

How to Create Certificates for a Client-to-Site VPN

<https://campus.barracuda.com/doc/29819544/>

Client-to-site VPNs need X.509 certificates to authenticate.

Follow the instructions in this article to create a server and client certificate with XCA for use with a client-to-site IPsec VPN.

Before You Begin

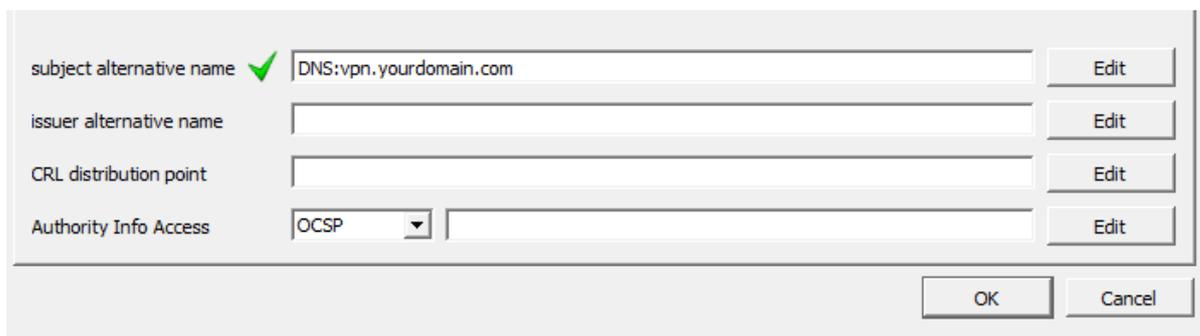
Create and export a root certificate in PEM format. For instructions, see [How to Create Certificates with XCA](#).

Step 1. Create a Server Certificate

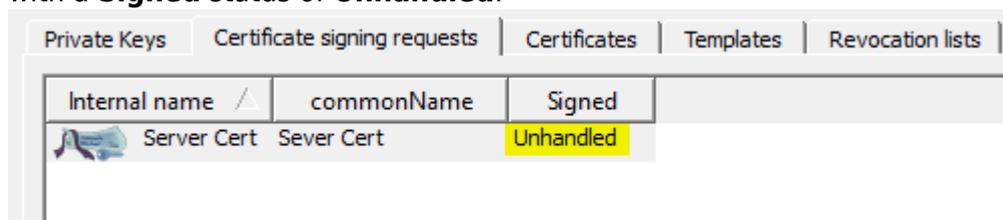
To create the server certificate:

1. In XCA, click the **Certificate signing requests** tab, and then click **New Request**. The **Create Certificate Signing Request** window opens.
2. Configure the identifying information.
 1. Click the **Subject** tab.
 2. Configure the settings 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**.
3. Configure the X.509 extensions.
 1. Click the **Extensions** tab.
 2. From the **Type** list, select **Not defined**.
 3. (Optional) Modify the **Validity** dates for the certificate.
 4. In the **subject alternative name** field, enter `DNS:vpn.yourdomain.com`. The hostname must resolve to the IP address that the VPN service is listening on.

As an alternative, iOS also supports the use of wildcards in the **subject alternative name**: `DNS:*`



4. Configure the key usage.
 1. Click the **Key usage** tab.
 2. From the left pane, select the following options:
 - **Digital Signature**
 - **Key Agreement**
 - **Certificate Sign**
5. Click **OK** to create the certificate. It then appears under the **Certificate signing requests** tab with a **Signed** status of **Unhandled**.

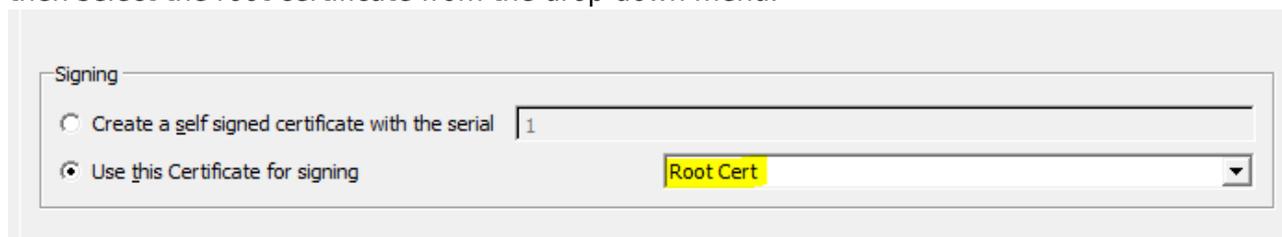


Private Keys	Certificate signing requests	Certificates	Templates	Revocation lists						
	<table border="1"><thead><tr><th>Internal name</th><th>commonName</th><th>Signed</th></tr></thead><tbody><tr><td>Server Cert</td><td>Sever Cert</td><td>Unhandled</td></tr></tbody></table>	Internal name	commonName	Signed	Server Cert	Sever Cert	Unhandled			
Internal name	commonName	Signed								
Server Cert	Sever Cert	Unhandled								

