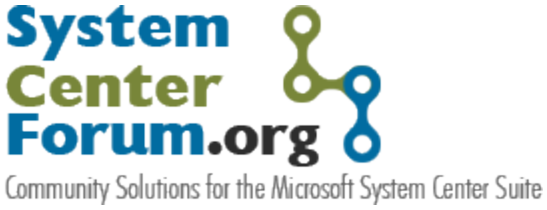


Gateway Server and Certificate-based Authorization Scenarios in Operations Manager 2007

Guidance for deployment of the Gateway Server role and certificate-based authorization for Operations Manager 2007 in a variety of common production scenarios

Authors:
Neale Brown, MCSA(Messaging)
Pete Zerger, MCSE(Messaging) | MCTS (SQL 2005) | MVP-MOM

Version: 1.2
May 2007

Contents

Introduction

The **Gateway Server** role introduced in Operations Manager 2007 allows the Discovery Wizard in Operations Manager to discover target computers in workgroups, across one-way trusted and untrusted domains, and provides communication between the target computer and the Management Server. The security requirements of Operations Manager 2007 also bring PKI into a prominent role in many environments where it is has previously been underutilized or non-existent. In this document we will discuss:

- Function of the Gateway Server role in Operations Manager 2007
- The role of Public Key Infrastructure (PKI) in mutual authentication of Operations Manager components
- Common deployment scenarios for the Gateway Server and certificate-based authorization
- How to utilize certificate-based authorization when Gateway Server deployment is not feasible
- Configuring the Gateway Server for High Availability (failover)

Background on the Gateway Server

We'll begin with a brief explanation of the function of the Gateway Server role in Operations Manager.

There are two primary goals for the gateway server:

1. Minimize the number of points of traffic between two secured environments, (for example, an Intranet and a DMZ)
2. Maximize the use of Kerberos based authentication when it is available, because the TCO associated with Kerberos is lower than with certificates.

To give these objectives context, it is first important to understand Operations Manager introduces a more secure communication model in that *mutual authentication is required* between agent and management server, as well as between Gateway Servers and Management Servers. So how can one achieve mutual authentication between Operations Manager components?

The first option is Kerberos. Mutual authentication can be achieved via Kerberos in trusted scenarios where all machines in the conversation are in the same Active Directory domain or in a domain with a two-way trust relationship with the domain containing the target Management Server. However, in cases where machines outside the trusted environment must be monitored, Kerberos authentication is not possible. In these cases, Operations Manager 2007 can utilize x.509 certificates for mutual authentication in a variety of scenarios. Certificates can be deployed to any Windows operating system that supports an Operations Manager 2007 agent.

As mentioned in the first point, the Gateway facilitates communication between the target agent-managed computers and a Management Server, easing management in untrusted and distributed environments. It may be easiest to think of a Gateway as a management server that simply relays information received from agents to another management server. A gateway is effectively a management server without direct database access. In fact, when you approve a gateway (a process illustrated later in this document), you'll see that it appears as a management server in the Operations Console. Truth be told, our understanding is that the code base for the Gateway Server role is very similar to that of the Management Server.

To ensure high availability, the Gateway Server can be configured for failover to a secondary management server, allowing Gateway communication to continue in the event of a Management Server failure, a configuration which will be addressed in this document.

Finally, it is also important to understand that the Gateway Server itself does not require membership in an Active Directory domain, so it will be appropriate for workgroup and some DMZ environments. However, the Gateway Server role is not a requirement in these scenarios. Alternatively, agent-managed computers can be configured to communicate directly to a management server while authenticating via certificates, a solution for this scenario will be addressed in this document.

A word on PKI and certificates…

While we won't go into the details of PKI, we'll address the concept to the degree necessary to facilitate testing. Links to additional resources on PKI are also available in the **Resources** section near the end of this document.

To issue certificates, a certificate server is required. If your organization does not already have a production Public Key Infrastructure (PKI), one must be deployed through installation of a root certificate authority to issue x.509 certificates for mutual authentication. See "**Installing a Root Certificate Authority**" in this document for instructions on deploying a stand-alone root certificate server.

It is important to note that while Operations Manager release candidate (RC) scenario documents illustrate this concept through configuration of the Management Server as a root certificate authority (CA) it is simply an example. This is not required and not recommended as a production deployment scenario. For sources of additional information on Certificate Services and PKI, see the **Resources** section at the end of this document

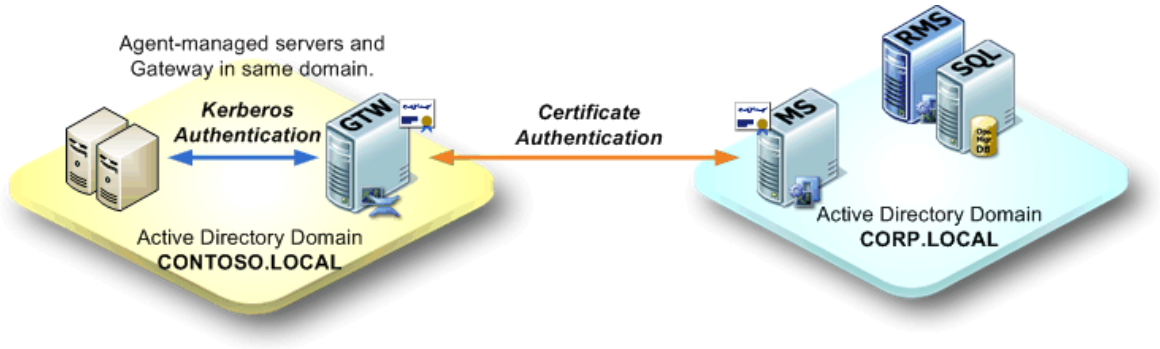
Common Deployment Scenarios

To ensure the concept of when and where certificates are required, see these diagrams of common deployment scenarios.

Gateway with Agent-managed Member Servers

In this scenario, monitoring of a remote, untrusted AD domain is desired. All servers desired for management in the remote domain are members of the same AD domain as the Gateway Server. There is no trust relationship between the two domains. In this scenario, certificate authentication will be required only between the management server and gateway server, as no trust relationship exists. Agent-managed computers in the remote AD domain will be authenticated via Kerberos for communication with the Gateway Server. Thus, certificates must be secured for both the Management Server and Gateway Server in the remote domain.

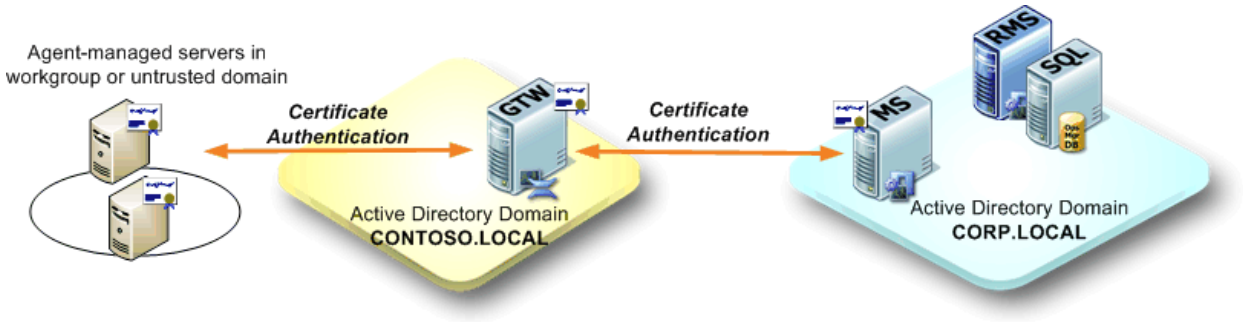
Machines requiring certificates: Management Server, Gateway Server



Gateway with Agent-managed Workgroup Servers

In this scenario, monitoring of a remote, untrusted AD domain is desired. Some servers desired for management by the Gateway Server are members of a workgroup. In this scenario, certificate authentication will be required not only between the management server and gateway server, but also between the Gateway Server and agent-managed computers.

