

How to Configure SecureEdge Access

<https://campus.barracuda.com/doc/98225590/>

The Barracuda SecureEdge Manager allows administrators to configure SecureEdge Access either via Barracuda Cloud Control or by syncing the Azure AD Tenant ID with the Zero Trust Access service and defining various parameters such as point of entry, agent web filtering, custom client network, and DNS suffix in client networks. SecureEdge Access lets you implement secure access to internal and external enterprise resources, whether they are on-premises or in the cloud, by using a Zero Trust endpoint solution known as the SecureEdge Agent. Barracuda SecureEdge Access brings Zero Trust access service to your endpoint with a quick and easy configuration.

SecureEdge Access Deployment via Barracuda Cloud Control


SecureEdge SaaS Edge Service and SecureEdge Access are subscriptions hosted and managed by Barracuda Networks. You can activate SecureEdge Access using a product activation key. For more information on how to activate SecureEdge Access, see [How to Activate the Edge Service and SecureEdge Access Using an Activation Key](#).

Before You Begin

- Create a Barracuda Cloud Control account. For more information, see [Create a Barracuda Cloud Control Account](#).

Step 1. Activate SecureEdge Access Using Activation Key

1. After your order is placed with Barracuda Networks, you will receive an email from Barracuda Customer Services with a product activation key. In the **Product Key** section, click **Activate**.
2. Log in with your Barracuda Cloud Control account.
3. Complete the 4-step product activation process.

 **Barracuda**

English · bob@example.at

1 Activation Key

2 Accept Terms

3 Confirm

4 Complete

Activate your Barracuda Product(s)


If you have an activation key, enter it below.

SecureEdge (& 1 more)

Activation Key *

XXXXXXXXXXXX-XXXX-XXXX-XXXX-XXXX

Choose a country

 Austria

X

Continue >

4. Accept the license agreement to complete the subscription. Your product subscription is activated as soon as the activation procedure is complete.

After accepting the terms, you are directed to the SecureEdge dashboard. You can verify your subscriptions in the SecureEdge Manager via **Profile > Subscription**. You can proceed from there.

Step 2. Points of Entry

The SecureEdge Manager allows you to configure the points of entry by selecting either an existing edge service, site, or firewall that the Barracuda SecureEdge Agent can connect to. For instructions on how to create a point of entry, see [How to Configure Points of Entry](#).

Step 3. Enroll Users

The Barracuda SecureEdge Manager allows administrators to enroll users. For instructions on how to enroll user, see [How to Enroll Users in Barracuda SecureEdge](#).

Step 4. Verify Enrolled Devices and Users

The Barracuda SecureEdge Manager allows administrators to verify your devices For instructions on how to verify devices, see [How to Verify Enrolled Devices and Users](#).

Step 5. Create a Zero Trust Access Policy

Barracuda SecureEdge allows administrators to define a number of policies that specify the access requirements associated with the various resources that the Barracuda SecureEdge Agent can connect to. For instructions on how to create a zero trust policy, [Zero Trust Access Policies](#).

SecureEdge Access Deployment via Microsoft Azure

You can configure SecureEdge Access with the following steps:

Step 1. Connect to Azure Active Directory

The Barracuda SecureEdge Manager allows you to select an Azure Active Directory Tenant ID and sync with Zero Trust access.

Demo Enterprises Inc./Production
Access > Settings

Azure AD Tenant ID T-12345678

In order to select an Azure AD for use with Zero Trust Access, you must configure and sync your Azure AD into your Barracuda Account [here](#). Instructions for setting up Azure AD in Barracuda can be found [here](#).

Agent Web Filtering Enforce

DNS Suffix ztna.example.com

ACCESS AGENT NETWORK CONFIGURATION

The Client Network is used to assign IPs to clients that connect via SecureEdge Access Agent. It is divided into pools that are then distributed to each Point of Entry.

Manual configuration ☒

Client Network * 10.14.0.0/16

Pool Bitmask * 26

This Client Network provides at least 62 client connections per Point of Entry.

Download and roll out this root certificate to all clients to ensure parallel operations with CloudGen Firewall client-to-site setups and SecureEdge Access Agent.

[Download certificate](#)

For more information, see [How to Connect Your Azure Active Directory with SecureEdge Access](#).

Step 2. Points of Entry

Barracuda SecureEdge supports three different types of points of entry: firewalls, edge services, and sites. The SecureEdge Manager allows you to configure the points of entry by selecting either an existing edge service, site, or firewall that the Barracuda SecureEdge Agent can connect to. Registration of CloudGen Firewall units is token based. The CloudGen Firewall fetches a requisite certificate and a zero trust access policy from the cloud services; however, it does not get security features or SD-WAN policies from the service. On the **Points of Entry** page, you can find information on enrolled points of entry in the Barracuda SecureEdge environment.

To select the CloudGen Firewall as a point of entry, you must first configure a CloudGen Firewall in Barracuda SecureEdge. For more information, see [How to Configure a Barracuda CloudGen Firewall in Barracuda SecureEdge](#).

