

## Point-to-Site

<https://campus.barracuda.com/doc/98223657/>

Barracuda SecureEdge offers point-to-site capabilities. Point-to-site connections are used to connect an individual device, such as a laptop, to the company network. The VPN client running on the client connects to the VPN service of Barracuda SecureEdge. Site authentication allows devices physically located within the network to authenticate against the Barracuda SecureEdge service to enforce [Security Policies](#).

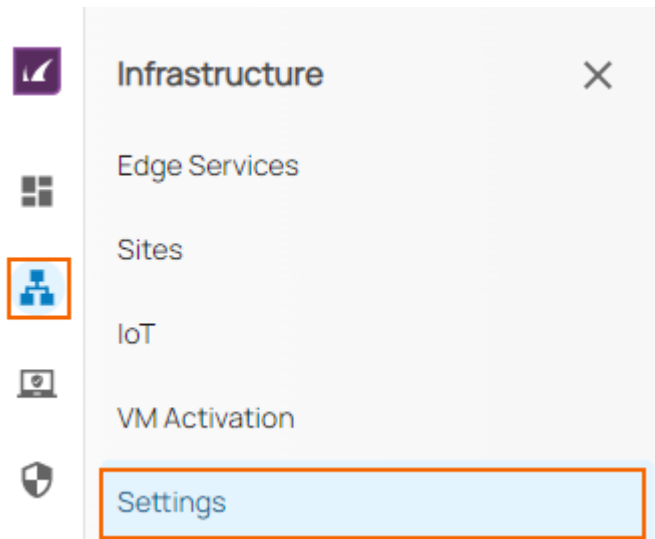
### Before You Begin

- If you want to use your Microsoft Entra ID users and groups for User Connectivity, Site Authentication, and [Security Policies](#), you must first connect your Microsoft Entra ID with Barracuda Cloud Control in order to synchronize users and groups.
- If you do not synchronize Microsoft Entra ID with Barracuda Cloud Control, you must create a user account in Barracuda Cloud Control for each of your users using User Connectivity. For more information, see [How to Connect Your Microsoft Entra ID with Barracuda Cloud Control](#).
- Create a SAML endpoint in Microsoft Azure. For more information, see [How to Create a SAML Endpoint in Microsoft Azure and Basic User Connectivity & Personal Security Configuration](#).
- If you are using a firewall, you must allow certain Barracuda and Microsoft domains before you continue. For more information, see [List of Required Barracuda Authentication & Discovery Services for Point-to-Site & Personal Security](#).

### Step 1. Enable / Disable User Connectivity and Site Authentication

For more information on the configuration, see Step 2 of [How to Create a SAML Endpoint in Microsoft Azure and Basic User Connectivity & Personal Security Configuration](#).

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. Go to **Infrastructure > Settings**.



3. The **Settings** window opens. Specify values for the following:

- **Enable User Connectivity** – Click to enable/disable.
- **Enable Site Authentication** – Click to enable/disable.

Point To Site

☒ Enable User Connectivity

☒ Enable Site Authentication

CLIENT NETWORK CONFIGURATION

The Client Network is used to assign IPs to clients that connect via User Connectivity. It is divided into pools that are then distributed to the Edge Services and sites. Sites are provided one pool for each User Connectivity enabled static WAN. Edge Services are automatically provided multiple pools depending on their deployed Scale Unit.

4. Click **Save**.

## Step 2. User Enrollment

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. Go to **Infrastructure > Settings**.
3. Scroll down to **USER ENROLLMENT**.
4. Copy the enrollment link and send it to the user, or click on **Email Invites**.

USER ENROLLMENT

Users can download the VPN client and enroll from this page: <https://cloudgenwan-demofeaturestr.dev.qa.cudaops.com/enrol/1> 

You can also email enrollment invitations using the tool below:

**Email Invites**

5. After clicking on **Email Invites**, the **Send Enrollment Invitations** window opens. Specify values for the following:
  - **To** – Enter an email address, or select user/groups from the drop-down menu. Note: To select user or groups, you must enable synchronization between Cloud Control and your Microsoft Entra ID. For more information, see [How to Connect Your Microsoft Entra ID with Barracuda Cloud Control](#).

