

Altiris™ IT Management Suite 7.5 from Symantec™ Beta Guide

Version 1.0



Altiris™ IT Management Suite 7.5 from Symantec™ Beta Guide

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

Copyright © 2012 Symantec Corporation. All rights reserved.

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

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 Web site 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

Technical Support	4
Chapter 1 About IT Management Suite 7.5 Beta	9
About IT Management Suite	9
Symantec beta process overview	9
About the beta test cycle	10
Beta objectives	10
Providing feedback	11
What's new in IT Management Suite 7.5	11
Limitations of the Cloud-enabled Management feature	12
Chapter 2 Performing a fresh installation of IT Management Suite and setting up Cloud-enabled Management	15
Installing IT Management Suite 7.5 Beta	15
Preparing your environment for Cloud-enabled Management	21
Setting up Cloud-enabled Management	26
Chapter 3 Evaluating Beta use cases	33
Evaluating Beta use cases	33
Setting up Cloud-enabled Management	34
Installing Symantec Management Agent on a computer that never connects to LAN or VPN	34
Running hardware and software inventory on remote computers without VPN	36
Tracking usage of the managed software products	37
Delivering software using a Quick Delivery task	39
Pre-staging a software	40
Delivering patches to remote computers and to local computers	41
Running a job on a CEM-enabled system	42
Disabling the Internet gateway	42
Verifying Cloud-enabled Management reports	43

Chapter 4 Known issues in IT Management Suite 7.5 Beta 45

 Known issues of the Symantec Management Platform 45

 General Known Issues 46

 Cloud-enabled Management 47

 Notification Server 48

 Task Server 49

 Package Server 50

 Known issues of the Solutions 50

 Asset Management Solution and CMDB Solution 51

 Deployment Solution 51

 Monitor Solution for Servers 52

 Patch Management Solution for Linux 53

 pcAnywhere Solution 53

About IT Management Suite 7.5 Beta

This chapter includes the following topics:

- [About IT Management Suite](#)
- [Symantec beta process overview](#)
- [About the beta test cycle](#)
- [Beta objectives](#)
- [Providing feedback](#)
- [What's new in IT Management Suite 7.5](#)
- [Limitations of the Cloud-enabled Management feature](#)

About IT Management Suite

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

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

Symantec beta process overview

Welcome to the Symantec Beta program! We appreciate your participation in our development process and highly anticipate your feedback. Please feel free to

contact the **Altiris™ IT Management Suite 7.5 from Symantec™** development team with any questions or concerns during this Beta cycle.

This document provides necessary information to complete the Beta cycle for IT Management Suite.

About the beta test cycle

The beta test cycle is intended to run until the generally available release. Your feedback is vital in helping us to build a high-quality product. Please report any defects or concerns to Symantec immediately to give us sufficient time to address the issue. Symantec will contact you on a regular basis during the Beta cycle to obtain your feedback.

The instructions for installing the IT Management Suite 7.5 Beta version are provided in the guide.

We have included specific use cases to help you in your testing process. Using these use cases lets us receive feedback on the product areas that are the focus of this Beta cycle.

Beta objectives

The objectives of the Beta release are to evaluate the behavior of specific features of the IT Management Suite under the environments that are different from Symantec's internal test beds. Therefore, you as a system administrator can run the product in your widely varied test environments, with increased user and environment product exposure. Specific use cases are provided to assist you in a thorough evaluation of certain areas of the product operation. As the current version is a Beta version of the product, some components may not be fully functional. The supplied use cases focus only on certain functional components.

The following use cases are the focus of this Beta release:

- Enabling Cloud-enabled Management. Setting up Internet gateways.
- Installing Symantec Management Agent on a computer that never connects to LAN or VPN.
- Running hardware and software inventory on remote computers without VPN.
- Metering software usage.
- Delivering software using Quick Delivery task.
- Pre-staging a software.
- Delivering patches to remote computers and to local computers.

- Running a job on a CEM-enabled system.
- Disabling one of the Internet gateways.
- Verifying Cloud-enabled Management reports.

Providing feedback

You can provide your feedback using your [SymBeta](#) account for IT Management Suite 7.5 Beta. If you cannot access SymBeta, then you can contact Beverly Brown, whose contact details are as follows:

Email: Beverly_Brown@symantec.com

What's new in IT Management Suite 7.5

In the 7.5 release of IT Management Suite, the following new features are introduced:

Table 1-1 List of new features

Component	Description
Cloud-enabled Management (CEM)	<p>Cloud-enabled Management (CEM) lets you manage traveling 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.</p> <p>The following solutions and functionality is supported over CEM:</p> <ul style="list-style-type: none"> ■ 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. CEM is supported on Windows computers only. ■ Software Management Solution ■ Patch Management Solution

Table 1-1

List of new features *(continued)*

Component	Description
The list of supported operating systems has been expanded.	<p>The following SQL Servers are now supported for Configuration Management Database (CMDB):</p> <ul style="list-style-type: none">■ Microsoft SQL Server 2008 R2 SP2■ Microsoft SQL Server 2008 R2 SP3■ Microsoft SQL Server 2012 <p>The following platforms are now supported for the installation of Symantec Management Platform and its components:</p> <ul style="list-style-type: none">■ Windows Server 2008 R2 SP2 (64-bit) <p>The following operating systems are now supported for the installation Symantec Management Agent:</p> <ul style="list-style-type: none">■ Windows 7 SP2■ Windows 8■ Windows Server 2008 R2 SP2■ Red Hat Enterprise Linux 5.7, 5.8, 6.2, and 6.3■ AIX 7.1
The SuppressReportAutorun functionality has been implemented.	<p>When SuppressReportAutorun is enabled and you open any report, the report does not run immediately. To see the results of the report, you must click Refresh.</p> <p>By default, the SuppressReportAutorun functionality is disabled. You can enable it in NS Configurator, under Core Settings > User Interface > Report > SuppressReportAutorun.</p>
UNIX, Linux, Mac Agent	<ul style="list-style-type: none">■ NTLMv2 is now supported for Mac computers.

Limitations of the Cloud-enabled Management feature

- In IT Management Suite 7.5 release, the limitations of the CEM feature are following:
- Monitor Solution, Deployment Solution (DS), Network Discovery (ND), Inventory for Network Devices, Virtual Machine Management (VMM), Symantec Endpoint Protection Integration Component (SEPIC), Out of Band Management Component (OOB), and Real-Time System Manager Component (RTSM) are not supported in the first CEM release.
ServiceDesk, Asset Management Solution, Barcode Solution, and IT Analytics are not affected by the CEM functionality.
 - CEM does not integrate with pcAnywhere.

Additionally, pcAnywhere Access Server is no longer part of the IT Management Suite and Client Management Suite, thus another remote control tool would have to be used for endpoints that are not on LAN or VPN. Product Management team is looking at providing a viable alternative in the Barcelona release timeframe.

- Server-initiated tasks run over CEM with some delay.
It should be noted though that clients accessing tasks will utilize pull functionality and not push. This means that an agent will only look for a task during its next task check-in cycle (every 30 minutes, by default). These cycles as well as task timeout settings can be managed in the Symantec Management Console, under **Settings > Notification Server > Task Settings > Task Agent Settings**. Also note that Task Server cannot communicate to the Notification Server computer through the gateway, which means that Task Server must be located on the local network with Notification Server.
- Placing all Internet gateways behind a hardware load balancer for security and optimal load balancing reasons is currently not officially supported. QA will not certify this environment in the first release.

