Sometimes the software update status does not get updated on the **Software Updates** tab of the Symantec Management Agent.	N/A

Other things to know

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

Table 10-7 Other things to know

Issue	Description	Article link
You can use the First Time Setup portal to configure Patch Management Solution for the first time.	If you want, you can use the wizard on the **Home > Notification Server Management > First Time Setup** page to configure Patch Management Solution for the first use. Perform the following steps in order: 1 On the portal page, under **Step 5 - Schedule Patch Management**, click **Schedule Patch**. 2 In the wizard, configure the schedules for the patch metadata import tasks. If you want to enable more than one task, make sure the schedules are staggered to prevent the server from overloading. When you turn on the Linux tasks, you must type the Novell Mirror Credentials and the Red Hat Network access credentials. By default, all vendors and all channels are enabled. You can customize the settings later on the appropriate Import Patch Data pages. 3 (Optional) Configure the notification options. If you enable administrator notifications, you must also configure the SMTP server settings. You can configure SMTP settings on the **Settings > Notification Server > Notification Server Settings** page. 4 On the next page, configure the assessment scan and update installation schedules or leave the default ones. 5 Click **Schedule patch**.	N/A
When a maintenance window is configured, the update installation does not run on the schedule.	If a maintenance window opens before the software update installation schedule, the schedule (including the **Start/End dates**) is disregarded and the software update gets installed before the scheduled time. This issue occurs when **Override Maintenance Windows settings** is not checked. This behavior is expected.	N/A

Table 10-7 Other things to know *(continued)*

Issue	Description	Article link
Close the **Altiris Log Viewer** to improve the performance of the patch data import task for Microsoft and Adobe.	If you close the **Altiris Log Viewer** when you run the **Import Patch Data for Windows** task, you can improve the task's performance by as much as 50 percent.	N/A
A log file is created on the endpoint.	A log file is created on the endpoint that lets you troubleshoot patch installation issues for the particular computer. The log file location is as follows: `%ALTIRIS_AGENT_INSTALL_FOLDER%\Agents\PatchMgmtAgent\`	N/A
Integrating Patch Management Solution with IT Analytics solution.	IT Analytics solution provides reports that display patch management data. By default, users with **Patch Administrator** role do not have access to these reports. To grant access, add the **IT Analytics Users** role to the users. For more information, see the IT Analytics documentation.	N/A
Interaction with the Windows Update service.	Installing software updates on Microsoft Windows Vista or later operating systems fails if the Windows Update service's startup type is set to **Disabled**. The service's startup type must be set to **Automatic** or **Manual** — when a software update is installing, it starts the service. The service is not stopped after the installation is complete. If you want to stop the service, you can run a post-deployment task. Altiris Real-Time System Manager software has a **Service Management** task that you can use.	N/A
With certain settings, the software update installation will fail to start on 7.1 SP1 client computers.	If you set the **Legacy Agent Communication** option to **OFF**, and then, on the **Windows Patch Remediation Settings** page, in the **Run with rights** drop-down list, click **Specified user**, the software update installation will fail to start on 7.1 SP1 client computers. To work around the issue, on the 7.1 SP1 client computers, in the **Run with rights** drop-down list, click **System Account**.	N/A

Table 10-7 Other things to know *(continued)*

Issue	Description	Article link
CPU usage highly increased during PMImport task, if the SQL database is not installed on a separate server.	Multiple code optimizations for Import operations are designed to utilize all CPU resources. If you want to reduce the increased CPU usage on Notification Servers, which also hold the SQL database, you can utilize the following workarounds: ■ Use SQL software performance settings to limit CPU usage. ■ Schedule task to run during non-business hours. ■ Use registry settings to set the **WindowsMaxWorkerThreads** count used by task, equal to the number of processor cores or lower, as follows: "WindowsMaxWorkerThreads"=dword:00000001 (change to count of processor's cores).	TECH210369

Chapter 11

Real-Time System Manager

This chapter includes the following topics:

Known issues

The following are the known issues for this release.

The known issues are separated into the following groups:

- SOL/IDE-R issues
  See Table 11-1 on page 102.
- RTCI known issues
  See Table 11-2 on page 104.
- Other known issues
  See Table 11-3 on page 105.

Table 11-1 SOL/IDE-R issues

Issue	Description
Non-Latin characters are not supported.	SOL terminal window does not support double-byte characters (Japanese, Chinese).
Intel AMT Serial-over-LAN does not work correctly with HP computers.	The following options must be configured in the ME BIOS advanced settings for Intel AMT Serial-over-LAN to work correctly with HP computers: ■ SOL Terminal Emulation Mode: ANSI ■ Disabled echo char: ON

Table 11-1 SOL/IDE-R issues *(continued)*

Issue	Description
IDE-Redirection to floppy does not work on Dell client computers.	When the SOL/IDE-R session is used to remotely boot a Dell client computer from a physical floppy diskette that is inserted into a floppy drive on the Notification Server computer, or from a binary floppy image file, the client computer performs a restart but does not load the operating system. On the client computer's monitor, the message "Attempting remote IDE boot" appears, but the Real-Time System Manager's terminal window remains blank until the session is terminated. This is a known issue with Dell computers (tested on Dell OptiPlex 745c). The workaround is to start the client from other media (physical CD-ROM, DVD-ROM, or ISO image file).
"SOL session terminated" error message appears when establishing a remote SOL connection to a computer.	If a SOL session window is already opened for a computer, you must close it before establishing a new remote SOL connection to the computer. Otherwise, you may get an "SOL session terminated" error message.
SOL and IDE-R disabled in the target computer's BIOS.	When SOL and IDE-R are disabled in the target computer's BIOS, the controls for these options on the **Intel AMT Settings** page (**Task progress window and remote control** and **Redirect to optical/floppy drive or image on a server**) are not disabled.
IDE-R session to MS-DOS boot image does not work correctly with certain HP client computers.	IDE-R session to an MS-DOS boot image may not work correctly with managed HP client computers that have BIOS versions earlier than 1.5. The workaround is to upgrade the client BIOS.
Alt+<key> sequences do not transfer to client computer during SOL session.	When you use any Alt+<key> sequence on the keyboard during the Serial-over-LAN session, the controlled computer may not receive it.
Cannot install Windows using IDE-R on HP Compaq dc7700p system.	Due to SOL emulation limitations, installation of a graphical operating system through IDE-R can lead to a BSOD on some Intel vPro implementations and is not fully supported by Intel AMT 2.x products. The problem affects HP Compaq Business Desktop System BIOS for Intel vPro Technology (786E1 BIOS). For resolution, download and install the latest BIOS/firmware update from the vendor's website.
The first line of the terminal output is not displayed in SOL/IDE-R session.	When you establish a SOL/IDE-R session with HP computers with Intel AMT 2.5, the first line of the terminal output is not displayed in the remote console.
Ctrl+Alt+Del sequence does not work in the SOL session.	Ctrl+Alt+Del key sequence does not work in the SOL session established with Intel AMT 2.5 devices.
Function keys do not work in the SOL session.	If some of the F1-F10 keys do not work in the SOL session, use the <Esc>+1 - <Esc>+0 key sequence to emulate the function keys. This problem only occurs with certain BIOS firmware.

Table 11-1 SOL/IDE-R issues *(continued)*

Issue	Description
SOL/IDE-R session terminates after 1 minute when it is run by wireless interface.	On some hardware (HP, Fujitsu), the SOL/IDE-R session initiated by wireless connection terminates after 1 minute. This is a hardware limitation. To work around this issue, do the following: 1 In the Notification Server computer's registry, set the following DWORD value to 1: HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Notification Server\ProductInstallation\ {13987439-8929-48d2-aa30-ef4bf0eb26a6}\InstantAMTPing. 2 Restart the IIS.
One-to-many server IDE-R task fails if the IDE-R session is left active from the one-to-one real-time task and vice versa.	You must wait until the previous session is expired or terminate the session manually.
Boot redirection options not available for DASH computers.	**Real-Time View > Administrative Tasks > Hardware management > Redirection** options are not available when connected to a DASH computer. This issue is firmware-dependent. Upgrading DASH firmware can solve the problem.

