



# Cloud Edge Secure Access Getting Started Guide

SONICWALL®

# Contents

|   |           |
|---|-----------|
| <b>Welcome to SonicWall Cloud Edge</b> .....  | <b>5</b>  |
| How Do I Get Started? .....                   | 5         |
| <b>Prerequisites</b> .....                    | <b>6</b>  |
| MySonicWall .....                             | 6         |
| Enabling Trial License .....                  | 7         |
| Licensing .....                               | 9         |
| Licensing a New Deployment .....              | 9         |
| Licensing for an Upgrade .....                | 10        |
| <b>Installation</b> .....                     | <b>12</b> |
| Accessing the Client Management Console ..... | 12        |
| Installation Methods .....                    | 13        |
| <b>Networks</b> .....                         | <b>14</b> |
| Understanding Networks .....                  | 14        |
| Network Components .....                      | 14        |
| SDP Networks .....                            | 15        |
| Creating a Network .....                      | 15        |
| Editing your network .....                    | 17        |
| Deleting your network .....                   | 18        |
| Regions and Gateways .....                    | 18        |
| Adding a region .....                         | 19        |
| Adding a gateway .....                        | 19        |
| Connecting Infrastructure .....               | 22        |
| Prerequisites .....                           | 22        |
| Site-to-Site Connections .....                | 24        |
| IPsec Tunnel .....                            | 25        |
| WireGuard Connector .....                     | 27        |
| Connect On-Prem Resources .....               | 34        |
| General Settings .....                        | 35        |
| Advanced Settings .....                       | 36        |
| General Tab .....                             | 39        |
| Security Policy .....                         | 39        |
| IKE Authentication .....                      | 39        |
| Network Tab .....                             | 40        |
| Local Networks .....                          | 40        |
| Remote Networks .....                         | 40        |

|  |            |
|--|------------|
| Proposals Tab .....                              | 40         |
| IKE (Phase 1) Proposal .....                     | 40         |
| IPsec (Phase 2) Proposal .....                   | 41         |
| Advanced Tab .....                               | 41         |
| Advanced Setting .....                           | 41         |
| Connect Cloud Resources .....                    | 42         |
| Create the Transit Gateway .....                 | 54         |
| Create the Transit Gateway VPC attachments ..... | 56         |
| Create the Transit Gateway VPN attachment .....  | 57         |
| Configuring the tunnel in the AWS Console .....  | 59         |
| <b>Groups and Members .....</b>                  | <b>107</b> |
| Members .....                                    | 107        |
| Inviting Members .....                           | 107        |
| Password Requirements .....                      | 109        |
| Managing Roles .....                             | 109        |
| Groups .....                                     | 111        |
| Managing Groups .....                            | 111        |
| Identity Provider Groups .....                   | 113        |
| Identity Providers (IdP) .....                   | 116        |
| Integrate Identity Providers .....               | 116        |
| Azure AD .....                                   | 118        |
| Google Suite .....                               | 137        |
| On-Premises Active Directory .....               | 149        |
| SAML 2.0 .....                                   | 156        |
| <b>Securing the Platform .....</b>               | <b>190</b> |
| Securing Networks .....                          | 190        |
| Segmenting Networks .....                        | 190        |
| Device Posture Check .....                       | 192        |
| Network Traffic Control .....                    | 196        |
| Firewall-as-a-Service .....                      | 199        |
| Securing User Access .....                       | 203        |
| Multi-Factor Authentication .....                | 203        |
| Agent-less Access .....                          | 207        |
| Windows 7 users: .....                           | 212        |
| Windows Server 2019 users: .....                 | 213        |
| Upstream error: .....                            | 213        |
| Additional Troubleshooting steps .....           | 213        |
| Agent-based Access .....                         | 221        |
| <b>Monitoring .....</b>                          | <b>228</b> |
| Activity Tracking .....                          | 228        |
| Activities and Logs .....                        | 228        |
| Member Devices .....                             | 231        |

|                                |            |
|--------------------------------|------------|
| Monitoring Dashboard .....     | 233        |
| Active Sessions .....          | 233        |
| General Information .....      | 233        |
| Active Agent Users .....       | 234        |
| Additional Information .....   | 234        |
| Integrations .....             | 235        |
| Amazon S3 .....                | 235        |
| Azure Sentinel .....           | 243        |
| Splunk Cloud .....             | 248        |
| <b>Compliance .....</b>        | <b>252</b> |
| HIPAA .....                    | 252        |
| Information Protection .....   | 252        |
| GDPR .....                     | 253        |
| Data Protection .....          | 253        |
| SOC 2 Type 2 .....             | 254        |
| Auditing .....                 | 254        |
| <b>SonicWall Support .....</b> | <b>255</b> |
| About This Document .....      | 256        |



# Welcome to SonicWall Cloud Edge

SonicWall Cloud Edge is a Zero Trust Network as a Service that helps you to secure your team's network, including valuable local and cloud resources. SonicWall Cloud Edge unifies network and security to be consumed as a service in the cloud edge with adaptive, centralized access control policies based on user/device identity and access context. Accordingly, authorized employees are only granted access to the corporate resources they need, and IT administrators can more easily monitor activity across the network and implement a full range of network security features that are easy to scale with organizational growth. The combination of this reduced attack surface and cloud-friendly approach makes it that much more difficult for bad actors to breach your network, but also saves significant IT overheads.

Better yet, it's easy and fast to implement. Read on below.

## How Do I Get Started?

It's simple to onboard your network resources, branch offices, and employees into the Management Platform in as little as 15 minutes.

1. **Create your network:** Set up an SDP secured network consisting of [regions and private gateways](#). [Click here](#) to learn more about our network components and structure.
2. **Connect your infrastructure:** Deploy [site-to-site connections](#) to securely connect your local and cloud resources ([click here](#) to find out if you meet all the prerequisites). You can integrate seamlessly with the SaaS applications and tools you rely on, such as Salesforce, [Microsoft Azure](#), [AWS](#) or [Google Cloud Platform](#). This allows you to build and secure your networks from one place - and model them in a simple, visual way.
3. **Invite your teammates:** [Create user groups](#) and attach them to a network according to the resources the group member needs access to, integrate with [your Identity Provider](#) and [invite your users](#).
4. **Regulate access to internal resources and enhance platform security:** [Configure agent-less access Zero Trust Applications](#), [Download our agents](#) and [adjust their configuration according to your own needs](#), apply [MFA Authentication](#).
5. **Monitor users' activity:** Track users' [activities](#) and [devices](#) and integrate with a SIEM platform ([Splunk](#)).

At any stage of the process, we'd love to answer questions and hear your feedback and idea. Feel free to contact your account manager, CSE or our [support engineers](#).

# Prerequisites

Prior to configuring and deploying the SonicWall Cloud Edge, several activities need to be completed:

- Create or validate your MySonicWall account in MySonicWall.
- Enable trial license of Cloud Edge Secure Access
- License or activate the Cloud Edge Secure Access software.

This chapter reviews these activities and provides guidance for ensuring their completion.

## MySonicWall

SonicWall requires a MySonicWall account prior to configuring your SonicWall Cloud Edge. MySonicWall is used to license your site and to activate or purchase licenses for other security services, support, or software specific to your security solution. If you haven't already done so, create a MySonicWall account; otherwise, you can skip to Licensing.

### *To create a new MySonicWall account from any computer:*

1. Navigate to <https://www.mysonicwall.com>.
2. In the login screen, click the Sign Up link.
3. Complete the **ACCOUNT** information, including email and password.  
① | **NOTE:** Your password must be at least 8 characters, but no more than 30 characters.
4. Enable two-factor authentication, if desired.
5. If you enable two-factor authentication, select one of the following authentication methods:
  - **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.
  - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code.
6. Click on **Continue** to go to the **COMPANY** page.
7. Complete the company information and click **Continue**.

8. On the **YOUR INFO** page, select whether you want to receive security renewal emails.
9. Identify whether you are interested in beta testing new products.
10. Click **Continue** to go to the **EXTRAS** page.
11. Select whether you want to add additional contacts to be notified for contract renewals.
12. If you opted for additional contacts, input the information and click **ADD CONTACT**.
13. Click **DONE**.
14. Check your email for a verification code and enter it in the **Verification Code\*** field. If you did not receive a code, contact Customer Support by clicking on the link.
15. Click **Done**. You are returned to the login window so you can login into MySonicWall with your new account.

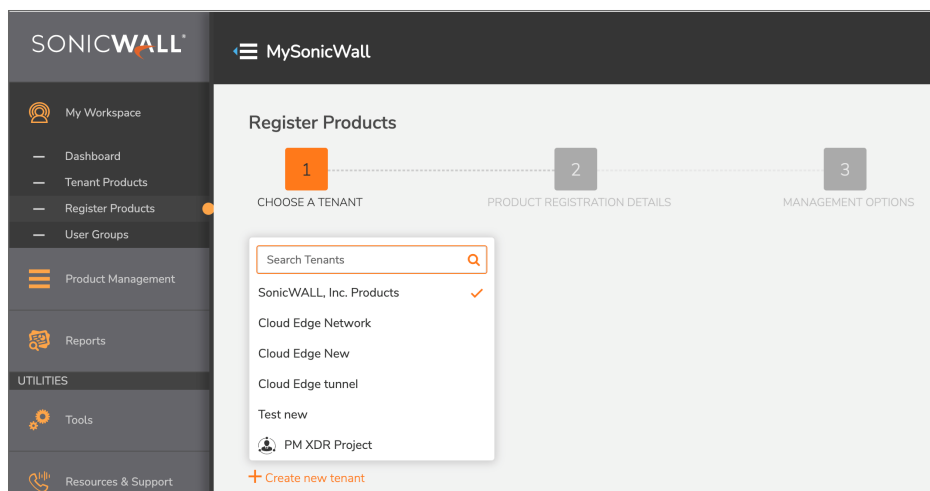
## Enabling Trial License

This section provides the details of enabling the trial license for Cloud Edge Secure Access.

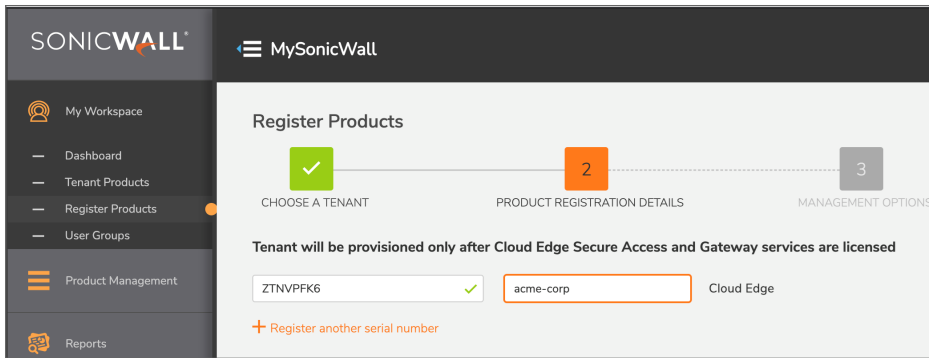
① **NOTE:** You need to have the **Cloud Edge Secure Trial Activation Key** and the **Gateway Activation Key** to enable the trial license.

### To enable a 30-day trial:

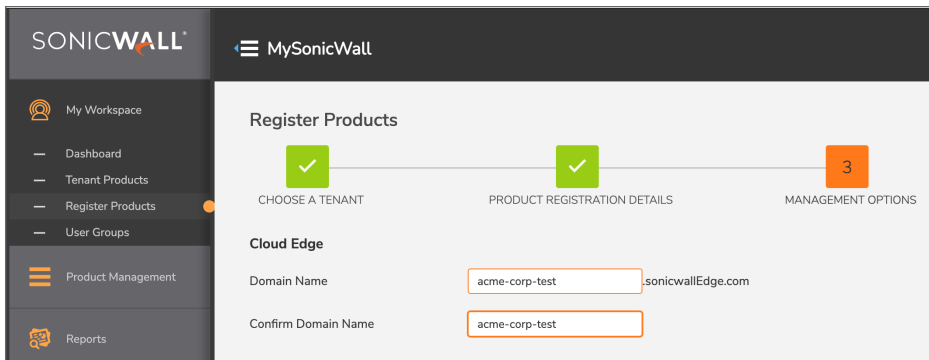
1. Login to <https://cloud.sonicwall.com> using your MySonicWall account credentials and click on MySonicWall Tile
2. Navigate to **My Workspace > Register Products**. Choose a tenant to deploy Cloud Edge or create a new tenant.



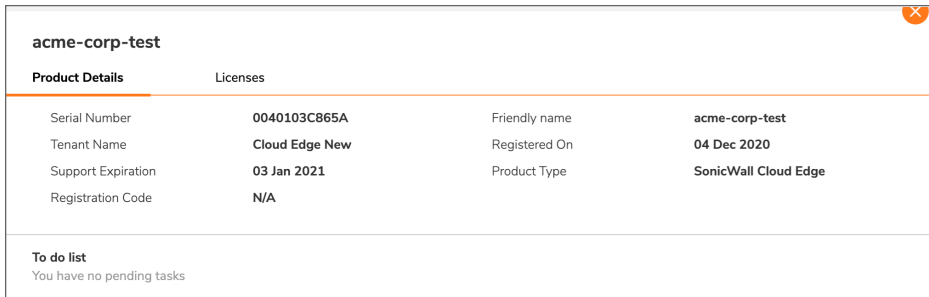
3. On the **Product Registration Details** page, enter the Cloud Edge **Trial Activation Key**. Enter a **Friendly name** for the Cloud Edge instance that is relevant to your organization, e.g. acme-corp.



4. Enter a **Domain name**. This will be the name of your Cloud Edge instance, e.g. acme-corp. Confirm the domain name.



5. When the product registration is completed, the **Product Details** page opens up. Click on the **Licenses** tab.



6. On the **Licenses** page, enter the Cloud Edge **Gateway Activation Key**. Click **Activate**. The default number of gateway is 1.
  - ① **NOTE:** Tenant will not be provisioned until both **Cloud Edge Secure Access** and **Gateway services** are licensed.

acme-corp-test 0040103C865A

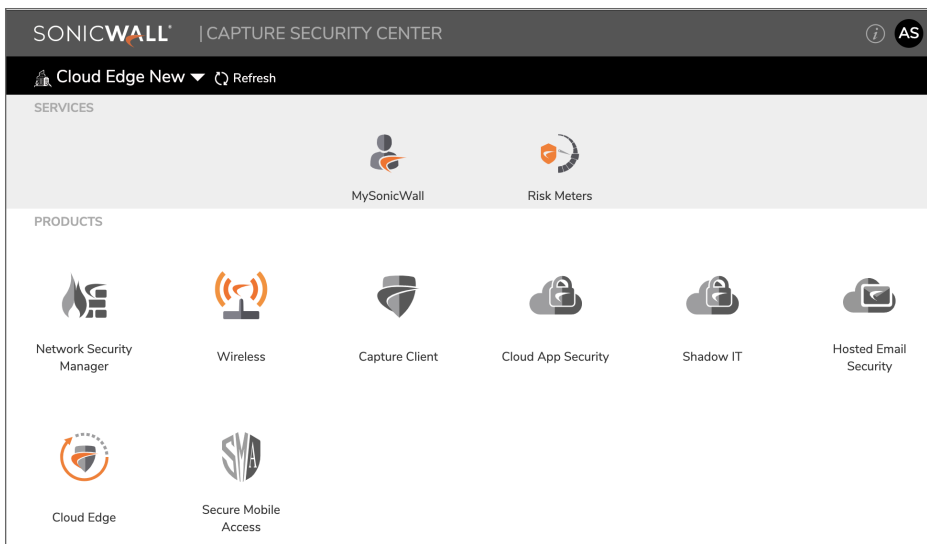
Tenant will not be provisioned until both Cloud Edge Secure Access and Gateway services are licensed.

Product Details      Licenses

Search: Show All Licenses      GW52VZGQ      Activate

| SERVICE NAME   | STATUS     | COUNT | EXPIRY DATE | ACTIONS  |
|--|------------|-------|-------------|--|
| <b>Cloud Services</b> (1 Licensed)<br>Cloud Edge Secure Access | Trial      | 25    | Jan 3 2021  | Activate              Buy              Start Trial |
| <b>Gateway Services</b> (0 Licensed)<br>Cloud Edge Gateway     | Unlicensed |       |             | Activate              Buy              Start Trial |
| <b>Support Services</b> (1 Licensed)<br>24x7 Support           | Trial      |       | Jan 3 2021  | Activate              Buy              Start Trial |

7. **Registration** is now complete. To launch the product, go to the **SonicWall Capture Security Center** homepage, choose the correct tenant and launch **Cloud Edge**.



## Licensing

To activate a brand new Cloud Edge license, refer to [Licensing a New Deployment](#). To activate a license for an existing Cloud Edge deployment, refer to [Licensing for an Upgrade](#).

## Licensing a New Deployment

The procedure for licensing Cloud Edge for a new deployment is very simple. You need to follow the exact same steps as [Enabling Trial License](#). The only difference is that you have to enter the Cloud Edge Secure Access Product Activation Keys instead of Trial Keys.

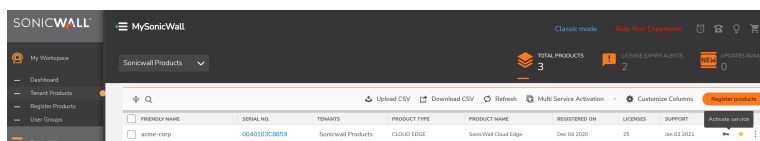
Once you license Cloud Edge, go to Installation for the next steps.

## Licensing for an Upgrade

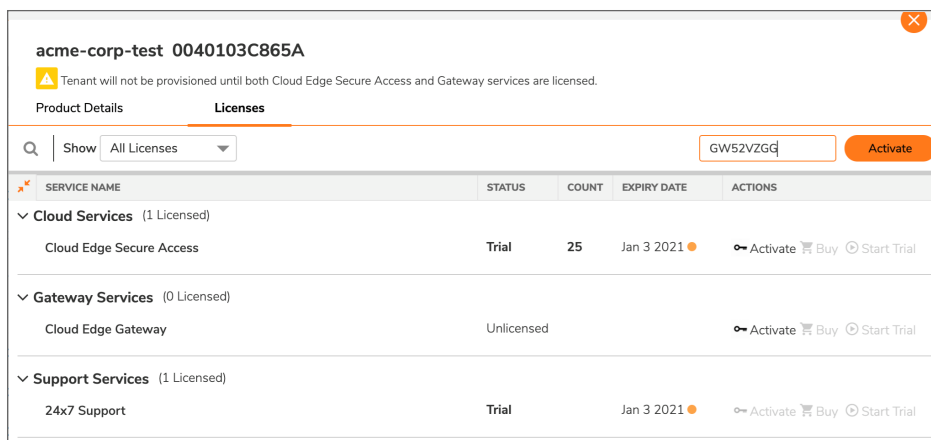
This section provides the details of upgrading the license for Cloud Edge Secure Access.

### To upgrade SonicWall Cloud Edge Secure Access:

1. Login to <https://cloud.sonicwall.com> using your MySonicWall account credentials and click on MySonicWall Tile
2. Navigate to **My Workspace > Tenant Products**. Select the Cloud Edge product that you want to upgrade and click on **Activate service**.

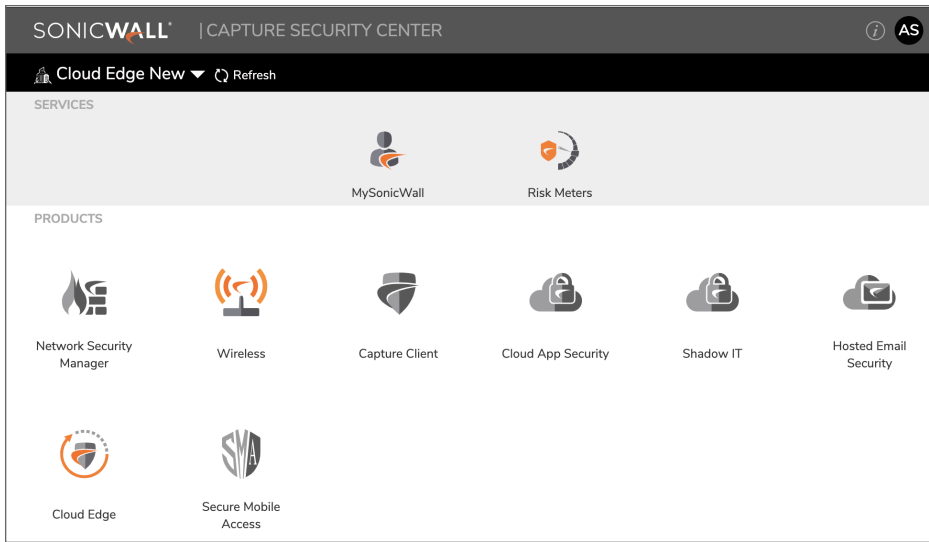


3. On the **Licenses** page, enter the Cloud Edge **Upgrade Activation Key**. Click **Activate**.



4. **License upgrade** is now complete. To launch the product, go to the **SonicWall Capture Security**

Center homepage, choose the correct tenant and launch **Cloud Edge**.



# Installation

SonicWall Cloud Edge Secure Access Agents can be deployed to the endpoints in several different ways. This chapter describes the key distribution methods, as well as how to access the Client Management Console.

## Topics:

- [Accessing the Client Management Console](#)
- [Installation Methods](#)

## Accessing the Client Management Console

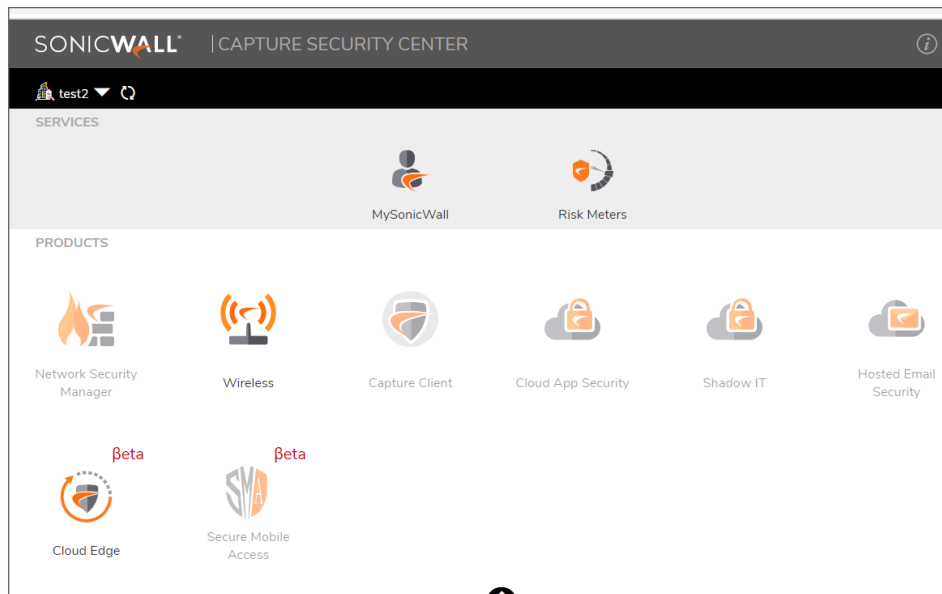
You can access the Client Management Console either by: Launching Cloud Edge Secure Access service from Capture Security Center (recommended) or Logging into the Cloud Edge Secure Access site.

### Launching Cloud Edge Secure Access service from Capture Security Center

1. Navigate to <https://cloud.sonicwall.com/>.
2. Log in with your MySonicWall credentials.
3. In the Capture Security Center homepage, select appropriate tenant in the TENANTS/GROUPS list.



4. Select Cloud Edge Secure Access to launch.



## Installation Methods

SonicWall Cloud Edge Secure Access can be easily installed on a client system. The client installers can be downloaded from the Downloads page located at **Management > Downloads**. Currently Windows, MacOS, iOS and Android are supported, and pre-configured installation scripts are provided. Once the license for your tenancy has been established, you can send a link to your users and have them download and install the client on their own devices. You need only provide the link to the console and the appropriate login credentials.

① | **NOTE:** Internet Explorer 11 browser does not support Cloud Edge Secure Access web client access.

# Networks

## Topics:

- [Understanding Networks](#)
- [SDP Networks](#)
- [Regions and Gateways](#)
- [Connecting Infrastructure](#)

## Understanding Networks

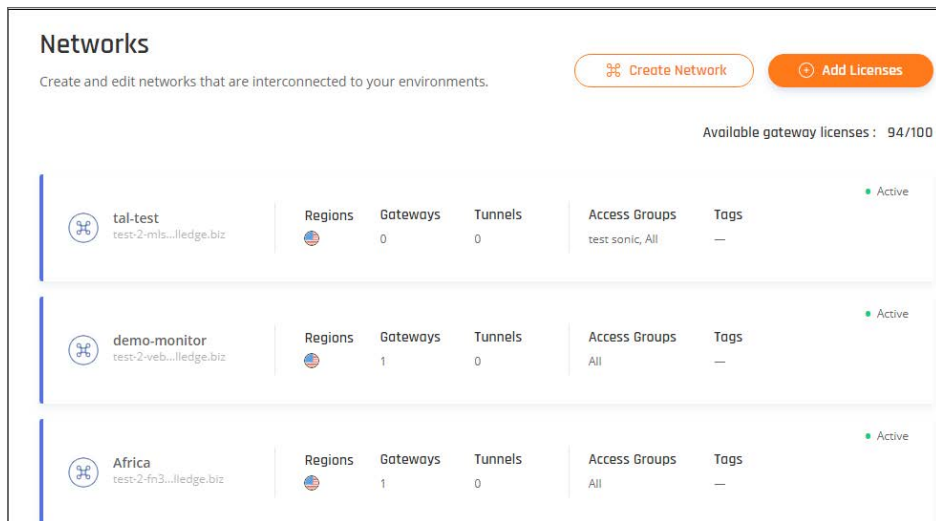
The ability to create your network is one of the fundamental features of the Management Platform. This article describes the components of a network.

Each network has three basic components - **Regions**, **Gateways**, and **Tunnels**.

Those components enable one or more **Groups** of your **Members** to securely access your on-premise and cloud-based resources.

## Network Components

- **Region(s)** - Physical locations where your **Gateway(s)** will be deployed. One **Network** can have several **Regions** for lower latency and better performance. **Members** connecting to a multi-regional **Network** will automatically be routed to the closest **Region**.
- **Private Gateway(s)** - Dedicated private servers deployed in your selected **Region(s)**. Every **Gateway** has its own static IP address and can be connected to others on-premise or cloud resources by **Tunnels**. One **Region** can have several **Gateways**, which improves the redundancy of your **Network** and ensures better load-balancing between the **Gateways**.
- **Tunnel(s)** - Site-to-Site securely encrypted connections deployed from your **Gateway(s)** to your on-premise and cloud-based resources in-order to connect them to your **Network**. A green dot indicates that the tunnel is up. A red dot indicates that the tunnel is traffic that does not flow from one site to another. **Tunnels** can be used to connect all of your branches to one **Network** by easily deploying a **Tunnel** to each one of them. One **Gateway** can have several Tunnel connections.



## SDP Networks

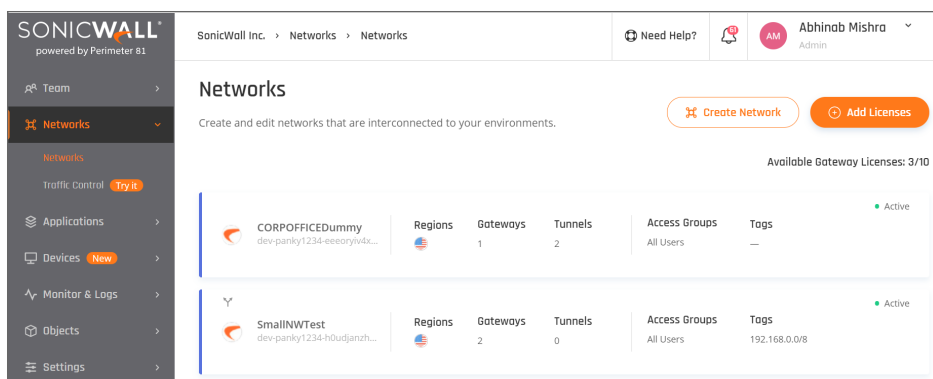
This article describes how to manage your Software-Defined Perimeter (SDP) Networks by:

- Creating a network
- Editing a network
- Deleting a network

## Creating a Network

*Follow these steps to create a network:*

1. Select **Create Network** on the **Networks** tab.



2. Fill in the following:

- **Network Name:** A name for the Network you are building. For example, HQ, Finance, or Staging.
- **Icon:** Use the default or select an icon of your choice.
- **Region:** Region is the physical location where the gateway will be deployed. Choose one or more regions from the available regions listed (Europe, North America, East Asia, Australia, and Israel).
- **Gateways:** The number of gateways you want to deploy in a particular region. Having multiple gateways enables high availability and a better load balance. The number of gateways should not exceed the number of available licenses.
- **Network Tags:** Use tags to help identify the different purposes and/or teams your Network will support.
- **Subnet:** *Optional.* If the subnet is not specified, it will receive a default value of 10.255.0.0/16.

### Shorter IP Ranges:

If you'd like to use the same subnet in SonicWall Cloud Edge as your existing networks you can reduce the subnet class, however, the SonicWallCloud Edge dedicated IP range cannot overlap with other connected networks.

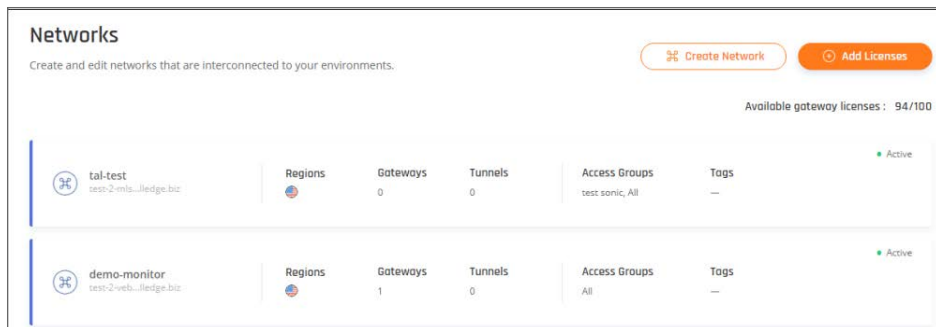
- For x.x.x.x/8 - SonicWallCloud Edge network range should be between x.x.x.x/21 and x.x.x.x/12
- For x.x.x.x/12 - SonicWallCloud Edge network range should be between x.x.x.x/21 and x.x.x.x/12
- For x.x.x.x/16 - SonicWallCloud Edge network range should be between x.x.x.x/21 and x.x.x.x/16

① | **NOTE:** x.x.x.x/21 is only available for networks with one Gateway.

Subnets **cannot be changed** after the Network is created. Please make sure that the selected Subnet **won't overlap** with the subnets that you use in your **on-premise and cloud-based** networks.

After defining your Network specifications, you can see your Network being created.

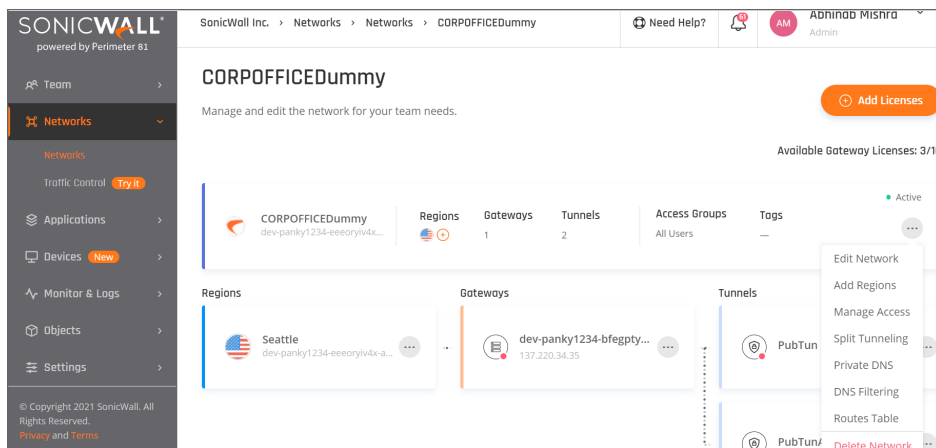
After the Network is successfully created, it will appear in the **Networks** tab.



Your new Network allows you to edit or delete customized networks that are multi-regional and interconnected to your cloud and on-premise environments.

## Editing your network

Once you have created a Network, you can easily edit the name, tags, and icon of your Network to help you identify the different purposes and/or teams your network will support.



### To edit your Network:

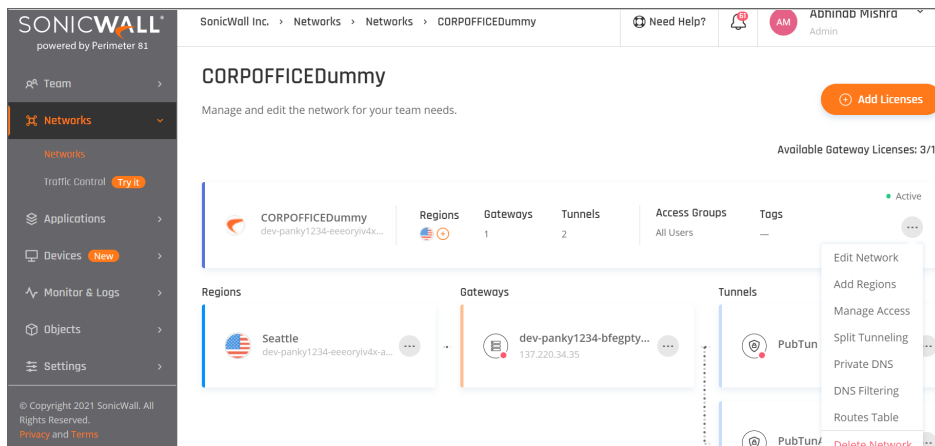
1. Select the **Networks** tab in the Management Platform. Select the three-dotted menu (...) to the right of your Network.

2. Make the changes and click **Save**.

## Deleting your network

1. To delete your Network, select the **Networks** tab in the Management Platform. Select the three-dotted menu (...) to the right of your Network.
2. Select the **Delete Network** option to delete the Network.

Deleting the Network will remove the selected Network and all its configurations.



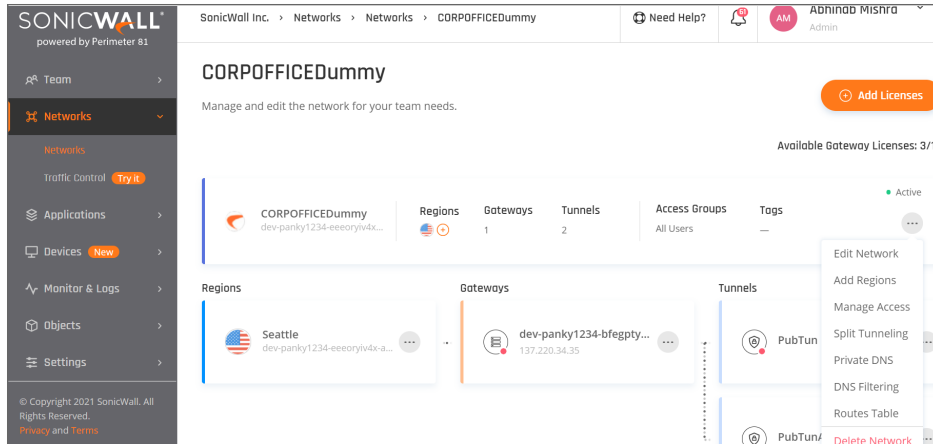
## Regions and Gateways

This article describes how to create two of the main network components:

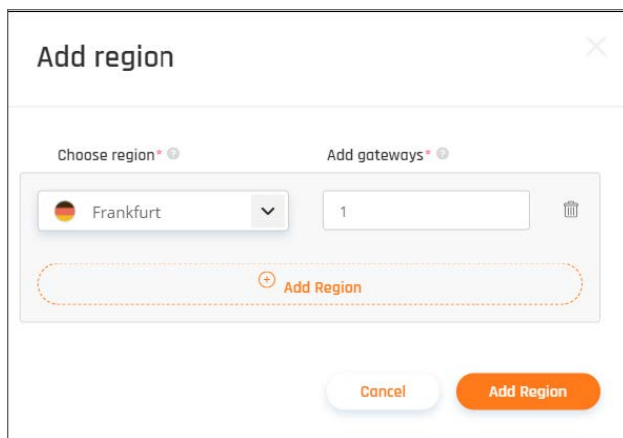
- Adding a region
- Adding a gateway

## Adding a region

1. To add a Region to your Network, select the three-dotted menu (...) to the right of your Network and choose **Add Region**.



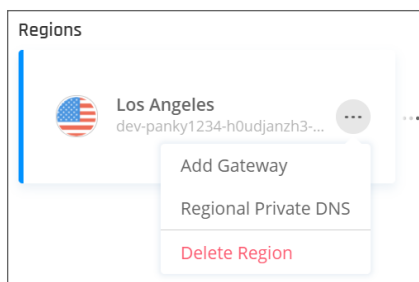
2. On the **Add Region** screen, choose from the available **Regions** and select the desired number of **Gateways** (limited to the number of available licenses).



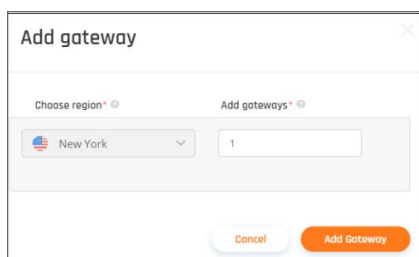
## Adding a gateway

The Multi-Regional Feature allows you to deploy private gateways in multiple locations, so you can create a network with distributed access points to best serve international branches, remote employees, and region-based Cloud-Resources with low latency and high availability.

1. To add a gateway to your Network, select the three-dotted menu (...) to the right of your Region and choose **Add Gateway**.



2. Add the desired number of gateways (limited to the number of available licenses).



3. Add the gateway information.
4. Select **Add Gateway**.

## Regions and Points-of-Presence

SonicWall Cloud Edge provides more than 30 Regions across the world. Gateways deployed in each Region are assigned with a dedicated static IP address and only accessible by the assigned Groups and Members according to your SonicWall Cloud Edge configuration.

Additional Regions and Gateways can be deployed to your existing Network at any time by a click-of-a-button from the SonicWall Cloud Edge Web-Console.

- When the same Region is listed more than once, that means that we have several different Data-Centers in the same Region.
- Regions marked in **Bold** are SonicWall Cloud Edge owned and managed Data-Centers. All other Regions are managed by trusted Cloud Providers and leased by SonicWall Cloud Edge.
- If for any reason you can't find a Region that fits you, we'd love to hear your feedback and resolve your request. Please contact your account manager or our support team.

### North America

- **Dallas**
- **Denver**
- **New York**
- **Silicon Valley**



- **Chicago 1**
- Atlanta
- Chicago
- Fremont
- Los Angeles
- Miami
- New Jersey
- New Jersey 2 (Newark)
- New York 2
- San Francisco
- San Jose
- Seattle
- Toronto
- Toronto 2

#### EMEA

- **Dubai**
- **Frankfurt**
- **London**
- **Stockholm**
- **Tel-Aviv**
- Frankfurt 2
- London 2
- Madrid
- Paris
- Frankfurt 2
- Helsinki
- London 2
- Madrid
- Paris
- Warsaw
- Amsterdam
- Frankfurt 3
- Johannesburg

#### APAC

- Bangalore
- Mumbai
- Singapore
- Singapore 2
- Sydney
- Sydney 2
- Tokyo
- Tokyo 2

#### LATAM

- Sao Paulo
- Mexico

## Connecting Infrastructure

#### Topics:

- [Prerequisites](#)
- [Site-to-Site Connections](#)
- [IPsec Tunnel](#)
- [WireGuard Connector](#)
- [Connect Cloud Resources](#)
- [Connect On-Prem Resources](#)

## Prerequisites

The SonicWall CloudEdge SASE Network offers several different ways to connect your cloud/on-premise infrastructure. While our solution is hardware-free, there are some minimal requirements for a successful Site-to-Site connection which will be covered in the following article:

- Internal network compliant subnet
- [IPSec tunneling](#) supporting router
- Wireguard Tunneling using a Linux Server that is free to host the connection (it can be a Virtual Machine)

## Internal Network Subnet

The SonicWall CloudEdge SASE network is designed according to internationally acknowledged standards and follows the RFC conventions regulated by the American internet authorities. In order to successfully incorporate SonicWall CloudEdge in your architecture please make sure that:

1. Your internal network follows industry-accepted design patterns.
2. VPCs or DC with overlapping subnets does not reside in the same network.
3. Your SonicWall CloudEdge network subnet does not overlap with your network subnet.
4. All subnet masks are either class B or C (HIGHLY RECOMMENDED).
5. Your internal network has a static public IP (RECOMMENDED).

**⚠ WARNING: 192.162.1.0/24, 192.168.0.0/24 and 10.0.0.0/24 are the most commonly used subnet for IoT applications. If you plan to connect a site with this CIDR, you could be experiencing an IP conflict with users trying to reach this from home.**

**You may want to change it to anything else (for example 192.168.81.0/24 or 10.81.0.0/24) prior to connecting a site to your SonicWall CloudEdge network.**

A Site-to-Site connection between your SonicWall CloudEdge Network and your Cloud infrastructure can be easily implemented with any IaaS provider, however, if you'd like to connect to your on-premise infrastructure make sure that at least one of the following requirements is fulfilled.

## IPSec Tunneling Support

Make sure your edge device (firewall or router) supports IPSec tunneling. If you are not sure, you can search it at our "Connect On-Prem Resources" section or look at the manufacturer's official documentation. If it is not supported, or if you prefer avoiding adjustments in your FW or Router Interface, move on to the next step.

## Wireguard Server

A Site-to-Site connection can also be achieved by deploying a SonicWall CloudEdge connector on a virtual/bare-metal Linux server fulfilling the following requirements:

1. **Kernel:** Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS or CentOS 7 (RedHat distributions)
2. **Packages Installed:** (UBUNTU) curl; dig; software-properties-common or (CentOS) curl, bind-utils
3. **Free Disc Space:** 20 GB available
4. **Free Memory:** 2GB RAM
5. **A static internal IP address**
6. A network adapter cannot be NAT - only Bridge.
7. If you are hosting the Linux machine on a Windows host, virtualization must be enabled on the Windows BIOS to allow Virtualization.

Once you make sure these prerequisites are fulfilled you can move on to the next stage, choosing the Site-to-Site connection type which fits your use case the best.

# Site-to-Site Connections

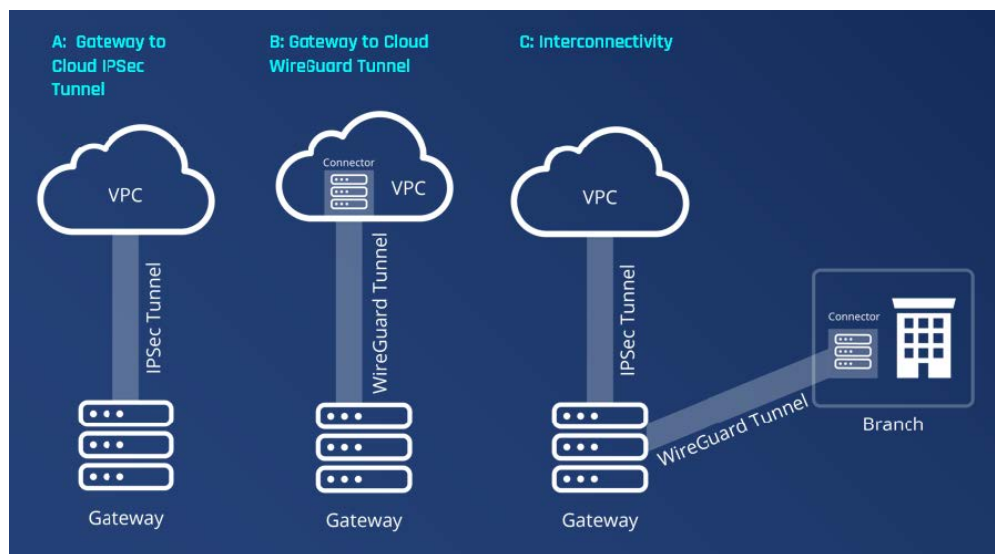
This article describes what site to site connectivity is, and compares the IPSec and Wireguard VPNs which can be used with the Platform.

## What is site to site connectivity?

This feature allows you to create a secure communication link between two different networks located at different sites. You can connect your gateway to your local network or cloud services.

## What options does SonicWall CloudEdge provide?

SonicWall CloudEdge offers the ability to use an IPSec tunnel or a [Wireguard connector](#).



## How do IPSec and Wireguard compare?

The following table shows a short comparison between the two VPNs.

## WireGuard Connector vs. IPsec Tunnel

|                             | WireGuard Connector | IPsec Tunnel    |
|-----------------------------|---------------------|-----------------|
| Site-to-Site Implementation | WireGuard           | strongSwan      |
| VPN Protocol                | WireGuard           | IKE             |
| Internet Protocol           | UDP                 | Any             |
| Setup Environment           | Linux               | Any             |
| Stability                   | High                | High            |
| Chipset Design Date         | 00's-10's           | 90's-00's       |
| Code Length                 | 4k                  | 400k-600k lines |

## IPsec tunnel

IPsec (IP Security) is a suite of protocols developed to ensure the integrity, confidentiality, and authentication of data communications over an IP network.

For more information, see the following sections:

- [Connecting On-Prem Infrastructure](#)
- [Connecting Cloud Infrastructure](#)

## Wireguard connector

WireGuard is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. It aims to be faster, simpler, leaner, and more useful than IPsec. WireGuard is designed as a general-purpose VPN for running on embedded interfaces and super computers alike, fit for many different circumstances.

For more information, see the [Configuring a WireGuard Connector](#) article.

## IPsec Tunnel

This article describes the IPsec Site-2-Site tunnel which is a security feature that allows you to create a secure communication link between two different networks located at different sites. By creating the IPsec Tunnel, you can connect your gateway to your local network or cloud services.

### ***To create a tunnel:***

Navigate to the **Networks** screen.

## Networks

Create and edit networks that are interconnected to your environments.

Available gateway licenses : 94/100

| Network                                 | Regions | Gateways | Tunnels | Access Groups   | Tags | Status |
|---|---------|----------|---------|-----------------|------|--------|
| tal-test<br>test-2-mls...lledge.biz     |         | 0        | 0       | test sonic, All | —    | Active |
| demo-monitor<br>test-2-veb...lledge.biz |         | 1        | 0       | All             | —    | Active |
| Africa<br>test-2-fn3...lledge.biz       |         | 1        | 0       | All             | —    | Active |

## Adding a tunnel

By selecting the three-dotted menu (...) on the right of the gateway, the **Add Tunnel** menu option will open the **IPSec Site-2-Site Tunnel** screen.

### To add a tunnel:

1. Select the **Add Tunnel** menu option and then **IPSec Site-2-Site Tunnel**.

### IPSec Site-2-Site Tunnel

Interconnect your cloud or on-premises with an IPSec site-2-site VPN connection.

#### General Settings

|   |   |
|---|---|
| <b>Name*</b> <input type="text" value="Enter name"/>  | <b>Shared Secret*</b> <input type="text" value="Enter shared secret"/> <input type="button" value="Generate"/>                        |
| <b>Public IP*</b> <input type="text" value="Enter public IP"/>  | <b>Remote ID*</b> <input type="text" value="Enter remote ID"/>  |
| <b>Perimeter B1 Gateway Proposal Subnets*</b> <input type="button" value="Any (0.0.0.0/0)"/> <input type="text" value="10.248.0.0/16"/> | <b>Remote Gateway Proposal Subnets*</b> <input type="button" value="Any (0.0.0.0/0)"/> <input type="text" value="Specified Subnets"/> |

#### Advanced Settings

|  |   |
|--|---|
| <b>IKE Version</b> <input type="button" value="V1"/> <input type="text" value="V2"/> | <b>IKE Lifetime</b> <input type="text" value="8h"/> |
|--|---|

2. Fill in the following details:

- **Name:** The name of the Tunnel you want to create.
- **Shared Secret:** A pre-shared key is a string of characters (like a password) that will be used by both of the tunnel parties.
- **Public IP:** This is the public IP address of the second end of the tunnel,
- **Remote ID:** In most cases, the ID of the remote tunnel is the public IP of the tunnel. However, it must be configured to the same value on both ends.
- **SonicWall CloudEdge Gateway Proposed Subnets:** The IPSec network selector must be configured to the same value at both ends of the tunnel.
- **Remote Gateway Proposed Subnets:** The remote subnet selector must be configured to the same value on both tunnels ends. If you do not specify the subnets, you will need to do so manually using the Routes Table configuration.

3. Select **Add Tunnel**.

The fields for the advanced settings depend on the network configuration, such as the type of VPC (Virtual Private Cloud) or firewall. The image below is just provided as an example.

The screenshot shows the 'Advanced Settings' configuration page for a tunnel. The settings are as follows:

| Setting                         | Value  |
|---------------------------------|--------|
| IKE Version                     | V1     |
| IKE Lifetime                    | 8h     |
| Tunnel Lifetime                 | 1h     |
| Dead Peer Detection Delay       | 10s    |
| Dead Peer Detection Timeout     | 30s    |
| Encryption (Phase 1)            | aes256 |
| Encryption (Phase 2)            | aes256 |
| Integrity (Phase 1)             | sha256 |
| Integrity (Phase 2)             | sha256 |
| Diffie-Hellman Groups (Phase 1) | 14     |
| Diffie-Hellman Groups (Phase 2) | 14     |

Buttons: Back, Add Tunnel

## WireGuard Connector

This article describes how to install a WireGuard based connector on a Linux server in your organization instead of creating a tunnel between your server and your Firewall/Router.

- Configuring the connector at the Management Platform
- Configuring the connector on your local Linux machine
- Verifying the connector is up

- ① **NOTE:** Cloud Edge Web Console Admin needs to add permissions for network controller in order to access SonicWall Cloud Edge agents using WireGuard protocol.

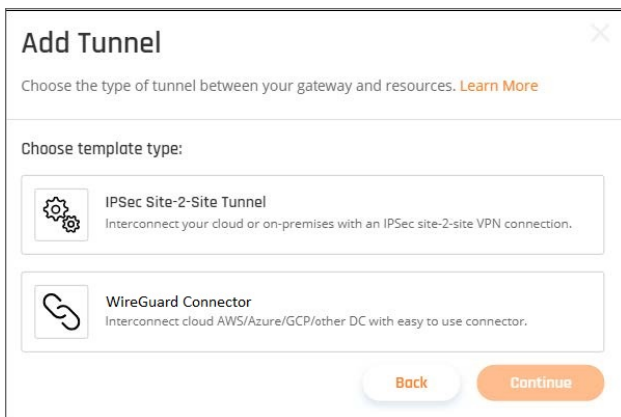
Please follow the steps below:

## Configuring the connector at the Management Platform

1. Under **Networks** in the **Management Platform** on the left side, select the name of the network in which you'd like to set the tunnel. Locate the desired gateway, select the three-dotted menu (...) and select **Add Tunnel**.

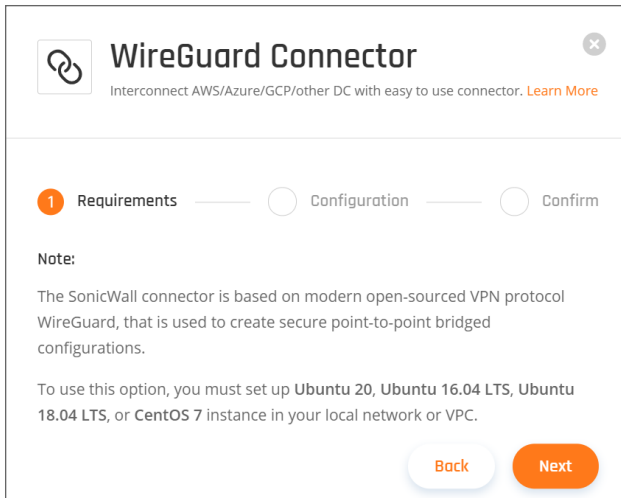


The following window displays:



2. Select **WireGuard Connector**, then select **Continue**.
3. Make sure you have a Windows server 2016, Ubuntu 16.04/18.04/20.04 LTS, CentOS/REHL7 or equivalent instance set within your local network or VPC, then select **Next**.



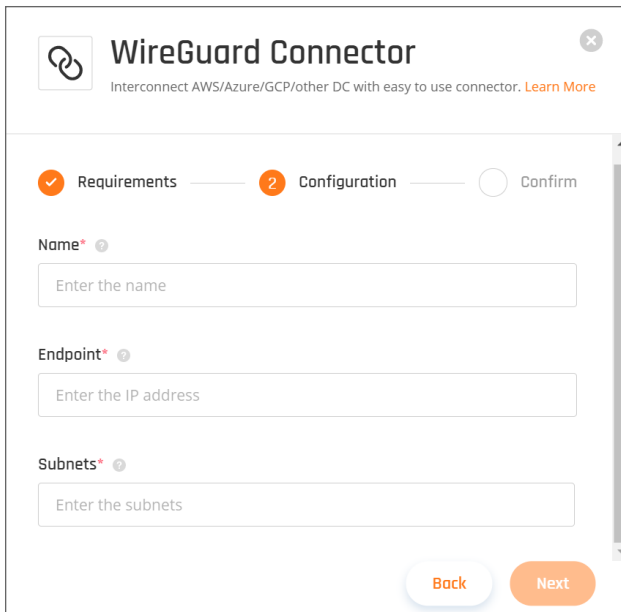


4. Enter a **Name** of your choice, and the **Endpoint**, meaning the IP address from which the Linux server is connecting to the internet, accompanied by the correlating **Subnet** range (the values in the attached image are for demonstration only).

5. Select **Next**.

① | **NOTE:** You can query the **Endpoint** by executing the following command in your Linux terminal:

```
dig +short myip.opendns.com @resolver1.opendns.com
```



6. Select **Confirm** and **Apply**, then wait until the deployment is finished (this may take several minutes).

## Configuring the connector on your local Linux machine

Make sure the machine that we'll be hosting the connector meets the following requirements:

## On Ubuntu:

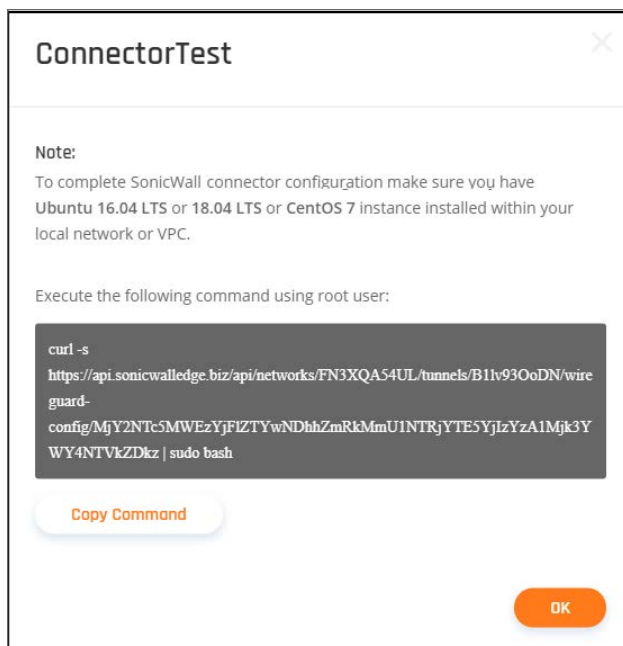
- Please see attached the [Prerequisites](#) for the machine.
- Your kernel is up to date.
- The following packages are installed:
  - curl
  - dig
  - software-properties-common

## On CentOS/REHL:

- Please see attached the [Prerequisites](#) for the machine.
- Your kernel is up to date.
- The following packages are installed:
  - curl
  - bind-utils

If you're not sure you possess the appropriate image installation files, you can find them [here](#) (Ubuntu 18.04).

1. You should now see the connector under the **Network** section. Select the three-dotted menu (...) besides its icon, then select **Configure**. A similar window will open (the displayed command varies from connector to connector):



2. Copy the command.
3. Open the Linux Terminal as Root user and run the copied command (select **Yes** at Stage 4 for access-only).
4. Follow the instructions during the connector installation on the Linux server.

## Verifying the connector is up

1. Connect to your SonicWall CloudEdge server with the designated app ( you can do it on any machine).
2. Open the terminal and run the following command:  
`ping xxxx.xxxx.xxxx.xxxx` (replace with one of the internal resources in your organization)
3. If the ping command fails, please make sure that port UDP/8000 is not blocked in your firewall/router, and that you went through all the steps.
4. If the issue persists, please contact our support services attaching the logs. These can be found at the following paths:  
##Configuration file  
`/etc/wireguard/wg0.conf`

## Setting up a WireGuard tunnel using a docker container

This article was written for the OSX Big Sur operating system, but should be able to support any system capable of running Docker. This behind the scenes process involves a similar setup to Wireguard Connector.

The basic docker container for WireGuard can run in its own container (We use the one from LinuxServer.io - but you can use one of your choice if you like). Then we download our peer config file for Wireguard and mount a shared folder to its location on the docker host in order to share it with the docker container. It's that easy!

### ***Install Docker on your OS:***

1. Get Docker
2. Pull the WireGuard Docker Container from LinuxServer.io

### ***Create a barebones config docker-compose.yaml file:***

#### **Linux Version**

```
---  
  
version: "2.1"  
  
services:  
  
  wireguard:  
  
    image: ghcr.io/linuxserver/wireguard  
  
    container_name: wireguard  
  
    cap_add:  
  
    - NET_ADMIN
```

```
- SYS_MODULE

environment:

- PUID=1000

- PGID=1000

- TZ=America/New_York

volumes:

- /var/tmp/config:/config

- /lib/modules:/lib/modules

ports:

- 8000:8000/udp

sysctls:

- net.ipv4.conf.all.src_valid_mark=1

restart: unless-stopped
```

## Windows Version

```
---

version: "2.1"

services:

wireguard:

image: ghcr.io/linuxserver/wireguard

container_name: wireguard

cap_add:

- NET_ADMIN

- SYS_MODULE

environment:

- PUID=1000
```

```
- PGID=1000

- TZ=America/New_York

volumes:

- C://wgConfig:/config

- /lib/modules:/lib/modules

ports:

- 8000:8000/udp

sysctls:

- net.ipv4.conf.all.src_valid_mark=1

restart: unless-stopped
```

The primary difference between Linux and Windows is the volume mount for the config file

#### **Create a wg0.conf file:**

- Make sure you create a config file and place it in this directory `/var/tmp/config`:
- `/var/tmp/config/wg0.conf`
- Reference for wg.conf file creation

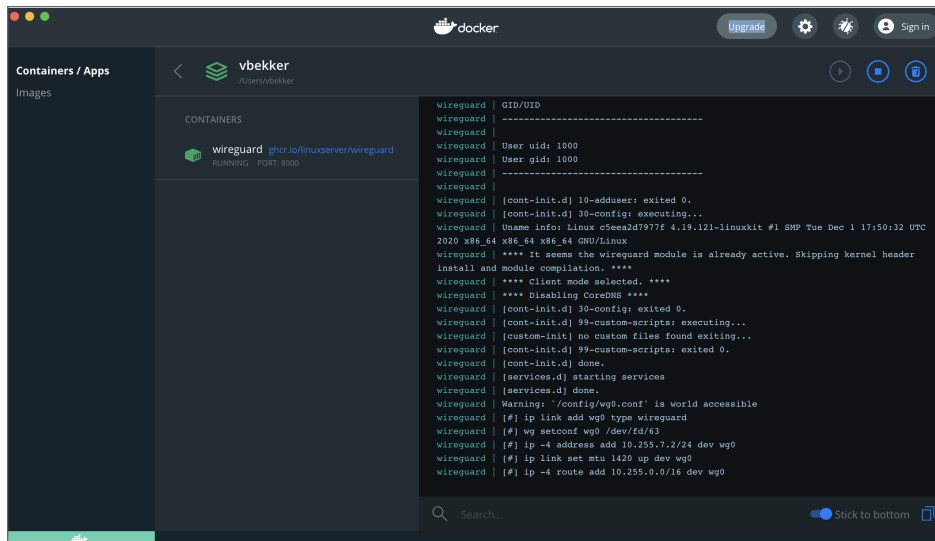
**⚠ CAUTION:** This config contains accurate information for tunnel establishment. This information must match exactly in order for the tunnel to come up. Please make sure that the wg0.conf file is created correctly. Please do not share your private key with anyone.

#### **Docker-compose run:**

Run the following command from command prompt or terminal. Make sure to run this from the directory where `docker-compose.yaml` resides

```
Docker-compose up -d
```

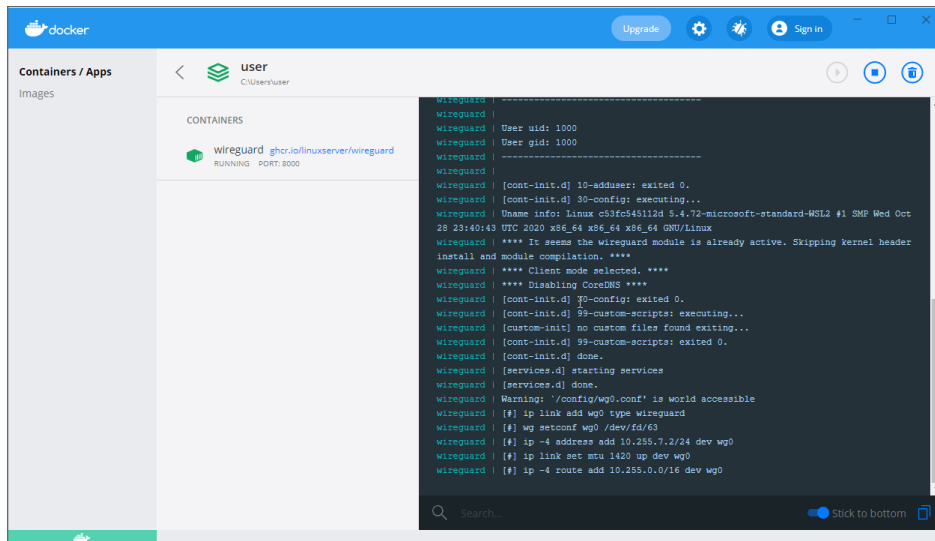
## Mac OSX



The screenshot shows the Docker Desktop interface on a Mac. The 'Containers / Apps' tab is active, showing a container named 'wireguard' running on port 8000. The terminal window displays the following output:

```
wireguard | GID/UID
wireguard | -----
wireguard | User uid: 1000
wireguard | User gid: 1000
wireguard | -----
wireguard | [cont-init.d] 10-adduser: exited 0.
wireguard | [cont-init.d] 30-config: executing...
wireguard | Uname info: Linux c5ea2d7977f2 4.19.121-linuxkit #1 SMP Tue Dec 1 17:50:32 UTC
2020 x86_64 x86_64 x86_64 GNU/Linux
wireguard | **** It seems the wireguard module is already active. Skipping kernel header
install and module compilation. ****
wireguard | **** Client mode selected. ****
wireguard | **** Disabling CoreDNS ****
wireguard | [cont-init.d] 30-config: exited 0.
wireguard | [cont-init.d] 99-custom-scripts: executing...
wireguard | [custom-init] no custom files found exiting...
wireguard | [cont-init.d] 99-custom-scripts: exited 0.
wireguard | [cont-init.d] done.
wireguard | [services.d] starting services
wireguard | [services.d] done.
wireguard | Warning: /config/wg0.conf is world accessible
wireguard | [#] ip link add wg0 type wireguard
wireguard | [#] wg setconf wg0 /dev/td/63
wireguard | [#] ip -4 address add 10.255.7.2/24 dev wg0
wireguard | [#] ip link set mtu 1420 up dev wg0
wireguard | [#] ip -4 route add 10.255.0.0/16 dev wg0
```

## Windows 10



The screenshot shows the Docker Desktop interface on Windows 10. The 'Containers / Apps' tab is active, showing a container named 'wireguard' running on port 8000. The terminal window displays the following output:

```
wireguard | -----
wireguard | User uid: 1000
wireguard | User gid: 1000
wireguard | -----
wireguard | [cont-init.d] 10-adduser: exited 0.
wireguard | [cont-init.d] 30-config: executing...
wireguard | Uname info: Linux c53fc545112d 5.4.72-microsoft-standard-WSL2 #1 SMP Wed Oct
28 23:40:43 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
wireguard | **** It seems the wireguard module is already active. Skipping kernel header
install and module compilation. ****
wireguard | **** Client mode selected. ****
wireguard | **** Disabling CoreDNS ****
wireguard | [cont-init.d] 30-config: exited 0.
wireguard | [cont-init.d] 99-custom-scripts: executing...
wireguard | [custom-init] no custom files found exiting...
wireguard | [cont-init.d] 99-custom-scripts: exited 0.
wireguard | [cont-init.d] done.
wireguard | [services.d] starting services
wireguard | [services.d] done.
wireguard | Warning: /config/wg0.conf is world accessible
wireguard | [#] ip link add wg0 type wireguard
wireguard | [#] wg setconf wg0 /dev/td/63
wireguard | [#] ip -4 address add 10.255.7.2/24 dev wg0
wireguard | [#] ip link set mtu 1420 up dev wg0
wireguard | [#] ip -4 route add 10.255.0.0/16 dev wg0
```

# Connect On-Prem Resources

## Topics:

- Firewalls

# Firewalls

## Topics:

- [General Settings](#)

## SonicWall

This article describes how to configure to establish a Site-To-Site IPSec VPN connection between a SonicWall firewall and the network.

