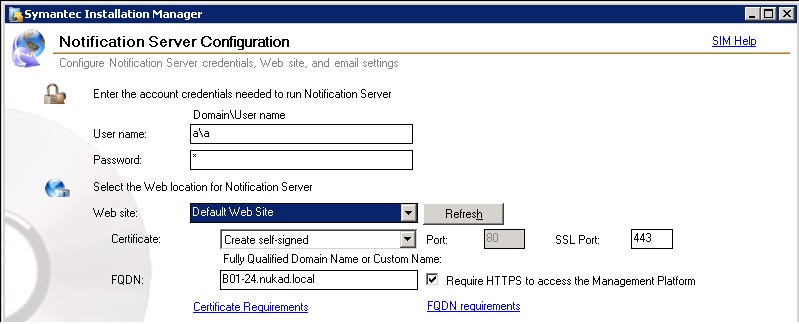
**What is basically required to have SMP 7.5.x CEM functionality working via HTTPs using self-signed or non self-signed certificates in your environment**

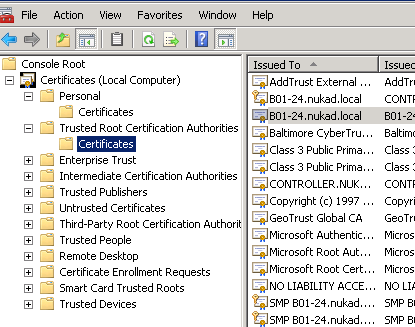
**All steps are created, using SMP 7.5 SP1 release**

* **SMP 7.5.x installation, using self-signed certificate**

If you don't have any 3rd party or internal MS CA certificates available for "*Default Web Site*", then you can choose "*Create a self-signed certificate*" for "*Default Web Site*" and enable "Require HTTPS" option

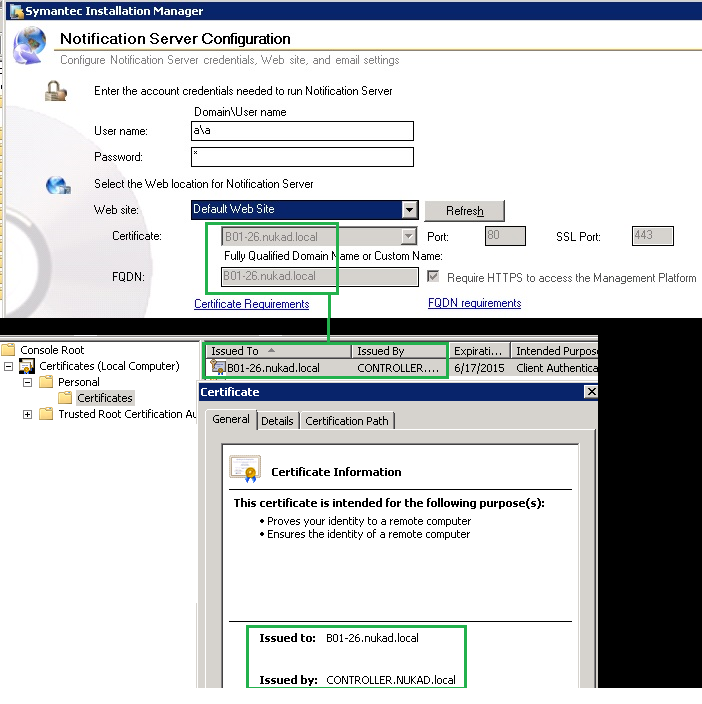
**Note:**

* Make sure that this self-signed certificate is installed in "*Trusted Root Certification Authorities*" on your SMP machine after completed configuration of SMP 7.5.x



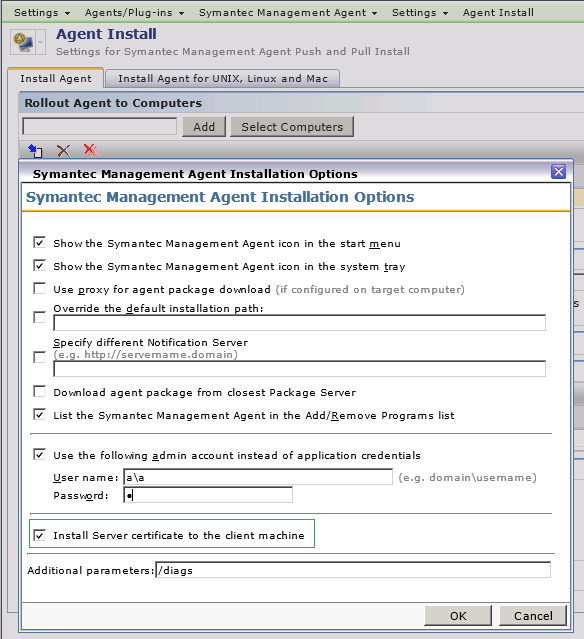
* **SMP 7.5.x installation, using non self-signed certificate**

If you have 3rd party commercial or internal MS CA certificates available for "*Default Web Site*", then you can choose it for "*Default Web Site*" and enable "Require HTTPS" option.



