

Getting Started

<https://campus.barracuda.com/doc/98223589/>

Follow the steps below to get the default configuration of Barracuda SecureEdge up and running. Completing the Barracuda SecureEdge welcome wizard takes you directly to the main dashboard. From there, you can navigate to the infrastructure configuration and add edge services and sites. Alternatively, you can subscribe to the Barracuda SecureEdge service in Microsoft Azure using an Azure subscription, deploy the appliance from the Azure Marketplace, and configure Barracuda SecureEdge in the Microsoft Azure cloud.

SecureEdge Deployment via Barracuda Cloud Control

To get started without an Azure subscription, access the Barracuda SecureEdge website and complete the simple welcome wizard.

Before You Begin

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

Step 1. Introduce the Barracuda SecureEdge Configuration

1. Go to <https://se.barracudanetworks.com>.
2. Log in with your Barracuda Cloud Control account.
3. Complete the 3-step welcome wizard.

Welcome to Barracuda SecureEdge

Barracuda SecureEdge secures your users, sites and things with one easy-to-deploy cloud-first platform that connects any device, app and any cloud/hybrid environment.

SecureEdge includes zero trust application access to any type of application, cloud delivered security for endpoints and automated SD-WAN connectivity for sites and industrial locations of all sizes.

[Create](#)[View demo](#)

4. Accept the license agreement to complete the enrollment.

After accepting the terms, you are directed to the SecureEdge dashboard. You can proceed from there.

The following steps are optional. You can either deploy multiple Barracuda CloudGen Firewall units in

SecureEdge, connect hardware and virtual site appliances via edge service, or both.

Step 2. Deploy Your CloudGen Firewalls in SecureEdge

With SecureEdge, you can enroll and monitor multiple Barracuda CloudGen Firewall units in one place. These can be hardware or virtual appliances. For information on how to integrate Barracuda CloudGen Firewall units with your SecureEdge deployment, see [How to Configure a Barracuda CloudGen Firewall in Barracuda SecureEdge](#).

Additionally, you can connect site appliances via edge services. For information on this procedure, continue with the next steps.

Step 3. Create a Private Edge Service in SecureEdge

For instructions on how to create a private edge service, see [How to Create a Private Edge Service in Barracuda SecureEdge](#).

Step 4. Create a Site Configuration in SecureEdge

For instructions on how to create a site configuration, see [How to Create a T/VT Site Configuration in Barracuda SecureEdge](#).

Step 5. Deploy Your Sites

You can use hardware and virtual appliances as your Barracuda SecureEdge site appliance. For more information on the deployment, see [Hardware Deployment](#) and [Virtual Systems \(VTx\) Deployment](#).

For information on available hardware models, see [Hardware Models](#). For information on available virtual models, see [Virtual Systems \(VTx\) Deployment](#).

SecureEdge Deployment in Microsoft Azure

In this guide, you will do the following:

- Subscribe to the Barracuda SecureEdge for Virtual WAN in Microsoft Azure
- Create a Microsoft Azure virtual WAN
- Create a hub in Microsoft Azure virtual WAN
- Create a private edge service in Microsoft Azure
- Create a site configuration in Barracuda SecureEdge
- Deploy a site appliance (virtual or hardware)

To add more resources to Barracuda SecureEdge, simply repeat the corresponding step.

