Cloud-enabled Management
Whitepaper for ITMS 8.1
Cloud-enabled Management Whitepaper

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

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

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, et seq. “Commercial Computer Software and Commercial Computer Software Documentation,” as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. 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.
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:

support.symantec.com

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:

support.symantec.com

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@symantec.com
Europe, Middle-East, and Africa  semea@symantec.com
North America and Latin America  supportsolutions@symantec.com
Introducing Cloud-enabled Management

This chapter includes the following topics:

- About Cloud-enabled Management
- Effects of Cloud-enabled Management on site server functionality
- Ways to configure package servers in a mixed environment

About Cloud-enabled Management

Cloud-enabled Management lets you manage client computers over the Internet even if they are outside of the corporate environment and cannot access the management servers directly. The managed computers do not need to use a VPN connection to your organization's network.

You can apply Cloud-enabled Management in the following scenarios:

- An organization with many employees traveling or working outside the office (outside the corporate intranet).
- A managed service provider (MSP) managing external companies.
- Highly distributed companies with many small offices or employees working from home.

When you implement Cloud-enabled Management, the Notification Server computer and site servers are not directly exposed to the Internet. Therefore, Symantec Management Agent communicates with the Notification Server computer and the site servers through an Internet gateway. Usually, two or more Internet gateways should be available to maintain reliable management of Cloud-enabled client computers and to provide failover options. Each Internet gateway can support routing to multiple independent Notification Servers.
To use cloud-enabled management, you must install an Internet gateway server. The Internet gateway works as a tunneling proxy. It ensures the privacy and safety of the data that is passed between an agent and a management server with HTTPS communications. The Internet gateway is located in a demilitarized zone (DMZ) between two firewalls. It accepts incoming connections from authorized client computers on the Internet and forwards them to the appropriate Notification Servers and site servers inside your network. The Internet gateway blocks any connection attempts by unauthorized client computers.

The Symantec Management Agent automatically determines whether routing the communication through the Internet gateway is needed or not. If a Cloud-enabled computer has direct access to the local network using VPN, the agent automatically switches to a direct communication with Notification Server. If a Cloud-enabled computer is outside the corporate network, the agent routes all communication on the Internet to Notification Server through the Internet gateway.

**Note:** Cloud-enabled Management is supported on Microsoft Windows computers and Mac OS X computers.

Not all solutions in IT Management Suite support Cloud-enabled Management. For more information on Cloud-enabled Management support for a particular solution, refer to the solution documentation.

To use the Cloud-enabled Management feature, you do the following:

- Set up the infrastructure and configure your servers and client computers to use SSL.
  See “Preparing your environment for Cloud-enabled Management” on page 14.
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 20.

(Optional) Perform troubleshooting and maintenance tasks. See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.

Effects of Cloud-enabled Management on site server functionality

Cloud-enabled Management has the following effects on package server and task server functionality:

Table 1-1 Effects of Cloud-enabled Management on site server functionality

<table>
<thead>
<tr>
<th>Effect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package servers on the internal network deliver packages to Cloud-enabled agents and Cloud-enabled package servers using HTTPS only.</td>
<td>However, the internal network package servers can still distribute packages to internal network clients using UNC or HTTP. Similarly, Cloud-enabled package servers in the local site can deliver packages to Cloud-enabled clients in the same local site using any protocol.</td>
</tr>
<tr>
<td>The server selection process on Cloud-enabled agents and package servers changes.</td>
<td>The server selection process for Cloud-enabled agents and package servers is as follows:</td>
</tr>
<tr>
<td>1 For cloud-enabled clients in the internal network, local package servers are used. Package servers are selected according to connection speed and the lowest number of connection errors.</td>
<td></td>
</tr>
<tr>
<td>2 For cloud-enabled clients outside the internal network, Internet site assigned or same site package servers are selected according to connection speed and the lowest number of connection errors.</td>
<td></td>
</tr>
<tr>
<td>3 When two package servers return the same number of errors, they are sorted randomly.</td>
<td></td>
</tr>
<tr>
<td>Additional activities are required when you delete a package server.</td>
<td>If you delete a package server from a computer that is added to the Internet gateway, for security reasons you must also delete the package server from the Internet gateway.</td>
</tr>
</tbody>
</table>
### Table 1-1  
Effects of Cloud-enabled Management on site server functionality  
*(continued)*

<table>
<thead>
<tr>
<th>Effect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A remote task server cannot be installed on a client computer with</td>
<td>However, the <strong>Cloud-enabled Management Settings</strong> policy can be applied to the client computer after the task server is installed. <strong>Note:</strong> Symantec does not recommend you to apply the <strong>Cloud-enabled Management Settings</strong> policy to a task server.</td>
</tr>
<tr>
<td>a Cloud-enabled Management Settings policy already applied to it.</td>
<td></td>
</tr>
<tr>
<td>Task servers cannot provide real-time notifications or real-time task</td>
<td>Periodic polling is the supported mode for running tasks on Cloud-enabled clients. By default the Symantec Management Agent checks for tasks every 30 minutes. You can change this setting for Cloud-enabled agents by modifying the <strong>Task Update</strong> setting in the <strong>Task Agent Settings</strong> policy. You find this policy page in the Symantec Management Console, under <strong>Settings &gt; Notification Server &gt; Task Settings</strong>.</td>
</tr>
<tr>
<td>delivery.</td>
<td></td>
</tr>
<tr>
<td>The speed test for task servers is replaced with random sorting.</td>
<td>The Client Task Agent randomizes the list of task servers in situations where the speed test-based ordering would otherwise be used. Note that the agent ignores the speed test only when it is in Cloud-enabled mode.</td>
</tr>
</tbody>
</table>
| By default, task servers work with both cloud-enabled and local agents.| Task servers that are assigned to Internet site work with agents located in the intranet and those which are Cloud-enabled.  
To force Cloud-enabled agents to communicate with selected task server, manually assign those agents to a given task server. |

#### Ways to configure package servers in a mixed environment

IT Management Suite supports a mixed environment where some site servers are internal and some site servers are Internet site servers. In a mixed environment, the Symantec Management Agent first tries to use the internal package servers. If no internal package servers are available, the agent reverts to using the Internet package servers that are behind the gateway.
Table 1-2: Ways to configure package servers in a mixed environment

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign at least one package server to each Internet Site.</td>
<td>The Internet package servers must be able to publish HTTPS codebases. At least one Unconstrained package server needs to be assigned to each Internet Site. Other package servers on site can be configured as Constrained. This means that those cannot download packages directly from Notification Server.</td>
</tr>
</tbody>
</table>

This configuration of package servers works in the following way:

1. The unconstrained package server downloads the packages from Notification Server or from another package server outside the site.
2. The packages are distributed from the unconstrained package server to constrained package servers.
3. The packages are distributed to client computers.

Note: For load balancing and failover options, Symantec recommends that you configure at least two unconstrained package servers in each site.
Preparing your environment for Cloud-enabled Management

This chapter includes the following topics:

- Preparing your environment for Cloud-enabled Management

Preparation your environment for Cloud-enabled Management

Configuring your environment to use SSL is a prerequisite for setting up Cloud-enabled Management (CEM). After you configure your environment to use SSL, you can set up Cloud-enabled Management.

See “Setting up Cloud-enabled Management” on page 20.
### Table 2-1  Process for preparing your environment for Cloud-enabled Management

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Configure your Notification Server computer and Symantec Management Agents to use HTTPS. | Make sure that your Notification Servers are configured for HTTPS access.  
Note that Notification Server is automatically configured to use HTTPS if you check **Require HTTPS to access the Management Platform** on the **Notification Server Configuration** page, in Symantec Installation Manager, during the installation of IT Management Suite.  
If the Notification Server computer allows both HTTP and HTTPS connection, the Symantec Management Agents are automatically configured to use HTTPS when they receive the **Cloud-enabled Management Settings** policy. |
| Step 2 | Configure site servers to use HTTPS.                                    | To serve Cloud-enabled agents, the site servers have to be configured to use HTTPS. This process is automated by the **Global Site Server Settings**. When a new site server is assigned to an Internet site, the CEM certificate is distributed and HTTPS binding is created on the port that is given in the settings.  
See “Configuring global site server settings” on page 15.  
You can also distribute a CEM certificate with individual installation settings to each site server separately.  
See “Distributing a certificate with individual installation settings to a site server” on page 18. |

### Configuring global site server settings

The **Global Site Server Settings** page lets you configure the security settings and distribute the intranet certificates and the CEM certificates.  
Note that you can also distribute the certificates with individual installation settings to each site server separately.  
See “Distributing a certificate with individual installation settings to a site server” on page 18.  
The **Certificates Rollout** settings are processed in different ways, depending on the settings and site server IIS configuration.
### Table 2-2  
**Processing of Certificates Rollout** settings

<table>
<thead>
<tr>
<th>Port of the existing HTTPS binding on the site server</th>
<th>Force overwrite HTTPS binding</th>
<th>Processing</th>
</tr>
</thead>
</table>
| Does not equal to the port that you specify under Certificates Rollout. | Disabled | A new SSL certificate is delivered and used to create a new SSL port binding. The action is automated.  
**Note:** Symantec recommends using this configuration for new site servers. |
| Equals to the port that you specify under Certificates Rollout. | Disabled | A new SSL certificate is delivered, but no binding is created.  
In this case, the Cloud-enabled client computers cannot communicate with the site server that is located in the Notification Server internal network.  
**Note:** Symantec recommends using this configuration for the site servers that are already using HTTPS. |
| Does not equal to the port that you specify under Certificates Rollout. | Enabled | A new SSL certificate is delivered and used to create a new SSL port binding. |
| Equals to the port that you specify under Certificates Rollout. | Enabled | A new SSL certificate is delivered and used to create a new SSL port binding.  
**Warning:** The existing SSL port binding is overwritten.  
In this case, the client computers that have been using this port in HTTPS mode to communicate with the site server cannot connect anymore. |

This task is a step in the process for preparing your environment for Cloud-enabled Management.