- Tunnel creation
- Creating objects in SonicWall Cloud Edge
- Site to site creation

## Tunnel creation

1. Go to the Gateway in your network from which you want to create the tunnel to Azure.
2. Select the three-dotted menu (...) and select **Add Tunnel**.

## General Settings

**IPSec Site-2-Site Tunnel**  
Interconnect your cloud or on-premises with an IPSec site-2-site VPN connection.

### General Settings

**Name\***

**Shared Secret\***

**Public IP\***

**Remote ID\***

**SonicWall Gateway Proposal Subnets\***

**Remote Gateway Proposal Subnets\***

3. Name - Set the name for the Tunnel.
4. Shared Secret - Put a shared secret or select **Generate**.
5. **Public IP** and **Remote ID** - put your SonicWall Public IP address.
6. In **Gateway Proposal Subnets** Choose **Any** or **Specific Subnet**.
7. In **Remote Gateway Proposal Subnets** put your internal subnet.

### IPSec Site-2-Site Tunnel

Interconnect your cloud or on-premises resources with an IPSec site-2-site VPN connection. [Learn More](#)

✕

#### Advanced Settings

IKE Version

V1

V2

IKE Lifetime

Tunnel Lifetime

Dead Peer Detection Delay

Dead Peer Detection Timeout

Encryption (Phase 1)

aes256
✕
▼

Encryption (Phase 2)

aes256
✕
▼

Integrity (Phase 1)

sha256
✕
▼

Integrity (Phase 2)

sha256
✕
▼

Diffie-Hellman Groups (Phase 1)

14
✕
▼

Diffie-Hellman Groups (Phase 2)

14
✕
▼

Back
Add Tunnel

## Advanced Settings

- **IKE Version:** V2
- **IKE Lifetime:** 8h
- **Tunnel Lifetime:** 1h
- **Dead Peer Detection Delay:** 10s
- **Dead Peer Detection Timeout:** 30s
- **Encryption (Phase 1):** aes256
- **Encryption (Phase 2):** aes256
- **Integrity (Phase 1):** sha1
- **Integrity (Phase 2):** sha1
- **Diffie-Hellman Groups (Phase 1):** 2
- **Diffie-Hellman Groups (Phase 2):** 2

8. Select **Add Tunnel**.

## Creating objects in SonicWall Cloud Edge

1. Go to **Objects** in SonicWall Cloud Edge.
2. Go to Address Object.
3. Select **Add**.
4. Add Gateway address.



The screenshot shows the 'Address Object Settings' dialog box. The 'Name' field is 'SDP VPN Gateway'. The 'Zone Assignment' dropdown is set to 'VPN'. The 'Type' dropdown is set to 'Host'. The 'IP Address' field is '172.105.57.96'. There are 'Cancel' and 'Save' buttons at the bottom.

- **Name:** SDP VPN Gateway
- **Zone Assignment:** VPN
- **Type:** Host
- **IP Address:** 172.105.57.96

5. Add Subnet Network.

The screenshot shows the 'Address Object Settings' dialog box. The 'Name' field is 'SDP Network'. The 'Zone Assignment' dropdown is set to 'VPN'. The 'Type' dropdown is set to 'Network'. The 'Network' field is '10.255.0.0'. The 'Netmask / Prefix Length' field is '255.255.0.0'. There are 'Cancel' and 'Save' buttons at the bottom.

- **Name:** SDP Network
- **Zone Assignment:** VPN
- **Type:** Network
- **Network:** 10.255.0.0
- **Netmask/Prefix Length:** 255.255.0.0

The screenshot shows the 'Address Object Settings' dialog box. The 'Name' field is 'SonicWall Local LAN'. The 'Zone Assignment' dropdown is set to 'VPN'. The 'Type' dropdown is set to 'Network'. The 'Network' field is '10.40.0.0'. The 'Netmask / Prefix Length' field is '255.255.0.0'. There are 'Cancel' and 'Save' buttons at the bottom.

- **Name:** SonicWall Local LAN
- **Zone Assignment:** VPN
- **Type:** Network
- **Network:** 10.40.0.0
- **Netmask/Prefix Length:** 255.255.0.0
- **Access Rule 1. Go to Policy:-> Rules.**

6. Select **Add**.

7. First Rule to add: **SDP WAN Rule**

**Editing Rule**

Name: SDP WAN Rule

Tags: add upto 3 tags, use comma as separator...

Description: provide a short description of your access rule...

Action: Allow (selected), Deny, Discard

Type: IPv4 (selected), IPv6

Schedule: Always

Enable: On

Security Rule Action: Default Profile

Source / Destination: User & Country, App/URL/Custom Match

**SOURCE**

Zone/Interface: VPN

Address: SDP VPN Gateway

Port/Services: Any

**DESTINATION**

Zone/Interface: WAN

Address: WAN Subnets

Port/Services: Any

Show Diagram:

Buttons: Cancel, Save As, Save

- **Policy Name:** SDP WAN Rule
- **Action:** Allow
- **Type:** IPv4
- **Schedule:** Always
- **Enable:** On
- **Security Rule Action :** Default Profile
- **Source Zone/Interface:** VPN
- **Source Address:** SDP VPN Gateway
- **Source Port/Services:** Any
- **Destination Zone/Interface:** WAN
- **Destination Address:** WAN Subnets
- **Destination Port/Services:** Any
- Select **Save**.

## Second Rule: VPN to LAN

**Editing Rule**

Name: SonicWall LAN Rule

Tags: add upto 3 tags, use comma as separator...

Description: provide a short description of your access rule...

Action: Allow (selected), Deny, Discard

Type: IPv4 (selected), IPv6

Schedule: Always

Enable: On

Security Rule Action: Default Profile

Source / Destination: User & Country, App/URL/Custom Match

**SOURCE**

Zone/Interface: VPN

Address: SDP Network

Port/Services: Any

**DESTINATION**

Zone/Interface: LAN

Address: SonicWall Local LAN

Port/Services: Any

Show Diagram:

Buttons: Cancel, Save As, Save

- **Policy Name:** SonicWall LAN Rule
- **Action:** Allow
- **Type:** IPv4
- **Schedule:** Always
- **Enable:** On
- **Security Rule Action :** Default Profile
- **Source Zone/Interface:** VPN
- **Source Address:** SDP Network
- **Source Port/Services:** Any
- **Destination Zone/Interface:** LAN
- **Destination Address:** SonicWall Local LAN
- **Destination Port/Services:** Any

- Select **Save**.

## Site-to-Site creation

1. Go to VPN.
2. Under **Base Settings** add **VPN Policy**.

## General Tab

The screenshot shows the 'VPN Policy' configuration page with the 'General' tab selected. The page is divided into two main sections: 'SECURITY POLICY' and 'IKE AUTHENTICATION'. In the 'SECURITY POLICY' section, the 'Policy Type' is set to 'Site to Site', the 'Authentication Method' is 'IKE Using Preshared Secret', the 'Name' is 'CloudEdgeIPSEC', the 'IPsec Primary Gateway Name or Address' is '172.105.57.96', and the 'IPsec Secondary Gateway Name or Address' is '0.0.0.0'. In the 'IKE AUTHENTICATION' section, the 'Shared Secret' and 'Confirm Shared Secret' fields are masked with asterisks, and the 'Mask Shared Secret' checkbox is checked. The 'Local IKE ID' is set to 'IPv4 Address' with the value '3.20.28.110', and the 'Peer IKE ID' is set to 'IPv4 Address' with the value '172.105.57.96'. At the bottom of the form are 'Cancel' and 'Save' buttons.

## Security Policy

- **Policy Type:** Site to Site
- **Authentication Method:** IKE using Preshared Secret
- **Name:** Give it name ex. "CloudEdgeIPSEC"
- **IPsec Primary Gateway Name or Address:** 172.105.57.96
- **IPsec Secondary Gateway Name or Address:** 0.0.0.0

## IKE Authentication

- **Shared Secret:** put the same shared secret you set in the Management Platform
- **Confirm Secret:** put the secret again
- **Local IKE ID:** IPv4 Address: 3.20.28.110
- **Peer IKE ID:** IPv4 Address: 172.105.57.96

# Network Tab

The screenshot shows the 'Network' tab of the 'VPN Policy' configuration page. It is divided into two sections: 'LOCAL NETWORKS' and 'REMOTE NETWORKS'. In the 'LOCAL NETWORKS' section, there is a dropdown menu for 'Choose local network from list' with 'SonicWall Local LAN' selected, and a radio button for 'Any address' which is unselected. In the 'REMOTE NETWORKS' section, there is a radio button for 'Use this VPN Tunnel as default route for all Internet traffic' which is unselected. Below it, there is a dropdown menu for 'Choose destination network from list' with 'SDP Network' selected, and another dropdown menu for 'Use IKEv2 IP Pool' with '-- Select Remote Network --' selected. At the bottom, there are 'Cancel' and 'Save' buttons.

# Local Networks

- Select a local network from the list: choose your local network object

# Remote Networks

- Select the destination network from the list: choose Network object

# Proposals Tab

The screenshot shows the 'Proposals' tab of the 'VPN Policy' configuration page. It is divided into two sections: 'IKE (PHASE 1) PROPOSAL' and 'IPSEC (PHASE 2) PROPOSAL'. In the 'IKE (PHASE 1) PROPOSAL' section, there are dropdown menus for 'Exchange' (IKEv2 Mode), 'DH Group' (Group 14), 'Encryption' (AES-256), and 'Authentication' (SHA256). There is also a text input field for 'Life Time (seconds)' with the value 28800. In the 'IPSEC (PHASE 2) PROPOSAL' section, there are dropdown menus for 'Protocol' (ESP), 'Encryption' (AES-256), and 'Authentication' (SHA256). There is a toggle switch for 'Enable Perfect Forward Secrecy' which is turned on. There is also a dropdown menu for 'DH Group' (Group 14) and a text input field for 'Life Time (seconds)' with the value 28800. At the bottom, there are 'Cancel' and 'Save' buttons.

# IKE (Phase 1) Proposal

- **Exchange:** IKEv2 Mode

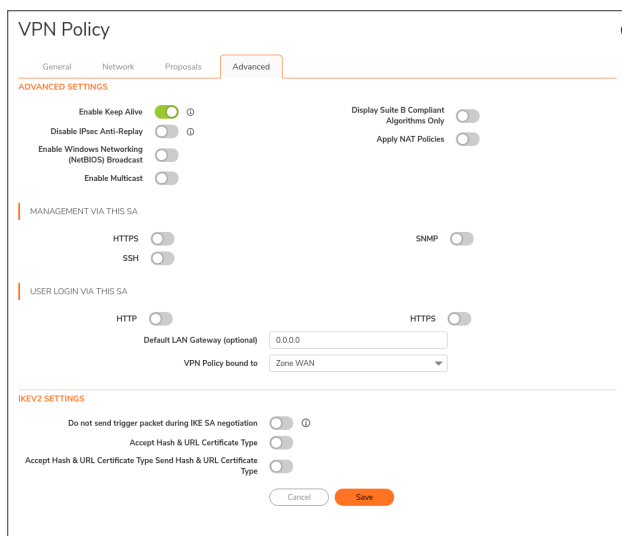
- **DH Group:** Group 14
- **Encryption:** AES-256
- **Authentication:** SHA256
- **Life Time (seconds):** 28800

## IPsec (Phase 2) Proposal

- **Protocol:** ESP
- **Encryption:** AES-256
- **Authentication:** SHA256
- **Select "Enable Perfect Forward Security"**
- **DH Group:** Group 14
- **Life Time (seconds):** 28800

You can use different Encryption, Authentication, and DH Group setting as long as you put the same settings in the Management Platform.

## Advanced Tab



## Advanced Setting

1. Mark v in **Enable Keep Alive**.
2. Select **OK** to create the new VPN Policy.

Make sure the new Policy you created is enabled. You can select the play button right to the **Currently Active VPN Tunnels** and you should see that your new tunnel is up.

If the tunnel won't start you should go to **Event Logs** and look for errors regarding the new VPN policy you created.

## Connect Cloud Resources

### Topics:

- [Amazon AWS](#)
- [Alibaba Cloud](#)
- [Microsoft Azure](#)
- [Google Cloud Platform](#)
- [Heroku Enterprise](#)
- [IBM Cloud](#)
- [Docker](#)

## Amazon AWS

### Topics:

- [AWS Virtual Gateway](#)
- [Create the Transit Gateway](#)

## AWS Virtual Gateway

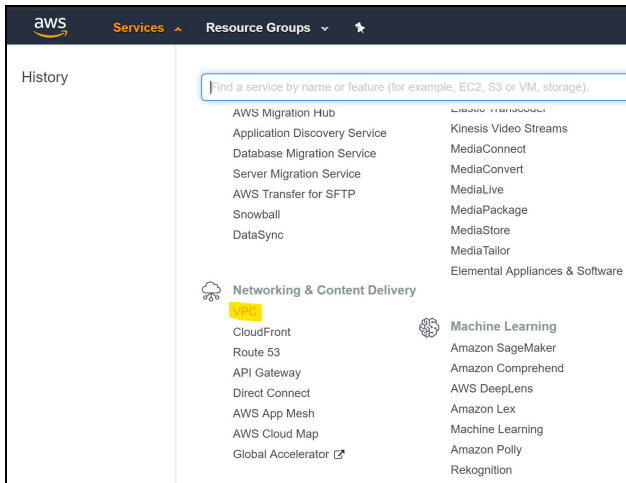
This article describes how to establish a Site-To-Site IPSec VPN connection between your AWS server and the SonicWall Cloud Edge network.

- [Configuring the tunnel in the AWS Console](#)
- [Configuring a virtual private gateway](#)
- [Creating a virtual private network connection](#)
- [Configuring the tunnel in your Management Platform](#)

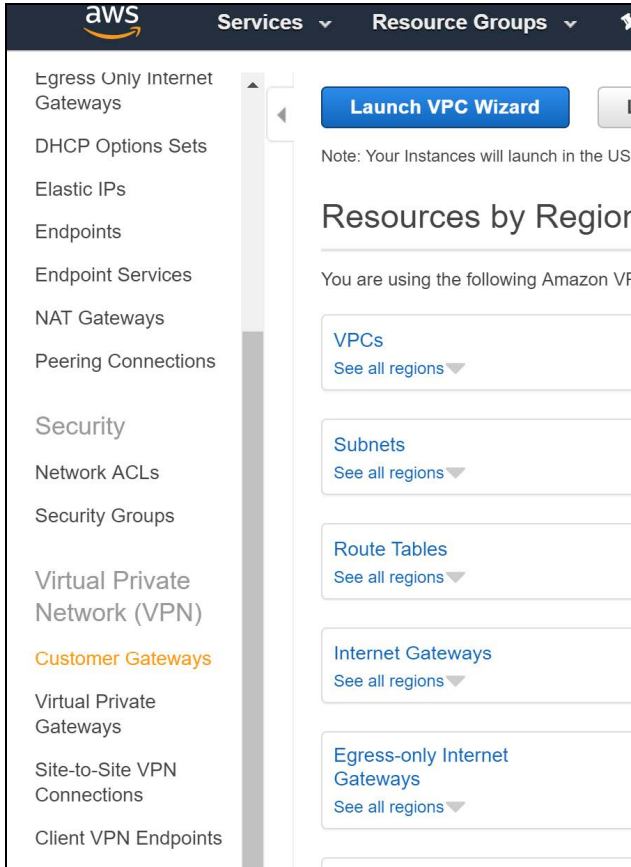
Please follow the steps below:

### Configuring the tunnel in the AWS Console

1. Go to the **VPC section** in the **AWS Console**.
2. Under **Services**, scroll down to **Networking & Content Delivery** and select **VPC**.



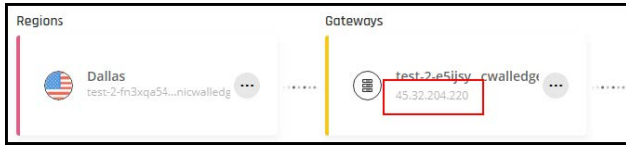
3. Under the left menu **VPN** section, go to **Customer Gateways**.



4. Select **Create Customer Gateway**.

5. Select **static** routing.

- Fill in the IP Address of the SonicWall Cloud Edge gateway. This can be obtained within the SonicWall Cloud Edge panel, under **Networks**.

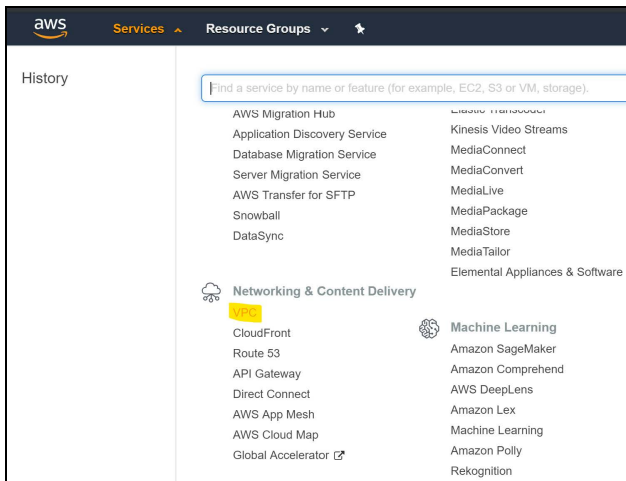


- Select **Create Customer Gateway**. A message should display indicating the gateway was created successfully.

## Configuring a virtual private gateway

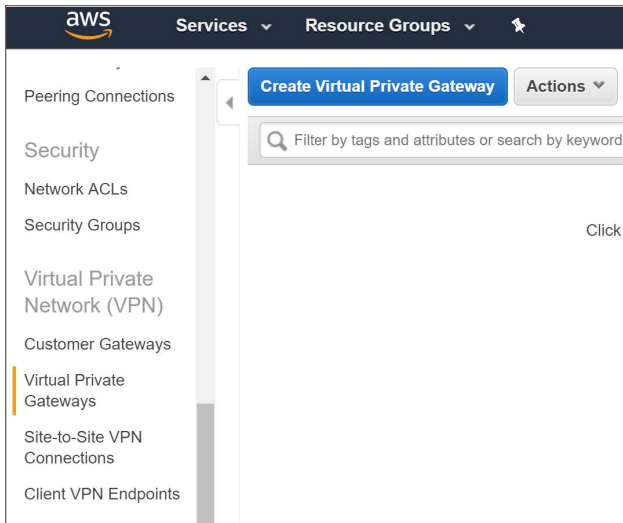
**IMPORTANT:** If you already have a virtual private gateway attached to your VPC, skip this section and continue at **Creating a virtual private network connection**.

- Go back to **Services**, scroll down to **Networking & Content Delivery**, and select **VPC**.

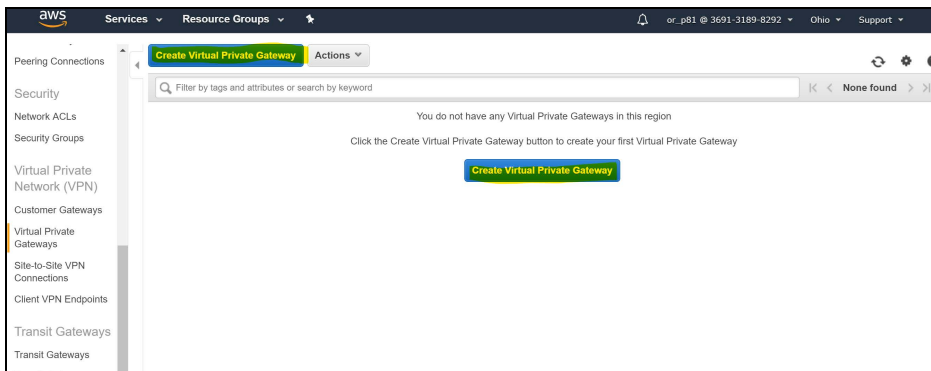




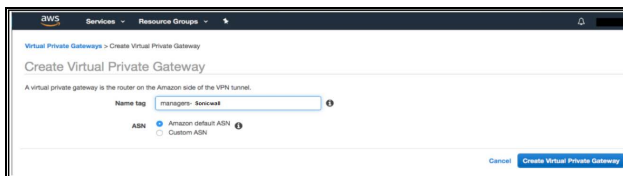
2. On the left side, under **Virtual Private Network (VPN)** select **Virtual Private Gateways**.



3. Select **Create Virtual Private Gateway**.

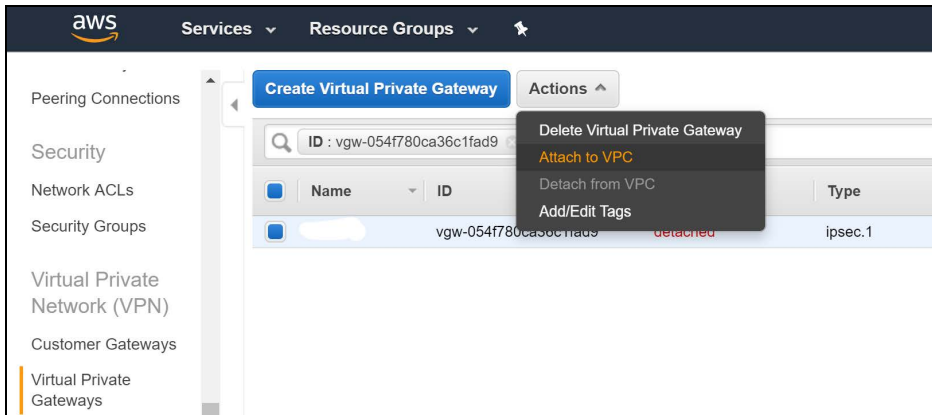


4. Type the name of the gateway (for example US\_HQ ).
5. Select **ASN** as Amazon default ASN.
6. Select **Create Virtual Private Gateway**.



A message should display indicating that the virtual **Private Gateway** was created successfully.

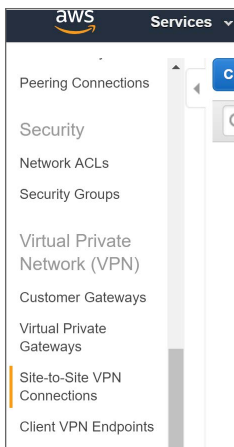
7. Select the newly created gateway and select **Actions**; on the context menu select **Attach to VPC**.



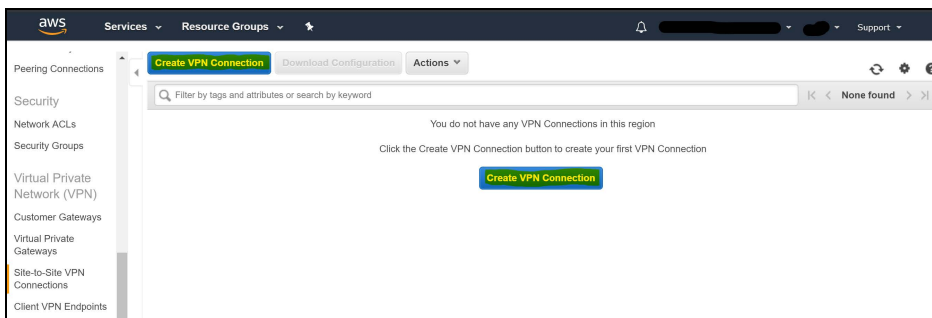
- From the drop-down menu, select the VPC and select **Yes, Attach**.

## Creating a virtual private network connection

- Under **Virtual Private Network** in the left menu, go to **Site-to-Site VPN Connections**.



- Select **Create VPN Connection**.



- Enter the name tag (for example US\_HQ).
- Select the created **Virtual Private Gateway**.

5. Under Customer Gateway, select **Existing**.
6. Select the **Customer Gateway** that you have created.
7. Under Routing Options, select **Static**.
8. Fill in the following Static IP Prefixes: **10.XXX.0.0/16** (according to your SonicWall Cloud Edge network subnet)
  - ① **IMPORTANT:** This address might differ in case you haven't chosen the default subnet mask for your tunnel.

The screenshot shows the 'Create VPN Connection' page in the AWS console. The 'Customer Gateway' is set to 'Existing' with ID 'cgw-0-3825f68fb'. 'Routing Options' are set to 'Static'. Under 'Static IP Prefixes', a table shows one entry with 'IP Prefixes' as '10.255.0.0/16', 'Source' as '-', and 'State' as '-'. An 'Add Another Rule' button is visible below the table.

9. Under **Tunnel Options** leave the default values as is.

① **IMPORTANT: Tunnel option**  
 AWS supports various types of Encryptions and hash formats for both of the tunnels they are offering, if the tunnel options are set to default (as shown below) it will accept any encryption suite you'd like for the handshake with SonicWall Cloud Edge.

The screenshot shows the 'Tunnel Options' section in the AWS console. It shows fields for 'Inside IPv4 CIDR for Tunnel 1', 'Pre-Shared Key for Tunnel 1', 'Inside IPv4 CIDR for Tunnel 2', and 'Pre-shared key for Tunnel 2', all with 'Generated by Amazon' as the default value. Below these are 'Advanced Options for Tunnel 1' and 'Advanced Options for Tunnel 2', both with 'Use Default Options' selected.

In this screen you can also select the inside subnets you would like to connect via the tunnel.

10. Select **Create VPN Connection**.

**Tunnel Options**  
Customize tunnel inside CIDR and pre-shared keys for your VPN tunnels. Unspecified tunnel options will be randomly generated by Amazon.

Inside IP CIDR for Tunnel 1  ⓘ

Pre-Shared Key for Tunnel 1  ⓘ

Inside IP CIDR for Tunnel 2  ⓘ

Pre-shared key for Tunnel 2  ⓘ

Advanced Options for Tunnel 1  
 Use Default Options  
 Edit Tunnel 1 Options

Advanced Options for Tunnel 2  
 Use Default Options  
 Edit Tunnel 2 Options

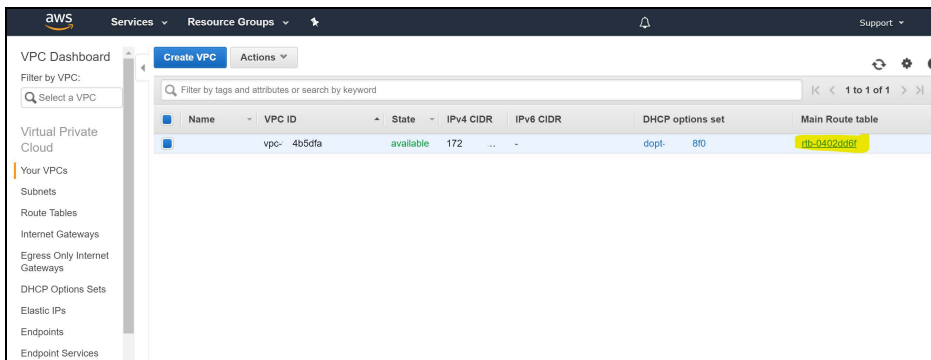
VPN connection charges apply once this step is complete. [View Rates](#)

\* Required Cancel [Create VPN Connection](#)

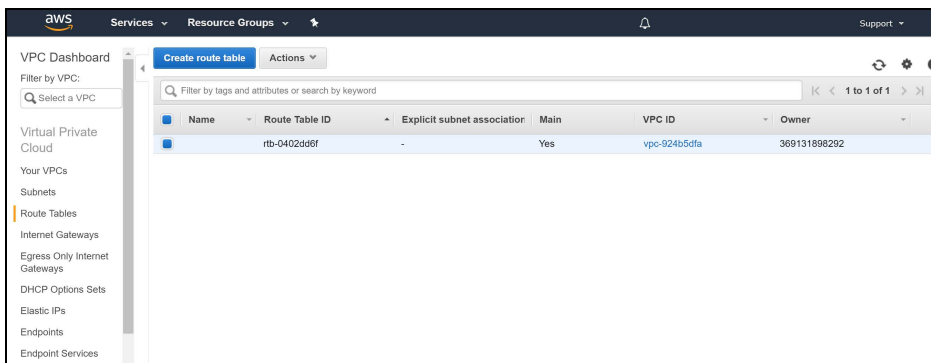
11. A message should display indicating that a **VPN Connection Request** was created successfully.

## Configuring the routing rules to the default gateway

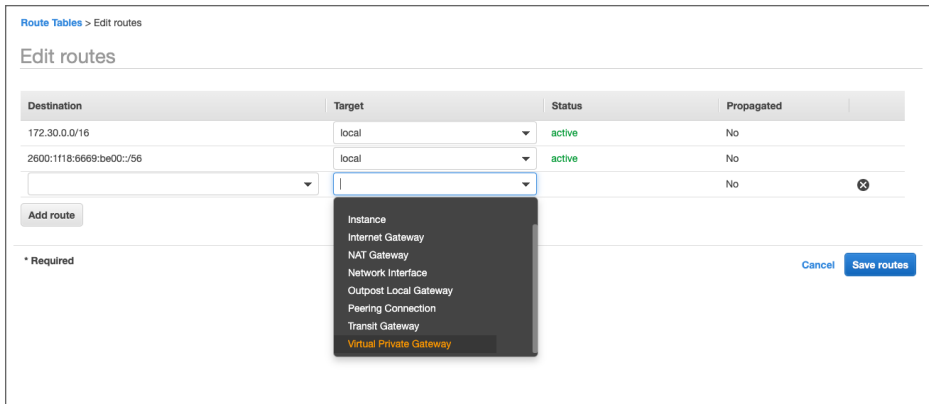
1. Select the **VPC** section in the **AWS Console** and enter the Route table associated with your VPC.



2. For the **Route Tables** menu option, select the routing table that is associated with the VPC you have created for the tunnel.



3. Select **Edit** and add the new static routes for the subnets below:



Fill in **10.2xx.0.0/16** (SonicWall Cloud Edge network subnet listed in the SonicWall Cloud Edge web portal, in Networks > Gateway > Settings) at the destination field and your new VPN Gateway ID as the target (it will appear under the subcategory Virtual Private Gateway).

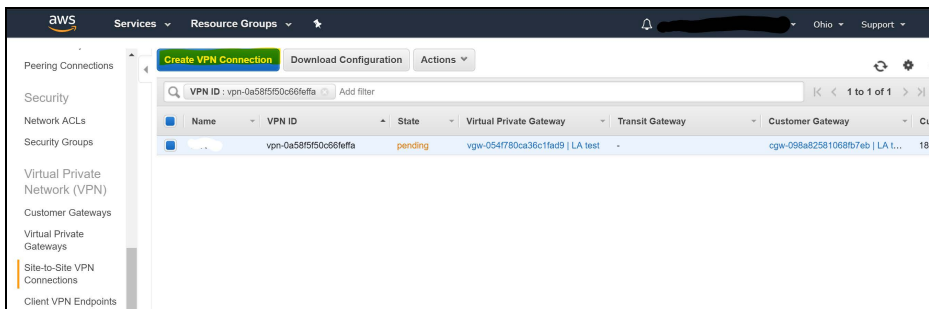
4. Select **Save**.

In case have a customized security group associated with your VPC:

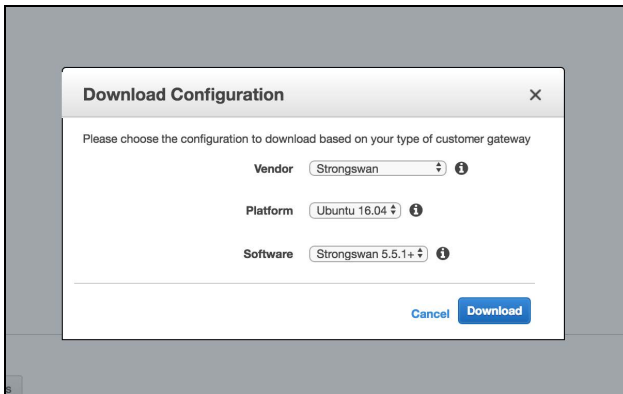
Allow incoming connections from the local network within your security groups: Configure your AWS security groups to allow all traffic from SonicWall Cloud Edge subnets (10.2xx.0.0/16) or allow only special traffic using the port or services from these sources.

## Configuring the tunnel in your Platform

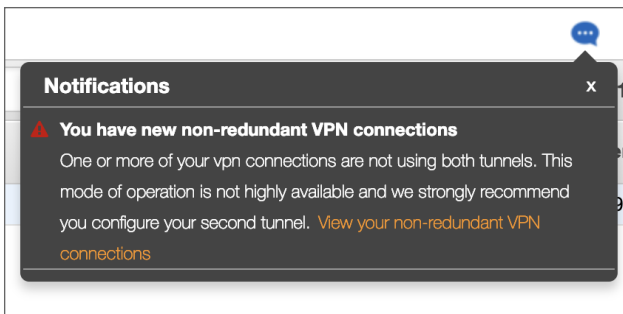
1. Return to **Site-to-Site VPN Connections** and select **Download Configuration**.



2. Fill in the following information, and download the config file:



- ❗ **IMPORTANT:** Examining the configuration file, you may notice that AWS has created two separate tunnels for the same VPN connection, however, SonicWall Cloud Edge utilizes only one of them. You may randomly choose any of the two, but for consistency purposes and in order to avoid possible confusion we advise you to use the one that appears first in the file.



3. Go to the Management Platform. Under the **Networks** tab in the left menu, select the name of the network where you'd like to set the tunnel.



4. Locate the desired gateway, select the three-dotted menu (...), select **Add Tunnel**, and then **IPSec Site-2-Site Tunnel**.
5. Open the configuration file that you have downloaded. Fill in the following fields according to the file's content: **Public IP**, **Remote ID** (both identical; marked in red in the attached example) and **Shared Secret** (marked in yellow; remember to omit the quotation marks).

```
4) Create a new file at /etc/ipsec.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!). This value authenticates the tunnel endpoints:
185.253.69.17 18.16.10.253 : PSK "0zquwHAc0TfLR0vuKRVrqSAb0"
```

6. The rest of the fields should be filled in with the following information:

**IPSec Site-2-Site Tunnel**  
Interconnect your cloud or on-premises with an IPSec site-2-site VPN connection.

### General Settings

Name\*

Shared Secret\*

Public IP\*

Remote ID\*

Perimeter B1 Gateway Proposal Subnets\*

Remote Gateway Proposal Subnets\*

### Advanced Settings

IKE Version

IKE Lifetime

- **Name:** Enter the name you chose for the tunnel.
- **SonicWall Cloud Edge Gateway Proposal Subnets:** By default, this should be set to 10.2xx.0.0/16.
- **Remote Gateway Proposal Subnets:** Select specified Subnets. Insert your VPC CIDR.

| Name              | VPC ID                | State     | IPv4 CIDR     |
|-------------------|-----------------------|-----------|---------------|
| Sonicwall Staging | vpc-0851a4a8314b63b94 | available | 172.30.0.0/16 |

- At the **Advanced Settings** section fill in the following information if you selected the default tunnel options on AWS:

**Advanced Settings**

IKE Version: V1 | IKE Lifetime: 8h

Tunnel Lifetime: 1h | Dead Peer Detection Delay: 10s | Dead Peer Detection Timeout: 30s

Encryption (Phase 1): aes256 | Encryption (Phase 2): aes256

Integrity (Phase 1): sha256 | Integrity (Phase 2): sha256

Diffie-Hellman Groups (Phase 1): 14 | Diffie-Hellman Groups (Phase 2): 14

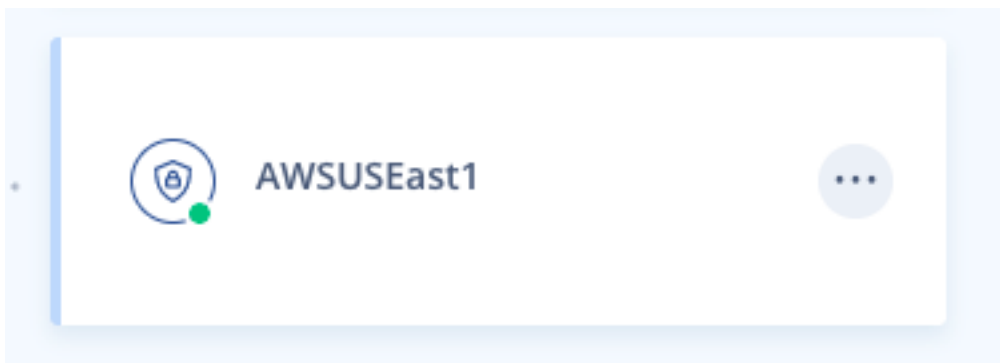
Back | Add Tunnel

- **IKE Version:** V2
- **IKE Lifetime:** 8h
- **Tunnel Lifetime:** 1h
- **Dead Peer Detection Delay:** 10s
- **Dead Peer Detection Timeout:** 30s
- **Encryption(Phase 1):** aes256
- **Encryption(Phase 2):** aes256
- **Integrity (Phase 1):** sha512
- **Integrity (Phase 2):** sha512
- **Diffie-Hellman Groups (Phase 1):** 21
- **Diffie-Hellman Groups (Phase 2):** 21

- Select Add Tunnel.

## Troubleshooting the connection

- To verify the tunnel is UP, check your SonicWall Cloud Edge interface for the Green dot next to the tunnel:



- You can check the tunnel routes via "Routes Table" inside the SonicWall Cloud Edge network



3. Even if the tunnel state is UP, you may still not be able to reach your VPC via the tunnel, further steps to verify AWS reachability may include:
  - Checking the route table that's associated with your VPC for a route that pushes traffic from the internal range for SonicWall Cloud Edge to the VPG
  - Checking the route table that's associated with the specific Subnet you are trying to access (if different from the main VPC route table)
  - Check to see if you have a Security Group that allows traffic from the internal range for SonicWall Cloud Edge to your AWS resource

## AWS Transit Gateway

This article describes how to connect multiple VPCs using a single Site-to-Site connection like AWS Transit Gateway (unlike the AWS Virtual Gateway which requires one Site-to-Site connection per VPC). Inter-region Transit Gateway peering is available in US East (N. Virginia), US East (Ohio), US West (Oregon), EU (Ireland), and EU (Frankfurt) while currently in other regions TG is restricted to a single region.

① **IMPORTANT:** The choice between Transit Gateway or a simple Virtual Gateway depends on your AWS architecture. If you are not sure, we encourage you to visit AWS's [official documentation](#).

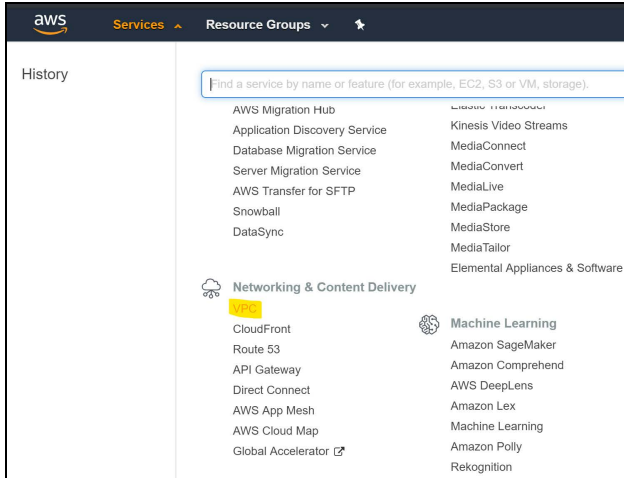
Please follow the steps below:

- Create the Transit Gateway & Transit Gateway attachments
- Configuring the tunnel in the AWS Console
- Configuring the tunnel on the SonicWallCloud Edge web platform
- Configuring the routing in the AWS Console
- Configuring the routing on the SonicWallCloud Edge web platform

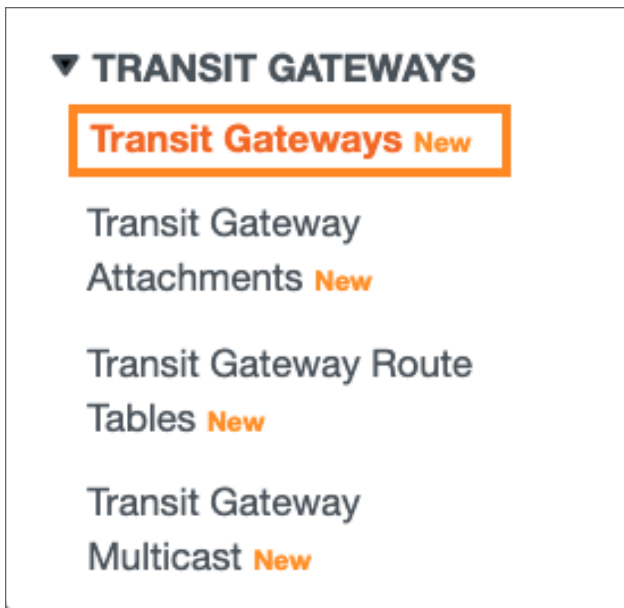
## Create the Transit Gateway & Transit Gateway attachments

# Create the Transit Gateway

1. Go to the **VPC** section in the **AWS Console**.



2. Under the left panel, click on **Transit Gateways**



3. On the top pane, click on **Create transit gateway**



4. Fill in the following information:

### Details - optional

**Name tag**  
Creates a tag with the key set to Name and the value set to the specified string.

**Description** [Info](#)  
Set the description of your transit gateway to help you identify it in the future.

### Configure the transit gateway

**Amazon side Autonomous System Number (ASN)** [Info](#)

**DNS support** [Info](#)

**VPN ECMP support** [Info](#)

**Default route table association** [Info](#)

**Default route table propagation** [Info](#)

**Multicast support** [Info](#)

### Configure cross-account sharing options

**Auto accept shared attachments** [Info](#)

### Transit gateway CIDR blocks

**CIDR - optional** [Info](#)

### Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add 50 more tags.

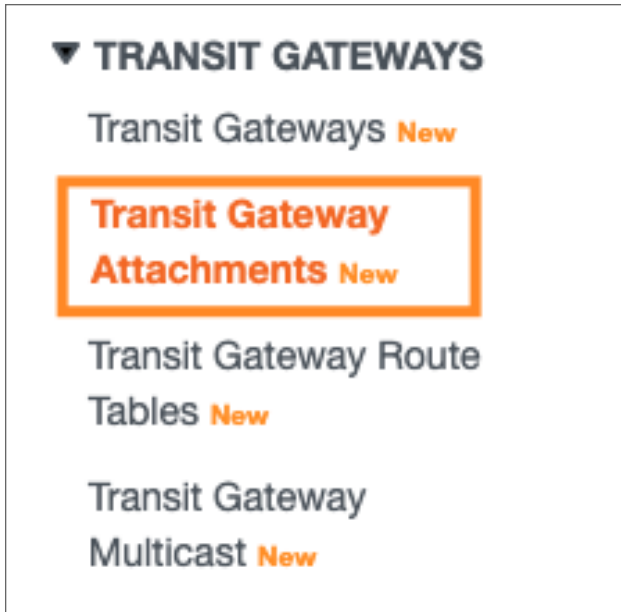
- **Name tag** - Insert the name of the Transit Gateway
- You can keep the default parameters for the rest of the attributes

5. Click on **Create transit gateway**.

## Create the Transit Gateway attachments

# Create the Transit Gateway VPC attachments

1. On the left pane, click on Transit Gateway Attachments



2. On the top pane, click on **Create transit gateway attachment**



3. Fill in the following information and click on **Create transit gateway attachment**:

**Details**

**Name tag - optional**  
Creates a tag with the key set to Name and the value set to the specified string.

transit-gateway-attachment-01

**Transit gateway ID** [Info](#)  
Select a transit gateway

**Attachment type** [Info](#)  
VPC

---

**VPC attachment**  
Select and configure your VPC attachment.

**DNS support** [Info](#)

**IPv6 support** [Info](#)

**VPC ID**  
Select the VPC to attach to the transit gateway.  
Select a VPC

---

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)  
You can add 50 more tags.

Cancel [Create transit gateway attachment](#)

- **Name Tag** - Insert the name of the Transit Gateway Attachment
- **Transit gateway ID** - Pick the newly created Transit gateway
- **Attachment Type** - VPC
- **VPC ID** - Select the relevant VPC
- You can keep the default parameters for the rest of the attributes

① | **NOTE:** Repeat the above process for each of the VPCs that you would like to gain access to.

## Create the Transit Gateway VPN attachment

1. On the top pane, click on **Create transit gateway attachment**.



2. Fill in the following information and click on **Create transit gateway attachment**:

### Create transit gateway attachment [Info](#)

A transit gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same AWS account or across AWS accounts.

**Details**

Transit gateway ID [Info](#)

Attachment type [Info](#)

**VPN Attachment**

Create a new customer gateway or select an existing customer gateway that you would like to connect to the transit gateway via a VPN connection.

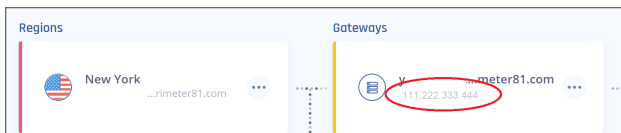
Customer Gateway [Info](#)  
 Existing  
 New

Customer Gateway ID [Info](#)

Routing options [Info](#)  
 Dynamic (requires BGP)  
 Static

Enable Acceleration (Improve performance of VPN tunnels via AWS Global Accelerator and the AWS global network) [Info](#)

- **Transit gateway ID** - Pick the newly created Transit gateway
- **Attachment Type** - VPN
- **Customer Gateway** - New
- **IP address** - This should be obtained within the SonicWall Cloud Edge Panel, under the relevant Gateway Name



- **BGP ASN**: Leave default values
- **Routing Options**: Static
- Keep the default values for the rest of the attributes
- Click on **Create transit gateway attachment**

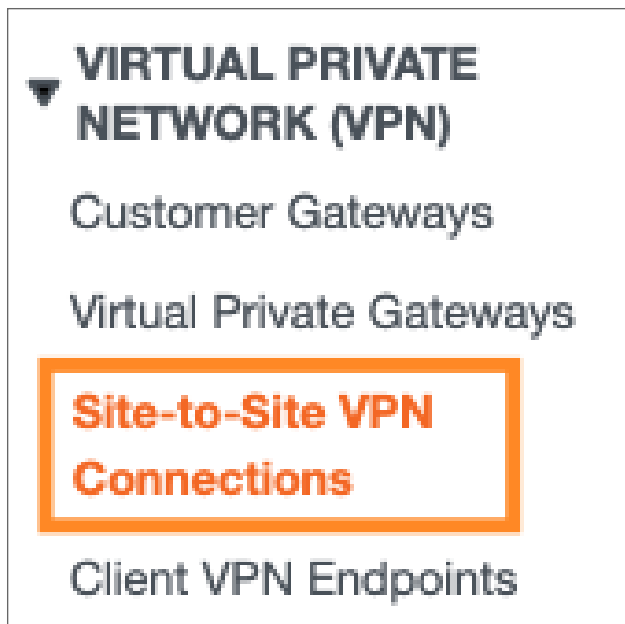
**NOTE:** This may take several minutes.

In case you have 2 VPCs, this is how your Transit gateway attachments section should look like

| Name                           | Transit gateway attachment ID | Transit gateway ID    | Resource type | Resource ID           | State     | Association route table ID |
|--------------------------------|-------------------------------|-----------------------|---------------|-----------------------|-----------|----------------------------|
| Transit Gateway VPN attachment | tgw-attach-0102463279a24c1    | tgw-0b371c180a0211f95 | VPN           | vpn-0201824e49ca5e545 | Available | rtb-rb-0d83a476a6a771c     |
| Transit Gateway VPC attachment | tgw-attach-0184718a101010101  | tgw-0b371c180a0211f95 | VPC           | vpn-0201824e49ca5e545 | Available | rtb-rb-0d83a476a6a771c     |
| Transit Gateway VPC attachment | tgw-attach-0a705110800a0005   | tgw-0b371c180a0211f95 | VPC           | vpn-0201824e49ca5e545 | Available | rtb-rb-0d83a476a6a771c     |

# Configuring the tunnel in the AWS Console

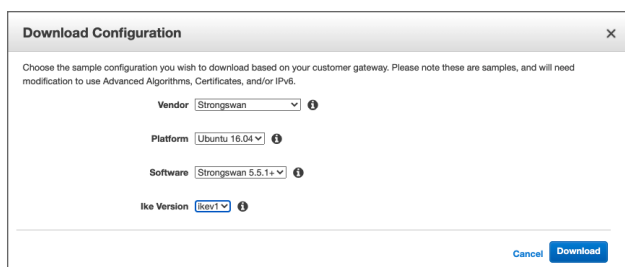
1. On the left pane, under Virtual Private Network (VPN), click on **Site-to-Site VPN Connections**



2. Pick the newly created Transit Gateway VPN connection record
3. On the top pane, click on **Download Configuration**



4. A pop-up will appear, choose the following and click on **Download**



- **Vendor** - Strongswan
  - **Platform** - Ubuntu 16.04
  - **Software** - Strongswan 5.5.1+
  - **Ike Version** - Ikev1
5. Open the configuration file that you have downloaded and copy the following attributes.

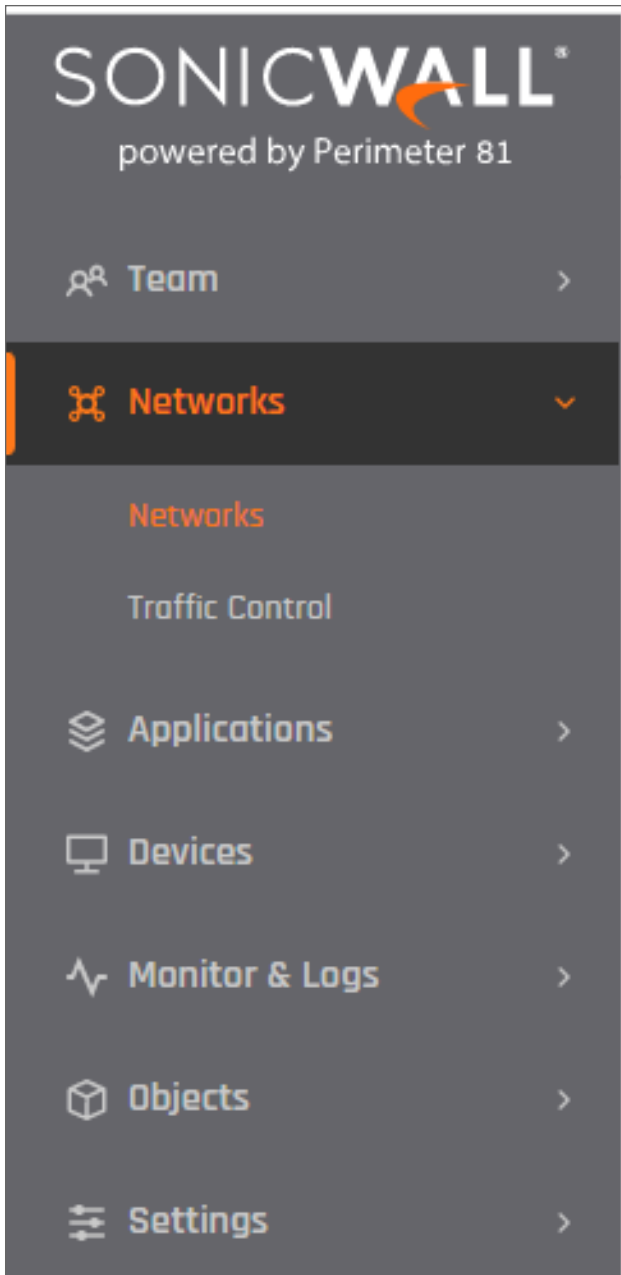
- **Endpoint** - Copy the 2nd IP (marked in red)
- **PSK** - Marked in yellow, remember to omit the quotation marks

```
4) Create a new file at /etc/ipsec.secrets if it doesn't already exist, and append this
line to the file (be mindful of the spacing!). This value authenticates the tunnel
endpoints:
185.253.69.17 18.16.10.253 : PSK "QzauwHAc0TfLR0vuKRVrdSAb0"
```

## Configuring the tunnel in the platform

1. Navigate to your SonicWall Cloud Edge web platform.
2. On the left pane, click on **Networks** and select the name of the network in which you'd like to set the tunnel.





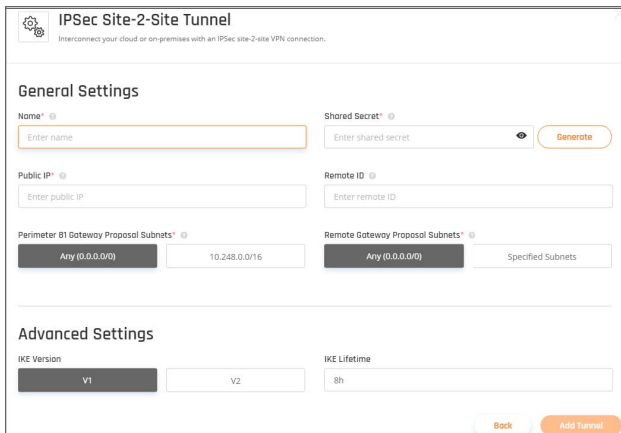
3. Locate the desired gateway, select the three-dotted menu (...), select **Add Tunnel**



4. A pop-up will appear, choose **IPSec Site-2-Site Tunnel** and click on **Continue**



5. Fill in the following information and click on **Add Tunnel**:



- **Name** - Enter the name of the tunnel
- **Shared Secret** - Paste the PSK value from the downloaded file (marked in yellow)
- **Public IP & Remote ID** - Paste the 2nd IP from the downloaded file (marked in red)

```
4) Create a new file at /etc/ipsec.secrets if it doesn't already exist, and append this line to the file (be mindful of the spacing!). This value authenticates the tunnel endpoints:
185.253.69.17 18.16.10.253 : PSK "OzquwHAc0TfLR0vuKRVrdSAb0"
```

- **SonicWall Cloud Edge Gateway Proposal Subnets**: by default, this should be set to 10.255.0.0/16.
- **Remote Gateway Proposal Subnets**: 0.0.0.0/0 or specify according to your customized settings.

6.

7. At the **Advanced Settings** section fill in the following information:

**Advanced Settings**

IKE Version: **V1** | IKE Lifetime: 8h

Tunnel Lifetime: 1h | Dead Peer Detection Delay: 10s | Dead Peer Detection Timeout: 30s

Encryption (Phase 1): aes256 | Encryption (Phase 2): aes256

Integrity (Phase 1): sha256 | Integrity (Phase 2): sha256

Diffie-Hellman Groups (Phase 1): 14 | Diffie-Hellman Groups (Phase 2): 14

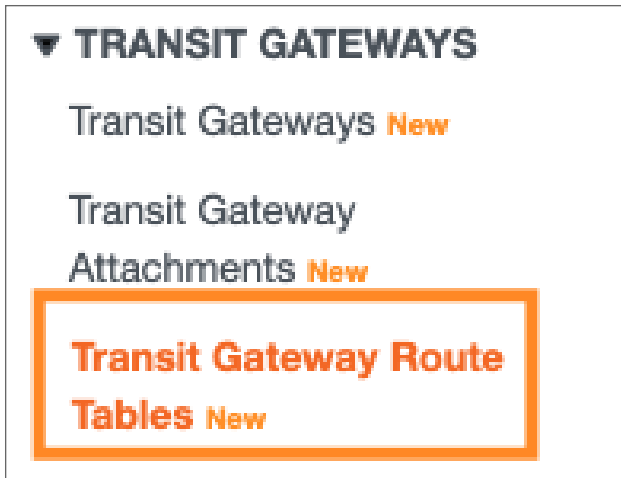
Buttons: Back, Add Tunnel

- **IKE Version:** V1
- **IKE Lifetime:** 8h
- **Tunnel Lifetime:** 1h
- **Dead Peer Detection Delay:** 10s
- **Dead Peer Detection Timeout:** 30s
- **Encryption(Phase 1):** aes128
- **Encryption(Phase 2):** aes128
- **Integrity (Phase 1):** sha1
- **Integrity (Phase 2):** sha1
- **Diffie-Hellman Groups (Phase 1):** 2
- **Diffie-Hellman Groups (Phase 2):** 2

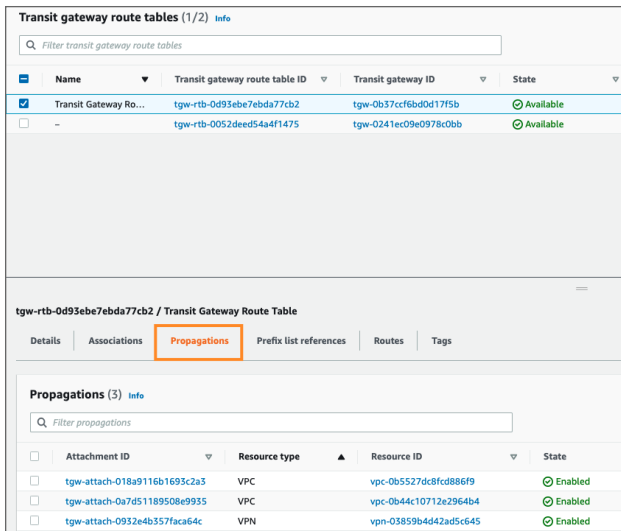
**NOTE:** This may take several minutes, you can move on to the next step.

## Configuring the routing on AWS

1. Go to the **VPC** section in the **AWS Console**. Under **Transit Gateways**, select **Transit Gateway Route Tables**.



2. Select the relevant Transit Gateway Route Table record
3. On the bottom, click on **Propagations**
4. Verify that all of the Transit Gateway Attachments are included, if you have 2 VPCs, this is how it should look like -



① **NOTE:** In case one of the Transit Gateway Attachments is missing, click on "Create propagation" and add the missing record

5. On the bottom, click on **Associations**
6. Verify that all of the Transit Gateway Attachments are included (same as step #4)
7. On the bottom, near the **Propagations** tab, click on **Routes**
8. Click on **Create static route** and fill in the following:

### Create static route Info

Add a static route to your transit gateway route table.

**Details**

Transit gateway ID  
 tgw-0053025d331338a3f

Transit gateway route table ID  
 tgw-rtb-0e4df7df428ce6a99

CIDR Info

Type Info  
 Active  
 Blackhole

Choose attachment

- **CIDR** - Insert your SonicWall Cloud Edge subnet, to find your SonicWall Cloud Edge network subnet perform the following:
  - Open your SonicWall Cloud Edge web platform
  - On the left pane click on "Networks" --> "Networks"
  - Select your network
  - Select the three-dotted menu (...) next to the Network
  - Click on "Edit Network"
- **Choose attachment** - Choose the VPN attachment

If you have 2 VPCs, this is how it should look like

**Transit gateway route tables (1/2)** [Info](#)

Filter transit gateway route tables

| Name  | Transit gateway route table ID | Transit gateway ID    |
|---|--------------------------------|-----------------------|
| <input checked="" type="checkbox"/> Transit Gateway Ro... | tgw-rtb-0d93ebe7ebda77cb2      | tgw-0b37ccf6bd0d17f5b |
| <input type="checkbox"/> -                                | tgw-rtb-0052deed54a4f1475      | tgw-0241ec09e0978c0bb |

**Filter routes by CIDR (2)**

**Exact CIDR**  
Select a valid IP4 or IPv6 CIDR.  
0.0.0.0/0, ::/0

**Longest prefix match**  
Enter a valid IP4 or IPv6 and press enter.  
0.0.0.0, ::

**Routes (3)**

Filter routes

| CIDR                                   | Attachment ID                | Resource ID                |
|--|------------------------------|----------------------------|
| <input type="checkbox"/> 10.231.0.0/16 | tgw-attach-0a7d51189508e9935 | vpc-0b44c10712e2964b4      |
| <input type="checkbox"/> 10.232.0.0/16 | tgw-attach-018a9116b1693c2a3 | vpc-0b5527dc8fcd886f9      |
| <input type="checkbox"/> 10.246.0.0/16 | tgw-attach-0932e4b357faca64c | vpn-03859b4d42ad5c645(...) |

- On the left pane, under Virtual Private Cloud, click on "Route Tables"

**VIRTUAL PRIVATE CLOUD**

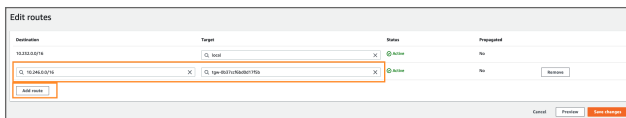
Your VPCs

Subnets

**Route Tables *New***

- Select the Route Table for one of the attached VPCs
- On the bottom, click on **Routes**

12. Click on **Edit Routes**, a new window will appear, click on **Add route** and fill in the following:



- **Destination**= Your SonicWall Cloud Edge network subnet
  - The value in the above screenshot it's just an example, to find your SonicWall Cloud Edge network subnet perform the following:
    - Open your SonicWall Cloud Edge web platform
    - On the left pane click on "Networks" --> "Networks"
    - Select your network
    - Select the three-dotted menu (...) next to the Network
    - Click on "Edit Network"



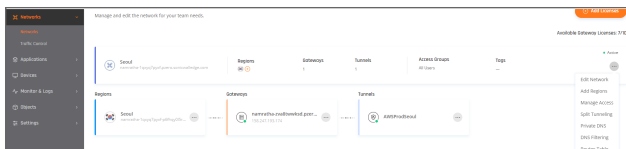
- **Target** = Choose Transit Gateway & pick the relevant Transit Gateway

13. Click on **Save changes**

14. Repeat steps 10-12 for other attached VPCs

## Configuring the routing on SonicWall Cloud Edge

1. Open your SonicWall Cloud Edge web platform
2. On the left pane click on "Networks" --> "Networks"
3. Select your network
4. Select the three-dotted menu (...) next to the Network
5. Click on **Route Table**



6. On the top right corner, click on **Add Route**
7. A pop-up will appear, fill in the following and click on **Apply Configuration**:
  - **Tunnel** - Choose the relevant tunnel
  - **Subnet** - Add the CIDRs of the attached VPCs (The VPCs to which you'd like to gain access)

# Alibaba Cloud

This article describes how to establish a Site-To-Site IPSEC VPN connection between Alibaba Cloud and SonicWall Cloud Edge Secure Access.

