Cloud Edge Secure Access

User Guide

SONICWALL®

Contents

1

Web-Console

Topics:

Accessing the Account

Topics:

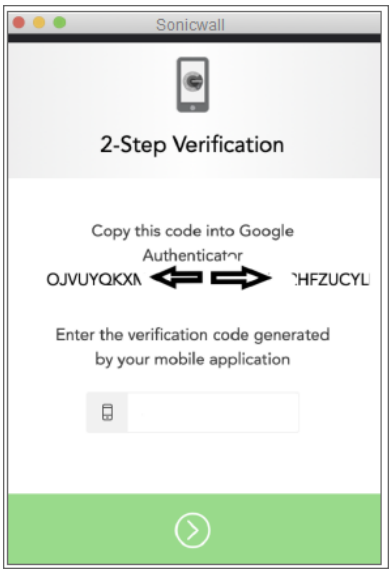
Google Authenticator

Topics:

First time Configuration

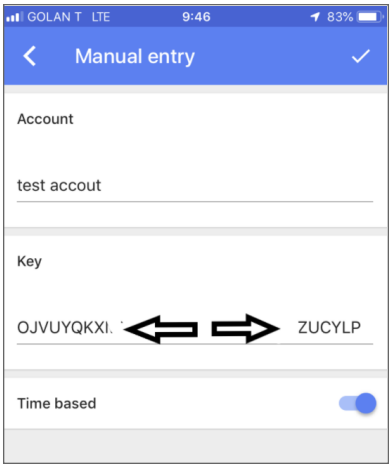
1. Download Google Authenticator on your Mobile:
    - Android
    - iOS

2. Once you have installed the application on your mobile, copy the code on the application (or scan the QR code):



The app will give you the authentication code to login in to the SonicWall Cloud Edge application.

3. On your Google Authenticator app on your mobile, tap on the " + " and then **Enter a provided key**.

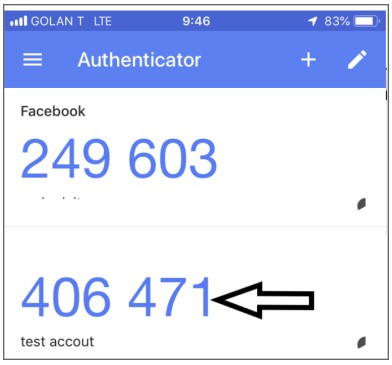


4. You need to type letter by letter the code that appears on your screen (this is done just once). This should set up your two-factor authentication and after this, you should be able to log in.
5. Make sure to switch the toggle to enable the**Time-Based** option, to ensure the code you are entering is aligned with the Authenticator's most recent passcode generation.

Login

Each time you log into the account you ensure you are connected with Google Authenticator.

1. Open the **Google Authenticator** app, and the app generates the a six-digit verification code. Enter the six-digit verification code.

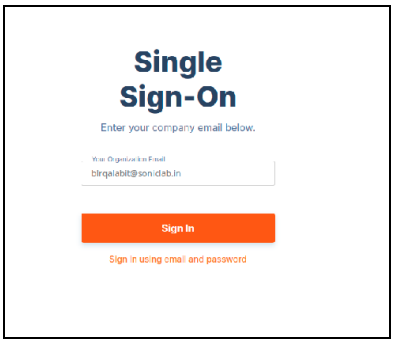


Reclaim Access after an IdP Lock

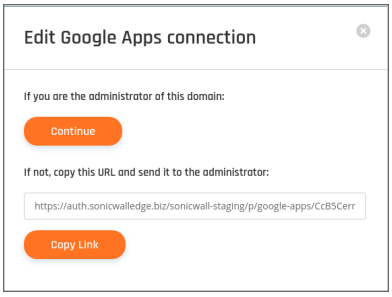
If you've successfully configured an IDP integration, however, you are unable to login to the SonicWall Cloud Edge Platform or apps, go through the following steps:

1. Go to *myworkspace.sonicwalledge.com* (insert your workspace name instead of myworkspace).
2. Enter your email address.

3. Select **Sign in using email and password** and enter your initial SonicWall Cloud Edge credentials.



4. Make sure to configure your settings so you can use your IDP Admin APIs. If you're the administrator, you can select **Continue** on the **Connection Settings** page. If not, provide the URL to the administrator, so the required settings can be adjusted.



Make sure your configurations are correlating our official guides (Google, Okta, OnLogin, or any other).

Managing the Account

Topics:

- Reset 2FA
- Deactivating 2FA
- Set Network Icon

Reset 2FA

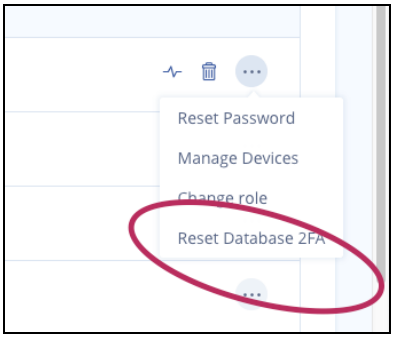
ⓘ | **IMPORTANT:** This action can be performed only by a Member with the role of an Admininstrator.

Reset MFA

When a user changes a mobile phone they may need to re-configure the Google 2FA on the new device.

To re-configure the Google 2FA on the new device:

1. Log in to the Web Administration Console
2. Navigate to **Team** > **Members**
3. Find the Member that needs the MFA reset and click on the three-dotted menu **(...)** on the right side of the Member's name:
4. Select **Reset Database 2FA**:

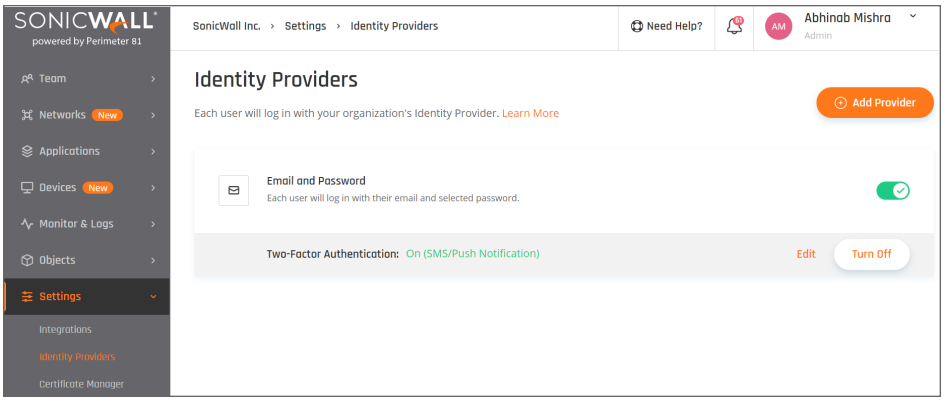


5. The system will prompt a confirmation message:

The Member will get an email confirmation with the two-factor authentication reset and a link to re-activate 2FA.

Deactivating 2FA

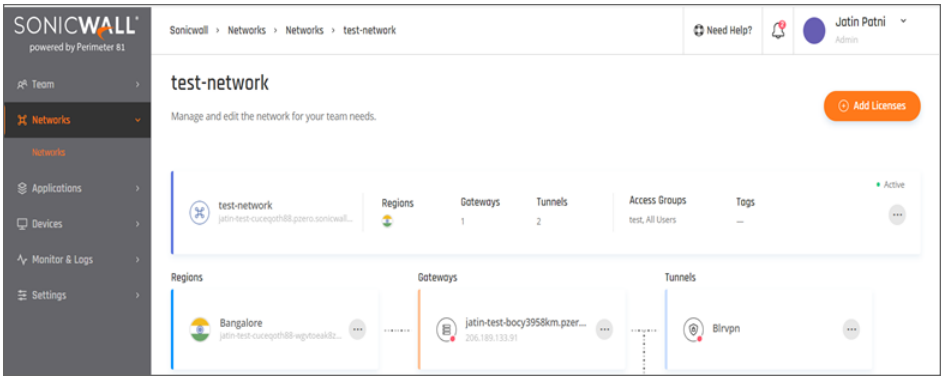
1. To deactivate two-factor authentication, select **Settings** in the **Management Portal** on the left side and then select the **Identity Providers** tab. Select **Two-factor Authentication** and select **Turn Off.**