See “Preparing your environment for Cloud-enabled Management” on page 14.
To configure global site server settings

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, and then click Global Site Server Settings.

3. On the Global Site Server Settings page, configure the following settings:

   Security Settings  Lets you create the Agent Connectivity Credential (ACC) on the site servers, provided the ACC is not a domain account. During this procedure, you can re-enable the created local account if it has been locked out and create the ACC even if the site server is also a domain controller.
Certificates Rollout

Let you distribute the intranet certificate and the CEM certificate to the site servers.

The intranet certificate is delivered to all site servers.

The CEM certificate is delivered to the site servers that are assigned to the Internet sites. The CEM certificate is required on the site servers that serve the Cloud-enabled client computers.

Specify the following settings for one or both of the certificates:

- **Install intranet certificate and Install CEM certificate** - controls if the Web server HTTPS binding is created, and if the certificate is installed.
- **Port** - port at the Web server where the HTTPS binding is created.
- **Force overwrite HTTPS binding** - controls if the existing certificate on the specified port is replaced if the HTTPS binding already exists on that port at the Web server.
- **Master certificate** - for the intranet certificate, you can select the master certificate that is used to sign the certificate that is installed at the Web server.

The Table 2-2 table explains how the Certificates Rollout settings are processed in different cases.

**Note:** To roll out the CEM certificates to the site servers with version 7.6 and lower, use the Legacy Cloud-enabled Management Site Server Settings policy at Cloud-enabled Management > Policy.

4 Click **Save changes**.

Distributing a certificate with individual installation settings to a site server

By default, the Global Site Server Settings policy distributes the intranet certificate and the CEM certificate globally to the site servers.

However, you can also distribute the certificates with individual installation settings to each site server separately. The custom settings override the global settings.

This task is an optional step in the process for preparing your environment for Cloud-enabled Management.

See “Preparing your environment for Cloud-enabled Management” on page 14.
To distribute a certificate with individual installation settings to a site server

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**, expand the site server to which you want to apply the certificate with individual installation settings, and then click **Certificates Rollout**.

3. In the right pane, under **Certificates Rollout**, click **Override the global settings by custom settings**.

4. In the **Custom certificate rollout settings** dialog box, edit the necessary settings.

   Note that the **Certificates Rollout** settings are processed in different ways, depending on the settings and site server IIS configuration. For more information, see the following topic:

   See “Configuring global site server settings” on page 15.

5. Enable the settings.

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

6. Click **Save changes**.

See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.
Setting up Cloud-enabled Management

This chapter includes the following topics:

- Setting up Cloud-enabled Management

Setting up Cloud-enabled Management

Before using Cloud-enabled Management, you must install and configure the Internet gateways. After that you must configure the Cloud-enabled Management policies and set up the Symantec Management Agents to support the Cloud-enabled Management environment.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure the <strong>Cloud-enabled Management Agent IIS Website Settings</strong>.</td>
<td>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. You must configure the Internet gateway to allow access only to Cloud-enabled agent site on Notification Server. See “Configuring the Cloud-enabled Management Agent IIS Website Settings” on page 23.</td>
</tr>
</tbody>
</table>
### Table 3-1 Process for setting up Cloud-enabled Management (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Prepare the Internet gateway computer.</td>
<td>The Internet gateway computer should be located in your organization's demilitarized zone (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 port. After the configuration, the port opens automatically. 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 VMXNET 3 network adapter. Note that VMXNET 3 is available only when you have VMware Tools installed on your virtual machine. For more information about the VMXNET 3 network adapter, see the following VMware Knowledge Base article: KB1001805. The computer must have the Windows Server 2008 R2 SP1 or Windows Server 2012 R2 operating system with the .NET Framework 4.5.1 feature enabled. Symantec Management Platform does not need to manage the gateway computer. The Internet gateway is typically unmanaged. Before starting the installation, 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, the FQDN, or the IP addresses that the Cloud-enabled agents attempt to connect to. See “About preparing the Internet gateway computer” on page 24.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Download and run the Internet gateway installation package.</td>
<td>To install the Internet gateway, you need to download and run the Internet gateway installation package from the Symantec Management Console. See “Downloading and running the Internet gateway installation package” on page 26.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **Step 4** | Configure the Internet gateway using the **Symantec Management Platform Internet Gateway Configuration** wizard and the **Symantec Management Platform Internet Gateway Manager**. | In the **Symantec Management Platform Internet Gateway Configuration** wizard, you specify the port for incoming connections, the SSL certificate information, and the user account.  
In **Symantec Management Platform Internet Gateway Manager**, add your Notification Server and your site servers to the list of servers that can communicate with the Internet gateway.  
You also need to copy the **Gateway Certificate Thumbprint** that you use for configuring the **Cloud-enabled Management Settings** policy. Note that if you enable the Internet gateway reporting, the thumbprint is automatically sent to **Cloud-enabled Management Settings** policy.  
See “Configuring the Internet gateway” on page 27. |
| **Step 5** | Enable the Internet gateway status reporting. | When Internet gateway reporting is turned on, the status information is sent cyclically to Notification Server.  
See “Enabling the Internet gateway status reporting” on page 29. |
| **Step 6** | Assign site servers to Internet sites. | The Cloud-enabled agents that are behind the Internet gateway use Internet sites for determining the site services.  
In the Symantec Management Console, you must add your site servers to a predefined **Default Internet Site** or other Internet sites that you create.  
See “Configuring sites and site servers to serve Cloud-enabled agents” on page 30. |
| **Step 7** | Make sure that the Internet site is properly configured. | On the Internet site page, make sure that the required site services are set up properly and that the settings apply to the appropriate resource target.  
You can access the Internet site page in the Symantec Management Console, on the **Site Server Settings** page, under **Site Management > Internet Sites**. |
| **Step 8** | Configure the **Cloud-enabled Management Settings** policy. | 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.  
See “Configuring the Cloud-enabled Management Settings policy” on page 32. |
### Table 3-1 Process for setting up Cloud-enabled Management (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Install the Symantec Management Agent on the computers that cannot directly connect to the internal network.</td>
</tr>
</tbody>
</table>

In some cases a computer that you want to manage may not have direct access to the network that hosts the Symantec Management Platform. To install the Symantec Management Agent on a computer that is located outside of the internal network, you must download the agent installation package from your Symantec Management Console, save it to suitable media, and then install it on the appropriate computers.

See “Generating and installing the Cloud-enabled Management offline package” on page 35.

### Configuring the Cloud-enabled Management Agent IIS Website Settings

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.

The Cloud-enabled Management Agent IIS site requires a connection that is secured with an SSL certificate. You can either import a commercial certificate or you can create a self-signed certificate.

See “Requirements and usage of third-party commercial certificates” on page 56.

This task is a step in the process for setting up Cloud-enabled Management.

See “Setting up Cloud-enabled Management” on page 20.

To configure the Cloud-enabled Management Agent IIS Website 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 **Cloud-enabled Management Agent IIS Website Settings**.
On the **Cloud-enabled Management Agent IIS Website Settings** page, check **Add IIS Website for cloud-enabled management agent connections**, and specify the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Lets you specify the name under which the website is displayed in the Internet Information Services (IIS) Manager.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Lets you specify the port on which the website will be available. To set up Cloud-enabled Management, it is required that the selected port is reachable by the Internet gateway computer.</td>
</tr>
<tr>
<td><strong>FQDN</strong></td>
<td>Lets you see the actual FQDN of the Notification Server computer. You can specify an alternate FQDN here. This FQDN is placed in certificate along with all other FQDN-s that are detected for Notification Server.</td>
</tr>
<tr>
<td><strong>Certificate</strong></td>
<td>Lets you import a commercial certificate or create a self-signed SSL certificate.</td>
</tr>
</tbody>
</table>

**Note:** **Name** and **FQDN** cannot be changed after the **Cloud-enabled Management Agent IIS Website** is created.

Click **Save changes**.