- Setting a tunnel on Alibaba Cloud
- Setting access rules in Alibaba security groups
- SonicWall Cloud Edge setting

Please follow the steps below:

## Setting a tunnel on Alibaba Cloud

1. Log in to the VPC console.
2. In the **Management Portal** on the left side, choose **VPN > IPsec Connections**.
3. Select a region.
4. On the **IPsec Connections** page, select **Create IPsec Connection**.
5. On the **Create IPsec Connection** page, configure the IPsec-VPN connection with the following information, and select **OK**.
  - **Name:** Enter the name of the IPsec-VPN connection.
  - **VPN Gateway:** Select the VPN Gateway to connect - If none exists, create a new one.
  - **Customer Gateway:** Select the customer gateway to connect. If none exists, create a new one for the gateway public IP.
  - **Local Network:** Enter the CIDR block of the VPC to be connected with the on-premises data center. This parameter is used for phase two negotiation.
  - **Remote Network:** Enter the CIDR block of the on-premises data center to be connected with the VPC. This parameter is used for phase two negotiation (if you didn't select a specific subnet) **default is - 10.255.0.0/16**.
  - **Effective Immediately:** Choose Yes.
  - **Advanced Configuration:** IKE Configurations.
    - **Pre-Shared Key:** Enter the pre-shared key used for the authentication between the VPN Gateway and the customer gateway. By default, it is an automatically generated value. But you can also specify a pre-shared key - this key should be used also in the connection side.
    - **Version:** IKEv1
    - **Negotiation Mode:** Main mode
    - **Encryption Algorithm:** aes256
    - **Encryption Algorithm:** sha1
    - **DH Group:** group2



- **SA Life Cycle (seconds):** Set the SA lifecycle for phase one negotiation. The default value is 86,400 seconds.
- **LocalId:** Local VPN Gateway public IP address
- **Remoteld:** Gateway public IP address

#### Advanced Configuration: IPSec Configurations

- **Encryption Algorithm:** aes256
- **Authentication Algorithm:** sha1
- **DH Group:** group2
- **SA Life Cycle (seconds):** Set the SA lifecycle for phase two negotiation. The default value is 86,400s.

#### Health Check - Optional

### Setting access rules in Alibaba security groups

1. Go to your security group that is associated with your server.
2. Add Allow rule with 10.255.0.0/16 object to the desired ports.

### Setting routes in Alibaba cloud

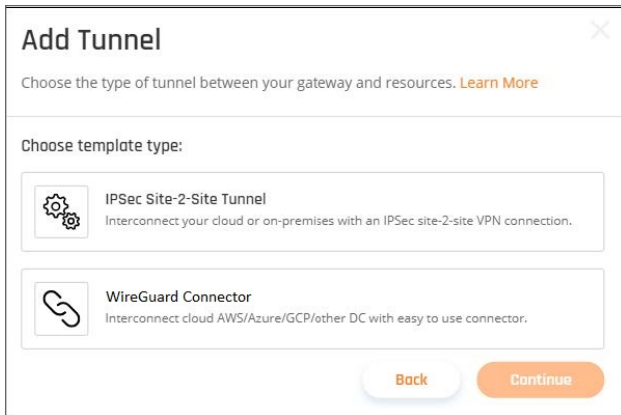
1. Go to your VPN.
2. Select **Route Tables**.
3. Add the following route under the System route table or on your custom route table: 10.255.0.0/16. The next hop should be the VPN Gateway you created for the connector.

### SonicWall Cloud Edge setting

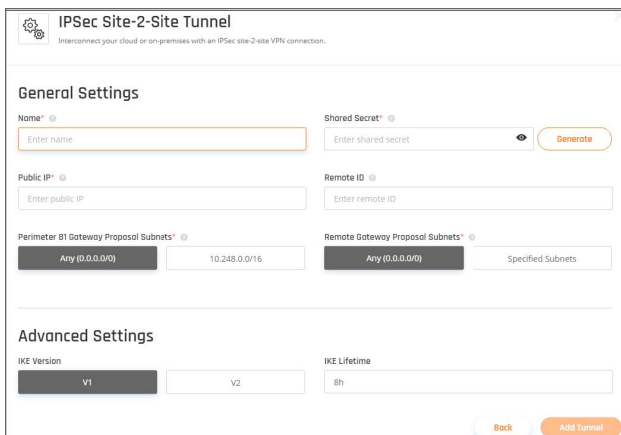
1. Go to the Gateway in your network from which you want to create the tunnel to Alibaba Cloud.
2. Select the three-dotted menu (...) and select **Add Tunnel**.



3. Select **IPSec Site-2-Site Tunnel** and select **Continue**.



4. Enter the General Settings:



**Name:** Set the name for the Tunnel.

**Shared Secret:** Put the same Shared secret you set in Alibaba Cloud.

**Public IP** and **Remote ID:** enter **AliBaba VPN Gateway** Public IP address.

In **Gateway Proposal Subnets**, select **Any** or **Specific Subnet**.

In **Remote Gateway Proposal Subnets** put your Alibaba Cloud subnet/s.

**Advanced Settings:**

1. Enter the Advanced Settings:

The screenshot shows the 'Advanced Settings' configuration page. It contains the following fields and values:

- IKE Version: V1
- IKE Lifetime: 8h
- Tunnel Lifetime: 1h
- Dead Peer Detection Delay: 10s
- Dead Peer Detection Timeout: 30s
- Encryption (Phase 1): aes256
- Encryption (Phase 2): aes256
- Integrity (Phase 1): sha256
- Integrity (Phase 2): sha256
- Diffie-Hellman Groups (Phase 1): 14
- Diffie-Hellman Groups (Phase 2): 14

Buttons: Back, Add Tunnel

- **IKE Version:** V1
- **IKE Lifetime:** 8h
- **Tunnel Lifetime:** 1h
- **Dead Peer Detection Delay:** 10s
- **Dead Peer Detection Timeout:** 30s
- **Encryption (Phase 1):** aes256
- **Encryption (Phase 2):** aes256
- **Integrity (Phase 1):** sha1
- **Integrity (Phase 2):** sha1
- **Diffie-Hellman Groups (Phase 1):** 2
- **Diffie-Hellman Groups (Phase 1):**2

3. Select **Add Tunnel**.

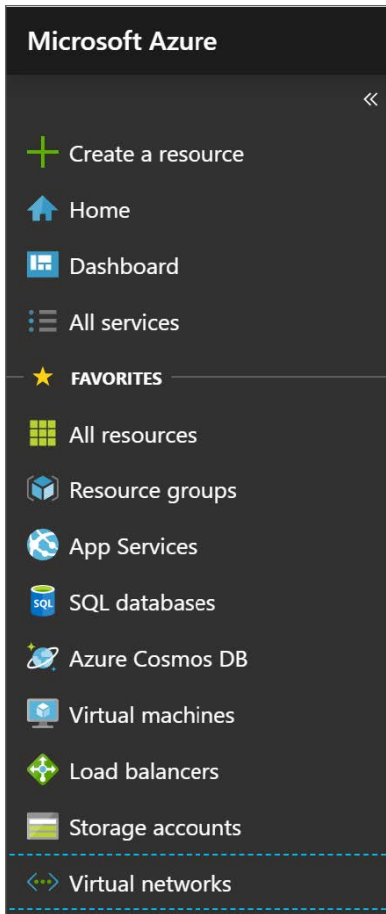
## Microsoft Azure

This article describes how to establish a Site-To-Site IPSec VPN connection between your Azure server and SonicWall Cloud Edge network. Please follow the steps below:

- [Creating a gateway subnet](#)
- [Creating a virtual network gateway](#)
- [Creating a local network gateway](#)
- [Creating the IPSEC tunnel connection](#)
- [SonicWall Cloud Edge Settings](#)
- [Verifying the VPN connection](#)

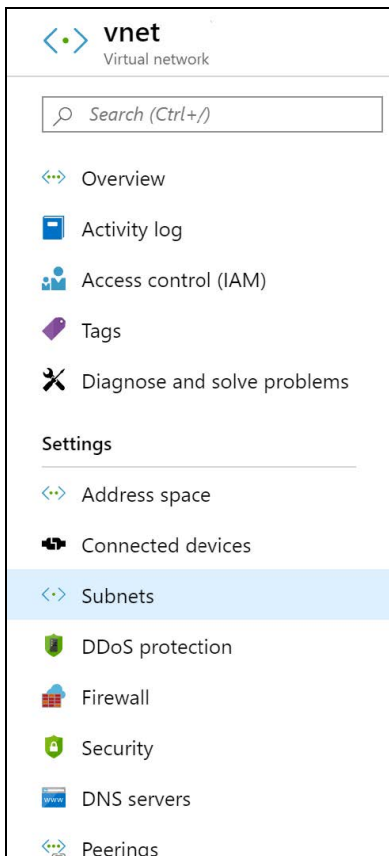
## Creating a gateway subnet

1. In your Azure Management Portal, navigate to the **Virtual networks**.

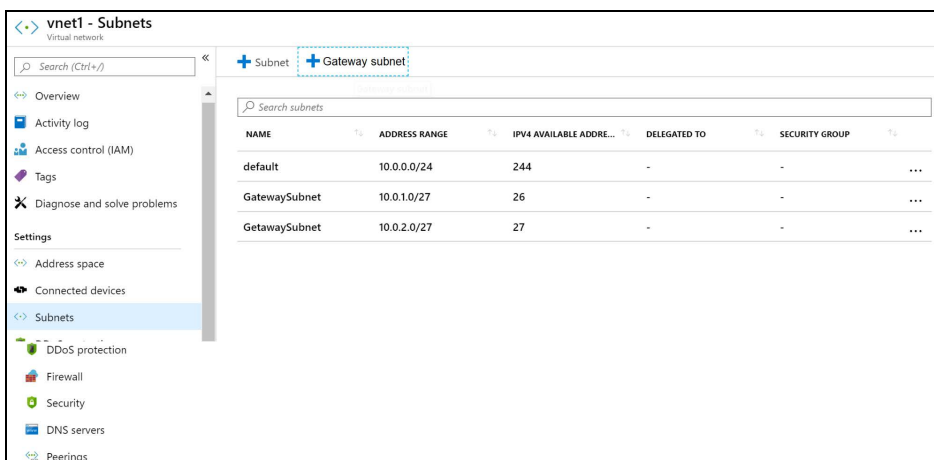


2. Select the name of the Virtual Network to which you'd like to create a gateway.

3. Under the **Settings** section of your VNet page, select **Subnets**.

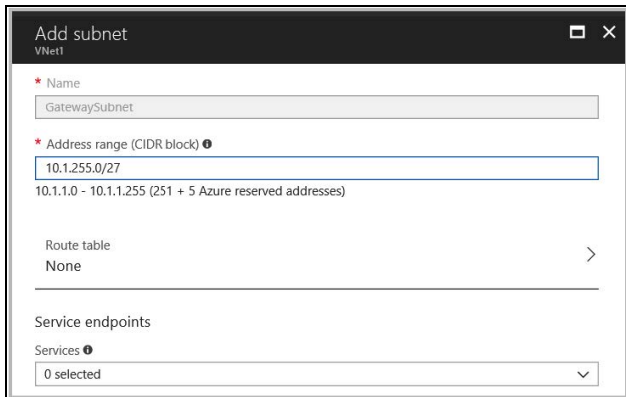


4. Select **+ Gateway subnet** (the name of the subnet is filled in with the value "Gateway subnet" by default).



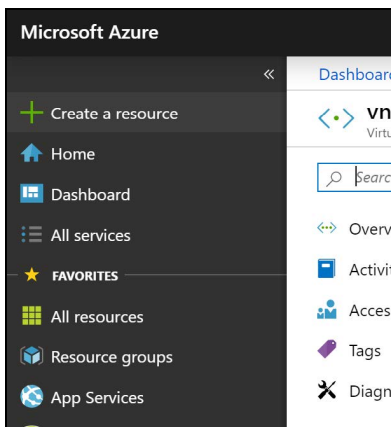
5. If needed, adjust the auto-filled Address range values to match your configuration requirements. In case this range is not automatically filled in:

- Go to address space-> +Add
- Select a random /27 bit mask subnet space (for example 10.1.255.0/27)

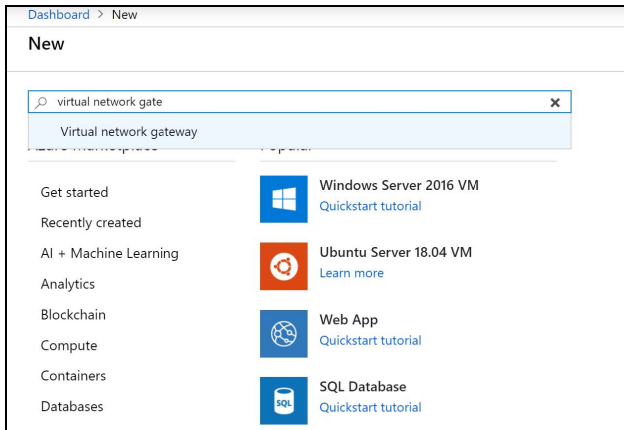


## Creating a virtual network gateway

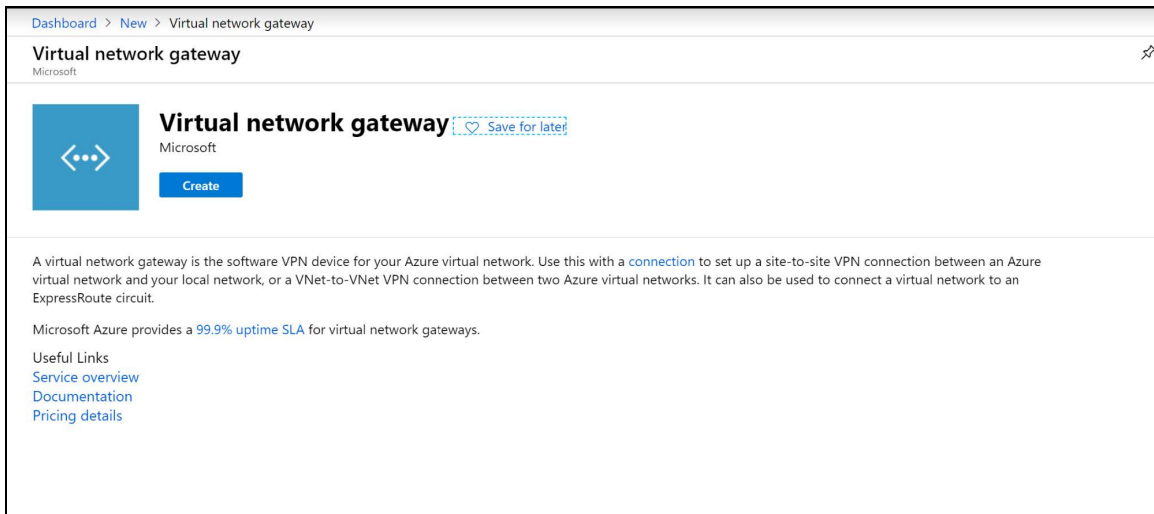
1. On the left side of the portal page, select + and type *Virtual Network Gateway* in the **Search** line.



2. Locate and select the **Virtual network gateway**.



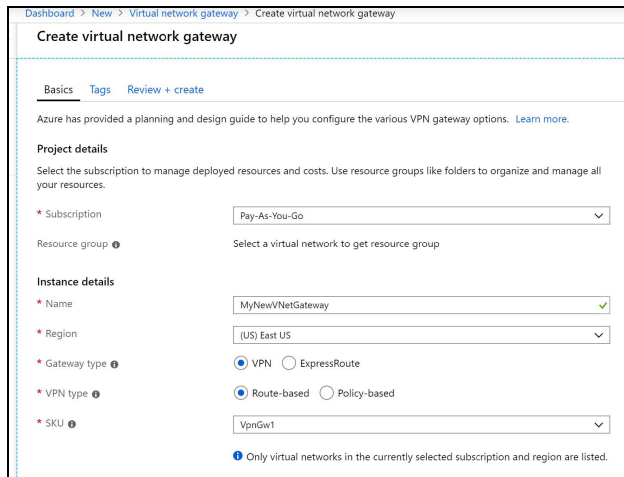
### 3. Select **Create**.



### 4. Fill in the fields with the following information:

- **Name:** Your gateway name.
- **Region/Location:** Your virtual network location/region where your resources are.
- **Gateway type:** Select **VPN**.
- **VPN type:** Select **Route-based**.


- **SKU:** Select the gateway SKU from the dropdown. The SKUs listed in the dropdown depend on the VPN you select.



- **Virtual network:** Select the Virtual network that contains the resources you want to reach via the tunnel.

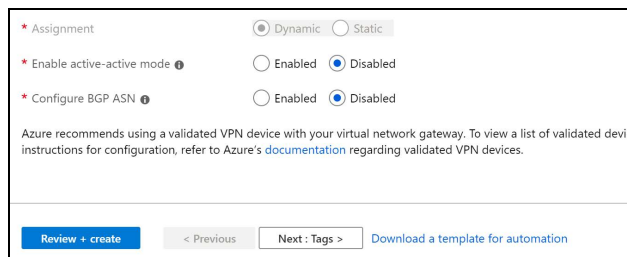
Select a **Virtual network** to open the **Choose a virtual network** page.

If you don't see your VNet, make sure the **Location/Region** field is pointing to the region in which your virtual network is located.



- **Gateway subnet address range:** You will only see this setting if you did not previously create a gateway subnet for your virtual network. If you previously created a valid gateway subnet, this field will not appear.
- **Public IP address:** This specifies the public IP address object that's associated with the VPN gateway. The public IP address is dynamically assigned to this object when the VPN gateway is created.
- **Enable active-active mode:** Disabled.
- **Configure BGP ASN:** Disabled.
- Select **Review+create** to begin creating the VPN gateway.

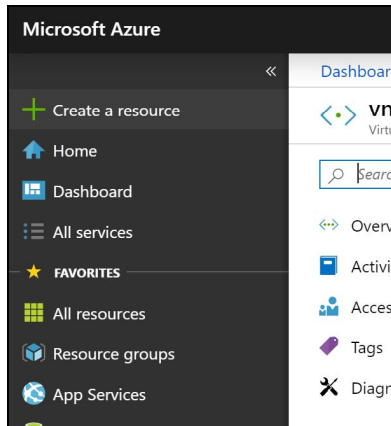
It can take up to 45 minutes for the task to be completed.



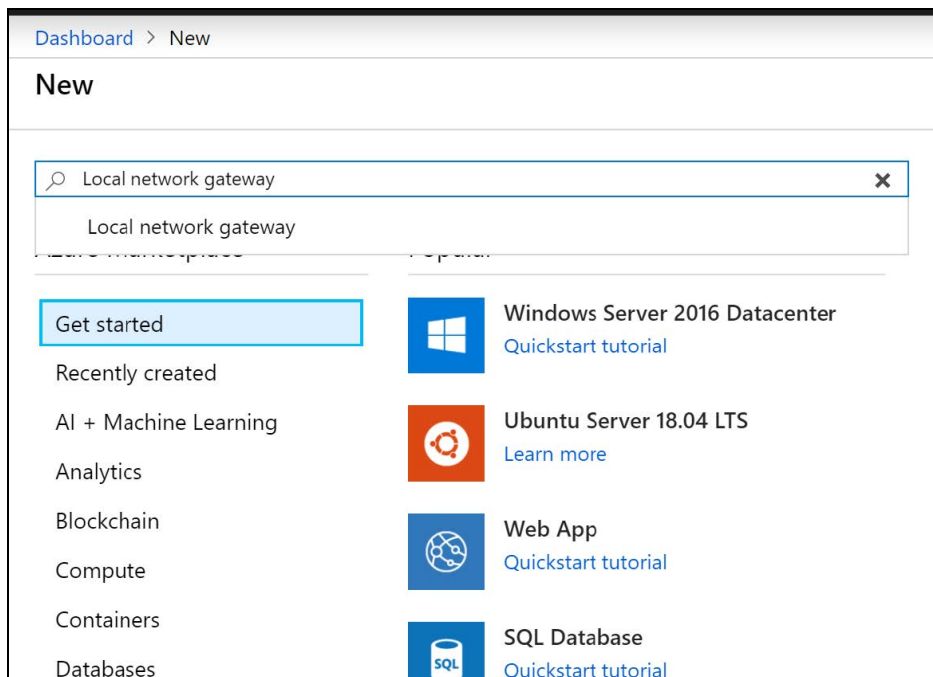


## Creating a local network gateway

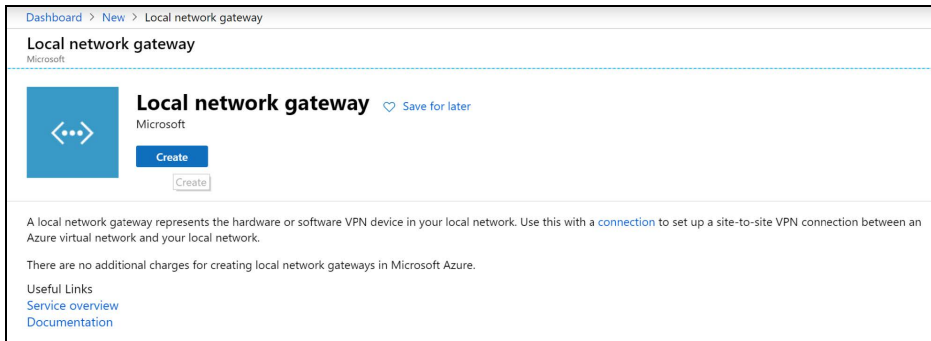
1. In the portal, select **+ Create a resource**.



2. In the search box type "Local network gateway".



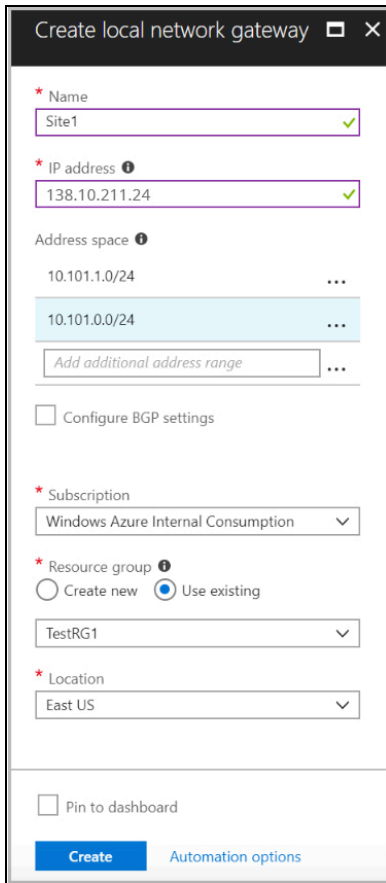
3. Select **Local network gateway**, then select **Create** to open the Create local network gateway page.



4. Fill in the fields with the following information:

- **Name** Your gateway name.
- **IP address**: This is the public IP address of the VPN device that you want Azure to connect to. Specify your SonicWall Cloud Edge gateway IP.
- **Address Space**: Insert your SonicWall Cloud Edge subnet (make sure that the ranges you specify here do not overlap with ranges of other networks that you want to connect to).
- **Subscription**: Verify that the correct subscription is showing.
- **Resource Group**: Select the resource group that you want to use. You can either create a new resource group or select one that you have already created.
- **Location**: Select a location that this object will be created in. You may want to select the location in which your Virtual Network resides, however it is not a requirement.
- **SKU**: Select the gateway SKU from the dropdown. The SKUs listed in the dropdown depend on the VPN you select.

5. Select **Create** at the bottom of the page to create the local network gateway.

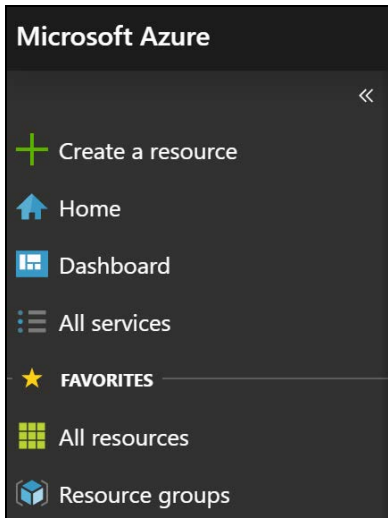


The screenshot shows a 'Create local network gateway' form with the following fields and options:

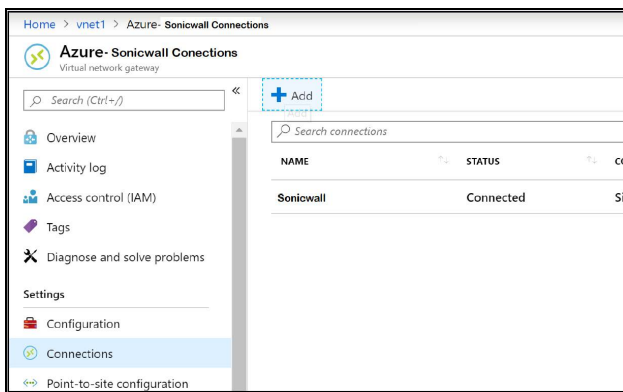
- Name:** Site1 (with a green checkmark)
- IP address:** 138.10.211.24 (with a green checkmark)
- Address space:** A list with '10.101.1.0/24' and '10.101.0.0/24' (the latter is highlighted in light blue). There is an 'Add additional address range' button below.
- Configure BGP settings:** An unchecked checkbox.
- Subscription:** Windows Azure Internal Consumption (dropdown menu)
- Resource group:** 'Create new' (unchecked) and 'Use existing' (checked) radio buttons, with 'TestRG1' selected in the dropdown below.
- Location:** East US (dropdown menu)
- Pin to dashboard:** An unchecked checkbox.
- Buttons:** A blue 'Create' button and a link for 'Automation options'.

## Creating the IPSEC tunnel connection

1. Open your virtual network gateway page.
2. On the sidebar, select **All resources**.



3. Select the **Virtual network gateway** you created. Once it opens, go to **Settings**, select **Connections**, and then **+Add**.



4. Fill in the fields with the following information:
  - **Name** Your connection name.
  - **Connection type** : Select Site-to-site (IPSec).
  - **Virtual network gateway**: Since you are connecting from this gateway this value (the IP you received from Azure) is fixed.
  - **Local network gateway**: The local network gateway (your SonicWall Cloud Edge network address) which you have just created is the fixed value.
  - **Shared Key**: The value here must match the value that you are using for your local on-premises VPN device.
  - The remaining values for **Subscription**, **Resource Group**, and **Location** are fixed as well.
  - Select **OK** to create your connection.

**Add connection**  
VNet1GW

\* Name  
VNet1toSite1 ✓

Connection type ⓘ  
Site-to-site (IPsec) ▾

\* Virtual network gateway ⓘ  
VNet1GW 🔒

\* Local network gateway ⓘ  
Site1 >

\* Shared key (PSK) ⓘ  
abc123 ✓

Subscription ⓘ  
Windows Azure Internal Consumption ▾

Resource group ⓘ  
TestRG1 🔒

Create new

Location ⓘ  
East US ▾

**OK**

## SonicWall Cloud Edge Settings

1. Open your SonicWall Cloud Edge Management Platform and go to the **Network** tab.

**SONICWALL**  
powered by Perimeter 81

SonicWall Inc. > Networks > Networks

Need Help? ⓘ AM Abhinab Mishra Admin

**Networks**

Create and edit networks that are interconnected to your environments.

Create Network Add Licenses

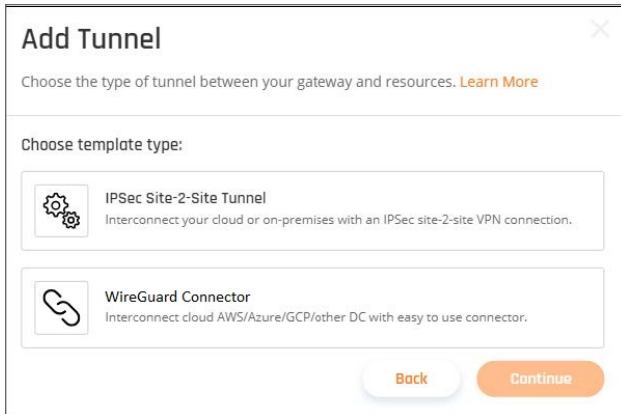
Available Gateway Licenses: 3/10

| Network  | Regions | Gateways | Tunnels | Access Groups | Tags          | Status |
|--|---------|----------|---------|---------------|---------------|--------|
| CORPOFFICEDummy<br>dev-panky1234-eeeooryv4x... | 1       | 2        | 0       | All Users     | —             | Active |
| SmallINWTest<br>dev-panky1234-h0udjanzh...     | 2       | 0        | 0       | All Users     | 192.168.0.0/8 | Active |

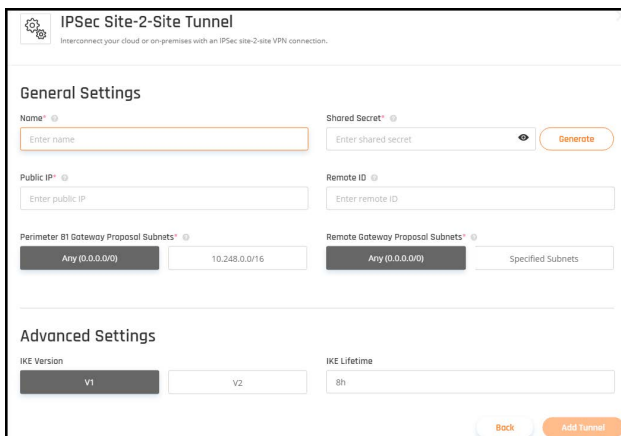
2. Go to the gateway in your network from which you want to create the tunnel to Azure, select the three-dotted menu (...) beside it, and select **Add Tunnel**.



3. Select **IPSec Site-2-Site Tunnel** and select **Continue**.



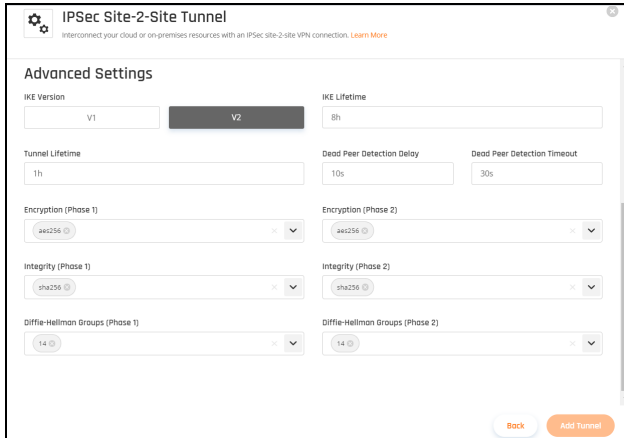
4. Fill in the fields with the following information:



- **Name:** Enter a name of your choice.
- **Shared Secret:** Enter the same Shared secret you set in the Azure Portal.
- **Public IP:** Enter the Azure **Virtual network gateway** public IP.
- **Remote ID:** Enter the Azure **Virtual network gateway** remote ID.
- **SonicWall Cloud Edge Gateway Proposal Subnets:** Choose the purposed IP range.
- **Remote Gateway Proposal Subnets:** Enter the Azure **Virtual network gateway subnet/range**.

## Advanced Settings

1. Enter the Advanced settings.



The screenshot shows the 'Advanced Settings' configuration page for an IPsec Site-2-Site Tunnel. The page is titled 'IPsec Site-2-Site Tunnel' and includes a sub-header 'Interconnect your cloud or on-premises resources with an IPsec site-2-site VPN connection. [Learn More](#)'. The settings are organized into several sections:

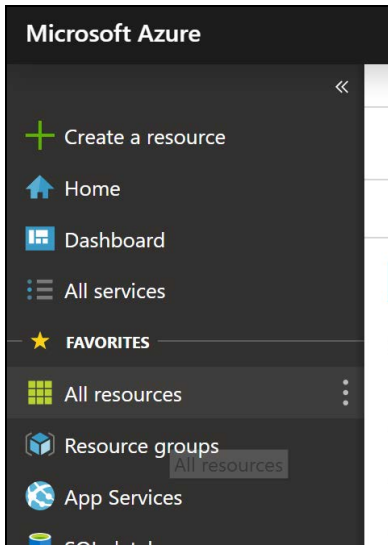
- IKE Version:** A dropdown menu with 'V1' and 'V2' options. 'V2' is selected.
- IKE Lifetime:** A text input field containing '8h'.
- Tunnel Lifetime:** A text input field containing '1h'.
- Dead Peer Detection Delay:** A text input field containing '10s'.
- Dead Peer Detection Timeout:** A text input field containing '30s'.
- Encryption (Phase 1):** A dropdown menu with 'aes256' selected.
- Encryption (Phase 2):** A dropdown menu with 'aes256' selected.
- Integrity (Phase 1):** A dropdown menu with 'sha256' selected.
- Integrity (Phase 2):** A dropdown menu with 'sha256' selected.
- Diffie-Hellman Groups (Phase 1):** A dropdown menu with '14' selected.
- Diffie-Hellman Groups (Phase 2):** A dropdown menu with '14' selected.

At the bottom of the form, there are two buttons: 'Back' and 'Add Tunnel'.

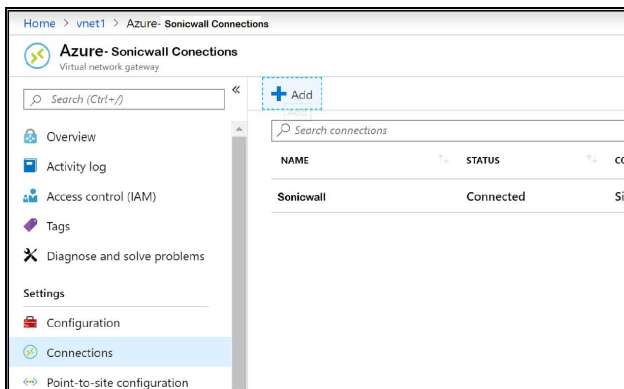
- **IKE Version:** V2
  - **IKE Lifetime:** 1h
  - **Tunnel Lifetime:** 1h
  - **Dead Peer Detection Delay:** 10s
  - **Dead Peer Detection Timeout:** 30s
  - **Encryption (Phase 1) :** aes256
  - **Encryption (Phase 2) :** aes256
  - **Integrity (Phase 1) :** sha1
  - **Integrity (Phase 2):** sha1
  - **Diffie-Hellman Groups (Phase 1):** 2
  - **Deffie-Hellman Groups (Phase 1):** 2
2. Select **Add Tunnel**.

## Verifying the VPN connection

1. Go to the Azure Portal and select **All Resources**.



2. Select the **Virtual network gateway**.
3. Go to **Connections**.

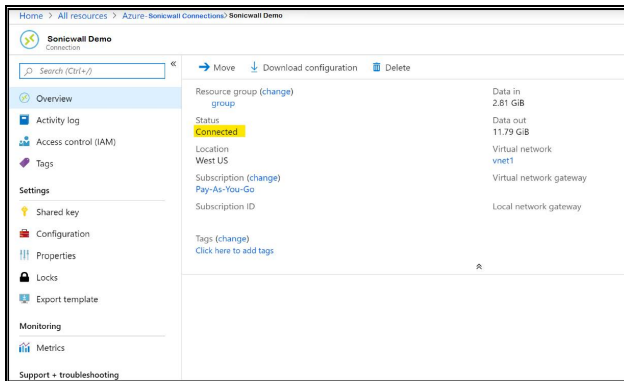


4. Select the connection you created.





5. Under the **Overview** tab, make sure that the **Status** is **Connected**.



## Google Cloud Platform

This article describes how to establish a Site-To-Site IPSEC VPN connection between Google Cloud Platform (GCP) and SonicWall Cloud Edge.

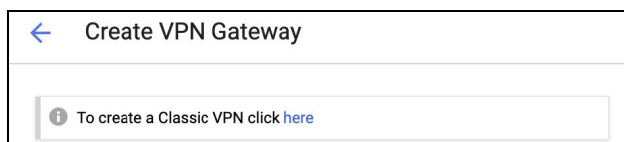
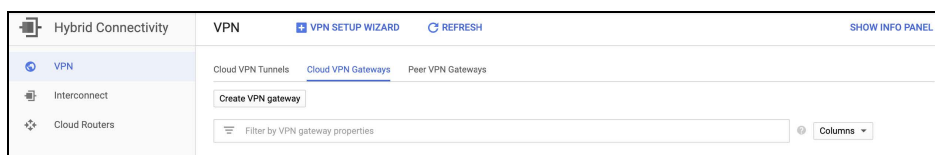
- Initial Google Cloud platform configuration
- SonicWall Cloud Edge Platform configurations
- Configuring the routing rules to the VPC network
- Allowing incoming connections from the SonicWall Cloud Edge local network using firewall rules

Please follow the steps below:

### Initial Google Cloud platform configuration

GCP includes few steps throughout the configuration and needs to be applied for every VPC.

1. **Create Virtual Private Gateway.**
  - a. Go to the **Hybrid Connectivity** in the **Google Cloud Platform Console**.
  - b. Under the left menu go to **VPN**, select **Cloud VPN Gateways**, then create **VPN Gateway**.



- c. **Select Classic VPN.**

d. Fill in the following information:

A virtual private network lets you securely connect your Google Compute Engine resources to your own private network. Google VPN uses IKEv1 or IKEv2 to establish the IPsec connectivity. [Learn more](#)

**Google Compute Engine VPN gateway** ?

**Name** ?  
Name is permanent

**Description** (Optional)

**Network** ?

**Region** ?

**IP address** ?

- **Name:** Enter a name of your choice.
- **Network:** Select default or a specific VPC.
- **Region:** Preferably the region in which your resources lie.
- **IP Address:** Create an IP address that will serve to connect your gateway.

**Reserve a new static IP address**

**Name** ?  
Name is permanent

**Description** (Optional)

[CANCEL](#) [RESERVE](#)

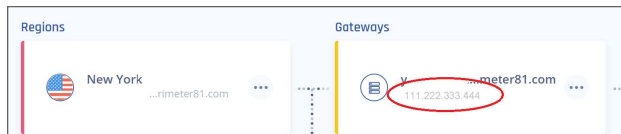
## 2. Create a Tunnel

- a. Scroll to the lower part of the page. Fill in the following information:

The screenshot shows the 'Create a VPN connection' form. The left sidebar has 'VPN' selected. The main area has a 'New item' header and the following fields:

- Name:** A text input field containing 'vpn-1-tunnel-1'.
- Description (Optional):** An empty text area.
- Remote peer IP address:** A text input field with an example '192.0.2.1'.
- IKE version:** A dropdown menu set to 'IKEv2'.

- **Name:** Enter a name of your choice.
- **Remote peer IP address:** Enter your SonicWall Cloud Edge Gateway IP (to obtain this, open the SonicWall Cloud Edge Platform, and under Network select the network that contains the gateway to which you'd like to create a tunnel).



- **IKE Version:** IKEv2

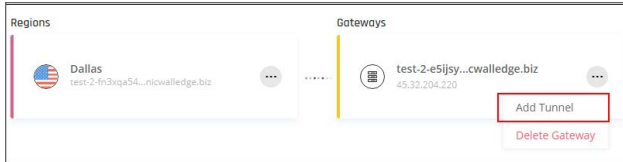
The screenshot shows the 'IKE pre-shared key' dialog box. It contains the following elements:

- IKE pre-shared key:** A text input field and a 'Generate and copy' button.
- Warning:** A yellow warning icon and text: 'Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)'
- Routing options:** Three tabs: 'Dynamic (BGP)', 'Route-based' (selected), and 'Policy-based'.
- Remote network IP ranges:** A text input field with the example '192.168.0.0/24 10.16.0.0/12'.
- Buttons:** 'Done' and 'Cancel' buttons at the bottom.

- **IKE pre-shared key:** Select **Generate and copy** or choose a key of your own and write it down.
- **Routing options:** Route-based
- **Remote network IP ranges:** 10.255.0.0/16 (unless customized)
- Select **Done**, then **Create**.

## SonicWall Cloud Edge Platform configurations

1. Enter the SonicWall Cloud Edge Management Platform. Under the **Networks** tab in the left menu, select the name of the network in which you'd like to set the tunnel.
2. Locate the desired gateway, select the three-dotted menu (...), select **Add Tunnel**, and then **IPSec Site-2-Site Tunnel**.



3. Fill in the following information:

- **Name:** Enter a name of your choice.
- **Shared Secret:** Enter the same IKE pre-shared key you inserted or generated in the Google Cloud Console.
- **Public IP:** Enter the VPN Gateway IP from the Google Cloud Console.
- **Remote Gateway Proposal Subnets:** Select Specified Subnets. Copy the subnets of the regions where your resources are installed. This can be queried in the Google Cloud Console here:

| VPC networks |             |         |      |                   |            |                |                        |           |
|--------------|-------------|---------|------|-------------------|------------|----------------|------------------------|-----------|
| Name ^       | Region      | Subnets | Mode | IP address ranges | Gateways   | Firewall Rules | Global dynamic routing | Flow logs |
| default      |             | 21      | Auto |                   |            | 7              | Off                    |           |
|              | us-central1 | default |      | 10.128.0.0/20     | 10.128.0.1 |                |                        | Off       |

4. Fill in the **Advanced Settings**:

**IPsec Site-2-Site Tunnel**  
Interconnect your cloud or on-premises resources with an IPsec site-2-site VPN connection. [Learn More](#)

**Advanced Settings**

IKE Version: V1 | **V2** | IKE Lifetime: 8h

Tunnel Lifetime: 1h | Dead Peer Detection Delay: 10s | Dead Peer Detection Timeout: 30s

Encryption (Phase 1): aes256 | Encryption (Phase 2): aes256

Integrity (Phase 1): sha256 | Integrity (Phase 2): sha256

Diffie-Hellman Groups (Phase 1): 14 | Diffie-Hellman Groups (Phase 2): 14

[Back](#) [Add Tunnel](#)

- **IKE Version: V2**
- **IKE Lifetime: 8h**
- **Tunnel Lifetime: 1h**
- **Dead Peer Detection Delay: 10s**
- **Dead Peer Detection Timeout: 30s**
- **Encryption(Phase 1): aes256**
- **Encryption(Phase 2): aes256**
- **Integrity (Phase 1): sha1**
- **Integrity (Phase 2): sha1**
- **Diffie-Hellman Groups (Phase 1): 2**
- **Diffie-Hellman Groups (Phase 2): 2**

## Configuring the routing rules to the VPC network

1. Go to the **VPC Network** in the **Google Cloud Platform Console**. Under the left menu go to **Routes**.



2. Select **Create Route Rule** and fill in the following information:

The screenshot shows a form for creating a route rule. It contains the following fields and options:

- Name \***: A text input field with a help icon. Below it, the text "Lowercase letters, numbers, hyphens allowed" is displayed.
- Description**: A text input field with a help icon.
- Network \***: A dropdown menu with "default" selected and a help icon.
- Destination IP range \***: A text input field with a help icon. Below it, the text "E.g. 10.0.0.0/16" is displayed.
- Priority \***: A text input field with "1000" entered and a help icon. Below it, the text "Priority should be a positive integer (lower values take precedence)" is displayed.
- Instance tags**: A text input field with a help icon.
- Next hop**: A dropdown menu with "Specify VPN tunnel" selected and a help icon.

- **Name:** The name of the VPN gateway.
- **Network:** The VPC network containing the instances that the VPN gateway will serve (should be the same network as selected in the previous steps).
- **Destination Network IP range:** Specify **10.255.0.0/16** (or customized)
- **Priority:** 1000
- **Next hop:** Select **Specify VPN Tunnel**.
- **Next hop VPN tunnel:** Select the VPN tunnel you created in the previous steps.
- Select **Create**.

## Allowing incoming connections from the local network using firewall rules

1. Go to the **VPC Network** in the **Google Cloud Platform Console**.
2. Under the left menu go to **Firewall Rules**.



3. Select **Create Firewall Rule** and fill in the following information:

**Name** <sup>?</sup>  
Name is permanent

**Description** (Optional)

**Logs**  
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. [Learn more](#)  
 On  
 Off

**Network** <sup>?</sup>

**Priority** <sup>?</sup>  
Priority can be 0 - 65535 [Check priority of other firewall rules](#)

**Direction of traffic** <sup>?</sup>  
 Ingress  
 Egress

- **Name:** Enter a name of your choice.
- **Logs:** Off
- **Network:** The VPC network containing the instances the VPN gateway will serve (should be the same network as selected in the previous steps).
- **Priority:** 1000
- The direction of traffic should be **Ingress**.

**Action on match** <sup>?</sup>  
 Allow  
 Deny

**Targets** <sup>?</sup>

**Target tags**

**Source filter** <sup>?</sup>

**Source IP ranges** <sup>?</sup>

**Second source filter** <sup>?</sup>

**Protocols and ports** <sup>?</sup>  
 Allow all  
 Specified protocols and ports

- **Action on match:** allow
- **Target tags:** optional

- **Source filter:** IP Ranges
- **Source IP ranges:** 10.255.0.0/16 (unless customized)
- **Second source filter:** none
- **Allowed protocols or ports:** all

## Heroku Enterprise

This article describes how you can configure a connection from your Heroku Private Services to SonicWall Cloud Edge using IPSec. This lets you connect to hosts on your private networks and vice versa. Connections are established over the public internet, but all traffic is encrypted using IPSec.

### Setting up the VPN connection

After you obtain your private SonicWall Cloud Edge gateway, set up a VPN gateway for the Private Space with the following command:

```
* Shell

Copy ```
heroku spaces:vpn:connect \
  --name Network \ --ip PUBLIC_IP_OF_YOUR_VPN_GATEWAY \ --cidrs '10.255.248.0/21'
\ --space SPACE
```

Setting up the gateway takes a few minutes. Use the Wait command to wait for the gateway to be ready:

```
* Shell

Copy ```
heroku spaces :vpn :wait --space SPACE network
```

When the gateway is ready, get the configuration with:

```
* Shell

Copy ```
heroku spaces :vpn :info --space SPACE network
```

This returns a table containing all the details you need to configure SonicWall Cloud Edge. Here is an example response:

```
* Text

Copy ```
heroku spaces:vpn:info --space SPACE network
=== SPACE VPNs
VPN Tunnel  Customer Gateway  VPN Gateway  Pre-shared Key  Routable Subnets  IKE Version
-----
```



```
Tunnel 1 52.91.173.226 34.203.187.158 abcdef12345 10.0.0.0 /16 1 Tunnel 2 52.91.173.226  
34.227.70.143 123456abcdef 10.0.0.0 /16 1
```

Please contact us to coordinate and share the configuration above securely.

## IBM Cloud

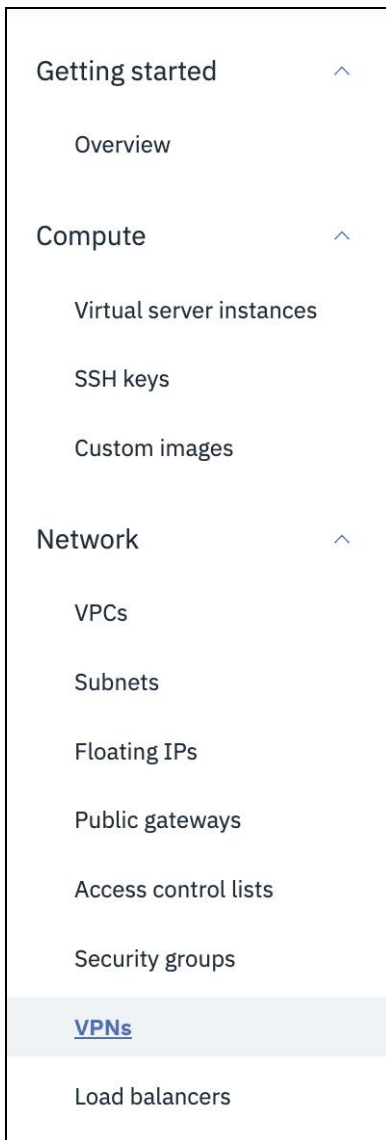
This article describes how to establish a Site-To-Site IPSec VPN connection between your IBM server and the SonicWall Cloud Edge network.

- Configuring a VPN gateway at the IBM Cloud Console
- Making sure the tunnel is up

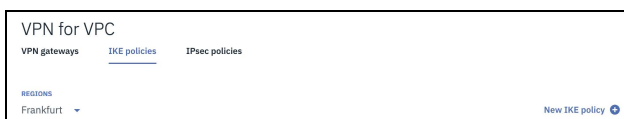
Please follow the steps below:

## Configuring a VPN gateway at the IBM Cloud Console

1. Open to the **VPC** section in the **IBM Cloud Console**. Go to **VPNs** (under the **Network** tab).



2. Open the **IKE Policies** tab, then select **New IKE Policy**.



3. Choose a **Name**, the **Region** in which the appropriate VPC lies, define the **Resource group**, then select **Create IKE policy**.

New IKE policy

Name: sonicwall-ike

Resource group: Default

View all resource groups

Region:

- Dallas
- Frankfurt (selected)
- London
- Sydney
- Tokyo

API </> Cancel Create IKE policy

4. Once the policy has been created, select the three-dotted menu (...) and select **Edit**.
5. Fill in the following information:
  - **IKE Version:** 1
  - **DH Group:** 2
  - **Authentication:** sha256
  - **Key Lifetime:** 28800
  - **Encryption:** aes256
6. Select **Save IKE policy**.
7. Open the **IPSecPolicies** tab, then select **New IPSec Policy**.
8. Choose an indicative **Name**, the **Region** in which the appropriate VPC lies and define the **Resource group**, then select **Create IPSec policy**.

New IPsec policy

Name: Sonicwall-phase2

Resource group: Default

View all resource groups

Region:

- Dallas
- Frankfurt (selected)
- London
- Sydney
- Tokyo

API </> Cancel Create IPsec policy

9. Once the policy has been created, select the three-dotted menu (...) and select **Edit**.

10. Fill in the following information:

- **Check:** PFS
- **DH Group:** 2
- **Authentication:** sha256
- **Key Lifetime:** 3600
- **Encryption:** aes256

11. Select **Save IPsec policy**.

The screenshot shows a dialog box titled "Update IPsec policy". It contains the following fields and options:

- Name:** Sonicwall-phase2
- Resource group:** Default
- Region:** Frankfurt
- Authentication:** sha256
- Encryption:** aes256
- PFS:**  PFS
- DH Group:** 2
- Key Lifetime:** 3600

At the bottom of the dialog, there are three buttons: "API </>", "Cancel", and "Save IPsec policy".

12. Open the **VPN gateways** tab, then select **New VPN gateway**.

13. Fill in the following information:

- **Name:** Enter a name of your choice
- **Virtual private cloud:** Choose the desired cloud
- **Resource group:** Choose the resource group

- **Subnet:** Choose the appropriate subnet

**New VPN gateway for VPC**

**Name**  
ipsec-tst

**Virtual private cloud**  
jonathan-test-vpc

**Resource group**  
The resource group can't be changed after the VPN gateway is created. [Learn about resource groups](#)  
Default

[View all resource groups](#)

**Subnet**  
subnet-a-jonathan

14. Check **New VPN Connection for VPC**.

15. Fill in the following information:

- **Connection name:** Set a name
- **Peer gateway address:** Insert your SonicWall Cloud Edge gateway IP
- **Preshared key:** Insert an 8 character (at least) string containing upper-case letters, upper-case letters, and numbers
- **Local subnet:** Specify one or more subnets in the VPC you want to connect
- **Peer subnet:** Unless you have custom configurations or multiple tunnels to the same gateway insert 10.255.0.0/16

**New VPN connection for VPC**

**Connection name**  
Sonicwall-test

**Peer gateway address**  
Enter IP address

**Preshared key**  
\*\*\*\*\*

**Local subnets**  
Subnets must be in CIDR notation (ex 192.168.0.0/24), cannot be duplicates, and must be separated by commas.  
Ex: 192.168.0.0/24

**Peer subnets**  
Subnets must be in CIDR notation (ex 192.168.0.0/24), cannot be duplicates, and must be separated by commas.  
Ex: 192.168.0.0/24

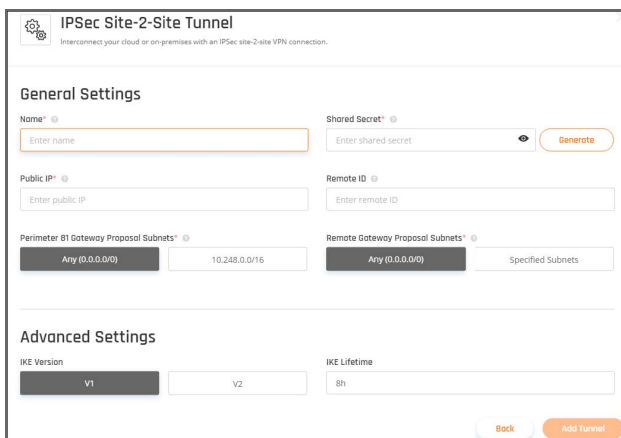
- **Dead peer detection action:** Restart
- **Interval:** 10 seconds
- **Timeout:** 30 seconds
- **IKE policy:** Choose the policy that was earlier
- **IPSec policy:** Choose the policy that was earlier

## Configuring the tunnel in the Management Platform

1. Enter the SonicWall Cloud Edge Management Platform. Under the **Networks** tab in the left menu, select the name of the network in which you'd like to set the tunnel.
2. Locate the desired gateway, select the three-dotted menu (...), select **Add Tunnel**, and then **IPSec Site-2-Site Tunnel**.



3. Fill in the General Settings:

A screenshot of the 'IPSec Site-2-Site Tunnel' configuration page. The page title is 'IPSec Site-2-Site Tunnel' with a subtitle 'Interconnect your cloud or on-premises with an IPSec site-2-site VPN connection.' The 'General Settings' section includes: 'Name' (text input), 'Shared Secret' (text input with a 'Generate' button), 'Public IP' (text input), 'Remote ID' (text input), 'Perimeter B1 Gateway Proposal Subnets' (checkbox with 'Any (0.0.0.0/0)' and '10.248.0.0/16' options), and 'Remote Gateway Proposal Subnets' (checkbox with 'Any (0.0.0.0/0)' and 'Specified Subnets' options). The 'Advanced Settings' section includes: 'IKE Version' (radio buttons for 'V1' and 'V2') and 'IKE Lifetime' (text input with '8h'). At the bottom right are 'Back' and 'Add Tunnel' buttons.

- **Name:** Specify a name
  - **Public IP:** Insert the IP of the VPN Gateway you have just defined
  - **Remote ID:** Identical to Remote IP
  - **Shared Secret:** Insert the same preshared key you chose before
  - **SonicWall Cloud Edge Gateway Proposal Subnets:** 10.255.0.0/16 or according to what you defined in the IBM Cloud portal
  - **Remote Gateway Proposal Subnets:** Specify one or more subnets in the VPC you want to connect
4. Fill in the Advanced Settings:

- **IKE Version: 1**
- **IKE Lifetime: 8h**
- **Tunnel Lifetime: 1h**
- **Dead Peer Detection Delay: 10s**
- **Dead Peer Detection Timeout: 30s**
- **Encryption (Phase 1): aes256**
- **Encryption (Phase 2): aes256**
- **Integrity (Phase 1): sha256**
- **Integrity (Phase 2): sha256**
- **Diffie-Hellman Groups (Phase 1): 2**
- **Diffie-Hellman Groups (Phase 2): 2**

## Making sure the tunnel is up

1. Under the **VPN gateways** tab select the name of the VPN Gateway that is associated with the tunnel.

| Status | Name                  | Resource Group | Gateway IP     | Location    |
|--------|-----------------------|----------------|----------------|-------------|
| Active | Sonicwall VPN Gateway | Default        | 158.177.189.83 | Frankfurt 1 |

2. Scroll down and select **View all connections**.
3. You'll be able to see the status of the tunnel. If for some reason the tunnel is down please make sure you configured all the fields according to this article. At any point, [our support team](#) will be happy to assist or troubleshoot.

| Status | Name                 | Peer Address   | IKE Policy    | IPsec Policy     | State   |
|--------|----------------------|----------------|---------------|------------------|---------|
| Active | Sonicwall-ibm-tunnel | 185.253.69.162 | Sonicwall-ike | Sonicwall-phase2 | Enabled |

# Docker

Docker enables more efficient use of system resources, application portability and shines for microservices architecture. This article helps in setting up WireGuard tunnel using a docker container. The WireGuard tunnel over docker container is able to support any system capable of running Docker.

Basic docker container for WireGuard can run its own container. We download our Cloud Edge peer configuration file for WireGuard and mount it on a shared folder to its location on the docker host in order to share it with the docker container. This will bring the connectivity of docker containers to Cloud Edge and we can securely access resources of docker container via Cloud Edge.

1. Install **docker** docker on your OS.
2. Create a barebones config YAML file for your docker container, "docker-compose.yaml", as per OS type and copy to the location mentioned in the script "Volumes" below:

## Linux Version

```
---
version: "2.1"
services:
  wireguard:
    image: ghcr.io/linuxserver/wireguard
    container_name: wireguard
    cap_add:
      - NET_ADMIN
      - SYS_MODULE
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=America/New_York
    volumes:
      - /var/tmp/config:/config
      - /lib/modules:/lib/modules
    ports:
      - 8000:8000/udp
    sysctls:
      - net.ipv4.conf.all.src_valid_mark=1
    restart: unless-stopped
```

① **NOTE:** You can change the Time Zone as per your docker container. By default this script will set to America / New York. Similarly you can set the volumes as per the location of this YAML config on your OS.

## Windows Version

```
---
version: "2.1"
services:
```



```
wireguard:
  image: ghcr.io/linuxserver/wireguard
  container_name: wireguard
  cap_add:
    - NET_ADMIN
    - SYS_MODULE
  environment:
    - PUID=1000
    - PGID=1000
    - TZ=America/New_York
  volumes:
    - C://wgConfig:/config
    - /lib/modules:/lib/modules
  ports:
    - 8000:8000/udp
  sysctls:
    - net.ipv4.conf.all.src_valid_mark=1
  restart: unless-stopped
```

3. Create a "wg0.conf" file using the Cloud Edge peer wireguard and copy the file as per the location mentioned in the volumes above.
4. Login to Cloud Edge as admin and configure WireGuard connector to the desired network.

## WireGuard Connector

Interconnect AWS/Azure/GCP/other DC with easy to use connector. [Learn More](#)

Requirements — 2 Configuration — Confirm

Name\* ?  
DockerTest

Endpoint\* ?  
115.114.16.13/

Subnets\* ?  
1/2.0.0.0/16 ? Enter the subnets

Back Next

5. Copy the URL in the configuration tab of the WireGuard connector on Cloud Edge.

## DockerTest ✕

**Note:**  
To use this option, you must set up **Ubuntu 20**, **Ubuntu 16.04 LTS**, **Ubuntu 18.04 LTS**, or **CentOS 7** instance in your local network or VPC.

Execute the following command using root user:

```
curl -s  
https://api.sonicwalledge.biz/api/networks/aZpXHYXrBm/tunnels/Y3EsML8iwb/wir  
eguard-  
config/Yzc0YjM3MDJlY2NlNzQwNDg5OTkxM2Q2Mjg2NDkzOTJjM2Q3MTUw  
ODg0ZDg5Mjlk | sudo bash
```

[Copy Command](#)

[OK](#)

① **NOTE:** Don't copy the command from this article as each tunnel will have a different URL and configuration file.

6. Paste the URL into a web browser and download the config file.
7. Open the config and copy the Interface information as highlighted in the screen shot below. Next copy and paste the code to the "wg0.conf" file.

```

Yzc0YjM3MDJiY2NiZnZQwNDg5OTkxM2Q2Mjg2NDkzOTJhM2Q3MTUwODg0ZDg5Mjlk (2) - Notepad
File Edit Format View Help
fi
$ pm postcommand >> $ _log
if [ $? -ne 0 ]; then
    $_pm_clean $_wg_packages >> $_log
    _stop_waite
    echo "ERROR: Cannot finish post installation tasks"
    return 1
fi
_stop_waite
echo " > Repository configured"
echo " > Successfully installed wireguard"
return 0
}
_configure_wireguard(){
    mkdir -p "${_wg_config_path}"
    cat > ${_wg_config_path}/${CONFIG_ifname}.conf << EOF
[Interface]
ListenPort = ${CONFIG_port}
PrivateKey = ${CONFIG_privateKey}
Address = ${CONFIG_address}
[Peer]
PublicKey = ${CONFIG_pubKey}
AllowedIPs = ${CONFIG_allowedIP}
PersistentKeepalive = 10
Endpoint = ${CONFIG_endpoint}
EOF
}
_stop_wireguard(){
    $_service status wg-quick@${CONFIG_ifname} >> $_log || return 0
    $_service stop wg-quick@${CONFIG_ifname} >> $_log || return 1
}
_start_and_enable_wireguard(){
    $_service enable wg-quick@${CONFIG_ifname} >> $_log
    $_service start wg-quick@${CONFIG_ifname} >> $_log || return 1
    return 0
}
_check_if_wireguard_is_up(){
    $_service status wg-quick@${CONFIG_ifname} >> $_log || return 1
    return 0
}

```

- Copy the Cloud Edge peer for wireguard, "CONFIG\_" from the config file. See the screen shot below of the config file and fill the details to the "wg0.conf" file.

```

Yzc0YjM3MDJiY2NiZnZQwNDg5OTkxM2Q2Mjg2NDkzOTJhM2Q3MTUwODg0ZDg5Mjlk (2) - Notepad
File Edit Format View Help
#!/bin/sh
exec 2>/tmp/p81-wg-connector.debug
set -x
CONFIG_pubKey="LX+qCkWP161zLX8K5TZm/8+Ijp0Mh3TvZ/vCkmYweg="
CONFIG_privateKey="yNA0veYfV5uLVzyi4Y1VR~0IdQA0LS18UCuMwabg86I="
CONFIG_endpoint="137.220.42.80:8000"
CONFIG_address="172.31.7.3/24" # IP address of the tunnel interface
CONFIG_allowedIP="172.31.0.0/16" # separated with whitespace
CONFIG_ifname="wg0"
CONFIG_port="8000"
CONFIG_p81subnet="172.31.0.0/16" # subnet as used at p81 GW
CONFIG_supportEmail="https://www.sonicwall.com/support/" # subnet as used at p81 GW

```

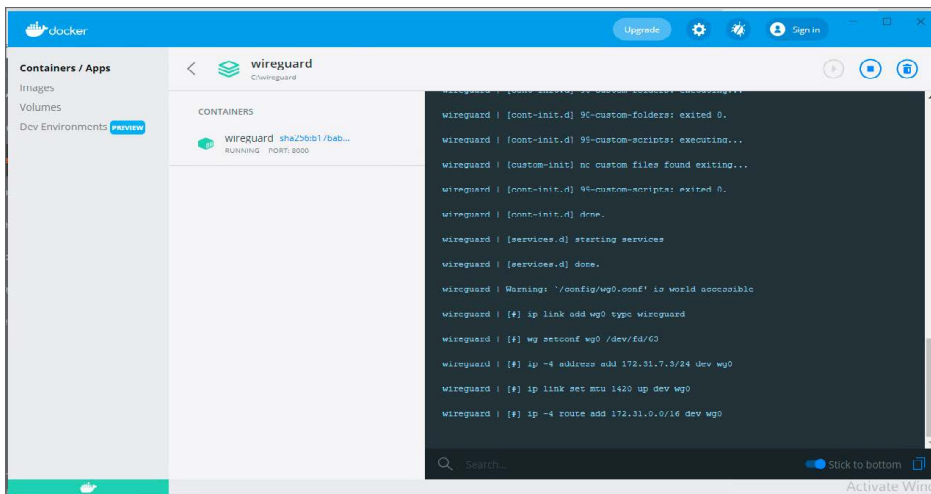
- Fill all data to the "wg0.conf" file as shown in the screenshot below.

```
wg0.conf - Notepad
File Edit Format View Help
[[Interface]
ListenPort = 8000
PrivateKey = yNA0veYfV5uLVzyi4Y1VRr0JdQA0LS18UCuMwAbg86I=
Address = 172.31.7.3/24
[Peer]
PublicKey = LX+qCkWP161zZLX8K5TZm/8+NpOMh3TvZ/vCkmYwewg=
AllowedIPs = 172.31.0.0/16
PersistentKeepalive = 10
Endpoint = 137.220.42.80:8000
```

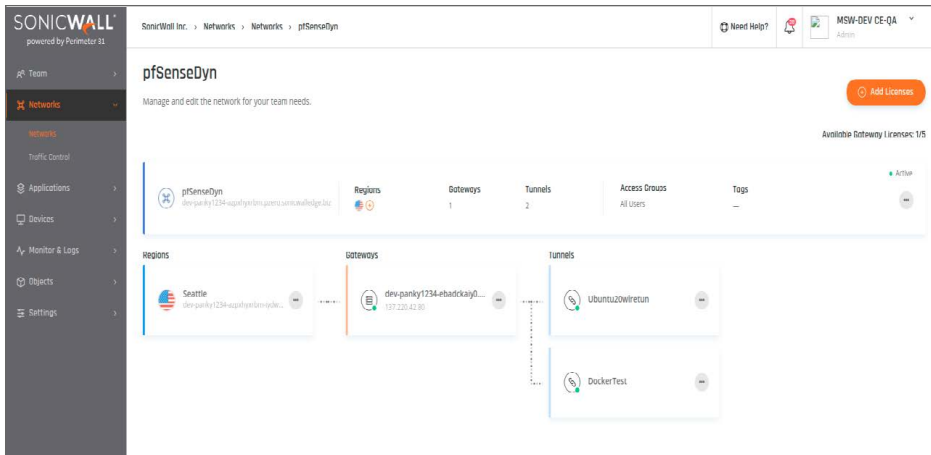
10. Run the following command from command prompt or terminal as admin. Make sure to run this from the directory where “**dockercompose.yaml**” is saved.

```
Select Administrator: Windows PowerShell
PS C:\wireguard>
PS C:\wireguard>
PS C:\wireguard> docker-compose up -d
- Network wireguard_default Created 0.6s
- Container wireguard Started 2.3s
PS C:\wireguard>
```

11. The docker container is up and running with the wireguard configuration.

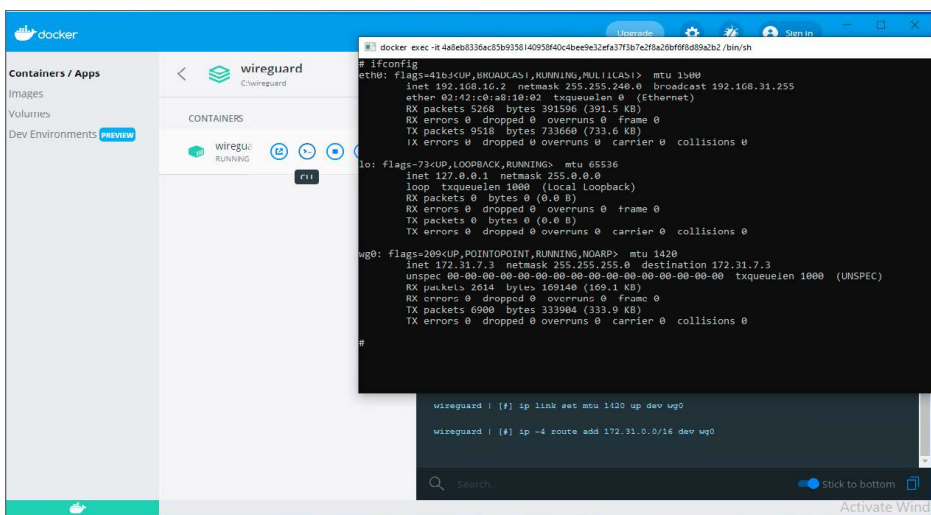


12. You can verify the Wireguard tunnel status from Cloud Edge.



## Troubleshooting

1. Connect to your Cloud Edge VPN agent or with the ZTNA application on any machine.
2. Open the terminal and run the following command:  
ping XXX.XXX.XXX.XXX - internal resource!
3. If the ping command fails, make sure that port UDP/8000 is not blocked in your docker container, and that you went through all the below steps:
  - Make sure the received bytes field fluctuates and increases. Wireguard will only communicate to an authenticated neighbor.
  - Ping the other side of the tunnel interface. If it works, then it's most likely your local firewall settings on the docker container.
4. Edit the WireGuard network settings (endpoint and subnet) later for restrict the specific network subnet or resources from your docker container. You can find the subnet/network details of the docker container by going to CLI.