Before You Begin

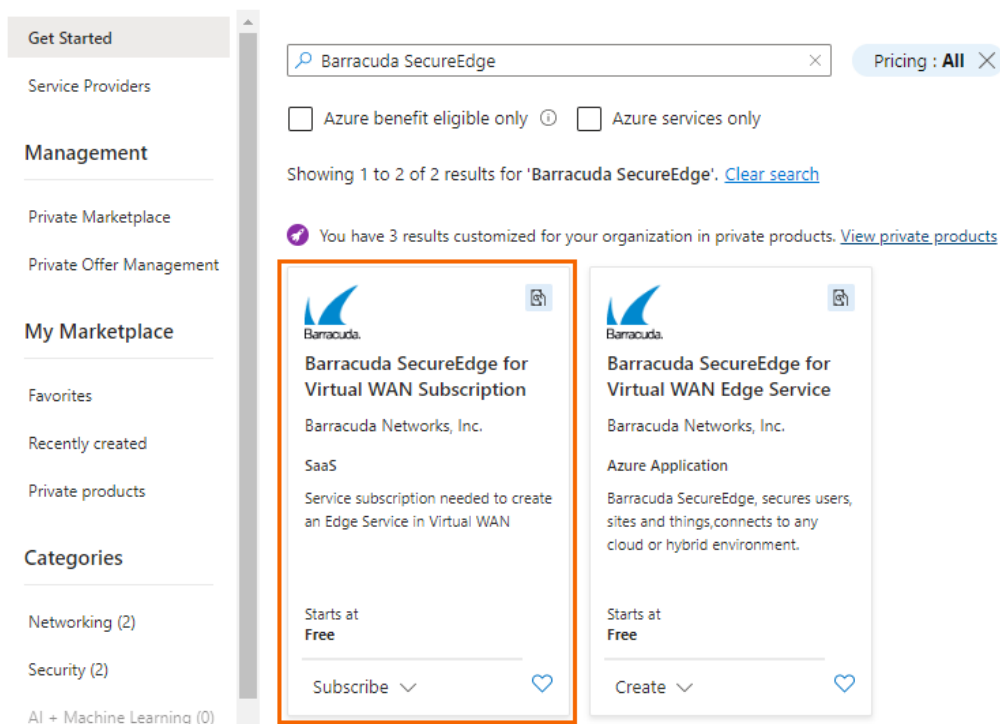
- Create a [Microsoft Azure account](https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/upgrade-azure-subscription#upgrade-your-azure-free-account). Note: If you have a free account, you must upgrade it according to the Microsoft documentation. For more information, see <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/upgrade-azure-subscription#upgrade-your-azure-free-account>.
- Create a Barracuda Cloud Control account. For more information, see [Create a Barracuda Cloud Control Account](#).

Step 1. Subscribe to the Barracuda SecureEdge for Virtual WAN in Microsoft Azure

This step is necessary only if you have not yet subscribed to the SecureEdge for Virtual WAN in Microsoft Azure.

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **Create a resource** and search for **Barracuda SecureEdge**.
3. Click **Barracuda SecureEdge for Virtual WAN Subscription**.

Marketplace ...



Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

Recently created

Private products

Categories

Networking (2)

Security (2)

AI + Machine Learning (0)

Barracuda SecureEdge

Pricing : All

☐ Azure benefit eligible only ☐ Azure services only

Showing 1 to 2 of 2 results for 'Barracuda SecureEdge'. [Clear search](#)

You have 3 results customized for your organization in private products. [View private products](#)

Barracuda SecureEdge for Virtual WAN Subscription
Barracuda Networks, Inc.
SaaS
Service subscription needed to create an Edge Service in Virtual WAN
Starts at Free
Subscribe

Barracuda SecureEdge for Virtual WAN Edge Service
Barracuda Networks, Inc.
Azure Application
Barracuda SecureEdge, secures users, sites and things, connects to any cloud or hybrid environment.
Starts at Free
Create

4. The **Barracuda SecureEdge for Virtual WAN Subscription** marketplace entry opens.
5. From the **Plan** drop down-menu, select **Default**.

Barracuda SecureEdge for Virtual WAN Subscription


Barracuda Networks, Inc.



Barracuda SecureEdge for Virtual WAN Subscription

Barracuda Networks, Inc. | SaaS

★ 4.9 (203 ratings)

 Azure benefit eligible

Plan

Default

Subscribe

6. Click **Subscribe**.

7. The **Subscribe To Barracuda SecureEdge for Virtual WAN Subscription** blade opens.

Specify values for the following:

- Subscription – Select your Microsoft Azure subscription.
- Resource group – Select an existing resource group, or click **Create new** to create a new resource group.
- Name – Enter a name for the Barracuda SecureEdge subscription, e.g., **Campus_SecureEdge_Subscription**.
- Recurring billing – Select either **On** or **Off**. When recurring bill is on, your subscription will renew at the end of the billing term.