- **Subject** – Keep the subject or enter your own subject.
  - **Body** – Keep the text or enter your own text.
6. Click **Send**.

### Step 3. Connect a Client

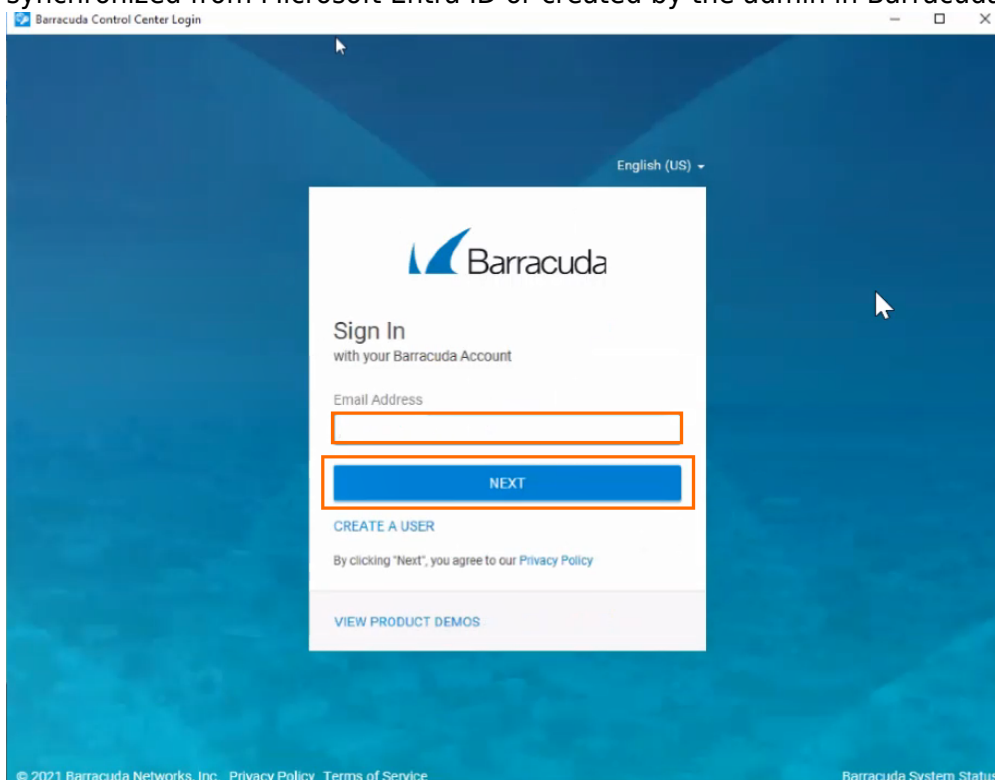
1. Install the VPN client. Open the link for enrollment retrieved in Step 2 and download the VPN client.
  - For more information on the installation on a Windows client, see [Installing the Barracuda Network Access/VPN Client for Windows](#).
  - For more information on the installation on a Mac client, see [Installing the Barracuda VPN Client for macOS](#).