# Groups and Members

## Topics:

- [Members](#)
- [Groups](#)
- [Identity Providers \(IdP\)](#)

## Members

### Topics:

- [Inviting Members](#)
- [Password Requirements](#)
- [Managing Roles](#)

## Inviting Members

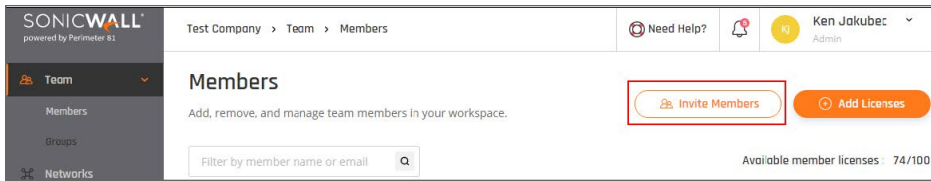
This article describes how users can gain access to **Networks** and **Applications** by authenticating within the workspace.

To have a seat in the platform, **Members** should be invited by the **Owner** or an **Admin**.

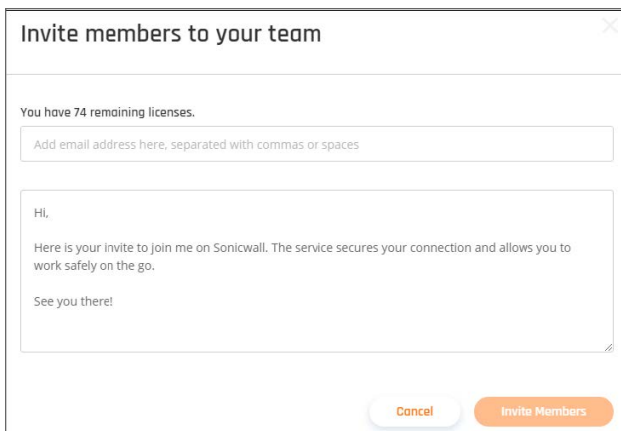
ⓘ | **NOTE:** Once the IdP is configured for the group, all the members can log into the interface.

## Inviting Members

1. Open **Team** in the **Management Platform**.
2. Click **Members**.
3. On the right top-side of the screen, click **Invite Members** on the top right side of the window.



4. Add the email addresses of the **Members** that you'd like to invite.



5. Select **Invite Members** when done.
  - You can send several invites at once, separating emails with commas. You can also modify the email body to make it more personal.
  - Alternatively, you can upload a CSV file listing up to 100 email addresses.
  - The member's **Email Address** is used as a unique identifier of **Members** in your workspace.
  - Email addresses will be confirmed by sending an invitation email with a unique registration link to each new **Member**.
  - You can send several invites at once, separating emails with commas. You can also modify the email body to make it more personal.
  - A sufficient number of available Team Member Licenses is required to invite new **Members** to your workspace.
  - You can see the number of available licenses above the **Invite Members** button on the right top corner of your screen.
6. Once the **Members** are invited, they will have to confirm their email addresses by following the link in the invitation email and set up their account.  
Once your **Members** create an account and log in to your workspace they'll be able to download the Agents and use Zero Trust Applications.
7. As an invited team member, each user will only have access to the servers and regions they are permitted access to by the administrator.



# Password Requirements

In order to ensure better system security, we enforce the use of a strong password. Your SonicWall password must include:

- 8 digits
- at least one upper case letter
- at least one lower case letter
- one number
- one special character

**NOTE:** Don't use a password you have used on another site or something too obvious like your pet's name.

# Managing Roles

This article describes how to use the Management Platform to assign different **Members** with different **Roles**.

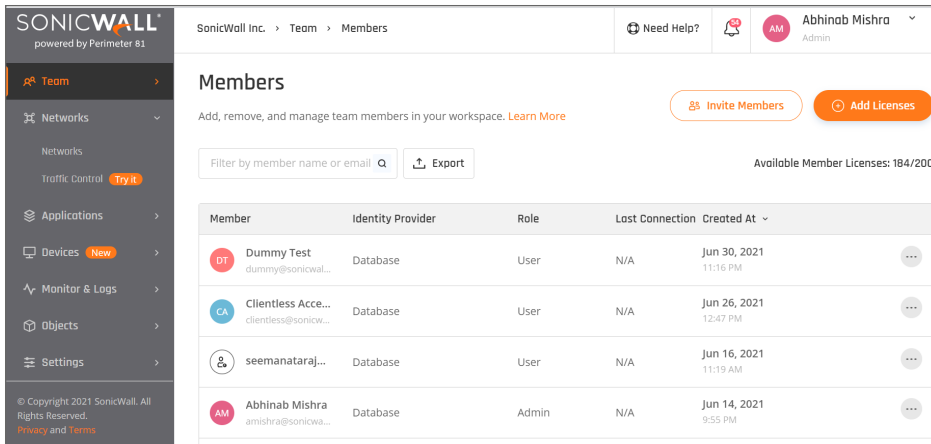
- Roles
- Assigning a role
- Breakdown of roles and permissions

## Roles

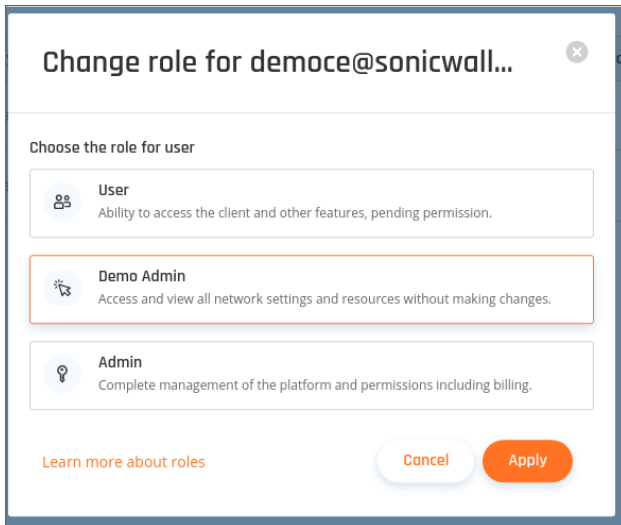
- **Admin:** Admins can modify permission settings and assign roles to other team members.
- **User:** A User can access the apps and download screen.

## Assigning a role

1. To modify User Roles as an administrator select **Team** in the **Management Platform** on the left side.
2. Select the **Members** tab.
3. Select the three-dotted menu (...) next to a team member's name to change the role.
4. Select **Change Role** in the drop-down list.



5. A window will appear with the different available roles. Select the desired role for your team member and select **Apply**.



**NOTE:** If admin wants to add more admin to be a portal administrator, a new admin must be selected to be the administrator. Demo Admins or users cannot assign themselves as admins.

## Breakdown of roles and permissions

| Role  | Manage Licenses | Manage Members | Manage Networks | Manage Configuration | View Activities |
|-------|-----------------|----------------|-----------------|----------------------|-----------------|
| Admin | Yes             | Yes            | Yes             | Yes                  | Yes             |
| User  | No              | No             | No              | No                   | No              |

# Groups

## Topics:

- [Managing Groups](#)
- [Identity Provider Groups](#)

## Managing Groups

This article describes the **Groups** feature that complements the user-centric access policy encouraged by both SSO and our Database authentication. **Groups** let you assign specific network access rules to your team, usually based on roles, responsibilities, or location.

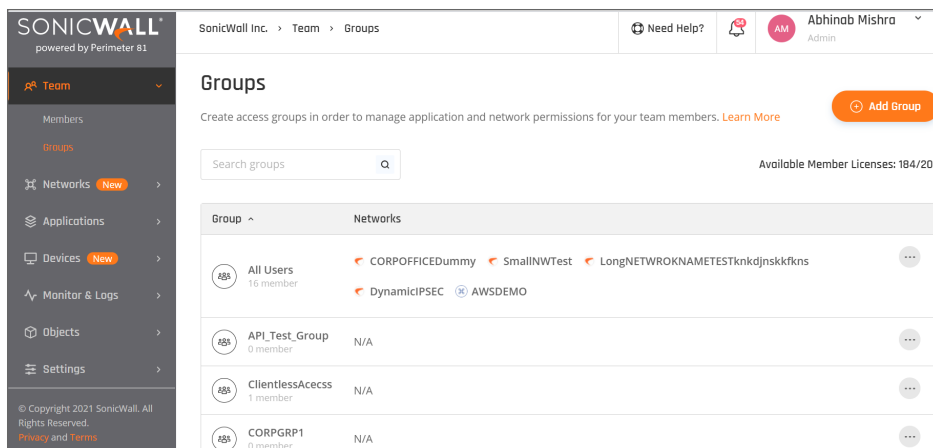
- Creating a user group
- Editing **members** in a group
- Managing access for groups

You can use **Groups** to better control your **Network** and **Zero Trust Application** Policies.

Sorting your **Members** into **Groups** provides your organization with a significantly reduced attack surface. Least-privilege access policies hinge on the ability to group employees by the resources they need to do their jobs.

## Creating a user group

1. To create a User Group, select the **Team** tab in the Management Platform.
2. Select the **Groups** tab below and select **Add Group** on the right side of the window.

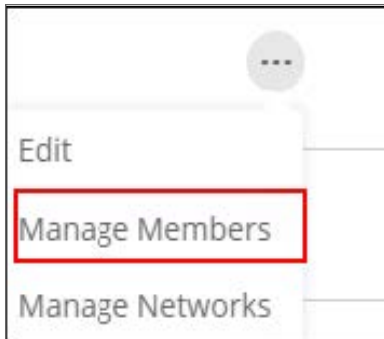


The screenshot shows the SonicWall Management Platform interface. The top navigation bar includes the SonicWall logo, the breadcrumb 'SonicWall Inc. > Team > Groups', and user information for Abhinab Mishra (Admin). The main content area is titled 'Groups' and includes a search bar, a 'Learn More' link, and an 'Add Group' button. Below this is a table listing existing groups and their associated networks.

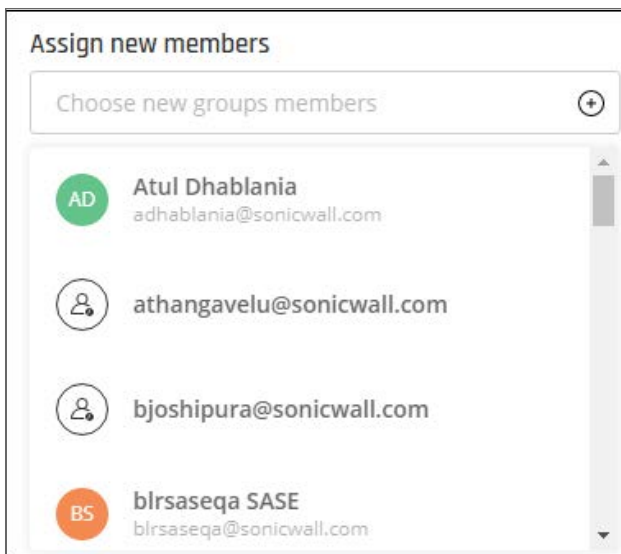
| Group                        | Networks  |
|------------------------------|---|
| All Users<br>16 member       | CORPOFFICEDummy SmallINWTest LongNETWROKNAMETESTknkdjnskkfkns<br>DynamicIPSEC AWSDEMO |
| API_Test_Group<br>0 member   | N/A   |
| ClientlessAccess<br>1 member | N/A   |
| CORPGRP1<br>0 member         | N/A   |

## Editing members in a group

1. Once you have created a Group, you can edit members by selecting the three-dotted menu (...) on the right side and choosing **Manage Members**.



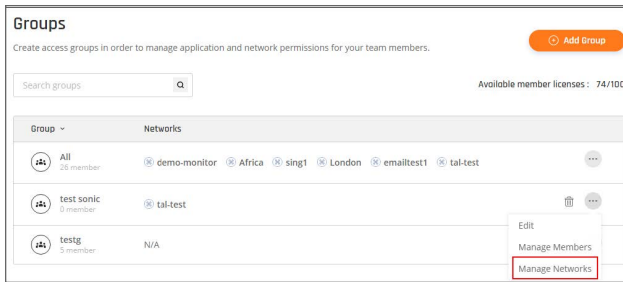
2. Select the + sign to list members. Select the team members you want to add to the Group. Please notice that you will see only non-members on the list.



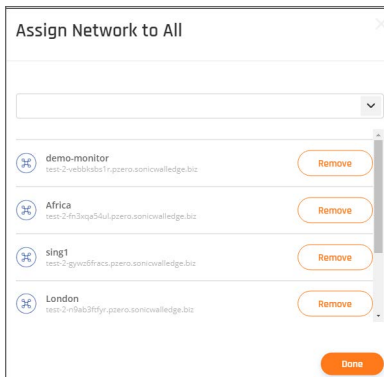
The new members are added to the group.

## Managing access for groups

1. Groups are created to control who can access which location. Select **Groups** in the left side panel.
2. Select the three-dotted menu (...) next to the group you'd like to limit or grant access to and select **ManageNetworks**.



3. Select or remove the teams as desired for this location.



4. Select **Done** when finished.

## Identity Provider Groups

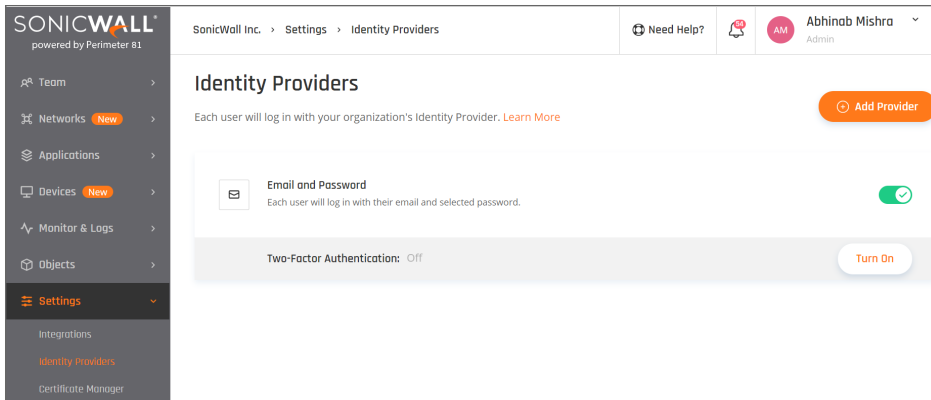
This article describes what to do if you have encountered an error while accessing your team member's account after configuring a third-party Identity Provider (IdP), for instance, G-Suite, Okta, JumpCloud, or your on-premise AD. You must make sure your SonicWall CloudEdge user group's names match the IDP user group's names.

- Using your IdP SSO for specific user groups
- Using your IdP SSO for all team members

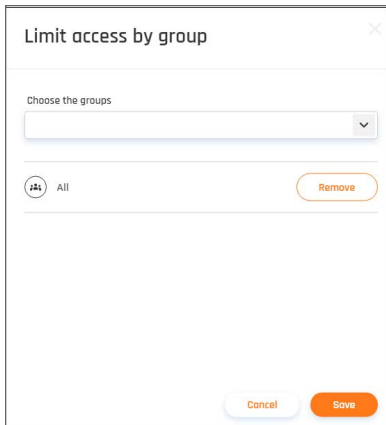
### Using your IdP SSO for specific user groups

1. Select **Settings** in the **Management Platform** on the left side.
2. Next, under the **Identity Providers** tab follow these steps:

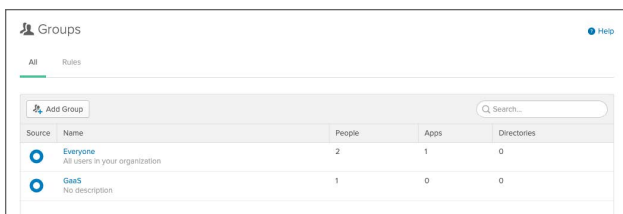
3. Select the lock icon.



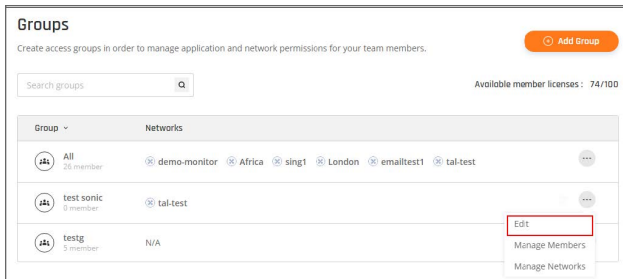
4. Choose the desired **group** and select **Save**.



5. Verify that the group has the same name (pay attention to lower and upper case) in your IDP management platform. For instance:

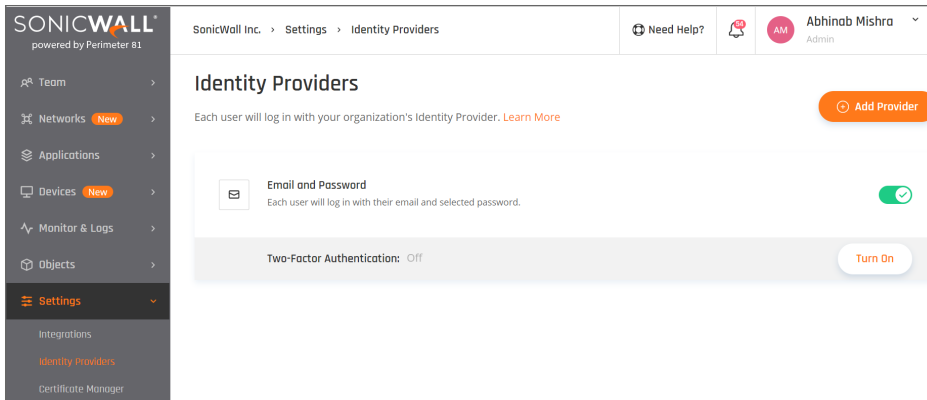


6. Make sure that SonicWall Cloud Edge is assigned to the appropriate groups at the IDP management platform (not relevant in Okta).
7. If you'd like to change your SonicWall Cloud Edge group name, go to the **Team** and select **Groups** and click the three-dotted icon beside the group name. Select **Edit**.

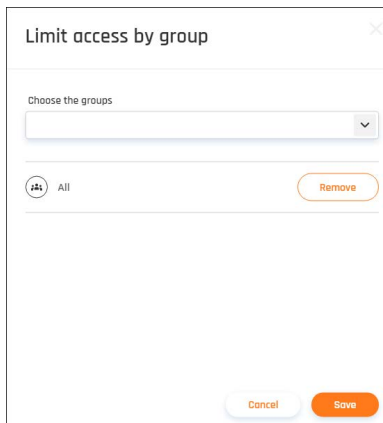


## Using your IDP SSO for all team members

1. Select **Settings** in the **Management Platform** on the left side.
2. Next, under the **Identity Providers** tab follow these steps:
3. Select the lock icon.



4. Remove 'All Users' from the limit access by the group page. This will allow all users to connect.



5. Select **Save**.

# Identity Providers (IdP)

## Topics:

- [Integrate Identity Providers](#)
- [Azure Active Directory](#)
- [Google Suite](#)
- [On-Premises Active Directory](#)
- [SAML 2.0](#)

## Integrate Identity Providers

### Identity Providers (IdP)

This article describes how to make secure login and policy-based access easy, with seamless Single Sign-On (SSO) integration with most industry-standard identity providers (IdP) so that you can onboard your entire team with total ease.

More importantly, integrating an Identity Provider and SSO makes for a safer and more user-friendly access policy:

- **Increase productivity** by giving employees single-click access to all the resources they need to succeed.
- **Manage risks to your network** by preventing employees from using their best judgment when it comes to password habits.
- **Reduce the burden on your IT** and Help Desk employees who no longer need to retrieve or manage company credentials.
- **Prevent former-employees or vendors** from accessing any company resources by removing their access rights in one centralized location.

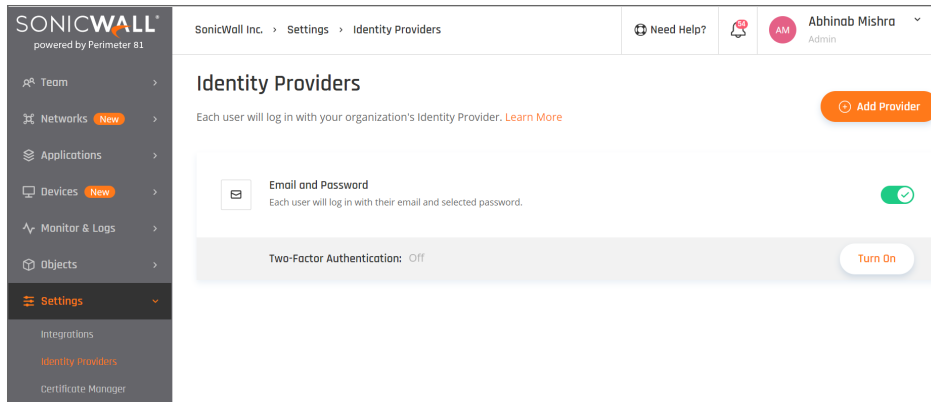
You can integrate various third-party identity providers such as:

- G-Suite / Google Cloud Services
- On-Premise Active Directory (LDAP)
- Microsoft Azure Active Directory
- **SAML 2.0** Identity Providers (OKTA, OneLogin, ADFS, etc.)

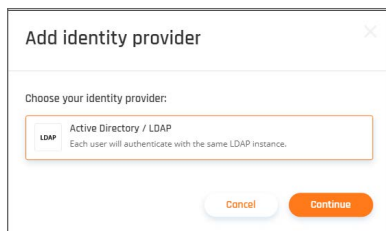


# Integrating with an IdP

1. To integrate an Identity Provider into the Management Platform, select **Settings** in the **Management Platform** on the left side.

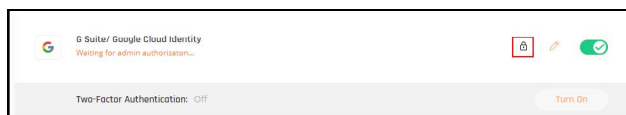


2. Select **Add Provider**.
3. A list of Identity Providers displays. Select your desired Identity Provider and select **Continue**.

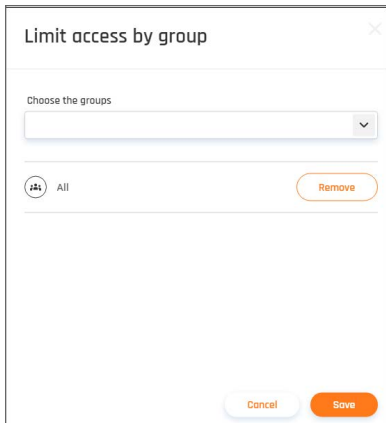


The default setting is that all Identity Provider users can log into the Management Platform.

4. If you would like to limit access to specific Identity provider groups, you can do so by selecting the lock symbol next to the name of your Identity Provider.



5. Select the different groups that you'd like to give access and select **Save**.



The screenshot shows a dialog box titled "Limit access by group". At the top, there is a close button (X). Below the title, there is a section labeled "Choose the groups" with a dropdown menu. Underneath the dropdown, there is a list of groups. The first group is "All", which has a "Remove" button next to it. At the bottom of the dialog, there are two buttons: "Cancel" and "Save".

## Azure AD

### Topics:

- [Azure Active Directory \(SAML 2.0\)](#)
- [Azure Active Directory](#)

## Azure Active Directory (SAML 2.0)

This article describes how to configure Azure Active Directory through SAML 2.0 to use as an identity provider for SonicWall Cloud Edge.

- [Configuring the Enterprise Application on Azure AD](#)
- [Exporting the signing certificate](#)
- [Configuring the SAML 2.0 connection in the Management Platform](#)

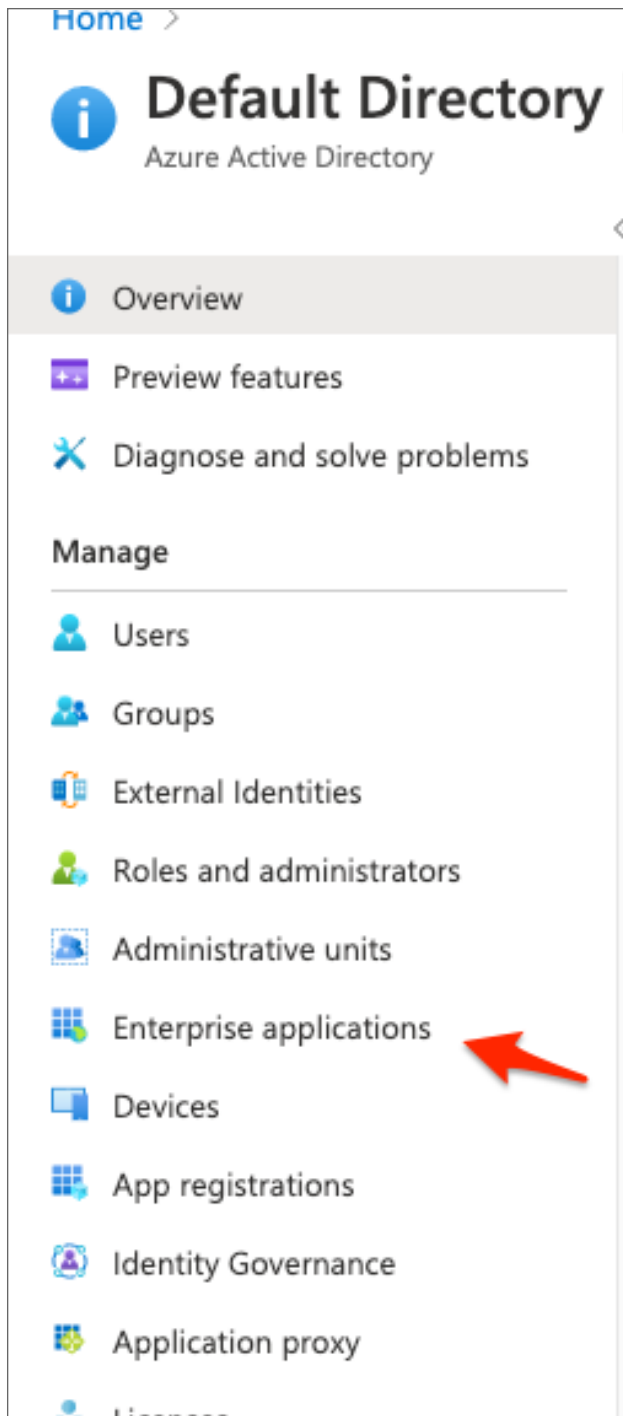
### NOTE:

#### Group Support

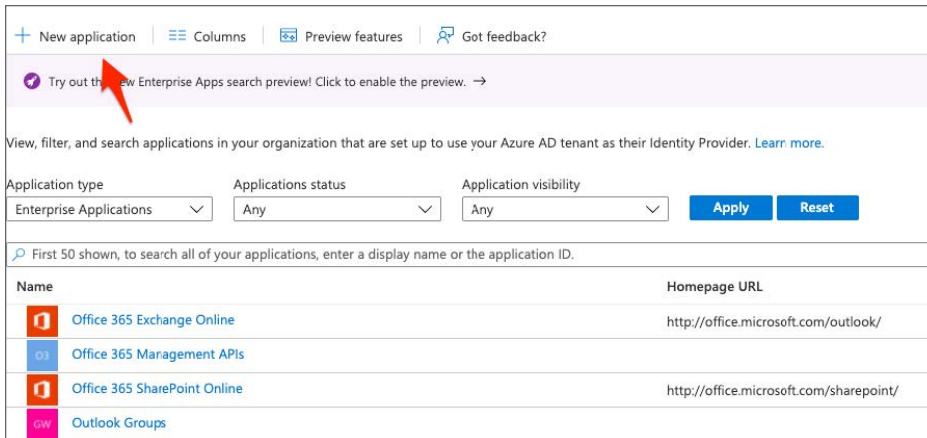
Be aware that if you choose to configure Azure AD through SAML 2.0, your user's groups will not automatically be synced with their account on the SonicWall Cloud Edge side (like with the App Registration). You will have to manually add or remove users from groups in your SonicWall Cloud Edge console.

## Configuring the Enterprise Application in Azure Active Directory

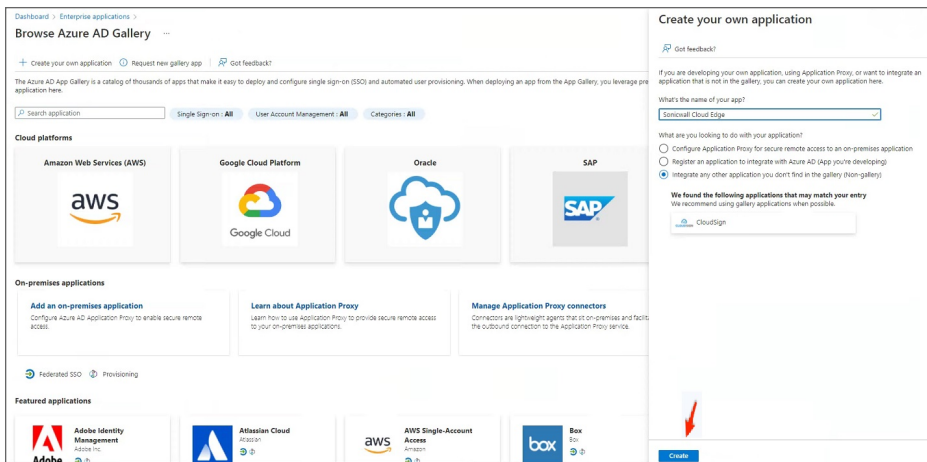
1. Start by signing into your **Azure Active Directory** and selecting **Enterprise Applications**.



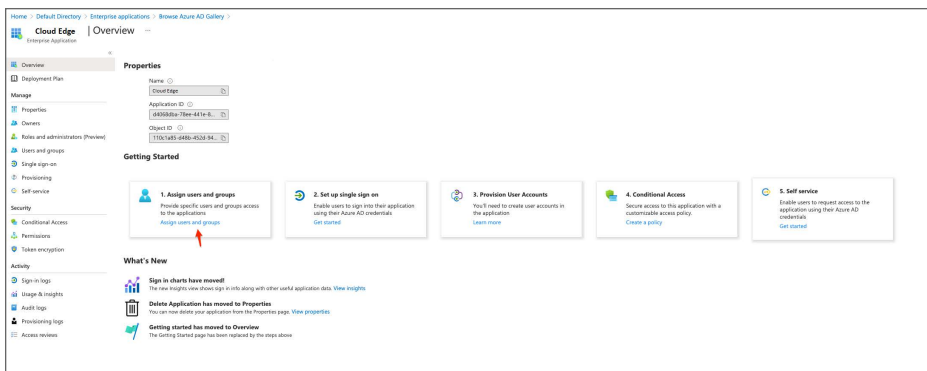
2. Search for the **"SonicWall Cloud Edge"** application and click to select it.



3. If no Application is found then select **"+ New Application"**.



4. Select **"Create"** (This may take a few minutes).
5. Next you need to assign access to users or groups (if you are using the Azure AD free edition you won't be able to select groups and will have to select individual users).



6. Once users have been added and saved select the second option to **"Set up single sign on"**.

**Properties**

Name

Client type

Application ID

Object ID

**Getting Started**

- 1. Assign users and groups**  
Provide specific users and groups access to the application.  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into that application using their Azure AD credentials.  
[Get started](#)
- 3. Provision User Accounts**  
You'll need to create user accounts in the application.  
[Learn more](#)
- 4. Conditional Access**  
Secure access to this application with a customizable access policy.  
[Create a policy](#)
- 5. Self service**  
Enable users to request access to the application using their Azure AD credentials.  
[Get started](#)

**What's New**

- Sign in charts have moved!**  
The new insights view shows sign in info along with other useful application data. [View insights](#)
- Delete Application has moved to Properties**  
You can now delete your application from the Properties page. [View properties](#)
- Getting started has moved to Overview**  
The Getting Started page has been replaced by the steps above

7. Select the **"SAML"** method.

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Select a single sign-on method [Help me decide](#)

- Disabled**  
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**  
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Linked**  
Link to an application in My Apps and/or Office 365 application launcher.

8. You need to edit the **"Basic SAML Configuration"**.

## Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating [Cloud Edge](#).

**1** Basic SAML Configuration Edit

|  |                 |
|--|-----------------|
| Identifier (Entity ID)                     | <b>Required</b> |
| Reply URL (Assertion Consumer Service URL) | <b>Required</b> |
| Sign on URL                                | <i>Optional</i> |
| Relay State                                | <i>Optional</i> |
| Logout Url                                 | <i>Optional</i> |

**2** Attributes & Claims Edit

|                        |                        |
|------------------------|------------------------|
| givenname              | user.givenname         |
| surname                | user.surname           |
| emailaddress           | user.mail              |
| name                   | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

**3** SAML Signing Certificate Edit

|                             |   |
|-----------------------------|---|
| Status                      | Active  |
| Thumbprint                  | [REDACTED]  |
| Expiration                  | 2/6/2026, 12:00:39 PM   |
| Notification Email          | [REDACTED]  |
| App Federation Metadata Url | <a href="https://login.microsoftonline.com/[REDACTED]">https://login.microsoftonline.com/[REDACTED]</a> |
| Certificate (Base64)        | <a href="#">Download</a>  |
| Certificate (Raw)           | <a href="#">Download</a>  |
| Federation Metadata XML     | <a href="#">Download</a>  |

9. On this step add the following as **"Identifier"**:

```
urn:auth0:SonicWall-production:YOURWORKSPACEHERE-oc
```

For the **"Reply URL (Assertion Consumer Service URL)"**, input the following:

```
https://auth.sonicwalledge.com/login/callback?connection=YOURWORKSPACE-oc
```

## Sign In

**This is your workspace**

Enter your workspace URL below.

Workspace URL

yourworkspace
.sonicwalledge.com

**Continue**

[Forgot Your Workspace?](#)

### Basic SAML Configuration

**3.) Save**

Save | Got feedback?

Identifier (Entity ID) \* ⓘ  
*The default identifier will be the audience of the SAML response for IDP-initiated SSO*

**1.) Change**

urn:auth0:SonicWall-production:YOURWORKSPACEHERE-oc ✓ [Default] [✓] [ⓘ] [🗑]

Patterns:

Reply URL (Assertion Consumer Service URL) \* ⓘ  
*The default reply URL will be the destination in the SAML response for IDP-initiated SSO*

**2.) Change**

https://auth.sonicwalledge.com/login/callback?connection=YOURWORKSPACE-oc ✓ [Default] [✓] [ⓘ] [🗑]

Patterns:

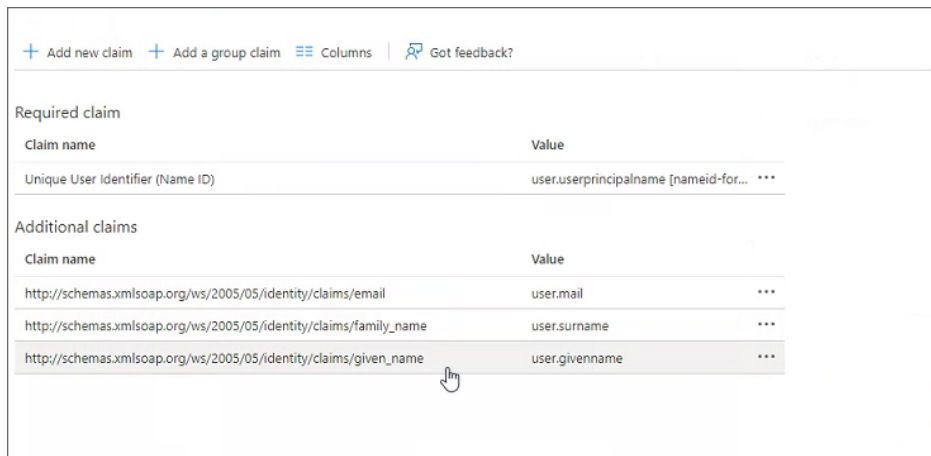
Sign on URL ⓘ  
 Enter a sign on URL

Relay State ⓘ  
 Enter a relay state

Logout Url ⓘ  
 Enter a logout url

10. After both have been added you can select the "Save" option.

11. Rename the "Attributes & Claims" in Step 2 to below given values.



The screenshot shows a configuration interface for 'Attributes & Claims'. At the top, there are navigation options: '+ Add new claim', '+ Add a group claim', 'Columns', and 'Got feedback?'. Below this, there are two sections: 'Required claim' and 'Additional claims'. Each section contains a table with 'Claim name' and 'Value' columns. In the 'Additional claims' table, the row for 'http://schemas.xmlsoap.org/ws/2005/05/identity/claims/given\_name' is highlighted, and a mouse cursor is pointing at it.

| Required claim                   |   |
|----------------------------------|---|
| Claim name                       | Value                                     |
| Unique User Identifier (Name ID) | user.userprincipalname [nameid-for... *** |

| Additional claims   |                    |
|---|--------------------|
| Claim name  | Value              |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/email       | user.mail ***      |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/family_name | user.surname ***   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/given_name  | user.givenname *** |

12. Finally you can download your SAML signing certificate in Step 3 (the Base64 version). In step 5 you need to expand the "Step-by-step instructions" and copy your Login URL.

① **NOTE:** Be sure to keep both your SAML Signing Certificate and Login URL accessible as you will be using them both very shortly in your SonicWall tenant.



**3** SAML Signing Certificate Edit

Status: Active

Thumbprint: [REDACTED]

Expiration: 11/11/2024, 12:08:25 PM

Notification Email: [REDACTED]

App Federation Metadata Url: [https://login.microsoftonline.com/\[REDACTED\]](https://login.microsoftonline.com/[REDACTED])

Certificate (Base64): [Click](#) [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

**4** Highly recommended: Install the Azure AD browser extension

The My Apps Secure Sign-in browser extension is not installed. This extension can make it easier to finish the set up by filling in the necessary fields. Make sure you allow third-party cookies if you have installed it but this message still shows up.

[Install the extension](#)

**5** Set up Cloud Edge

You'll need to configure the application to link with Azure AD.

- ✓ Fill out required fields in Step 1
- ⚠ Download the My Apps extension

[Set up Cloud Edge](#)

[Or, view step-by-step instructions](#) [Click](#)

Configuration URLs

- Login URL: [https://login.microsoftonline.com/\[REDACTED\]](https://login.microsoftonline.com/[REDACTED]) [Click](#)
- Azure AD Identifier: [https://sts.windows.net/\[REDACTED\]](https://sts.windows.net/[REDACTED])
- Logout URL: [https://login.microsoftonline.com/\[REDACTED\]](https://login.microsoftonline.com/[REDACTED])

## Configuring the SAML 2.0 Application on SonicWallCloud Edge

1. Click on settings in your SonicWall Cloud Edge Tenant. Go to your Identity Providers and select the option to "**+ Add Provider**".

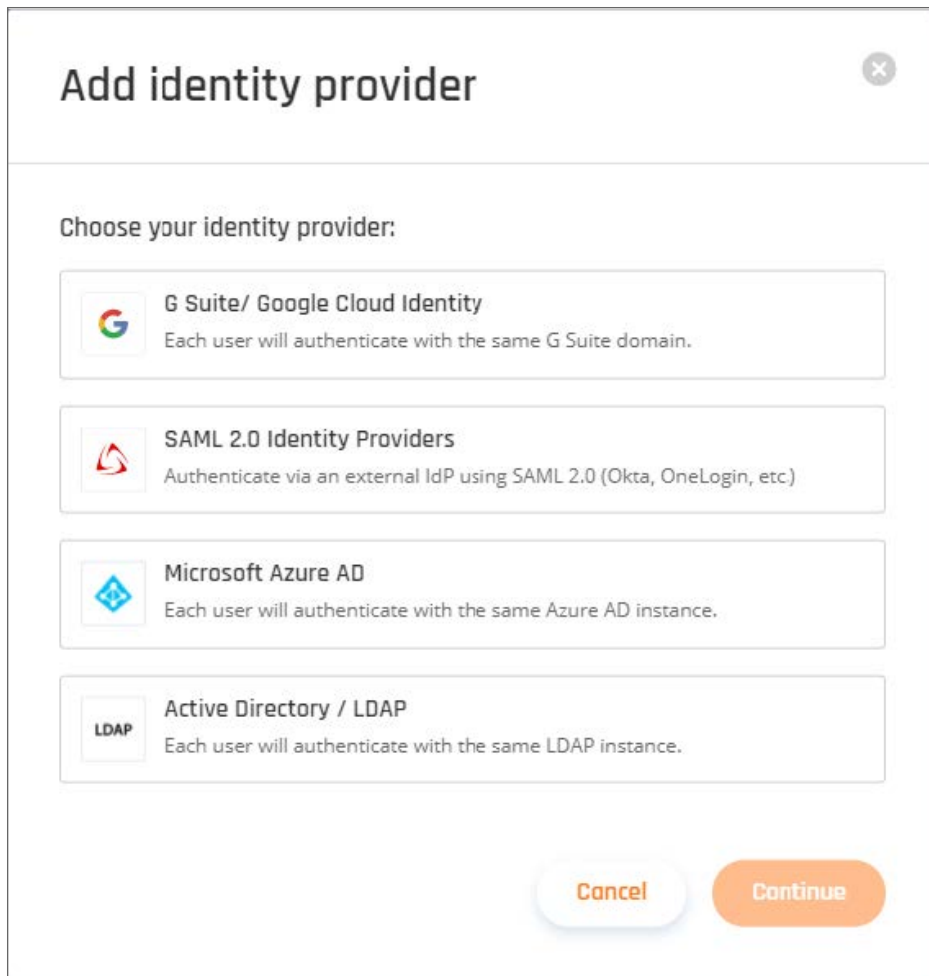
**Identity Providers** [Add Provider](#)

Each user will log in with your organization's Identity Provider. [Learn More](#)

**Email and Password**  
Each user will log in with their email and selected password.

**Two-Factor Authentication:** Off [Turn On](#)

2. Select "**SAML 2.0 Identity Providers**" and then "**Continue**".



3. Fill out the following:

- **Sign in URL:** This will be your "Login URL" you copied from Azure.
- **Domain Aliases:** This will be the domain used by your users (everything after the "@" sign in their email).
- **X509 Signing Certificate:** This will be the certificate you downloaded from Azure.

The screenshot shows a configuration window titled "SAML 2.0 Identity Providers" with a close button in the top right corner. Below the title, there is a link: "If you have any questions about setting up an SAML, [click here](#)." The form contains three main sections: "Sign In URL\*" with a text input field containing "Sign in URL"; "Domain Aliases\*" with a text input field containing "Add business's domain name, separated by commas or spaces"; and "X509 Signing Certificate\*" with a large text area containing "X509 Signing Certificate\*" and an "Upload PEM/CERT File" button with an upload icon. At the bottom right, there are two buttons: "Cancel" and "Done".

4. After everything has been added, select **"Done"**.

## Azure Active Directory

This article describes how to allow users to log in using a Microsoft Azure Active Directory account, either from your company or from external directories. You must register your application through the Microsoft Azure portal. If you don't have a Microsoft Azure account, you can sign up for free.

- Creating a new application
- Configuring the permissions
- Allowing access from external organizations (optional)
- Configuring the key
- Configuring Reply URLs
- Configuring IDP connection

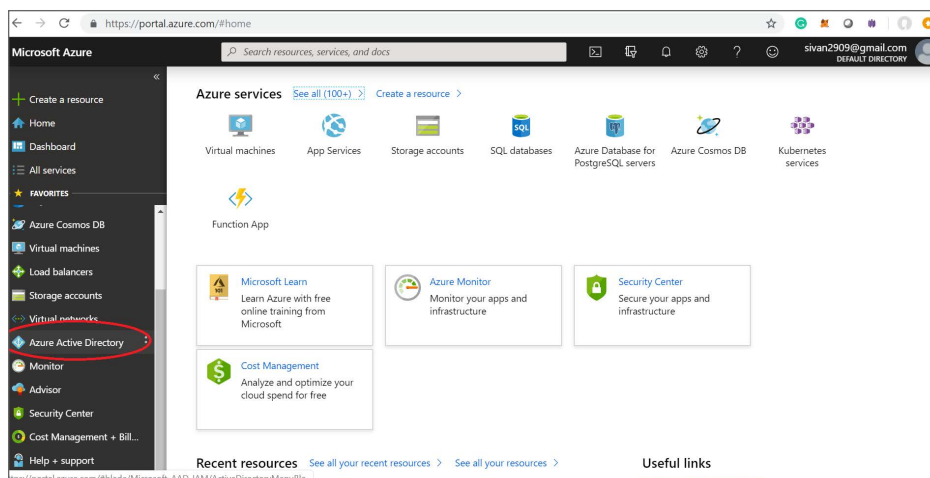
You can access the Azure management portal from your Microsoft service, or visit <https://portal.azure.com/> and sign in to Azure using the global administrator account used to create the Office 365 organization.

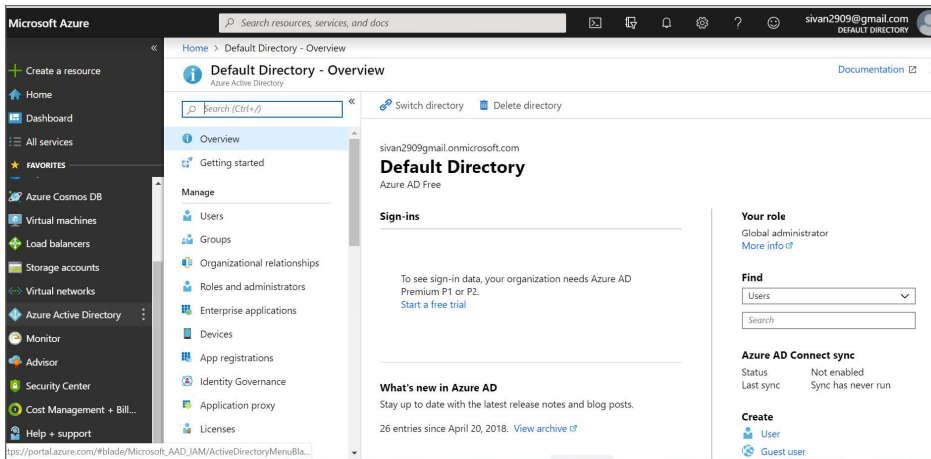
If you have an Office 365 account, you can use the account's Azure AD instance instead of creating a new one. To find your Office 365 account's Azure AD instance:

1. Sign in to Office 365.
2. Navigate to the **Office 365 Admin Center**.
3. Open the Admin centers menu options located on the left menu.
4. Select **Azure AD**. This will take you to the **Admin Center** of the Azure AD instance backing your Office 365 account. Follow the steps below to connect your SonicWall Cloud Edge Account to Azure Active Directory (images below):
5. Create a new application.
6. Configure the permissions.
7. Allow access from external organizations (optional).
8. Create the key.
9. Configure Reply URLs.
10. Configure SonicWall Cloud Edge IDP connection.

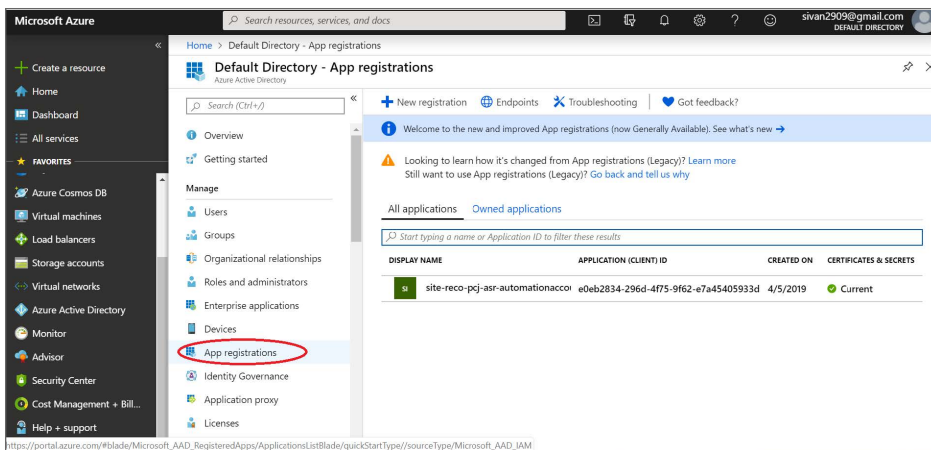
## Creating a new application

1. Log in to Microsoft Azure and choose **Azure Active Directory** from the sidebar.

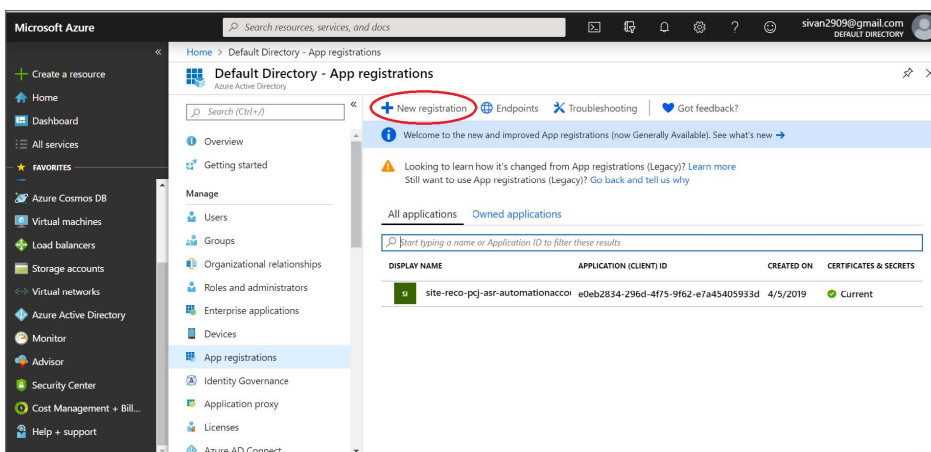




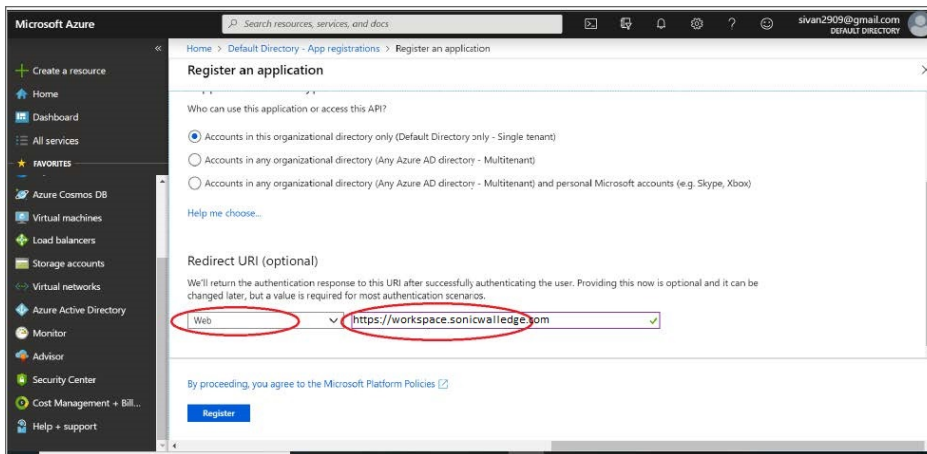
## 2. Under Manage, select App registrations.



## 3. Select NewRegistration to add a new application.

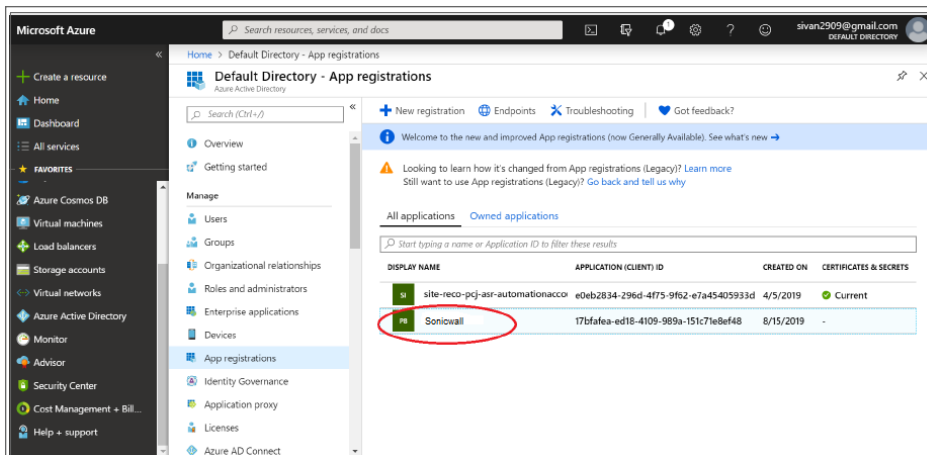


4. Enter the name "SonicWall Cloud Edge" for the application, select **Web app/API** as the Application Type, and for Sign-on URL enter your application URL with your workspace name: [https://workspace.sonicwalledge.com].

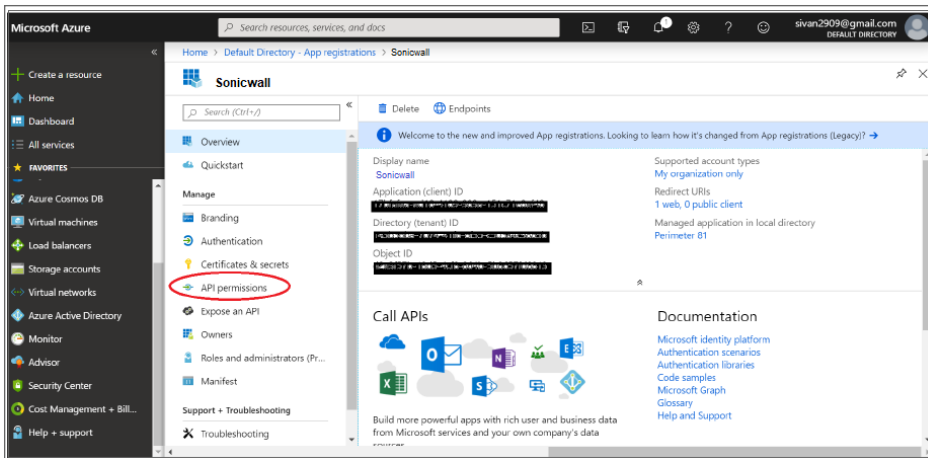


## Configuring the permissions

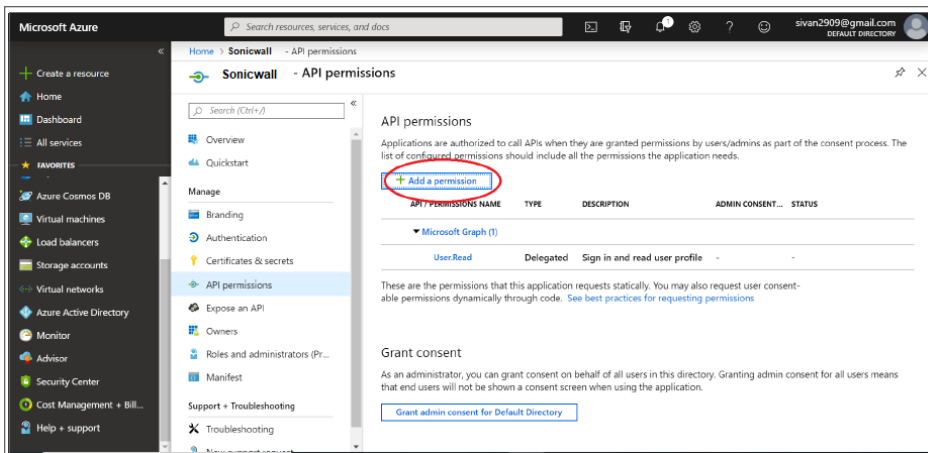
1. Once the application has been created, you will have to configure the permissions. Select the name of the application SonicWall Cloud Edge to open the **Settings** section.



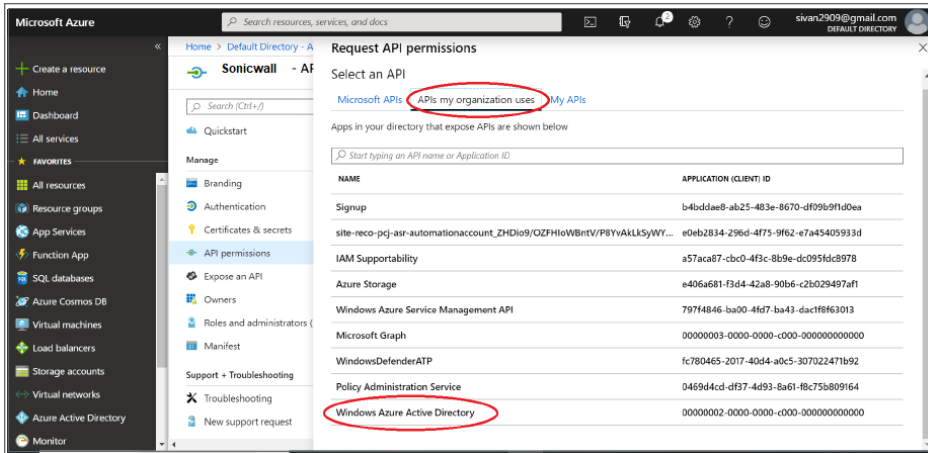
2. Select API permissions.



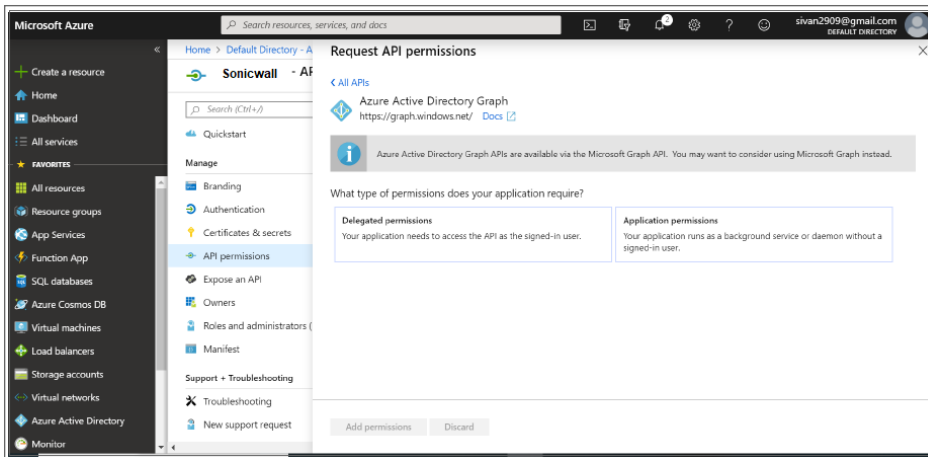
3. Select Add a permission.



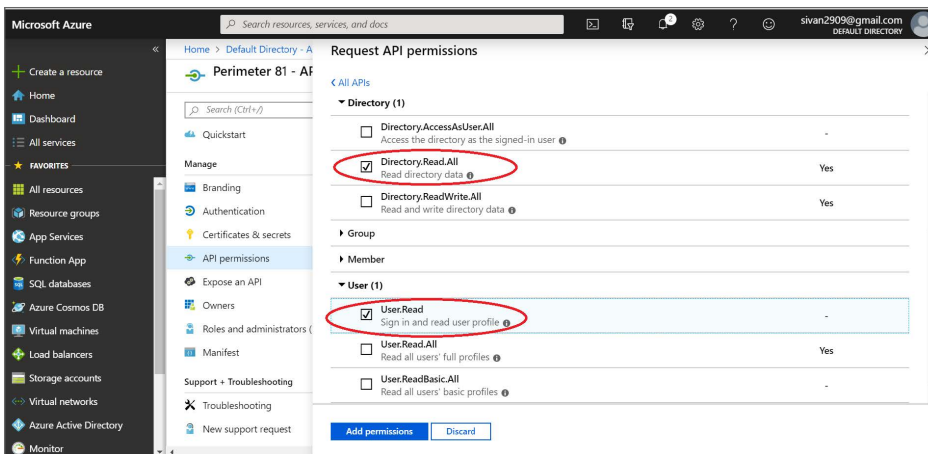
4. Select APIs my organization uses and choose Windows Azure Active Directory to change the access level.



