How to Use and Manage Certificates with the Certificate Manager

https://campus.barracuda.com/doc/44434291/

The Barracuda NextGen Firewall X-Series uses the Certificate Manager as a central repository to manage all X.509 certificates on the device. You can create self-signed certificates or upload your own certificates. All certificates are available for all X-Series Firewall services, as long as they meet the requirements for that service.

Create a Self-Signed Certificate

1. Go to **ADVANCED > Certificate Manager**.
2. Click **Create**. The **Create Certificate** pop-over opens.
3. Enter the certificate information.
    - **Certificate Name** – Enter a name to identify this certificate.
    - **Common Name** – Enter the domain name (DN) that is used to access the service, e.g., "mycompany.vpn.com", **.domain.com* It must contain at least one dot (**.**)
    - **Country Code (2 characters)** – Enter the two–letter ISO country code of the location of the organization.
    - **State or Province** – Enter the full name of the state or province of the location of the organization.
    - **Location** – Enter the full name of the city where the organization is located.
    - **Organization** – Enter the name of your organization or company.
    - **Organizational Unit** – Enter the department or unit within the organization.
    - **Key Size (bits)** – Select the private key size for the certificate from the dropdown list. The default key size is 2048 bits. Use 2048 bits if you want stronger and more secure encryption.
    - **Disallow Private Key Download** – Selecting this option will lock the private key corresponding to this certificate. Normally, certificates are downloaded in PEM format, which includes the private key and certificate. When a key is locked, the PEM file will only contain the certificate.

      > Private keys are not included in the backup. Download the private key and keep it in a safe location.

    - **Expiration Date** – Click the calendar icon to select a date.
    - **Subject Alt Name** – Set the **Email**, **DNS**, **URI** or **IP** for this certificate.

      > For a Client–to–Site VPN connection to a mobile device, set the DNS to the FQDN of the X-Series Firewall. The FQDN must resolve to the IP address of the VPN service on the X-Series Firewall.

    - **Add to VPN Certificates** – Automatically add this certificate to the list of VPN certificates. You can also manually add the certificate to the VPN certificates later on the **VPN > Settings** page.
4. Click **Save**.

Upload a Certificate

You can upload certificates in PEM or PKCS12 files. PEM files can either contain a single certificate or multiple certificates. Multiple PEM files must contain one or more certificates and the private key in order to create a complete chain of trust.

1. Go to **ADVANCED > Certificate Manager**.
2. Click **Upload**. The **Upload Certificate** pop-over opens.
3. Enter the **Certificate Name**.
4. Select the **Certificate Type** to match your certificate file.
5. (optional) If you want to use the certificate for the VPN service, select **Add to VPN Certificates**.
6. Click **Browse** to select the **Certificate File**.
7. (multiple PEM files) Click **Browse** to select the **Certificate Key File**.
8. (optional) Enter a **Certificate Password**.
9. (optional) Select **Disallow Private Key Download**. This action cannot be reversed.

   > Private keys are not included in the backup. Download the private key and keep it in a safe location.
10. Click **Save**.

Download or View a Certificate or Certificate Signing Request (CSR)

1. Go to **ADVANCED > Certificate Manager**.
2. Click ✏ to open the **View Certificate** pop-over.
3. You can now:
   - Click **Details** to see the complete certificate information.
   - Click **Lock Key** to disable the private key download. This change is permanent.
   - Click **Replace Upload** to upload a new certificate. You cannot upload a new certificate if the old certificate has already expired.
   - Click **Replace Self-Signed** to create a new self-signed certificate. You cannot create a new self-signed certificate if the old certificate has already expired.
   - Click **Download Certificate** to download the certificate in a PEM file.
   - Click **Download Key** to download the private key in a PEM file.
   - Click **Download CSR** to download a *.csr file. Submit the CSR to your certificate authority to received signed SSL certificates.

Delete a Certificate

You cannot delete certificates that are in use. Change the certificate for all services listed in the

Usage column and then click 🗑 in the **Action** column to delete the certificate.

Add Certificates to the VPN Certificates

Certificates that are to be used for the VPN service must be added to the VPN certificates. If you did not select **Add to VPN Certificates** when creating or uploading the certificates, you can also add it to the VPN Certificates in the **VPN Settings**. Root CA certificates must be CA certificates.

1. Go to **VPN > Settings**.
2. Select the certificate you want to add from the **Local Certificates** dropdown and click **+**.
3. Select the certificate you want to add from the **Root CA Certificates** dropdown and click **+**.
4. Click **Save**.

Select the SSL Inspection Certificate

You can only use certificates with the **CA** option for SSL Inspection.

1. Go to **FIREWALL > Settings**.
2. Verify that **Enable SSL Inspection** is set to **Yes**.
3. Select the certificate from the **Select Certificates** dropdown.
4. Click **Save**.

Select the SSL Certificate for the Web Interface

1. Go to **ADVANCED > Secure Administration**.
2. Select the certificate from the **Certificate for SSL** dropdown.
3. Click **Save**.

Select the SSL Certificate for the SSL VPN

It is recommended to use signed certificates for the SSL VPN service.

1. Go to **VPN > SSL VPN**.
2. Click on the **Server Settings** tab.
3. Select the certificate from the **Certificate** dropdown.
4. Click **Save**.

Figures