

Deploying SCOM Gateway server

Brad Hearn

Steps taken

1. Put a change request into the Network group to open TCP ports 5723 and 5724 both ways from the Gateway server to the MS server
2. Certificates need to be deployed (2 types of certificates)
3. The root CA needs to be installed on all management servers
4. A custom cert template needs to be created on the issuing CA for OpsMGR
5. The Custom OpsMgr cert needs to be installed on all management servers
6. Run the momcertimport on all management server after the certs have been installed. This makes some specific registry changes for scom to help pick the correct cert.
7. Approve gateway server on RMS using a approval tool.
8. Manual install of agents on servers to be monitored
9. Approve agents in SCOM console

Open and test ports

Put a change request into the Network group to open TCP ports 5723 and 5724 both ways from the Gateway server to the MS server.

To test if the ports are open. Log on to gateway server. From a command prompt type

Telnet SRVNAME261 5723

If you get a cursor at the top left corner then the port is open. Any other errors indicate that the port is still closed.

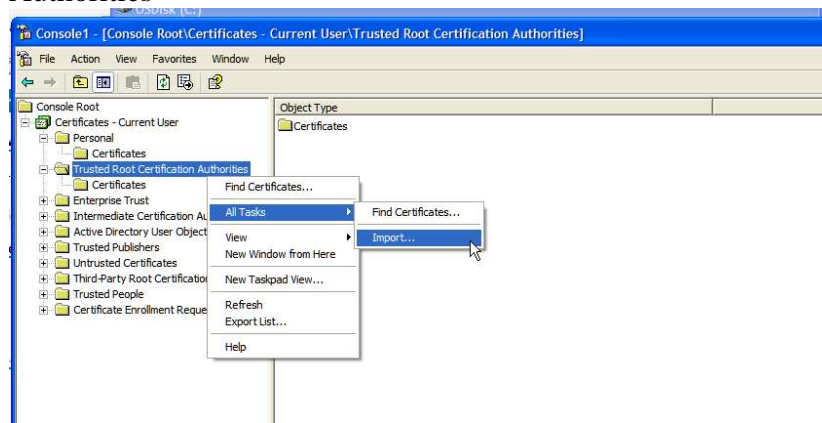
Do the same from the management server back to the gateway server.

Certificates need to be deployed (2 types of certificates)

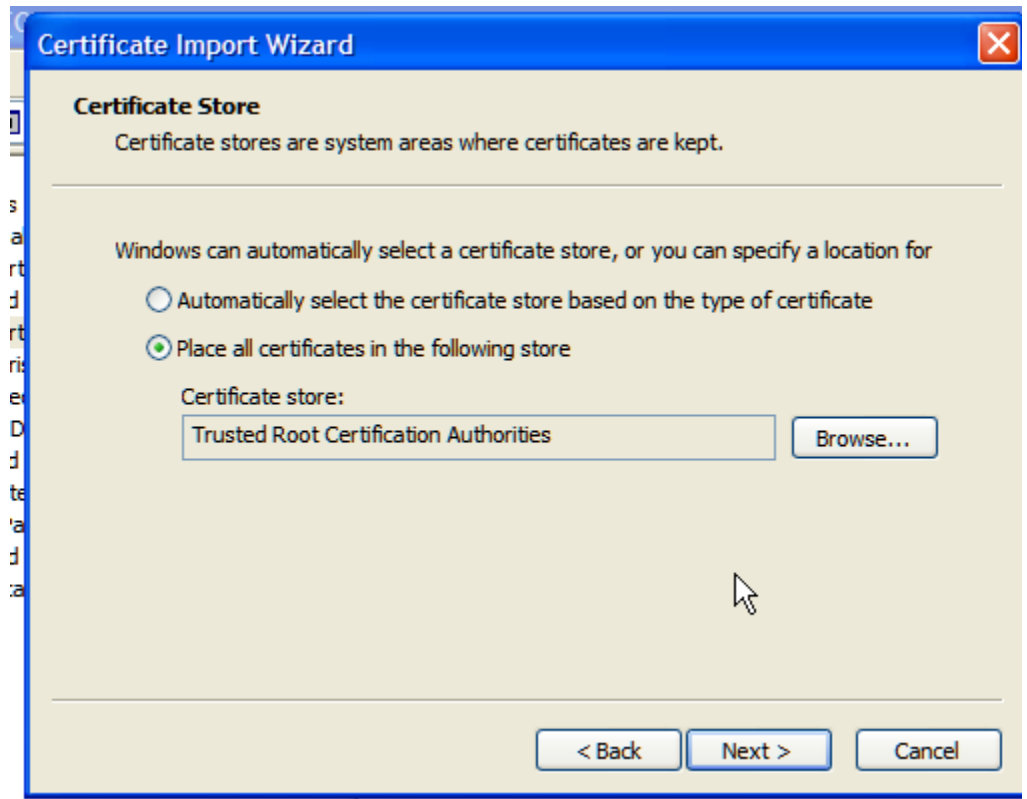
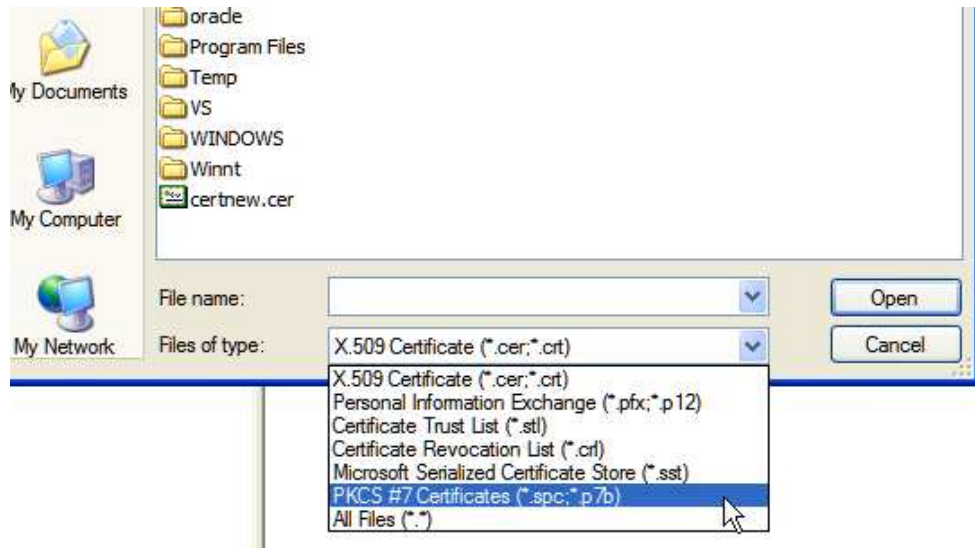
1. Root certificate

