

Cloud Secure Edge

Getting Started Guide

Contents

About Cloud Secure Edge (CSE) **4**
Benefits of Cloud Secure Edge 4
Use Cases 5
- Remote Access via Service Tunnel 6
- Protecting SaaS Applications 6
- Using Zero Trust Network Access 6
- Blocking Malicious Content 6
- Monitoring Device Posture 7

Using this Document 7

CSE Licensing **8**
Choosing Your License 8
Procuring a License 9
Activating a License 9
- Registering CSE Activation Keys in MySonicWall 10
- Registering with a Free Trial 12
- Registering with Monthly Billing 12

Successful Activation 13

Prerequisites **14**
Supported SonicWall Product Versions 14
Secure Backups 14
Configuration Workflow 15

Firewall Connector Setup **16**
Connector Concepts 16
Configuring the CSE Connector on the Firewall 16

Setting Up Cloud Secure Edge **18**
Set Up the User Directory 18
Connect Your Network 19
Configuring Remote Access 19
Blocking Malicious Content 20
Protecting SaaS Applications 21
Configuring ZTNA 22
Checking the Device Posture 23

Monitoring Performance **24**

Best Practices **25**

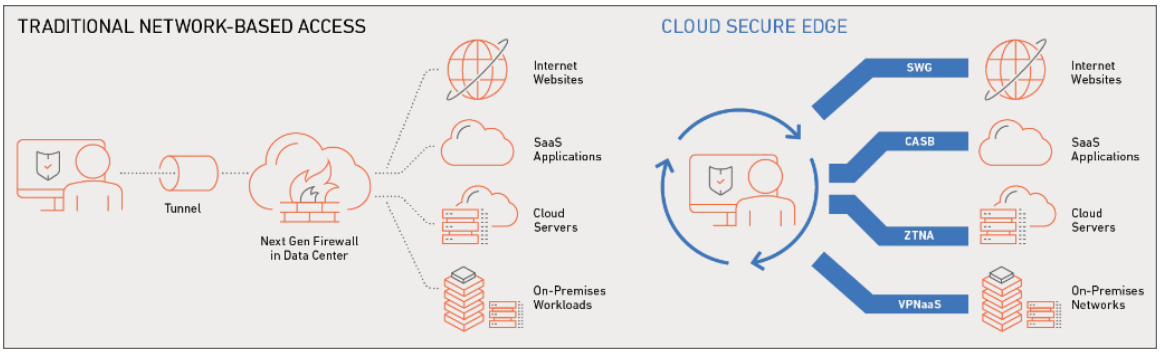
SonicWall Support **26**

About This Document 27

1

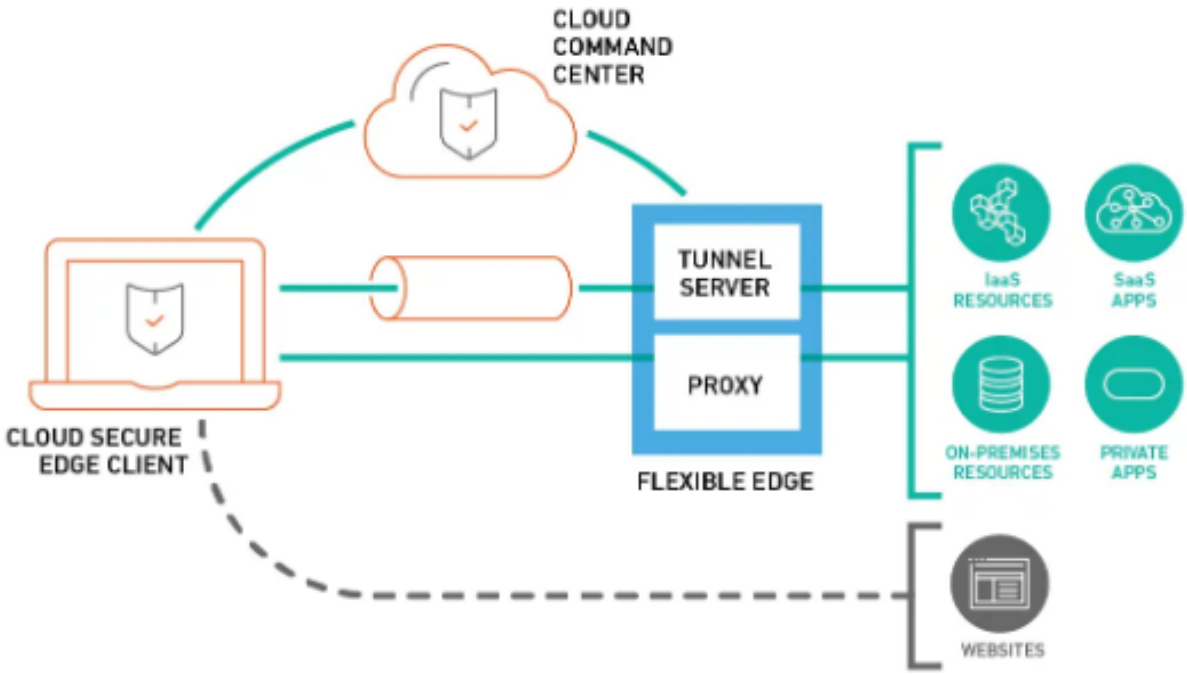
About Cloud Secure Edge (CSE)

SonicWall Cloud Edge Secure Access (CSE) is an easy-to-adopt Security Service Edge (SSE) solution, enabling secure access to any resource from any device. It delivers simple, secure, zero-trust access to private and internet resources for all your employees and third parties, regardless of their network location. To accomplish that, CSE combines the functionality of multiple traditional network appliances—remote access VPN, web proxy, firewall, etc.—into a unified cloud solution, improving the security posture and user experience for the entire workforce.



Benefits of Cloud Secure Edge

Traditional VPNs reveal significant performance, manageability, and security limitations when trying to provide simple, safe, secure access to the applications and resources users need across hybrid, multi-cloud, and SaaS environments. They also leave users accessing internet-based information and applications open to attack. To address these realities, a scalable and comprehensive approach is required.



