



# Cloud Enabled Management Design and Implementation

**Tomas Chinchilla**, Sr. Regional Product Manager, Endpoint Management

**Brian Sheedy**, Sr. Principal TEC, Endpoint Management



# Agenda

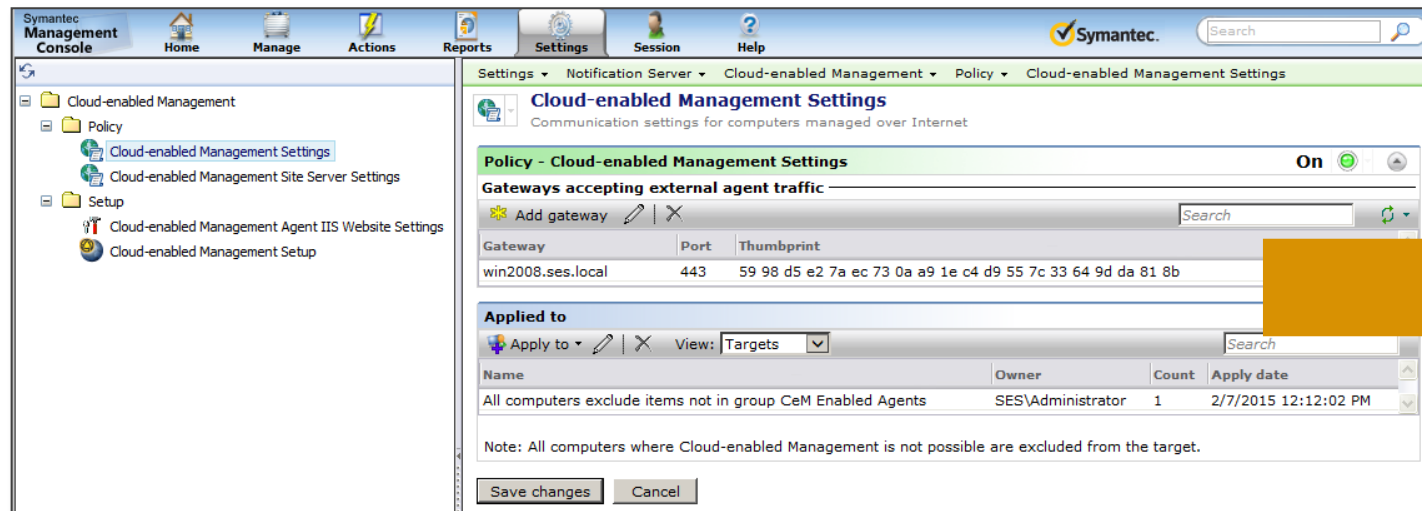
1	New Features in Cloud Enabled Management
2	Preparing your Environment for Cloud Enabled Management
3	Implementing the Cloud Enabled Infrastructure
4	Provisioning Cloud Enabled Management to the Endpoint



# What's new in Cloud Enabled Management

# Simplified CeM Agent Enablement

- **Configure your Notification Server and Symantec Management Agents to use HTTPS.**
  - The Symantec Management Agents are automatically configured to use HTTPS when they receive the **Cloud-enabled Management Settings** policy.



# Package Server Multi-Codebase support

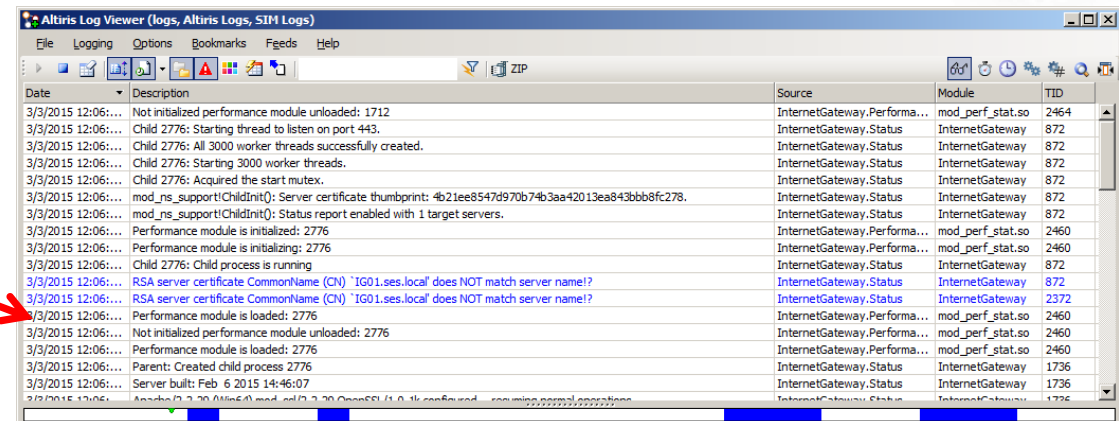
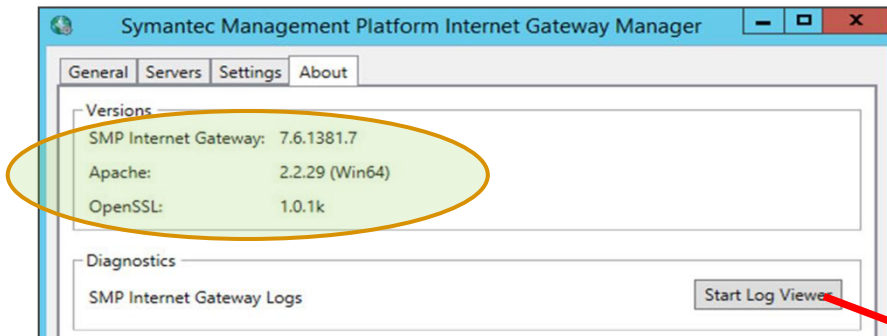
- Site Servers now have the ability to run multiple (2) HTTPS bindings for both internal clients on SSL:443 and CeM Agents on SSL:4726
- It is easily configurable using CEM Site Server Settings policy.
- New Site Server installs will default to port 4726 (Assignable)
- This use case does not necessarily apply to all customers.
- This setting is global for All Site Servers assigned to Internet Sites
- ***Force Override HTTPS Binding*** follows this logic:

Existing HTTPS binding on SS	Force Override HTTPS Binding	Policy Action
NO	DISABLED	<b><i>A new SSL certificate is delivered, and used to create a new SSL port binding.</i></b>  Use this configuration for new site servers.
YES	DISABLED	<b><i>A new SSL certificate is delivered, and an additional binding is created using the configured port (default 4726).</i></b>  Use this configuration for site servers, that already use HTTPS
YES	ENABLED	<b><i>A new SSL certificate is delivered, and used to overwrite the existing SSL port binding.</i></b>  <i>This results in a single HTTPS Binding</i>



