

## How to Manage Certificates in the Certificate Store



<https://campus.barracuda.com/doc/99123545/>

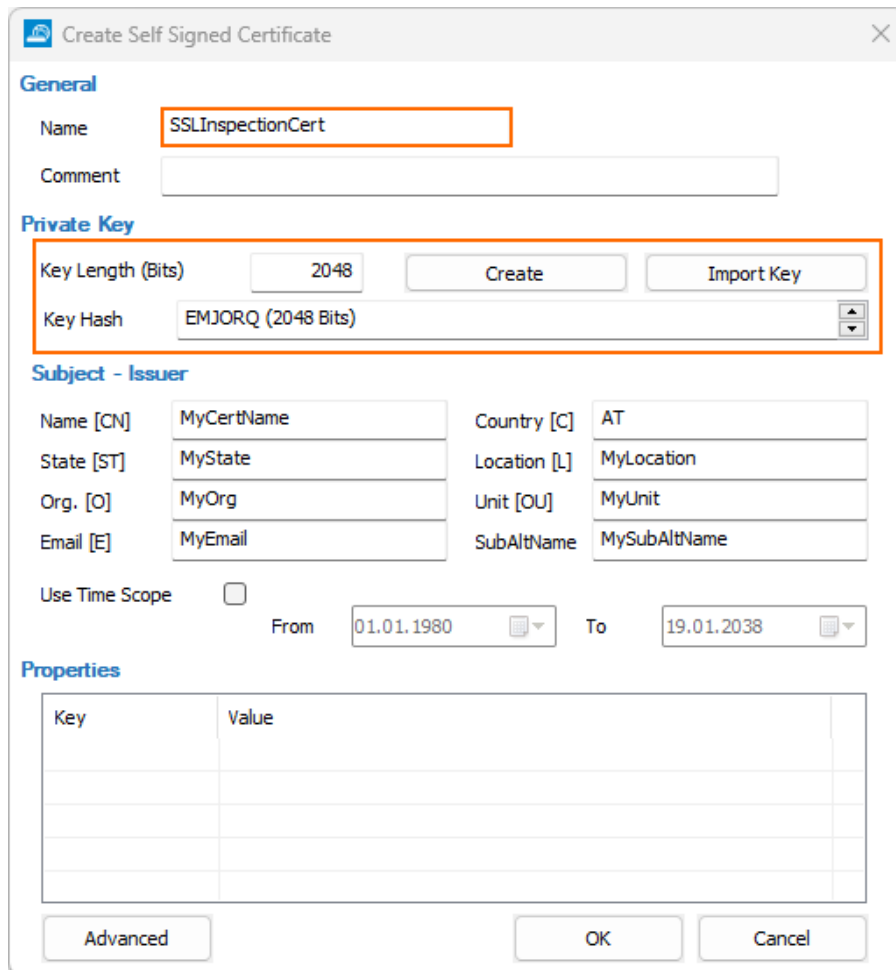
The certificate store allows administrators to manage certificates and certificate chains on the Control Center and stand-alone firewalls. The certificate store is available on stand-alone firewalls, and on the global, range, and cluster level on the Control Center for managed firewalls. Managed firewalls do not have their own certificate store and can only use certificates in the Control Center certificate stores. For information on how to view and manage certificate details, see [Certificate Store Page](#).

The certificate store can be used by the following services:

- CloudGen Firewall TLS Inspection. For more information, see [TLS Inspection in the Firewall](#).
- TLS/SSL Inspection for email traffic. For more information, see [Mail Security in the Firewall](#).
- CloudGen Firewall Access Control service. For more information, see [Access Control Service](#).
- Client-to-site, site-to site, and SSL VPN. For more information, see [VPN](#).

### Create a Certificate

1. Go to the certificate store:
  - Stand-alone Firewall – **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Certificate Store**.
  - Control Center Global – **CONFIGURATION > Configuration Tree > Multi-Range > Global Settings > Certificate Store**.
  - Control Center Range – **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > Range Properties > Certificate Store**.
  - Control Center Cluster – **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Cluster Properties > Certificate Store**.
2. Click **Lock**.
3. Right-click in the table, or click the certificate sign () at the top right of the window.  