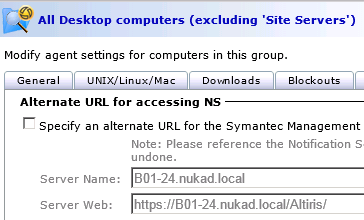
* What certificates can be used for SMP Web Site and for "Symantec Agent" CEM Web Site
* <http://www.symantec.com/docs/DOC7438>
* **Install "Symantec Management Agent" 7.5.x on client machine(s) and on remote server(s), which will be as remote Site Service(s)**

SMP Console, open "**Agent Install**" page ⇒ specify there all required client computers and servers, where "Symantec Management Agent" will be installed. Enable "*Install Server certificate to the client machine*" ⇒ then it will install SMP's server self-signed certificate in "*Trusted Root Certification Authorities*" of each client/server machines to have a successful SSL connection handshake.



Ensure that "SMA Download" link and "Targeted Agent Settings" have SMP HTTPs URL





* **Install remote Site Servers -"Task Server" or "Package Server"**

**1) Self-signed certificates in IIS of Site Servers:**

If you will have remote Site Servers, which will use own self-signed certificate, then make sure that:

* All clients and SMP server have these self-signed certificates installed in "*Trusted Root Certification Authorities*"
* All Site Servers have installed each other self-signed certificates in in "*Trusted Root Certification Authorities*"

= Otherwise, if certificates will be un-trusted between Site Servers - SMP and clients, then client won't be able to establish successful connection to remote Site Servers.

**2) Server Role(s) and features for "Task Server" installation in IIS 7.0 or IIS 7.5**

* <http://www.symantec.com/docs/HOWTO47804>

To install task server on any server operating system, it is required to have following components. If the requirements mentioned below, are not met then task server will not function correctly:

**Prerequisites:**1) IIS is Required  
- Select "Web Management Tools" with all sub-components (IIS 6 Management Compatibility, IIS Management Console, IIS Management Scripting and Tools, IIS Management Service)  
- Select "World Wide Web Services"   
- Select "Microsoft .NET Framework 3.0" (If the option is available)  
- Make sure that ASP.NET and ASP are selected

2) Application Server is required  
- Select "Microsoft .NET Framework 3.5" (If the option is available)  
- Select "IIS Support"  
- If Site server is also going to be used as Mobile Management server, then enable "Message queuing Activation"

3) Firewall (Windows or any other third-party) needs to have provision for inbound/outbound connection allowed on Port 50120, 50121, 50123, 50124. Please note this ports are specifically used for Task server, Symantec Management Platform uses other ports as well for various purposes. For more information, please refer to product user guide.

**Post Configuration:**1) Classic App Pool   
Task doesn't know how to use the new methodology in IIS 7 for the Default App Pool.  Therefore, you will need to direct Task Server to use the Classic App Pool.  There are a number of ways to do this, but the easiest way is actually after the installation of Task on the server.  Once the product is installed, go into IIS, and under Default Web Site\Altiris, select ClientTaskServer.  Edit the Basic Settings and select the Classic App Pool instead of the Default App Pool

**3) Server Role(s) and features for "Package Server" installation in IIS 7.0 or IIS 7.5**

* <http://www.symantec.com/docs/HOWTO47803>
* <http://www.symantec.com/docs/HOWTO63116>

To prepare a Windows 2008 R2 computer with IIS 7.0 for use as a site server

1. In Windows on the Start menu, click **Administrative Tools > Server Manager**.
2. On the Server Manager page, in the left pane click **Roles**.
3. On the Roles page, click **Add Roles**.
4. In the Add Roles Wizard dialog box, check the **Web Server (IIS)** checkbox, and then click **Next**.
5. Under Select Role Services make sure that you check **IIS 6 Compatibility**, **ASP.NET**, **ASP** and **Windows Authentication** Role Services.
6. Click **Next**, and then click **Install**, and after installation is completed, click **Close**.
7. On the Server Manager page, in the left pane click **Features**.

On the Features page, click **Add Features**.

1. In the Select Features dialog box, check the **.Net Framework 3.5** checkbox.
2. Click **Next** and follow the steps in the wizard to completion.