**Note:** A package refresh task is part of the website creation process. In environments with large number of tasks it can take considerable amount of time. You can safely close Symantec Management Console once the following messages are logged:

- Agent site creation task \{Task_Guid\} started.
- Starting Package Refresh for all the packages.

---

**About preparing the Internet gateway computer**

The Internet gateway lets Symantec Management Agents on the Internet communicate with the Symantec Management Platform. The Internet gateway forwards requests from authenticated Symantec Management Agents to specific port numbers on Notification Server instances or site servers behind the gateway.
By default, all requests are forwarded from the default HTTPS port 443 on the gateway to port 4726 on the Notification Server computer.

The Internet gateway creates a virtual tunnel through the internal firewall. It lets the authorized client computers on the Internet access the appropriate internal servers, but it keeps out all unauthorized client computers. The Cloud-enabled Symantec Management Agent communicates with the Internet gateway directly, through the Internet. No VPN is required. When a Cloud-enabled agent connects to it, the gateway and the agent exchange and verify each other’s certificates. The gateway checks that the certificate was issued by a known Notification Server. The gateway then creates a tunnel that the agent can use to communicate directly to the appropriate Notification Server and site servers using HTTPS. When the agent has finished communicating with the target server, the tunnel connection is closed.

The Cloud-enabled Management feature does not support the use of proxy servers. You cannot set up a proxy between a Cloud-enabled Symantec Management Agent and the Internet gateway.

Symantec recommends that you configure at least two Internet gateways to provide failover options, load balancing, and to maintain communication continuity. Each Internet gateway can serve multiple Notification Servers. This configuration is supported even if Notification Servers are organized in a hierarchy. Each Internet gateway supports 1-35,000 endpoints and 3,000 concurrent connections.

The following examples help you decide how many Internet gateways you need in your environment:

- When you have 20,000 client computers 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 can easily handle this configuration.

- If you have 180,000 client computers split across 2 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.

Before you install the Internet gateway, you need to configure the host computer. The gateway computer should be located in your organization's demilitarized zone (DMZ) to ensure that it is protected from both the external and the internal networks. You need to configure the firewall on the Internet 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 VMXNET 3 network adapter. Note that VMXNET 3 is available only when you have VMware Tools installed on your virtual machine. For more information about the VMXNET 3 network adapter, see the following VMware Knowledge Base article: KB1001805.
Note: The Internet gateway computer must have the Windows Server 2008 R2 SP1 or Windows Server 2012 R2 operating system with the .NET Framework 4.5.1 feature enabled.

Symantec Management Platform does not need to manage the gateway computer. The Internet gateway is typically unmanaged.

Before you begin installation, verify that the Internet 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.

This task is a step in the process for setting up Cloud-enabled Management. See “Setting up Cloud-enabled Management” on page 20.

Downloading and running the Internet gateway installation package

If you want to install or upgrade an Internet gateway, you first need to obtain the appropriate Internet gateway installation package. The installation package is an .EXE file that you can download from the Symantec Management Console. The package contains an installation wizard that guides you through the installation process.

Note: The installation package is also used to upgrade the Internet gateway.

If you can access the Symantec Management Console remotely from the Internet gateway computer, you can choose to run the Internet gateway installation package directly. Alternatively, you can save the file on any other media, copy it to the appropriate Internet gateway computer, and then run it.

Warning: Exit all Windows programs before you run the Internet gateway installation package.

This task is a step in the process for setting up Cloud-enabled Management. See “Setting up Cloud-enabled Management” on page 20.

To download and run the Internet gateway installation package

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Cloud-enabled Management.

2. In the left pane, expand Setup, and then click Cloud-enabled Management Setup.
3 On the **Cloud-enabled Management Setup** page, on the **Internet Gateway Setup** tab, click **Download the Internet gateway installation package**.

4 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**.

5 Navigate to the SMP Internet gateway installation package that you downloaded, and double-click **SMP_Internet_Gateway**.

6 In the **Open File - Security Warning** dialog box, click **Run**.

7 In the **Symantec Management Platform Internet Gateway Setup** dialog box, click **Next**.

8 Click **I accept the licence agreement**, and then click **Next**.

9 Specify the path to the destination folder where you want to install the Internet gateway files, click **Next**, and then click **Next**.

10 Make sure that **Start configuration wizard** box is checked, and then click **Finish**.

### Configuring the Internet gateway

After the Internet gateway is successfully installed, you must configure it to work together with the Symantec Management Platform. You configure the Internet gateway using the **Symantec Management Platform Internet Gateway Configuration** wizard and the **Symantec Management Platform Internet Gateway Manager**.

In the **Symantec Management Platform Internet Gateway Configuration** wizard, you specify the port for incoming connections, the SSL certificate information, and the user account.

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. You also obtain the **Gateway Certificate Thumbprint** that you need for configuring the **Cloud-enabled Management Settings** policy.

This task is a step in the process for setting up Cloud-enabled Management.

See “**Setting up Cloud-enabled Management**” on page 20.
To configure the Internet gateway using the Symantec Management Platform Internet Gateway Configuration wizard

1. On the Internet gateway computer, 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. However, you can specify a different port number if necessary. All of the specified port numbers must be TCP ports (these are numbered 1-65535).

   You should use the IP address of the Internet gateway computer. You can specify only one port number and only one IP address. If you choose to use all available IP addresses, the same port number is used for all IP addresses. If you require more granular control of IP addresses and port numbers, you need to edit the Apache configuration file directly.

2. On the *SSL FIPS* page, check the *Enable FIPS mode* box if you want to enable FIPS mode on your Internet gateway, and then click *Next*.

3. 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 configuration wizard generates a self-signed SSL certificate based on the information that you provide.

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

   Normally, you can use the *LocalService* account to set up the Internet gateway service. However, you can also use a dedicated user account if it is required for security reasons.

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

To configure the Internet gateway in the 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 Servers 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 edit the SSL Port number if necessary. If you add a Notification Server, make sure that This is a SMP server box is checked. Click OK.

Note that the SSL Port of the Notification Server computer must be the same as the one that you specify on the CEM Agent Site Settings page, in the Symantec Management Console.

If the Certificate Warning dialog box appears, click Ignore.

If the Restart Service? dialog box appears, click Yes.

To copy the Gateway Certificate Thumbprint that you need for configuring the Cloud-enabled Management Settings policy in the Symantec Management Console, click Copy To Clipboard on the General tab of the Symantec Management Platform Internet Gateway Manager.

See “Configuring the Cloud-enabled Management Settings policy” on page 32.

Enabling the Internet gateway status reporting

Internet gateway provides a reporting capability. When Internet gateway reporting is turned on, the status information is sent cyclically to Notification Server. You can adjust the reporting interval, where the lowest value is 15, and the highest is 1440 minutes.

This task is a step in the process of setting up Cloud-enabled Management.

See “Setting up Cloud-enabled Management” on page 20.

To enable Internet gateway status reporting

1 On the Internet gateway computer, start the Symantec Management Platform Internet Gateway Manager.

2 In the Symantec Management Platform Internet Gateway Manager, on the Servers tab, under Notification Server that you want the Internet gateway to report the status to, click Enable.

3 In the Enter credentials dialog box, provide the administrator credentials that are used to access Notification Server, and then click OK.

If the status reporting is enabled, on the Servers tab, a green square is displayed.
4  (Optional) In the **Symantec Management Platform Internet Gateway Manager**, on the **Settings** tab, under **Status Report**, click **Change** to change the **Report interval**.

5  (Optional) In the **Status Report Settings** dialog box, type the interval value in minutes, and then click **OK**.

You can use any integer value between 15 and 1440.

To view the reports that are generated from Internet gateway status reporting, in the Symantec Management Console, on the **Reports** menu, click **Reports > Notification Server Management > Cloud-enabled Management > Gateway**.

See “Viewing Cloud-enabled Management reports” on page 50.

### Configuring sites and site servers to serve Cloud-enabled agents

The computers that you want to manage over the Internet should be organized into one or more sites. These sites should be dedicated to Cloud-enabled agents and must not contain any directly managed agents. Note that the Symantec Management Platform provides you with a predefined **Default Internet Site** with the **All Computers where the Cloud-enabled management feature is enabled** target. You should then assign the appropriate site servers to the predefined site or to the sites that you create.

---

**Note:** Each internet site must have at least one site server assigned to it.

Cloud-enabled Management supports Internet package servers and Internet task servers, which the Symantec Management Agent accesses through an Internet gateway. Cloud-enabled Management also supports Cloud-enabled package servers, which are the package servers located in the same site as the Cloud-enabled agents. Only the local agents can access a Cloud-enabled package server, and they use a direct connection. However, Cloud-enabled task servers are not supported.