A Security Service Edge (SSE) solution is a collection of integrated, cloud-centric security capabilities that facilitates safe access to websites, software-as-a-service (SaaS) applications and private applications. SSE offers a simple, scalable and secure way to provide users one-click access to the applications and resources needed to do their jobs while protecting them from advanced internet threats.

The biggest benefits for using Cloud Secure Edge include:

Security posture verification	Ensures that devices meet the minimum security requirements before being allowed to access corporate resources. This includes ensuring that devices have the latest security updates and patches, have anti-virus software installed, and are not jail-broken or rooted.
Intelligent routing	Ensures traffic is directed through the most secure and efficient route to the resource. This includes routing traffic through secure gateways and ensuring that sensitive data is encrypted.
User verification	Ensures that only authorized users can access corporate resources. This includes implementing multi-factor authentication and restricting resource access based on user roles and privileges.

Use Cases

Cloud Secure Edge can be used as a stand-alone product, or it can be added to a SonicWall firewall. It offers many features, but five of the most popular are reviewed here. You may opt to configure only one use case, all use cases, or some combination of them. Whatever combination of options you choose, they can be configured with or without the firewall. The key use cases include:

- Remote Access via Service Tunnel
- Protecting SaaS Applications
- Using Zero Trust Network Access
- Blocking Malicious Content
- Monitoring Device Posture

Remote Access via Service Tunnel

One of the core capabilities of Cloud Secure Edge is that it acts as a virtual private network as a service (VPNaaS). It provides modern high-performance, tunnel-based access to networks, incorporating zero trust enhancements like continuous authorization and device trust. Remote access via Service Tunnels also provides third-parties easy, secure access only to the specific resources they need without over-provisioning. It ensures access based not only on the security posture of the user and device, but also on their roles and what they are authorized to view. Management is simple with groups and roles that can be pre-identified and applied as necessary from one central console. No need to patch or configure hardware—ever.

Protecting SaaS Applications

Protecting SaaS applications is just one step in internet threat protection. Cloud Access Security Broker provides SaaS application access security. Layered security provides easily managed controls for managing who can access your SaaS application and which devices they can use to connect. You can route public traffic destined for the internet. Internet traffic routed through your Service Tunnels uses the source IP of a CSE Access Tier. Administrators can then whitelist the IP to restrict user access on log in and throughout a user's session on a SaaS platform.

Using Zero Trust Network Access

Using Zero Trust Network Access (ZTNA) provides simple, least-privilege access to applications and services across hybrid- and multi-cloud infrastructures. It leverages your existing enterprise identity and security tools investments.

Rather than rely on coarse tools like firewalls and legacy VPNs to protect company resources, Cloud Secure Edge enables access to specific applications and servers based on the combined real-time, contextual factors of user and device trust, and resource sensitivity. It is cloud-based and can be applied independently or with pre-existing security infrastructures.

Blocking Malicious Content

SonicWall has deployed high-performance global edge PoP (Point of Presence) networks to ensure the most efficient and direct routing while applying consistent enforcement controls to protect against every type of attack or risky exposure. This provides simple and effective protection against phishing attacks and malicious websites

while also applying content filtering as desired. Device security is verified upfront before access is granted—the way it should be.

You can also set up a Secure Web Gateway (SWG) in Cloud Secure Edge to help malicious content by routing traffic to your private networks. The SWG protects users from being phished, straying onto malicious websites, or being exposed to ransomware. Optional controls enable organizations to block specific website categories, such as gambling and pornography.

Monitoring Device Posture

Cloud Secure Edge takes a layered approach to security that easily manages controls for who can access your SaaS applications, and which devices they can use Trust Profiles are built using a predefined set of Trust Factores and Trust Effects and are applied to resources within your network.

Using this Document

This document provides an overview and acts as a checklist for configuring Cloud Secure Edge. It guides you to the different pieces of documentation needed to define and configure the different features. This document includes the following content:

- CSE Licensing
- Prerequisites
- Firewall Connector Setup
- Setting Up Cloud Secure Edge
- Monitoring Performance
- Best Practices

An overview of the Configuration Workflow shows the high-level actions to take when configuring Cloud Secure Edge.

2

CSE Licensing

Cloud Secure Edge (CSE) is available for purchase with two license options: Secure Private Access and Secure Internet Access. Your license decision will be driven by what you want to accomplish. The two options are both available in two tiers: Basic and Advanced. Licenses are sold on a per-user basis. Refer to the Data Sheet to see what features are associated with each license.

Topics

- Choosing Your License
- Procuring a License
- Activating a License
    - Registering CSE Activation Keys in MySonicWall
    - Registering with a Free Trial
    - Registering with Monthly Billing
- Successful Activation

Choosing Your License

The Secure Private Access license provides safe access to resources on the internal networks. It provides two core capabilities:

- **Tunnel-based ZTNA** (Cloud VPN or VPNaaS): Secure network access to specific network segments.
- **Proxy-based ZTNA**: Secure access to private resources such as internal HTTP applications and TCP services.

Secure Internet Access license provides three core capabilities:

- **DNS-Layer Security** (DNS): Domain-level threat protection blocking malicious domains and enforcing acceptable use policies.
- **Cloud Access Security Broker** (CASB): Enforcement device trust policies to access SaaS applications.
- **Secure Web Gateway** (SWG): Web content filtering to block malware and other threats hidden in encrypted web traffic.

The following licensing is recommended based on what you are trying to accomplish with Cloud Secure Edge:

Function	License Requirement
To set up remote access:	Secure Private Access
To block malicious content:	Secure Internet Access
To protect SaaS applications:	Secure Internet Access Advanced
To set up ZTNA:	Secure Private Access Advanced
To check device security posture:	Secure Private Access

For a deeper understanding of licensing, you can refer to Cloud Edge Licenses.

Procuring a License

SonicWall offers several options to acquire a CSE license.