2. A verification screen will appear. Select **Deactivate** to confirm.

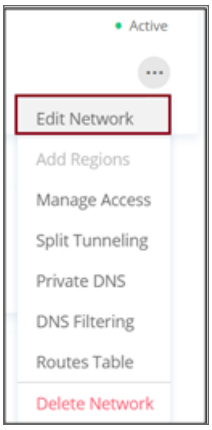
Set Network Icon

1. In **Management Portal** on the left pane, select **Networks**.

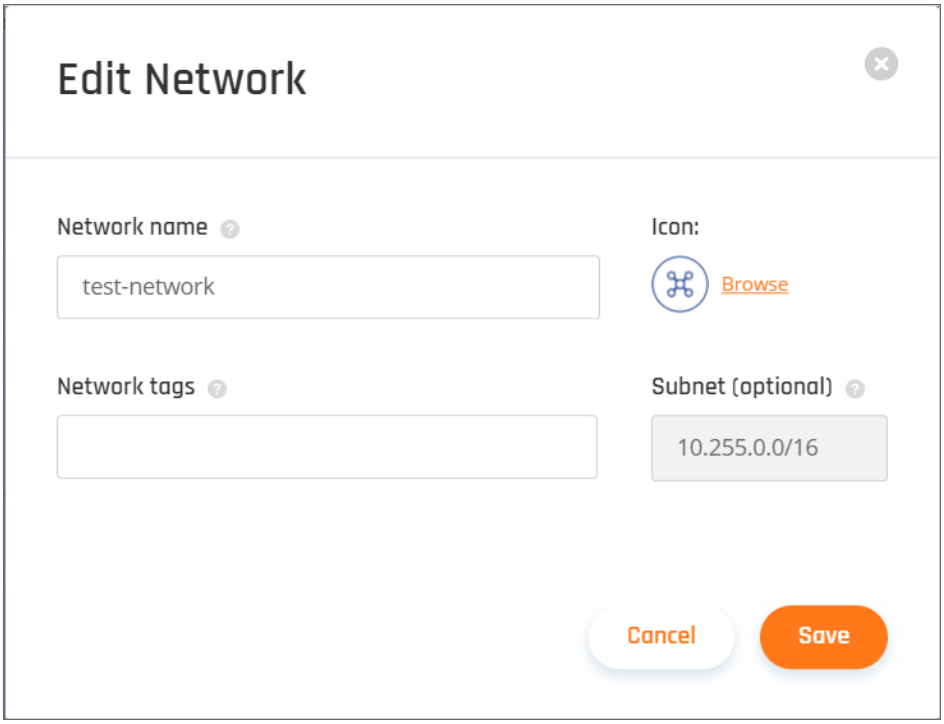


   The existing **Networks**, **Regions**, **Gateways**, **Tunnels**, **Access-Groups**, and **Tags** appear.

2. Select the three-dotted menu (...).
3. Click **Edit Network**.



4. Under **Icon**, click **Browse**.



5. Browse to the folder where the required icon is saved.
6. Select the required icon and click **Save**.
   The selected network icon appears.

Tracking the billing

Topics:

- Modify Subscription Plan

Modify Subscription Plan

There are several different plans and every organization can find a plan that best fits its need. Each plan is scalable and if you wish, you can always choose to change your plan.

How can I upgrade my plan?

You can always contact SonicWall Support services to know more details on the upgrade plans and visit www.mysonicwall.com to renew the licenses.

Troubleshooting

Topics:

- IPSec Troubleshooting

IPSec Troubleshooting

The following guide presents a methodical way through which you'll be able to self diagnose and resolve some of the common errors encountered when setting up an IPSec site-to-site connection.

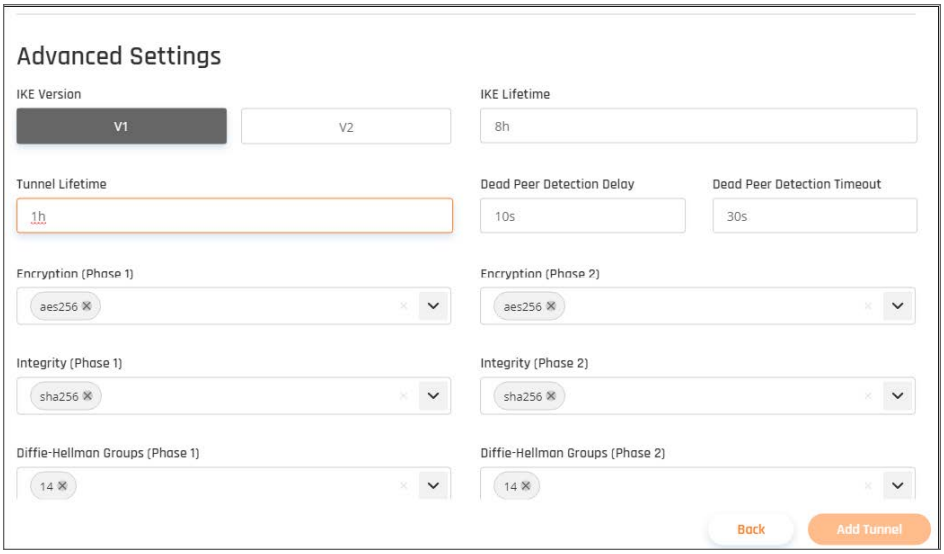
Examining the logs from your router/firewall

The most important tool that can assist you in analyzing networking issues is of course the logs derived from the edge device (your firewall or router).

We highly recommend exporting it and looking for errors and for details related to the topics mentioned below for an optimized workflow.

The console indicates the tunnel is down

Mismatched Parameters



Every site-to-site connection depends on filling in the fields with the exact same values in both the SonicWall Cloud Edge Management Platform **AND** your firewall or router Management Interface. A mismatch that occurs between any of these would prevent the tunnel from establishing, make sure that both the interfaces are absolutely identical in both platforms. When filling in **IKE Mode** choose **Main Mode** (aggressive mode is not supported).

It is important to verify that you have entered the same shared secret (sometimes referred to as PSK) on both platforms.

Network Addresses

Another common error may occur due to confusing terminology used to describe the different addresses involved in the process of a tunnel establishing.

When filling in the parameters in the SonicWall Cloud Edge platform:

- Public IP/Remote ID refers to the public IP address through which your on-premises network/VPC connects to the internet.

- SonicWall Cloud Edge Gateway Proposal Subnet refers to your SonicWall Cloud Edge subnet (in CIDR notation). This value must be identical to the value set as Remote Subnet in your router/FW/IaaS platform, therefore if you choose to set it to 0.0.0.0/0 on one platform you must set on the other.
- Remote Gateway Proposal Subnet refers to your on-premises/cloud network subnet (in CIDR notation). This value must be identical to the value set as Local Subnet in your router/FW/IaaS platform, therefore if you choose to set it to 0.0.0.0/0 on one platform you must set it to the same on the other.

  IMPORTANT: Unless specified differently in our designated guide, we recommend setting up the exact address range and not 0.0.0.0/0 (any).

The console indicates the tunnel is up, but I am still unable to access internal resources

Route Table

While some router or firewall interfaces automatically adjust the route table upon the creation of a tunnel, others do not. Make sure you have an inbound rule allowing traffic from your SonicWallCloud Edge subnet to your internal network, as well as an outbound rule allowing traffic from your internal network to the SonicWallCloud Edge subnet.

Firewall Rules/Security Group

- IPSec based connections utilize the following ports: UDP 4500; UDP 500.

  Make sure that these are open for both inbound and outbound traffic.
- Check your current firewall rules or the security group associated with the resource that you ae trying to reach, and verify that no rules prevent access to it. Rules hierarchy may also affect this.

Subnets

A subnet overlap would interfere with traffic flow.

Make sure that:

- Your SonicWallCloud Edge address range does not overlap with a subnet within your VPC/internal network.
- Each branch within the VPC/on-premises network has its own unique subnet.

