Getting Started

https://campus.barracuda.com/doc/2458427/

Follow the instructions in this guide after you complete the steps explained in the Barracuda SSL VPN Quick Start Guide (PDF) that shipped with your appliance or the Barracuda SSL VPN Vx Quick Start Guide if you are using a Barracuda SSL VPN Vx.

Before you begin

- Install Java Runtime version 1.6 or above on your client computers.
- Register a full DNS name for the Barracuda SSL VPN (e.g., `sslvpn.example.com`).
- (Recommended) Purchase an SSL certificate signed by a trusted CA.

Step 1. Install the SSL certificate

To prevent certificate errors whenever your users connect to the Barracuda SSL VPN, it is recommended that you install an SSL certificate signed by a trusted CA. You can generate the signing request directly on the Barracuda SSL VPN. Your SSL certificate must use the full DNS name (e.g., `sslvpn.example.com`) for the **Common Name** attribute.

Step 1.1. (Optional) Generate a CSR request

To generate a CSR request:

1. Log into the appliance web interface (e.g., `https://sslvpn.example.com:8443`).
2. Go to the **BASIC > SSL Certificate** page.
3. From the **Certificate Type** list, select **Trusted (Signed by a trusted CA)**.
4. In the **Trusted (Signed by a trusted CA)** section, click **Edit Data**.
5. In the **CSR Generation** window, enter the full DNS name (e.g., `sslvpn.example.com`), enter the requested information about your organization, and then click **Save Changes**.
6. Click **Download CSR**.

You can now submit the CSR to your Certificate Authority.

Step 1.2. Upload signed certificates

When the certificates are uploaded to the Barracuda SSL VPN, the **Certificate Candidates** table displays the current status of the certificates. The **Status** column displays **OK** when all required certificates have been uploaded.

1. Log into the appliance web interface (e.g., `https://sslvpn.example.com:8443`).
2. Go to the **BASIC > SSL Certificate** page
3. From the **Certificate Type** list, select **Trusted (Signed by a trusted CA)**.
4. In the **Trusted (Signed by a trusted CA)** section, upload the certificates that you received from the CA in the following order:
    1. Root CA certificate (PEM or PKCS12)
    2. (Depending on your CA) Intermediate CA certificate (PEM or PKCS12)
    3. SSL server certificate (PEM or PKCS12)
5. Click **Use**.
6. In the **Synchronize SSL** section, click **Synchronize**.

Your SSL certificate is now installed on both the appliance and the SSL VPN web interface. To avoid Java runtime certificate errors, use the full DNS name to connect to your Barracuda SSL VPN.

Step 2. Configure system contact and alert e-mail addresses

Specify the e-mail addresses of those who should receive notifications from the Barracuda SSL VPN and emails from Barracuda Central.

1. Log into the appliance web interface (e.g., `https://sslvpn.example.com:8443`).
2. Go to the **BASIC > Administration** page.
3. In the **Email Notification** section, enter the e-mail addresses of those who should receive system alerts and security news and updates.
4. Click **Save Changes**.

Step 3. Change the administrator's password for the SSL VPN web interface

Change the password used by ssladmin to log into the SSL VPN web interface.

1. Log into the SSL VPN web interface (e.g., `https://sslvpn.example.com`) with the default username and password of `ssladmin`.
2. Click **Manage System**, and then go to the **ACCESS CONTROL > Accounts** page.
3. In the **Accounts** section, locate the ssladmin user and click **More**.
4. Select **Set Password**.
5. Enter the new password and click **Save**. The password must conform to the password rules defined for the appliance.

Next steps

After you set up and explore the Barracuda SSL VPN, you can complete the following tasks:

Task	Articles
Configure a User Database.	• How to Configure User Databases • Example - Create a User Database with Active Directory
Configure Authentication Schemes.	Authentication Schemes
Configure Policies.	How to Configure Policies
Configure Access Rights.	Access Rights
Configure Resources.	Resources
(Optional) Configure L2TP/IPsec or PPTP access.	• How to Configure IPsec • How to Configure PPTP