Search

Adding your enterprise CA as a trusted certificate authority

If you used an enterprise CA on your network, or if you created a CA for demos, as described in Self-signed certificates: Creating a Certificate Authority for development, the CA's root certificate must be installed as a trusted root certificate authority in the following locations:

- The servers where Web, Mobile Server, or Web Services are installed, as applicable. For steps, see To add your enterprise CA as a trusted certificate authority for Web, Mobile Server, or Web Services.
- Mobile devices, such as iPhone, iPad, or Android phones and tablets. For steps to add a trusted CA for iPhone and iPad, see To add your enterprise CA as a trusted certificate authority for iOS devices.

  For Android devices, you must add the certificate as a trusted certificate while creating a configuration for your devices in Mobile Administrator. For steps to configure Android devices, see the *Administering MicroStrategy Mobile* chapter in the MicroStrategy Mobile Design and Administration Guide.

Prerequisite

- You must have access to a copy of your enterprise CA's root certificate to perform this procedure.

  If your enterprise CA uses Microsoft Certificate Services, open the following URL in a browser window: `http://hostname/CertSrv`, where *hostname* is the computer on which Certificate Services is installed, click **Download a CA certificate, certificate chain, or CRL**, and under **Encoding method**, select **Base 64**. Click **Download CA certificate** and save it to the computer.

  If your enterprise CA uses OpenSSL, contact your administrator for a copy of the certificate.

To add your enterprise CA as a trusted certificate authority for Web, Mobile Server, or Web Services

---

1. On the machine where Web, Mobile Server, or Web Services is installed, from the **Start** menu, select **Run**, type `mmc`, and press Enter. The Microsoft Management Console opens.
2. From the **File** menu, select **Console**, and then select **Add/Remove Snap-in**. The Add/Remove Snap-in dialog box opens.
3. Click **Add** to open the Add Standalone Snap-in dialog box, click **Certificates**, and then click **Add**. The Certificates Snap-in dialog box opens.
4. Select **Computer Account** and click **Next**. The Select Computer page opens.
5. Click **Local Computer** and then click **Finish**. The Certificates snap-in is displayed in the list of selected snap-ins.

6 Click **OK** to return to the Console Root dialog box.

7 On the left, expand the **Certificates** snap-in, then expand Trusted Root Certificate Authorities.

8 Click **Action**, then **All Tasks**, then **Import**. The Certificate Import Wizard opens.

9 Click **Browse**, and select the certificate you downloaded from your CA.

10 Click **Next**. The Certificate Store page opens.

11 Select **Place all certificates in the following store**.

12 Click **Browse**, and select the **Trusted Root Certification Authorities** folder.

13 Click **Next**, then click **Finish**. A message is displayed, indicating that the import was successful.

To add your enterprise CA as a trusted certificate authority for iOS devices

1 To distribute your enterprise CA's root certificate to users, do one of the following:

- Send the certificate as an email attachment to all iOS users.
- On a server on your network, create a basic web page that allows users to download the certificate, and email the URL of the web page to your users.

The following steps must be performed for every iOS device in your organization.

2 On an iPhone or iPad, open the email or URL that contains the link to the certificate.

3 Tap the link to download the certificate. The certificate is downloaded, and is opened in the Install Profile dialog in the device's Settings screen.

4 In the Install Profile dialog, tap **Install**. A warning may be displayed, indicating that the authenticity of the certificate cannot be verified.

5 Click **Install**. The certificate is installed, and is shown as a trusted certificate.

If the device is protected with a passcode, you must type the passcode to install the certificate.