Step-by-step installation guide for monitoring untrusted servers using Operations Manager (Part 3 of 3)

Manual installation of agents and importing the SCOM certificate to the servers to be monitored:

Before starting the agent installation on any untrusted server, make sure that you can ping the Operations Manager Server using FQDN from the untrusted domain/DMZ or Gateway server and vice versa. To achieve this, you may need to use static host entries on the local computers but it is important that this step is completed before moving onto the next steps.

You will also need to ensure that traffic is allowed over the relevant ports as per Microsoft Documentation (particularly TCP port 5723)

To test the port access between agent server and root management server, you may Log on to the agent server and from command prompt, type Telnet <Management Server> 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.

Once communication between the Operations Manager Management Servers and the untrusted domain / DMZ or SCOM Gateway server has been established, Logon to the Ops manager Management Server, then open the Operations Manager console and then go to the Administration tab and then select Settings on the left hand side of the screen.
Double click on the Security option in the middle of the screen to open the Global Management Server Settings – Security window as below.
From the ‘Global Management Server Settings – Security’ window that opens, you need to select ‘Review new manual agent installations in pending management’ and then also decide whether or not you want SCOM to ‘Automatically approve new manually installed agents’

If you leave the ‘Automatically approve new manually installed agents’ tick box unchecked, then you will need to go to the ‘Pending Management’ queue after an agent is manually installed and allow it to be monitored within your SCOM environment.

Before we start installation of SCOM agent on the untrusted server, we need to have the required certificates ready with us.

We require following certificates for configuring untrusted server for authenticating to SCOM root Management Server:

- Trusted Root (CA) Certificate
- SCOM certificate issued in the name of “Untrusted Server”

**Download the Trusted Root (CA) Certificate:**
The trusted root certificate must be installed on the untrusted domain servers. To download the trusted root certificate, Log on to the computer where you want to install a certificate and connect to the Certificate Enrolment URL on the certificate Authority Server. For example, http://<CAservername>/certsrv

In case the server in DMZ or untrusted domain cannot reach the certificate Authority Server, you may download the Root (CA) Certificate to any server which has access to the Certificate Enrolment URL on the certificate Authority Server. Then copy the certificate using removable media and imports the same to desired server in DMZ or untrusted domain.

Detailed steps for Downloading Trusted Root (CA) Certificate is mentioned in the document Monitoring Untrusted Servers Using Operations Manager Part 1 of 3
SCOM certificate issued in the name of “Untrusted Server”

Request a SCOM certificate issued in the name of “Untrusted Server” from the enterprise CA:
Log on to the untrusted server where you want to request and install a certificate. In case the untrusted server is in restricted network and do not have access to the root CA certificate server, you can request the certificate for untrusted servers from your management server and once installed, export the same and import to the respective servers.

Pay extra attention while giving the correct FQDN or host name (is server is member of workgroup) while requesting the certificate for untrusted servers.

If you are planning to request the operations manager certificate directly from the untrusted server, make sure that you can ping the Operations Manager Server using FQDN from the untrusted server and vice versa. To achieve this, you may need to use static host entries on the local computers but it is important that this step is completed before moving onto the next steps. Also make sure the enterprise root CA certificate is installed on the requesting server.


The steps to Request a SCOM certificate issued in the name of “Untrusted Server” from the enterprise CA are same as it is mentioned in the document “Monitoring Untrusted Servers Using Operations Manager Part 2 of 3”
Here I am going to repeat few important areas where you will have to give extra attention so that the certificate you generate is valid and the server is able to authenticate using the generated certificate.
On the Request a Certificate page, click **Or, submit an advanced certificate request.**

On the Advanced Certificate Request page, click **Create and submit a request to this CA.**

On the Advanced Certificate Request page, click **Create and submit a request to this CA.**

Click on **Yes** to the Web Access Confirmation to continue.

Under the **Certificate Template**, pull down the list and select **Opsmgr Template**. Then enter the **Fully Qualified Domain Name (FQDN) of the requesting server** into the **Name** field.
From the same window, scroll down to the end and ensure that the Mark Keys as exportable option is selected, choose your key size (or leave at the default of 2048) and then again enter the FQDN of your requesting server into the Friendly Name field at the end of the page.

Once you have entered all of the information required and are happy to proceed, click the Submit button at the bottom of the page to complete the request.

Click on Yes to the Web Access Confirmation to continue.

Click on the Install this certificate link to install the certificate onto your requesting server.
You will see a window to confirm the new certificate has been successfully installed.

Although the above screen states that the new certificate has been installed onto your computer, when you open the local certificate store, you will not find the certificate under Local computer and you might think that the import was not successful.

No need to worry, this is because the certificate template creation within Windows Server 2008 R2 doesn’t have provision to specify where exactly the certificate will be stored. When you click Install This Certificate, it automatically installs the new certificate into the **Current User** instead of **Local Computer**.

