HARMONY

29 July 2024

# HARMONY SASE

Administration Guide

CHECK POINT™

# Check Point Copyright Notice

© 2024 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page for a list of our trademarks.

Refer to the Third Party copyright notices for a list of relevant copyrights and third-party licenses.

# Important Information



### Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



### Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.



### Check Point Harmony SASE Administration Guide



### Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.



### Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

## Related Documents

## Revision History

| Date | Description |
|---|---|
| DD MMM YYYY | First release of this document |

# Table of Contents

**Introduction to Harmony SASE** ... *13*
Private Access ... *13*
Internet Access ... *14*
Harmony SASE Agent ... *14*
Supported Devices and Operating Systems ... *15*
How it Works ... *16*
Use Cases ... *16*
Benefits ... *17*
**Getting Started** ... *18*
Creating an Account in Harmony SASE (Perimeter 81) ... *20*
Activating Harmony SASE (Perimeter 81) Subscription ... *21*
**Migrating the Harmony SASE (Perimeter 81) Workspace to Check Point Infinity Portal** ... *22*
Using Check Point User Center for Billing and Subscription ... *22*
Creating an Account in the Infinity Portal ... *23*
Accessing the Harmony SASE Administrator Portal ... *23*
Licensing the Product ... *27*
Specific Service Roles ... *28*
**Overview** ... *29*
My Clients ... *30*
Member Licenses ... *30*
Gateway Licenses ... *30*
Organizations ... *30*
Adding an Organization ... *31*
Managing Billing ... *34*
Invoices ... *35*
**Billing** ... *37*
Manage Plan ... *38*

Updating the Subscription Plan ... 38
Modifying Member Licenses ... 40
Modifying Gateway / Application Licenses ... 42
Adding a Payment Method ... 44
Cancelling Subscription ... 45
Invoices ... 46
Billing Details ... 46
**Dashboard** ... ***49***
Active Sessions ... 49
Member Licenses ... 50
Gateway Licenses ... 50
Applications ... 51
Active Agent Users ... 51
Users Bandwidth ... 52
OS Distribution ... 52
Device Type Distribution ... 52
Agent Version by OS ... 53
**Team** ... ***54***
Members ... 55
Member Roles and Permissions ... 56
Invite Members ... 57
Inviting Members Manually ... 57
Inviting Members Using an Identity Provider ... 57
Managing Members ... 58
Changing Member Role ... 58
Unblocking Members ... 58
Generating Sign-Out Code ... 58
Resetting a Member Password ... 59
Resetting Google Authenticator Two-Factor Authentication for a Member ... 59
Adding Licenses ... 61

Groups 63
Creating a Group 63
User Configuration Profiles 65
Adding a Configuration Profile 65
Web Platform Configuration 65
General Configuration 66
Agent Configuration 66
General Configuration 66
Agent Upgrades 67
Network Configuration 68
Windows 69
Use VPN Interface DNS 69
Notify Reconnect 69
Android / Chromebook 70
Default Protocol 70
Mac 70
Use VPN Interface DNS 70
iOS 71
Auto Reconnect 71
**Devices** 72
Device Inventory 73
OS Distribution 73
Posture Status 73
Device Inventory Details 74
Logging Out the Device 75
Removing Device 75
Posture Check 76
Supported Posture Requirement Checks 76
Specifying the Device Posture Check Requirements 77
Downloads 84

Downloading and Deploying the Harmony SASE Agent ... 84
Certificates ... 85
Deploying the Harmony SASE Agent ... 88
Deploying the Agent Manually ... 88
Deploying the Agent Using an MDM Application ... 89
Common Commands ... 89
Installing Harmony SASE on Chromebook ... 90
Using the Harmony SASE Agent ... 93
Troubleshooting System Extension Installation on macOS ... 98
Uninstalling the Harmony SASE Agent ... 100
Windows ... 100
macOS ... 100
Linux ... 100
Ubuntu ... 100
Android / iOS ... 101
Collecting Logs Manually ... 102
Windows ... 102
macOS ... 103
Linux ... 104
**Networks** ... ***105***
High-Level Procedure ... 105
Regions and Point-of-Presence ... 106
Gateways ... 109
Private Gateways ... 109
[DEPRECATED] Shared Gateways ... 109
Tunnels ... 112
IPSec Site-2-Site VPN Tunnel ... 112
WireGuard Connector Tunnel ... 113
OpenVPN Tunnel ... 113
Internal Network Subnet ... 114

Defining a Network ... 115
Adding Gateways to an Existing Network ... 117
Deactivating a Gateway ... 118
Adding a Tunnel ... 121
IPsec Site-2-Site VPN Tunnel ... 122
Prerequisites ... 122
IPSec Handshake ... 122
Phase I (IKE or Gateway) ... 122
Phase II (ESP or Tunnel): ... 122
Policy-Based and Route-Based IPSec Connection ... 123
Supported Integrations ... 124
High-Level Procedure ... 124
WireGuard Connector Tunnel ... 126
Prerequisites ... 126
Configuring a WireGuard Connector Tunnel ... 126
Configuring the Connector in the Harmony SASE Administrator Portal ... 126
Installing the WireGuard Connector on a Linux Server ... 129
Verifying the Setup ... 130
Removing the WireGuard Connector ... 131
OpenVPN Tunnel ... 132
Configuring the OpenVPN Tunnel in the Harmony SASE Administrator Portal ... 132
Installing a VPN and Configuring the OpenVPN Tunnel on the Device ... 134
Verifying the Setup ... 140
Managing a Network ... 141
Editing a Network ... 141
Adding Regions ... 142
Managing Access ... 143
Firewall Rules ... 145
Split Tunneling ... 145
Private DNS ... 147

DNS Filtering 151
Routes Table 154
Deleting a Network 157
**Private Access** 159
Firewall 160
Use Case 160
Prerequisite 160
Access Rules Order 160
Creating a Firewall Access Rule 160
Enabling or Disabling Firewall Logs 162
Applications 164
Use Case 164
Prerequisites 164
Adding an Application 165
Adding an HTTP/HTTPS Zero Trust Application 167
Adding an RDP Zero Trust Application 172
Prerequisite 172
Additional Registry Configuration 177
Windows 7 177
Windows Server 2016 177
Windows Server 2019 178
Troubleshooting 178
Upstream Error 178
Additional Troubleshooting Steps 179
Adding a SSH Zero Trust Application 181
Prerequisite 181
Adding a VNC Zero Trust Application 186
Prerequisite 186
Accessing an Application by a Member 190
Application Policies 191

Creating an Application Access Policy ... 191
Assigning a Policy to an Application ... 193
**Internet Access** ... **194**
High-level Procedure ... 194
Web Filter Rules ... 195
Creating a Web Filter Rule ... 195
Bypass Rules ... 202
Creating a Bypass Rule ... 202
Bypass Rules for Certificate Pinning ... 211
Default Bypass Rules ... 215
Finding the Process Name of an Application ... 219
**Monitor & Logs** ... **222**
Active Sessions ... 223
Member Activity ... 224
Web Activity ... 226
Insights ... 226
Web Events Blocked ... 226
Top Web Categories ... 227
Events Per User ... 227
All Web Activities ... 227
Malware Protection ... 229
Insights ... 229
Incidents Blocked ... 229
Malware Types ... 230
Blocked Malware Per User ... 230
All Malware Activities ... 230
Admin Activity ... 232
Tunnels Status ... 236
Firewall Events ... 237
**Objects** ... **239**

Addresses 240
Creating an Address Object 240
Managing Addresses 241
FQDN-based Firewall Objects 243
FQDN Wildcards 243
Multi-Level Sub-domains 243
Important Considerations 243
Limitations 243
Services 245
Creating a Service Object 245
Managing Services 248
Custom URLs 249
Creating a Custom URL Object 249
Managing Custom URLs 250
**Settings** 252
Integrations 253
Security Information and Event Management (SIEM) Integrations 253
Professional Services Automation (PSA) Integrations 253
Splunk Cloud 253
Integrating Splunk Cloud 253
Step 1 - Setting Up the HTTP Event Collector 253
Step 2 - Enabling an HTTP Event Collector 253
Step 3 - Creating an Event Collector Token 254
Configuring the Splunk Integration in the Harmony SASE Administrator Portal 255
Troubleshooting 257
Microsoft Sentinel 258
Configuring the Integration in the Microsoft Azure Portal 258
Step 1 - Setting up a Log Analytics Workspace 258
Step 2 - Linking the Log Analytics Workspace to Microsoft Sentinel 259
Step 3 - Finding your Log Analytics Workspace ID and Primary Key 260

Configuring the Microsoft Sentinel Integration in the Harmony SASE Administrator Portal 261
Troubleshooting 262
Amazon S3 262
Prerequisites 262
Configuring the Integration in the AWS Management Console 263
Step 1 - Creating a New Bucket 263
Step 2 - Creating a New IAM Policy 265
Step 3 - Creating an AWS User 267
Step 4 - Creating an AWS Access Key 267
Configuring the Amazon S3 Integration in the Harmony SASE Administrator Portal 269
Troubleshooting 270
ConnectWise PSA 271
Generating API Key in ConnectWise PSA 271
Configuring the Integration in the Harmony SASE Administrator Portal 275
Mapping Customers and Agreements 276
Identity Providers 278
Two-Factor Authentication 279
Activating Two-Factor Authentication 279
Configuring Duo Security for Two-Factor Authentication 280
Deactivating Two-Factor Authentication 281
Certificate Manager 282
Support Access 285
Granting the Support Access Role 285
Access History 286

# Introduction to Harmony SASE

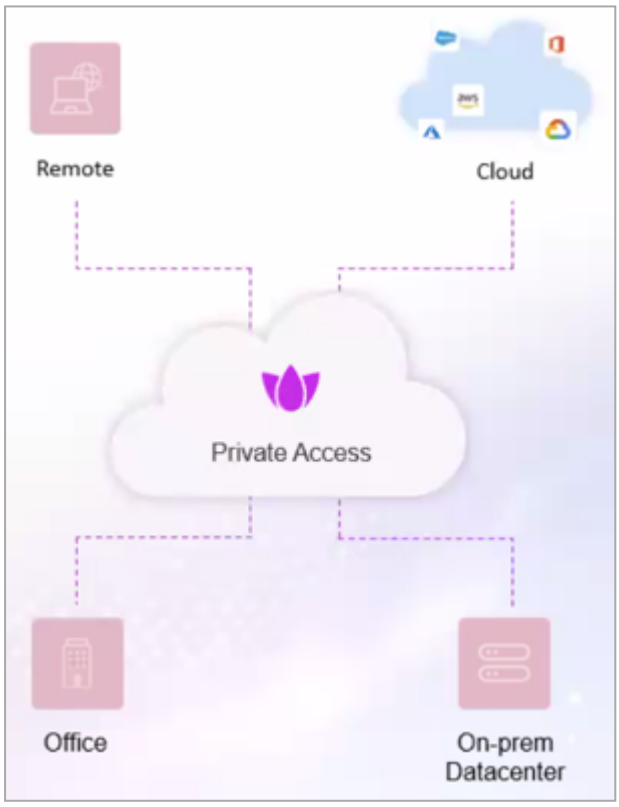
Harmony SASE is a cloud-based Secure Access Service Edge (SASE) solution that provides secure private and internet access to your remote and branch office users.




## Private Access

Private access includes:

- Complete Zero-Trust Network Access to all your corporate resources (on-premises and cloud data centers) to your remote or office workforce.

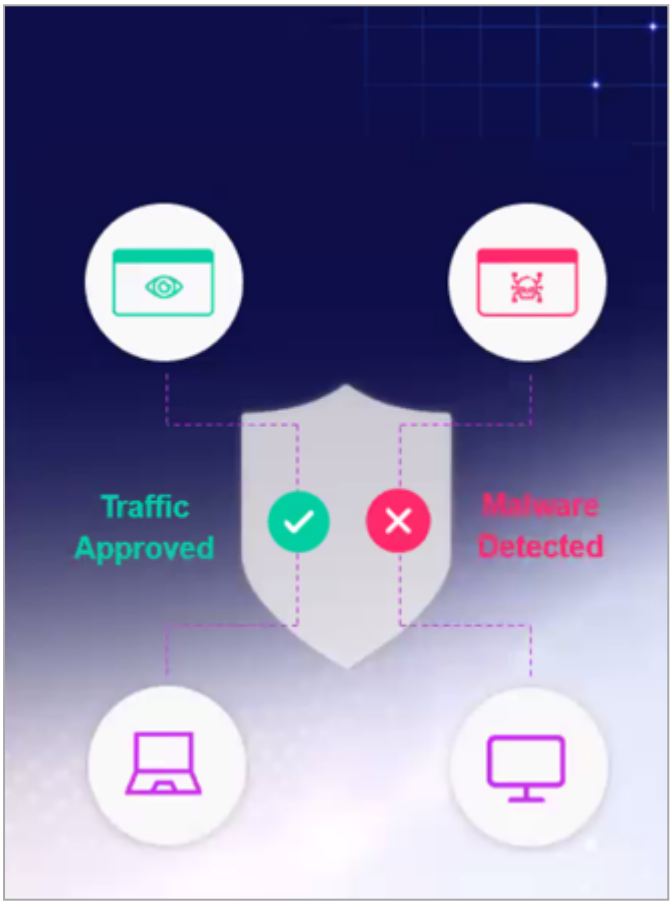



- Agentless access to only specific applications only to authorized members (also known as Application Access), for example, users with BYOD and contractors. The supported types of applications include:

| Application Type | Example |
|---|---|
| HTTP/HTTPS | Bitbucket |
| RDP | My Desktop |
| SSH | Staging Web Server |
| VNC | Build PC |

# Internet Access

Internet access includes safe access to all the web traffic to to your remote or office workforce.




# Harmony SASE Agent

Harmony SASE Agent is an application that is installed on desktops or mobile devices to enforce safe private and internet access.

**Note** - The agent is not required for application access.

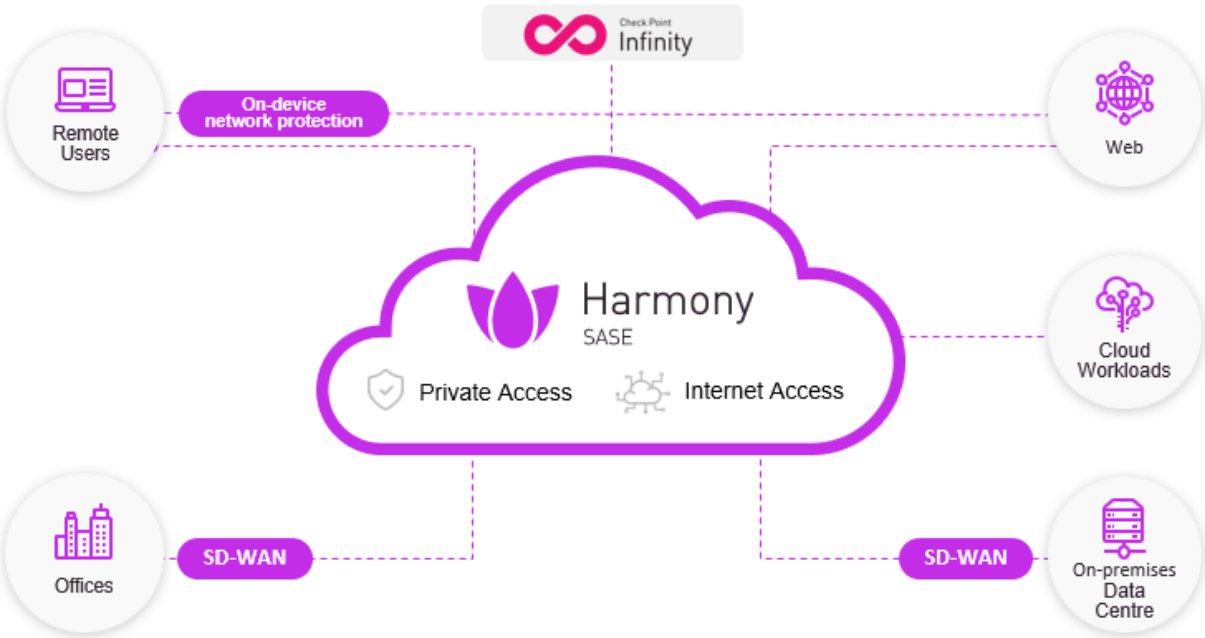
# Supported Devices and Operating Systems

| Operating System | Version | Action |
|---|---|---|
| **Desktops and Servers** | | |
| Windows EXE | Windows 10 or later | EXE file is downloaded. For example, Perimeter81_ 10.1.1.1438.exe. |
| Windows MSI | Windows 10 or later | MSI file is downloaded. For example, Perimeter81_ 10.1.1.1438.msi. |
| macOS | macOS 11 or later | PKG file is downloaded. For example, Perimeter81_ 10.3.0.601.pkg |
| Ubuntu | Ubuntu 20.04 or later | Deb file is downloaded. For example, Perimeter81_ 8.0.4.735.deb. |
| Red Hat | RedHat 7 or later | RPM file is downloaded. For example, Perimeter81_ 8.0.4.735.rpm. |
| Fedora | Fedora 30 or later | RPM (Fedora) file is downloaded. For example, Perimeter81_ 8.0.4.735-fedora.rpm tar.xz. |
| Linux - Others | Linux 7.0 or later | tar.xz file is downloaded. For example, Perimeter81_ 8.0.4.735.tar.xz. |
| **Mobile Devices** | | |
| Android / Chromebook | Android 8.1.0 or later | Redirected to Google play. |
| iOS | iOS 15 or later | Redirected to App store. |

# How it Works

Harmony SASE's cloud-gateway integrates with your SD-WAN (edge) devices in your branch offices or data centers. Its primary function is to process the private access rules, such as firewall rules and application rules. This gateway connects to the Harmony SASE Agent to provide a secure full network access. It also connects to a web portal (agentless) to provide secure application access.

For secure internet access, the Harmony SASE uses the in-built Secure Web Gateway (SWG) equipped with a Malware Protection Engine (On-device Network Protection capability) in the Harmony SASE Agent to process the web filter rules without requiring a separate gateway.




# Use Cases

- You want to provide secure internet access to your remote workforce.
- You want to provide zero-trust network access to your remote workforce.
- You want to provide secure access to only particular corporate applications (not entire private access) to your temporary workforce, such as contractors.
- You want to provide both secure internet and private access to your workforce operating from your offices.

# Benefits

- Easy-to-deploy SASE solution.
- 2x faster internet security with on-device protection.
- Improved privacy
- Accurate location services
- Web filtering
- Malware protection and traffic inspection
- Automatically detect and protect non-secure WiFi traffic
- Zero-trust access to network and SaaS
- Full mesh any-to-any connectivity to your private network.
- A SASE solution that also integrates with your on-premises or cloud SD-WAN infrastructure.
- Secure access to internal corporate applications (SSH, RDP, Web, Tunnel, and Database) residing in the data center, public or private clouds. Ideal for BYOD and third-party users with no agent installation or management required.

# Getting Started

**To get started with Harmony SASE:**

1. Create an account in Perimeter 81.
2. Activate your Perimeter 81 subscription.
3. <To be linked-Creating a Network>Create your secure network with <To be linked-Networks> regions and private gateways.
4. Connect your On-Premises and Cloud Infrastructure:

   <To be linked-Connect Infrastructure> Deploy site-to-site tunnels to securely connect your local and cloud resources. You can integrate seamlessly with any cloud IaaS environment (such as <To be linked-Networks> AWS, <To be linked-Networks>Azure, and <To be linked-Networks> GCP), on-premises firewalls (such as <To be linked-Networks> Check Point, Palo Alto Networks, SonicWALL, and more), routers, or SD-WAN devices.
5. Add users to your workspace:
   - To add members, see <To be linked-Users and groups> Inviting Users.
   - To enable single sign-on, see <To be linked-Users and groups> integration with Identity Providers.
   - Create or import your user groups and build user-centric network or application policies accordingly.
6. To set up Secure Access Rules (Zero Trust Network Access):
   - <To be linked-Agents> Download and deploy our agents to your organization-managed devices
   - Configure <To be linked-Applications> agent-less access, Zero Trust Applications.
   - Configure user-centric firewall policies
   - Configure device posture check rules
7. To set up Secure Internet Rules (Secure Web Gateway)*, configure the <To be linked-Internet Access> Web Security policies, and set up Bypass Rules for traffic that should not be inspected. <To be linked-Topic> Advanced Malware Protection is enabled by default.

   *SWG add-on required.
8. Start to watch your network:

<To be linked-Monitor Logs> Track member activities and alerts, <To be linked-Monitor Logs> active sessions, user devices, compliance status, malware reports, web activity reports, network firewall logs, and more.

# Creating an Account in Harmony SASE (Perimeter 81)

**To create an account in Perimeter 81:**

1. Go to Harmony SASE portal.

   The home page appears.

2. Click **Get Started**.
3. Enter:
   - **Name**
   - **Work Email address**
4. Click **Next**.
5. In the **Company Name** field, enter the name of your company.
6. From the **Company Size** list, select the approximate number of employees in your company.
7. Click **Next**.

   Perimeter 81 sends a confirmation code to your registered email address.

8. Enter the confirmation code.
9. Enter the workspace URL to log in to your tenant. For easy identification, Perimeter 81 recommends adding your organization's name in the URL.

   For example, if you enter the workspace URL as CompanyABC, then Harmony SASE creates the workspace URL as *https://CompanyABC.perimeter81.com*

   **Note** - You cannot change the workspace name after you create it.

10. Click **Next**.
11. Create a password to log in to your workspace.
12. Click **Get Started**.

    Harmony SASE creates the account and sends you a confirmation email.

    The dashboard page of your workspace appears.

    **Note** - Optionally, you can click **Get Started** in the confirmation email to go to your workspace's dashboard page.

# Activating Harmony SASE (Perimeter 81) Subscription

**Note** - This is available only for the accounts in the Perimeter 81 workspace.

**To activate your Harmony SASE (Perimeter 81) subscription:**

1. Log in to your Harmony SASE (Perimeter 81) workspace.
2. In the **Dashboard** page, click **Activate Subscription**.
3. In the **Activate Your Plan** page, choose the billing plan.
4. Click **Continue to Payment** and complete the payment.

   **Note** - If you have issues to activate your subscription, contact *Check Point Support*.

# Migrating the Harmony SASE (Perimeter 81) Workspace to Check Point Infinity Portal

**Note** - This is applicable only for the users with an existing Harmony SASE (formerly Perimeter 81) workspace and who want to migrate and access it through the Check Point Infinity Portal.

**To migrate and access an existing Harmony SASE (formerly Perimeter 81) workspace through the Check Point Infinity Portal:**

1. Create an account in the Check Point Infinity Portal.
2. If you already have a Check Point Infinity Portal account, make sure that the data residency of the account matches the data residency of the Harmony SASE ( Perimeter 81) workspace. If the data residency does not match, then do one of these:
   - Contact *Check Point Support* to migrate the Harmony SASE (Perimeter 81) workspace to the same data residency region as your Check Point Infinity Portal account.
   - Create a new Infinity Portal account with the same data residency as the Harmony SASE (Perimeter 81) workspace.
3. To associate the Infinity Portal account with the Harmony SASE workspace, send a request to Harmony SASE support with these information:
   - Harmony SASE (Perimeter 81) workspace name
   - Infinity Portal account ID
   - Infinity Portal data residency region
4. To verify, access the Harmony SASE Administrator Portal from the Infinity Portal.

# Using Check Point User Center for Billing and Subscription

After migration to Check Point Infinity Portal, you can continue to use the current billing process to manage subscription. However, you can optionally use Check Point User Center to manage licenses and subscription that allows you to use other Check Point products.

**To create a User Center account and associate it with your Infinity Portal account:**

1. Create a User Center account. See sk22716.
2. Obtain licenses for Check Point products. See sk22564.
3. Link the Infinity Portal account with the User Center account. See Associated Accounts.

# Creating an Account in the Infinity Portal

Check Point Infinity Portal is a web-based interface that hosts the Check Point security SaaS services.

With Infinity Portal, you can manage and secure your IT infrastructures: networks, cloud, IoT, endpoints, and mobile devices.

To create an Infinity Portal account, see the Infinity Portal Administration Guide.

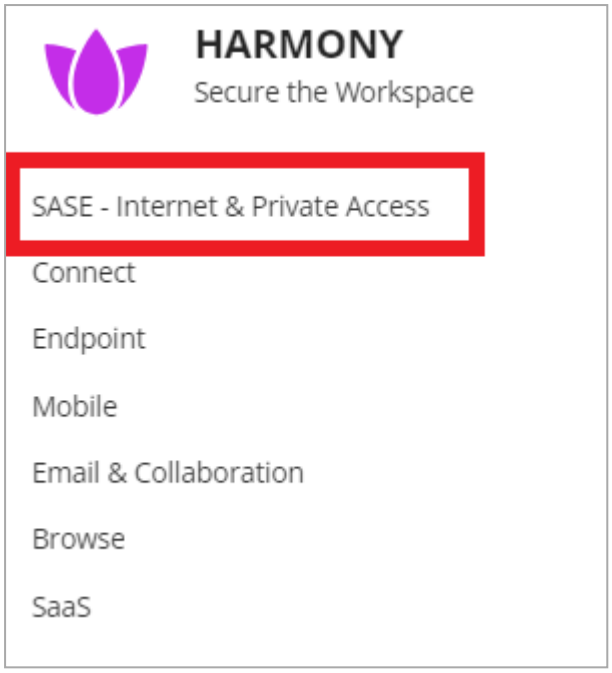
# Accessing the Harmony SASE Administrator Portal

**To access the Harmony SASE Administrator Portal:**

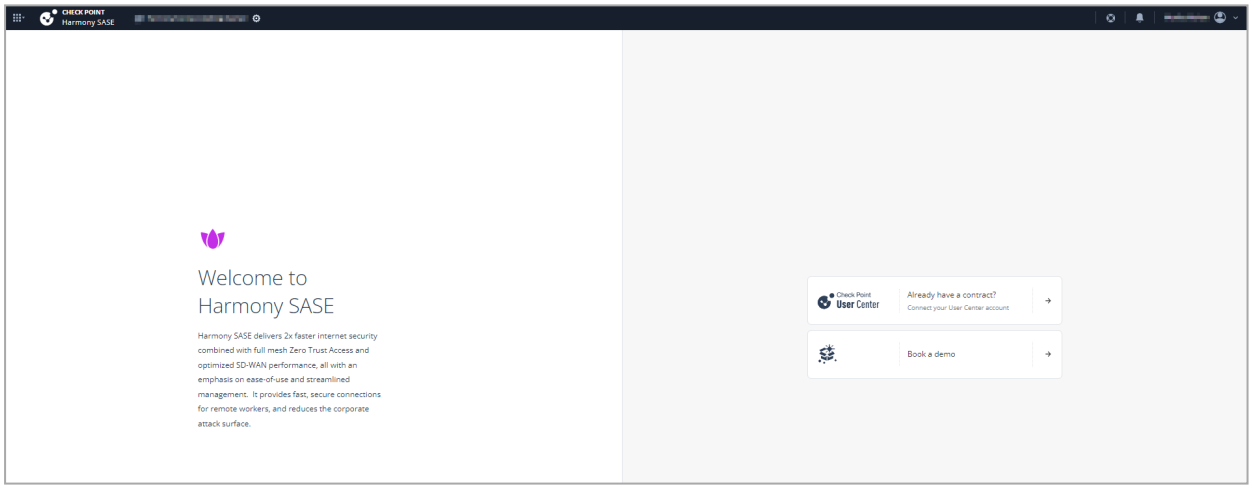
1. Sign in to Check Point Infinity Portal.
2. Click the **Menu** icon in the top left corner.




3. In the **Harmony** section, click **SASE - Internet & Private Access**.



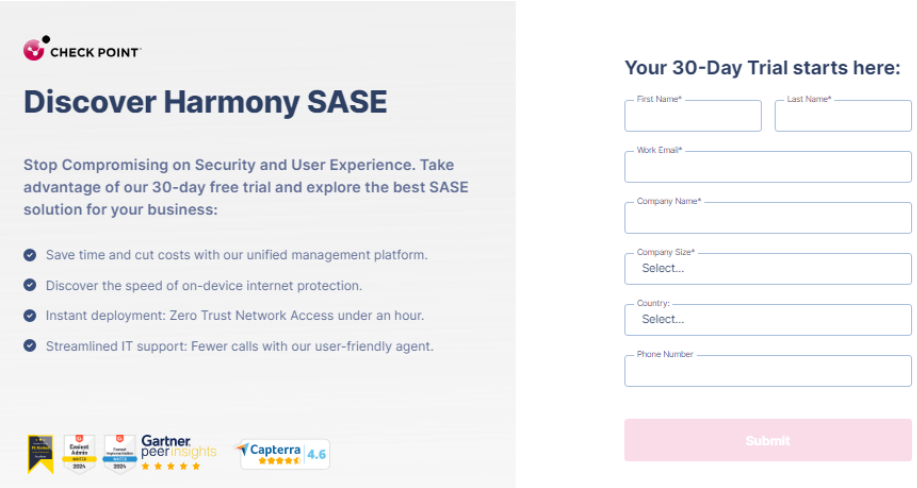

4. If you are accessing the portal for the first time, do one of these:



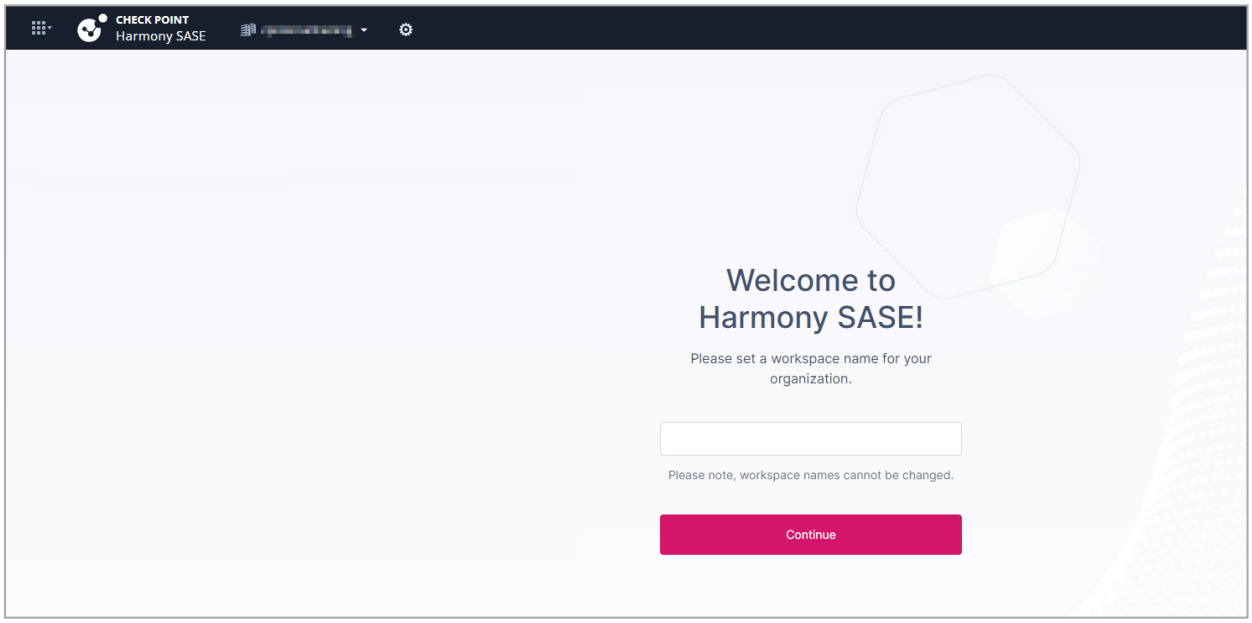

   - If you already have a Check Point contract, click **Already have a contract** to attach the contract to the product. For more information, see **Associated Accounts** in Infinity Portal Administration Guide.

- If you want to trial the product, click **Book a demo**.

  Fill and submit the form. An email is sent with the trial status and further instructions to proceed.

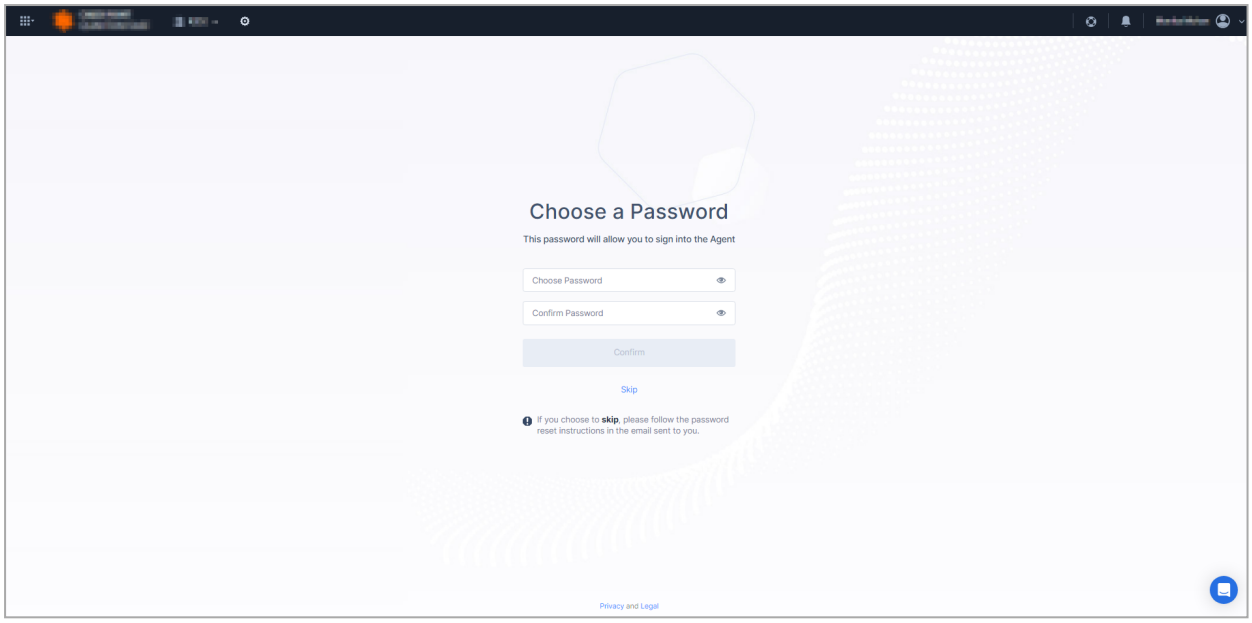



5. Once you fill and submit the form, or If you have already attached the contract with the product, the **Welcome to Harmony SASE** page appears.




6. Enter a name for your workspace. This is used when signing in to the Harmony SASE Agent and when accessing Zero Trust Architecture (ZTA) applications.
7. Click **Continue**.

   The **Choose a Password** page appears.




8. (Optional) Enter the credentials to log in to the Harmony SASE Agent.

   The password must be at least eight characters long with at least one:

   a. Upper case letter

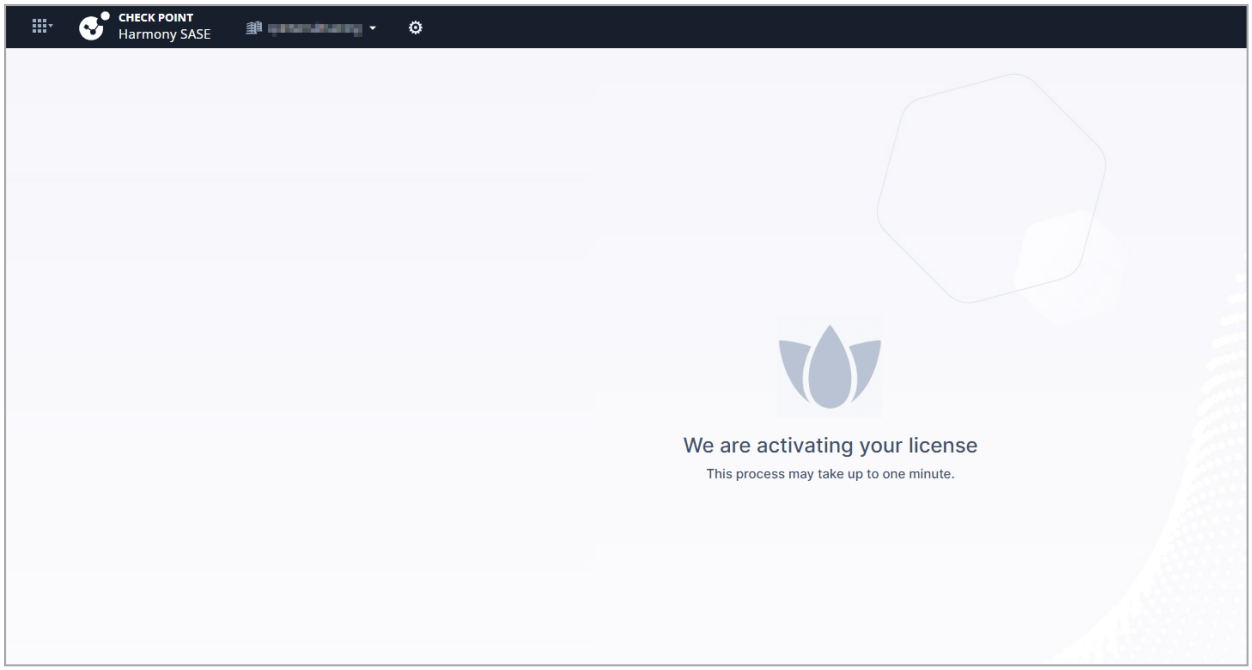
   b. Lower case letter

   c. Number 0-9

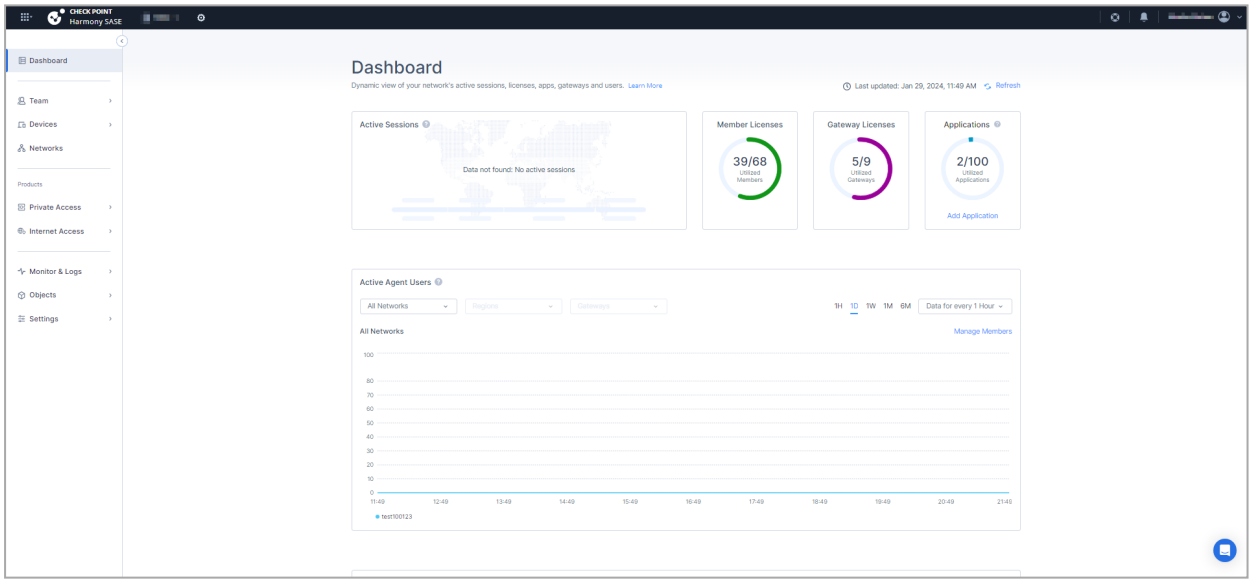
   d. Character !*#%$

   **Notes** - You can click **Skip** to skip this step. The system sends an email with instructions to reset the password.

9. Click **Confirm**.




The license gets activated and the Dashboard page appears.




# Licensing the Product

When you create an account in the Infinity Portal and access the service, you get a free 30-day trial. After the 30-day trial period, you must purchase a software license to use the product. To purchase a license, you must create a Check Point User Center account. For instructions, see sk22716.

After you create a User Center account, contact your Check Point sales representative to purchase a license.

If you have licensed the product, you can view your current contract (license) information from the **Infinity Portal** > **Global Settings** > **Contracts** page.

# Specific Service Roles

Harmony SASE supports specific service roles. The specific service roles are in addition to the global roles and do not override them. For more information, see Specific Service Roles in the *Infinity Portal Administration Guide*.

To access **Specific Service Roles**, go to **Global Settings** > **Users** > **New** > **Add User** and expand **Specific Service Roles**.

| Service Roles | Description |
|---|---|
| Admin | Provides read and write access to full application. |
| Read-Only | Provides full visibility across your Infinity Account. |

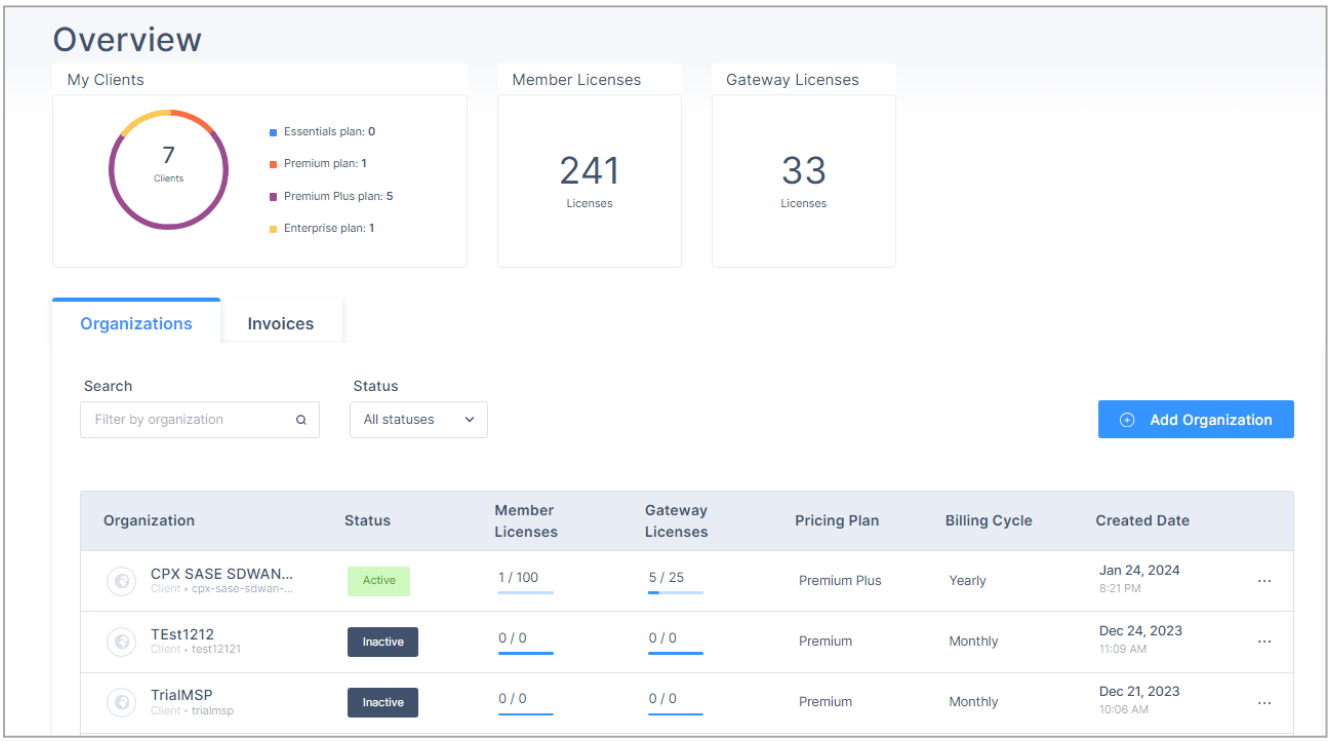
# Overview

**Note** - This page is available only for the MSSP accounts in the Perimeter 81 workspace.

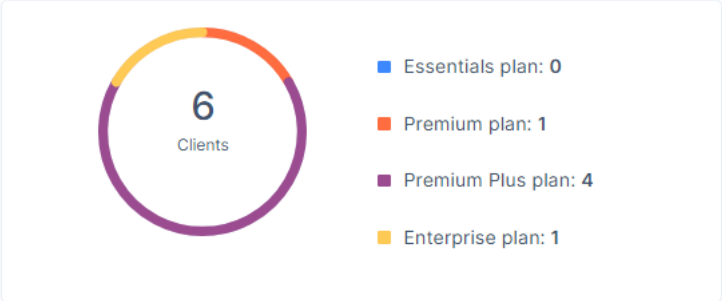
The **Overview** page allows you to view:

- *"My Clients" on the next page*
- *"Member Licenses" on the next page*
- *"Gateway Licenses" on the next page*
- *"Organizations" on the next page*
- *"Invoices" on page 35*

To view the **Overview** page, access the **Harmony SASE** (Perimeter 81) Administrator Portal and click **Overview**.



# My Clients




**My Clients** widget shows the number of clients and their subscription plans.

# Member Licenses

The **Member Licenses** widget shows the total number of purchased member licenses.



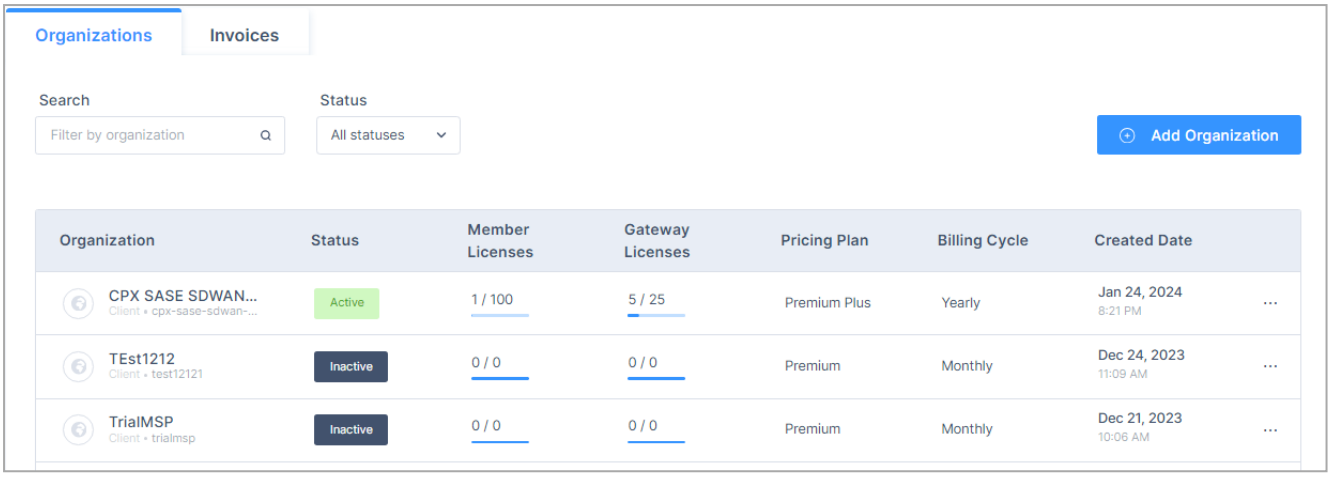

# Gateway Licenses

The **Gateway Licenses** widget shows the total number of purchased gateway licenses.



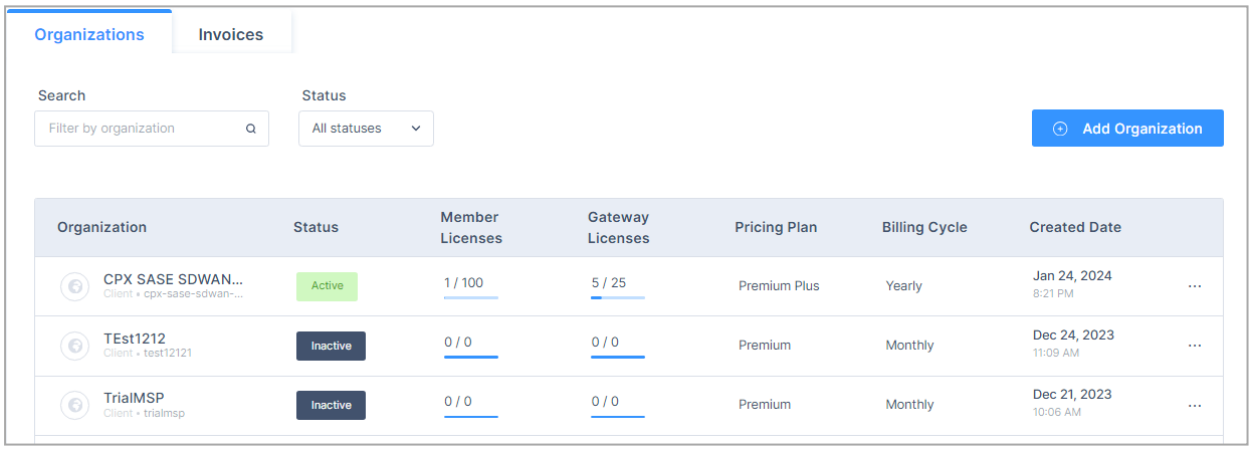

# Organizations

The **Organizations** tab allows you to view and manage billing for the organizations.

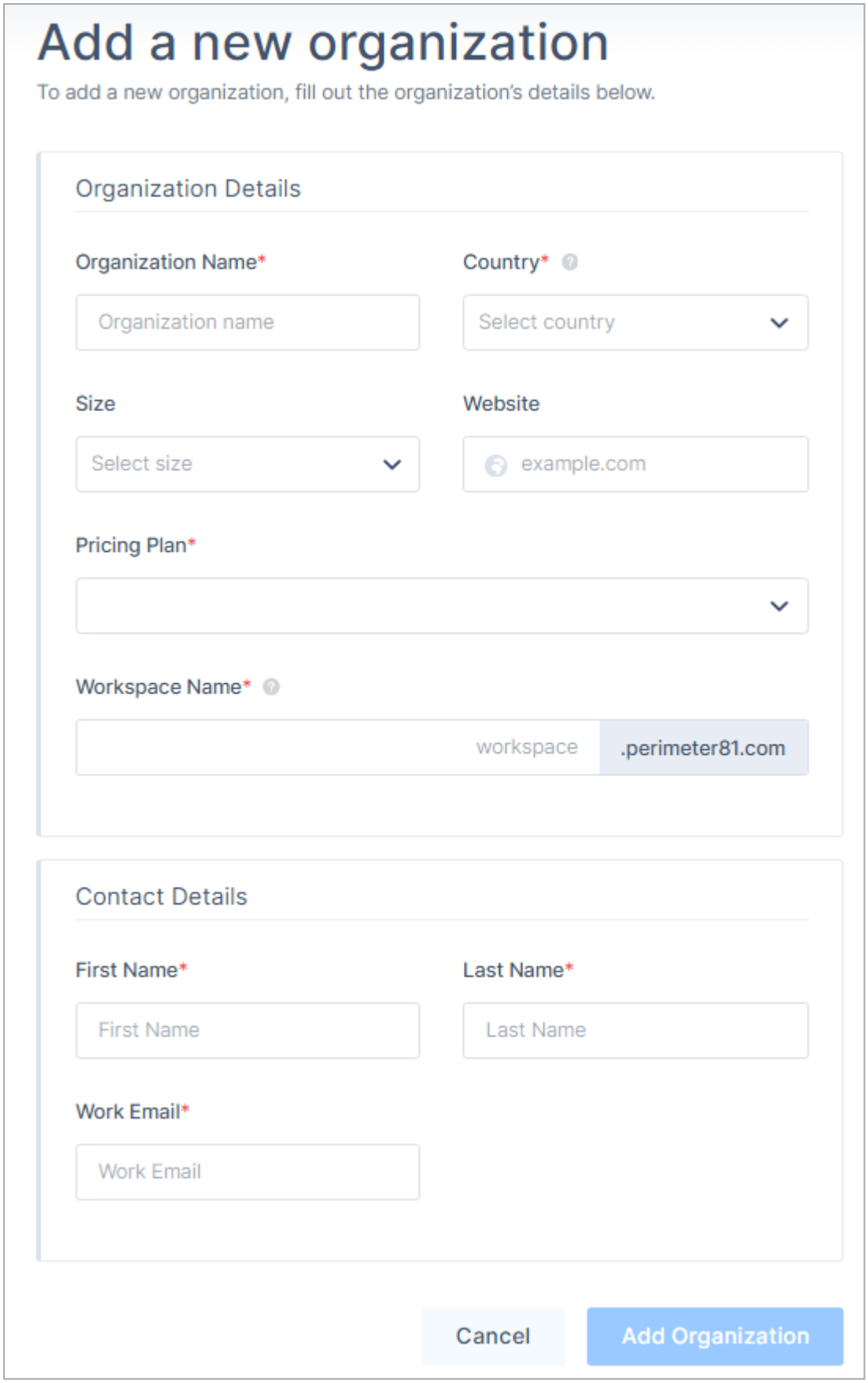



# Adding an Organization

1. Access the **Harmony SASE** (Perimeter 81) Administrator Portal and go to **Overview** and then click the **Organizations** tab.
2. Click **Add Organization**.




The **Add a new organization** window appears.



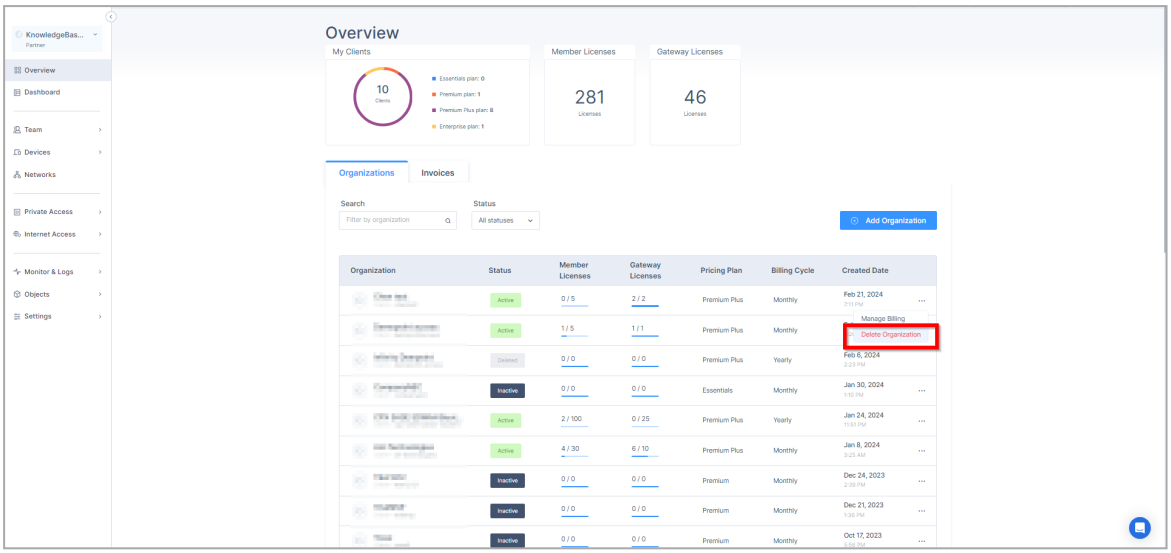

3. In the **Organization Details** section, specify these:

- **Organization Name**
- **Country**
- **Size**
- **Website** - Your organization's website address.
- **Pricing Plan**
- **Workspace Name**.

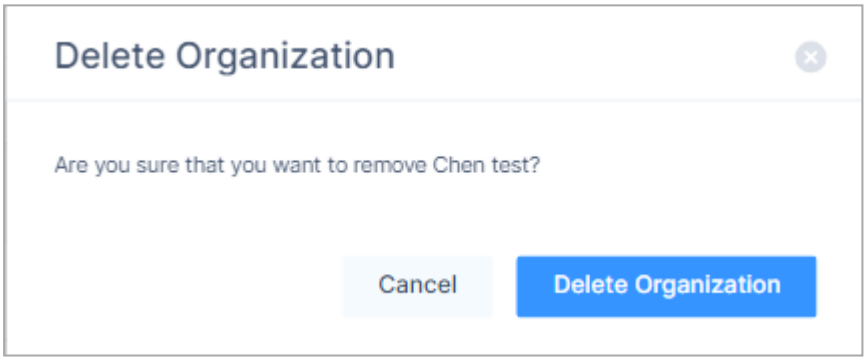
**Note** - You cannot change the workspace name after you create it.

4. In the **Contact Details** section, enter these:
   - **First Name**
   - **Last Name**
   - **Work Email**
5. Click **Add Organization**.
6. To delete an organization, scroll to the end of the row and click ··· .

a. Select **Delete Organization**.



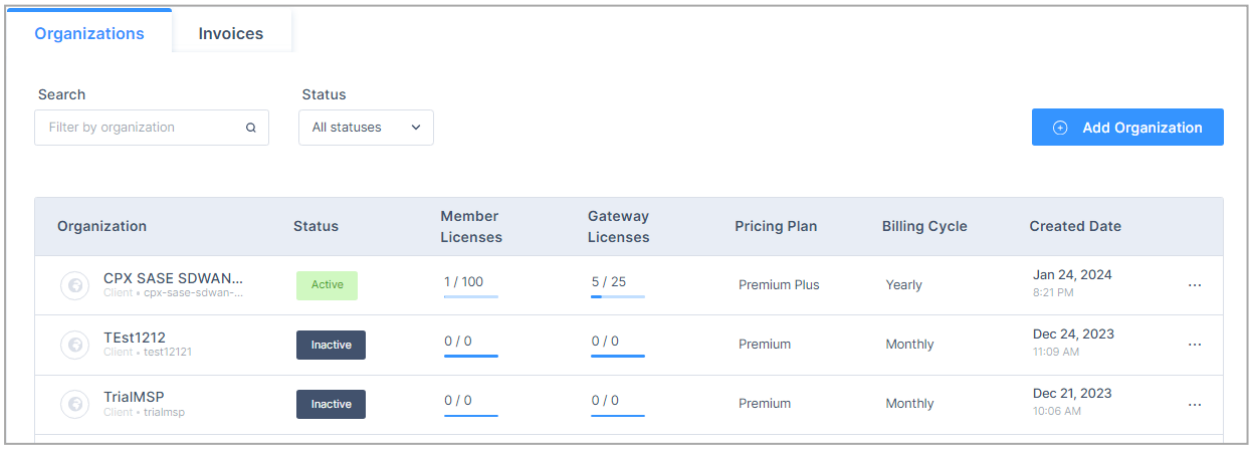

The **Delete Organization** window appears.



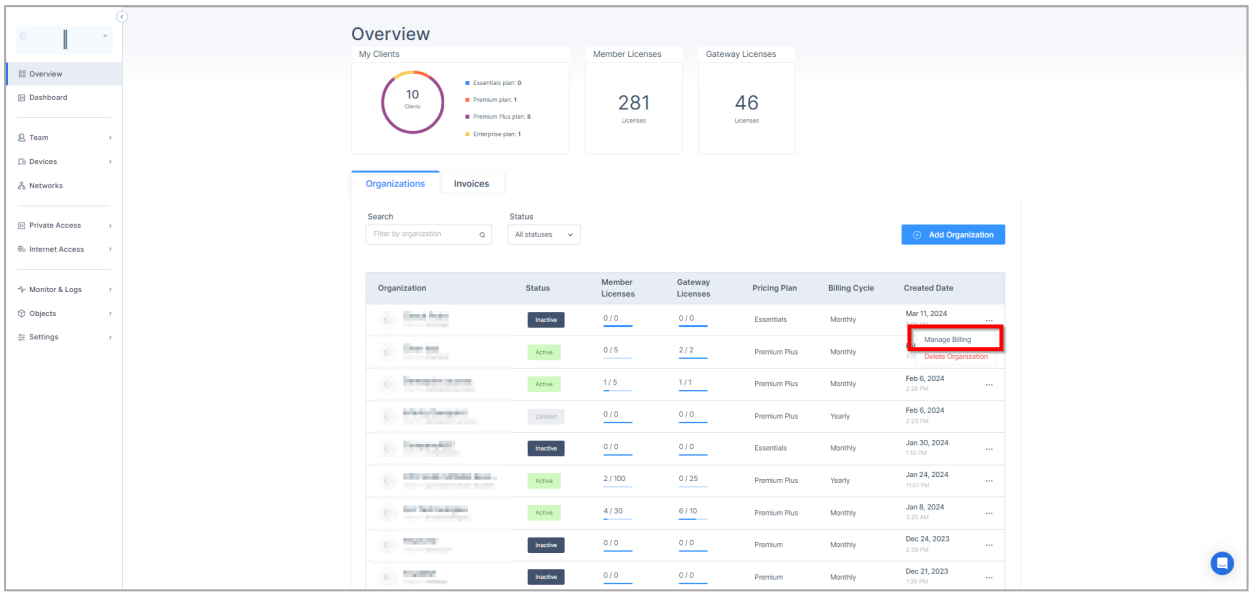

b. Click **Delete Organization**.

## Managing Billing

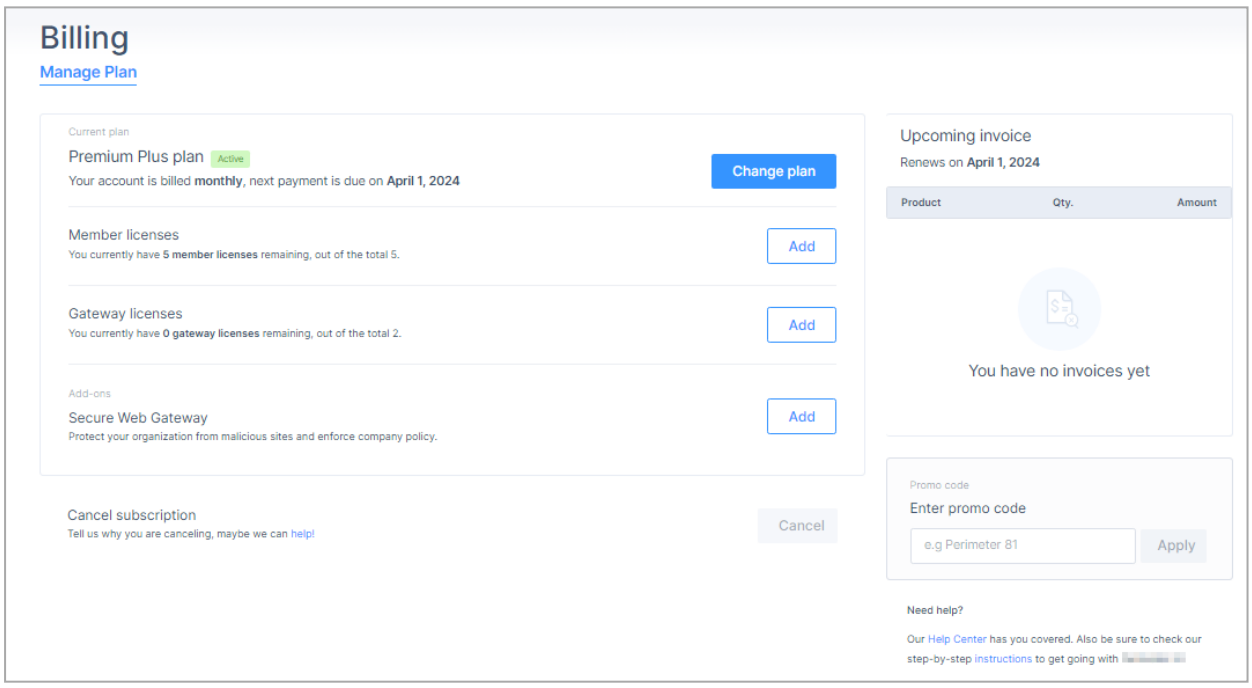
1. Access the **Harmony SASE** (Perimeter 81) Administrator Portal and go to **Overview** and click the **Organizations** tab.