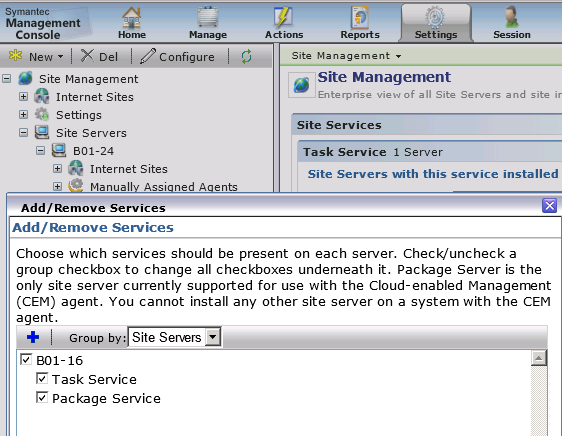
To prepare a Windows 7 computer with IIS 7.0 for use as a site server

1. In Windows on the Start menu, click **Control Panel**.
2. In the Control Panel window click **Programs > Programs and Features**.

In the left pane, click **Turn Windows features on or off**.

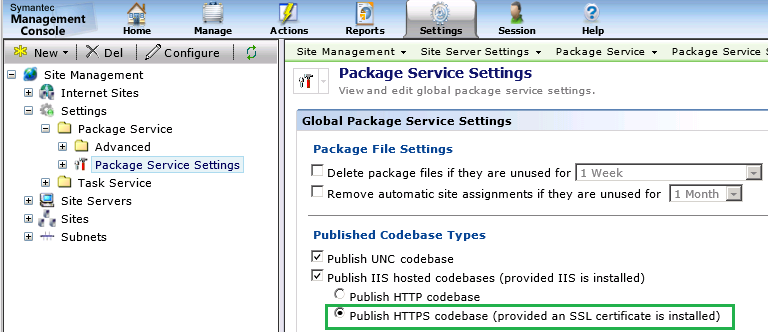
1. In the Windows Features dialog box, check the **Internet Information Services** and **Microsoft .Net Framework 3.5** checkboxes.

**4) When all pre-requisites are installed, then you can add this remote server as Site Server and rollout there Package Server or Task Server.**



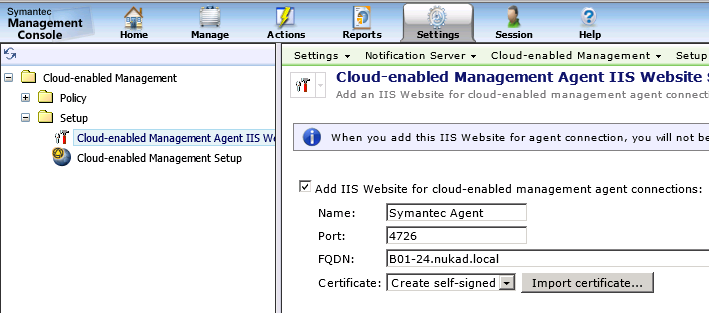
**Note:**

Make sure that you have enabled "HTTPs" codebases publishing for your Package Server(s), because clients, which are in CEM mode will download packages via HTTPs.

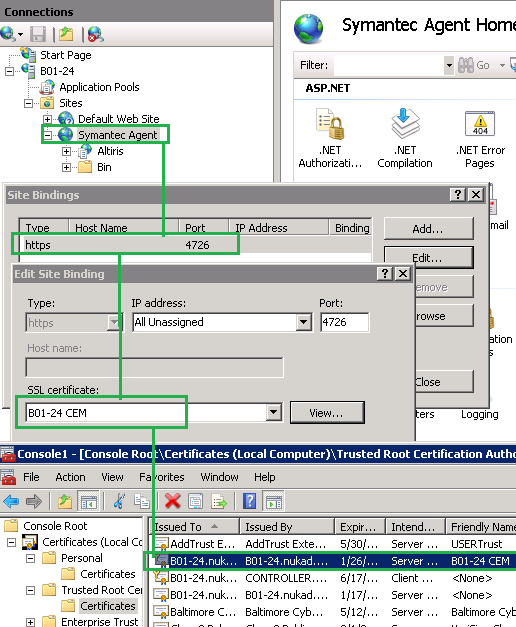
****

**"CEM Symantec Agent Web Site" creation with self-signed certificate**

Open SMP Console ⇒ "*Settings*" ⇒ "*Notification Server*" ⇒ "*Cloud-Enabled Management*" ⇒ create "**Symantec Agent**" web site with "**Create self-signed**" certificate option.