Table 11-2 RTCI issues

Issue	Description
Not possible to run out-of-band tasks on IPMI computers.	It is not possible to run one-to-many out-of-band tasks on IPMI computers. That is because the IP address of the IPMI management controller differs from the computers's IP address. Notification Server does not know the IPMI controller's IP. Running one-to-many out-of-band task is not possible on IPMI computers.
Restore State power action cannot restore S4 and S3 states.	The **Restore State** power action is not capable of putting computers into Stand-by (S3) or Hibernate (S4) states. Consequently, the **Restore State** power action turns off the computer (if needed) in an attempt to restore the Hibernate (S4) state and turns on the computer (if needed) to restore the Stand-by (S3) state
Some Intel AMT inventory data is not collected.	The following Intel AMT inventory is not collected by the **Get Out-of-Band Inventory** task: ■ RTCI AMT Battery Serial Number ■ RTCI AMT Battery Manufacture Date

Table 11-3 Other known issues

Issue	Description	Article link
Error while performing power management operation **Reboot** command.	One-to-one and one-to-many **Reboot** power management command using WS-MAN connection executes with an error *Power management operation failed* on the UI, despite the fact that the computer successfully restarts This problem is known for Dell Precision T3500 computers.	N/A
Not possible to connect to Intel AMT 5.0 using secure WS-MAN connection.	It is not possible to connect to Intel AMT 5.0 using secure WS-MAN connection. To solve this limitation, you need to upgrade the Intel AMT 5.0 firmware to the latest Intel AMT 5.2.	N/A
Unable to connect to Intel DASH computer configured in mutual authentication mode.	Secure connection, using the WSMAN protocol, to an Intel DASH computer that is configured in “Mutual authentication” mode is not supported.	N/A
IDE redirection does not work with "Kerberos" user.	When you are connected to a client using the "Kerberos" user, starting IDE redirection session can fail.	N/A
Firewall settings prevent WMI connection to a computer running Windows XP Service Pack 2.	If you provided valid WMI credentials, but cannot establish a WMI connection to a computer that is running Windows XP Service Pack 2 (WMI is not in the list of supported protocols on the Real-Time Consoles page), check the firewall settings on the target computer. The default configuration of the Windows Firewall program in Windows XP SP2 blocks incoming network traffic on Transmission Control Protocol (TCP) port 445. Configure the firewall to allow incoming network traffic on TCP port 445. For possible resolution methods, see the topics on troubleshooting in the *Real-Time System Management User Guide*.	N/A

Table 11-3 Other known issues *(continued)*

Issue	Description	Article link
Firewall settings prevent remote connection to Windows Vista or Windows 7 client computer.	When using Real-Time System Manager to remotely connect to Windows Vista or Windows 7 client computers, you must make sure that Windows Firewall is configured to allow remote Windows Management Instrumentation (WMI) connections on the client computer. To enable WMI connections on Windows Vista, in the Control Panel, click **Windows Firewall > Change Settings > Exceptions**, and then check **Windows Management Instrumentation (WMI)**. Additionally, for standalone Windows Vista and Windows 7 clients (not in a domain), you must disable the User Account Control (UAC). To do this for Windows Vista, in the Control Panel click **User Accounts > Turn User account control on or off** and then uncheck **Use User Account Control (UAC) to help protect your computer**. Optionally, you can disable the UAC for the built-in administrator account (if you want to use this account for remote connection). To do this, in the **Control Panel > Administrative Tools > Local Security Policy** MMC snap-in, click **Local Policies > Security Options** and disable the **User Account Control: Admin Approval mode for Built-in Administrator account** policy. For more information, see the topics on troubleshooting in the *Real-Time System Management User Guide*.	N/A
Connection capabilities limited when connecting to computers that have multiple network cards.	Real-Time System Manager's connection to client computers that have more than one NIC (network interface card) has been improved. The following limitations still apply: ■ The Real-Time System Manager connection timeout is 10 minutes. ■ The Symantec Management Agent must have the Configuration Management Database (CMDB) updated with the new IP address after the client computer connects to the network.	N/A
One-to-many tasks cannot manage resources by an IP address.	To manage a computer from the **Real-Time** view one-to-one, you can enter an IP address and connect to the computer. One-to-many tasks do not work in this way. To run one-to-many tasks, the target computer's FQDN must be resolvable correctly from the Notification Server computer.	N/A
Cannot power off Intel ASF hardware from S3 state.	Some Intel ASF hardware does not support power off from the S3 state. You can try to turn on the computer and then run the turn off command again. Broadcom ASF does not have this problem.	N/A

Table 11-3 Other known issues *(continued)*

Issue	Description	Article link
PXE Boot does not work with some ASF hardware.	When in the **Real-Time** view you select the **Reboot** command and choose to boot from PXE, some ASF hardware fails to boot from PXE. This is a hardware limitation. HP with Broadcom ASF, DELL Precision T3400, and a few other computers are known to have this problem. You can try to turn off the computer and then turn on and boot from PXE.	N/A
Managed Service Provider configurations are not supported.	Both one-to-one and one-to-many tasks in the Real-Time System Manager software require a direct connection to the target computer that you want to manage. It is not possible to manage computers located behind NAT-enabled routers.	N/A
Graceful shutdown or restart returns an error on Microsoft Windows Vista and Windows 7.	A "Graceful reboot or power off is not possible" error can appear when you check **Allow user to save data before power operation** and try to **Reboot** or **Power off** a Microsoft Windows Vista or Windows 7 computer. This occurs because one of the following: ■ The specified computer does not support a shutdown interface. ■ The caller does not have the required privilege to perform this operation. ■ The specified computer does not exist or is not accessible. ■ An invalid set of parameters was passed. ■ A shutdown has already been started on the specified computer. ■ A system shutdown has already been scheduled. ■ The system shutdown cannot be initiated because there are other users logged on to the computer. ■ The format of the specified computer name is invalid. You can uncheck **Allow user to save data before power operation** and try to perform a hard reset of the target computer, losing all unsaved data.	N/A
Not possible to update operating system properties on some computers.	It is not possible to update properties on the **Operating System** page in the **Real-Time** view if the target computer is running Microsoft Windows Vista (32-bit and 64-bit editions).	N/A
Only secure CIRA connections are supported.	Intel AMT computer management using CIRA is possible only with Intel AMT 4.0 and later computers that are configured to use TLS or TLS with mutual authentication.	N/A
Unable to connect to Intel DASH computer configured in mutual authentication mode.	Secure connection, using the WSMAN protocol, to an Intel DASH computer that is configured in “Mutual authentication” mode is not supported.	N/A

Table 11-3 Other known issues *(continued)*

Issue	Description	Article link
Setup and Configuration Server address is not displayed.	In the **Real-Time** view, on the **Intel AMT Configuration Mode** page, the setup and Configuration Server address is not shown for computers with Intel AMT version 2.6 and 4.0.	N/A
During upgrade, custom configuration of Network Filtering resets to default.	During the upgrade to 7.5 any custom filters of Network Filtering are reset to the default configuration. To keep using the custom setting you need to do the following: ■ On your NS Server, from the *\RTSM\Web\UIData* folder, copy the `CBFilters.bak` file. ■ Rename the `CBFilters.bak` file to `CBFilters.xml`. ■ Replace the original xml with the one containing the custom configuration.	N/A

Chapter 12

Software Management Solution

This chapter includes the following topics:

What's new in this release

In Software Management Solution 7.5, the following new features are introduced:

Table 12-1 List of new features

Feature	Description
Support of Cloud-enabled Management.	Support of Cloud-enabled Management is added for Managed Software Delivery, Quick Delivery (not real time) and Software Inventory. There is no support for Software Portal. **Note:** Cloud-enabled Management is supported only for Windows clients.

Table 12-1 List of new features *(continued)*

Feature	Description
ASDK update	The Administrator Software Development Kit (ASDK) is updated to include support for Software Management Solution and Software Management Framework. ASDK includes new Application Programming Interfaces (APIs) that access the functionality of Software Management Framework and Software Management Solution. These improvements let you import packages into the Software Catalog in a programmatic manner. In addition you can create detection rules, modify command lines, and create and modify Managed Software Delivery policies. Symantec Administrator SDK documentation contains information of how to use ASDK and a complete list of available methods can be accessed. To find the Symantec Administrator SDK Help, on the **Start** menu, click **All Programs > Symantec > ASDK > ASDK Help**.
Support for creating Mac packages in Software Catalog.	The Software Management Framework can create default command lines for Mac packages embedded inside of archive files. This addition means that the Desktop administrator can add Mac packages to the Software Catalog. Once the Mac packages are added to the Software Catalog, the administrator can manage it by using the functionality available in the Software Catalog. For example, the desktop administrator may like to use the Command Line Builder functionality that is part of the Software Catalog for Mac packages.
Enhanced software management in Software Catalog.	The Software Management Framework provides software categorization by the operating system and software platform. This enhancement simplifies software management for administrators, especially, in heterogeneous environments. The new options are available on the Software resource page **Association** tab, in the **Association Type** drop-down menu as **Applies to Operating System** and **Applies to Software Platform**.
Support for the latest SWV Agent.	Software Management Solution supports the latest version of the SWV Agent 7.5.522.
The Wise Toolkit and the Wise Connector removal.	The Wise Toolkit and the Wise Connector components of the Software Management Solution are being deprecated in this release as a result of the end-of-life of Wise Package Studio. Customers who require the Wise Toolkit should contact Technical Support.