2. Scroll to the end of the row and click ... and select **Manage Billing**.



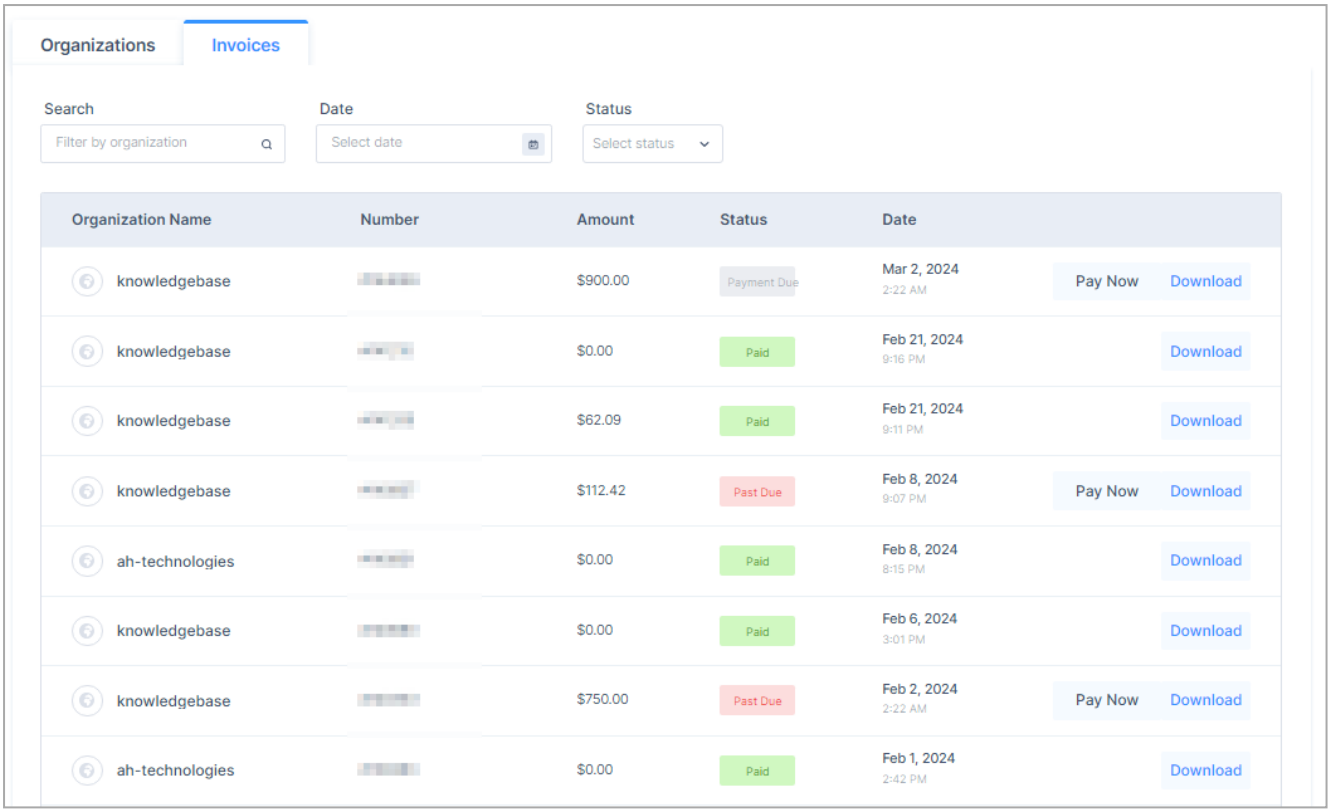

The **Billing** page appears.




3. To change the subscription plan, see Updating the Subscription Plan.
4. To modify member license, see Modifying Member Licenses.
5. To add or remove the gateway license, see Modifying Gateway / Application Licenses.
6. To cancel the subscription, see Cancelling Subscription.

# Invoices

The **Invoices** tab allows you to view, pay and download the invoices.




To pay an invoice, click **Pay Now**.

To download an invoice, click **Download**.

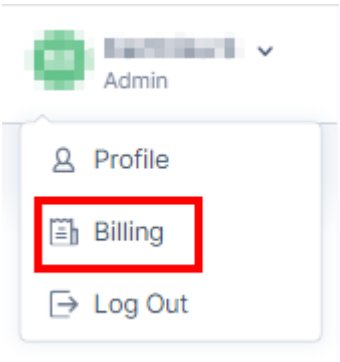
# Billing

**Note** - This page is available only for the MSSP accounts in the Perimeter 81 workspace.

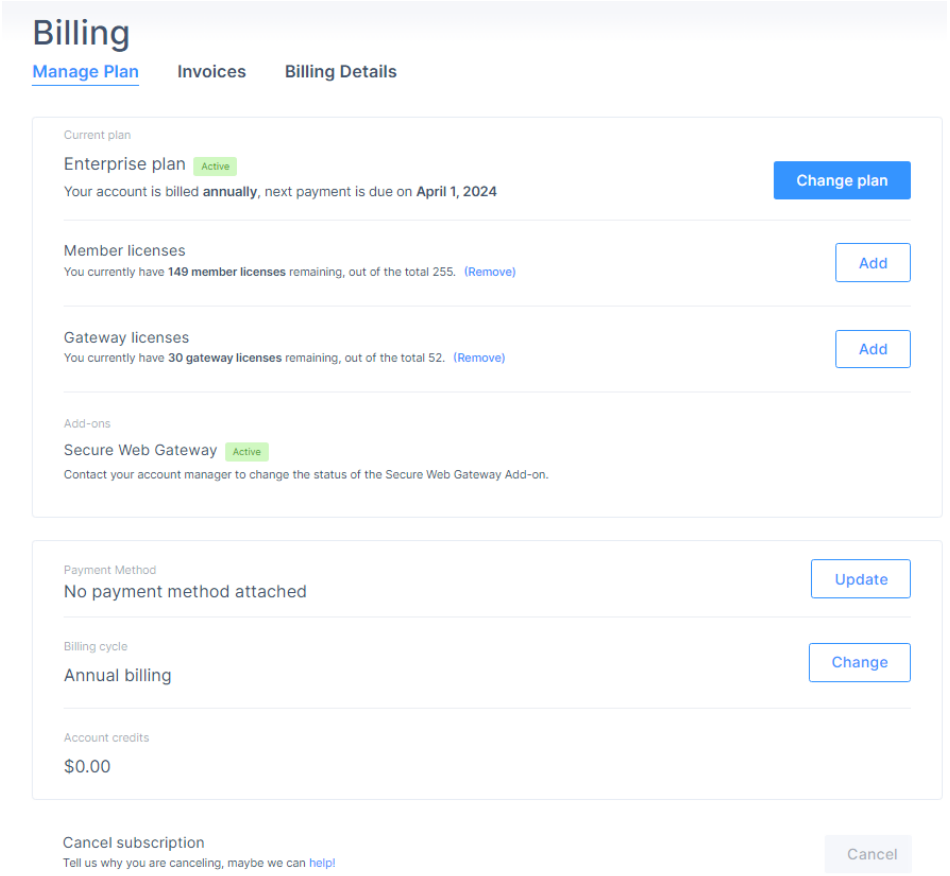
**Billing** allows you to manage your billing plan, pay invoices and update billing details.

To view **Billing**:

1. Access the Harmony SASE Administrator Portal.
2. In the top-right corner, click the username and then click **Billing**.




The **Billing** page appears. The **Manage Plan** tab is displayed by default.




# Manage Plan

The **Manage Plan** tab allows you to manage your billing plan.

- Update your Subscription Plan
- Modify Member Licenses
- Modify Gateway / Application Licenses
- Add a payment method
- Cancel subscription

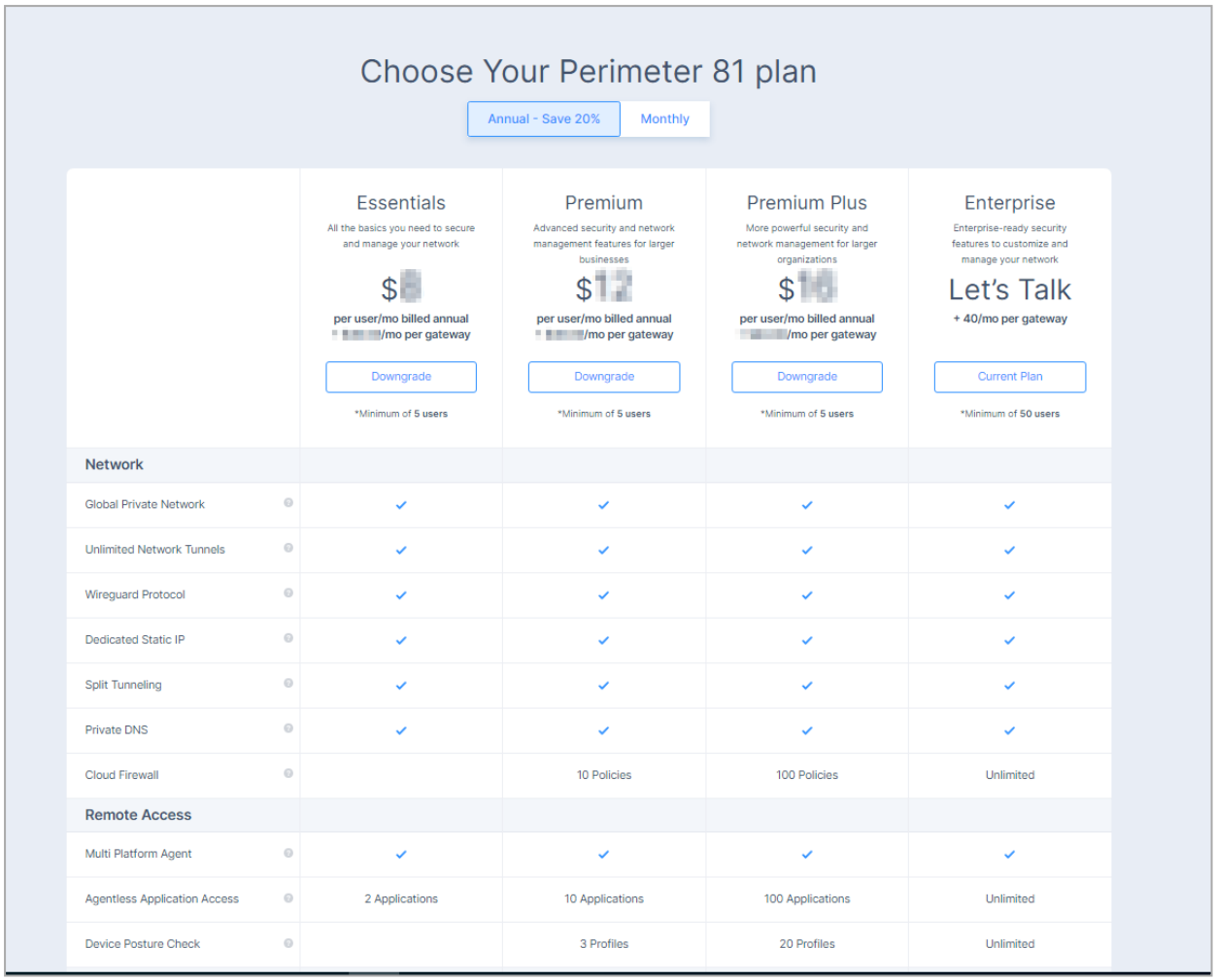
## Updating the Subscription Plan

1. In the **Current plan** section, click **Change plan**.




The system displays the available plans.

**Note** - Default is the **Essentials** Plan.

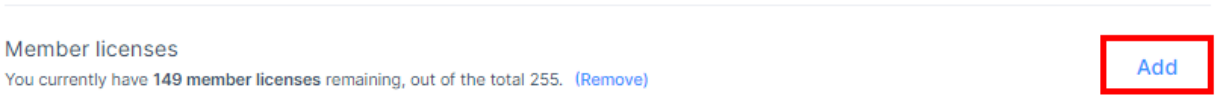



2. Select your billing cycle:
   - Annual
   - Monthly

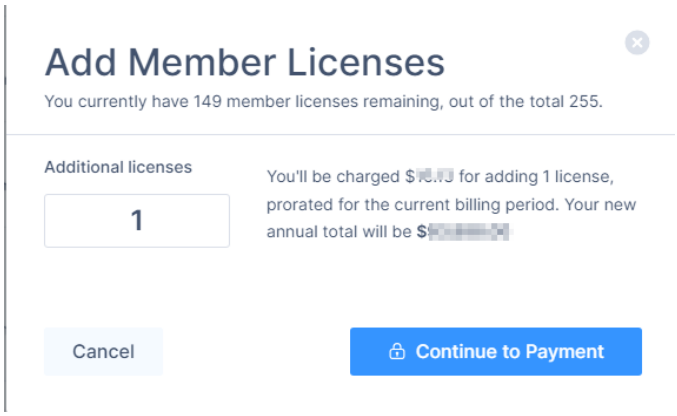
   **Note** - The billing cycle starts at the beginning of the month. If you purchase a subscription mid-month, you are charged a prorated amount.
     - Monthly billing - You are charged the full subscription amount on the 1st of the following month. For example, you purchased on 15 April, you are charged $5 on the same day, then $10 on 1 May and every following month.
     - Annual billing - You are charged the full subscription amount on the 1st of the purchased month. For example, you purchased on 15 April, you are charged $92 on the same day, then $100 on 1 April next year.
3. Select the plan you want to upgrade to.

# Modifying Member Licenses

1. In the **Member licenses** section, click **Add**.

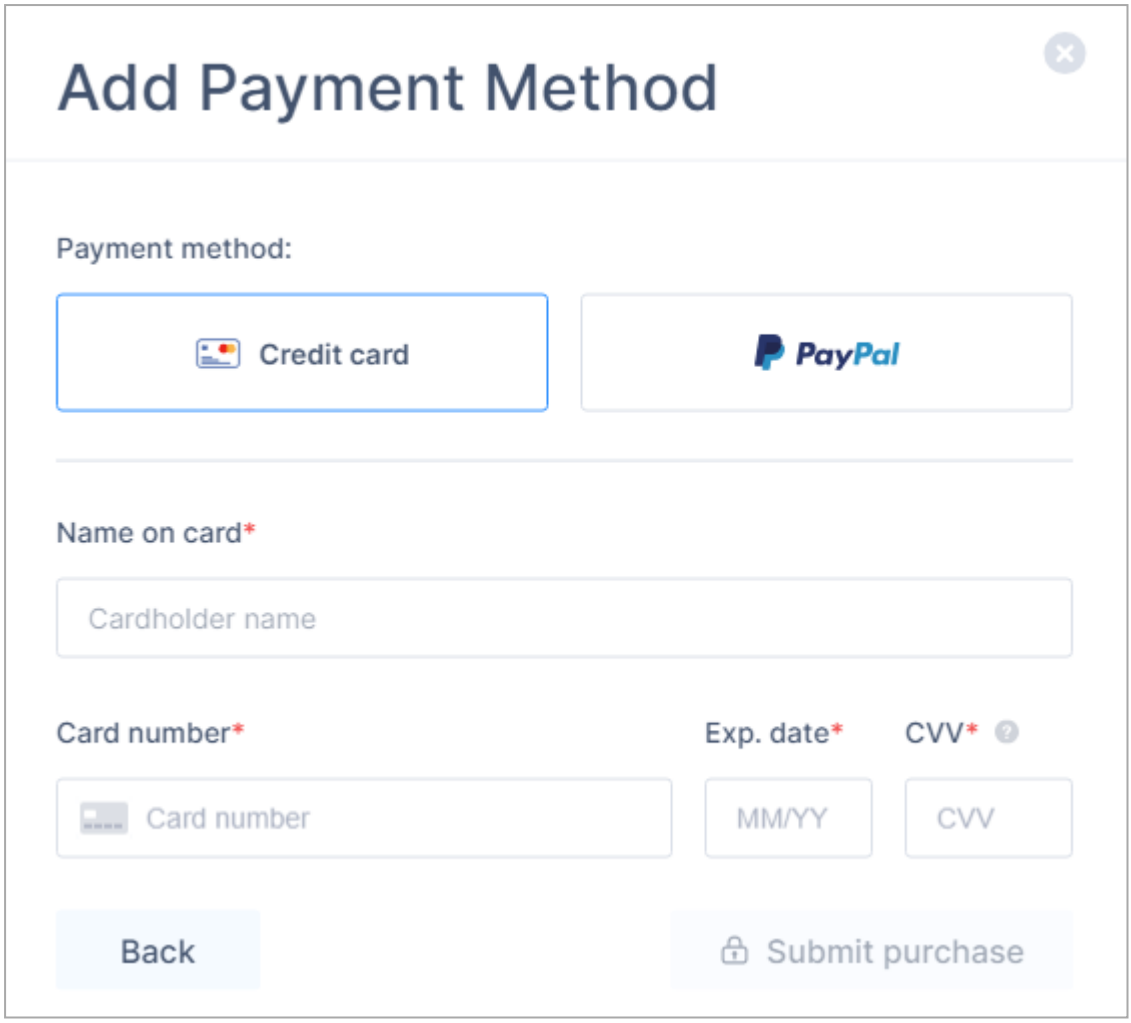



   The **Add Member Licenses** window appears.




2. In the **Additional licenses** field, enter the number of member licenses.
3. Click **Continue to Payment**.

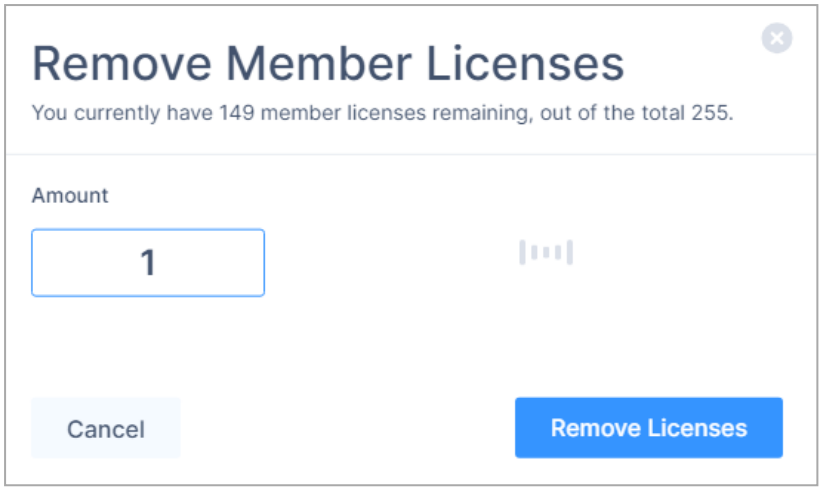
   The **Add Payment Method** window appears.




4. Select the payment method and enter the details.
5. Click **Submit purchase**.
6. To remove a member license, in the **Member licenses** section, click **Remove**.



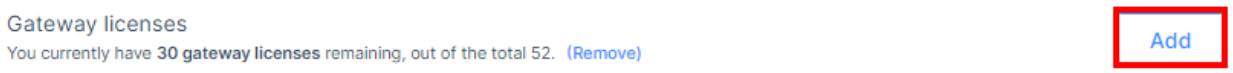

The **Remove Member Licenses** window appears.



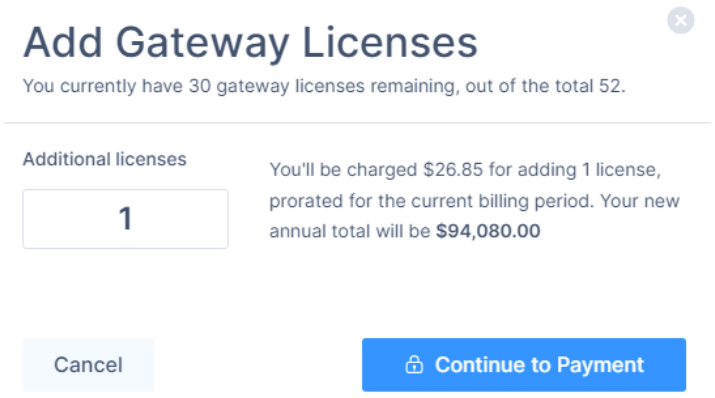

7. Enter the number of licenses to remove and click **Remove Licenses**.

# Modifying Gateway / Application Licenses

1. To add a Gateway license, in the **Gateway licenses** section, click **Add**.

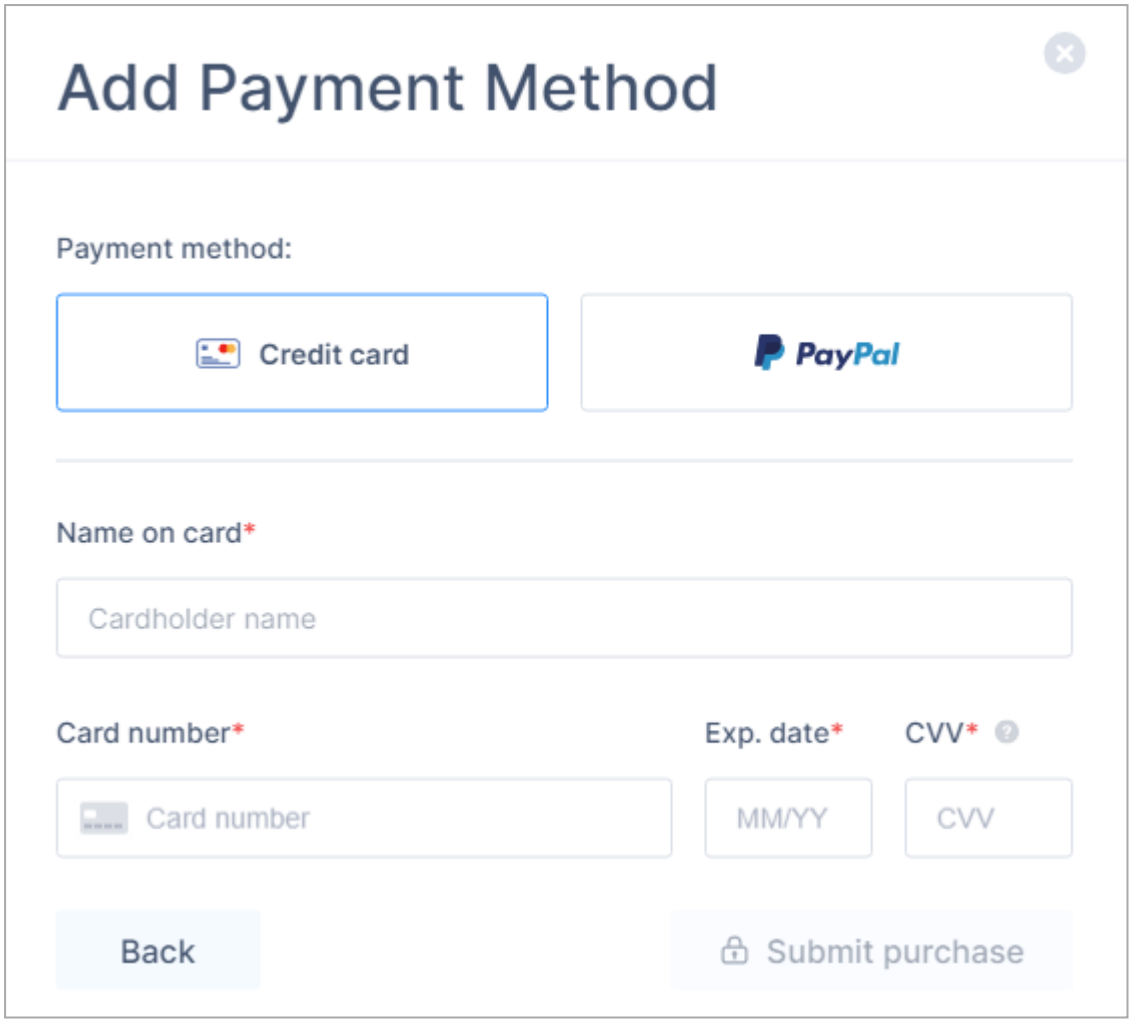



The **Add Gateway Licenses** window appears.




2. In the **Additional licenses** field, enter the number of gateway licenses.
3. Click **Continue to Payment**.

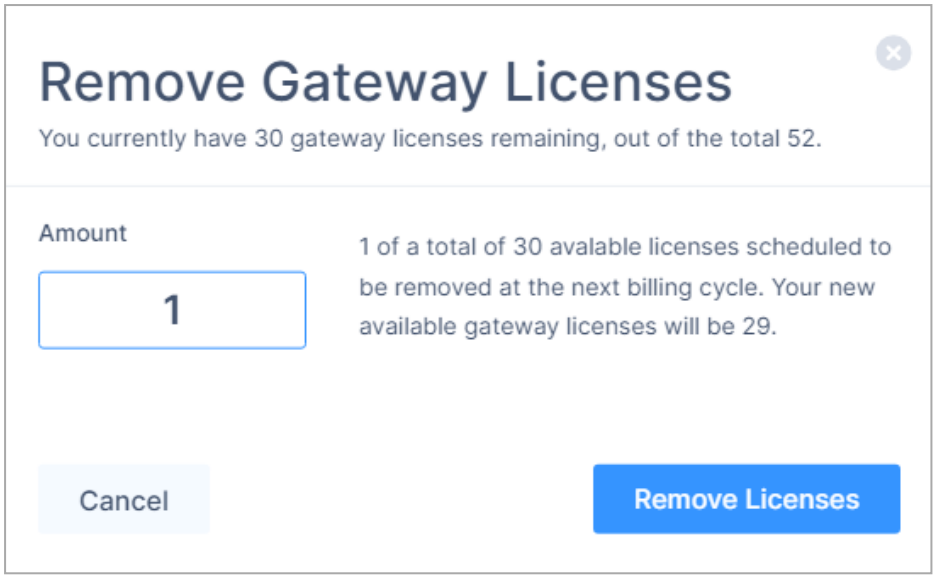
   The **Add Payment Method** window appears.




4. Select the payment method and enter the details.
5. Click **Submit purchase**.
6. To remove a Gateway license, in the **Gateway licenses** section, click **Remove**.




The **Remove Gateway Licenses** window appears.



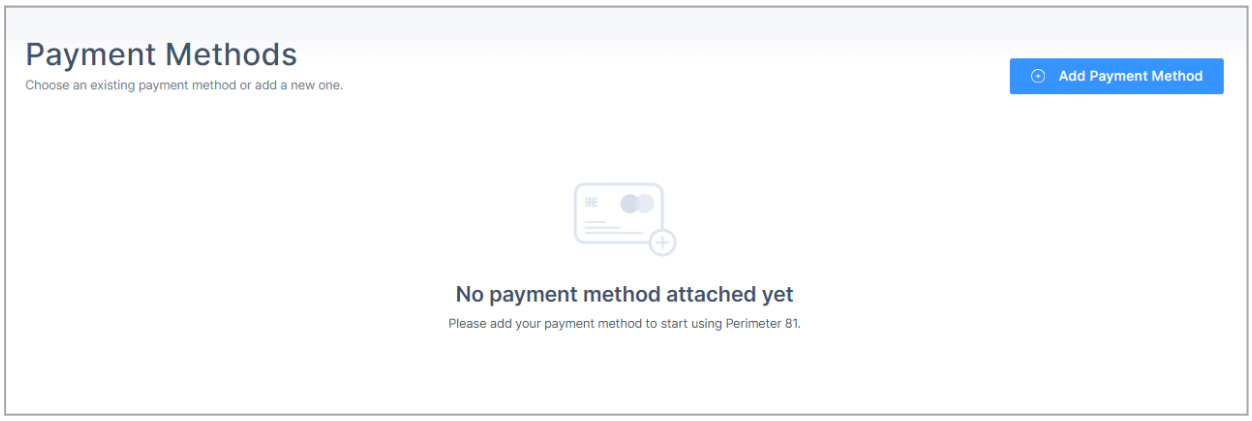

7. Enter the number of licenses to remove and click **Remove Licenses**.

# Adding a Payment Method

1. In the **Payment Method** section, click **Update**.

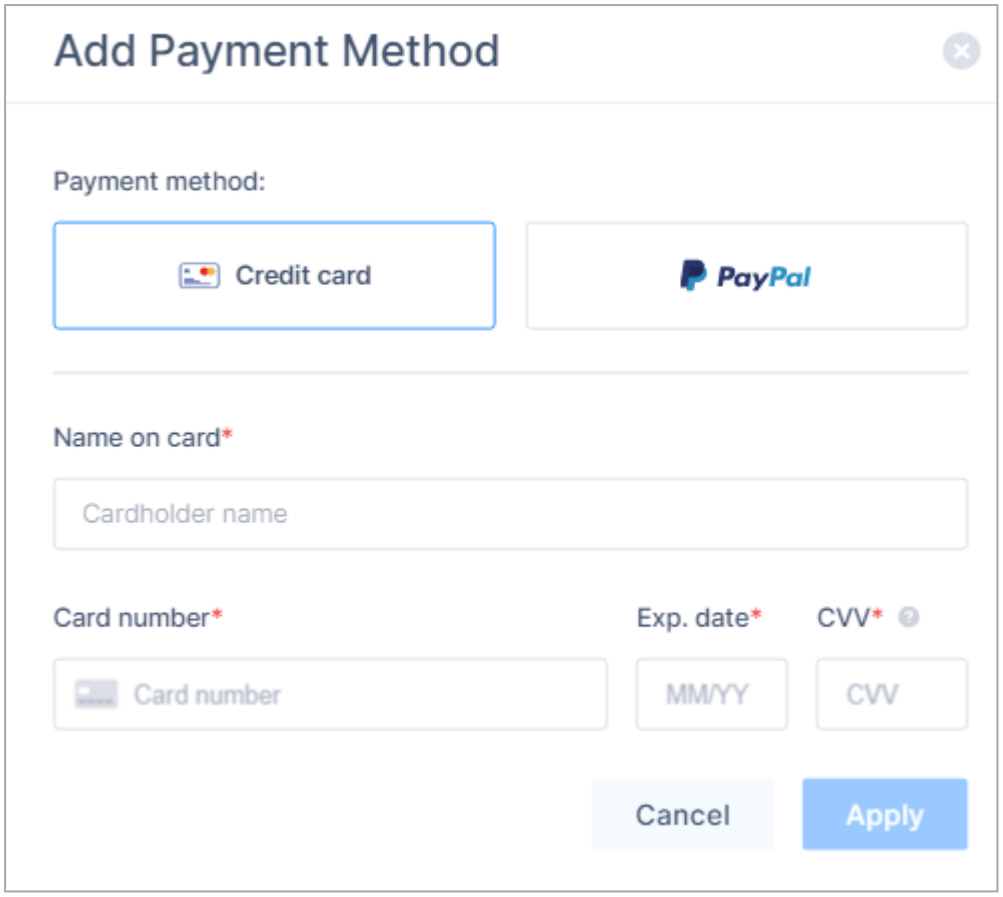



The **Payment Methods** page appears.




2. Click **Add Payment Method**.

The **Add Payment Method** window appears.




3. Select the payment method and enter the details.
4. Click **Apply**.

   After the payment method is added, you receive a confirmation email.

# Cancelling Subscription

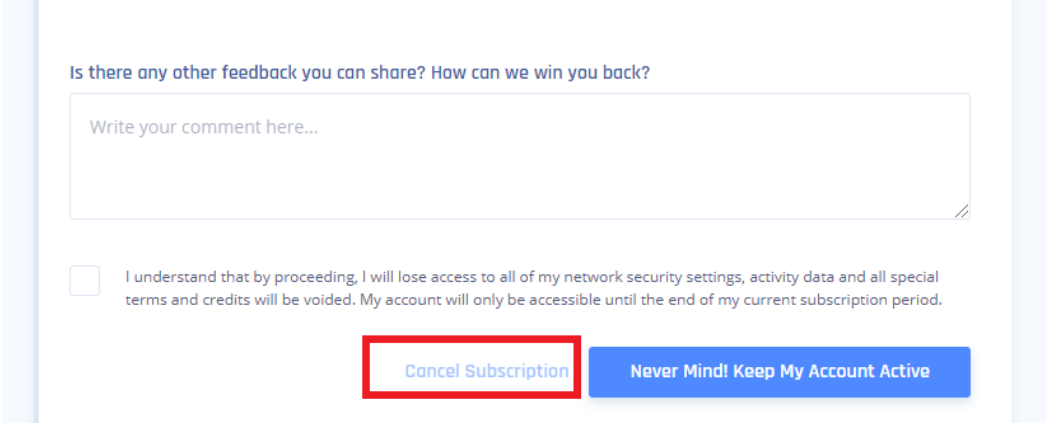
**Notes -**

- If you cancel the subscription within 30 days of activating your account, you get a full refund.
- After you cancel your subscription, your account is accessible only till the end of the current subscription period.

1. To cancel your account subscription, in the **Cancel subscription** section, click **Cancel**.



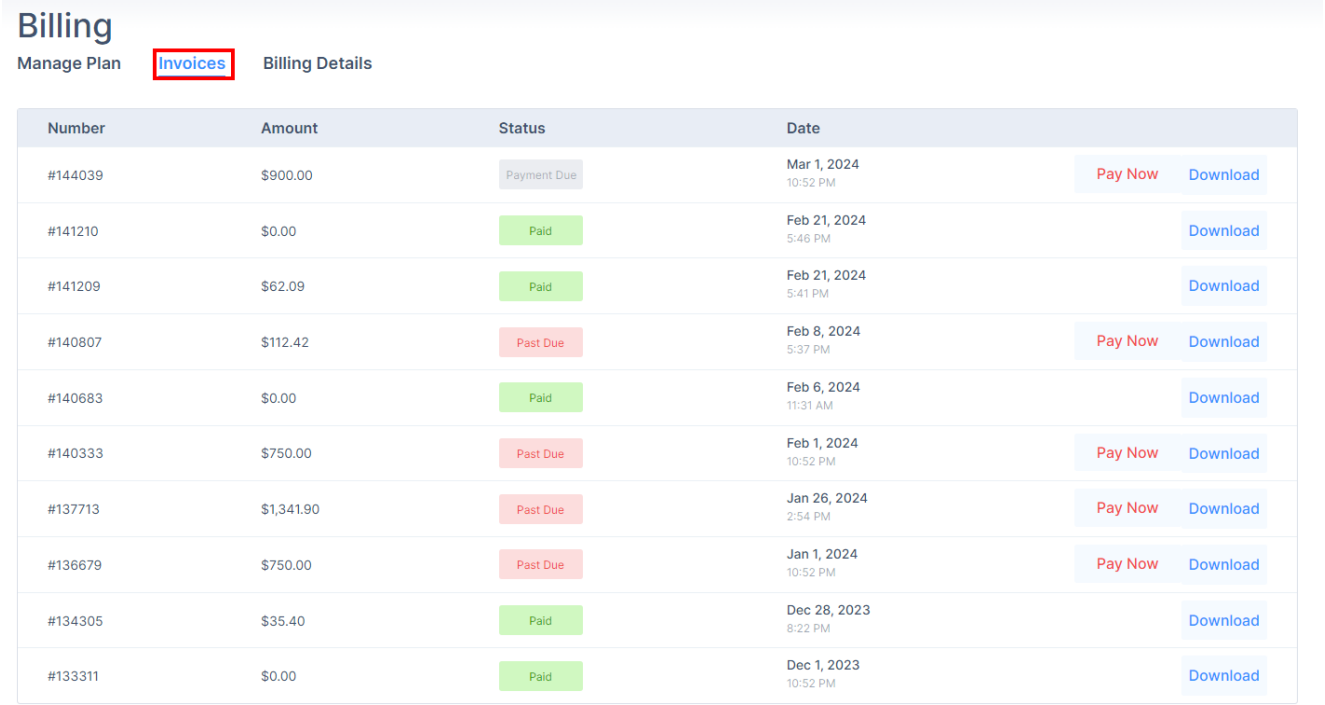
2. Enter a feedback (optional), select the checkbox and then click **Cancel Subscription**.




# Invoices

The **Invoices** tab allows you to pay and download your invoices.

To view **Invoices**, access the **Billing** page and click the **Invoices** tab.




To pay an invoice, click **Pay Now**.

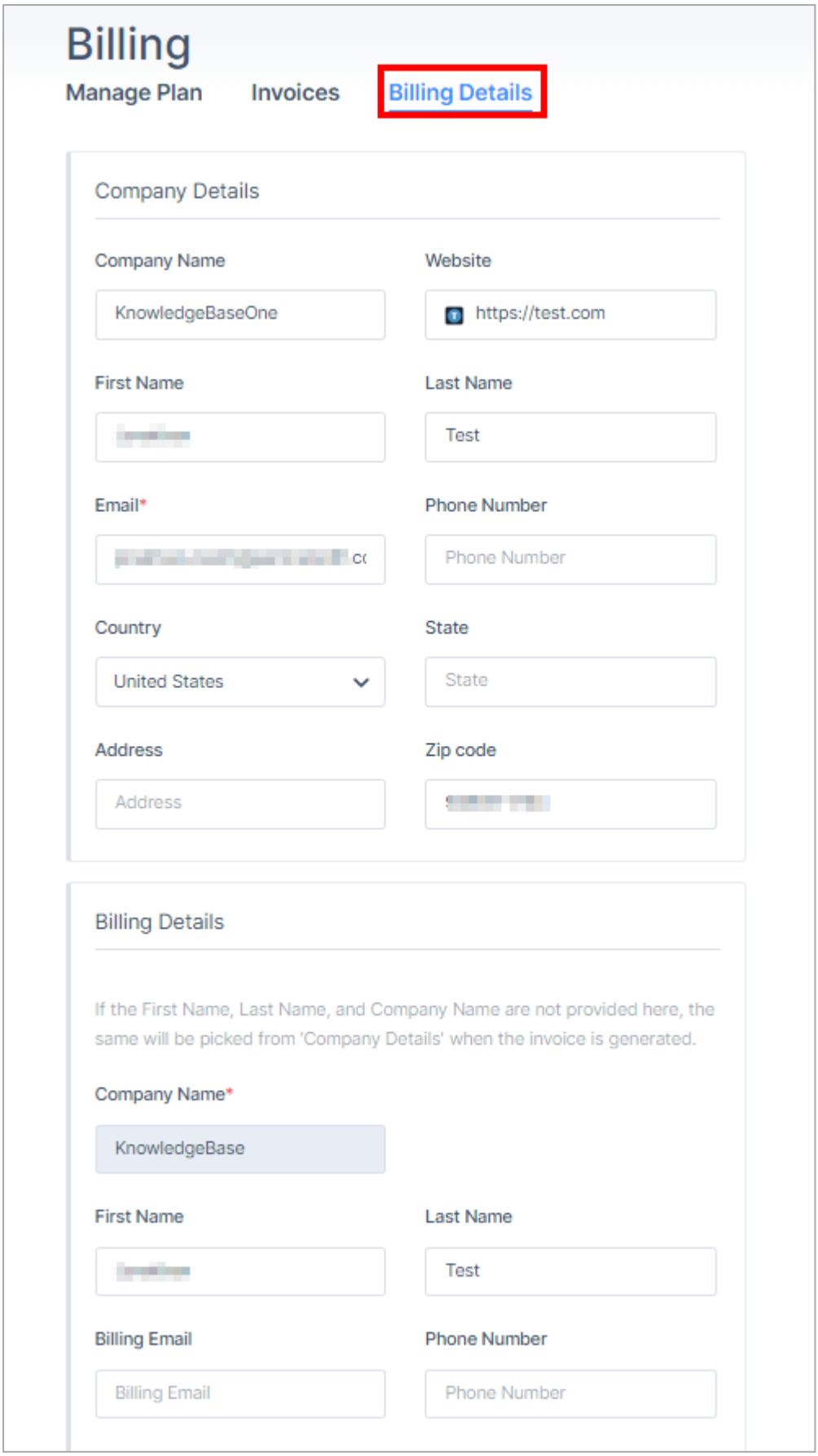
To download an invoice, click **Download**.

The system download the invoice in PDF format.

# Billing Details

The **Billing Details** tab allows you to update the billing information for your organization.

To view **Billing Details**, access the **Billing** page and click the **Billing Details** tab.



To update the billing details, enter the required changes and click **Save**.

# Dashboard

The **Dashboard** page shows statistical data on:


- *"Active Sessions" below*
- *"Member Licenses" on the next page*
- *"Gateway Licenses" on the next page*
- *"Applications" on page 51*
- *"Active Agent Users" on page 51*
- *"Users Bandwidth" on page 52*
- *"OS Distribution" on page 52*
- *"Device Type Distribution" on page 52*
- *"Agent Version by OS" on page 53*


To view the **Dashboard** page, access **Harmony SASE** and click **Dashboard**.

# Active Sessions



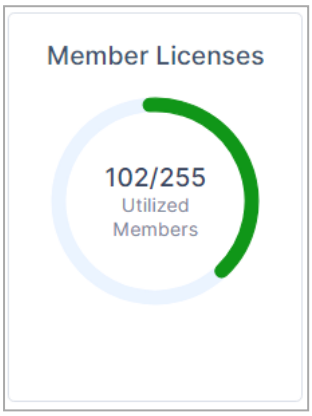

The **Active Sessions** widget shows:

- **Agent Sessions**: The number of users connected to a network through the Harmony SASE Agent.
- **App Sessions**: The number of users accessing the Zero Trust Applications.
- **Total Sessions**: Total number of Agent and Application sessions.

For example, if a member is connected to a network through the Harmony SASE Agent, and is accessing two Zero Trust Applications, then the **Active Sessions** widget shows three active sessions, one **Agent Session** and two **App Sessions**.

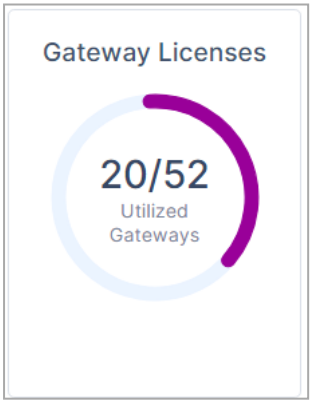
To view the detailed information, click **Expand**. The system redirects to the *"Active Sessions" on page 223* page.

# Member Licenses



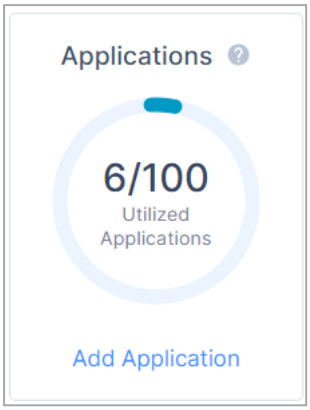

The **Member Licenses** widget shows the number of member licenses utilized out of the purchased licenses.

# Gateway Licenses




The **Gateway Licenses** widget shows the number of gateway licenses utilized out of the purchased licenses.

# Applications




The **Applications** widget shows the number of applications accessed out of the applications created by you.

To add an application, click **Add Application**. For more information, see *"Applications" on page 164*.

# Active Agent Users

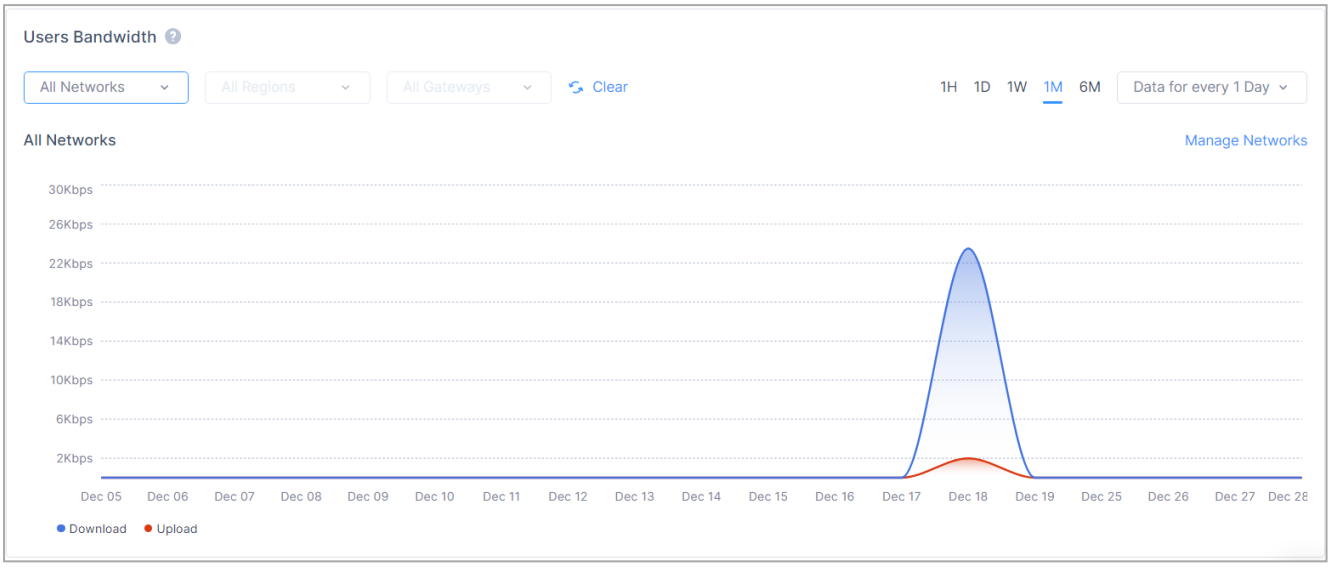



The **Active Agent Users** widget shows the live and historical data of members connected to a network through the Harmony SASE Agent.

You can filter the data by **Network**, **Region**, **Gateway**, time frame and scale.

For a network and region, you can compare the data for up to three gateways.

# Users Bandwidth

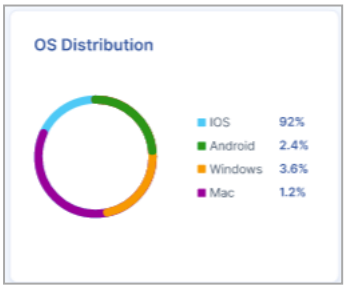



The **Users Bandwidth** widget shows the live and historical bandwidth used (upload and download) by members connected to the Harmony SASE Agent.

You can filter the data by **Network**, **Region**, **Gateway**, time frame and scale.

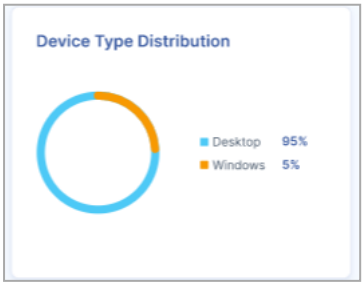
For a network and region, you can compare the data for up to three gateways.

# OS Distribution



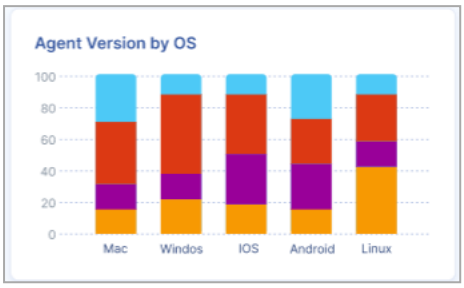

The **OS Distribution** widget shows the distribution of devices by operating systems.

# Device Type Distribution



The **Device Type** widget shows the distribution of devices by type.

# Agent Version by OS




The **Agent Version by OS** widget shows the distribution of Harmony SASE Agent across different operating systems.

# Team

The **Team** page allows you to manage:

- *"Members" on page 55*
- *"Groups" on page 63*
- *"User Configuration Profiles" on page 65*

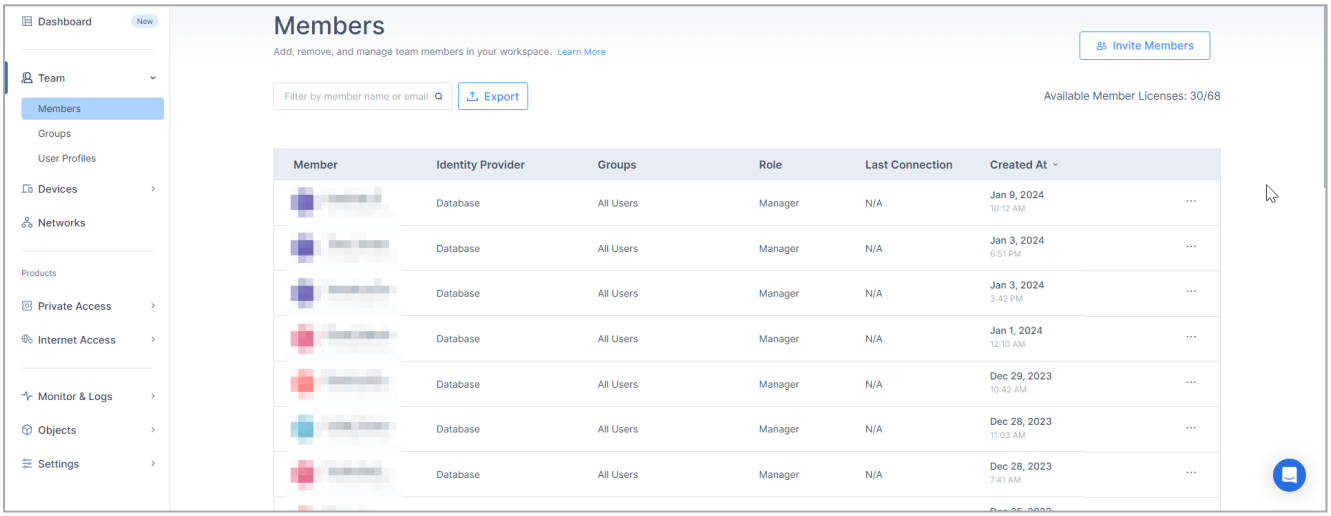
# Members

Members are either administrators that manage the Harmony SASE Administrator Portal or end-users that you want to provide safe private and internet access.

The **Members** page allows you to:

- Invite members
- Manage members
- Add licenses

To view the **Members** page, access **Harmony SASE** and click **Team** > **Members**.




| Column | Description |
|---|---|
| Member | Full name and email address of the member. |
| Identity Provider | Configured Identity Providers (IdP) for the member.<br>**Database** means that the member is invited from the Harmony SASE Administrator Portal. See *"Invite Members" on page 57*. |

| Column | Description |
|---|---|
| Role | Role of the member:<br>■ **Admin** - Full privileges and permissions.<br>■ **Billing** - Manage billing information, view invoice, licenses, and payments.<br>■ **Manager** - Manage networks, applications, members, groups, and monitor activity.<br>■ **User** - End-user that you want to provide safe private and internet access.<br>For permissions associated with each role, see *"Member Roles and Permissions" below*. |
| Groups | Group(s) to which the member is assigned. |
| Last Login | Date and time of the last connected session. |
| Created At | Date and time when the member was created. |

# Member Roles and Permissions

| Role | Permissions | | | | | |
|---|---|---|---|---|---|---|
| | Manage Licenses | Manage Members | Manage Network | Manage Configuration | View Activities | Manage Billing |
| Admin | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Manager | – | ✓ | ✓ | ✓ | ✓ | – |
| Billing | ✓ | – | – | – | – | ✓ |
| User | – | – | – | – | – | – |

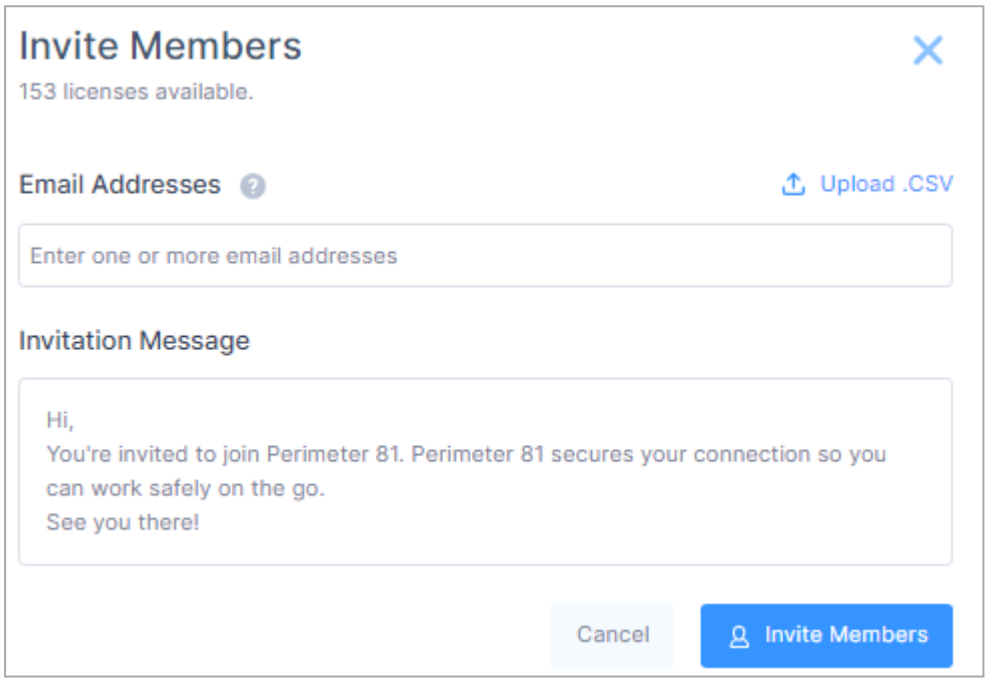
# Invite Members

You can invite members either manually or using an Identity Provider (IdP).

## Inviting Members Manually

1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click **Inviting Members**.

   The **Invite Members** window appears.




3. In the **Email Addresses** field, specify the email address of the member.
   - To invite multiple members, enter the email addresses separated by a comma or space.
   - If you have a CSV file with a list of email addresses (maximum 100), click **Upload.CSV** and upload the file.
4. (Optional) In the **Invitation Message** field, edit the email message.
5. Click **Invite Members**.

   The system sends an email to members with a link to accept the invite and download the Harmony SASE Agent. The invitation is valid for 30 days. If the invitation expires, you must resend the invitation. For more information, see *"Managing Members" on page 58*.

## Inviting Members Using an Identity Provider

See *"Identity Providers" on page 278*.

# Managing Members

1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click the ··· icon in the last column for the member.
3. To resend the invitation to members that did not accept the invitation within the validity period, click **Resend Invite**.
4. To reset the password, click **Reset Password** and in the confirmation pop-up that appears, click **Reset Password**.
5. To manage the devices of the user, click **Manage Devices**. The system redirects to the **Device Inventory** page. For more information, see *"Device Inventory" on page 73*.
6. To view the activity of a member, click the icon. The system redirects to the **Member Activity** page. See *"Member Activity" on page 224*.
7. To delete a member, click the icon and in the confirmation pop-up that appears, click **Delete Member**.

## Changing Member Role

1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click the ··· icon in the last column for the member.
3. Click **Change role** and select the role.
4. Click **Apply Role**.

## Unblocking Members

Harmony SASE blocks members if there are multiple failed login attempts into the Harmony SASE Agent. Blocked members are greyed-out with a lock icon.

**To unblock the members:**

1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click the ··· icon in the last column for the member.
3. Click **Unblock User** and in the confirmation pop-up that appears, click **Unblock User**.

## Generating Sign-Out Code

You can prevent members from unauthorized sign-out of the Harmony SASE Agent. The sign-out is authorized only after the member enters a sign-out code generated by you.

**To generate the sign-out code:**

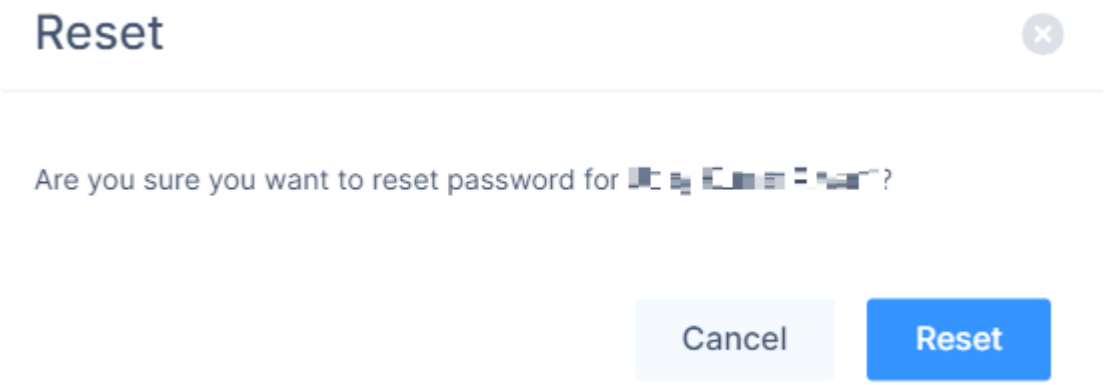
1. Access the Harmony SASE Administrator Portal.
2. Make sure *"Disable Sign-Out" on page 66* is enabled for the member or group.
3. Go to **Team** > **Members**.
4. Click the ··· icon in the last column for the member.
5. Click **Generate Sign-Out Code**.

   A pop-up appears with the sign-out code.
6. Copy the code and share it with the member.

## Resetting a Member Password

1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click the ··· icon in the last column of the member.
3. Click **Reset**.

   The **Reset** prompt appears.




4. Click **Reset**.

## Resetting Google Authenticator Two-Factor Authentication for a Member

When a member changes his device that has Google Authenticator used for Two-Factor Authentication, they must reconfigure it on the new device. To do that, the administrator must reset their Two-Factor Authentication.

**To reset Two-Factor Authentication for a member:**

1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click the ⋯ icon in the last column for the member.
3. Select **Reset Database 2FA**.
4. Click **Reset** in the confirmation pop-up that appears.

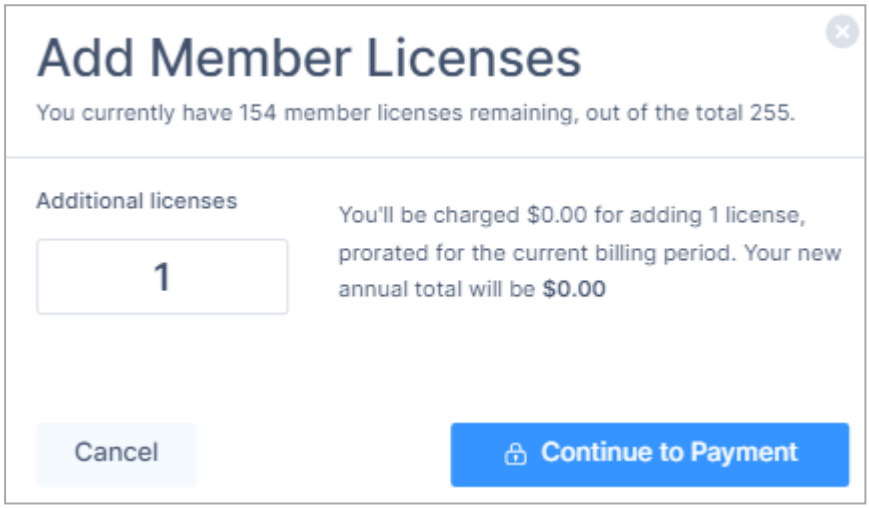
   The member receives a confirmation email for the Two-Factor Authentication reset and a link to re-activate it.

# Adding Licenses

**Note** - This option is available only for the Perimeter 81 workspace accounts.

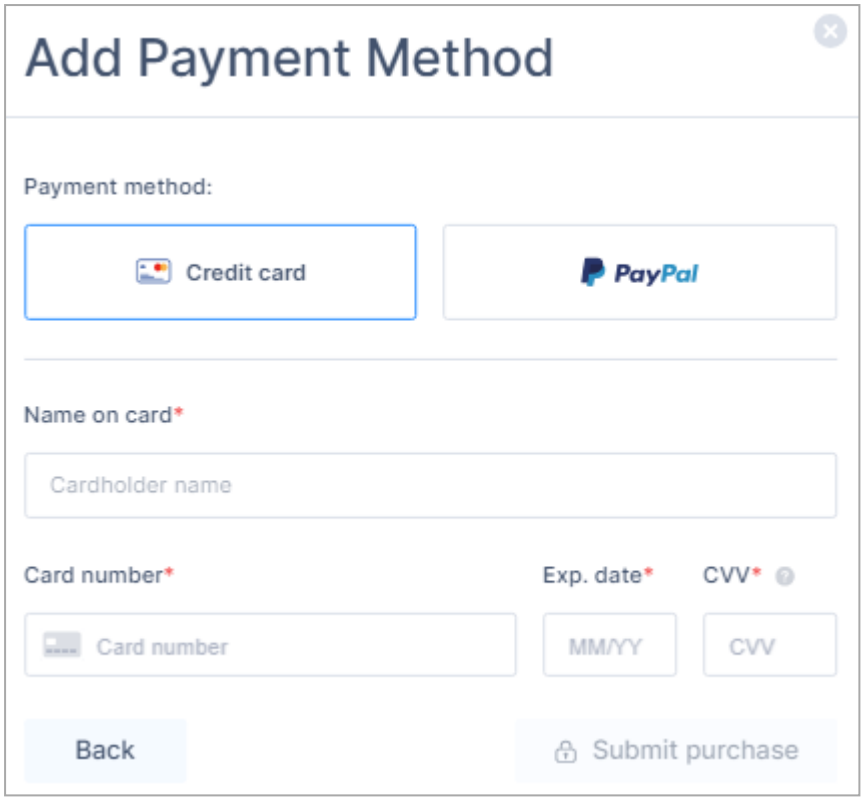
1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click **Add Licenses**.

   The **Add Member Licenses** window appears.
3. In the **Additional licenses** field, enter the number of licenses you want to add.




4. Click **Continue to Payment**.

   The **Add Payment Method** window appears.