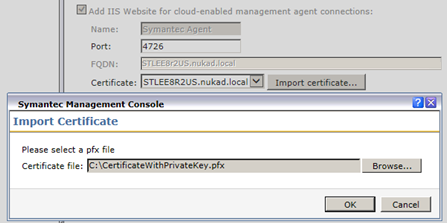


Now there is "**Symantec Agent**" web site with self-signed certificate and **:4726** port binding

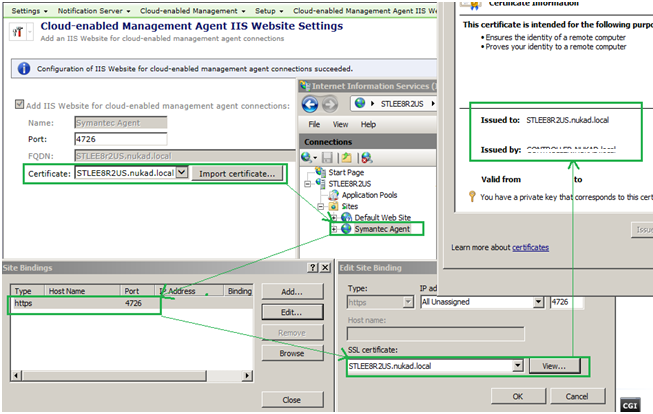


**"CEM Symantec Agent Web Site" creation with non self-signed certificate**

* Click "Add IIS Website for cloud-enabled management agent connection"
* Take .pfx file of your non self-signed certificate and import it -> click "OK" and "Save Changes"

****

* After "Symantec Agent" web site creation and .pfx import, you can check your certificate in IIS

****

**"CEM" SMP Internet Gateway installation**

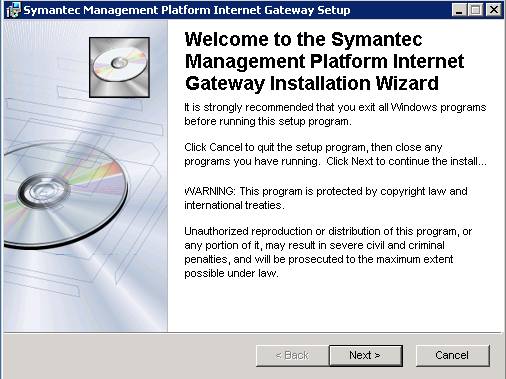
**About "CEM" gateway hardware requirements:**

<http://www.symantec.com/docs/DOC5670> | Chapter 4 - page 61|

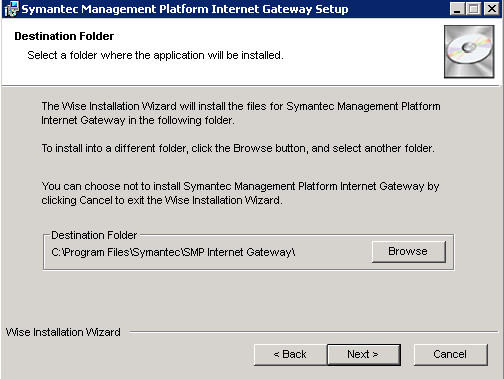
* **Operating System:** Windows 2008 R2 Sp1 with .NET Framework 3.5.1.feature
* **Processor:** Dual Core CPU
* **Disk Capacity:** At least 40GB
* **RAM**: 8 GB

**How to install "CEM" Gateway:**

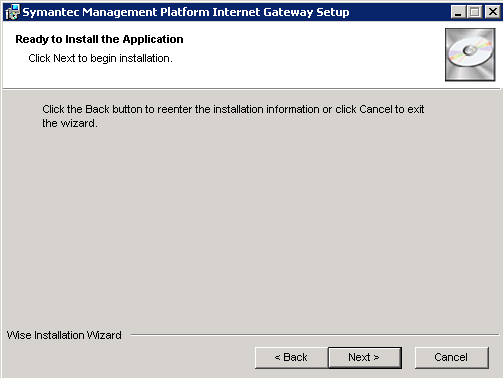
* Download "**SMP\_Internet\_Gateway.msi**" from SMP Server's folder" **\\%SMPServer%\NSCap\bin\Win64\X64\** to remote Windows 2008 R2 SP1 x64 Server
* Begin "**SMP\_Internet\_Gateway.msi"** installation



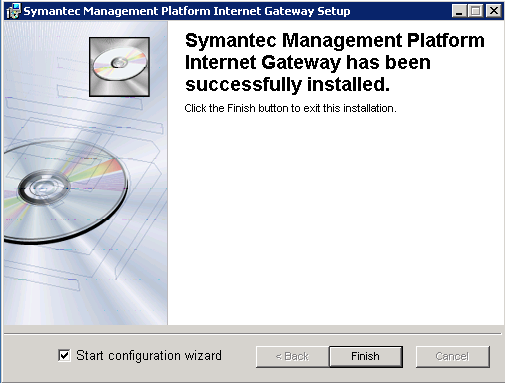
* Choose location where Gateway will be installed