# Internet Gateway Improvements

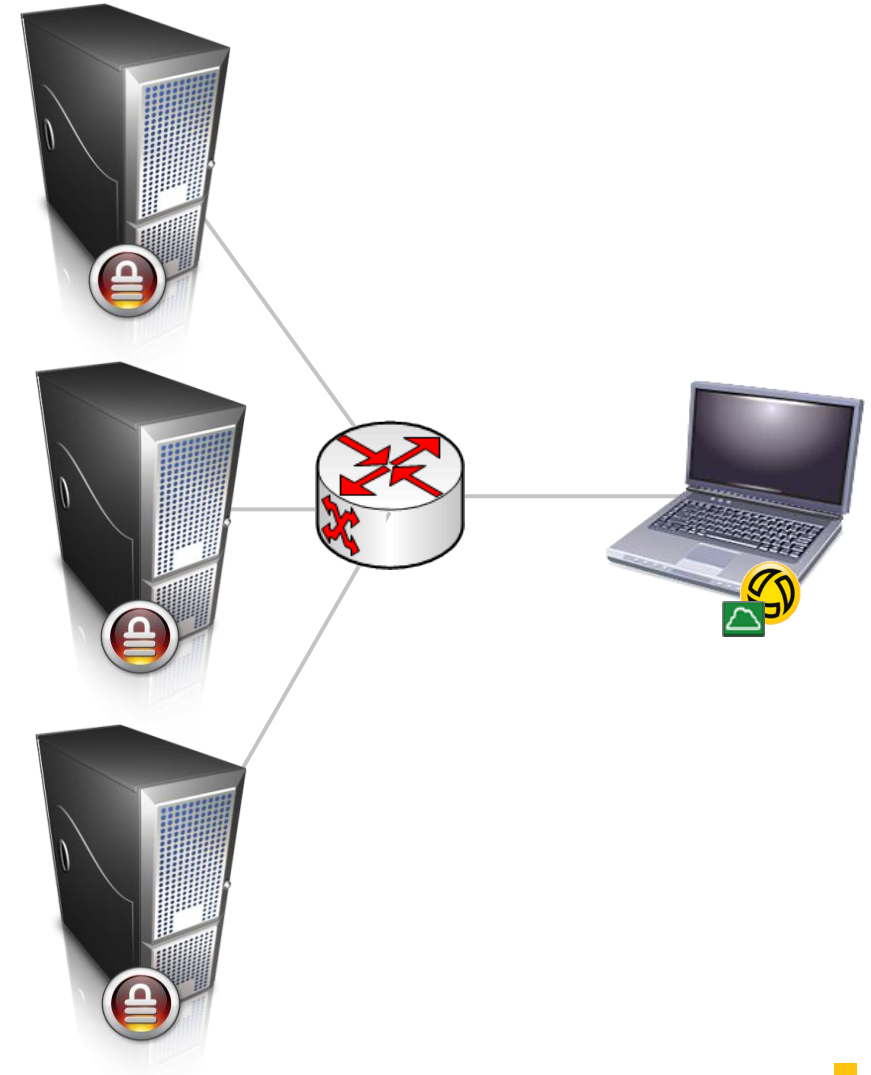
- Full support for 3rd Party & Commercial certificates
  - Just manually replace the certificate and the key files after the IG Install
  - For step by step instructions please refer to the CEM Whitepaper
- Apache and OpenSSL versions were upgraded



- Internet Gateway logging and report content improved

# Official support for BigIP F5 load balancers

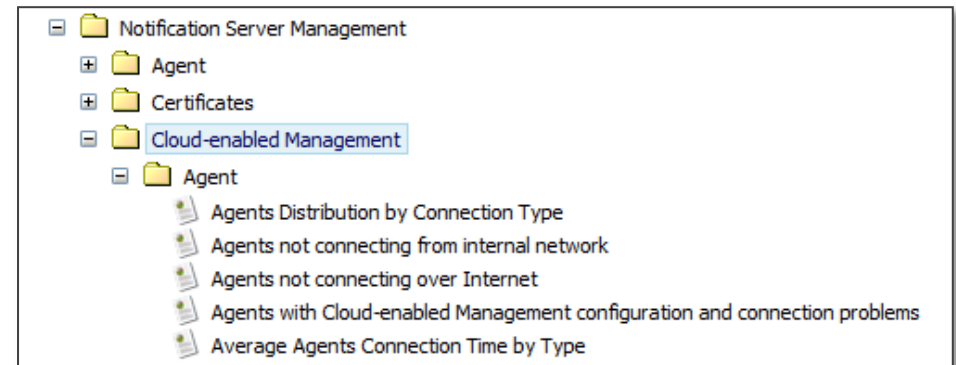
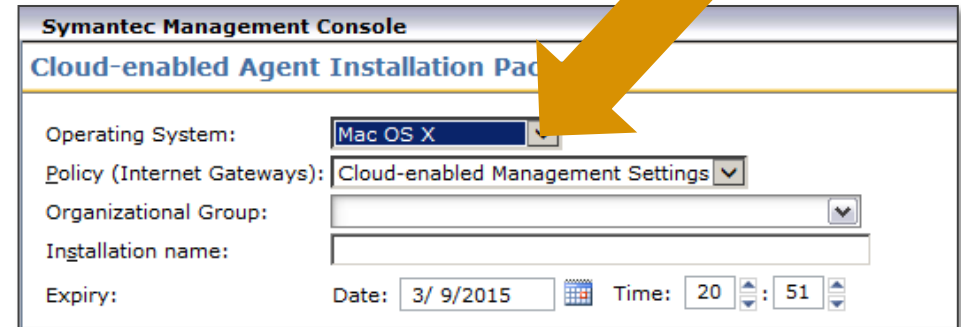
- We are supporting two different Use Cases:
- Using the F5 as a fully glorified NAT'ing device,
  - Where both “balancing and SSL offloading” are turned off.
  - You will still need independent FQDN's and IP's published on the Internet per gateway.
  - Only BigIP F5 supported at this point.
- Using the F5 as a load balancer (No SSL offloading)
  - By publishing a single FQDN and IP address on the internet and having the F5 balance the connection across multiple Gateways.
  - This can be accomplished by using either 3rd party or Self-Signed certificates on the internet gateways.
  - This option would allow you to have a single FQDN and IP registered on the internet and multiple gateways sitting behind the F5
  - All gateways must be running the same Digital SSL Certificate whether this is self-signed or commercial/3rd party.)