Licensing Method	Information
License purchase	A customer can buy a CSE license from their distributor or vendor (SonicWall partner) in the same way they would any other SonicWall product. Once the purchase is made, the customer receives an email that includes the activation key for the license.
MySonicWall's Monthly Billing program	Qualified SonicWall partners (MSSPs) can purchase specific products using a monthly usage model. As part of this model, partners can provision and be billed for eligible products by themselves without requiring activation keys or pre-purchasing credits. This is done using the MSSP Monthly feature in MySonicWall. At the end of every month, the MSSPs are billed for usage of these products via their distributors.
New trial in MySonicWall	Customers can try a free 30-day trial of a new product by activating the product in MySonicWall. After logging in, they can go to **Product Management > Free Trials** and click on the icon for the Cloud Secure Edge application.

NOTE: CSE licenses may also be offered as a part of a SonicWall promotion. Reach out to your partner or sales representative to see what opportunities you can take advantage of.

Activating a License

You can activate a CSE license two different ways:

- Registering CSE Activation Keys in MySonicWall
- Registering with a Free Trial
- Registering with Monthly Billing

IMPORTANT: If you don't already have a MySonicWall account, sign up for one. You can follow the KB article, How do I create a MySonicWall.com account?

IMPORTANT: After activating your license, you need to wait about 5 minutes before starting to configure the Cloud Secure Edge settings. The system needs some time to synchronize and recognize your license.

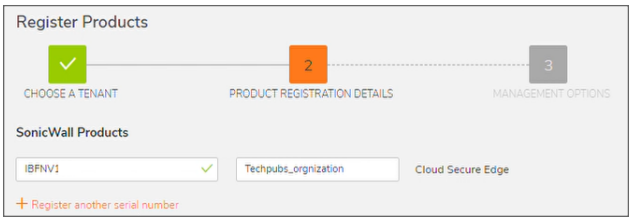
Registering CSE Activation Keys in MySonicWall

To register a CSE license, sign into your MySonicWall account. If you have not signed up for a MySonicWall account, refer to the KB article, How do I create a MySonicWall.com account?

VIDEO: You can also refer to the video at SonicWall University to see how use activation keys to register a Cloud Secure Edge license.

To register a Cloud Secure Edge in MySonicWall:

1. Login to MySonicWall.
2. Navigate to **My Workspace > Register Products**.
3. Select a **Tenant** under which you want to register a Cloud Secure Edge.
4. Enter your Cloud Secure Edge Activation key in the box with **Serial Number/Activation Key/Assign Token**. If you have both a SIA and SPA key, you can shoose either one for this step.
5. Enter a friendly name for the Cloud Secure Edge to identify in the **Products** list.



6. Enter a unique **Cloud Secure Edge Name** to identify on the CSE portal.

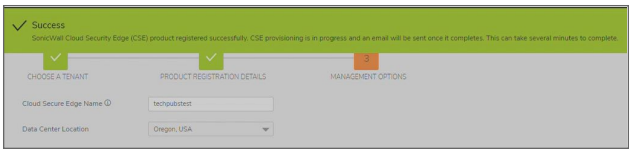
   NOTE: Follow the below criteria to define the name:
   - Name should start with a letter.
   - Only lowercase letters a-z, numbers 0-9, and hyphen (-) are allowed.
   - The length of the name should be between 4 and 30 characters.

7. Update the **Data Center Location** if required.

   By the default, the Data Center Location is selected.

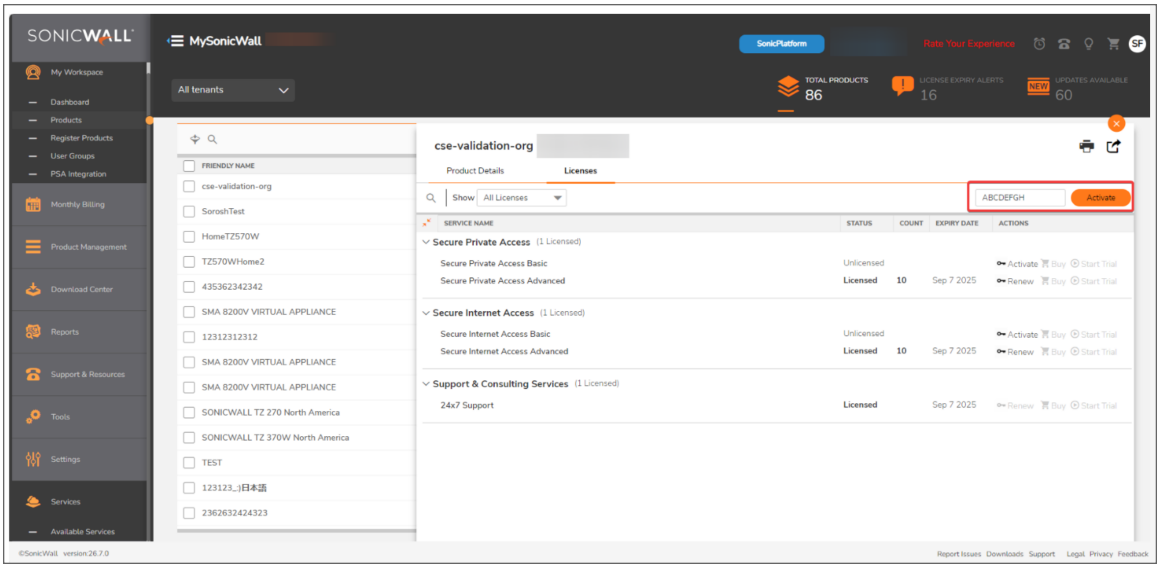
8. Click **Done**.

   NOTE:
   - On successful registration, you get a **Success** message on the page. However, the CSE provisioning takes several minutes to complete.
   - You get an email notification on successful provisioning, and service is available on Capture Security Center.
   - You can view the registered license under **MyWorkspace > Products**.

