

# Monitoring Untrusted Forests

---

## Configuring Certificates

### Using a Windows 2008 Stand-alone Certificate Authority

<http://technet.microsoft.com/en-us/library/dd362655.aspx>

The high-level process to obtain a certificate from a stand-alone certification authority (CA) is as follows:

1. Download the Trusted Root (CA) certificate to each Management Server \ Gateway (or agent if Gateway not used)
2. Import the Trusted Root (CA) certificate to each Management Server \ Gateway (or agent if Gateway not used)
3. Create a setup information file to use with the CertReq command-line utility.
4. Create a request file for each Management Server \ Gateway (or agent if Gateway not used).
5. Submit a request to the CA using the request file.
6. Approve the pending certificate request.
7. Retrieve the certificate from the CA.
8. Import the certificate into the certificate store for each Management Servers \ Gateway (or agent if Gateway not used)
9. Import the certificate into Operations Manager using MOMCertImport for each Management Servers \ Gateway (or agent if Gateway not used)

\*\*\* Management Server includes the Root Management Server \*\*\*

## To download the Trusted Root (CA) certificate to each Management Server \ Gateway \ Agent

1. Log on to the computer where you want to install a certificate
2. Start Internet Explorer, and connect to the computer hosting Certificate Services; for example, <https://<servername>/certsrv>.
3. On the **Welcome** page, click **Download a CA Certificate, certificate chain, or CRL**.

Microsoft Active Directory Certificate Services -- Westside-LDN-SC-VMM-CA

---

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the program, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate request. You can also view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

4. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Encoding method**, click **Base 64**, and then click **Download CA certificate chain**.

Microsoft Active Directory Certificate Services -- Westside-LDN-SC-VMM-CA

---

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:**

Current [Westside-LDN-SC-VMM-CA]

**Encoding method:**

☐ DER

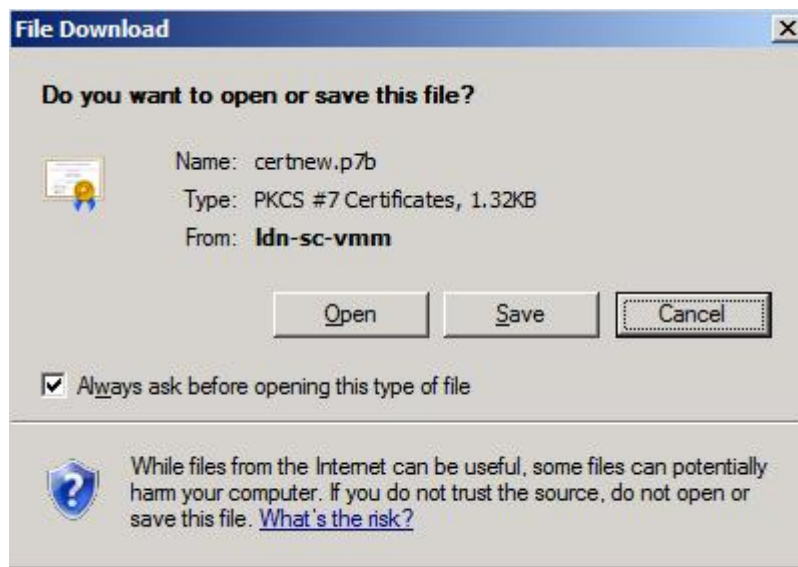
☒ Base 64

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

5. In the **File Download** dialog box, click **Save** and save the certificate; for example, **Trustedca.p7b**.



6. When the download has finished, close Internet Explorer.

## To import the Trusted Root (CA) Certificate

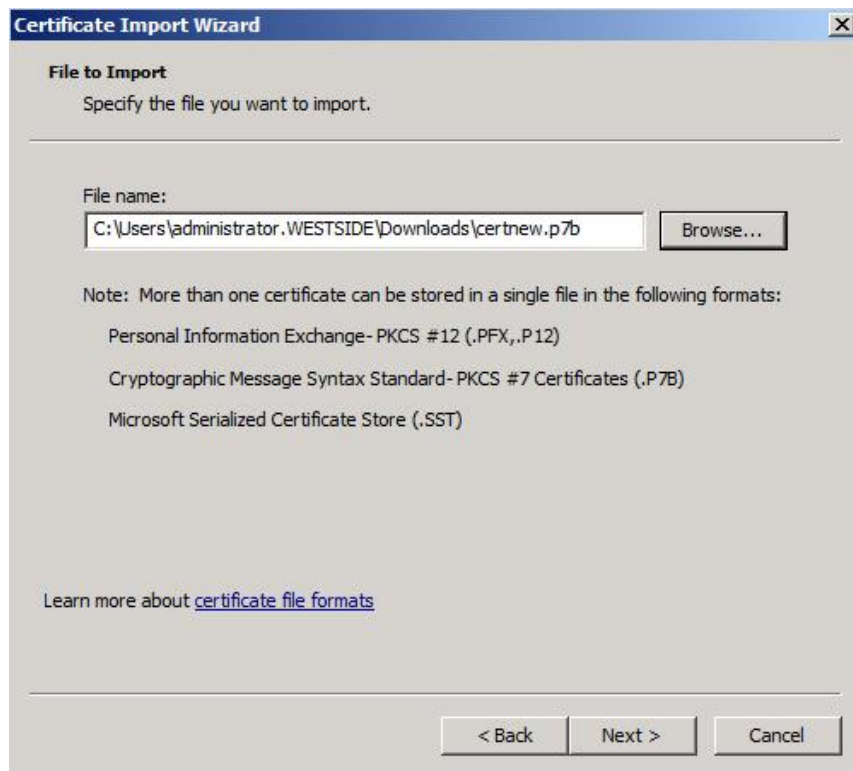
On each Management Server (including the RMS) \ Gateway (or agent if a gateway is not being used).