# CEM support for Mac Agent

- CEM Installation Package for Mac Agent
- CEM package security:
  - Installer app signed with Apple certificate, password-encrypted certificates and install.xml
- Consistency of Mac & Windows Agents in CEM mode
- CEM mode icon in System tray and dock
- Additional CEM reports
- Troubleshoot connectivity problems using Terminal

```
# aex-helper info cem -l
# aex-helper debug on (Verbose Mode)
```





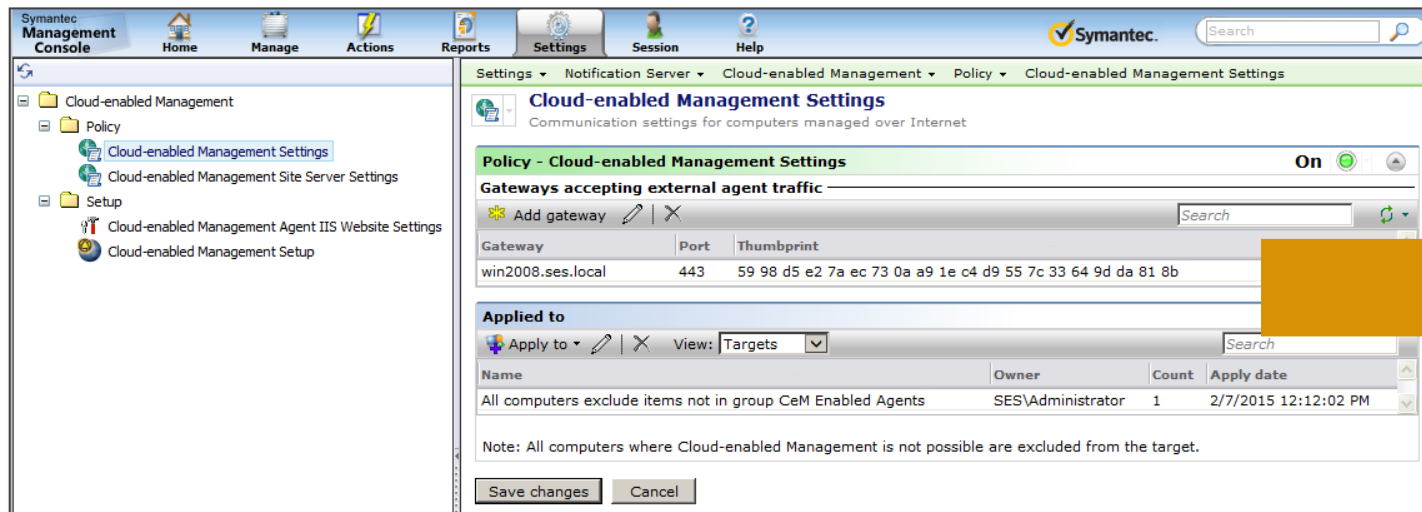


# Preparing Your Environment for Cloud Enabled Management

# Steps to Prepare the SMP Environment for CeM

## 1. Configure your Notification Server and Symantec Management Agents to use HTTPS.

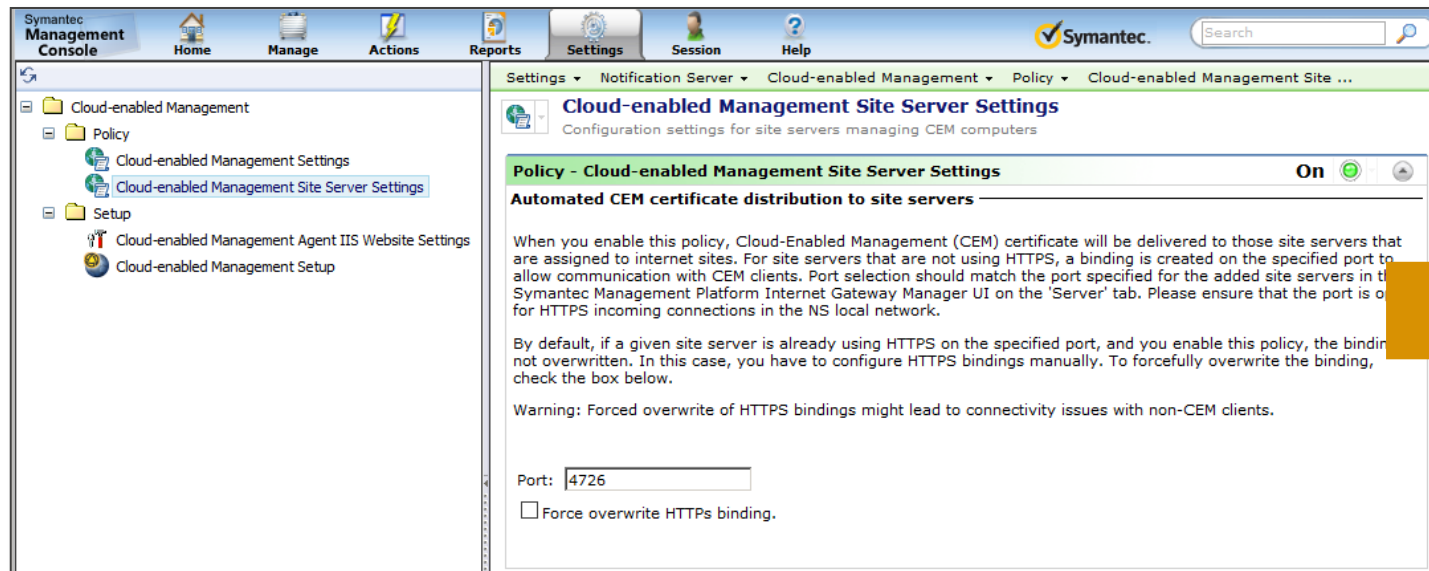
- The Notification Server is automatically configured to use HTTPS if you check **Require HTTPS to access the Management Platform** on the **Notification Server Configuration** page in SIM
- The Symantec Management Agents are automatically configured to use HTTPS when they receive the **Cloud-enabled Management Settings** policy.