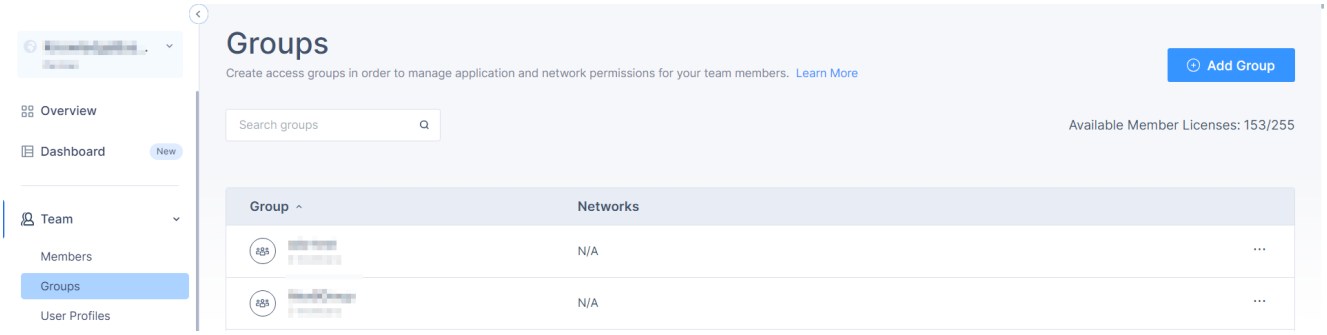

5. Enter the payment details and click **Submit purchase**.

# Groups

The **Groups** page allows you to create groups of members, for example, based on roles and locations. It allows you to apply *"Web Filter Rules" on page 195* to multiple members and restrict access only to a segment of the network.

**Note** - Segmenting networks uses the Software Defined Perimeter (SDP) technology. This isolates sensitive data and reduces the attack surface, minimizing the impact during security breaches.

To view the **Groups** page, access the Harmony SASE Administrator Portal and click **Team** > **Groups**.




| Column | Description |
|---|---|
| Group | Group name. |
| Networks | Name of the networks assigned to the group. |

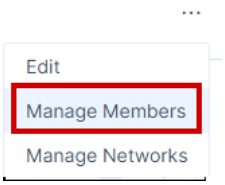
## Creating a Group

1. Access the Harmony SASE Administrator Portal and click **Team** > **Groups**.
2. Click **Add Group**.

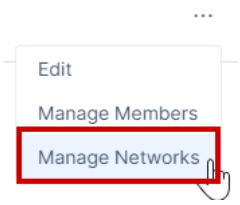
   The **Create new group** window appears.




3. Enter the group name and click **Create Group**.
4. To add members to the group:
   a. Click the ··· icon in the last column of the group and then select **Manage Members**.




   b. In the **Assign new members** section, click **+** and select the required members.
5. To add networks to a group or to grant access to a network segment:
   a. Click the ··· icon in the last column of the group and then select **Manage Networks**.




   The **Assign Network to Group** pop-up appears.
   b. Select the network and click **Done**.

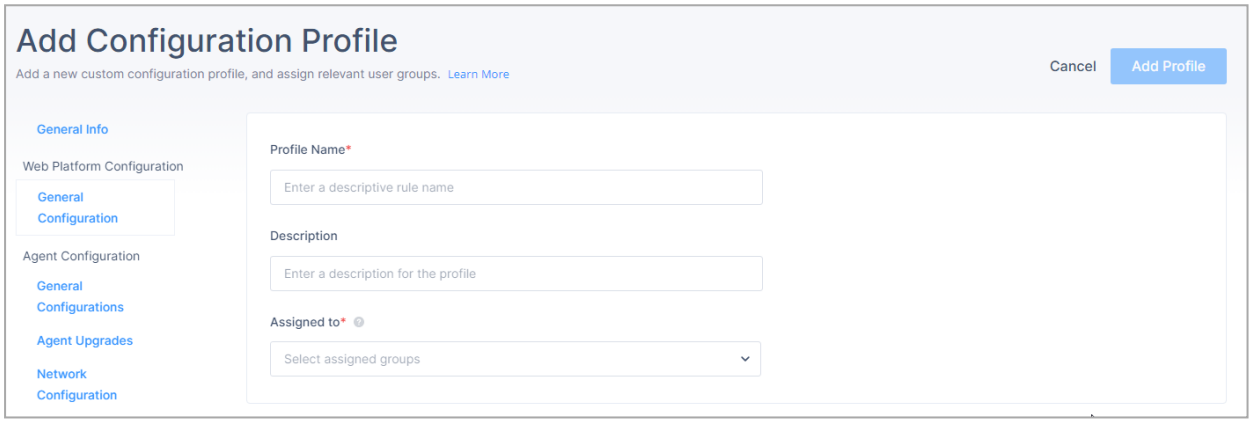
   The members can access only the selected networks from the Harmony SASE Agent.

# User Configuration Profiles

**User Configuration Profiles** allows you to create profiles with custom settings and apply them to member groups and devices.

## Adding a Configuration Profile

1. Access the Harmony SASE Administrator Portal and click **Team** > **User Profiles**.
2. Click **Add Configuration Profile**.
3. In the **Profile Name** field, enter a name for the profile.



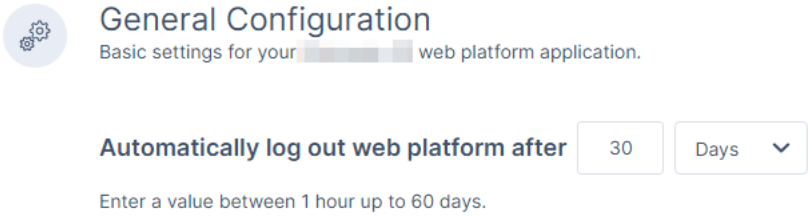

4. (Optional) In the **Description** field, enter a description for the profile.
5. In the **Assigned to** field, select the member groups.
6. Configure *"Web Platform Configuration" below* and *"Agent Configuration" on the next page*.
7. Click **Add Profile**.

The order of the profile indicates its priority. For example, Profile #1 has higher priority than Profile #2.

## Web Platform Configuration

The **Web Platform Configuration** settings allows the administrators to configure settings for the Harmony SASE Administrator Portal.

### General Configuration




In the **Automatically log out web platform after** field, enter the duration after which the system automatically logs out the member from the Harmony SASE Administrator Portal. The supported duration is one hour to 60 days.

## Agent Configuration

The **Agent Configuration** settings allows the administrators to configure settings for the Harmony SASE Agent.

### General Configuration

From the **General Configuration** section of the **Agent Configuration**, you can configure the basic settings for your Harmony SASE Agent.

| Setting | Description |
|---|---|
| Disable Sign-Out | Prevents members from signing out of the Harmony SASE Agent without the sign-out code.<br>The administrator must generate the sign-out code and share it with the member to successfully sign-out from the Harmony SASE Agent. See *"Generating Sign-Out Code" on page 58*. |
| Automatically Log Out Agent After | Logs out the member from the Harmony SASE Agent automatically after the specified duration. The supported duration is one hour to 180 days. |
| [DEPRECATED] Shared Network | Allows members to connect to shared Harmony SASE gateways. This enhances speed and performance if the member's physical location is far from your private gateway location.<br>For more information about shared networks, see *" [DEPRECATED] Shared Gateways " on page 109*. |

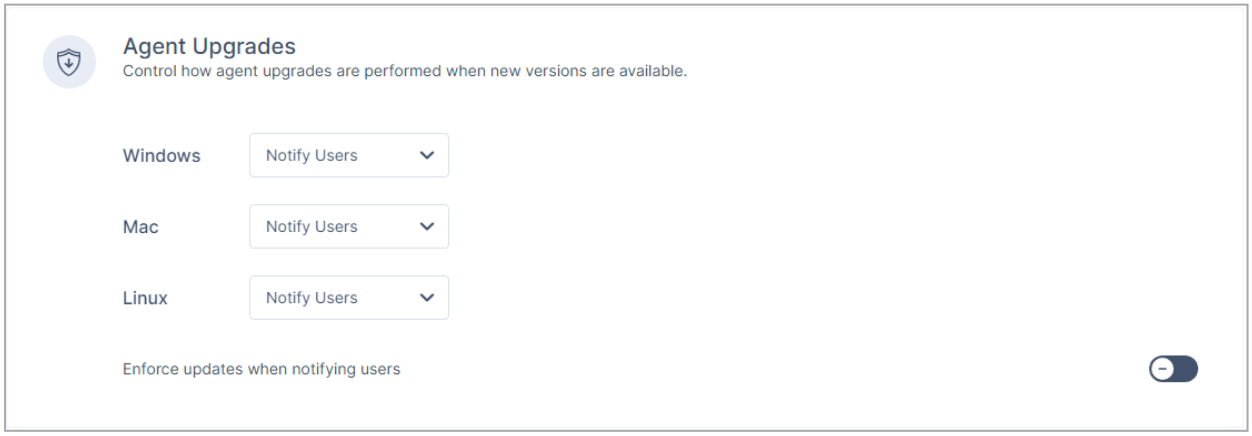
| Setting | Description |
|---|---|
| Connect on Launch | Automatically starts the Harmony SASE Agent when the device starts and connects to the most recent network location.<br>**Notes**:<br>▪ This setting applies only to Windows and macOS devices.<br>▪ The member can modify this setting from their device. |
| Connect / Disconnect Notification | Shows a pop-up notification on the device when the Harmony SASE Agent connection status changes.<br>**Notes**:<br>▪ This setting applies only to Windows and macOS devices.<br>▪ The member can modify this setting from their device. |
| Snowplow Report | Allows you to send the Snowplow (user tracking) data to Harmony SASE. |

## Agent Upgrades

**Agent Upgrades** allows you to control how to perform Harmony SASE Agent upgrades when new versions are released.

**To control how to perform Harmony SASE Agent upgrade:**

1. Go to **Team** > **User Profiles**.
2. Open a user profile with the required group of members or create a new user profile. See *"Adding a Configuration Profile" on page 65*.
3. Scroll-down to the **Agent Upgrades** section.




4. Select the option required for **Windows**, **Mac**, and **Linux**.

- **Automatic Silent**: Automatically upgrades the Harmony SASE Agent when new version is available.
- **Notify Users**: Notifies the user about the new version.
- **Disabled**: Does not upgrade the Harmony SASE Agent.

5. To automatically upgrade the Harmony SASE Agent while notifying the member, turn on the **Enforce updates when notifying users** toggle button.
6. Click **Apply**.

## Network Configuration

**Network Configuration** allows you to configure the network settings for your Harmony SASE Agent.

| Feature | Description |
|---|---|
| Automatic VPN Connection [1] | Automatically connects to the VPN when an internet connection is available. |
| Always-On VPN | Automatically connects to the VPN when an internet connection is available. |
| Kill Switch [1] | Automatically disconnects internet connection when the VPN disconnects. |
| Trusted Routers (Always-On Exceptions) [1, 2] | Bypasses Harmony SASE VPN if you have a trusted router and connects directly to your network.<br><br>**To add trusted routers:**<br>1. Click **Add Trusted Router**.<br>2. In the **Name** field, enter the router name.<br>3. In the **Router MAC Address** field, enter the router MAC address.<br>4. Click **Add**.<br>5. To add multiple routers, repeat steps 1 to 4.<br>6. Click **Apply**. |
| Automatic Wi-Fi Security [1] | The Harmony SASE Agent automatically connects to Harmony SASE VPN if the device connects to an unsecured Wi-Fi. |

| Feature | Description |
|---|---|
| Trusted Wireless Networks (Automatic Wi-Fi Security Exceptions) [2] | Harmony SASE Agent does not enable **Automatic Wi-Fi Security** if the device connects to a trusted Wi-Fi network.<br><br>**To add trusted Wi-Fi network:**<br>1. Click **Add Wi-Fi Network**.<br>2. In the **Name** field, enter the SSID of the network.<br>3. Click **Add**.<br>4. To add multiple trusted Wi-Fi networks, repeat steps 1 to 3.<br>5. Click **Apply**. |

[1] The member can modify this setting on their device.

[2] This setting applies only to Windows and macOS devices.

## Windows

Allows you to define the settings for Windows devices running the Harmony SASE Agent.

**To configure the default protocol:**

1. Click the drop down next to **Default Protocol**.
2. Select the protocol:
   - **WireGuard**
   - **OpenVPN**
3. Click **Apply**.

### Use VPN Interface DNS

Sets the device DNS server as the Harmony SASE server. The agent uses this DNS server for DNS requests specified on the VPN network interface.

If this is disabled, then the DNS resolver is set to the DNS used by your local adapter. This is useful if you use other DNS providers.

**Note** - The member can modify this setting on their device.

### Notify Reconnect

The Harmony SASE Agent automatically notifies upon reconnecting with the network.

**Note** - The member can modify this setting on their device.

## Android / Chromebook

From the **Android / Chromebook** settings, the administrators can control the settings for the Harmony SASE Agent running on Android or Chromebook devices.

### Default Protocol

**To configure the default protocol:**

1. Click the drop down next to **Default Protocol**.
2. Select the protocol:
   - **WireGuard**
   - **OpenVPN**
3. Click **Apply**.

## Mac

From the **Mac** settings, the administrators can control the settings for the Harmony SASE Agent running on macOS.

**To configure the default protocol:**

1. Click the drop down next to **Default Protocol**.
2. Select the protocol:
   - **WireGuard**
   - **OpenVPN**
3. Click **Apply**.

### Use VPN Interface DNS

Sets the device DNS server as the Harmony SASE server. The agent uses this DNS server for DNS requests specified on the VPN network interface.

If this is disabled, then the DNS resolver is set to the DNS used by your local adapter. This is useful if you use other DNS providers.

**Note** - The member can modify this setting on their device.

# iOS

From the **iOS** settings, the administrators can control the settings for the Harmony SASE Agent running on iOS devices.

### Auto Reconnect

Automatically reconnects all the iOS agents to the VPN if the session disconnects or the device connects to Wi-Fi or 3G networks that do not require login credentials.

**Note** - The member can modify this setting on their device.

# Devices

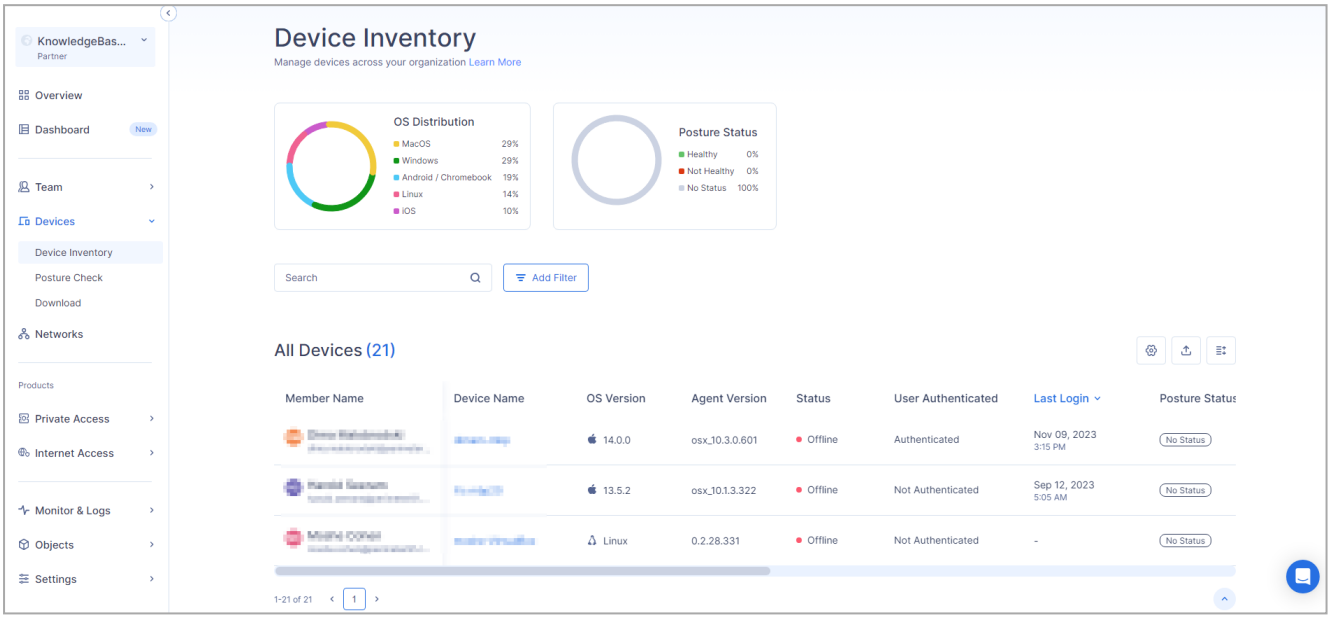
In the **Devices** page, you can:

- View inventory details about your devices
- Configure device posture check profiles
- Download the Harmony SASE Agent

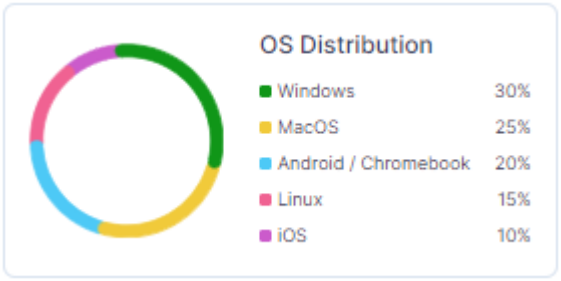
# Device Inventory

The **Device Inventory** page provides inventory details about your devices.

To view the **Devices** page, access **Harmony SASE** and click **Devices** > **Device Inventory**.

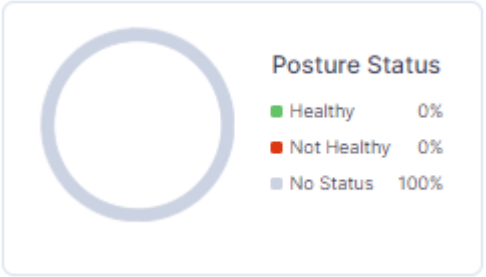



## OS Distribution



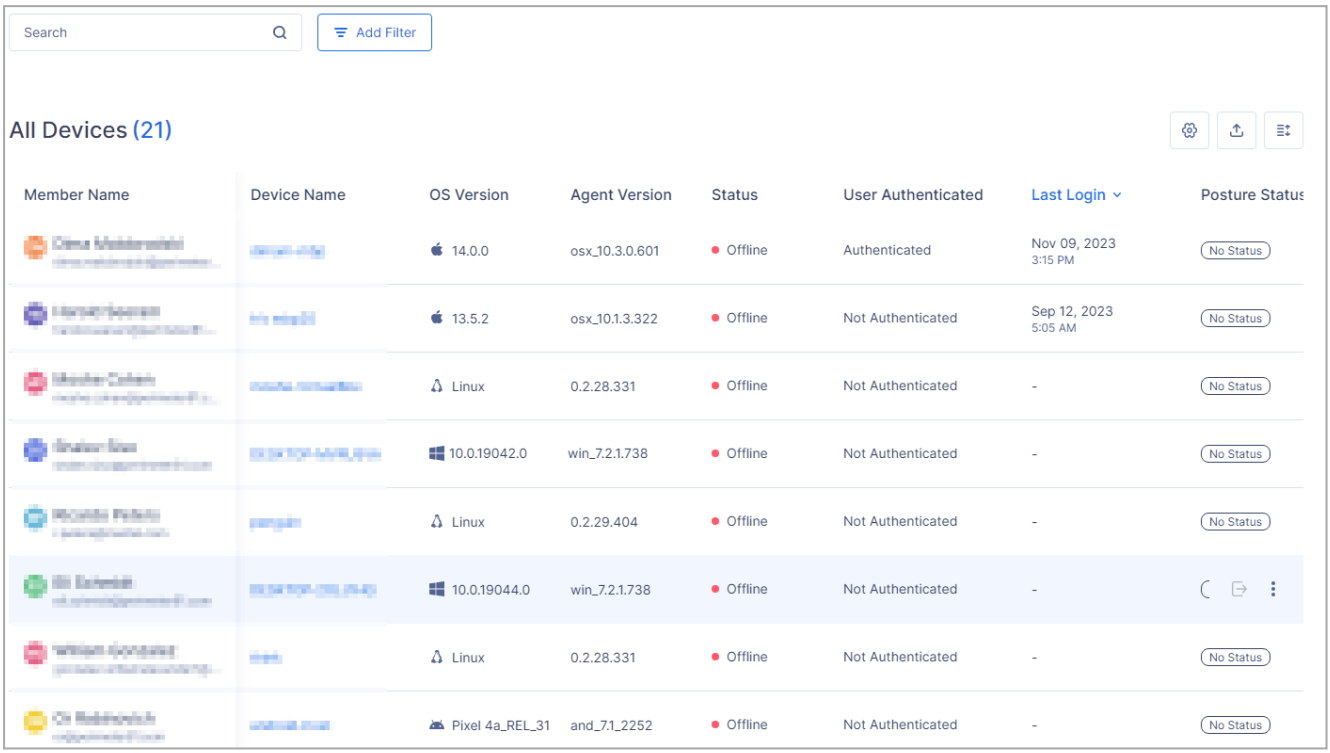

The **OS Distribution** widget shows the distribution of operating systems across devices by percentage.

## Posture Status



The **Posture Status** widget shows the posture status of your devices by percentage. For more information, see Manage DPC.

# Device Inventory Details




| Column | Description |
|---|---|
| Member Name | User of the device. |
| Device Name | Name of the device. |
| OS Version | Operating System and version of the device. |
| Agent Version | Agent version installed on the device. |
| Status | The last known device status.<br>■ **Online** - Agent is running and the user is signed in but not connected to the VPN.<br>■ **Offline** - Device is turned off or not connected to the internet.<br>■ **Connected** - Agent is connected to the VPN. |
| User Authenticated | User authentication status.<br>■ **Authenticated** - User has signed in to the agent with valid credentials.<br>■ **Not Authenticated** - User authentication has expired or invalid credentials entered. |

| Column | Description |
|---|---|
| Last Login | Date and time of the last login. |
| Posture Status | Device Posture Check (DPC) status.<br>■ **Healthy** - Device is compliant with the DPC policy.<br>■ **Not Healthy** - Device is not compliant with the DPC policy.<br>■ **No Status** - User has not signed in since the DPC policy assignment or no DPC policy assigned to the device. |
| Security Warning | Reason for the failed DPC. For example, Missing Anti-Virus software on the device. |
| Last Posture Check | Date and time when the posture check was last done. |
| Posture Policy | DPC policy applied to the device. |
| Device Serial / ID | Unique identifier of the device. For macOS, it is the serial number generated by macOS. For other operating systems, it is generated by Harmony SASE. |
| Device Type | Type of the device.<br>■ Desktop<br>■ Mobile |

# Logging Out the Device

1. For the device you want to log out, scroll to the end of the row and click .
2. Go to **Actions** and click **Logout Device**.

# Removing Device

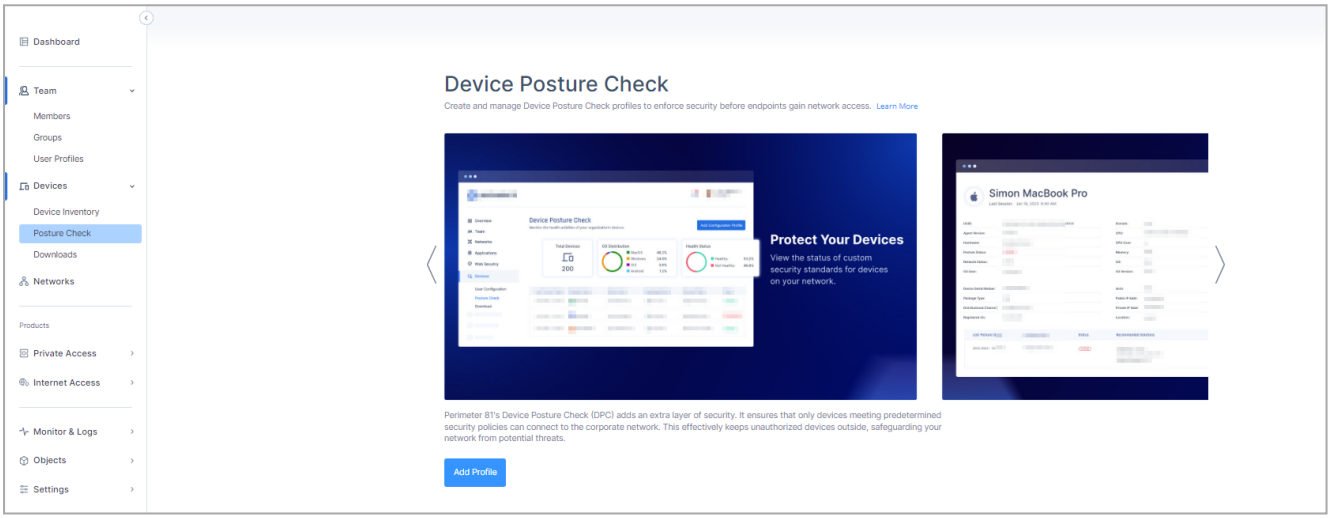
1. For the device you want to remove, scroll to the end of the row and click .
2. Go to **Actions** and click **Remove Device**.

# Posture Check

The **Posture Check** page allows you to specify the posture requirements for the device. If the device does not meet the specified posture requirement, then the Harmony SASE Agent blocks private and internet access.

The posture check is performed periodically while the device connected to a network or every time when the device connects to the network.

To view the **Posture Check** page, access the Harmony SASE Administrator Portal and click **Devices** > **Posture Check**.




## Supported Posture Requirement Checks

| Posture Requirement | Windows | macOS | Linux |
|---|---|---|---|
| Specific or any Anti-Virus software is active and up to date on the device.* | Yes | Yes | Yes |
| Specific or any firewall or Windows Security Center is active and up to date on the device. | Yes | No | No |
| The device has the specific OS installed and running on the device. | Yes | Yes | No |
| Check for required or banned specific files on the device. | Yes | Yes | Yes |
| Check for required or banned registry keys and values on the device. | Yes | No | No |
| Check for required or banned processes on the device. | Yes | Yes | Yes |

| Posture Requirement | Windows | macOS | Linux |
|---|---|---|---|
| Hard drive on the device is encrypted. | Yes | Yes | No |
| Valid device certificate is installed trusted by a CA. | Yes | Yes | No |
| The user has signed in to a specified AD domain. | Yes | No | No |

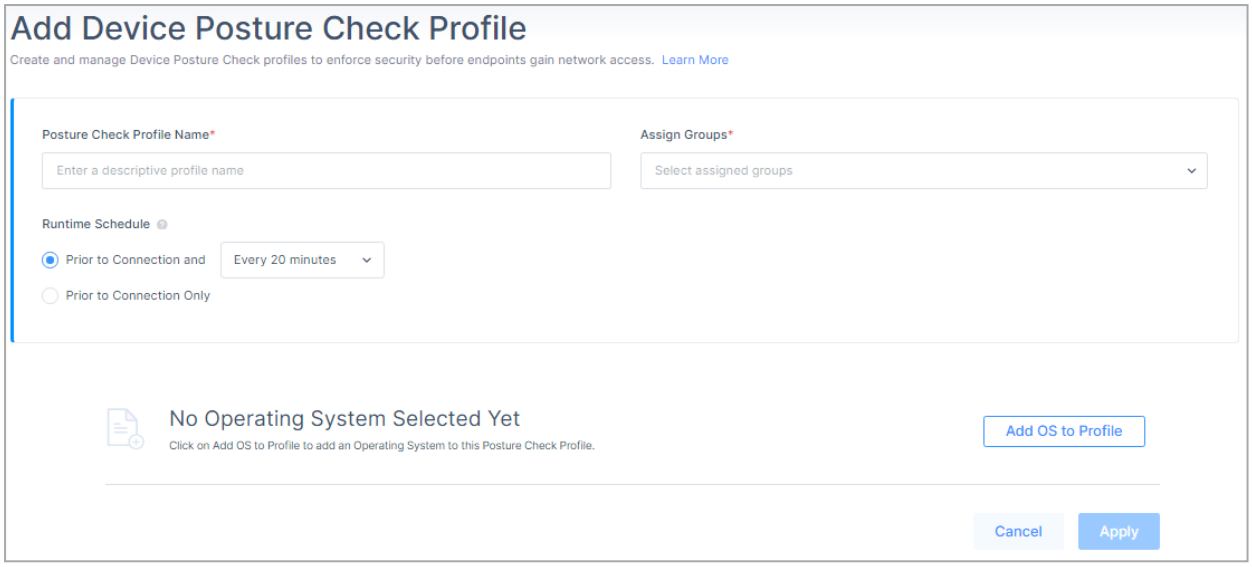
* The supported Anti-Virus software are:

- Windows Defender
- Symantec Norton
- McAfee
- Avast
- Kaspersky
- SentinelOne
- Falcon Crowdstrike
- Bitdefender Total Security
- Eset
- Malwarebytes
- Webroot
- ESET NOD32
- ClamAV
- Check Point Harmony Endpoint

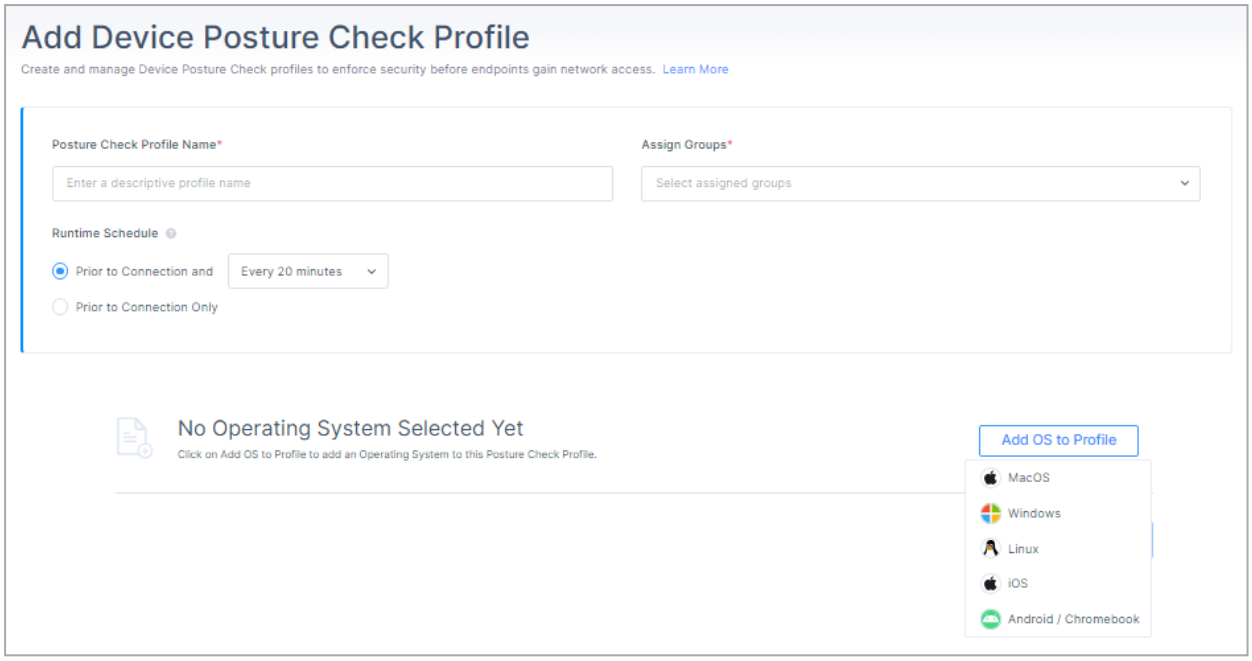
# Specifying the Device Posture Check Requirements

1. Access the Harmony SASE Administrator Portal and click **Devices** > **Posture Check**.
2. Click **Add Profile**.

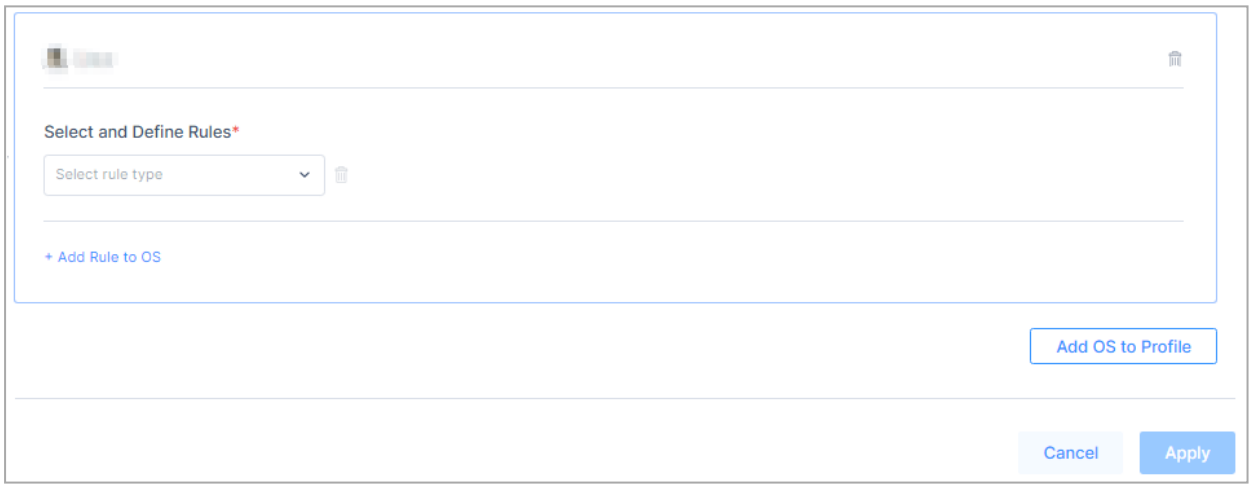
   The **Add Device Posture Check Profile** window appears.




3. In the **Posture Check Profile Name** field, enter a profile name.
4. From the **Assign Groups** list, select the member group(s) to which you want to apply the posture check.
5. In the **Runtime Schedule** section, select when to run the device posture check:
   - **Prior to Connection** and select the interval:
     - **Every 20 minutes**
     - **Every 40 minutes**
     - **Every 60 minutes**
   - **Prior to Connection Only**
6. To add operating system, click **Add OS to Profile**.
7. Select the Operating System from the list:
   a. **MacOS**
   b. **Windows**
   c. **Linux**
   d. **iOS**
   e. **Android / Chromebook**




8. From the **Select and Define Rules** list, select the rule type:

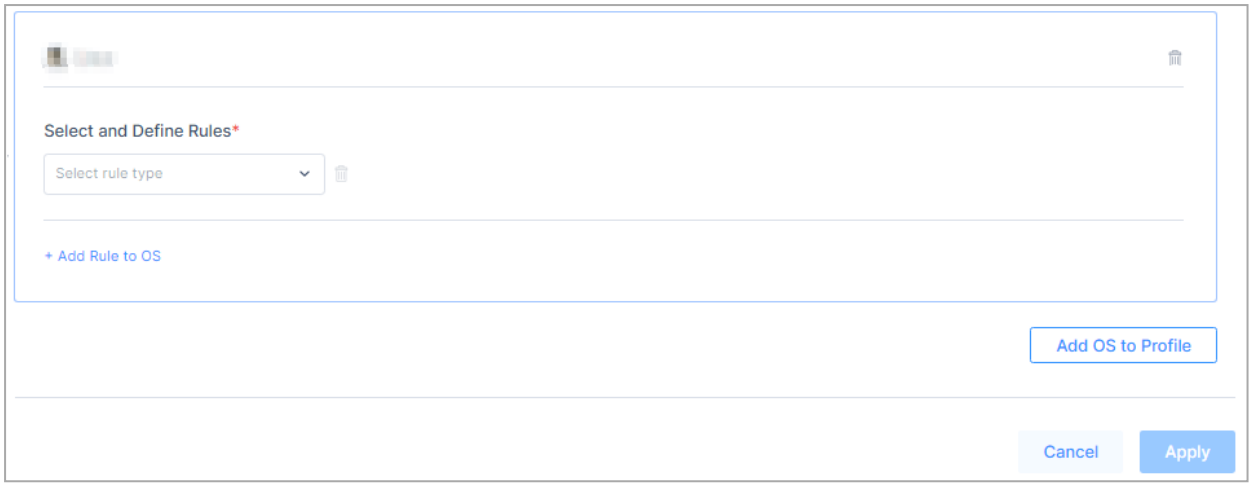


| Posture Check Requirement | Description | Action |
|---|---|---|
| **Anti-virus** | Verifies if the specified Anti-Virus is installed, up-to-date and running. | Select the Anti-Virus software products from the list. |
| **File Exists** | Verifies if certain file exist or do not exist (banned) in the specified path. | Enter the path with forward slash. For example, `C:/user/testing` |
| **Disk Encryption** | Verifies that the OS hard drives are encrypted. | N/A |
| **Certificate** | Verifies that a specific certificate is installed on the device (Mac Keychain). | Enter the certificate name. |

| Posture Check Requirement | Description | Action |
|---|---|---|
| **Process Running** | Verifies that certain processes are running or not running (banned) on the device. | Enter the process name with the extension *.exe*. For example, `winload.exe`.<br>To get the process name, see Certificate Pinning. This can also be used to check Anti-viruses which are not pre-defined under the Anti-virus category. |
| **Operating System version** | Verifies if the specified OS version or higher is running. | Select the operator and then enter the OS version number. For example, `10`, `10.0` or `10.0.19045`. |
| **Registry** | Verifies if the specific registry key exists or do not exist (banned). | ■ In the **Enter registry key in HKEY_format** field, enter registry key name that must start with HKEY and must not end with \. For example, `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\New Key`).<br>■ (Optional) In the **Value** field, enter the value of the registry key. |

| Posture Check Requirement | Description | Action |
|---|---|---|
| **Windows Security Center** | Verifies if the specified Firewall, Anti-virus, or Windows Security Center is installed and active. | Select a list:<br>▪ **Antivirus**<br>▪ **Firewall**<br>▪ **Windows Security Center Service** |
| **Active Directory Association** | Verifies if the user is signed in to a specified AD domain. | Enter the domain name. You can add two domains by adding `OR` between the domain names. |
| **Define Access Permission** | Allows or blocks the network access to the device. Default is **Allow**. | Select an action from the **Define Access Permission** list:<br>▪ To allow mobile devices to access networks, select **Allow**.<br>▪ To block mobile devices from accessing networks, select **Deny**.<br>▪ To allow chromebook and prevent android devices to access networks, select **Allow Chromebook only**. |

9. To add more rules to OS, click **Add Rule to OS** and repeat step 8.



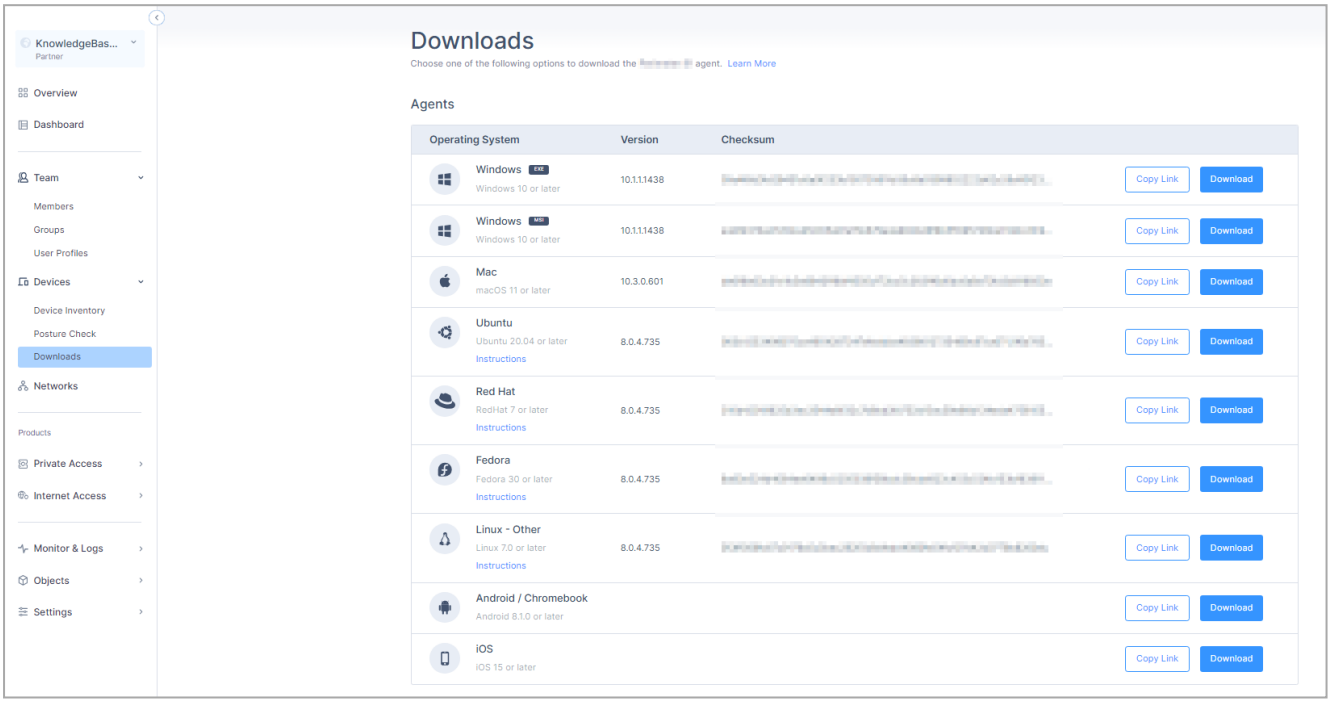

10. Click **Apply**.

    The Device Posture Check profile is created.

# Downloads

In the **Downloads** page, you can download the Harmony SASE Agent.

To view the **Downloads** page, access the Harmony SASE Administrator Portal and click **Devices** > **Downloads**.




**Notes**:

- The Harmony SASE Agent versions on this page may be newer than the default version for some customers, as a gradual rollout is in progress. For the latest Harmony SASE Agent versions, see sk182466.
- The Harmony SASE Agent is not supported on devices with ARM processor.

## Downloading and Deploying the Harmony SASE Agent

1. Access the Harmony SASE Administrator Portal and click **Devices** > **Downloads**.
2. Do one of these:

- Click **Download**.

  The system downloads the file.

| Operating System | Version | Downloaded File |
|---|---|---|
| Windows EXE | Windows 10 64-bit or later | Downloads an exe file. |
| Windows MSI | Windows 10 64-bit or later | Downloads a MSI file. |
| Mac | macOS 11 or later | Downloads a PKG file. |
| Ubuntu | Ubuntu 20.04 or later | Downloads a Deb file. |
| Red Hat | RedHat 7 or later | Downloads a RPM file. |
| Fedora | Fedora 30 or later | Downloads a RPM (Fedora) file. |
| Linux - Others | Linux 7.0 or later | Downloads a tar.xz file. |
| Android / Chromebook[1] | Android 8.1.0 or later | Redirects to Google Play Store. |
| iOS | iOS 15 or later | Redirects to Apple App Store. |

[1]To install Harmony SASE on Chromebook, see *"Installing Harmony SASE on Chromebook" on page 90*.

- Click **Copy** to copy the download link. Share the link with members.

3. To verify that the downloaded file is authentic, use the **Checksum**.
4. *"Deploying the Harmony SASE Agent" on page 88*.

# Certificates

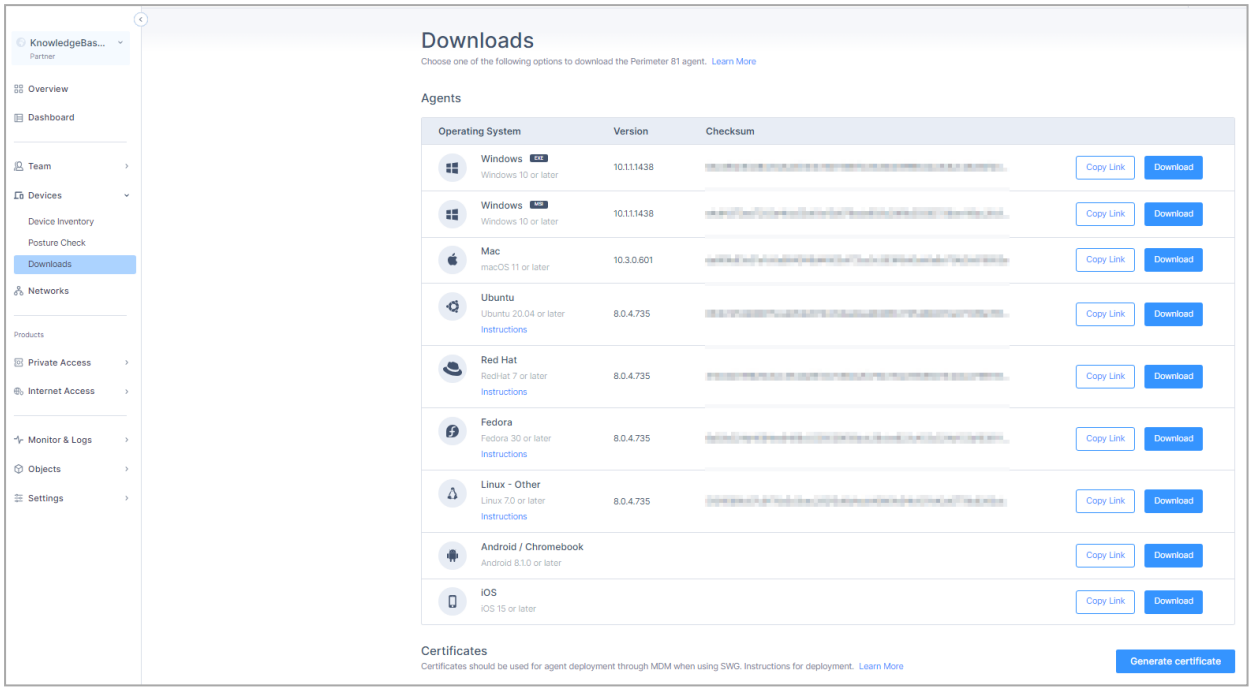
You can download Secure Web Gateway (SWG) root certificate and install it on macOS devices either manually or using an MDM application. The SWG root certificate is required for Internet Access.

**Notes**:

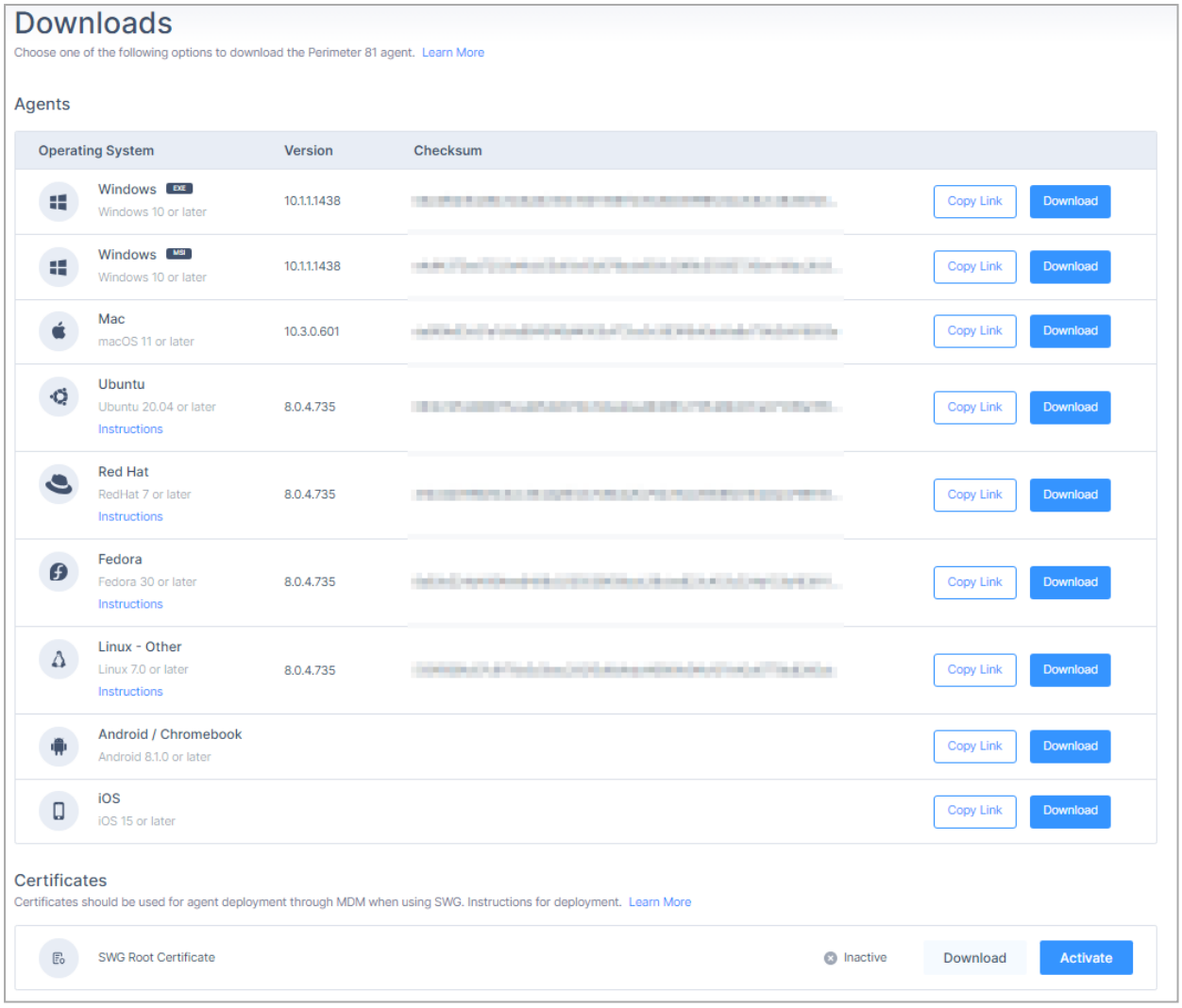
- It is supported only with the macOS Harmony SASE Agent version 10.4 and higher.
- The **Revoke** button is disabled. It will be supported in the future.

## To download the SWG root certificate:

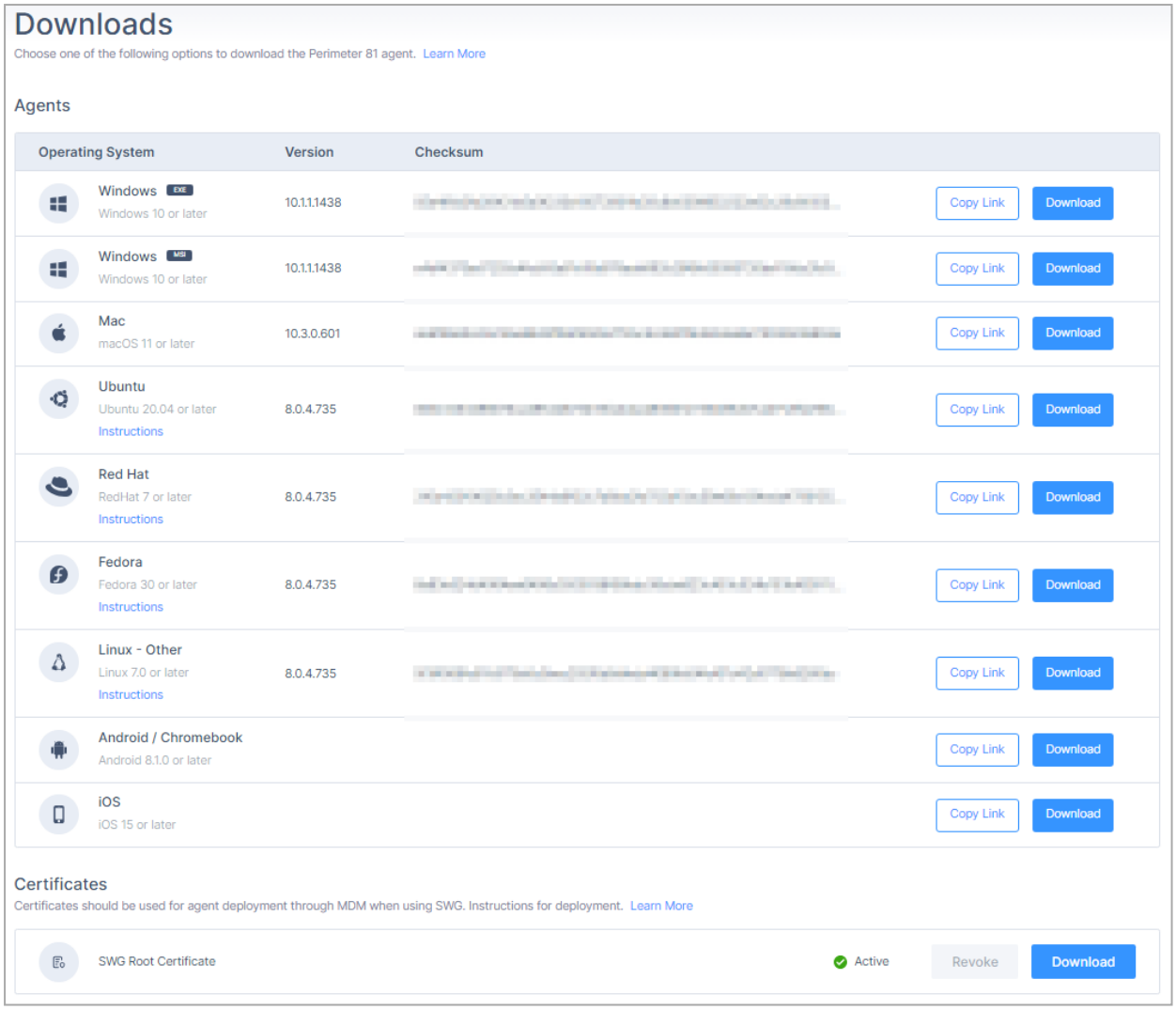
1. Access the Harmony SASE Administrator Portal and click **Devices** > **Downloads**.




2. In the **Certificates** section, click **Generate certificate**.




3. Click **Activate** to activate the SWG root certificate.




4. When the certificate is active, click **Download**.

   The system downloads a PEM file.

5. Install the certificate on macOS devices either:

   - Manually
   - Using an MDM application. Refer to the MDM's documentation.

     **Best Practice** - Configure the required app permissions in the MDM so that it is installed without user intervention.

# Deploying the Harmony SASE Agent

You can deploy the Harmony SASE Agent manually or using a Mobile Device Management (MDM) provider.

## Deploying the Agent Manually

To deploy the agent manually:

- *"Invite Members" on page 57*

  The system sends an email to members with a link to accept the invite and download the Harmony SASE Agent. The invitation is valid for 30 days. If the invitation expires, you must resend the invitation.

- Download the agent and distribute it manually, for example, through email.
- Copy the agent download link and share it manually, for example, through email.

# Deploying the Agent Using an MDM Application

You can deploy the agent using any of these popular Mobile Device Management (MDM) applications:

- Cisco Meraki
- JAMF Cloud
- ManageEngine
- Microsoft Intune
- Microsoft System Center Configuration Manager (SCCM)
- MobileIron
- VMWare AirWatch

## Common Commands

| Operating System<br>Command for | Windows | macOS |
|---|---|---|
| Silent Installation | `msiexec /quiet /i Perimeter81_x.x.x.xxx.msi`<br>To know the installation status after the silent installation, run:<br>1. `start /wait msiexec /quiet /i "Perimeter81_x.x.x.xxx.msi"`<br>2. `echo %errorlevel%` | `$ sudo installer -pkg Perimeter81_x.x.x.xxx.pkg -target /`<br>To change the agent permissions after the installation, run:<br>1. `$ sudo chown -R $(stat -f%Su /dev/console) "/Applications/Perimeter81.app"`<br>2. `$ chmod -R u=rwx "/Applications/Perimeter81.app"` |

| Operating System<br>Command for | Windows | macOS |
|---|---|---|
| Pre-populating the tenant or workspace name | `msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name"` | `$ sudo defaults write com.perimeter81d workspace workspace_name`<br>To remove pre-populated workspace/tenant name, run:<br>`$ sudo defaults delete com.perimeter81d workspace`<br>This is supported only with agent version 8.0.4.116 and higher. |
| Pre-populating the data residency region | `msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet REGION="EU or US"`<br>For `REGION`, add `"EU"` for Europe and `"US"` for America. | `$ sudo defaults write com.perimeter81d region "EU or US"`<br>For `region`, add `"EU"` for Europe and `"US"` for America. |
| Pre-populating the tenant or workspace name and data residency region | `msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name" REGION="EU or US"`<br>For `REGION`, add `"EU"` for Europe and `"US"` for America. | To pre-populating the tenant or workspace name, run:<br>`$ sudo defaults write com.perimeter81d workspace workspace_name`<br>To pre-populating the data residency region, run:<br>`$ sudo defaults write com.perimeter81d region "EU or US"`<br>For `region`, add `"EU"` for Europe and `"US"` for America. |
| Uninstallation | `msiexec /x "Perimeter81_x.x.x.xxx.msi"` | Run the uninstall script. |

# Installing Harmony SASE on Chromebook

1. Download the **Harmony SASE** Agent. For more information, see Downloads.
2. To enable **Developer Mode**:

a. Restart your Chromebook.

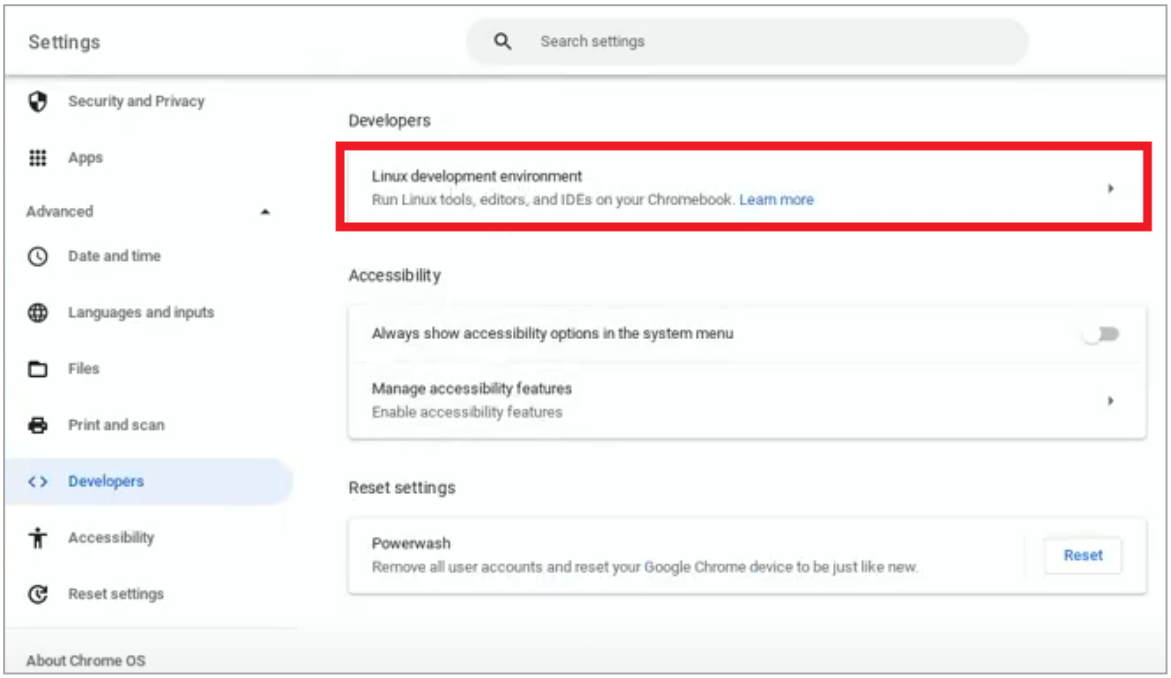
b. Press **Esc** + **Refresh button** + **Power button** simultaneously during restart.

c. Press **Ctrl** + **D** when a warning is displayed.

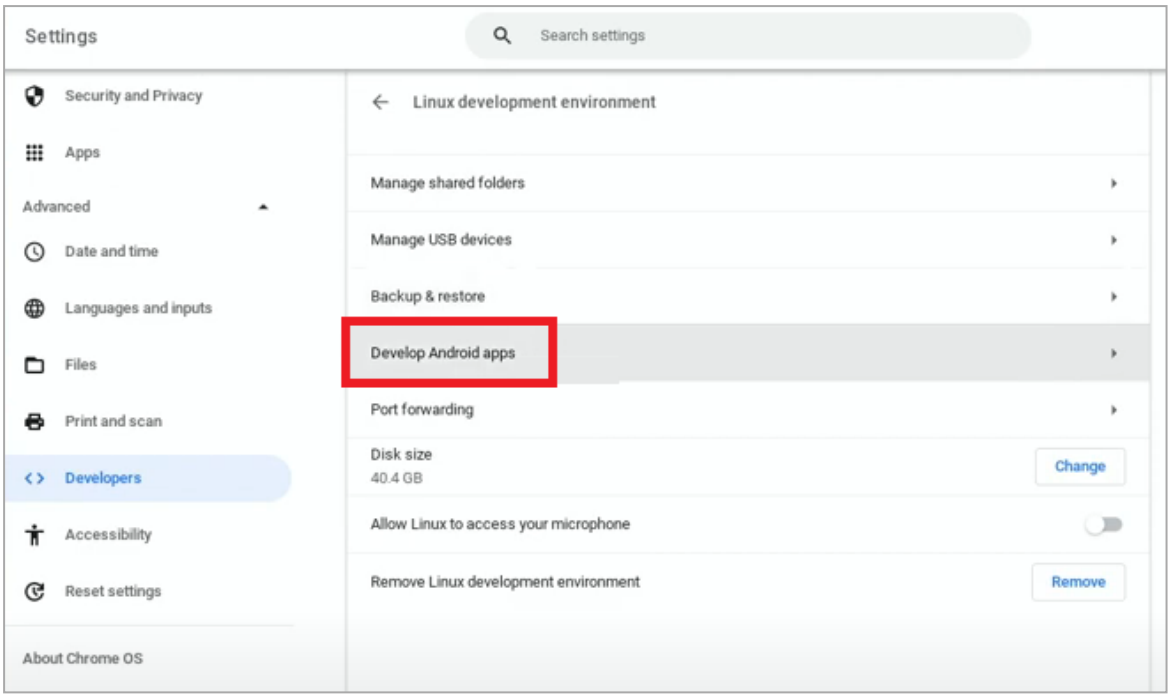
   The **Developer Mode** is enabled.