2

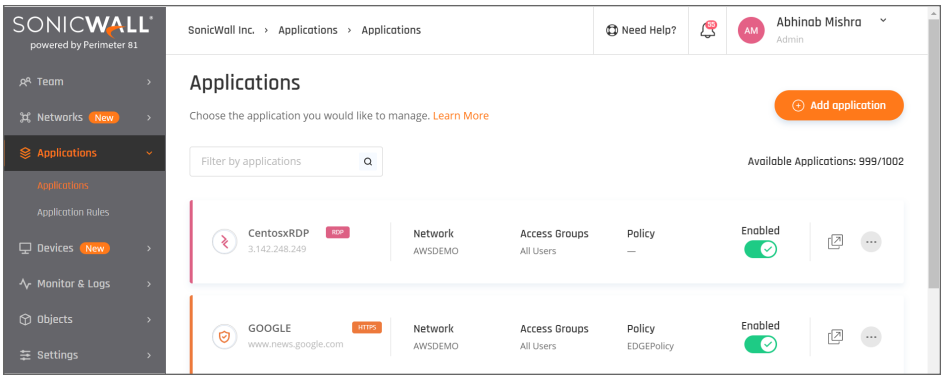
Zero-Trust Application

Topics:

End User Instructions

Zero Trust applications can be opened directly from any computer, without the network connection. All you need is internet access and browser.

1. In order to have access to your applications, you will need to log into your workspace: your_workspace.sonicwalledge.com.
   The list of your available application will be shown under the **Applications** tab:



2. Select the application which will open the application on your browser.

If your connection does not satisfy the policy for this application, an 'Authorisation Failed' screen will appear with the reason.

.HAR File

This article describes how to generate HAR files. When troubleshooting complex issues related to web applications (Zero Trust), it is sometimes necessary for our customer service team to obtain additional information about the network requests that are generated in your browser when an issue occurs. A customer service team member may request that you record a HAR file, or a log of network requests, while that issue is occurring and then provide that to them for further analysis.

- Generating the HAR file in Chrome
- Generating the HAR file in Safari

Keep in mind:

HAR files contain sensitive data, including the content of the pages you downloaded while recording and your cookies. This may allow others to impersonate your account or review information that you've submitted while recording the session (personal details, passwords, credit card numbers, etc.).

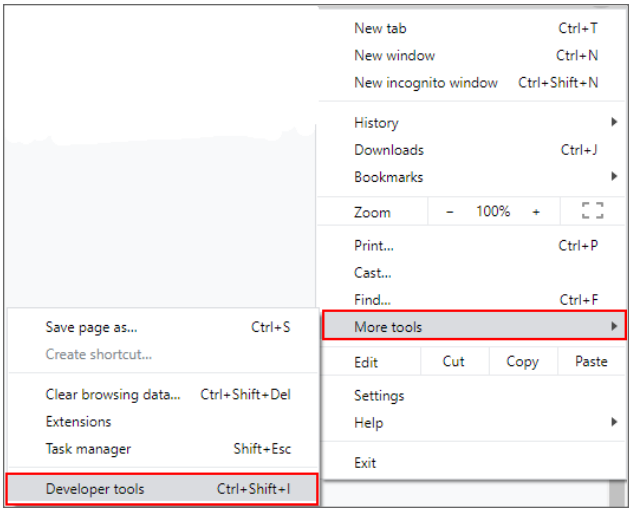
ⓘ | **NOTE:** We highly recommend encrypting the file before sending the HAR file

Below are some instructions about how you can easily generate a HAR file using different browsers.

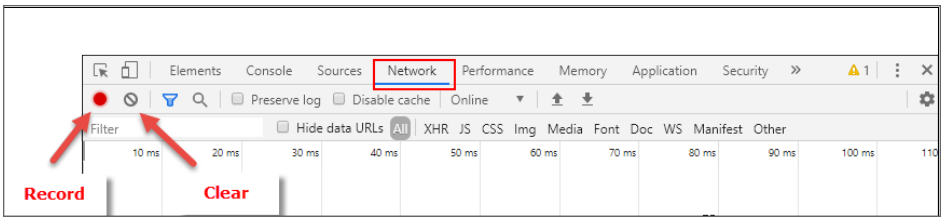
- Chrome
- Safari

Generating the HAR file in Chrome

1. Open Google Chrome and go to the page where the issue is occurring.
2. From the three-dotted menu (...) select **More Tools>Developer Tools**.



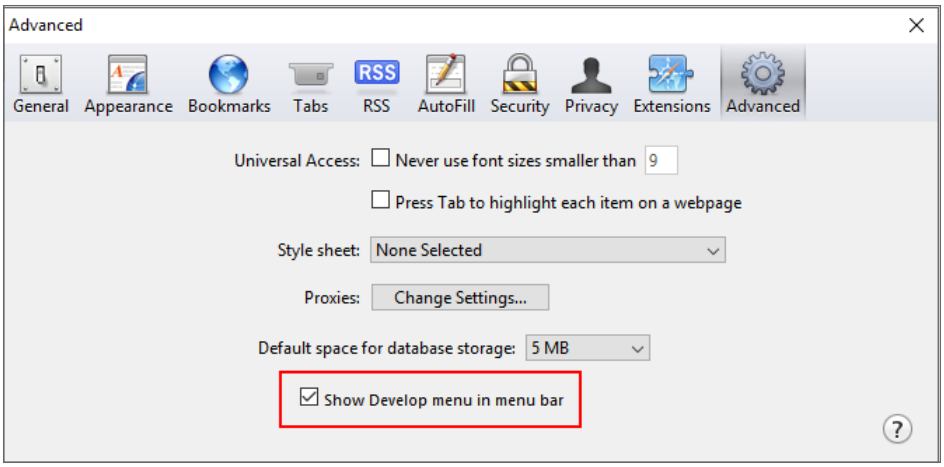
3. From the opened panel, select the **Network** tab.



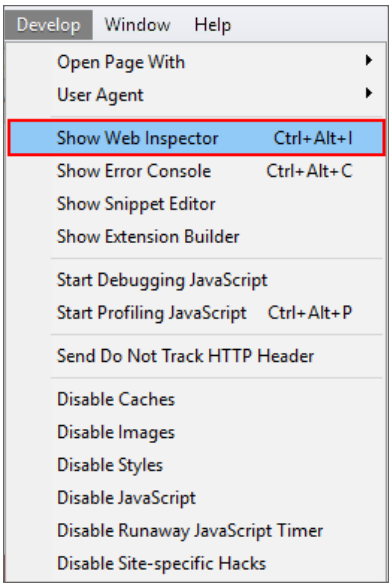
4. Verify that **Record** in the upper left corner of the tab is red. If it is grey, select it once to start recording.
5. Check the **Preserve log** box**.**
6. Select **Clear** (next to **Record**) to clear any existing logs from the **Network** tab.
7. Reproduce the issue that you were experiencing before, while the network requests are being recorded.
8. Once you have reproduced the issue, right-click anywhere on the grid of network requests, select **Save as HAR with Content**, and save the file to your computer.
9. Upload your HAR file to your ticket or attach it to your email so that the SonicWall Cloud Edge Support team can analyze it.

Generating the HAR file in Safari

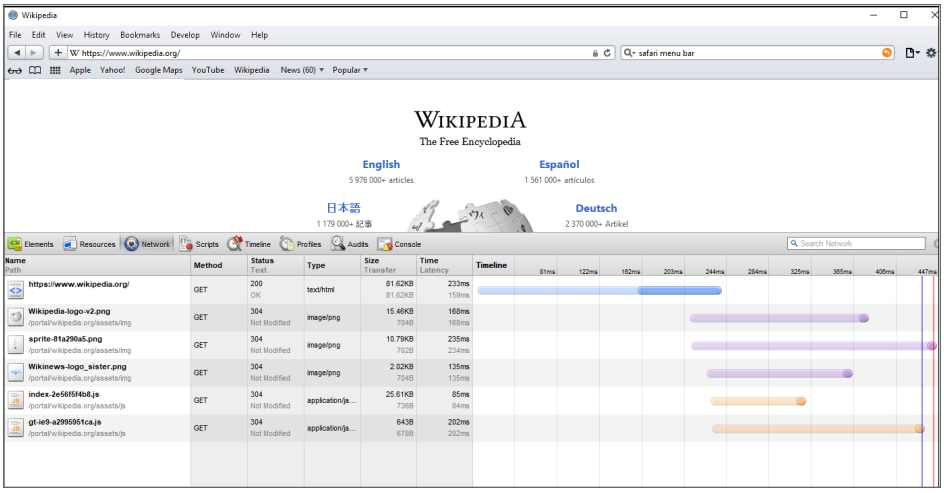
Before generating the HAR file, make sure you can see the **Develop** menu in Safari. If it is not there, follow the instructions under Use the developer tools in the Develop menu in Safari on Mac. In Windows, go to **Settings>Preferences.** Then select the **Advanced** tab. Select the checkbox to show the **Develop** tab on the menu.