# Steps to Prepare the SMP Environment for CeM

## 2. Create/Configure your Site Servers to use HTTPS.

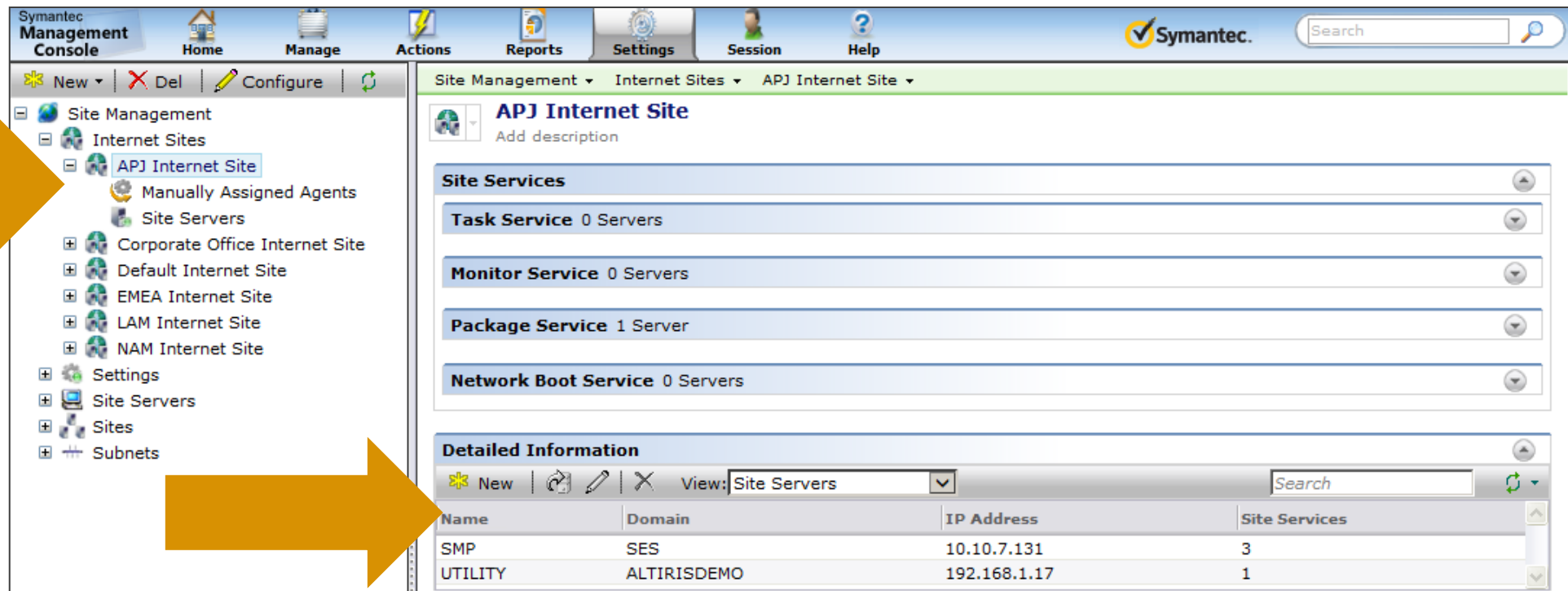
- To serve Cloud-enabled agents, site servers have to be configured to use HTTPS.
- This process is automated by the **Cloud-enabled Management Site Server Settings** policy.
- By default, this policy does not overwrite the existing HTTPS binding on the specified port



# Steps to Prepare the SMP Environment for CeM

## 3. Assign Site Servers to Internet Sites

- The Cloud-enabled agents that are behind the Internet gateway use **Internet sites**
- Add your site servers to the predefined **Default Internet Site** or other Internet sites that you create.



The screenshot displays the Symantec Management Console interface. The left sidebar shows the 'Internet Sites' tree with 'APJ Internet Site' selected. The main pane shows the 'APJ Internet Site' details, including 'Site Services' and 'Detailed Information'.

**Site Services**

Service	Servers
Task Service	0 Servers
Monitor Service	0 Servers
Package Service	1 Server
Network Boot Service	0 Servers

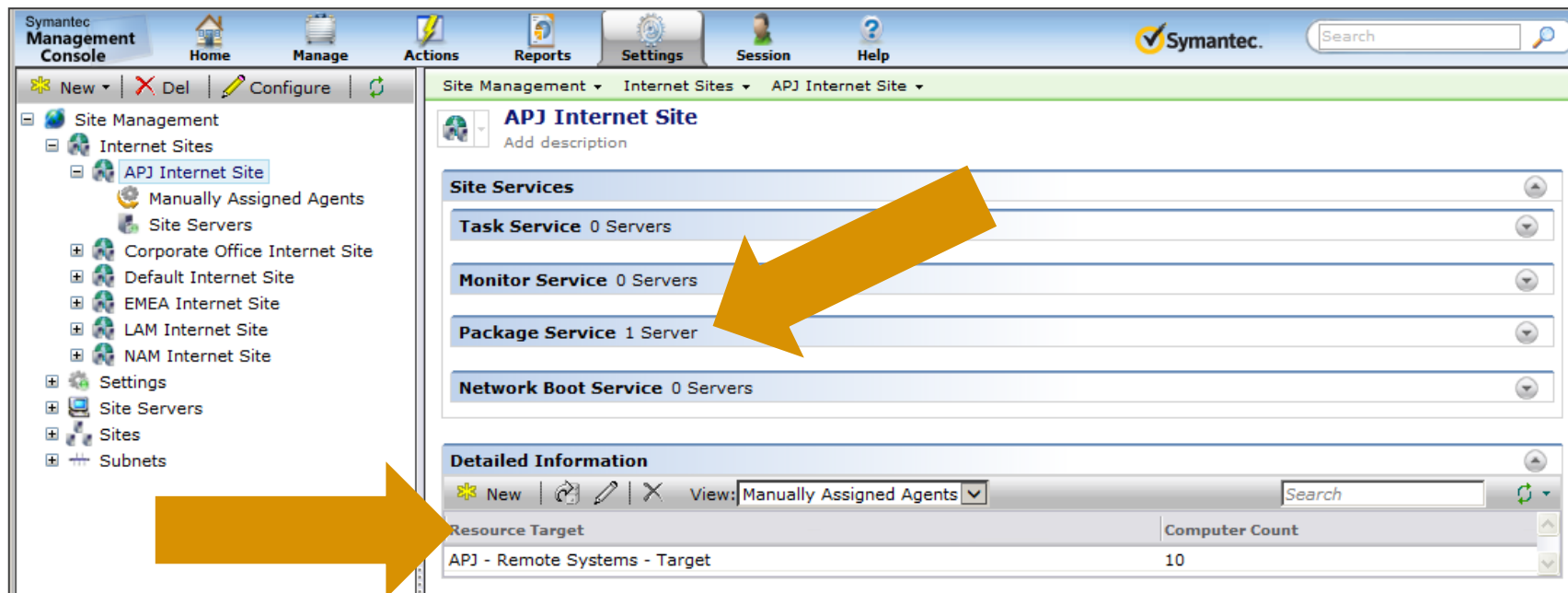
**Detailed Information**

Name	Domain	IP Address	Site Services
SMP	SES	10.10.7.131	3
UTILITY	ALTIRISDEMO	192.168.1.17	1

# Steps to Prepare the SMP Environment for CeM

## 4. 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
- Ensure that the settings apply to the appropriate resource target.