Performing a fresh installation of IT Management Suite and setting up Cloud-enabled Management

This chapter includes the following topics:

- [Installing IT Management Suite 7.5 Beta](#)
- [Preparing your environment for Cloud-enabled Management](#)
- [Setting up Cloud-enabled Management](#)

Installing IT Management Suite 7.5 Beta

You install this product by using the Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *IT Management Suite Planning and Implementation Guide* at the following URL:

<http://www.symantec.com/docs/DOC4827>

Table 2-1

Process for installing the Symantec Management Platform products

Step	Action	Description
Step 1	Configure IIS compatiblity	<p>IIS must be configured with the roles and features that are required for IT Management Suite installation.</p> <p>Run the following command from a command prompt window:</p> <pre>ServerManagerCMD.exe -Install Web-Server Web-ASP AS-Web-Support Web-Mgmt-Compat Net-HTTP-Activation Net-Non-HTTP-Activ</pre>

Table 2-1 Process for installing the Symantec Management Platform products
(continued)

Step	Action	Description
Step 2	Meet the recommended system requirements.	<p>When you install Symantec Management Platform products, Symantec Installation Manager checks for the minimum system requirements. If the minimum system requirements are not met, it does not proceed with the installation.</p> <p>IT Management Suite 7.5 hardware recommendations for Notification Server and for Microsoft SQL Server (for Beta testing, the two services can be installed on the same server):</p> <ul style="list-style-type: none"> ■ Operating system: Windows 2008R2 SP1 ■ Processors: Dual-core ■ Disk Speed: SAS 10k ■ Disk Capacity: 80 GB ■ RAM: 6-8 GB <p>IT Management Suite 7.5 physical and virtual hardware recommendations for a Task Server (10-100 endpoints):</p> <ul style="list-style-type: none"> ■ Operating system: Windows desktop operating system with IIS 6.0 or IIS 7.0 and .NET Framework 3.5 features enabled ■ Processors: One core ■ Disk Capacity: 5 GB ■ RAM: 4 GB <p>IT Management Suite 7.5 physical and virtual hardware recommendations for a package server (10-100 endpoints):</p> <ul style="list-style-type: none"> ■ Operating system: Windows desktop operating system ■ Processors: One core ■ Disk Capacity: 5 GB ■ RAM: 4 GB <p>IT Management Suite 7.5 physical and virtual hardware recommendations for an Internet gateway server (up to 3000 concurrent connections):</p> <ul style="list-style-type: none"> ■ Operating system: Windows 2008 R2 SP1 with .NET Framework 3.5.1 feature enabled ■ Processors: One core ■ Disk Capacity: 100 - 250 GB ■ RAM: 4 GB ■ Two 1Gbit network adapters. Dual NICs are recommended as a security best practice, however a single NIC is supported.

Table 2-1 Process for installing the Symantec Management Platform products
(continued)

Step	Action	Description
		<p>Note: Symantec Installation Manager automatically checks the following items during its Installation Readiness Check (IRC). It will either automatically install them for you or provide you with a download link.</p> <p>The Symantec Management Platform products also require the following third-party software.</p> <ul style="list-style-type: none"> ■ Adobe Flash Player 10 ■ Adobe Reader ■ AJAX 1.0 ■ Microsoft Access 2010 OLEDB driver ■ Microsoft .NET 3.5 SP1 ■ Microsoft IE 7, IE 8, or IE 9 (compatibility mode only) ■ Microsoft Silverlight 5.0 ■ Application Server role and IIS 6 Management Compatibility, ASP, and Web Server role services ■ Sun Java Runtime 6 <p>For more information about the software and hardware requirements, see the <i>IT Management Suite Planning and Implementation Guide</i> at the following URL:</p> <p>http://www.symantec.com/docs/DOC4827</p>
Step 3	Download beta components	<p>Go to https://ymbeta.symantec.com/home.html and follow the instructions to download the following files:</p> <ul style="list-style-type: none"> ■ SymantecInstallationManagerSetup.exe - is the installation executable. ■ itms_7_5.pl.xml - is the product listing file that points to the individual component .msi files. ■ ITMS 7.5 Beta License.zip - contains the 30-day trial licenses (for 10 clients). ■ PF_2858297_Install.zip - is a point fix for a Deployment Solution issue. ■ Altiris IT Management Suite 7.5 from Symantec Beta Guide.pdf - provides necessary information to complete the Beta cycle.
Step 4	Install Symantec Installation Manager	Run SymantecInstallationManagerSetup.exe.

Table 2-1 Process for installing the Symantec Management Platform products
(continued)

Step	Action	Description
Step 5	Point to the Beta product listing.	<p>To install the beta versions of the IT Management 7.5 components, you need to point Symantec Installation Manager to the Beta product listing.</p> <ol style="list-style-type: none"> 1 In Symantec Installation Manager, on the Install New Products page, click Cancel. 2 On the Installed Products page, click Settings. 3 In the Settings dialog box, click Change product listing.... 4 In the Manage Product Listings dialog box, click Add. 5 In the Add New Product Listing dialog box, paste the path to the product listing file: <code>itms_7_5.pl.xml</code>. 6 Click OK. 7 Now proceed to installing the new products on the Install New Products page. <p>Note: On the Installation Summary page, a message appears that asks whether you want to participate in the Symantec Product Improvement Program. This program is not enabled in the Beta version of IT Management Suite 7.5.</p>
Step 6	Configure Notification Server to use HTTPS	<p>You must configure Notification Server to use HTTPS if you want to set up Cloud-enabled management.</p> <p>In Symantec Installation Manager, on the Notification Server Configuration page, do the following:</p> <ol style="list-style-type: none"> 1 Check Require HTTPS to access the Management Platform. 2 In the Certificate drop-down list, click either your self-signed certificate or your domain certificate.
Step 7	Configure SQL	<p>On the Database Configuration page, configure the database to reside on the same server as Notification Server (on-box configuration).</p> <p>For beta and testing purposes, using the SQL Express database installed through Symantec Installation Manager is sufficient. This database automatically populates the SQL Server name field. All you have to do is provide the administrator credentials.</p>

Table 2-1 Process for installing the Symantec Management Platform products
(continued)

Step	Action	Description
Step 8	Apply licenses	<p>Apply licenses by going to Add/Update licenses and pointing to the license file that is included in the beta downloads.</p> <p>Beta licenses are also available directly from the Beta site, but in certain instances they may not install. In this case, you must first remove the existing licenses before you can replace them. To remove a pre-existing license:</p> <ol style="list-style-type: none"> 1 Run <code>C:\program Files\Altiris\Notification Server\Bin\Tools\RemoveLicense.exe</code> 2 Select the licenses that you want to remove and click Remove. 3 Load Symantec Installation Manager and select Add/Update licenses. 4 Click Install licenses. 5 Browse to the new license, select it, and then click Open. 6 Click Yes to install the license. 7 Click Close, and then click Restart Services.
Step 9	Install Deployment Solution point fix	<p>This point fix addresses the following issue with Deployment Solution: When the Initial Deployment Menu is not set , or the Initial Deployment menu is killed before the task starts, Task server does not get assigned to unknown computer.</p> <ol style="list-style-type: none"> 1 Extract the two files from the <code>PF_2858297_Install.zip</code> file to Notification Server (in any location). 2 Open the command prompt via "Run as administrator" and run <code>PF_2858297_Install.cmd</code>.
Step 10	Perform a Network Discovery	<p>Before you can manage computers, you must first discover the computers in your network. For more information, go to www.symantec.com/docs/DOC4730.</p>
Step 11	Roll out Symantec Management Agent	<p>Roll out the Symantec Management Agent to computers you want to manage. For more information, go to www.symantec.com/docs/DOC4730.</p>