In this situation, all we need to do is to export this certificate from the Current User store and import it into the Local Computer store to enable SCOM to use it for authentication of the computer.

Go to **Start** and then click **Run**. In the Run dialog box, type **mmc**, and then click OK.
In the Console1 window, click **File**, and then click **Add/Remove Snap-in**.

In the Add or Remove Snap-in dialog box, under the available snap-ins, select **Certificates**, and then click **Add**.
In the Certificates snap-in dialog box, select **My user account**, and then click **Next**.

Expand **Certificates Current Users** and then expand **Personal** and click **Certificates**.
Select the newly created certificate and then **Right-click** on the **certificate** and select **All Tasks** and then the **Export**.

Click through the Certificate Export Wizard to export the certificate.
On the Export Private Key page, select **Yes, export the private key** then click **Next**.

Leave the Export file Format to **.FPX (default)** and then click **Next**.
On the Password page, type a **password** (you should remember this password for installing this certificate in the future).

Specify the name and location of the certificate to export and click **Next** to continue.
Complete the certificate export wizard by clicking **Finish**.

![Certificate Export Wizard](image)

Close the mmc. Now you should be able to see the exported certificate (ScomCertificate.fpx) file on the root of your C:\ drive.

*If you have requested the untrusted server certificate from any server other than the untrusted server, copy the above certificate ScomCertificate.fpx to the untrusted server and continue the following step to import the certificate to the local certificate store on the untrusted server.*

To import this certificate into our Certificates – Local Computer store using the Certificates MMC snap-in again.

*Go to Start and then click Run. In the Run dialog box, type mmc, and then click OK. In the Console1 window, click File, and then click Add/Remove Snap-in. In the Add or Remove Snap-in dialog box, under the available snap-ins, select Certificates, and then click Add.*
In the Certificates snap-in dialog box, select **Computer account**, and then click **Next**.

Expand **certificates (Local Computer)** and then Right Click on **Personal**, then select **All Tasks**, and then click on **Import**.
Click through the Certificate Import Wizard to import the certificate.

On the File Import page, locate the exported file on the C:\ drive and click **Next**
On the Password page, type the password assigned to the file while exporting. Leave rest of the settings default and click **Next**.

Make sure that under Place all certificates in the following store shows **Personal**.
Click **Finish** to complete the certificate import wizard.

All is well... the following screen shows the certificate is valid and is in the proper location.

The **Trusted Root (CA) Certificate** must be imported before you import the SCOM certificate otherwise the certificate will not be valid.
Now we have the certificates installed on the untrusted server and we are ready to proceed with SCOM agent installation.

To install agent manually, log on to the computer in the untrusted domain / DMZ with an account that is a member of the ‘Local Administrators’ group. Create a new folder on the C: drive of the server and call it ‘SCOM_Agent_Files’. Copy the SCOM Agent installation folder from the original SCOM installation media here.

Open command prompt with Administrative privilege and browse to the AMD64 folder within the copied folder (select i386 folder if you are installing on a 32 bit windows Operating System) and run MOMAgent.msi.

The SCOM agent needs to be installed on the server that you wish to monitor before you can import the certificate into SCOM. To install the SCOM agent,
Click next to start the installation wizard, leave the default location as install location and then click next.

Select Specify Management Group Information and then click next
Provide name of the root management server name and management group name, leave the port number as default 5723. Click next.

Leave Local system as selected and click on Next to continue.
Select ‘I don’t want to use Microsoft Update’ and click on Next to continue.

Click on ‘Install’ button from the final screen to install the SCOM agent from the original installation media.
When the agent installation is completed, make sure you read ‘The setup wizard has successfully installed System Centre Operations Manager 2007 R2 Agent’. Click on Finish to close the agent installation wizard.

**Import the server’s certificate to SCOM.**
After successfully installing agent on the untrusted server, you need to import the scom certificate issued for untrusted server (the same certificate which we imported into the local certificate store of untrusted server) to import the certificate with private key,

Copy the **MOMCertIMport.exe** Tool from the `\SupportTools\i386` folder of the Operations Manager 2007 distribution files to C:\SCOM_Agent_Files folder.

Then copy the SCOM certificate (**ScomCertificate.fpx**) into the above folder.
Go to the command prompt and change the working directory to C:\SCOM_Agent_Files.
Type MOMCertImport.exe <Untrusted Server Certificate.pfx> and press enter.

At the password prompt, type the password which you set while exporting the certificate. Make sure to type the keys properly as the screen will not show any characters while typing the password.

Below window shows that the certificate is successfully imported to SCOM configuration.

Go to the Services and restart the System Centre Management Service
Once the service started, go to the event viewer and confirm that the agent is able to communicate to SCOM management group.

Congratulations!
You are done. Go back to the SCOM console and notice the new agent listed under the Agent Managed section under Administration.
As usual wait for couple minutes so that the SCOM agent and Management group shares all the information related to the OS version, application installed, Recourse details etc. according to the available imported Management Packs.