# Implementing the Cloud Enabled Infrastructure

# Implementing CeM in the SMP 7.6 Environment



1. Setup the CeM Agent IIS Website
2. Setup Internet Gateway(s)
  - Prepare the IG Server
  - Download & Run the IG Installation
  - Configure the Internet Gateway
3. Enable IG status reporting
4. Configure the CeM Settings Policy.
  - Add Gateway Information



# Setup the Cloud Enabled Management Agent IIS Website

Symantec Management Console

Home Manage Actions Reports Settings Session Help

Cloud-enabled Management

- Policy
  - Cloud-enabled Management Settings
  - Cloud-enabled Management Site Server Settings
- Setup
  - Cloud-enabled Management Agent IIS Website Settings**
  - Cloud-enabled Management Setup

Settings > Notification Server > Cloud-enabled Management > Setup > Cloud-enabled Manage...

### Cloud-enabled Management Agent IIS Website Settings

Add an IIS Website for cloud-enabled management agent connections

When you add this IIS Website for agent connection, you will not be able to delete it or change its name.

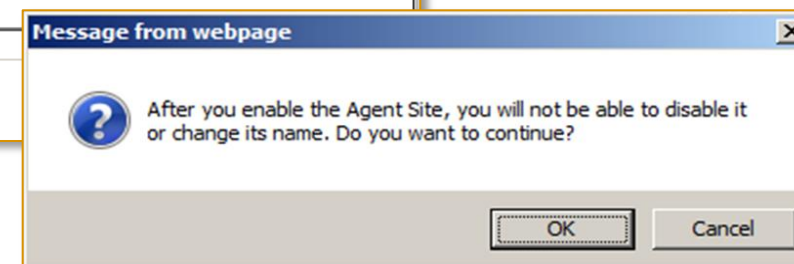
☒ Add IIS Website for cloud-enabled management agent connections:

Name:

Port:

FQDN:

Certificate:



When you return to this page after the CEM agent site is created, the only configuration you will be able to change is the Agent site Port and Certificate.



# Preparing the Internet Gateway Server

- 1. The gateway computer should be located in your organization's demilitarized zone (DMZ)**
  - Ensures that it is protected from both the external and the internal networks.
- 2. The Server must have the Windows Server 2008 R2 SP1 or Windows Server 2012 R2 operating system with the .NET Framework 4.5.1 feature enabled.**
- 3. Configure the Internet Gateway firewall:**
  - Allow incoming connections from the Internet only to the appropriate gateway ports.
  - Allow outgoing connections only to specific servers on your internal network.
- 4. Verify that the IG can access the SMP and any required Site Server computers.**
  - Use the host names or the IP addresses that the Cloud-enabled agents attempt to connect to.
- 5. If the IG is on a VMware virtual machine, you should use the VMXNET 3 network adapter.**
  - VMXNET 3 is available only when you have VMware Tools installed on your virtual machine.
  - See: VMware Knowledge Base article: KB1001805



# Download the Internet Gateway Installation file

The screenshot displays the Symantec Management Console interface. The left sidebar shows a tree view with 'Cloud-enabled Management' expanded, containing 'Policy' and 'Setup'. The 'Setup' folder is further expanded, showing 'Cloud-enabled Management Agent IIS Website Settings' and 'Cloud-enabled Management Setup'. The main content area is titled 'Cloud-enabled Management Setup' and includes tabs for 'Introduction', 'Internet Gateway Setup', and 'Symantec Management Agent Configuration'. The 'Internet Gateway Setup' tab is active, displaying instructions for setting up the Internet gateway computer. A red arrow points from the 'Download the Internet gateway installation package' section to a Windows security warning dialog box at the bottom. The dialog box asks, 'Do you want to run or save SMP\_Internet\_Gateway.msi (6.84 MB) from smp?' and includes a warning icon and the text 'This type of file could harm your computer.' The dialog box has 'Run', 'Save', and 'Cancel' buttons.

Symantec Management Console

Home Manage Actions Reports Settings Session Help

Cloud-enabled Management

- Policy
  - Cloud-enabled Management Settings
  - Cloud-enabled Management Site Server Settings
- Setup
  - Cloud-enabled Management Agent IIS Website Settings
  - Cloud-enabled Management Setup

Settings Notification Server Cloud-enabled Management Setup Cloud-enabled Management Setup

### Cloud-enabled Management Setup

Configure infrastructure to support Cloud-enabled Management

Introduction Internet Gateway Setup Symantec Management Agent Configuration

To set up the Internet gateway computer, you need to perform the following steps:

**Download and run the Internet gateway installation package**

To install a new Internet gateway, you need to download the Internet gateway installation package from the Symantec Management Console.

[Download the Internet gateway installation package](#)

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. The installation wizard guides you through the Internet gateway installation process.

**Configure an SMP 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.

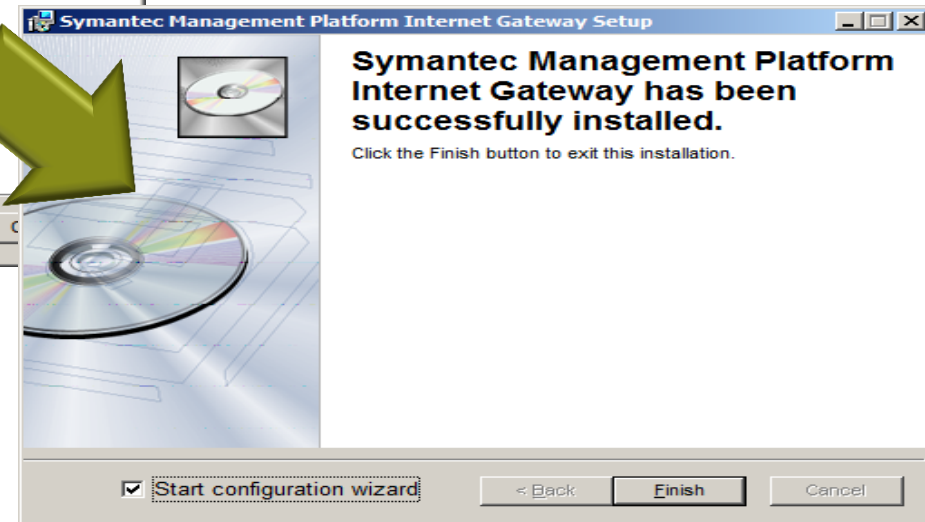
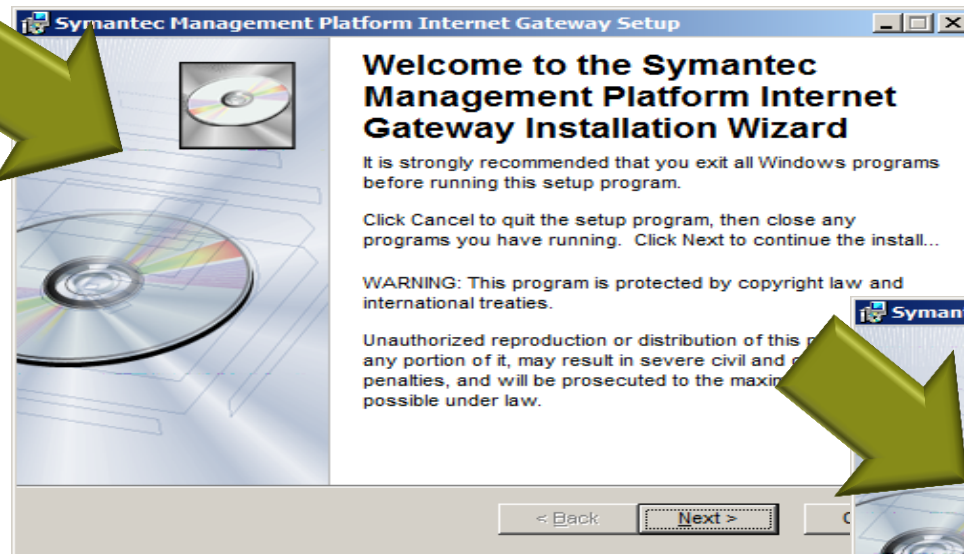
Do you want to run or save **SMP\_Internet\_Gateway.msi** (6.84 MB) from smp?

