

How to Set Up Barracuda VPN CA VPN Certificates

<https://campus.barracuda.com/doc/96026074/>

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.

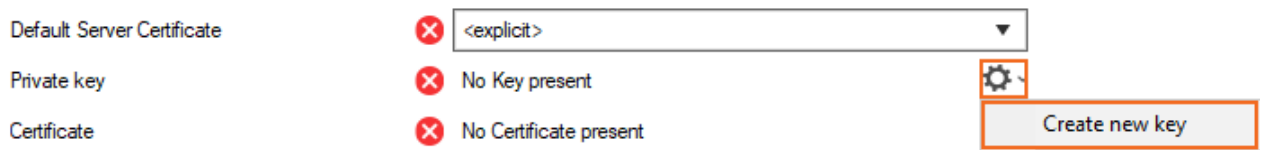
Step 1. Create Default Server Certificate and Key




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**.



Default Server Certificate	 <explicit>
Private key	 No Key present
Certificate	 No Certificate present

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 To

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	<input checked="" type="checkbox"/>
Maximum number of tunnels	<input type="text" value="<auto>"/>
CRL poll time (minutes)	<input type="text" value="0"/>
Site to Site authentication	<input checked="" type="checkbox"/>
Add VPN routes to main routing table	<input type="text" value="No"/>
Allow concurrent user sessions	<input checked="" type="checkbox"/>
Use Perfect Forward Secrecy	<input type="text" value="Yes"/>
Accounting information storage time (days)	<input type="text" value="14"/>
Send SDWAN data to Control Center	<input type="text" value="<auto>"/>

Default Server Certificate	 <input type="text" value="<explicit>"/>
Private key	 Hash: LQNVWR 2048 Bits 
Certificate	 Hash: LQNVWR 2048 Bits (self signed) 

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.

Figures

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