

# How to Create Certificates with XCA

#### https://campus.barracuda.com/doc/28475773/

When certificate-based authentication is required, you must have three types of X.509 certificates that come with a valid chain of trust:

- The trust anchor is the Certificate Authority (CA) signed root certificate.
- The server certificate for the Barracuda Networks appliance (e.g., Barracuda CloudGen Firewall).
- The client certificate for the VPN device (e.g., Barracuda VPN Client and iOS device).

If CA-signed X.509 certificates are not available, you can use self-signed certificates instead. These certificates must also have a valid chain of trust. Typically, X.509 certificates are created through a Public Key Infrastructure (PKI) that allows creating, signing, or revoking certificates. Examples of PKIs that you can use include Microsoft's PKI with Active Directory and **XCA - X Certificate and key management**. This article provides instructions on how to create certificates required for a complete chain of trust with XCA version 0.9.3 (September 2013).

### **Download and Install XCA**

- 1. Download XCA from <a href="http://sourceforge.net/projects/xca/">http://sourceforge.net/projects/xca/</a>.
- 2. Install XCA. You must have administrative rights.

#### **Create an XCA Database**

Each CA is stored in an XCA database file (\*.xdb). Use one XCA database for every PKI that you want to create.

- 1. Click File > New Database.
- 2. In the **Open XCA Database** window, enter the name for the XCA database and then click **Save**.
- 3. In the **New Password** window, enter a password to encrypt the private keys in the database file. You must enter this password whenever you open the XCA database.



of Open X	CA Database				×
		✓ 🖒 Search C	ertStor		Q
Organize 🔻 New folder				-	0
Desktop Name Name	Date modified No items match your sea	Type rch.	Size		
Win8 (C:)   BMD Leistungser  Mixed Linux Shar					
File name:       XCADatabase.xdb         Save as type:       XCA Databases (*.xdb )					>
Hide Folders		Sav	/e	Cancel	

#### **Create the Root Certificate**

The root certificate or CA is the trust anchor in the chain-of-trust. To create the root certificate:

- 1. Click the **Certificates** tab, and then click **New Certificate**. The **Create X509 Certificate** 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**.



Source Subject	Extensions Key usage Netscape Advanced
Internal name	X Certificate and Key management ? ×
localityName	New key   Please give a name to the new key and select the desired keysize   Key properties   Name   Root Cert   Keytype   RSA   Keysize   2048 bit

- 3. Configure the X.509 extensions.
  - 1. Click the **Extensions** tab.
  - 2. From the **Type** list, select **Certification Authority**.

Create x509 Certificate	Contraction of the
Source Subject Extensions Key usage Netscape Advanced	
Basic constraints	Key identifier
Type Certification Authority	Subject Key Identifier
Path length Critical	Authority Key Identifier

- 3. (Optional) Modify the **Validity** dates for the certificate. Usually, certificates are valid from five to ten years.
- 4. Configure the key usage.
  - 1. Click the **Key usage** tab.
  - 2. From the left pane, select the following items:
    - Digital Signature
    - Key Agreement



OK

Cancel

	X Certificate and Key management	?
eate x509 Certificate	Key usage Netscape Advanced	
Critical          Digital Signature         Non Repudiation         Key Encipherment         Data Encipherment         Certificate Sign         CRL Sign         Encipher Only         Decipher Only	Critical           TLS Web Server Authentication           TLS Web Client Authentication           Code Signing           E-mail Protection           Time Stamping           Microsoft Individual Code Signing           Microsoft Trust List Signing           Microsoft Server Gated Crypto           Microsoft Encrypted File System           Netscape Server Gated Crypto           Microsoft EFS File Recovery           IPSec End System           IPSec Tunnel           IPSec User           IP security end entity           Microsoft Smartcardlogin           OCSP Signing           EAP over PPP           EAP over Lan	g ning

5. Click **OK** to create the certificate. It then appears under the **Certificates** tab.

#### **Export the Root Certificate**

You must export the root certificate as a PEM file.

- 1. Click the **Certificates** tab.
- 2. Select the root certificate and then click **Export**.
- 3. In the **Certificate Export** window, select **PEM** from the **Export Format** list and then click **OK**.



Internal name	commonName	CA	Serial	Expiry date	Revocation		
Root Cert tec	hlib root cert	Ves	01	2023-09-03	CRL expires: 2043-09-03	3	New Certificate
Client Key Cli	-1 C - 1	v	Cortificat	to and Koy ma	nagomont	? ×	Export
🦾 🍂 Server Cert Se	•	^	Certifical	të anu key ma	nagement		Import
	Certificate	e expo	ort			Perminade Co	Show Details
Delete							
	Please enter the filename for the certificate.				Import PKCS#12		
					Import PKCS#7		
	DER is a binary format of the Certificate PEM is a base64 encoded Certificate				Plain View		
	PKCS#7 is an of PKCS#12 is an e	ficial Certifi encrypted o	cate exchang fficial Key-Ce	ge format ertificate exchange	format		
	Export Format	PKCS #12				<b>_</b>	
					ОК	Cancel	

### **Next Steps**

Create the certificates that are required by services for X.509 authentication. For instructions on how to create certificates for specific services, see the following table:

Service	Instructions
Client-to-Site VPN	To create certificates for a client-to-site VPN, go to <u>How to Create Certificates</u> for a Client-to-Site VPN.
SIP Proxy	To create a SSL certificate to encrypt SIP data, go to <u>How to Create Certificates</u> for the SIP Proxy.



#### Figures

- 1. create\_xca\_database.PNG
- 2. generate\_new\_key.PNG
- 3. extension\_select\_CA.PNG
- 4. key\_usage.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.