3. To enable **ADB debugging**:

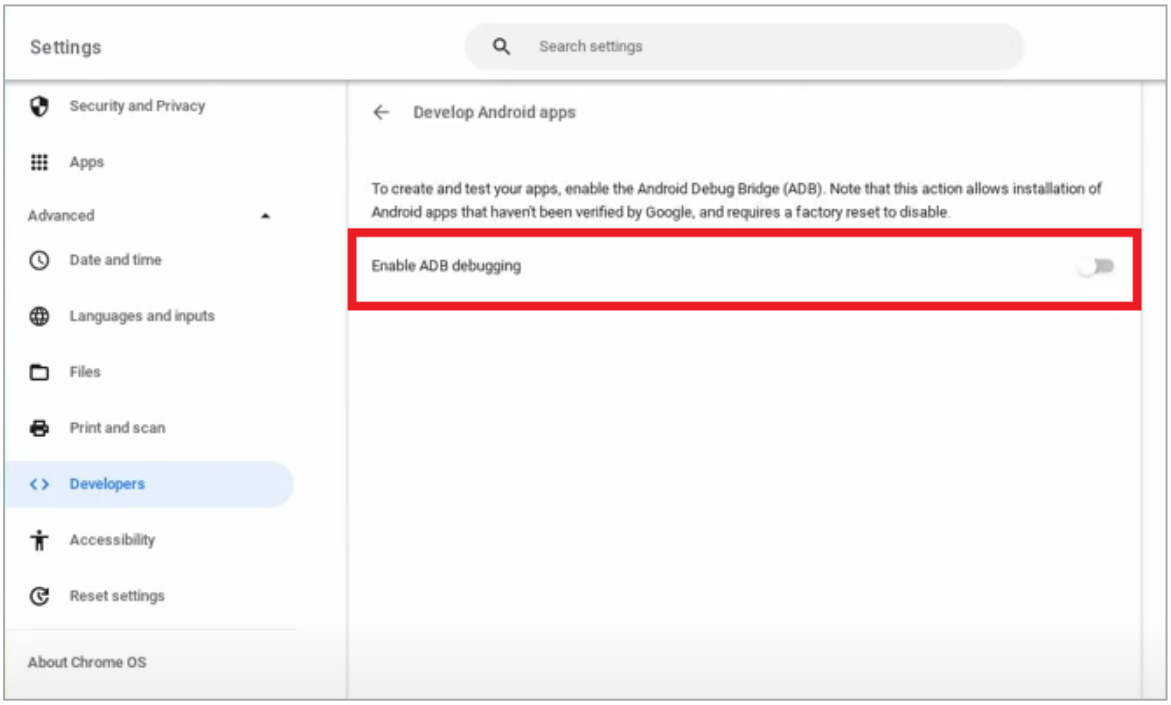
   a. Go to **Settings** > **Advanced** > **Developers**.



b. Click **Linux development environment** > **Develop Android apps**.




c. Turn on the **Enable ADB debugging** toggle button.




The **Enable ADB debugging** window appears.

d. Click **Restart and continue**.

e. Click **Allow**.

The **ADB debugging** is enabled and the Chromebook restarts.

4. To install the ADB platform tools, go to your **Linux apps** folder and open **Terminal**.
5. Click **penguin** to open a Linux terminal and run:

   ```
   sudo apt-get install android-tools-adb -y
   ```

   The Android Package Kit (APK) file gets downloaded.
6. Navigate to **Linux** > **My files** > **Linux files**.
7. Drag and drop the downloaded APK file to the **Linux files** folder. This creates a new directory in the Linux terminal.
8. To check the default location where the new directory is created, go to the penguin Linux terminal and run:

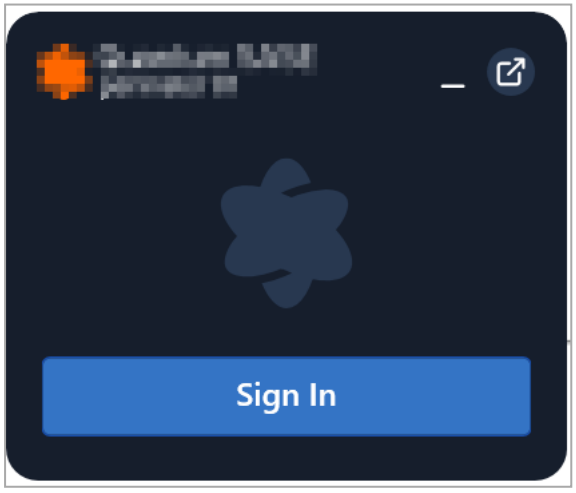
   ```
   df -h /boot/
   ```
9. Navigate to the file system `cd /dev/hda1` should be the default folder where the API file is located at.
10. To install Harmony SASE Agent, run:

    ```
    adb install <filename>.apk
    ```

# Using the Harmony SASE Agent

Before you begin, contact your System administrator for your workspace URL.

1. Open the Harmony SASE Agent.
2. Click **Sign In**.

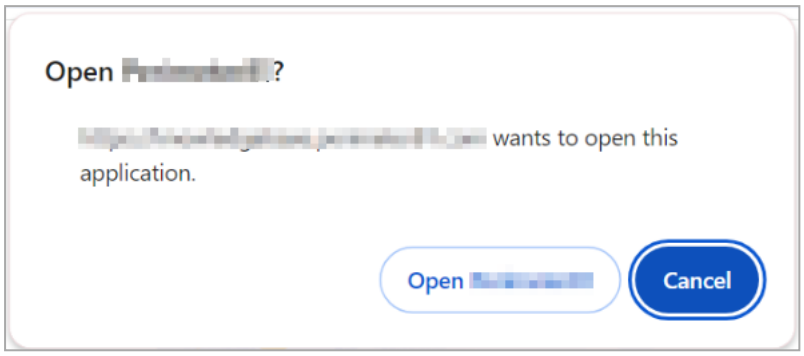



   The system opens a web browser for authentication.
3. In the **Workspace URL** field, enter the workspace URL and click **Continue**.
4. Enter your credentials and click **Sign In**.

If you do not know your credentials, contact your System Administrator.

A prompt appears.

5. Click **Open Harmony SASE**.

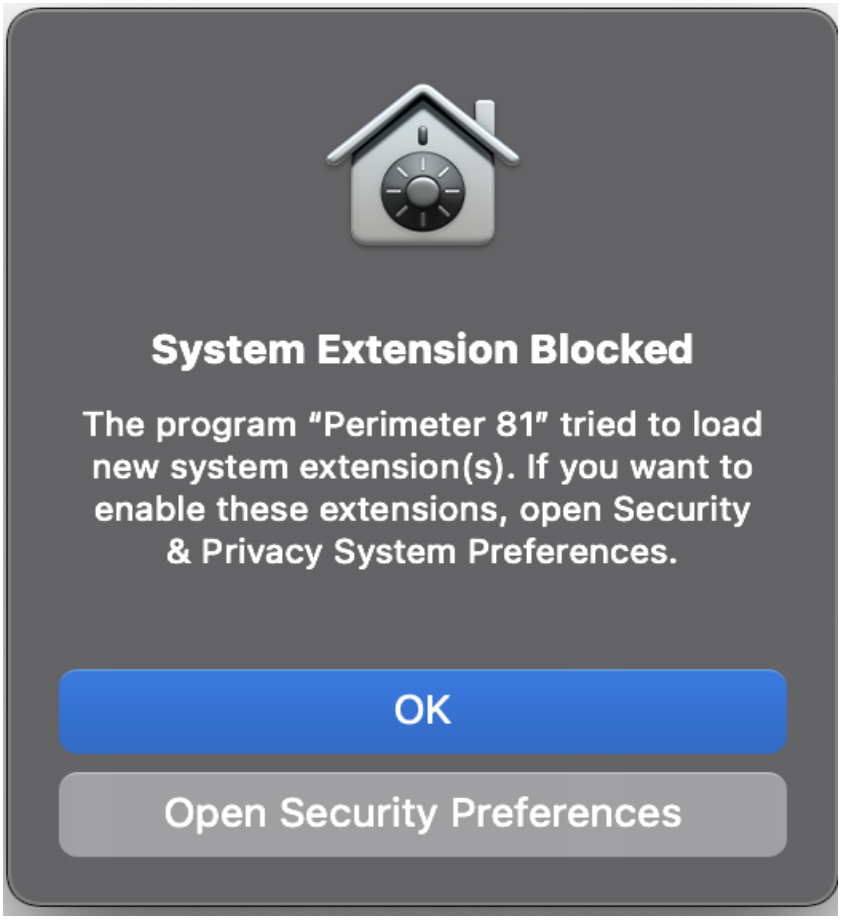



The Harmony SASE Agent opens and automatically connects to a **Network**.

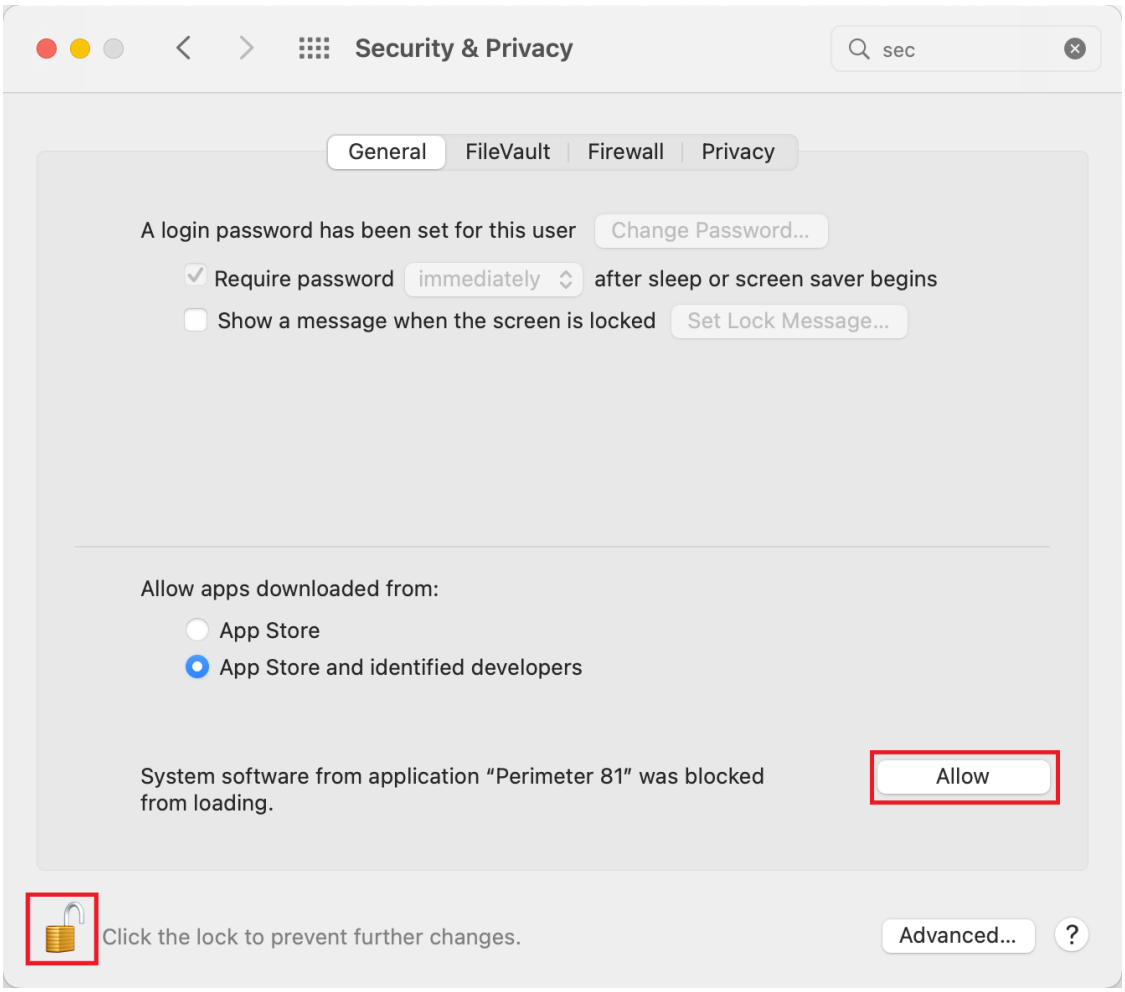
6. For macOS devices, if internet access is enabled, then do these (otherwise, skip the step):

**Note** - If you download the Secure Web Gateway (SWG) root certificate, skip the step. For more information, see Certificates.

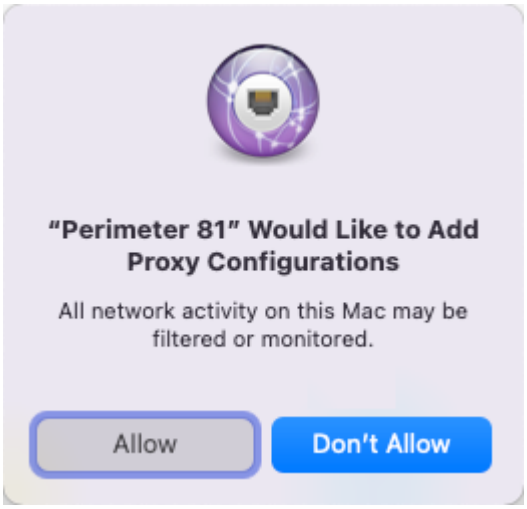
a. Click **Open Security Preferences**.



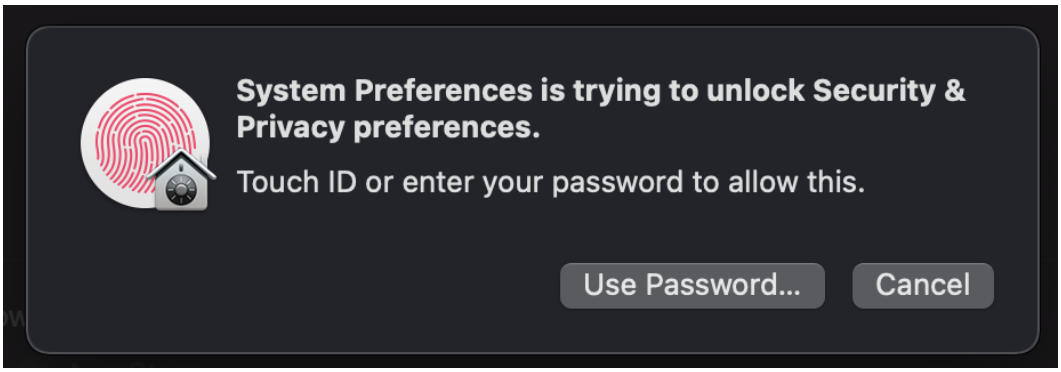
b. Click the lock icon at the bottom left and click **Allow**.



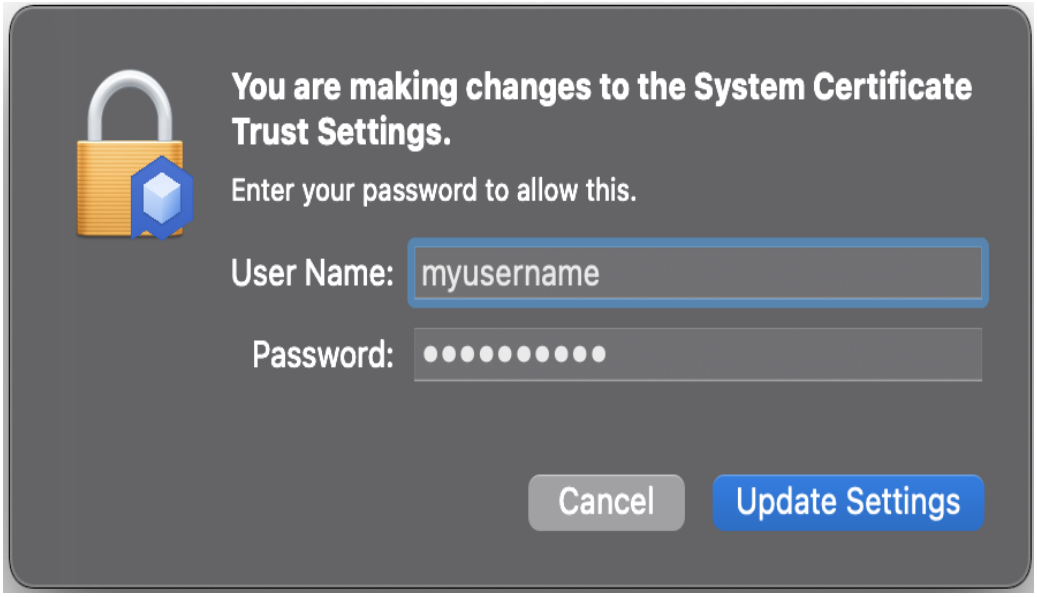

c. At this prompt, click **Allow**.



d. In this prompt, click **Use Password**.




e. Enter your device credentials and click **Update Settings**.




7. To connect to a specific network, on the **Home** tab, click **Change Network** and then select a network.
8. To make changes to the Harmony SASE Agent, click the icon at the bottom left.

| Setting | Description |
|---|---|
| **General tab** | |
| Connect of Launch | Automatically starts the Harmony SASE Agent when the device starts and connects to the most recent network. |
| Enable Notifications when Connected/Disconnected | Shows a pop-up notification on the device when the Harmony SASE Agent connection status changes. |

| Setting | Description |
|---|---|
| Enable Notification when Reconnecting | Shows a pop-up notification on the device when the Harmony SASE Agent reconnects with the network. |
| Check For Updates | Checks and shows the latest version of Harmony SASE Agent if available. |
| Automatic Updates | Automatically upgrades to the latest version of the Harmony SASE Agent.<br>**Note** - Available only if the System Administrator has enabled it. See *"Agent Upgrades" on page 67*. |
| Snowplow report. | Sends the Snowplow (user tracking) data to Harmony SASE. |
| Use VPN Interface DNS | Sets the device DNS server as the Harmony SASE server. The agent uses this DNS server for DNS requests specified on the VPN network interface.<br>If this is disabled, then the DNS resolver is set to the DNS used by your local adapter. This is useful if you use other DNS providers. |
| **Network tab** | |
| Always-On VPN | Automatically connects to the VPN when an internet connection is available. |
| Automatic Wi-Fi Security | The Harmony SASE Agent automatically connects to Harmony SASE VPN if the device connects to an unsecured Wi-Fi. |
| Trusted Wi-Fi Networks | The Harmony SASE Agent does not enable **Automatic Wi-Fi Security** if the device connects to a trusted Wi-Fi network.<br>**Note** - This option shows only the trusted networks added by the administrator. See *"Network Configuration" on page 68*. |
| **Protocols tab** | |
| Default | Automatically connects to the network using a protocol configured by the administrator. See *"Network Configuration" on page 68*. |
| WireGuard | Connects to the network using WireGuard protocol. |

| Setting | Description |
|---|---|
| OpenVPN | Connects to the network using OpenVPN protocol. |

9. Go the **Support** tab and do these:
   - To reset the agent, click **Reset Agent**.
   - To view the documentation, click **User Guides**.
   - To start a live chat with a Harmony SASE expert, click **Live Chat**.
   - To run a quick health check and send the results to Harmony SASE, click **Send Logs to Support**.

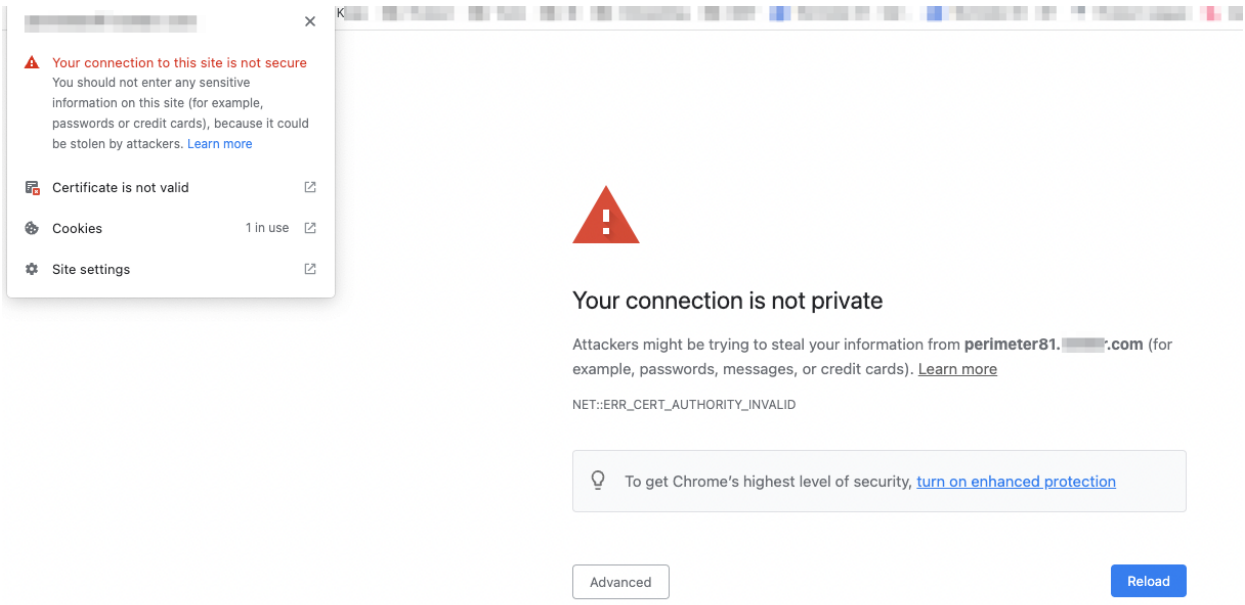
     If automatic log collection does not work, see *"Collecting Logs Manually" on page 102*.
10. To sign out of the agent, click the  icon.

    If this option is disabled by the administrator, the agent prevents the member from signing out without a sign-out code. For more information, see *"Disable Sign-Out" on page 66*.
11. To exit the agent, click the  icon. This disables the agent and stops the secure private and internet access.

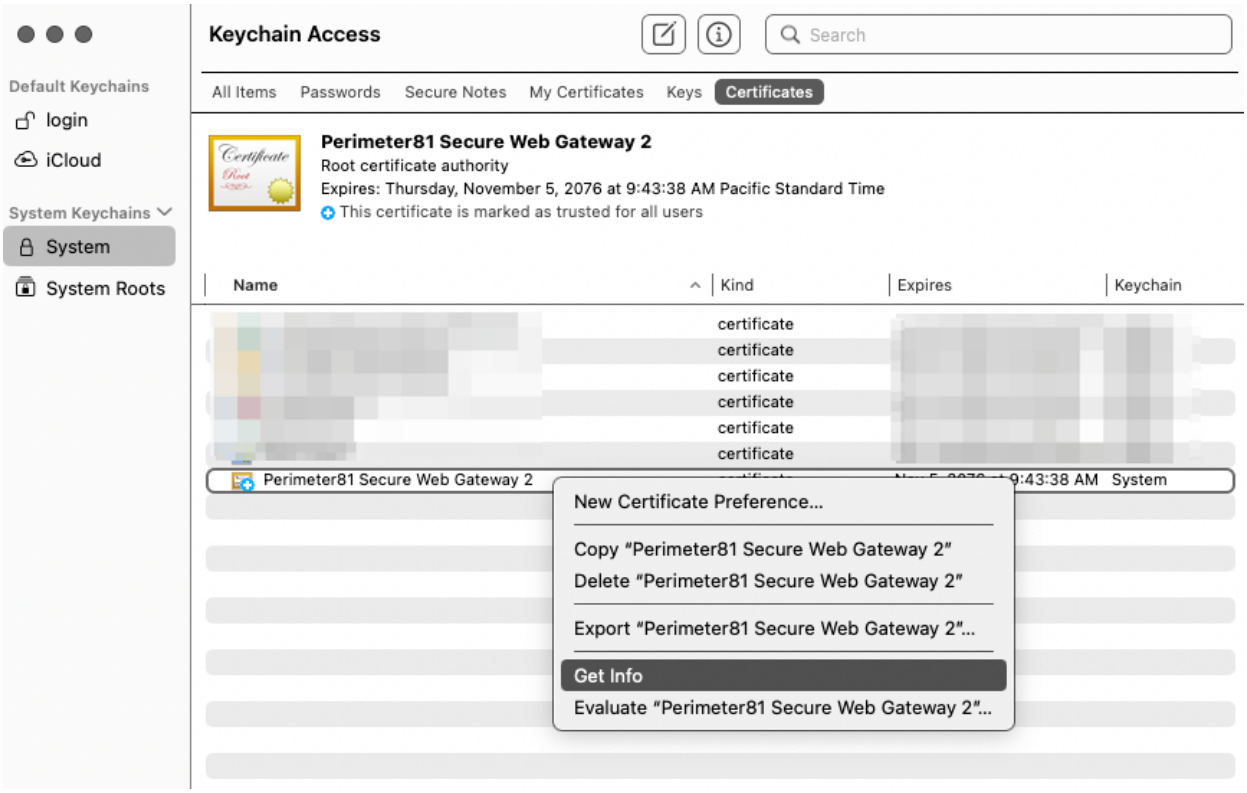
# Troubleshooting System Extension Installation on macOS

If the member does not complete the system extension installation during the agent installation:

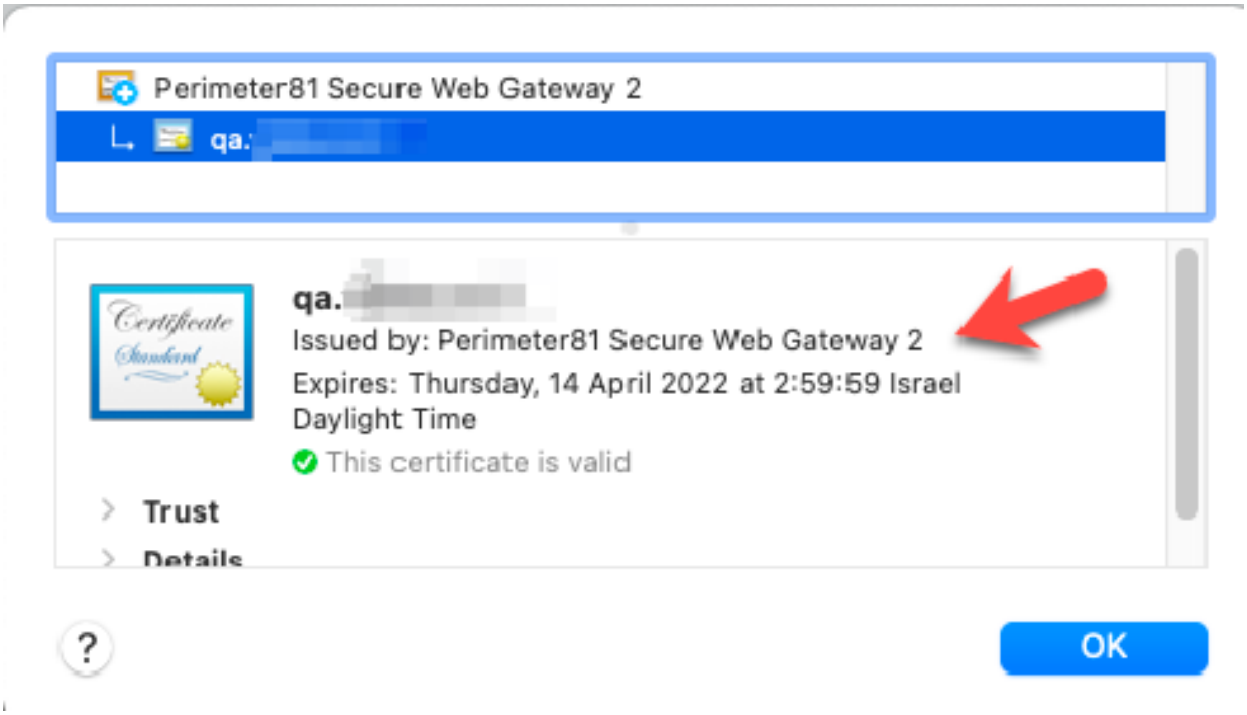
1. Sign out and sign in to the agent.
2. If the Secure Web Gateway certificate installation is blocked, then this error message appears.




3. Open **Keychain Access**.




4. Right click **Perimeter 81 Secure Web Gateway 2** certificate and click **Get Info**.
5. Modify the permission to **Always trust**.




# Uninstalling the Harmony SASE Agent

## Windows

Follow the computer's procedure to uninstall the agent.

## macOS

- Follow the computer's procedure to uninstall the agent.
- Run the uninstall script on the device.
- If you use an MDM, execute the script through the MDM on the devices.

**Note** - If you use Harmony SASE Secure Web Gateway (SWG), deploy the SWG-enabled agents in the presence of your Customer Success Engineer.

## Linux

### Ubuntu

To uninstall the Harmony SASE Agent, run:

```
CLICLIsudo apt remove --purge <Perimeter 81 package name>
sudo rm -Rf /etc/Perimeter81
sudo rm -Rf $HOME/.config/Perimeter81
sudo rm -Rf /opt/Perimeter81
```

# Android / iOS

Follow the device's procedure to uninstall the agent.

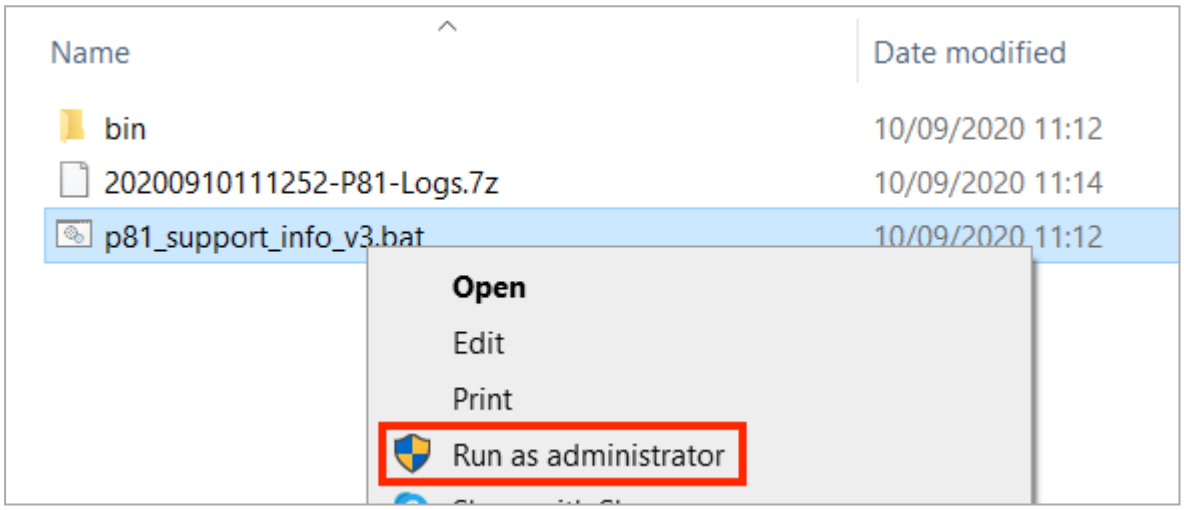
# Collecting Logs Manually

If the Harmony SASE Agent fails to perform automatic log collection, you can manually collect and send the logs using scripts.

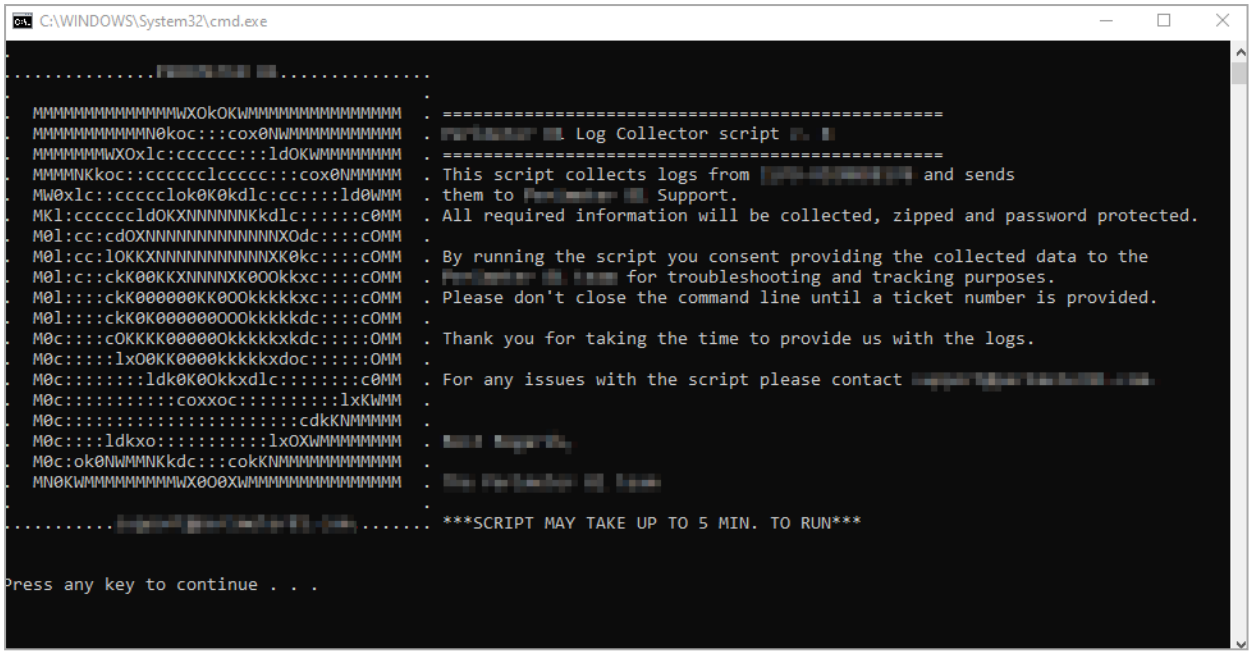
**Note** - This option is available only for the Perimeter 81 workspace accounts.

## Windows

1. Download and extract the script file WinTroubleshooting.zip.
2. Right-click the *.bat* file and click **Run as administrator**.



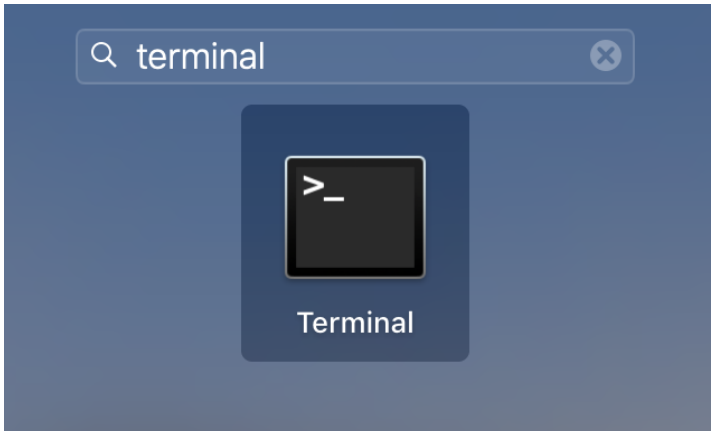

3. Provide your email, workspace name, and ticket number (if applicable). The system automatically sends the log files to *Check Point Support*.




4. To manually locate log files on your machine:
   - For connection log file, go to *%LOCALAPPDATA%\Perimeter81\Log*
   - For application log file, go to *%WINDIR%\System32\config\systemprofile\AppData\Local\Perimeter81*

# macOS

1. Download and extract the script file MacTroubleshooting.zip.
2. On your Mac machine, open the **Terminal** application.




3. Run:

```
sudo bash /Users/*/Downloads/Customer_logs*.sh
```

4. Provide your email, workspace name, and ticket number (if applicable). The system automatically sends the log files to *Check Point Support*.
5. To manually locate log files on your machine:

- For connection log file, go to */var/log/Perimeter81*
- For application log file, go to */tmp/Perimeter81.log*

## Linux

1. On your Linux machine, open the **Terminal** application and run:

   ```
   /opt/Perimeter81/perimeter81 collect-logs
   ```

2. Send the log file to *Check Point Support*.

# Networks

The **Networks** page allows you to specify your network for private access. A network consists of three basic components:

- *"Regions and Point-of-Presence" on page 106*
- *"Gateways" on page 109*
- *"Tunnels" on page 112*

## High-Level Procedure

*"Defining a Network" on page 115*.

*"Adding a Tunnel" on page 121*.

*"Managing a Network" on page 141*.

# Regions and Point-of-Presence

Regions are the physical locations of your Harmony SASE gateway(s). You can deploy the Harmony SASE gateway in a single or multiple (Lower latency, redundancy and better performance) regions. Harmony SASE automatically connects your members to the nearest Harmony SASE gateway.

| North America | EMEA | APAC | LATAM |
|---|---|---|---|
| ■ Ashburn 1, VA, USA [1]<br>■ Boston, MA, USA[1]<br>■ Chicago 1, IL, USA [1]<br>■ Dallas 1, TX, USA [1]<br>■ Denver, CO, USA [1]<br>■ Los Angeles 1, CA, USA[1]<br>■ New York 1, NY, USA [1]<br>■ New York 3, NY, USA[1]<br>■ Silicon Valley 1, CA, USA [1]<br>■ Vancouver, Canada [1]<br>■ Ashburn 2, VA, USA<br>■ Atlanta 1, GA, USA<br>■ Atlanta 2, GA, USA<br>■ Chicago 2, IL, USA<br>■ Dallas 2, TX, USA<br>■ Fremont, CA, USA<br>■ Honolulu, HI, USA<br>■ Los Angeles 2, CA, USA<br>■ Miami, FA, USA<br>■ New Jersey 1, NJ, USA<br>■ New Jersey 2, NJ, USA<br>■ New York 2, NY, USA | ■ Dubai, UAE [1]<br>■ Frankfurt 1, Germany [1]<br>■ London 1, UK [1]<br>■ London 3, UK[1]<br>■ Manchester 1, UK [1]<br>■ Stockholm 1, Sweden [1]<br>■ Tel Aviv 1, Israel [1]<br>■ Amsterdam 1, Netherlands<br>■ Amsterdam 2, Netherlands<br>■ Frankfurt 3, Germany<br>■ Frankfurt 4, Germany<br>■ Helsinki, Finland<br>■ Johannesburg, South Africa<br>■ London 2, UK<br>■ London 4, UK<br>■ Madrid 1, Spain<br>■ Madrid 2, Spain<br>■ Manchester 2, UK<br>■ Milan, Italy<br>■ Paris, France<br>■ Paris 2, France<br>■ Stockholm 2, Sweden<br>■ Tel Aviv 2, Israel<br>■ Warsaw 1, Poland<br>■ Warsaw 2, Poland | ■ Bangalore 1, India<br>■ Bangalore 2, India<br>■ Chennai, India<br>■ Jakarta, Indonesia<br>■ Melbourne, Australia<br>■ Mumbai 1, India<br>■ Mumbai 2, India<br>■ New Delhi, India<br>■ Osaka, Japan<br>■ Osaka 2, Japan<br>■ Seoul, South Korea<br>■ Singapore 2<br>■ Singapore 3<br>■ Sydney 1, Australia<br>■ Sydney 2, Australia<br>■ Tokyo 1, Japan<br>■ Tokyo 2, Japan | ■ Mexico City, Mexico<br>■ Santiago, Chile<br>■ Sao Paulo 2, Brazil<br>■ Sao Paulo 3, Brazil |

| North America | EMEA | APAC | LATAM |
|---|---|---|---|
| ■ San Francisco, CA, USA<br>■ Seattle, WA, USA<br>■ Seattle 2, WA, USA<br>■ Silicon Valley 2, CA, USA<br>■ Toronto 2, Canada<br>■ Toronto 3, Canada | | | |

**Notes** -

- [1] Data centers managed by Harmony SASE. All other data centers are managed by trusted cloud service providers.
- If you cannot find a suitable region, contact *Check Point Support*.

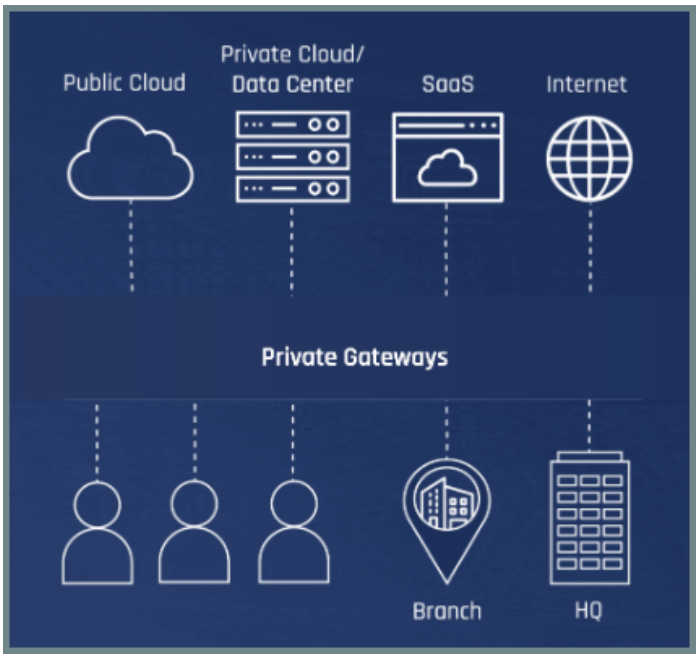
# Gateways

Gateways are the cloud-based Harmony SASE servers deployed in the region you select. Each gateway is assigned a unique static IP address that can be connected to your on-premises or cloud resources through tunnels. You can deploy multiple gateways for redundancy, and load balancing. Harmony SASE supports two types of gateways:

- *"Private Gateways" below*
- *"[DEPRECATED] Shared Gateways " below*

## Private Gateways

Private gateways are the dedicated gateways deployed for you. By default, all gateways are deployed as private. If you deploy multiple gateways, then at least one gateway must be private.




**Note** - The default gateway is of the type private. Every Harmony SASE network must consist of at least one private gateway.

## [DEPRECATED] Shared Gateways

Shared gateways are shared among customers. They are suitable if you cannot find a private gateway in your preferred region.

Harmony SASE supports shared gateways in these regions:

- Austria
- Argentina

- Australia
- Belgium
- Brazil
- Canada
- Cyprus
- Denmark
- Finland
- France
- Germany
- Hong Kong
- Hungary
- India
- Ireland
- Israel
- Italy
- Japan
- Mexico
- The Netherlands
- New Zealand
- Norway
- Poland
- Portugal
- Romania
- Russia
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland

- USA East
- USA West
- The United Kingdom

**Notes:**

- By default, all gateways are deployed as private. If you want to deploy a shared gateway, at least one gateway must be private.
- Shared gateways support only internet access. They do not support private access.

To allow members to connect to a shared gateway, see *"[DEPRECATED] Shared Network" on page 66*.

# Tunnels

Tunnels are encrypted secure connections between the Harmony SASE gateway and your SD-WAN device (on-premises or cloud) on your network. You can connect all your branches to a network using a single or multiple tunnels.

Harmony SASE supports three types of tunnels:

- *"IPSec Site-2-Site VPN Tunnel" below*
- *"WireGuard Connector Tunnel" on the next page*
- *"OpenVPN Tunnel" on the next page*

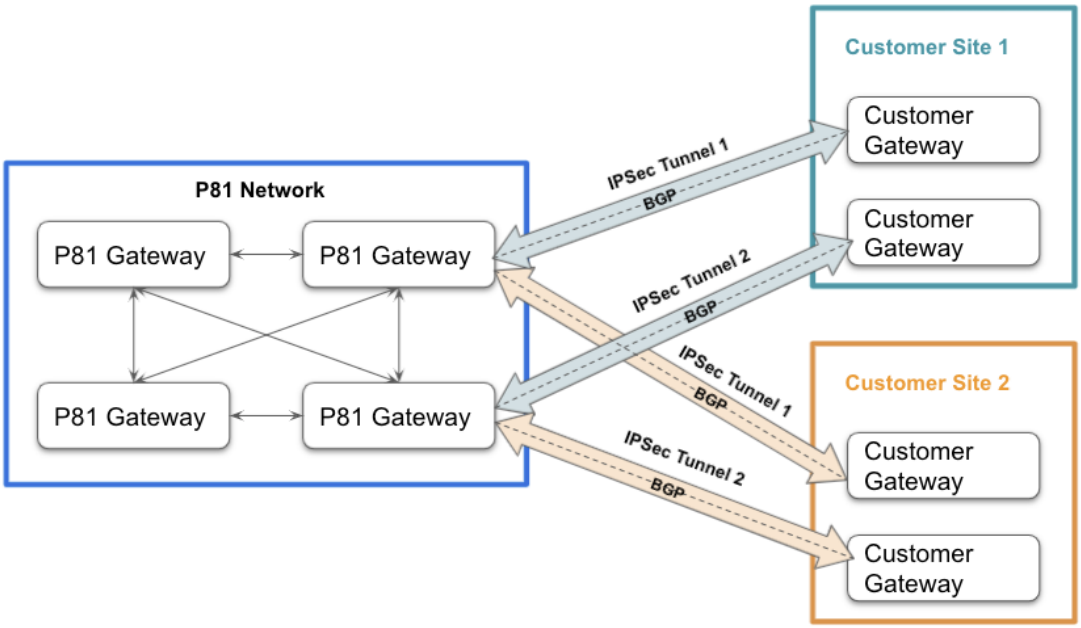
## IPSec Site-2-Site VPN Tunnel

IPSec (IP Security) is a protocol suite designed to secure data communication over IP networks to ensure integrity, confidentiality, and authentication. It uses the IKE VPN protocol to establish a secure communication between networks. An IPSec tunnel connects your Harmony SASE gateway with your local network.

You can configure either a **single IPSec Site-2-Site VPN tunnel** or **redundant tunnels**.

With a single tunnel, all the traffic is routed through this tunnel.

With redundant tunnels, traffic is routed through multiple tunnels. This offers high network availability, redundancy, better performance by routing traffic to the closest tunnel.

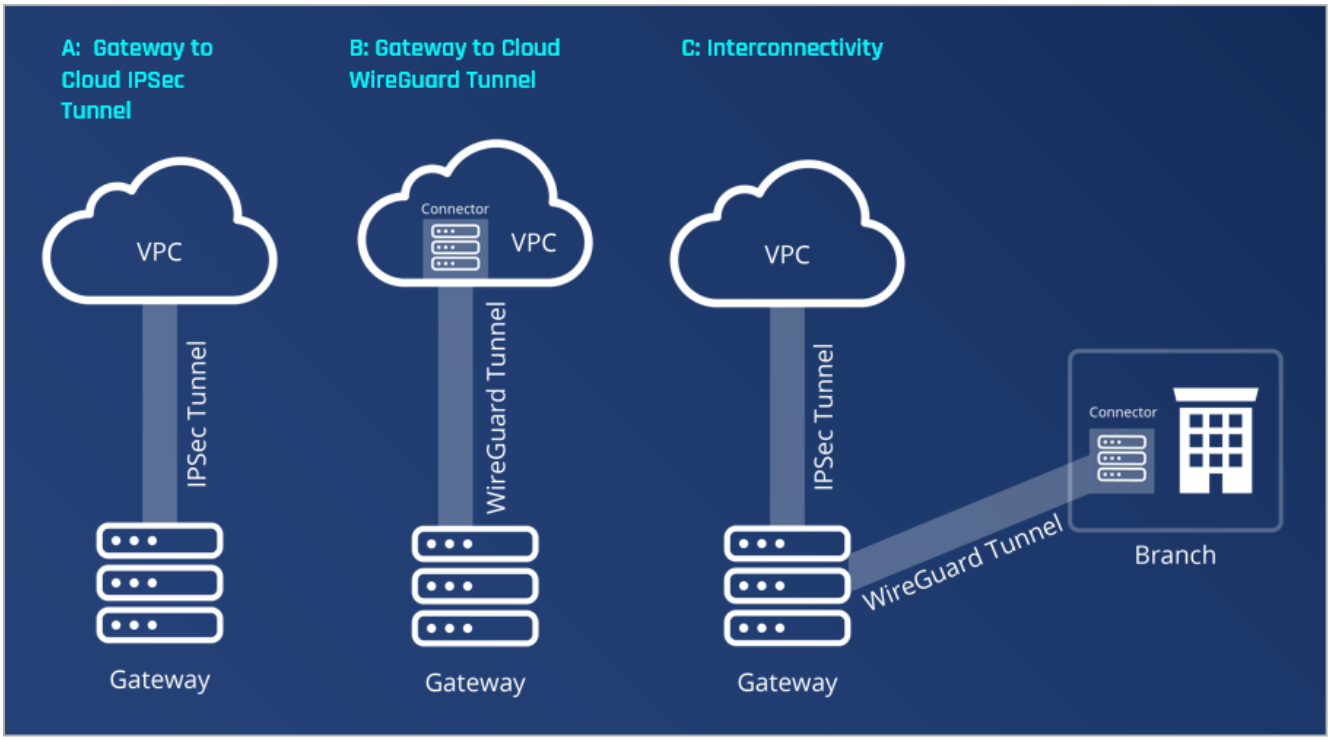



**Best Practice** - For redundancy, we recommend that you deploy the gateways in different regions depending on users' location.

# WireGuard Connector Tunnel

WireGuard Connector is a fast and modern VPN that utilizes state-of-the-art cryptography. It is designed as a general-purpose VPN to run on embedded interfaces and super computers alike.

This shows an example of tunnel usage in a network.




This table shows a comparison between Wireguard connector and IPSec tunnels.

# OpenVPN Tunnel

The OpenVPN protocol creates secure and private site-to-site connections using the SSL encryption. It is suitable in these scenarios:

- Incompatible operating system. For supported operating systems, see *"Downloading and Deploying the Harmony SASE Agent" on page 84*.
- You want to create a dedicated Harmony SASE connection with a single machine.
- The device does not support the Harmony SASE Agent.

**Caution** - The OpenVPN tunnel does not offer advanced security as the agent, such as Split Tunneling, DNS Filtering, Configuration Profiles, Firewall, Activity, SWG, DPC, and Single Sign-On.

# Internal Network Subnet

The Harmony SASE SASE network is designed according to internationally acknowledged standards and follows the RFC conventions regulated by the American internet authorities. To successfully incorporate Harmony SASE in your architecture, make sure that:

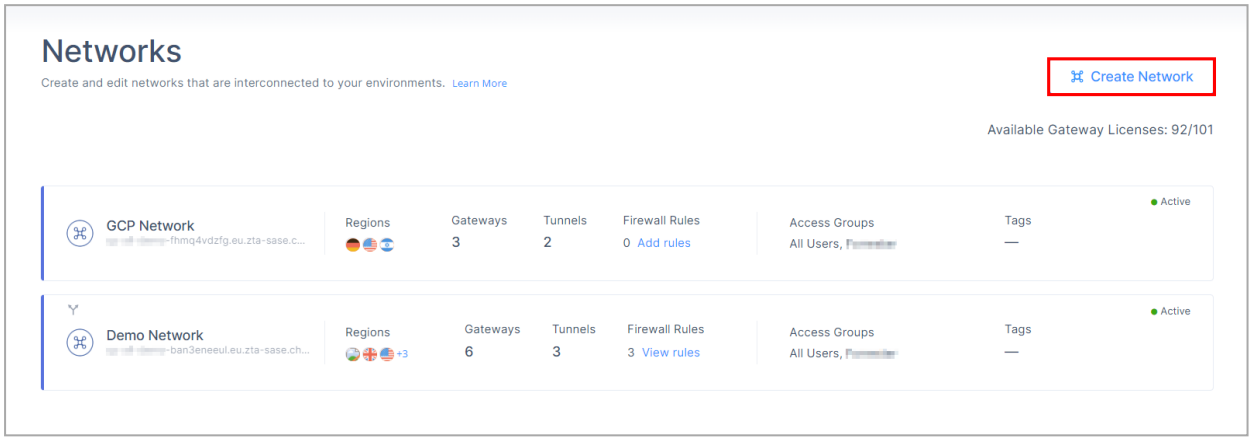
1. Your internal network follows industry-accepted design patterns.
2. Virtual Private Cloud (VPCs) or Data Centers (DC) with overlapping subnets do not reside in the same network.
3. Your Harmony SASE network subnet does not overlap with your network subnet.
4. (Highly Recommended) All subnet masks are either class B or C.
5. (Recommended) Your internal network has a static public IP.



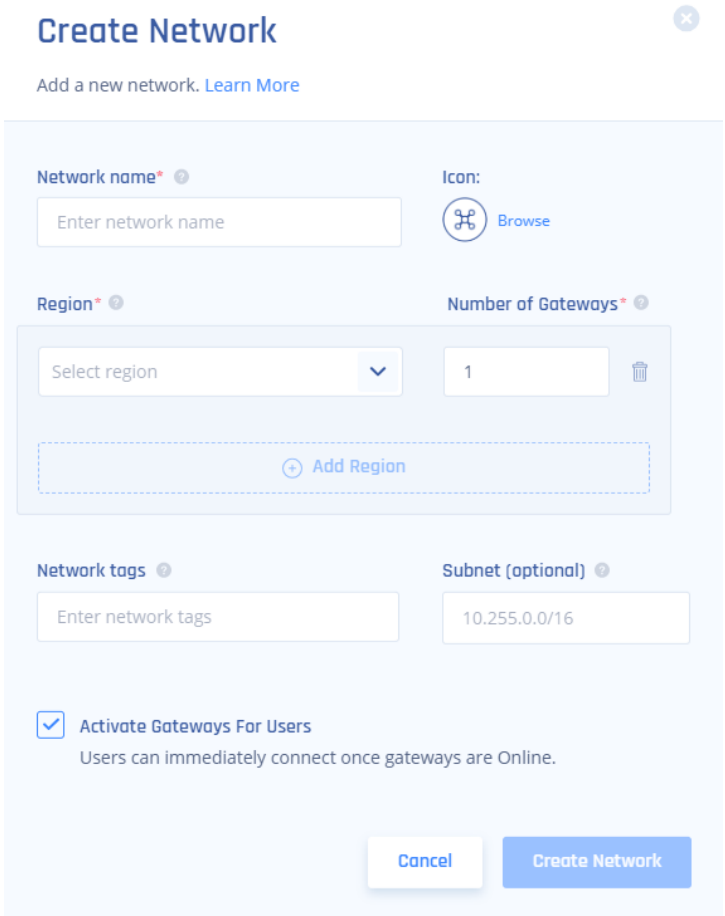
**Caution** - 192.168.1.0/24 and 10.0.0.0/24 are the most commonly used subnets for IoT applications.
If you connect to a site with this CIDR from a typical home location, it causes an IP conflict. Use 192.168.81.0/24 or 10.81.0.0/24 as the subnet to connect your site to Harmony SASE.

# Defining a Network

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click **Create Network**.




The **Create Network** window appears.




3. Enter these:

a. **Network name** - Name for your network. For example, HQ, Finance, or Staging.

b. **Icon** - Icon for your network.

   The default is . To change the icon, click **Browse** and select the icon.

c. **Region** - Region to deploy the Harmony SASE gateway.

   We recommend that you choose a region that is closest to your members.

d. **Number of Gateways** - The number of private gateways you want to deploy in the region.

   Make sure that the number does not exceed the purchased licenses.

e. To add another region, click **Add Region** and repeat steps c and d.

f. **Network Tags** - Network tags to identify the different purposes and/or teams that your Network supports.

g. **(Optional) Subnet** - Your network subnet IP address. The default is 10.255.0.0/16. For information on possible subnets and bit masks, see sk182225.

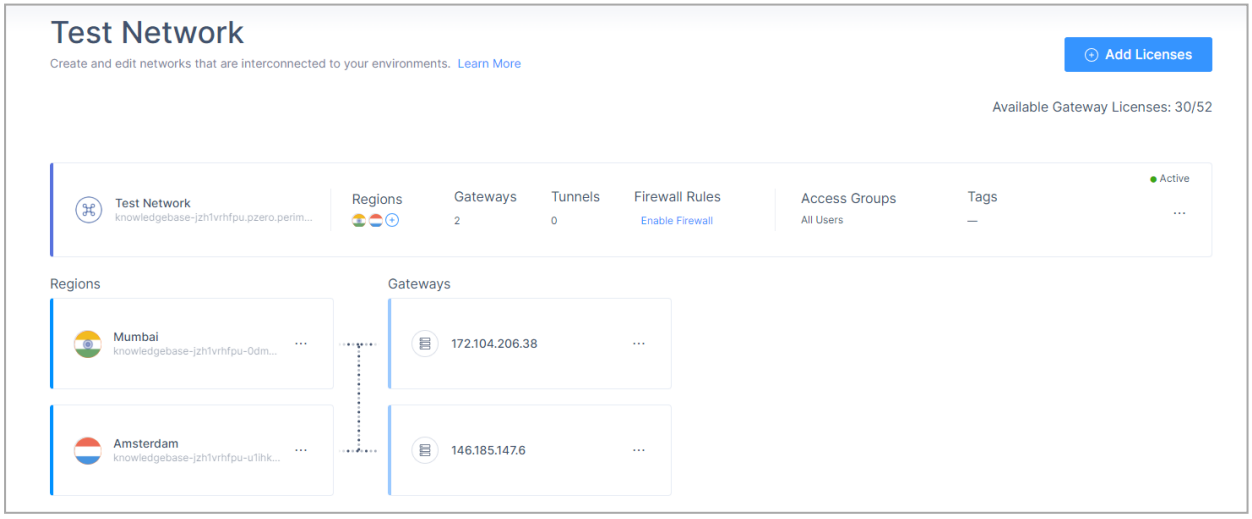
   **Warning** - You cannot change your subnet after you create your network. Make sure that the subnet does not overlap with your SD-WAN device's subnets.

4. The **Activate Gateways For Users** checkbox is selected by default. Clear it if you want to deactivate the gateway.

5. Click **Create Network**.

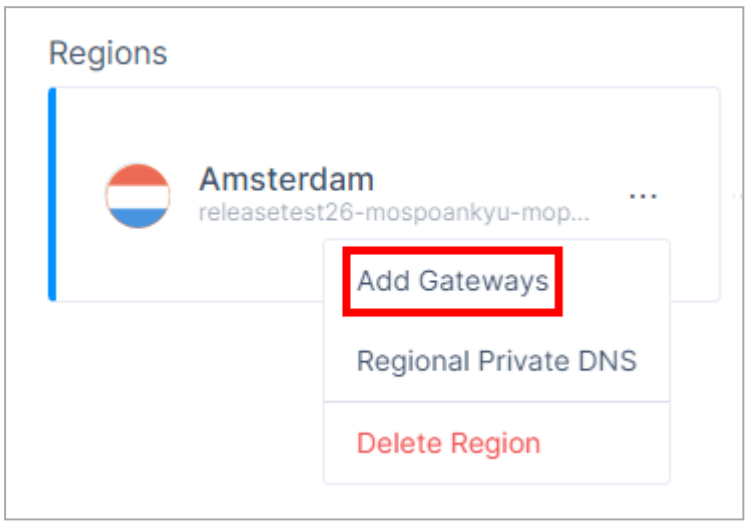
   The system creates the network and it is listed in the **Networks** page.

6. To view the network architecture, click the network name.

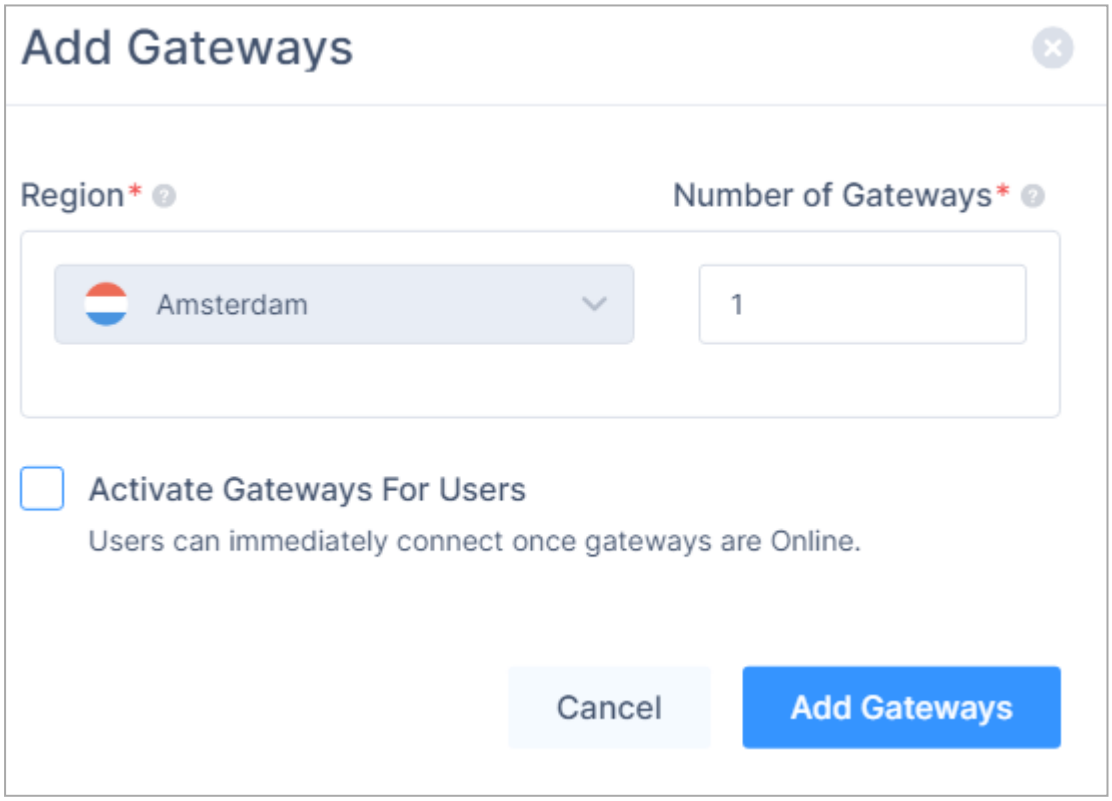


# Adding Gateways to an Existing Network

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· on your Region and then click **Add Gateways**.




The **Add Gateways** window appears.




The gateway is inactive by default.