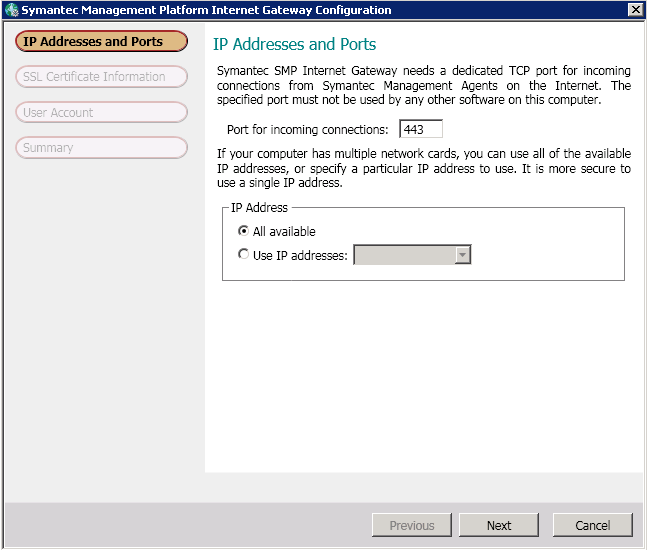
* Proceed with next step



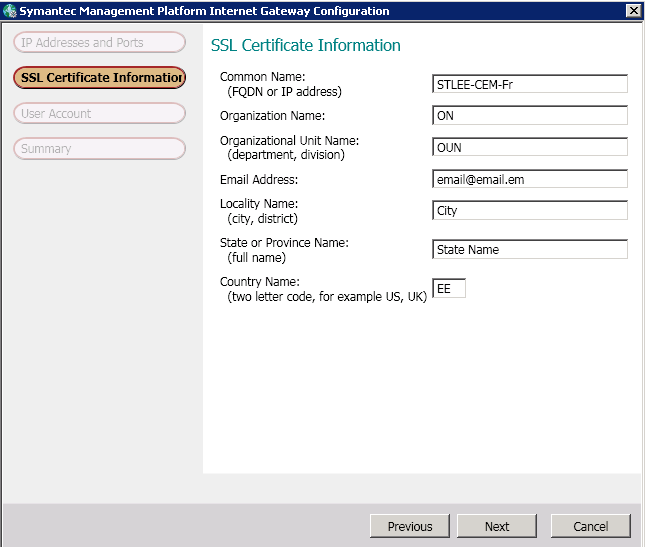
* Start configuration wizard



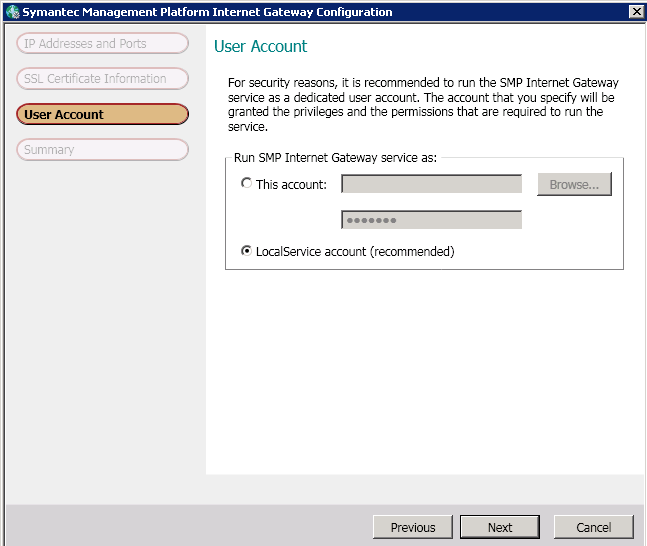
* Specify SSL listening port and IP Address for CEM Gateway

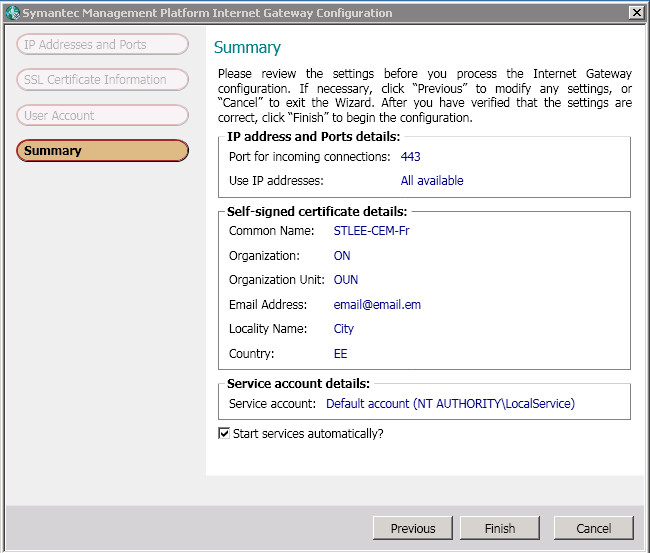


* Specify common name of CEM Gateway server and other fields for self-signed certificate generation