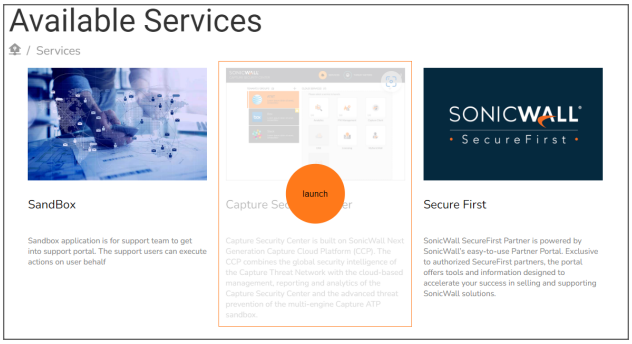


IMPORTANT: To use Connector on the SonicWall firewall, make sure that the firewall is registered under the same MSW tenant as the CSE license. The firewall does not need a license to use the Connector. A licensed CSE product under the same MSW tenant is sufficient.

9. If you have a second activation key to apply, navigate to **MyWorkSpace > Products**, find and click on your **CSE Serial Number > License Details**. You can input your second key here to activate both SPA and SIA on the same serial number.



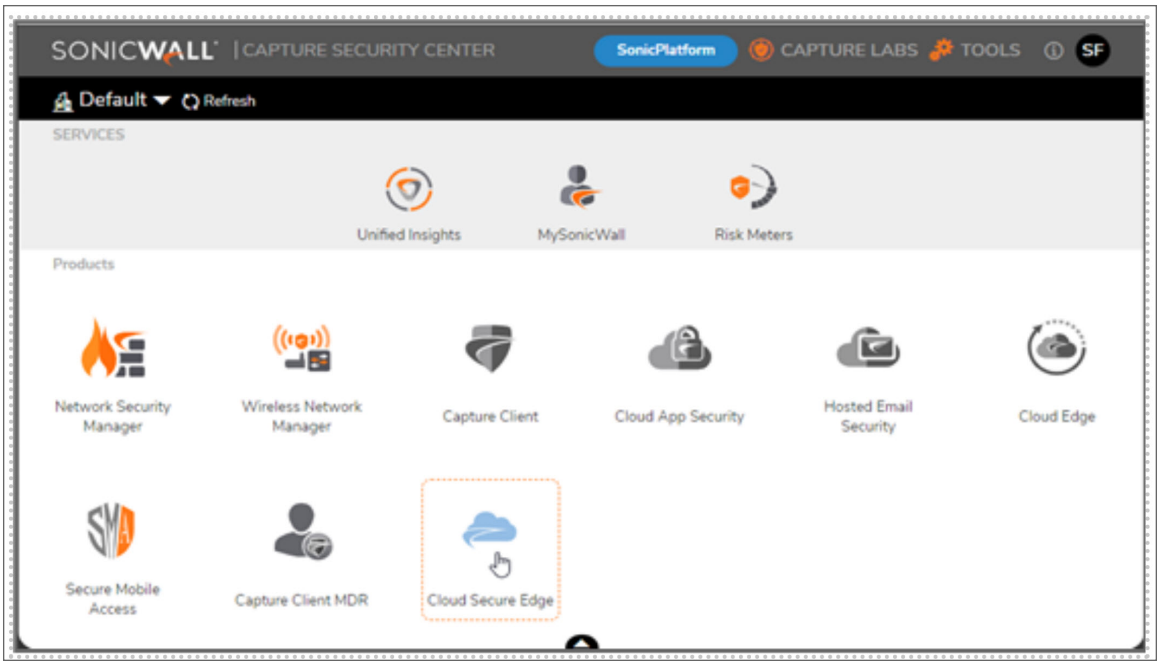
10. After you receive the confirmation email, launch CSE from the Capture Security Center.
    a. Navigate to Capture Security Center and log in.
    b. In MySonicWall, navigate to **Services > Available Services**.
    c. Hover over the **Capture Security Center** and click **Launch**.



11. Select your tenant in the **Capture Security Center** portal.

If your tenant or product is unavailable, click the **Refresh** icon and check the dashboard.

12. Click the **Cloud Secure Edge** icon to use your single sign-on (SSO) credentials to log into the product console, also known as the CSE Command Center.



For more information, refer to SonicOS Cloud Secure Edge Feature Guide.

Registering with a Free Trial

The CSE free trial can be enabled in MySonicWall. It is a free 30-day license for 25 users, and you can choose between the Advanced Secure Private Access (SPA) or the Advanced Secure Internet Access (SIA).

1. Log into MySonicWall.
2. Go to **Product Management > Free Trials.**
3. Click on the icon for the Cloud Secure Edge application.
4. Provide a **Friendly Name**.
5. Select a tenant from the drop-down box and click **Try Now**.

A short video is available to show you how to convert a Cloud Edge Secure Access trial license into a production license.

Registering with Monthly Billing

Partners who are part of the Service Provider Program can deploy CSE and get billed in arrears baseed on consumption with no commitments. Speak to your sales representive about joining the program.

Once enabled, you can follow the steps outlined Provisioning Cloud Secure Edge to deploy Cloud Secure Edge.

Successful Activation

Once your license has been successfully activated, you receive an email from MySonicWall stating that the CSE instance is ready.

Once you receive confirmation, you can begin configuration. If your configuration includes a SonicWall firewall, you should configure the firewall first. If you don't have a firewall in your configuration, you can skip to Setting Up Cloud Secure Edge to install the connector on the CSE infrastructure.

3

Prerequisites

Prerequisites are those things you need to plan and consider prior to configuring Cloud Secure Edge or the firewall connector.

Topics:

- Supported SonicWall Product Versions
- Secure Backups
- Configuration Workflow

Supported SonicWall Product Versions

The following are the SonicWall products and versions that support Cloud Secure Edge:

SonicWall Products	Versions
SonicOS	7.1.2 or higher
NSM (Network Security Manager) SaaS	2.5.0 or higher

Secure Backups

If you are working with a firewall already existing in your configuration, you should make a system backup prior to configuring the firewall to work with Cloud Secure Edge. The backup is a snapshot of your current system state, SonicOS image, and configuration preferences. The snapshot becomes the new system backup image.