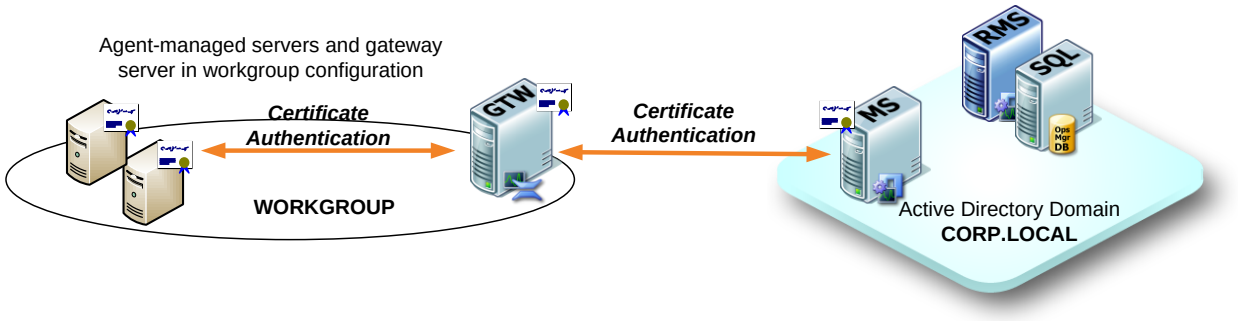
Machines requiring certificates: Management Server, Gateway Server, agent-managed workgroup servers.



Agent-managed Workgroup Servers - Gateway in Workgroup

In this scenario, monitoring of a remote, DMZ or workgroup environment is desired. An additional requirement to minimize the number of points of communication between the isolated environment and the Management Server exists, making deployment of a Gateway Server an appropriate choice. In this scenario, certificate authentication will be required not only between the management server and gateway server, but also between the Gateway Server and agent-managed computers.

Machines requiring certificates: Management Server, Gateway Server, agent-managed workgroup servers.



Agent-managed Workgroup Servers - No Gateway

In this scenario, monitoring of a remote, untrusted workgroup or environment otherwise isolated from any Active Directory domain is desired. However, there is no requirement to minimize points of communication. Additionally, budget constraints dictate meeting the monitoring need with a minimum of expense. In this case, a Gateway Server is not necessary. In this scenario, certificate authentication will be required between the management server and agent-managed workgroup servers, which will authenticate and communicate directly to the management server.

Machines requiring certificates: Management Server, agent-managed workgroup servers.

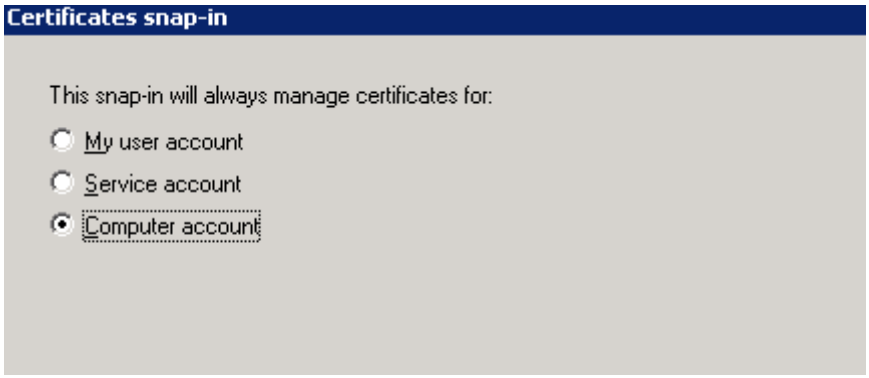
With the background information out of the way, we'll proceed with a detailed walkthrough of the certificate deployment process for Operations Manager Gateway, Management Server and Agent-Managed computers.

Generating Certificates for the Gateway and Management Server

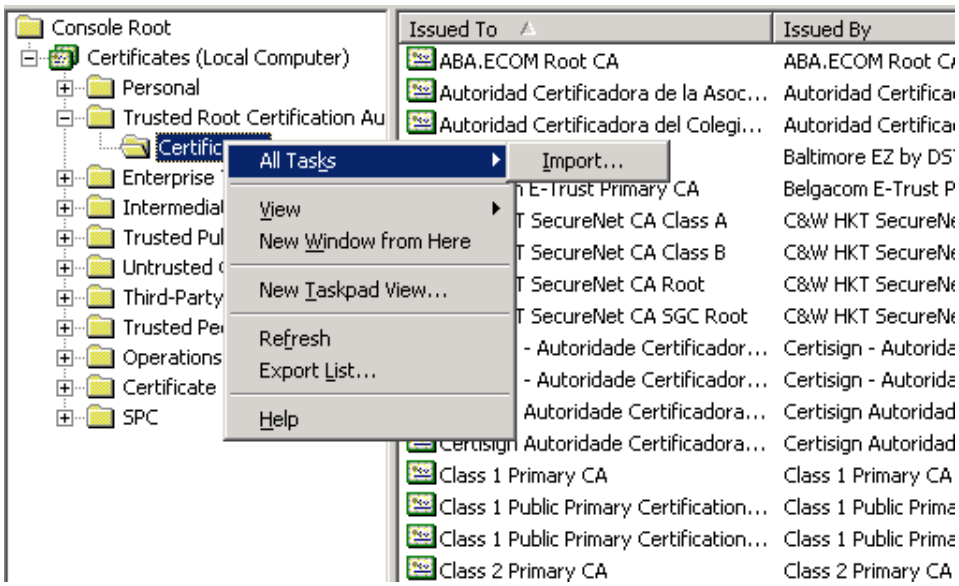
The certificate request and installation steps will completed on both Management and Gateway Servers. You must have a Root Certificate Authority installed and must be able to create an 'Other' certificate using OIDS. If you do not have a Root CA setup, see the section called "**Installing a Root Certificate Authority**" near the end of the document

Step 1: Retrieve and install the Root CA certificate

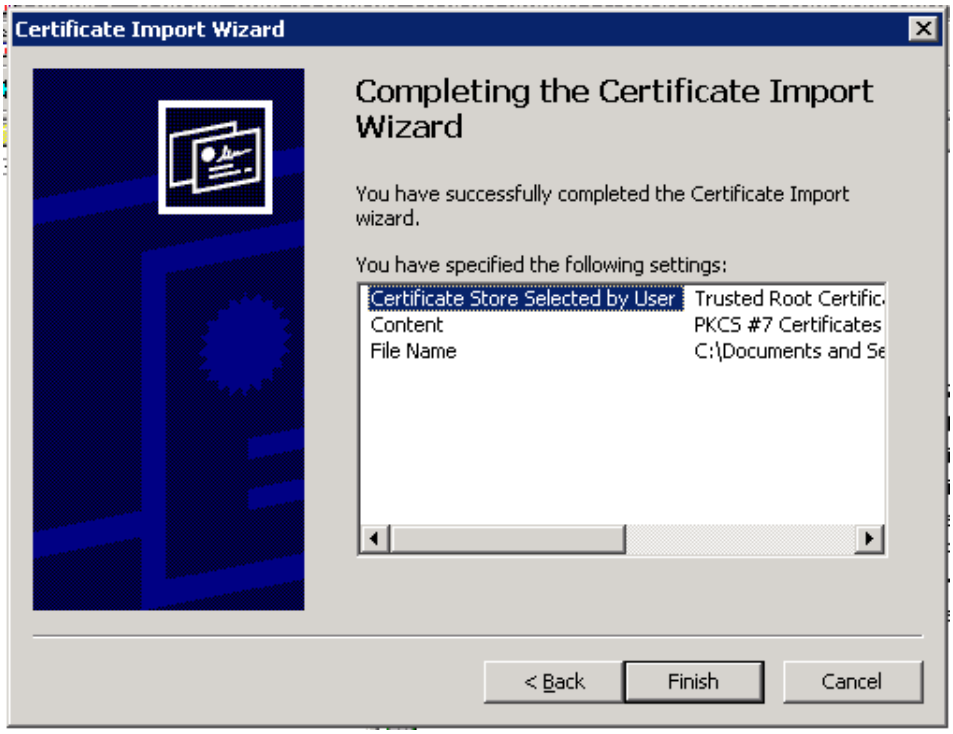
1. From the server desktop , open a web browser and point it to your certificate server *http://<certificateserver>/certsrv*
2. Click the **Download a CA certificate, certificate chain, or CRL** link.
3. Click the **Download CA certificate chain** link.
4. This should initiate a download of a certificate called certnew.p7b which can be saved to the desktop.
5. Once the download is finished, open an **MMC** (Microsoft Management Console) instance by clicking on Star, then Run and type MMC.EXE and click **OK**.
6. Once the MMC console is opened, click **Add/Remove Snap-In**, click **Add**, and then click on **Certificates** located in available Standalone Snap-ins.
7. Once you click **Add**, it will give you three choices and you will need to pick **Computer**. Click **Next**.