Step 2. Sign the Server Certificate

To sign the server certificate:

1. Click the **Certificate signing requests** tab.
2. Right-click the server 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. Create a Client Certificate

To create a client certificate:

1. Click the **Certificate signing requests** tab, and then click **New Request**. The **Create Certificate Signing Request** window opens.
2. Configure the identifying information.
 1. Click the **Subject** tab.
 2. Configure the settings 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**.
3. Configure the X.509 extensions.
 1. Click the **Key usage** tab.
 2. From the left pane, select **Digital Signature**.
 3. From the right pane, select **TLS Web Client Authentication**.
4. Click **OK** to create the certificate. It then appears under the **Certificate signing requests** tab with a **Signed** status of **Unhandled**.

Step 4. Sign the Client Certificate

To sign the client certificate:

1. Click the **Certificate signing requests** tab.
2. Right-click the client 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**.

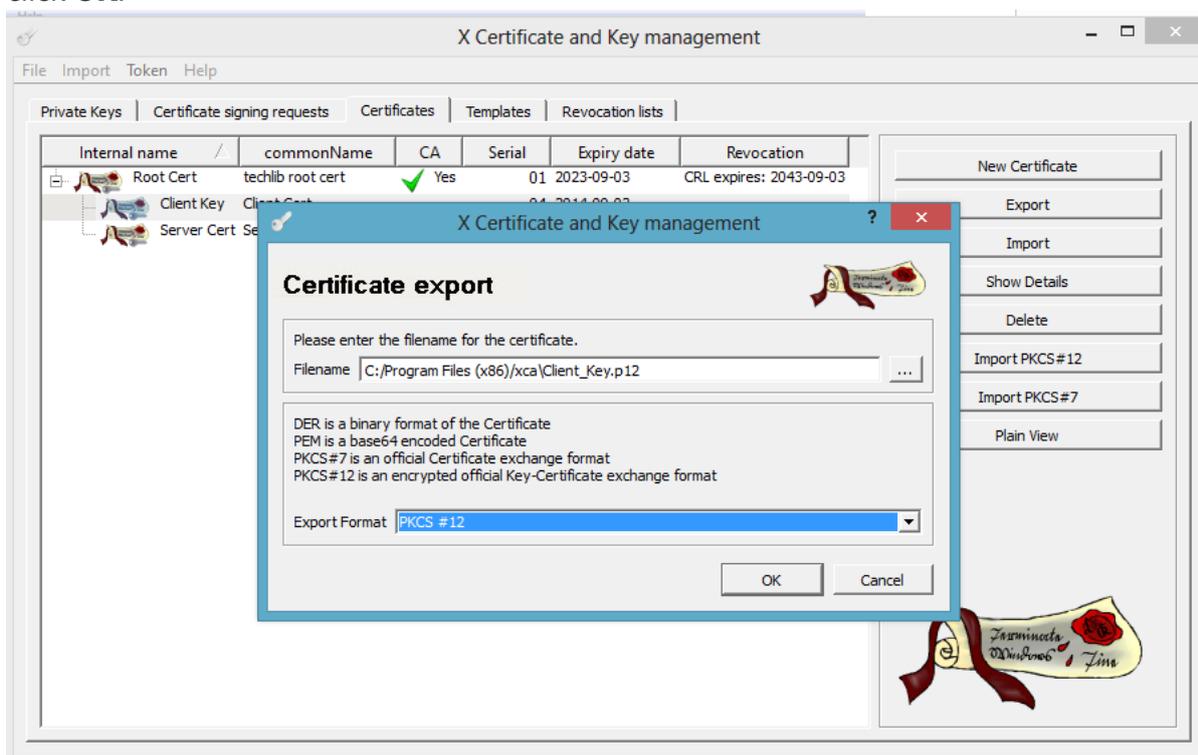


Private Keys	Certificate signing requests	Certificates	Templates	Revocation lists
	Internal name /	commonName	Signed	
	Client Key	Client Cert	✓ Signed	
	Server Cert	Sever Cert	✓ Signed	

Step 5. Export the Client and Server Certificates

You must export the client and server certificates as PKCS#12 files.

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



Next Steps

You can import the certificates on the Barracuda CloudGen Firewall and clients that need X.509 certificates. For Windows clients, you can use an Active Directory Policy to distribute the certificates automatically. 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 CloudGen Firewall	<ul style="list-style-type: none"> • Root certificate • Server certificate
Client	Client certificate

Figures

1. sub_alt_name_server_cert.PNG
2. server_cert_unsigned.PNG
3. choose_root_cert.PNG
4. keys_signed.PNG
5. cert_exp.jpg

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.