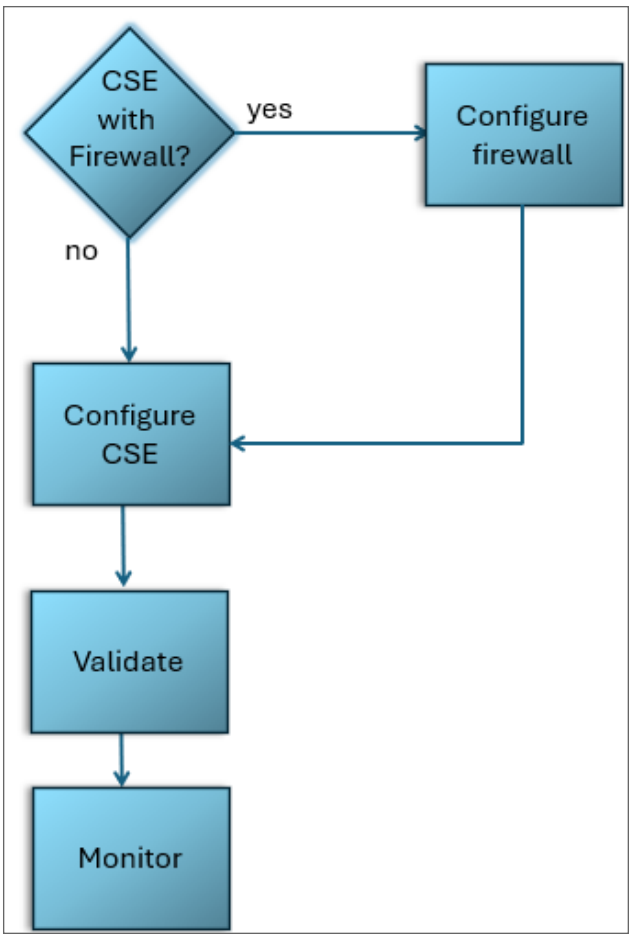
To make a firewall backup:

1. On your SonicWall firewall, navigate to **Device | Settings > Firmware and Settings**.
2. Click **Create Backup**.
3. If you want to **Retain Local Backup**, enable the switch and add a description to the **Comments** field.
4. Click **OK**.

For more information about backups on the firewall, refer to SonicOS 7.1 Device Settings Administration Guide or the SonicOS 8 Device Settings Administration Guide, as needed.

Configuration Workflow

When configuring Cloud Secure Edge, follow the general workflow illustrated below. If you integrate a firewall, configure the firewall first and then set up the Cloud Secure Edge.



For a solution with SonicWall firewall, go to Firewall Connector Setup for information about setting it up. If not, skip to Setting Up Cloud Secure Edge to begin setting up the Cloud Secure Edge.

4

Firewall Connector Setup

If your configuration includes a SonicWall firewall, you should configure it prior to configuring CSE. If you don't have a firewall, you can skip to Setting Up Cloud Secure Edge to install the connector on the CSE infrastructure.

SonicOS 7.1.2 and later supports the Global Edge Network deployment type. With this capability, any organization can deploy SonicOS as a Cloud Secure Edge Connector. The Connector is a dial-out connector that establishes a secure tunnel with CSE's Global Edge Network. It can be deployed in any location with connectivity to your internal services. There is no change to the control plane. The Cloud Command Center is always delivered as a cloud Software-As-A-Service (SaaS) offering. For more information on Cloud Secure Edge, refer to the CSE documentation.

Connector Concepts

The Connector is a dial-out connector that establishes a secure tunnel with the Global Edge Network. It deploys in any location that has connectivity to your internal services. Each Connector only connects outbound and does not need any inbound open ports to operate correctly.

The CSE Connector for SonicWall firewall allows secure remote access to private resources behind the firewall. CSE infrastructure enforces access control, not by the SonicWall firewall. Traffic ingresses SonicOS via WireGuard tunnels from CSE PoPs (Point of Presence networks). Only inbound access (WAN to protected zones from a firewall perspective) is allowed. SonicOS Group Address Object is created automatically (per Connector). The firewall administrator configures the allowed private IPv4 addresses (Group address object) and private domains, if any, that SonicWall firewall needs to resolve for the CSE clients. The Connector establishes a WireGuard tunnel to CSE PoPs.

Configuring the CSE Connector on the Firewall

You can use the following checklist to help you set up and configure the CSE on your firewall. The full procedure is documented in the SonicOS Cloud Secure Edge Feature Guide.

1. If not already done, activate Cloud Secure Edge in MySonicWall (Registering CSE Activation Keys in MySonicWall).
2. Enable Cloud Secure Edge on the firewall (SonicOS Cloud Secure Edge Feature Guide).

ⓘ | **VIDEO:** You can also view the video that shows your how to enable Cloud Secure Edge.

3. Configure the Connector on the firewall (SonicOS Cloud Secure Edge Feature Guide).
4. On the firewall, navigate to **Device | Log > Settings** to confirm Connector status. Find the log category **Cloud Secure Edge** in the table.

Once you configure this connector on the firewall, be sure to record and remember the name of the connector. You need this name later so you can tell which connector the CSE needs to access.

5

Setting Up Cloud Secure Edge

The following provides information on how to set up Cloud Secure Edge (CSE). Before configuring your use cases, you need to Set Up the User Directory and Connect Your Network. After that you set up your use cases. The most common use cases are listed below. You can set up just one in your environment, or you may take advantage and configure multiple use case.

ⓘ **NOTE:** If you are connecting a firewall in this deployment, the firewall must be set up for Cloud Secure Edge before configuring the settings in the following sections. For the firewall configuration, refer to Firewall Connector Setup.

Common Use Cases:

- Configuring Remote Access
- Blocking Malicious Content
- Protecting SaaS Applications
- Configuring ZTNA
- Checking the Device Posture

Set Up the User Directory

Setting up a way to validate your end users is a key component of the Cloud Secure Edge. If you already have a system set up, you can configure the identity provider. The following links provide the details for specific offerings:

- Okta
- Microsoft Entra ID (formerly Azure AD)
- G Suite
- Other IDPs

If you don't have an existing identity provider, you can use Cloud Secure Edge's Local User Management to get started.