Known issues

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

The known issues are separated into the following groups:

- General issues
  See Table 12-2 on page 111.
- Managed software delivery issues
  See Table 12-3 on page 112.
- Cloud-enabled Management issues
  See Table 12-4 on page 114.
- Software Portal issues
  See Table 12-5 on page 115.
- Hierarchy and replication issues
  See Table 12-6 on page 115.
- Non-Windows-specific issues
  See Table 12-7 on page 115.
- Software Management Framework issues
  See Table 12-8 on page 116.
- Other issues
  See Table 12-9 on page 119.

Table 12-2 General issues

Issue	Description	Article link
Symantec Management Agent and Software Management Plug-in require upgrade to run Managed Delivery Policies and Quick Delivery tasks under specific user credentials.	After upgrade from IT Management Suite 7.0, previous versions of Symantec Management Agent and Software Management Plug-in may fail to run Managed Delivery Policies and Quick Delivery tasks under specific user credentials. Workaround: Upgrade Symantec Management Agent and Software Management Plug-in or run Managed Delivery Policies and Quick Delivery tasks using Symantec Management Agent credentials.	N/A
Full inventory is required to gather missing uninstall string for a software resource.	The uninstall string from Add/Remove programs for a software resource could be missing from the inventory, gathered by the previous versions of the Symantec Management Agent. After the upgrade, delta inventory does not gather this information. Workaround: To fix this issue, run the Collect Full Inventory task.	N/A

Table 12-2 General issues *(continued)*

Issue	Description	Article link
Compliance reports still display computers after they are removed from the policy target.	If a computer, to which a specific Managed Software Delivery policy is applied, is displayed in any of the corresponding compliance reports, it will still be displayed in these reports after it is removed from the policy target.	N/A
Unable to generate a command line for a package from a Software Library.	If the Software Library is specified as a source for a package containing large files, while editing an existing software resource, the command lines are not generated for this software resource.	N/A
Software discovery creates second software resource for software resource, imported from MSI.	If after running the Software Discovery task or gathering software inventory, Software Catalog duplicates previously imported software resources as newly discovered software resources, this means, that the corresponding imported MSI files contained different software keys. Workaround: To fix the issue, run the Merge Duplicate Resources scheduled task. If this task does not fix all issues, merge the software resources manually.	N/A
Software Path Update task fails for a software, which is installed for a specific user.	Software Path Update task fails to update source path for an installed software, if the task is run under currently logged on user or specific user accounts.	N/A
Source Path Update execution requires Symantec User credentials.	Source Path Update will only work under Symantec User Credentials.	N/A

Table 12-3 Managed software delivery issues

Issue	Description	Article link
Managed Software Delivery policies stay in the detection check state after upgrade.	If Managed Software Delivery policies stay in the detection check state on the client computer for a long time after upgrade, then they may not get executed. Workaround: To fix this issue, restart the affected client computer or the corresponding Symantec Management Agent.	N/A
Managed Software Delivery policies cannot be run from servers on client computers running Windows Vista or Windows 7.	If the **Run from server if bandwidth is above some speed** advanced option is checked for a Managed Software Delivery download settings, the policy will fail with a 1619 error code on the client computers running Windows Vista or Windows 7 operating systems.	N/A

Table 12-3 Managed software delivery issues *(continued)*

Issue	Description	Article link
Dependent software installation issue.	If Managed Software Delivery policy is created for a software, which has a dependency on another software, using **Managed Software Delivery** wizard, where on the **Specify dependencies and updates** page the **Verify dependencies** option is checked and the software resource option is unchecked for the corresponding software, the dependent software is not installed even if the dependency option is later checked in the policy settings. Workaround: To fix the issue, remove the software resource from the Managed Software Delivery policy and add it again.	N/A
Managed Software Delivery policies and Quick Delivery tasks fail to run from a directory on the Notification Server computer.	Managed Software Delivery policy or a Quick Delivery task fail with a 1619 error code, if the following conditions are met: ■ There are no package servers in an environment; ■ A software resource is imported from a Notification Server; ■ The **Use the following settings to download and run** option is checked; ■ The **Download and run locally if bandwidth is above** is unchecked; ■ The **Run from server if bandwidth is above any connection speed** is checked; ■ The **Current logged-in user** option is checked on the Run Options settings.	N/A
File Version detection check does not support the %user name% environment variable.	When running a Managed Software Delivery policy under **Currently logged in user**, the file version detection check fails to detect a file, which is located under the %user name% folder. Workaround: To fix the issue, in the file location path, use the %useprofile% environment variable, which points to the same folder.	N/A
Registry Key/File Path to File Version rule does not support environment variables.	When running a Managed Software Delivery policy under **Currently logged in user**, the **Registry Key/File Path to File Version** detection check fails to detect a file, if the path is specified using environment variables.	N/A

Table 12-3 Managed software delivery issues *(continued)*

Issue	Description	Article link
Client computer restarts on completing the software installation may confuse the computer users in case of different settings, specified by multiple users.	If multiple users log in locally or remotely to the client computer, on which a software resource is installed by a Managed Software Delivery Policy, and specify different settings, when prompted to restart the computer after the software installation is complete, the following situations may occur: ■ If a client computer user snoozes the computer restart, after a software resource is installed by a Managed Software Delivery policy, computer can only restart, when this user is logged in again. If another user logs in to the same client computer and selects to restart the computer after the installation is complete, the computer does not restart. ■ If a user has accepted computer restart, but it was snoozed by another user, or the maintenance window has not started yet, the computer will then restart unexpectedly for the first user, when the snooze period, specified by another user expires or the maintenance windows starts.	N/A

Table 12-4 Cloud-enabled Management issues

Issue	Description	Article link
The support of **Run from server if bandwidth is above some speed** setting is limited in CEM mode.	The usage of this setting on Internet-managed client computers is limited as follows: ■ If the setting is enabled for a Quick Delivery task or a Package Delivery task, these tasks will fail with timeout error, unless the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached. ■ If the setting is enabled for a Managed Delivery policy, the policy will not run, until the client computer connects remotely or locally with corresponding bandwidth to the Notification Server computer or Package Server, to which it is assigned, before the task timeout period is reached.	N/A
Computers in CEM mode cannot be turned on if necessary.	The **Power on computers if necessary** compliance setting is not supported for Internet-managed client computers due to limitations of remote power management technology.	N/A

Table 12-5 Software Portal issues

Issue	Description	Article link
Software Portal publishing permissions are incorrectly migrated during upgrade from Software Management Solution 6.x	When migrating from Software Management Solution 6.x the Software Portal publishing permissions for a software resource change their status from **Approved** to **Requesting Approval**.	N/A
Software Portal becomes inaccessible in case of invalid Kerberos configuration.	If the application identity user is a domain user with enabled **Use Kerberos DES Encryption types for this account** encryption option, the Software Portal page will be inaccessible from the client computers to any domain users.	N/A

Table 12-6 Hierarchy and replication issues

Issue	Description	Article link
Managed Delivery policy, which contains a software resource with applicability checks, is not replicated to the Child Notification Server.	If on the Parent Notification Server you create a Managed Software Delivery policy, which contains a software resource with Applivability checks, apply it to client computers, assigned to the Child Notification Server and then run an emergency update on that policy, the policy is not replicated to the Child Notification Server Workaround: To fix the issue, run the differential replication task.	N/A
Managed Software Delivery policies and Quick Software Delivery tasks execution requires Symantec Management Agent upgrade.	Due to significant changes in this component, Symantec Management Agent has to be upgraded to version 7.5 in an environment with hierarchy, to execute Managed Software Delivery policies and Quick Software Delivery tasks	N/A

Table 12-7 Non-Windows-specific issues

Issue	Description	Article link
A false-positive status for a software package on a Mac client computer may be reported, if the user cancels the software interactive installation.	If a user of a Mac client computer cancels a Quick Delivery task or a Managed Delivery task, which has an interactive install, the success execution event is sent to the Notification Server, leading to a false-positive status for this installation. At the same time, the software scan for the Quick Delivery task and the detection check for the Managed Delivery task provides the correct information.	N/A
Prerequisite checks are skipped during the installation of a single item from the MPKG files.	If a single item is specified from an MPKG file for installation on a Mac OS client computer, then the prerequisite checks are ignored during the installation on the client computer.	N/A