This type of file could harm your computer.

Run Save Cancel



# Installing the Internet Gateway



# Configuring the Internet Gateway

**Symantec Management Platform Internet Gateway Configuration**

**IP Addresses and Ports**

Symantec SMP Internet Gateway needs a dedicated TCP port for incoming connections from Symantec Management Agents on the Internet. The specified port must not be used by any other software on this computer.

Port for incoming connections:

If your computer has multiple network cards, you can use all of the available IP addresses, or specify a particular IP address to use. It is more secure to use a single IP address.

IP Address

☒ All available

☐ Use IP addresses:

**Symantec Management Platform Internet Gateway Configuration**

**SSL Certificate Information**

Common Name: (FQDN or IP address)

Organization Name:

Organizational Unit Name: (department, division)

Email Address:

Locality Name: (city, district)

State or Province Name: (full name)

Country Name: (two letter code, for example US, UK)

**Symantec Management Platform Internet Gateway Configuration**

**Summary**

Please review the settings before you process the Internet Gateway configuration. If necessary, click "Previous" to modify any settings, or "Cancel" to exit the Wizard. After you have verified that the settings are correct, click "Finish" to begin the configuration.

**IP address and Ports details:**

Port for incoming connections: 443

Use IP addresses: [All available](#)

**Self-signed certificate details:**

Common Name: IG01.ses.local

Organization: Symantec

Organization Unit: symantec@symantec.com

Email Address: symantec@symantec.com

Locality Name: London

Country: US

**Service account details:**

Service account: Default account (NT AUTHORITY\LocalService)

☒ Start services automatically?

**Symantec Management Platform Internet Gateway Configuration**

**User Account**

For security reasons, it is recommended to run the SMP Internet Gateway service as a dedicated user account. The account that you specify will be granted the privileges and the permissions that are required to run the service.

Run SMP Internet Gateway service as:

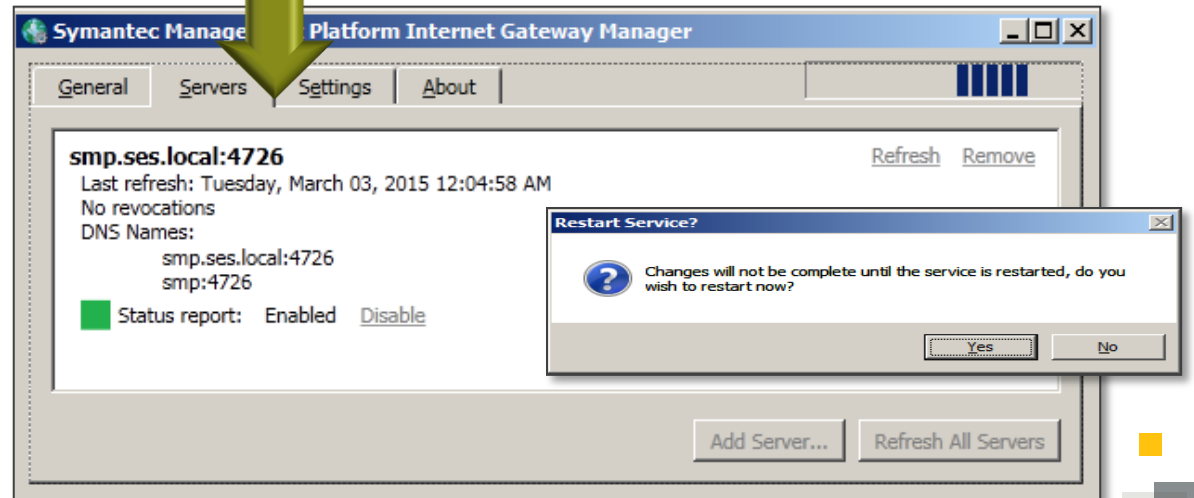
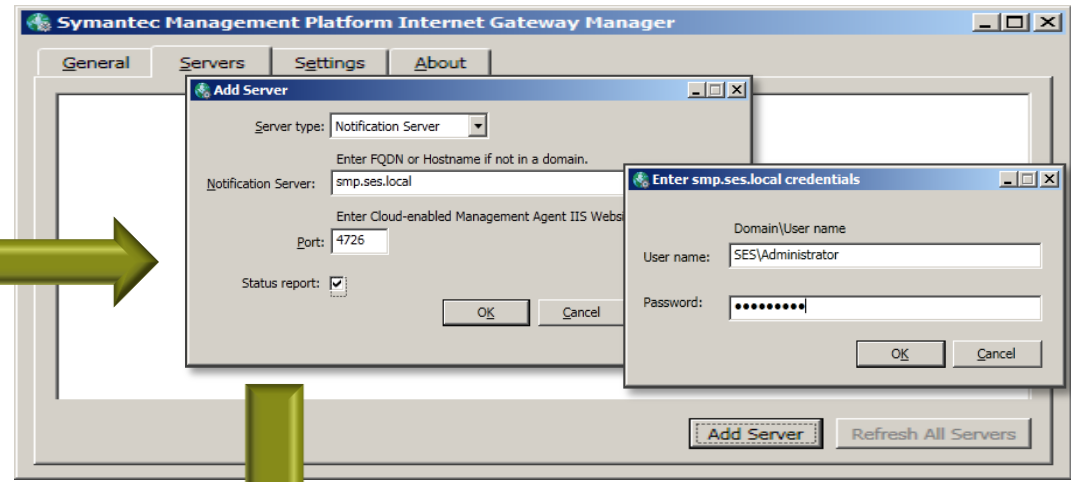
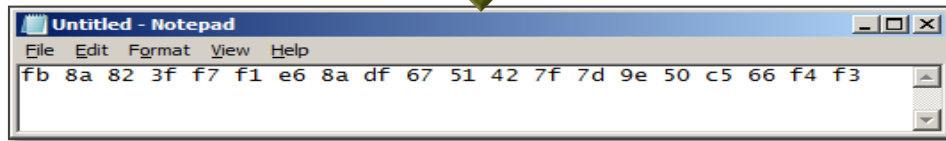
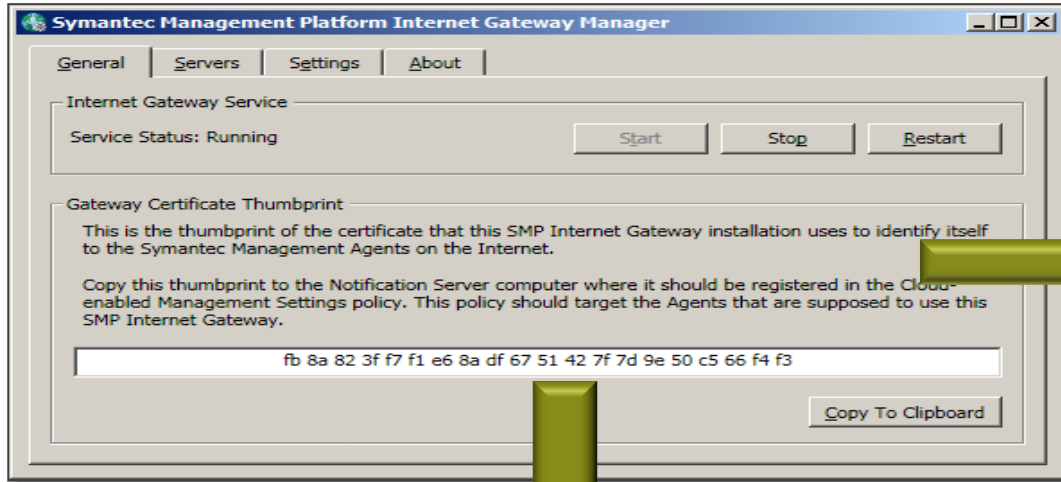
☐ This account:

☒ LocalService account (recommended)

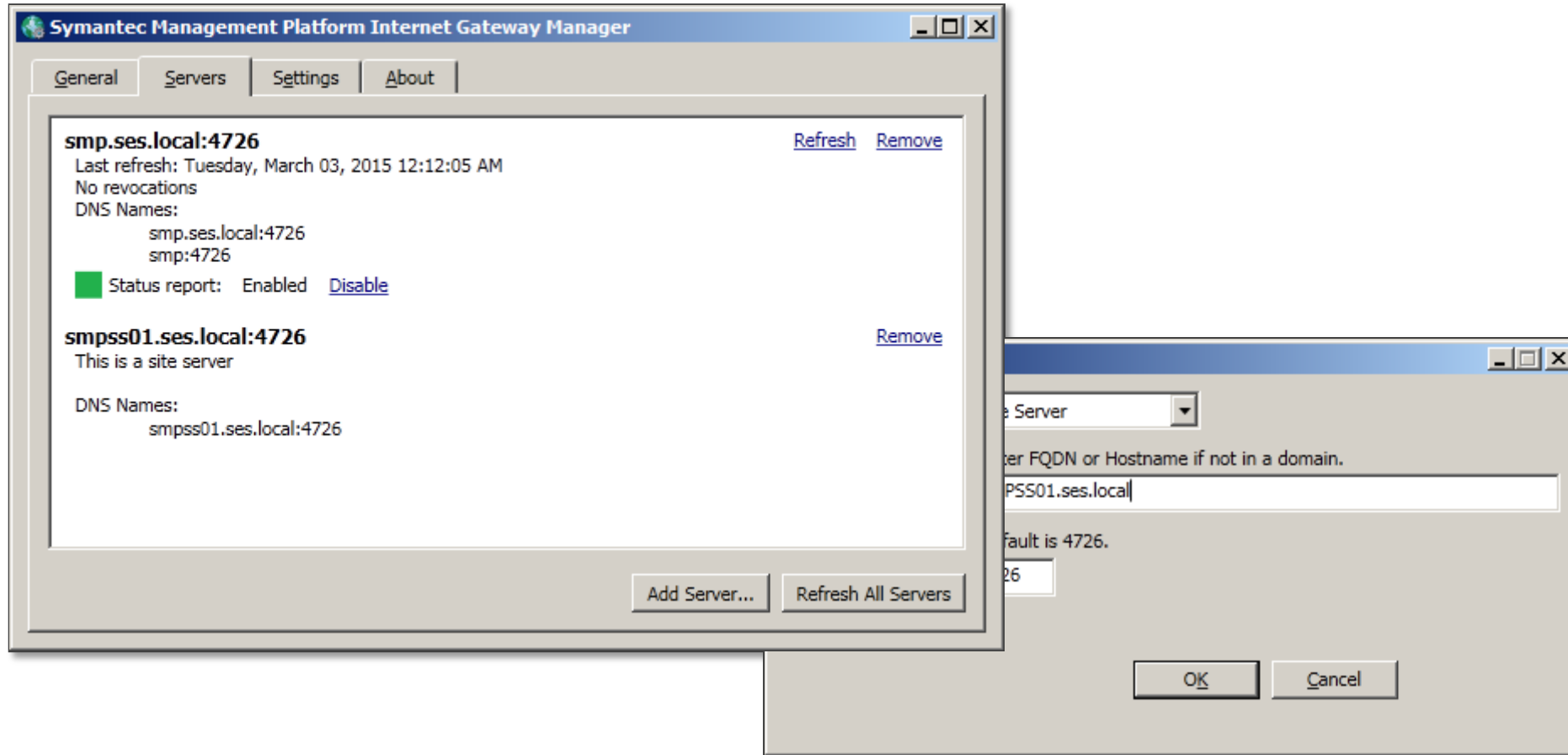
Certificate will be stored at:  
%program files%\Symantec\SMP Internet Gateway\Apache\certs\server.crt