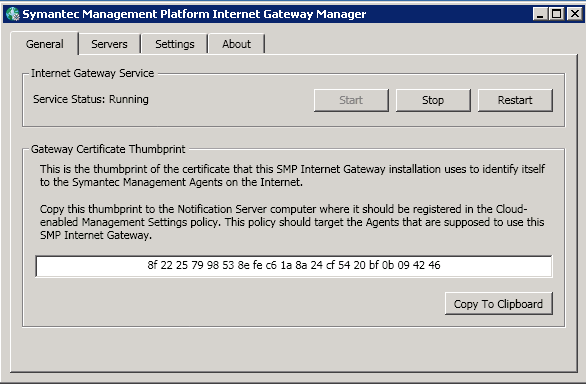


* Complete wizard configuration

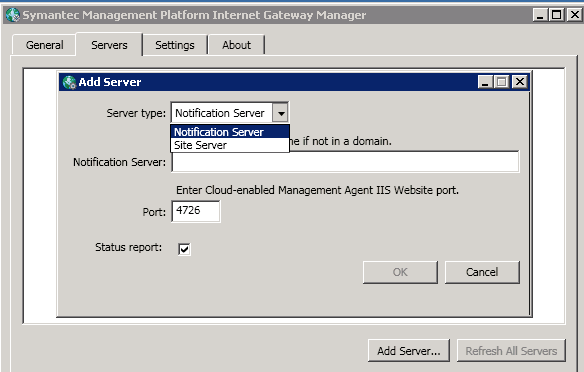




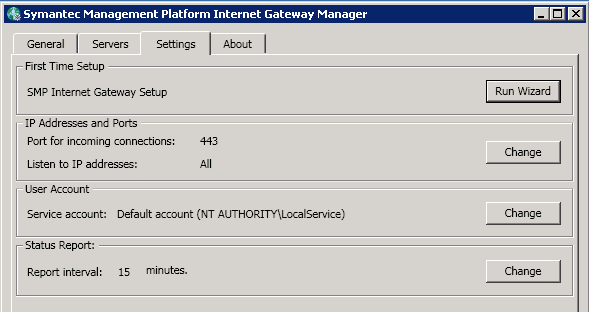
* Now you have installed CEM Gateway and there will be these tabs available in IGM UI



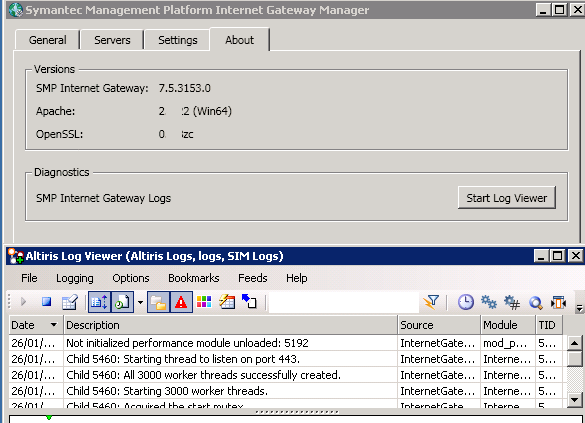
**In "Servers" tab you will add there "SMP Server's Symantec Agent" web site :4726 and other existing remote Site Servers, like Package Server or Task Server :443**



**In "Settings" tab you can change available settings**

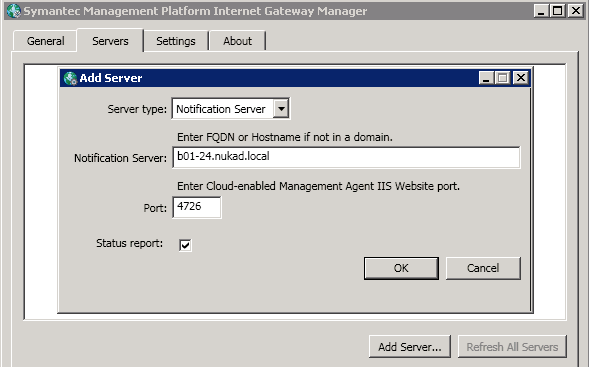


**In "About" tab you can see version of Apace/OpenSSL**



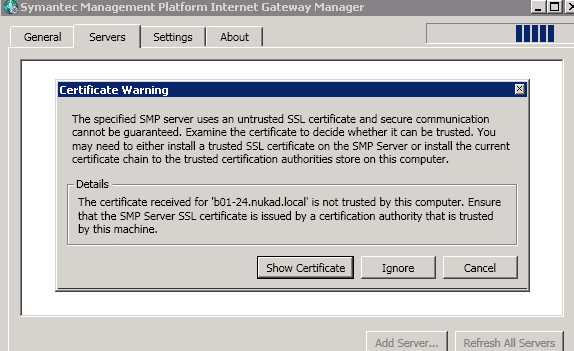
**Adding a "SMP Server" - "Symantec Agent:4726" Web Site in CEM Gateway**

