Installing a Certificate Chain for Communicator Web Access

Communications Server 2007 R2

Topic Last Modified: *2009-07-21*

A certificate chain establishes a "chain of trust" from a certification authority (CA) to an individual certificate. Trust occurs if a valid certificate from that CA can be found in your root certificate directory. As long as you trust the CA, you will automatically trust any other certificates signed by that CA.

If you create your own certificates, your Communicator Web Access (2007 R2 release) server probably already has a chain of trust with your internal CA. If not, you can establish this chain of trust by downloading and installing a certificate chain.

Installing the certificate chain is especially important if your CA is running Windows Server 2003 and your Communicator Web Access server is running Windows Server 2008. Because of changes in Windows Server 2008, you cannot request a certificate from a Windows Server 2003 CA without first installing the certificate chain. If you request a certificate without installing the certificate chain, you will receive the following error message:

Delayed or Immediate Request: The request was submitted to the Certification Authority successfully.

However, request processing failed. Restart the wizard and retry the operation.

Task failed: Failed to generate certificate signing request. Ensure that you have sufficient privileges to perform certificate operations

By installing the certificate chain, you prevent this error from occurring.

To download a certificate chain

1. Log on to the computer as a member of the local Administrators group.
2. Open a Web browser and then, in the address bar, type the URL to the CA. For example, if your certificate server has a fully qualified domain name (FQDN) of certserver.contoso.com, the URL would be https://certserver.contoso.com/certsrv.
3. After connecting to the **Welcome** page, click **Download a CA certificate, certificate chain, or CRL**.
4. On the **Download a CA Certificate, Certificate Chain, or CRL** page, click **Download CA certificate chain**.
5. In the **File Download** dialog box, click **Save**, and then save the downloaded .p7b file (a file format used to store certificates) to a folder on the local computer.
6. If the **Download Complete** dialog box appears, click **Close**.

To install a certificate chain

1. Click **Start**, and then click **Run**.
2. In the Open box, type **mmc**, and then click **OK**.
3. On the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add/Remove Snap-in** dialog box, click **Add**.
5. In the list of **Available Standalone Snap-ins**, select **Certificates**.
6. Click **Add**.
7. Select **Computer account**, and then click **Next**.
8. In the **Select Compute**r dialog box, ensure that **Local computer (the computer this console is running on)** is selected, and then click **Finish**.
9. Click **Close**, and then click **OK**.
10. In the left pane of the **Certificates** console, expand **Certificates (Local Computer)**.
11. Expand **Trusted Root Certification Authorities**.
12. Right-click **Certificates**, point to **All Tasks**, and then click **Import**.
13. In the Import Wizard, click **Next**.
14. Click **Browse**, go to the location where you saved the certificate chain, select the .p7b file, and then click **Open**.
15. Click **Next**.
16. Accept the default value **Place all certificates in the following store**. Under **Certificate store**, ensure that **Trusted Root Certification Authorities** appears.
17. Click **Next**.
18. Click **Finish**.

Community Additions