# Configuring the Internet Gateway



# Adding a Site Server to the Internet Gateway

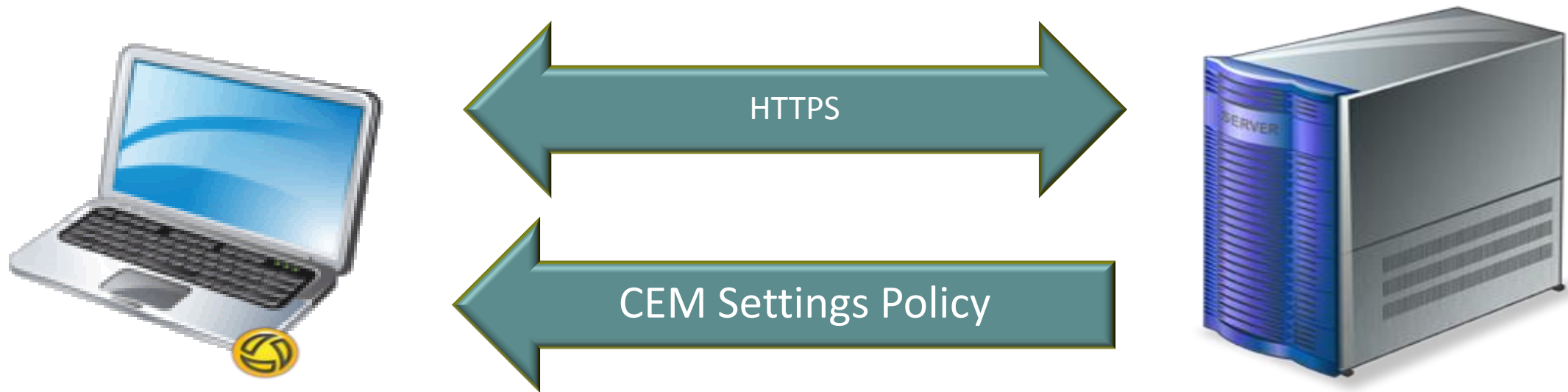




# Enabling Cloud Enabled Management on the Endpoint

# Enabling the Symantec Management Agent's CeM Mode

- CeM mode is enabled when both conditions are met:
  - The Symantec Management Agent has been set to communicate via HTTPS
  - The Agent has received a Cloud-enabled Management Settings policy or Ran the CeM Install Package





# Cloud Enabled Agent Deployment

## Existing Managed Client



### 1. Apply CeM policy

- **Client receives:**
  - Permanent CeM certificate
  - List of Internet Gateways and Authentication

## New Endpoint



1. **Generate CEM Installation Package**
  2. **Install CEM installation Package on computer.**
- **Package includes:**
    - List of Internet Gateways
    - SSL Certificate(s) for the SMP
    - Temporary policy for the Internet Gateway
    - Temporary SMP Cert for CEM agent



# Configuring the Cloud Enabled Management Policy

The screenshot displays the Symantec Management Console interface. The left sidebar shows the navigation tree with 'Cloud-enabled Management' expanded, and 'Policy' > 'Cloud-enabled Management Settings' selected. The main pane shows the 'Cloud-enabled Management Settings' configuration page. The 'Policy - Cloud-enabled Management Settings' is set to 'On'. Under 'Gateways accepting external agent traffic', there is a table with one entry: 'win2008.ses.local' on port '443' with thumbprint '59 98 d5 e2 7a ec 73 0a a9 1e c4 d9 55 7c 33 64 9d da 81 8b'. The 'Add gateway' button is circled in red. Below this is the 'Applied to' section, which shows a table with one entry: 'All computers exclude items not in group CeM Enabled Agents' owned by 'SES\Administrator' with a count of '1' and an apply date of '2/7/2015 12:12:02 PM'. A red arrow points from the 'Add gateway' button to the 'Add Gateway Server' dialog box. The dialog box has fields for 'Server' (set to 'IG01.SES.local'), 'Port' (set to '4726'), and 'Thumbprint' (set to '11 98 d5 e2 7a ec 73 0a a9 1e c4 d9 55 7c 33 64 9d da 81 99').

**Symantec Management Console**

Settings > Notification Server > Cloud-enabled Management > Policy > Cloud-enabled Management Settings

### Cloud-enabled Management Settings

Communication settings for computers managed over Internet

**Policy - Cloud-enabled Management Settings** On

**Gateways accepting external agent traffic**

Add gateway Search

Gateway	Port	Thumbprint
win2008.ses.local	443	59 98 d5 e2 7a ec 73 0a a9 1e c4 d9 55 7c 33 64 9d da 81 8b

**Applied to**

Apply to View: Targets Search

Name	Owner	Count	Apply date
All computers exclude items not in group CeM Enabled Agents	SES\Administrator	1	2/7/2015 12:12:02 PM

Note: All computers where Cloud-enabled Management is not possible are excluded from the target.

Save changes Cancel

### Symantec Management Console

#### Add Gateway Server

Server:

Port:

Thumbprint:

OK Cancel

# Creating the Cloud Enabled Agent Package for Distribution

**Cloud-enabled Agent Installation Package**

Operating System:

Policy (Internet Gateways):

Organizational Group:

Installation name:

Expiry: Date:  Time:  :

**Package installation limits**

☒ Automate certificate distribution

☒ Limit number of agent registrations:

IP mask:

**Package Security**

☐ Sign using

☒ Thumbprint:

☐ File:

☒ Password protect package

Password:

Confirm password:

**Symantec Management Agent Installation Options**

Override the default installation path:

Additional parameters:

Display Symantec Management Agent in the:

☒ Start menu

☒ System tray

☒ Add/Remove Programs list

**Cloud-enabled Agent Installation Package**

**Agent installation parameters:**

Agent installation path: Default

Notification Server URL: Default

Gateways: win2008.ses.local:443

**Warning:**

The Cloud-enabled Agent installation package that you have generated is valid only for a limited period of time. This package expires on:

**Friday, March 20, 2015 11:07:00 PM**

If you use this package to install the Agent after it has expired, the installed Agent is not able to use the SMP Internet gateway for communication. You then have to reinstall the Agent using a newly generated installation package.

**Download package**

Make sure that "Do not save encrypted pages to disk" Internet Explorer advanced security option is switched off, otherwise download will be impossible.

If you use this package to install the Agent after the package has expired, the installed Agent will not be able to use the Internet Gateway for communications. You will need to reinstall the Agent using a newly generated installation package.

**CeMAgentInst all.exe**



# Q&A



# Thank you!

**Tomas Chinchilla**

[Tomas.Chinchilla@Symantec.com](mailto:Tomas.Chinchilla@Symantec.com)

**Brian Sheedy**

[Brian\\_sheedy@symantec.com](mailto:Brian_sheedy@symantec.com)

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo 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 document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.