The following page displays:



- The next step is to modify permissions so your app can read the directory. Under **Delegated permissions**, check next to **Sign in and read user profile** and **Read directory data**.





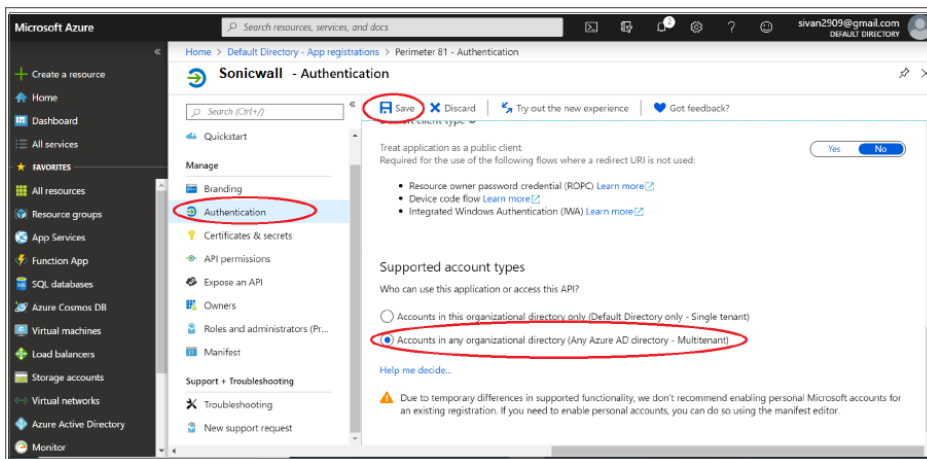
6. Grant Admin Consent if requested.

## Support user groups

1. If you want to enable **user group** support you will need to enable the following permissions:
  - **Application Permissions:** Read directory data
  - **Delegated Permissions:** Access the directory as the signed-in user.
2. Select **Save** at the top to save these changes.
3. Grant Admin Consent if requested.

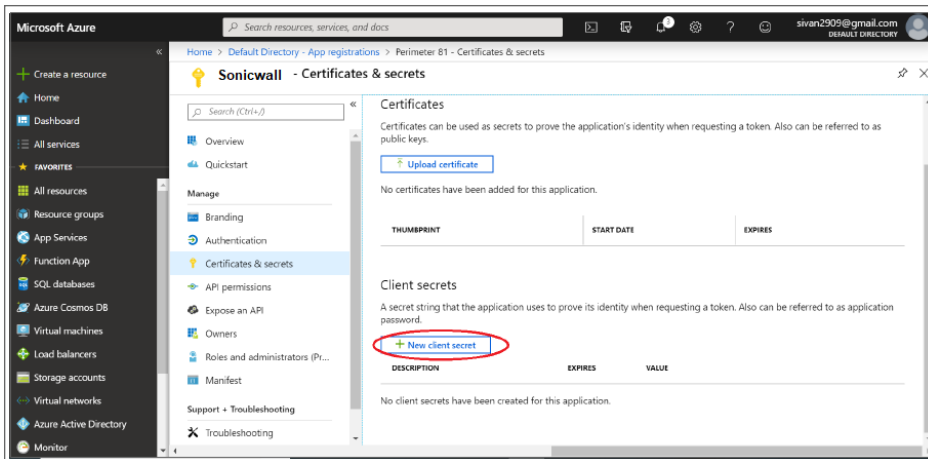
## Allowing access from external organizations (optional)

1. If you want to allow users from external organizations (such as other Azure directories) to log in, you will need to enable the **Multi-Tenant** option for this application. In the **Authentication** section, choose the **Multi-tenant option**.
2. Select **Save** at the top to save these changes.
3. Grant Admin Consent if requested.



## Configuring the key

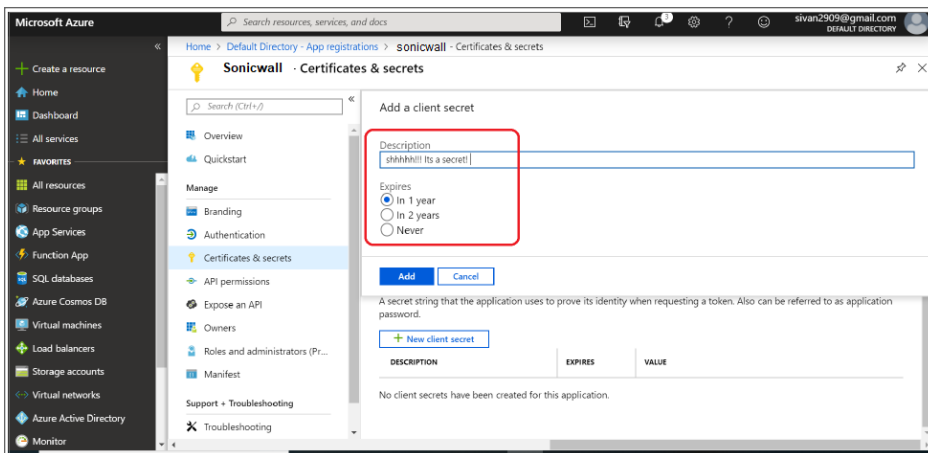
1. You will need to create a key (secret password) that will be used as the **Client Secret** in the SonicWall Cloud Edge IDP connection. Select **Certificates and secrets** from the **Application** menu.

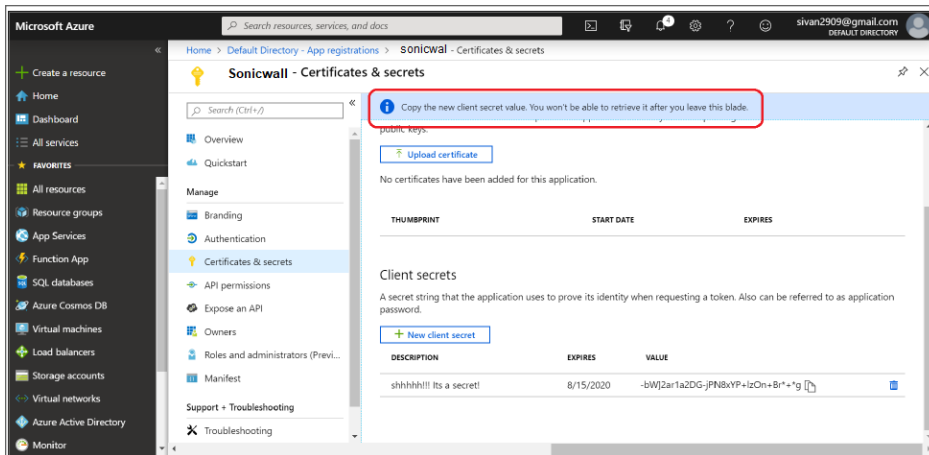


2. Enter a name for the key and choose the desired duration.

If you choose an expiring key, make sure to record the expiration date in your calendar, as you will need to renew the key (get a new one) before that day to ensure users don't experience a service interruption.

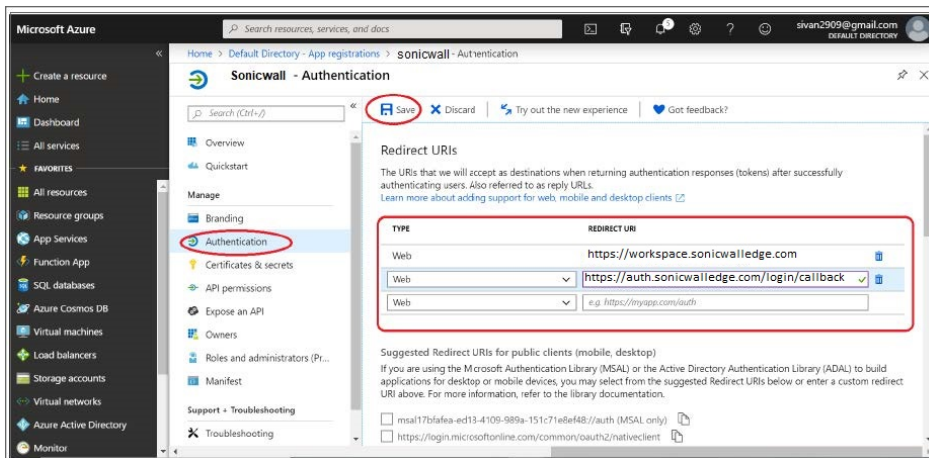
Select **Add** and the key will be displayed. Make sure to copy the value of this key before leaving this screen, otherwise, you may need to create a new key. This value is used as the **Client Secret** in the next step.





## Configuring Reply URLs

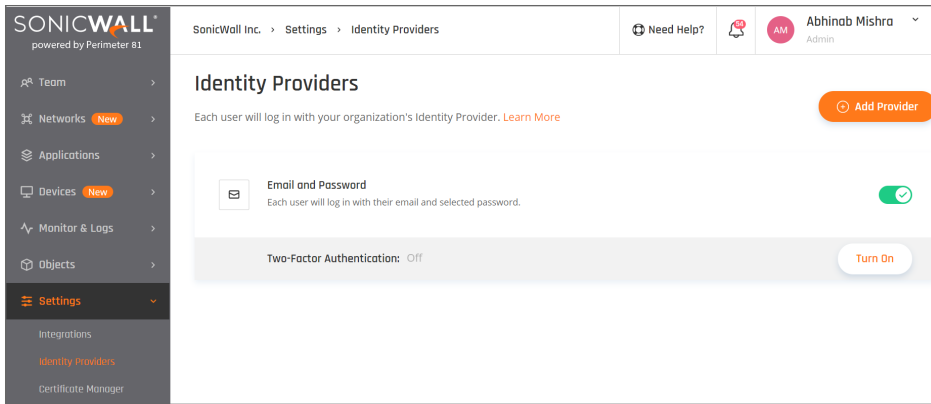
1. Next, you need to ensure that your Auth0 callback URL is listed in allowed reply URLs for the created application.
2. Navigate to **Azure Active Directory**, then **Apps registrations** and select the SonicWall Cloud Edge app. Then select **Authentication**, go to **Redirect URLs** and add the following link:  
<https://auth.sonicwalledge.com/login/callback>



3. Select **Save**.

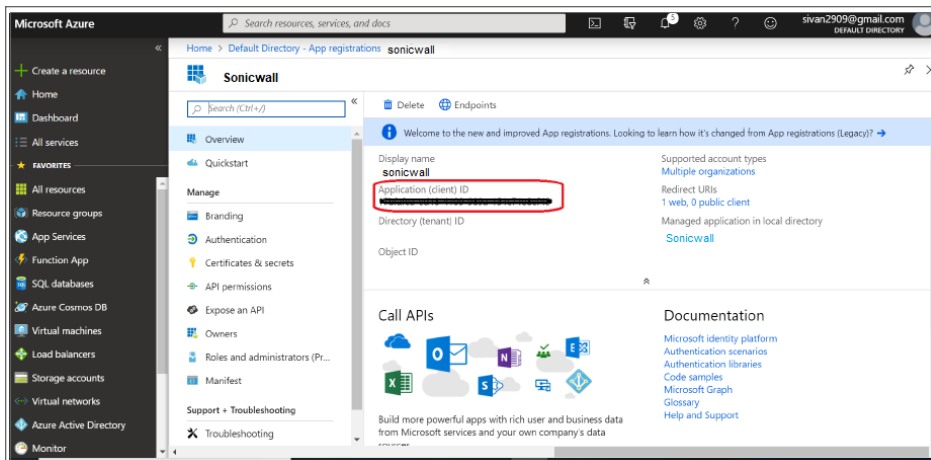
## Configuring IDP connection

1. Log in to your SonicWall Cloud Edge Management Platform, navigate to **Settings**, and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Choose **Microsoft Azure AD**.

4. Fill in Microsoft Azure AD **Domain** (your domain - for example sonicwall.com), **Domain Aliases** (optional), **Client ID**, and **Client Secret**. For the **Client ID**, this value is stored as the Application ID in Azure AD.



5. For the **Client Secret** use the value that was shown for the key when you created it in the previous step.
6. Under **Domain** set the name of the **Microsoft Azure AD Domain** and under **Domain Aliases** insert any email domain that corresponds to the connection.
7. Select **Done**.  
If your users are getting access errors after the configuration, please [check these steps](#).

## Google Suite

### Topics:

- [Google Services](#)
- [Google Apps \(SAML 2.0\)](#)

## Google Services

This article describes the two ways to set Google Suite as your [identity provider](#) using **Google Service** or using **Google SAML** applications.

- Configuring Google Suite as your IdP using Google Services
- Generating the Google Client ID and Client Secret
- Enabling the Admin SDK Service
- Enabling and Configuring the Google Suite Connection
- Access Error troubleshooting

When choosing one over the other please keep in mind:

- While (at the moment) a SAML integration does not lead to any additional costs on Google's side, applying this configuration using Google Services may increase your Google Suite pricing, depending on your Google customer tier.
- A SAML integration enables you to force all users to authenticate using Google Suite, as opposed to setting up a Google Service which is more flexible and can be applied to particular groups of users only.

## Configuring Google Suite as your IdP using Google Services

You can connect your Account to Google Suite by providing the Google Client ID and Client Secret to SonicWall Cloud Edge. Follow the steps below:

- Generate the Google Client ID and Client Secret
- Enable the Admin SDK service
- Enable and configure the SonicWall CloudEdge GSuite Connection

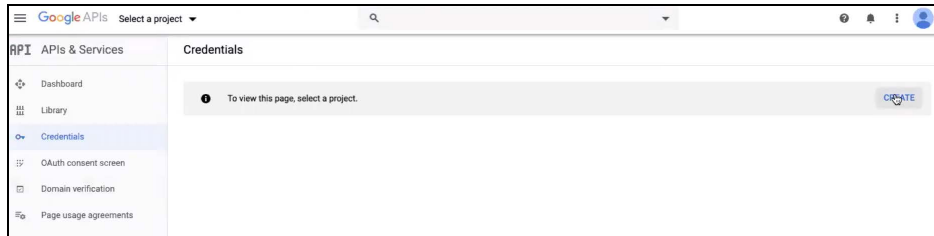
## Generating the Google Client ID and Client Secret

1. While logged in to your Google admin account, go to the API Manager and then **Credentials** in the **Management Portal** on the left side.

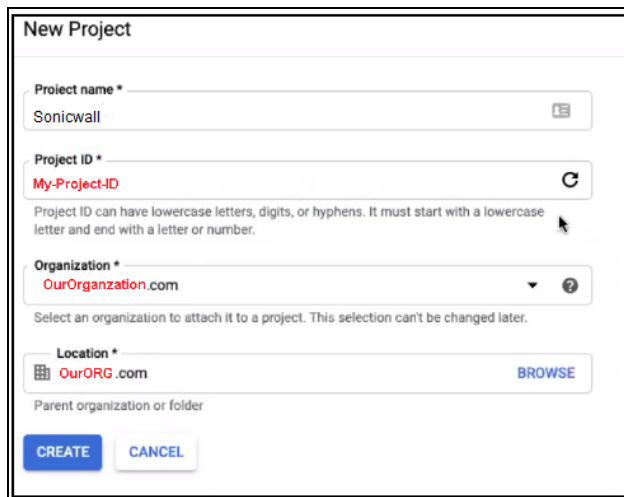
(<https://console.developers.google.com/projectselector/apis/credentials?pli=1> )

You should follow steps 2-3 only in case you do not have already a project defined on Google Cloud Platform.

2. Select **Create** to create a new project.



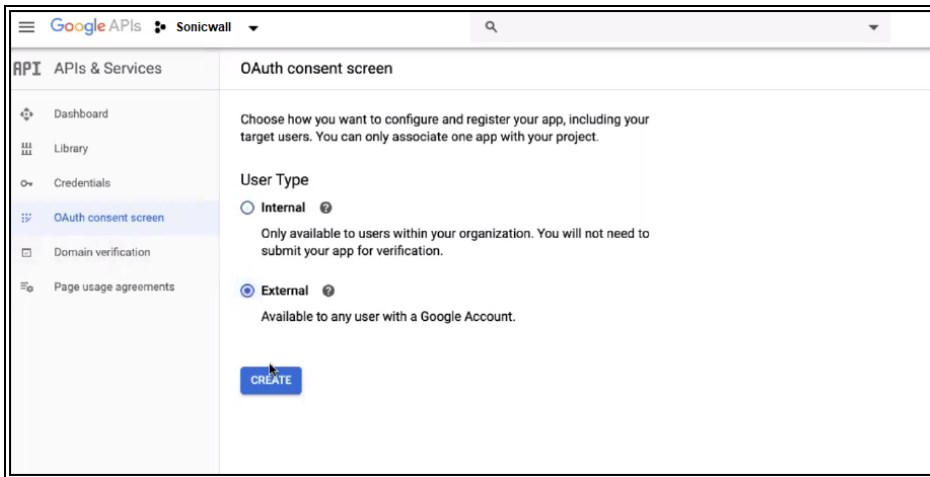
3. In the dialog box that appears, provide a Project name, answer Google's email- and privacy-related questions, and select **Create**:

A screenshot of the "New Project" dialog box. It contains the following fields and options:

- Project name \***: A text input field containing "Sonicwall".
- Project ID \***: A text input field containing "My-Project-ID". Below it is a note: "Project ID can have lowercase letters, digits, or hyphens. It must start with a lowercase letter and end with a letter or number."
- Organization \***: A dropdown menu showing "OurOrganization.com". Below it is a note: "Select an organization to attach it to a project. This selection can't be changed later."
- Location \***: A dropdown menu showing "OurORG.com". Below it is a note: "Parent organization or folder".

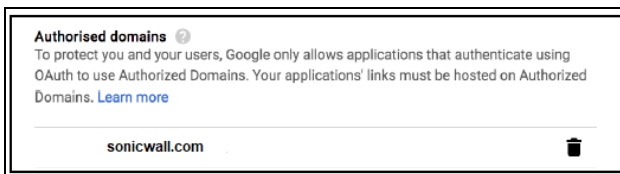
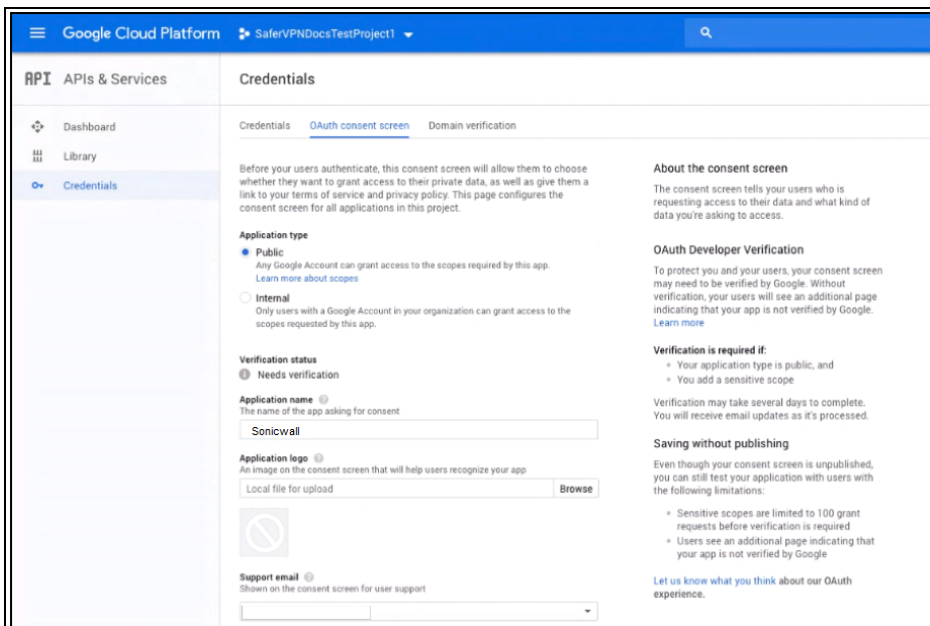
At the bottom, there are two buttons: "CREATE" and "CANCEL".

4. Under OAuth consent screen, **User Type** is External.

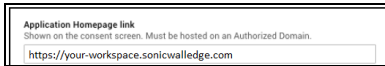


5. Click **Create**.

**Application Type** is **Public**, write down the **Application Name** (for example, SonicWall CloudEdge). You will need to add “sonicwall.com” into the “Authorized domains” list on “Credentials” -> “OAuth consent screen”.

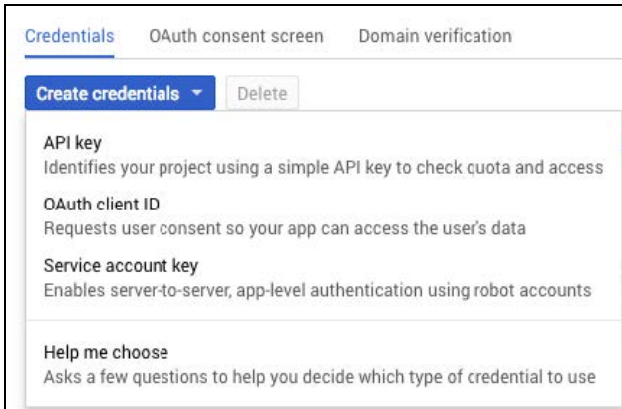


6. Fill in the application Homepage Link with your workspace URL and then select **Save**.



Application Homepage link  
Shown on the consent screen. Must be hosted on an Authorized Domain.

7. Google will take a moment to create your project. When the process completes, Google will prompt you to create the credentials you need.

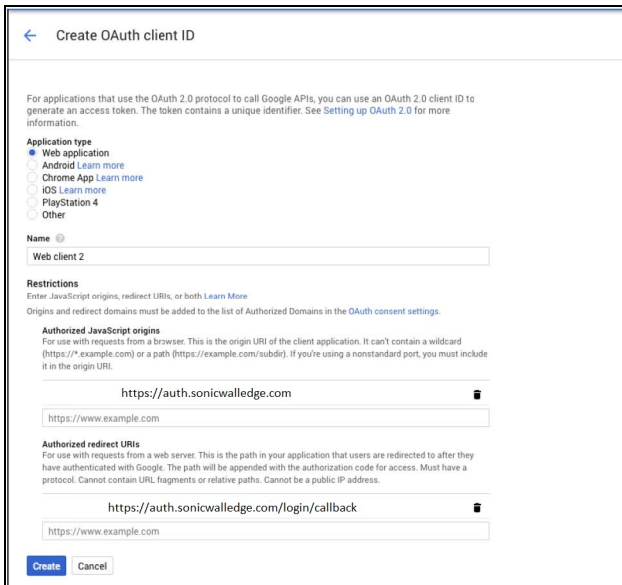


Credentials OAuth consent screen Domain verification

Create credentials Delete

- API key**  
Identifies your project using a simple API key to check quota and access
- OAuth client ID**  
Requests user consent so your app can access the user's data
- Service account key**  
Enables server-to-server, app-level authentication using robot accounts
- Help me choose**  
Asks a few questions to help you decide which type of credential to use

8. Select **Create credentials** to display a pop-up menu listing the types of credentials you can create. Select the **OAuth client ID** option.
9. At this point, Google will display a warning banner that says, "To create an OAuth client ID, you must first set a product name on the consent screen." Select the **Configure consent screen** to begin this process. Provide a **Product Name** that will be shown to users when they log in through Google.



← Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See [Setting up OAuth 2.0](#) for more information.

**Application type**

- Web application
- Android [Learn more](#)
- Chrome App [Learn more](#)
- iOS [Learn more](#)
- PlayStation 4
- Other

**Name**

**Restrictions**

Enter JavaScript origins, redirect URIs, or both. [Learn More](#)

Origins and redirect domains must be added to the list of Authorized Domains in the [OAuth consent settings](#).

**Authorized JavaScript origins**

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://\*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.

**Authorized redirect URIs**

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

Create Cancel

At this point, you will be prompted to provide additional information about your newly-created app.

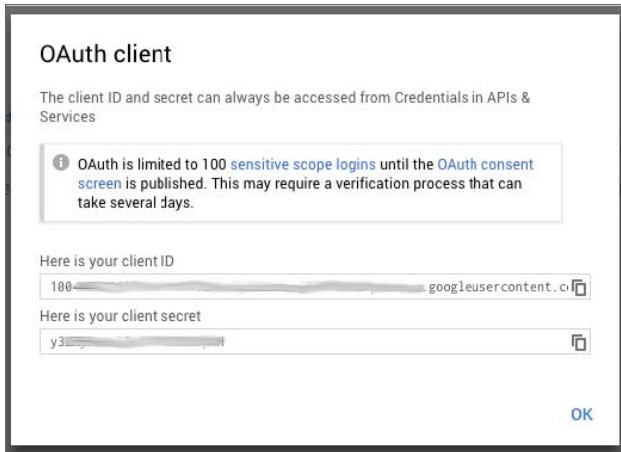
10. Select **Web application**, and enter SonicWall Cloud Edge as the name for the app.
11. Under **Restrictions**, enter the following information:



- Authorized JavaScript origins: <https://auth.sonicwalledge.com>
- Authorized redirect URI: <https://auth.sonicwalledge.com/login/callback>

12. Select **Create**. Your Client ID and Client Secret will be displayed.

Google may show an "unverified app" screen before displaying the consent screen for your app. To remove the unverified app screen, complete the [OAuth Developer Verification](#) process.

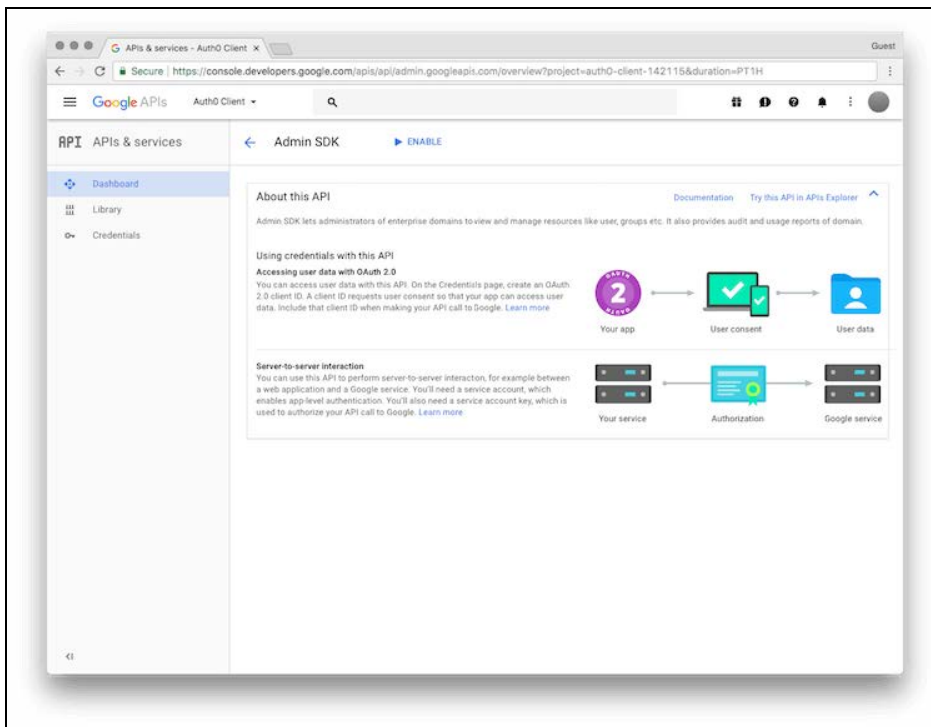


13. Save your **Client Id** and **Client Secret** in a separate location to enter later into the Connection settings in SonicWall Cloud Edge.

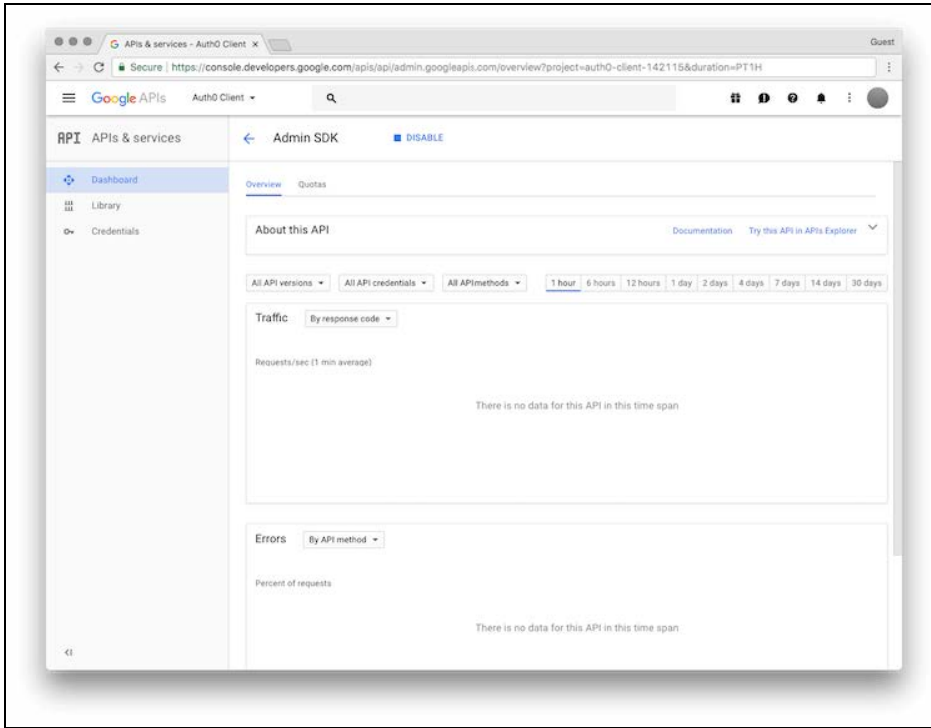
## Enabling the Admin SDK Service

If you are planning to connect to Google Suite enterprise domains, you will need to enable the Admin SDK service.

1. Navigate to the **Library** page of the API Manager.
2. Select **Admin SDK** from the list of APIs.

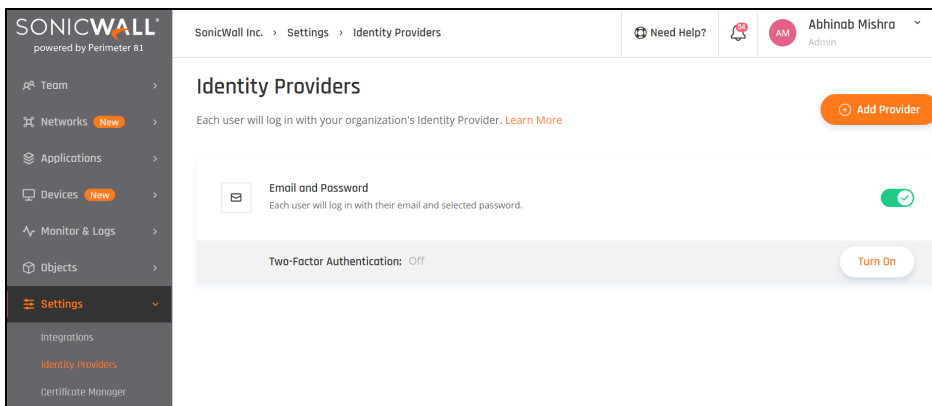


3. On the **Admin SDK** page, select **Enable**.

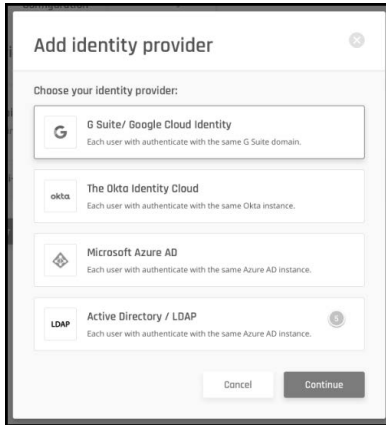


## Enabling and Configuring the Google Suite Connection

1. Log in to your SonicWall Cloud Edge Management Platform, and navigate to **Settings** and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Select **G Suite/Google Cloud Identity**.



4. Fill in the **Domain name**, **Domain aliases** (optional), **Google client ID**, and **Client secret**.

5. Select **Save**.
6. You will need to configure your settings so that your app can use Google's Admin APIs. If you're the administrator, you can select **Continue** on the Connection's Settings page to do so. If not, provide the URL you're given to your administrator so that the required settings can be adjusted.

① **NOTE:** Best practice is to authenticate this with a service user (such as it@<yourcompany>.com) with sufficient permissions. If the user leaves the organisation you will have to create new Client ID and Secret and then re-authenticate with a new user.

You're all set. Google Suite is now connected and users should be able to login with their GSuite account.

# Google Apps (SAML 2.0)

This article describes the two ways to set Google Suite as your identity provider: using **Google Service** or using **Google SAML applications**.

- Configuring Google Suite as your IdP using SAML
- Configuring SonicWall

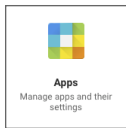
When choosing one over the other please keep in mind:

- While (at the moment) a SAML integration does not lead to any additional costs on Google's side, applying this configuration using Google Services may increase your Google Suite pricing, depending on your Google customer tier.
- A SAML integration enables you to force all users to authenticate using Google Suite, as opposed to setting up a Google Service which is more flexible and can be applied to particular groups of users only.

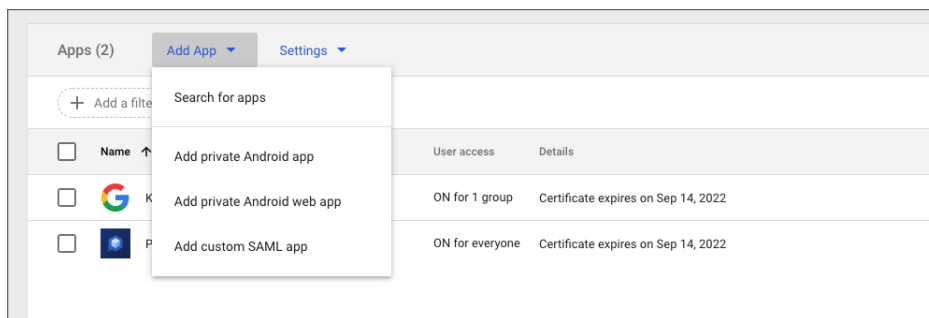
## Configuring Google Suite as your IdP using SAML

### Configuring the app at the G suite management console

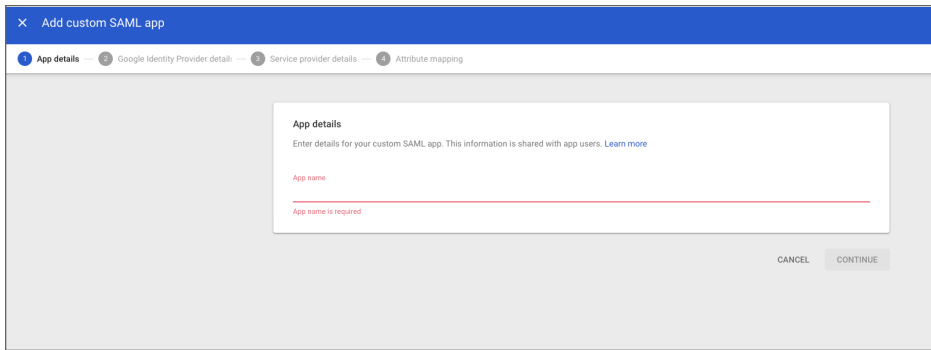
1. Open the G Suite management console.
2. Select **Apps**.



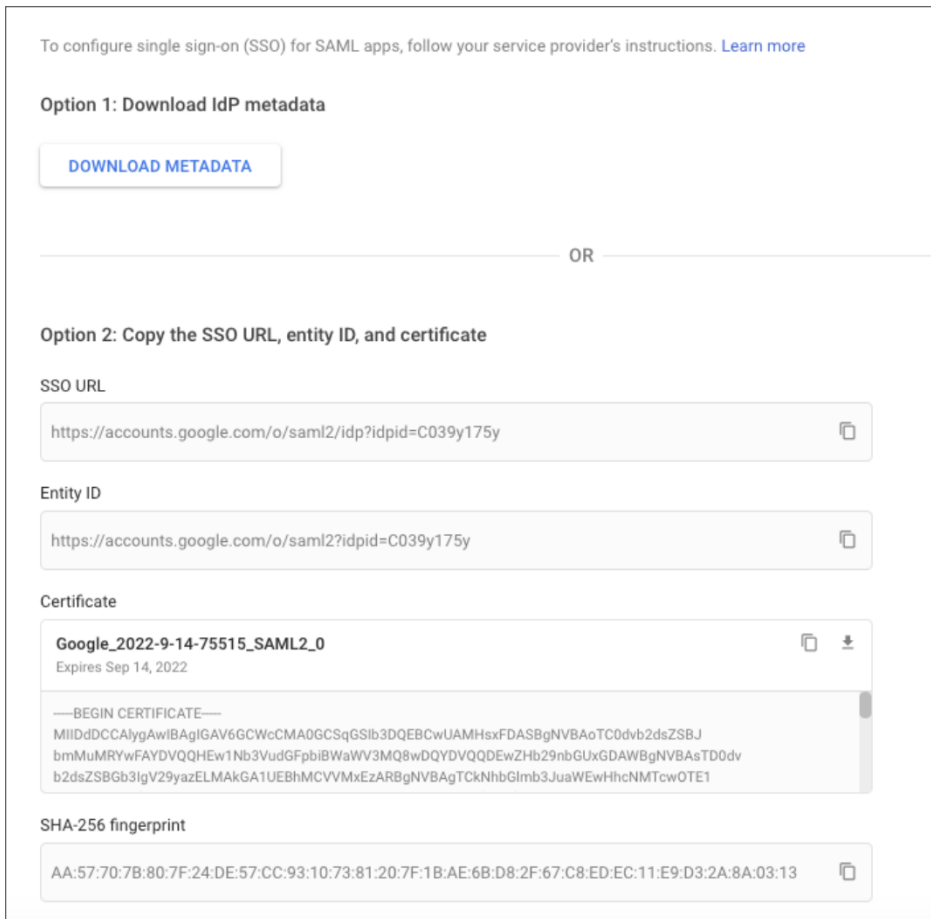
3. Select **Add custom SAML app**.



4. Enter an indicative name of your own choice.



5. Copy the SSO URL and download certificate, then select next.



6. Enter the desired name, description, and logo.

Step 3 of 5 X

### Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name \*  app-id: sonicwall

Description

Upload logo

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.

PREVIOUS CANCEL NEXT

7. Fill in the following information:

- **ACS URL** : <https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>
- **Entity URL** : urn:auth0:sonicwall-production:tenantname-oc
- Make sure to replace tenantname with your tenantname (for example, if you log in to the platform using *myworkspace.sonicwalledge.com*, replace {{WORKSPACE}} with my workspace )
- **Name ID**: Basic Information and Primary Email
- **Name ID Format**: UNSPECIFIED

Step 4 of 5 X

### Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL \*

Entity ID \*

Start URL

Signed Response

Name ID

Name ID Format

PREVIOUS CANCEL NEXT

8. Fill in the following attributes then select add mapping:

**Basic Information/Primary email:** email

**Basic Information/Last Name:** family\_name

**Basic Information/First Name:** given\_name

**Employee Details/Department:** groups

**Attributes**

Add and select user fields in Google Directory, then map them to service provider attributes. Attributes marked with \* are mandatory. [Learn more](#)

| Google Directory attributes          |   | App attributes |
|--------------------------------------|---|----------------|
| Basic Information ><br>Primary email | → | _____ X        |
| Basic Information ><br>Last name     | → | _____ X        |
| Basic Information ><br>First name    | → | _____ X        |
| Employee Details ><br>Department     | → | _____ X        |

[ADD MAPPING](#)

9. Once the application has been created select **Status**, and then turn it on for everyone.

Turn on **Sonicwall-demo** for everyone

› Sonicwall-demo will be turned ON for everyone in your domain.

These changes may take up to 24 hours to propagate to all users.

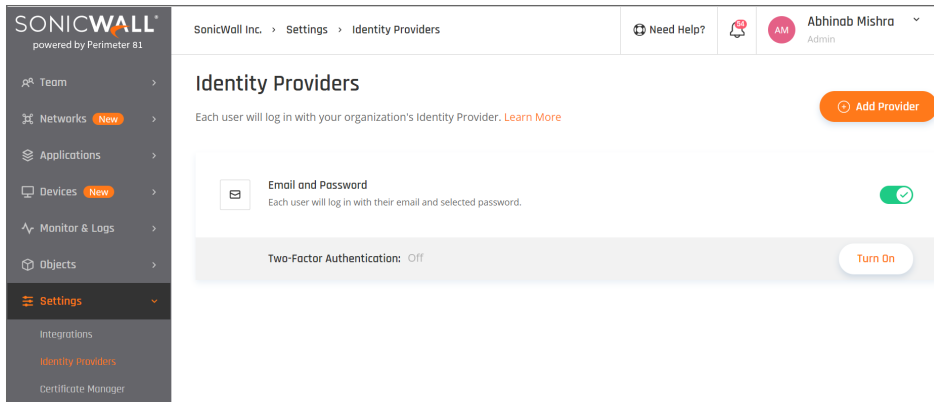
[CANCEL](#) [TURN ON FOR EVERYONE](#)

## Configuring SonicWall CloudEdge

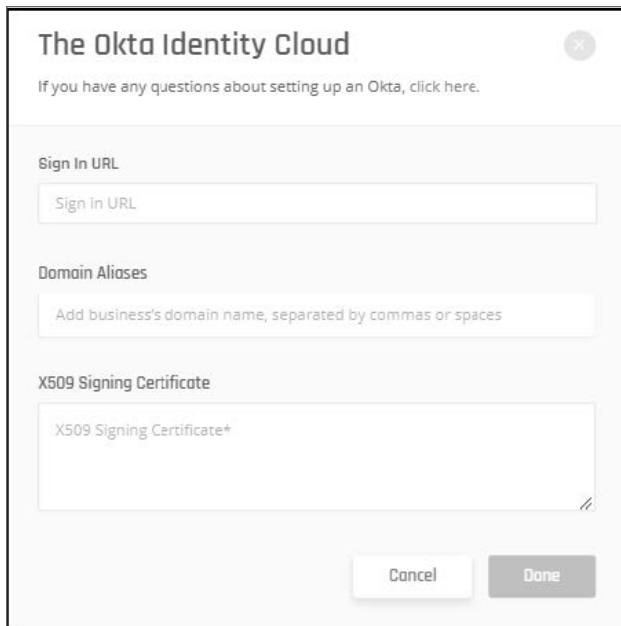
You need to configure the integration from the SonicWall CloudEdge side.

1. Log in to your Management Platform, navigate to **Settings**, and then **Identity Providers**.





2. Select **+ Add Provider**.
3. Select **Okta Identity Cloud**.
4. Fill in **SSO URL**.
5. Add your organization domain.
6. Paste the certification (begin and end line included).



6. Select **Done**.

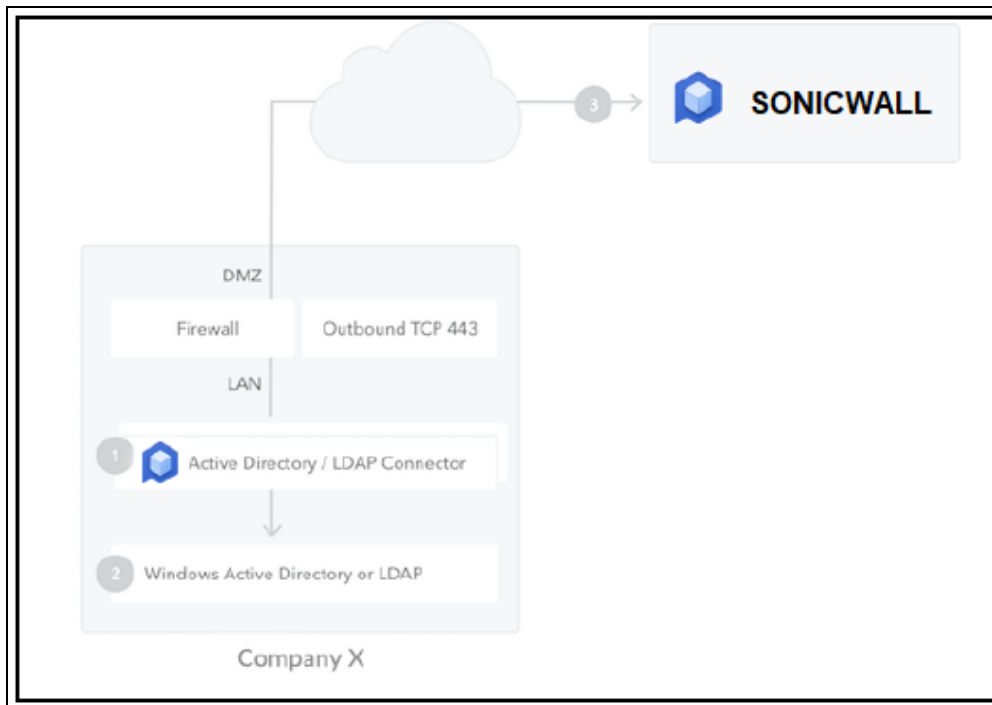
## On-Premises Active Directory

This article describes integration with Active Directory/LDAP through the Active Directory/LDAP Connector that you install on your network.

- The LDAP connector
- Enabling an AD/LDAP Connection
- Installing the connector on your network
- Access Error troubleshooting

## The LDAP connector

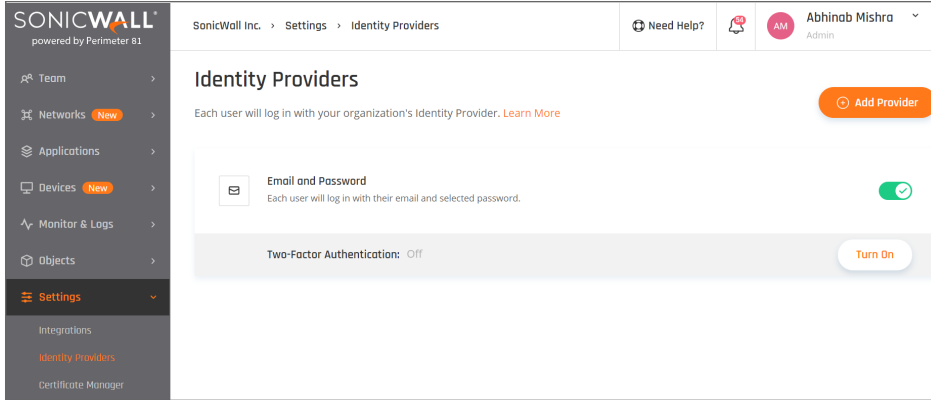
The AD/LDAP Connector (1), is a bridge between your Active Directory (2) and the Service (3). This bridge is necessary because AD is typically restricted to your internal network, and it is a cloud service running in a completely different context.



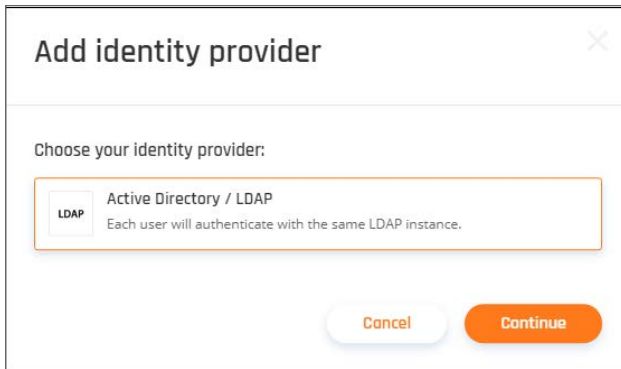
For high availability and load balancing, you can install multiple instances of the connector. All connections are outbound from the connector to the network, so changes to your firewall are generally unnecessary

# Enabling an AD/LDAP Connection

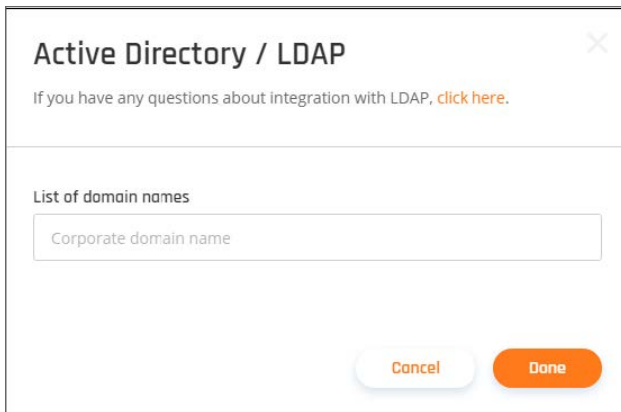
1. Log in to your Management Platform, and navigate to **Settings** and then **Identity Providers**.



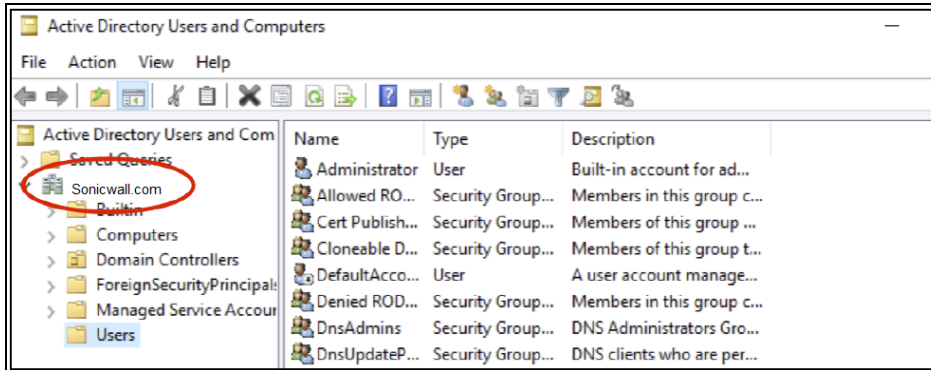
2. Select **+ Add Provider**.
3. Choose **Active Directory / LDAP** and select **Continue**.



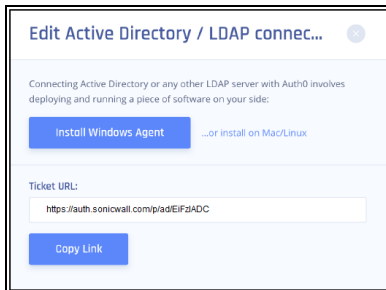
4. In the **List of domain names** field, list the user email domains that will be allowed to log in to this AD/LDAP connection. For example *sonicwall.com*.



If you are not sure what is your domain name, you can find it under **Active Directory Users and Computers**.



5. Select **Done**.



6. Download the **Install Windows Agent** on the next page to your machine. Make sure to keep the **TICKET URL** on hand as you will need it later.

## Installing the connector on your network

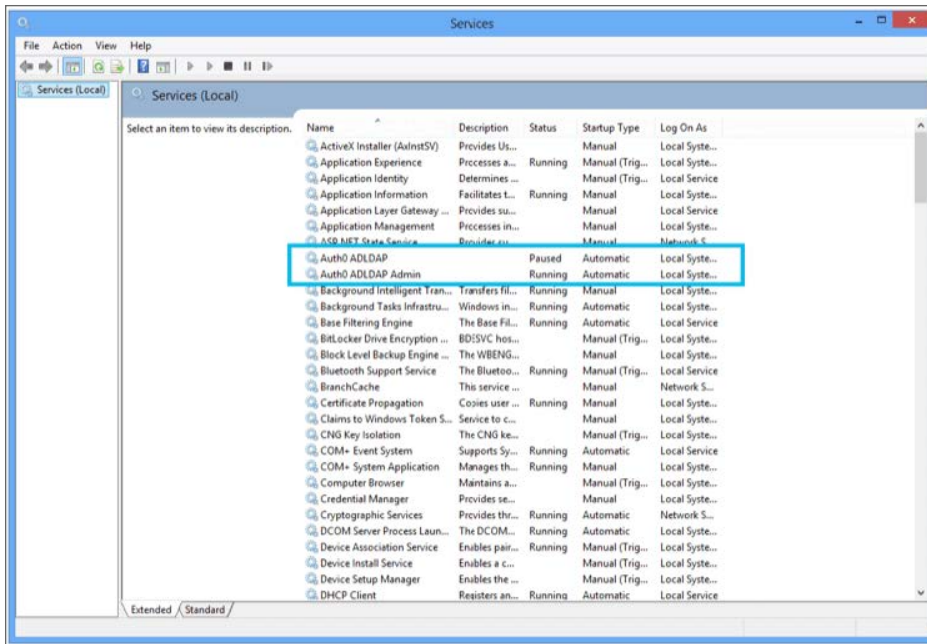
The Connector is packaged as a standard Microsoft Installer file (MSI).

### Run the installer

1. You will need to install the connector on the same machine that the Active Directory is running. Run the installer and follow the instructions:

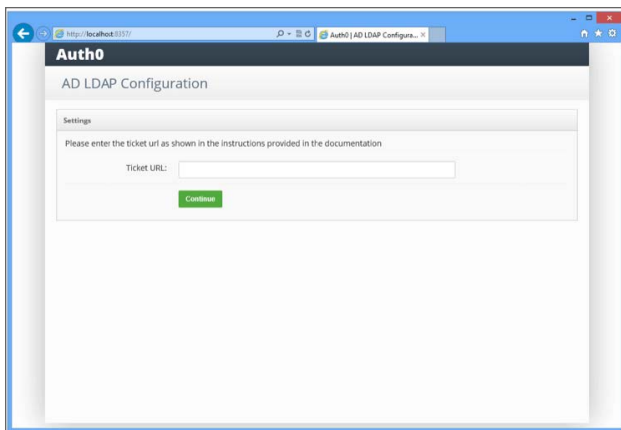


The AD/LDAP Connector in Windows is installed as a Windows Service:



### Link to SonicWall

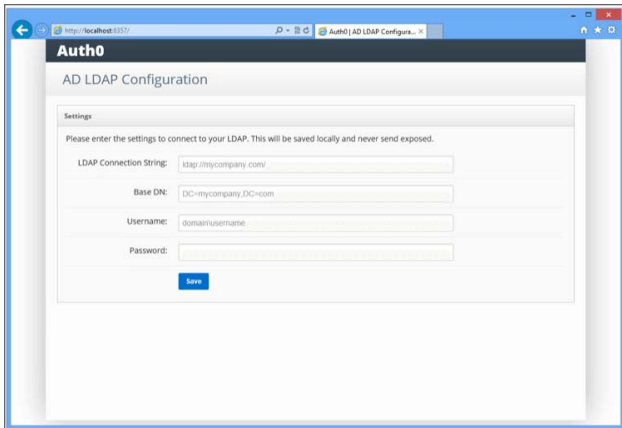
Once the installation is complete, you will see the following screen in a browser pointing to localhost:



2. Enter the **TICKET URL** provided when you provisioned the connection in the initial step above. The **TICKET URL** uniquely identifies this connector. The Connector will use this to communicate with our service and automatically complete the configuration
- ① **NOTE:** If you receive an "unable to get local issuer certificate" error, you need to set an environment variable `NODE_TLS_REJECT_UNAUTHORIZED` with value 0 in your Windows/Linux system, and then restart the two Auth0 services (further instructions [here](#)).

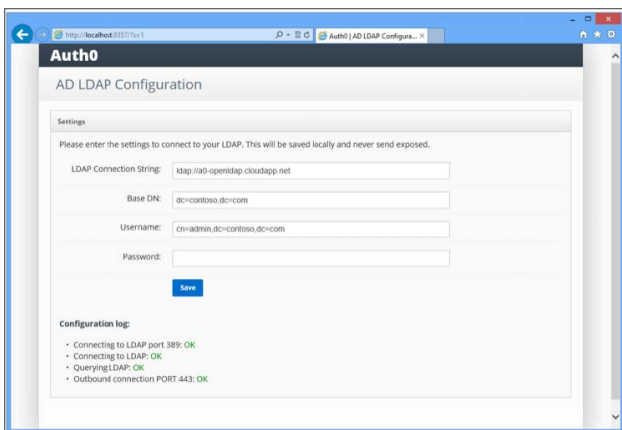
## Link to LDAP

1. Once you have entered the TICKET URL, you need to enter the LDAP settings:



- **LDAP Connection String (e.g., ldap://ldap.internal.acme.com):** This is the protocol + the domain name or IP address of your LDAP server. Your LDAP server is the local domain controller where Active Directory is installed. The protocol can be either LDAP or LDAPS. If you need to use LDAPS make sure that the certificate is valid in the current server (auto-populate).
- **Base DN (eg: dc=acme,dc=com):** This is the base container for all the queries performed by the connector (auto-populate).
- **Username (eg: cn=svcauth0,dc=services,dc=acme,dc=com):** The full name of a user with administrator rights to perform queries.
- **Password:** The password of that user.
- **No need to fill in any of the other fields.**

Once you submit the above information, the connector will perform a series of tests:



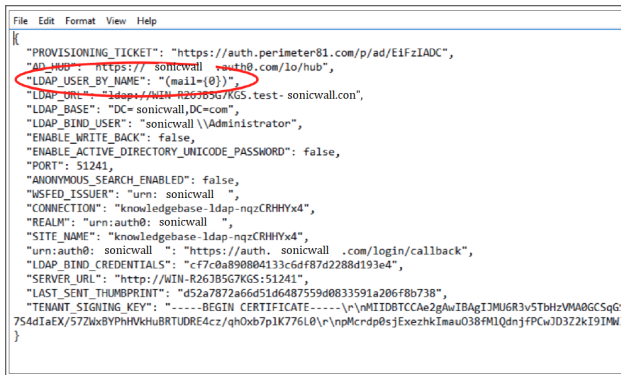
Make sure that all tests are in green.

2. Apply custom configuration to the connector config file.

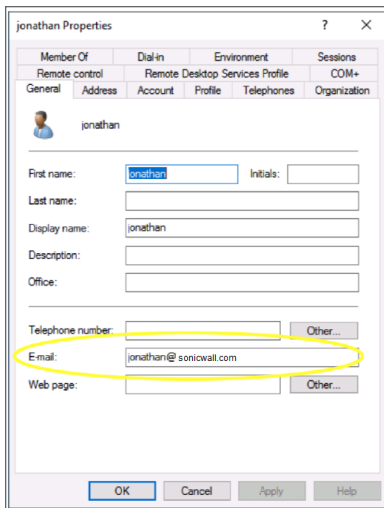
The config.json file is the AD/LDAP Connector's main configuration file. The file is located in the install directory for the AD/LDAP Connector, which (for Windows) is usually found at C:\Program Files (x86)\Auth0\AD LDAP Connector.

3. Add the following row into the json file (can be opened in any text editor) right after the second row:

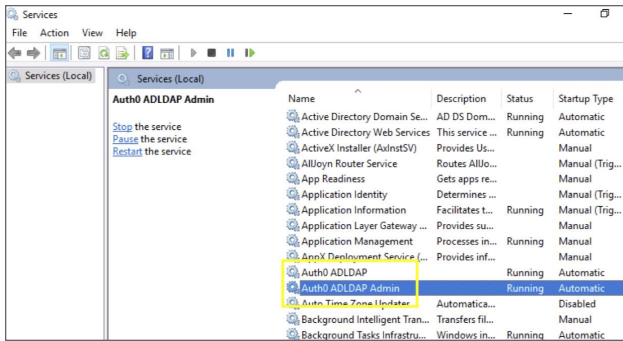
```
Shell '"LDAP_USER_BY_NAME": "(mail={0})",`
```



4. Save the config.json file.
5. Note: The integration will not be successful unless all users have their email addresses filled in.



6. Restart the AD/LDAP Connector service (the Auth0 ADLDAP and Auth0 ADLDAP Admin services in Windows).



Congratulations, your AD/LDAP is installed, connected and ready to use within SonicWall.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

## SAML 2.0

### Topics:

- [Generic SAML](#)
- [Active Directory Federation Services \(ADFS\)](#)
- [Auth0](#)
- [Okta](#)
- [OneLogin](#)
- [PingOne for Enterprise](#)
- [JumpCloud](#)

## Generic SAML

This article describes how SonicWall Cloud Edge allows users to authenticate against an external IdP using the Security Assertion Markup Language (SAML) protocol. The platform can automatically manage the IdP added **Members** and assign them to IdP correlating **Groups**.

- [Introduction to SAML](#)
- [Integration with a generic SAML IdP](#)
- [Configuring SonicWall Cloud Edge](#)

You can also review our integration guides for [Okta](#), [OneLogin](#), [PingIdentity](#), [ADFS](#), and other SAML IdPs.

## Introduction to SAML

SAML-based federation involves two parties:



An **identity provider (IdP)**: authenticates users and provides to Service Providers an Authentication Assertion if successful.

A **service provider (SP)**: relies on the Identity Provider to authenticate users. SonicWall Cloud Edge supports the SAML protocol and can serve as the service provider for users that are authenticated by different IdPs.

During the login process, **Members** will be redirected to the IdP in order to authenticate. Once the user is authenticated, the SonicWall Cloud Edge will get a SAML assertion and associate the **Member** with the appropriate role and policies.

## Integration with a SAML IdP

In order to integrate with a SAML IdP, you will need to create a dedicated SonicWall Cloud Edge application within your SAML IdP.

Most of the IdPs will require the following information when creating a new application:

- **Single sign-on URL**: `https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc`
- **Audience URI (SP Entity ID)**: `urn:auth0:sonicwall-production:tenantname-oc`

① | **NOTE**: Remember to replace `tenantname` with your actual tenant name

In order to map the IdP members correctly the following attributes have to be passed to the platform:

| IdP Attribute | SonicWall Cloud Edge Mapping |
|---------------|------------------------------|
| Email Address | email                        |
| First Name    | given_name                   |
| Last Name     | family_name                  |

Should you require to pass group memberships to SonicWall Cloud Edge:

| IdP Object | SonicWall Cloud Edge Mapping |
|------------|------------------------------|
| Groups     | groups                       |

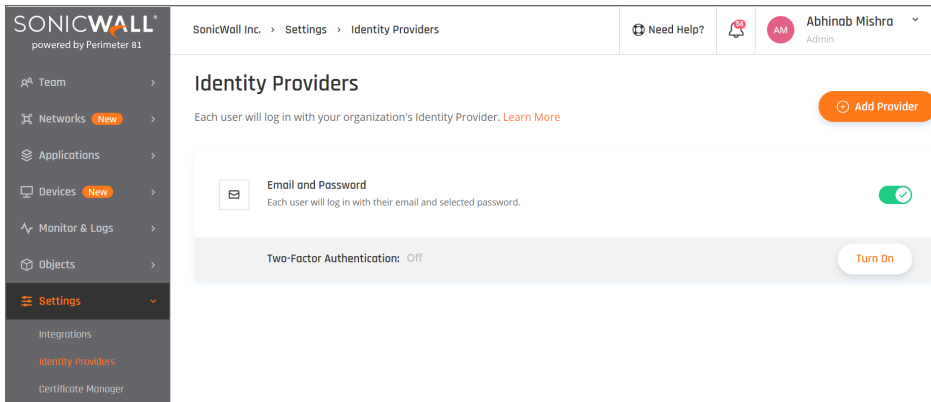
Once the application is created you'll be provided with the following information:

- **X.509 Certificate**
- **IdP Sign-in URL**

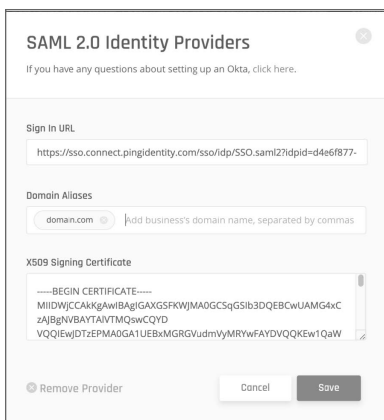
## Configuring SonicWall Cloud Edge

You need to configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge **Management Platform**, and navigate to **Settings** and then **Identity Providers**.
2. Select **+ Add Provider**.