Table 2-1 Process for installing the Symantec Management Platform products
(continued)

Step	Action	Description
Step 12	(Optional) Upgrade ITMS 7.1 SP2 Agents	<p>If you want to test the upgrade of certain ITSM 7.1 SP2 Symantec Management Agents you can do one of the following options.</p> <p>Warning: Upgrading agents should be done in your evaluation environment only. It is not recommended to upgrade production computers to the Beta version of the Symantec Management Agent.</p> <p>If you installed ITMS 7.5 Beta in SSL mode, do the following:</p> <ul style="list-style-type: none"> ■ Push the agents to the target computers. Make sure the option Install Server certificate to the client machine is selected. <p>If you installed ITMS 7.5 Beta in mixed mode, do the following:</p> <ul style="list-style-type: none"> ■ Redirect the targeted computers to point to the 7.5 Beta Notification Server computer. ■ Configure an agent upgrade policy to upgrade the target computers to version 7.5. ■ Deploy the certificates to the target computers. ■ Use the Target Agent Settings options to change the client computer connection method to SSL.

Preparing your environment for Cloud-enabled Management

To use Cloud-enabled Management (CEM), your environment must be configured to use SSL communications.

Make sure that you followed step 6 in the previous section to configure Notification Server for HTTPS access. When you roll out Symantec Management Agents from a Notification Server that uses HTTPS, the Symantec Management Agents also are automatically configured to use HTTPS.

Note: CEM agents and non-CEM agents can co-exist in the environment. However, non-CEM agents cannot communicate through to Notification Server when they are outside of the corporate network.

For more information about configuring your environment to use SSL, see the following knowledge base articles:

- <http://www.symantec.com/docs/DOC1240>

■ <http://www.symantec.com/docs/HOWTO53002>

Table 2-2 Process for preparing your environment for Cloud-enabled Management

Step	Action	Description
Step 1	Prepare your site server computers.	<p>On the computers where you plan to host site services, you must install site server certificate for CEM agent access. A server certificate is a prerequisite for any site server that serves Symantec Management Agents on the Internet. Cloud-enabled Management does not assign server certificates to site servers. You need to apply server certificates to site servers in order for them to be accessible using HTTPS.</p> <p>Note that on task server computers you must have IIS 6.0 or IIS 7.0 and .NET Framework 3.5 features enabled.</p> <p>To make sure that the agent on the site server can communicate with Notification Server using HTTPS, you must apply the root certificate authority to the site server computer.</p> <p>You can use your own certificate or Notification Server can generate a certificate for you.</p> <p>If you do not have your own corporate certificate authority, the Notification Server computer includes a tool to help you generate certificates. This tool is called <code>AeXgenSiteServerCert.exe</code>. <code>AeXgenSiteServerCert.exe</code> generates the certificates that are signed by the special Notification Server CA certificate for CEM-enabled clients. It lets you set up HTTPS certificates for your site servers.</p> <p>When you create the certificate, the certificate name must match the name of site server computer. You must use the fully qualified domain name.</p> <p><code>AeXgenSiteServerCert.exe</code> stores the certificate in the Program Files\Altiris\Notification Server\Bin\Tools folder.</p> <p>See “STEP 1: Prepare your site server computers” on page 23.</p>
Step 2	Roll out Site Services.	<p>After you prepare the site server computers, you can roll out the site services.</p> <p>Note: Running a Task Server on a Cloud-enabled, Internet-managed client computer is not supported and can lead to undesirable behavior.</p> <p>See “STEP 2: Roll out site services” on page 24.</p>

Table 2-2 Process for preparing your environment for Cloud-enabled Management (*continued*)

Step	Action	Description
Step 3	Configure package servers to publish HTTPS package codebases.	<p>You need to ensure that your Cloud-enabled agents or package servers can source packages from Notification Server or internal package servers. To allow them to download packages, both Notification Server and the internal package servers must publish HTTPS package codebases.</p> <p>See “STEP 3: Configure the package servers to publish HTTPS package codebases” on page 24.</p>
Step 4	Assign site servers to the Default Internet Site .	<p>CEM Agents that are behind the Internet gateway use Internet Sites for determining site services. In the Symantec Management Console, add your site servers to the predefined Default Internet Site or other Internet sites you want to use.</p> <p>Note: This step should be done after the Symantec Management Agent site is configured.</p> <p>See “STEP 4: Assign site servers to the Default Internet Site” on page 25.</p>
Step 5	Make sure that the Default Internet Site is properly configured.	<p>On the Default Internet Site page, make sure that the required site services are set up properly and the settings apply to the appropriate resource target.</p> <p>See “STEP 5: Make sure that the Default Internet Site is properly configured” on page 25.</p>

STEP 1: Prepare your site server computers

- 1 (Optional) If you are not using your own certificate, you can generate a site server certificate with the AexGenSiteServersCert.exe tool.

To generate a certificate for a remote site server, do the following:

- On the Notification Server computer, open the command prompt and go to the following location:

```
C:\Program Files\Altiris\Notification Server\Bin\Tools\
```

- Run the following command:

For Task Server: AexGenSiteServersCert.exe

```
hostname_of_your_remote_task_server -p password
```

For Package Server: AexGenSiteServersCert.exe

```
hostname_of_your_remote_package_server /p password
```

- 2 Copy the certificate file to the remote site server computer.
- 3 On the remote site server computer, open the **Internet Information Services (IIS) Manager** and go to the **Server Certificates** page.

- 4 In the right pane, click **Import** to import the certificate.
Browse for the certificate file and click **OK**.
- 5 In the **Internet Information Services (IIS) Manager**, in the left pane, expand **Sites** and then click **Default Web Site**.
- 6 In the right pane, click **Bindings...** and in the **Site Bindings** dialog box, add binding for the port 443, select the imported certificate for it, and then click **OK**.
- 7 In the **Internet Information Services (IIS) Manager**, restart **IIS**.

STEP 2: Roll out site services

- ◆ For more information about how to roll out site services, see the Symantec Management Platform User Guide at the following URL:

<http://www.symantec.com/docs/DOC4730>

STEP 3: Configure the package servers to publish HTTPS package codebases

- ◆ Do one of the following:

Configure HTTPS globally on all your package servers

Warning: If you configure all of your package servers for HTTPS, then there will not be any package servers available to service HTTP requests.

To Configure HTTPS globally on all your package servers, do the following:

- In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- In the left pane, expand **Site Management > Settings > Package Service** and then click **Package Service Settings**.
- On the **Package Service Settings** page, under **Global Package Service Settings**, click **Publish HTTPS codebase**.
- Click **Save changes**.

Configure individual package server to use HTTPS To configure individual package server to use HTTPS, create the following registry key and values on each package server computer that is located in the same site as Notification Server:

- **Registry location:**
HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Package Server
- **Key Type:** DWORD
- **Name:** EnableHTTPOverride
- **Value:** 1

This registry key overrides the HTTP codebase configuration on the package server and makes it publish HTTPS codebases instead.