Demo Enterprises Inc./Production
Access > Points of Entry

[Add points of entry](#)

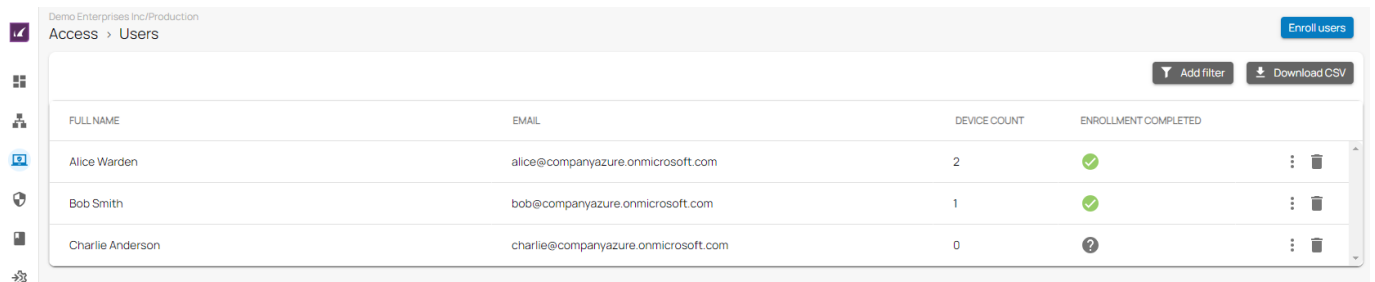
[Add filter](#) [Edit columns](#) [Download CSV](#)

NAME	TYPE	PUBLIC IPS	SIZE	LOCATION
Austria	Edge Service		T600D	Austria
EuropeWest-Offline	Edge Service		50 Mbit	West Europe
France	CloudGen Firewall	52.95.154.72	F180	Paris, 75001, France
Vienna	Site		T200B	Vienna, 1100, Austria

For more information, see [How to Configure Points of Entry](#).

Step 3. Enroll Users

The Barracuda SecureEdge Manager allows you to enroll users. A single user can enroll multiple devices on the same token. On the **Users** page, you can find detailed information on enrolled users.

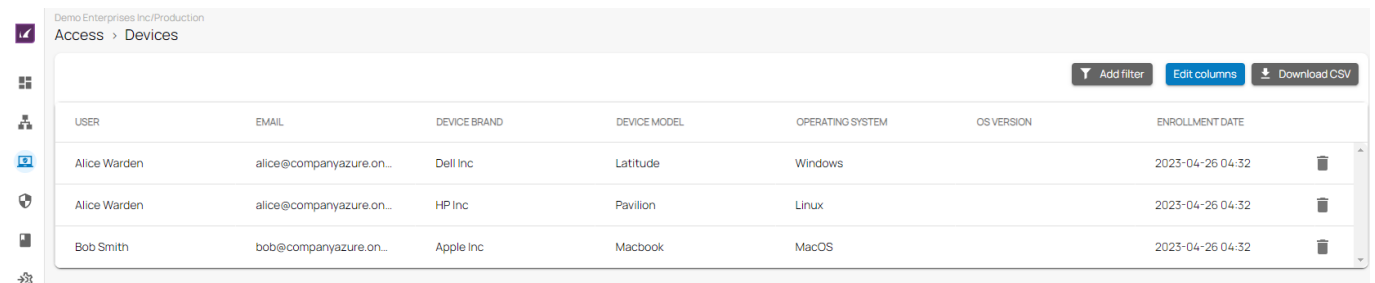


FULL NAME	EMAIL	DEVICE COUNT	ENROLLMENT COMPLETED
Alice Warden	alice@companyazure.onmicrosoft.com	2	✓
Bob Smith	bob@companyazure.onmicrosoft.com	1	✓
Charlie Anderson	charlie@companyazure.onmicrosoft.com	0	?

For more information, see [How to Enroll Users in Barracuda SecureEdge](#).

Step 4. Verify Enrolled Devices and Users

The Barracuda SecureEdge Manager allows administrators to enroll users with their respective devices. After the enterprise enrollment process is completed, your device protection will be automatically enabled. On the **Devices** page, you can find detailed information on enrolled devices.



USER	EMAIL	DEVICE BRAND	DEVICE MODEL	OPERATING SYSTEM	OS VERSION	ENROLLMENT DATE
Alice Warden	alice@companyazure.on...	Dell Inc	Latitude	Windows		2023-04-26 04:32
Alice Warden	alice@companyazure.on...	HP Inc	Pavilion	Linux		2023-04-26 04:32
Bob Smith	bob@companyazure.on...	Apple Inc	Macbook	MacOS		2023-04-26 04:32

For more information, see [How to Verify Enrolled Devices and Users](#).

Step 5. Create a Zero Trust Access Policy

The Zero Trust Access policy defines the resources made available to end users of the Barracuda SecureEdge Agent and the associated access restrictions. The **Zero Trust Access** page displays all defined policies with respect to your selected workspace.

Demo Enterprises Inc./Production

Security Policy > Access > Zero Trust Access

Last Mile Optimization ☐

[Add filter](#) [Add policy](#) [Download CSV](#)

ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE	
1	AuditorsAndExecs	Enforce Auditor and Exec compliance		Auditors Executive Team	Intranet Mediaserver	Enforce Compliance	
2	Engineering	Log Engineering compliance	alice@companyazure.onmicrosof... bob@companyazure.onmicrosof...	Engineering	SAP-prod-environment website-production	Log Violations	
3	RestrictedUsers	Enforce restricted users compliance	eve@companyazure.onmicrosof...		website-production	Enforce Compliance	

For more information, see [Zero Trust Access Policies](#).

Additional Information

To add a Zero Trust Access Policy for Zero Trust Access to reach a website for which no pre-defined apps exists (for example, zoom.us, msn.com, microsoft.com, tiktok.com, or whatsapp.com), you must define a custom web application. However, this overwrites the 'non-interceptable' property that states that SSL Inspection should not inspect such a website. In this case, you must configure an SSL Inspection rule with the respective client network as source and a custom web application as destination, and set SSL Inspection for these websites to **Do Not Inspect**.

Figures

1. select_country.png
2. goto-AccessSetting.png
3. PoE-9.0.png
4. UserEnroll-9.0.png
5. enrolled-device.png
6. ZeroTrustAccess.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.