3. Select **SAML 2.0 Identity Cloud**.
4. Fill in the **Sign In URL** provided by the IdP.
5. Add your organization domains.
6. Paste the X.509 Certificate provided by the IdP.



7. Select **Save**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

## Active Directory Federation Services (ADFS)

This article describes how to configure ADFS to use as an [identity provider](#) for SonicWall Cloud Edge.

- Configuring ADFS
- Editing the claim issuance policy
- Exporting the signing certificate

- Configuring the ADFS connection at the Management Platform
- Access Error troubleshooting

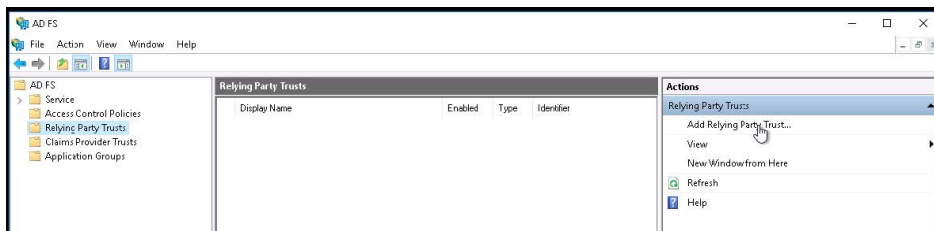
Please follow the steps below:

## Configuring ADFS

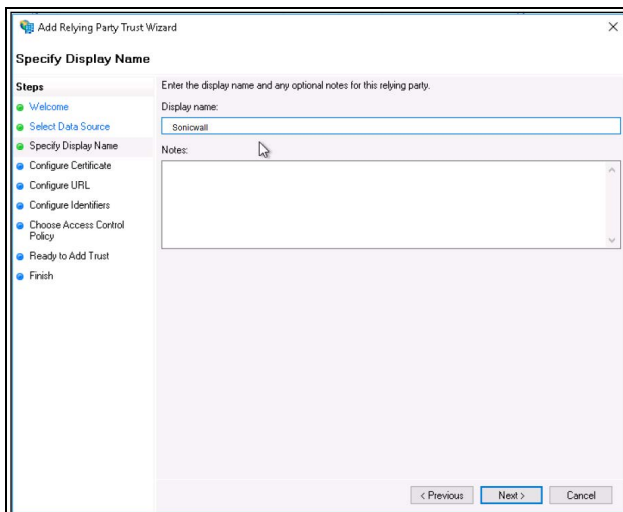
### Adding a Relying Party Trust

See [Create a relying party trust](#) for complete details.

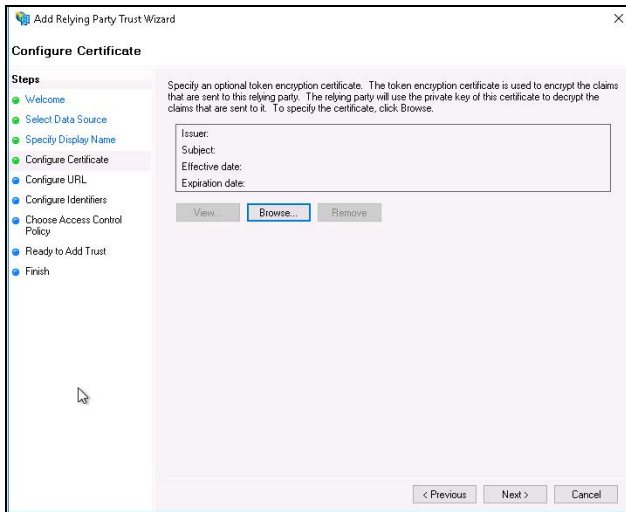
Launch your instance of ADFS and start the **Add Relying Party Trust** wizard.



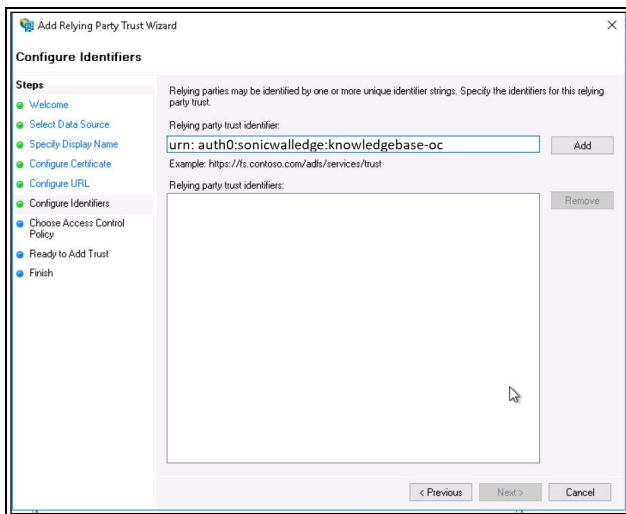
1. On the **Welcome** page, choose **Claims aware** and click **Start**.
2. On the **Select Data Source** page, select **Enter data about the relying party manually** and click **Next**.
3. On the **Specify Display Name** page, provide a descriptive name for your relying party (the typical name is SonicWall Cloud Edge) and a brief description under **Notes**. Click **Next**.



4. On the **Configure Certificate** page, click **Next**.



5. On the **Configure URL** page, check the box for **Enable support for the SAML 2.0 WebSSO protocol**.
6. Set **Relying party SAML 2.0 SSO service URL** to `https://{{YOUR.ADFS.DOMAIN}}/login/callback?connection={{WORKSPACE}}-oc` . Click **Next** .
7. On the **Configure Identifiers** page, set the **Relying party trust identifier** to `urn:auth0:sonicwalledge:{{WORKSPACE}}-oc`. Click **Add** and **Next**.

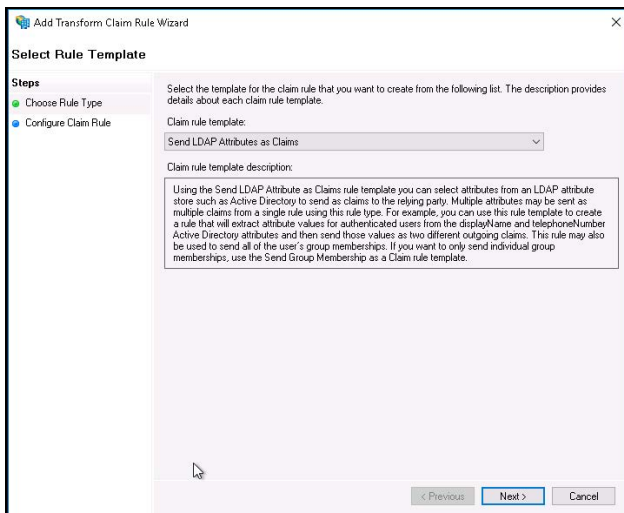


8. On the **Choose Access Control Policy** page, select **Permit everyone** and click **Next**.
9. Review the settings you provided on the **Ready to Add Trust** page and click **Next** to save your information. If you were successful, you'll see a message indicating that on the **Finish** page.
10. Make sure that the **Configure claims issuance policy for this application** checkbox is selected, and click **Close**.

## Editing the claim issuance policy

After you close the **Add Relying Party Trust** wizard, the **Edit Claim Issuance Policy** window appears.

1. Click **Add Rule...** to launch the wizard.
2. Select **Send LDAP Attributes as Claims** for your **Claim rule template**, and click **Next**.



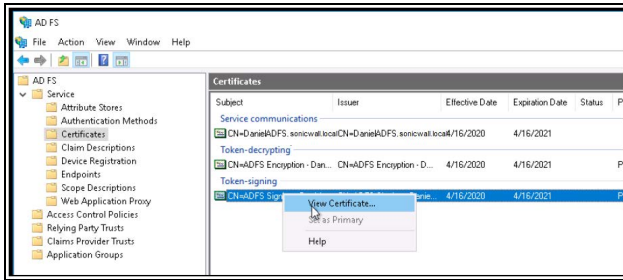
3. Provide a value for the **Claim rule name**, such as "LDAP Attributes" (it can be anything you want).
4. Choose **Active Directory** as your **Attribute Store**.
5. Map your LDAP attributes to the following outgoing claim types:

|                                |             |
|--------------------------------|-------------|
| E-mail Addresses               | email       |
| Given-Name                     | given_name  |
| Surname                        | family_name |
| Token-Groups Unqualified-Names | groups      |
| User-Principal-Name            | user_id     |

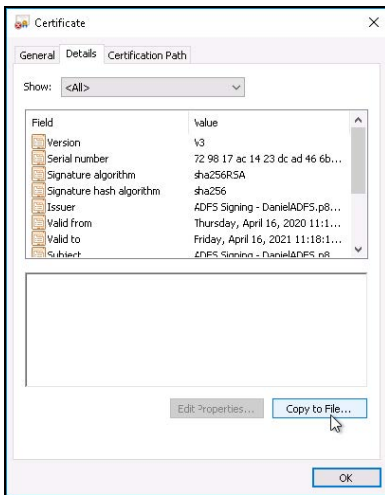
6. Click **Finish**.
7. In the **Edit Claim Issuance Policy** window, click **Apply**. You can now exit out of this window.

## Exporting the signing certificate

1. Using the left-hand navigation pane, go to **ADFS > Service > Certificates**.
2. Select the **Token-signing** certificate, and right-click to select **View Certificate**.



3. On the **Details** tab, click **Copy to File...**



4. In the **Certificate Export Wizard** Click **Next**.
5. Choose **Base-64 encoded X.509 (.CER)** . Click **Next**.

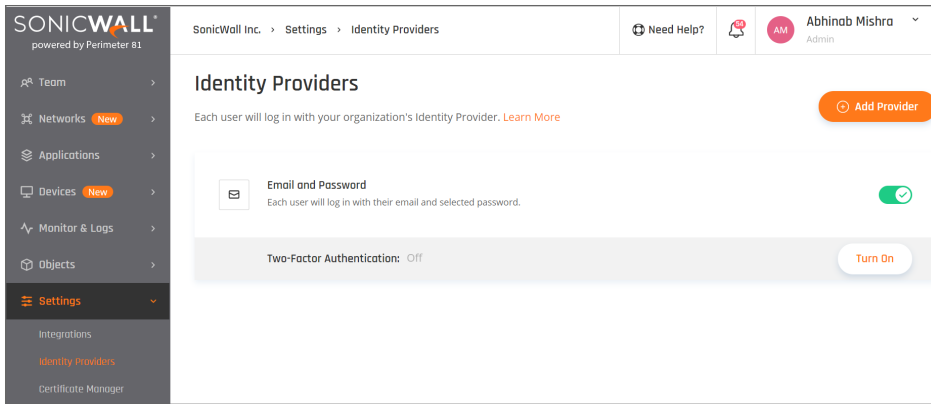


6. Provide the location for the certificate to be exported. Click **Next**.
7. Verify that the certificate and click **Finish**.

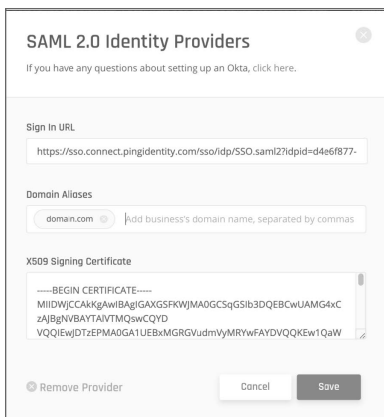
## Configuring the ADFS connection at the Management Platform

At this point, you will configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge **Management Platform**, and navigate to **Settings** and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Choose **SAML 2.0 Identity Providers**.
4. Sign In URL: **https://{{YOUR.ADFS.DOMAIN}}/adfs/ls**.
5. Add your organization domain.
6. Open the **ADFS X.509 certificate** file in a UNIX operating system and paste its content into the **X509 Signing Certificate** box.



7. Select **Save**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

## Auth0

This article describes how to configure Auth0 for use as an [identity provider](#) for SonicWall Cloud Edge.

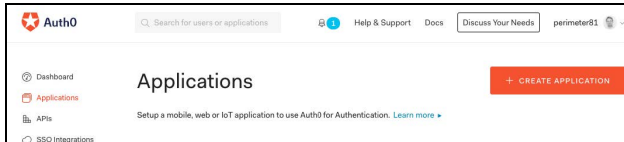
- Configuring the Auth0 SSO application
- Configuring Auth0 at the Management Platform

- Access Error troubleshooting

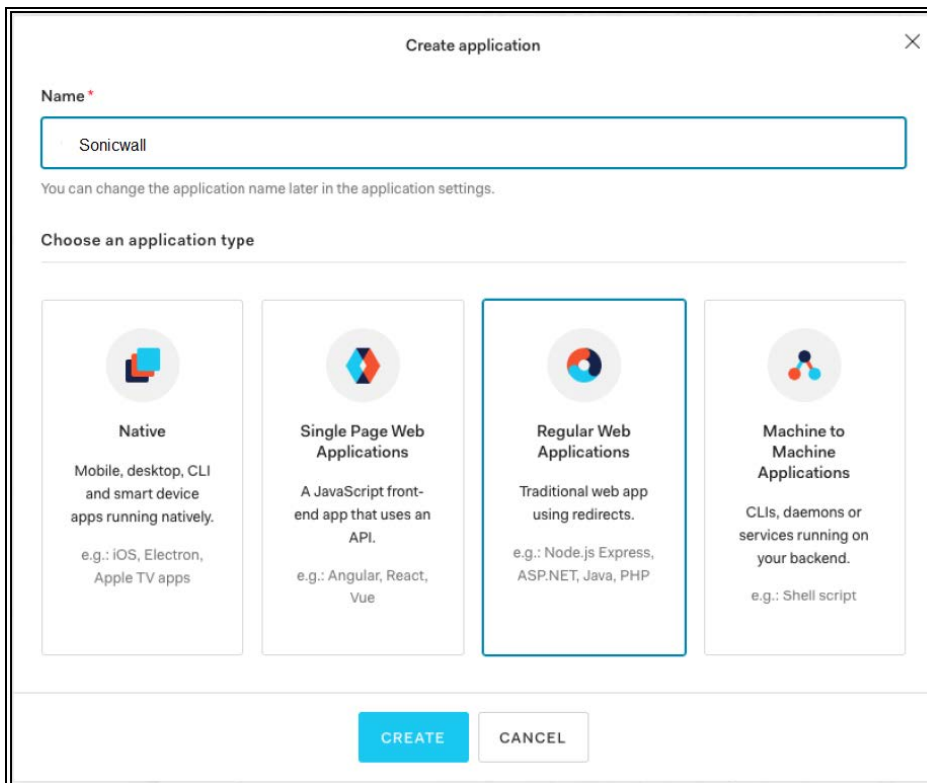
Please follow the steps below:

## Configuring the Auth0 SSO application

1. Open the [Auth0 Administrator Console](#).
2. Select **Applications** in the main navigation panel.
3. Select the **+ Create Application** on the upper side of the screen.

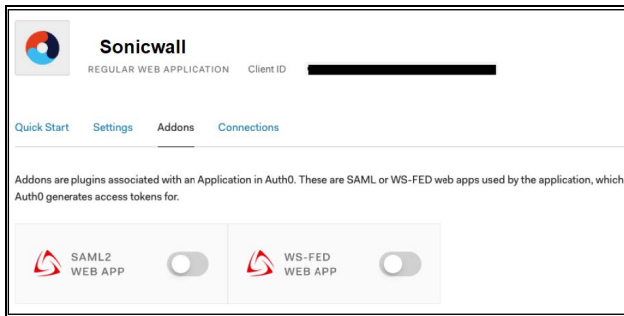


4. Add SonicWall Cloud Edge as the name of your Application.
5. Select the **"Regular Web Application"** type, and click on **Create**.



6. Navigate to **"Addons"** and turn on the **"SAML2 Web App"** toggle.



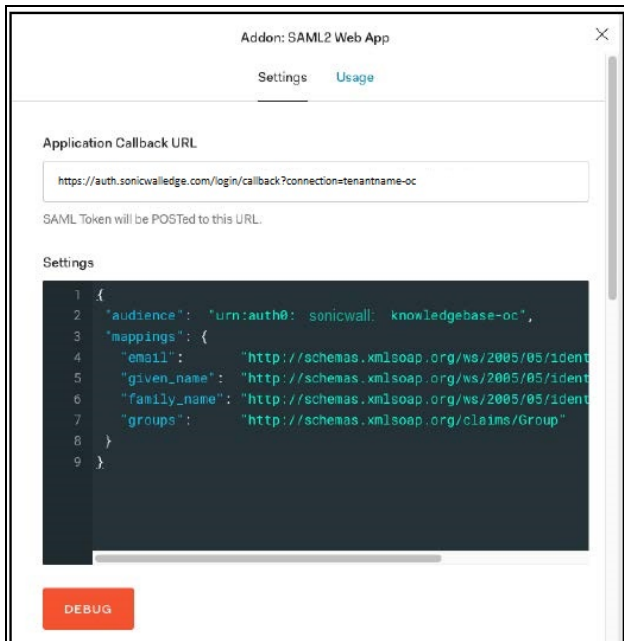


7. In the Addon: **SAML2 Web App** window:

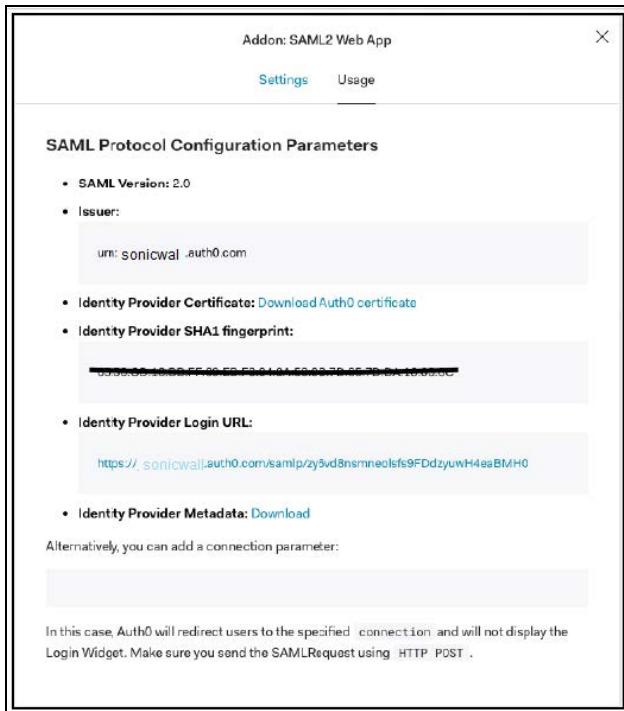
- **Application Callback URL** :Enter <https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>
- **Settings**: Copy the following configuration`**:**`

```
{  
  "audience": "urn:auth0:connector: **tenantname** -oc",  
  "mappings": {  
    "email": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress",  
    "given_name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname",  
    "family_name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname",  
    "groups": "http://schemas.xmlsoap.org/claims/Group"  
  }  
}
```

① | **NOTE:** Remember to replace the tenantname with your actual tenant name.



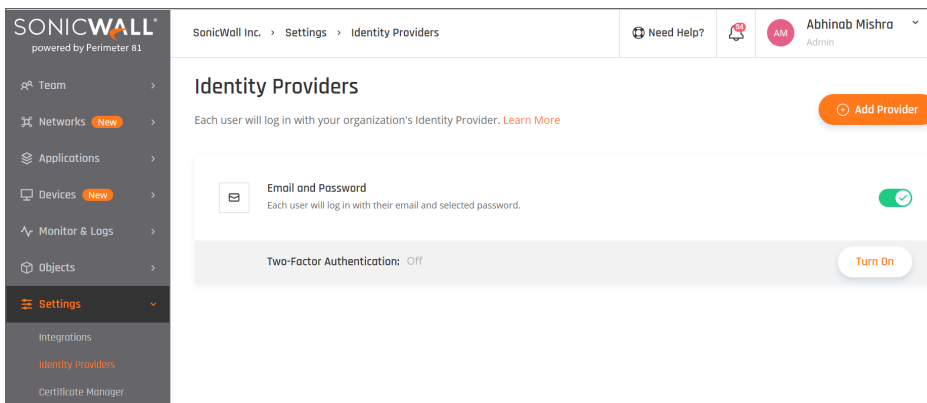
8. Click **Enable** to save and activate the Application.
9. Click on **Debug** and verify your configuration.
10. Navigate to **Usage**.
11. Click on **Download Auth0 certificate**.
12. Write down the **Identity Provider Login URL**.



## Configuring Auth0 at the Management Platform

At this point, you will configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge Management Platform, and navigate to **Settings** and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Choose **SAML 2.0 Identity Providers**.
4. Sign In URL: **Identity Provider Login URL**
5. Add your organization domain.

6. Open the **Auth0 certificate** file and paste its content into the **X509 Signing Certificate** box.

**SAML 2.0 Identity Providers**

If you have any questions about setting up an Okta, click [here](#).

**Sign In URL**

https://sso.connect.pingidentity.com/sso/dp/SSO.saml2?dpid=44e6f877-

**Domain Aliases**

doman.com Add business's domain name, separated by commas

**X509 Signing Certificate**

```
-----BEGIN CERTIFICATE-----
MIIDWjCCAKgAwIBAgIjGAXGSFKWJMA0GCSjSb3DQEBCwUAMG4xC
zAJBgNVBAYTAjVMTQswCQYD
VQQIEwJDTzEPMADGA1UEBxMGRGVudmVjMRwFAFYDVQKKEw1QaW
```

Remove Provider

Cancel Save

7. Select **Save**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

## Okta

This article describes how to set Okta as your [identity provider](#).

- Configuring your Okta account
- Configuring SonicWall Cloud Edge
- Access Error troubleshooting

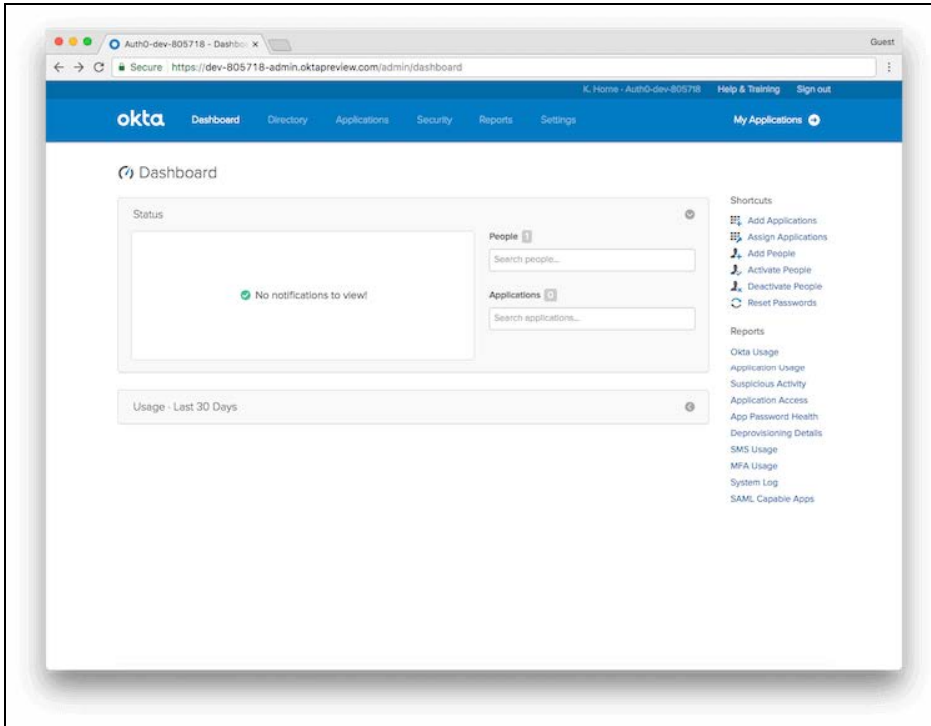
Please follow the steps below:

**NOTE:** To successfully integrate Okta and SonicWall Cloud Edge you must have admin access in both platforms.

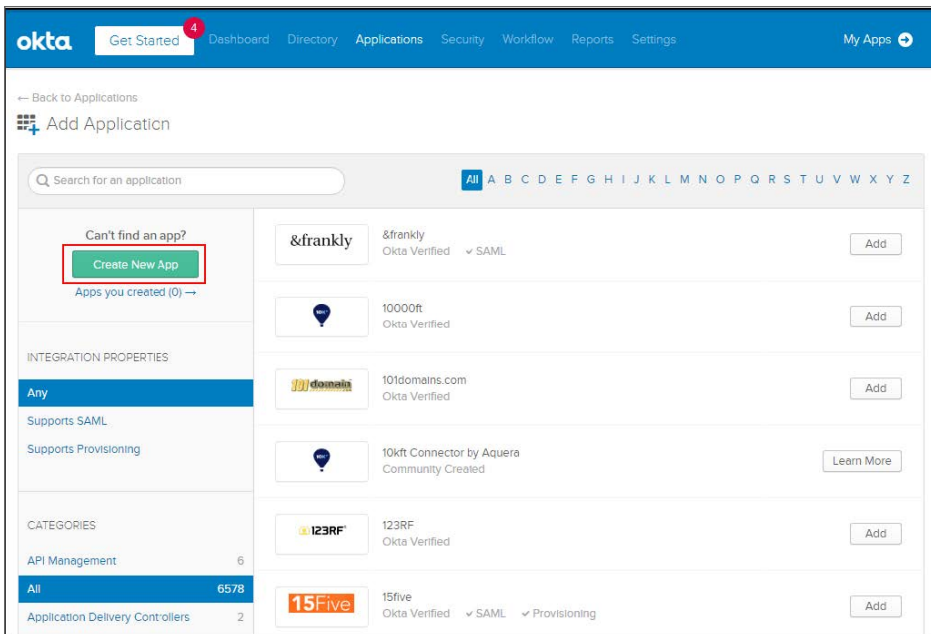
## Configuring your Okta account

1. Log in to your Okta account.
2. On the general Okta dashboard, select **Dashboard**. This takes you to the **Okta Admin Dashboard**.

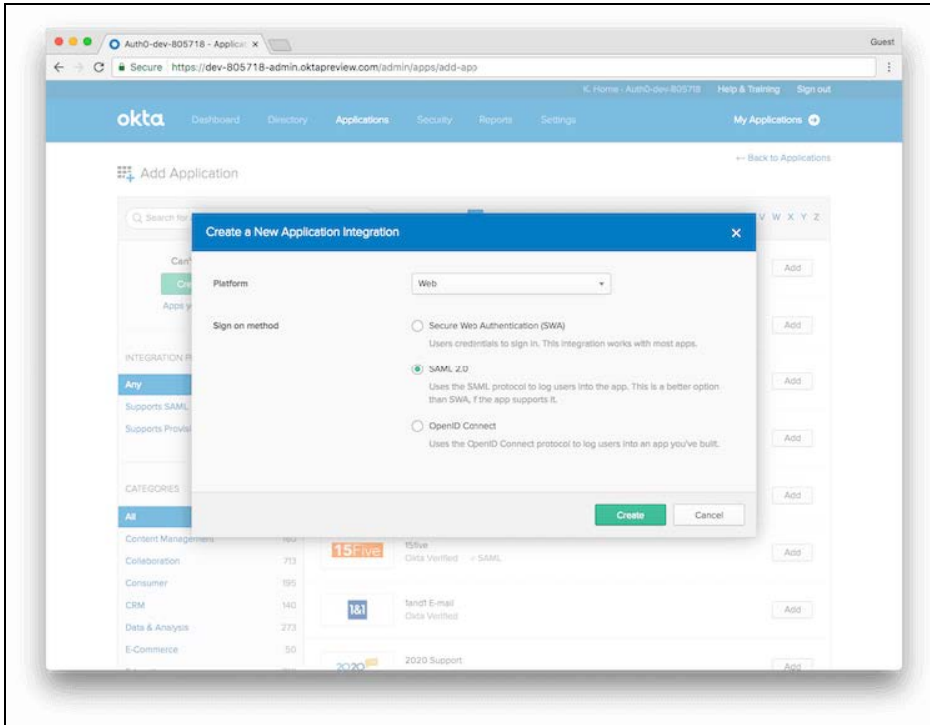
- Using the list of shortcuts at the right-hand side of the screen, select **Add Applications**.



- On the **Add Application** page, select **Create New App**.

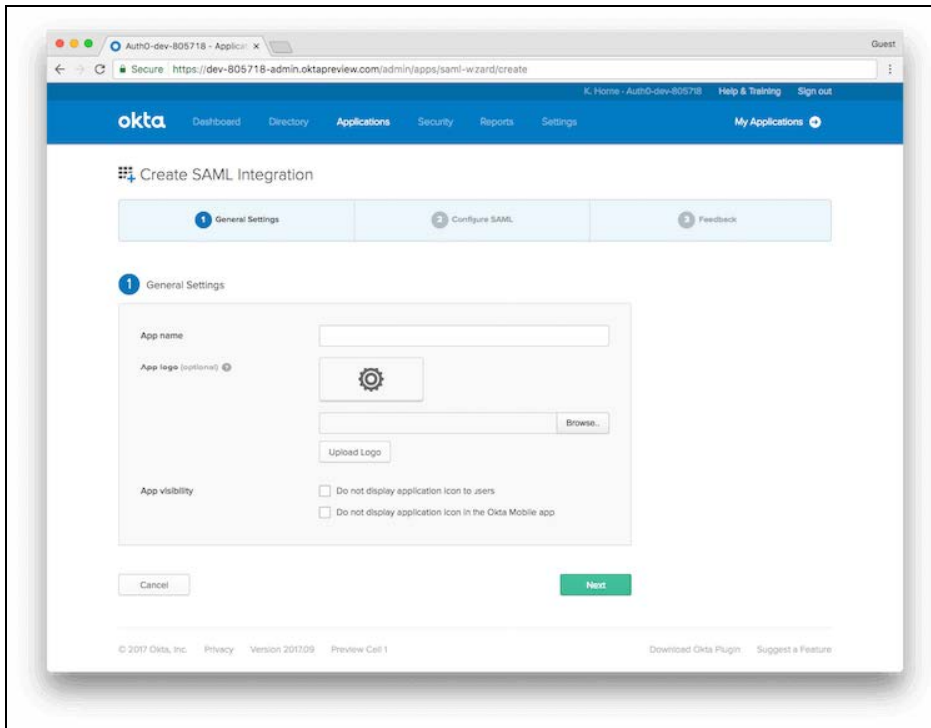


5. On the **Create a New Application Integration** pop-up window, select **Web** as the **Platform** for your application and choose **SAML 2.0** as the sign-on method. Select **Create** to proceed.

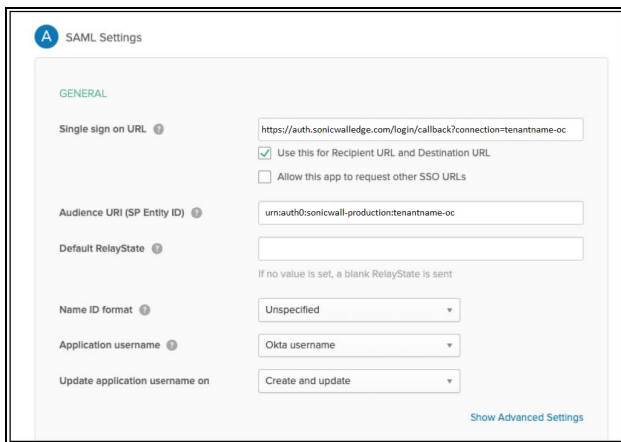


6. You will now create your SAML integration. On the **General Settings** page, provide the following:
  - **App name:** Your choice
  - **App Logo:** (Optional)
  - **App visibility:** select whether you want your users to see your application icon and in what settings.

7. Select **Next** to proceed.



8. Next, you will see the SAML Settings page. Enter the following values into the appropriate fields:  
**Single sign-on URL** : <https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>  
**Audience URI (SP Entity ID)**: urn:auth0:sonicwall-production:tenantname-oc  
For example, `tenantname.sonicwalledge.com workspace` should translate to `urn:auth0:sonicwall:tenantname-oc`



9. You will also need to add the following Attributes Statement:

- **Name**: email
- **Name format (optional)**: Unspecified

- **Value:** \${user.email}
- **Name:** given\_name
- **Name format (optional):** Unspecified
- **Value:** \${user.firstName}
- **Name:** family\_name
- **Name format (optional):** Unspecified
- **Value:** \${user.lastName}

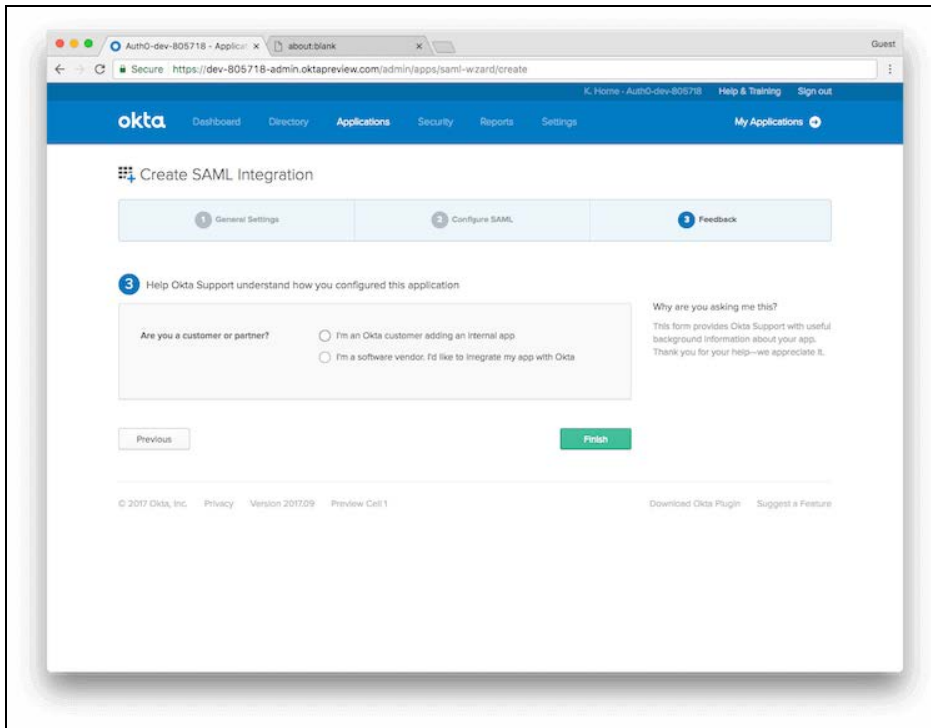
10. Now add the Group Attribute statement:

- **Name:** groups
- **Name format (optional):** Unspecified
- **Filter type:** Matches regex
- **Value:** .\*

11. You can select **Preview the SAML assertion** to generate an XML file that can be used to verify that your provided settings are correct.
12. Select **Next** to proceed.
13. Finally, answer **Are you a customer or partner?** by selecting **I'm an Okta customer adding an internal app.**

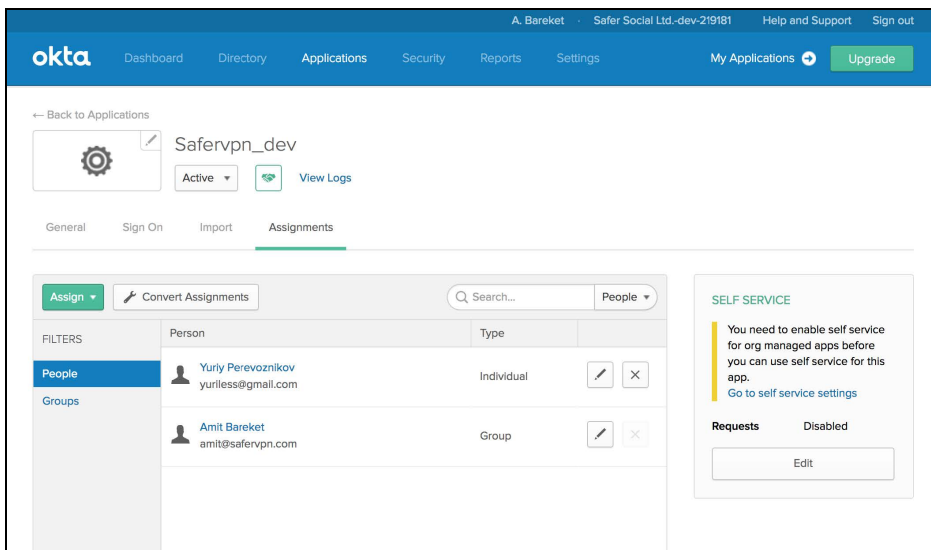


14. Select **Finish** (filling in the questions on this page is not mandatory).

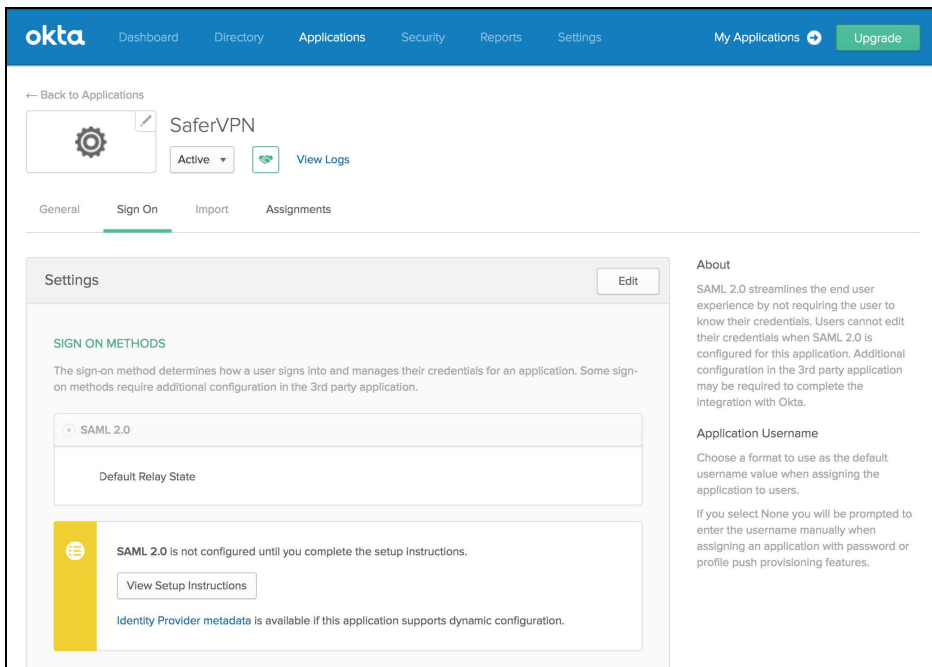


You'll be directed to the **Sign-On** page for your newly-created app.

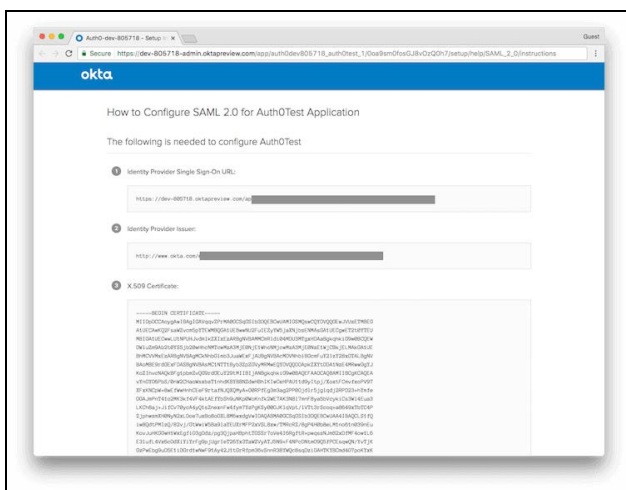
15. Select **Assignment** then **Assign** to create either groups or individual assignments from your Identity Provider to the application (this will determine who can access it).



16. Select **Sign-On** and then **View Setup Instructions** to complete the process.



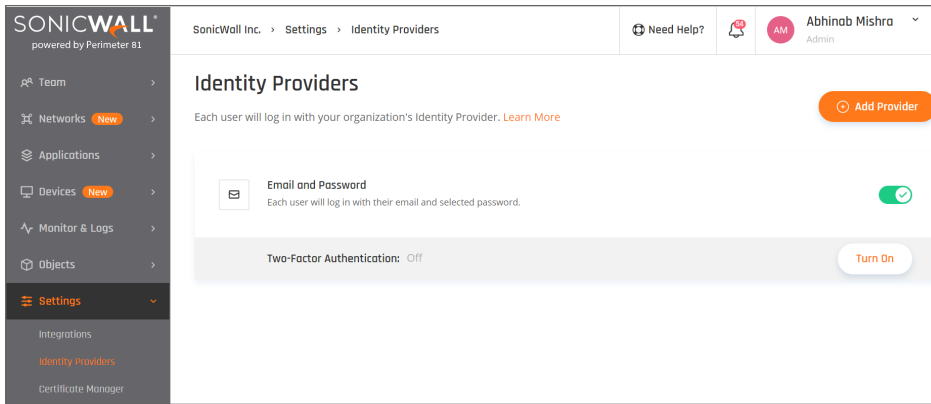
17. Take note of the **Identity Provider Single Sign-On URL**, and download or copy the **X.509 certificate**.



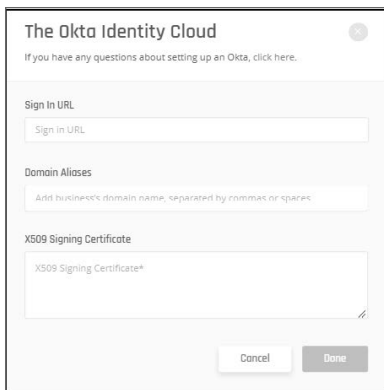
## Configuring SonicWall

You need to configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge **Management Platform**, and navigate to **Settings** and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Select **Okta Identity Cloud**.
4. Fill in Sign In URL and X.509 Signing Certificate you previously copied.
5. Add your organization domain.



6. Select **Done**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

## OneLogin

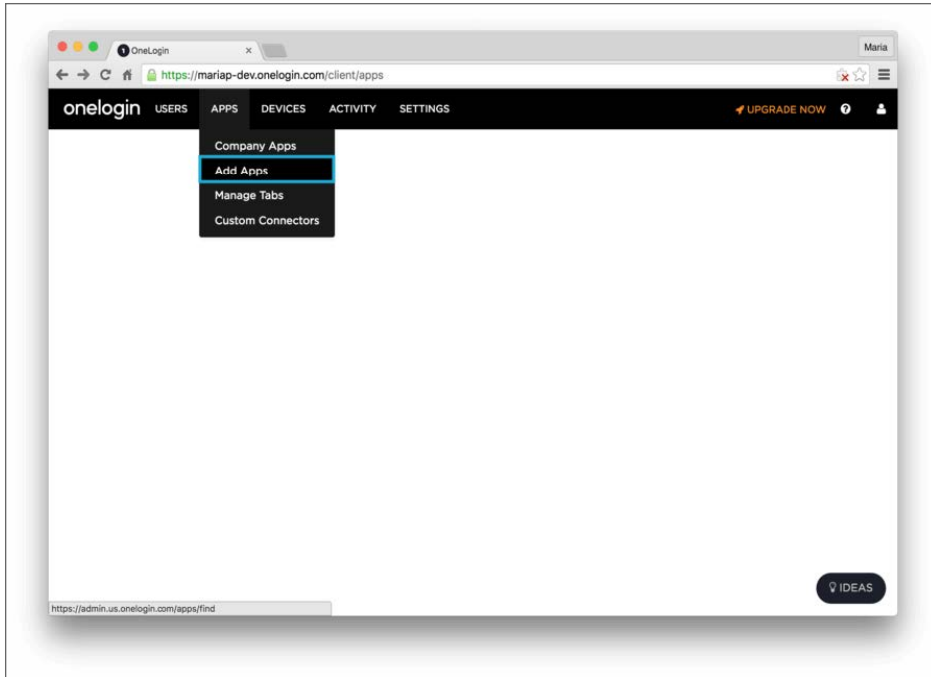
This article describes how to configure OneLogin for use as an **identity provider** for SonicWall.

- Configuring OneLogin
- Configuring SonicWall
- Access Error troubleshooting

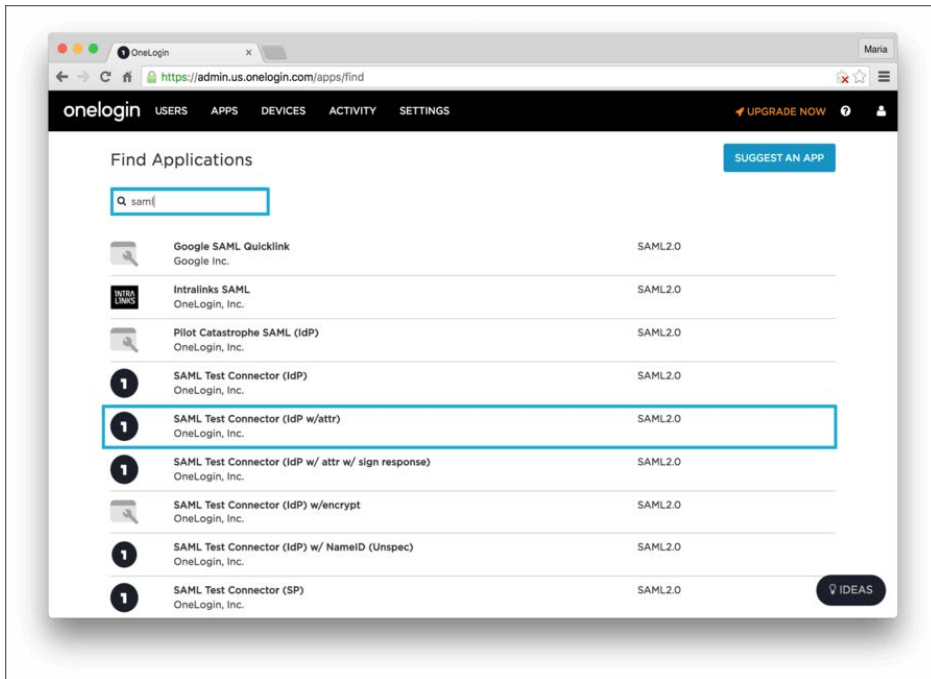
Please follow the steps below:

## Configuring OneLogin

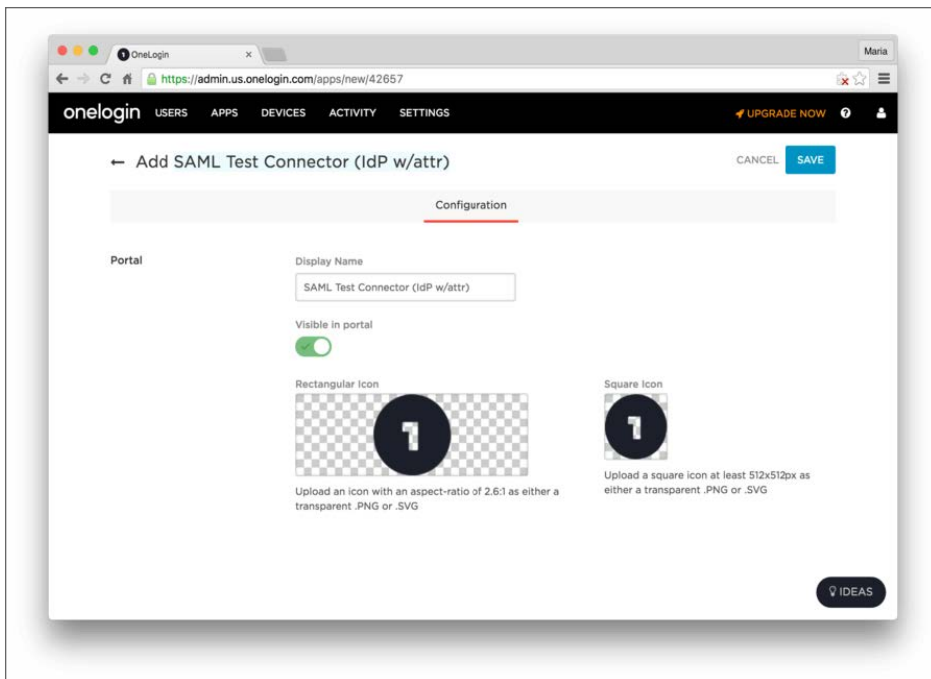
1. Log in to your OneLogin account. If you don't already have one, you will need to create one.
2. Select **Apps** and then **Add Apps**.



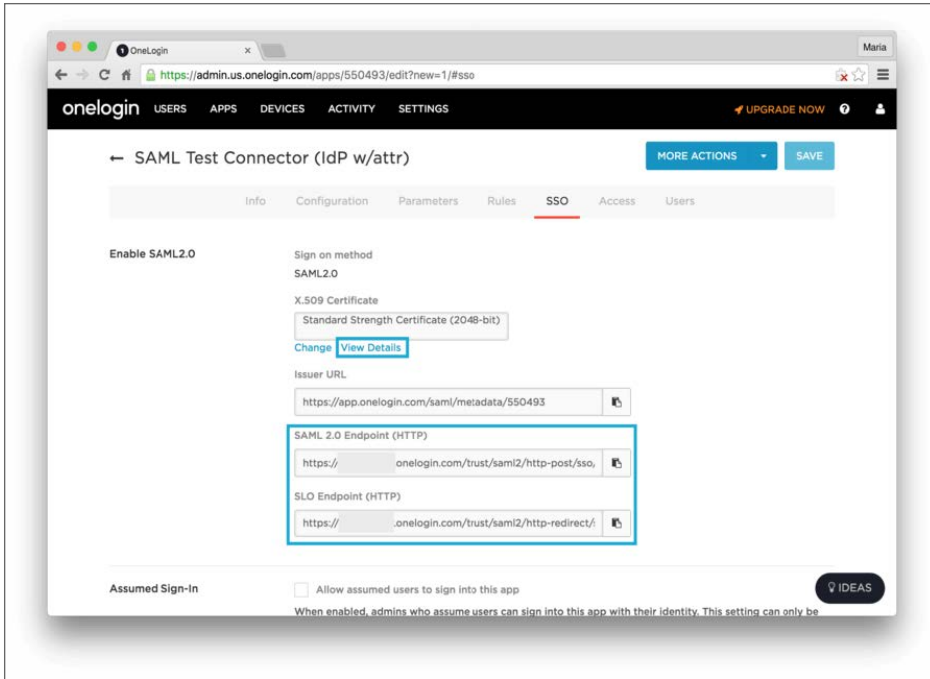
3. Search for saml, and select SAML Test Connector (IdP w/attr).



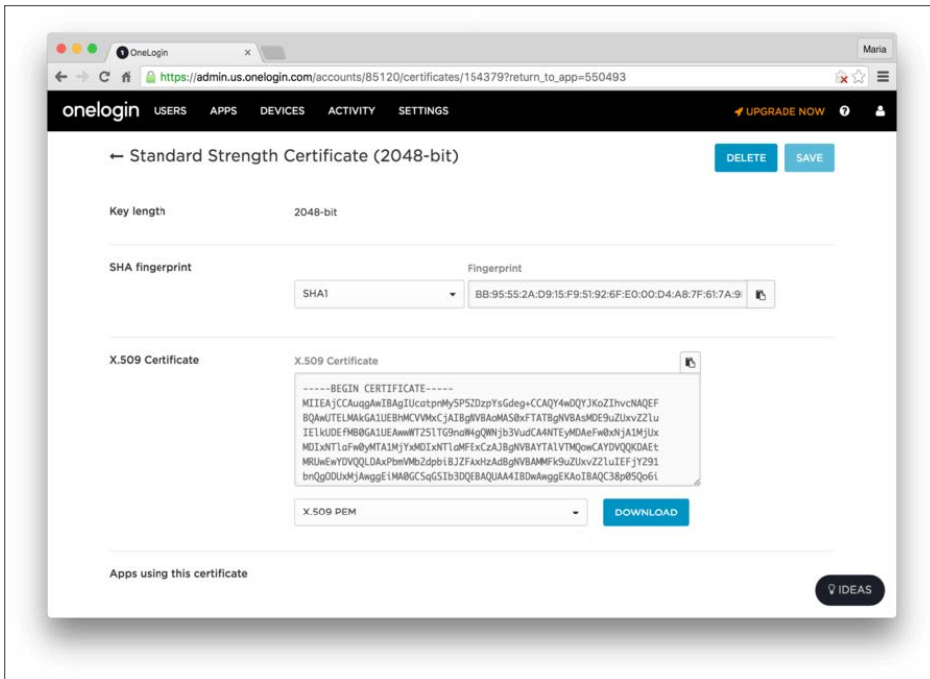
4. Change the **Display Name** to Connector. Select **Save**.



5. Go to the **SSO** tab, and copy the values for **SAML 2.0 Endpoint (HTTP)** and **SLO Endpoint (HTTP)**.
6. Select the **View Details** link at the X.509 Certificate field.

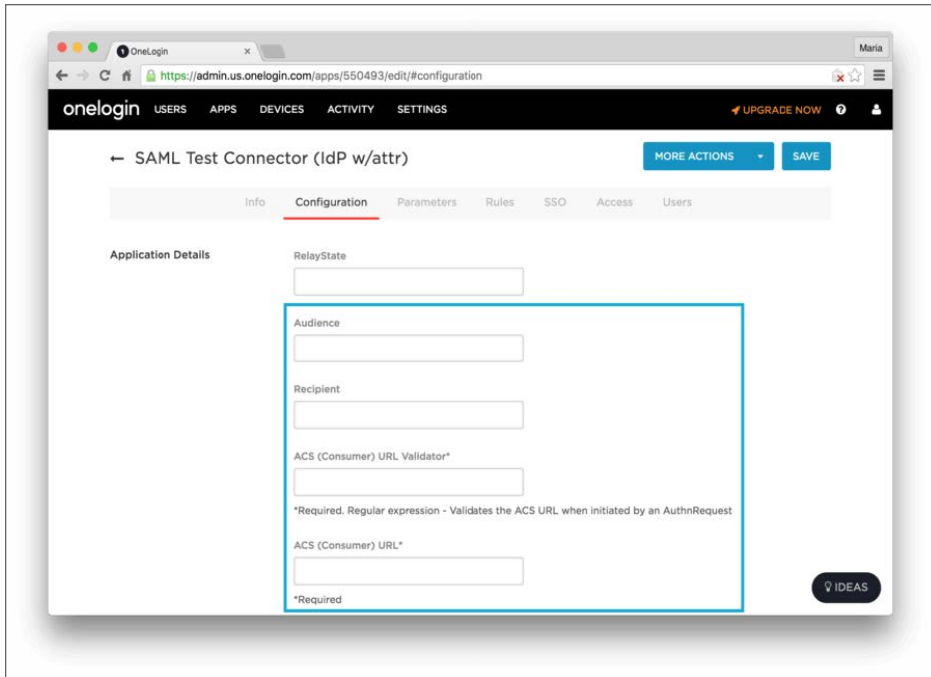


7. Download the X.509 certificate **onelogin.pem**.

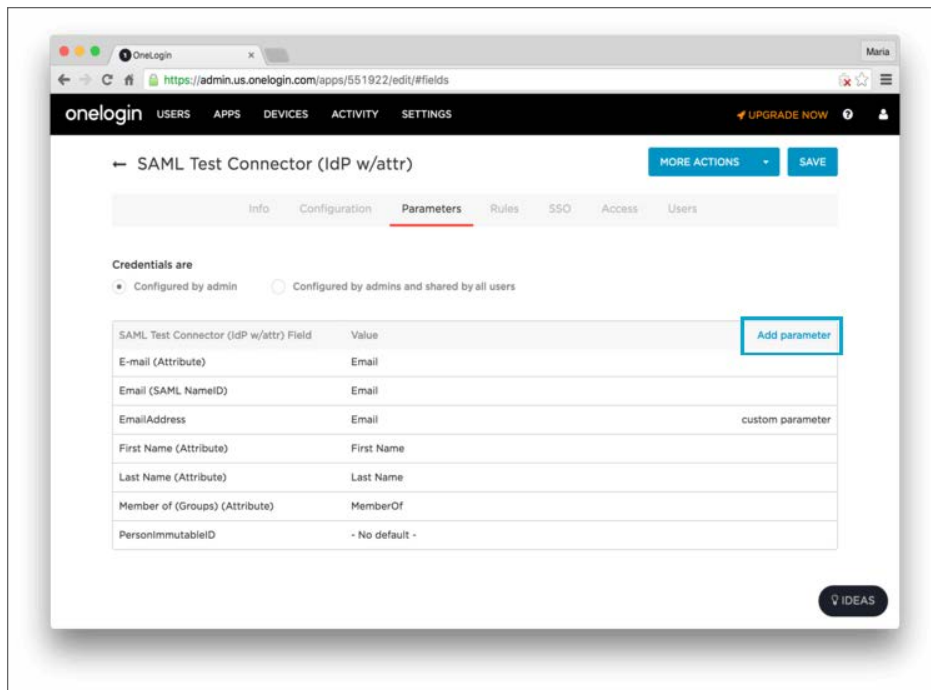


8. Go back to the **Configuration** tab.
9. Enter the following values into the appropriate fields:

- **Audience:** urn:auth0:sonicwall-production:tenantname-oc
- **Recipient:** <https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>
- **ACS (Consumer) URL:** <https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>
- **ACS (Consumer) URL Validator field:**  
<https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>

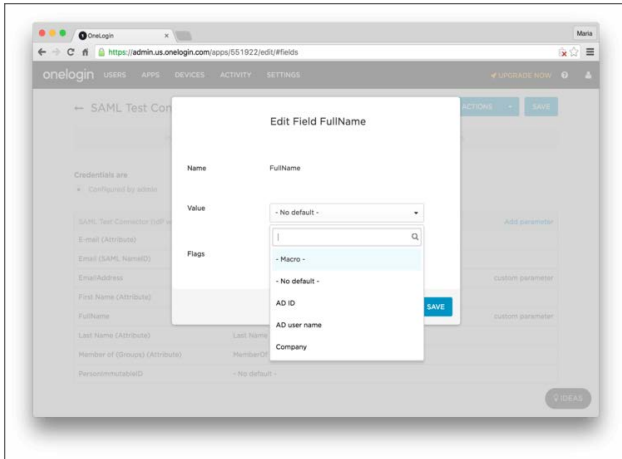


10. On the **Parameters** tab, select **Add Parameter**.



11. In the popup, set a name for your new custom attribute using the **Field name** text box. Make sure you check the Include in the **SAML assertion flag**. Select **Save**.
12. The new attribute you created is displayed. Select the **Value** field, which is currently displaying **- No default**.
13. Select the **Value** dropdown menu and select **Macro**.
14. Add the following set of properties:
  - **Field Name:** email, **Macro text box value:** {email}, **SAML assertion flag:** Checked
  - **Field Name:** given\_name, **Macro text box value:** {firstname}, **SAML assertion flag:** Checked
  - **Field Name:** family\_name, **Macro text box value:** {lastname}, **SAML assertion flag:** Checked

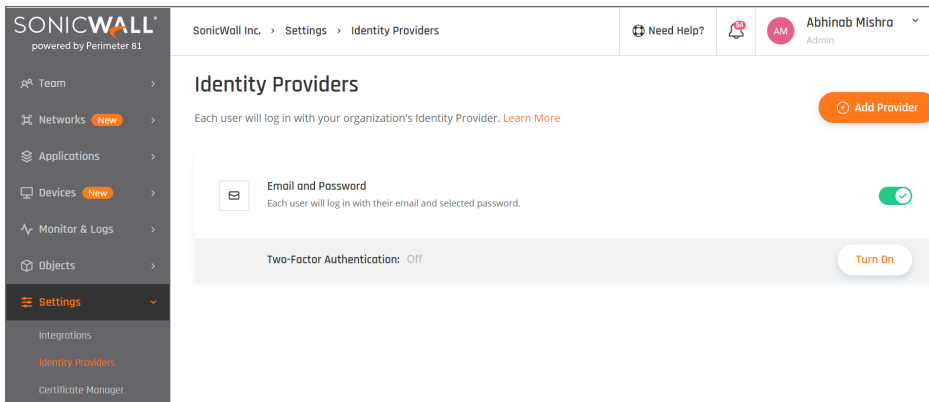




At this point, we're ready to configure SonicWall.

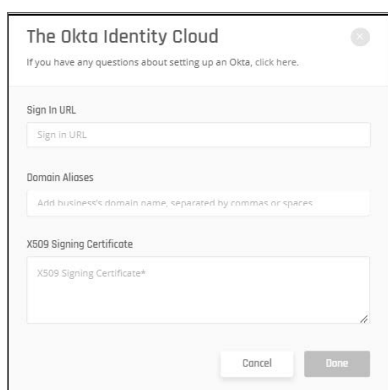
## Configuring SonicWall

1. Log in to your **Management Platform**, and navigate to **Settings** and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Choose **Okta Identity Cloud** (Okta connection will work for OneLogin).
4. Fill **Sign In URL**, **Signing Certificate** as follows:
  - The SAML 2.0 Endpoint (HTTP) value you saved above into the **Sign In URL** field
  - The SLO Endpoint (HTTP) value into the **Sign Out URL** field.

- Finally, upload the **onelogin.pem** certificate using Upload Certificate.



5. Select **Done**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

## PingOne for Enterprise

This article describes how to configure PingOne for Enterprise for use as an **identity provider** for SonicWall Cloud Edge.

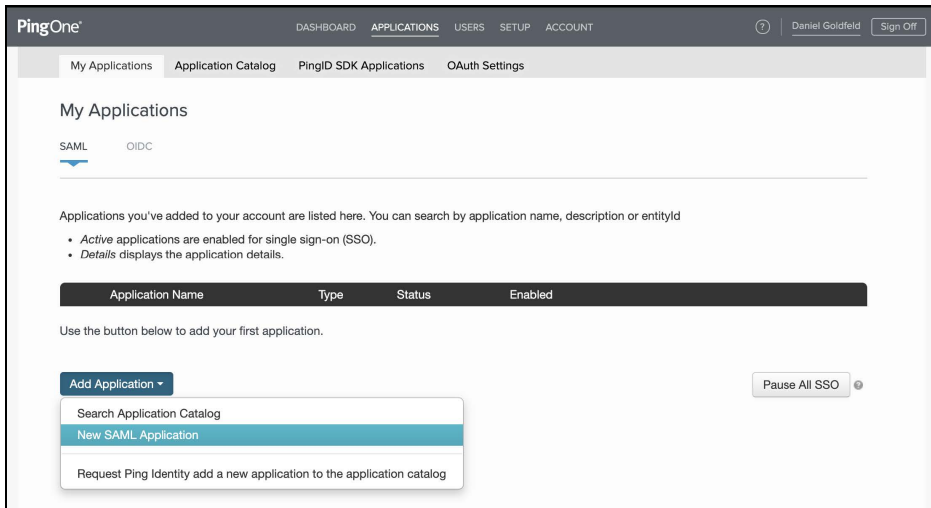
- Configuring your PingOne for Enterprise account
- Configuring SonicWall Cloud Edge

Please follow the steps below:

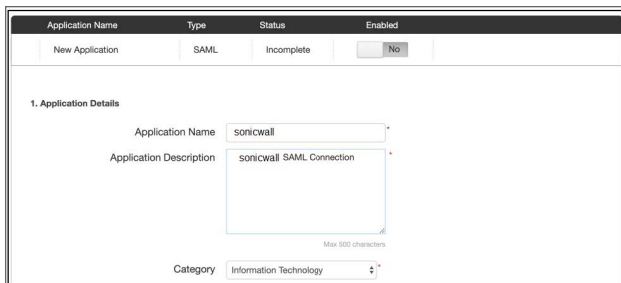
① **NOTE:** To successfully integrate PingOne for Enterprise and SonicWall Cloud Edge, you must have admin access on both platforms.