**1.** Specify FQDN/Hostname of your SMP Server, where "Symantec Agent" web site is running on :4726 port and click "OK"



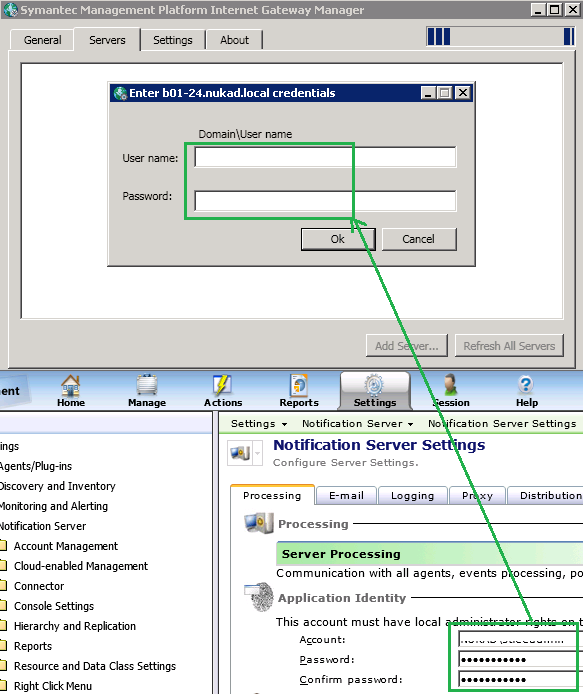
**2.** After that CEM Gateway will throws "Certificate Warning" message (It offers to install self-signed certificate of "Symantec Agent":4726 web site in "*Trusted Root Certification Authorities*" on your CEM Gateway machine.

* Click "Show Certificate" ⇒ click "Install Certificate" ⇒ choose "*Trusted Root Certification Authorities*" for Local Computer ⇒ click "OK" ⇒ After that click on "Ignore" button on "Certificate Warning" message.

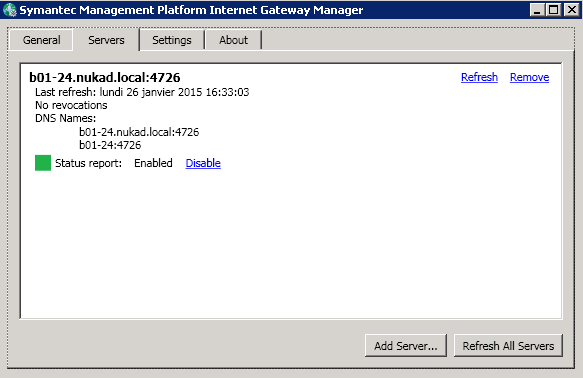


**3.** Then CEM Gateway will offers to specify SMP Server Symantec Administrators account to enable reporting functionality for this SMP.

**Note!** You should use **Symantec Administrator account**, which is "**Application Identity**" account!



**4.** After specifying "**Application Identity**" account, you will have enabled reporting functionality for added SMP Server in CEM Gateway

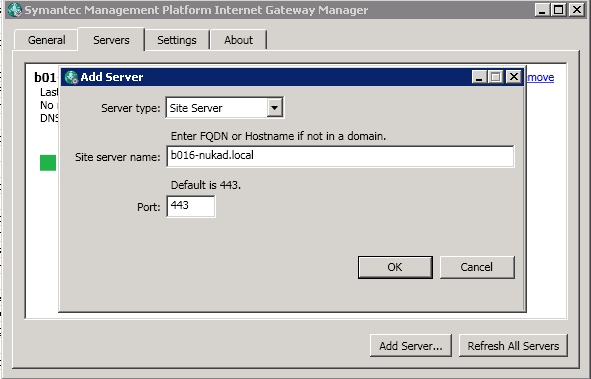


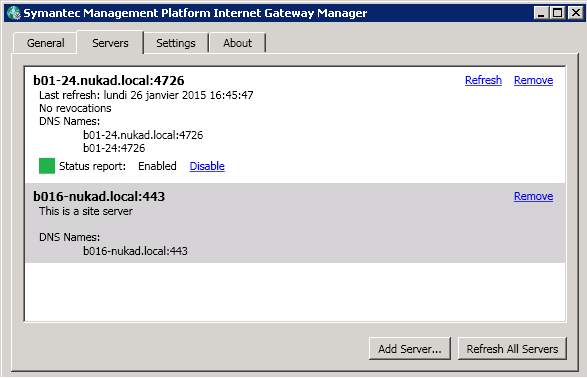
**Adding remote Site Server(s) in CEM Gateway**

When you have determined list of remote Site Servers (Task Server and Package Server) which will serve all your CEM clients, you need to add these Site Servers in CEM Gateway.