4. To activate the gateway, select the **Activate Gateways For Users** checkbox.
5. Click **Add Gateways**.

# Deactivating a Gateway

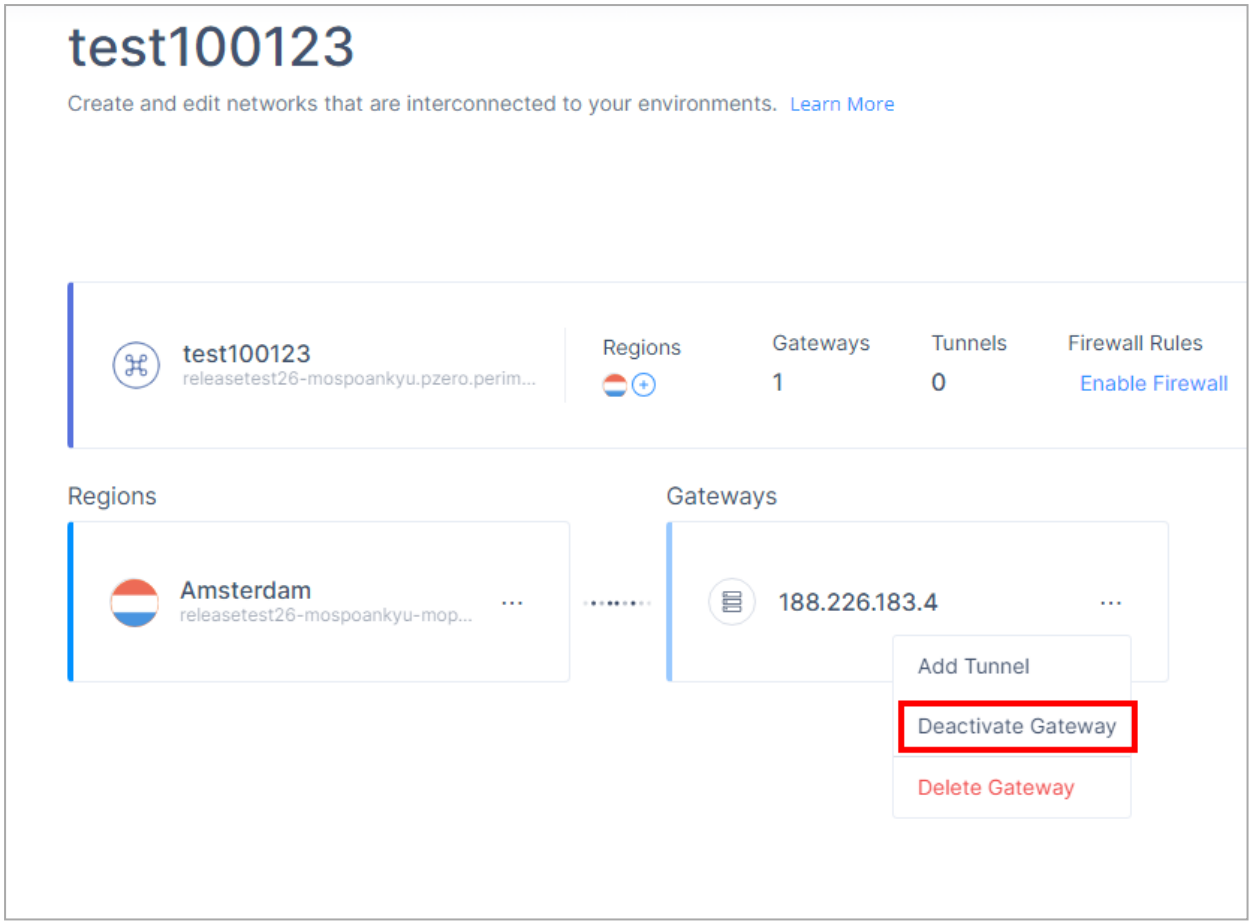
You can deactivate a gateway to block members from accessing the network resources (including Zero trust Applications) connected to the gateway. However, the gateway remains operational and configurable.

When you deactivate a gateway:

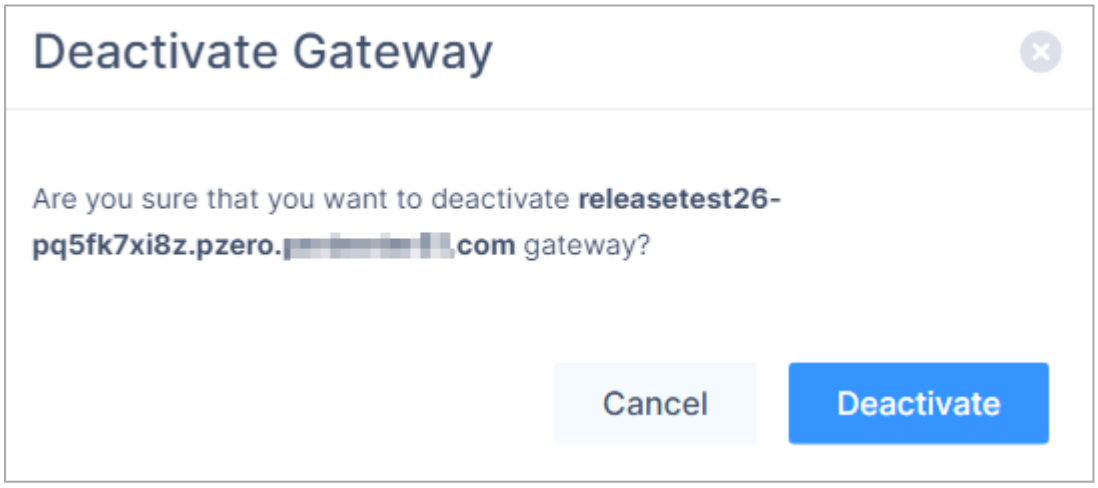
- Members and applications cannot connect to the gateway and are redirected to alternate gateways (if available).
- Members already connected to the gateway stay connected until they disconnect. After which, they are connected to an alternate gateway (if available).

**To deactivate a gateway:**

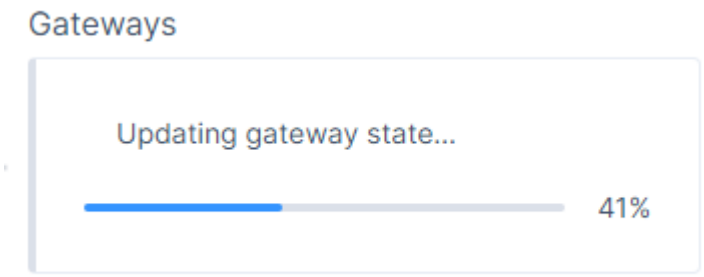
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· on your gateway and then click **Deactivate Gateway**.



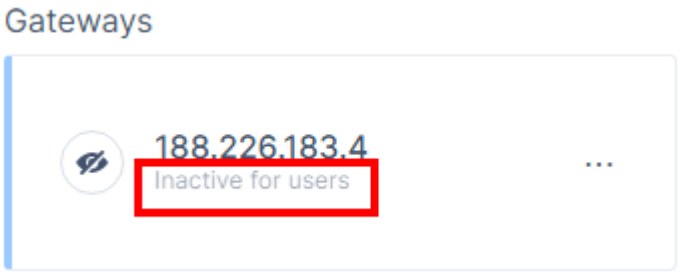

4. Click **Deactivate**.




The system shows the progress of the gateway status.




After the gateway is deactivated, it is marked as **Inactive for users**.




5. To re-activate your gateway, click ··· and then click **Activate Gateway**.

# Adding a Tunnel

Harmony SASE supports three types of tunnels:

- *"IPsec Site-2-Site VPN Tunnel" on page 122*
- *"WireGuard Connector Tunnel" on page 126*
- *"OpenVPN Tunnel" on page 132*

# IPsec Site-2-Site VPN Tunnel

## Prerequisites

Make sure your edge device (firewall or router) supports IPsec point to point tunnel using IKEv1 or IKEv2 protocols.

## IPSec Handshake

The IPSec Site-2-Site VPN tunnel employs a two-phase handshake.

### Phase I (IKE or Gateway)

This is the security association responsible for the external IP communication between the Harmony SASE network and the remote IP through the port 500/4500. The following information is required for Phase I. This information must match in both Harmony SASE and the remote side of the tunnel:

- **Shared Secret**
- **Public IP**
- **Remote ID**
- **IKE Version**
- **IKE Lifetime**
- **Encryption (Phase I)**
- **Integrity (Phase I)**
- **Diffie-Hellman Groups (Phase I)**

### Phase II (ESP or Tunnel):

This is the security association responsible for the internal LAN range or subnet handshake after establishing the IKE SA .

The following information is required for Phase II. This information must match in both Harmony SASE and the remote side of the tunnel:

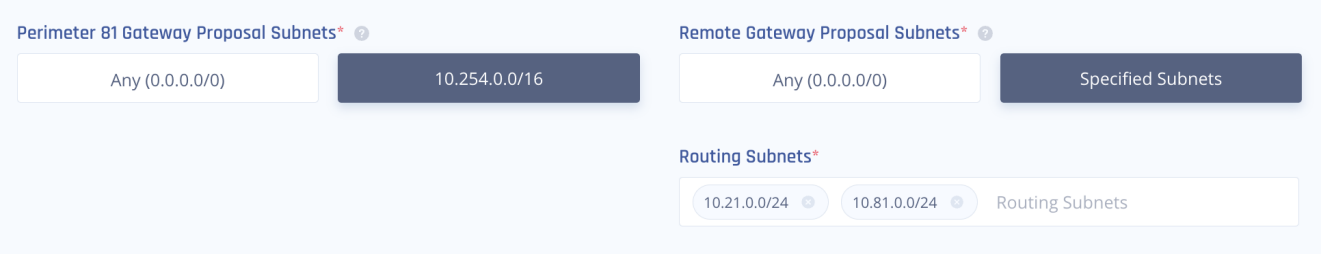
- **Harmony SASE Gateway Proposal Subnets**
- **Remote Gateway Proposal Subnets**
- **Tunnel Lifetime**
- **Dead Peer Detection (DPD)**
- **Encryption (Phase II)**

- **Integrity (Phase II)**
- **Diffie-Hellman Groups (Phase II)**

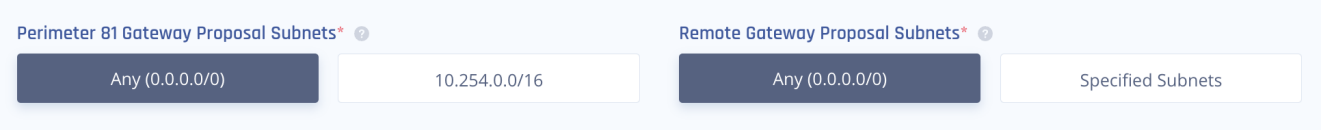
## Policy-Based and Route-Based IPSec Connection

Policy-based connection is easier to set up but is more vulnerable to IPSec tunnel value mismatch.

Depending on your device, a single missing subnet may cause the Phase II negotiation to fail.




Route-based connection is also known as a Tunnel Interface or VTI.




It is a more modern and stable method of IPSec tunneling. Once established, it uses one subnet (0.0.0.0/0) for the handshake, thereby reducing the chances of an error during renegotiation.

## Supported Integrations

| On-premises SD-WAN | | Cloud-based SD-WAN |
|---|---|---|
| Firewall | Router | |
| ■ *Barracuda Firewall*<br>■ *Check Point Firewall*<br>■ *Cisco ASA Firewall*<br>■ *Cisco Meraki Router*<br>■ *FortiGate Next Generation Firewall*<br>■ *Juniper Networks ScreenOS Firewall*<br>■ *Juniper (JunOS) SRX*<br>■ *Palo Alto Firewall*<br>■ *pfSense Firewall*<br>■ *SonicWall Firewall*<br>■ *Sophos XG Firewall*<br>■ *UniFi USG Firewall*<br>■ *WatchGuard Firewall*<br>■ *Zyxel USG Firewall* | ■ *Cisco Meraki Router*<br>■ *D-Link DSR Series Router*<br>■ *DrayTek Vigor2862 Router*<br>■ *DrayTek Vigor3900 Router*<br>■ *EdgeMax Router*<br>■ *Linksys Router*<br>■ *Netgear BR500 Router* | **Single Tunnel**<br>■ *AWS Virtual Gateway*<br>■ *AWS Transit Gateway*<br>■ *Google Cloud Platform*<br>■ *Azure Virtual Network Gateway*<br>**Redundant Tunnels**<br>■ *AWS Redundant Tunnels - Virtual Private Gateway*<br>■ *AWS Redundant Tunnels - Transit Gateway*<br>■ *Google Cloud Platform Redundant Tunnels*<br>■ *Azure Redundant Tunnels - Virtual Network Gateway*<br>■ *Azure Redundant Tunnels - Virtual WAN*<br>**Other Cloud Options**<br>■ *Alibaba Cloud*<br>■ *Heroku Enterprise*<br>■ *IBM Cloud* |

## High-Level Procedure

1. Make sure you have the required prerequisites.
2. Configure the tunnel in the Harmony SASEAdministrator Portal.

3. Configure the required Firewall / Router / Cloud Management Portal:

| On-premises | | Cloud-based Resource |
|---|---|---|
| Firewall | Router | |
| ■ *Barracuda Firewall*<br>■ *Check Point Firewall*<br>■ *Cisco ASA Firewall*<br>■ *Cisco Meraki Router*<br>■ *FortiGate Next Generation Firewall*<br>■ *Juniper Networks ScreenOS Firewall*<br>■ *Juniper (JunOS) SRX*<br>■ *Palo Alto Firewall*<br>■ *pfSense Firewall*<br>■ *SonicWall Firewall*<br>■ *Sophos XG Firewall*<br>■ *UniFi USG Firewall*<br>■ *WatchGuard Firewall*<br>■ *Zyxel USG Firewall* | ■ *Cisco Meraki Router*<br>■ *D-Link DSR Series Router*<br>■ *DrayTek Vigor2862 Router*<br>■ *DrayTek Vigor3900 Router*<br>■ *EdgeMax Router*<br>■ *Linksys Router*<br>■ *Netgear BR500 Router* | **Single Tunnel**<br>■ *AWS Virtual Gateway*<br>■ *AWS Transit Gateway*<br>■ *Google Cloud Platform*<br>■ *Azure Virtual Network Gateway*<br>**Redundant Tunnels**<br>■ *AWS Redundant Tunnels - Virtual Private Gateway*<br>■ *AWS Redundant Tunnels - Transit Gateway*<br>■ *Google Cloud Platform Redundant Tunnels*<br>■ *Azure Redundant Tunnels - Virtual Network Gateway*<br>■ *Azure Redundant Tunnels - Virtual WAN*<br>**Other Cloud Options**<br>■ *Alibaba Cloud*<br>■ *Heroku Enterprise*<br>■ *IBM Cloud* |

4. Verify the setup.

# WireGuard Connector Tunnel

## Prerequisites

A Linux machine with these specifications:

- **Kernel**: Any of these packages installed:
  - Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS, 23.04
  - CentOS 7, or CentOS 8 (RedHat distributions)
- **Packages installed**:
  - Ubuntu - curl; dig; software-properties-common
  - CentOS - curl, bind-utils
- 20 GB free disk space
- 2 GB RAM
- Static internal IP address
- Network adapter that supports bridge connection.

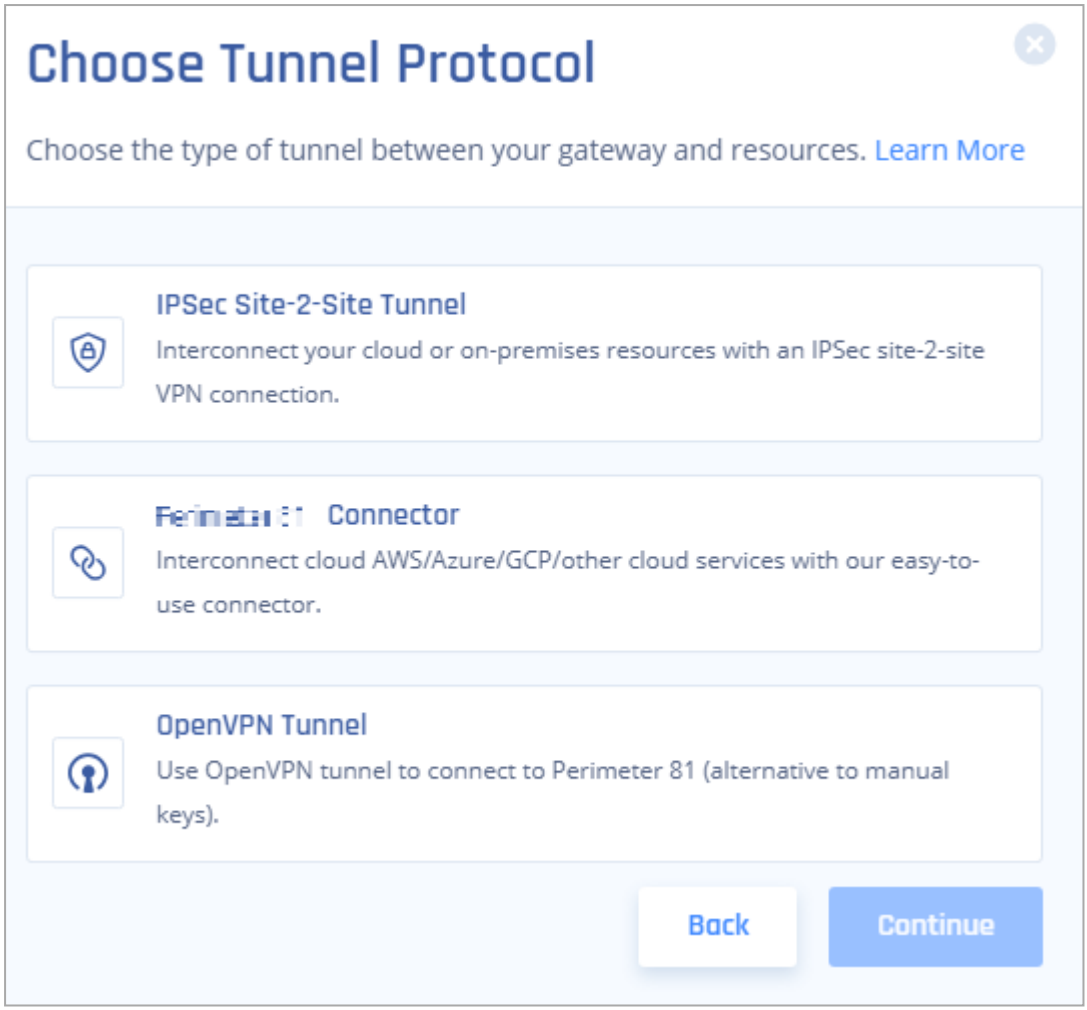
  **Note** - For Linux deployed on a Windows host, enable virtualization on Windows BIOS.

## Configuring a WireGuard Connector Tunnel

### Configuring the Connector in the Harmony SASE Administrator Portal

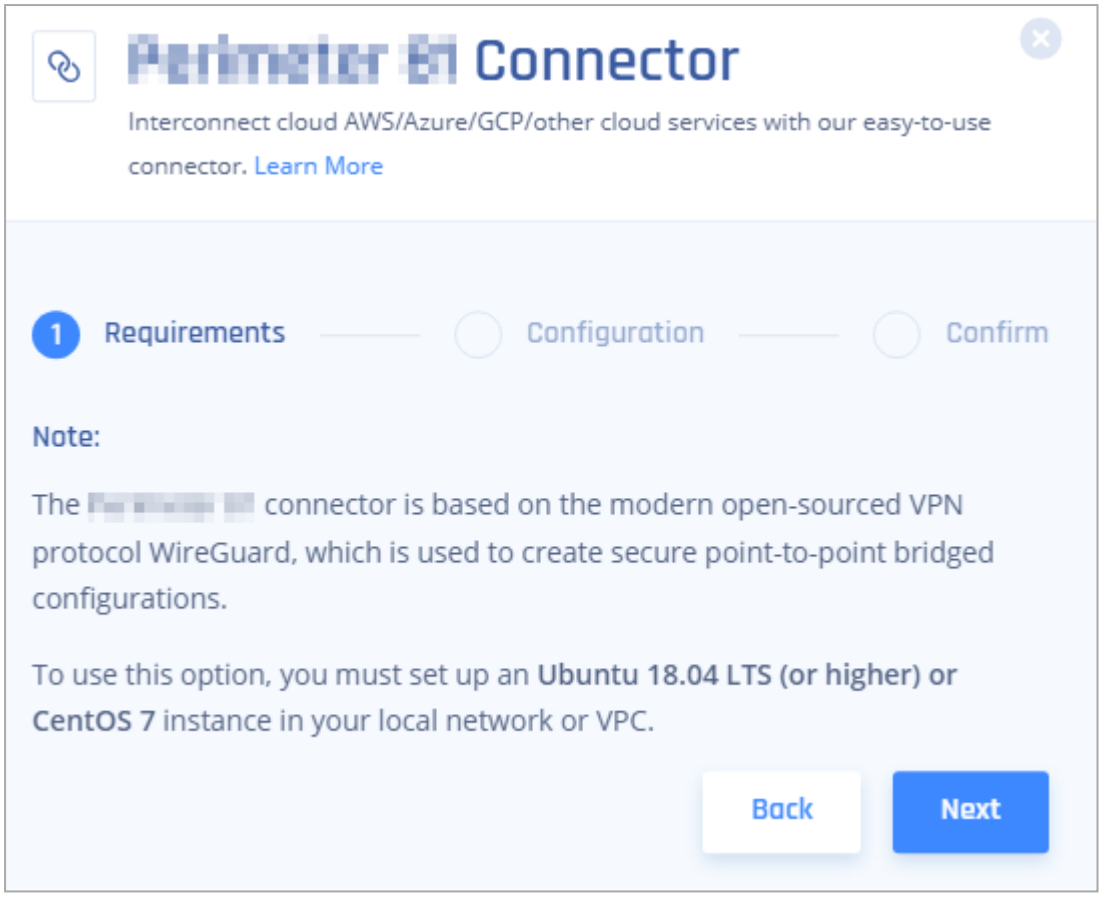
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. For the gateway to which you want to add the WireGuard Connector tunnel, click ··· and click **Add Tunnel**.

   The **Choose Tunnel Protocol** window appears.




4. Select **WireGuard Connector** and click **Continue**.

   The **Harmony SASE Connector** window appears.

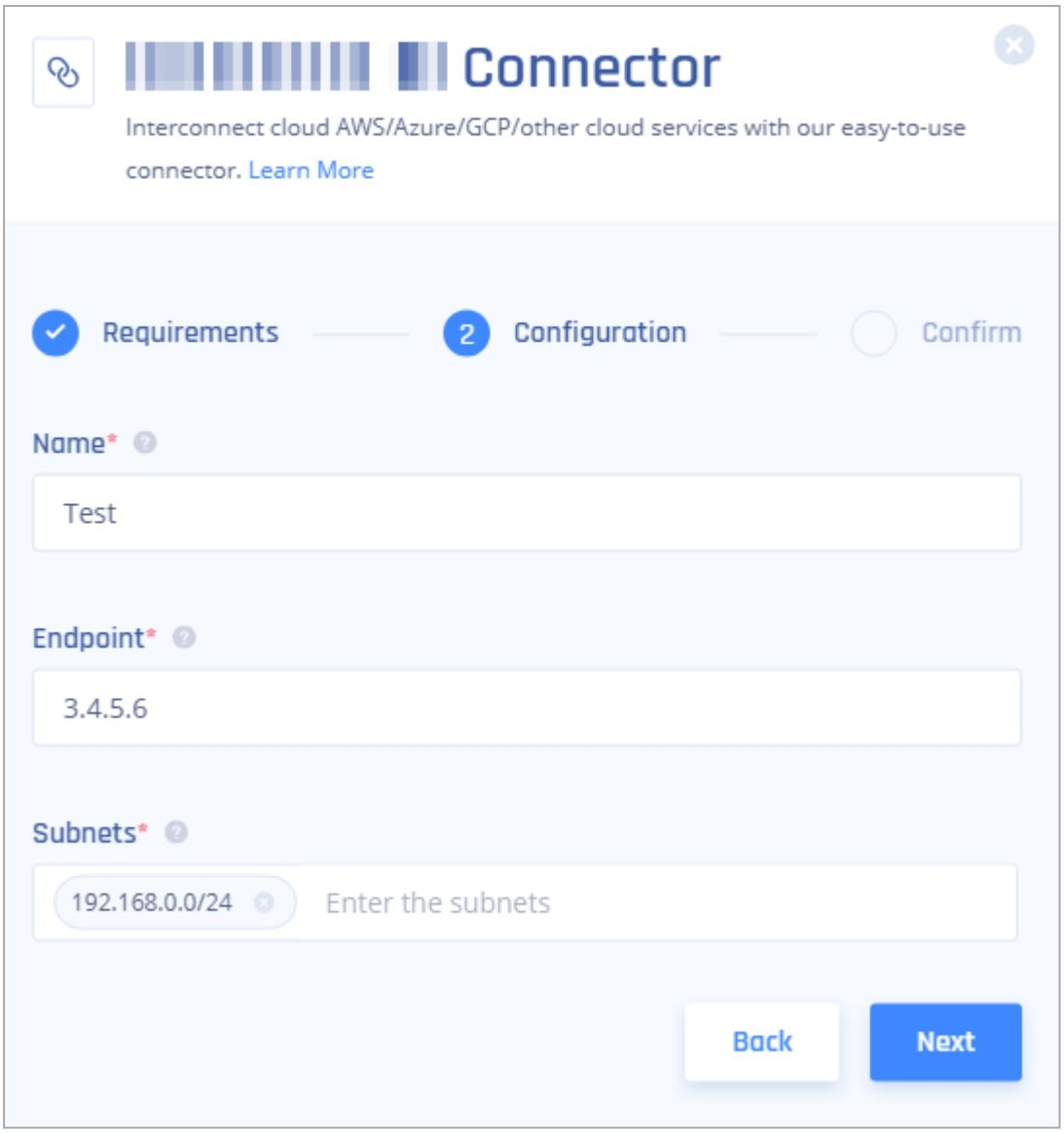



5. In the **Requirements** section, read the requirements and make sure they are met. Click **Next**.
6. In the **Configuration** section, enter these:
   a. **Name** - Name for the connector.
   b. **Endpoint** - IP address of the Linux server that has the WireGuard Connector installed.

      If you are using a dynamic public IP address, enter 0.0.0.0

      **Note** - If you do not know the IP address, query the server by running this command in your Linux terminal:
      `dig +short myip.opendns.com @resolver1.opendns.com`

c. **Subnets** - Subnets of your local network.




d. Click **Next**.

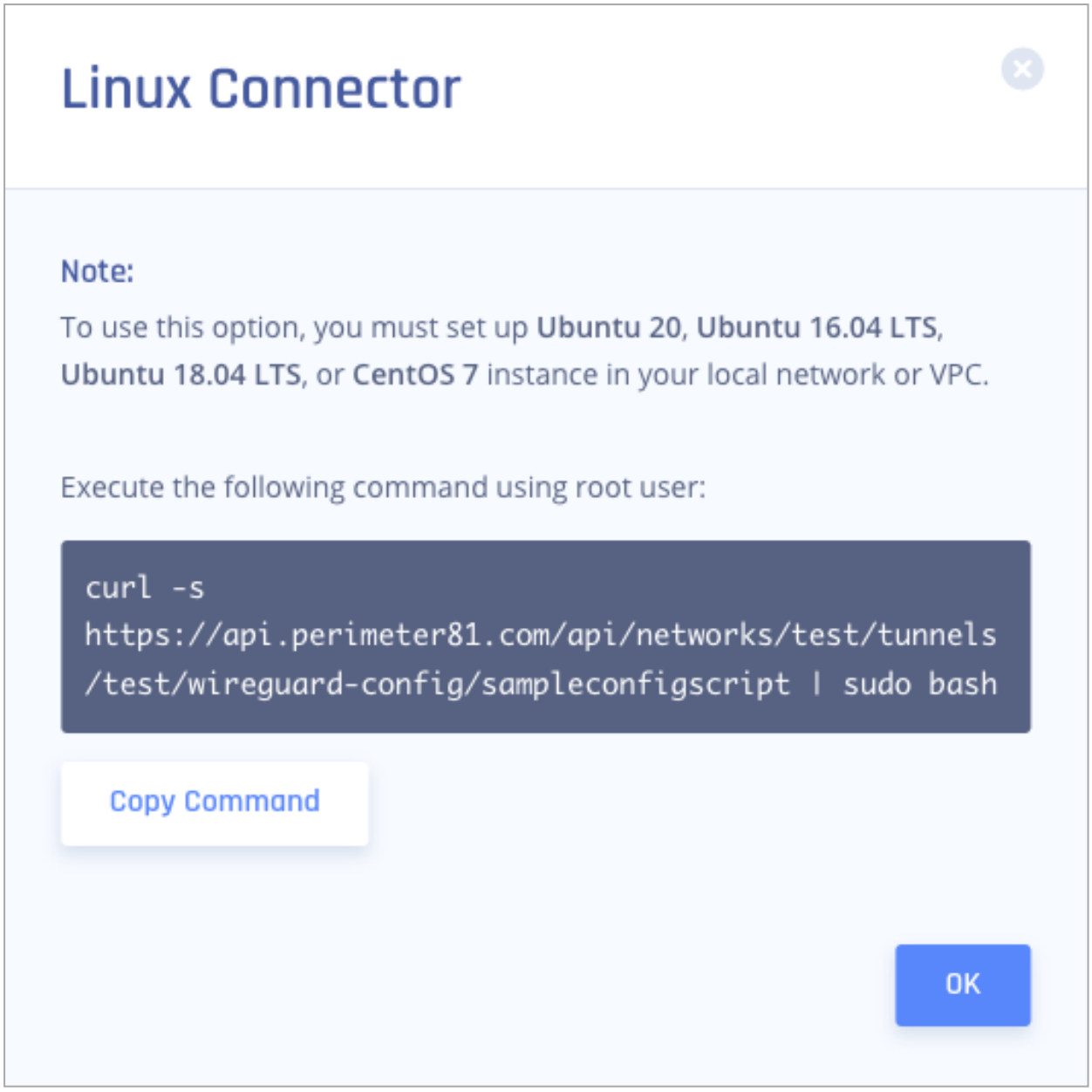
7. In the **Confirm** section, click **Apply**.

   After deployment, the connector appears in the **Networks** page.

### Installing the WireGuard Connector on a Linux Server

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click ··· for the WireGuard Connector tunnel that you just configured and then click **Configuration**.

   The **Linux Connector** window appears.




3. Click **Copy Command**.

   **Note** - The command is unique to each connector.

4. Open the Linux terminal and connect as Root user.
5. Run the copied command.
6. Select **Yes** at Stage 4 for access or mode - **Remote Access only** and follow the instructions to install the connector.

### Verifying the Setup

1. Connect to your network using the Harmony SASE Agent on a device.
2. Open the command line and run:

```
ping <Internal resource IP address>
```

3. If the command fails, make sure that port UDP/8000 is not blocked in your firewall/router, and that you have followed all the steps.
4. If the issue persists, on the Linux server, collect these logs and contact *Check Point Support*. The logs are available in:

```
##Configuration file
/etc/wireguard/wg0.conf

##Connection logs
/tmp/p81-wg-connector.log
```

## Removing the WireGuard Connector

Connect to the command line of Linux server where you have installed the WireGuard Connector and run:

```
# Locate the WireGuard packages # (the output of this command will
show you all wireguard packages installed on the machine)
dpkg -l | grep wireguard

# Delete all packages found that are associated with WireGuard
# (Run this command for each package found, replace  with the output
from the previous command)
apt-get remove --purge # Locate the WireGuard packages # (the output
of this command will show you all wireguard packages installed on the
machine)
dpkg -l | grep wireguard
```

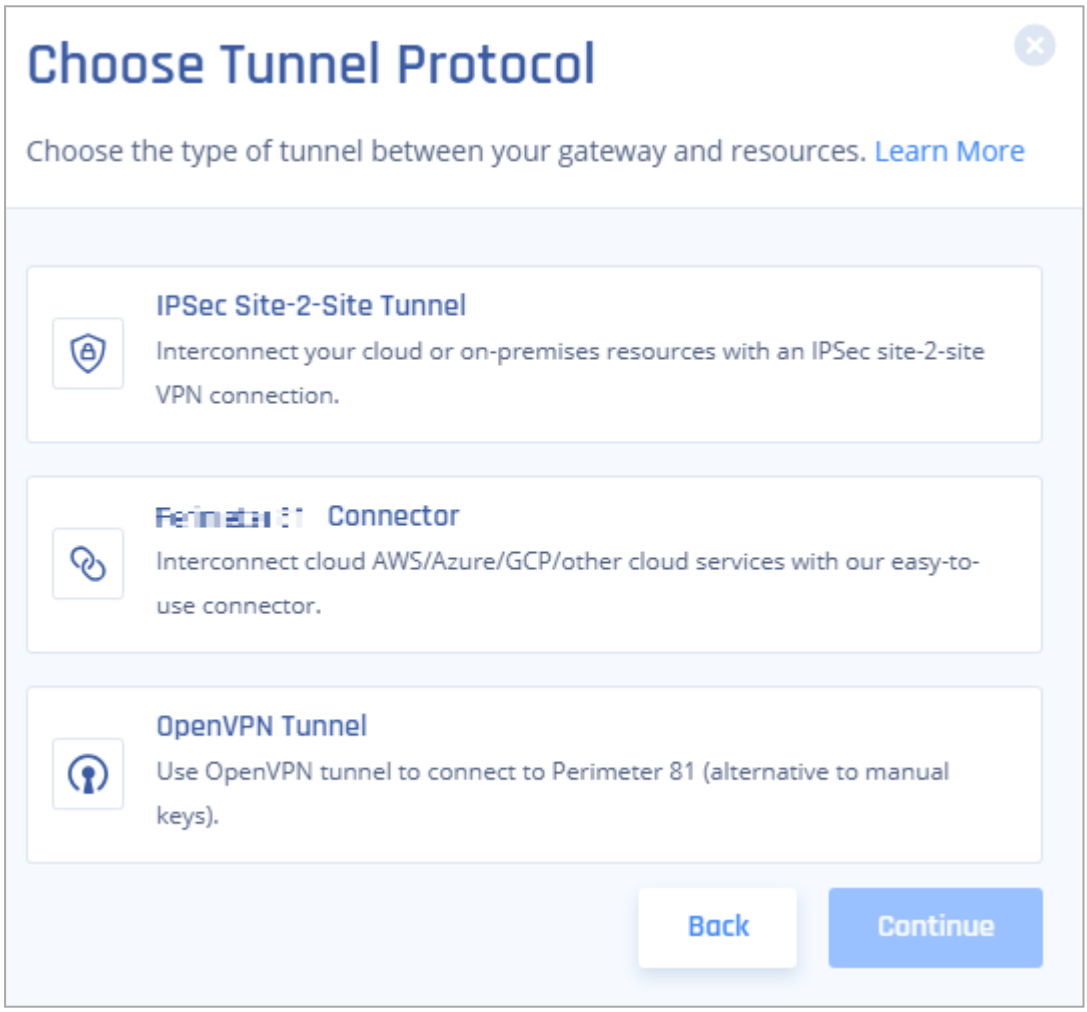
```
# Locate the WireGuard packages # (the output of this command will
show you all wireguard packages installed on the machine)
yum list installed | grep wireguard

# Delete all packages found that are associated with WireGuard# (Run
this command for each package found, replace  with the output from the
previous command)
yum remove # Locate the WireGuard packages # (the output of this
command will show you all wireguard packages installed on the machine)
yum list installed | grep wireguard
```

# OpenVPN Tunnel

## Configuring the OpenVPN Tunnel in the Harmony SASE Administrator Portal

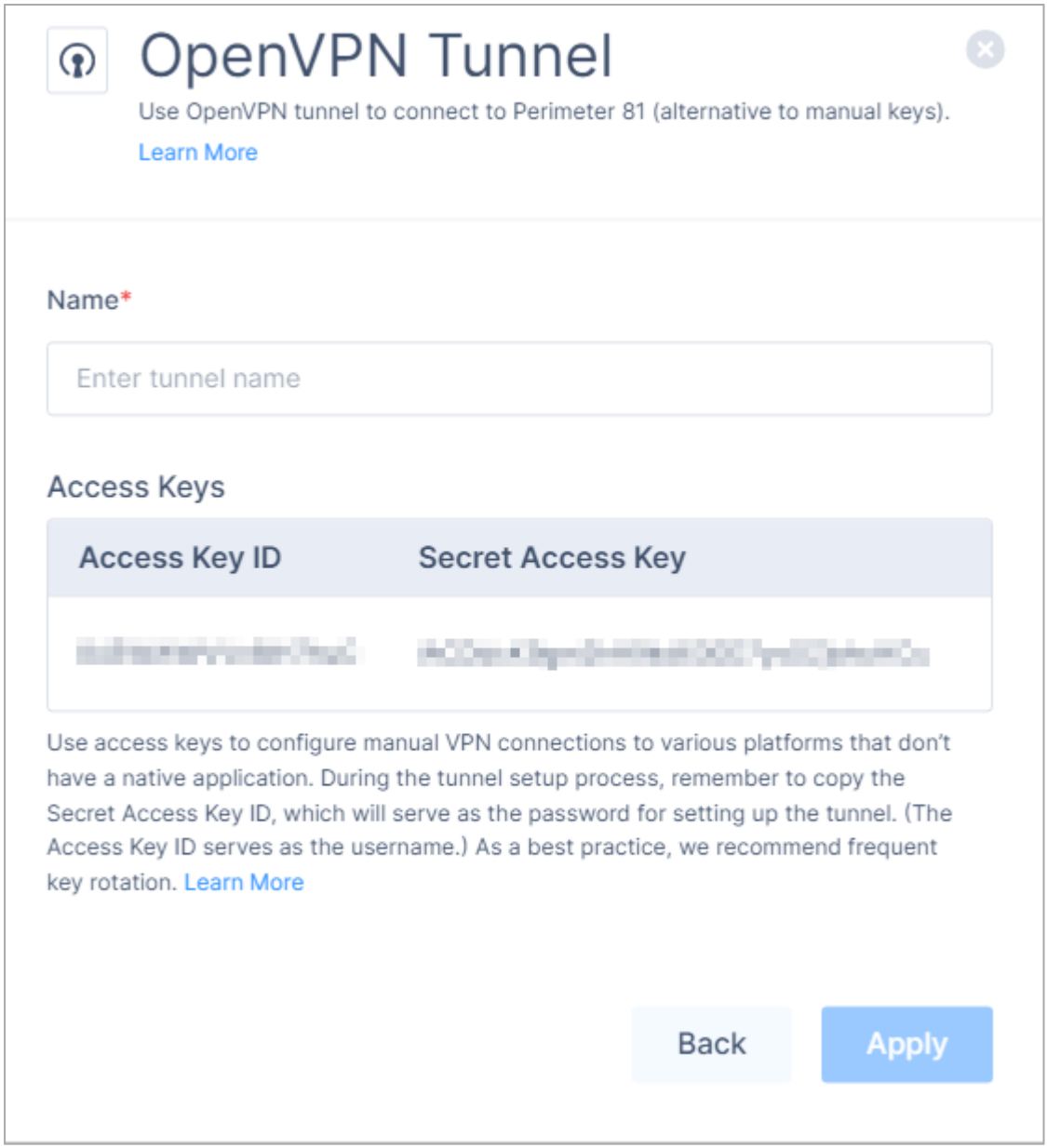
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. For the gateway to which you want to add the OpenVPN tunnel, click ··· and click **Add Tunnel**.

   The **Choose Tunnel Protocol** window appears.




4. Select **OpenVPN Tunnel** and click **Continue**.

   The **OpenVPN Tunnel** window appears.

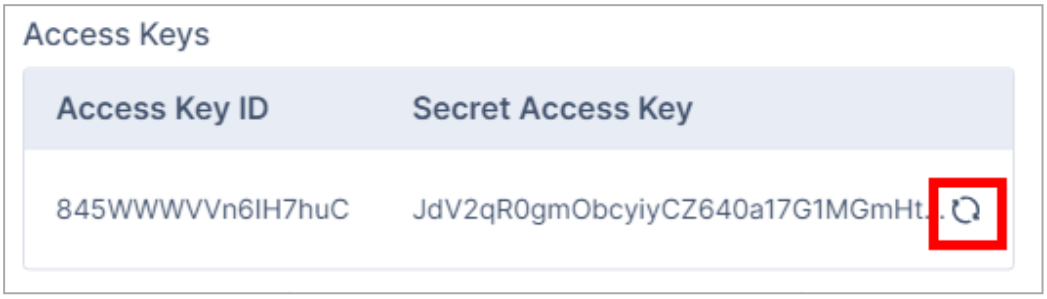



5. In the **Name** field, enter a name for the tunnel.
6. Save the **Access Keys** credentials.

**Caution** - Save the Access Keys credentials before you click **Apply**. Otherwise, regenerate the Access Keys:

a. To regenerate the Access Keys, in the newly created OpenVPN tunnel, click ··· > **Edit Tunnel**.

b. In the **Access Keys** section, click ↻.

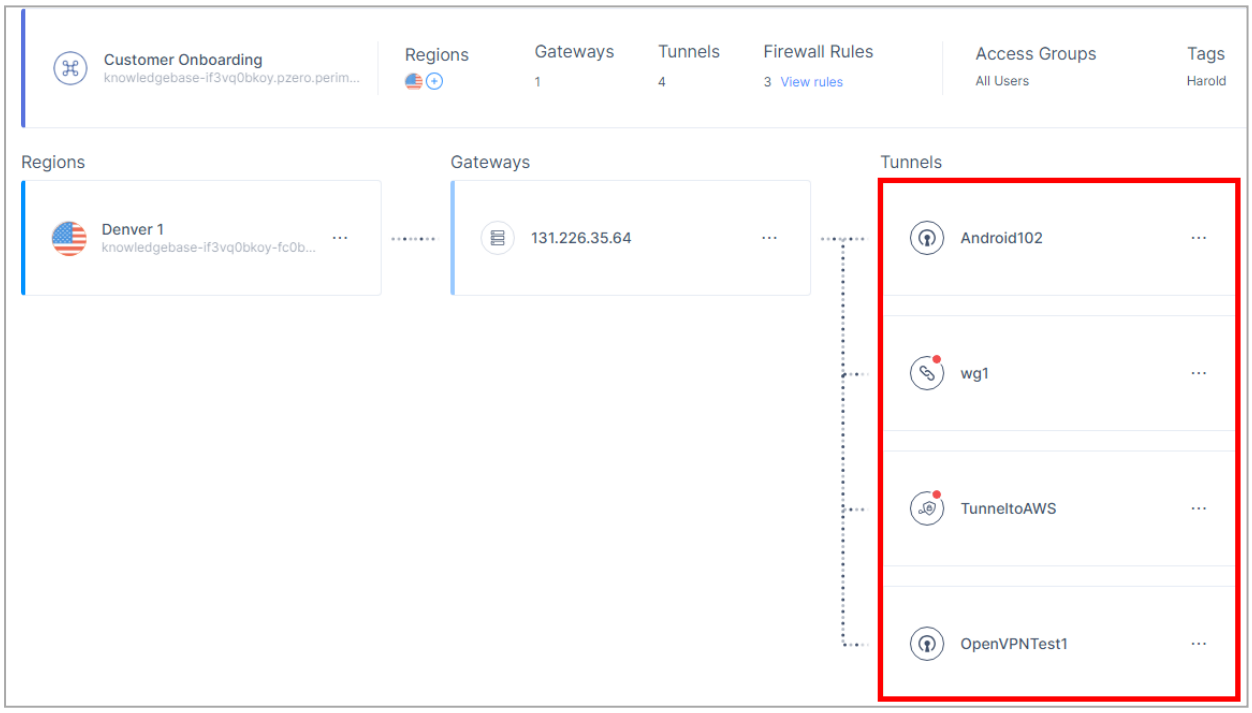



The system regenerates the **Access Key ID** and **Secret Access Key** values.

c. Click **Apply**.

7. Click **Apply**.

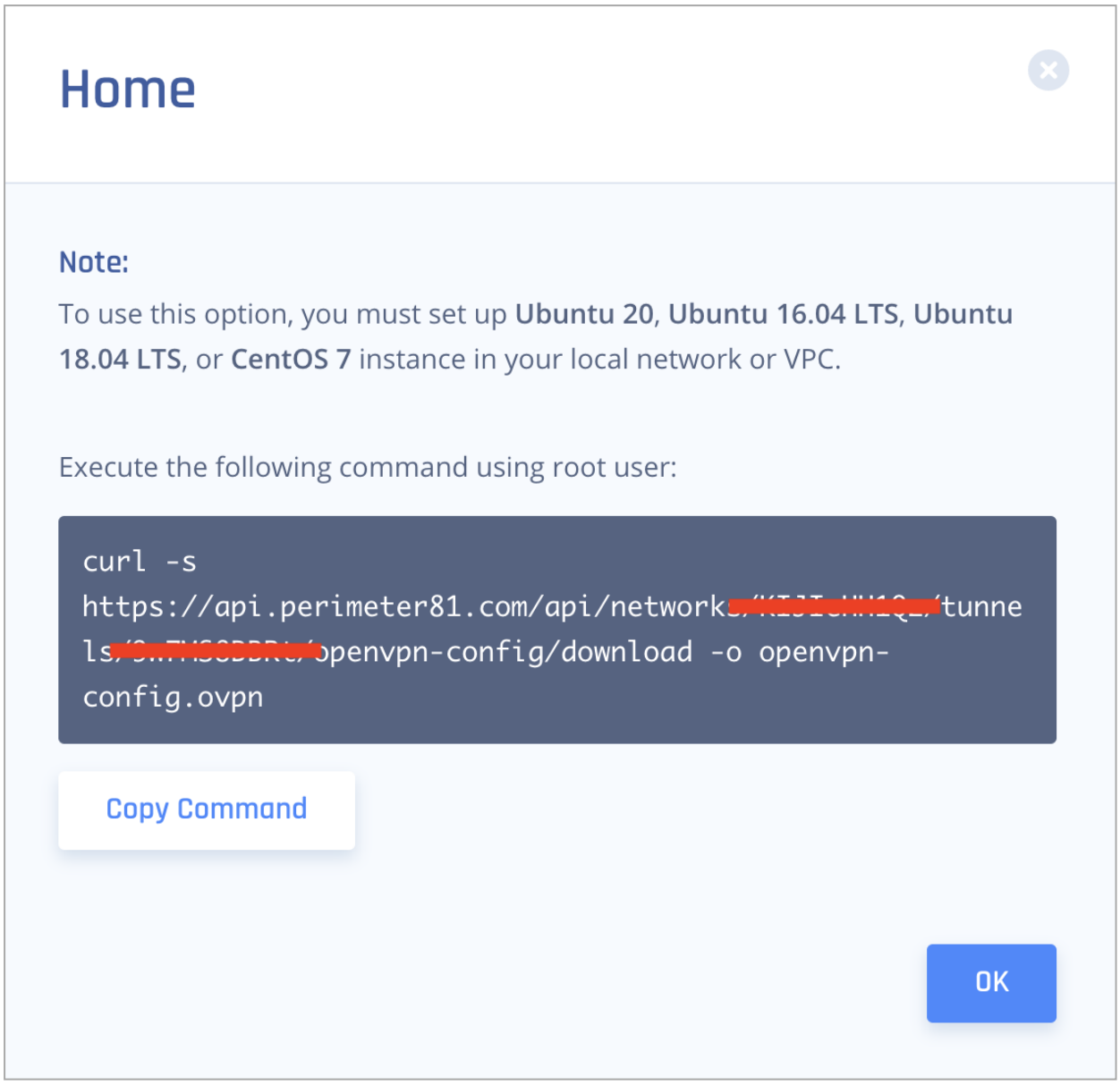
The system creates an OpenVPN tunnel and displays it in the **Tunnels** section.




## Installing a VPN and Configuring the OpenVPN Tunnel on the Device

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.

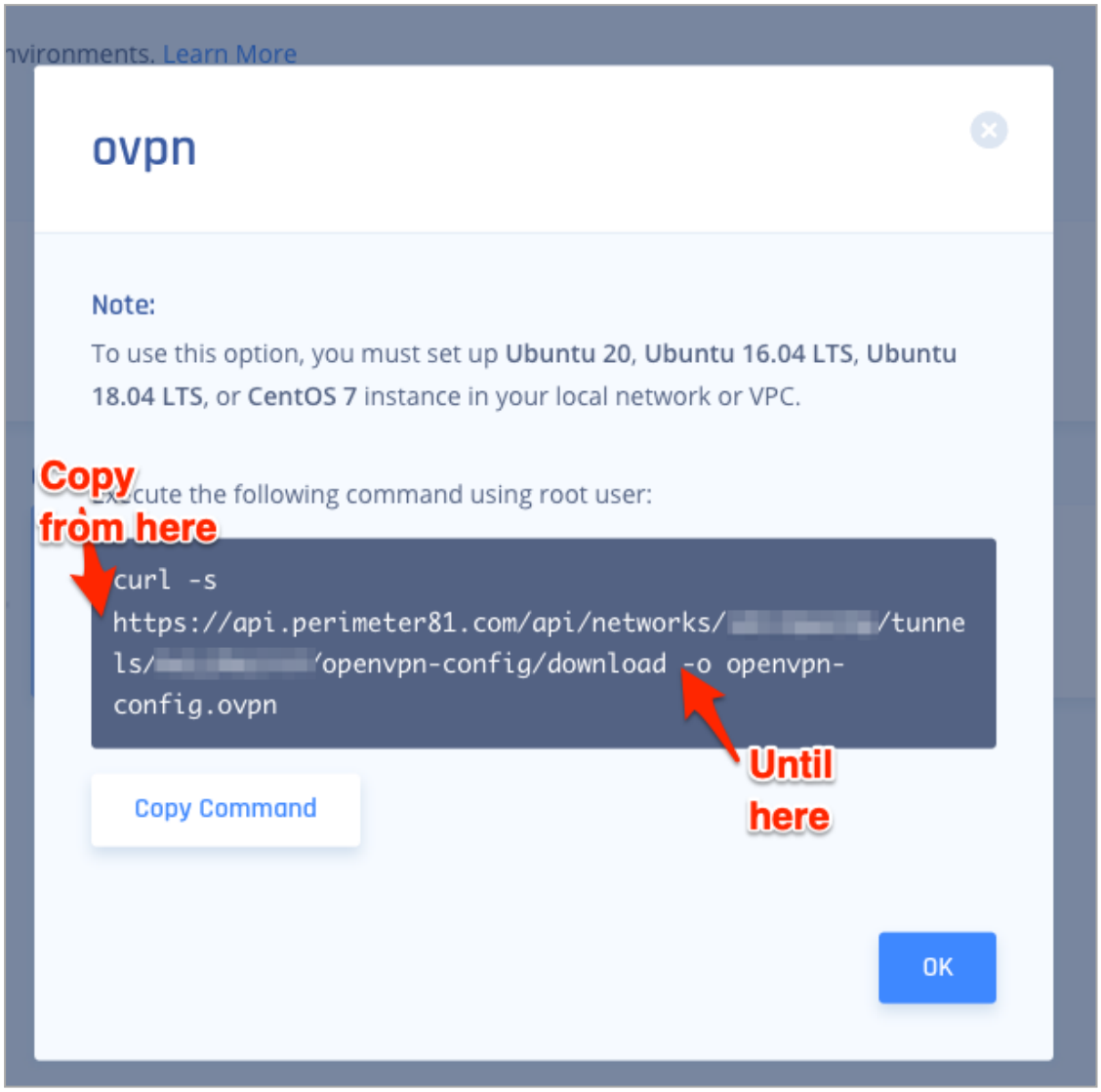
3. In the gateway where you added the OpenVPN tunnel, click ··· and then click **Configuration**.




4. Copy the command and run it in the terminal window on the device.

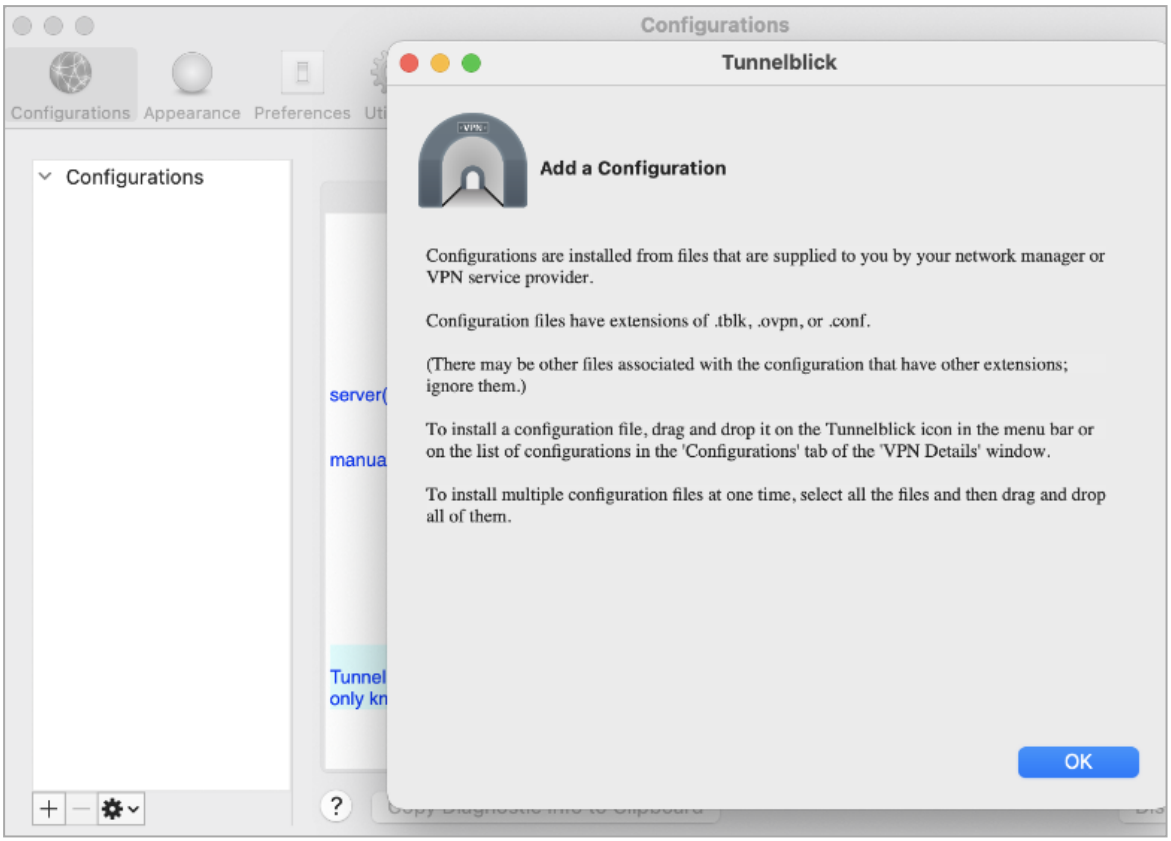
   The system downloads the *saferx-openvpn-client.pvpn* configuration file.

**Note** - If the device's operating system does not support a terminal window, copy the command from `https` until `download`. Paste the command in a browser address bar and press **Enter**. The system downloads the *saferx-openvpn-client.ovpn* configuration file.



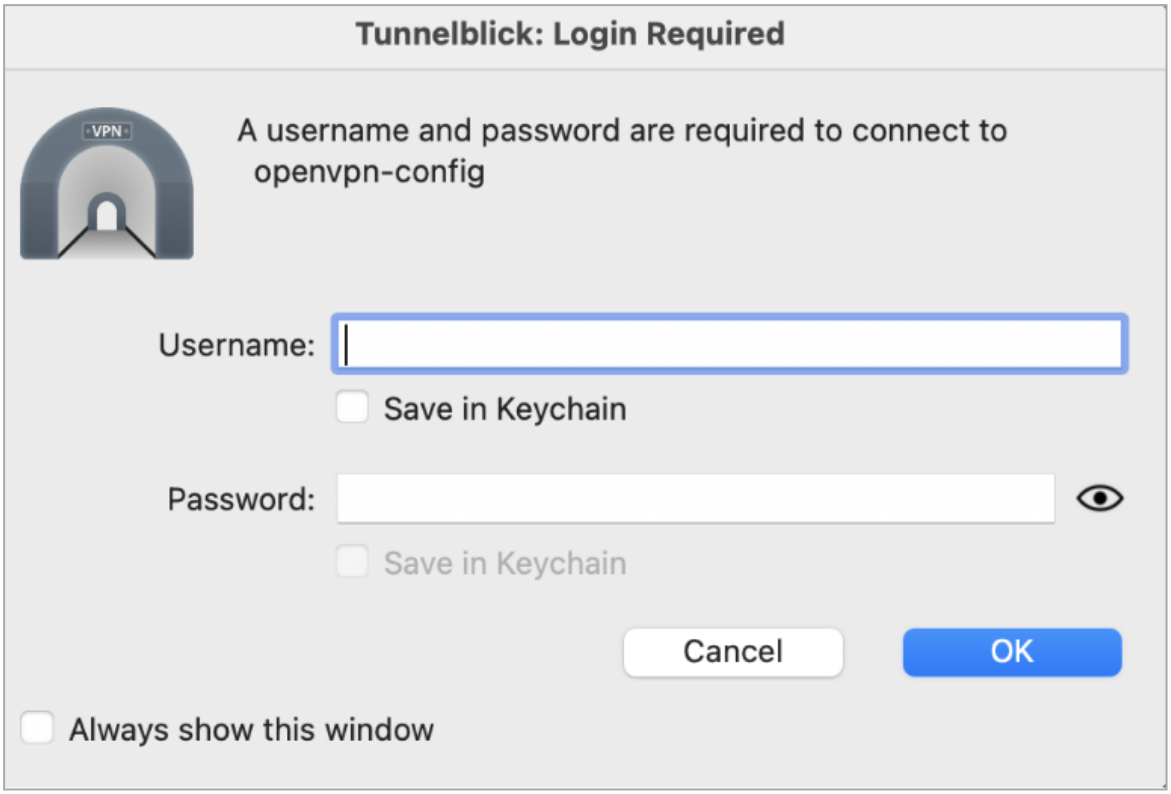

5. On a macOS device:
    a. Download and install a VPN client. Check Point recommends Tunnelblick VPN client.

b. Drag and drop the *openvpn-config.ovpn* file into the client to add the configuration.




c. To connect to the VPN, in the **Username** field, enter the **Access Key ID** that you copied when you created the tunnel.

d. In the **Password** field, enter the **Secret Access Key** that you copied when you created the tunnel.

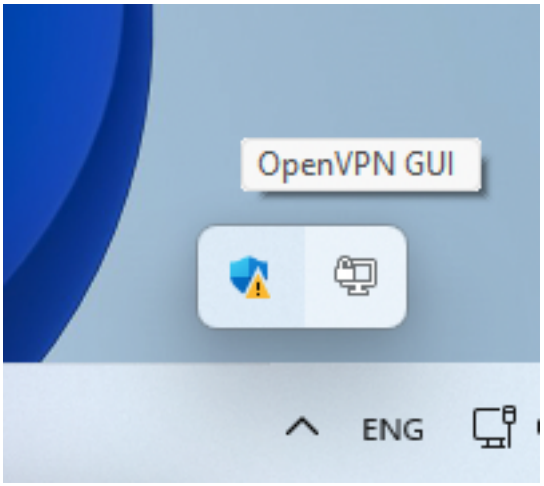



e. Click **OK**.

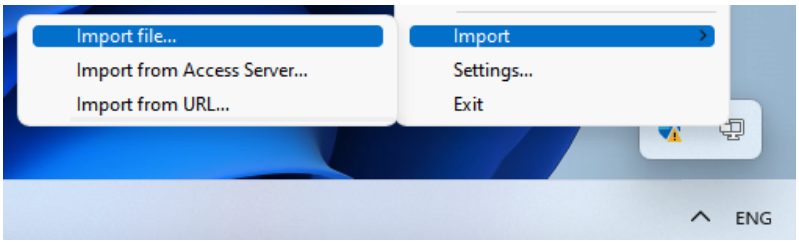
6. On a Windows device:

a. Download and install the OpenVPN Client. Check Point recommends https://openvpn.net/community-downloads/

b. Click the **OpenVPN** icon.



c. Click **Import** > **Import file...**



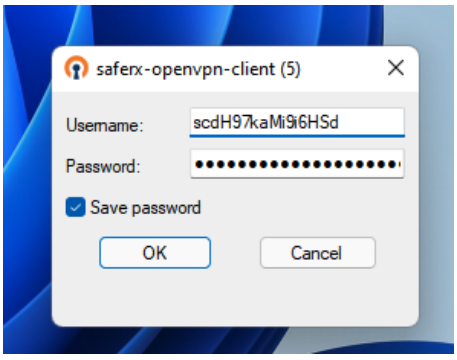

d. Select the downloaded file *saferx-openvpn-client.ovpn*

e. After you import the file, right-click the OpenVPN client and then click **Connect**.




The OpenVPN client window appears.

f. In the **Username** field, enter the **Access Key ID** that you copied when you created the tunnel.




g. In the **Password** field, enter the **Secret Access Key** that you copied when you created the tunnel.

**Note** - If the **Secret Access Key** starts with *$6$perimeter81$*, it indicates that the key is encrypted.
Regenerate the access keys. See step 6 in *"Configuring the OpenVPN Tunnel in the Harmony SASE Administrator Portal" on page 132*.

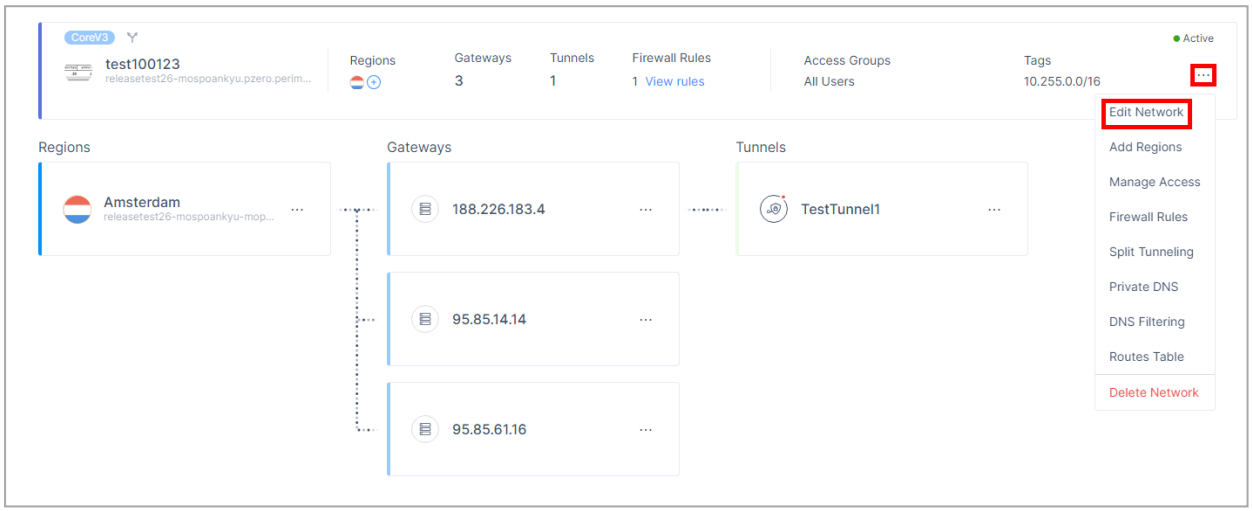
# Verifying the Setup

1. In the Harmony SASE Administrator Portal, click **Networks** and verify that the tunnel is up.
2. In the Harmony SASE Agent, connect to the network and access a resource. If you are unable to connect to the resource, contact *Check Point Support*.