- a. Import the root certificate for the management servers on the same domain as the CA server

- i. Logon on the management server. Open a web Browser and navigate to `http://SRVNAME342/certsrv/`
 - ii. Click on Download a CA certificate, certificate chain, or CRL
 - iii. Click on Download CA Certificate chain
 - iv. Click on save. And save to a location of your choice. The default file name is `certnew.p7b`. This is fine. (You can use this cert for all your management servers and gateway server to skip the initial download on this servers if you like.
- b. To import the downloaded cert open the certificate MMC
- i. Open run and type MMC
 - ii. Click on file, add/remove snap-in
 - iii. Click on Add and select Certificates, and click on add again.
 - iv. Select computer account and say finish
 - v. Close the window and say ok to the add remove window.
 - vi. Expand certificates and right click on “Trusted Root Certification Authorities”



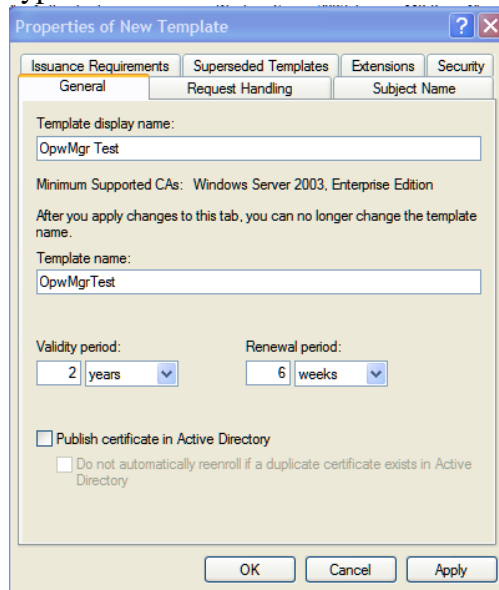
- vii. When the wizard opens navigate to the downloaded cert is `certnew.p7b` . You will need to change the file type to PKCS #7



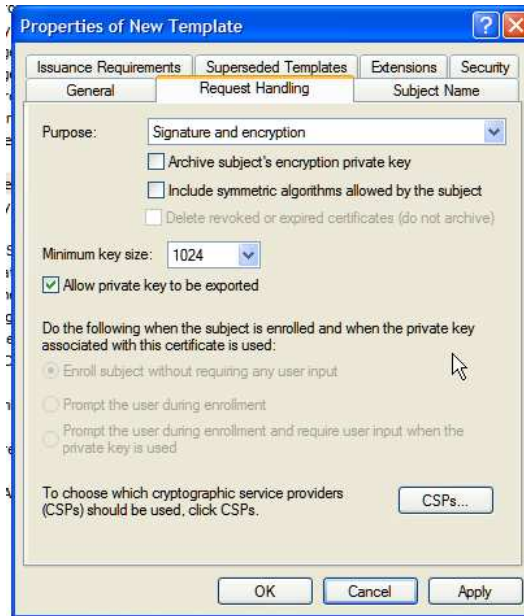
- viii. Accept the defaults and finish
- ix. Do this on all management servers inside the domain
- c. Import the root certificate for the Gateway server that is not attached to the domain as the CA server.
 - i. Perform step one above to save certnew.p7b. Or use the same cert that was downloaded above. And copy to the gateway server. Then perform step 2 above.

