How to Create SSL Certificates

https://campus.barracuda.com/doc/30114587/

To secure web services and applications that use HTTP, create SSL certificates.

Follow the instructions in this article to use XCA to create, sign, and export SSL certificates.

Before You Begin

Create and export a root certificate in PEM format. For instructions, see How to Create Certificates with XCA.

Step 1. Create a SSL Server Certificate

To create the SSL server certificate:

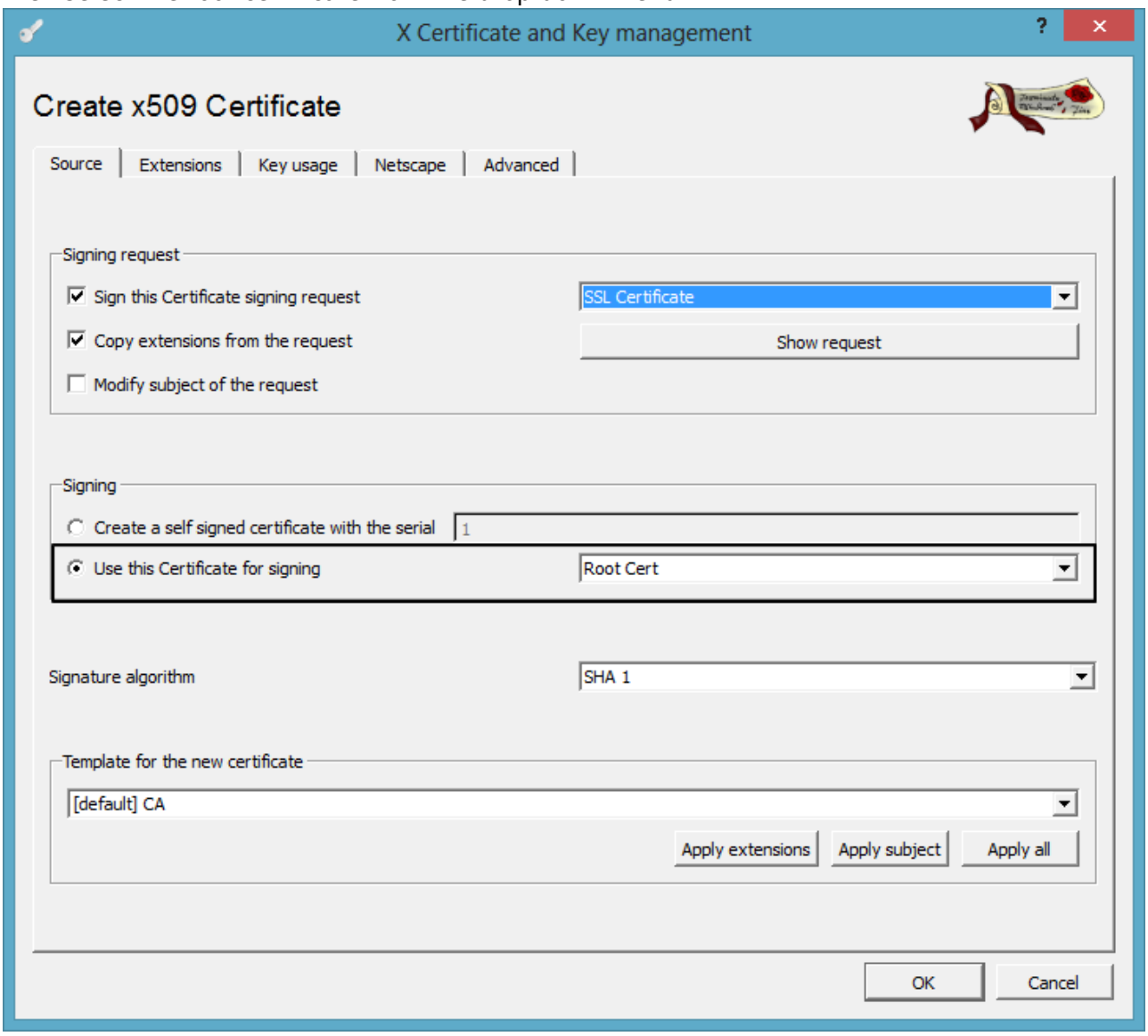
1. In XCA, click the **Certificate signing requests** tab, and then click **New Request**. The **Create Certificate Signing Request** window opens.
2. Use the HTTPS Server template:
    1. Click the **Source** tab.
    2. From the **Template for the new certificate** list, select **[default] HTTPS_Server**.
    3. Click **Apply extensions**.
3. Configure the identifying information.
    1. Click the **Subject** tab.
    2. Fill out the fields in the **Distinguished name** section.
    3. Click **Generate a new key**.
    4. In the **New Key** window, enter a name for the certificate, select a key size, and then click **Create**.
4. Click **OK**.

