

How to Set Up Barracuda VPN CA VPN Certificates

<https://campus.barracuda.com/doc/73719104/>

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

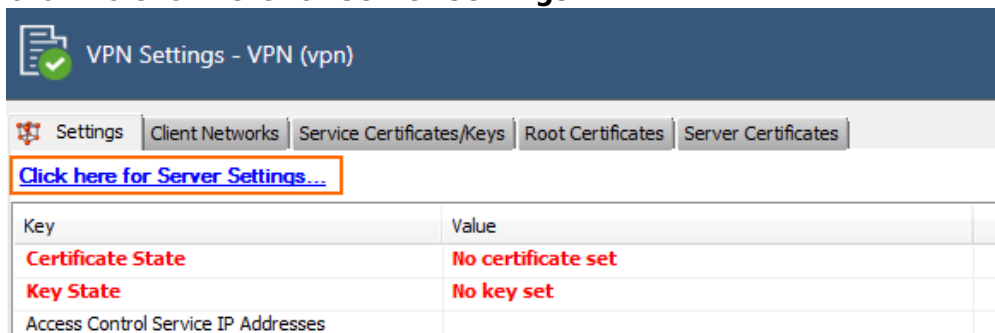
Step 1. Create Default Server Certificate and Key

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

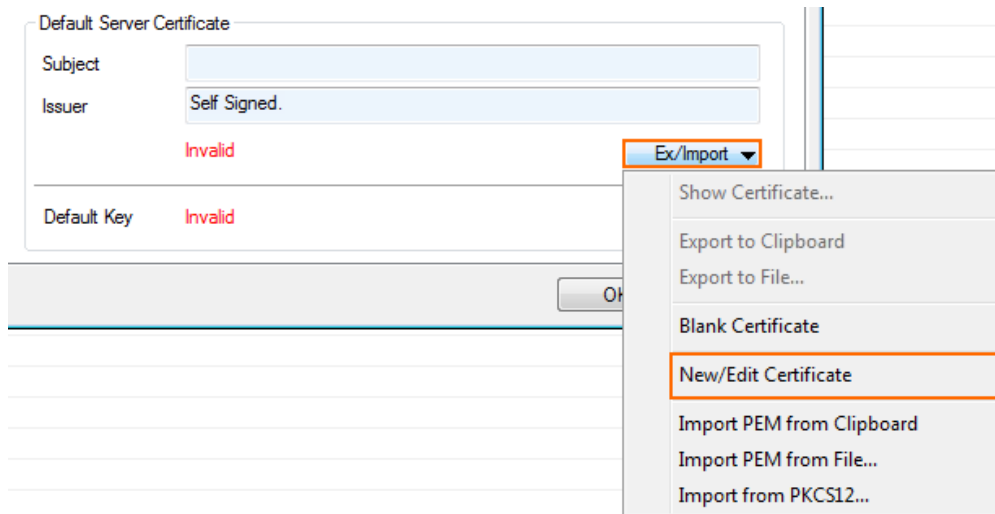
Create Certificate and Private Key in Barracuda Firewall Admin

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

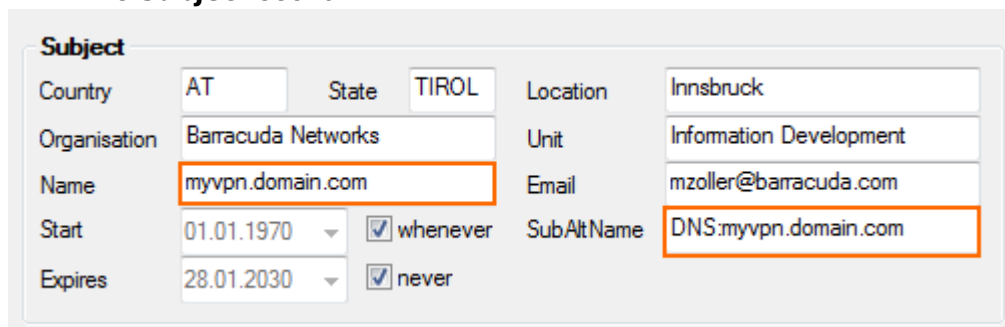
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Settings** tab.
4. Click the **Click here for Server Settings** link.



5. In the **Default Server Certificate** section, click **Ex/Import** and select **New/Edit Certificate**. The **Certificate View** window opens.