2. Create the Custom OpsMgr Certificate

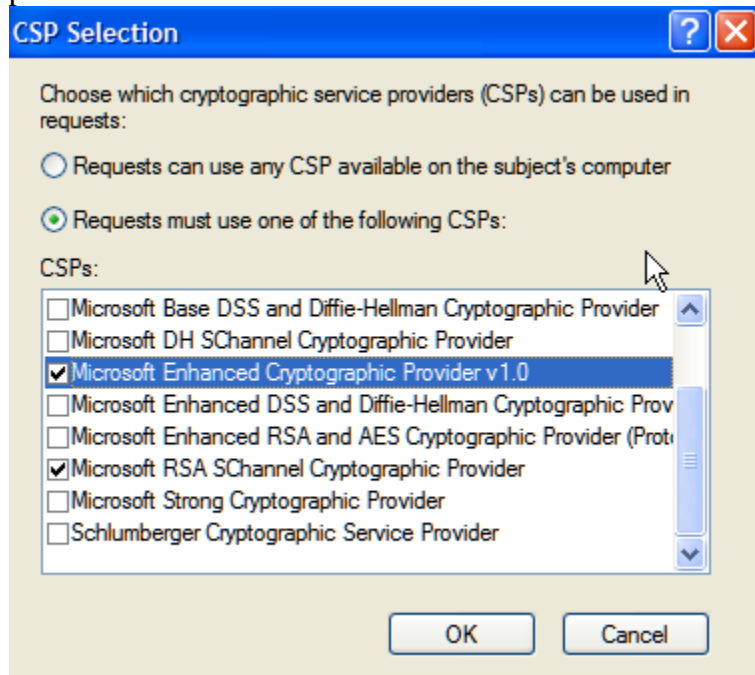
- a. To create the cert. We will use two consoles to do this. Certification Authority mmc and certificate templates mmc
 - i. Open run and type MMC
 - ii. Click on file, add/remove snap-in
 - iii. Click on Add and select Certificate Templates and Certification Authority, and click on add again. And finish
- b. Select Certificate Templates
- c. In the Certificate Templates Console right click **IPSec (Offline request)** and then select **duplicate template**
 - i. General Tab
 - ii. Type a name



- iii. Request Handling
 1. select **Allow private key to be exported**

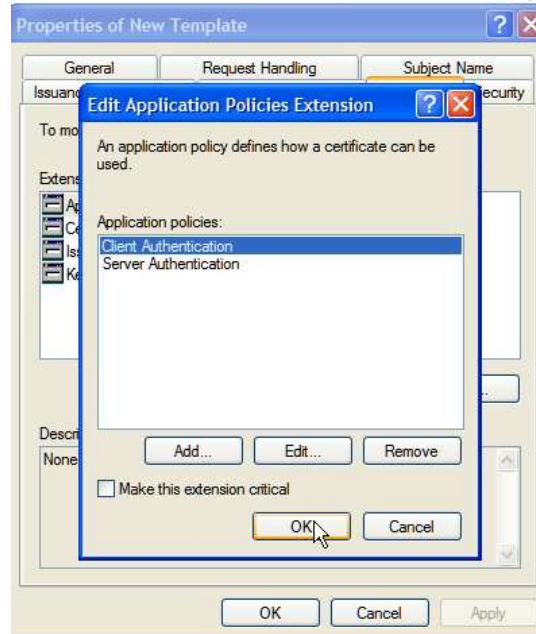


2. Click on **CSPs...**
3. select Microsoft RSA SChannel Cryptographic provider for windows 2003 and Microsoft Enhanced Cryptographic provider 1.0 for windows 2000



- iv. Extensions Tab
 1. select the Applications Policies and click on edit
 2. remove **IP security IKE intermediate**
 3. Click on add..

4. Select **Client Authentication and Server Authentication**, and



click on ok twice.

- v. Security Tab
 1. Users should have read
 2. Say ok and close.

3. Add the new custom cert to the certificate authority

- i. Open the Certification Authority mmc console
- ii. Expand it and right click on certificate templates
- iii. Select new, certificate template to issue
- iv. Scroll through the list until you find the one you just created. Select it and say ok.
- v. It should now show in the right window.