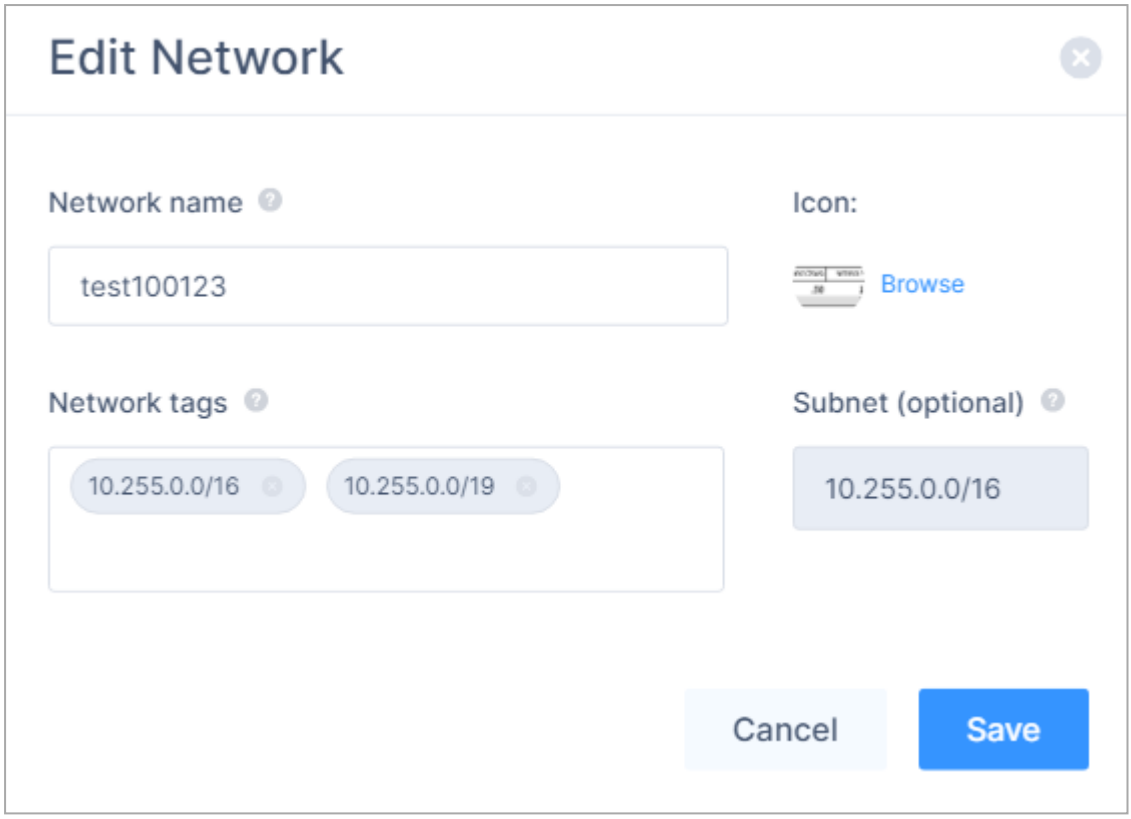
# Managing a Network

## Editing a Network

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Edit Network**.



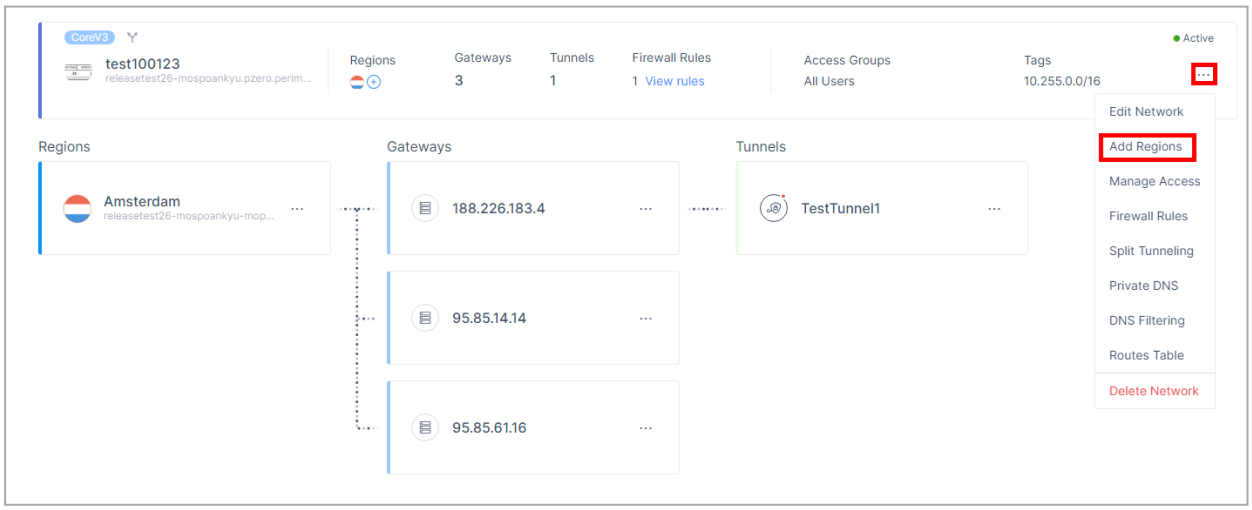

The **Edit Network** window appears.



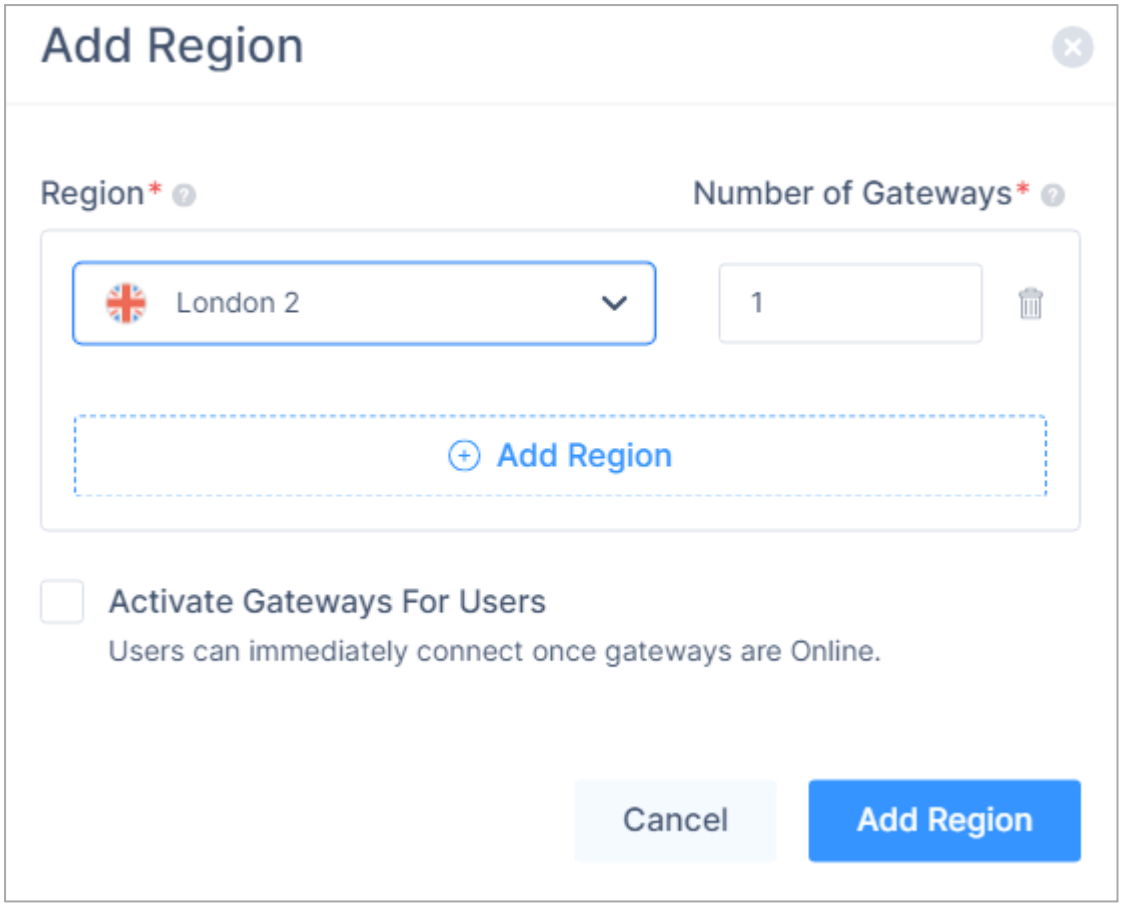

4. Make the required changes and click **Save**.

# Adding Regions

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Add Regions**.




The **Add Region** window appears.



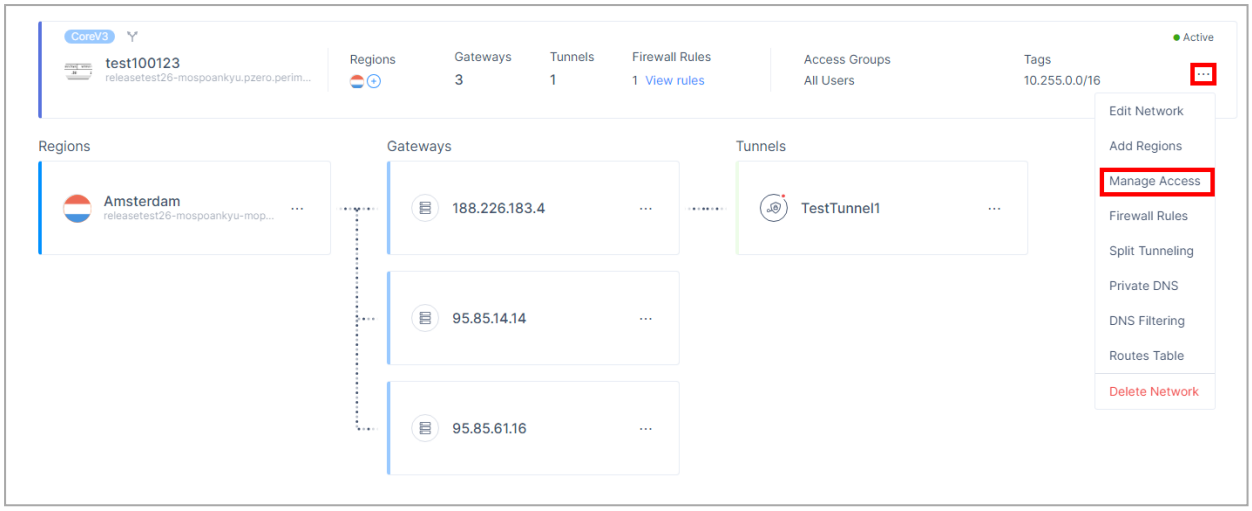

4. From the **Region** list, select the region to deploy the Harmony SASE gateway.
5. In the **Number of Gateways** field, enter the number of private gateways you want to deploy in the region.
6. To add another region, click **Add Region** and repeat steps 4 and 5.
7. To activate the gateway for users, select the **Activate Gateways For Users** checkbox.
8. Click **Add Region**.

# Managing Access

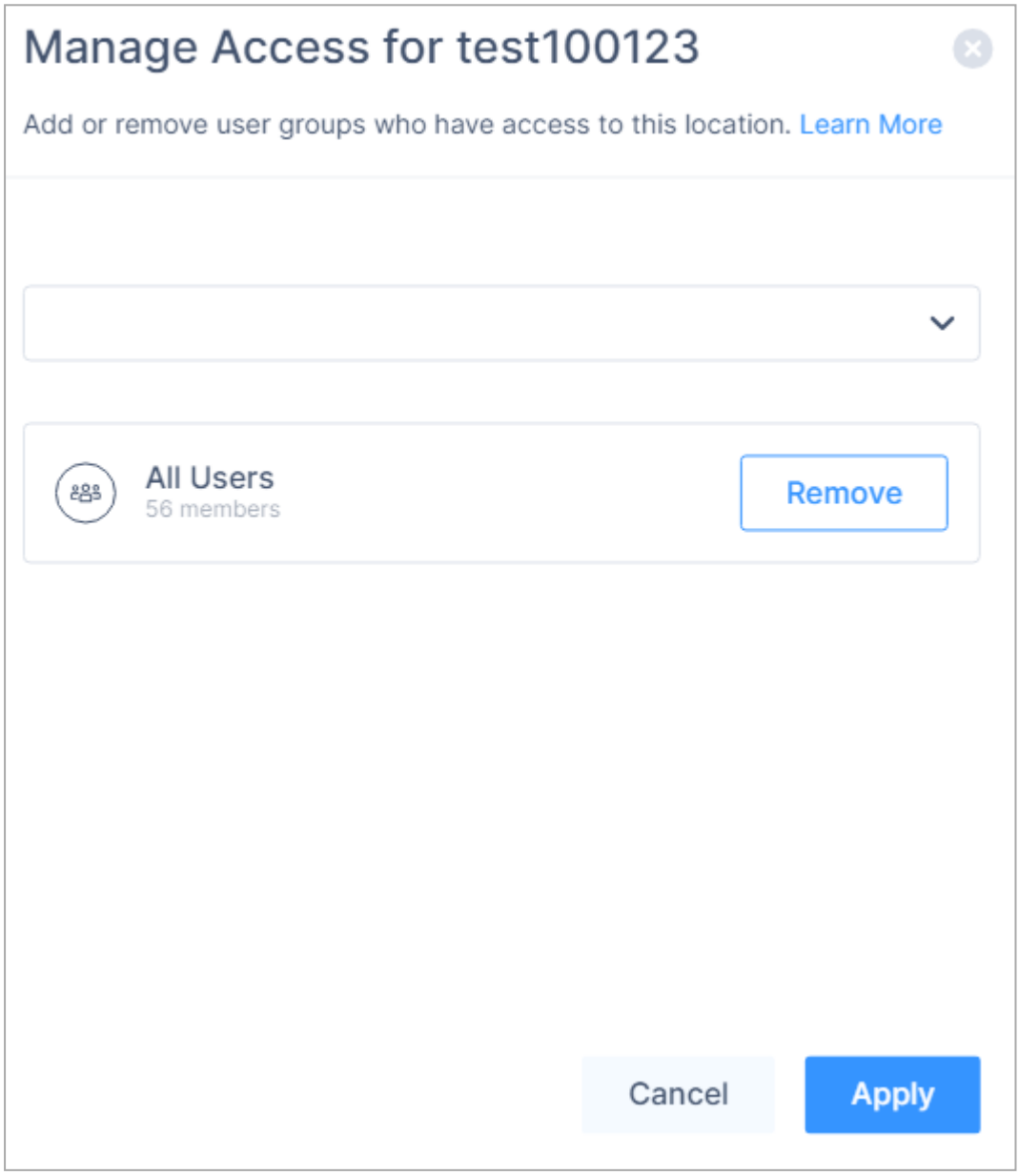
Manage Access allows you to select the member groups who can access the network.

**To manage access to a network:**

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **Manage Access**.




The **Manage Access** window appears.



4. From the list, select the member groups who can access the network.
5. To remove a member group, click **Remove**.
6. Click **Apply**.

# Firewall Rules

Firewall Rules allows you to set the firewall access rules for your network.

To set the rules, see *"Creating a Firewall Access Rule" on page 160*.

# Split Tunneling

Split tunneling allows you to choose the traffic that should pass through the tunnel and the traffic that should bypass the tunnel and access the resource directly.

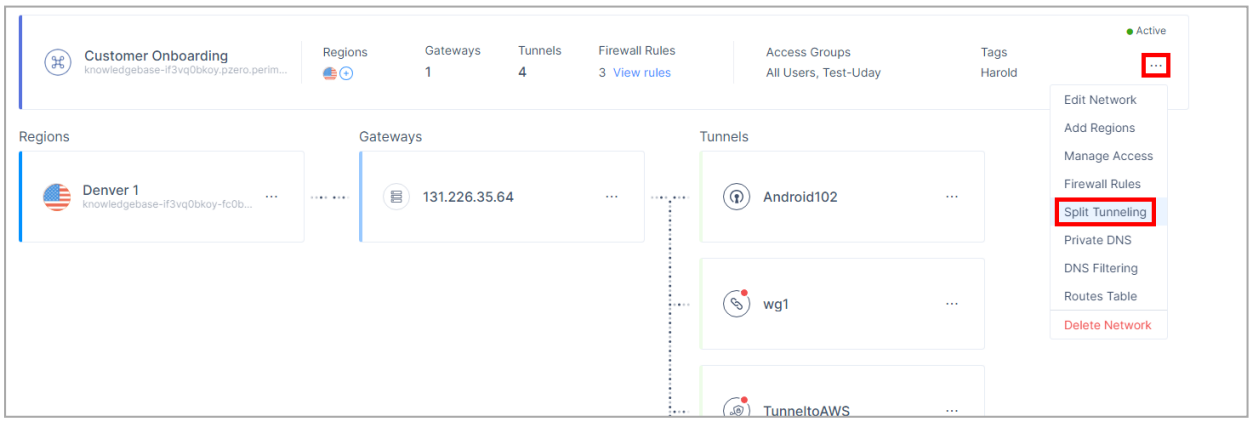
**Best Practices -**

- Identify the IP addresses and IP ranges to bypass the tunnel.
- Review the bypassed IP addresses periodically.

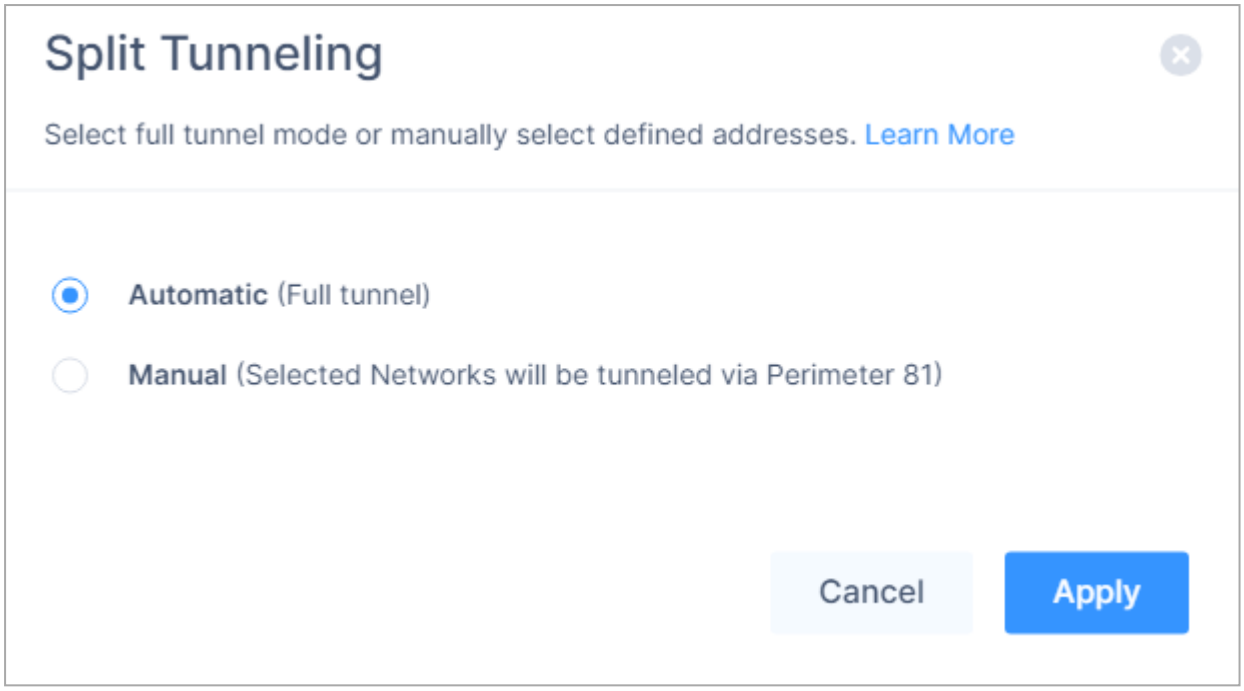
**Note** - Split tunneling by FQDN is supported only for Harmony SASE Agents10.1.x and higher. With older agent versions, split tunneling by FQDN is ignored and reverts to full tunneling.

**To configure split tunneling for a network:**

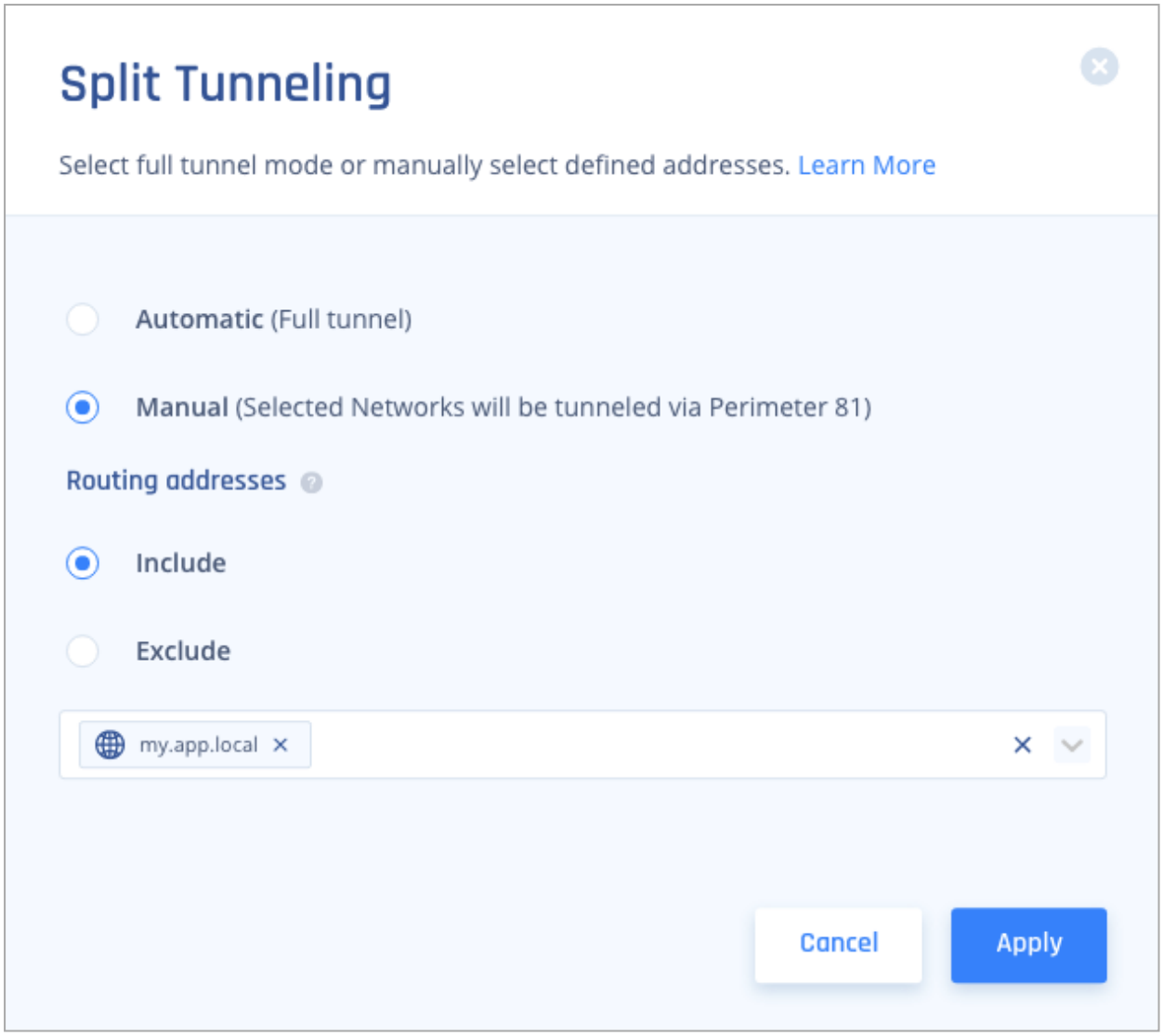
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select your network.
3. Click ··· and then click **Split Tunneling**.




The **Split Tunneling** window appears.




4. Select one of these:




| Item | Description |
|---|---|
| Automatic (Full tunnel) | Allows all the traffic through the tunnel. That is, split tunneling is disabled. This is the default setting. |
| Manual | ▪ **Include** - Enter the subnets, FQDN, or IP addresses that you want to pass through the tunnel. This is the default setting.<br>▪ **Exclude** - Enter the subnets, FQDN, or IP addresses that you want to bypass the tunnel. |

**Important** - The processing time depends on the system resource. It takes up to 3 seconds for every 500 subnets.

5. Click **Apply**.

# Private DNS

A private DNS allows you to use your local DNS to resolve host names into IP addresses.

Harmony SASE supports DNS at two levels:

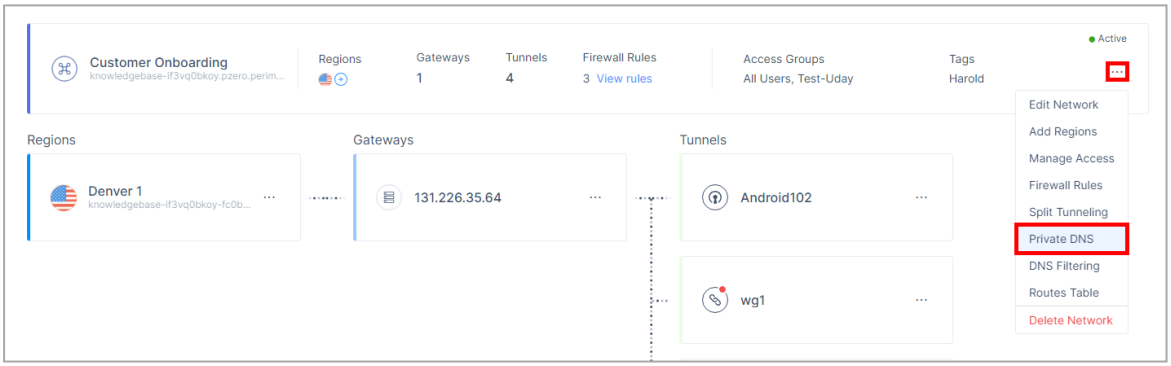
- Network - Allows you to utilize your organization's DNS server and local domain names.
- Region - Allows your users to resolve resources through a local DNS server rather than waiting for a remote server response.

**Notes -**

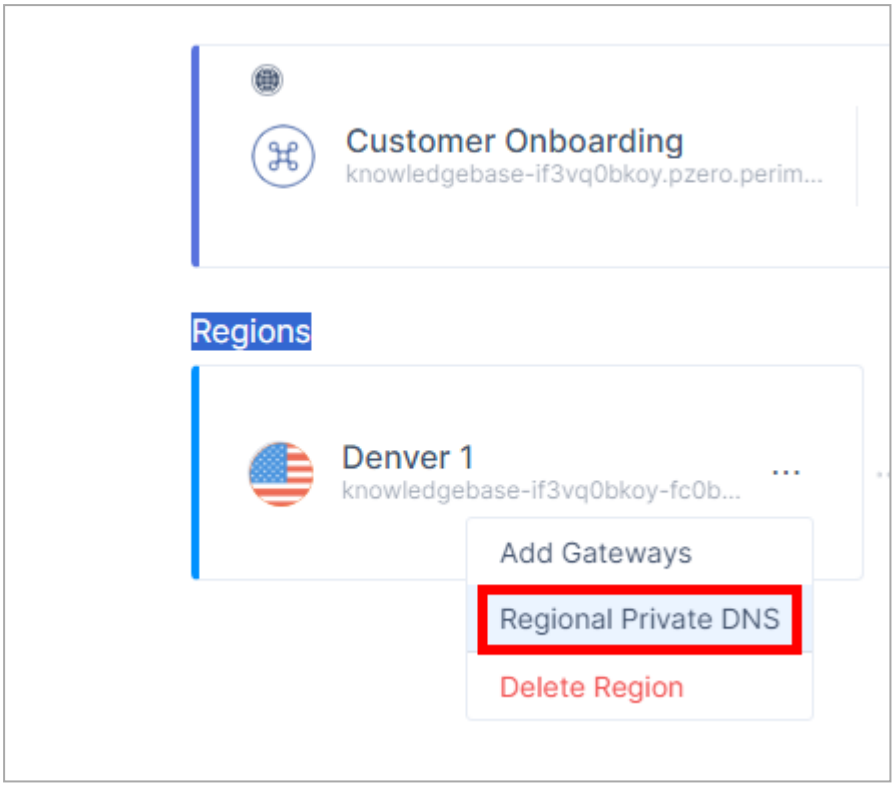
- Do not use Public DNS *8.8.8.8*, *8.8.4.4*, *1.1.1.1*, and *1.0.0.1* for your private DNS.
- If your private DNS server does not have a public IP address, then Check Point recommends to use the IPSec or WireGuard connector tunnel.

### To configure a private DNS for a network:

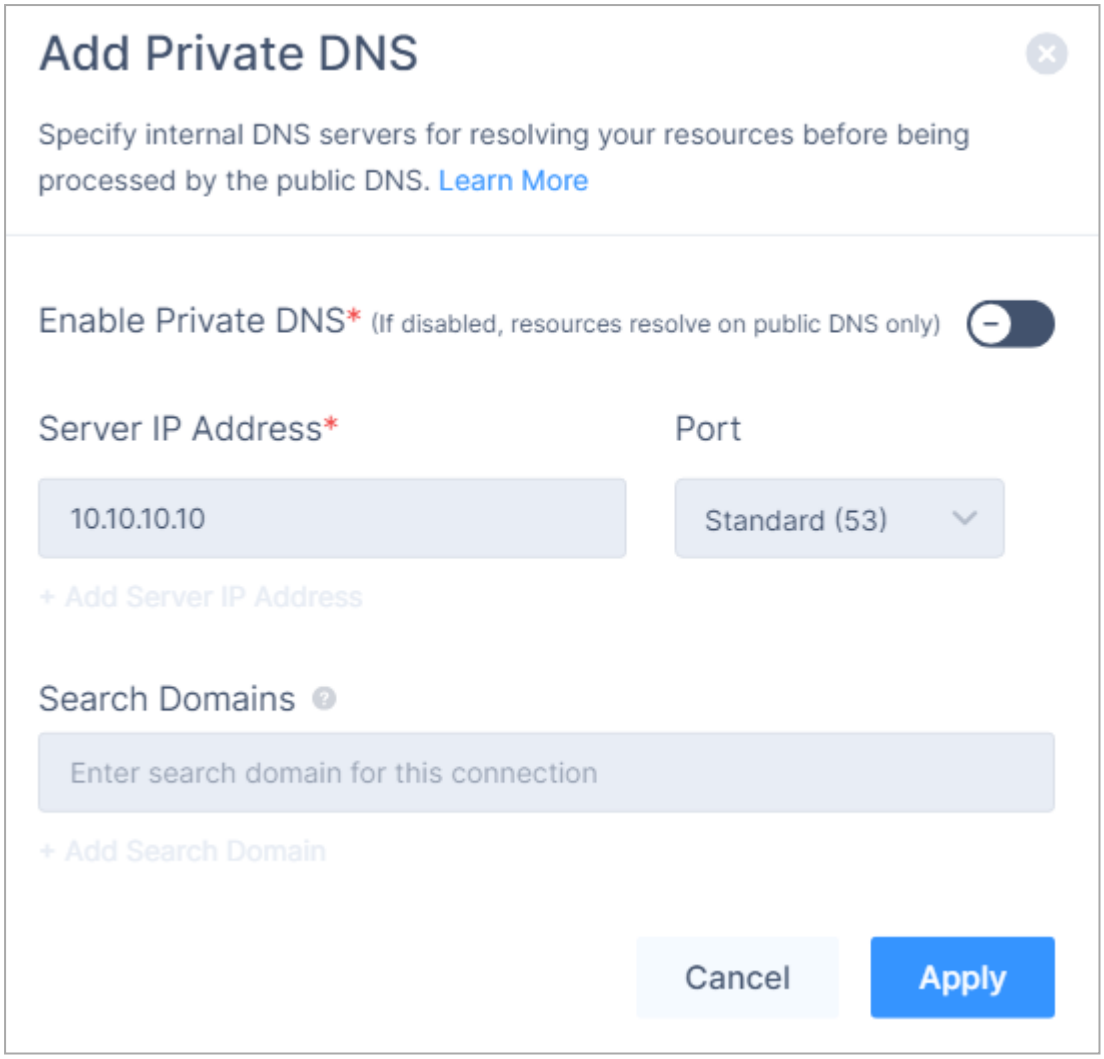
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. To add a private DNS:
   - For a network, click ··· and then click **Private DNS**.



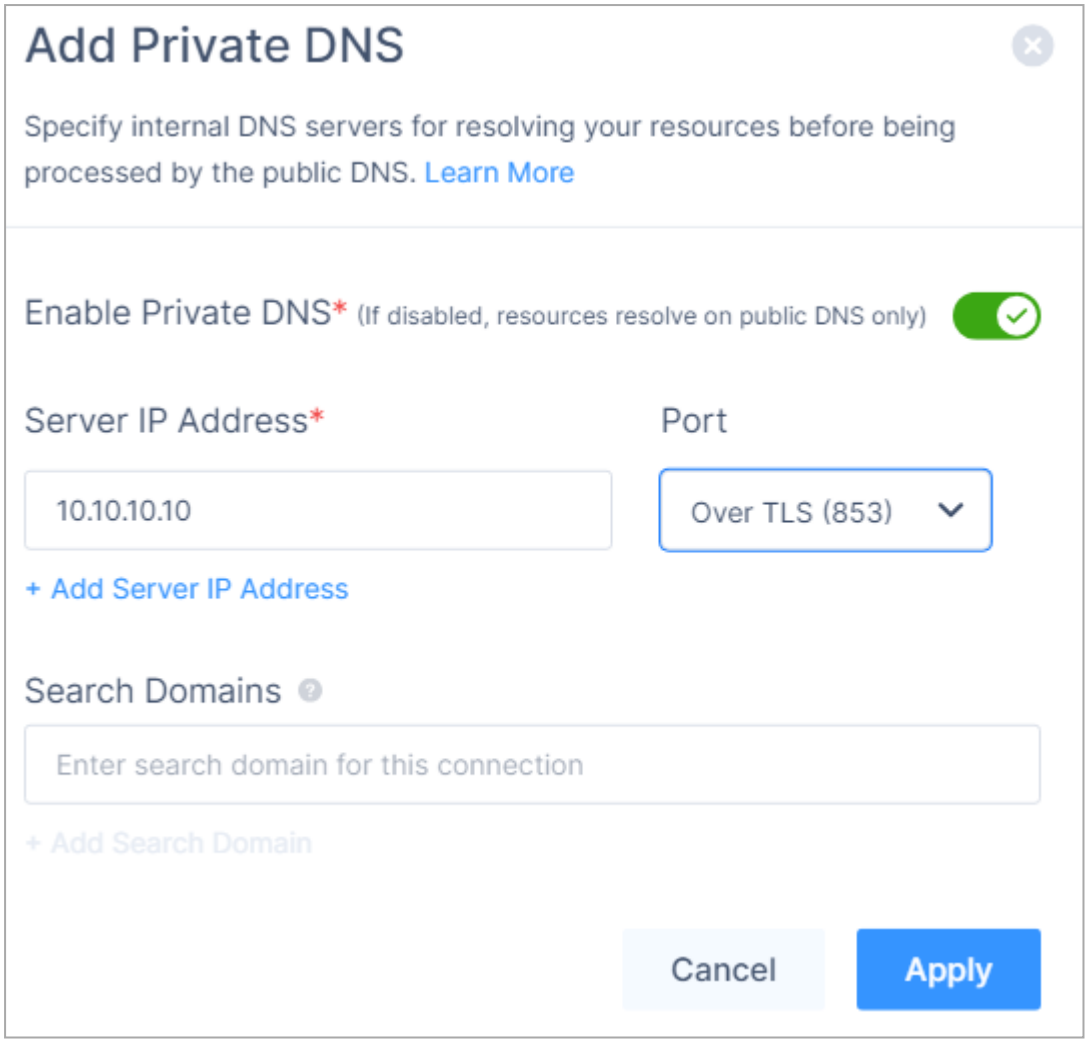
- For a region, in the **Regions** section, click ··· and then click **Regional Private DNS**.




The **Add Private DNS** window appears.




4. Turn on the **Enable Private DNS** toggle button.
5. If your Private DNS Server(s) supports DoT, from the **Port** list, select **Over TLS** (otherwise your requests are sent over HTTPS).




**Note** - You can configure multiple private DNS servers for load balancing. Make sure that the DNS endpoint has zone sharing or zone forwarding enabled. This is supported by both cloud-based and on-premises DNS resolvers.

6. In the **Server IP Address** field, enter the IP address of your DNS servers. You can enter up to four IP addresses.
7. In the **Search Domains** field, enter the suffix for the DNS query.

   For example, if the domain is *checkpoint.com*, if your enter *support*, then the system automatically redirects to *support.checkpoint.com*.
8. Click **Apply**.

   Wait for the network status to change from **Deploying...** to **Active**.

# DNS Filtering

DNS Filtering allows you to manage internet access for members in your network by blocking or allowing websites using allow-list and block-list.

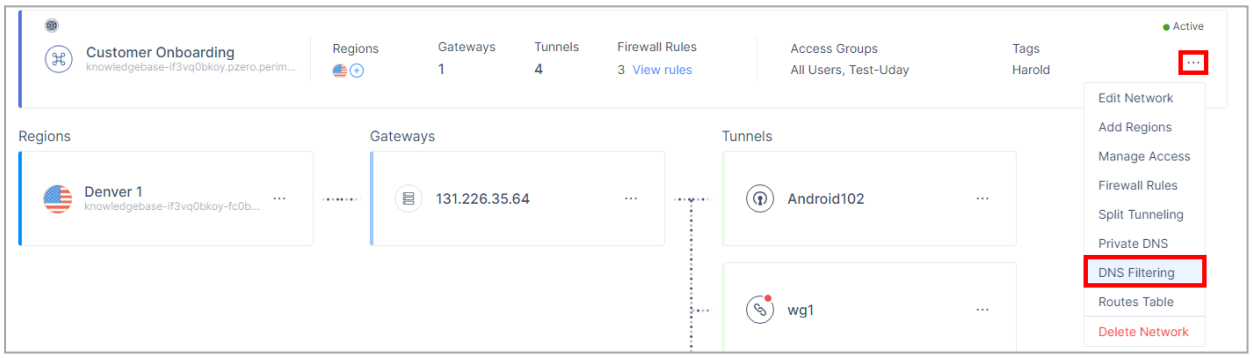
**Best Practices -**

- Make sure that you have the list of URLs to block and allow.
- Make sure that the DNS filter settings work as expected.

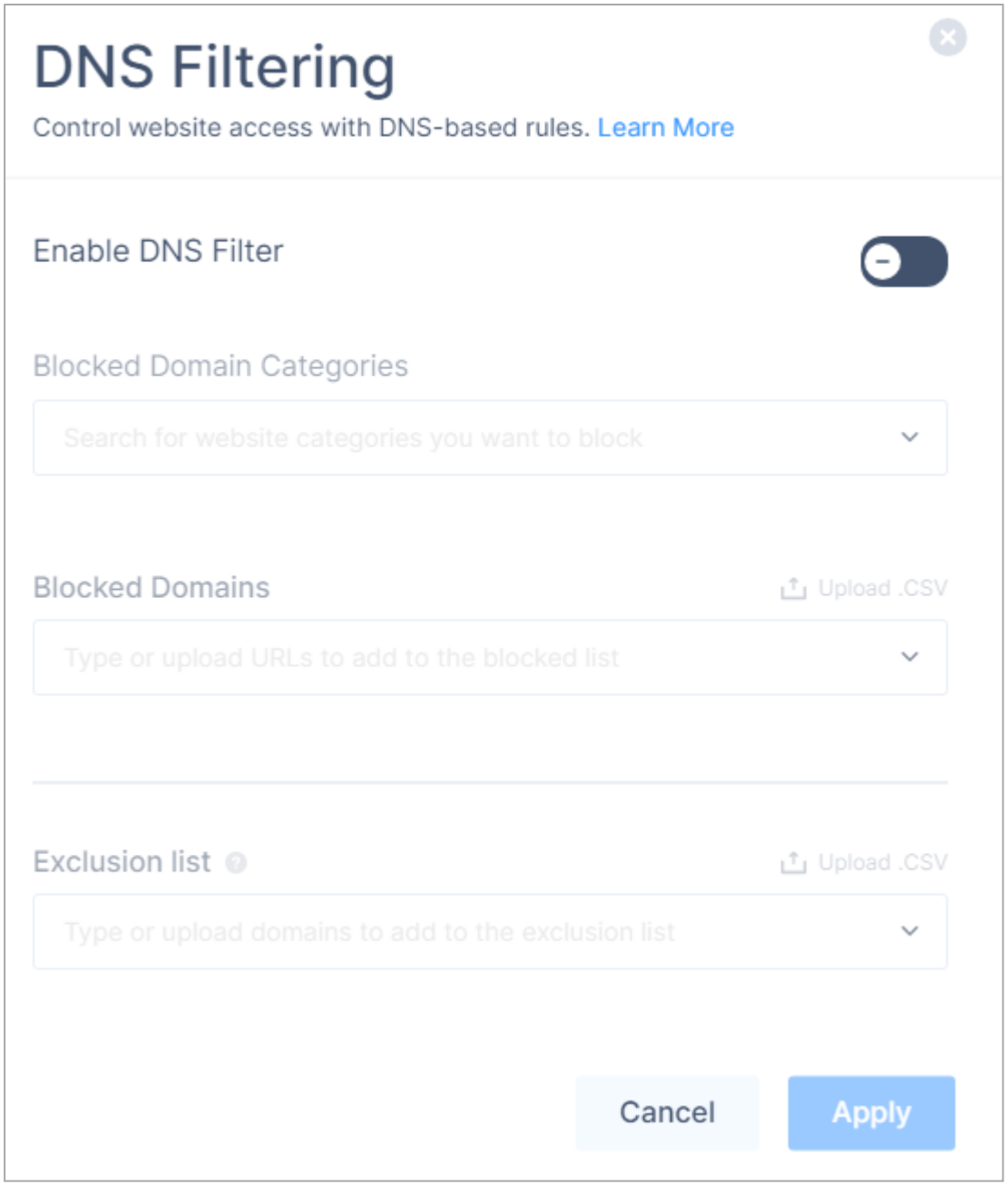



**To configure DNS filtering for a network:**

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· and then click **DNS Filtering**.




The **DNS Filtering** window appears.




4. Turn on the **Enable DNS Filter** toggle button.
5. From the **Blocked Domain Categories** list, select the website categories you want to block.
6. In the **Blocked Domains** field, enter the domains you want to block or upload a .CSV file with the domains.

   Make sure that the .CSV file:

   - Contains all the entries in a single column.
   - Each cell contain only one entry.

- The number of entries does not exceed 1000.
- Each entry is in the form *domain.com*, without **www**, **HTTP**, **HTTPs** prefixes.

| | A |
|---|---|
| 1 | badpineapple.com |
| 2 | fakenews.co.uk |
| 3 | loveistheanswer.fr |

**Note** - When you block a domain, the system blocks the related sub-domains as well.

7. In the **Exclusion list** field, enter the URLs you want to exempt from the blocked domains list or upload a .CSV file with the domains.
8. Click **Apply**.

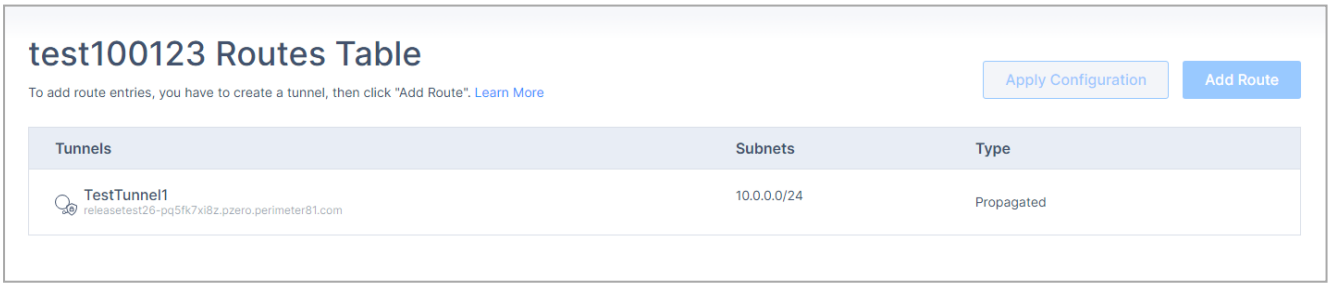
   After the settings are applied, a tooltip shows that DNS filtering is activated in your network.




   The changes are enforced the next time when the member connects to your network using the Harmony SASE Agent.

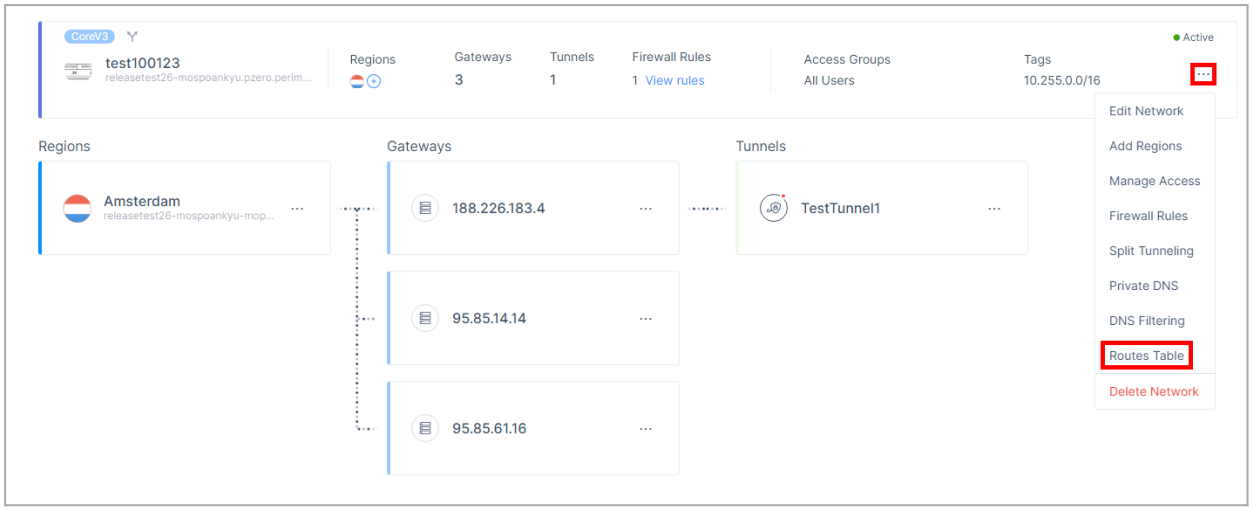
# Routes Table

Routes Table shows the routes created for the tunnels in your network.

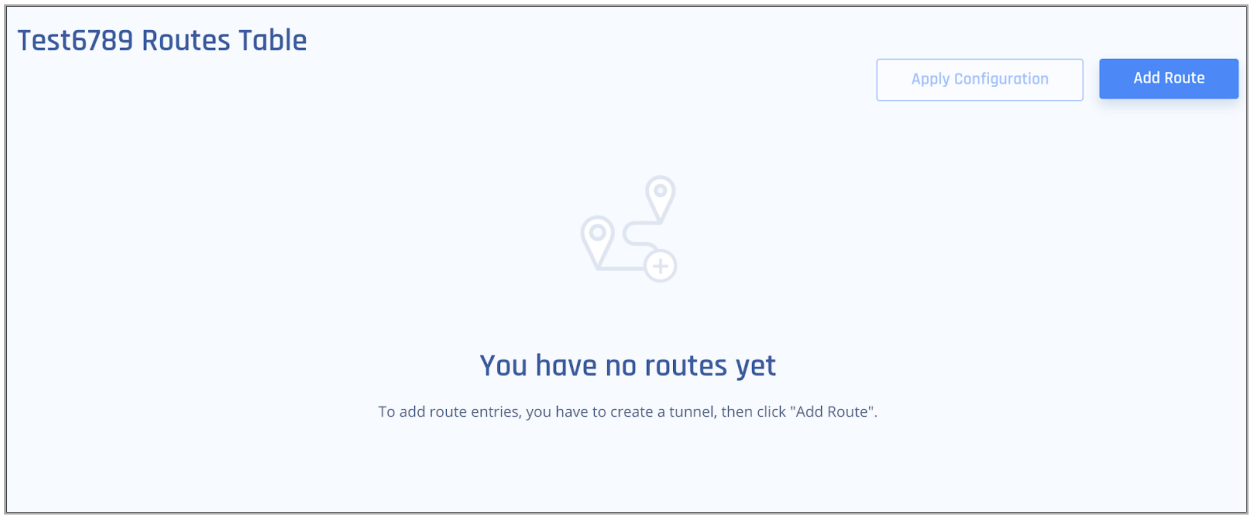



### To add a new route to a tunnel in your network:

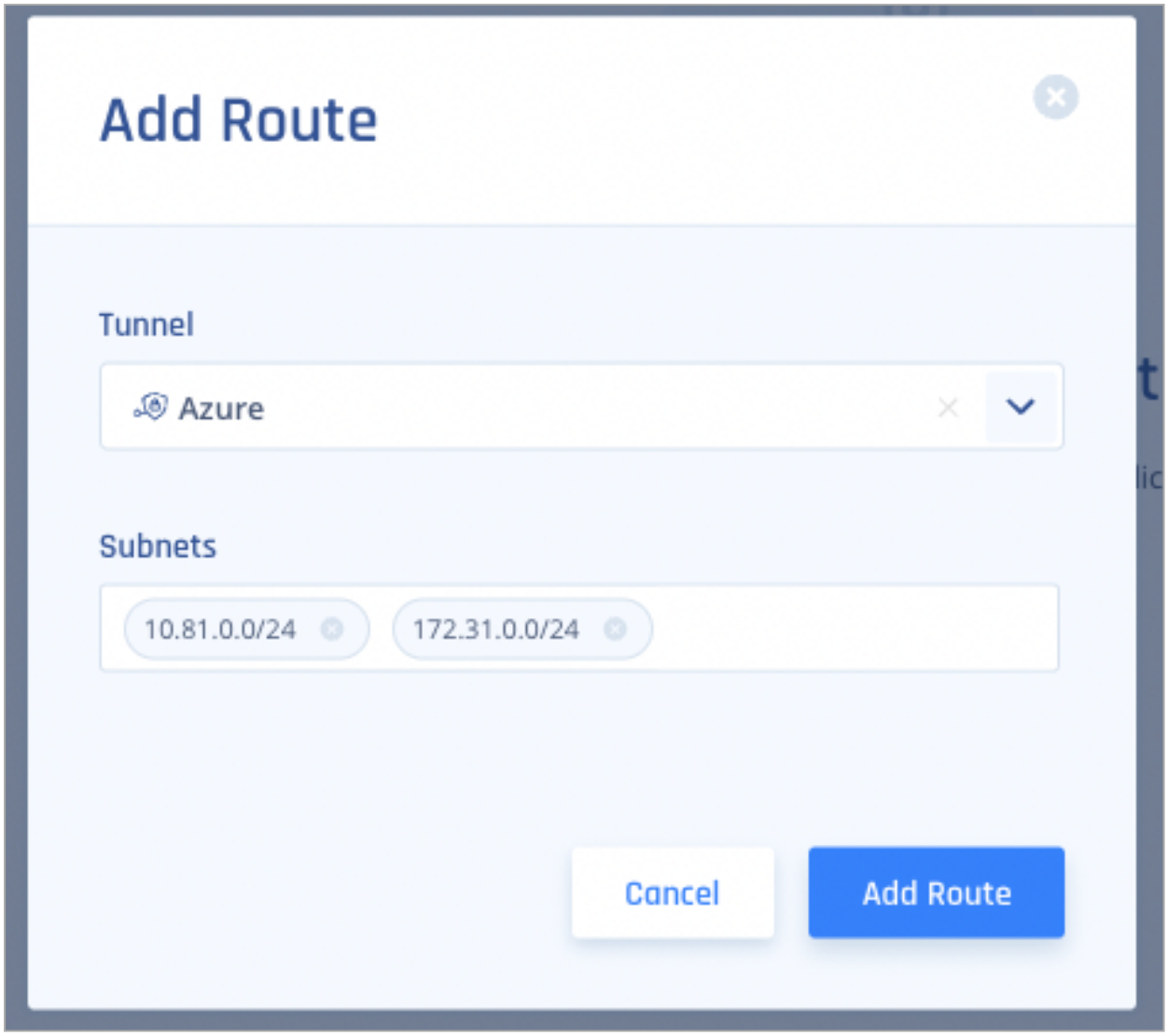
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· at the right end of the network and then select **Routes Table**.




4. Click **Add Route**.

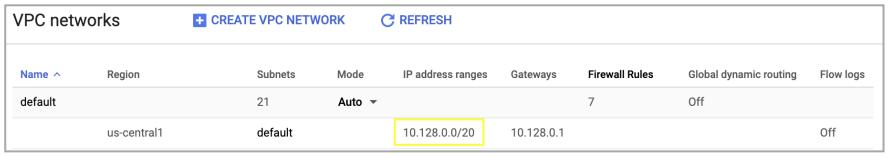



5. Enter all the subnets on the remote side of the tunnel and then click **Add Route**.

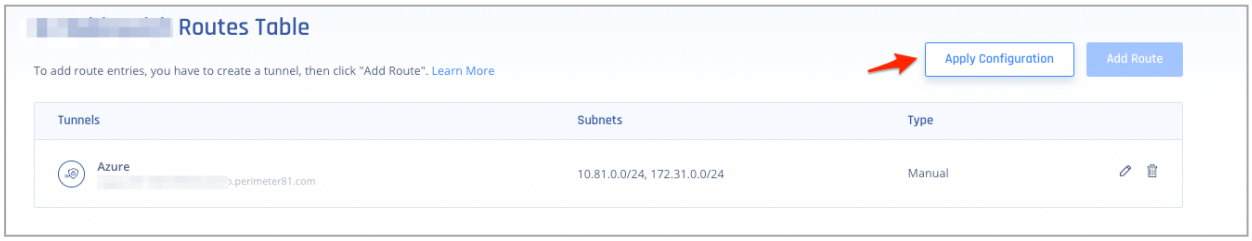



For cloud-based resources, enter these values for your vendor.

| Tunnel Type | Subnets |
|---|---|
| **Amazon AWS** | |
| AWS Single Tunnel - Transit Gateway | CIDRs of the attached VPCs (The VPCs to which you want to gain access) |
| AWS Single Tunnel - Virtual Gateway | Subnets you want to reach on the AWS side of the tunnel. |

| Tunnel Type | Subnets |
|---|---|
| AWS Redundant Tunnels - Transit Gateway | Subnets you want to reach on the AWS side of the tunnel.<br>**Note** - Ensure that the added route matches the route transmitted by BGP. Any discrepancies, such as incorrect subnetting or supernetting, are strictly prohibited. |
| AWS Redundant Tunnels - Virtual Private Gateway | |
| **Google Cloud Platform** | |
| Single Tunnel | From the GCP console, copy the subnets of the regions where your resources are installed.<br> |
| Redundant Tunnels | |
| **Microsoft Azure** | |
| Single Tunnel - Virtual Network Gateway | Subnets of the regions where your resources are installed. |
| Redundant Tunnels - Virtual Network Gateway | |
| Redundant Tunnels - Virtual WAN | |

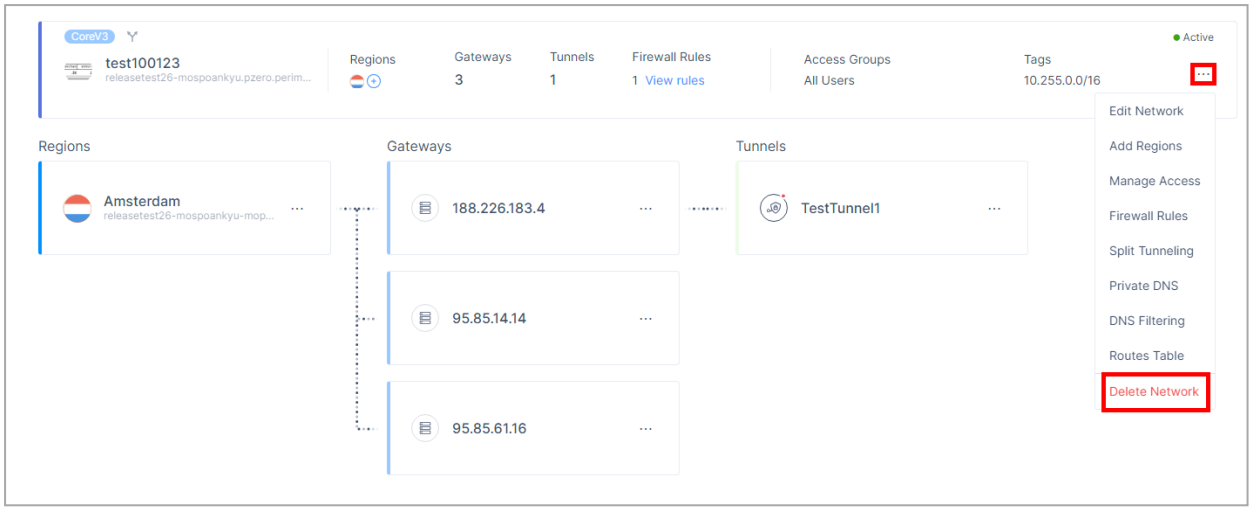
6. Click **Apply Configuration**.



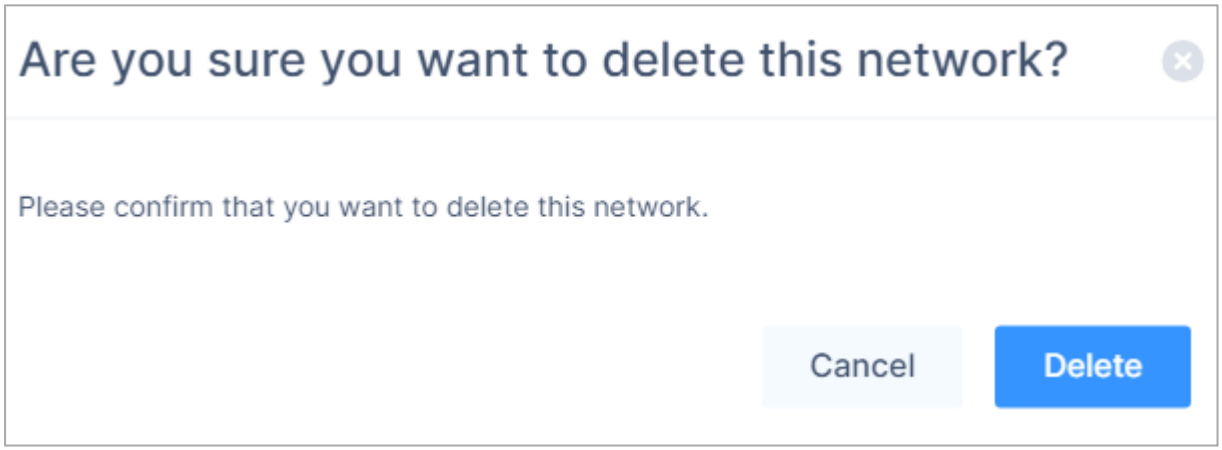

# Deleting a Network

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.

3. Click ··· and then click **Delete Network**.




4. Click **Delete**.



# Private Access

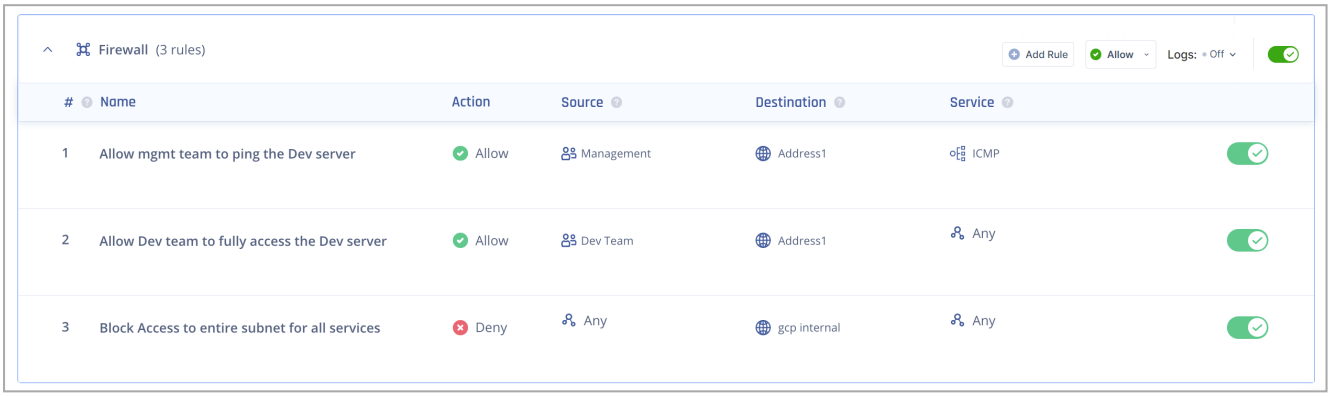
**Private Access** allows you to:

- Create firewall rules for your network.
- Define applications for Zero Trust Access.
- Create policies for application access.

# Firewall

The **Firewall** page allows you to create access rules for your network.

To view the **Firewall** page, access the Harmony SASE Administrator Portal and click **Private Access** > **Firewall**.




## Use Case

- Create rules for specific user groups, resources, and protocols. For example, deny access to the management user group to a certain resource if accessed through the Internet Control Message Protocol (ICMP).
- Create a comprehensive rule for the entire network traffic. For example, block all traffic on a specific port.