Table 12-8 Software Management Framework issues

Issue	Description	Article Link
Incorrect association results for two Notification Servers in a hierarchy in a certain situation.	Consider two Notification Servers in a hierarchy. This problem occurs if the parent and child have the same software resource imported but have different software products associated with the resource. When you perform replication from the parent to the child under these circumstances, the affected software resource on the child shows an incorrect association. Instead of showing one association from the parent Notification Server, the affected software resource shows two associations: one from the parent and one from the child. Workaround: Perform a second replication from parent to child. After this second replication, the affected software resource shows the correct association.	TECH176457
The **Software Data Provider Status** report does not show results.	When you add or run data providers and then try to view the status of the data providers using the **Software Data Provider Status** report, the report does not show results.	N/A
A Managed Software Delivery policy only logs off a single user session when there are multiple active or disconnected terminal sessions.	The **Log off user** option in the **Managed Software Delivery** policy logs off only a single session rather than all sessions when multiple sessions are active. For more information, see topics on Results-based actions settings in Software Management Solution in the *IT Management Suite Administration Guide* at the following URL: http://www.symantec.com/docs/DOC5330 Workaround: Use the **Log off** option available with the **Restart Computer** task to successfully log off every session.	N/A
The **Windows Language** applicability rule does not work properly when **Neutral** language is selected.	The applicability check status should evaluate as **Detected** and the software installs successfully. Instead, the applicability check evaluates as **Not Detected** and the software is not installed.	N/A
Software Components do not replicate using **Replicate Now**.	Replication of software components does not work from a parent or child Notification Server when you use **Replicate Now** in the following situations: ■ In the **Software** view, when you use the right-click menu **Hierarchy > Replicate Now** on either **Software Releases** or **Software Updates**. ■ In the **Manage** menu, select **All Resources**, and right -click on a software component. From the right-click menu select **Hierarchy > Replicate Now**.	N/A

Table 12-8 Software Management Framework issues *(continued)*

Issue	Description	Article Link
An incorrect version is reported for Microsoft Internet Explorer 8.	When you run **Collect Full Inventory** on a client computer with Microsoft Internet Explorer 8 installed, the version is incorrectly displayed in the inventory report.	N/A
If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails.	If an externally initiated restart is performed during Managed Software Delivery, then the software that is installed after the restart fails. The reason the installation fails is that the software starts to install while a user logoff is still pending	N/A
Software resource associations of a software component to file are not present if an application is installed on a client computer for a specific user.	Consider a software application that is installed on a client computer by a specific user. A **Collect Full Inventory** is then run for that client after a different user logs in to this computer. In this situation, the resource associations of the software component to file is lost for this software resource. The problem occurs because Software Discovery tries to load values from a user-specific registry. However, it is unable to load those values because the specific user is not logged on.	N/A
Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	Files in the **File Inventory** tab are overwritten if a software resource is moved to **Managed Software** and metering is turned on for this software resource.	N/A
Quick Delivery tasks fail to execute by timeout when maintenance window is set up on clients.	If you create a Quick Delivery task and the task times out before the maintenance window is activated on the client, the task fails. By default, a task times out after 300 minutes. On the **Task options** tab of the Advanced settings, you can change when a task ends.	N/A
Problems with the applicability check in a Managed Software Delivery policy.	If a Managed Software Delivery policy delivers two software resources and the second software resource is dependent on the first software resource, the applicability check for the second resource fails. The failure occurs because this check runs before the first software resource is installed.	N/A
Applications with large installation paths fail to execute.	With a Managed Software Delivery policy or Quick Delivery task, applications with large installation paths fail to execute.	TECH133459

Table 12-8 Software Management Framework issues *(continued)*

Issue	Description	Article Link
When creating a package by ASDK command lines may get not generated for the package.	When creating a package by ASDK **AutoGenerateCommandLines** parameter set to **True**, no command lines are generated for the package.	N/A
Unable to add one large file or a very big number of small files, estimating around 2 GB in total, while editing a software resource.	If you add one large file or a very big number of small files, estimating around 2 GB in total, the procedure will fail with errors in the Notification Server computer log file, while editing a software resource.	N/A
Java Update software component is not added into the Software Catalog after running the Software Discovery task.	Java 6 Update software component, which is installed on the client computer, is not added into the Software Catalog after running the Software Discovery task.	N/A
Installation error code descriptions are not migrated when upgrading from Software Management Solution 7.0.	Modified installation error code descriptions are reset to default values, after upgrading from Software Management Solution 7.0.	N/A
Agents and plug-ins, which versions are before 7.1 SP2, cannot execute software delivery policies and tasks on the client computers, after upgrading to Software Management Solution 7.5.	After the upgrade to Software Management Solution 7.5, none of the software delivery tasks or policies can be executed on the client computers by the agents and plug-ins, which versions are before 7.1 SP2, due to significant security changes, introduced in version 7.1 SP2. Workaround: To fix this issue, upgrade agents and plug-ins on the client computers.	N/A
Weak ACL for a shared location, which is used for the Software Library, may lead to issues with Software Library data safety.	Setting weak ACL, such as "Everyone", for a shared location, which is used for the Software Library, may lead to intentional or unintentional loss of Software Library data or lack of storage on the corresponding server. Workaround: To prevent the issues, set strong ACL for UNC path, which leads to the Software Library repository.	N/A
Old **AddRemoveProgram** data class entries are displayed in the Resource Manager after the corresponding software is upgraded on the client computers.	If a client computer software, for which the data is already gathered by the **Collect full inventory** task, is upgraded, old entries in the AddRemoveProgram data class are visible in the Resource Manager, even after running the **Collect full inventory** task on this client computer. Workaround: To fix the issue, run the **Collect full inventory** task on this client computer once again.	N/A

Table 12-8 Software Management Framework issues *(continued)*

Issue	Description	Article Link
Importing packages, if package files contain sensitive information in unencrypted form, may lead to a possibility of information disclosure threat.	When importing software packages using Import Software wizard, package files can be read by an unauthorized party during data transfer from package store to the Notification Server computer. If package files contain sensitive information, such as passwords inside scripts, in unencrypted form, then such software import can be a subject to information disclosure threat	N/A
Users with enabled required privileges and permissions cannot create delivery tasks.	Level 1 Worker with enabled required privileges and permissions cannot create a Quick Software Delivery task and a Managed Software Delivery Policy	TECH195077
An error appears, when trying to install Wise Toolkit.	An error appears, when trying to install Wise Toolkit on a server with installed Software Management Solution 7.5 as a result of the end-of-life of Wise Package Studio.	TECH210284
Migrated software components are not merged with newly discovered software components if those components have separate 32-bit and 64-bit versions.	After upgrading to Software Management Solution 7.5, software component duplicates appear in Software Catalog, after running Software Discovery for those components which have 32-bit and 64-bit separate versions	N/A

Table 12-9 Other issues

Issue	Description	Article link
Software resource “conflicts with” association is lost after detailed export – import procedure.	If you run a Detailed Export for a software resource, which has a "conflicts with" association, then this association is not displayed after importing the resource from the XML file.	N/A

Fixed issues

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

Table 12-10 Fixed issues

Issue	Description	Article link
The emergency policy update launched from a task you added in the Managed Delivery policy does not get replicated on child-level Notification Server computers.	The emergency policy update launched from a task you added in the Managed Delivery policy does not get replicated on child-level Notification Server computers. An exception occurs in Notification Server logs stating "does not have any package items associated with it".	N/A
Agent does not load user's environment variables when software delivery jobs are executed under non-root user.	Task fails when running software delivery in Mac UI under currently logged-in user. The user was logged as "tester" (not root) and "Run Task" button was pressed under Utilities -> Altiris Agent -> Software Delivery. Command line was used as : `whoami >> $HOME/task1.log` The result was not written in appropriate directory and history showed an error. Running "aex-swdapm" from command-line did not reproduce this error. Command was run successfully and result written to $HOME/task1.log file. This also applies for Run as option in advanced option of software delivery policy.	N/A
Software resource names mapping is discarded during the IT Management Suite upgrade.	The changes that are made to the Known As mapping of the software resource are discarded during the upgrade from IT Management Suite 7.1 to IT Management Suite 7.1 SP2.	N/A

Chapter 13

Symantec Endpoint Protection Integration Component

This chapter includes the following topics:

System requirements

Endpoint Protection Integration Component requires the following software to be installed:

- Symantec Management Platform 7.5.
  When you install Endpoint Protection Integration Component using Symantec Installation Manager, the Symantec Management Platform is installed automatically.
- Symantec-Real Time Console Infrastructure 7.5.