If you want to deploy this registry key change to multiple package servers, you can create and then run a .REG file with the following syntax.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Altiris Agent\Package Server]

"EnableHttpsOverride"=dword:00000001
```

STEP 4: Assign site servers to the Default Internet Site

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Site Servers > *your_site_server_name***, and then click **Internet Sites**.
- 3 In the right pane, under **Detailed Information**, click **New**.
- 4 In the **Select a Internet site** dialog box, click **Default Internet Site**, and then click **OK**.

STEP 5: Make sure that the Default Internet Site is properly configured

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Site Server Settings**.
- 2 In the left pane, expand **Site Management > Internet Sites**, and then click **Default Internet Site**.
- 3 On the **Default Internet Site** page, make sure the following:
 Under **Site Services**, the Task Servers and package servers that you added in STEP 4 are displayed.

Setting up Cloud-enabled Management

Before you can take advantage of the functionality that Cloud-enabled Management offers, you must install and configure the Internet gateways. After that you should configure the Cloud-enabled Management policies and also set up the Symantec Management Agents so that they support the Cloud-enabled Management environment.

Table 2-3 Process for setting up Cloud-enabled Management

Step	Action	Description
Step 1	Configure the Agent Site Settings.	<p>A separate agent site on Notification Server is required for Cloud-enabled agents. This site contains only agent interfaces and does not provide access to any of the Symantec Management Console pages. It also performs additional certificate and resource access checks to enforce security measures for agents connecting from the Internet.</p> <p>You must configure the Internet gateway to allow access only to the agent site on Notification Server.</p> <p>See “STEP 1: Configure the Agent Site Settings” on page 27.</p>
Step 2	Prepare the Internet gateway computer.	<p>Before you install the Internet gateway, you need to prepare the host computer.</p> <p>The following examples help you decide how many Internet gateways you need in your environment:</p> <ul style="list-style-type: none">■ When you have 20000 clients on one Notification Server and 30% of them are Cloud-enabled, the best practice is to have two Internet gateways to ensure high availability. However, even one Internet gateway is able to easily handle this configuration.■ If you have 180000 clients split across two hierarchies with 70% of them Cloud-enabled, you need to have at least four Internet gateways: three to handle the node load and one for fault-tolerance. <p>See “STEP 2: Prepare the Internet gateway computer” on page 27.</p>
Step 3	Download and run the Internet gateway installation package.	<p>To install Internet gateway, you need to download and run the Internet gateway installation package from the Symantec Management Console.</p> <p>See “STEP 3: Download and run the SMP Internet gateway installation package” on page 28.</p>

Table 2-3 Process for setting up Cloud-enabled Management *(continued)*

Step	Action	Description
Step 4	Configure the Internet gateway using the Symantec Management Platform Internet Gateway Configuration wizard and the Symantec Management Platform Internet Gateway Manager .	<p>In the Symantec Management Platform Internet Gateway Configuration wizard, you specify the port for incoming connections, the SSL certificate information, and the user account.</p> <p>In Symantec Management Platform Internet Gateway Manager, you add your Notification Server and your site servers to the list of servers that can communicate with the Internet gateway.</p> <p>You also need to copy the Gateway Certificate Thumbprint that you need for configuring the Cloud-enabled Management Settings policy.</p> <p>See “STEP 4a: Configure the Internet gateway using the Symantec Management Platform Internet Gateway Configuration wizard” on page 29.</p> <p>See “STEP 4b: Configure the Internet gateway in Symantec Management Platform Internet Gateway Manager” on page 29.</p>
Step 5	Configure the Cloud-enabled Management Settings policy.	<p>The Cloud-enabled Management Settings policy lets you target the computers that you want to manage over the Internet. The policy also contains the list of Internet gateways that are available for the targeted client computers to use.</p> <p>See “STEP 5: Configure the Cloud-enabled Management Settings policy” on page 30.</p>

STEP 1: Configure the Agent Site Settings

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
- 2 In the left pane, expand the **Setup** folder, and then click **Agent Site Settings Setup**.
- 3 On the **Agent Site Settings Setup** page, do the following:
 - Check **Enable Agent site**.
 - Make sure that the **Agent site port** is **4726**.
 - In the **Certificate** drop-down list, click the certificate that you created for the **Default Web Site** during the installation of IT Management Suite.
- 4 Click **Save changes**.

STEP 2: Prepare the Internet gateway computer

- ◆ Use the following guidelines to prepare your Internet gateway computer:
 - For optimal scalability, Symantec recommends a hardware-based Internet gateway with at least 8GB of RAM, 40GB HDD, dual-core CPU, and two

1Gbit network adapters. Note that using a VM-based Internet gateway can lower its scalability by up to 40%.

- The Internet gateway computer must have the Windows 2008 R2 SP1 operating system with the .NET Framework 3.5.1 feature enabled.
- The gateway computer should be located in your organization's DMZ to ensure that it is protected from both the external and the internal networks.
- You need to configure the firewall on the gateway computer to allow incoming connections from the Internet only to the appropriate gateway ports. You also need to configure the firewall to allow outgoing connections only to specific servers on your internal network. If the gateway runs on a VMWare virtual machine, you should use the VMXNET3 network adapter.
- Symantec Management Platform does not need to manage the gateway computer. The Internet gateway is typically unmanaged. Before starting the install, you should verify that the gateway computer can access the Notification Server computer and any required site server computers. When you verify the connection, use the host names or the IP addresses that the Cloud-enabled agents attempt to connect to.

STEP 3: Download and run the SMP Internet gateway installation package

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand the **Settings > Notification Server > Cloud-enabled Management. > Setup** folder.
- 3 Click **Setup Cloud-enabled Management**.
- 4 On the **Setup Cloud-enabled Management** page, on the **SMP Internet Gateway Setup** tab, under **Install a new SMP Internet Gateway**, click **Download the SMP Internet Gateway installation package**.
- 5 If you are on the gateway computer, you can click **Run** to run the installer immediately.

If you want to save the package as a file to run later, or to run on a different computer, click **Save**. Specify the appropriate folder, and then click **OK**.
- 6 Navigate to the SMP Internet gateway installation package that you downloaded and double-click `SMP_Internet_Gateway.msi`.
- 7 In the **Open File - Security Warning** dialog box, click **Run**.
- 8 In the **Symantec Management Platform Internet Gateway Setup** dialog box, click **Next**.
- 9 Click **I accept the license agreement**, and then click **Next**.

- 10 Specify the path to the destination folder where you want to install the Internet gateway files, click **Next**, and then click **Next**.
- 11 Make sure that **Start configuration wizard** is checked and then click **Finish**.

STEP 4a: Configure the Internet gateway using the Symantec Management Platform Internet Gateway Configuration wizard

- 1 In the **Symantec Management Platform Internet Gateway Configuration** wizard, on the **IP Addresses and Ports** page, specify the appropriate IP address and ports, and then click **Next**.

By default, the port for incoming connections is 443. You should use the Internet gateway computers IP address. You can specify only one port number and only one specified IP address. If you choose to use all available IP addresses, the same port number is used for all IP addresses.

- 2 On the **SSL Certificate Information** page, specify the appropriate certificate information, and then click **Next**.

The Internet gateway must have an SSL certificate available so that Symantec Management Agents can communicate with it. The installation wizard generates a self-signed SSL certificate based on the information you provide.

- 3 On the **User Account** page, specify the appropriate user account information and then click **Next**.

For security reasons Symantec recommends running the SMP Internet gateway service as a dedicated user account. Use the **LocalService** account.

- 4 On the **Summary** page, review your setup, and then click **Finish**.

STEP 4b: Configure the Internet gateway in Symantec Management Platform Internet Gateway Manager

