How to Configure PKI Certificates

https://campus.barracuda.com/doc/53248578/

To create a PKI certificate, use a predefined template or specify custom settings. Certificate templates can also be added and edited. You can also export and import certificates.

Before You Begin

Before creating your Barracuda NextGen Control Center PKI certificates, you must create and configure the PKI service. For more information, see How to Configure the PKI Service.

Create a Certificate

1. Click the **PKI** tab.
2. Click **Lock**.
3. Click **Create Certificate**.
4. In the **Create Certificate** window, specify the general settings for the certificate:
   - **Signing CA** – Select the certificate authority that must sign the new certificate.
   - **CA Sign Password** – The password required for the CA signature. If you do not enter a password, a request is created instead of a certificate.
   - **Template** – Select a predefined template that you can edit to create the certificate.
5. From the **General Settings**, **Subject**, and **V3 Extensions** tabs, you can edit additional certificate settings. For more information about these settings, see PKI Certificate Settings.

Configure a Certificate Template

You can add a new template or edit an existing template.

1. Click the **PKI** tab.
2. Click **Lock**.
3. Click **Edit Templates**.
4. To edit an existing template:
   1. From the **Select Template** list, select the required template.
      From the **General Settings**, **Subject**, and **V3 Extensions** tabs, edit the template settings. For more information about these settings, see PKI Certificate Settings.
   2. Click **Save Template**.
5. To add a new certificate template:
   1. In the **Select Template** field, enter a name for the new template

2. From the **General Settings**, **Subject**, and **V3 Extensions** tabs, edit the template settings. For more information about these settings, see PKI Certificate Settings.
3. Click **Save Template**.

Try to avoid deleting predefined templates. A predefined template can only be restored by deleting and recreating the PKI service. When you delete the PKI service, all PKI certificates are also deleted.

Import a Certificate

1. Click the **PKI** tab.
2. Click **Lock**.
3. Click **Import Certificate**.
4. In the **Import Certificate** window, select the required certificate and enter the certificate password.
5. Click **Import**. The PKI reloads the certificates automatically. If available, an end-user certificate is added to the signing certificate.

Export a Certificate

1. Click the **PKI** tab.
2. Click **Lock**.
3. Right-click the certificate and select **Export Certificate**.
4. In the **Export Certificate** window, select the export format and private key.
5. Click **Save to File**.

View and Manage Certificates

On the **PKI** page, the certificates are listed in a hierarchical tree. The top level shows all root certificates that need to be certificate authorities. Additionally, there are the box certificates to get information about all the NextGen F-Series Firewalls that are managed by the Barracuda NextGen Control Center. This information is generated automatically when the PKI service is started. By default, the common name of each certificate is displayed. To display the full subject of each certificate, right-click a root node and select **Show Full Subject**. Each CA node contains four subdirectories:

- **Valid** – Contains all valid certificates that have not expired.
- **Pending** – Contains all unsigned certificate requests.

- **Expired** – Contains all expired certificates.
- **Revoked** – Contains all certificates that have been revoked by the administrator.

The following table provides instructions on how to manage the certificates, requests, and private keys in the subdirectories of each CA node:

Task	Instructions
View certificate settings	Right-click the certificate and select **View Certificate**. In the **View Certificate** window, all of the certificate settings are displayed.
Revoke a certificate	In the **Valid** folder, right-click the certificate and select **Revoke Certificate**. When prompted, enter the parent **CAs Sign Password**. The revoked certificate is moved to the **Revoked** folder.
Delete a request	In the **Pending** directory, right-click the request and select **Delete Request**. Click **Yes**.
Approve a request	Right-click the request and select **Approve Request**. A window opens and displays the values of the request. Enter the sign password of the CA.
Export a private key from a certificate	Right-click the certificate and select **Export Private Key**. In the **Export Private Key** window, select an export format. You can save the private key to a file or the clipboard. For exporting to clipboard only PEM format is allowed since DER is a binary format.

Export a CRL	A Certificate Revokation List (CRL) is a list of client certificates that were revoked before they expired. To export a CRL, right-click the CA and select **Export CRL**. In the **Export CRL**window, select an export format. Enter the CA password and how many days the CRL is valid.You can save the CRL to a file, clipboard, or distribution points. The distribution points are on the ldap server as configured in the PKI service configuration and the local http server of the CC box. The CRL is accessible at:
	`ldap://mcip/cn=CommonName,dc=AsInConfig`
	`ldaps://mcip/cn=CommonName,dc=AsInConfig`
	`mcip/pki/CommonName.crl`
	Example:
	`192.168.10.10/pki/VPN-Root.crl`
	`ldaps://192.168.10.10/cn=VPN-Root,dc=barracuda,dc=com`
	To grant access to the local http server, create a local redirect rule for the Barracuda NextGen Control Center.

Search a certificate	Right-click the certificate and select **Search Certificate**. In the **Search Certificate** window, enter your search criteria. For example, if you enter `lient` in the **Common Name** field, all certificates containing this string in the common name will be found. Certificates that contain words such as *Client, Client,* or *MILIENT* are listed in your search results. To step through all the certificates in your search results, press **F3**.