The operating systems that are supported by the Symantec Management Platform are also supported by Endpoint Protection Integration Component.

For more information, see the product support matrix at the following URL:
http://www.symantec.com/docs/HOWTO9965

Known issues

The following are the known issues for this release:

Table 13-1 Known issues

Issue	Description
Collecting Antivirus Inventory for F-Secure Anti-Virus 2012	The **Antivirus inventory** task is unable to collect inventory for F-Secure Anti-Virus 2012.
Support for McAfee 2011 v10.5.227 in JP/CS/CH/KN languages	Endpoint Protection Integration Component does not support McAfee 2011 in the following languages: ■ Chinese Simplified ■ Japanese ■ Korean ■ Chinese Traditional
Endpoint Protection Integration Component task issues with Symantec Endpoint Protection 12.1	Endpoint Protection Integration Component scan tasks such as full scan and Quick Scan fail on Symantec Endpoint Protection 12.1.
Endpoint Protection Integration Component repair task execution	Endpoint Protection Integration Component repair task does not execute for the supported Symantec Endpoint Protection versions except Symantec Endpoint Protection 11.0.7072.1031.
Registry entries and folders	Few registry entries and folders are present even after you uninstall the existing antivirus. The count of these entries and folders varies for the antivirus solutions.

Table 13-1 Known issues *(continued)*

Issue	Description
Uninstallation and inventory of localized antivirus software	The Endpoint Protection Integration Component 7.5 does not support inventory or uninstallation of the localized versions of the following antivirus software: ■ F-Secure AV 2012 ■ F-Secure IS 2012 ■ F-Secure AV for workstations 9.30 ■ Kaspersky Endpoint Protection Integration Component 7.5 by default supports the uninstallation and inventory of the following localized antivirus software: ■ ESET NOD32 5.0 ■ ESET SMART SECURITY 5.0 ■ CA Antivirus Plus 2010 ■ McAfee Antivirus Plus 2012 ■ McAfee Total Protection 2012 ■ Trend Micro Office Scan Client 10.5 ■ F-Secure AV for Windows Servers 9.20 ■ SAVCE 10.1.9000.1 ■ SOPHOS Antivirus 9.7 Endpoint Protection Integration Component 7.5 supports the uninstallation of the following localized antivirus software: ■ MS Forefront Endpoint Protection 2010 ■ SAVCE 10.1.9000.9
32-bit and 64-bit package	If a 32-bit package is selected for installation on a 64-bit computer, or a 64-bit package is selected for installation on a 32-bit computer, then the migration job fails.
Power Sensitive Malware Scanning and Remote Machine Repair via IDER and SERT tasks are not supported on CEM environment.	The **Power Sensitive Malware Scanning** and Remote Machine Repair via IDER and SERT tasks do not work in CEM environment as the **Power On** task is not supported on the CEM environment.
Support for uninstallation of Kaspersky Antivirus	The Symantec Endpoint Protection Integration Component 7.5 does not support the uninstallation of Kaspersky antivirus.

Fixed issues

The following are the fixed issues for this release:

Table 13-2 Fixed Issues

Issue	Description
The pie chart legend summary displayed incorrect client computer numbers.	The pie chart legend summary of the managed, unmanaged, unprotected, and managed protected computers displayed incorrect client computer numbers. This issue has been fixed.
The SEPIC migration job succeeded when the CA Antivirus Plus v2.0.0.265 and the CA Internet Security Suit 6.0.0.285 were installed on the client computer.	The SEPIC migration job succeeded when the CA Antivirus Plus v2.0.0.265 and CA Internet Security Suit 6.0.0.285 were installed on the client computer. This issue has been fixed.
SEPIC used all resources instead of all computers as resource targets.	The Endpoint Protection Integration used all resources instead of all computers as resource target. This issue has been fixed.
Notification Server web applications had the view state MAC disabled.	Notification Server web applications had the view state MAC disabled and was a security threat. This issue has been fixed.
Endpoint Protection Integration failed to uninstall ESET-NOD32 Ver4.0, after installing SEP Client on the client computer.	The Endpoint Protection Integration failed to uninstall ESET-NOD32 Ver4.0, after installing SEP Client on the client computer. This issue has been fixed.
The SEPIC 7.1.1037 - RTCI security privileges were changed during SEPIC configuration.	The SEPIC 7.1.1037 - RTCI security privileges were changed during SEPIC configuration. This issue has been fixed.
The **System Jobs and Task contents** did not display the description about Symantec Endpoint Protection Management.	The **System Jobs and Task contents** did not display description about Symantec Endpoint Protection Management This issue has been fixed.
The Endpoint Protection Integration task issue on delivery of the SEP 12.1 package to the client computers.	The Endpoint Protection Client Integration Migration task failed to delivery of SEP12.1 package on the client computers which had ESET NOD 32 antivirus installed. This issue has been fixed.

Table 13-2 Fixed Issues *(continued)*

Issue	Description
Installation of SEP 12 RU1 failed on client computers installed with SOPHOS 9.5.	The installation of SEP12 RU1 failed on client computers that are installed with SOPHOS 9.5 This issue has been fixed.
The SEP installation failed on client computers where McAfee 2011 was installed.	The SEP installation failed during migration of SEP12 RU1 package on client computers installed with McAfee 2011. This issue has been fixed.

Other things to know

Following are things to know about this release.

- Deprecated features
  See Table 13-3 on page 125.
- Things to know
  See Table 13-4 on page 125.
- Technology: Wake-on-LAN option or Intel vPro option
  See Table 13-5 on page 126.
- Testing results for multiple vPro scenarios
  See Table 13-6 on page 127.

Table 13-3 Deprecated features

Issue	Description
The **Repair Symantec Endpoint Protection Client** task does not support SEP 12.1 onwards.	The repair capability in SEPIC is limited to supported SEP versions older than 12.0. This capability is not available for newer versions

Table 13-4 Things to know

Issue	Description
Remote SERT Boot Task : IDER takes time to boot depending on size of an image	After you perform an IDE-Redirection, the vPro client takes some time to boot depending on the size of the image. There is no progress indicator provided on the **Remote SERT Boot Task** page. Once the restart is done, you can connect to the remote computer through the pcAnywhere **Remote Control** button. This could be verified if you try to connect to the vPro client immediately after redirection and if you are not able to connect to the client computer. This issue indicates that the client computer is in booting state.

Table 13-4 Things to know *(continued)*

Issue	Description
Remote SERT Boot Task : IDER is performed only on one computer at a time	The **Remote SERT Boot Task** is performed only on one computer at a time. If you select multiple computers, the redirection operation is performed on all the computers although you can take remote control of only one computer at a time. The Stop Redirection operation is performed on all the selected vPro computers
Power Sensitive Malware Scanning: Power On task fails on Wake-on-LAN enabled computers	Since the **Power On** task is designed for vPro computers, the task is expected to fail on non-vPro Wake-on-LAN enabled computers. The job continues to the next Wake-on-LAN task, which turns on non-vPro computers. The Wake-on-LAN task succeeds on vPro computers
Default connection profile should be configured before you execute **Remote SERT Boot Task** and **Power Sensitive Malware Scanning** Job	Before executing **Remote SERT Boot Task** and **Power Sensitive Malware Scanning** Job, you must configure the Default connection profile pertaining to the vPro computer's credentials (AMT protocol in Edit Default connection profile Window), so that the tasks execute successfully on vPro clients.
Default connection profile should be selected while executing **Remote SERT Boot Task** and **Power Sensitive Malware Scanning** Job.	When you create a **Remote SERT Boot Task** instance or **Power Sensitive Malware Scanning** Job instance, you should select the Default connection profile which has been configured for use on vPro computers. **Note:** For the **Power Sensitive Malware Scanning** Job, AMT credentials for all selected vPro computers must be the same.
Viewing the summary of unmanaged, managed unprotected and managed protected computers	The information pertaining to view the unmanaged, managed unprotected, and managed protected computers report was not incorporated in the User Guide. Do the following to view the summary of unmanaged, managed unprotected, and managed protected computers 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**. 2 In the left pane, click **Reports > Symantec Endpoint Protection Management > Details of unmanaged, managed unprotected and managed protected computers**.