Connect Your Network

SonicWall Cloud Secure Edge offers two deployment models for access to your organization's private resources:

- Self-hosted Private Edge
- Global Edge (used for Firewall and stand-alone Connectors)

In most cases, your organization would be provisioned, so you can use one or both deployment models. Most of our customers opt to use the Global Edge deployment model and, therefore, deploy a Connector to connect their network. Refer to Deployment Models for more information on each option. If you have already enabled your firewall Connector, skip to the next step.

Configuring Remote Access

With today's distributed data centers and data in the cloud, anyone can access log-in portals that stand in front of protected resources. Anyone, then, can attempt to gain access to these protected resources; so long as the user is authenticated, they are granted access. But there's no way to verify that users who have gained access to a VPN are authorized to access all, or a subset of, the private resources within the network.

Service Tunnel accounts for this lost authorization aspect: it offers a built-in continuous authorization functionality. Users who may be attempting to access protected resources from one IP, and then from another IP, are authorized on each access attempt. In these authorization events, Service Tunnel evaluates whether the user role and device Trust Level align with the Service Tunnel's pre-defined access policy.

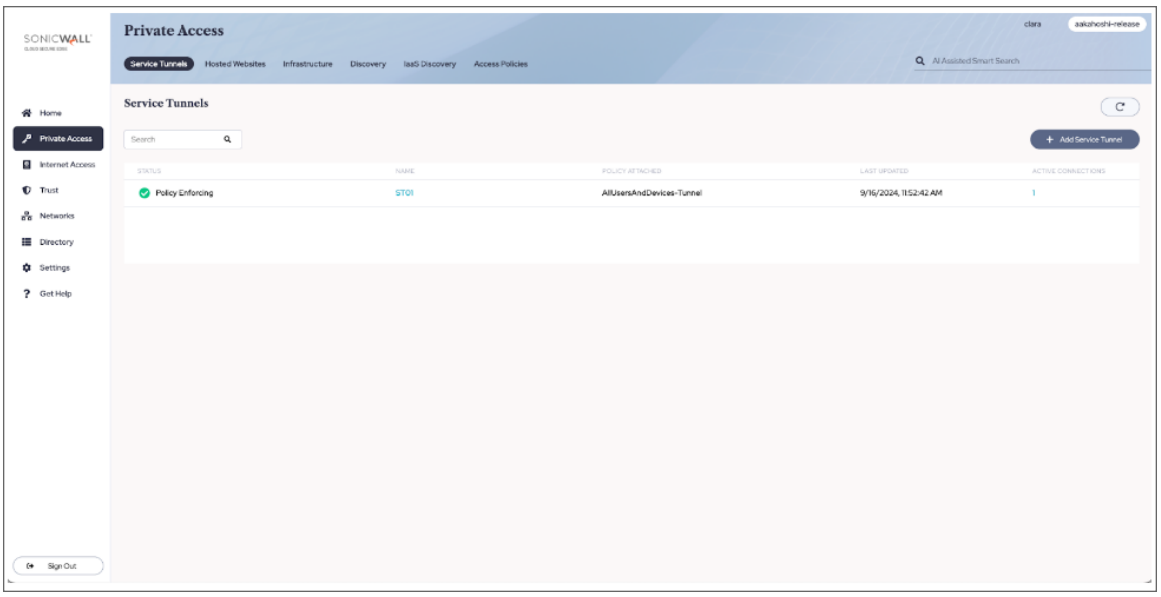
The following provides a checklist for setting up remote access; for more details, follow the links provided.

ⓘ | **VIDEO:** This video also describes how to set up a remote access service tunnel in Cloud Secure Edge.

To create a Service Tunnel Policy:

1. Navigate to the document Publish a Service Tunnel.
2. Scroll down to the **Steps to Publish a Service Tunnel** and follow the directions for creating the Tunnel Policy.
3. Continue to **Step 2: Publish a Service Tunnel** and follow the steps to create a Service Tunnel.
4. Apply the Tunnel Policy to the tunnel so your end users can access the Service Tunnel.

To validate that your Service Tunnel is up and running, navigate from **Private Access > Service Tunnels** in the Cloud Edge Command Center. If your Service Tunnel is running, you see it in the Service Tunnels list with a **Policy Enforcing** status.



Blocking Malicious Content

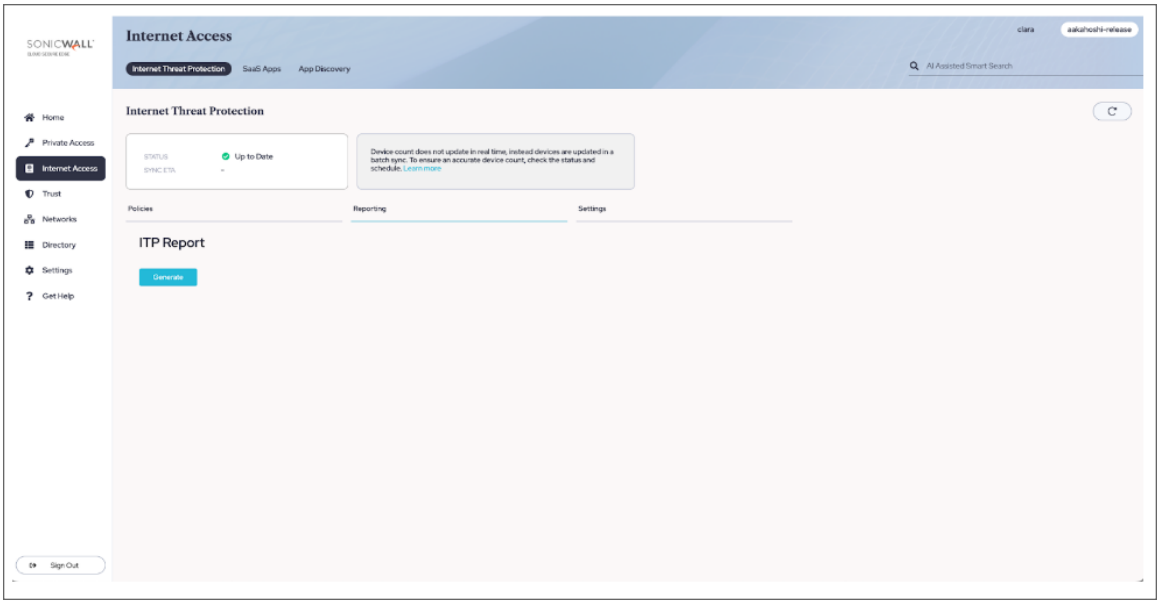
Blocking malicious content is a function of managing Internet Threat Protection (ITP) policies, which are designed to protect users and devices from untrusted internet resources. Administrators can create and manage ITP policies in the Command Center and assign them to users and devices via Roles, like other protected services in Cloud Secure Edge.