4. Deploy the Custom OpsMgr Certificate to the management servers on the same domain as the CA (need to do the full steps individually for each server)

- a. Logon on the management server. Open a web Browser and navigate to <http://SRVNAME342/certsrv/>
- b. Click on **Request a certificate**
- c. Click on **Create and submit a request to this CA**
- d. Select the custom Template
- e. Enter a name for the template. This is the full unc name of the server that you are going to install the cert on.
- f. Enter the rest of the identity info if you like.
- g. Under Key options select the csp that fits your operating system. select Microsoft RSA SChannel Cryptographic provider for windows 2003 and Microsoft Enhanced Cryptographic provider 1.0 for windows 2000
- h. Key size 1024

- i. Mark keys as exportable
- j. Check off **Store cert in local computer cert store...**
- k. Use full unc path as friendly name.

Advanced Certificate Request

Certificate Template:

OpsMgr 

Identifying Information For Offline Template:

Name:

E-Mail:

Company:

Department:


City:

State:

Country/Region:

Key Options:

Create new key set Use existing key set

CSP: 

Key Usage: Exchange

Key Size: Min: 1024
Max: 16384 (common key sizes: [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))


Automatic key container name User specified key container name

Mark keys as exportable
 Export keys to file

Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

Request Format: CMC PKCS10

Hash Algorithm: 
Only used to sign request.

Save request to a file

Attributes:

Friendly Name:

- l. Click on submit, say yes.
- m. Click on **Install this certificate**
- n. Open run and type MMC
- o. Click on file, add/remove snap-in
- p. Click on Add and select Certificates, and click on add again.
- q. Select computer account and say finish
- r. Close the window and say ok to the add remove window.
- s. Expand certificates and right click on Personal certificates
- t. You should see the new cert here.

5. Deploy the custom Certificate to the Gateway servers in the DMZ.

- a. Because the gateway is not part of the same domain as the CA. We need to create the certificate on a different server and export it to a USB drive or other storage device. Then manually copy it to the gateway server and import it.
- b. First create the cert from a server on the same domain as the CA. [Follow the steps in step 4 first.](#)
- c. Next we will export the cert
 - i. Open run and type MMC
 - ii. Click on file, add/remove snap-in
 - iii. Click on Add and select Certificates, and click on add again.
 - iv. Select computer account and say finish
 - v. Close the window and say ok to the add remove window.
 - vi. Expand certificates and right click on Personal certificates
 - vii. You should see the new cert here.
 - viii. Right click on the cert and select **All tasks, export**
 - ix. The export wizard will open, say next
 - x. Select **Yes, export private key**
 - xi. Select **enable strong protection**
 - xii. Enter a password for the import. You will need this password when you export the cert.
 - xiii. Specify a location and name to save it too.
 - xiv. And finish
- d. Import the cert.
 - i. Copy the cert to the gateway server. It will have a .pfx extension.
 - ii. Open run and type MMC
 - iii. Click on file, add/remove snap-in
 - iv. Click on Add and select Certificates, and click on add again.
 - v. Select computer account and say finish
 - vi. Close the window and say ok to the add remove window.
 - vii. Expand certificates and right click on Personal certificates
 - viii. Select **All tasks, Import**
 - ix. Browse to the cert you copied over. You will need to change the file type to PFX to see the cert.
 - x. Select **open, say next, enter password.**
 - xi. Check off **Mark this key as exportable.**

- xii. Say next, make sure the certificate store is **personal**, click next and finish.

6. Run the momcertimport utility

- a. In this step we are going to use the same pfx certificate (the custom personal cert) that we created in step 4. This tool writes the certificate serial number to the registry. This will help OpsMgr components find the proper certificate for authenticating easily.
- b. You will find the momcertimport utility on the install cd under supporttools\i386.
- c. Copy momcertimport.exe and the pfs certificate into the same folder.
- d. Open a command prompt, navigate to the folder with both files and type the following command
 - i. `C:\>MOMCertImport.exe certfilename.pfx`
 - ii. There is NO response after the command is successfully initiated.
- e. So this on all SCOM management servers. RMS, MS, and Gateway

7. Approve the Gateway Server

- a. We will use the gateway approval tool to achieve this. This will setup the gateway server as a management server in SCOM. Once done you can confirm this by looking in the SCOM console under administration, Device Management, Management Servers.
- b. The tool has to be run from `c:\program Files\System Center Operations Manager 2007`
- c. Copy `Microsoft.EnterpriseManagement.GatewayApprovalTool.exe` from the support tools directory to `c:\program Files\System Center Operations Manager 2007`
- d. Open the command prompt and type the following command
 - i. `microsoft.enterprisemanagement.gatewayapprovaltool.exe /managementservername=SRVNAME261.domainName.com /gatewayname=domainNamedmz22.domainNamedmz.com /action=create`

8. Next you now ready to manually install the agents on the servers in the DMZ

9. Approve the agents in the SCOM console.