## Configuring your PingOne for Enterprise Account

1. Log in to your PingOne for Enterprise account.
2. On the upper toolbar in your PingOne for Enterprise screen select **Applications**. This takes you to the **My Applications** screen.
3. Click on **SAML**. Open the **Add Application** drop-down and select **New SAML Application**.



4. On the pop-up window, fill in the following details:
  - **Application Name:** SonicWall Cloud Edge
  - **Application Description:** SonicWall Cloud Edge SAML Connection
  - **Category:** Information Technology
  - **Graphics:** Add the SonicWall Cloud Edge Logo (*Optional*)



5. Click **Continue to Next Step** to proceed.
  6. On the **Application Configuration** window click on **I have the SAML configuration**.
  7. Fill in the following information:
    - **Signing Certificate:** PingOne Account Origination Certificate
    - **Protocol Version:** SAML v 2.0
    - **Assertion Consumer Service (ACS):**  
<https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>
    - **Entity ID:** urn:auth0:sonicwall-production:tenantname-oc
- ① | **NOTE:** : The tenantname should be changed to your SonicWall Cloud Edge tenant name.

I have the SAML configuration
I have the SSO URL

You will need to download this SAML metadata to configure the application:

Signing Certificate PingOne Account Origination Certificate ↓  
 SAML Metadata [Download](#)

Provide SAML details about the application you are connecting to:

Protocol Version  SAML v 2.0  SAML v 1.1

Upload Metadata Select File [Or use URL](#)

Assertion Consumer Service (ACS)

Entity ID

Application URL

Single Logout Endpoint example.com/slo.endpoint

Single Logout Response Endpoint example.com/slo/response.endpoint

Single Logout Binding Type  Redirect  Post

Primary Verification Certificate Choose File No file chosen

8. Click **Continue to Next Step** to proceed. On the **SSO Attribute Mapping** window, you will need to map the following attributes: | **Application Attribute** | **Identity Bridge Attribute or Literal Value** |

| -- | -- |  
 | email | Email |  
 | given\_name | First Name |  
 | family\_name | Last Name |  
 | groups | memberOf |

| Application Name | Type | Status | Enabled                                       |
|------------------|------|--------|---|
| Perimeter 81     | SAML | Active | Yes <span style="float: right;">Remove</span> |

### 3. SSO Attribute Mapping

Map the necessary application provider (AP) attributes to attributes used by your identity provider (IdP).

|   | Application Attribute | Identity Bridge Attribute or Literal Value | As Literal               | Advanced                 | Required                 |   |
|---|-----------------------|--|--------------------------|--------------------------|--------------------------|---|
| 1 | email                 | Email                                      | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ✕ |
| 2 | given_name            | First Name                                 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ✕ |
| 3 | family_name           | Last Name                                  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ✕ |
| 4 | groups                | memberOf                                   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | ✕ |

Add new attribute

NEXT: Group Access Cancel Back **Continue to Next Step**

9. Click **Continue to Next Step** to proceed.
10. On the **Group Access** window select the user groups that should have access to the PingOne for Enterprise Login Page. To allow access to all users we recommend adding **Users@Directory**.

**4. Group Access**

Select all user groups that should have access to this application. Users that are members of the added groups will be able to SSO to this application and will see this application on their personal dock.

Group 1, Group 2, etc

| Group Name                      |                                    |
|---------------------------------|------------------------------------|
| Domain Administrators@directory | <input type="button" value="Add"/> |
| Users@directory                 | <input type="button" value="Add"/> |

NEXT: Review Setup

- Click **Continue to Next Step** to proceed.
- On the **Review Setup** window copy the "idpid" and click on the **Download** link next to **Signing Certificate**.

|                                   |   |
|-----------------------------------|---|
| saasid                            | d8a5292c-6655-46d3-825e-e85fab5c70ef  |
| Issuer                            | https://pingone.com/idp/cd-622867948_sonicwall  |
| idpid                             | d4e6f877-2c65-4e22-8f74-ce92dd9f469a  |
| Protocol Version                  | SAML v 2.0  |
| ACS URL                           | <a href="https://auth.sonicwalledge.com/login/callback?connection=oc">https://auth.sonicwalledge.com/login/callback?connection=oc</a>   |
| entityid                          | urn:auth0:sonicwalledge=oc  |
| Initiate Single Sign-On (SSO) URL | <a href="https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=d8a5292c-6655-46d3-825e-e85fab5c70ef&amp;idpid=d4e6f877-2c65-4e22-8f74-ce92dd9f469a">https://sso.connect.pingidentity.com/sso/sp/initssso?saasid=d8a5292c-6655-46d3-825e-e85fab5c70ef&amp;idpid=d4e6f877-2c65-4e22-8f74-ce92dd9f469a</a> |
| Single Sign-On (SSO) Relay State  | <a href="https://pingone.com/1.0/d8a5292c-6655-46d3-825e-e85fab5c70ef">https://pingone.com/1.0/d8a5292c-6655-46d3-825e-e85fab5c70ef</a>   |
| Signing Certificate               | <a href="#">Download</a>  |
| SAML Metadata                     | <a href="#">Download</a>  |

- Click **Save and Close**.
- On **My Applications** screen verify that the application is set to **Enabled - Yes**.

**My Applications**

SAML  | OIDC

Applications you've added to your account are listed here. You can search by application name, description or entityid

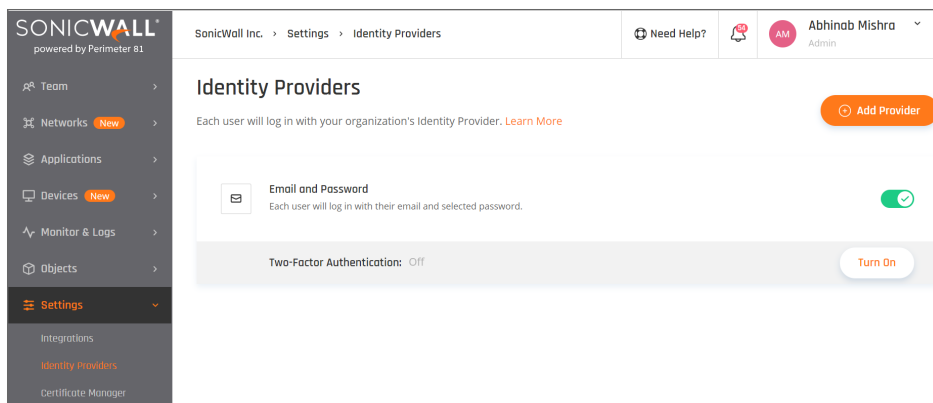
- Active applications are enabled for single sign-on (SSO).
- Details displays the application details.

| Application Name | Type | Status | Enabled                             |  |
|------------------|------|--------|-------------------------------------|--|
| sonicwall        | SAML | Active | <input checked="" type="checkbox"/> | <input type="button" value="Remove"/> <input type="button" value="▶"/> |

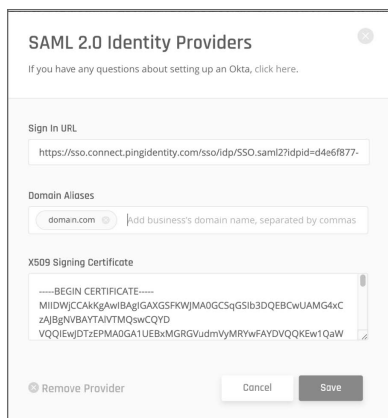
## Configuring SonicWall Cloud Edge

You need to configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge Management Platform, and navigate to **Settings** and then **Identity Providers**.
2. Select **+ Add Provider**.



3. Select **SAML 2.0 Identity Cloud**.
4. Fill in the **Sign In URL** with the following URL:  
**`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`** (fill in the idpid from step 14).
5. Add your organization domains.
6. Paste the certification from the downloaded **idp-signing.crt** file (begin and end line included).



7. Select **Save**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

# JumpCloud

This article describes how to configure JumpCloud for use as an **identity provider** for SonicWall Cloud Edge.

- Configuring the JumpCloud SSO application
- Configuring JumpCloud at the Management Platform
- Access Error troubleshooting


**Please follow the steps below:**

## Configuring the JumpCloud SSO application

1. Open the **JumpCloud Administrator Console**.
2. Select **Applications** in the main navigation panel.
3. Select the **+** in the upper left, then select **Configure** at the SAML 2.0 line.



4. At the **General Info** section insert values of your own choice.
5. At the **Single Sign-On configuration** section, fill in according to the following. Replace `{{workspace}}` with your SonicWall Cloud Edge workspace name (see attached example).



- **IDP Entity ID:** Enter <https://workspace.sonicwalledge.com>
- **SP Entity ID:** Enter `urn:auth0:sonicwall-production:tenantname-oc`

- **ACS URL:** Enter <https://auth.sonicwalledge.com/login/callback?connection=tenantname-oc>

6. Make sure to leave the rest of the fields with the default values:



SAMLSubject NameID:

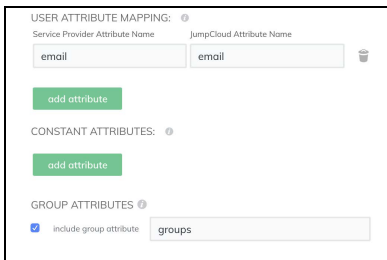
SAMLSubject NameID Format:

Signature Algorithm:

7. Define the user attributes as follows:

| Service Provider Attribute Name | JumpCloud Attribute Name |
|---------------------------------|--------------------------|
| email                           | email                    |
| given_name                      | firstname                |
| family_name                     | lastname                 |

8. Enable group attributes and specify the group attribute - **groups**.



USER ATTRIBUTE MAPPING:

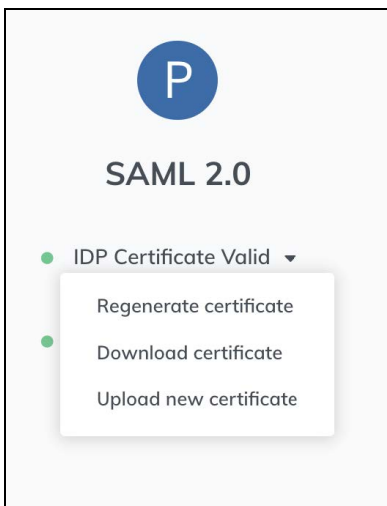
| Service Provider Attribute Name | JumpCloud Attribute Name |
|---------------------------------|--------------------------|
| email                           | email                    |

CONSTANT ATTRIBUTES:

GROUP ATTRIBUTES:

include group attribute

9. Select **Activate**.



**SAML 2.0**

- IDP Certificate Valid ▾
  - Regenerate certificate
  - Download certificate
  - Upload new certificate

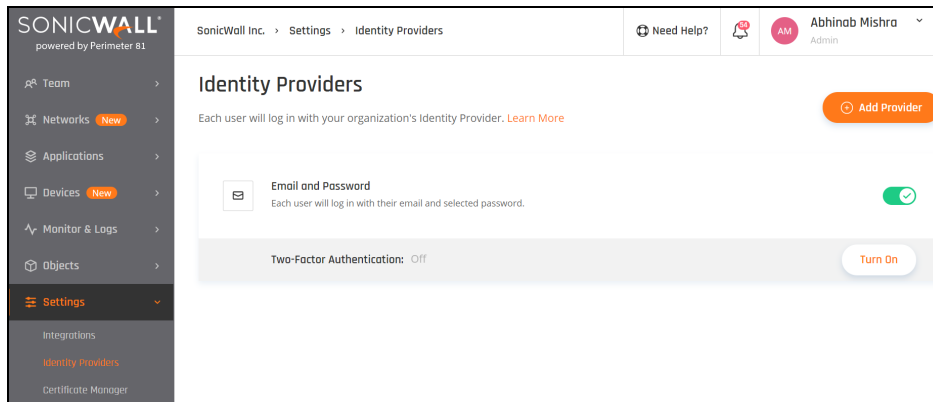
10. Select the application you've just created and download the IdP certificate.



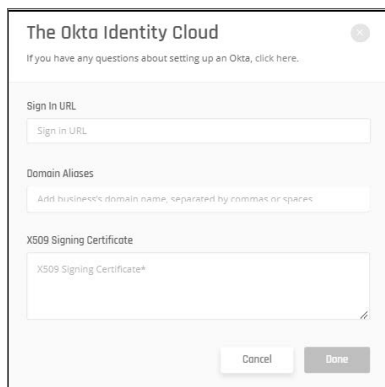
## Configuring JumpCloud at the Management Platform

At this point, you will configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge **Management Platform**, and navigate to **Settings** and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Choose **Okta Identity Cloud**.
4. **Sign In URL:** <https://sso.jumpcloud.com/saml2/saml2>
5. Add your organization domain.
6. Paste the certification from JumpCloud.



7. Select **Done**.

## Access Error troubleshooting

If your users are getting access error after the configuration, please [check these steps](#).

# Securing the Platform

## Topics:

- [Securing Networks](#)
- [Securing User Access](#)

## Securing Networks

### Topics:

- [Segmenting Networks](#)
- [Device Posture Check](#)
- [Network Traffic Control](#)

## Segmenting Networks

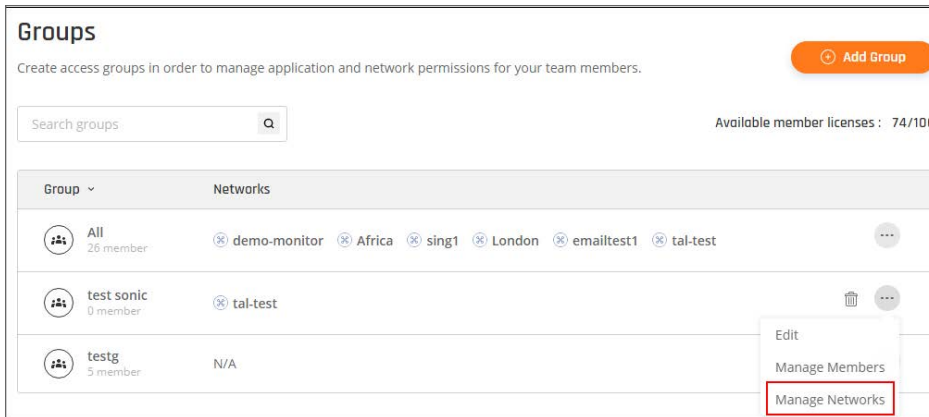
This article describes why and how you can segment your network. It isn't just about sorting employees into groups based on which applications and resources they use and then providing them with encrypted tunnels to these resources. It's also about creating secure ways to access individual networks and specific resources within your organization.

This is easy with a **Software-Defined Perimeter (SDP)**. SDP helps you limit network access and at the same time provide customized user permissions to systems based on the least-privilege model: defining which users, devices, roles, and locations can connect to the network.

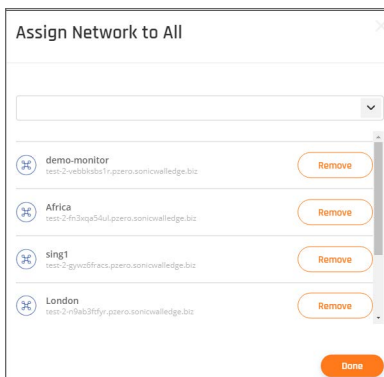
For example, you can assign **groups** of your users (each with their access policy) to specific parts of a certain network or only to some of your SDPs.

# Segmenting your network

1. Select the **Team** tab in the Management Platform and then the **Groups** tab below.
2. Select the group whose permissions you'd like to manage. Then select **Manage Networks** from the three-dotted menu (...) on the right side of the window.



3. Select which locations that particular user group can access. When the users subsequently log in to their client application, they will only be able to access the designated server locations specified in their permissions.



4. Select **Done**.

# Device Posture Check

SonicWall Cloud Edge **Device Posture Check (DPC)** allows administrators to ensure that only devices that comply with their predefined security policies can connect using a SonicWall Cloud Edge agent to a **Network**, and gives them the reporting they need to ensure that **Networks** stay secure while **Members** can easily access the resources they need.

Device Posture Check performs checks on the connecting device either once upon connecting, or continuously at intervals chosen by the administrator.

Policies can differentiate between different members or member groups, further ensuring that sensitive **Networks** and resources are protected with an extra layer of security.

For example, administrators can allow access to **Networks** only from devices that are complying with one or more of the following policies:

- The presence of specific antivirus software on the device
- Whether a specific (authorization) file can be found on the device.
- Whether the device's storage is encrypted.
- Whether a device holds the appropriate certificate (as defined by the administrator).

## Add Device Posture Check profiles

You can set device profiles per operating system. Each profile can apply to a specific **Group**, operating system or both.

The Device Posture Check profiles will be applied to all **Networks** in your SonicWall Cloud Edge tenant.

In order to add a Device Posture Check profile:

1. Navigate to **Devices > Posture Check**.
2. Click on **(+) Add Profile**.
3. Enter a **Posture Check Profile Name**.
4. Select the **Group(s)** that should comply with the profile.

**ⓘ | NOTE:** Check the **All Users** Group to apply the profile to all your SonicWall Cloud Edge users.

5. Select the suitable **Runtime Schedule**

**NOTE:** The **Device Posture Check** can be verified periodically while a **Member** is connected to a **Network** or with every connection to a **Network**.

The screenshot shows a web form titled "Add Device Posture Check Profile". Below the title is a subtitle: "Create and manage Device Posture Check profiles to enforce security before endpoints gain network access. [Learn More](#)". The form contains the following fields and options:

- Posture Check Profile Name:** A text input field with the placeholder "Enter a descriptive profile name".
- Assign Groups:** A dropdown menu with the placeholder "Select assigned groups".
- Runtime Schedule:** A section with a toggle icon. It contains two radio button options:
  - Prior to Connection and** (selected), followed by a dropdown menu showing "Every 20 minutes".
  - Prior to Connection Only**

## Define Posture Check per OS

Administrators can define different profiles or requirements for different operating systems within the same profile or create separate profiles for each operating system.

Each OS Profile can have one or more which must be met in order to gain access to **Networks**.

### **Windows:**

1. Click **Add OS to Profile**
2. Select and **Define Rules**

You can pick one of the following options:

**Antivirus** - the SonicWall Cloud Edge agent will verify the presence of the selected Antivirus application.

**File-Exists** - the SonicWall Cloud Edge agent will verify the presence of a specific file in a specific path.

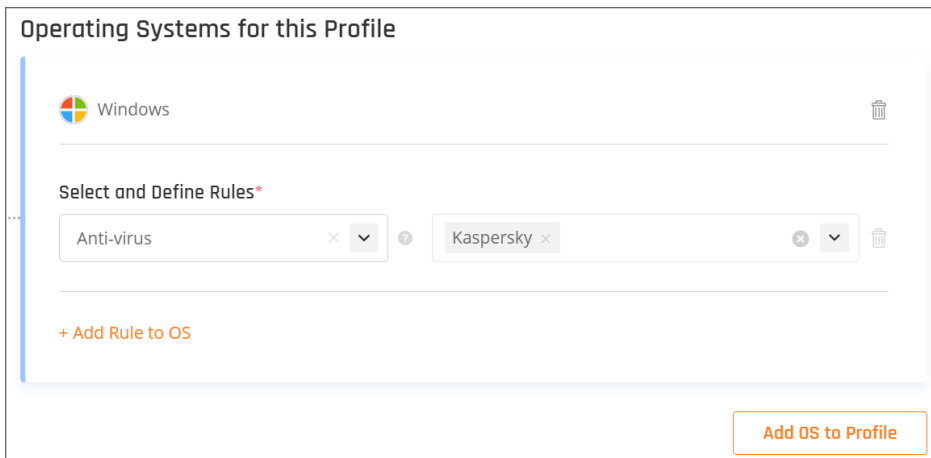
**Disk Encryption** - the SonicWall Cloud Edge agent will verify that the OS hard-drive is encrypted.

**Certificate** - the SonicWall Cloud Edge agent will verify that a specific certificate's subject is installed on the device (in the local Windows CA store or MacOS Keychain)

**Registry** - the SonicWall Cloud Edge agent will verify a specific registry key.

(Example: HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\New Key)

3. Click on **Add Rule to OS** (if needed)



### MacOS:

1. Click **Add OS to Profile**
2. Select and Define Rules

You can pick one of the following options:

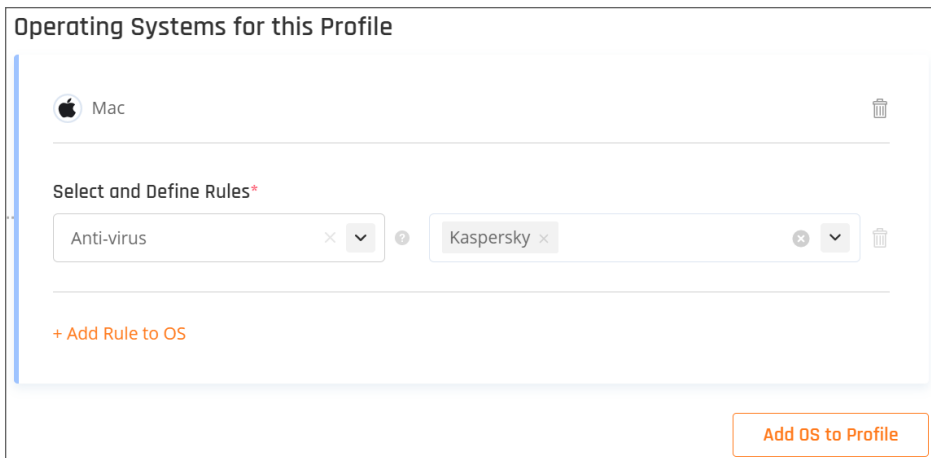
**Antivirus** - the SonicWall Cloud Edge agent will verify the presence of the selected Antivirus application.

**File-Exists** - the SonicWall Cloud Edge agent will verify the presence of a specific file in a specific path.

**Disk Encryption** - the SonicWall Cloud Edge agent will verify that the OS hard-drive is encrypted.

**Certificate** - the SonicWall Cloud Edge agent will verify that a specific certificate is installed on the device (Mac Keychain).

3. Click on **Add Rule to OS** (if needed)



### Linux:

1. Click **Add OS to Profile**

2. Select and Define Rules

You can pick one of the following options:

**Antivirus** - the SonicWall Cloud Edge agent will verify the presence of the selected Antivirus application.

**File-Exists** - the SonicWall Cloud Edge agent will verify the presence of a specific file in a specific path.

3. Click on **Add Rule to OS** (if needed)

### iOS:

1. Click **Add OS to Profile**

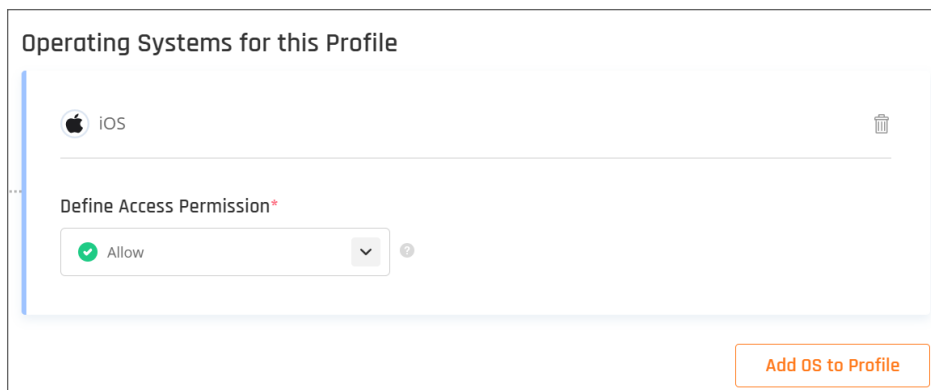
2. Select and Define Rules

You can pick one of the following options:

**Allow** - Mobile devices using the SonicWall Cloud Edge application will be allowed into **Networks**.

**Deny** - Mobile devices using the SonicWall Cloud Edge application will be denied access into **Networks**.

3. Click on **Add Rule to OS** (if needed)



### Android:

1. Click **Add OS to Profile**

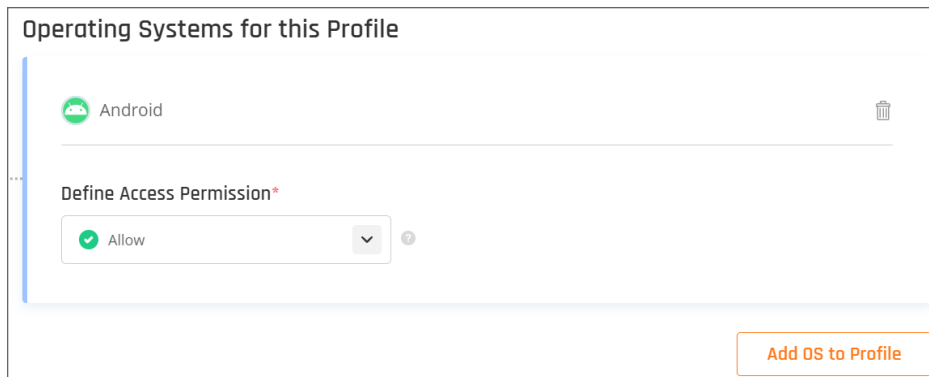
2. Select and Define Rules

You can pick one of the following options:

**Allow** - Mobile devices using the SonicWall Cloud Edge application will be allowed into **Networks**.

**Deny** - Mobile devices using the SonicWall Cloud Edge application will be denied access into **Networks**.

3. Click on **Add Rule to OS** (if needed)



## Network Traffic Control

This article describes why and how you can protect and limit access to your resource(s) by defining policies and rules based on user groups, origin and/or destination IPs, ports, and/or network protocols.

It isn't just about controlling your inbound or outbound network traffic but being able to manage your entire network traffic based on user-based and network-based Rules that define which applications, resources, regions, and data-centers can be accessed through encrypted tunnels.

By enabling **Network Traffic Control** you'll secure and control the entire traffic on one unified **Software-Defined Perimeter (SDP)**.

For example, you can allow **Groups** of your users (each with their own policies and rules) to specific parts of a certain network, only using a specific protocol and only when coming from your internal subnet IP range.

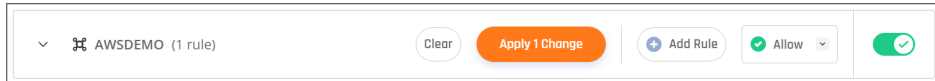
## Activate Network Traffic Control

You can activate a set of **Rules and Policies** per SASE Network. In case you have more than one Network in your tenant you can activate the **Network Traffic Control** to some or all of your **Networks**.

In order to activate Network Traffic Control on an existing Network:

1. Navigate to **Network > Network Traffic Control**.
2. In the Network Traffic Control screen, you will see all the **Networks** that you've created in your tenant.
3. Select the appropriate **Network**, set the Network's **Default Action**, and turn on the toggle.
  - ① **NOTE:** The **Default Action** defines how to treat connections and traffic which doesn't have a specific Network Policy Rule.
    - Allow** - All traffic will be allowed to all connected resources unless a specific **Rule** defines a different action.
    - Deny** - All traffic will be blocked to all connected resources unless a specific **Rule** defines a different action.
4. Click on **Apply Changes**.





## Add a Rule

The **Network Traffic Control** is combined out of a list of **Rules** that defines the access and traffic routing policies. You can create multiple rules that will apply specific policies for specific **User Groups, Resources, and Protocols** as well as wide Policies that will be applied to the entire **Network** traffic (i.e block all traffic on a specific port).

### To create a new Rule:

1. Navigate to **Networks > Network Traffic Control**.
2. Click on **(+) Add New Rule**.
3. Select the **Network** where the **Rule** should be added.
4. Provide an indicative **Name**.
5. Select the **Action** type.
6. Add **Source** and **Destination** Objects.

**NOTE:** The **Source** and **Destination** define the conditions that have to be met in order for the **Action** to be applied to the traffic.

There are four types of Objects that can be used in the **Source** and **Destination** conditions:

**Any** - All traffic on all protocols and ports coming from any of the End-Points or encrypted tunnels.

**Groups or Members** - All traffic routed from/to a specific **Member** or **Users Group**.

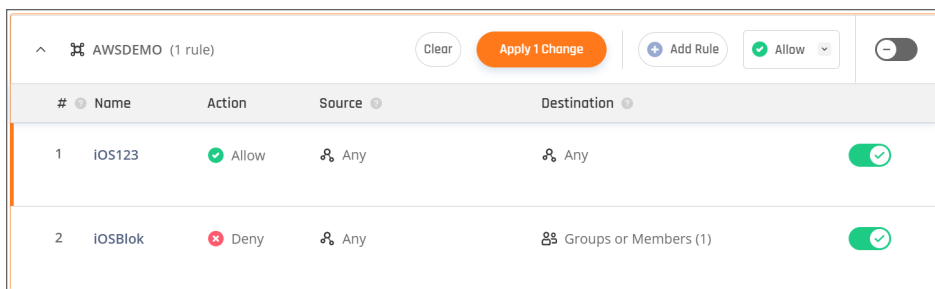
**Addresses** - Traffic routed from/to an IP Address, Subnet, or List of IPs.

**Services** - Traffic routed on a specific **Protocol** or **Ports**.

7. Drag the new **Rule** to the right **Priority**.

**NOTE:** Rules are applied based on the priority of the **Rule**. Should different rules overlap, the rule with the Lower Priority Number will take precedence (i.e. Rule with Priority #2 will take precedence over Rule with Priority #5).

8. Click on **Apply Changes**.



## Create Objects

When configuring Firewall rules you'll be defining **Rules** that are based on **Objects** and **User Groups**.

- The **Objects** will be used in order to specify **IP Addresses**, **Subnets**, **Network Protocols**, and **Ports**.
- The **User Groups** will be used in order to manage access of users to/from **Objects** and can be managed via the **Groups** tab.

## Addresses

The **Addresses Object** allows you to define subnets, IP lists, and specific IP addresses that can be used in the **Network Traffic Control** rules.

To create a new Address Object:

1. Navigate to **Objects > Addresses**.
2. Click on **(+) Add Address**.
3. Provide an indicative **Name** and **Description**.
4. Select the type of **Object** (IP, Subnet, or List) and provide the values.
5. Click on **Add Address**.

### Add Address ✕

Add a new address to your address object library. [Learn More](#)

**Name\***

**Description**

**Type\***

IP ▼

[Cancel](#) [Add Address](#)

## Services

The Services **Object** allows you to define Network Protocols, Port lists, and specific Ports that can be used in the **Network Traffic Control** rules.

To create a new Services Object:

1. Navigate to **Objects > Services**.
2. Click on **(+) Add Service**.
3. Provide an indicative **Name** and **Description**.
4. Select the **Protocol** (Port, Range, or List) and provide the values.
5. Click on **Add Service**.

### Add Service ✕

Add a custom service to your service object library. [Learn More](#)

---

**Name\***

**Description**

**Protocol\***

TCP ▼    Port ▼   

[+ Add New Protocol / Port](#)

Cancel Add Service

## Firewall-as-a-Service

This article describes why and how you can protect and limit access to your resource(s) by defining policies and

rules based on user groups, origin and/or destination IPs, ports, and/or network protocols.

It isn't just about controlling your inbound or outbound network traffic but being able to manage your entire network traffic based on user-based and network-based Rules that define which applications, resources, regions, and data-centers can be accessed through encrypted tunnels.

By enabling the Firewall you'll secure and control the entire traffic on one unified Software-Defined Perimeter (SDP).

For example, you can allow Groups of your users (each with their own policies and rules) to specific parts of a certain network, only using a specific protocol and only when coming from your internal subnet IP range.

## Activate the Firewall

You can activate a set of Rules and Policies per SASE Network. In case you have more than one Network in your tenant you can activate the Firewall on some or all of your Networks.

In order to activate the Firewall on an existing Network:

1. Navigate to Network -> Firewall.
2. In the Firewall screen, you will see all the Networks that you've created in your tenant.
3. Select the appropriate Network, set the Network's Default Action, and turn on the toggle.
  - ① **NOTE:** The Default Action defines how to treat connections and traffic which doesn't have a specific Network Policy Rule.
    - Allow** - All traffic will be allowed to all connected resources unless a specific Rule defines a different action.
    - Deny** - All traffic will be blocked to all connected resources unless a specific Rule defines a different action.
4. Click on **Apply Changes**.

## Add a Rule

The Firewall policy for a network is a list of Rules that defines the access and traffic routing policies. You can create multiple rules that will apply specific policies for specific User Groups, Resources, and Protocols as well as wide policies that will be applied to the entire Network traffic (i.e block all traffic on a specific port).

To create a new Rule:

1. Navigate to Networks -> Firewall
2. Click on (+) Add New Rule
3. Select the Network where the Rule should be added
4. Provide an indicative Name
5. Select the Action type
6. Add Source and Destination Objects the rule will apply to
7. Add Services the rule will apply to

① **NOTE:** The Source and Destination define the conditions that have to be met in order for the Action to be applied to the traffic.

There are three types of Objects that can be used in the Source and Destination conditions:

**Any** - All traffic (any address or user).

**Groups or Members** - All traffic routed from/to a specific Member or Users Group

**Addresses** - Traffic routed from/to an IP Address, Subnet, or List of IPs.

For services, there are two types:

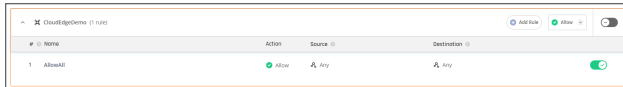
**Any** - All traffic on all protocols and ports

**Services** - Traffic routed on a specific Protocol or Ports.

8. Drag the new Rule to the right Priority.

① **NOTE:** Rules are applied based on the Priority of the Rule, from the top down (lowest number to highest). Should different Rules overlap, the Rule with the Lower Priority Number will take precedence (i.e. Rule with Priority #2 will take precedence over Rule with Priority #5)

9. Click on **Apply Changes**.



## Create Objects

When configuring Firewall rules you'll be defining Rules that are based on Objects and User Groups.

- The Objects will be used in order to specify IP Addresses, Subnets, Network Protocols, and Ports.
- The User Groups will be used in order to manage access of users to/from Objects and can be managed via the Groups tab.

## Addresses:

The Addresses Object allows you to define subnets, IP lists, and specific IP addresses that can be used in the Firewall rules.

To create a new Address Object:

1. Navigate to **Objects -> Addresses**
2. Click on **(+) Add Address**
3. Provide an indicative **Name** and **Description**
4. Select the type of **Object** (IP, Subnet, or List) and provide the values

5. Click on **Add Address**

**Add Address** ✕

Add a new address to your address object library. [Learn More](#)

**Name\***

Enter address name

**Description**

Enter a description that will help you recognize the address

**Type\***

IP ▼ Enter IPv4 address

Cancel Add Address

## Services:

The Services Object allows you to define Network Protocols, Port lists, and specific Ports that can be used in the Firewall rules.

To create a new Services Object:

1. Navigate to **Objects -> Services**.
2. Click on **(+) Add Service**.
3. Provide an indicative **Name** and **Description**.
4. Select the **Protocol, type of Service** (Port, Range, or List) and provide the values.

5. Click on **Add Service**.

**Add Service**

Add a custom service to your service object library. [Learn More](#)

**Name\***

Enter service name

**Description**

Enter a description that will help you recognize the service

**Protocol\***

TCP Port Enter port

[+ Add New Protocol / Port](#)

Cancel Add Service

## Securing User Access

### Topics:

- [Agent-based Access](#)
- [Agent-less Access](#)
- [Multi-Factor Authentication](#)

## Multi-Factor Authentication

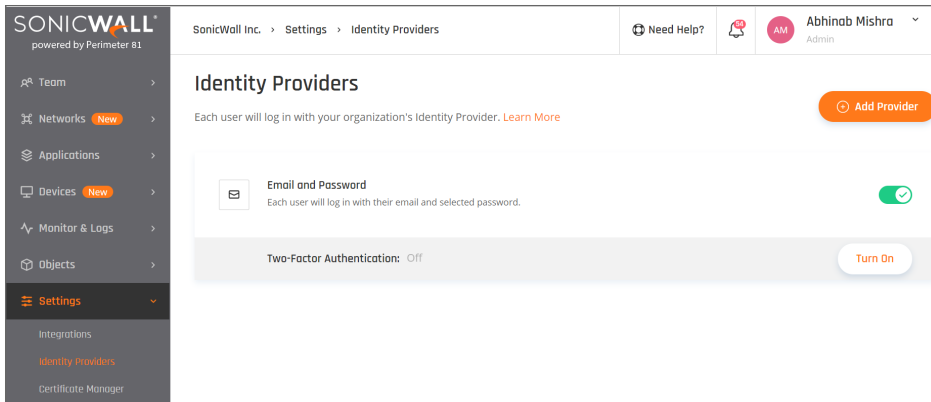
### Topics:

- [MFA Authentication](#)
- [DUO Security](#)

## MFA Authentication

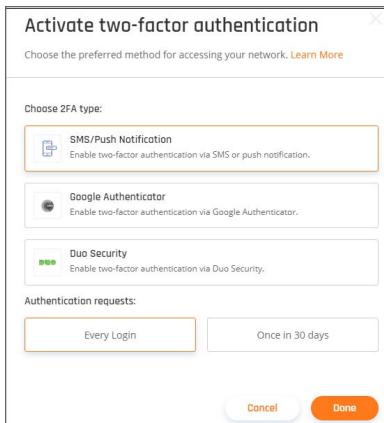
This article describes how to activate two-factor authentication.

1. To activate two-factor authentication, select **Settings** in the **Management Platform** on the left side and then select the **Security** tab. Select **Two-Factor Authentication** and select **Turn On**.



2. Select one of the following two-factor authentication methods:

- **SMS/Push Notification** - Team members will receive a code via SMS or push notification for secure login.
- **Google Authenticator**
- **Duo Security**



3. You can also choose to select team members that will be required to complete two-factor authentication either for every login or once every 30 days.

4. Select **Done**.

When the users are authenticating for the first time they will be requested to provide their phone number (SMS) or scan the QR code (Google Authenticator).

In case it is needed, you will be able to reset the MFA through the portal and it will prompt for the phone number or QR code on the next user login.

① **NOTE:** Please be aware that the two-factor authenticator is defined per IdP and cannot be assigned to a specific user.



# DUO Security

This article describes how to configure DUO security for SonicWall.

- Configuring the DUO SSO application
- Configuring SonicWall

Please follow the steps below.

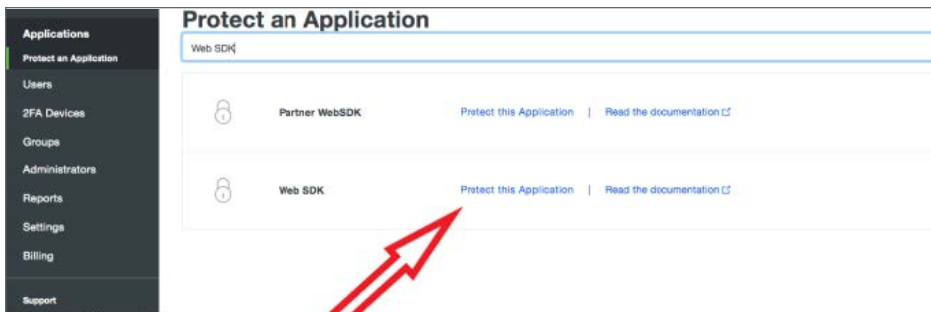
## Configuring the DUO SSO application

You must generate an integration key, API hostname, and Secret key to connect SonicWall to DUO.

1. On the **Applications** page select **Protect an Application**.



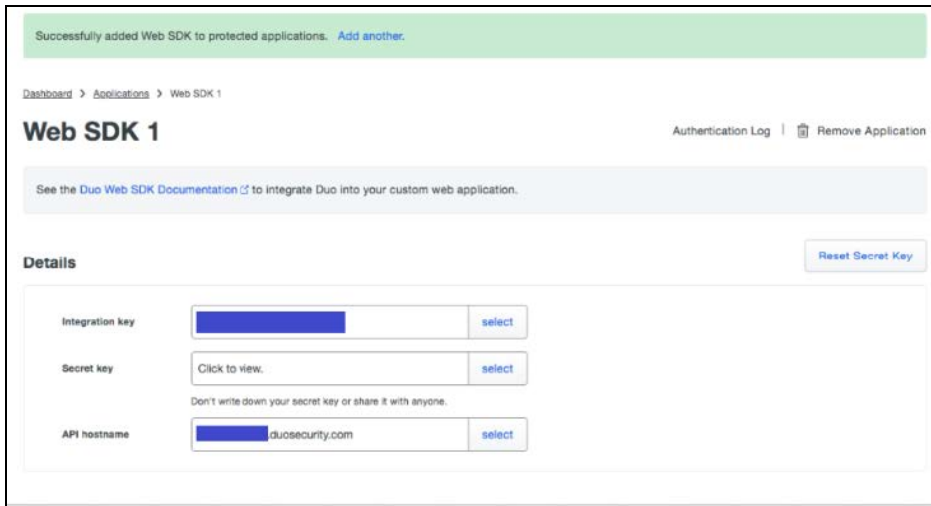
2. In the search bar type "Web SDK" and select "Protect this Application" as shown in the image below.



3. Change the Name.

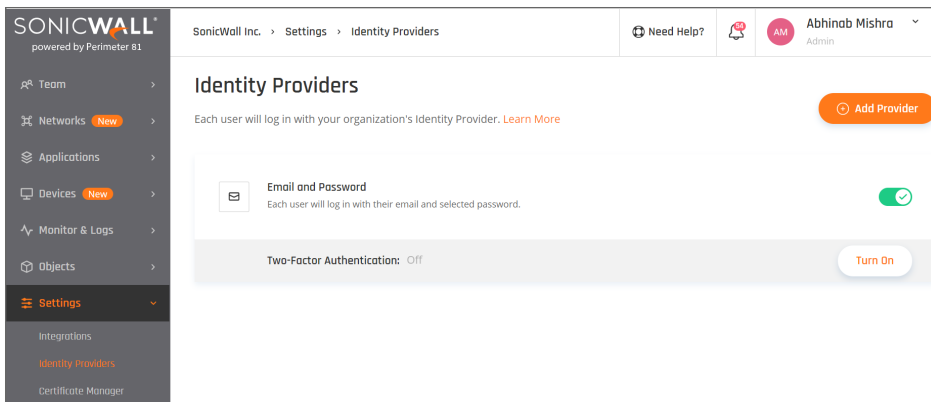


After accepting you can find the integration key, API hostname, and Secret key in the Details section.



## Configuring SonicWall

1. Log in to your **Management Platform**, navigate to **Settings**, and then **Identity Providers**.



2. Select **+ Add Provider**.
3. Choose Two-factor authentication on the desired IDP by selecting **Turn On**.
4. In the page that displays, select **Duo Security**.
5. Fill the integration key, API hostname, and Secret key from the DUO configuration.

**Activate two-factor authentication**

Choose the preferred method for accessing your network. [Learn More](#)

Choose 2FA type:

SMS/Push Notification  
Enable two-factor authentication via SMS or push notification.

Google Authenticator  
Enable two-factor authentication via Google Authenticator.

Duo Security  
Enable two-factor authentication via Duo Security.

Integration key:  API hostname:

Secret key:

6. Select **Done**.

## Agent-less Access

### Topics:

- [Zero Trust Application](#)
- [Zero Trust Policies and Rules](#)

## Zero Trust Application

This article describes how SonicWall Cloud Edge's [Zero Trust Application Access](#) provides your workforce with secured, zero trust access to popular web applications - without an agent. Based on customized protocols, you can deploy four types of application access to your workforce.

To get started, you'll need to add an application to your SonicWall Cloud Edge account. Next, you will need to configure the application by filling out the General Settings form. Also, you will have the option to choose which groups of users will have access to the application and which policy will be included.

Now, a list of the applications that you have deployed will be available. To change the application permissions access, select the application setting option. Now you will have full control of the application's settings including rules of access.

For each policy, you can set up customized rules for user's access. The identification rules can be based on network, device, location, work schedule, and connection time. If the user's identification and policy rules match up, you will have access to the application deployed on the network.

Each user will see a complete list of available applications that you have permission to access. Once you select the application you will be automatically connected and will be able to work securely.

See the following articles for specific steps:

- [How to add an SSH application](#)
- [How to add an HTTPS application](#)
- [How to add an HTTP application](#)
- [How to add an RDP application](#)
- [How to add a VNC application](#)

After you have created an application, a list of the applications that you deployed will be available. You will be able to switch which group of users will have access and which policy will be enabled for the application. If the user's identification and policy rules match up, they will have access to the application deployed on the network. Each user will see a complete list of available applications that they have permission to access.

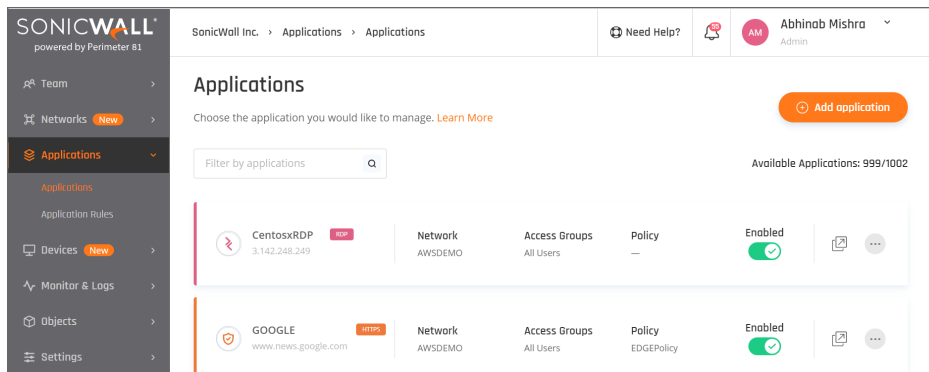
Once they select the application they will be automatically connected and will be able to work more securely.

## HTTP/HTTPS

### Adding an HTTP/HTTPS Zero Trust application

This article describes how to configure an HTTP/HTTPS connection to a remote web page.

1. Go to the **Applications** tab at the **Management Platform**. Select **Add application**.



2. Fill in the following information:

**Add application**

To add a new application, fill out the application's details below. [Learn More](#)

**General Settings**

**Application Name\***  **Protocol\***  **Icon**

**Host\***  **Port\***

**Network\***

**Display Application Icon at Login Screen**

**URL Alias**

**What is the HTTP application protocol?**

HTTP is a protocol for web applications, usually runs over port 80. It is commonly used for web applications such as internal web pages, Jenkins, MySQL and others.

[Learn about how to create HTTP application](#)

- **Application Name:** Enter a name of your choice.
  - **Protocol:** HTTP/HTTPS
  - **Icon:** Use default or choose an icon of your own choice.
  - **Host:** Enter the internal IP address (if custom DNS is configured you can alternatively enter the hostname) of the server to which you'd like to connect.
  - **Port:** 80 for HTTP or 443 for HTTPS.
  - **SSL Certificate Validation (HTTPS Only):** Once you enter an SSL Certificate, if you tick this box, the application will be accessible only as long as the SSL Certificate is valid.
  - **Network:** Choose the network that contains the gateway from which you created a tunnel to the environment that hosts the server you'd like to connect to.
  - **Add Start URI (Optional):** Enter a subpath to which the user will be directed once launching the app.
  - Example: If you entered [www.sonicwall.com](http://www.sonicwall.com) as Host and `/careers` users will be directed to [www.sonicwall.com/careers](http://www.sonicwall.com/careers) when launching the app.
  - **Display Application Icon at Login Screen:** Choose according to your preference.
  - **URL Alias (Optional):** See Advanced Setting Guide.
  - **Custom HTTP Headers:** Mandatory in case you inserted an explicit DNS as the host parameter
- ① **NOTE:** Some web browsers fail to display graphical components in the destination HTTP(S) page if a host header is missing, so it is advised to configure a custom header in any case (at the **Name** field insert **Host**; at **Value** field insert your internal FQDN).

- **Access Groups:** State the names of the user group who'll have access to the HTTP application.
  - **Policy:** Leave blank, or choose a policy that was previously created and matches your needs.
4. Select **Apply**.
  5. To connect to the application insert the application FQDN in the URL line of your browser or connect through the platform.

## RDP (Remote Desktop Protocol)

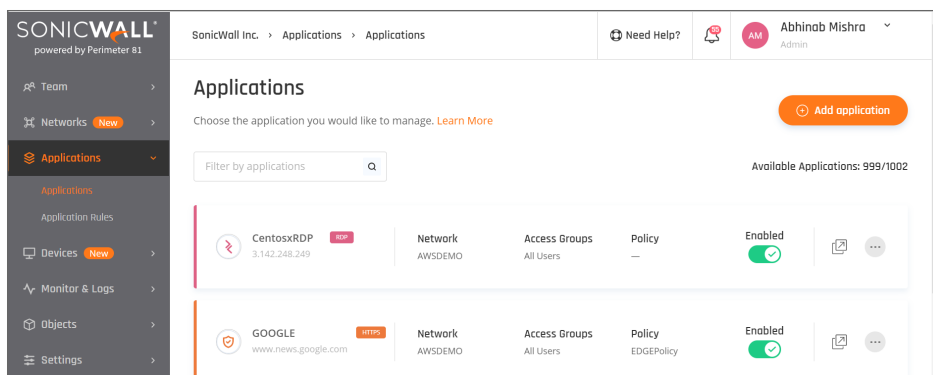
### Adding an RDP Zero Trust application

This article describes how to configure a Zero Trust RDP Application to a remote Windows instance, such as Windows Server 2016 / Windows 10.

Before we begin

Make sure you are familiar with the server's authentication methods (username and password or RDP keys) and that you have a tunnel connecting your network and the environment that hosts the Windows instance.

1. Go to the **Applications** tab at the SonicWall Cloud Edge Platform. Select **Add application**.



2. Fill in the following information:

### Add application

To add a new application, fill out the application's details below. [Learn More](#)

**General Settings**

**Application Name\***  **Protocol\*** ⓘ  **Icon**

**Host\*** ⓘ  **Port\*** ⓘ

**Network\*** ⓘ  **Max. # of connections\*** ⓘ

**Ignore server certificate**  **Admin console**

**Display Application Icon at Login Screen** ⓘ

**What is the RDP application protocol?** ✕

RDP is an application protocol that provides a connection to Windows servers or remote Windows-based workstations, usually runs over port 3389.

[Learn about how to create RDP application](#)

- **Application Name:** Choose an indicative name of your own choice.
- **Protocol:** RDP
- **Icon:** Use default or choose an icon of your own choice.
- **Host:** Enter the internal IP address of the server to which you'd like to connect.
- **Port:** 3389
- **Network:** Choose the network that contains the gateway from which you created a tunnel to the environment that hosts the server you'd like to connect to.
- **Max number of connections:** The maximum number of concurrent RDP sessions.
- **Ignore server certificate:** Yes, unless you activate an RDP over SSL.
- **Admin console:** Connect directly to the console session on the Windows server.
- **Display Application Icon at Login Screen:** Choose according to your preference.
- **Enable copy-paste from RDP to clipboard:** Default: yes
- **Enable printing from RDP:** Default: yes
- **URL Alias (Optional):** See *Advanced Setting Guide*.
- **Security Mode:** This mode dictates how data will be encrypted and what type of authentication will be performed if any. By default, a security mode is selected based on a negotiation process that determines what both the client and the server support.

**Security Mode** [Learn More](#)

Select Security Mode ⓘ

⬆

- Any
- Network Level Authentication (NLA)
- Extended Network Level Authentication (NLA-EXT)
- Transport Layer Security (TLS)
- VMConnect
- Remote Desktop Protocol

- **Authentication:**
  - Username and Password:** Enter one set of credentials as predefined on the server. You will not be required to enter any parameter with the login.
  - Domain:** If applicable, enter your active directory FQDN.
  - ① **NOTE:** If the Authentication toggle is **Disabled**, you'll need to enter your credentials as predefined on the Windows instance with every new RDP login.
  - ① **NOTE:** Windows Server 2016 and Windows 10 instances will need an additional configuration. Please follow the "Windows Server 2016 / Windows 10" section below.
- **Access Groups:** State the names of the user groups that will have access to the RDP application.
- **Policy:** Leave blank, or choose a policy that was previously created and matches your needs.

The screenshot shows a configuration window with three main sections:

- Authentication:** A toggle switch is turned on (green). Below it are input fields for Username (placeholder: "Enter username"), Password (placeholder: "Enter password"), and Domain (placeholder: "Enter domain").
- Access Groups:** A dropdown menu labeled "Groups\*" with the placeholder text "Select groups".
- Policy:** A dropdown menu labeled "Policy Name" with the placeholder text "Select policy".

At the bottom right, there are two buttons: "Cancel" (white with orange border) and "Apply" (orange).

## Configuration and troubleshooting

### Windows 7 users:

Registry modifications may be required in case you're operating on a Windows 7 device.

- Navigate to HKEY\_LOCAL\_MACHINE -> Software -> Microsoft -> Windows NT -> Terminal Services.
- Select "fServerEnableRDP8".



- Set the value type to "REG\_DWORD".
- Make sure that the enabled value is 1 (disables value is 0).
- Reboot the machine.

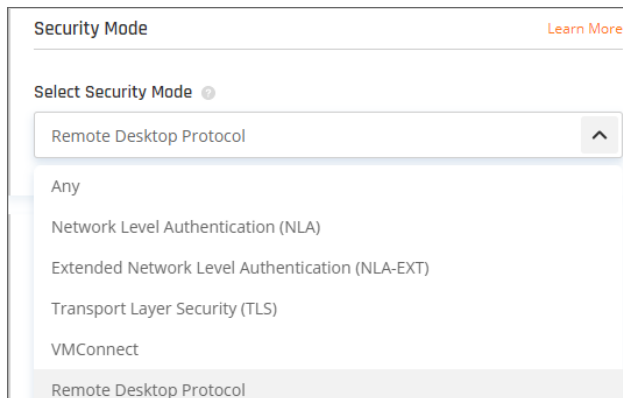
## Windows Server 2019 users:

Registry modifications may be required in case you're operating on a Windows 2019 server.

- Navigate to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
- Select "SecurityLayer" and change the value to 0.
- Reboot the machine.

## Upstream error:

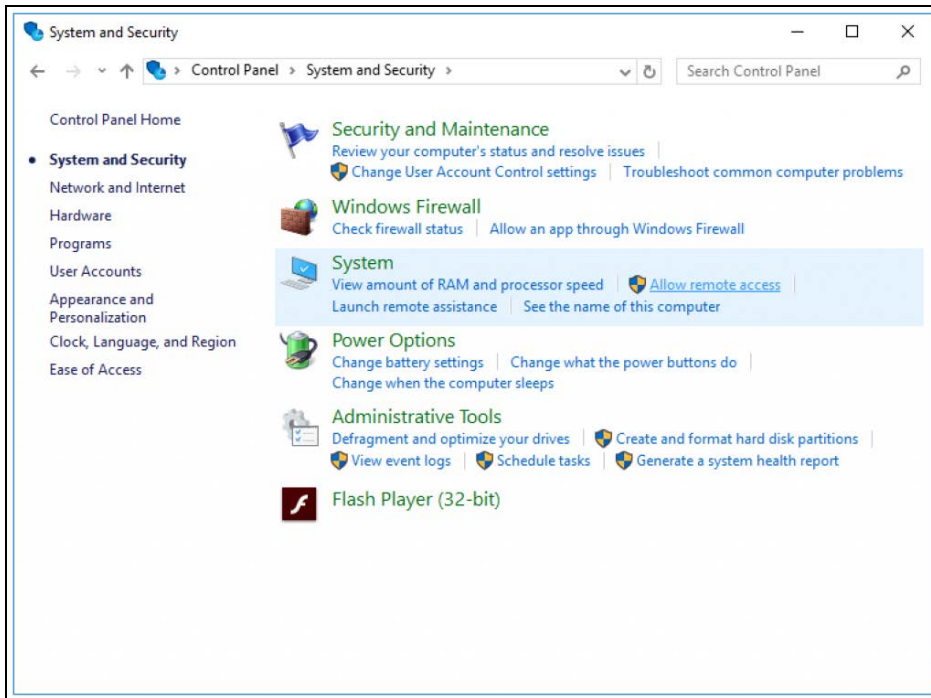
1. If password authentication is enabled, and any security mode is selected, then the upstream error implies a wrong password or username. Please make sure your credentials are correct.
2. If password authentication is disabled, simply edit the application and choose TLS as your security mode.



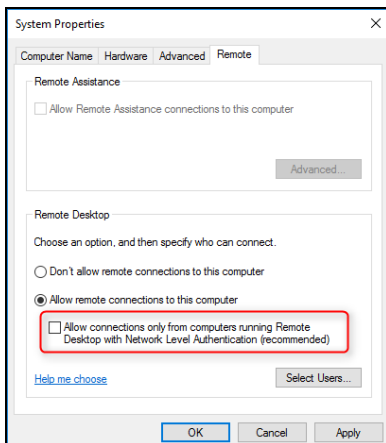
## Additional Troubleshooting steps

### Disable NLA on the local machine:

1. Open **Control Panel**. Ensure that the control panel is showing items by *Category* (i.e., not in *Classic View*).
2. Click on **System and Security**.
3. Under **System** click on **Allow remote access**.



4. Under the **Remote** group, un-tick the checkbox "Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)".



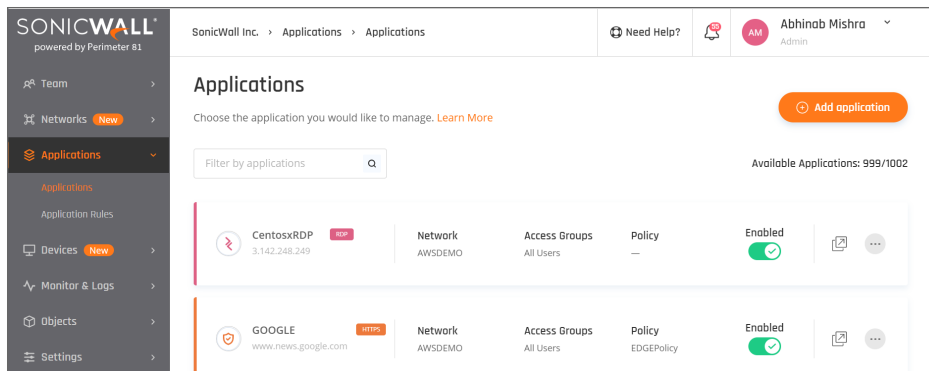
5. Click OK.

## SSH (Secure Shell)

### Adding an SSH Zero Trust application

This article describes how to configure an SSH connection to a remote server. Make sure you are familiar with the server's authentication methods (username and password or SSH keys) and that you have a tunnel connecting your network and the environment that hosts the server before you begin.

1. Go to the **Applications** tab at the SonicWall Cloud Edge Platform. Select **Add application**.



2. Fill in the following information:

The 'Add application' form is displayed with the following fields and options:

- General Settings**
- Application Name\***: Text input field with placeholder 'Enter application name'.
- Protocol\***: Dropdown menu set to 'SSH'.
- Icon**: 'Browse' button.
- Host\***: Text input field with placeholder 'Enter application hostname'.
- Port\***: Text input field with value '22'.
- Network\***: Dropdown menu with placeholder 'Select network'.
- Max. # of connections\***: Text input field with value '32'.
- Display Application Icon at Login Screen**: Toggle switch (checked).
- URL Alias**: Toggle switch (unchecked).

A help popup titled 'What is the SSH application protocol?' is visible on the right, explaining that SSH is a network protocol for secured services and is commonly used for remote connections to Linux servers on port 22. A link 'Learn about how to create SSH application' is provided.

- **Application Name:** Enter a name of your choice.
- **Protocol:** SSH
- **Icon:** Use default or choose an icon of your own choice.
- **Host:** Enter the internal IP address of the server to which you'd like to connect.
- **Port:** 22
- **Network:** Choose the network that contains the gateway from which you created a tunnel to the environment that hosts the server you'd like to connect to.
- **Display Application Icon at Login Screen:** Choose according to your preference.
- **URL Alias (Optional):** See Advanced Setting Guide.

The screenshot shows a configuration window with three main sections: Authentication, Access Groups, and Policy. The Authentication section is active, indicated by a green checkmark. It contains three input fields: Username (placeholder: Enter username), Password (placeholder: Enter password), and Domain (placeholder: Enter domain). The Access Groups section has a dropdown menu for Groups (placeholder: Select groups). The Policy section has a dropdown menu for Policy Name (placeholder: Select policy). At the bottom, there are two buttons: Cancel and Apply.

- **Authentication:** If disabled, you'll need to enter your credentials as predefined on the server with every login.
- **Username and Password:** Enter one set of credentials as predefined on the server. You will not be required to enter any parameter with the login.
- **Private Key/Username/Passphrase:** Enter your RSA-SSH key under Private Key with a correlating username (according to user settings predefined in the server). Note that a certificate typically starts with a prefix and a suffix such as the following:

```

`-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----`

```

If a passphrase is a set along with SSH key, enter it as well, else leave blank.

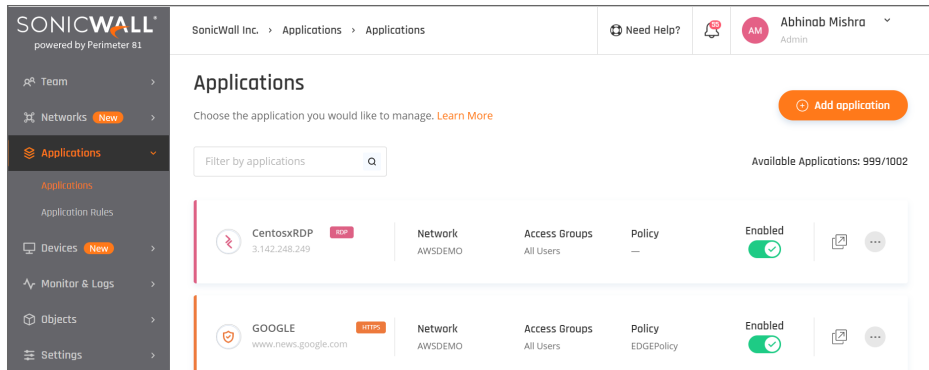
- **Access Groups:** State the names of the user groups which have access to the SSH application.
  - **Policy:** Leave blank, or choose a policy that was previously created and matches your needs.
4. Select **Apply**.
  5. To connect to the application insert the application FQDN in the URL line of your browser or connect through the **Management Platform**.

# VNC (Virtual Network Computing)

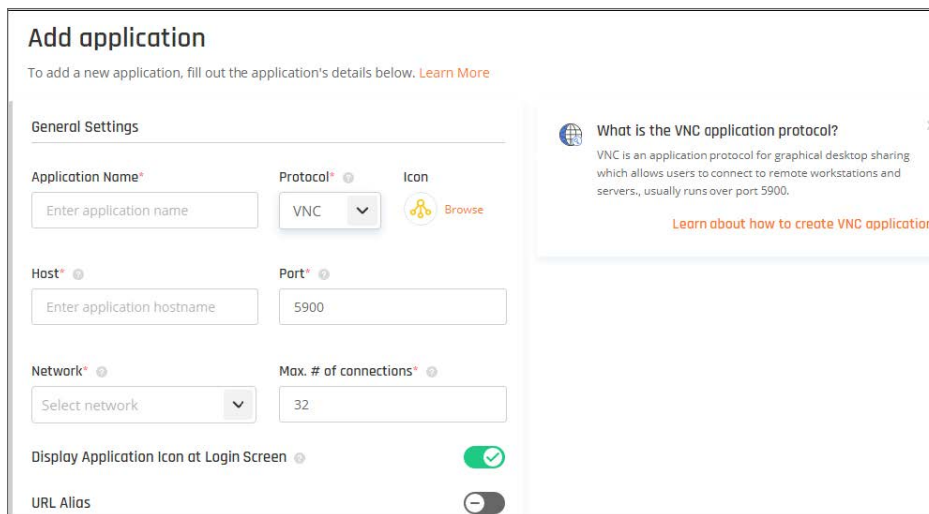
## Adding a VNC Zero Trust application

This article describes how to configure a VNC connection to a remote server (Linux or Windows). Make sure you are familiar with the server's authentication methods and that you have a tunnel connecting your network and the environment that hosts the server before you begin.