Step 2. Sign the SSL Certificate

To sign the SSL certificate:

1. Click the **Certificate signing requests** tab.
2. Right-click the SSL certificate and then click **Sign**. The **Create x509 Certificate** window opens.
3. In the **Signing** section under the **Source** tab, select **Use this Certificate for signing** and

then select the root certificate from the drop-down menu.

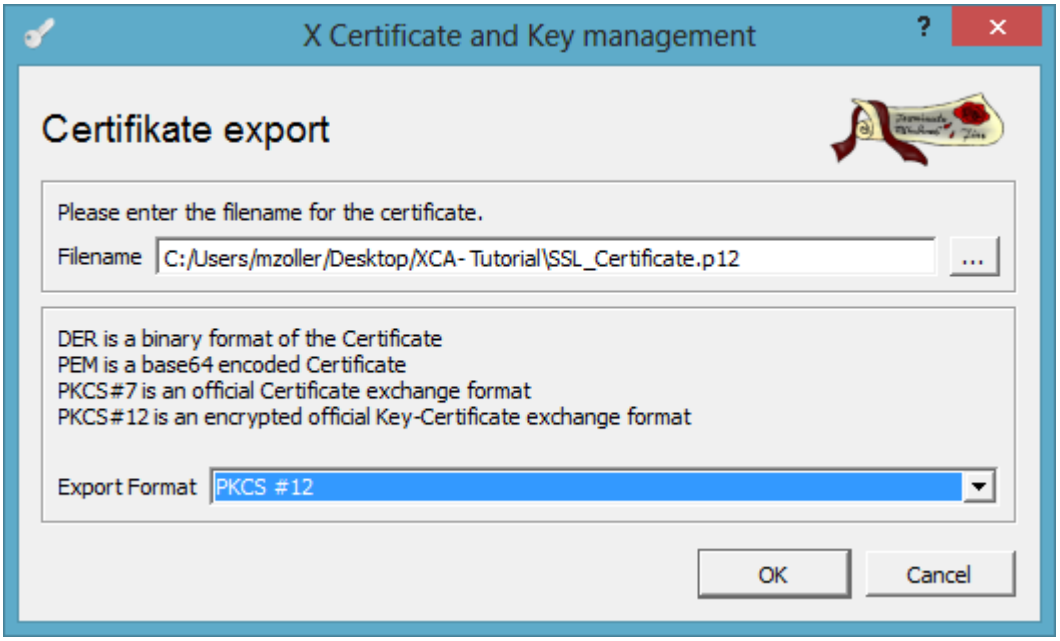


4. Click **OK** to sign the certificate. It then appears under the **Certificate signing requests** tab with the status of **Signed**.

Step 3. Export the SSL Certificate

You must export the certificate as a PKCS#12 file. To export the SSL server certificate:

1. Click the **Certificates** tab.
2. Select the certificate that you want to export and then click **Export**.
3. In the **Certifikate Export** window, select **PKCS #12** from the **Export Format** list and then click **OK**.



Next Steps

You can import the certificates on the Barracuda Networks appliances that need the SSL certificate. For Windows clients, you can use an Active Directory policy to distribute the root certificate. On iOS and Android, certificates must be imported manually or by the Mobile Device Management platform.

The following table lists the certificates that are required on each appliance or device:

Appliance or Device	Required Certificates
Barracuda Appliance	• Root certificate • SSL certificate
Client	Root certificate

Figures

1. SSL_cert_sign.png
2. SSL_cert_export.png