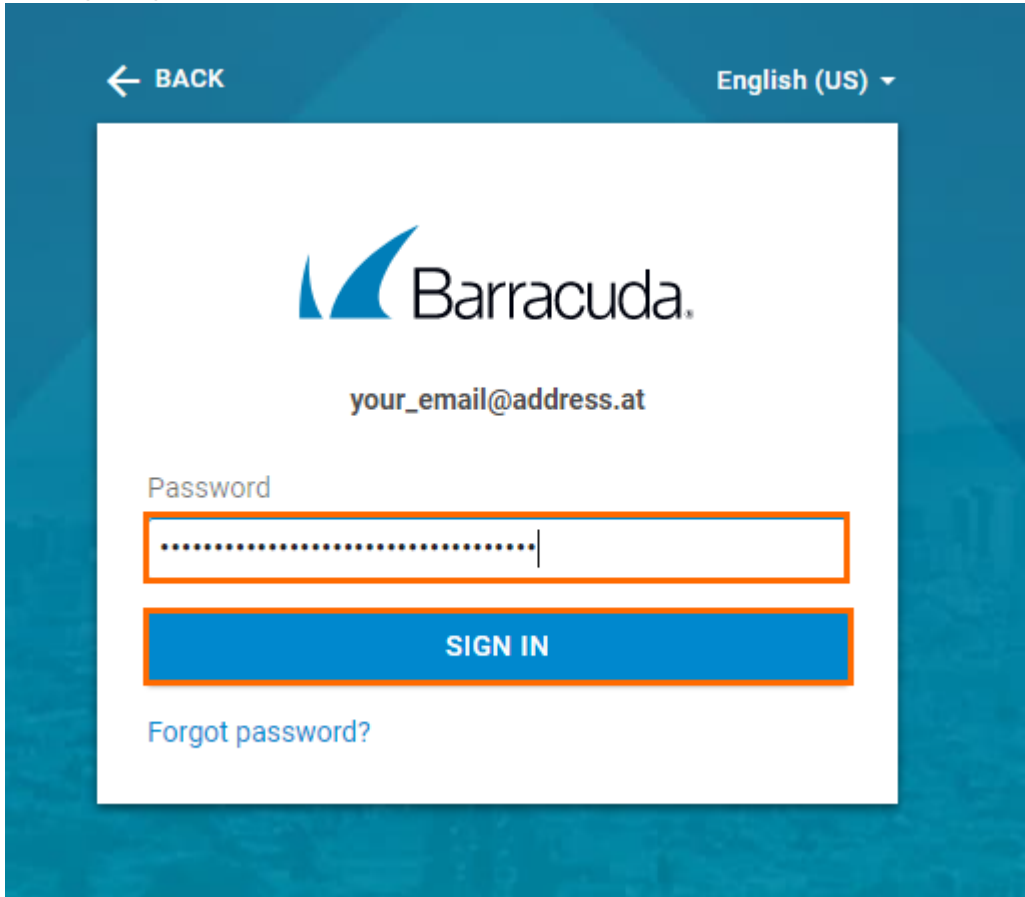
2. Click **Enroll now**.



3. The Barracuda VPN client opens and the user must log in with the credentials that were either synchronized from Microsoft Entra ID or created by the admin in Barracuda Cloud Control.