- 1 To open the **Symantec Management Platform Internet Gateway Manager**, click **Start > Programs > Symantec > Internet Gateway Manager**.

Note that after the **Symantec Management Platform Internet Gateway Configuration** wizard finishes, the **Symantec Management Platform Internet Gateway Manager** opens automatically.

- 2 To add your site servers and Notification Server to the list of servers that can communicate with the Internet gateway, do the following:
 - In the **Symantec Management Platform Internet Gateway Manager**, on the **Servers** tab, click **Add Server**.
 - In the **Add Server** dialog box, add a **Host Name**, and then click **OK**. When you add Notification Server, make sure that you enter the same SSL port as you did on the **Agent Site Settings** page in STEP 1. By default this port should be port 443.

- If the **Certificate Warning** dialog box appears, click **Ignore**.
 - In the **Restart Service?** dialog box, click **Yes**.
- 3 To copy the **Gateway Certificate Thumbprint** that you need for configuring the **Cloud-enabled Management Settings** policy in STEP 6, do the following:
- In the **Symantec Management Platform Internet Gateway Manager**, on the **General** tab, click **Copy To Clipboard**.

STEP 5: Configure the Cloud-enabled Management Settings policy

- 1 In the Symantec Management Console, on the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
- 2 In the left pane, expand **Policy** and then click **Cloud-enabled Management Settings**.
- 3 On the **Cloud-enabled Management Settings** page, configure the policy as follows:

Set up the list of Internet gateways that accept external agent traffic.

To add an Internet gateway, in the **Edit Gateway Server** dialog box, specify its parameters as follows:

- **Server**
The FQDN of the Internet gateway computer.
- **Port**
The port number that the Symantec Management Agent must use to connect to the Internet gateway. The default is port 443.
- **Thumbprint**
Paste the **Gateway Certificate Thumbprint** value that you copy on the Internet gateway computer, in the **Symantec Management Platform Internet Gateway Manager**, on the **General** tab.

Specify the target computers to which the policy applies.

A newly installed agent is automatically added to the resource target of the policy that was specified in the agent installation package. If necessary, you can remove the agent from the default policy and reassign it to another policy.

If you want to bring the existing Symantec Management Agents under Cloud-enabled Management, you need to add these computers to the policy. After the agent on a client computer receives the **Cloud-enabled Management Settings** policy, it connects to Notification Server and requests its unique client certificate. When the agent has received its certificate and without a direct connection with Notification Server, it attempts to connect through the available Internet gateways that were specified in the policy. After the agent has connected successfully, it switches from directly managed mode and becomes a Cloud-enabled agent.

Note: If you plan to use the installation package to install agents on disconnected computer, you must include those clients in the policy. If you do not do that, these clients gateway settings are deleted when they connect directly to the local network. The clients gateway settings are deleted because they are not automatically members of the **Cloud-enabled Management Settings** policy. You should therefore define the scope of clients before the roll out of the installation package.

4 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

5 Click **Save Changes**.

After the Symantec Management Agent receives the policy, it is ready to use Cloud-enabled Management feature. Until the client computer is connected to the internal network, the Cloud-enabled Management mode remains disabled. When you disconnect the client computer from the internal network, and the Symantec Management Agent is able to connect to Notification Server through an Internet gateway, the Cloud-enabled Management becomes active automatically.

You can check the status of the Cloud-enabled Management mode in the Symantec Management Agent of the client computer, on the **Symantec Management Agent Settings** tab, under **Network Status**.

Evaluating Beta use cases

This chapter includes the following topics:

- [Evaluating Beta use cases](#)
- [Setting up Cloud-enabled Management](#)
- [Installing Symantec Management Agent on a computer that never connects to LAN or VPN](#)
- [Running hardware and software inventory on remote computers without VPN](#)
- [Tracking usage of the managed software products](#)
- [Delivering software using a Quick Delivery task](#)
- [Pre-staging a software](#)
- [Delivering patches to remote computers and to local computers](#)
- [Running a job on a CEM-enabled system](#)
- [Disabling the Internet gateway](#)
- [Verifying Cloud-enabled Management reports](#)

Evaluating Beta use cases

The following use cases are the focus of this Beta release:

- [Setting up Cloud-enabled Management and configuring Internet gateways.](#)
- [Installing Symantec Management Agent on a computer that never connects to LAN or VPN.](#)
- [Running hardware and software inventory on remote computers without VPN.](#)
- [Metering software usage.](#)

- Delivering software using Quick Delivery task.
- Pre-staging a software.
- Delivering patches to remote computers and to local computers.
- Running a job on a CEM-enabled system.
- Disabling one of the Internet gateways.
- Verifying Cloud-enabled Management reports.

Setting up Cloud-enabled Management

As a test task, set up Cloud-enabled Management for your remote systems only. For fault-tolerance purposes, set up two Internet gateways.

Table 3-1 Process for setting up Cloud-enabled Management

Step	Action	Description
Step 1	Prepare your environment for Cloud-enabled Management.	You must set up the infrastructure and configure your servers and client computers to use SSL. See “Preparing your environment for Cloud-enabled Management” on page 21.
Step 2	Set up Cloud-enabled Management.	You must install and configure the Internet gateways, configure the Cloud-enabled Management policies, and set up the Symantec Management Agents to support the Cloud-enabled Management environment. See “Setting up Cloud-enabled Management” on page 26.

Installing Symantec Management Agent on a computer that never connects to LAN or VPN

As a test task, install Symantec Management Agent on a remote computer that never connects to LAN or VPN using the offline client package.

Table 3-2 Process for installing the Symantec Management Agent on a disconnected computer

Step	Action	Description
Step 1	Generate the Symantec Management Agent installation package.	Generate a Symantec Management Agent installation package from the Symantec Management Console.

Table 3-2 Process for installing the Symantec Management Agent on a disconnected computer (*continued*)

Step	Action	Description
Step 2	Run the agent installation package on a disconnected computer.	Run the agent installation package to install the Symantec Management Agent on the computer.

STEP 1: Generate the Symantec Management Agent installation package

- 1 In the Symantec Management Console, on the **Settings** menu, click **All Settings**.
- 2 In the left pane, expand **Settings > Notification Server > Cloud-enabled Management > Setup**, and then click **Setup Cloud-enabled Management**.
- 3 In the **Setup Cloud-enabled Management** page, on the **Symantec Agent Installation Configuration** tab, under **Install new Symantec Management Agents over the Internet**, click **Download Symantec Management Agent for Internet Installations**.
- 4 In the **Cloud-enabled Agent Installation Package** window, specify the appropriate package parameters.
In the **Package Encryption Password** field, the password must meet the following criteria:
 - A minimum of four characters.
 - A capital letter.
 - A lower-case letter.
 - A symbol character.
- 5 Click **Generate Agent Installation Package**.
The package generation may take a few minutes. When the package is ready, you are prompted to run or save the file.
- 6 In the **File Download** dialog box, click **Save**, and then specify the location to which to save the file.
- 7 When the package download is complete, click **Close**.
- 8 In the **Cloud-enabled Agent Installation Package** window, click **Close**.

STEP 2: Install the Symantec Management Agent on a disconnected computer

- 1

Place the Symantec Management Agent installation package on the appropriate disconnected computer.
- 2

Run the agent installation package on the disconnected computer.

The agent package is a self-extracting executable and the installation runs silently.
- 3

Verify that the installation was successful. You can use the Symantec Management Console to view the reports to check that the newly managed computer is present. You can view the report under **Reports > Notification Server Management > Certificates > CEM Installation Packages**.

If you specified an organizational group in the installation package, you can also check that the new computer has been added to the appropriate group.