ⓘ **VIDEO:** In addition to the procedure below, you can refer to the video that describes how to block malicious or inappropriate content.

To create and select ITP Policy :

1. Navigate to the document Managing Internet Threat Protection Policies.
2. Scroll down to **Step1: Create an ITP Policy** and follow the directions for creating the ITP Policy.
3. If SCIM (System for Cross-domain Identity Management) is enabled, assign the users to your ITP Policy.
   If SCIM Is not enabled, admins should instruct end users to log into Cloud Secure Edge and register their devices. When done, the admin can assign the end users to the policy.
4. Scroll down to **Exclude Users from ITP Policies** in Managing Internet Threat Protection Policies and follow the steps provided.

To validate that your Internet Threat Protection (ITP) Policy is active, navigate to **Internet Access > Internet Threat Protection**. Select your ITP policy from the list, under **Policies**. Verify that the status is **green** and reads **Up to Date**. Under the **Reporting** tab, select **Generate** to generate an ITP Report.



Protecting SaaS Applications

The following describes how to protect SaaS applications.

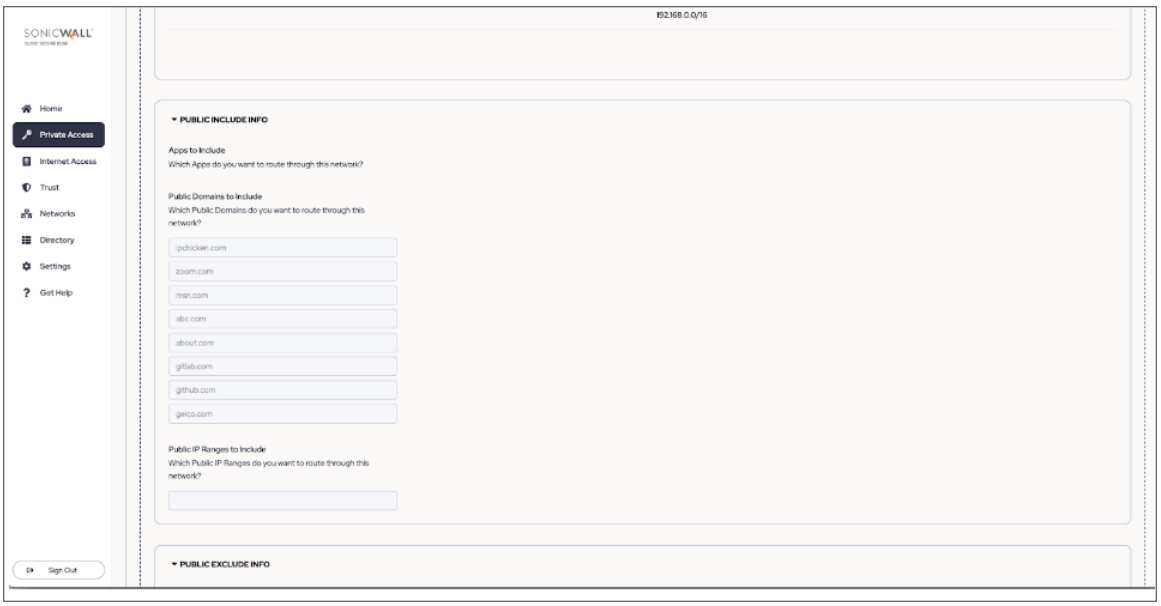
ⓘ | **VIDEO:** You can also refer the video that discusses protecting a SaaS service with Allow Lists.

To protect SaaS applications:

1. Navigate to the document Publish a Service Tunnel.
2. Scroll down to the **Steps to Publish a Service Tunnel** and follow the directions for creating the Tunnel Policy. This policy determines which of your end users can access your Service Tunnel.
3. If SCIM (System for Cross-domain Identity Management) is enabled, assign the users to your Tunnel Policy.

   If SCIM Is not enabled, admins should instruct end users to log into Cloud Secure Edge and register their devices. When done, the administrator can assign the end users to the policy.
4. Continue to **Step 2: Publish a Service Tunnel** and follow the steps to create a Service Tunnel.
5. Scroll down to **Network Settings, Step 2.4** and follow the steps to configure a SaaS application configuration (via following IPs).

To validate that your SaaS application is protected, navigate to **Private Access > Service Tunnels** in the Cloud Secure Edge Command Center. Select the Service Tunnel on which you configured the SaaS applications. Review the configuration under **Public Include Info** and verify that your SaaS applications are correctly entered into the **Apps to Include** field.



Configuring ZTNA

SonicWall Cloud Secure Edge authenticates your end users so that they can securely access select websites via their web browsers. Registering a hosted web service allows you to enforce a zero-trust policy when users try to access your internal website or web application.

ⓘ **VIDEO:** In addition to the procedure below, you can refer to a video that describes how to configure Zero Trust Network Access (ZTNA).

To setup ZTNA:

1. Navigate to the document Register a Hosted Website to Users.
2. Scroll down to **Step1: Create a Policy for web access** in the **Steps to create a hosted Website** section.
3. Follow the directions for creating a Web Policy.
4. If SCIM (System for Cross-domain Identity Management) is enabled, assign the users to your Web Policy.