Subscribe To Barracuda SecureEdge for Virtual WAN Subscription

Subscribe to plan

* Basics Tags Review + subscribe

Fill out the plan details. After you've finished subscribing, configure your SaaS account on the publisher's website to complete the process.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ⓘ

NetSec-cust2

Resource group * ⓘ

RG-Campus-VWAN

[Create new](#)

SaaS details

Name * ⓘ

CampusSecureEdge ✓

Plan

Default - 1-month subscription

Hourly pricing for Barracuda SecureEdge for Virtual WAN Edge Service and optionally also SecureEdge sites device through Azure Marketplace. Edge Service for Virtual WAN instances are billed on a per Scale Unit/h (500Mbps). SecureEdge site devices are billed on a per-day basis using hourly rate.

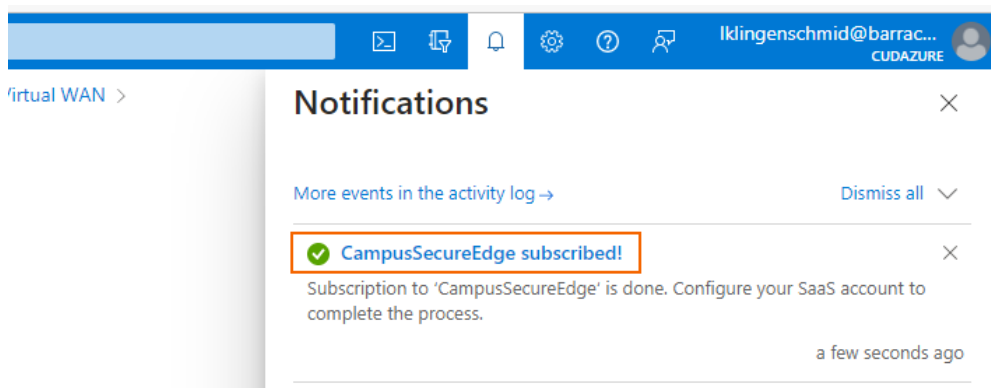
[Change plan](#)

8. Click **Review + subscribe**.

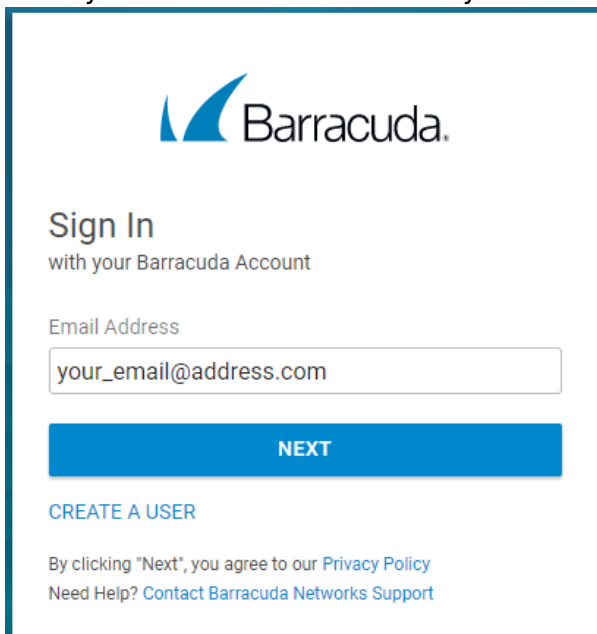
9. Click **Subscribe**.

10. You will receive an email notification from Microsoft Azure Marketplace. You can ignore the email and continue in Azure.

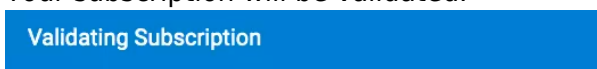
11. Click on the bell notification icon to go to the newly created subscription.