Running hardware and software inventory on remote computers without VPN

As a test task, make sure that you receive hardware and software inventory from remote computers without VPN.

Note that the process in the table below gives you steps that you take in case you run hardware and software inventory using the **Collect Full Inventory** policy. If you want to collect inventory using other methods or want to collect inventory on your servers, please refer to the *Inventory Solution User Guide*, at the following URL:

<http://www.symantec.com/docs/DOC4729>

Table 3-3 Process for running hardware and software inventory on managed computers

Step	Action	Description
Step 1	Prepare managed computers for inventory.	Target computers must be managed and have the Inventory Plug-in installed. Use the Inventory Plug-in Install policy to install the Inventory Plug-in. By default, the policy is set to run as soon as possible and on any new computer without Inventory Plug-in.
Step 2	Use a predefined inventory policy to collect inventory.	The simplest way to collect hardware and software inventory is to use the predefined Collect Full Inventory policy. By default, the policy runs weekly, every Monday at 6:00 P.M. and applies to all computers with the Inventory Plug-in installed.

Table 3-3 Process for running hardware and software inventory on managed computers (*continued*)

Step	Action	Description
Step 3	View inventory results.	<p>You can view the gathered inventory data by viewing reports and data in the Resource Manager.</p> <p>To view inventory reports, in Symantec Management Console, in the left pane, under Reports, expand Discovery and Inventory > Inventory > Windows or Discovery and Inventory > Inventory > Cross-platform.</p> <p>To view inventory data in the enhanced Symantec Management Console Computers view, under All Computer Views, select the organizational view or group, and then in the central pane, click the computer whose reports you want to view.</p>

Tracking usage of the managed software products

As a test task track the usage of a specific software on at least two computers. Track its usage for a week and do not use the software on one of the computers.

Note that the process in the table below describes only the process of tracking the usage of the predefined software products that are installed with an MSI-based installer. If you want to track the usage of other types of software using other methods, please refer to the *Inventory Solution User Guide*, at the following URL:

<http://www.symantec.com/docs/DOC4729>

Table 3-4 Process for tracking usage of the managed software products

Step	Action	Description
Step 1	Prepare computers for metering.	<p>Target computers must be discovered, managed with the Symantec Management Agent, and have the Inventory Plug-in and the Application Metering Plug-in installed.</p> <p>Use the Application Metering Plug-in for Windows Install policy to install the Application Metering Plug-in. By default, the policy is set to run as soon as possible and on any new Windows computer without Application Metering Plug-in.</p>
Step 2	Gather software inventory.	<p>You can track usage of a software product only if the software product is installed and discovered in your environment.</p> <p>Use the predefined Collect Full Inventory policy to collect software inventory. By default, the policy runs weekly, every Monday at 6:00 P.M. and applies to all computers with the Inventory Plug-in installed.</p>

Table 3-4

Process for tracking usage of the managed software products
(continued)

Step	Action	Description
Step 3	Make sure that the software products that you want to track are ready for usage tracking.	<p>You can track usage of a software product only if the software product is managed and has at least one software component associated to it. Also at least one software component in the software product must have the association with one or more key program files.</p> <p>To help you manage major software products, Inventory Solution provides the list of predefined software products. If the software product that you want to track is in the list, the NS.Nightly schedule to associate Software component to software product task automatically associates the discovered software components with the relevant predefined software product and makes the software product managed. The predefined task runs automatically on the Notification Server computer every night at 12:30 A.M. To immediately get the results, you can run the task manually.</p> <p>To run the NS.Nightly schedule to associate Software component to software product task, do the following:</p> <ul style="list-style-type: none">■ On the Notification Server computer, in the taskbar, click Start > Administrative Tools > Task Scheduler.■ On the Task Scheduler page, in the left pane, click Task Scheduler Library.■ In the central pane, right-click the task NS.Nightly schedule to associate Software component to software product.{a48d3b11-5169-464b-9773-6c0f476e7748}, and then click Run. <p>To make the usage tracking process easy for you, Inventory Solution also automatically associates the key program files that are installed with an MSI-based installer with the software components of the software products.</p> <p>You can view the managed software products, their components, and the key program files that are associated with the software components.</p>
Step 4	Enable tracking usage of the managed software products on target computers.	In the Software Product dialog box, on the Meter / track usage tab, you need to check the Turn on metering / usage tracking for this software product option for the managed software that you want to track at the product level.

Table 3-4 Process for tracking usage of the managed software products
(continued)

Step	Action	Description
Step 5	View usage tracking results.	<p>You can view application summary data for the managed software product in the following application metering reports:</p> <ul style="list-style-type: none">■ Concurrent Usage■ Executable Usage■ Underutilized Software <p>You use the enhanced Symantec Management Console Software view to track the following usage events for the managed software products:</p> <ul style="list-style-type: none">■ The usage of the software product at the product or component and version level■ Last usage time

Delivering software using a Quick Delivery task

As a test task, rollout a software to a particular remote system. Use **Quick Delivery** task to accomplish this.

Note that the process in the table below describes only creating a Quick Delivery task using the **Quick Delivery** wizard. If you want to create a Quick Delivery task using other methods, please refer to the *Software Management Solution User Guide*, at the following URL:

<http://www.symantec.com/docs/DOC4661>

Table 3-5 Process for delivering software using a Quick Delivery task

Step	Action	Description
Step 1	Prepare computers for software delivery.	<p>To deliver and manage software, you must install Software Management Solution Plug-in on client computers.</p> <p>Use the Software Management Solution Plug-in Install policy to install the Software Management Solution Plug-in. By default, the policy is set to run as soon as possible and on any new computer without Software Management Solution Plug-in.</p>
Step 2	Create a Quick Delivery task.	The Quick Delivery wizard is the fastest and easiest way to create and run a Quick Delivery task with minimum configuration.
Step 3	After the task runs, view the reports.	You can access the Software Management reports, in the Symantec Management Console, on the Reports page, under Software > Delivery > Status .

Pre-staging a software

As a test task, pre-stage a software within your entire environment on Tuesday morning. The software should be automatically installed on Thursday at 9:00 A.M. However, users of remote systems should be able to trigger the installation of the pre-staged software on their own as well (before the Thursday deadline).

Note that the table below only describes the manual process of creating a Managed Software Delivery policy. If you want to create the Managed Software Delivery policy using other methods, please refer to the *Software Management Solution User Guide*, at the following URL:

<http://www.symantec.com/docs/DOC4661>

Table 3-6 Process for performing advanced software deliveries

Step	Action	Description
Step 1	Prepare computers for software delivery.	<p>To deliver and manage software, you must install Software Management Solution plug-in on client computers.</p> <p>Use the Software Management Solution Plug-in Install policy to install the Software Management Solution Plug-in. By default, the policy is set to run as soon as possible and on any new computer without Software Management Solution Plug-in.</p>

Table 3-6 Process for performing advanced software deliveries (*continued*)

Step	Action	Description
