

Main page: [Cisco Unified Presence, Release 7.x](#)

Contents

- [1 Previous Topic](#)
- [2 Downloading the CA Certification Chain for Microsoft OCS](#)
 - ◆ [2.1 Procedure](#)
 - ◆ [2.2 Troubleshooting Tips](#)
 - ◆ [2.3 What To Do Next](#)
 - ◆ [2.4 Installing the CA Certification Chain for Microsoft OCS](#)
 - ◇ [2.4.1 Before You Begin](#)
 - ◇ [2.4.2 Procedure](#)
 - ◇ [2.4.3 What To Do Next](#)
 - ◆ [2.5 Submitting the Certificate Request on the CA Server for Microsoft OCS](#)
 - ◇ [2.5.1 Before You Begin](#)
 - ◇ [2.5.2 Procedure](#)
 - ◇ [2.5.3 Troubleshooting Tips](#)
 - ◇ [2.5.4 What To Do Next](#)
 - ◆ [2.6 Approving and Installing the Certificate for Microsoft OCS](#)
 - ◇ [2.6.1 Before You Begin](#)
 - ◇ [2.6.2 Procedure](#)
 - ◇ [2.6.3 What To Do Next](#)
 - ◆ [2.7 Configuring the Installed Certificate for Microsoft OCS](#)
 - ◇ [2.7.1 Before You Begin](#)
 - ◇ [2.7.2 Procedure](#)
 - ◇ [2.7.3 What To Do Next](#)

Previous Topic

- [Configuring Cisco Unified Presence Release 7.x with Microsoft OCS for Remote Call Control](#)

- [Downloading the CA Certification Chain for Microsoft OCS](#)
- [Installing the CA Certification Chain for Microsoft OCS](#)
- [Submitting the Certificate Request on the CA Server for Microsoft OCS](#)
- [Approving and Installing the Certificate for Microsoft OCS](#)
- [Configuring the Installed Certificate for Microsoft OCS](#)

Downloading the CA Certification Chain for Microsoft OCS

Procedure

1. Select **Start > Run**.
2. Perform the following actions:
 1. Type [http://<name of your Issuing CA Server>/certsrv](#).
 2. Select OK.

3. Click **Download a CA certificate, certificate chain, or CRL** from Select a task.
4. Select **Download CA certificate chain**.
5. Select **Save** in the File Download dialog box.
6. Save the file on a hard disk drive on your server.

Troubleshooting Tips

The certificate file has an extension of .p7b. If you open this .p7b file, the chain will have the following two certificates:

- name of Standalone root CA certificate
- name of Standalone subordinate CA certificate (if any)

What To Do Next

Installing the CA Certification Chain for Microsoft OCS

Installing the CA Certification Chain for Microsoft OCS

Before You Begin

Download the CA Certification Chain.

Procedure

1. Select **Start > Run**.
2. Perform the following actions:
 - ◇ Enter **mmc**.
 - ◇ Select **OK**.
3. Select **File > Add/Remove Snap-in**.
4. Select **Add** in the Add/Remove Snap-in dialog box.
5. Select **Certificates** in the list of Available Standalone Snap-ins.
6. Select **Add**.
7. Select **Computer account**.

8. Select **Next**.
9. Perform the following actions from the Select Computer dialog box:
 - ◇ Ensure Local computer: (the computer this console is running on) is selected.
 - ◇ Select **Finish**.
 - ◇ Select **Close**
 - ◇ Select **OK**.
10. Expand Certificates (Local Computer) in the left pane of the Certificates console.
11. Expand Trusted Root Certification Authorities.
12. Right-click **Certificates**.
13. Perform the following actions:
 - ◇ Point to **All Tasks**.
 - ◇ Select **Import**.
14. Select **Next** in the Import Wizard.
15. Select **Browse** and locate the certificate chain on your computer.
16. Select **Open**.
17. Select **Next**.
18. Leave the default value Place all certificates in the following store selected.
19. Ensure Trusted Root Certification Authorities appears under the Certificate store.
20. Select **Next**.
21. Select **Finish**.

What To Do Next

[Submitting the Certificate Request on the CA Server for Microsoft OCS](#)

Submitting the Certificate Request on the CA Server for Microsoft OCS

Before You Begin

Install the CA Certification Chain.