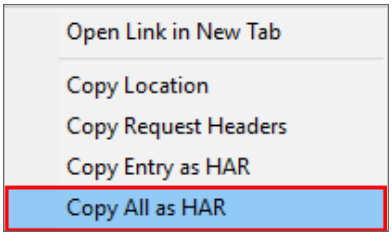
1. Open the **Develop** menu and select **Show Web Inspector**.



2. Select the **Network** tab and complete the activity that is causing issues.



3. Right-click in the Web Inspector and select **Copy All as HAR** and save the web archive file.



4. Send the file to the SonicWallCloud EdgeSupport team.

3

Using the Agents

Topics:

Settings

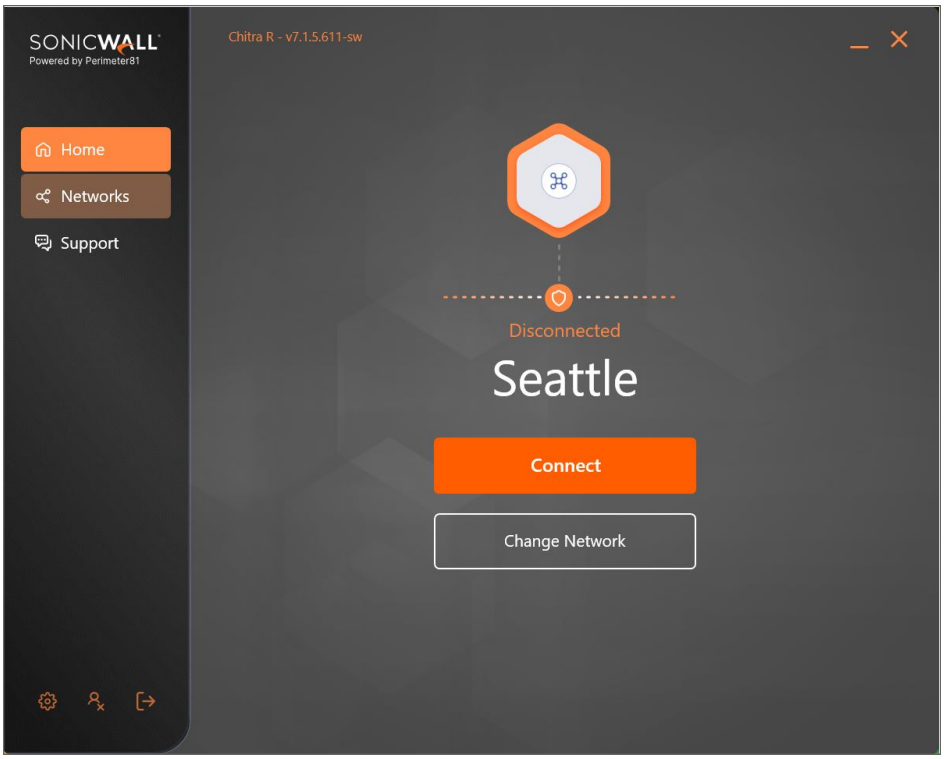
This procedure describes how you can manage the desktop or mobile clients settings.

ⓘ **NOTE:** Some of the configuration settings are pre-configured by the Workspace Manager and cannot be changed.

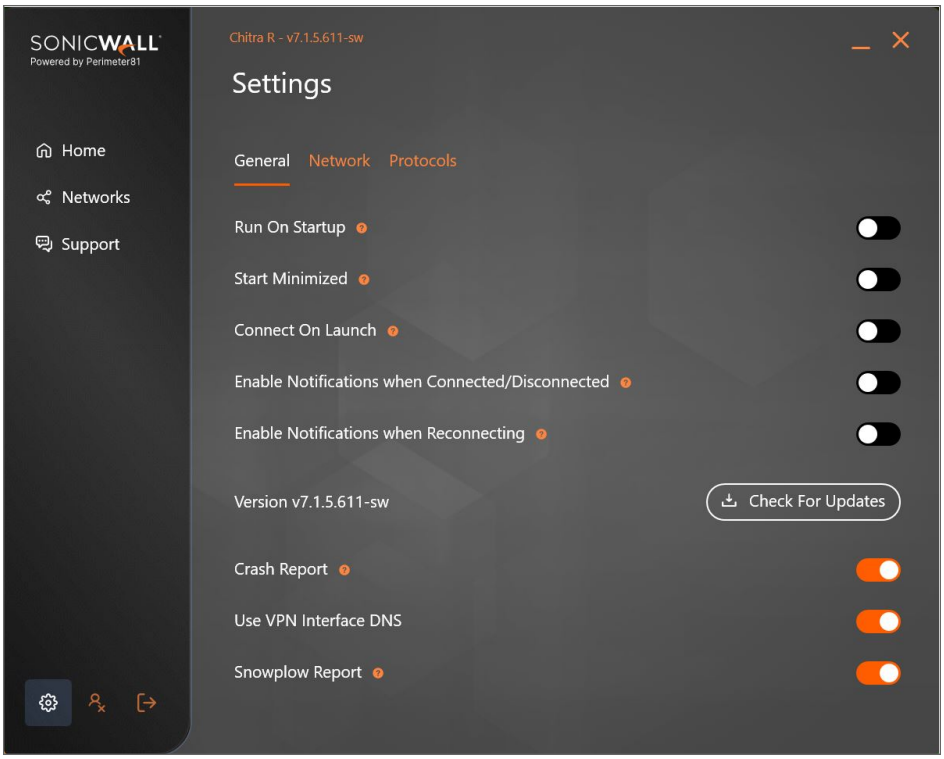
ⓘ **NOTE:** You can change the configuration settings, only if the administrator unlocks the respective settings in **User Configuration > Client Configurations**.

Opening the Settings area

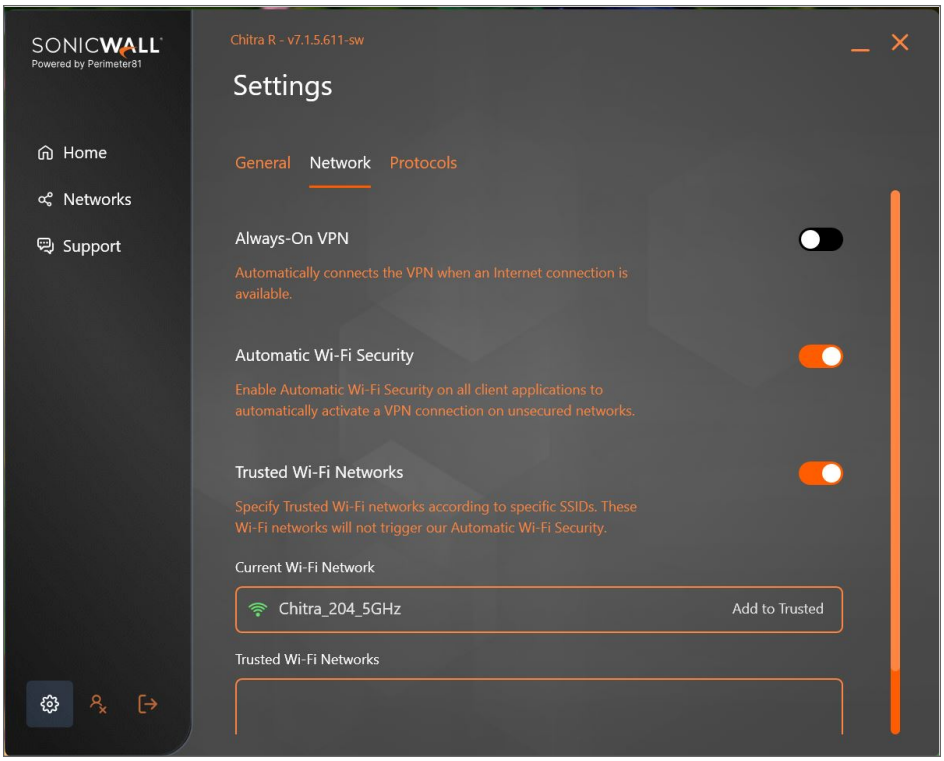
1. Double click the application icon. Select **Sign in to SonicWall Cloud Edge**.
   The **Sign in** web page appears.
2. Enter the workspace URL and select **Continue**.
   The application **Home** tab appears. The application prompts to connect.