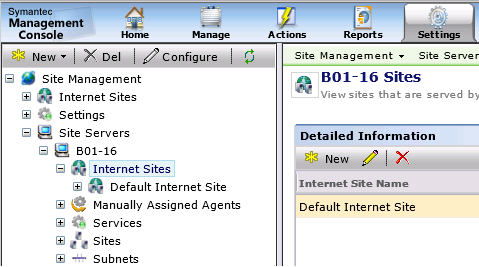
**Note:** If you don't have any remote Site Server(s), then CEM clients will communicate only with SMP Site Server.

**1.** Choose Server type as "Site Server" and specify FQDN/Hostname of your remote Site Server (Package Server or Task Server) in CEM Gateway, using appropriate SSL port, which is bind (by default 443)



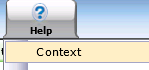
Click "OK" and then added Site Server will be shown in CEM Gateway

When you have added all required Site Servers in CEM Gateway, then you can assign "Default Internet S Site" for this Site Server(s) on Site Server Management Page = otherwise these Site Server(s) now will serve all managed endpoints, which are currently in Internet.

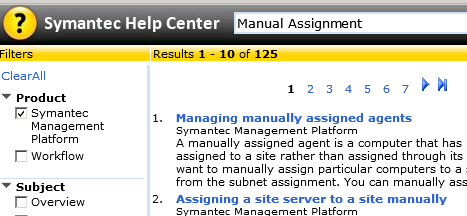


You can read more about Site Assignments per Site Server in SMP Console "Symantec Help Center"

* Open SMP Console -> click "Help" -> "Context"

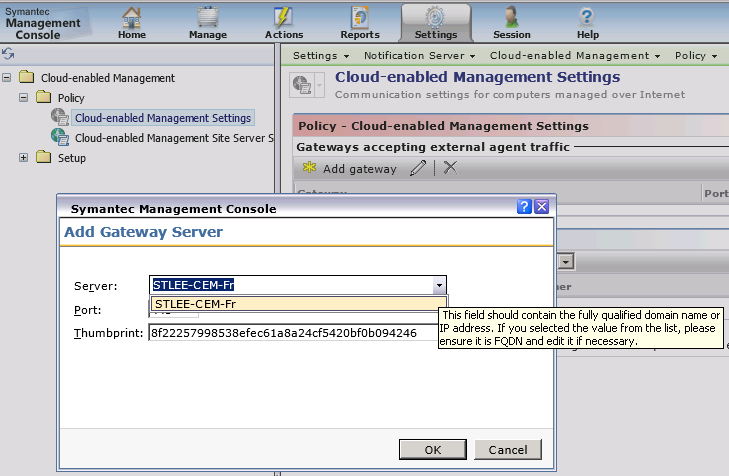


* Then type "Manual Assignment" in search field



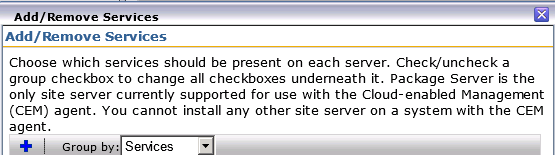
**Adding CEM Gateway in "Cloud-enabled Management Settings" policy on SMP Console**

Open SMP Console ⇒ "Settings" ⇒ "Notification Server" ⇒ "Cloud-enabled Management" ⇒ open "Cloud-enabled Management Settings" policy ⇒ click "Add Gateway" button ⇒ from drop-down menu choose your common name of CEM Gateway and save changes.

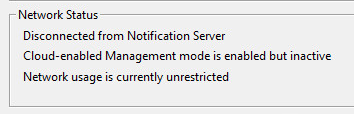


Enable this policy and set appropriate "Resource Target" to deliver this CEM Policy settings to all required managed endpoints, which will be switching from Intranet to Internet.

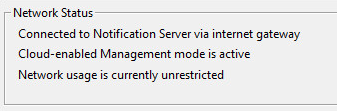
**Note**: Pay attention to do not include unnecessary managed server(s), because if they will have CEM Settings policy applied, then it will be impossible to set them as Task Server.



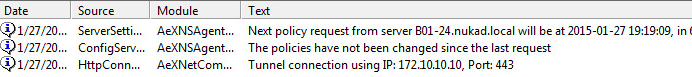
* **Client side when CEM settings policy arrives**
* When managed endpoint will receive "Cloud-enabled Management Settings" policy, then it should show that "CEM" is enabled but inactive, in case if managed endpoint is in Intranet and not in Internet:



* When managed endpoint with "CEM Settings" policy will goes from Intranet to Internet mode, then it should show:



* SMA log output, when it successfully connects via CEM Gateway



Thanks,

IP.