Step 2	Create a Managed Software Delivery policy.	<p>The Managed Software Delivery policy lets you perform one or more advanced software delivery actions.</p> <p>On the Managed Software Delivery policy page, specify the settings as follows:</p> <ul style="list-style-type: none"> ■ Expand Applied to section and click Apply to > Computers. In the Select Computers dialog box, click Add rule, and select All computers with installed Software Management Plug-in as the filter. ■ Expand Schedule section to define the delivery schedule. Under Compliance, add the compliance schedule to repeat daily starting 11:00 and ending at 17:00. Set the During window, check every option value to 3 hours. ■ Under User interaction, to allow remote systems to able to trigger the installation, ensure that you check Prompt user when this policy is available. ■ Under Remediation, to enforce installation at a fixed deadline, set a remediation schedule. To set a remediation schedule, check If the software is not found, install it, and choose Schedule from the drop-down menu. For example, if you want a deadline of Thursday, June 15th at 9:00 A.M., in the Advanced options dialog box, set the Start and End values to 6/15/2012. <p>Warning: Symantec recommends that you only set a remediation schedule when the software installation does not disturb the end user. For example, for a software installation that requires a restart it is better to use a maintenance window for out of office hours.</p>
Step 3	After the policy runs, view reports.	You can access the Software Management reports, in the Symantec Management Console, on the Reports page, under Software > Delivery .

Delivering patches to remote computers and to local computers

As a test task, rollout Patch bulletin to remote computers and local computers. Compare rollout success and Patch compliance.

Note that the process in the table below describes the simplest way of delivering patches. If you want to have more information about delivering patches, please refer to the *Patch Management Solution for Windows User Guide*, at the following URL:

<http://www.symantec.com/docs/DOC4814>

Table 3-7 Process for installing software updates

Step	Action	Description
Step 1	Prepare computers for patch management.	Use the Software Update Plug-in Install policy to install the Software Update Plug-in. By default, the policy is set to run as soon as possible and on any new computer without Software Update Plug-in.
Step 2	Download the Windows software updates metadata.	Download the Windows software updates metadata and configure metadata update schedule.
Step 3	Review and distribute available software updates.	View which software bulletins you need to install, then download updates and create software update policies. On the Select computers page, click Add rule and then configure a rule to exclude computers not in the All Computers where the Cloud-enabled Management feature is enabled filter.
Step 4	Evaluate the results.	You can access the software update delivery summary reports, in the Symantec Management Console, on the Reports page, under Software > Patch Management > Remediation Status .

Running a job on a CEM-enabled system

As a test task, start a job or a large delivery on a CEM-enabled system connected to LAN with a wired connection, go to standby, connect to WiFi (not on LAN), after some delay connect to VPN. Repeat the disconnect, connect to WiFi, connect to VPN sequence a few times.

Disabling the Internet gateway

As a test task, disable one of the Internet gateways and verify Symantec Management Agent behavior with one Internet gateway down.

Table 3-8 Process for disabling the Internet gateway

Step	Action	Description
Step 1	Stop Internet gateway service.	To stop the Internet gateway service, open the command prompt window on the Internet gateway server, and run the following script: <code>Apache\bin\StopService.cmd</code> Alternatively, you can also stop the service by clicking the Stop button in the Internet Gateway user interface.

Table 3-8 Process for disabling the Internet gateway (*continued*)

Step	Action	Description
Step 2	Verify the Symantec Management Agent behavior.	You can check the status of the Cloud-enabled Management mode in the Symantec Management Agent of the client computer, on the Symantec Management Agent Settings tab, under Network Status .

Verifying Cloud-enabled Management reports

As a test task, verify that you can get all need CEM-specific information from Cloud-enabled Management reports.

You can access the Cloud-enabled Management reports in the Symantec Management Console, on the **Reports** page, under **Notification Server Management > Agent > Cloud-enabled Management**.

Known issues in IT Management Suite 7.5 Beta

This chapter includes the following topics:

- [Known issues of the Symantec Management Platform](#)
- [Known issues of the Solutions](#)

Known issues of the Symantec Management Platform

The known issues of the Symantec Management Platform are separated into the following components:

- See [“General Known Issues”](#) on page 46.
- See [“Cloud-enabled Management”](#) on page 47.
- See [“Notification Server”](#) on page 48.
- See [“Task Server”](#) on page 49.
- See [“Package Server”](#) on page 50.
- See [“Known issues of the Solutions”](#) on page 50.

General Known Issues

Table 4-1 General Known Issues in the Beta

Issue	Description	Article ID
Beta licenses for solutions cannot override existing license.	<p>Under certain circumstances you may need to add a new license. A known issue exists where the new license is not applied properly.</p> <p>To work around this issue you must manually remove the old license before you install the new one.</p>	NA
Some documentation is missing from Help system.	<p>Some of the documentation is not properly installed into the Beta Help system.</p> <p>The following documentation is missing from the Help system:</p> <ul style="list-style-type: none">■ Asset Management Documentation■ CMDB Documentation■ Patch Management for Windows Documentation■ Patch Management for Linux Documentation■ Patch Management for Mac Documentation■ Inventory for Network Devices Documentation■ Inventory Solution Documentation■ Software Management Solution Documentation <p>To work around this issue, a pdf file for each of the missing documentation items is included in a ZIP file. You can access the ZIP file from the Beta site.</p>	NA

Cloud-enabled Management

Table 4-2 Known issues in Cloud-enabled Management

Issue	Description	Article link
In CEM environment, distributing certain software fails.	<p>In CEM environment, distributing certain software (like SQL Server 2008 R2, SQL Server 2012) is not possible because IIS configuration on the Notification Server computer hides some file and folder types preventing them to be downloaded or accessed via HTTP. For example, *.config files are hidden among many other file types.</p> <p>In LAN environment, this is not a problem because in this case the files are downloaded via UNC. However, in CEM environment, Symantec Agent is unable to use UNC paths, fails to download the software package, and therefore the installation of the software cannot be performed.</p> <p>Workaround: Repackage the software into a single self-extractable EXE or MSI file.</p>	N/A
The minimum Download Speed setting is working incorrectly on CEM-enabled clients.	<p>Measuring of the download speed is working incorrectly on Internet-based client computers that have Cloud-enabled Management enabled. In agent log you can see the following warnings:</p> <ul style="list-style-type: none"> ■ "Unable to select a server. This may be because all servers are excluded, have reported more than 20 errors recently, or are not responding to speed tests" ■ "Connection speed to server xxx of 1.00 KByte/s is lower than required for download 512.00 KByte/s or execution 0.00KByte/s" 	NA
The Cloud-enabled Management Client Task Agents are not working with Remote Task Servers if the Remote Task Server is configured in HTTP.	This issue is known to occur with HTTP settings only. To work around this problem, configure the Remote Task Servers in HTTPS.	N/A
When gathering full inventory in a CEM environment, you may see errors.	When gathering full inventory in a CEM environment, you may see the following error in Log Viewer: "Failed to process NSE "Failed to load inventory. Current user does not have required permission read to load item "Software Key Executable"".	NA

Notification Server

Table 4-3 Known issues in Notification Server

Issue	Description	Article link
The resources of child organizational units are not imported.	If you are using Internet Explorer 9 and you perform import of an Active Directory with nested structure and select only the parent organizational unit for import, the resources of child organizational units are not imported. This issue has not been reproduced on Internet Explorer 8.	N/A
Creating new site service can cause a time-out.	The Symantec Management Console times out during the creation of a new site service. This issue is known to occur with a large number of packages. For example, having greater than 2000 packages.	N/A
During replication, errors appear in the logs of child Notification Server.	During the replication, the following error may appear in the logs of child Notification Server: Unexpected error while attempting to proactively update replication hash cache Note that the error does not cause any functional problems and the replication still continues.	N/A