## Prerequisite

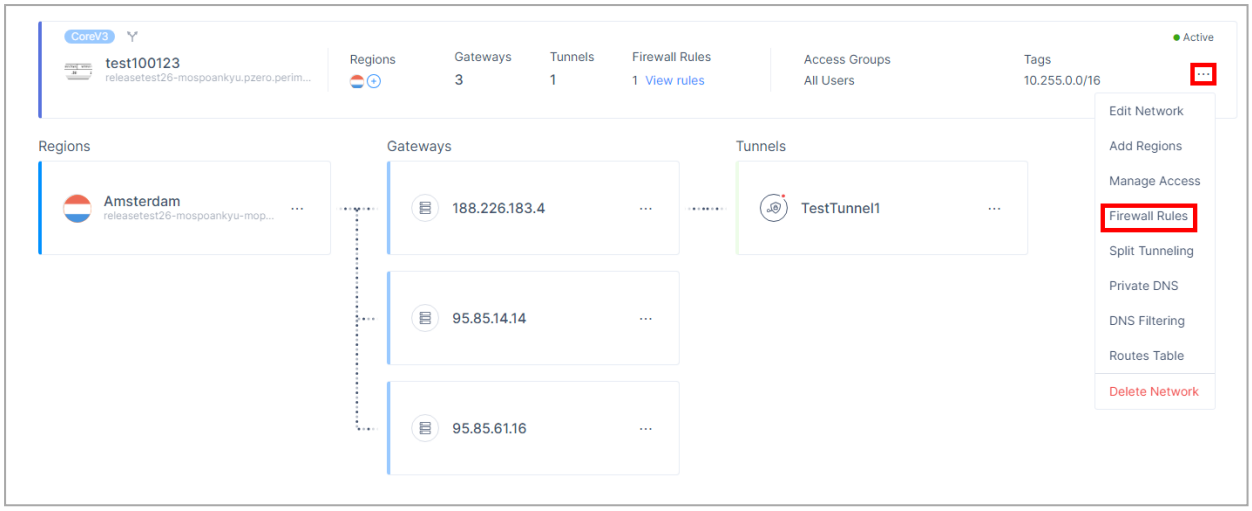
Define your network with IPSec or Harmony SASE Connector tunnel. See *"Adding a Tunnel" on page 121*.

## Access Rules Order

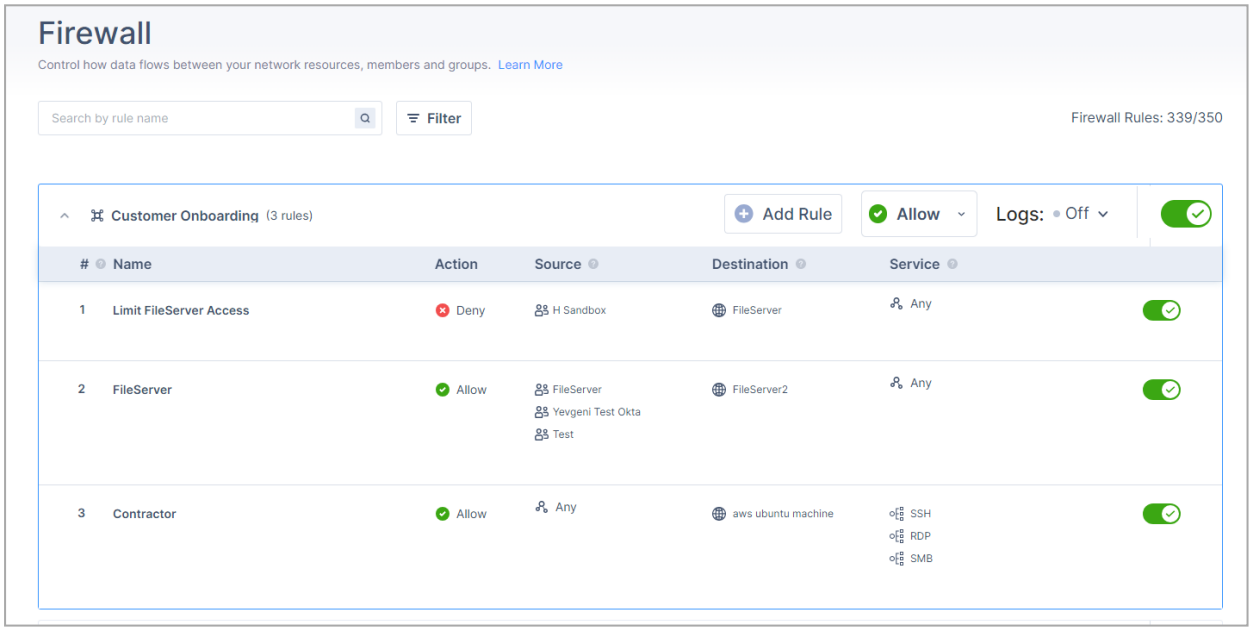
The order of the rules indicate the sequence in which the system checks and applies the rules. For example, if a user tries to access a resource, then the system first checks if the traffic matches rule #1. If it does, it applies the rule. Otherwise, the system checks if the traffic matches rule #2, and so on. If none of the rules match, then the system applies the default rule.

## Creating a Firewall Access Rule

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network for which you want to create firewall access rules.
3. Click ··· and then click **Firewall Rules**.

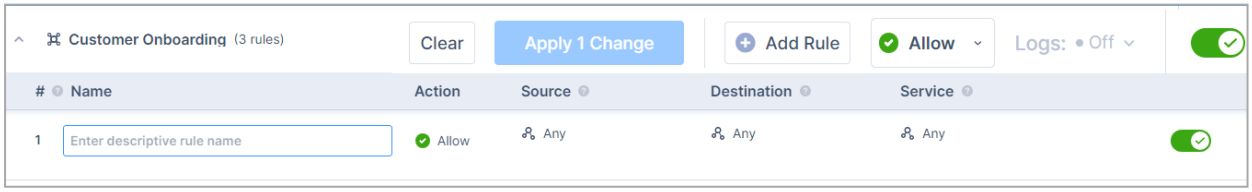



The **Firewall** page appears.




4. Click **Add Rule**.

   The system places the new rule at the top, and it is enabled by default.



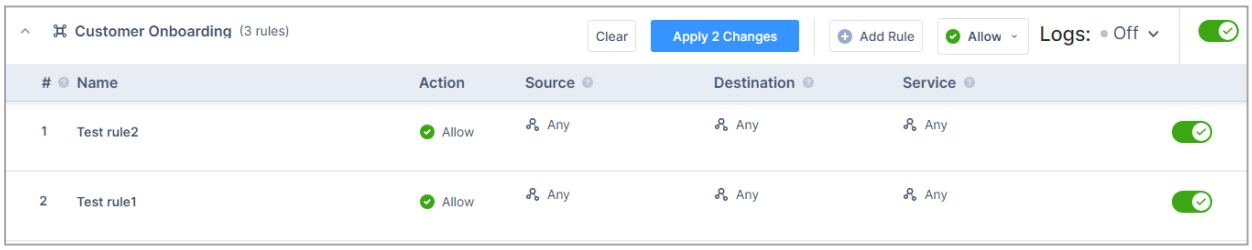

5. In the **Name** field, enter a name that describes the rule.
6. From the **Action** list, select the action type:

- **Allow**
- **Deny**

7. In the **Source** field, click **Add Source** and select the traffic source for this rule.
8. In the **Destination** field, click **Add Destination** and select the traffic destination for this rule.

   **Note** - The **Source** and **Destination** define the conditions for the **Action** to be applied to the traffic.
   You can specify three types of objects in the **Source** and **Destination** fields:
   - **Any** - All traffic (any address or member).
   - **Groups or Members** - All traffic routed from/to a specific member or member group.
   - **Addresses** - Traffic routed from/to an FQDN, IP address, subnet, or list of IP addresses.

9. In the **Service** field, select one of these:
   - **Any** - Traffic routed on all protocols and ports.
   - **Services** - Traffic routed on a specific protocol or port.
10. Drag the rule and place it in required position in the order.
11. Click **Apply Changes**.




   The **Apply Changes** window appears.

12. Click **Apply**.

# Enabling or Disabling Firewall Logs

1. Access the Harmony SASE Administrator Portal and go to **Private Access** > **Firewall**.
2. For the network you want to enable or disable firewall logs, from the **Logs** list, select one of these:
   - **On** - Enable

- **Off** - Disable



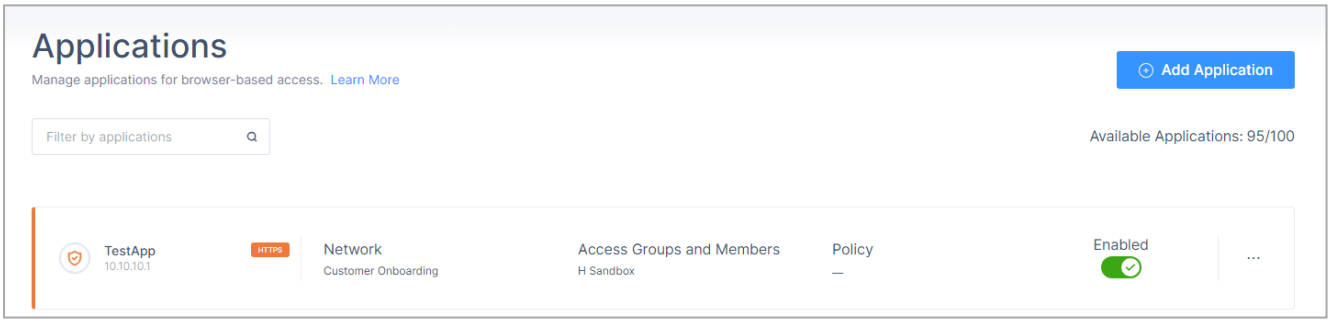
# Applications

The **Applications** page allows to you define your applications and offer an agent-less access to these applications.

The type of applications include:

| Application Type | Example |
|---|---|
| HTTP/HTTPS | Bitbucket |
| RDP | My Desktop |
| SSH | Staging Web Server |
| VNC | Build PC |

To view the **Applications** page, access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.




## Use Case

You want to provide agentless access only to specific applications for members or third-party users with official devices or BYOD in your organization.

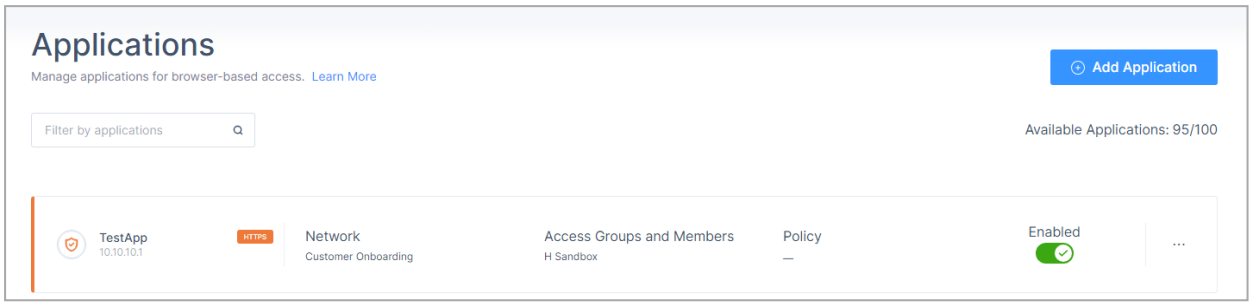
**Note** - To provide secure access for public SaaS applications, such as Microsoft Office 365, Gmail and so on, use the Harmony SASE Agent.

## Prerequisites

1. Define your network with IPSec or Harmony SASE Connector tunnel. See *"Networks" on page 105*.
2. Verify that the application is accessible through the Harmony SASE Agent.

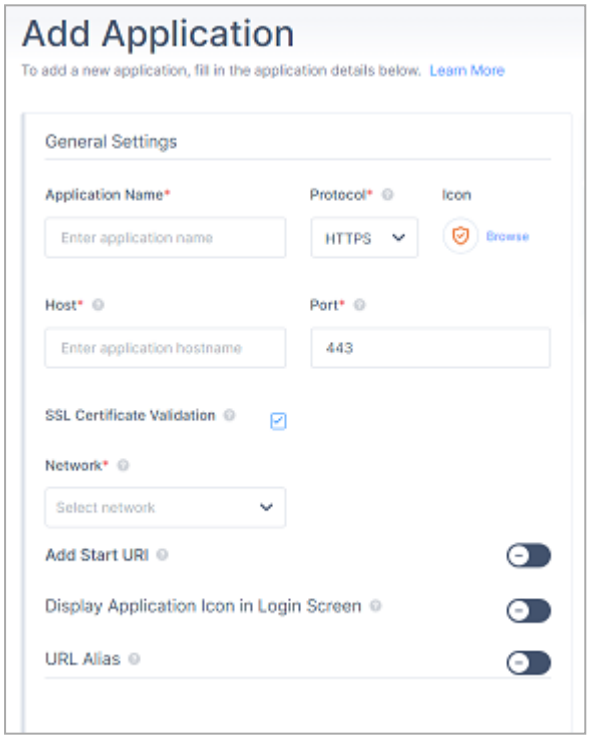
# Adding an Application

1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.




2. Click **Add Application**.

   The **Add application** window appears.

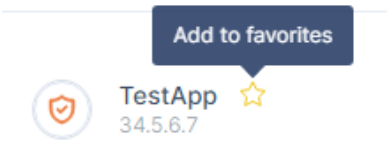



3. Select the application type:

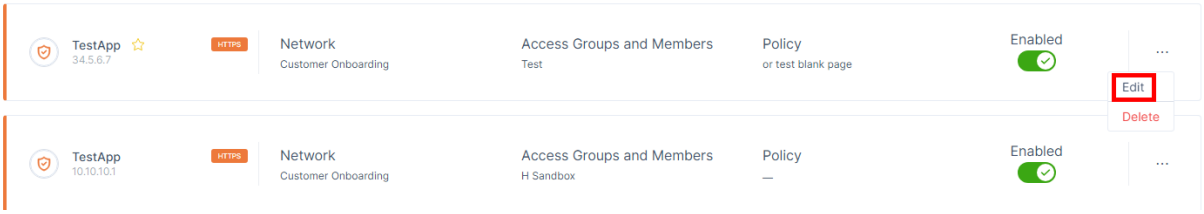
   - HTTP/HTTPS application
   - RDP application
   - SSH application
   - VNC application

   After you add an application, it is enabled by default.

4. To add the application to favorites, hover over the application name and click the ☆ icon.



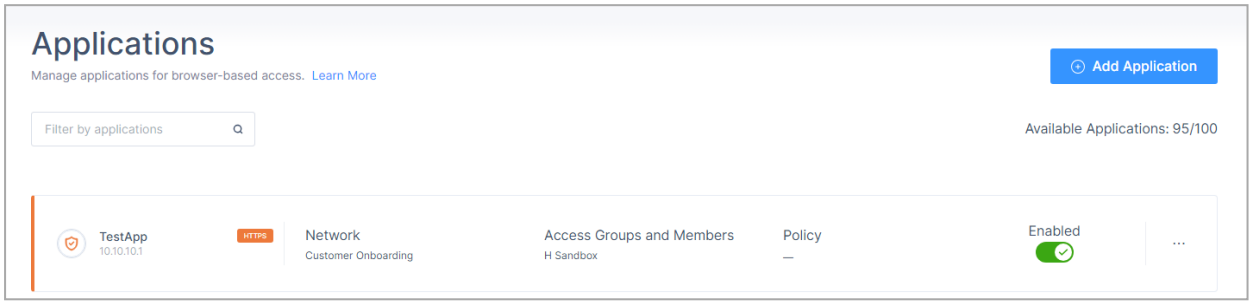

5. To edit the application details, click ··· and then click **Edit**.



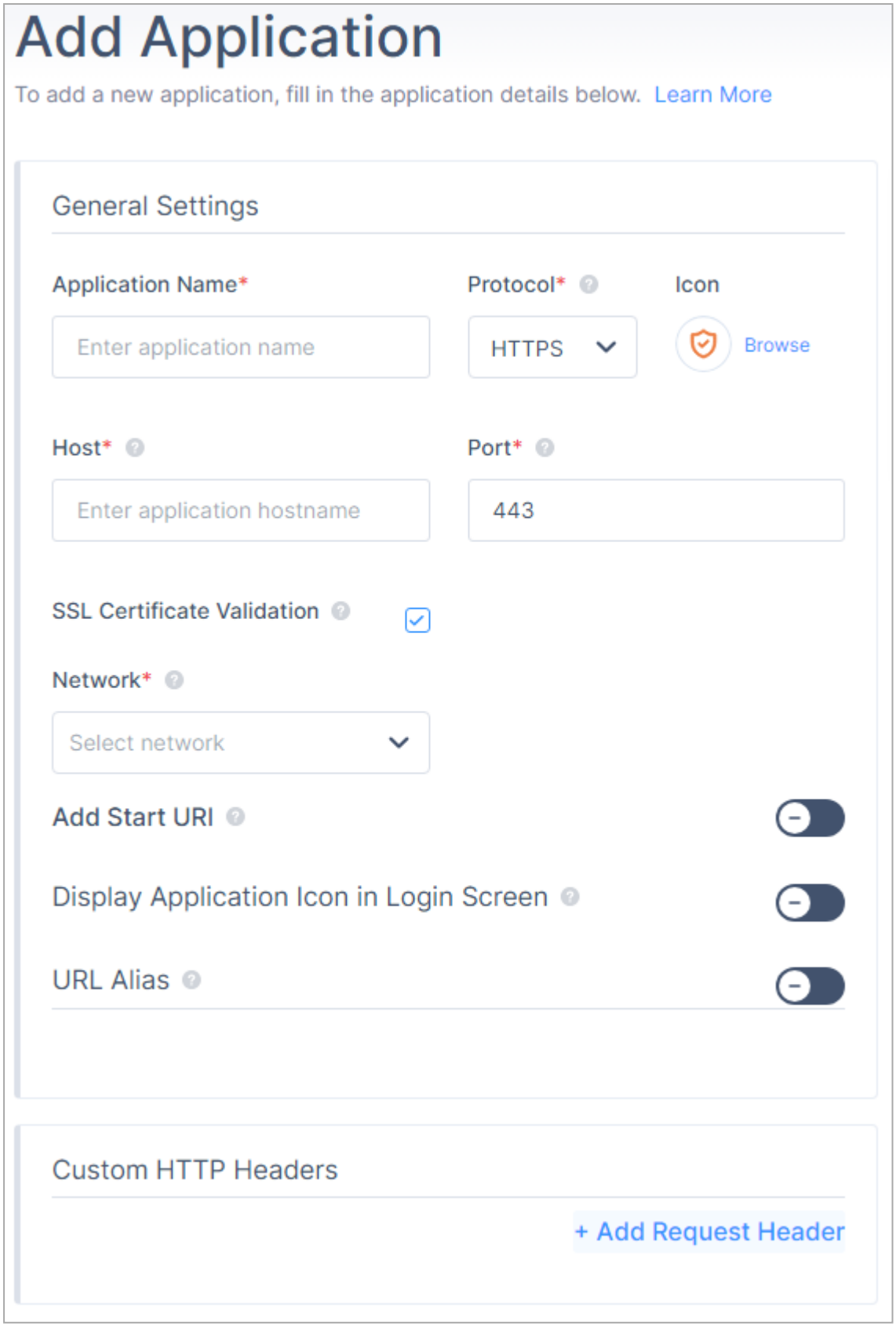

6. Make the required changes and click **Apply**.

# Adding an HTTP/HTTPS Zero Trust Application

1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.




The **Add application** window appears.




3. In the **General Settings** section, enter these:

a. **Application Name** - Name of the application.

b. **Protocol** - HTTP or HTTPS

c. **Icon** - Icon for the application.

d. **Host** - Internal IP address of the server hosting the application. If custom DNS is configured, enter the hostname.

e. **Port** -

   - 80 for HTTP
   - 443 for HTTPS

f. (HTTPS Only) **SSL Certificate Validation** - Indicates that the application is accessible only if the application has a valid SSL certificate.

g. **Network** - Network that hosts the application.

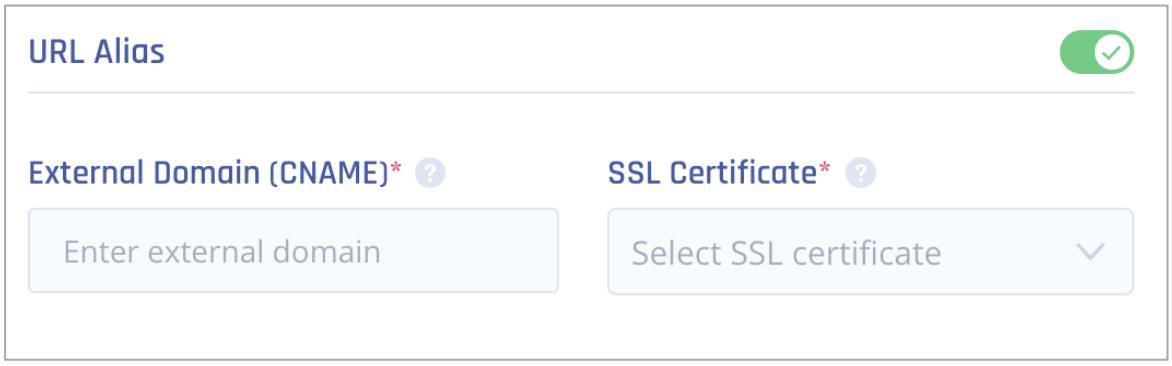
h. (Optional) **Add Start URI** - Subpath to which the system must redirect after the member launches the application.

   For example, if a member enters *www.company.com* and if you want to be redirect to *www.company/careers*, then enter */careers*.

i. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

j. (Optional) **URL Alias** - URL for members to access the application.

   **Important** - You cannot add a URL alias after you create the application.

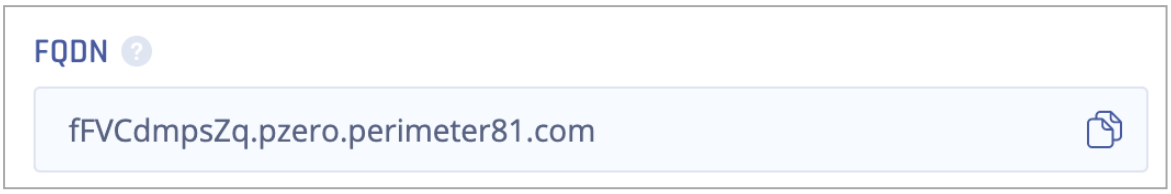



k. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

l. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

m. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

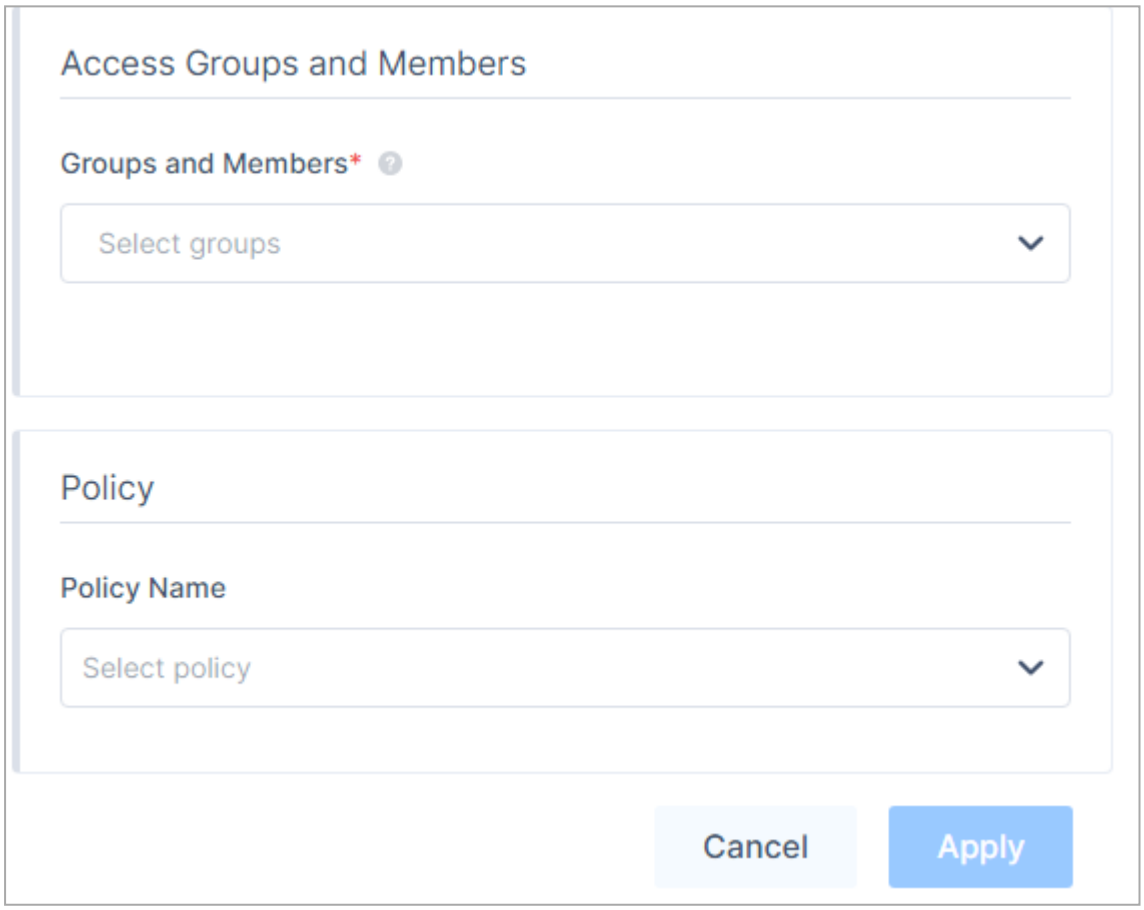
Under your domain, use the CMANE specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.




n. **Custom HTTP Headers** - Click **Add Request Header** and enter **Name** (host) and **Value** (internal FQDN).

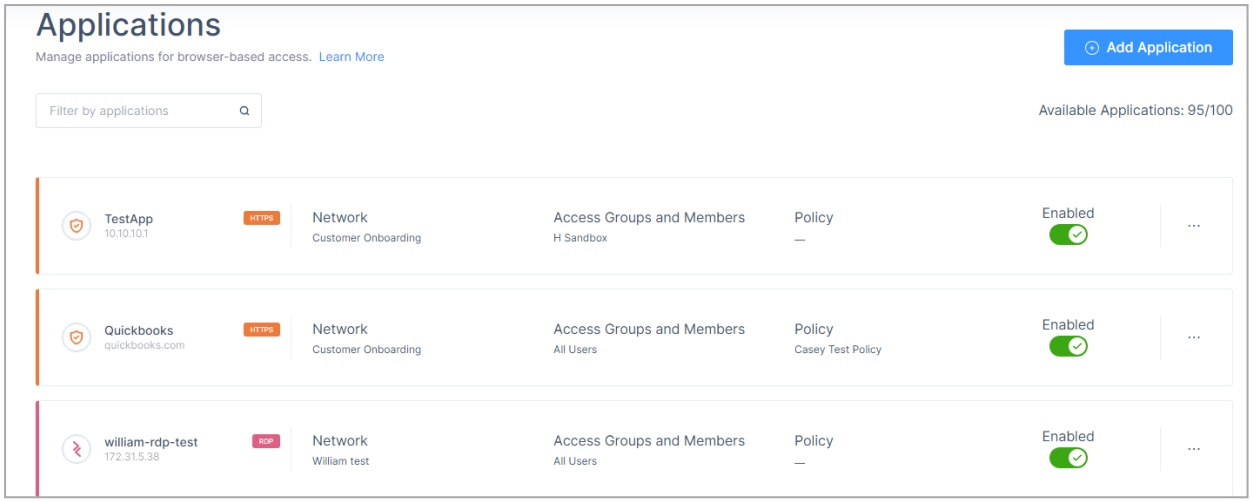
Mandatory if you have specified DNS in the **Host** field.

4. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.




5. (Recommended) In the **Policy Name** list, select an application policy.
6. Click **Apply**.

The system lists the application in the **Applications** page and enables it by default.




7. For members to access the application, see *"Accessing an Application by a Member" on page 190*.

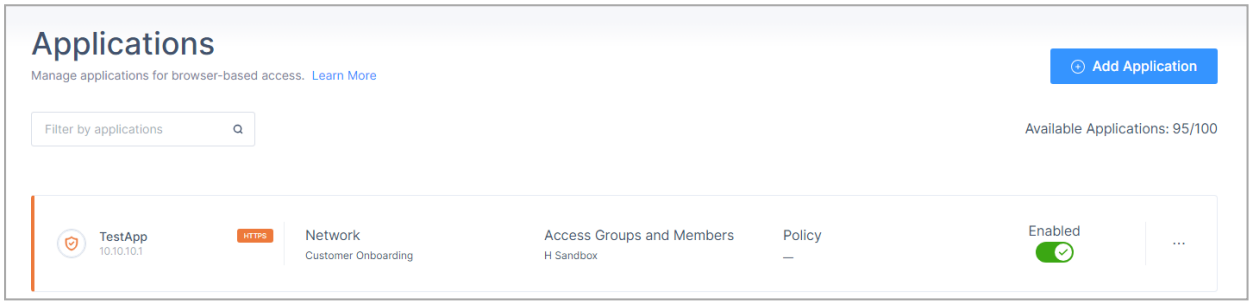
# Adding an RDP Zero Trust Application

## Prerequisite

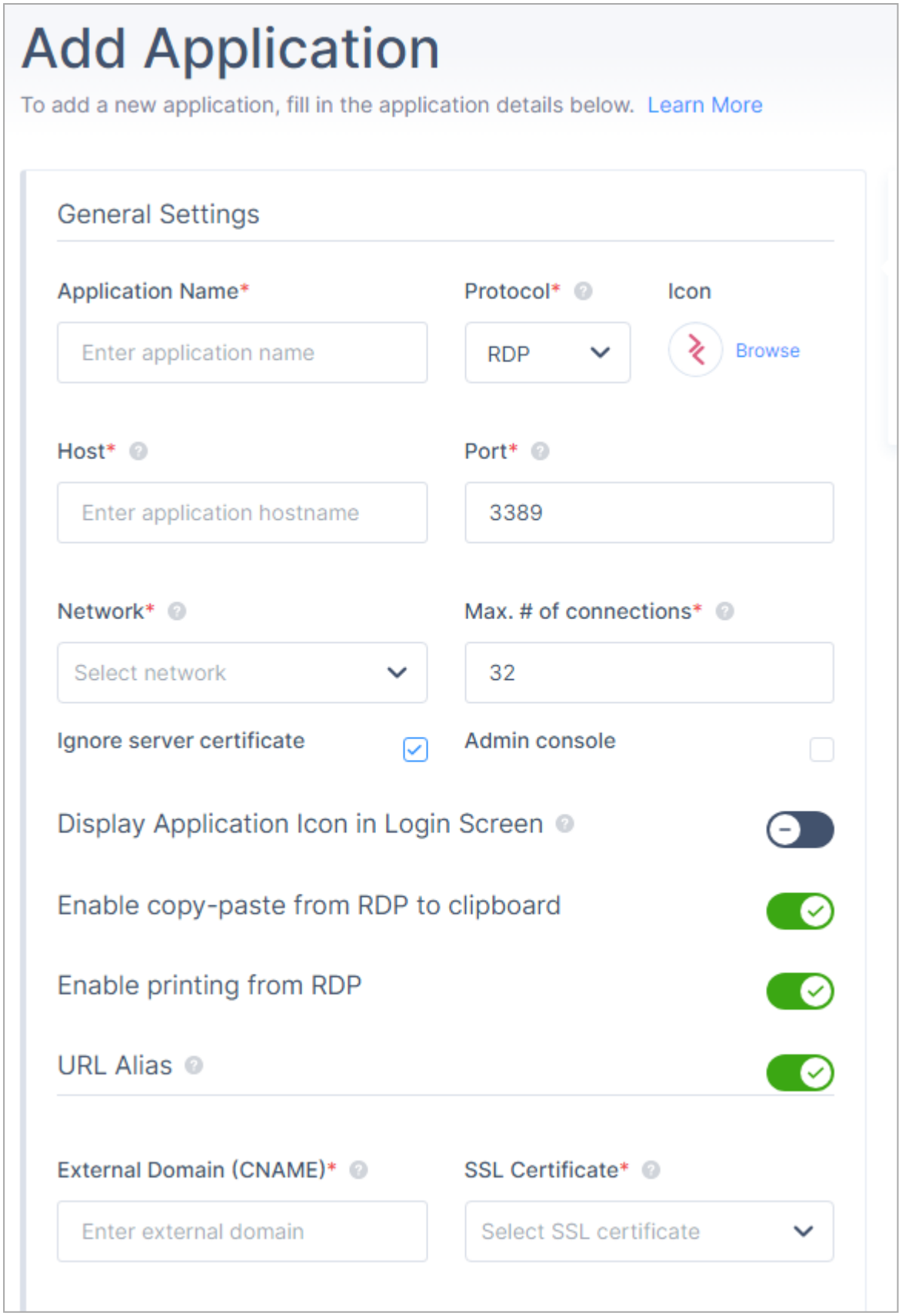
Make sure you have the credentials to access the application over RDP.

### To add an RDP Zero Trust Application:

1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.




The **Add application** window appears.




3. In the **General Settings** section, enter these:

a. **Application Name** - Name of the application.

b. **Protocol** - RDP

c. **Icon** - Icon for the application.

d. **Host** - Internal IP address of the server to which you want to connect.

e. **Port** - 3389

f. **Network** - Network that hosts the application.

g. **Max number of connections** - Maximum number of concurrent RDP sessions.

h. **Ignore server certificate** - Select **Yes** to ignore the SSL certificate, unless you activate RDP over SSL.

i. **Admin console** - Select the checkbox to connect directly to the console session on the Windows server.

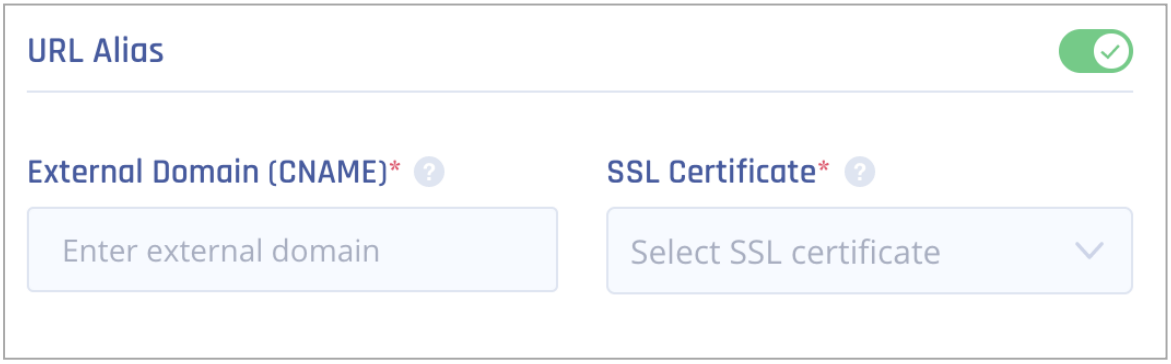
j. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

k. (Optional) **Enable copy-paste from RDP to clipboard** - Enables to copy data from RDP to clipboard.

l. (Optional) **Enable printing from RDP** - Enables to print data from RDP.

m. (Optional) **URL Alias** - URL for members to access the application.

**Important** - You cannot add a URL alias after you create the application.

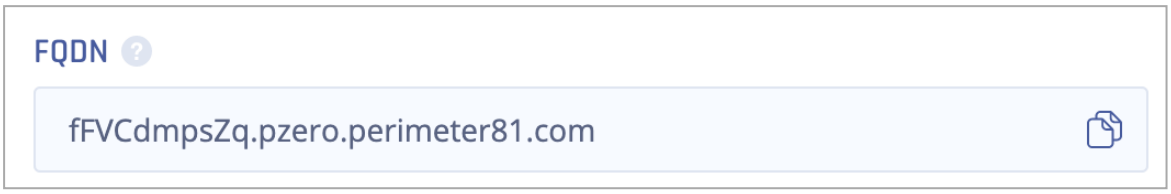



n. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

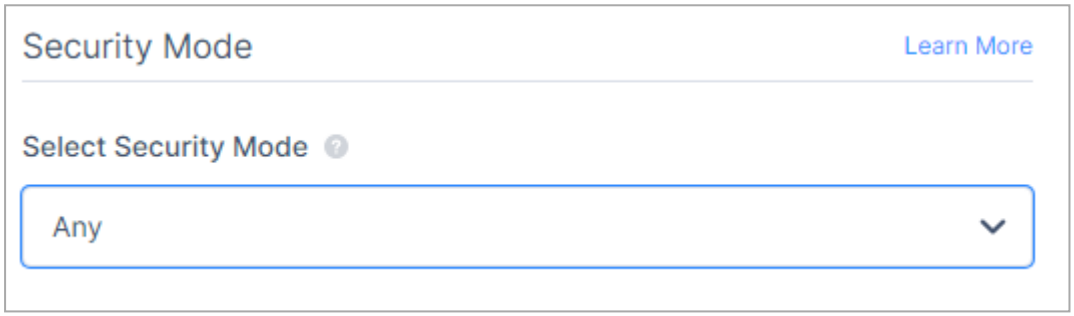
o. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

p. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

Under your domain, use the CMANE specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.

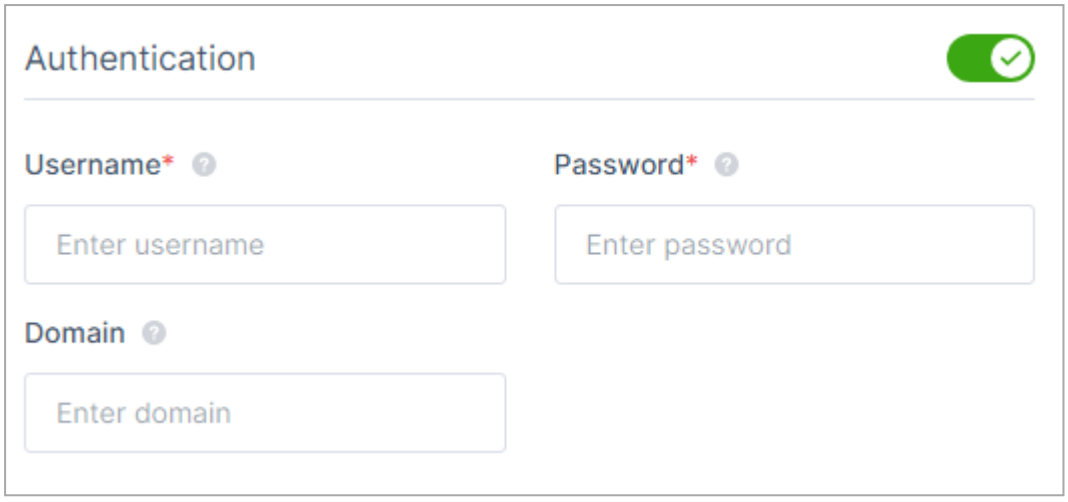



4. From the **Select Security Mode** list, select a security mode. It indicates the encryption and authentication mode.




- **Any** (default) - Select the security mode automatically based on the security protocols supported by the client and the server.
- **Network Level Authentication (NLA)** - Uses the TLS encryption and requires credentials to access the application. Also referred to as hybrid or CredSSP (the protocol that drives NLA).
- **Extended Network Level Authentication (NLA-EXT)** - Sends Early User Authorization Result from the server to the client after the NLA handshake.
- **Transport Layer Security (TLS)** - RDP authentication and encryption through TLS (RDPTLS). This is suitable for load balancing where the primary RDP server redirects the connection to secondary servers.
- **VMconnect** - Selects a security mode supported by Hyper-V or VMConnect automatically based on the supported protocol by client and server.
- **Remote Desktop Protocol (RDP)** - Suitable for machines running old Windows version where a login screen is required.

5. In the **Authentication** section, enter these:

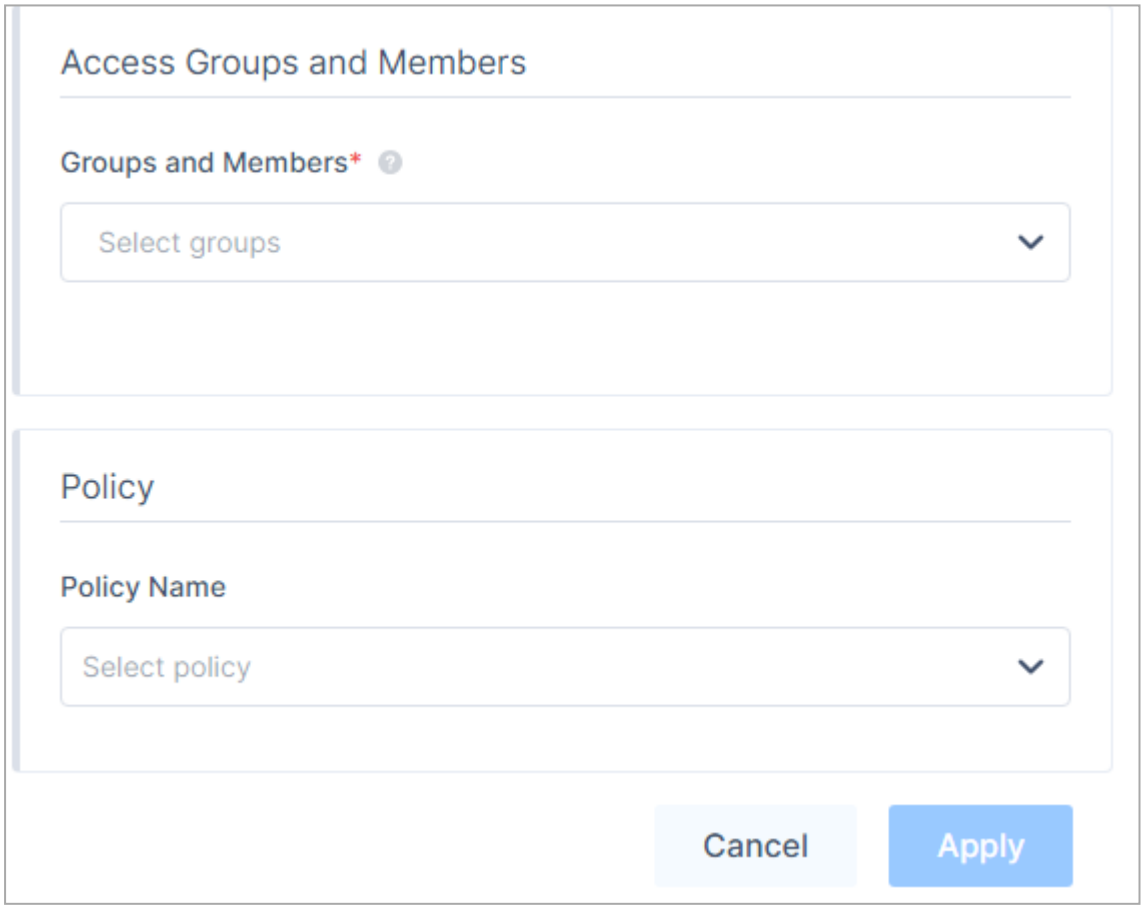



a. **Username** and **Password** - Credentials of the server.

b. **Domain** - Your active directory FQDN.

**Note** - If you disable **Authentication**, then the member must enter the credentials when accessing the application.

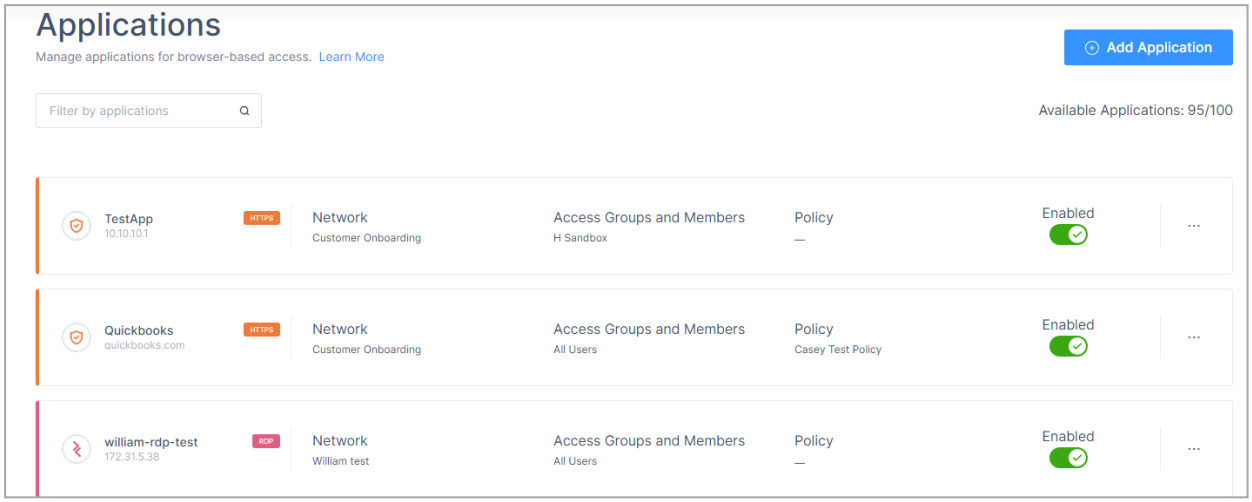
6. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.




7. (Recommended) In the **Policy Name** list, select an application policy.

8. Click **Apply**.

   The system lists the application in the **Applications** page and enables it by default.




9. For members to access the application, see *"Accessing an Application by a Member" on page 190*.

## Additional Registry Configuration

### Windows 7

1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE** > **Software** > **Microsoft** > **Windows NT** > **Terminal Services**.
3. Select **fServerEnableRDP8**.
4. Set the value type to **REG_DWORD**.
5. Set the value to **1**.
6. Reboot the machine.

### Windows Server 2016

1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
3. Select **SecurityLayer** and change the value to **1**.
4. Select **UserAuthentication** and change the value to **0**.

### Windows Server 2019

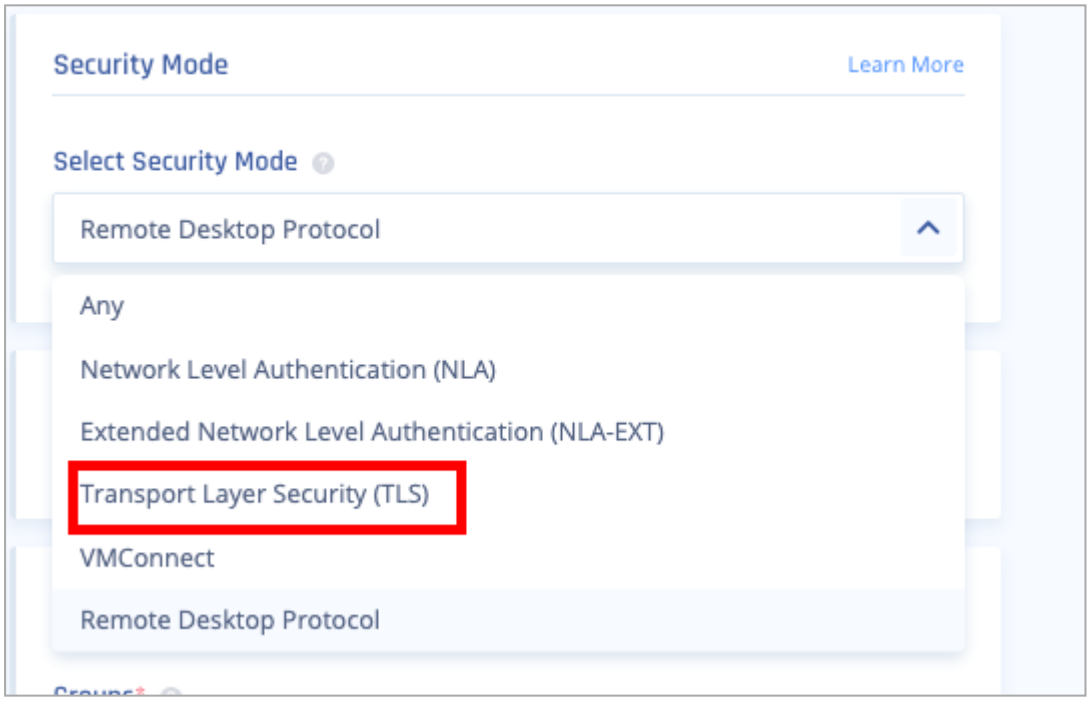
1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
3. Select **SecurityLayer** and change the value to **0**.
4. Reboot the machine.

## Troubleshooting

### Upstream Error

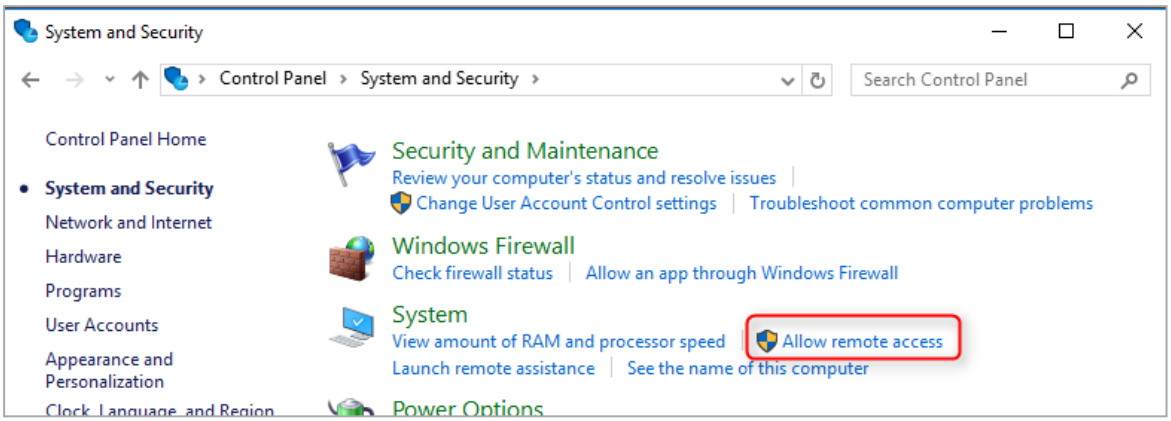
1. If **Authentication** is enabled (see Authentication ), verify the credentials.

   If it is disabled, change the security mode to **Transport Layer Security (TLS)**.



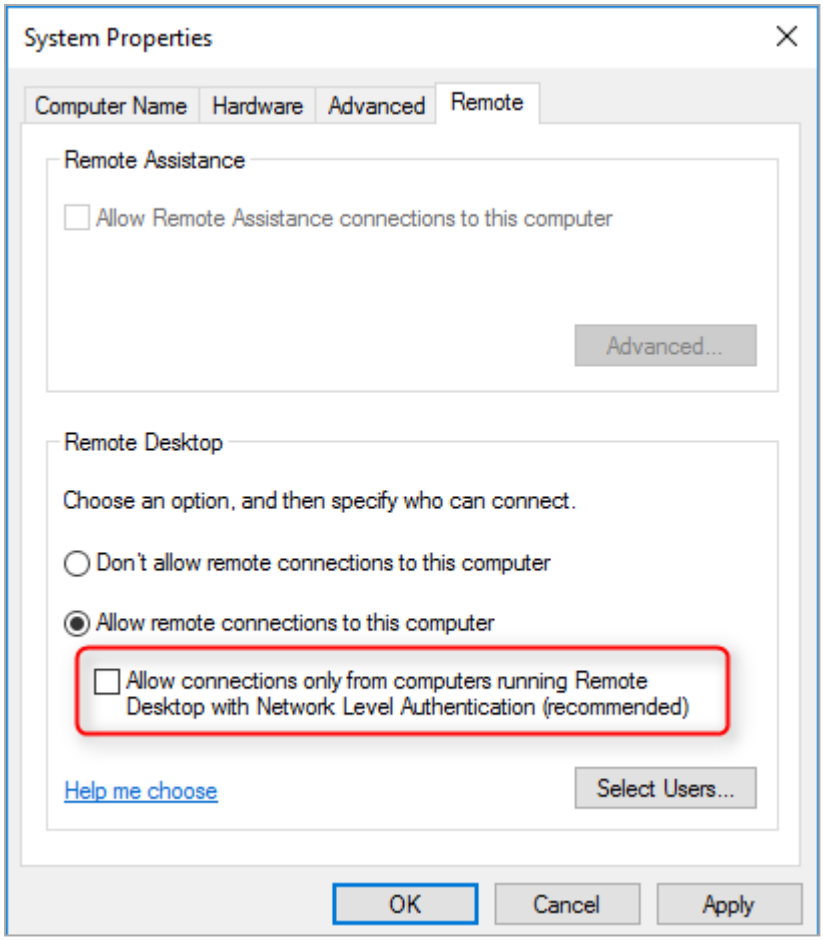
### Additional Troubleshooting Steps

1. Disable NLA on the remote machine:
   a. Open the **Control Panel**.
   b. Click **System and Security** and under **System**, click **Allow remote access**.




   The **System Properties** window appears.

2. Go to the **Remote** tab and in the **Remote Desktop** section, clear the **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** checkbox.


System Properties
Computer Name
Hardware
Advanced
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
Advanced...
Remote Desktop
Choose an option, and then specify who can connect.
Don't allow remote connections to this computer
Allow remote connections to this computer
Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
Help me choose
Select Users...
OK
Cancel
Apply

3. Click **OK**.

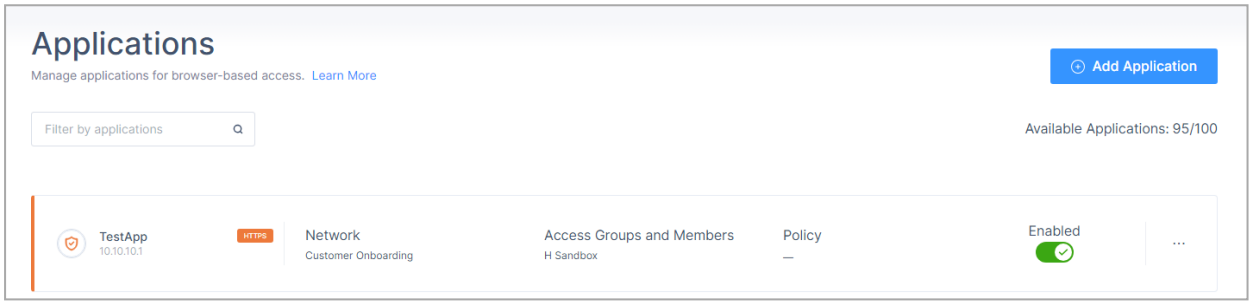
# Adding a SSH Zero Trust Application

## Prerequisite

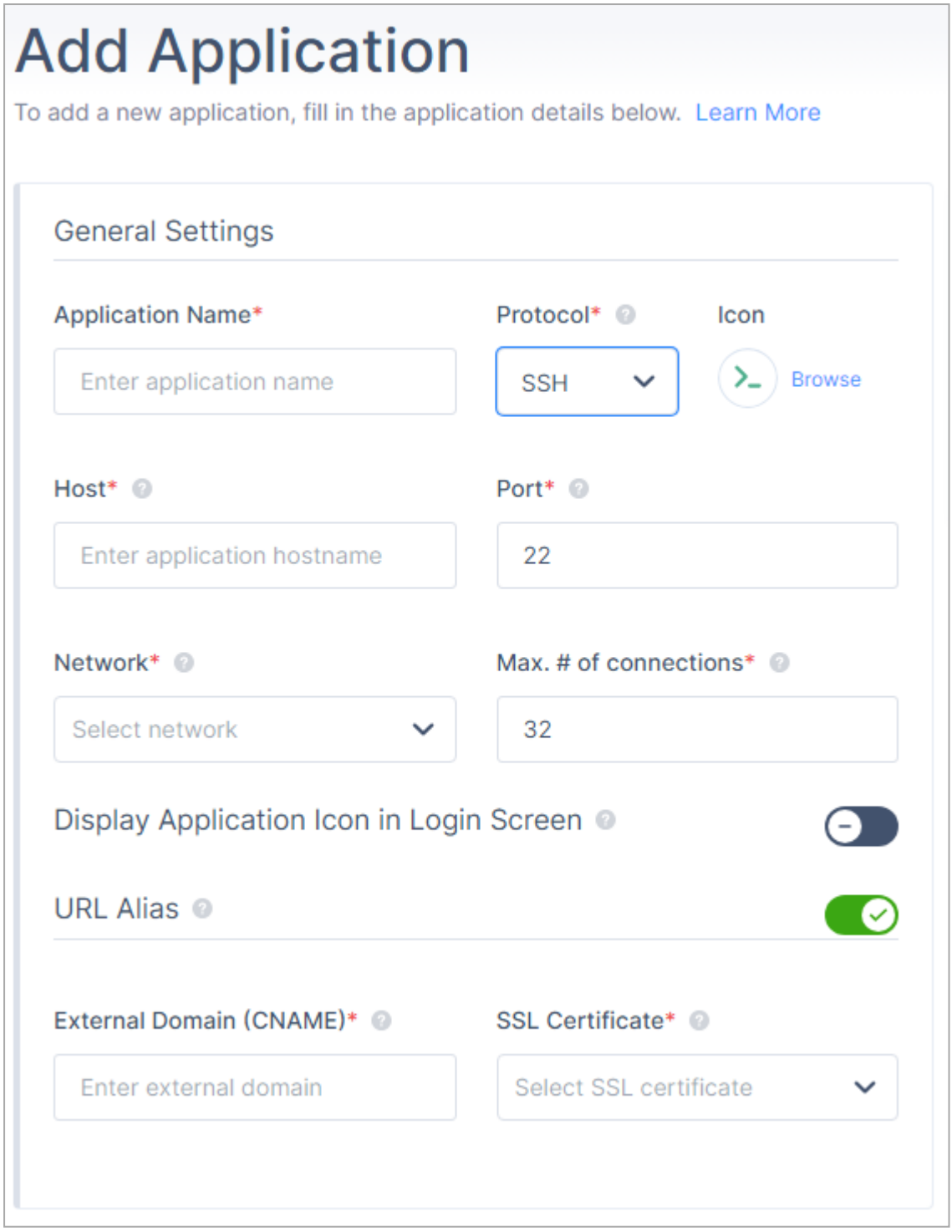
Make sure you have the credentials to access the application over SSH.

### To add an SSH Zero trust Application:

1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.




The **Add application** window appears.




3. In the **General Settings** section, enter these:
    a. **Application Name** - Name of the application.
    b. **Protocol** - SSH
    c. **Icon** - Icon for the application.
    d. **Host** - Internal IP address of the server to which you want to connect.

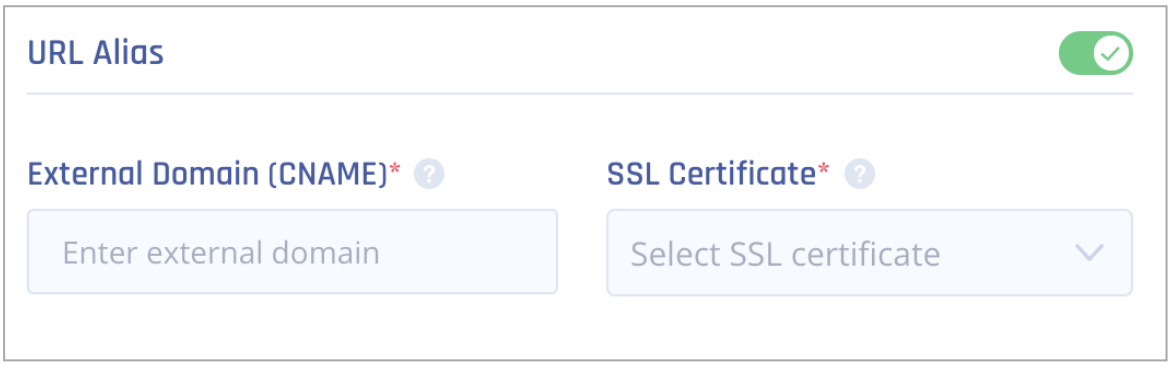
e. **Port** - 22

f. **Network** - Network that hosts the application.

g. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

h. (Optional) **URL Alias** - URL for members to access the application.

**Important** - You cannot add a URL alias after you create the application.

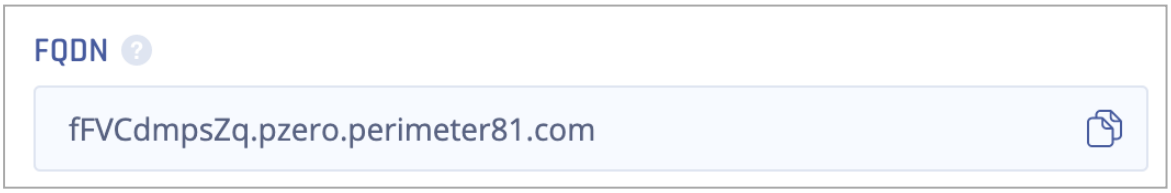



i. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

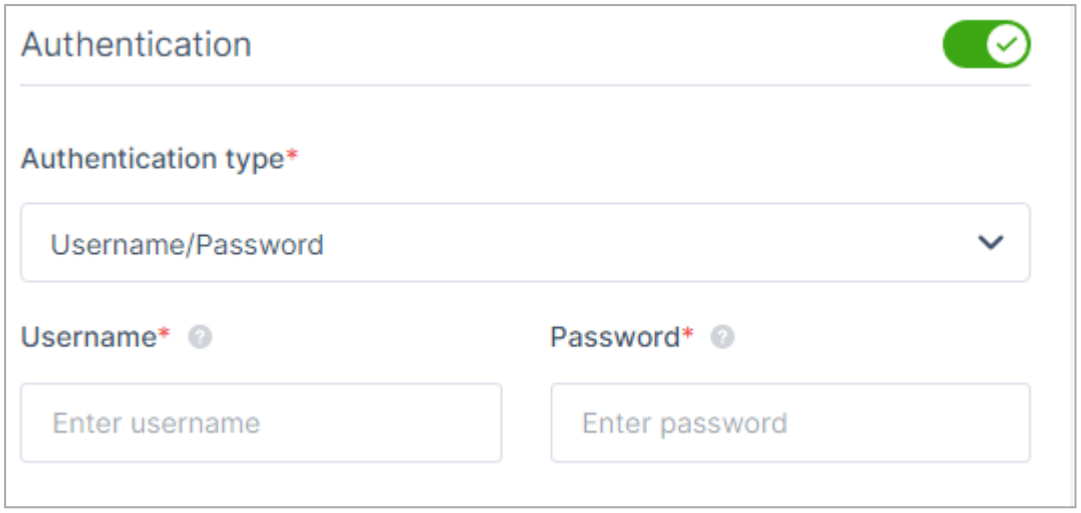
j. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

k. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

Under your domain, use the CMANE specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.