Cloud-enabled computers must be manually assigned to sites that are based on resource targets. Cloud-enabled agents do not recognize site assignments based on IP addresses and subnets. Manual assignment ensures that each computer remains a member of the appropriate site regardless of where the computer is physically located.

You can manually assign a Cloud-enabled agent to multiple sites or site servers. The site servers that are available to the agent are a union of all the site servers in the assigned sites.
You can configure your site server settings for Cloud-enabled agents in the following ways:

Create and configure new sites. You can create and configure as many sites as required to suit your environment setup. A Cloud-enabled agent or package server that is assigned to multiple sites receives the union of all the site servers in the assigned sites.

Assign the Cloud-enabled agents directly to the site servers. You can assign a resource target directly to the site server to ensure that the target members are given access to that particular site server only. The assignment by site method makes all of the site servers that are members of the assigned site available to the targeted Cloud-enabled agents.

See “Preparing your environment for Cloud-enabled Management” on page 14.

To configure an Internet site to serve the Cloud-enabled agents

1 (Optional) In the Symantec Management Console, create a new site and assign the appropriate resource target to the site.

   This resource target contains the Cloud-enabled agents and package servers. You can reuse the same resource target that is applied to the Cloud-enabled Management Settings policy.

2 Assign the appropriate site servers to the site in one of the following ways:

   To manually assign the site server to the 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 the Internet site to which you want to assign the site server, and then click OK.
To assign the subnet(s) of the local site servers to the site

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Site Server Settings.
2. In the left pane, click Site Management > Subnets.
3. In the right pane, select the appropriate subnet.
4. On the toolbar, click Assign to site.
5. In the Select a site window, select the site to which you want to assign the subnet.

**Note:** A local site server is the one that exists in the same disconnected site as the Cloud-enabled agents that it serves.

This type of assignment requires the disconnected site to have a unique subnet that does not overlap with subnets of internal client computers, if any. This configuration is not common, so this approach is not generally recommended.

To directly assign Cloud-enabled agents to a site server

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Site Server Settings.
2. In the left pane, expand the site server that you want to modify, and then click Manually Assigned Agents.
3. In the right pane, click New, specify the resource target that contains the appropriate Cloud-enabled agents, and then click OK.

**Configuring the Cloud-enabled Management Settings policy**

The **Cloud-enabled Management Settings** policy lets you target the computers that you want to manage over the Internet. The policy contains the list of Internet gateways that are available for the targeted client computers. To specify the available Internet gateways, enter the appropriate details of each gateway.

Normally, you need to configure only one **Cloud-enabled Management Settings** policy. You need multiple policies only if you want to have finer grained control over which Internet gateways serve which Cloud-enabled computers or if you want to perform manual load-balancing.

To generate an agent installation package, you need to create or select a **Cloud-enabled Management Settings** policy and apply it to the appropriate target...
computers. The list of available Internet gateways for the selected policy is included in the agent installation package. This list allows the newly installed agent to start communicating with Notification Server immediately. The new Cloud-enabled computer is automatically added to the resource target of the selected policy.

Note that a Cloud-enabled computer automatically reverts to direct communication with the local Notification Server when direct network access is available. It also automatically changes back to Cloud-enabled mode when the direct connection is no longer available. For example, a laptop computer that is normally used at remote locations may be used occasionally in the office and connected to the internal network.

While the Cloud-enabled Management Settings policy targets a computer, the computer continues to communicate using the appropriate Internet gateways. If the internal network is properly configured, all traffic between the agent, the Internet gateway, and Notification Server stays inside the internal network. If the Cloud-enabled Management Settings policy is disabled or no longer targets the computer, the computer uses the Internet gateway for communication until the direct connection becomes available. Then the computer reverts to direct communication with the local Notification Server.

This task is a step in the process for setting up Cloud-enabled Management.

See “Setting up Cloud-enabled Management” on page 20.

To 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 fully qualified domain name (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 have copied on the Internet gateway computer, in the **Symantec Management Platform Internet Gateway Manager**, on the **General** tab.
  See “Configuring the Internet gateway” on page 27.

Specify the target computers to which the policy applies.

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 has no direct connection to 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 to CEM mode.

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 the Cloud-enabled Management feature. Until the client computer is connected to the internal network, the Cloud-enabled Management mode remains inactive. When you disconnect the client computer from the internal network, Symantec Management Agent can connect to Notification Server through the Internet gateway, and 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**.
Generating and installing the Cloud-enabled Management offline package

In some cases, a computer that you want to manage may not have direct access to the network that hosts the Symantec Management Platform. To install the Symantec Management Agent on a computer that is located outside of the internal network, you first need to download the agent installation package from the Symantec Management Console.

After you generate the agent installation package from the appropriate Symantec Management Platform instance, you need to send it to the remote site. You can upload the package to a certain location or send it on a physical medium such as CD or flash drive. The users at the remote site then run the agent installation package to install the Symantec Management Agent on their computers. The newly installed Symantec Management Agent immediately connects to Notification Server through the appropriate Internet gateway. You can use the same installation package to install the Symantec Management Agent on all of the computers at a particular remote site.

This task is a step in the process for setting up Cloud-enabled Management. See “Setting up Cloud-enabled Management” on page 20.

To generate and install Cloud-enabled Management offline package

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Cloud-enabled Management.

2. In the left pane, expand Setup, and then click Cloud-enabled Management Setup.

3. On the Cloud-enabled Management Setup page, on the Symantec Management Agent Configuration tab, click Generate and download Symantec Management Agent installation package.

4. In the Cloud-enabled Agent Installation Package dialog box, specify the appropriate package parameters.

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.

The generated installation package is a self-extracting agent installation package that includes the following components and settings:

- Symantec Management Agent installer for the appropriate platform.
- Notification Server address (including protocol and port number to use).
- Notification Server certificate with CA chain.
The Internet gateway certifies the thumbprint and the temporary certificate. The temporary certificate is used to connect to the gateway for the first time. The temporary certificate is essential as it is used to generate a permanent client certificate request.

- List of the Internet gateways that are available for the Cloud-enabled agent to use.
- Organizational group to which the computer is added automatically.
- Scripts for configuring the Symantec Management Agent to use the specified settings.

**Warning:** The Symantec Management Agent installation package is valid for a limited time period (by default, 7 days) from the moment it was generated. The temporary certificate that is included in the package expires after this time. If you use the package after its temporary certificate has expired, the installed agent cannot use the Internet gateway for communications. You need to reinstall the agent using a newly generated installation package that contains a valid certificate.

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** dialog box, click **Close**.

9. Place the Symantec Management Agent installation package on the appropriate computer.
10 Run the agent installation package on the computer.

Note: Windows agent package is a self-extracting executable file that requires a password to decrypt data and perform the installation.

OS X package is a compressed file that contains Symantec_Management_Agent_Installer.pkg file to perform the interactive installation, a Resource folder with the actual signed agent packages, and cem_package.sh file to perform the silent installation using terminal.

After the installation, the Symantec Management Agent automatically configures itself, and then renegotiates its certificate.

The agent requests and receives a new certificate from Notification Server: The new certificate is specific to that client computer and replaces the temporary certificate that was included in the agent installation package.

11 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.

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.

See “Viewing Cloud-enabled Management reports” on page 50.
Performing Cloud-enabled Management tasks

This chapter includes the following topics:

- Cloud-enabled Management troubleshooting and maintenance tasks

Cloud-enabled Management troubleshooting and maintenance tasks

This section outlines the troubleshooting and maintenance tasks that you may need to perform.