8. Then accept the default computer (which is localhost) and click **Finish**. Click **Close** and then click **OK** which should conclude the MMC snap-in configuration.
9. Navigate to **Trusted Root Certificate Authorities**.
10. Right click on Certificates (which is located right under Trusted Root Certificate Authorities) and click **Import**.



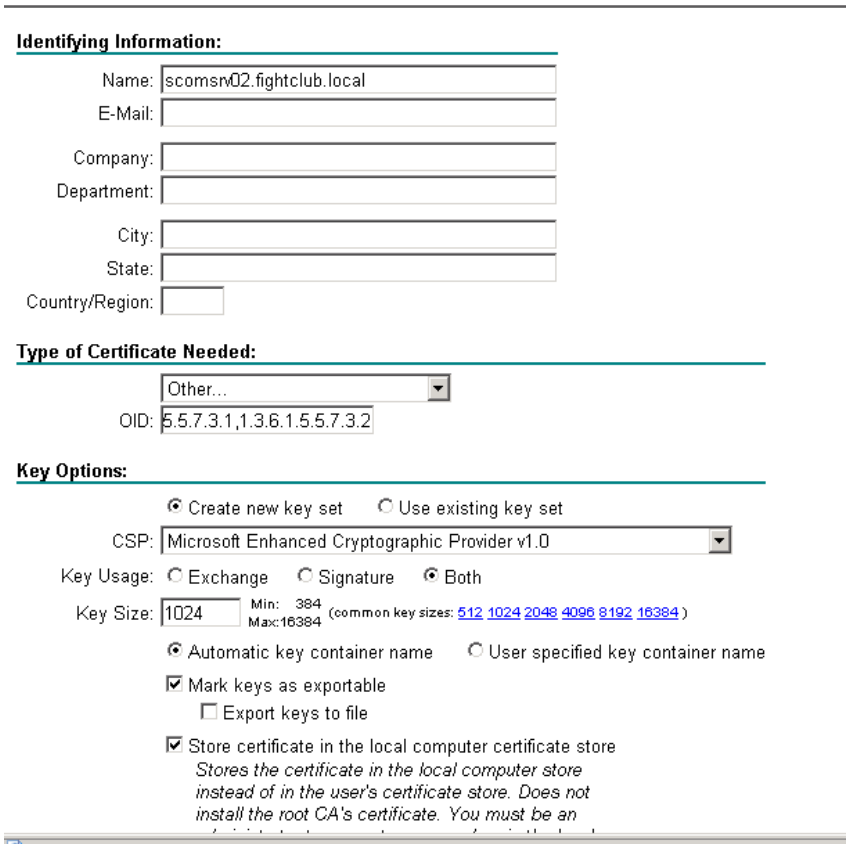
11. Click on **Import** and when prompted click **Next**.
12. At this point you will be prompted for the certificate file, click **Browse**.
13. Change **Files of Type to PKCS #7 Certificates (*.spc,*.p7b)**
14. Click the appropriate certificate file downloaded from the CA (default name is certnew.p7b).



15. Click **Open**, then Click **Next**, Accept defaults and Click **Next**, then Click **Finish**.
16. We have just imported the Root CA that will validate our next certificate.

Step 2: Request and install the proper certificate from the Root CA Server.

1. From the Server Console, open a web browser and point it to your certificate server *http://<certificateserver>/certsrv*
2. Click the **Request a Certificate** link.
3. Click the **advanced certificate request** link.
4. Click **Create and Submit a request to this CA** link.
5. In the **Name** field, enter the FQDN (Fully Qualified Domain Name) of the Operations Manager Server.
6. In the **Type of Certificate Needed** field, select **Other**.
   i. In the **OID** field, enter the following: **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2** (no spaces between the OIDs or around the comma separating OIDs).
7. Click the **Mark keys as exportable** check box.
8. Click the **Store certificate in the local computer certificate store** check box.
9. Enter the FQDN of the Operations Manager Server in the **Friendly Name** field.
10. Click **Submit**.



11. Once the certificate has been approved, you can return to the webpage of your CA server to retrieve the authorized certificate.
12. Click the **View the status of a pending certificate request** link.
13. When you click the proper certificate you will be directed to a new page with the opportunity to install the certificate.

14. Click **Install this Certificate** and click yes to the Security warning dialog.
15. This should finish installing the required certificates for the server.

Configuring the Management Server

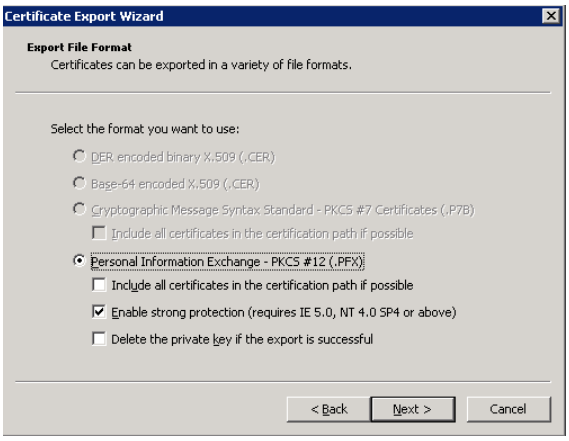
Step 1: Copy the files required to prepare the Management Server for Communication Gateway Server.

1. Copy the MOMCertIMport.exe Tool from the \SupportTools\i386 folder of the Operations Manager 2007 distribution files to anywhere on the local machine.
2. Copy the Gateway Approval Tool from the \SupportTools folder of the Operations Manager 2007 distribution files to the installation folder of the Ops Mgr 2007 installation folder. The name of the executable is Microsoft.EnterpriseManagement.GatewayApprovalTool.exe. In this example, both the MOMCertImport.exe tool and the Exported Certificate will be located on the root of t in this example.

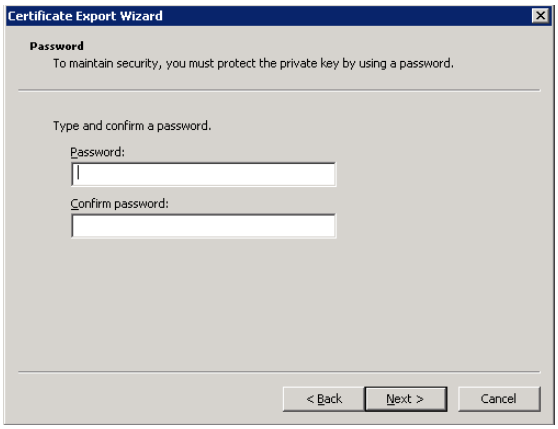
Step 2: Install Certificate on Management Server

Perform the following steps on the Management Server.