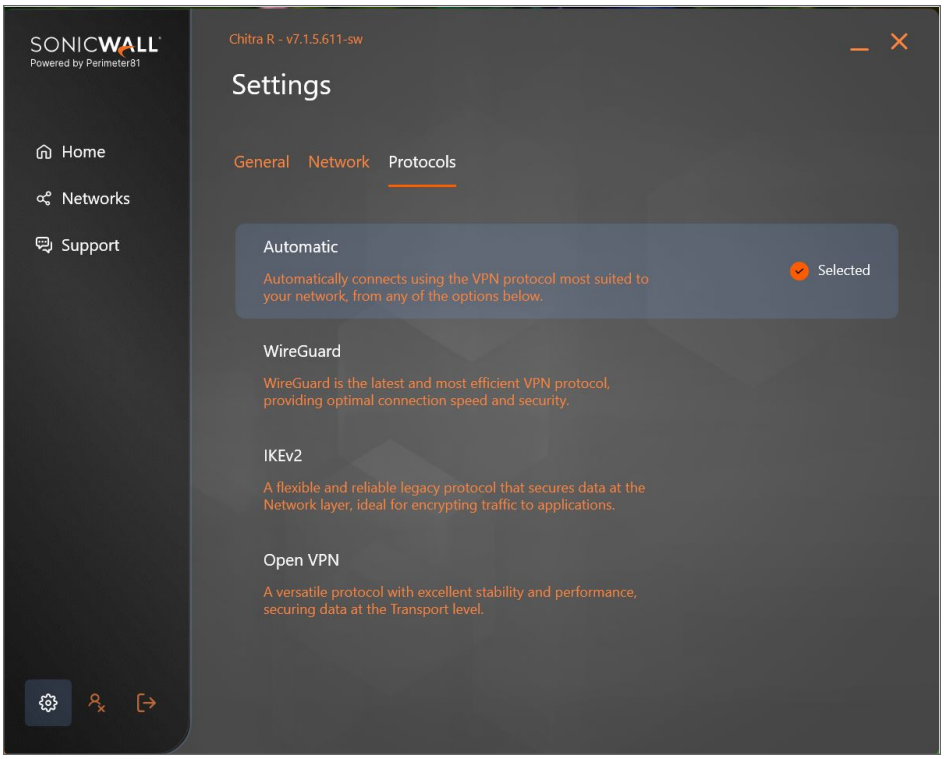
3. At the bottom left corner select the settings icon.
   The **Settings** tab appears.


SONICWALL
Powered by Perimeter81
Chitra R - v7.1.5.611-sw
Settings
Home
Networks
Support
General
Network
Protocols
Run On Startup
Start Minimized
Connect On Launch
Enable Notifications when Connected/Disconnected
Enable Notifications when Reconnecting
Version v7.1.5.611-sw
Check For Updates
Crash Report
Use VPN Interface DNS
Snowplow Report

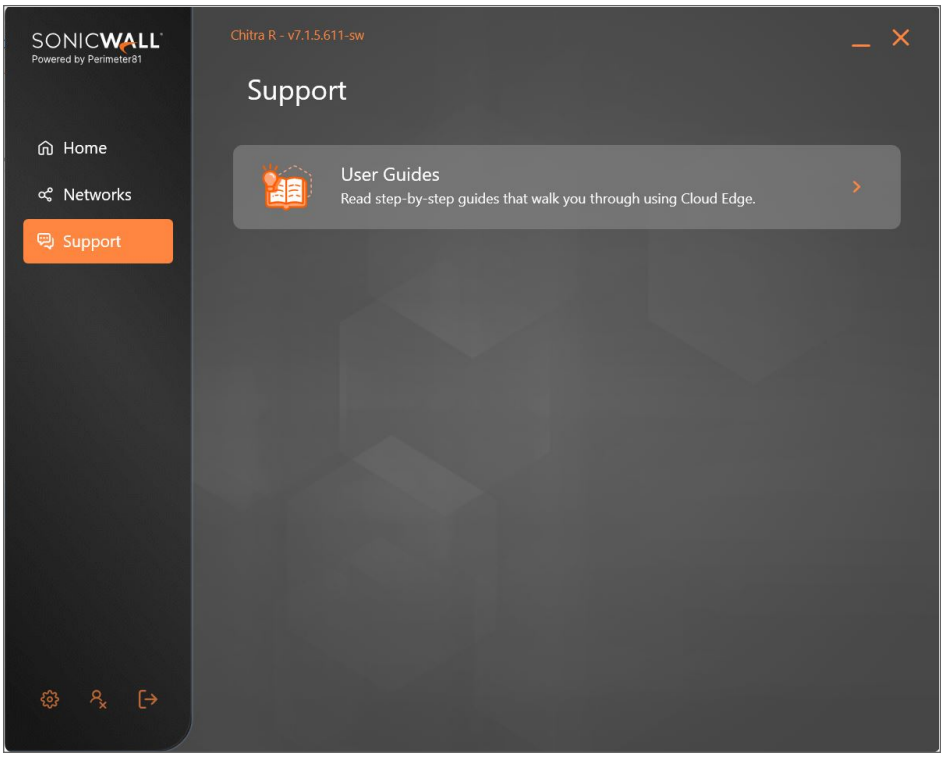
Tab name	Description	
General	The **General** tab allows you to manage startup, notifications, app updates, and advanced settings.	
	Run on Startup	The SonicWallCloud Edge application starts automatically when you boot your device.
	Start minimized	The SonicWallCloud Edge application window minimize to the taskbar.
	Connect on Launch	The SonicWallCloud Edge application connects to the network when launched.
	Enable Notifications when Connected/Disconnected	Notifications are shown whether the device is connected or disconnected.
	Enable Notifications when Reconnecting	Notifications are shown whenever the device is reconnected.
	Check for Updates	Select to check for updates to the application.
	Crash Report	Enabling sends crash reports.
	User VPN Interface DNS	Enabling VPN Interface DNS prevents DNS leaks, the application will only allow DNS requests via the DNS server specified on the VPN network interface.
	Snowplow Report	Enabling sends reports of user experience to Snowplow.



Tab name	Description	
Network	The **Network** tab allows to set the network connections.	
	Always-On VPN	Enabling this setting allows you to enable the VPN to connect automatically when an internet connection is available.
	Automatic Wi-Fi Security	Enabling this setting allows you to select automatic wi-fi security and manage trusted wi-fi networks.
	Trusted Wi-Fi Networks	Enabling this setting specifies the trusted Wi-Fi networks according to specific SSIDs. These Wi-Fi networks will not trigger **Automatic Wi-Fi Security** setting. This setting applies to Mac and Windows operating systems only.
	Current Wi-Fi Network	This displays all available SSIDs when**Automatic Wi-Fi Security**is enabled.



Tab name	Description
Protocols	The **Protocols** tab allows you to choose one of the following protocols. Read the description of each option to see which works best for your environment. • Automatic (set by you workspace admin) • WireGuard • IKEv2 • OpenVPN



Tab	Description	
Support	The Support tab allows you to use:	
	User Guides	Check out the knowledge base.

Tab	Description
Automatic Silent Updates	This options gives the administrator the ability to enable automated client version upgrades. When enabled, the VPN client is upgraded automatically and silently as new versions become available without the user's or administrator's involvement. This feature can be controlled by the administrators and the users: Administrators can enable and lock it down via the SonicWallCloud Edge application (*myworkspace.sonicwalledge.com*) where it can be enabled or disabled per operating system. Currently, we only support desktop operating system and hope to bring this functionality to the mobile platforms in the future. Users can also enable or disable the feature directly from the client (unless it's locked by the workspace administrator), using: **Settings -> General -> Automatic Updates**.