The timeouts that are defined for each task in the Power Sensitive Malware are as follows:

Table 13-5 Technology: Wake-on-LAN option or Intel vPro option

Task	Hours
Wake on LAN/Power On (vPro)	60 mins /Approximately 1 hr

Table 13-5 Technology: Wake-on-LAN option or Intel vPro option *(continued)*

Task	Hours
Update Antivirus Definition	30 mins
Quick Scan /Full scan	60 min/10 hrs
Power off	30 mins

The results of the tests for multiple vPro scenarios are as follows:

Table 13-6 Testing results for multiple vPro scenarios

Type of scan	Scenario	Result
Power Sensitive Malware Scan	Select Both technologies (vPro and Wake On LAN) and execute a job on multiple computers (WOL and vPro), keeping one or more vPro computers unplugged.	Success. Job continues in other plugged computers.
Power Sensitive Malware Scan	Select Both technologies and execute a job on multiple computers (WOL and vPro), keeping one or more WOL computers unplugged.	Success. Job continues in other plugged computers.
Power Sensitive Malware Scan	Select Both technologies and execute a job on multiple computers (vPro only), keeping one or more vPro computers unplugged.	Success. Job continues in other plugged computers.
Power Sensitive Malware Scan	Select Both technologies and execute a job on multiple computers (WOL only), keeping one or more WOL computers unplugged.	Success. Job continues in other plugged computers.
Remote SERT Boot Task	Execute a task on Multiple vPro computers.	IDER task does not work on multiple vPro computer. It is designed for single vPro computer.

Table 13-6 Testing results for multiple vPro scenarios *(continued)*

Type of scan	Scenario	Result
Remote SERT Boot Task	Execute a task on Multiple vPro computers and stop IDER by clicking on Stop Redirection button.	Stop Redirection functionality does not work on multiple vPro computer. But it works for single redirected vPro computer.

Chapter 14

Virtual Machine Management

This chapter includes the following topics:

What's new in this release

In Virtual Machine Management 7.5, the following new features are introduced:

Table 14-1 List of new features

Feature	Description
Ability to create a virtual machine from a virtual machine template.	New **Deploy VM** task is introduced to create a new virtual machine from a predefined virtual machine template. You can access the **Deploy VM** task from both Virtual Machine Management portal page and **Jobs and Tasks** menu.
New **Template Details** page is introduced on the Virtual Machine Management portal page.	A new **Template Details** page is added in the Virtual Machine Management portal page to show the template details such as **Name**, **Host Name**, **Host IP Address**, etc.

Table 14-1 List of new features *(continued)*

Feature	Description
Enhanced support for Guest level tasks and Host level tasks.	Now, all the Host level tasks such as **Create VM**, **Create Disk**, **Create Network**, **Run Inventory** and all the Guest level tasks such as **Create Snapshot**, **Restart**, **Shut Down**, **Start**, **Stop**, **Suspend** are available through right-click option on **Manage > All Resources** page.
Enhanced Guest Summary report.	New fields such as **Percent CPU Usage**, **Snapshot Counts**, **Current Snapshot Name**, **Current Snapshot Description**, and **Current Snapshot Location** have been added in the **Guest Summary Report**.
Support for latest versions of the guest operating systems.	Now, Virtual Machine Management supports following latest versions of guest operating systems: ■ Windows 8 ■ Windows Server 2012
Introduced one new **Orphaned Virtual Machine Report** .	New **Orphaned Virtual Machine Report** report has been added to show the orphaned virtual machine details such as orphaned virtual machine name, operating system installed on it, when inventory has been run on the virtual machine, etc. Orphaned virtual machines are VMs that were deleted without VMware vCenter knowledge.
Better Support for Hosts and VM under cluster and folder.	Now, VMM supports hosts, virtual machines under cluster and folder.
New logos added for Virtual Machine Management tasks and templates.	All the existing VMM tasks logos has been replaced with the new user-friendly logos. The new logos help you to easily identify different VMM tasks and templates.
Support for latest versions of hypervisors.	Now, Virtual Machine Management supports following latest versions of hypervisors: ■ VMware ESXi 5.1 ■ Microsoft HyperV 2012
Support for Distributed switch port-group network.	Now, Virtual Machine Management supports existing Distributed switch port-group network to create virtual machines through the **Create Virtual Machine** wizard, and to deploy a virtual machine using the **Deploy VM** task.
New field is added in all Virtual Machine Management reports.	In all Virtual Machine Management report, a new field - **Last Inventory run time** has been added to inform you about the time when the last inventory was taken.
Better support to choose host operating system.	In the **Create VM** wizard, the **OS version** drop-down list displays only those operating systems, which are supported by the host on which , you are creating a virtual machine.

System requirements

Virtual Machine Management 7.5 requires the following software to be installed:

- Symantec Management Platform 7.5.
  When you install Virtual Machine Management using Symantec Installation Manager, the Symantec Management Platform is installed automatically.

The operating systems that are supported by the Symantec Management Platform are also supported by Virtual Machine Management.

For more information, see the product support matrix at the following URL:

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

Installing

Install the solutions and components in the following sequence:

- Symantec Management Platform 7.5
- Deployment Solution 7.5
- Symantec Virtual Machine Management 7.5

Supported hypervisors

The following are the hypervisors supported in Virtual Machine Management 7.5:

- ESX 4.0
- ESX 4.1
- ESXi 4.0
- ESXi 4.1
- ESXi 5.0
- ESXi 5.1
- Hyper-V (Win 2K8 R2 enterprise)
- Hyper-V (Win 2K8 R2 SP1)
- Hyper-V (Win Server 2012)

vCenter 4.0, vCenter 4.1, vCenter 5.0, and vCenter 5.1 are also supported. They can be used to manage ESX 4.0, ESX 4.1, ESXi 4.0, ESXi 4.1, and ESXi 5.0 ESXi 5.1.

Known issues

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

Table 14-2 Known issues in Virtual Machine Management 7.5

Issue	Description	Article Link
All the guest operating systems are not available for selection while creating a virtual machine using the **Create VM** task.	To work around this issue, the desired unavailable guest operating systems can be installed on the new virtual machines by selecting other relevant operating systems, which are available for selection. For example, you can create a virtual machine with 'Windows Server 2008' x64 bit by selecting 'Windows Server 2008 R2 (64bit)'.	N/A
Base or old snapshot disk files, which are associated with a virtual machine, can be deleted or used as existing disk for new virtual machines.	Base or old snapshot disk files that are associated with the virtual machines and have at least single snapshot then they can be deleted or used as existing disk for new VM. These virtual machines include any Hyper-V VM or VMs whose exiting disks are used in ESX servers.	N/A
Virtual machine tasks are queued.	Virtual Machine Management tasks are queued because discovered virtual machines do not get assigned to site servers. The workaround is to explicitly assign 'All discovered Hypervisors' and 'All Virtual machines' to site servers.	N/A
Some VMs do not appear in the 'Inv_Vm_Guest' table.	Some VMs do not appear in the 'Inv_Vm_Guest' table after a network discovery task due to reasons like duplicate VM or template name exists under same host or VM\template with duplicate IP address. VMs do not appear in the left pane on the VMM portal, but do exist in the vSphere client. As a result, you cannot run any VMM tasks. The VMs do appear in ND logs.	N/A
Network Discovery task is not running on vCenter 4.0, but it is running on other Hypervisors after Microsoft patch installation.	The Network Discovery tasks are failing on vCenter 4.0, but they are running on other Hypervisors after Microsoft patch installation. This issue is happening because the vCenter 4.0 certificate is using 512-bit RSA keys. To work around this issue, use vCenter certificates with a minimum RSA key length as 1024. Alternatively, you can execute the command below on the task or NS server and set the minimum allowed RSA key length to 512. `certutil -setreg chain\minRSAPubKeyBitLength 512`	kb/2661254