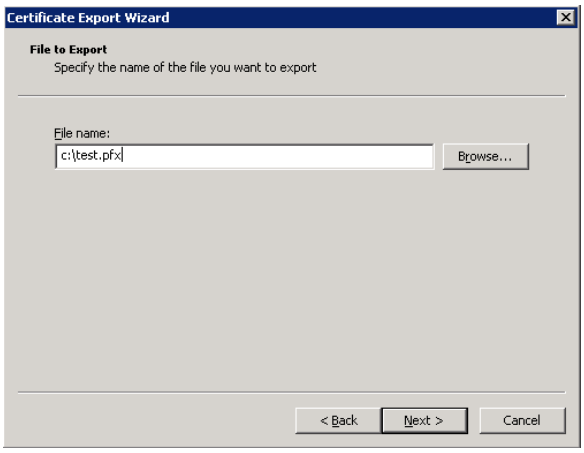
1. To start the process of importing a certificate, open a MMC by clicking the **Start Menu** and then click **Run**. Type **MMC** and press **Enter**.
2. Add Certificates and click **Add**. Click **Computer Account** and then click **Finish**.
3. In the Certificate Tree on the left hand side, click **Personal** and the click **Certificates**.
4. You will see you certificate on the right hand side. Right click on the certificate and click **All Tasks** and then **Export**.
5. A Wizard will prompt you telling you that it is starting the export process, click **Next**.
6. The next step will ask you if you want to export the **Private Key**. In this case, click the selection "**Yes, export the private key**" and click **Next**.
7. The "**Personal Information Exchange – PKCS #12 (.PFX)** is your only export format and be sure "**Delete the private key if the export is successful**" is **not** selected. Click **Next**.



8. The Wizard will prompt you for a password for security purposes. Once you have entered a password, click **Next**.



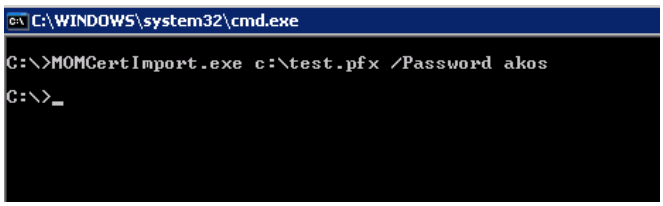
9. The Wizard will prompt you for a location to save the exported certificate. I recommend you save it to the same directory where the **MOMCertImport.exe** tool is located. Once you have entered a location and name click **Nex**t.



10. Verify the information is correct and hit **Finish.**

11. To import the certificate into Operations Manager 2007 we will use the MOMCertImport.exe tool. In this example both the tool and the certificate will be located on the root of the C: drive. The command line arguments are as follows:

Usage: MOMCertImport.exe <Certificate file> [/Password <YourPasswordHere>]
example: MOMCertImport.exe c:\MyCert.pfx
MOMCertImport.exe c:\MyCert.pfx /Password dummypassword
MOMCertImport.exe /SubjectName <Certificate Subject Name>
example: MOMCertImport.exe xyz.domain.net
***Note you will not receive any response after you import the certificate*



NOTE: The MOMCertImport tool basically writes the certificate serial number or hash to the registry so Operations Manager components can easily determine which certificate to present for authentication.

12. Once this completes you will need to restart the Operations Manager 2007 Health Service to load the certificate
    - To restart the Operations Manager 2007 Health Service, click **Start**, then click **Run** and type **services.msc**. Locate the service called **MOM Health Service** and restart the service by clicking the **Restart** icon on the services toolbar.

Step 3: Approve the Gateway Server

Perform the following steps on the Management Server.

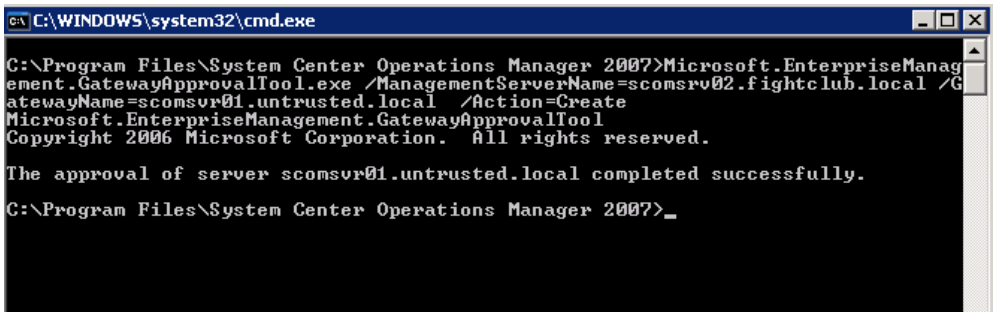
1. Now it is time to use the Gateway Approval Tool to approve our Gateway server in this Operations Manager 2007 environment. As stated before, this utility must be installed as the same directory as the Operations Manager 2007 Management Server installation folder which is usually C:\Program Files\System Center Operations Manager 2007 (as of RC2)

   The syntax of the command is as follows:

   Microsoft.EnterpriseManagement.GatewayApprovalTool.exe /ManagementServerName=<RMS FQDN>
   /GatewayName=<Gateway FQDN> /SiteName=<optional> /Action=<Create|Delete>
   /ManagementServerName = The fully qualified DNS name of the management server
   /GatewayName = The fully qualified DNS name of the gateway server
   /SiteName = Site name of the site gateway management server
   /Action= Create | Delete the gateway server and site

2. Here is the example command line used in this demonstration:

   Microsoft.EnterpriseManagement.GatewayApproval.exe /ManagementServerName scomsvr02.fightclub.local
   /GatewayName=scomsvr01.untrusted.local /Action=Create



3. Once the approval is successful, you can move on to the Gateway Server.

Configuring the Gateway Server

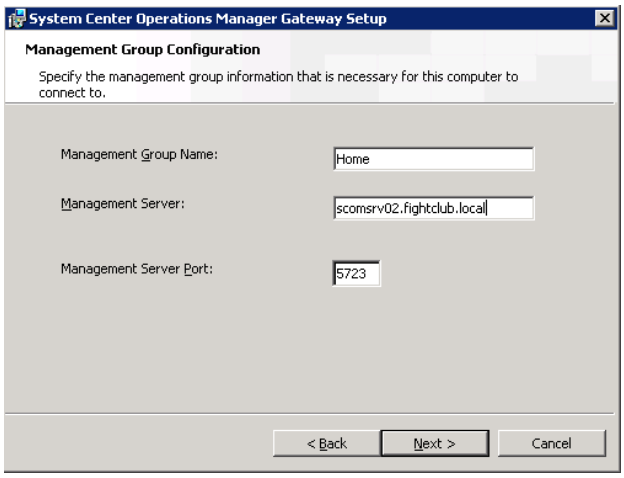
Step 1: Copy the files required to continue the Gateway deployment process.

1. Copy the MOMCertIMport.exe Tool from the \SupportTools\i386 folder of the OpsMgr2007 distribution to anywhere on the local machine.

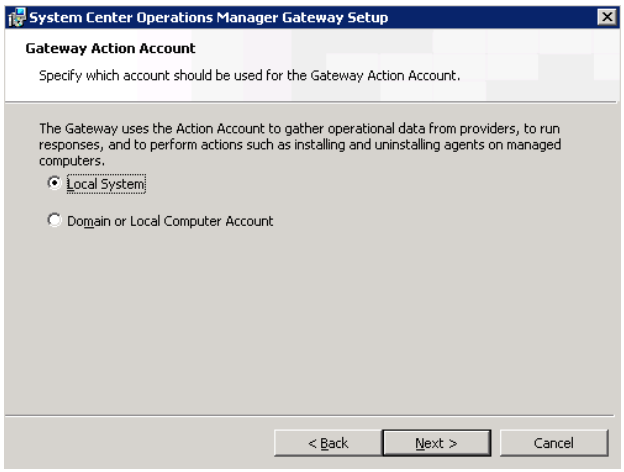
Step 2: Install Operations Manager 2007 Gateway services

1. To start the install process for the Operations Manager 2007 Gateway Service, run MOMGateway.msi in the \Gateway\i386 folder of the OpsMgr2007 distribution on the gateway server.
2. After executing the MSI, you should get a Welcome screen. Click **Next**.
3. Accept default destination folder, click **Next**.
4. The next page is where you enter the Management Group Name, Management Server, and Management Server Port. Click **Next** once you entered the information requested.