1. On the Windows desktop, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **mmc**, and then click **OK**.
3. In the **Console1** window, click **File**, and then click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the **Add Standalone Snap-in** dialog box, click **Certificates**, and then click **Add**.
6. In the **Certificates snap-in** dialog box, select **Computer account**, and then click **Next**.
7. In the **Select Computer** dialog box, ensure that **Local computer: (the computer this console is running on)** is selected, and then click **Finish**.
8. In the **Add Standalone Snap-in** dialog box, click **Close**.
9. In the **Add/Remove Snap-in** dialog box, click **OK**.
10. In the **Console1** window, expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**, and then click **Certificates**.
11. Right-click **Certificates**, select **All Tasks**, and then click **Import**. (or on windows 2008, Action, Import, Certificates).
12. In the Certificate Import Wizard, click **Next**.

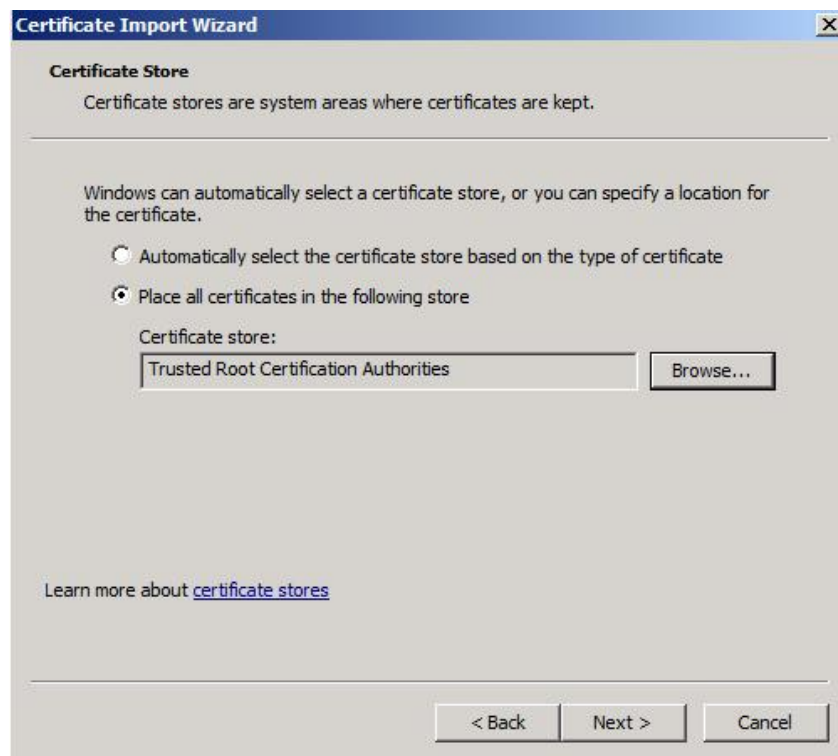




13. On the **File to Import** page, click **Browse** and select the location where you downloaded the CA certificate file, for example, TrustedCA.p7b, select the file, and then click **Open**.



14. On the **File to Import** page, select **Place all certificates in the following store** and ensure that **Trusted Root Certification Authorities** appears in the **Certificate store** box, and then click **Next**.



15. On the **Completing the Certificate Import Wizard** page, click **Finish**.

## To create a setup information (.inf) file

1. On the computer hosting the Operations Manager component for which you are requesting a certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **Notepad**, and then click **OK**.
3. Create a text file containing the following content:

**[NewRequest]**

**Subject="CN=<FQDN of computer you are creating the certificate, for example, the gateway server or management server.>"**

**Exportable=TRUE**

**KeyLength=2048**

**KeySpec=1**

**KeyUsage=0xf0**

**MachineKeySet=TRUE**

**[EnhancedKeyUsageExtension]**

**OID=1.3.6.1.5.5.7.3.1**

**OID=1.3.6.1.5.5.7.3.2**

4. Save the file with an .inf file name extension, for example, RequestConfig.inf.
5. Close Notepad.

## To create a request file to use with a stand-alone CA

1. On each computer hosting the Operations Manager component for which you are requesting a certificate (all management servers \ gateways \ agents that aren't using a gateway), click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq -New -f <path>RequestConfig.inf <path>CertRequest.req**, and then press ENTER.
4. Open the resulting file (for example, CertRequest.req) with Notepad. Copy the contents of this file onto the clipboard.