<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing certificates.</td>
<td>The <strong>Manage Certificates</strong> page lets you check the certificates that are used in your environment and perform necessary management tasks. You can replace the certificates where necessary. You can revoke or renew agent certificates.</td>
</tr>
<tr>
<td></td>
<td>See “Managing certificates” on page 40.</td>
</tr>
<tr>
<td>Applying a CEM certificate with individual installation settings to a site server.</td>
<td>You can distribute a CEM certificate with individual installation settings to each site server separately.</td>
</tr>
<tr>
<td></td>
<td>See “Distributing a certificate with individual installation settings to a site server” on page 18.</td>
</tr>
</tbody>
</table>
Table 4-1  Cloud-enabled Management troubleshooting and maintenance tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restoring Cloud-enabled Management communication after an off-box upgrade.</td>
<td>After you perform an off-box upgrade of the IT Management Suite to the latest version, you may need to restore the communication with cloud-enabled client computers. See “Restoring Cloud-enabled Management communication after an off-box upgrade” on page 42.</td>
</tr>
<tr>
<td>Revoking a client certificate on a managed computer.</td>
<td>If you think a particular client certificate has been compromised and should no longer be trusted, you can revoke the certificate. For example, if a Cloud-enabled laptop computer is lost or stolen you need to revoke its certificate immediately. Revoking the certificate prevents the managed computer from accessing your network in Cloud-enabled mode. See “Revoking a Cloud-enabled Management certificate” on page 44.</td>
</tr>
<tr>
<td>Viewing site server certificates.</td>
<td>You can view site server certificates that are used in your environment. See “Viewing the site server certificates” on page 47.</td>
</tr>
<tr>
<td>Forcing a Cloud-enabled agent to use a specified Internet gateway.</td>
<td>If the agent does not have a valid list of Internet gateways, you can force it to communicate through a specified set of gateways. You can add and remove Internet gateways from the list as required. <strong>Note:</strong> You can perform this task on Windows computers only. See “Forcing the Symantec Management Agent to use a specified Internet gateway” on page 47.</td>
</tr>
<tr>
<td>Backing up and restoring Internet gateway.</td>
<td>You can back up your Internet gateway settings and restore its original state in case of a failure. See “Backing up and restoring an Internet gateway” on page 49.</td>
</tr>
<tr>
<td>Configuring the load balancer to work with the Cloud-enabled Management traffic.</td>
<td>Cloud-enabled Management feature requires firewall to redirect all inbound CEM traffic directly to the Internet gateway. In a situation where all the inbound traffic (including CEM traffic) must be routed through the organization's load balancer, you must configure the load balancer to handle the Cloud-enabled Management traffic. The following knowledge base article explains, how to perform the configuration in <strong>F5 BIG-IP Local Traffic Manager.</strong> <a href="http://www.symantec.com/docs/HOWTO109667">http://www.symantec.com/docs/HOWTO109667</a></td>
</tr>
<tr>
<td>Viewing Cloud-enabled Management reports.</td>
<td>A set of predefined reports is provided to help you monitor and manage your Cloud-enabled computers. See “Viewing Cloud-enabled Management reports” on page 50.</td>
</tr>
</tbody>
</table>
Managing certificates

The Certificate Management page gives you a complete overview of the certificates that are used in your environment and lets you perform necessary management tasks.

See “Cloud-enabled Management SSL certificates” on page 52.

**Note:** This page is available starting from IT Management Suite 8.1 RU2.

Note that information about the certificates is available immediately after the upgrade. However, before performing any certificate management tasks, you must upgrade the Symantec Management Agent to the latest version on all client computers. If you have implemented Cloud-enabled Management (CEM) in your environment, you must also upgrade the Internet gateway(s).

The Certificate Management page lets you check the state of the certificates. If a problem with a certificate is detected, the status of the certificate changes accordingly. For example, a certificate has a weak signature or its expiration date is near. In the list of certificates, you can filter out the certificates with detected problems and take required steps to fix the issues. Depending on the certificate type, you can replace, renew, or revoke selected certificates.

**Note:** Currently, the certificates that are manually added to the Communication Profiles are not displayed on the Certificate Management page.

To manage certificates

1. In the Symantec Management Console, on the Settings menu, click All Settings.
2. In the left pane, expand Notification Server, and then click Certificate Management.
3. On the Certificate Management page, you can do the following:
To perform the replacement of certificate:

1. Click the certificate that you want to replace, and then, on the toolbar, click **Replace**.

2. Select the new certificate and confirm the replacement process.

   Note that the replacement of the certificate does not occur immediately and the replacement process does not break the connectivity.

   After you initiate the replacement, the certificate is distributed to the required computers. On the **Certificate Management** page, you can check the progress of certificate distribution.

3. When the distribution of certificate is completed, you can finalize the replacement.

   Click the certificate that is being replaced, and then, on the toolbar, click **Finalize**.

   The finalization task replaces the current certificate with a new one. After finalization, the new certificate will be in use.

If you have not enabled the **Auto Refresh**... option in the **Internet Gateway Manager**, on the **Servers** tab, take the following steps to perform the replacement of NS root certificate:

1. Initiate the replacement of NS root certificate.

2. On the Internet gateway computer, in the **Internet Gateway Manager**, on the **Servers** tab, manually refresh the required server.

3. Wait until the certificate is distributed to all client computers.

4. Finalize the replacement process.

5. On the Internet gateway computer, in the **Internet Gateway Manager**, on the **Servers** tab, manually refresh the required server.

   Note that while the replacement is in progress, you can cancel it. Canceling the replacement process does not break connectivity and the old certificate remains in use.
Renew certificate

The renewal task lets you re-create CEM Agent certificates on cloud-enabled agents.

This task also lets you re-create an Internet gateway reporting certificate that the Internet gateway uses for sending its inventory to Notification Server.

To renew a certificate:

◆ Click the certificate that you want to renew, and then on the toolbar, click Renew.

If you have not enabled the Auto Refresh... option in the Internet Gateway Manager, on the Servers tab, take the following steps to perform the renewal of Internet gateway reporting certificate:

1. Initiate the renewal of Internet gateway reporting certificate.

2. On the Internet gateway computer, in the Internet Gateway Manager, on the Servers tab, manually refresh the required server.

Revoke certificate

Revoking a CEM Agent certificate prevents the managed computer from accessing your network in cloud-enabled mode. For example, if a cloud-enabled laptop computer is lost or stolen you need to revoke its certificate immediately.

To revoke a certificate:

◆ Click the certificate that you want to revoke, and then on the toolbar, click Revoke.

Restoring Cloud-enabled Management communication after an off-box upgrade

After you perform an off-box upgrade of the IT Management Suite 7.6 HF7 or 8.0 HF6 to the latest version, you may need to restore the communication with cloud-enabled client computers.

In most cases, when you upgrade the IT Management Suite onto a new server, the server has a different IP address and FQDN than the previous one. This means that the new server has a new set of SSL certificates that are used for Cloud-enabled Management (CEM) communication, and you need to set up CEM on the new Notification Server.
The following procedures describe the possible ways to redirect cloud-enabled clients after an off-box upgrade.

To restore CEM communication on Mac OS X computers that have no direct connection with Notification Server after an off-box upgrade of the IT Management Suite 7.6 HF7

1. After you install the latest version of IT Management Suite on the new server, configure CEM environment the same way, as for a new installation.

   For more information on how to configure Cloud-enabled Management, see the IT Management Suite Administration Guide, or the Cloud-enabled Management Whitepaper.

2. On the new Notification Server, generate an offline installation package for CEM, extract `cem_package.sh` from the generated zip archive, and then place the package in a location accessible from old Notification Server.

3. On the old Notification Server, import the package into Software Catalog, and then set up the following Install command line option for the package:

   ```bash
   sh cem_package.sh -reinstall -pwd 'yourpassword' -bg
   ```

   This command line enables automated upgrade and switching to a new Notification Server.

4. From the old Notification Server, deploy the offline installation package to cloud-enabled clients with a Managed Software Delivery or a Software Delivery task.

5. When the clients are upgraded, on the new Notification Server, make sure that the newly upgraded clients are members of all needed filters and organizational groups.

To restore CEM communication on Mac OS X computers after an off-box upgrade of the IT Management Suite 7.6 HF7 or 8.0 HF6

1. Ensure that the 7.6 HF7 or 8.0 HF6 clients are able to communicate with the latest version of Notification Server without using CEM.

2. On the 7.6 HF7 or 8.0 HF6 Notification Server, disable the CEM policy to remove the old CEM settings from the clients.

3. In the Symantec Management Console, click Settings > Agents/Plug-in Settings > Targeted Agents Settings.
4 On the **Targeted Agents Settings** page, on the **Advanced** tab, redirect the clients to the latest version of Notification Server.

5 On the latest version of Notification Server, enable the CEM policy.

   After the 7.6 HF7 or 8.0 HF6 clients register on the latest version of Notification Server and receive the CEM policy, they receive the new CEM settings.

To restore CEM communication on Windows or Mac OS X computers after an off-box upgrade of the IT Management Suite 7.6 HF7 or 8.0 HF6

1 After you install the latest version of IT Management Suite on the new server, configure CEM environment the same way, as for a new installation.

   For more information on how to configure Cloud-enabled Management, see the *IT Management Suite Administration Guide*, or the *Cloud-enabled Management Whitepaper*.

2 On the new Notification Server, export the default connection profile that includes CEM settings.

3 On the old Notification Server, import the connection profile.

4 In the **Symantec Management Console**, click **Settings > Agents/Plug-in Settings > Targeted Agents Settings**.

5 On the **Targeted Agents Settings** page, on the **Advanced** tab, check **Specify an alternate URL for the Symantec Management Agent to use to access the NS**, and then select and configure the imported connection profile.

6 Apply **Targeted Agent Settings** policy to the cloud-enabled clients that you want to upgrade, and then enable the policy.

7 Ensure that the targeted cloud-enabled clients receive the policy and use the imported connection profile to access Notification Server.