4. Select the required settings on each tab and click **Apply** to update the settings.

Connecting to a SASE Network

Topics:

Connecting to a Gateway

This article describes how to connect to a gateway.

- Logging in
- Changing the server
- Checking your IP
- Resolving a Max Session Limit error

Each team member must be invited to use the Management Platform. This can be done in two ways: team members can be invited by email, or if the organization is using an identity provider, team members may log in via the client after downloading the application.

Logging in

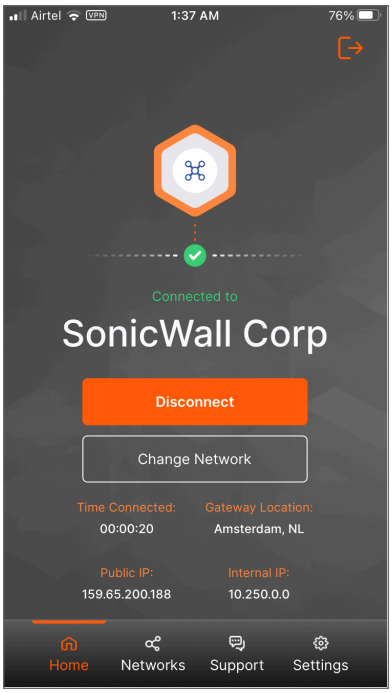
To log in, you will need to provide your organization's workspace, followed by your credentials or your organization's identity provider. If you're not sure what your workspace is, you can find the URL here. If your organization is using a two-factor-authenticator, you will be sent an SMS or a Google Authenticator code. After logging in you will see the main interface for the application.

Changing the server

Selecting **Change** will allow you to change the server you would like to connect to. By navigating between the tabs you will be able to choose if you would like to connect your private or public servers.

Checking your IP

While you are connected to the application, select the IP address button on the top right of the screen to display your IP address.

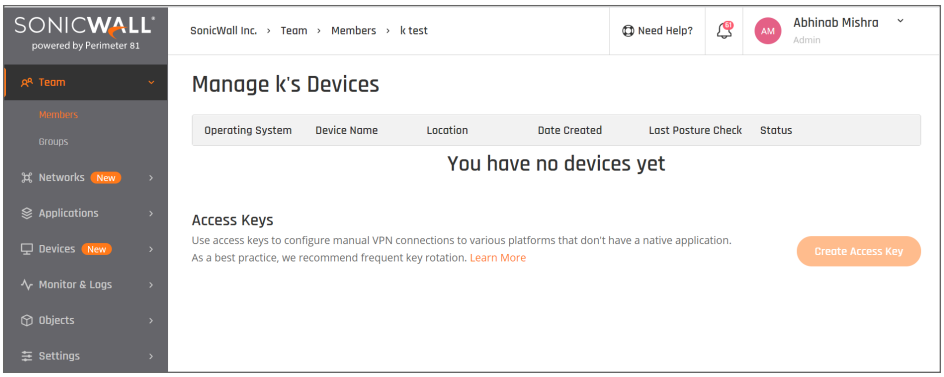


Resolving a Max Session Limit error

This error appears when a user has already connected five devices and is trying to log in with an additional device. Each user is allowed to connect with five different devices and two private keys at the same time. To

connect to a new device, you must sign out from one of the previous devices you've logged in or ask your administrator to force log out of one of the other devices.

1. Select **Members** from the **Team** tab.
2. Select **Manage Devices** from the three-dotted menu (...) beside the member's name.
3. The list of devices displays. Select **Log Out** for the selected device:



After this device has been logged out, you will now be able to log in to a new device.

Private and Public Servers

Public Server

By default, all accounts include access to our 36 global server locations. With our servers, the outgoing IP address is shared amongst several accounts simultaneously. These IP addresses rotate periodically. Public Servers are advisable if you need a VPN connection.

Private Server

You can purchase a private server for your team members who can share a single static outgoing IP address, which only is accessible by your organization. This creates the opportunity for many security capabilities which are only possible with a static IP address. For example, remote users can always connect to the gateway first, then have their IP address whitelisted to a security group in AWS.

Installation and Upgrade

Where can I download the connector applications?

You can find all the download links for our applications here:

- Mac: https://static.sonicwalledge.com/apps/osx/sdp/SonicWallCloudEdge.dmg
- Windows: https://static.sonicwalledge.com/apps/windows/sdp/SonicWallCloudEdge.exe
- Android: https://play.google.com/store/search?q=sonicwall
- iOS: https://www.apple.com/in/search/sonicwall?src=serp
- Linux x64: https://static.sonicwalledge.com/apps/linux/amd64/SonicWallCloudEdge.deb

Troubleshooting

Topics:

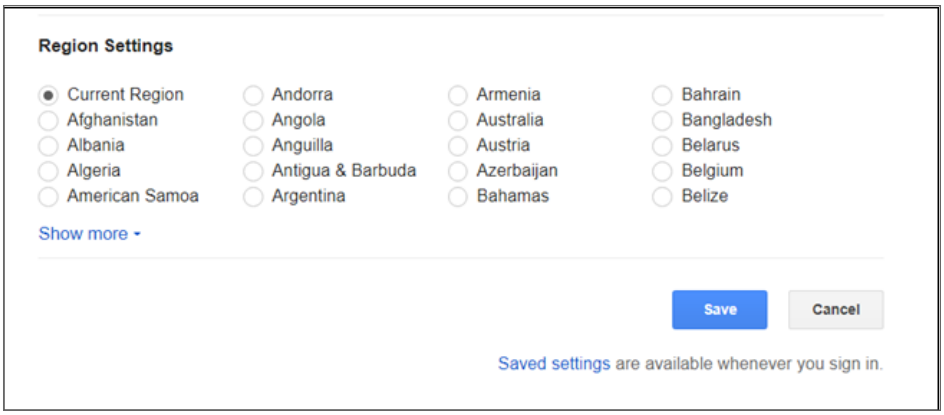
Check Location and Language for Accurate Google Search Results

While using SonicWall Cloud Edge, if you see Google displaying a location/language different than your IP Address' location, there is a simple solution.

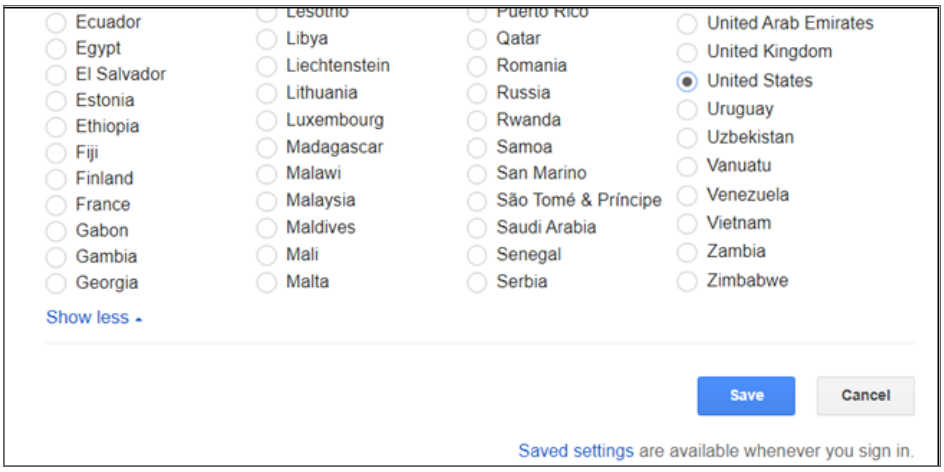
Lots of websites/services, including reputable ones don't update their Geolocation databases to the latest information. It is very common that Google identifies the wrong location with our product.