   If SCIM Is not enabled, admins should instruct end users to log into CSE and register their devices. When done, the administrator can assign the end users to the policy.
5. Complete **Step 2: Register the web application as a hosted website**.
6. Complete **Step 3: Securely access the hosted website via your device**.

To validate that your private resource (for example, the hosted website or SSH service) is protected, navigate to select your Service Name. In your service, select **Test Connection** (the check icon in the upper right corner of the page). This shows you the status of your connection, detailing whether your domain name or hostname is resolvable and whether the Access Tier and backend port are reachable.

Checking the Device Posture

The first step to checking the device posture is to understand Trusted Profiles. A Trust Profile applies administrator-defined Trust Factors to a specific subset of devices within an organization. Trust Profiles allow administrators to assign a set of Trust Factors (with designated Trust Effects) to user groups, device serial numbers, operating systems, and device ownership types.

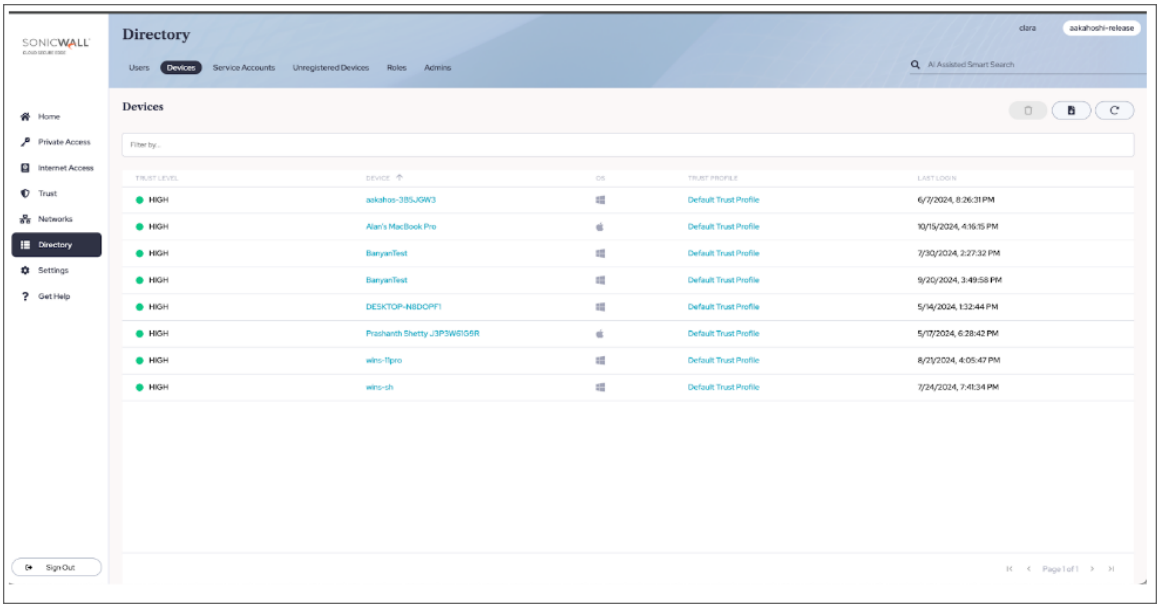
ⓘ **IMPORTANT:** Trust Profiles can take up to 10 minutes to associate with a device. This delay only occurs when the Trust Profile assignment has been edited, or the Trust Profile prioritization has been adjusted. Changes to Trust Factors are reflected the next time the application synchronizes with the Command Center.

ⓘ **VIDEO:** In addition to the procedure below, a video is available that describes how to check the device posture.

To check a device's security posture:

1. Navigate to the document Trust Profile.
2. Review the material provided to learn about Trust Profiles and how they function.
3. Using a sample Trust Profile configuration as a template (for example, the Application Check Trust Factor), configure a Trust Profile to check the devices' security posture.

To validate that your organization's end users' devices are reporting a **High Trust Level**, navigate from **Directory > Devices** in the Cloud Edge Command Center. Here you can view a list of all devices in your organization and their **Trust Level** status.



6

Monitoring Performance

Both the firewall and Cloud Secure Edge have different logs that you can use to monitor your system's activity.

Device Log Setting on the firewall	SonicOS collects and displays log events for the CSE Connector. On the firewall, navigate to **Device | Log > Settings** to view the settings table. For more information, refer to the SonicOS Cloud Secure Edge Feature Guide.
Events Viewer for CSE	Use the Events Viewer to review security events associated with end-user activity in your Cloud Secure Edge organization. You can filter and explore different lists of events. For more information, refer to Events Viewer.
System Log for CSE	The System Log provides a time-stamped log of administrators' actions performed via the Cloud Secure Edge API or web console so that their previous actions can be reviewed and understood for auditing purposes. In the log, you can view: • Actions taken • Administrator who took the action • Time of the action • Details about the action • Written notes about the action For more information, refer to System Log.

7

Best Practices

The following suggests best practices for maintaining and optimizing your Cloud Secure Edge environment.

Recommendation	Guideline
Regular policy audits	Periodically review security policies and network segmentation.
Patch management	If you have a solution that includes a Firewall Connector, be sure SonicOS is updated with the latest security patches and maintenance releases.
License renewals and upgrades	Monitor license expiration dates to ensure service continuity.
User management	If you use SCIM, most user management tasks are automated. If you don't, you should regularly review and update user roles, access levels, and remove inactive accounts.
Trust Scoring	Cloud Secure Edge calculates Trust Levels for all the devices in your fleet for use in access policies. Trust Status should be reviewed regularly to be sure the defined criteria are the most up to date.

If you need more information on any of these best practices or want to explore more detail on the features available, refer to the following Cloud Secure Edge documentation:

- Cloud Secure Edge Documentation
- Technical Documentation portal for SonicOS documentation related to Cloud Secure Edge
- Cloud Secure Edge Documentation Guide
- Knowledge Base articles
- Cloud Secure Edge videos

8

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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

About This Document

Cloud Secure Edge Getting Started Guide
Updated - December 2024
232-006214-00 Rev B

Copyright © 2024 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