   Management Group Name: Enter the Management Group Name from your Operations Manager 2007 Management Server
   Management Server: FQDN of Management Server
   Management Server Port: Keep the default unless you have specifically changed the port.



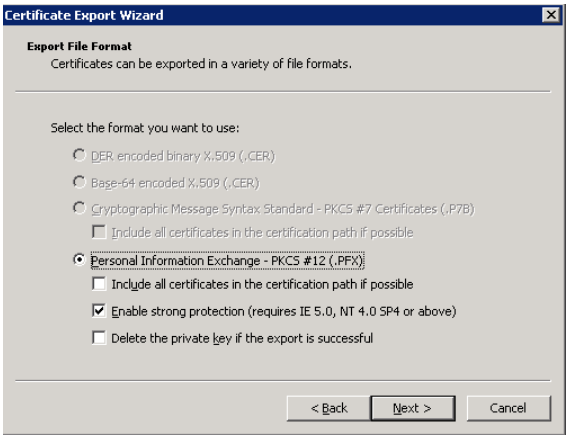
5. Next page will ask you for a Gateway Action Account. If you are unsure, select Local System and click **Next**.



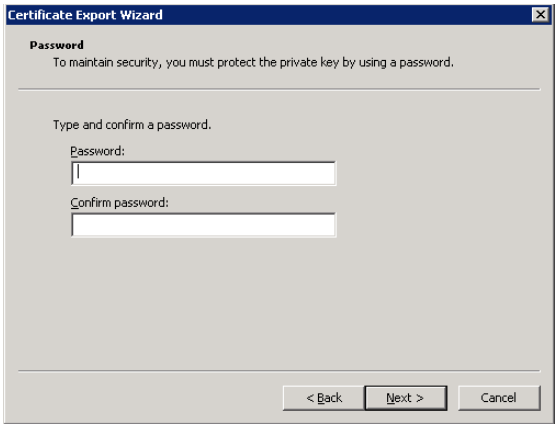
6. At the **Ready to Install** page, click **Install**.
7. When the installation finishes, just click **Complete** to exit the program.

Step 3: Import Certificate into Operations Manager 2007.

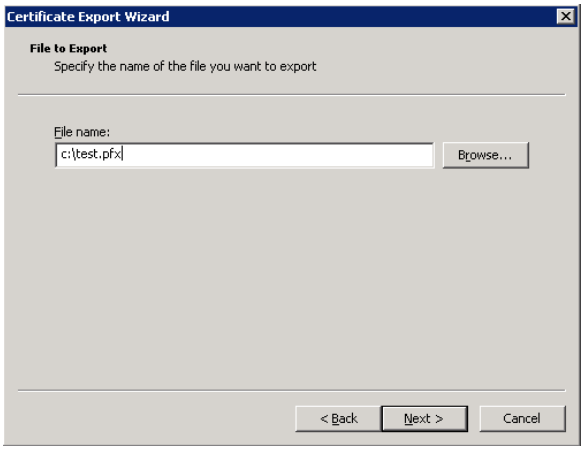
1. To start the process of importing a certificate, open a MMC by clicking the **Start Menu** and then click **Run**. Type **MMC** and press **Enter**.
2. Add Certificates and click **Add**. Click **Computer Account** and then click **Finish**.
3. In the Certificate Tree on the left hand side, click **Personal** and the click **Certificates**.
4. You will see you certificate on the right hand side. Right click on the certificate and click **All Tasks** and then **Export**.
5. A Wizard will prompt you telling you that it is starting the export process, click **Next**.
6. The next step will ask you if you want to export the **Private Key**. In this case, click the selection "**Yes, export the private key**" and click **Next**.
7. The "**Personal Information Exchange – PKCS #12 (.PFX)** is your only export format and be sure "**Delete the private key if the export is successful**" is **not** selected. Click **Next**.



8. The Wizard will prompt you for a password for security purposes. Once you have entered a password, click **Next**.



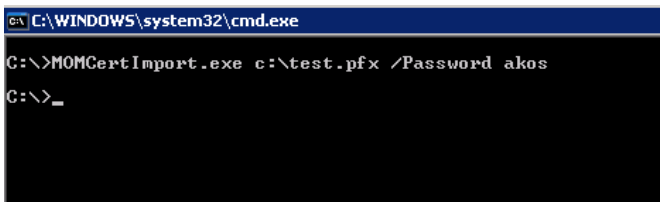
9. The Wizard will prompt you for a location to save the exported certificate. I recommend you save it to the same directory where the **MOMCertImport.exe** tool is located. Once you have entered a location and name click **Nex**t.



10. Verify the information is correct and hit **Finish.**

11. To import the certificate into Operations Manager 2007 we will use the MOMCertImport.exe tool. In this example both the tool and the certificate will be located on the root of the C: drive. The command line arguments are as follows:

Usage: MOMCertImport.exe <Certificate file> [/Password <YourPasswordHere>]
example: MOMCertImport.exe c:\MyCert.pfx
MOMCertImport.exe c:\MyCert.pfx /Password dummypassword
MOMCertImport.exe /SubjectName <Certificate Subject Name>
example: MOMCertImport.exe xyz.domain.net
***Note you will not receive any response after you import the certificate*

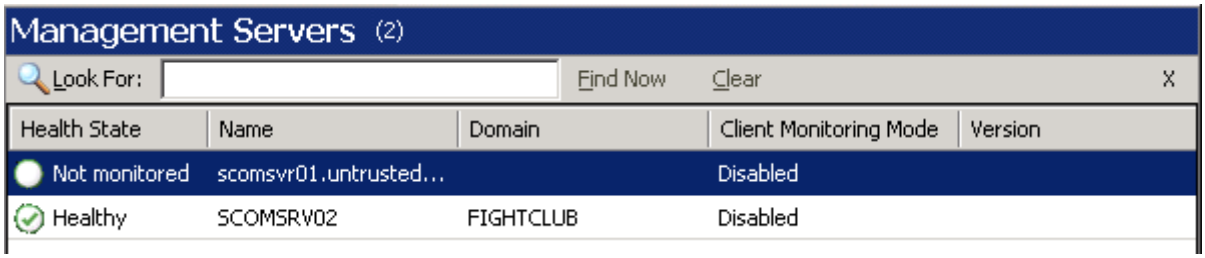


NOTE: The MOMCertImport tool basically writes the certificate serial number or hash to the registry so Operations Manager components can easily determine which certificate to present for authentication.

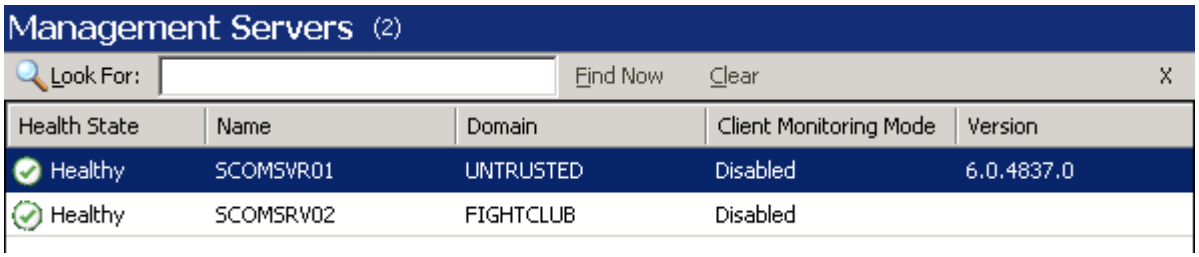
12. Once this completes you will need to restart the Operations Manager 2007 Health Service to load the certificate
    - To restart the Operations Manager 2007 Health Service, click **Start**, then click **Run** and type **services.msc**. Locate the service called **MOM Health Service** and restart the service by clicking the **Restart** icon on the services toolbar.