1. Make sure you are connected to the VPN.
2. Go to www.google.com.
3. Select **Settings > Search Settings**.

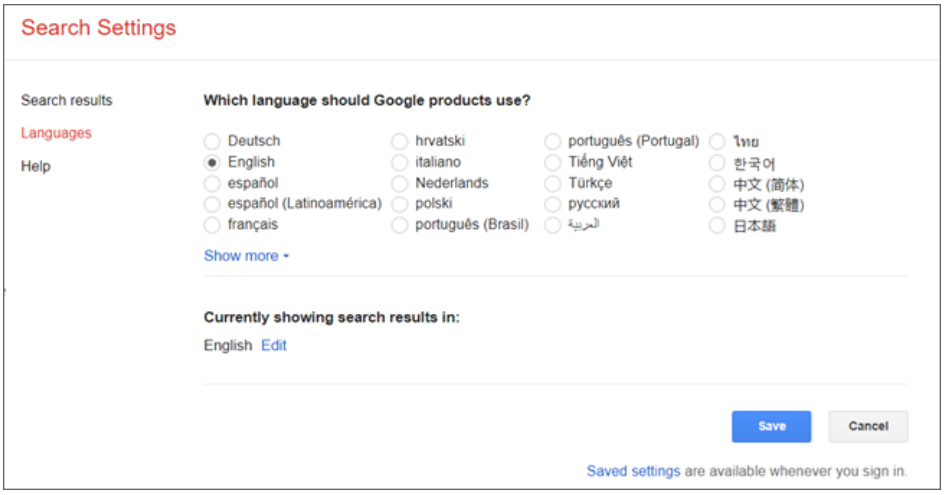
4. Scroll down to find **Region Settings**, select **Show More**.



5. Select the desired country, ideally the same as your IP's.



6. Now click **Languages**, select your desired language, and select **Save**.



Can't connect? SonicWall Cloud Edge's Internet Connection Troubleshooting Guide

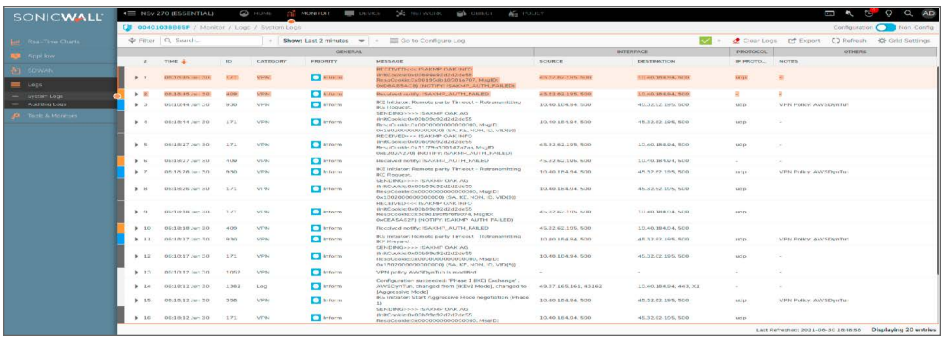
This article describes the basic troubleshooting steps in case of connection issues.

Step 1: Analyze Logs:

Every Cloud Edge agent generates logs on the client machine and store log events locally. For any issues like network connectivity issue, socket issue, driver issue, login issue etc., you can collect these logs and evaluate the failure. In case you need help from support, you can send these logs to support for further help.

Step 2: Troubleshoot IPSEC Error:

Usually, IPSEC tunnel slows down due to configuration issues like misconfiguration of subnet, network addresses, firewall rules/security groups, routing table etc. The most important tool that can assist you in analyzing networking issues is the logs derived from the edge device (your firewall or router).

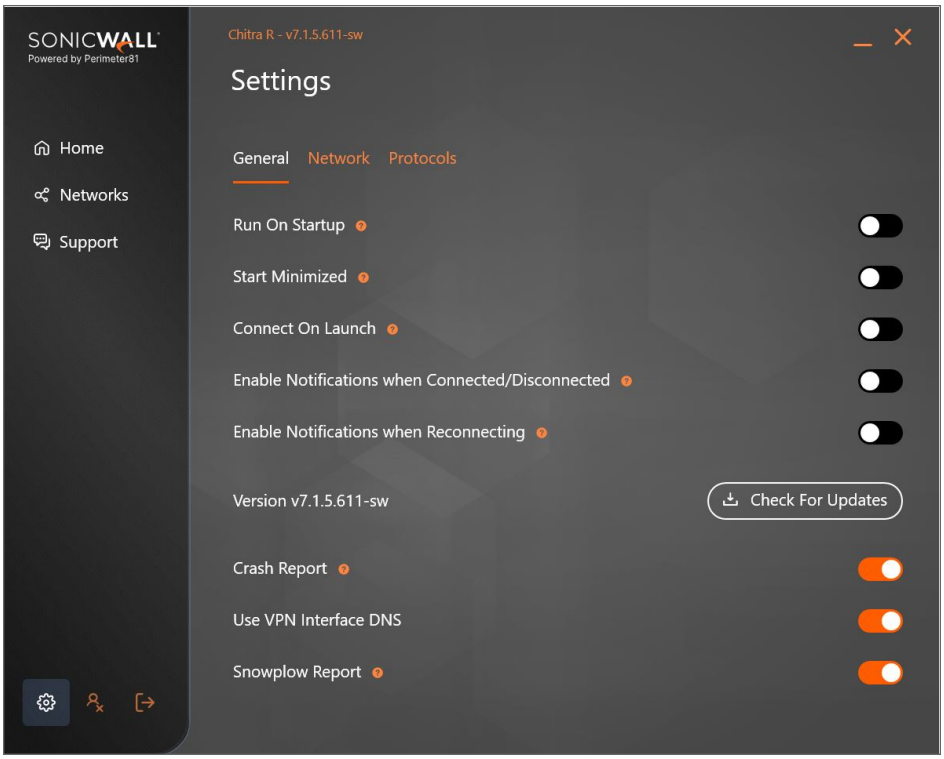


Step 3: Change the Connection Protocol

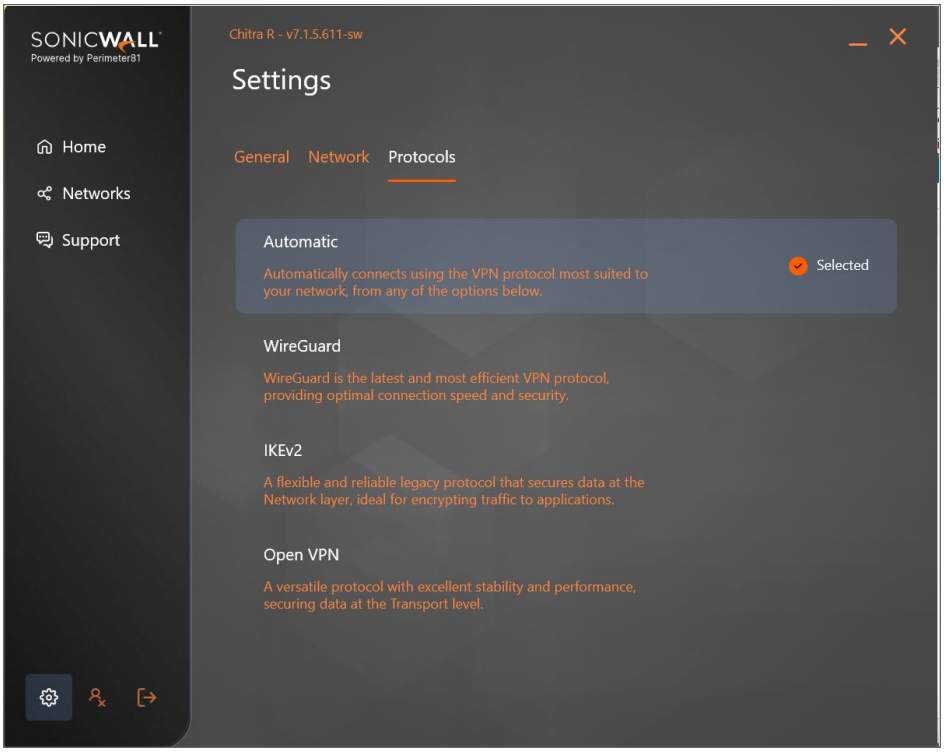
The SonicWall Cloud Edge application offers three major VPN protocols through which you can connect to your public and private gateways: **Wireguard**, **OpenVPN** and **IKEv2** .

While each displays excellent results in both speed and security, in some cases, depending on the internet connection itself, one outperforms the other. We strongly recommend testing both and see which one delivers better results.