## To submit a request to a stand-alone CA

1. On each computer hosting the Operations Manager component for which you are requesting a certificate (all management servers \ gateways \ agents that aren't using a gateway), start Internet Explorer, and then connect to the computer hosting Certificate Services (for example, <https://<servername>/certsrv>).
2. On the **Microsoft Active Directory Certificate Services Welcome** screen, click **Request a certificate**.



3. On the **Request a Certificate** page, click **advanced certificate request**.



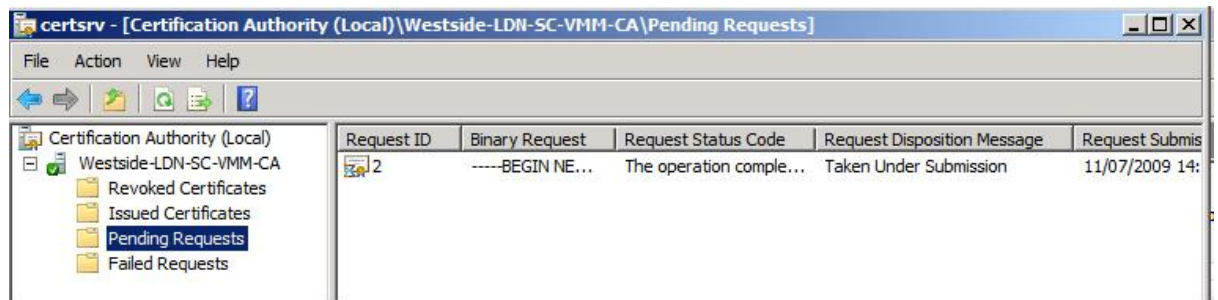
4. On the **Advanced Certificate Request** page, click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.





## To approve the pending certificate request

1. Log on as a certification authority administrator to the computer hosting Active Directory Certificate Services.
2. On the Windows desktop, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**.
3. In **Certification Authority**, expand the node for your certification authority name, and then click **Pending Requests**.



4. In the results pane, right-click the pending request from the previous procedure, point to **All Tasks**, and then click **Issue**.
5. Click **Issued Certificates**, and confirm the certificate you just issued is listed.



6. Close Certification Authority.

## To retrieve the certificate

1. Log on to the computer where you want to install a certificate; for example, the gateway server or management server.
2. Start Internet Explorer, and connect to the computer hosting Certificate Services (for example, <https://<servername>/certsrv>).
3. On the **Microsoft Active Directory Certificate Services Welcome** page, click **View the status of a pending certificate request**.

Microsoft Active Directory Certificate Services -- Westside-LDN-SC-VMM-CA

### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can identify to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list. You can also view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

#### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

4. On the **View the Status of a Pending Certificate Request** page, click the certificate you requested.

Microsoft Active Directory Certificate Services -- Westside-LDN-SC-VMM-CA

### View the Status of a Pending Certificate Request

Select the certificate request you want to view:

[Saved-Request Certificate \(11 July 2009 14:30:18\)](#)

5. On the **Certificate Issued** page, select **Base 64 encoded**, and then click **Download certificate**.

Microsoft Active Directory Certificate Services -- Westside-LDN-SC-VMM-CA

### Certificate Issued

The certificate you requested was issued to you.

☐ DER encoded or ☒ Base 64 encoded



[Download certificate](#)

[Download certificate chain](#)

6. In the **File Download – Security Warning** dialog box, click **Save**, and save the certificate; for example, as certnew.cer.



7. On the **Certificate Installed** page, after you see the message that **Your new certificate has been successfully installed**, close the browser.
8. Close Internet Explorer.

### To import the certificate into the certificate store

1. On the computer hosting the Operations Manager component for which you are configuring the certificate, click **Start**, and then click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. In the command window, type **CertReq -Accept <path>certnew.cer**, and then press ENTER.



## To import the certificate into Operations Manager using MOMCertImport

Make sure you install the agent onto servers that are not using gateways. Then use MOMCertImport and then restart the agent.

1. Log on to the computer where you installed the certificate with an account that is a member of the Administrators group.
2. On the Windows desktop, click **Start**, and then click **Run**.
3. In the **Run** dialog box, type **cmd**, and then click **OK**.
4. At the command prompt, type **<drive\_letter>:** (where **<drive\_letter>** is the drive where the Operations Manager 2007 installation media is located), and then press ENTER.
5. Type **cd\SupportTools\i386**, and then press ENTER.

### **Note**

On 64-bit computers, type **cd\SupportTools\amd64**

6. Type the following:  
  
**MOMCertImport /SubjectName <Certificate Subject Name>**
7. Press ENTER.