Gateway Services Verification

Once the Operations Manager Event Log shows that the Gateway Service has received configuration information, the Gateway should show up as another management server.



As you can see here, the Gateway server SCOMSVR01 is approved but has not reported to the Management Server. This could take a while so don't worry if it is reported as 'Not Monitored' at first. After about five minutes, you should see something like this…



At this point, the Gateway server is successfully communicating with the Management Server. You can now install agents on the remote domain and point those agents to the Gateway server. The Management Server should see the agents as manual installation. Since Operations Manager 2007 uses Mutual Authentication for all servers that members of the same domain, what does it use for servers

that are not? Well, in order to get an agent on server that is in Workgroup to communicate with an Operations Manager 2007 Management Server, you will need to use certificates on the Workgroup servers. My next example will show you how to get a Server in workgroup mode to communicate with the Gateway server.

NOTE: By default, an Operations Manager 2007 installation will reject manual installations. You need to change that setting for this to work. It is recommended you change the setting to 'Review new manual installation….". You can change this setting in the **Administration** workspace under **Settings**, and **Server Security**.

Certificate Installation on an Agent-Managed Workgroup Server

There are four basic steps to get this to work and you will essentially repeat the same Certificate request/retrieval process you used in configuring communication between the Management Server and the Gateway Server. Don't worry, now that you have requested/imported the certificate a couple of times, it shouldn't be a problem.

Here are the general steps we will take to configuration the standalone server:

1) Generate and import certificates into OS certificate store
2) Install Operations Manager 2007 agent and configure it to use the Gateway Server as its primary Management Server.
3) Export certificate from the local certificate store and import that into the Operations Manager 2007 application using the MOMCertImport tool.
4) Restart Operations Manager 2007 Health Service and check the console for the manual agent installation approval request.

You can see from this outline that it is nearly the same setup as the Gateway except you are installing the agent.

NOTE: You will need to copy the MOMCertImport.exe Tool from the \SupportTools\i386 folder of the Operations Manager 2007 distribution files to anywhere on the local machine.

Step 1: Importing the certificate.

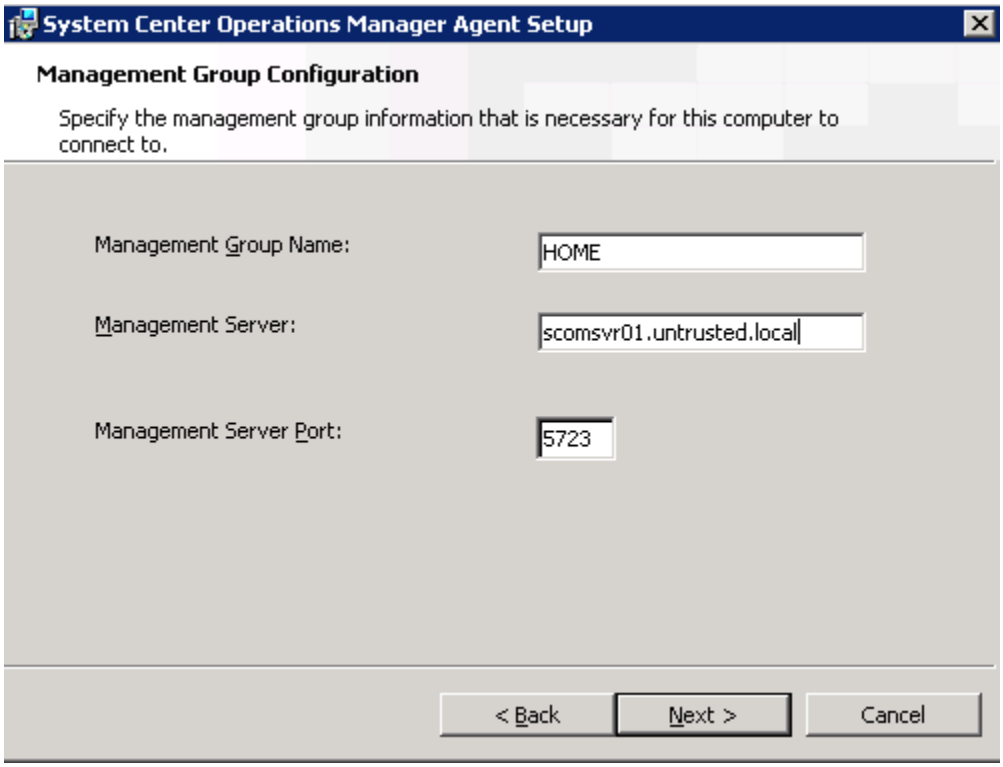
5) This process is exactly the same as the process for the Gateway and RMS server. If you follow the section called "**Step 1: Retrieve and install the Root CA certificate**" and "**Step 2: Request and install the proper certificate from the Root CA Server**", this will install the appropriate certificate required for secure agent communication with the Gateway Server.

Step 2: Agent Installation

Since you are performing a manual installation of the agent, you will need to find the agent setup executable, available in the \Agent\i386 folder in the Ops Mgr 2007 distribution

1. Execute MOMAgent.msi
2. On the **Welcome** screen, click **Next**.
3. It will ask for a folder destination for the software, accept the default and click **Next**.
4. The next page will ask you if you want to configure Management group information, accept the defaults and click **Next**.
5. The setup will now as you for the Management group name, Management Server, and Port. Click next after you have entered the information.
   NOTE: The FQDN of the Gateway Server is specified in the Management Server in the

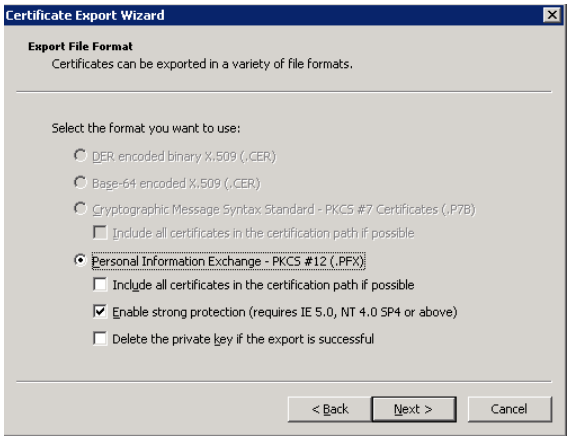
screenshot below.



7. The next step will ask you about your action account. Accept the defaults (**Local System account**) and click **Next**.
8. At this point, you can review all information entered and decide if it is correct. Assuming it is, just click **Install** to start the installation.
9. When it prompts you that it is finished, just click **Finished** to exit installation**.**

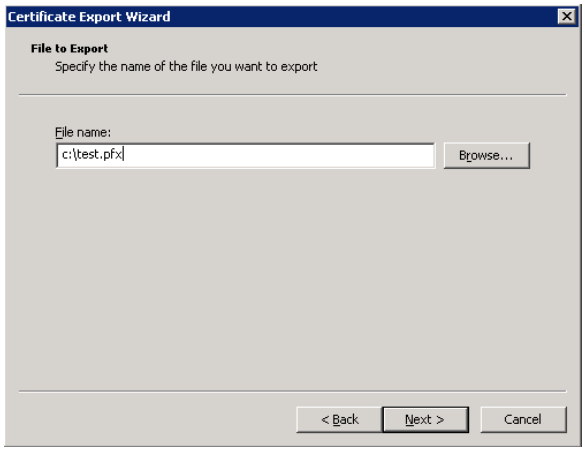
Step 3: Import Certificate into Operations Manager 2007.