A resource item that contains a foreign key cannot be deleted through Symantec Management Console.	A resource item that contains a foreign key cannot be deleted and thus for example, any managed computer that has requested a policy once cannot be deleted through the Symantec Management Console.	N/A
Large number of warnings appear in logs during Software Discovery.	During Software Discovery, a large number of warnings (approximately 250 warnings per second) can appear in Notification Server logs. This issue is known to occur when running tasks frequently under heavy load. For example, running many software discovery tasks at a high frequency can create a large amount of data flow to the Notification Server computer.	N/A
Replicating local users that have identical user names both on parent Notification Server and its child server causes problems.	When you replicate local users with an identical user name from the parent Notification Server to a child server, the user data on the child Notification Server is overwritten by the data from parent Notification Server. The users of the child Notification Server cannot access the Symantec Management Console after the replication runs.	N/A
It is only possible to select parent-level organizational units for import.	If you are using Internet Explorer 9, and you perform an import of Active Directory with nested structure and you expand the parent-level organizational unit to also select the child-level organizational units, the infinite message Loading... is displayed instead of child organizational units. Therefore, you can only select parent-level organizational units for import. This issue has not been reproduced on Internet Explorer 8.	N/A

Table 4-3 Known issues in Notification Server (*continued*)

Issue	Description	Article link
Log Warning: "Resource save failed: Unable to update the specified item from the Altiris NS database".	If a very large number of new resources are reported to the Symantec Management Platform in a short period of time, deadlock warnings may appear in log. However; the resources are still properly created.	N/A
If there are two connected network adapters on a client CEM, then CEM Reports: IP address of only one adapter is shown in 'Package Certificate Request Status'.	If an offline installation package was used to install the Symantec Management Agent and the client computer has several network adapters with IP addresses assigned, then only one of if the IP Addresses is shown in the drill-down of the "Package Certificate Request Status" report. This report is where permanent certificate requests are approved.	N/A

Task Server

Table 4-4 Known issues in Task Server

Issue	Description	Article link
Errors are displayed during the installation of Symantec Management Platform.	<p>During the installation of Symantec Management Platform, the following error re-occurs in Notification Server log:</p> <pre>Failed to increment performance counter instance value - Task Server - HTTP Handlers, Http Handler Posts per Second. Exception Details: System.InvalidOperationException: Category does not exist. Source: Altiris.TaskManagement.Common.Performance. PerformanceMonitor.IncrementCounterInstance</pre>	N/A
A task that is deleted on Notification Server, still runs on a client computer.	After you delete a task on Notification Server, it still runs on a client computer. This problem occurs only on the client computers that are connected to the Internet and where the Cloud-enabled Management mode of the Symantec Management Agent is Active.	N/A
Errors appear after upgrading the plug-ins.	<p>After you upgrade Software Management plug-in, Patch Management plug-in, and Inventory plug-in from 7.1 SP2 to 7.5 on your client computers, many <code>CATrsException</code> exceptions appear in the Symantec Management Agent log.</p> <p>Note that these errors don't cause any functional problems.</p>	N/A

Table 4-4 Known issues in Task Server (continued)

Issue	Description	Article link
Symantec Management Agent stops responding in module <code>client task agent.dll</code> .	Symantec Management Agent stops responding in module <code>client task agent.dll</code> when evaluating a managed delivery policy that contains several task delivery items.	N/A
In Symantec Management Agent, in the Task History dialog box, the task execution history is not displayed.	On client computer, in Symantec Management Agent, the Task History dialog box does not display the task execution history of many tasks that have actually ran on this client computer.	N/A
The Allow the user to defer execution of this task option does not work properly.	When you create a task with the Allow the user to defer execution of this task option enabled, this task does not run at all in case the user is logged off.	N/A

Package Server

Table 4-5 Known issues in Package Server

Issue	Description	Article link
Processing Package Server Cubes fails.	In the Beta, processing Package Server Cubes fails. To work around this issue, exclude the cubes from the processing schedule.	NA

Known issues of the Solutions

- The known issues of the IT Management Suite solutions are separated into the following components:
- See “[Asset Management Solution and CMDB Solution](#)” on page 51.
 - See “[Deployment Solution](#)” on page 51.
 - See “[Monitor Solution for Servers](#)” on page 52.
 - See “[Patch Management Solution for Linux](#)” on page 53.
 - See “[pcAnywhere Solution](#)” on page 53.

Asset Management Solution and CMDB Solution

Table 4-6 Known issues in Asset Management Solution and CMDB Solution

Issue	Description	Article link
CMDB manager users are unable to delete the resources that they create.	CMDB manager users are unable to delete the resources that they create. The error log logs a warning message that the resource item cannot be deleted.	NA

Deployment Solution

Table 4-7 Known issues in Deployment Solution

Issue	Description	Article link
For unknown client computers, the default jobs that are configured through the Initial Deployment Settings menu does not execute after the client computers boot in the preboot environment as no Task Server is assigned to the client computers	To be able to perform initial deployment, the stored procedure has to be applied manually.	NA
Issue with MAC Address filtering on NBS settings page	When using MAC filtering on the NBS settings page, after adding the MAC addresses the user has to navigate away from the page. In case a session time-out occurs, all the MAC reservation will be lost and the page should be refreshed.	NA
CEM-enabled package servers do not store images.	In case of CEM-enabled environments, the non-CEM package server computer has to be manually removed from the filter of "All Computers meeting Cloud-enabled Management criteria" on the Cloud-enabled Management Settings page. A CEM-enabled package server is not used to store images or personality captures.	NA
Issue where the PXE service does not stop when using the dummy.0 file	In some cases if the dummy.0 file is present, the PXE service does not stop. In this case the PXEFixup is not called. In this case the PXE service needs to be stopped (or killed) forcefully.	NA

Table 4-7 Known issues in Deployment Solution (*continued*)

Issue	Description	Article link
Issue with partition information for HTTP servers.	Partition information is not displayed when the image is located on HTTP servers.	NA
SOI provisioned clients cannot be used for NBS	Clients that are provisioned via SOI cannot be used for NBS. In case it has to be used, the webconfig needs to be modified.	NA
Deployment Solution Hierarchy and Upgrade are not supported in the Beta program	Deployment Solution Hierarchy and Upgrade are not supported in the Beta program.	NA
Deployment Solution for Mac is not included in the Beta.	Deployment Solution for Mac is not included in the Beta.	NA

Monitor Solution for Servers

Table 4-8 Known issues in Monitor Solution for Servers

Issue	Description	Article link
Agentless monitor/Real-time Performance Viewer stops working after saving (editing) agentless monitor policy.	Agentless monitor/Real-time Performance Viewer stops working after saving (editing) agentless monitor policy. To work around this issue, you must restart the Altiris monitor agent service.	NA
Monitor Solution is not able to monitor agentless resource.	Monitor Solution is not able to monitor agentless resource. To work around this issue, you must restart the monitor service.	NA
An incorrect link is generated in the Monitoring and Alerting portal/Monitored agents for Event Console dialog box.	An Incorrect link is generated in the Monitoring and Alerting portal/Monitored agents for Event Console dialog box. When the link is clicked, the user gets events for all monitored resources, not for selected one.	NA

Patch Management Solution for Linux

Table 4-9 Known issues in Patch Management Solution for Linux

Issue	Description	Article link
Software update policy creation fails.	When you try to create a software update policy that contains 50-100 bulletins, you receive an Index was outside the bounds of the array error and policy creation fails.	N/A

pcAnywhere Solution

Table 4-10 Known issues in pcAnywhere Solution

Issue	Description	Article link
In the 7.5 Beta, you cannot provision the pcAnywhere plug-in.	In the 7.5 Beta, you cannot provision the pcAnywhere plug-in.	NA