4. Select **Create Self Signed Certificate**. The **Create Self Signed Certificate** window opens.
5. Enter a **Name** for the certificate.
6. Click **Create** to create a key, or chose an option to import the key:
  - **from Clipboard**
  - **from File**



The dialog box 'Create Self Signed Certificate' contains the following sections:

- General**: Name (SSLInspectionCert), Comment (empty).
- Private Key**: Key Length (Bits) (2048), Key Hash (EMJORQ (2048 Bits)).
- Subject - Issuer**: Name [CN] (MyCertName), State [ST] (MyState), Org. [O] (MyOrg), Email [E] (MyEmail), Country [C] (AT), Location [L] (MyLocation), Unit [OU] (MyUnit), SubAltName (MySubAltName).
- Use Time Scope**: From (01.01.1980) To (19.01.2038).
- Properties**: Table with Key and Value columns.

Buttons: Advanced, OK, Cancel.

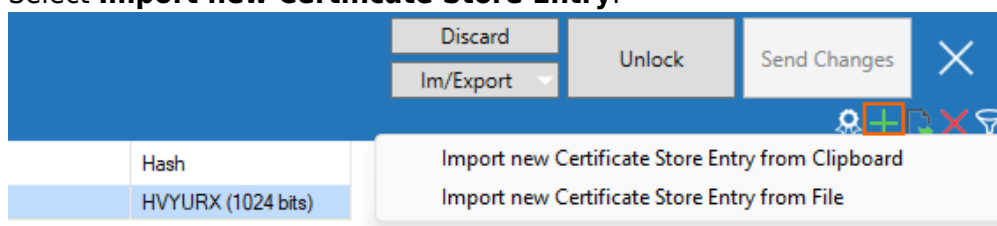
7. In the **Certificate** section click **Edit**.
8. Click **OK**.

The certificate is now added to the certificate store and can be used for configuration.

## Import a Certificate

If you must import a certificate, check if it is part of a certificate chain. If so, you must import the complete certificate chain into the certificate store so as not to break the chain of trust.

1. Go to the certificate store.
2. Click **Lock**.
3. Right-click in the table, or click the plus sign at the top right of the window.
4. Select **Import new Certificate Store Entry**.



5. Chose an option to import the certificate:
  - **from Clipboard**
  - **from File**
6. Select the certificate to import, and click **Open**.
7. Import the certificate.

The certificate is now added to the certificate store and can be used for configuration.

## Add Key to Certificate

If a certificate has no public key assigned, you can assign a key in the certificate store.

1. Right-click the certificate you want to add the key to.
2. Select **Assign Key to Certificate Store Entry** from the context drop-down menu.

Name	Ref by	Subject	Issuer	Is CA	Has...	Expires
MailServerCert	n				✓	
WebServerCert					✓	
			sj1net.com			03.04.2022
			sj1net.com	✓		02.04.2027
				✓		02.04.2027
				✓		03.04.2020

3. Import the key **from Clipboard** or **from File**.

## Export a Certificate

1. Go to the certificate store.
2. Click **Lock**.
3. Right-click the certificate you want to export.
4. Select **Export**.
5. Select your desired export option from the context drop-down menu.
6. Choose **to Clipboard** or **to File**.

Name	Ref by	Subject	Issuer	Is CA	Has...	Expires
MailServerCert	n				✓	
WebServerCert					✓	

7. When selecting **to File**, enter a name for the certificate and save it to a chosen location.

## Edit a Comment on a Certificate

In some cases, you might want to add extra information to a certificate entry. To do so, use the **Comment** field.

1. Select the **Comment** field for the certificate you want to add the comment to.
2. Click the pen icon in the top right corner of the field, or right-click the certificate and select **Edit Comment**.

Issuer	Is CA	Has Key	Expires	Comment
		✓		
		✓		
subCA2.sj1net.com			03.04.2022	
subCA1.sj1net.com	✓		02.04.2027	
rootCA.sj1net.com	✓		02.04.2027	
rootCA.sj1net.com	✓		03.04.2020	

3. Enter your comment.

## Delete a Certificate

1. Right-click the certificate you want to delete.
2. Select **Delete Certificate Store Entry** from the context drop-down menu.

You can also delete a certificate by selecting it and clicking the red cross sign (x) at the top right of the window.

## Enable the Certificate Store on a Control Center

1. Go to the **Range Properties** or **Cluster Properties** page.
  - Control Center Range - **CONFIGURATION > Configuration Tree > Multi-Range > your range > Range Properties**.
  - Control Center Cluster - **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Cluster Properties**.
2. Click **Lock**.
3. Set **Own certificate store Settings** to **Yes**.
4. Click **Send Changes** and **Activate**.

The certificate store is now added to the range or cluster.

## Figures

1. cert\_ico.png
2. cert\_create1.png
3. cert\_create2\_01.png
4. cert\_import.png
5. cert\_key.png
6. cert\_export.png
7. cert\_comment.png

© 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.