Table 14-2 Known issues in Virtual Machine Management 7.5 *(continued)*

Issue	Description	Article Link
Run Inventory task is failing due to protocol issues.	The Run Inventory task is failing due to protocol issues. To work around this issue, it is recommended that any discovery tasks that include vCenter servers in their scan range must use a connection profile where the VMware protocol is enabled and include the corresponding vCenter credential information. Be aware that enabling the VMware protocol in tasks with large scan ranges can take considerably longer to execute. You should consider excluding vCenter servers from these tasks so the VMware protocol does not need to be enabled for them, thus avoiding unsuccessful attempts to use the VMware protocol on a wide range of nodes. Instead, you can create vCenter-specific discovery tasks, where the individual vCenter servers are identified and the tasks use a connection profile where the VMware protocol as well as any other protocols needed to communicate to that server are enabled.	N/A
No operating system is displayed on the portal page.	On the **Virtual Machine Management** portal page, if you click a virtual machine on a Hyper-V server, the portal page does not display any operating system.	N/A
Capacity of the unassociated virtual disk is not displayed on the portal page.	On the **Virtual Machine Management** portal page, if you select an ESX server, the capacity of the virtual disk is not displayed if the disk is not associated with any virtual machine	N/A
Error displayed when you run a network discovery task on multiple ESX computers with the same name.	When you run a network discovery task on multiple ESX computers with the same name consecutively, the task updates the same resource entry. It does not create a separate resource entry for every ESX server.	N/A
Creation or deletion of virtual disks.	For the successful creation or deletion of virtual disks on the hosts, which are managed and discovered by a vCenter, the credentials for the hosts and respective vCenter must be the same.	N/A
Limitations to the Add host function.	On the **Virtual Machine Management** portal page, if you want to add a host, only the default connection profiles work.	N/A
You cannot delete the virtual resources and the snapshots that have special characters in their names.	You can successfully create virtual machines, virtual disks, virtual networks, and the snapshots that have special characters in their names. However, if you run the delete task to delete any of these resources, the task fails and does not delete the item. To work around this issue, do not use the following characters in the names of the virtual resources: "&", "<", ">".	N/A

Table 14-2 Known issues in Virtual Machine Management 7.5 *(continued)*

Issue	Description	Article Link
The Virtual Machine Management portal page does not show edited data.	The Virtual Machine Management portal page does not show the edited data of your virtual resources. After you successfully perform any of the Virtual Machine Management tasks, the information on the **Virtual Machine Management** portal page is not updated. To work around this issue, on the **Virtual Machine Management** portal page, in the left pane, click the **Refresh** symbol to refresh the page and to see the edited data.	N/A
The data on the Virtual Machine Management portal page is not updated after you delete any virtual resources.	After you manually delete a virtual network, virtual disk, or snapshot on the host server, the resources are still displayed on the **Virtual Machine Management** portal page. To work around this issue, run the VMM inventory task to get the updated data.	N/A
The Virtual Machine Management portal page displays a virtual machine that is deleted manually in the list of virtual machines.	After you manually delete a virtual machine on the host server, the virtual machine still appears on the **Virtual Machine Management** portal page, in the list of virtual machines. However, if you create and run any Virtual Machine Management tasks on this virtual machine, these tasks fail. To work around this issue, run the discovery task on the host machine.	N/A

Fixed issues

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

Table 14-3 Fixed issues in Virtual Machine Management 7.5

Issue	Description	Article link
Run Inventory task was failing in cases where no virtual disks are attached or known to the virtual machines.	Run Inventory task was failing due unattached or unknown virtual disk of a virtual machine.	TECH199029
ESX hosts were swapped between two vCenters, which are managing more than one ESX hosts each.	ESX hosts were swapped between two vCenters, which are managing more than one ESX hosts each. Due to this, the hosts were not displayed properly as they displayed in the vSphere client.	N/A

Table 14-3 Fixed issues in Virtual Machine Management 7.5 *(continued)*

Issue	Description	Article link
Run Inventory task was failing on ESX hosts, which were under Cluster in vCenter.	Run Inventory task was not working successfully with ESX hosts under Cluster in vCenter.	N/A
Run Inventory task was failing due to timeout of the inventory tasks.	Run Inventory task was failing as it was taking a very long time to gather a large amount of Virtual Machine Management data.	N/A

Other things to know

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

Table 14-4 Other things to know

Issue	Description	Article link
Run the **Network Discovery** task and **Run Inventory** task, before viewing the **Orphaned Virtual Machine Report** report.	Before viewing the **Orphaned Virtual Machine Report** report, you must perform the **Network Discovery** task and **Run Inventory** task to get better results through the report.	N/A
Recommended Hyper-V ISO file paths.	In the **Create Virtual Machine** wizard, for a host, the ISO paths are available for selection only if they are under the parent folder or a root folder of the host In case of Hyper-V ISO files, the ISO paths are available for selection only in following scenarios: ■ ISO files are located under default Hyper-V disk path where `.vhd` files get saved. ■ ISO files, which are referred or used by existing VMs irrespective of file path location. If ISO files are not available for selection then you can specify the path manually.	N/A
Change in the preconfigured Virtual Machine Management Inventory task instance.	The preconfigured Virtual Machine Management inventory task instance is updated to let you edit and delete the task instance. By default, the task is configured to run at 6:30 P.M. daily on all discovered hypervisors. After the preconfigured VMM Inventory task instance is updated, the default schedule is changed based on the modified schedule.	N/A

Table 14-4 Other things to know *(continued)*

Issue	Description	Article link
Prerequisites for the **Shut Down** and **Restart** power control options support.	Before performing the **Shut Down** or **Restart** task, ensure that the following prerequisites are met: ■ Virtual machine is in **Power ON** state. ■ Operating system is running on the virtual machine. ■ VMware Tools for VMware or Integration Services for Hyper-V, is installed on the virtual machine. Currently, the **Shut Down** and **Restart** tasks are not available for all the guest operating system types.	N/A
Use alphanumeric characters.	The names of the virtual disks and virtual networks must only contain alphanumeric characters.	N/A
Enable the Hyper-V server to work with remote WMI calls.	Hyper-V server communication uses the WMI protocol. The default firewall settings block WMI connections. You must enable Hyper-V server to work with WMI calls.	N/A
Additional information about the **Create Virtual Machine** wizard.	You need to select a Deployment Solution job only in the last step of the wizard that includes the partition task and the **Scripted Operating System Install** task.	N/A

Chapter 15

Workflow Solution

This chapter includes the following topics:

What's new in this release

In Workflow Solution 7.5, the following new features are introduced:

Table 15-1 List of new features in Workflow Solution 7.5

Feature	Description
Web Application project type	Web Application project type feature lets you use multiple models in the same project. Following are the uses of Web Application project type: ■ You can use Workflow, Dialog, and Service Models in the same project. ■ You can use multiple entry points to control how the Web Application project type is consumed. ■ You can use the **Start Workflow** component to invoke a Workflow Model from another Model Type.
Workflow Solution Center	The Workflow Solution Center is an online repository that contains the following items: ■ Prebuilt Workflow templates and updated Workflow component packs for you to download. ■ Videos and documentation on how to implement the templates and the component packs.

Table 15-1 List of new features in Workflow Solution 7.5 *(continued)*

Feature	Description
Collaborative component wiki	Symantec Connect has created a wiki page for each component that is included with the default installation of Workflow. This new component wiki model makes structured, community-based content available at its point of use. Following are the features of the component wiki pages: ■ All component information is now stored on Symantec Connect in the collaborative component pages. ■ Each component has its own wiki page. ■ The collaborative component pages are community-based. ■ You can also access the component wiki pages from the Workflow Designer.
Active Directory auto-authentication is supported in Google Chrome and Mozilla Firefox	Active Directory auto-authentication is supported in Google Chrome and Mozilla Firefox in addition to Internet Explorer. For any additional configurations that may be required, see the knowledge base article, *Pass-thru Authentication with Chrome & Firefox on ServiceDesk & Workflow* at the following URL: http://www.symantec.com/docs/TECH204270

Known issues

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

Table 15-2 Known issues in this release

Issue	Description	Article link
JavaScript error encountered in Internet Explorer 9 when expanding or collapsing groupings, resizing columns, or sorting columns.	When you log in to the Process Manager portal using Internet Explorer 9, click the My Tasks Lists tab, and perform one of the tasks listed above, you find that the JavaScript functionality is lost. The loss of functionality usually occurs shortly after the page refreshes. The following error message is displayed in Internet Explorer 9: `SCRIPT5007: Unable to get value of the property 'init' object is null or undefined ig_WebGrid_dom.js, line 4911 character 2.`	N/A

Table 15-2 Known issues in this release *(continued)*

Issue	Description	Article link
Cannot start Workflow Designer tool on computers on which User Account Control (UAC) is enabled.	The Windows Explorer does not have permissions to access the Workflow Designer executable file. Additionally, the following error message is displayed: `Windows cannot access the specified device, path, or file. You may not have the appropriate permissions to access the item.` **Workaround**: Execute the Windows Explorer using **Run as Administrator** privilege. Then start the Workflow Designer tool using the Windows Explorer instance that has full administrative privileges.	N/A

