How to Set Up Barracuda VPN CA VPN Certificates

https://campus.barracuda.com/doc/17322/

If you are using a client-to-site or site-to-site tunnel using the Barracuda VPN CA, you can either create the certificates directly in the VPN settings via Barracuda Firewall Admin or import certificates from an external CA.

This article describes the specific use case of how to set up Barracuda VPN CA certificates. These certificates are used in a large number of use cases.

Therefore, note that the practical relevance of this article depends on the parent use case that gives overall meaning to this article.

Step 1. Create Default Server Certificate and Key

You can create the certificate via Barracuda Firewall Admin or import external certificates.

Create Certificate and Private Key in Barracuda Firewall Admin

VPN certificates generated directly in the VPN settings are signed by the self-signed Barracuda root certificate of the firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. In the left menu, select **General**.
3. Click **Lock**.
4. In the **Default Server Certificate** field, select **explicit**.
5. Expand the drop-down menu next to the **Private key** field.
6. Select **Create new key**.

7. Next to **Key Length**, select **2048 Bit** for fully licensed firewalls or **512 Bit** for export-restricted firewalls or firewalls in demo mode.
8. Click **OK**.
9. Expand the drop-down menu next to the **Certificate** field.
10. Select **Create new certificate**.

11. Fill in the **Subject** section.

Certificate View   ✕

Subject

Name [CN]	myvpn.domain.com	Country [C]	AT
State [ST]	Tirol	Location [L]	Austria
Org. [O]	Barracuda Networks	Unit [OU]	Information Development
Email [E]	admin@myvpn.domain.com	SubAltName	DNS:myvpn.domain.com

Use Time Scope ☑

From 01.01.1970 ▦▾   To 19.01.2038 ▦▾

12. Click **OK**.
13. Click **Send Changes** and **Activate**.

The **Default Server Certificate** and the **Private Key** are now listed with a valid (green) signature.

Service

Listen on port 443	☑
Local VPN listen port	691 ▾
Maximum number of tunnels	<auto> ▾
CRL poll time (minutes)	0
Site to Site authentication	☑
Add VPN routes to main routing table	No ▾
Allow concurrent user sessions	☑
Use Perfect Forward Secrecy	Yes ▾
Accounting information storage time (days)	14
Send SDWAN data to Control Center	<auto> ▾
Log VPN user accounting	Off ▾
Log SDWAN	Off ▾
C2S Reconnect Cache Timeout	30

Default Server Certificate	✅	<explicit> ▾
Private key	✅	Hash: LQNVWR 2048 Bits ⚙▾
Certificate	✅	Hash: LQNVWR 2048 Bits (self signed) ⚙▾
Certificate Chain		No Certificate Chain present ⚙▾

Import Certificate and Private Key

You can also import certificates created in an external CA into the Barracuda VPN CA.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Expand the drop-down menu next to the **Private key** field.
4. Select **Import from File** and import the private key.
5. Expand the drop-down menu next to the **Certificate** field.
6. Select an import option for the external certificate, depending on the format.
7. Click **Send Changes** and **Activate**.

If the certificates are valid, the **Default Server Certificate** and the **Private Key** are now listed with a valid (green) signature.

Step 2. Create a Service Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, select **Service Keys**.
4. Right-click the table and select **New Key**.
5. Enter a **Key Name** and click **OK**.
6. Select the **Key Length** and click **OK**.
7. Click **Send Changes** and **Activate**.

Your key appears under the **Service Keys** tab.

Continue your configuration setup and return to the article you came from.

Figures

1. new_key.png
2. cuda_ca.png
3. ca_cert_01.png