8 On the new Notification Server, enable the upgrade policy.

9 Ensure that the targeted cloud-enabled clients receive the policy and upgrade successfully.

**Revoking a Cloud-enabled Management certificate**

Revoking a Cloud-enabled Management (CEM) certificate prevents the managed computer from accessing your network in Cloud-enabled mode. For example, if a Cloud-enabled laptop computer is lost or stolen you need to revoke its certificate immediately.

The agent has two CEM certificates. One certificate lets the agent create connection to the Internet gateway, and another certificate lets the agent connect to Notification Server. If the certificate that lets the agent connect to Notification Server is revoked,
Notification Server declines connection from such client computer. However, Internet gateway cannot receive the information on revoked certificates from Notification Server directly. To revoke a particular certificate on Internet gateway, you need to add the certificate details to the Certificate Revocation List (CRL) on Notification Server, generate an updated CRL file, and then apply the updated CRL file to the appropriate Internet gateway.

**Note:** You need to apply the updated CRL file to every Internet gateway that the revoked agent might use.

Note that revocation of the Cloud-enabled certificate only blocks the managed computer from accessing Notification Server in Cloud-enabled mode. If the agent trust is not revoked, the agent can continue to operate in local mode.

**To revoke a Cloud-enabled Management certificate**

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.

2. In the left pane, under **Reports**, expand **Notification Server Management > Certificates**, and then click **Certificate by Thumbprint**.

3. On the **Certificate by Thumbprint** report page, right-click the certificate that you want to revoke, and then click **Revoke Certificate**.

If you revoke the certificate on the **Certificate by Thumbprint** report page, the certificate details are added to the CRL file automatically.

The CRL is stored in the root computer store, although the certificates are stored in the Configuration Management Database (CMDB). The certificate revocation tool (AeXRevokeCertificate.exe) first loads the existing CRL if it exists. If no CRL exists in the certificate store, the tool creates one. The tool then adds the certificate serial number to the list and generates a PEM-encoded file containing the updated CRL. You then place the generated CRL file on the Internet gateway computer and run a script to apply the updated list to the Internet gateway.

By default, the CRL file is at the following location on Notification Server:

\Program Files\Altiris\Notification Server\bin\Tools\AeXRevokeCertificate\EMEncodedFile.CRL

**To add a Cloud-enabled Management certificate to the CRL manually**

1. Obtain the serial number and thumbprint of the client certificate that you want to revoke.

   If you have access to the client computer, you can use the Microsoft Management Console (MMC) to look up the client certificate details.
If you do not have access to the client computer, you can use one of the following methods:

- In the Symantec Management Console, open the Resource Manager and view basic inventory information for the client computer. The menu path is **View > Data Classes > Inventory > Basic Inventory > AeX AC Certificate**. The full details of the client certificate are shown, including the serial number and the thumbprint.

- Use a SQL query to search for the serial number and the thumbprint of the client certificate in the Symantec Management Platform CMDB, in the **CertificateRegistration** table.

- On the Internet gateway, open the access log file and look for an entry that relates to the client computer. The **access.log** file is stored in the **Apache\logs** folder in the Internet gateway installation folder. Each entry in the log file includes the name of the computer that accessed the Internet gateway and the corresponding certificate serial number.

2 On the Notification Server computer, in the command prompt window, run the following command line with the appropriate parameters:

```
\Program Files\Altiris\Notification Server\bin\Tools\AeXRevokeCertificate -o <PEMEncodedFile.CRL> <-t Sha256ThumbPrint | -s SerialNumber>
```

- **PEMEncodedFile.CRL** The full path and name of the PEM-encoded CRL file that you want to generate. Without this parameter, the generated file is saved in the local directory.

- **Sha256ThumbPrint** The unique identifier of the certificate.

- **SerialNumber** If more than one certificate in the database is with the same serial number, use an SHA256 thumbprint to identify the certificate. If two certificates have the same thumbprint, identify the certificate by serial number.

**Warning:** Sometimes, the thumbprint and the serial number may be displayed as space-separated octets. However, when you specify them as command line parameters, they must not include any spaces between the characters.

The updated CRL file is generated.
To apply the CRL to an Internet gateway

1. Place the generated CRL at the following location on the Internet gateway computer:

   \[\text{Internet gateway installation folder}\]Apache\certs\crl

   The default Internet gateway installation folder is \Program Files x86\Symantec\SMP Internet Gateway. However, the path depends on the target directory that was specified during the Internet gateway installation.

2. In the same folder, double-click UpdateCrlHashes.cmd to run the Update CRL script.

   This script performs the necessary configuration, and then restarts the Internet gateway to apply the changes.

   See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.

Viewing the site server certificates

Under the Organizational Views and Groups, the Digital Certificate view displays the certificates that the site servers use. Note that the Digital Certificate view is disabled by default.

See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.

To view the site server certificates

1. In the Symantec Management Console, on the Manage menu, click Organizational Views and Groups.

2. In the left pane, click Default.

3. In the right pane, on the upper right corner, click Filter.

4. In the Filter Visible Groups dialog box, under Default > All Resources, check Digital Certificate box, and then click OK.

5. In the left pane, expand Default > All Resources, and then click Digital Certificate.

Forcing the Symantec Management Agent to use a specified Internet gateway

(Windows agent only)

If the agent does not have a valid list of Internet gateways, you can force it to communicate through a specified set of gateways. You force a specific list of
gateways from the command line or by modifying the registry settings. A command line is available for adding individual gateways.

To remove an Internet gateway from the Symantec Management Agent configuration, you need to edit the registry.

The Internet gateway details are stored in the registry. To add or remove Internet gateways, edit the entries under the following key:

\HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications\Secure Gateways

Each Internet gateway has a set of values under the <GatewayName> key.

---

**Note:** You need to restart the Symantec Management Agent to apply these settings.

---

**To force the Symantec Management Agent to use a specified Internet gateway**

- On the client computer, in the command prompt window, run the following command line:

  \Program Files\Altiris\Altiris Agent\AeXNSAgent.exe
  /gw=gatewayName,port,thumbprint

  **gatewayName** The name or IP address of the gateway computer.

  **port** The port number that the Symantec Management Agent must use to connect to the gateway. The default port is 443.

  **thumbprint** The certificate thumbprint of the certificate that the gateway uses for secure connections.

  **Warning:** Sometimes, the thumbprint may be displayed as space-separated octets. However, when you specify it as a command line parameter, it must not include any spaces between the characters.

  Each parameter needs to be separated with a comma. No spaces or other punctuation is allowed.

  For example:

  \Program Files\Altiris\Altiris Agent\AeXNSAgent.exe
  /gw=myGateWay.symantec.com,443,0f8753ef3da6bc4

  See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.
Back up and restore an Internet gateway

Backing up your Internet gateway lets you restore its original state in case of a failure. You can perform a partial restore if some files from the backup list are missing or corrupted. You can also perform a full restore in case of fatal corruptions in the Internet gateway configuration. For example, if you have replaced a hard disk on your Internet gateway computer.

You can perform a backup without stopping the Internet gateway service.

You can manually back up the files in given folders as follows:

- `openssl.cnf`, `server.crt`, and `server.key` files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\certs` folder
- All files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\certs\client` folder
- All files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\certs\crl` folder
- All files in the `C:\Program Files\Symantec\SMP Internet Gateway\Apache\conf` folder

You can also create a backup file in the Symantec Management Platform Internet Gateway Manager.

To create a backup file

1. In the Symantec Management Platform Internet Gateway Manager, on the About tab, under Disaster Recovery, click Save.
2. In the Save configuration dialog box, enter the file name and password, and then click OK.

To perform a manual restore

1. On the Internet gateway computer, open the Symantec Management Platform Internet Gateway Manager.
2. On the General tab, under Internet Gateway Service, click Stop to stop the Internet gateway service.
3. Restore the required items from the backup list.
4. In the Symantec Management Platform Internet Gateway Manager, on the General tab, under Internet Gateway Service, click Start to start the Internet gateway service.

After you start the service, make sure that the Internet gateway settings are correct and the functionality is working properly.
To perform a full restore using the backup file

1. Perform a new installation of Internet gateway.
   See “Downloading and running the Internet gateway installation package” on page 26.

2. In the Symantec Management Platform Internet Gateway Configuration wizard, on the First Time Setup page, select Use existing configuration, and then click Browse.

3. In the Restore Configuration dialog box, select the configuration file, enter the password, and then click OK.


5. On the User Account page, specify the Internet gateway service credentials, and then click Next.

6. On the Summary page, review the settings, and then click Finish.
   After the service starts, make sure that the Internet gateway settings are correct and the functionality is working properly.

   See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.

Viewing Cloud-enabled Management reports

A set of reports is provided to help you monitor and manage your Cloud-enabled computers. You can also create custom reports to suit your requirements.