Fixed issues

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

Table 15-3 Fixed issues in this release

Issue	Description	Article link
Enhanced Grid Component	The updated web form Grid Control lets end users edit data in the grid without the need for constant post-backs. This change provides a better user experience.	N/A
Menu Select Component	The **Menu Select** component now has the **Open On Click** property. Additionally, the issue of retrieval of previous category items and sub items when the user has moved to a different category item is resolved.	N/A
<style > tag in Process History entry	Improved handling of <style> tags in the **Process History** Web Part.	N/A
Creation of a new group from an existing group crashes the group creation process	You can now create a new group from an existing group document, along with copying category permissions from the existing group to the new group.	N/A
Using the ServiceDesk classification as an administrative user breaks the global sessions, and does not let you classify or reclassify incidents	You can now log on as an administrative user and classify a new ServiceDesk incident or an existing ServiceDesk incident without breaking the global sessions. Additionally, the **EnsembleMenuSelect** component is not disabled across the environment.	N/A

Table 15-3 Fixed issues in this release *(continued)*

Issue	Description	Article link
HTML editor is removed from the comment editor of the **Process View** page	The HTML editor is removed from the comment editor in the **Process View** page. Additionally, if you enter any script tag in **HTML** view or **Design** view, then the following error message is displayed: `A potentially dangerous Request.QueryString value was detected from the client.`	N/A
SQL SymQ had bad queries that used `BINARY_CHECKSUM`	SQL SymQ had bad queries that used `BINARY_CHECKSUM`, which resulted in the processes that had tasks belonging to other processes. The issue is resolved with creation of newly- computed columns that apply SQL collation for case sensitivity.	N/A
Email template information did get updated after updating the rule sets	The email that is sent now gets updated with the modified template information and modified rule set information.	N/A
Could not log on large number of users with longer session time to the Workflow portal	The issue is resolved after the SYMQ `local.ensemble.credentials`, which maintains cache information for `LBME.ProcessManagerSessions` has the **Init Procedure** setting that is configured to `DoNotLoad` value by default.	N/A
Report Process ID field was not displayed for **IFrame** Web Part in the report	The report now displays **Report Process ID** field for **IFrame** Web Part.	N/A
Could not authenticate Workflow users of Workflow, and therefore ServiceDesk 7.5 users with locked down flows could not send email to people outside their domain.	The Workflow user is now authenticated by sending an email to the SMTP server using the **Master Settings** page of the Process Manager.	N/A
For automation rule set that was configured to **Any group satisfies** setting, the rule was always evaluated as conditions being met and rule action was executed	Automation rule set that is configured to **Any group satisfies** setting now evaluates for any one created group to have the associated conditions satisfied. After the associated conditions for any one group are met, the rule action is executed.	N/A
Report Viewer Web Part	The report entries now appear as expanded or contracted as per the report settings in the **Report Viewer** Web Part.	N/A
Pass-through authentication	Pass-thru authentication now works for login pages created in project by Process Manager Login component.	N/A

Table 15-3 Fixed issues in this release *(continued)*

Issue	Description	Article link
Search feature for the **Service Catalog** Web Part	The search feature for**Service Catalog** Web Part can now be displayed or hidden per the configuration in the **Service Catalog Settings** page. Select or clear the **Show Search** check box to show or hide the **Search Service Item** option.	N/A

For more information about additional fixed issues in Workflow Solution 7.5, see the following URL:

http://www.symantec.com/docs/DOC6715

Other things to know

The following are the things to know about this release. If additional information about an item or feature is available, a corresponding article link is provided.

Table 15-4 Things to know

Component	Description	Article link
Improved security controls on the Workflow Server	Symantec has improved security controls on the Workflow Server. The improved security can potentially block the ability to deploy from a local Workflow Designer to a remote Workflow Server. If you cannot deploy to a remote Workflow Server, change the following setting on the remote Workflow Server before attempting to deploy. To allow remote connections: ■ On the Workflow Server, right-click on the **Task Tray Tool** and click **Settings**. ■ In the **Workflow Server** section next to **Workflow Server Configuration**, click the ellipsis. ■ In the **General** section, check **Allow Remote Connections**. Please note that the Symantec security best practice is to revert this setting after you are finished deploying. For more information on Symantec security best practices, see the article *ServiceDesk/Workflow General Security Best Practices*.	DOC6160
Cloud-enabled Management	Workflow does not support Cloud-enabled Management.	N/A

Table 15-4 Things to know *(continued)*

Component	Description	Article link
Support for Workflow and ServiceDesk	The knowledge base article lists the guidelines for support of Workflow and ServiceDesk, and the Symantec supportability statement for these solutions.	HOWTO92270
Obsolete exchanges that are displayed in **SymQ Configurations** tab.	Following is the list of obsolete exchanges that were removed from the **SymQ Configurations** tab in the Workflow Explorer: ■ `WebServiceExchange` ■ `TransactionalFileexchange` ■ `ThreadLocalMemoryExchange` ■ `SynchronizedExchange` ■ `SecuredInMemoryExchange` ■ `RemoteServerexchange` ■ `RemoteSecureServerExchange` ■ `RedundantBranchQueueExchange` ■ `MailTargetExchange` ■ `DualTransactionalExchange`	N/A
The session timeout setting for Process Manager is changed from days to minutes.	The session timeout for Process Manager is changed from number of days to number of minutes. Additionally, the default session timeout is changed from 90 days to 90 minutes. After the configured session timeout in minutes, the user needs to log on to access Process Manager.	N/A
The functionality of remotely installing of Workflow Server from Symantec Management Platform is removed in Workflow Solution 7.5.	The remote installation of Workflow Server from Symantec Management Platform is removed from Workflow 7.5 for security reasons. Therefore, you cannot install Workflow Server using the **Workflow Enterprise Management** page. To install Workflow Server, you must download and execute the Workflow installer and then register the server with Enterprise Management.	N/A

Table 15-4 Things to know *(continued)*

Component	Description	Article link
The Process Manager session ID is now read directly from the Process Manager authentication cookie.	For security reasons, the Process Manager session ID is now read from the authentication cookie instead of the `EnsembleSessionID` query string value. For this scenario, both the Process Manager and any application that uses the Process Manager login component must have the same computer key.	For more information on configuring the computer key using the IIS Manager for the Process Manager and any other application, see the following Microsoft TechNet article: http://technet.microsoft.com/en-us/library/cc772287(v=ws.10).aspx
FileBrowserWebpart	The FileBrowser Web Part has been deprecated, and is no longer available from the following navigation path: **Process Manager > Admin > Portal > Webparts Catalog > UI**	N/A
Non-native PDF components have been removed.	The non-native PDF components are removed from Workflow Solution 7.5, because the two separate third-party libraries that are used by the components are deprecated. In Workflow Solution 7.5, only native PDF components are available.	N/A
MySQL driver has been removed.	The MySQL driver is removed from Workflow Solution 7.5, and therefore any Workflow Integration projects using MySQL would be affected. You can rebuild these projects using the ODBC driver.	N/A
Cannot use reserved names to create components names or property names in the Workflow Web Service Generator.	A few words are reserved or protected and must not be used to create component names or property names in the Workflow Web Service Generator. Errors can occur if you use the reserved names in the component names or property names.	For a complete list of the reserved names, see the following knowledge base article: HOWTO85069
Cube reporting	Cube reporting has been deprecated.	N/A
Workflow Installation and Configuration Guide	The *Workflow Installation and Configuration Guide* has been deprecated. The installation and the configuration instructions that were in this guide are now in the *Workflow User Guide*.	See the Symantec™ Workflow 7.5 User Guide.

Table 15-4 Things to know *(continued)*

Component	Description	Article link
Workflow Component Guide	The *Workflow Component Guide* has been deprecated. All component information is now stored on Symantec Connect in the collaborative component pages.	See the *Viewing the component help (wiki pages)* topic at the following URL: http://www.symantec.com/connect/blogs/contributing-workflow-s-collaborative-component-pages
Library Project Type	The Library Project Type is no longer an available in **Project Types** tab in the **New Project** dialog box.	N/A
Encrypted Process Manager connection string	The Process Manager connection string is encrypted. To change the encrypted Process Manager connection string, you use the **lbutil.exe** tool. Note that in previous versions of Workflow, you changed the Process Manager connection string in the web.config file. You can no longer change the connection string in the web.config file. For more information about using the **lbutil.exe** tool, see the article *Using the lbutil.exe tool to update connection strings*.	HOWTO80684
MySQL database connector	The MySQL database provider that is used in the SQL components generator has been deprecated in Workflow 7.5. If you use MySQL components, a message is displayed to inform you that the MySQL database connector can no longer be implemented. You can continue to integrate the Workflow SQL generator to a MySQL database by using the ODCB provider. See the *About the query script generator* topic.	See the Symantec™ Workflow 7.5 User Guide.