12. Click on the entry of your newly created subscription, e.g., **CampusSecureEdge subscribed!**.
13. Click **Configure Account now**.
14. You will be redirected to the SecureEdge user interface.
15. Enter your email address used for your Barracuda Cloud Control account, and click **NEXT**.

A screenshot of the Barracuda 'Sign In' page. The page has the Barracuda logo at the top. Below it, the text 'Sign In with your Barracuda Account' is displayed. There is a text input field for 'Email Address' containing 'your_email@address.com'. Below the input field is a blue button labeled 'NEXT'. At the bottom, there is a link 'CREATE A USER' and a disclaimer: 'By clicking "Next", you agree to our Privacy Policy' and 'Need Help? Contact Barracuda Networks Support'.

16. Enter your password, and click **SIGN IN**.
17. Your subscription will be validated.



Validating your subscription details.

18. After successful validation, the **DASHBOARD** tab is displayed.

The subscription process was successful. Continue with Step 2.

Step 2. Create a Virtual WAN in Microsoft Azure

Either create a new virtual WAN with a hub in Microsoft Azure, or use an existing virtual WAN with an existing hub. For more information on creating a new Microsoft Azure virtual WAN with a hub,

see [How to Create a Microsoft Azure Virtual WAN](#).

Step 3. Create an Edge Service in Microsoft Azure

For instructions on how to create an edge service in Microsoft Azure, see [How to Create a SecureEdge for Virtual WAN Edge Service in Microsoft Azure](#).

Step 4. Create a Site Config in Barracuda SecureEdge

With SecureEdge, you can connect multiple sites through your edge services. You can also enroll Barracuda CloudGen Firewall units.

- For information on how to create a site configuration, see [How to Create a T/VT Site Configuration in Barracuda SecureEdge](#).
- For information on how to integrate Barracuda CloudGen Firewall units with your SecureEdge deployment, see [How to Configure a Barracuda CloudGen Firewall in Barracuda SecureEdge](#).

Step 5. Deploy Your Sites

You can use hardware and virtual appliances as your Barracuda SecureEdge site appliance. For more information on the deployment, see [Hardware Deployment](#) and [Virtual Systems \(VTx\) Deployment](#).

For more information on available hardware models, see [Hardware Models](#). For more information on available virtual models, see [Virtual Systems \(VTx\) Deployment](#).

Next Steps

To achieve your specific goals or tasks, you can deploy and perform following with Barracuda SecureEdge:

SD-WAN

Barracuda SecureEdge provides a common set of SD-WAN policies out-of-box. It offers a default configuration for SD-WAN policies that uses a predefined application database to cover the most common use cases. However, if your setup requires a different SD-WAN profile for certain applications, you can define your custom policies by defining the Override Categories policies. For more information, see [SD-WAN](#).

ZTNA Deployments via SaaS Edge Service and SecureEdge Access

SecureEdge Access uses a Zero Trust Network Access (ZTNA) solution known as the SecureEdge Access Agent that lets you implement secure access to internal and external enterprise resources,

whether they are on-premises or in the cloud. SecureEdge Access brings Zero Trust/BeyondCorp Security to your endpoint with a quick and easy configuration. For more information on how to get started with SecureEdge Access, see [SecureEdge Access](#).

Secure Web Gateway (SWG)

Barracuda SecureEdge offers a security solution that filters unwanted malware from user-initiated web or internet traffic and enforces corporate policies. You can configure modern SWG features that monitor, inspect, detect, and prevent suspicious traffic from entering or leaving an organization's network. These features include web filter policies, web monitoring policies, Safe Search enforcement, silent ad blocking, custom categories, and custom response pages. For more information on the Secure Web Gateway, see [Secure Web Gateway \(SWG\)](#).

Figures

1. se_wizard.png
2. vWAN-subscription.png
3. vWAN-subscribe.png
4. SE-Subscription.png
5. bell_notify.png
6. login_mail.png
7. validation821.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.