Cloud-enabled Management reports are grouped into the following folders:

- **Agent**: The reports contain data about Cloud-enabled computers.
- **Certificates**: The reports contain data about SSL certificates, CEM offline installation packages, and their registration requests.
- **Gateway**: The reports contain data about Internet gateways.

   See “Enabling the Internet gateway status reporting” on page 29.
To view Cloud-enabled Management reports

1. In the Symantec Management Console, on the Reports menu, click All Reports.

2. In the left pane, click Reports > Notification Server Management > Agent > Cloud-enabled Management, and then click Agent, Certificates, or Gateway.

3. Click the report that you want to view.

See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.
About SSL certificates

This chapter includes the following topics:

- Cloud-enabled Management SSL certificates
- About implementation of SSL in Cloud-enabled Management
- Requirements and usage of third-party commercial certificates

Cloud-enabled Management SSL certificates

Using SSL certificates lets you verify the identity of parties that exchange information, ensure that the information is not corrupted, and protect it from being captured by third parties.

Previously, Symantec Management Platform provided management capabilities for client computers inside a corporate network, as a part of intranet or VPN. The Cloud-enabled Management (CEM) required an introduction of additional security measures to allow secure management of client computers outside the corporate network. For example, it required an extended usage of SSL certificates to secure the agent’s connections and verify the identities of client computers.

Starting from IT Management Suite version 8.1 RU2, you can manage all certificates on the Manage Certificates page.

See “Managing certificates” on page 40.
### Table 5-1  
Cloud-enabled Management SSL certificates

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Purpose</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NS root certificate</td>
<td>Used for internal authorization.</td>
<td>The NS root certificate is a self-signed certificate that is generated during the installation of the Symantec Management Platform. This certificate is stored in Trusted Root on Symantec Management Platform and is used as Certificate Authority (CA) for issuing CEM Agent certificates. <strong>Warning:</strong> Do not edit, replace, or delete the NS root certificate. If this certificate is modified, the CEM stops functioning properly.</td>
</tr>
<tr>
<td>NS Website certificate</td>
<td>To establish and secure the HTTPS connection to the Symantec Management Console.</td>
<td>This certificate is automatically applied during the installation of Symantec Management Platform and installed on the Internet Information Services website that is connected to Symantec Management Platform. If you do not want to use the default certificate, you can import a third-party certificate in the Symantec Installation Manager. See “Importing the NS Website certificate in the Symantec Installation Manager” on page 58.</td>
</tr>
<tr>
<td>CEM Website certificate</td>
<td>To provide the secure back-end connection for the agents that use CEM.</td>
<td>For security reasons, the HTTPS connection is required for communication with the agents that are managed through CEM. The certificate is automatically generated when you create a CEM site in the Symantec Management Console. This certificate is similar to the NS Website certificate. It is also installed on the Internet Information Services website that is connected to Symantec Management Platform. If you do not want to use the default certificate, you can configure it in the Symantec Management Console, on the <strong>Cloud-enabled Management Agent IIS Website Settings</strong> page, at <strong>Settings &gt; Notification Server &gt; Cloud-enabled Management &gt; Setup</strong>. You can also use a third-party commercial certificate, or re-use the NS Website certificate. See “Importing the CEM Website certificate in the Symantec Management Console” on page 59.</td>
</tr>
</tbody>
</table>
### Table 5-1: Cloud-enabled Management SSL certificates (continued)

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Purpose</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site server certificate</td>
<td>To authenticate site servers.</td>
<td>When a Cloud-enabled agent connects to a site server, this certificate is evaluated to establish an HTTPS connection and confirm the identity of the site server. The Global Site Server Settings lets you apply a CEM certificate to every site server that is assigned to an Internet Site. The policy creates an HTTPS binding on site server and installs certificate signed by the Notification Server Certificate Authority (CA), which means that Cloud-enabled Management agents would trust this site server. Both self-signed and third-party commercial certificates can be used on site servers. Note that the same certificates must be distributed to Cloud-enabled endpoints to establish the SSL trust.</td>
</tr>
<tr>
<td>Internet gateway certificate</td>
<td>To authenticate the Internet gateway computer.</td>
<td>This certificate is automatically created during the installation of the Internet gateway package. When a Cloud-enabled agent connects to the Internet gateway, the validity of this certificate is evaluated to confirm the identity of the Internet gateway computer. By design, this certificate is self-signed. You can also use a third-party commercial certificate. See “Importing a third-party certificate on Internet gateway” on page 60.</td>
</tr>
<tr>
<td>Internet gateway agent certificate</td>
<td>To authenticate the Internet gateway on Notification Server.</td>
<td>This certificate is created during the configuration of the Internet gateway, when you register the Internet gateway on Notification Server.</td>
</tr>
<tr>
<td>CEM Agent certificate</td>
<td>To authenticate Cloud-enabled agents on Internet gateway.</td>
<td>When the agent receives the Cloud-enabled Management Settings policy or after the installation of the Cloud-enabled agent offline installation package, the agent performs the registration on Notification Server. During the registration, Cloud-enabled agent receives the certificate from Notification Server. This certificate is evaluated when the Cloud-enabled agent connects to the Internet gateway. It is unique for every agent and it ensures that no untrusted agents can connect to the Internet gateway. Note that in addition to the client certificate, the Symantec Management Agent receives a thumbprint of the Internet gateway certificate. The thumbprint is delivered with the Cloud-enabled Management Settings policy or with the Cloud-enabled agent offline installation package.</td>
</tr>
</tbody>
</table>
### Table 5-1  Cloud-enabled Management SSL certificates (continued)

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Purpose</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temporary certificates for Cloud-enabled agent offline installation package</td>
<td>Allows the Cloud-enabled agents to obtain permanent CEM certificates.</td>
<td>When you install the Cloud-enabled agent using the offline installation package, the temporary CEM certificates allow the agent to connect to Notification Server and obtain the permanent CEM certificates. You can manage these certificates in the Symantec Management Console, at Reports &gt; Notification Server Management &gt; Cloud-enabled Management &gt; Certificates &gt; CEM Installation packages.</td>
</tr>
</tbody>
</table>

### About implementation of SSL in Cloud-enabled Management

Before you install IT Management Suite or perform an upgrade from a previous version, you have to consider which SSL certificate architecture to implement. You can select to use one of the following architectures or use a mixed architecture.

**Table 5-2  SSL certificate architecture options**

<table>
<thead>
<tr>
<th>Implementation</th>
<th>Description</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| Certificate generation tools that are shipped with IT Management Suite | Symantec Management Platform provides a set of tools that you can use to sign and validate SSL certificates. | Before you use the certificate generation tool that is shipped with the IT Management Suite, consider the following:  
- Certificates are generated with 20-years validity period. You can change the length of the validity period with the certificate generation tools, like AeXGenSiteServerCert.  
- To use package and task servers over HTTPS, you need to apply SSL certificate for each site server.  
- To verify the identity of site servers, client computers need to have agent root certificate authority installed. |
Considerations

Before you use third-party commercial certificates, consider the following:

■ An imported SSL certificate has to comply with the requirements that are listed in the following section:

See "Requirements and usage of third-party commercial certificates" on page 56.

■ It is required to import a wildcard SSL certificate (*.domain.com) with Microsoft Management Console before you install the IT Management Suite.

A single address (smp.domain.com) certificate can be imported with the Symantec Installation Manager.

■ For Cloud-enabled Management (CEM) the certificate has to be issued for an FQDN that can be resolved internally and by the Internet gateway. Third-party vendors require that the top-level domain name in the FQDN is a public domain.

Mixed architecture examples

To implement Cloud-enabled Management, you can use a combination of self-signed and third-party commercial certificates. Consider the following examples:

■ You acquire and provision a wildcard SSL certificate to establish HTTPS connection with Symantec Management Console and Cloud-enabled Management Agent Website, and you use self-signed certificates for site servers and client computers.

■ You acquire and provision an SSL certificate to establish HTTPS connection with Symantec Management Console, and use self-signed certificates in the remaining cases.

Requirements and usage of third-party commercial certificates

Before you use a third-party commercial SSL certificate within Symantec Management Platform infrastructure, make sure that the certificate fulfils the technical requirements. Each type of the third-party commercial certificate has to comply with the general requirements for SSL certificates and the specific requirements, like the import procedure.

For detailed description and import procedure for a given certificate, see the following:
- **NS Website certificate**
  See “Importing the NS Website certificate in the Symantec Installation Manager” on page 58.

- **CEM Website certificate**
  See “Importing the CEM Website certificate in the Symantec Management Console” on page 59.

- **Internet gateway certificate**
  See “Importing a third-party certificate on Internet gateway” on page 60.