1. To start the process of importing a certificate, open a MMC by clicking the **Start Menu** and then click **Run**. Type **MMC** and press **Enter**.
2. Add Certificates and click **Add**. Click **Computer Account** and then click **Finish**.
3. In the Certificate Tree on the left hand side, click **Personal** and the click **Certificates**.
4. You will see you certificate on the right hand side. Right click on the certificate and click **All Tasks** and then **Export**.
5. A Wizard will prompt you telling you that it is starting the export process, click **Next**.
6. The next step will ask you if you want to export the **Private Key**. In this case, click the selection "**Yes, export the private key**" and click **Next**.
7. The "**Personal Information Exchange – PKCS #12 (.PFX)** is your only export format and be sure "**Delete the private key if the export is successful**" is **not** selected. Click **Next**.



8. The Wizard will prompt you for a password for security purposes. Once you have entered a password, click **Next**.

9. The Wizard will prompt you for a location to save the exported certificate. I recommend you save it to the same directory where the **MOMCertImport.exe** tool is located. Once you have entered a location and name click **Nex**t.

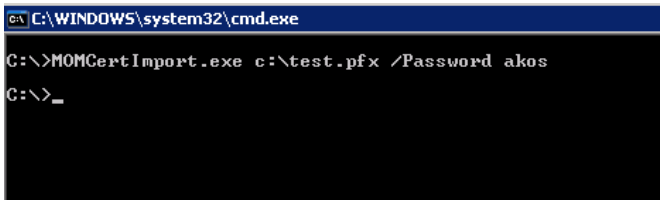


10. Verify the information is correct and hit **Finish.**

11. To import the certificate into Operations Manager 2007 we will use the MOMCertImport.exe tool. In this example both the tool and the certificate will be located on the root of the C: drive. The

command line arguments are as follows:

Usage: MOMCertImport.exe <Certificate file> [/Password <YourPasswordHere>]
example: MOMCertImport.exe c:\MyCert.pfx
MOMCertImport.exe c:\MyCert.pfx /Password dummypassword
MOMCertImport.exe /SubjectName <Certificate Subject Name>
example: MOMCertImport.exe xyz.domain.net
***Note you will not receive any response after you import the certificate*

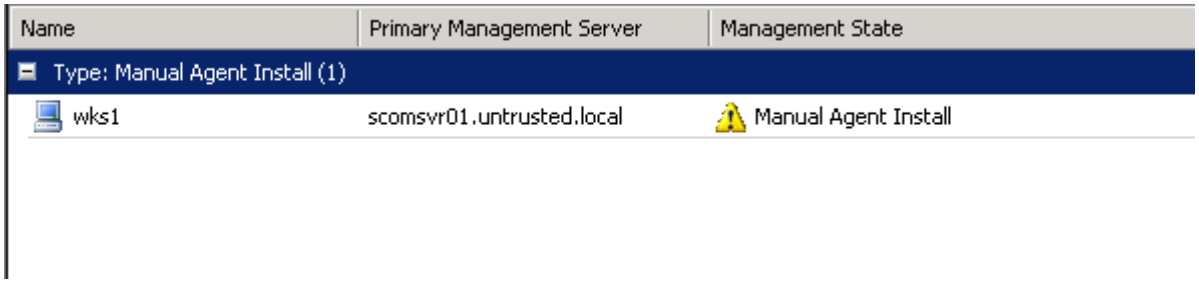


NOTE: The MOMCertImport tool basically writes the certificate serial number or hash to the registry so Operations Manager components can easily determine which certificate to present for authentication.

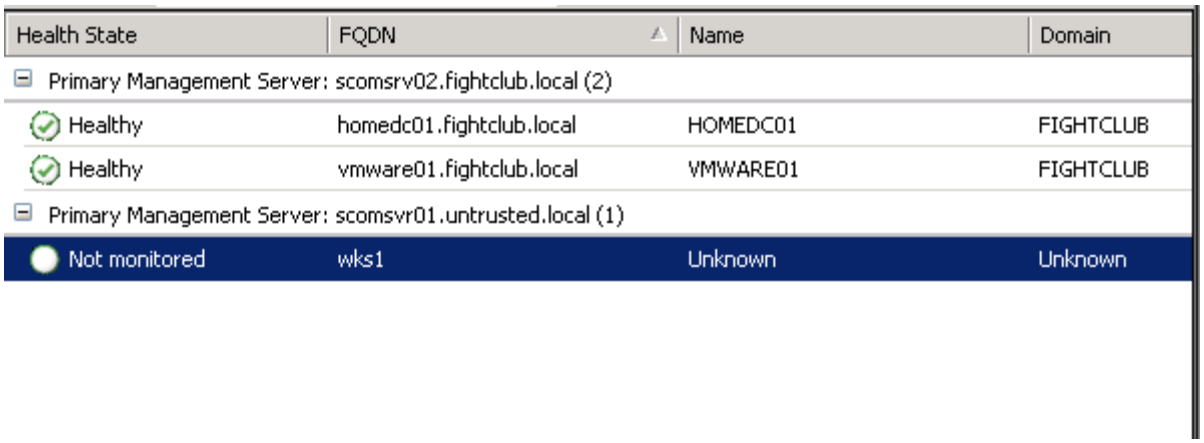
12. Once this completes you will need to restart the Operations Manager 2007 Health Service to load the certificate
    - To restart the Operations Manager 2007 Health Service, click **Start**, then click **Run** and type **services.msc**. Locate the service called **MOM Health Service** and restart the service by clicking the **Restart** icon on the services toolbar.

Agent Installation Verification

The next step is to check whether the Management Server sees a manual installation and requests approval. This should take a little time (maybe five to ten minutes) so don't worry if you don't see it right away.



If you accept the manual installation, then the Agent will show up in the Managed Agents view associated with the Gateway.



Health State	FQDN	Name	Domain
Primary Management Server: scomsrv02.fightclub.local (2)			
Healthy	homedc01.fightclub.local	HOMEDC01	FIGHTCLUB
Healthy	vmware01.fightclub.local	VMWARE01	FIGHTCLUB
Primary Management Server: scomsvr01.untrusted.local (1)			
Not monitored	wks1	Unknown	Unknown

Installing a Root Certificate Authority

This section will give you a step by step on how to install a Root Certificate Authority in your domain. This step-by-step is simply to tell you how to install a certificate server for use with the Gateway scenario.

In my example, the CA services were installed on the Domain Controller. You can install the Root CA anywhere in your domain, but the example below is taking place on a domain controller.

Root CA Installation

1. Login to a domain controller.
2. Go to **Start** -> **Control Panel** - > **Add/Remove Programs** and click "**Add/Remove Windows Components**".
3. Scroll down until you find '**Certificate Services**' and select it. There are sub-options for this service so be sure to select both of the sub options.
4. When you select the component, it will give you a warning. This warning basically tells you not to change the name of the machine or its domain membership. Read the warning and click '**Yes**' to continue. Click **Next**.
5. The wizard should now prompt you for the CA Type. For this scenario, you will want to pick '**Stand-Alone Root CA**'. Click **Nex**t.
6. On this step the wizard is asking you for a '**Common name for this CA**'. You can usually use the NetBIOS or DNS hostname. In this example, it would be DC01. Click **Next**.
7. The next step is database settings. Just accept the defaults and click **Next**.
8. At this point it should install the Certificate Services on the server. To access the services, go to http://<your _server>/certsrv (in this example it would be http://dc01/certsrv).