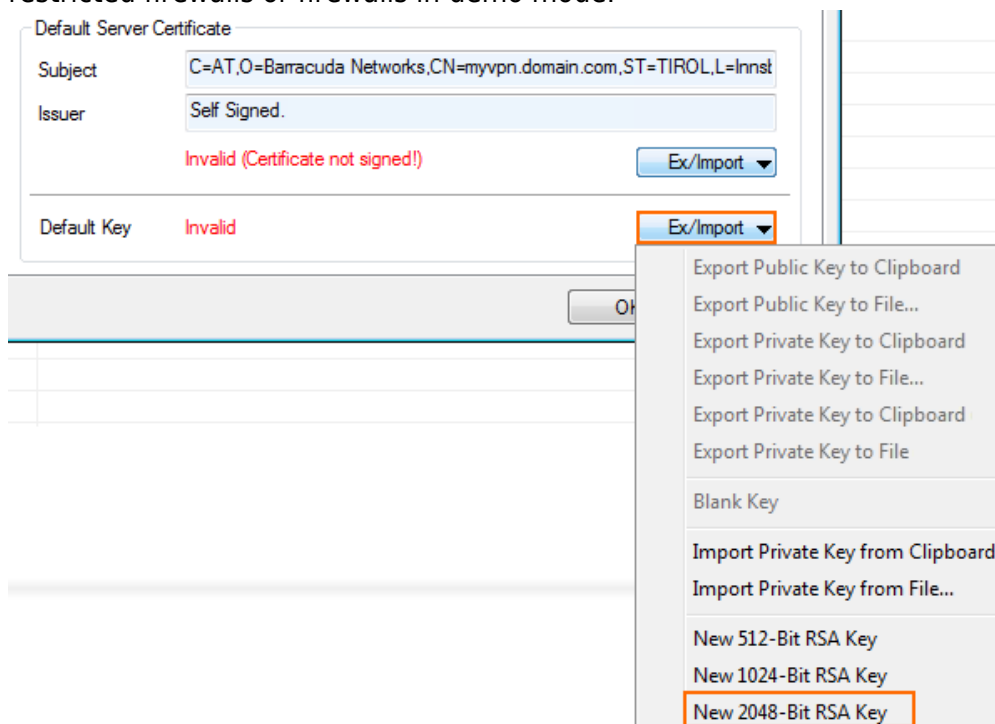
6. Fill in the **Subject** section.



7. Click **OK**.

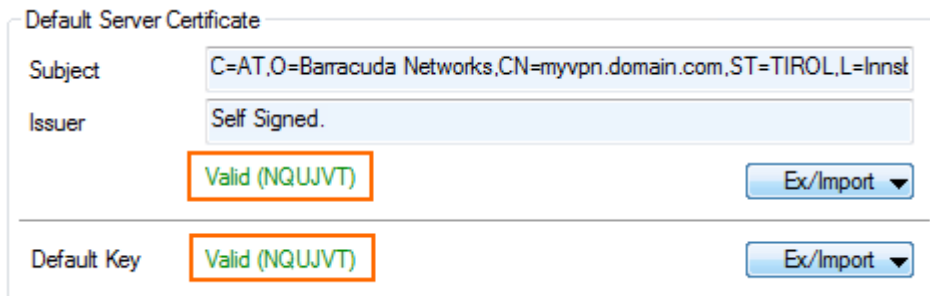
8. In the **Default Key** section, click **Ex/Import**.

9. Select **New 2048-Bit RSA key** for fully licensed firewalls or **New 512-Bit RSA key** for export restricted firewalls or firewalls in demo mode.



10. Click **Yes**.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.

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



Default Server Certificate	
Subject	C=AT,O=Barracuda Networks,CN=myvpn.domain.com,ST=TIROL,L=Innst
Issuer	Self Signed.
	Valid (NQUJVT) Ex/Import ▼

Default Key	Valid (NQUJVT) Ex/Import ▼

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 > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Settings** tab.
4. Click the **Click here for Server Settings** link.
5. In the **Default Server Certificate** section, click **Ex/Import** and select either **Import PEM from file** or **Import from PKCS12**, depending on the external certificate format.
6. In the **Default Key** section, click **Ex/Import** and select **Import Private Key from File**.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

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

Step 2. Create a Service Certificate/Key

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Service Certificates/Keys** tab.
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 server certificate appears under the **Service Certificates/Keys** tab.

Settings	Client Networks	Service Certificates/Keys	Root Certificates	Server Certificates
Keyname	Hash	Comment	Bits	
VPNServiceCertKeys	VWTXOK		2048	

Figures

1. cuda_ca_01.png
2. cuda_ca_02.png
3. cuda_ca_03.png
4. cuda_ca_04.png
5. cuda_ca_05.png
6. cuda_ca_06.png

© Barracuda Networks Inc., 2020 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.