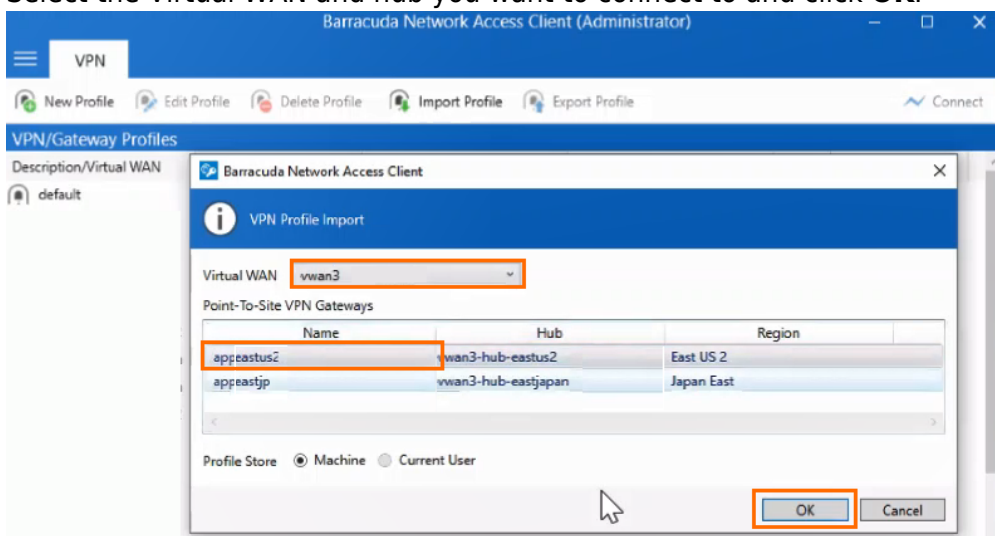


4. Click **NEXT**.
5. Enter your password and click **SIGN IN**.

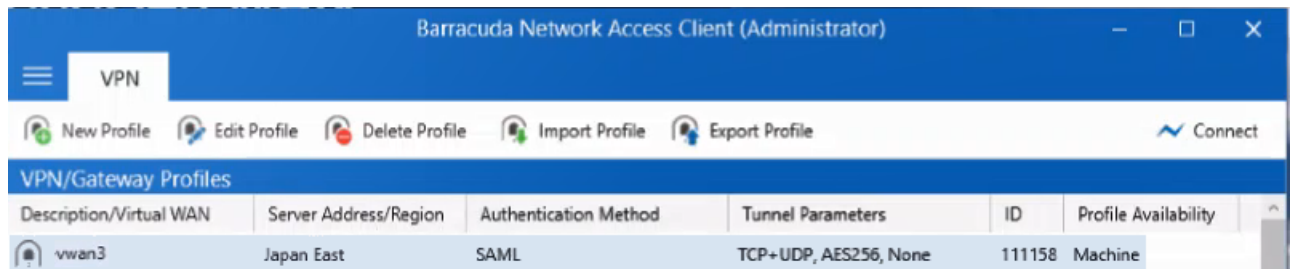


The login screen features a blue header with a 'BACK' button and a language dropdown set to 'English (US)'. The Barracuda logo is centered above the email field, which contains 'your\_email@address.at'. Below the email field is a 'Password' label and a password input field with a masked password '.....'. An orange box highlights the password field and the 'SIGN IN' button below it. A 'Forgot password?' link is located at the bottom left of the login area.

6. The profile is imported in the VPN client and opens automatically.
7. Select the Virtual WAN and hub you want to connect to and click **OK**.



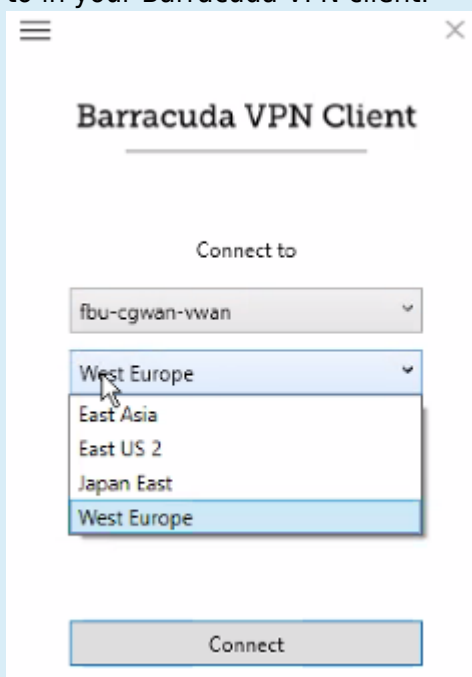
8. The new profile is imported and appears in the list.



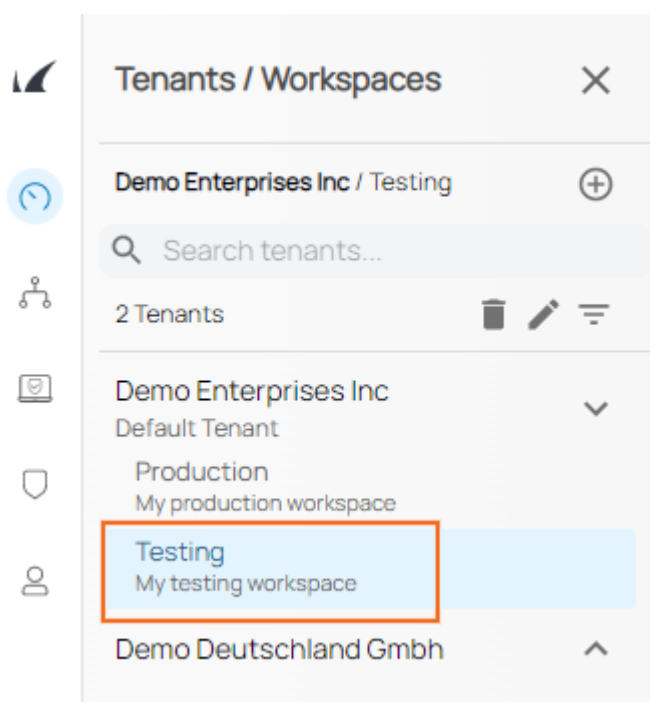
9. Follow this guide to establish a connection: [How to Establish a VPN Connection Using Barracuda VPN Client for Windows](#) or [How to Establish a VPN Connection Using Barracuda VPN Client for macOS](#).
10. All available Barracuda SecureEdge VPN endpoints are in the Barracuda VPN client.