Procedure

1. On the computer requiring a certificate, open a Web browser.
2. Enter the URL <http://<name of your Issuing CA server>/certsrv>.
3. Select **Enter**.
4. Select **Request a Certificate**.
5. Select **Advanced certificate request**.
6. Select **Create** and submit a request to this CA.
7. Select **Other** in the Type of Certificate Needed list.
8. In the Name field of the Identifying Information section, enter the FQDN. The name must match the name of the Microsoft OCS, which is usually the FQDN.
9. In the OID field, type the following OID: 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2.

Note: A comma separates the two 1s in the middle of the OID.

10. Perform one of the following procedures:
 - ◇ If you are using Windows Certificate Authority 2003, check **Store certificate** in the local computer certificate store in Key Options.
 - ◇ If you are using Windows Certificate Authority 2008, refer to the workaround described in the Troubleshooting Tips of this topic.
11. Enter a friendly name.
12. Select **Submit**.
13. Select **Yes** in the Potential Scripting Violation dialog box.

Troubleshooting Tips

If you are using Windows Certificate Authority 2008, you no longer have the option to store the certificate in the local computer store on the certificate enrollment page. Perform the following workaround to replace Step 10 in the procedure:

1. Sign out of the Microsoft OCS server.

2. Sign in to the Microsoft OCS server as a Local user.
3. Create the certificate.
4. Approve the certificate from the CA server.
5. Export the certificate to a file.
6. Sign out of the Microsoft OCS server.
7. Sign in to the Microsoft OCS server as a Domain user.
8. Import the certificate file using the Certificate wizard. The certificate displays in the Microsoft OCS certificate tab (because it is installed in the Local Computer store).

What To Do Next

Approving and Installing the Certificate for Microsoft OCS

Approving and Installing the Certificate for Microsoft OCS

Before You Begin

Submit the Certificate Request on the CA Server.

Procedure

1. Sign in to the enterprise subordinate CA server with Domain Administrator credentials.
2. Select **Start > Run**.
3. Perform the following actions:
 - ◇ Enter **mmc**.
 - ◇ Select **Enter**.
4. Select **File > Add/Remove Snap-in**.
5. Select **Add**.
6. Select **Certification Authority** in Add Standalone Snap-in.
7. Select **Add**.
8. In Certification Authority, accept the default option Local computer (the computer this console is running on).
9. Select **Finish**.

10. Select **Close**.
11. Select **OK**.
12. In the MMC, expand Certification Authority and expand your issuing certificate server.
13. Select **Pending request**.
14. In the Details pane, perform the following actions:
 - ◇ Right-click the request identified by its request ID.
 - ◇ Point to **All Tasks**.
 - ◇ Select **Issue**.
15. Select **Start > Run** on the server from which you requested the certificate.
16. Type <http://<name of your Issuing CA Server>/certsrv>.
17. Select **OK**.
18. Select **View the status of a pending certificate request** from Select a task.
19. Select your certificate request.
20. Select **Install this certificate**.

What To Do Next

Configuring the Installed Certificate for Microsoft OCS

Configuring the Installed Certificate for Microsoft OCS

Before You Begin

Approve and install the Certificate.

Procedure

1. Select **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.
2. Expand the (local computer) tree on the right pane.

Procedure

3. Select Default Web Site.
4. Right-click to open the Properties dialog box.
5. Select the Certificate tab from the Default Web Site Properties dialog box.
6. If a certificate has already been selected, select **Delete Certificate** to remove the selection
7. Select **Certificate** to launch the Certificate Wizard.
8. Using the Certificate Wizard, select the certificate that was installed for Microsoft OCS.
9. Launch the Microsoft Office Communications Server 2007 application.
10. In the right pane, select the server that represents the local machine.
11. Right-click on the server.
12. Select **Properties > Front End Properties**.
13. Select the Certificate tab.
14. Select **Select Certificate**.
15. Find and select the installed certificate for Microsoft OCS.

Note: If you are using Microsoft LCS, follow steps 1-7 above and then open the Microsoft Live Communications Server 2005 application. From the Administration Page, right-click on the desired server to open the Properties dialog box. Select the Security tab, select Select Certificate and select the newly installed LCS certificate.

What To Do Next

[Configuring a TLS Route for Cisco Unified Presence on Microsoft OCS](#)