1. Go to the **Applications** tab at the SonicWall Cloud Edge Platform. Select **Add application**.



2. Fill in the following information:



**Add application**

To add a new application, fill out the application's details below. [Learn More](#)

**General Settings**

Application Name\*  Protocol\*  Icon

Host\*  Port\*

Network\*  Max. # of connections\*

Display Application Icon at Login Screen

URL Alias

**What is the VNC application protocol?**

VNC is an application protocol for graphical desktop sharing which allows users to connect to remote workstations and servers., usually runs over port 5900.

[Learn about how to create VNC application](#)

- **Application Name:** Choose an indicative name of your own choice.
- **Protocol:** VNC
- **Icon:** Use default or choose an icon of your own choice.
- **Host:** Enter the internal IP address of the server to which you'd like to connect.
- **Port:** 5900

- **Network:** Choose the network that contains the gateway from which you created a tunnel to the environment that hosts the server you'd like to connect to.
- **Max number of connections:** 1
- **Display Application Icon at Login Screen:** Default: No
- **Enable copy-paste from VNC to clipboard.** Default: Yes
- **URL Alias (Optional):** See Advanced Setting Guide.

The screenshot shows a configuration window with three main sections:

- Authentication:** A toggle switch is turned on (green checkmark). Below it are input fields for Username (placeholder: "Enter username"), Password (placeholder: "Enter password"), and Domain (placeholder: "Enter domain").
- Access Groups:** A dropdown menu labeled "Groups\*" with the placeholder text "Select groups".
- Policy:** A dropdown menu labeled "Policy Name" with the placeholder text "Select policy".

At the bottom right of the window are two buttons: "Cancel" (light blue) and "Apply" (orange).

- **Authentication:** The password predefined in your VNC.
  - **Access Groups:** State the names of the user group who'll have access to the VNC application.
  - **Policy:** Leave blank, or choose a policy that was previously created and matches your needs.
4. Select **Apply**.
  5. To connect to the application insert the application FQDN in the URL line of your browser or connect through the SonicWall Cloud Edge Platform.

## Zero Trust Policies and Rules

This article describes how to understand and use **Zero Trust** Policies and Rules.

- Understanding policies and rules
- Defining and applying policies

Zero Trust is key for using unmanaged devices on unmanaged networks as it allows you to isolate these unprotected connections from your internal networks.

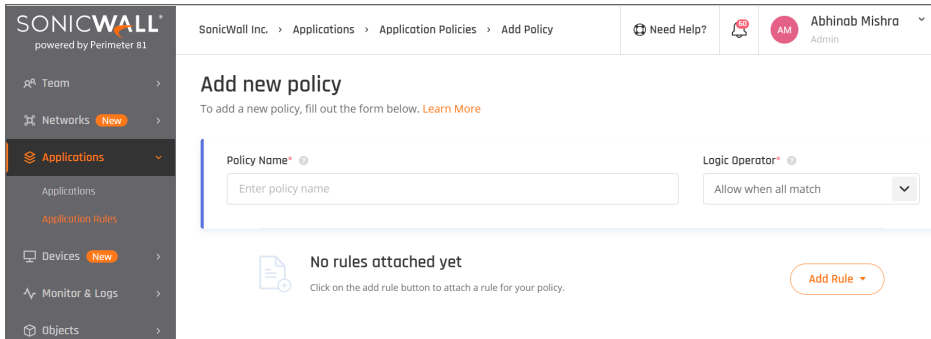
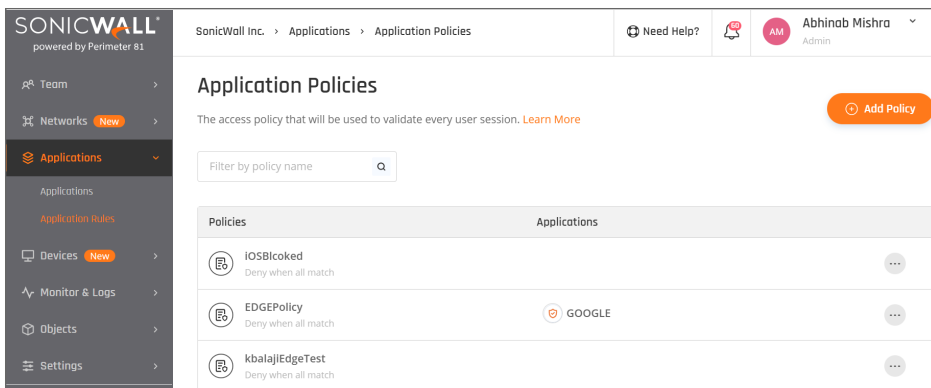
## Understanding policies and rules

Policies and rules are an additional layer of security for our Zero Trust Applications. They provide **Administrators** and **Managers** with the ability to set granular sets of rules into **Policies** that will limit access to internal and cloud resources based on **Groups, Date and Time, Geo-location, Operating Systems, rowers** and much more.

Please follow the steps below:

## Defining and applying policies

1. To set up the policy rules, go to the **Application Rules** tab under **Applications**, and select **Add Policy**.



2. Select **Add Rule**.

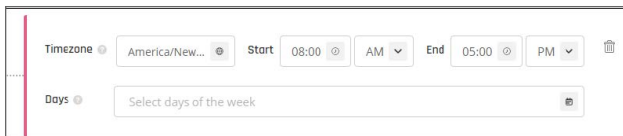


3. Choose a type of rule from the drop-down list.
4. Rules can be defined with the following parameters:

#### Group



#### Date and Time



#### Location (IP)

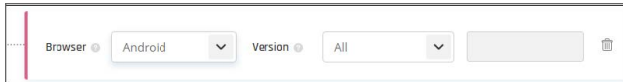


#### Location (Country)

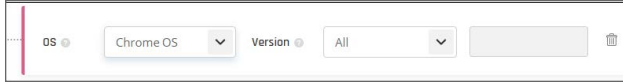


#### Browser





OS



## Agent-based Access

### Topics:

- [SonicWall Agents](#)
- [Agents Configuration](#)

## SonicWall Agents

### Topics:

- [Downloading and Installation](#)

## Downloading and Installation

### Downloading the agents

You can also find the Agents download links in the "**Downloads**" tab in your Management Web-Console. Those links are available to your end-users as-well.

#### Download links:

| Operating System | Download                  |
|------------------|---------------------------|
| MacOS            | <a href="#">DMG</a>       |
| Windows          | <a href="#">EXE, MSI</a>  |
| Linux x64        | <a href="#">DEB</a>       |
| iOS              | <a href="#">App Store</a> |
| Android          | <a href="#">PlayStore</a> |

If the devices in your organization are managed through a central desktop management tool you may prefer remote installation instead of having team members download and install the agent on their own.

## Minimum requirements

End-users should run a supported version of one of the following operating systems: Windows, Mac, iOS, Android, Linux, Chrome Browser, and routers.

① | **NOTE:** Internet Explorer 11 browser does not support Cloud Edge Secure Access web client access.

## Agents Configuration

### Topics:

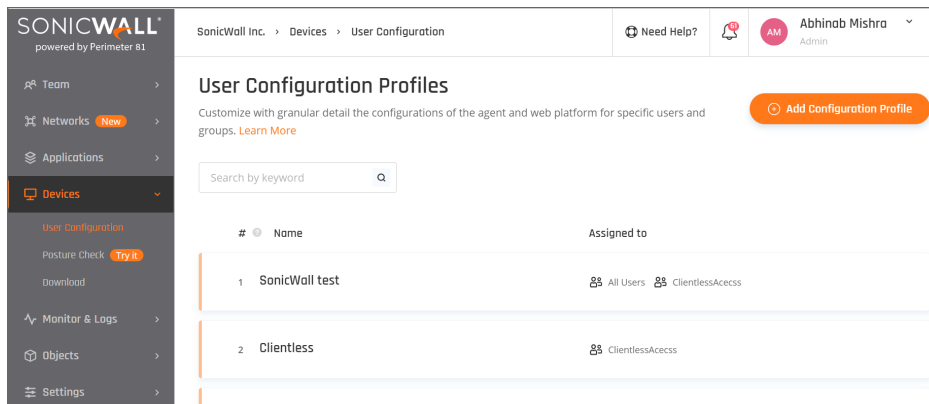
- [User-Groups Policies](#)
- [Managing Configurations](#)
- [General Configurations](#)
- [Network Configuration](#)
- [OS-Specific Configurations](#)

## User-Groups Policies

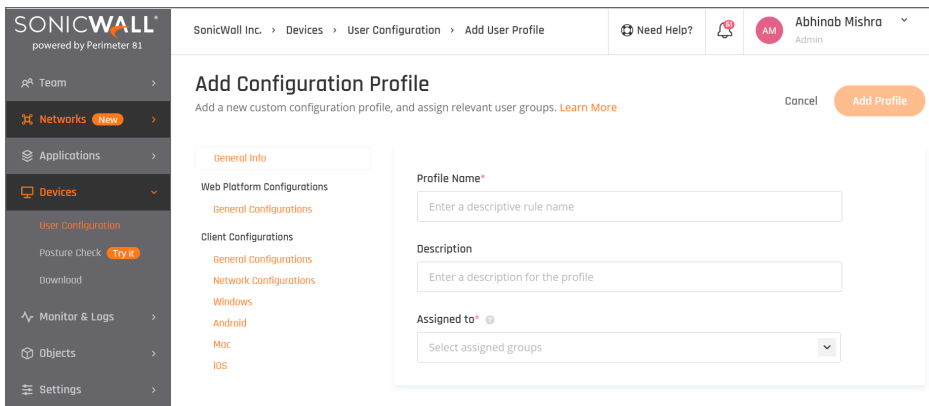
SonicWall Cloud Edge enables platform administrators to set a unique set of configurations for a specific group or multiple groups of users. Each set of configurations is called a **profile**.

### How to add a new profile?

1. Select **Devices** and then **User Configuration** on the left side of the screen.

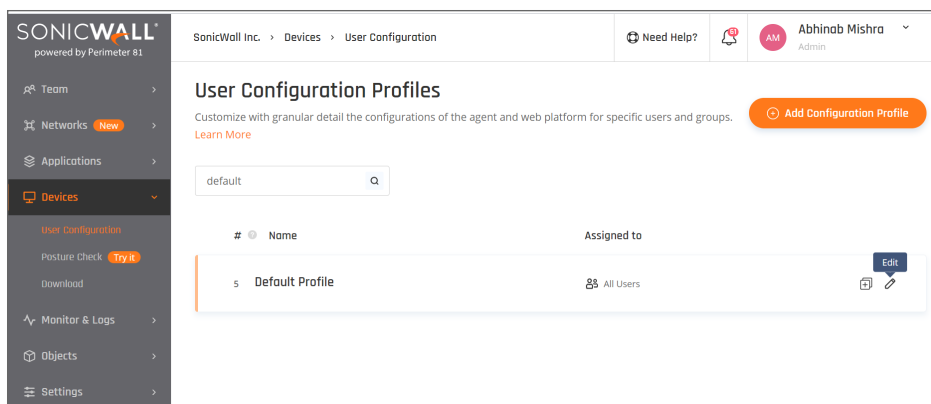


2. Select **Add Configuration Profile**.



3. Name the profile and fill in an appropriate description.
4. Assign the profile to one or more user groups.
5. Set **General Configurations**, **Network Configuration**, and **OS-Specific Configurations** according to the profile's use case.

## Default Profile



The default profile is a set of default configurations associated with every user whose group doesn't have a matching profile.

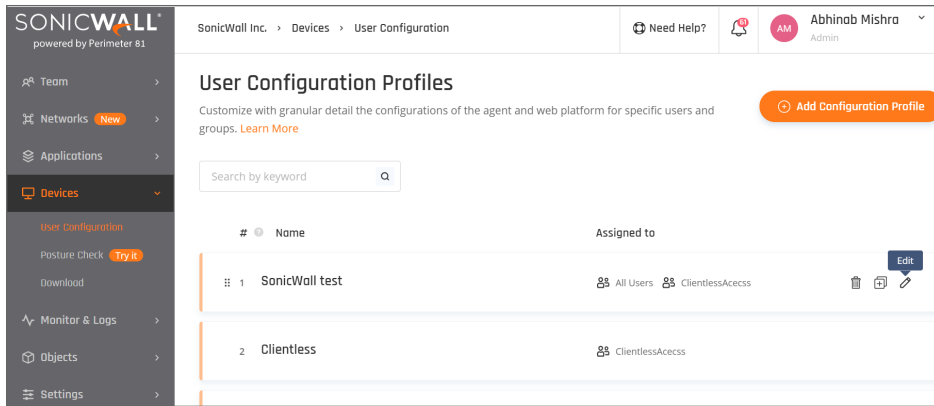
You can customize the default profile by selecting the pen icon you.

## Profile prioritization

You may have noticed that one group of users can be associated with several profiles, and one user can belong to more than one group.

The profiles that will be presented to the users once they've logged into the endpoint client will be the last profile created (in case it's associated with one of the groups that the users belong to).

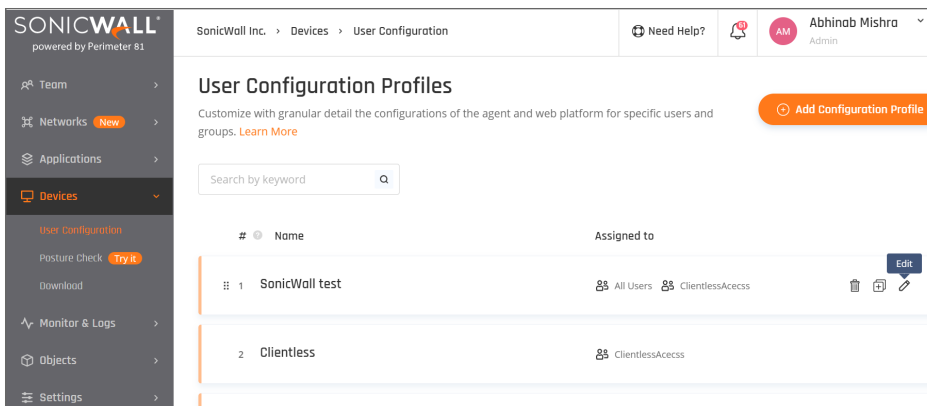
You can also customize the priority of the profile as shown below (the greater the index number is, the higher the priority it gets):



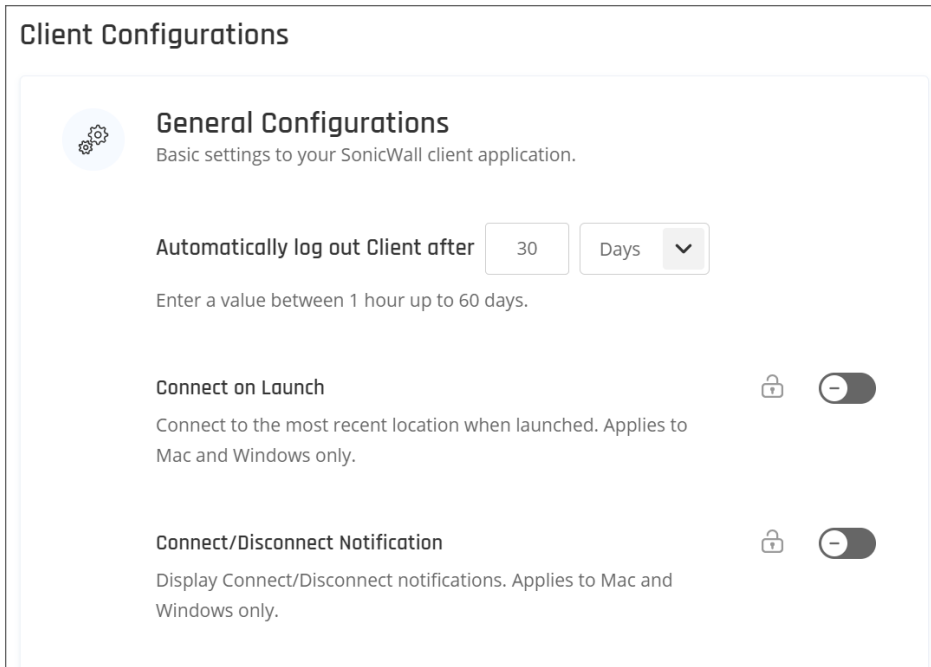
## Managing Configurations

This article describes how you can manage settings like Automatic Wi-Fi Security, Kill Switch, Crash Report, Connect on Launch, Connect/Disconnect Notification, and Trusted Wi-Fi Networks. VPN Interface DNS and iOS Auto Reconnect can be set on the Tenant Level, and you can restrict end-users to change them.

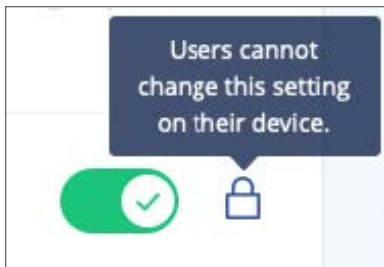
1. Select **Devices** and then **User Configuration** on the left side of the screen.



2. Select the **Client Configurations** tab.

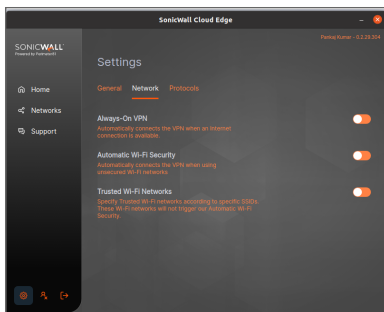


3. Select the lock icon beside the application you wish to enable or disable.



It will block the possibility for end-users to change these settings on their devices.

When end-users go to their application and open the **Settings** menu, they will see these options disabled as the trusted Wi-Fi settings here:



## General Configurations

This article describes how you'll be able to modify the following at the **General Configuration** section.

### 1. **Automatically log out Client**

Once enabled, all users will be logged out of the agents every hour (or up to 30 days, according to the value you entered).

This feature is available for Enterprise and Premium customers only.

### 2. **Public VPN Locations**

Public VPN Locations are shared secured gateways spread world-wide. While connecting to one of these will not allow you to connect to your internal resources, it can improve latency and performance-related issues (since you can pick a gateway that is close to your physical location). It can also encrypt the data being sent over the network which is highly important in case you are connected to a public Wi-Fi.

① | **NOTE:** This feature is available for Enterprise and Premium customers only.

### 3. **Connect on Launch**

Once your operating system launches, you'll be connected to the last network you've used.

① | **NOTE:** This feature is available for MacOS and Windows only.

### 4. **Connect/Disconnect Notification**

Easily monitor your connection status, with pop-up notification alerting on any disconnection or reconnection.

### 5. **Upgrade Application**

Enforce automatic application upgrades on all client applications when new versions become available.

### 6. **Crash Report**

Help us improve by sharing your crash report.

### 7. **Snowplow Report**

Help us monitor our services by sharing event and user tracking reports.

## Network Configuration

This article describes how every account administrator or manager can modify the following network settings:

### 1. **Automatic Wi-Fi Security**

Proactively protects your team members - whether they are traveling for business or working from a local cafe - from dangerous public Wi-Fi threats. Logging into unsecured public Wi-Fi hotspots can be dangerous for employees, resulting in the theft of private business data and compliance violations. This will automatically activate a VPN connection on unsecured networks as well as enable access to your company's internal resources.

### 2. **Trusted Wi-Fi Networks**

Specify Trusted Wi-Fi networks according to specific SSIDs. These Wi-Fi networks will not trigger our Automatic Wi-Fi Security feature. Applies to Mac and Windows only.

### 3. **Trusted Wired Networks**

Specify Trusted Networks according to specific MAC address of the router. These networks will not trigger our Automatic Wi-Fi Security feature or Always on VPN. Applies to Mac and Windows only.

### 4. **Always-on VPN**

Always-on VPN ensures if your VPN connection is broken, your internet connection will be cut until the VPN connection is successful.

#### 5. **Kill Switch**

This instantly kills the Internet connection should the VPN disconnect, protecting data from temporary exposure.

## OS-Specific Configurations

This article describes how some of the configurations are adapted for particular operating systems or particular devices.

### MacOS/Android

- **Default Protocol**

Depending on your local infrastructure, ISP, and internet connection type you may want to set a default protocol. While OpenVPN is an industry-standard, WireGuard is more economic in terms of CPU usage.

### iOS

- **Auto Reconnect**

Automatically reconnect to the VPN if the session disconnects or the device connects to Wi-Fi or 3G networks- without requiring login credentials.

### Windows

- **Default Protocol**

Depending on your local infrastructure, ISP, and internet connection type you may want to set a default protocol. While OpenVPN is an industry-standard, IKE is more economic in terms of CPU usage.

- **Use VPN Interface DNS**

In case split tunneling is applied, to prevent DNS leaks, the app will only allow DNS requests via the DNS server specified on the VPN network interface (if split tunneling isn't applied this will be done by default).

- **Notify Reconnect**

Display notification when the Windows application reconnects to the VPN.

# Monitoring

## Topics:

- [Activity Tracking](#)
- [Integrations](#)

## Activity Tracking

### Topics:

- [Activities and Logs](#)
- [Member Devices](#)

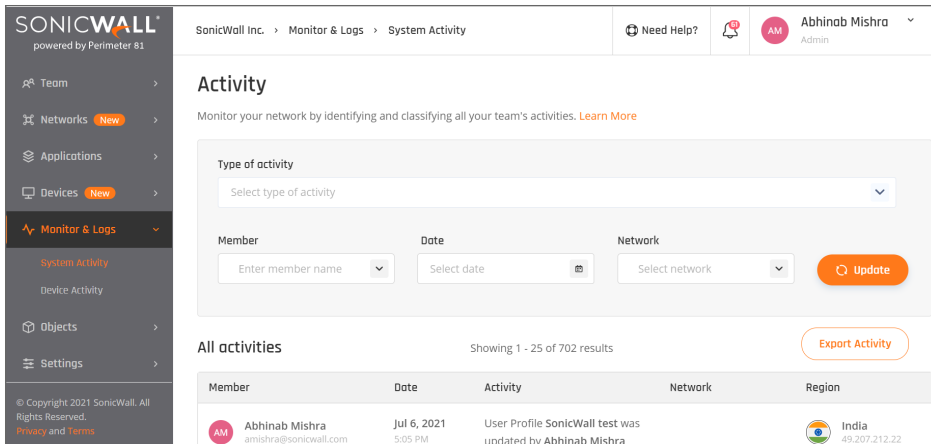
## Activities and Logs

This article describes how to use the Activity Log. Whether it be the status of your server deployments, new groups created, or recent logins, your Activity Log is the place where you can quickly get the full picture of what's going on with your network.

## Finding System Activity Logs

1. To view your system's activity, select **System Activity** in the **Monitor and Logs** section on the left side.
2. You'll see a list of team members, the date of their last activity, their latest activity on the platform, and the server location they connected to.

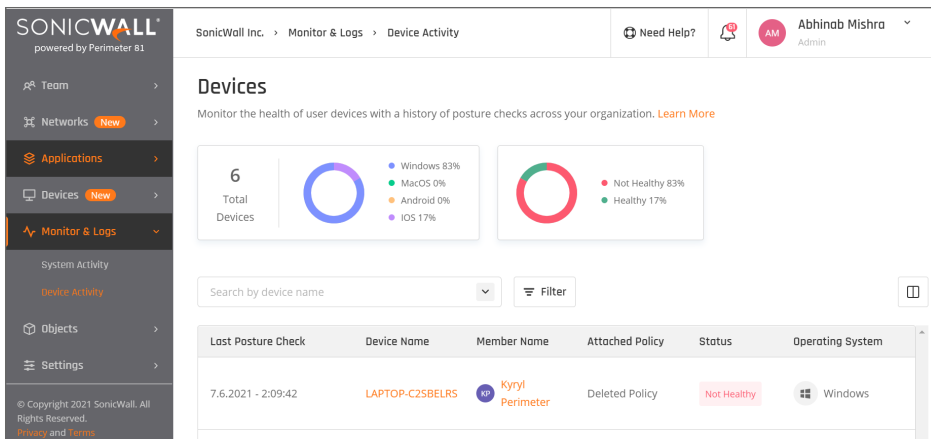




3. In the menu at the top of the screen, you can sort activities by type, date range, team member, and network (server location). You can even export this data if you wish.

## Finding Device Activity Logs

1. To view your system's activity, select **Device Activity** in the **Monitor and Logs** section on the left side.
2. You'll see a list of device posture check, device name, member name, attached policy, status, and the device operating system.



3. In the menu at the top of the screen, you can view a graph of the total devices, operating system percentage and their health status percentage.

## Monitored Activities

### Authentication

#### Event

User successfully logged into the agent

---

User failed to log into the agent

---

User successfully logged into a gateway

---

User failed to log into a gateway

---

## Groups

---

### Events

---

Group created

---

Group deleted

---

Member added to group

---

Member deleted from group

---

Group assigned to network

---

Group detached from network

---

## Members

---

### Event

---

Network deployed

---

Network deployment failed

---

Network destroyed

---

Region added

---

Region removed

---

Gateway added

---

Gateway removed

---

Gateway restarted

---

Tunnel added

---

Tunnel removed

---

Tunnel updated

---

## Zero Trust Application

---

### Event

---

Application added

---

Application deployment failed

---

Application updated

---

Application removed

---

Application user authorisation

---

Application user failed authorisation

---

Application session started

---

Application session ended

---

## Zero Trust Applications Policy

---

---

**Event**

---

Policy added

---

Policy updated

---

Policy deleted

---

**IdP**

---

**Event**

---

IdP added

---

IdP disabled

---

IdP deleted

---

**Integration**

---

**Event**

---

Integration created

---

Integration disabled

---

Integration enabled

---

Integration deleted

---

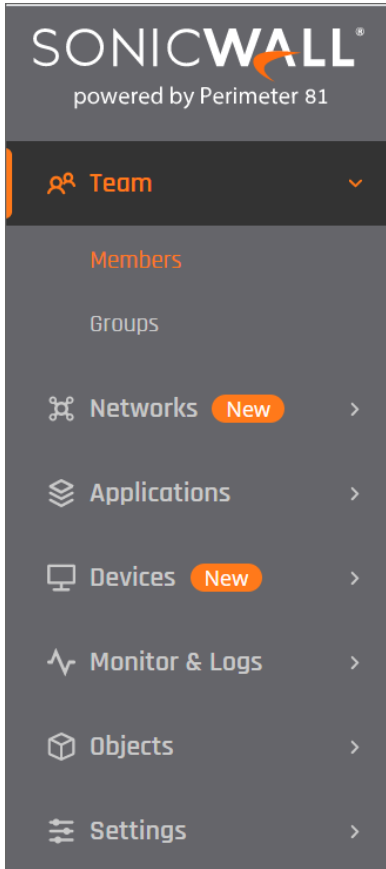
## Member Devices

This article describes how Admins and managers can easily track the devices through which end-users are connected to the SonicWall network. Please follow the steps below in order to monitor or remove one of the logged-in devices.

Important

Each user is limited to five different devices only.

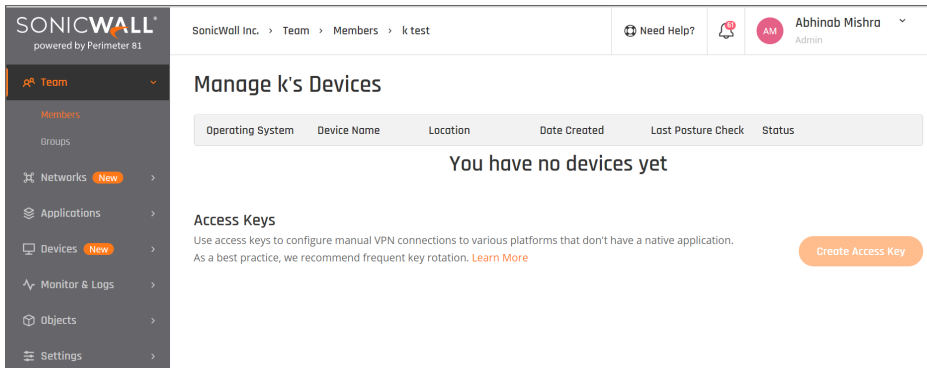
1. Open the **Management Platform**.
2. Select **Team**, then **Members**.



3. Search the member you're looking for, select the three-dotted icon, then select **Manage Devices**.

| Member                                     | Identity Provider | Role  | Last Connection | Created At               |  |
|--|-------------------|-------|-----------------|--------------------------|--|
| k test<br>kryl+test1@peri...               | Database          | User  | N/A             | Jul 5, 2021<br>8:44 PM   |  |
| Dummy Test<br>dummy@sonicwal...            | Database          | User  | N/A             | Jun 30, 2021<br>11:16 PM |  |
| Clientless Acce...<br>clientless@sonicw... | Database          | User  | N/A             | Jun 26, 2021<br>12:47 PM |  |
| seemanataraj...                            | Database          | User  | N/A             | Jun 16, 2021<br>11:19 AM |  |
| Abhinab Mishra<br>amishra@sonicwa...       | Database          | Admin | N/A             | Jun 14, 2021<br>9:55 PM  |  |

- You'll be able to see the devices through which the user connected to your network, as well as force them to log out.



## Monitoring Dashboard

This article describes how to use the Monitoring Dashboard.

The Monitoring Dashboard (beta) allows administrators and managers to gain visibility about utilisation of the various features SonicWallCloud Edge offers, as well as visualisation of usage, including active sessions, member licenses, gateway licenses and Zero Trust Applications configured.

## Active Sessions

**Agents:** Each user connected through an agent is considered an active session.

**Applications:** Each Zero Trust Application is considered a session.

For example: If a user is connected to the Network with an agent, and has two active ZTA sessions - that's a total of three active sessions.

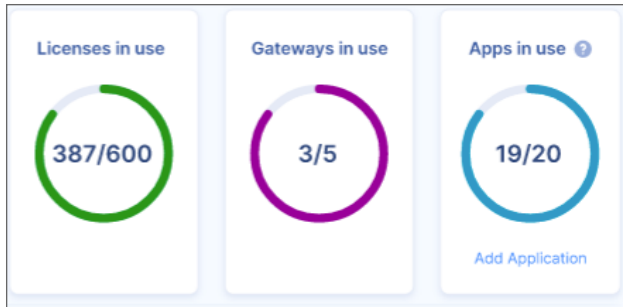


## General Information

**Member Licenses:** Number of utilized user licenses from the purchased amount.

**Gateway Licenses:** Number of utilized gateway licenses from the purchased amount.

**Applications:** Number of utilised Zero Trust Applications from the purchased amount.



## Active Agent Users

Each user connected with an agent is aggregated in this graph, you can change the view based on the Network (Private and Public), Region, Gateway, timeframe, and scale.

For example: gives the administrator the ability to know how many users were connected at a given day/time, on the Network and even Gateway level.

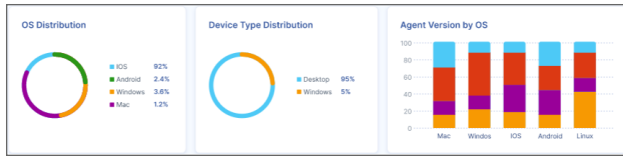


## Additional Information

**OS Distribution:** Shows the various Operating Systems used by the users.

**Device Type Distribution:** Shows Desktop and Mobile connections.

**Agent Version by OS:** Shows the version used, divided by OS.



# Integrations

## Topics:

- [Amazon S3](#)
- [Azure Sentinel](#)
- [Splunk Cloud](#)

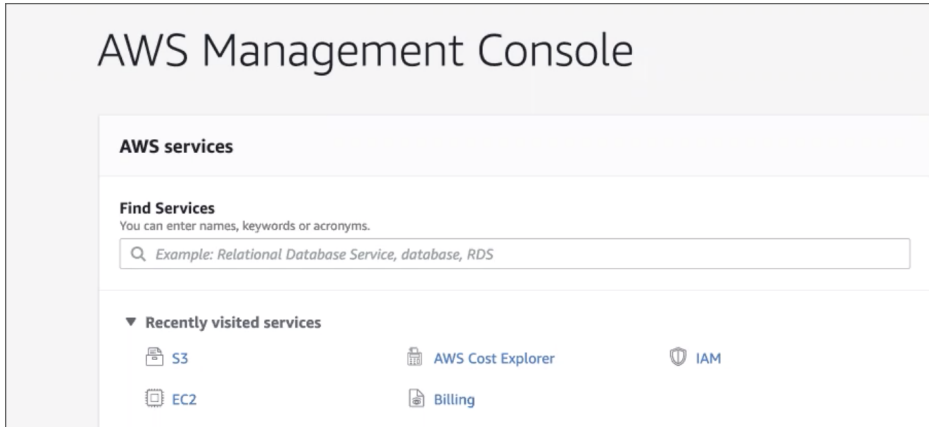
## Amazon S3

This article describes the Amazon S3 service and how to configure it. Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. You can configure your SonicWall Cloud Edge data stream to an S3 bucket to have full visibility of your SonicWall Cloud Edge activity.

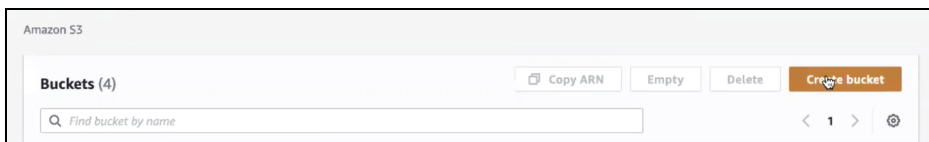
- Creating a new bucket
- Creating a new IAM Policy
- Creating an AWS Access Key
- Connecting the S3 bucket to SonicWall Cloud Edge
- Dealing with possible error codes

# Create a new Bucket

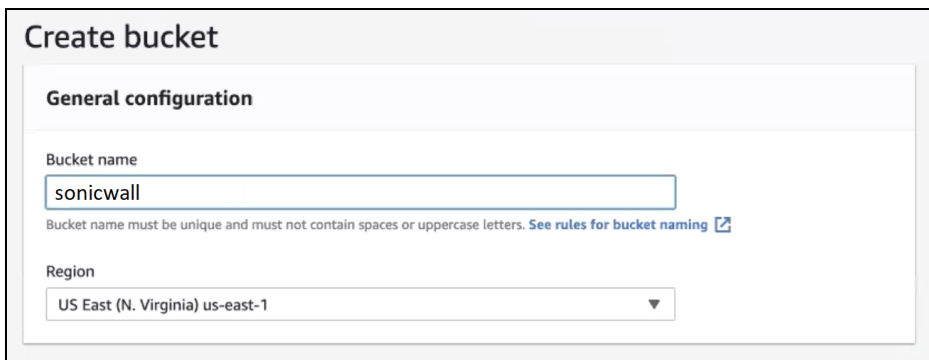
1. Open the AWS Management Console and select **S3**.



2. Select **Create Bucket**.



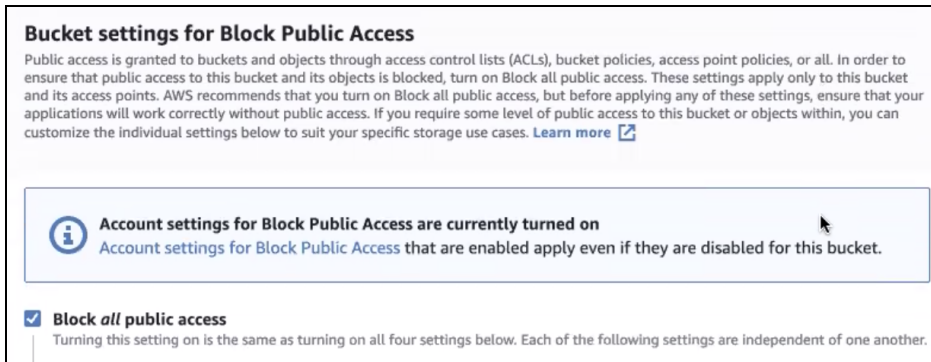
3. Fill in the following information:



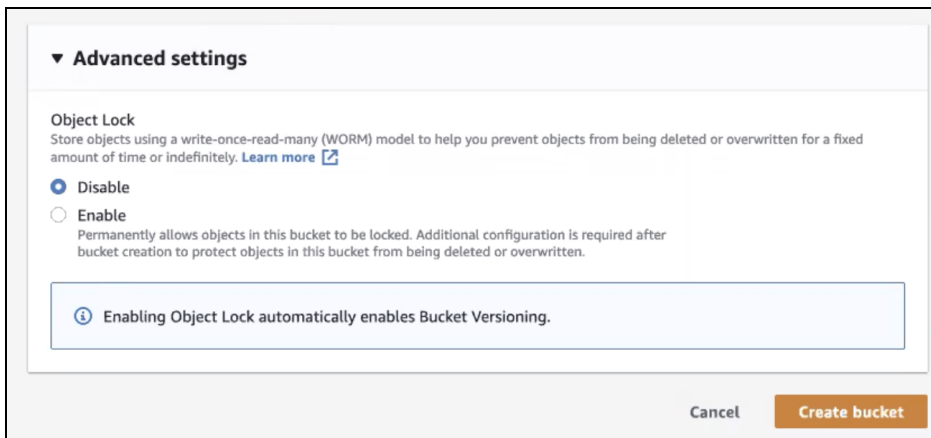
- **Bucket name:** Enter a name of your choice.
- **Region:** Amazon S3 creates buckets in a Region you specify. To optimize latency, minimize costs, or



address regulatory requirements, choose any AWS Region that is geographically close to you.



- Block all public access is checked by default. You may choose to customize it according to your company policy.

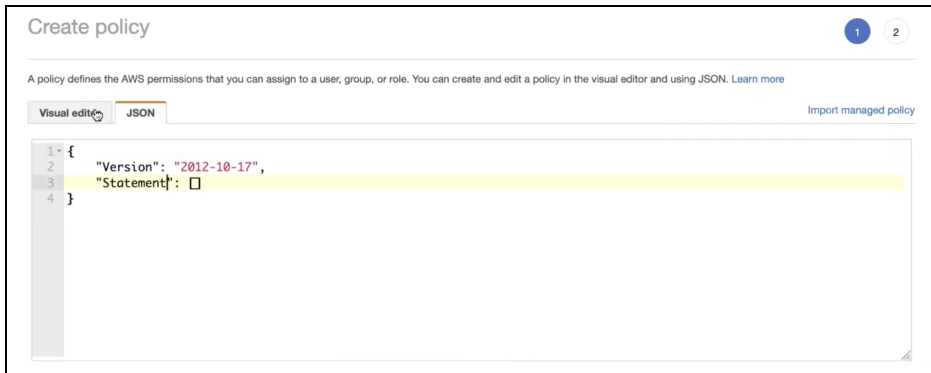


- Disable object lock, then select **Create bucket**.

## Create a new IAM Policy

① **IMPORTANT:** At this point, you can choose to grant the user full access to your S3 buckets (by attaching the appropriate AWS managed policy) or create a new policy that applies only to the SonicWall Cloud Edge bucket. If you choose the first option, you may skip this section.

1. Open the AWS Identity and Access Management (**IAM**) dashboard.
2. Go to the **Policies** tab and select **Create policy**.
3. Paste the following snippet as a JSON file. Replace test with the bucket name, then select **Review policy**.



```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test"
        },
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test/*"
        }
    ]
}

```

- ❶ **IMPORTANT:** The template presented above, while scoped to a single bucket associated with SonicWall Cloud Edge's logs only, will grant a wide variety of permissions. If for any reason you choose to limit the list of permissions, make sure that at the very least it includes parts highlighted below:

```

{
  "Version" : "2012-10-17" ,
  "Statement" : [
    {
      "Effect" : "Allow" ,
      "Action" : ["s3:ListBucket" ],
      "Resource" : ["arn:aws:s3::: test  " ]
    },
    {
      "Effect" : "Allow" ,
      "Action" : [
        "s3:PutObject" ,

```

```

    "s3:GetObject" ,
    "s3:DeleteObject" ],
    "Resource" : [ "arn:aws:s3::: test /*" ]
  }
]
}

```

**Review policy**

**Name\***   
Use alphanumeric and "+,=,@,\_" characters. Maximum 128 characters.

**Description**   
Maximum 1000 characters. Use alphanumeric and "+,=,@,\_" characters.

**Summary**

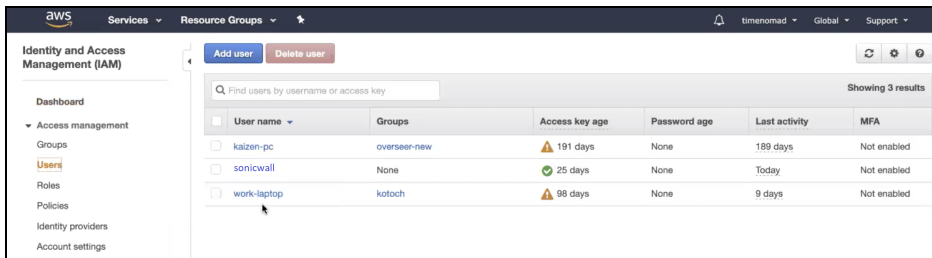
| Service                                      | Access level               | Resource | Request condition |
|--|----------------------------|----------|-------------------|
| Allow (1 of 226 services) Show remaining 225 |                            |          |                   |
| S3   | Limited: List, Read, Write | Multiple | None              |

4. Fill in the following information, and then select **Create policy**.

- **Name:** Enter a name of your choice.
- **Description** (optional): Let other users in your account know what this policy aims for.

## Create an AWS access key

1. Open the AWS Identity and Access Management (IAM ) dashboard.
2. Go to the **Users** tab and select **Add user**.



- Fill in the following information, then select **Next**.

The screenshot shows the 'Add user' page with step 1 highlighted. The 'Set user details' section has a text input for 'User name\*' containing 'sonicwall-iam-user' and a blue '+ Add another user' button. The 'Select AWS access type' section has two radio buttons: 'Programmatic access' (selected) and 'AWS Management Console access'.

- Username:** Enter a name of your choice.
  - Access type:** Select **Programmatic access**.
- Select **Attach existing policies directly** and choose the policy you created earlier (if you skipped the previous section, select the S3 full access AWS managed policy). Select **Next**.

The screenshot shows the 'Add user' page with step 2 highlighted. The 'Set permissions' section has three buttons: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly' (highlighted). Below is a 'Create policy' button and a table of policies.

| Policy name  | Type             | Used as |
|--|------------------|---------|
| <input checked="" type="checkbox"/> iam-user-for-sonicwall | Customer managed | None    |

- Add tags you may find useful in identifying the user (optional), then select **Next**.

The screenshot shows the 'Add user' page with step 3 highlighted. The 'Add tags (optional)' section has a table with columns 'Key', 'Value (optional)', and 'Remove'. There is an 'Add new key' button and a text input field.

| Key                                      | Value (optional)     | Remove |
|--|----------------------|--------|
| <input type="text" value="Add new key"/> | <input type="text"/> |        |

- Review and select **Create user**.

6. Copy and save the **Access key ID** and the **Secret access key**, then select **close**.

| User               | Access key ID        | Secret access key |
|--------------------|----------------------|-------------------|
| sonicwall-iam-user | AKIA5IZ3STOTYDXCZBEG | ***** Show        |

## Connect the S3 bucket to SonicWall Cloud Edge

1. Log in to your SonicWall Cloud Edge **Management Platform**, and navigate to **Settings/Integrations** and select **Add** at the Amazon S3 row.

**Integrations**  
Integrate SonicWall with your applications.

- Splunk**  
Forward SonicWall events to your Splunk instance. [Add](#)
- Azure Sentinel**  
Forward SonicWall events to Azure Sentinel. [Add](#)
- Amazon S3**  
Forward SonicWall event batches to Amazon S3. [Add](#)

2. Fill in according to the values copied in the previous steps (the primary key will be used as your workspace key).

## Amazon S3 ✕

If you have any questions about integration with Amazon S3, [click here](#).

**Access Key ID\*** ?

**Secret Access Key\*** ?

**Bucket Name\*** ?

**Bucket Region\*** ?

Cancel
Validate

3. Select **Validate**.

## Handling possible error codes

| Status message               | Action required  |
|------------------------------|--|
| Success                      | None   |
| S3_INVALID_ACCESS_KEY_ID     | Make sure you copied correctly the access key ID   |
| S3_INVALID_SECRET_ACCESS_KEY | Make sure you copied correctly the secret access key.  |
| S3_INVALID_BUCKET            | Make sure the Bucket name in SonicWall Cloud Edge matched the Bucket name in S3 (case sensitive).                    |
| S3_ACCESS_DENIED_BUCKET      | The IAM user doesn't have the required access permissions to the bucket. Make sure to attach the appropriate policy. |

# Azure Sentinel

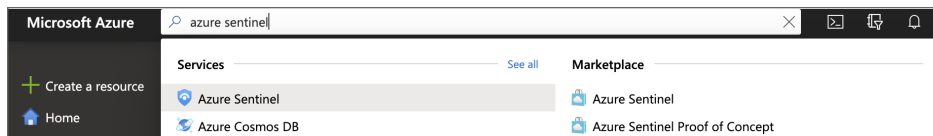
This article describes how to set up and use Azure Sentinel. It is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution that integrates with the SonicWall Cloud Edge platform. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. You can configure your SonicWall Cloud Edge data stream to Azure Sentinel to have full visibility of your SonicWall Cloud Edge activity.

- Setting up a Log Analytics workspace
- Linking the Log Analytics Workspace to Azure Sentinel
- Finding your Log Analytics Workspace ID and Primary Key
- Configuring the integration in the Management Platform
- Handling possible error codes

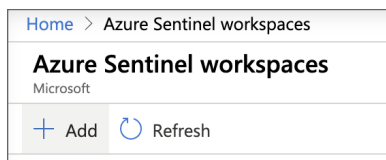
## Setting up a Log Analytics workspace

If you are using an existing log analytics workspace, you may skip this part.

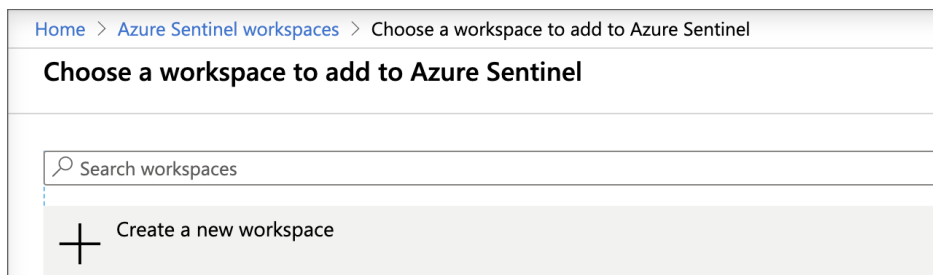
1. Open the Azure portal and select **Azure Sentinel**.



2. Select **+Add**.



3. Select **Create a new workspace**.



4. Fill in the following information:

### Create Log Analytics workspace

**Basics** Pricing tier Tags Review + Create

With Azure logs, you can easily store, retain, and query your Azure and other resources for valuable insights and monitoring. Azure Logs workspace is the logical storage unit where your various logs are stored. [Learn more](#)

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

Subscription \* ⓘ

Resource group \* ⓘ   
[Create new](#)

**Instance details**

Name \* ⓘ

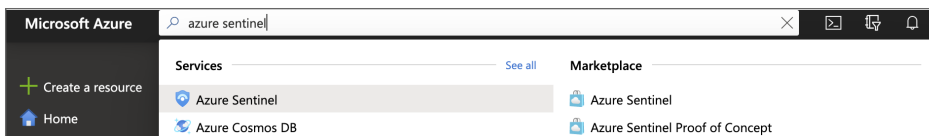
Region \* ⓘ

[Review + Create](#) << Previous Next: Pricing tier >

- **Subscription:** Choose a subscription according to your business's needs.
- **Resource group:** Associate the log analytics workspace with the appropriate business unit.
- **Name:** Choose an indicative name of your own choice. The workspace name should include 4-63 letters, digits, or '-'. The '-' shouldn't be the first or the last symbol.
- **Region:** The physical location of the server generating the event collector. Choose according to pricing and business needs.
- (Optional) Review the pricing tiers and set appropriate tags for the workspace.
- Select **Review + Create**.

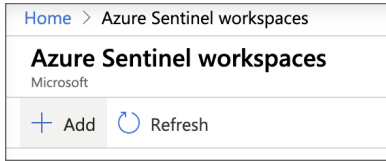
## Linking the Logs Analytics workspace to Azure Sentinel

1. Open the Azure portal and select **Azure Sentinel**.



2. Select **+Add**.

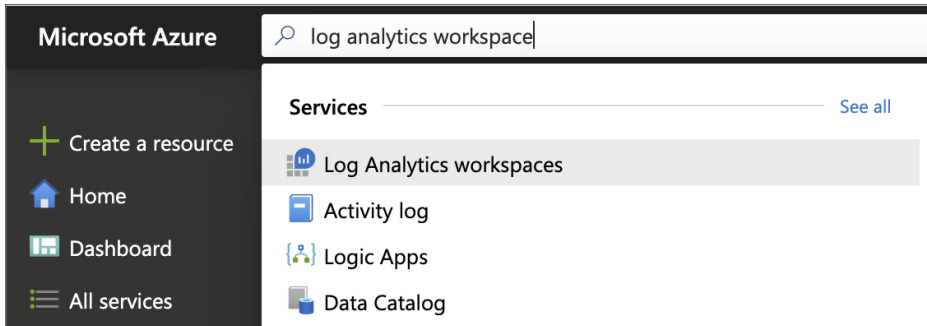




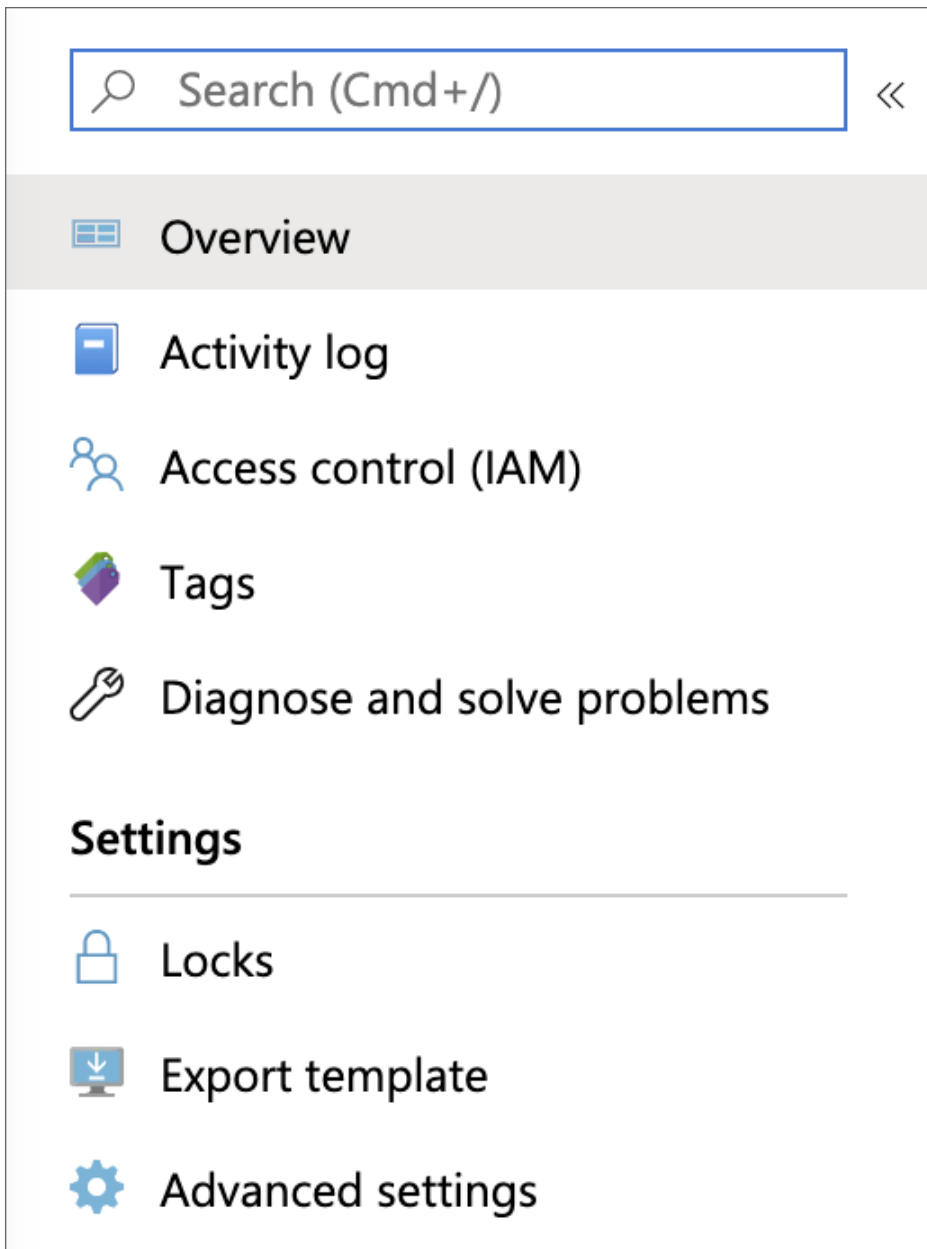
3. Select the **Logs Analytics Workspace** that you've just created or an existing one you'd like to utilize.

## Finding your Log Analytics workspace ID and primary key

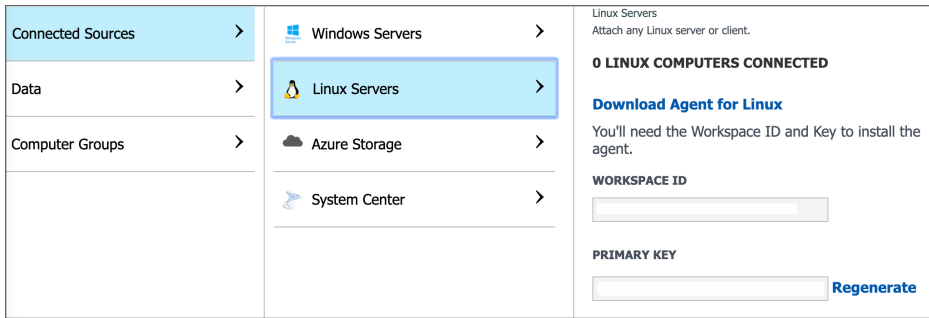
1. Open **Log Analytics Workspace**.



2. Select the workspace you've just connected to Azure Sentinel.
3. Select **Advanced settings**.



4. Select **Connected Sources**, then **Linux Servers**. Copy the **Workspace ID** as well as the **Primary key**.



## Configuring the integration at the Management Platform

1. Log in to your Management Platform, and navigate to **Settings/Integrations**, and select **Add** at the Azure Sentinel row.
2. Fill in according to the values copied in the previous steps (the primary key will use as your workspace key).

### Azure Sentinel ✕

If you have any questions about integration with Azure Sentinel, [click here](#).

**Workspace ID\*** ?

**Workspace Key\*** ?

Cancel
Validate

3. Select **Validate**.

## Handling possible error codes

| Status Message | Action Required |
|----------------|-----------------|
| Success        | None            |

---

|                                |  |
|--------------------------------|--|
| SENTINEL_INACTIVE_CUSTOMER     | The workspace has been deactivated.  |
| SENTINEL_INVALID_CUSTOMER_ID   | Please make sure you inserted the correct customer ID.   |
| SENTINEL_INVALID_AUTHORIZATION | The service failed to authenticate the request. Verify that the workspace ID and connection key are valid. |

---

## Splunk Cloud

This article describes how to configure Splunk Cloud. It is a software product that enables you to search, analyze, and view the data gathered from the components of your IT infrastructure or business. Splunk collects data from websites, applications, sensors, devices, and so on. You can configure Splunk Cloud to have full visibility of your SonicWall Cloud Edge activities.

- Setting up the Splunk Event Collector
- Enabling an HTTP Event Collector
- Creating an Event Collector token
- Configuring the Management Platform
- Handling possible error codes

## Setting up the Splunk Event Collector

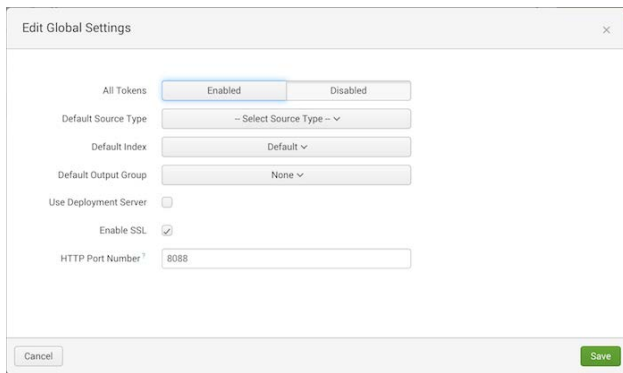
The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token-based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. This process eliminates the need for a Splunk forwarder when you send application events.

After you enable HEC, you can use HEC tokens in your app to send data to HEC. You do not need to include Splunk credentials in your app or supported files.

## Enabling an HTTP Event Collector

**NOTE:** According to official Splunk documentation, **Managed Splunk Cloud** customers may need to contact Splunk support to perform this step.

1. Click **Settings > Data Inputs**.
2. Click **HTTP Event Collector**.
3. Click **Global Settings**.



4. In the **All Tokens** toggle button, select **Enabled**.
5. To have HEC listen and communicate over HTTPS rather than HTTP, click the **Enable SSL** checkbox (This is enabled by default in Splunk Cloud and can be disabled in Splunk Enterprise only).
6. Click **Save**.

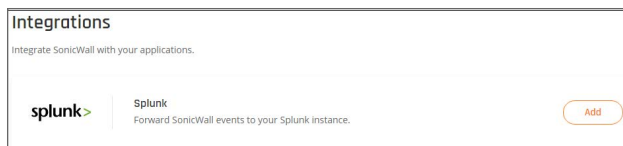
## Creating an Event Collector token

1. Click **Settings > Add Data**.
2. Click **monitor**.
3. Click **HTTP Event Collector**.
4. In the **Name** field, enter a name for the token.
5. Make sure indexer acknowledgment is disabled for this token.
6. Click **Next**.
7. Click **Review**.
8. Confirm that all settings for the endpoint are what you want.
9. If so, click **Submit**.

## Configuring the Management Platform

You need to configure the integration from the SonicWall Cloud Edge side.

1. Log in to your SonicWall Cloud Edge Management Platform, and navigate to **Settings** and select **Add** at the Splunk row.



2. Fill in the following information:

- **HEC Host:** Enter an appropriate value according to your Splunk tier (replace {hostname} with your Splunk server hostname).
  - Splunk Cloud (paid): inputs-<host>
  - Splunk Cloud (free-trial): <host> OR inputs.<host>
- **HEC port:** 8088 for Splunk Cloud free trial and 443 for Splunk Cloud paid
- **Protocol:** HTTP for a free trial and HTTPS for paid.
- **Verify Server SSL Certificate (HTTPS only):** If you are using a self-signed certificate disable SSL verification, however, if you are using a CA-signed certificate make sure to enable it.
- **HEC URI:** Filled automatically
- **Authentication token:** Insert the token you generated at Splunk.

3. Select **Validate**.

## Handling possible error codes

The following status codes have particular meaning for all HTTP Event Collector endpoints:

| HTTP status code ID | HTTP status code | Status message        | Action required  |
|---------------------|------------------|-----------------------|--|
| 200                 | Ok               | Success               | None   |
| 403                 | Forbidden        | Token disabled        | Enable token at Splunk Web.  |
| 401                 | Unauthorized     | Invalid authorization | Please make sure you inserted a valid token.   |
| 403                 | Forbidden        | Invalid token         | Please make sure you inserted a valid token.   |
| 500                 | Internal Error   | Internal server error | Please contact our support team indication the error. We will examine the integration logs and further instruct you. |

---

|     |                     |                                  |  |
|-----|---------------------|----------------------------------|--|
| 503 | Service Unavailable | Server is busy                   | There are too many requests pending in the Splunk server queue. Please try again later.                              |
| 400 | Bad Request         | Data channel is missing          | Edit the token at the Splunk Platform and make sure to untick Indexer Acknowledgement.                               |
| 400 | Bad Request         | Error in handling indexed fields | Please contact our support team indicating the error. We will examine the integration logs and further instruct you. |

---

# Compliance

## Topics:

- [HIPAA](#)
- [GDPR](#)
- [SOC 2 Type 2](#)

## HIPAA

### Information Protection

This article describes what HIPAA is and how it relates to your organization. HIPAA compliance encompasses limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals' rights with respect to their health information. SonicWall offers [two-factor authentication](#) via SMS/push notifications, Google Authenticator, and Duo Security.

### Integrity Controls

HIPAA compliance requires that covered entities must implement policies and procedures to ensure that ePHI is not improperly altered or destroyed. VPNs use authentication to confirm whether data has been accessed or tampered with, providing straightforward integrity control. Using pre-shared keys, a VPN can identify, authenticate, and authorize user access.

### Access Control

A covered entity must implement centrally-controlled unique credentials for each user. A VPN that offers a centralized cloud management platform allows organizations to create customized user access to sensitive data. That includes cloud environments, SaaS services, sandbox and production environments, and more.



## Network Security

To protect against unauthorized public access to ePHI, authorized users must encrypt all data that is sent beyond an internal firewalled server. Using a VPN, data passing over any network is secured with advanced encryption. This creates a virtual tunnel so data can't be intercepted by snoopers, hackers, or third parties.

## GDPR

### Data Protection

This article describes what are the **General Data Protection Regulation** (GDPR) requirements. These requirements include 160 different regulations on how you collect, store, and use customer data, which is why finding an effective security solution is essential for compliance. Penalties for violations of record-keeping, security, breach notifications, or privacy obligations can reach ten million euros, or two percent of income – whichever is larger.

### Detect

Allows businesses to identify personal data bound by GDPR requirements, determine where it is located, and secure these resources accordingly.

### Manage

Customize user access to the network to secure sensitive data with the connector. By assigning user roles to groups and securing resources with private servers, you can finally govern how data is used.

### Protect

Protect user data beyond EU regulatory standards with a holistic security solution that encrypts transmitted data and secures access to the network both on-site and remotely.

### Report

With SonicWall's Activity feature, IT staff can monitor, report, and respond to data requests and breaches. With GDPR in full effect, you must implement necessary security measures to secure customer data. With SonicWall, we make security simple and easy to use so that you can protect your data worry-free.

# SOC 2 Type 2

## Auditing

This article describes what SOC 2 is and how it relates to your organization. SOC 2 is a technical audit that requires companies to establish and follow strict information security policies and procedures. A SOC 2 compliant service must follow these five “trust service principles” when managing customer data.

## Security

System resources must be protected from unauthorized access or improper disclosure of information. To secure access, organizations can implement security tools such as [two-factor authentication](#), web application firewalls (WAFs), Cloud VPNs, and [Software-Defined Perimeters](#) (SDPs).

## Availability

Accessibility of the system is determined by a contract or service level agreement (SLA). While this doesn't apply to system functionality, it does require network performance to be monitored, including security incidents, site failover, and other security-related issues that may affect availability.

## Processing Integrity

To achieve processing integrity, the system must provide efficient data processing by delivering complete and valid information to the right place at the right time. By monitoring data and implementing quality assurance, organizations can begin to ensure processing integrity.

## Confidentiality

Confidential data must be hidden from unauthorized persons or organizations. Network and application firewalls along with access controls are essential for safeguarding sensitive data. Additionally, encryption can be used to protect confidentiality during transmission.

## Privacy

Organizations must meet privacy standards that address the collection, use, retention, disclosure, and disposal of personal information by the AICPA's Generally Accepted Privacy Principles (GAPP).

# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

Cloud Edge Secure Access Getting Started Guide  
Updated - March 2023  
232-005537-00 Rev F

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035