1. Open your SonicWall Cloud Edge application. Open the drop-down menu at the top right corner and select **Settings**.



2. Go to the **Protocol** tab.



3. Select **IKEv2**, then **Apply** and connect again to your network. If the issue does not resolve, go through the same procedure, and this time select **OpenVPN** .

   If you still didn't receive a successful outcome, go to the next step.

Step 4: Make sure your firewall allows outgoing traffic from the used ports

	UDP	TCP
All Protocols		5050
WireGuard	8055	
IKEv2	4500, 500	
OpenVPN	1194, 636	1195, 8443
L2TP manual connections only)	1701	

Step 5: Help us diagnose the issue and open a support ticket

As part of the troubleshooting methodology, we would like to find out if the problem is unique to a particular network or website or occurs in every connection attempt a user makes.

- If you are using a public Wi-Fi please connect to the internet using a mobile hotspot and then try to connect to the app.
- A connectivity issue may also be related to a particular site orSonicWall Cloud Edge application. Try and access different sites and application and see if you receive different results.

Open a support ticket and attach your findings. Make sure to include the log files, a full description of the issue, a time-stamp of the first occurrence of the issue and the extent of it, your operating system, your physical location, and any other details you find relevant.

Log Files

If you're unsure where the logs files are located or how to securely send them to our team, see the Logs section to read more.

Logs

How do I query the logs?

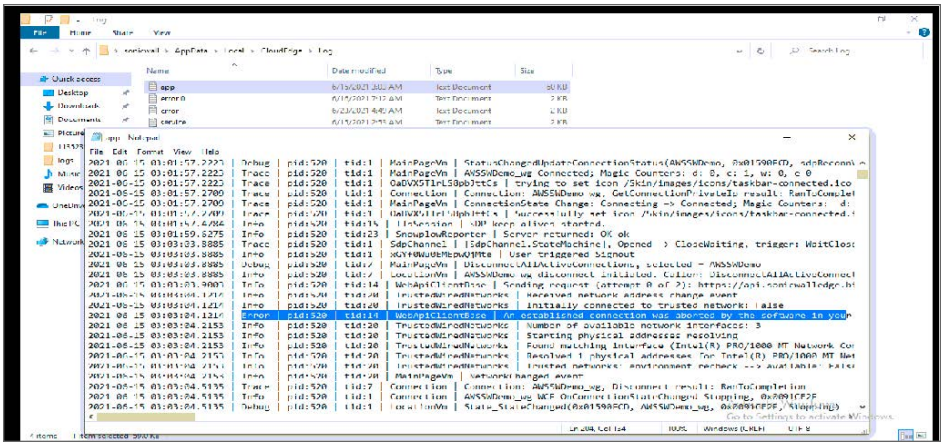
Logs analysis is a key tool in troubleshooting agent and network-related issues.

The following guide contains information on how to securely send the log files to our support team using a designated script created by our R&D team.

Windows Application

If you would like to examine the connection and application logs yourself you can find them at the following paths:

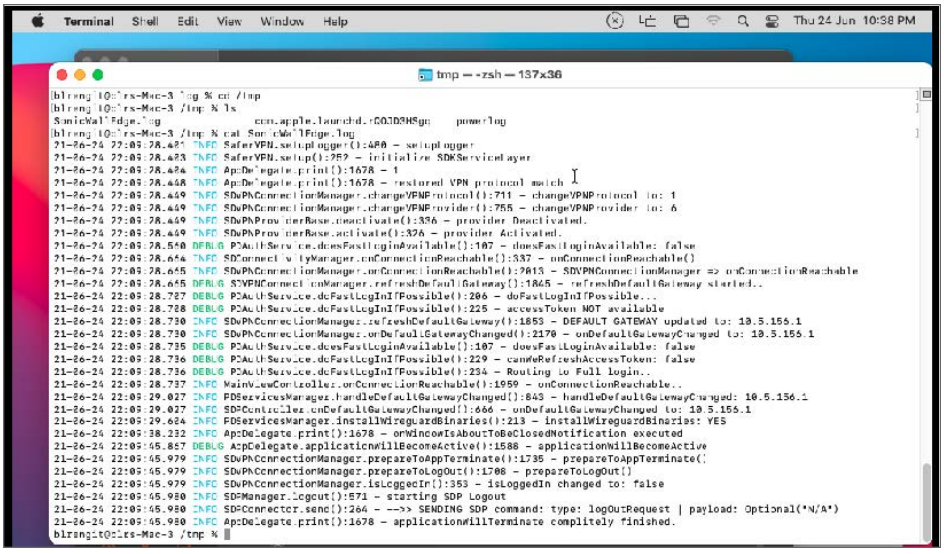
%LOCALAPPDATA%\CloudEdge\Log



MacOS Application

You can find mac agent logs at the following location:

/tmp/SonicWallEdge.log

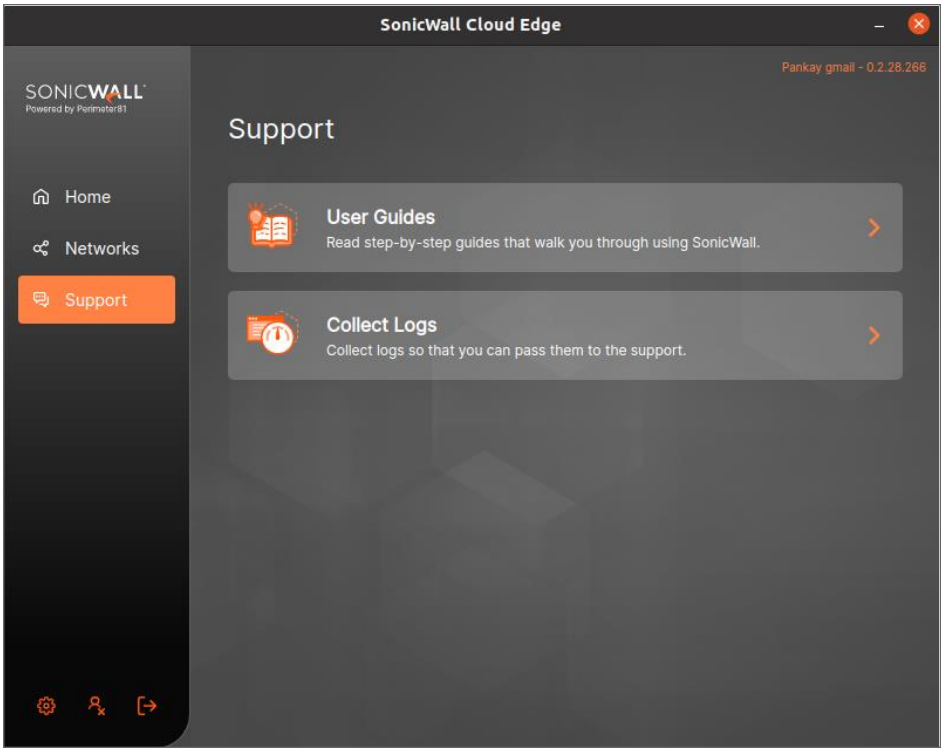


Linux Application

You can find linux agent logs at the following location:

/var/log "perimeter81helper-error.log perimeter81helper.log"

You can click **Collect Logs**, to generate all required logs for debugging.



iOS Application

Cloud Edge iOS agent does not store any logs on iOS device due to limited memory and other security constraints.

You can install tools like XCode or BugFender on your computer and connect the iOS device. While you connect to the Cloud Edge iOS agent , you can find all Cloud Edge activities on the xCode or BugFender console.

If you see any issues on the iOS Cloud Edge VPN application then take the screen shot of the error along with the iOS device information and send this to SonicWall Support for further assistance.

Android Application

Cloud Edge Android agent does not store any logs on android device due to limited memory and other security constraints.

You can install tools like ADB (Android Debug Bridge) on your PC and connect the Android device. While you connect to the CE agent on Android , you can see all Cloud Edge activities on the ADB console.

If you see any issues on the Android Cloud Edge VPN application then take the screen shot of the error along with the android device information and send this to SonicWall Support for further assistance.

4

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

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

Cloud Edge Secure Access User Guide
Updated - March 2022
232-00005536-00 Rev E

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