Approving Certificate Requests

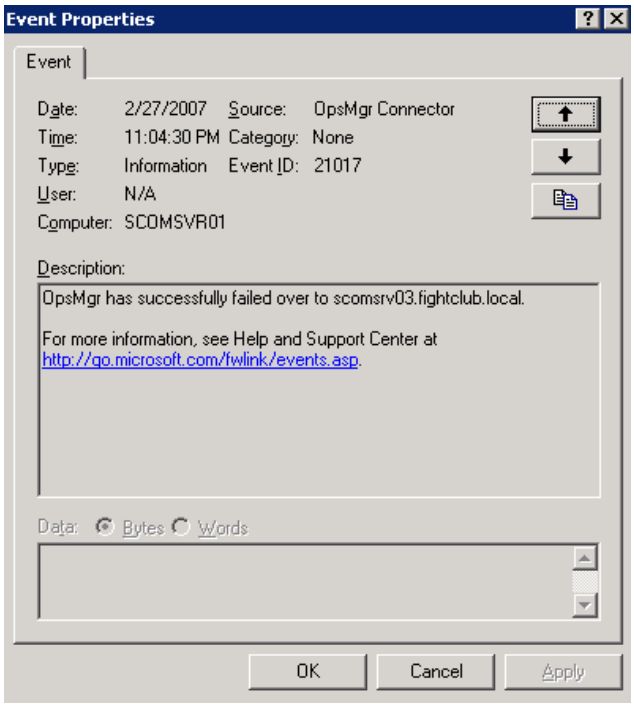
Certificate requests submitted via the web must be approved by an administrator to issue the certificate. For anyone unfamiliar with the certificate approval process, the necessary steps are detailed below.

All of the steps below must be done on the console of the server with the CA or from another machine in the domain.

1. Open a MS Management Console (MMC) from **Start** -> **Run**.
2. Click **File** and **Add/Remove Snap-ins**. Then click **Add**.
3. Add Certificate Authority and click **Add**.
    a. If logged into the CA server: Just accept the defaults and click **Finish**.
    b. From everywhere else: Change the computer scope from Local Computer to the server name of the current Root CA role holder. Our example from the installation is DC01. Click **Finish** when complete.
4. Click **Close** and then click **OK** to return to the MMC console.
5. Expand the Server and then click **Pending Requests.**
6. Find the proper request in the right-hand pane and right-click the request. To activate the request click **Issue** and to deny the request click **Deny**.

Configuring Gateway Scenarios for High Availability

The only way to configure a failover MS for a Gateway is to use the Set-Management Server Operations Manager Shell command. This command is invoked from a Management server and will remotely configure the Gateway server with a failover MS. Currently there is not a command or process to determine if the settings were applied correctly to the Gateway server. To determine the Gateway server received the proper configuration, I disabled the Health Service on the primary MS to cause a failover. An event was logged (see screenshot below) that indicated that Gateway server, did in fact, failover to the correct MS.



Gateway Failover Configuration Steps

1. Logon to a console of a Management Server.

   NOTE: This command can only be run using Powershell.

2. From the **Start Menu**, click **Command Shell** located in the **System Center Operations Manager 2007** program group.
3. At this point we will need to issue the following commands to setup our variables for the failover configuration. Since Powershell is object-oriented, will need to use other Operations Manager 2007 based commands to get the objects we need and assign those objects to variables.

   Set Primary Management Server variable.
   $primaryMS = Get-ManagementServer | where {$_.Name –eq 'scomsrv02.fightclub.local' }

   ```
   >$primaryMS = Get-ManagementServer | where {$_.Name -eq 'scomsrv02.fightclub.local' }
   PS Monitoring:\scomsrv02
   ```

   Set Failover Management Server variable.
   $failoverMS = Get-ManagementServer | where {$_.Name –eq 'scomsrv03.fightclub.local' }

   ```
   >$failoverMS = Get-ManagementServer | where {$_.Name -eq 'scomsrv03.fightclub.local' }
   PS Monitoring:\scomsrv02
   ```

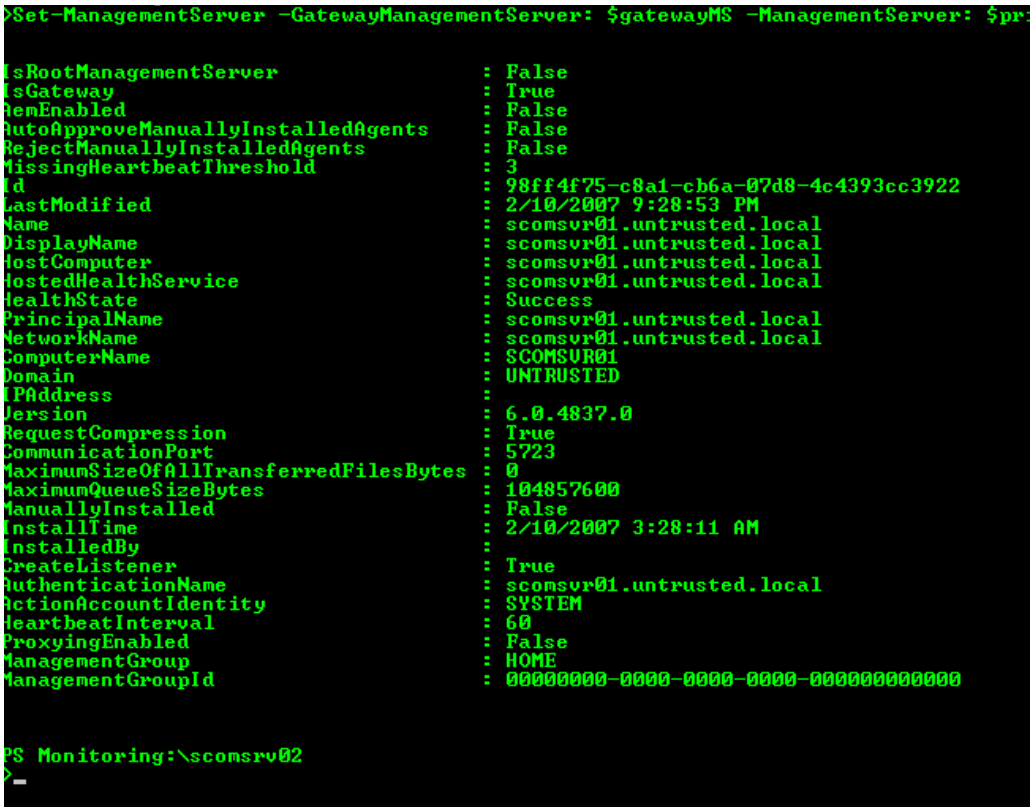
   Set Gateway Management Server variable.
   $gatewayMS = Get-ManagementServer | where {$_.Name –eq 'scomsvr01.untrusted.local' }

   ```
   >$gatewayMS = Get-ManagementServer | where {$_.Name -eq 'scomsvr01.untrusted.local' }
   PS Monitoring:\scomsrv02
   ```

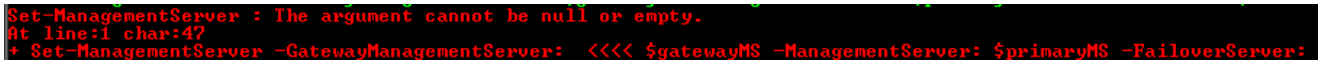
4. Now that the variables have been configured we can construct the command to configure the failover parameters on the remote Gateway server.

   Set-ManagementServer -GatewayManagementServer: $gatewayMS -ManagementServer: $primaryMS -FailoverServer: $failoverMS

5. The output below is the successful result of the **Set-Management** command. It is very similar (if not the same), to the output of the **Get-ManagementServer** command. Configuration of Gateway Server failover is now complete.



Troubleshooting Tip: If you receive an error, Powershell will let you know what caused the error but it can be hard to understand. The screenshot below indicates that the **$gatewayMS** variable does not have the object that the command requires. You need to check the syntax of the command and in this case the FQDN of the gateway was incorrect so the variable filter did not work.



Conclusion

Hopefully this document has clarified some aspects of Gateway Server configuration, certificate deployment and mutual authentication in Operations Manager 2007. Your feedback is always welcome at administrator@systemcenterforum.org.

Resources

For more information on Certificate Services, visit the Certificate Services overview at http://technet2.microsoft.com/WindowsServer/en/library/7d30a7ec-438f-41f8-a33a-f2e89d358b121033.mspx?mfr=true

Pulic Key Infrastructure for Windows 2003 Homepage
http://www.microsoft.com/windowsserver2003/technologies/pki/default.mspx