#### Step 4. (Optional) Download the VPN Profile from the Edge Service or Site

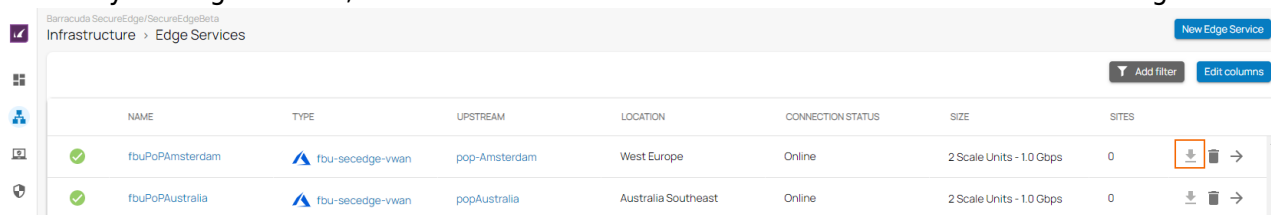
Note: When importing the VPN profile, you can either import a Site VPN profile or a Gateway VPN profile. Barracuda SecureEdge will automatically add all available VPN endpoints to connect to in your Barracuda VPN client.



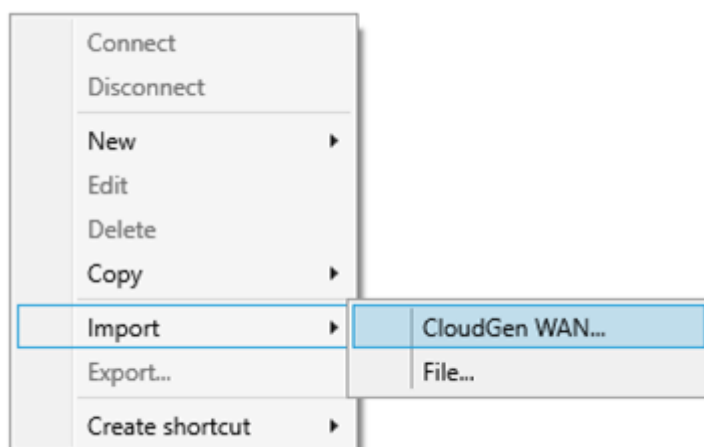
1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon.
3. From the drop-down menu, select the workspace containing your gateway.



4. Go to **Infrastructure > Edge Services**. The **Edge Services** page opens.
5. Next to your edge service, click on the download icon to download the client VPN configuration.



6. When importing the downloaded VPN configuration file, make sure to select **SecureEdge**. For more information, see [How to Establish a VPN Connection Using Barracuda VPN Client for Windows](#) or [How to Establish a VPN Connection Using Barracuda VPN Client for macOS](#).



## Further Information

- 
- For more information on enabling User Connectivity via a site, see [How to Enable User Connectivity on a Site](#).
  - For more information on the VPN client, see [VPN Client & Network Access Client](#).
  - For more information on importing VPN profiles, see [How to Import a \\*.vpn File into the VPN Client](#).
  - For more information on configuring the VPN client, see [How to Configure the Barracuda VPN Client for Windows](#) and [How to Configure the Barracuda VPN Client for macOS](#).
  - For more information on establishing VPN connections, see [How to Establish a VPN Connection Using Barracuda VPN Client for Windows](#) and [How to Establish a VPN Connection Using Barracuda VPN Client for macOS](#).



## Figures

1. inf\_set.png
2. pts.png
3. mail\_invite\_90.png
4. download\_client.png
5. enroll\_now.png
6. bcc1.png
7. password.png
8. profile.png
9. imported.png
10. cgw\_profiles\_82a.png
11. workspace\_testing\_90.png
12. edge\_dl.png
13. cgw\_vpn import.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.