- **Wildcard SSL certificate**
  A wildcard SSL certificate does not provide additional functionality for the Symantec Management Platform. It is used to provide HTTPS connection to a number of subdomains. Due to that fact, its requirements, and import procedure are different.
  See “Importing the wildcard SSL certificate” on page 61.

### Table 5-3  Requirements for third-party certificates

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital signature</td>
<td>The certificate has a valid digital signature.</td>
</tr>
<tr>
<td>Trust</td>
<td>The certificate is issued by Certificate Authority that is trusted by the Notification Server computer. Note that for site server the Certificate Authority must also be trusted by the client computers.</td>
</tr>
<tr>
<td>Validity</td>
<td>The certificate is valid at least for 30 days from the import date.</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>The Enhanced Key Usage value of the certificate is Server Authentication OID (1.3.6.1.5.5.7.3.1).</td>
</tr>
</tbody>
</table>
Table 5-3  Requirements for third-party certificates (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject name or subject alternate name</td>
<td>The requirements for subject name or subject alternate name are as follows:</td>
</tr>
<tr>
<td>■ NS Website certificate</td>
<td>Subject or subject alternate name matches the Notification Server computer Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>■ CEM Website certificate</td>
<td>Subject or subject alternate name matches the Notification Server computer Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>■ Wildcard SSL certificate</td>
<td>Subject or subject alternate name matches the Notification Server computer domain name. For example, if Notification Server’s FQDN is ns.example.com, the certificate subject or alternate subject should contain *.example.com</td>
</tr>
<tr>
<td>■ Site server SSL certificate</td>
<td>Subject or subject alternate name matches the site server computer Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>For Cloud-enabled Management (CEM), the certificate has to be issued for an FQDN that can be resolved internally and by the Internet gateway. Third-party vendors require that the top-level domain name in the FQDN is a public domain.</td>
<td></td>
</tr>
<tr>
<td>Hashing algorithm</td>
<td>The certificate uses one of the following hashing algorithms:</td>
</tr>
<tr>
<td>■ SHA1 (Symantec recommends not to use it)</td>
<td></td>
</tr>
<tr>
<td>■ SHA256</td>
<td></td>
</tr>
<tr>
<td>■ SHA384</td>
<td></td>
</tr>
<tr>
<td>■ SHA512</td>
<td></td>
</tr>
<tr>
<td>Asymmetric algorithm</td>
<td>The certificate uses the RSA asymmetric algorithm.</td>
</tr>
<tr>
<td>File format</td>
<td>.pfx</td>
</tr>
</tbody>
</table>

Importing the NS Website certificate in the Symantec Installation Manager

The NS Website certificate is used for establishing an HTTPS connection with the Symantec Management Console, and is also required if you plan to use the Cloud-enabled Management (CEM) feature.

You can import the NS Website certificate before installing the Symantec Management Platform or after the installation process. If you install a new instance
of Symantec Management Platform, Symantec recommends installing this certificate in the Symantec Installation Manager.

You can import the certificate in following ways:

- In the Symantec Installation Manager, during the installation process.
  See "To import the NS Website certificate in the Symantec Installation Manager during the installation" on page 59.

- After the Symantec Management Platform is installed, in the Internet Information Services (IIS Manager).
  The process to import the NS Website certificate and set up HTTPS connection after Symantec Management Platform is installed is beyond the scope of this document. For more information, see the IT Management Suite Installation and Upgrade Guide.

To import the NS Website certificate in the Symantec Installation Manager during the installation

1. In the Symantec Installation Manager, in the Notification Server Configuration step, in the Certificate drop-down, click Import.

2. In the Select a security certificate file, click the .pfx file that you want to import, and then click Open.

3. In the next window, enter your certificate password, and then click OK.

4. (Optional) In the SSL port text field, enter the port that you want to use. By default, 443 port is used.

5. (Optional) Click Require HTTPS to access the Management Platform.
   Symantec recommends performing this step to increase the security stance of Symantec Management Platform.

6. Click Next.

Importing the CEM Website certificate in the Symantec Management Console

The CEM Website certificate is used to connect with a special Internet website that is dedicated for Cloud-enabled access. It is not accessed publicly, only the Cloud-enabled agents use this certificate to verify the connection to Notification Server.

You can import the third-party certificate after the Symantec Management Platform is installed, in the Symantec Management Console.
To import the CEM Website certificate

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 **Cloud-enabled Management Agent IIS Website Settings**.
3. In the right pane, click **Add IIS Website for cloud-enabled agent connections**.
4. Click **Import certificate**, and then, in the **Import Certificate** window, click **Browse**.
5. In the **Choose File to Upload**, specify the path and the file name of the .pfx certificate file that you want to import, and then click **Open**.
6. In the **Import Certificate** window, click **OK**.
7. Specify the remaining CEM Website settings, and then click **Save changes**.

Importing a third-party certificate on Internet gateway

If you do not want to use the certificate that is automatically created by the Internet gateway configuration wizard, you can install a third-party certificate on your Internet gateway computer.

See “Cloud-enabled Management troubleshooting and maintenance tasks” on page 38.

To import a third-party certificate on Internet gateway

1. In the **Symantec Management Platform Internet Gateway Manager**, click **Import Certificate**.
2. In the **Import Certificate** dialog box, specify the location of the certificate file, enter the certificate password, and then click **OK**.

   In the **Import Certificate** dialog box, you can also mark if you want to backup the certificate that is currently in use.

3. In the Symantec Management Console, do the following:

   - On the **Settings** menu, click **Notification Server > Cloud-enabled Management**.
   - In the left pane, expand **Policy**, and then click **Cloud-enabled Management Settings**.
   - On the **Cloud-enabled Management Settings** policy page, under **Gateways accepting external agent traffic**, select the Internet gateway that you want to edit, and then on the toolbar click the **Edit** icon.
In the Edit Gateway Server dialog box, paste the new thumbprint, and click OK.

Under, Applied to, apply the edited Cloud-enabled Management Settings policy to the client computers that you want.

Click Save changes.

Importing the wildcard SSL certificate

If you use a number of servers within the same domain, you might want to consider obtaining a wildcard SSL certificate. This certificate is issued with the subject name of *.domain.com, which allows the certificate to be used for all servers within the same domain. For example, a single wildcard certificate can be used for smp.domain.com, cloud.domain.com and hr.domain.com.

You can import the wildcard certificate in the Microsoft Management Console.

To import a wildcard SSL certificate

1 Place the certificate file in a location that is accessible from the managed computer.
2 On the managed computer, start Microsoft Management Console.
3 Add the Certificates snap-in for the Computer account > Local Computer and then open the Console Root > Certificates (Local Computer) folder.
4 Right-click Personal Certificates Store and then select All Tasks > Import.
5 In the Certificate Import Wizard, specify the path and the file name of the .pfx certificate file that you want to import.
6 Click Next to accept the default location and other settings, and then click Finish.
AeXRevokeCertificate.exe

command line parameters 44

CEM Agent IIS Website
settings 23

CEM Agent Settings
configuring 23

CEM certificate
revoking 44

CEM Website
- SSL certificate 59

certificates
- report 47
- viewing 47

Cloud-enabled agent
- installing offline package 35
- Internet gateway selection, forcing 47
- troubleshooting 38

Cloud-enabled Management
- about 9
- configuring Cloud-enabled Management Settings
  policy 32
- Internet gateway 20
- mixed environment 12
- package servers 11
- preparing site servers 14
- preparing the environment 14
- prerequisite activities 14
- reports 29, 50
- revoking certificate 44
- site servers 11
- task servers 11
- usage of SSL certificates 52

Cloud-enabled Management Settings policy
- configuring 32
- disabling 32
- enabling 32

digital certificate 47

global site server settings
- configuring 15

individual site server settings
- applying 18

Internet gateway
- backing up 49
- configuration files 20
- configuring 27
- configuring host computer 24
- downloading installation package 26
- forcing selection on Cloud-enabled agent 47
- full restore 49
- log files 20
- overview 20
- partial restore 49
- port 27
- preparing 24
- process for installing 20
- reporting 29
- running installation package 26
- setting up 20
- status 29
- third party certificate 60

Notification Server
- configuring to use HTTPS 14

package servers
- configurations 12
R
reports
  Cloud-enabled Management 50

S
site
  configuring for Cloud-enabled agents 30
site server
  global certificates rollout 15
  global security settings 15
  individual settings 18
site servers
  assigning to a site 30
  configuring for Cloud-enabled agents 30
site server certificate
  individual settings 18
SSL certificates
  CEM Website 59
  implementation 55
  requirements 52, 56
  Symantec Management Platform 58
  third party 56, 58–59, 61
  types 52
  use cases 55
  wildcard 61
Symantec Management Agent
  installing offline package 35
  redirecting to use HTTPS 14
  troubleshooting for Cloud-enabled Management 38
Symantec Management Platform
  SSL certificate 58

T
third party certificate
  installing 60

W
Wildcard
  SSL certificate 61