4. In the **Authentication** section, select the **Authentication type**:



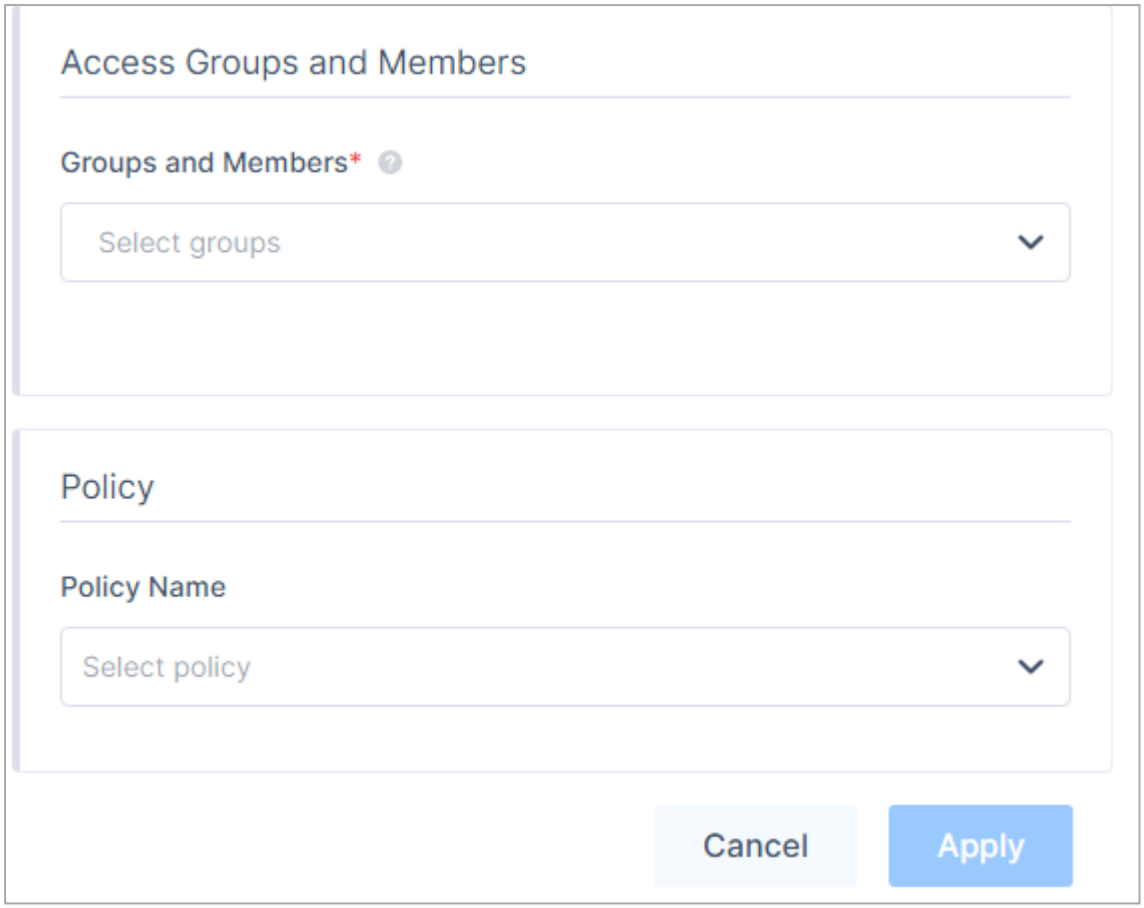

- For **Username/Password**, enter the username and password as predefined on the server.
- For **Private Key/Username/Passphrase**, enter these:
  a. **Username**: Username predefined on the server.
  b. **Private Key**: Your RSA-SSH key. Note that a certificate typically starts with a prefix and a suffix such as the following:

     ```
     -----BEGIN RSA PRIVATE KEY-----
     -----END RSA PRIVATE KEY-----
     ```

  c. **Passphrase**: The passphrase set with SSH key. If there is no passphrase, leave as blank.

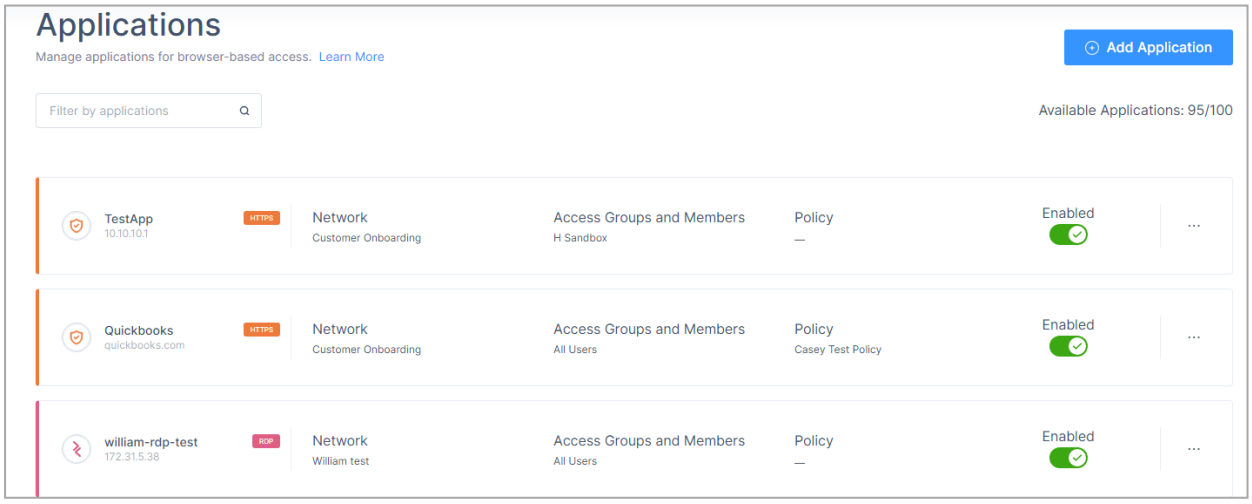
**Note** - If you disable **Authentication**, then the member must enter the credentials when accessing the machine.

5. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.




6. (Recommended) In the **Policy Name** list, select an application policy.
7. Click **Apply**.

   The system lists the application in the **Applications** page and enables it by default.




8. For members to access the application, see *"Accessing an Application by a Member" on page 190*.

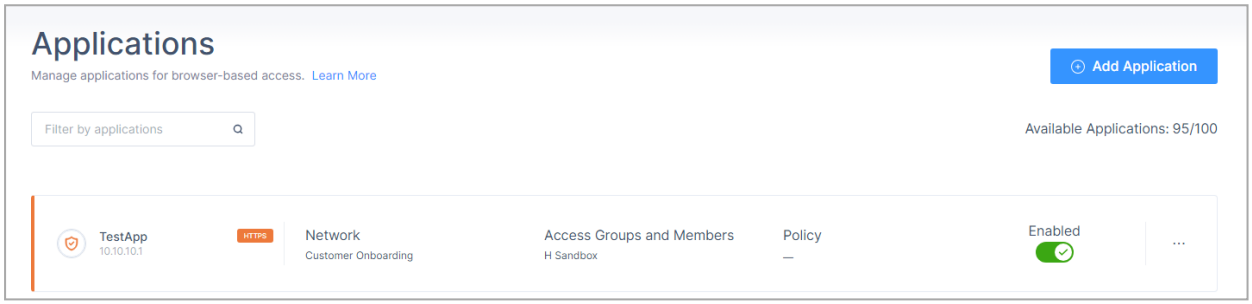
# Adding a VNC Zero Trust Application

## Prerequisite

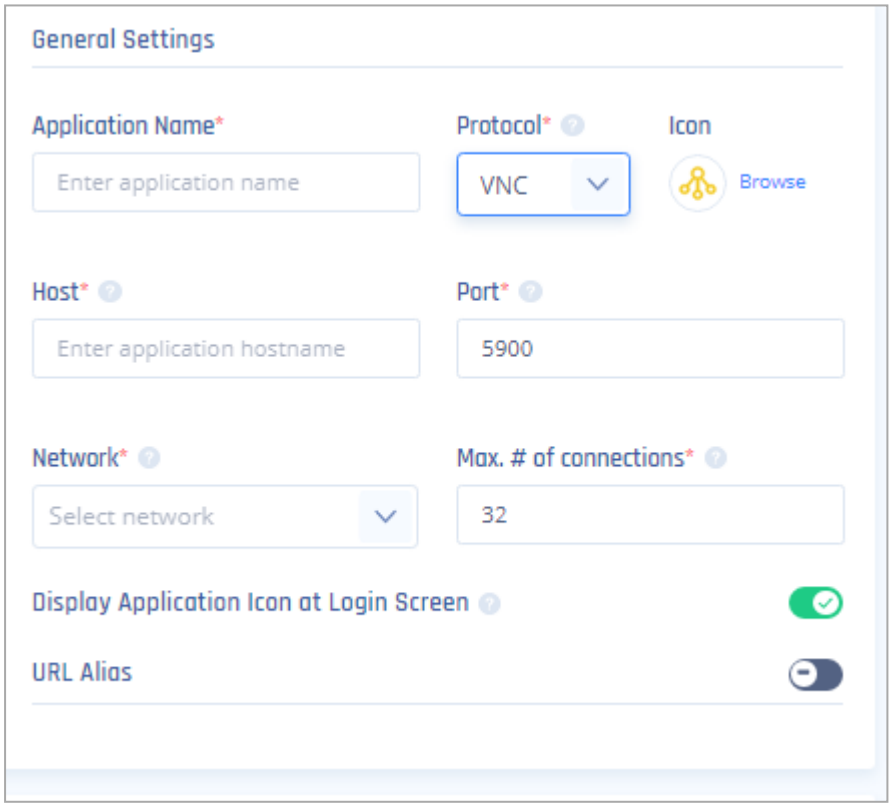
Make sure you have the credentials to access the application over VNC.

### To add a VNC Zero trust Application:

1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click **Add Application**.




The **Add application** window appears.




3. In the **General Settings** section, enter these:

a. **Application Name** - Name of the application.

b. **Protocol** - VNC

c. **Icon** - Icon for the application.

d. **Host** - Internal IP address of the server to which you want to connect.

e. **Port** - 5900

f. **Network** - Network that hosts the application.

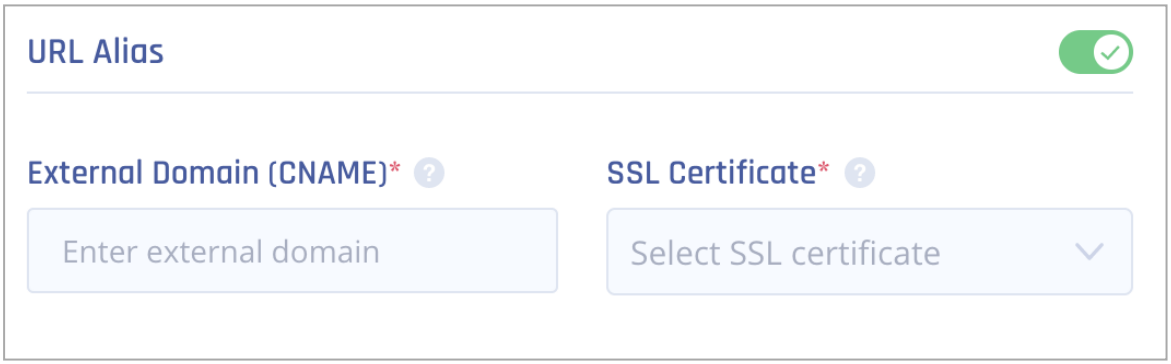
g. **Max number of connections**: 1

h. (Optional) **Display Application Icon at Login Screen** - Displays the application icon for the member in the login page.

i. (Optional) **Enable copy-paste from VNC to clipboard** - Enables to copy data from VNC to clipboard.

j. (Optional) **URL Alias** - URL for members to access the application.

**Important** - You cannot add a URL alias after you create the application.

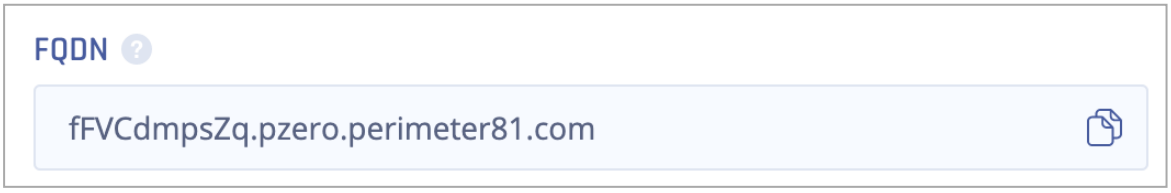



k. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

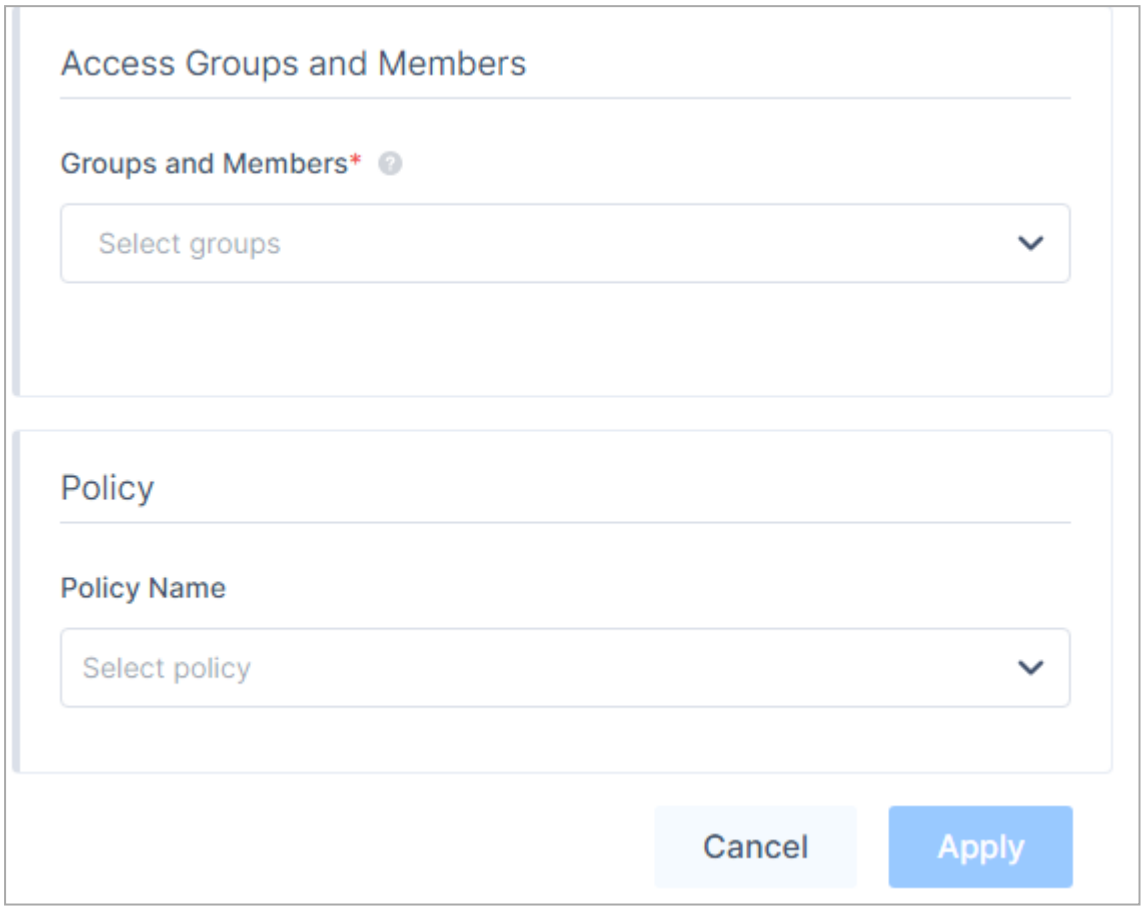
l. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

m. Go to your DNS administrator (for example, GoDaddy or R53 in AWS).

Under your domain, use the CMANE specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.

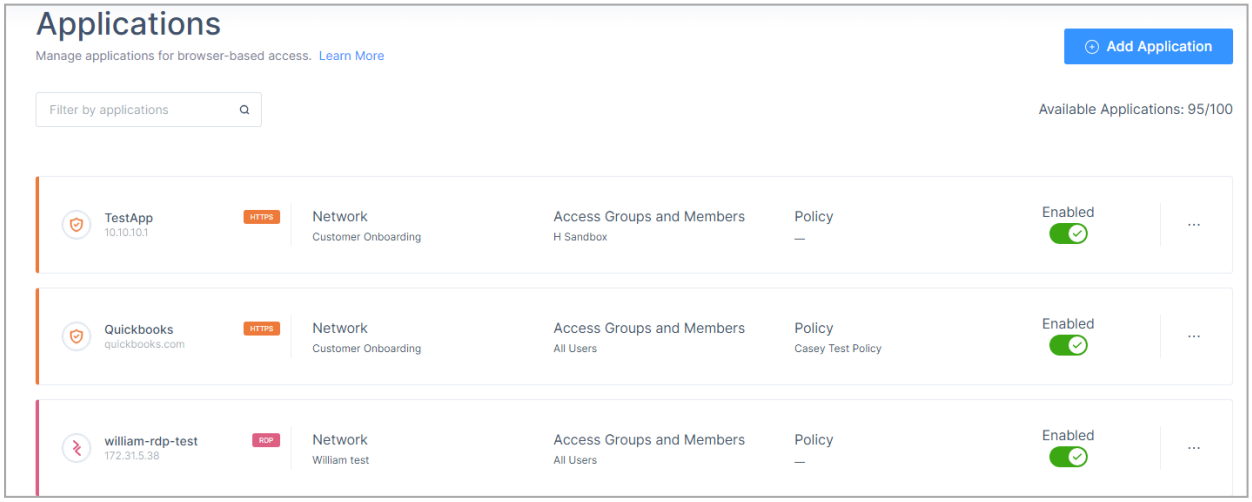


4. In the **Authentication** section, in the **Password** field, enter the password predefined in your VNC.
5. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.




6. (Recommended) In the **Policy Name** list, select an application policy.
7. Click **Apply**.

   The system lists the application in the **Applications** page and enables it by default.

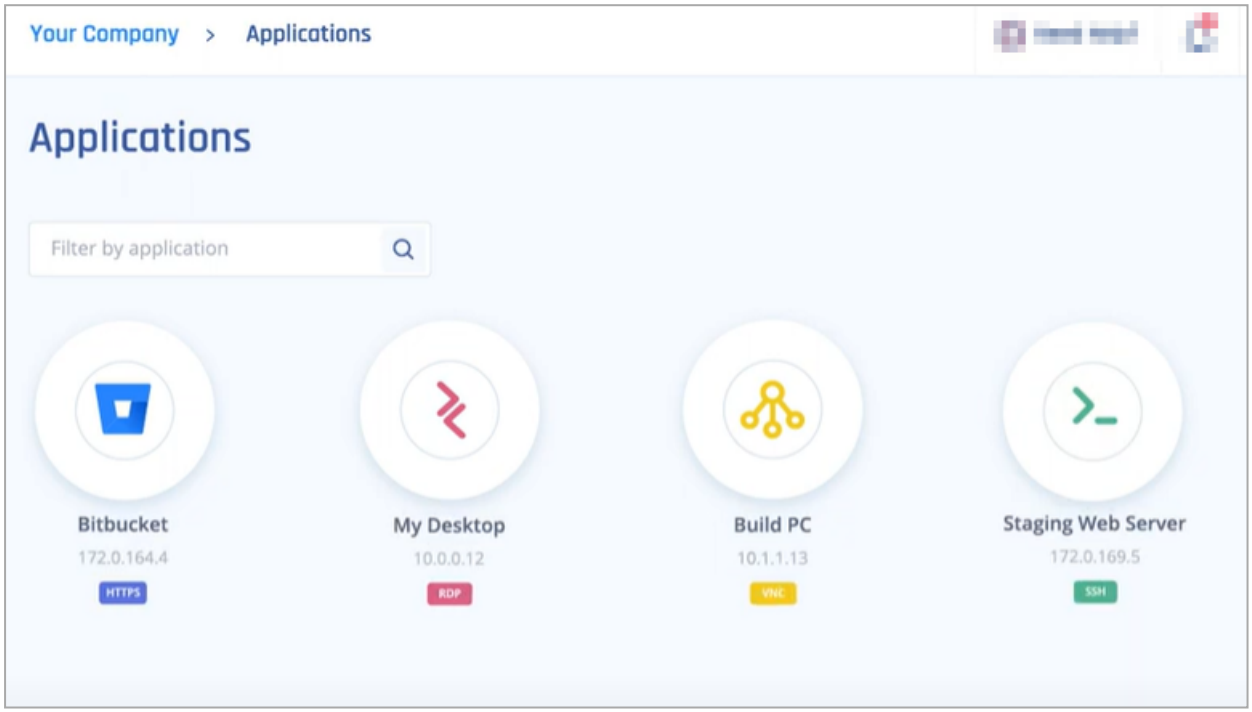


8. For members to access the application, see *"Accessing an Application by a Member" on page 190*.

# Accessing an Application by a Member

1. Share your Harmony SASE Administrator Portal URL and its credentials with your members or third-party users.
2. After your members or third-party sign in to the Harmony SASE Administrator Portal, navigate to **Private Access** > **Applications**.

   The system shows the authorized applications.

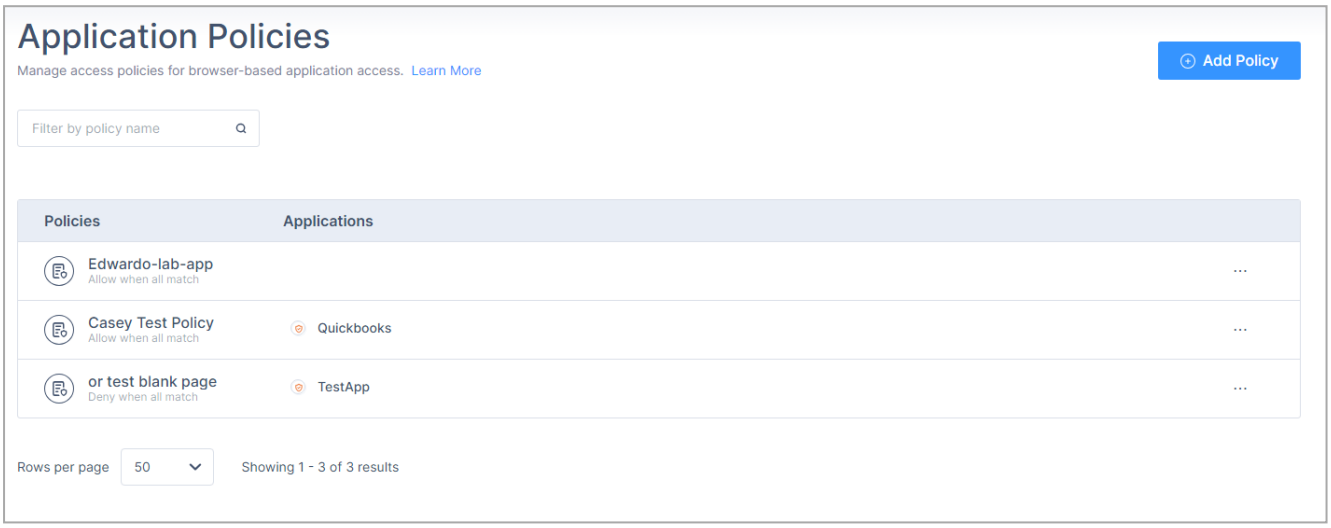



3. Click the application to access it.

# Application Policies

The **Application Policies** page allows you create policies to grant authorized users permission to access applications.

To view the **Application Policies** page, access the Harmony SASE Administrator Portal and click **Private Access** > **Application Policies**.



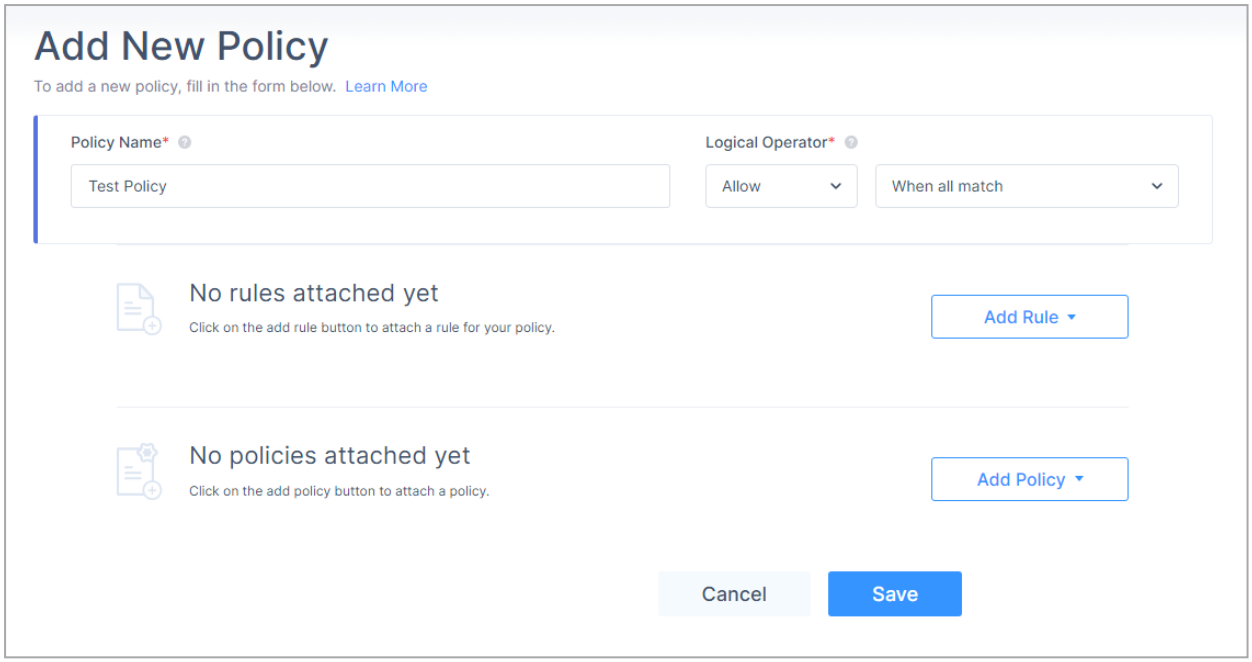

**Best Practices -**

- Review your policies periodically to align with your organizational requirements.
- Test policies on a small test group before enforcing it at the organizational level.

## Creating an Application Access Policy

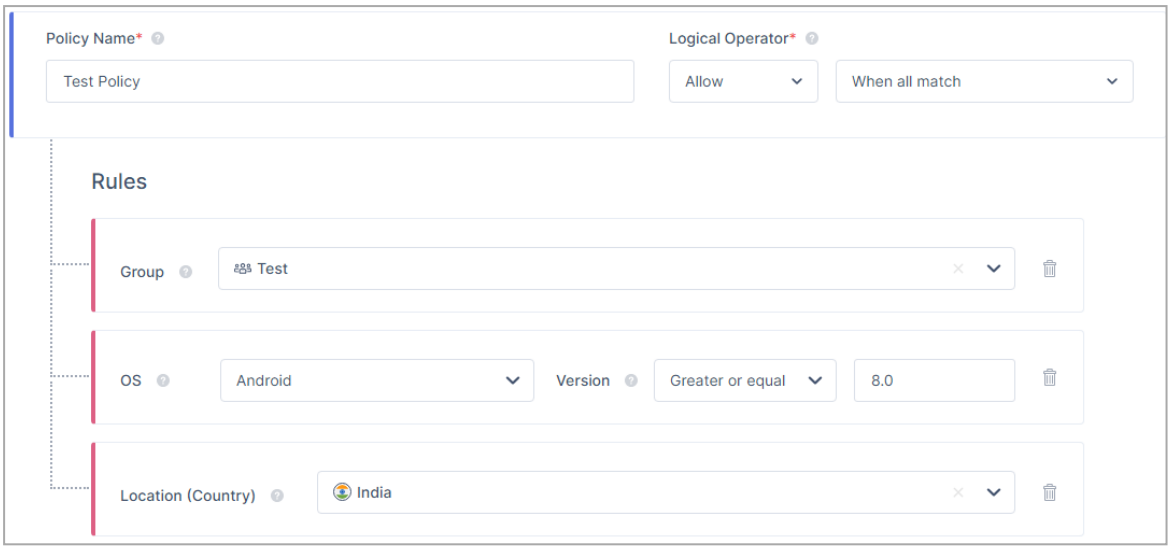
1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Application Policies**.
2. Click **Add Policy**.

   The **Add New Policy** page appears.




3. Enter these:
   a. **Policy Name** - Name of the policy.
   b. **Logical Operator** - Policy action:
      - **Allow**
      - **Deny**
   c. Select the condition to apply the policy.
4. To add the rules for the policy, click **Add Rule** and specify these:
   - Group
   - Date and Time
   - Location (IP)
   - Location (Country)
   - Browser

- OS and Version

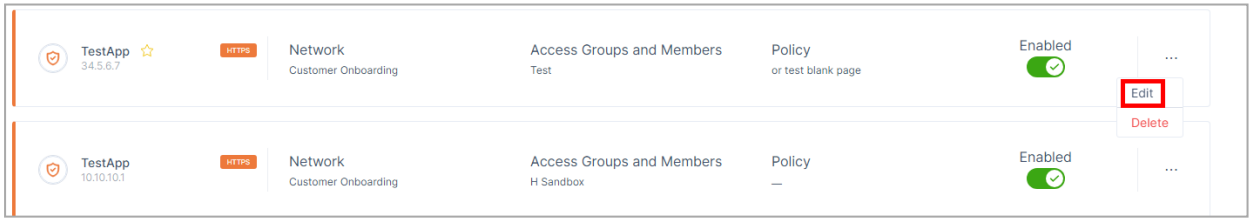



5. To attach an existing policy with the new policy, click **Add Policy** and select a policy.
6. Click **Save**.

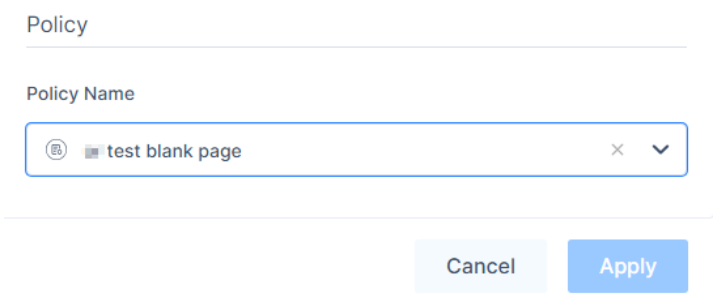
The new policy is listed in your **Policy** page.

## Assigning a Policy to an Application

1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Applications**.
2. Click ··· for the application and click **Edit**.




3. In the **Policy** section, from the **Policy Name** list, select a policy.




4. Click **Apply**.

# Internet Access

Internet Access allows you to configure:

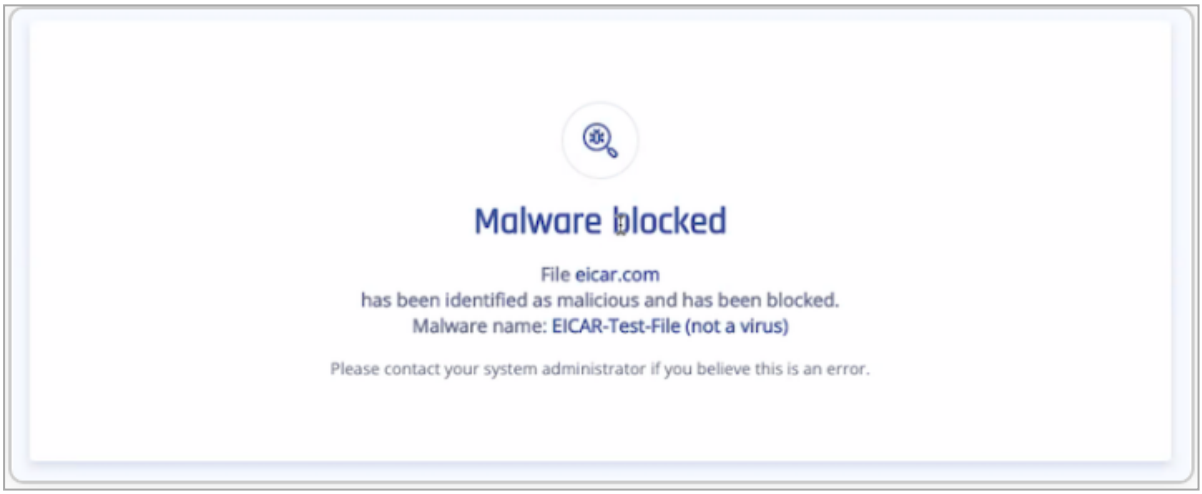
- Web Filter Rules
- Bypass Rules

The Web Filter Rules are directly applied on the device through the Harmony SASE Agent. The agent uses the in-built Secure Web Gateway (SWG) equipped with a Malware Protection Engine that:

- Scans the file and blocks access if it is malicious.
- Scans the traffic on the device without affecting the SWG performance.

**Notes**:

- The Malware Protection Engine can scan files less than 10 MB only.




- This is applicable only to internet traffic through a browser.
- The SWG inspects TLS traffic through the Harmony SASE Agent on port 443.

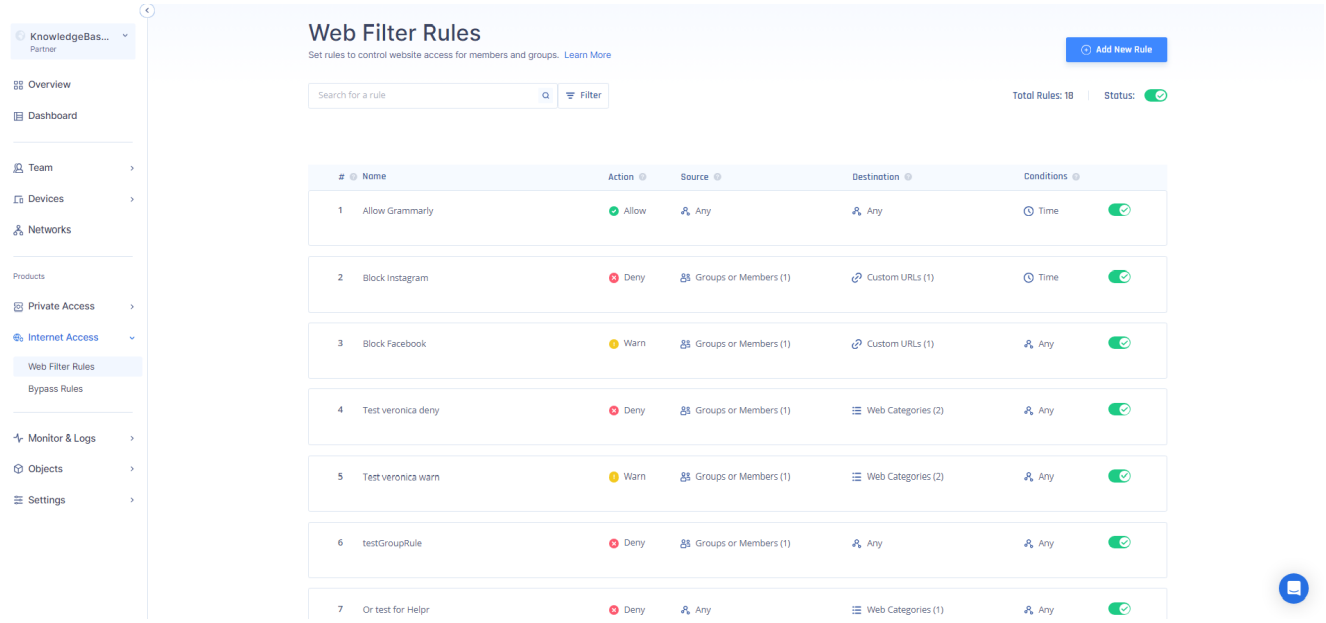
# High-level Procedure

1. Create your internet access policy. See *"Web Filter Rules" on page 195*.
2. (Optional) Configure bypass rules. See *"Bypass Rules" on page 202*.
    a. Configure the Secure Web Gateway (SWG) to bypass applications known to utilize certificate pinning. For more information, see *"Bypass Rules for Certificate Pinning" on page 211*.

# Web Filter Rules

The **Web Filter Rules** page allows you to create internet access policies.

To view the **Web Filter Rules** page, access the Harmony SASE Administrator Portal and click **Internet Access** > **Web Filter Rules**.

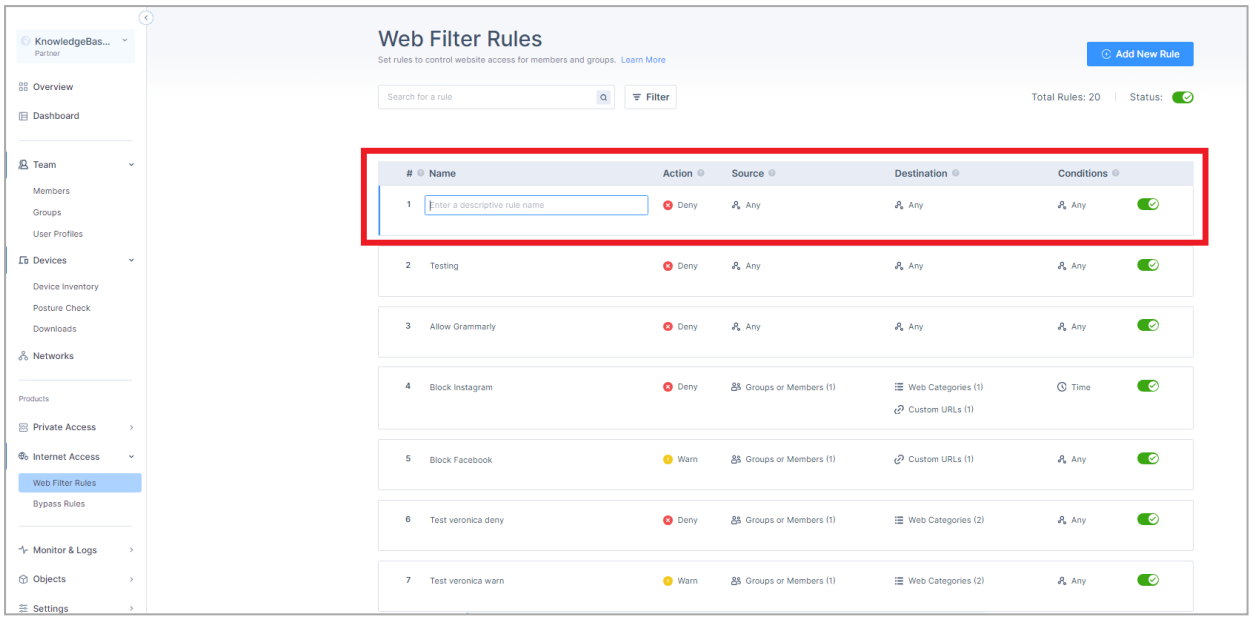



| Column | Description |
|---|---|
| Name | Name of the Rule. |
| Action | Action for web traffic:<br>■ **Deny** - Blocks web traffic.<br>■ **Allow** - Permits web traffic.<br>■ **Warn** - Allows web traffic and logs the event. See Web Activity. |
| Source | Groups or members to which the rule is applied. |
| Destination | Destination of the web traffic generated by the source (**Managed categories** and/or **Custom URLs**). |
| Conditions | Condition for the rule. |

## Creating a Web Filter Rule

1. Access the Harmony SASE Administrator Portal and click **Internet Access** > **Web Filter Rules**.
2. Click **Add New Rule**.

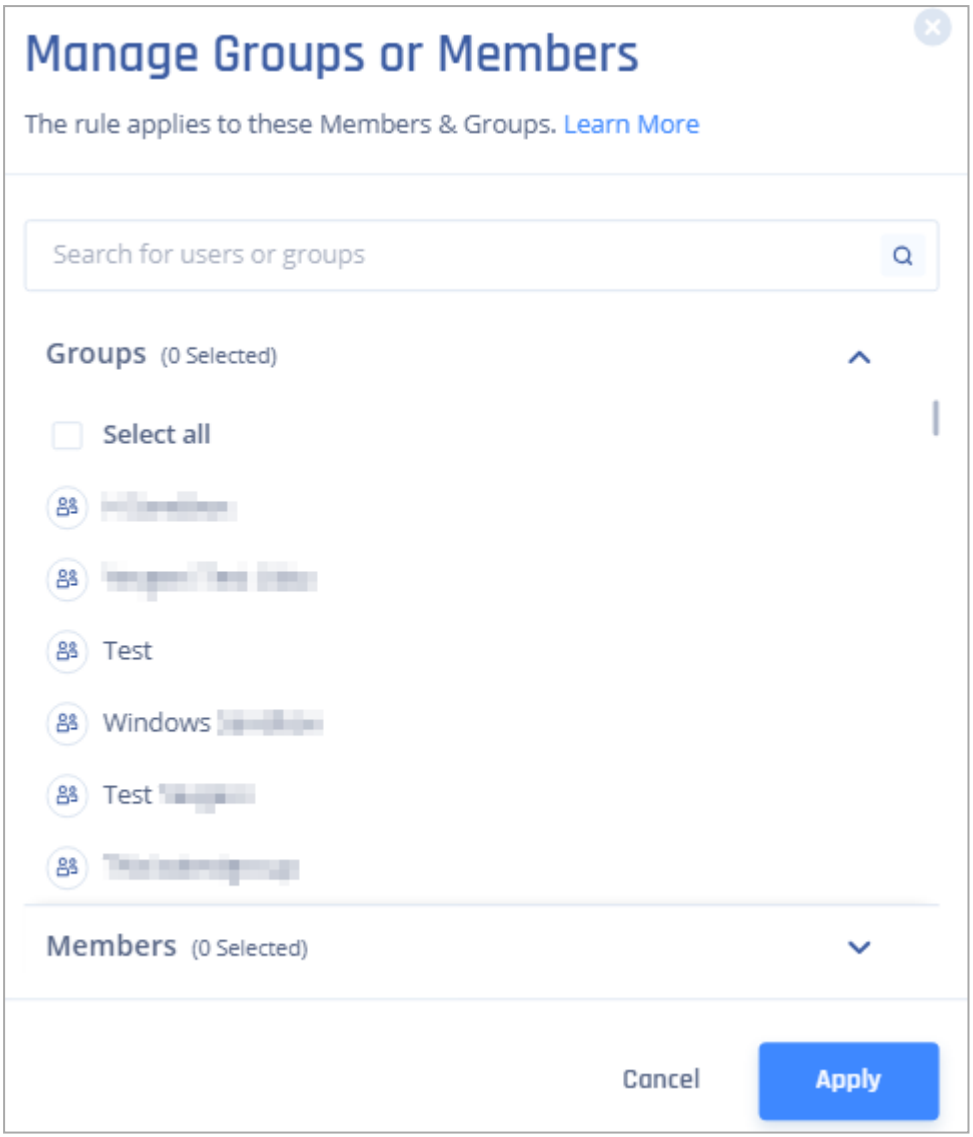
A new rule appears in the table.




3. In the **Name** field, enter a name for the rule.
4. From the **Action** list, select one:
   - **Deny** (default)
   - **Allow**
   - **Warn**

   **Notes**:
   - The Secure Web Gateway (SWG) do not support wildcards. However, you can block the domain and its subdomains within the same object.
   - URLs containing protocols, queries, parameters, or anchors are not supported.
5. In the **Source** field, add user or group list to which you want to apply the rule. Default is **Any**.

a. Click **Any** > **Add Source** > **Groups or Members**.




b. Select group(s) or member(s) from the list.

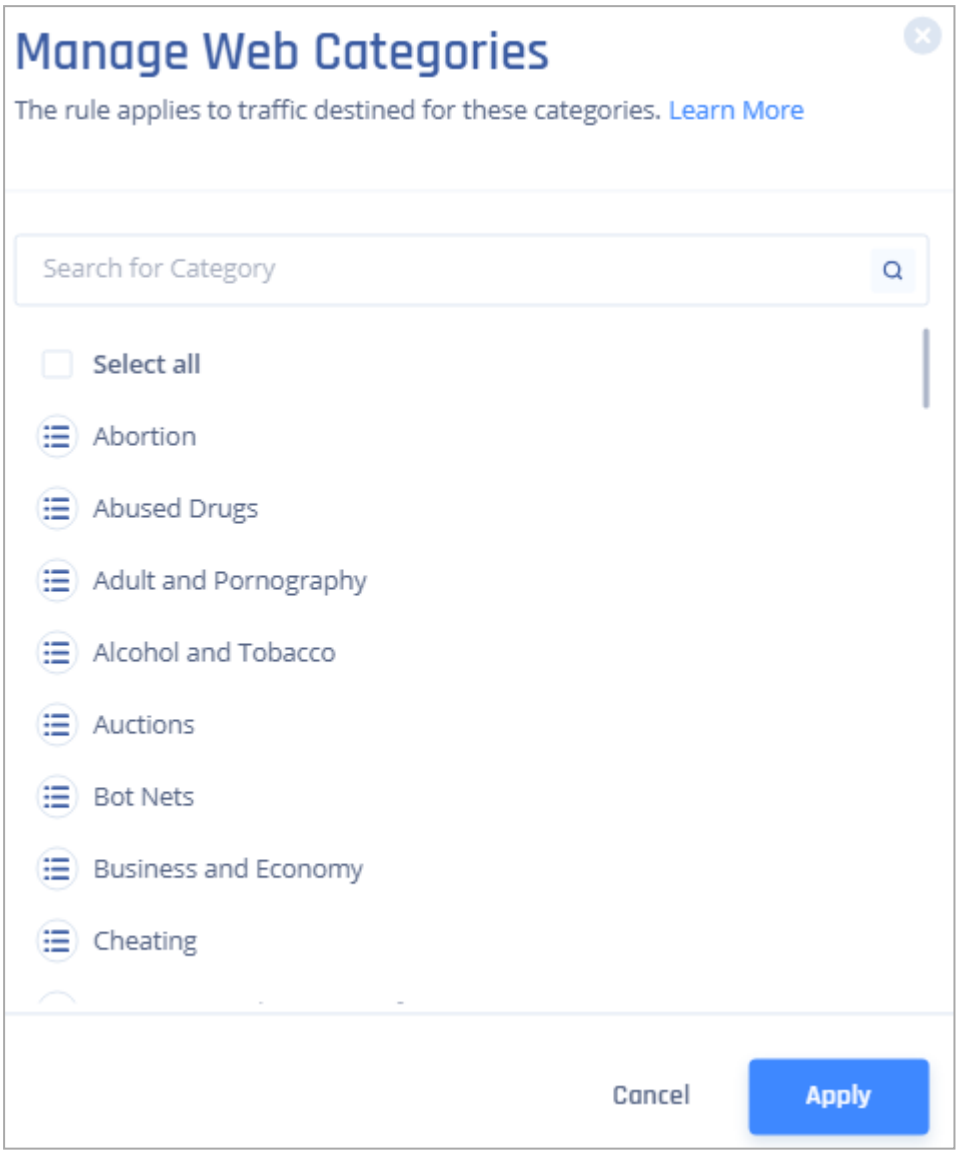
c. Click **Apply**.

6. In the **Destination** field, select the destination. Default is **Any**.

a. Click **Any** > **Add Destination.**

b. To add web categories, select **Web Caregories**.

The **Manage Web Categories** window appears.

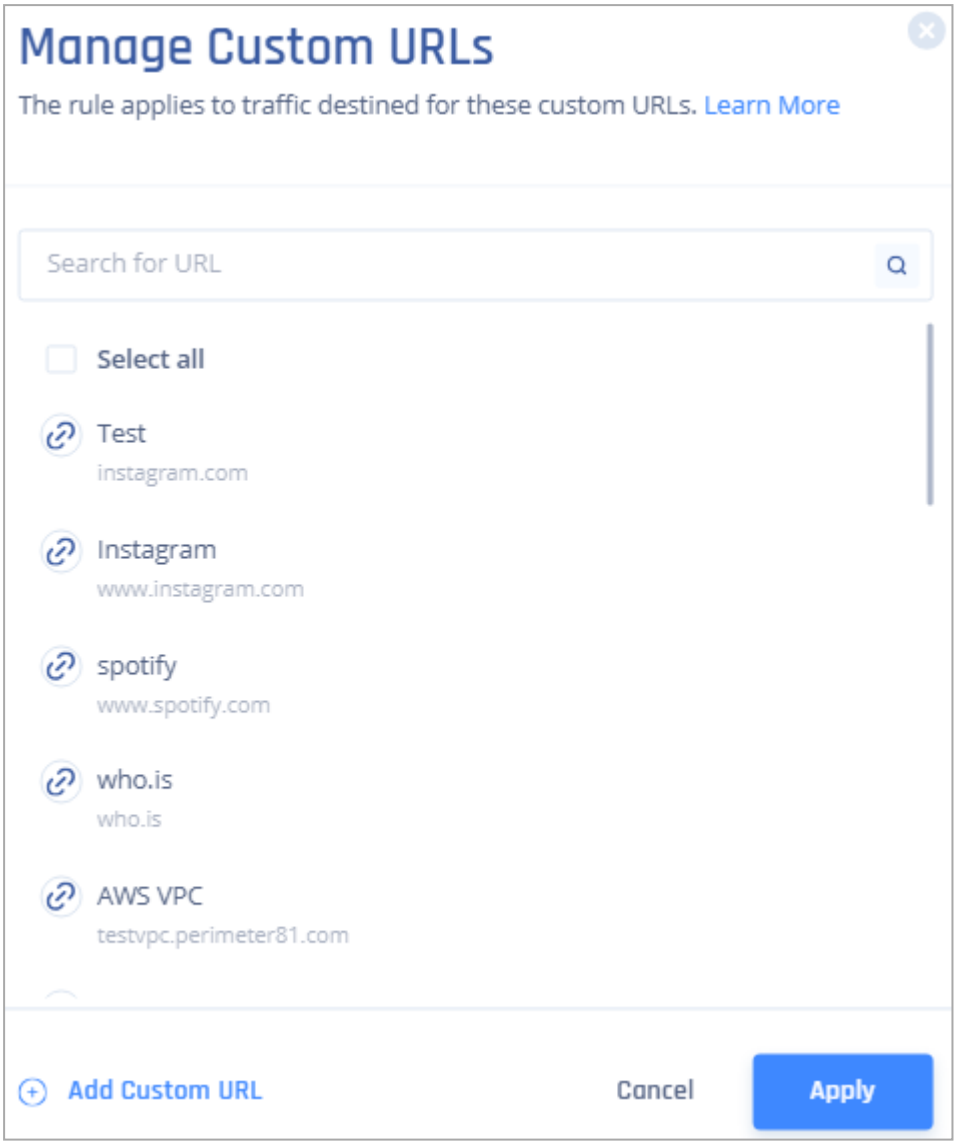



c. Select the categories from the list.

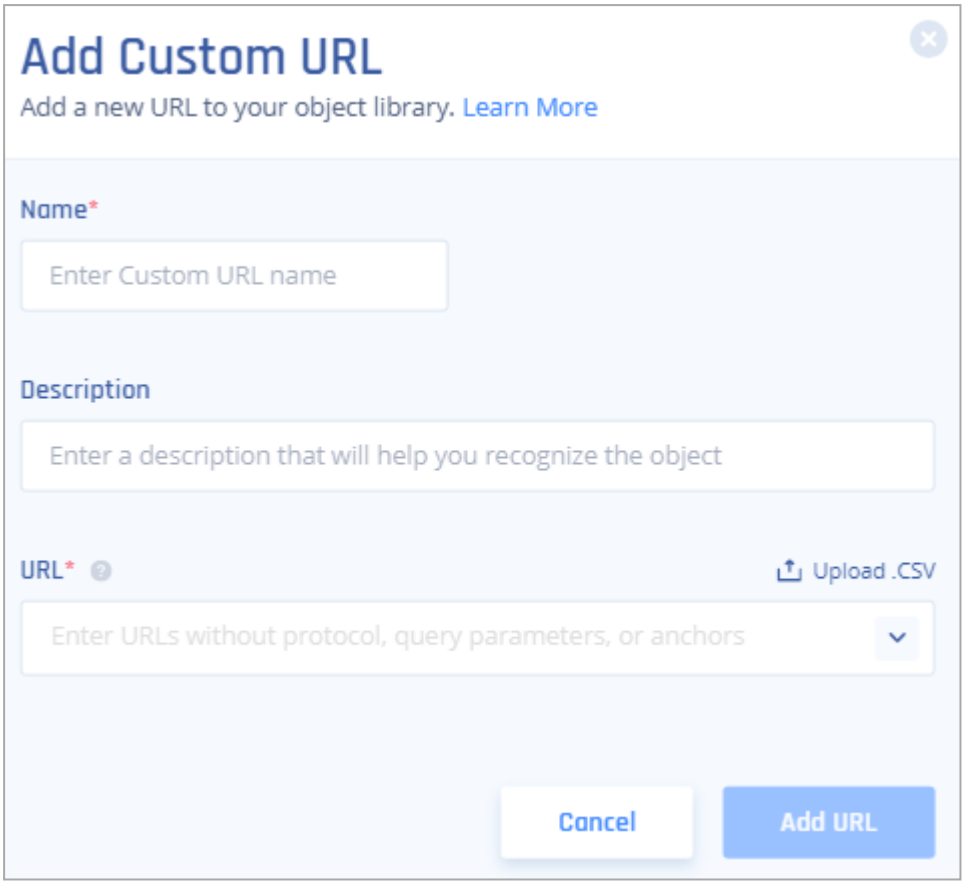
d. Click **Apply**.

e. To add custom URLs, select **Custom URLs**.

The **Manage Custom URLs** window appears.



f. Select the custom URL. If the URL is not listed, click **Add Custom URL** and specify these and click **Add URL**:




- **Name**
- **Description**
- **URL**

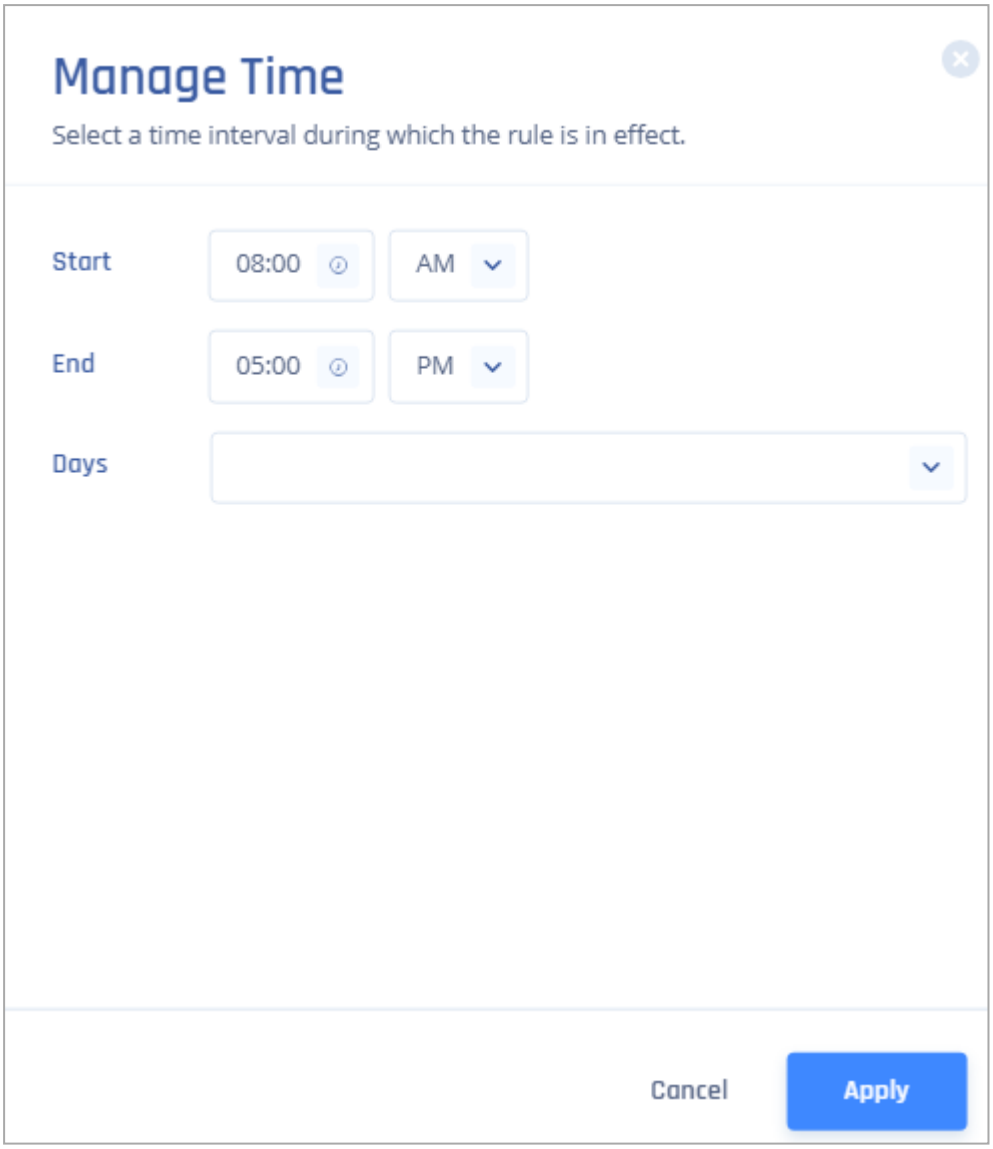
Optionally, click **Upload .CSV** to upload a .csv file with list of URLs.

g. Click **Apply**.

7. In the **Conditions** field, specify the duration for which the rule must be active.

a. Click **Any** > **Add Condition** > **Time**.

The **Manage Time window** appears.




b. Select the **Start** time from the list.

c. Select the **End** time from the list.

d. Select the **Days** from the list.

e. Click **Apply**.

8. Turn on the **Status** toggle button.
9. Click **Apply** in the bottom of the page.

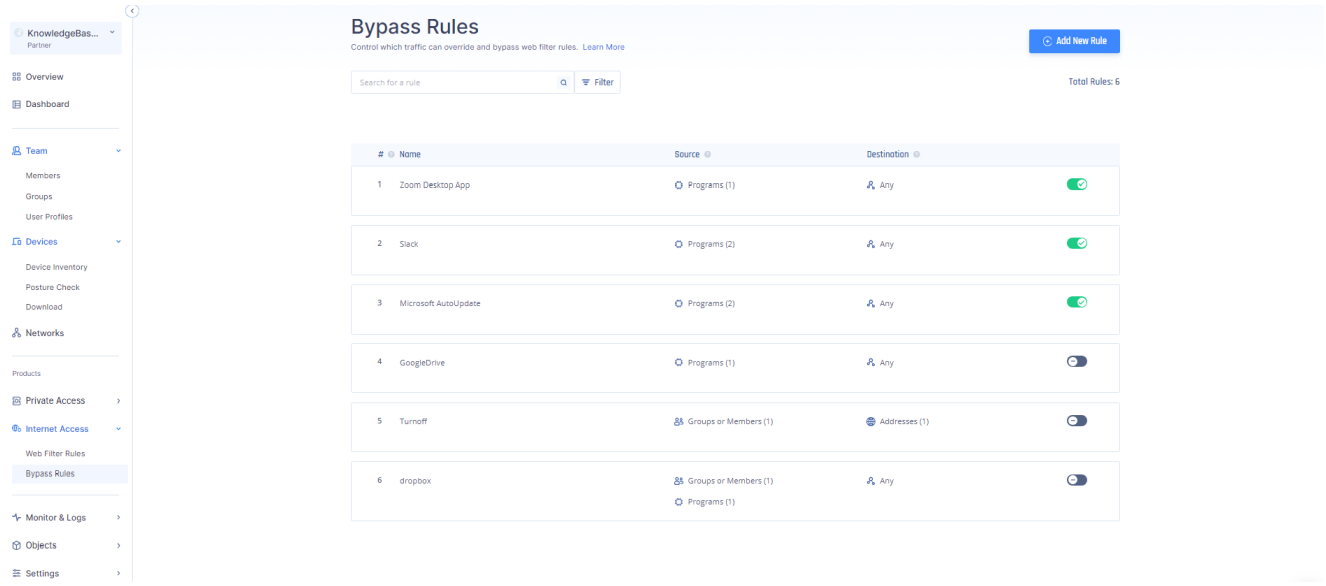



10. Click **Apply**.

# Bypass Rules

The **Bypass Rules** page allows you to specify traffic that must be ignored by the Web Filtering Rules.

To view the **Bypass Rules** page, access the Harmony SASE Administrator Portal and click **Internet Access** > **Bypass Rules**.

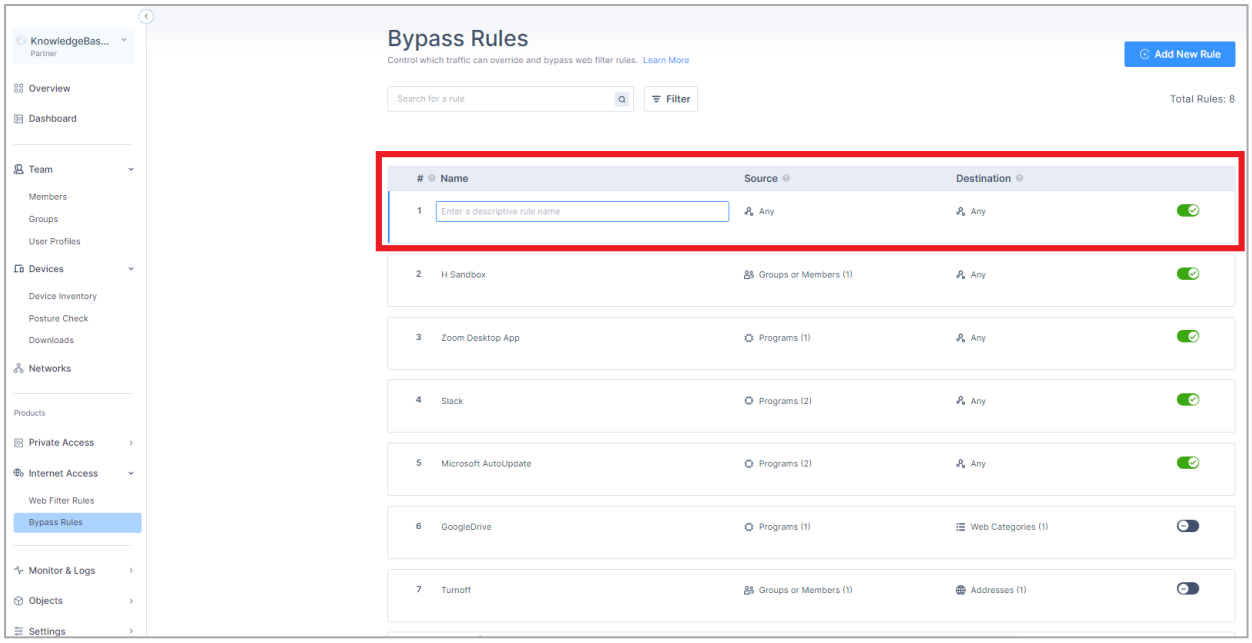



| Column | Description |
|---|---|
| Name | Name of the rule. |
| Source | Programs, groups or members to which the bypass rule is applied. |
| Destination | Destination of the web traffic. |

## Creating a Bypass Rule

1. Access the Harmony SASE Administrator Portal and click **Internet Access** > **Bypass Rules**.
2. Click **Add New Rule**.

   A new rule appears in the table.

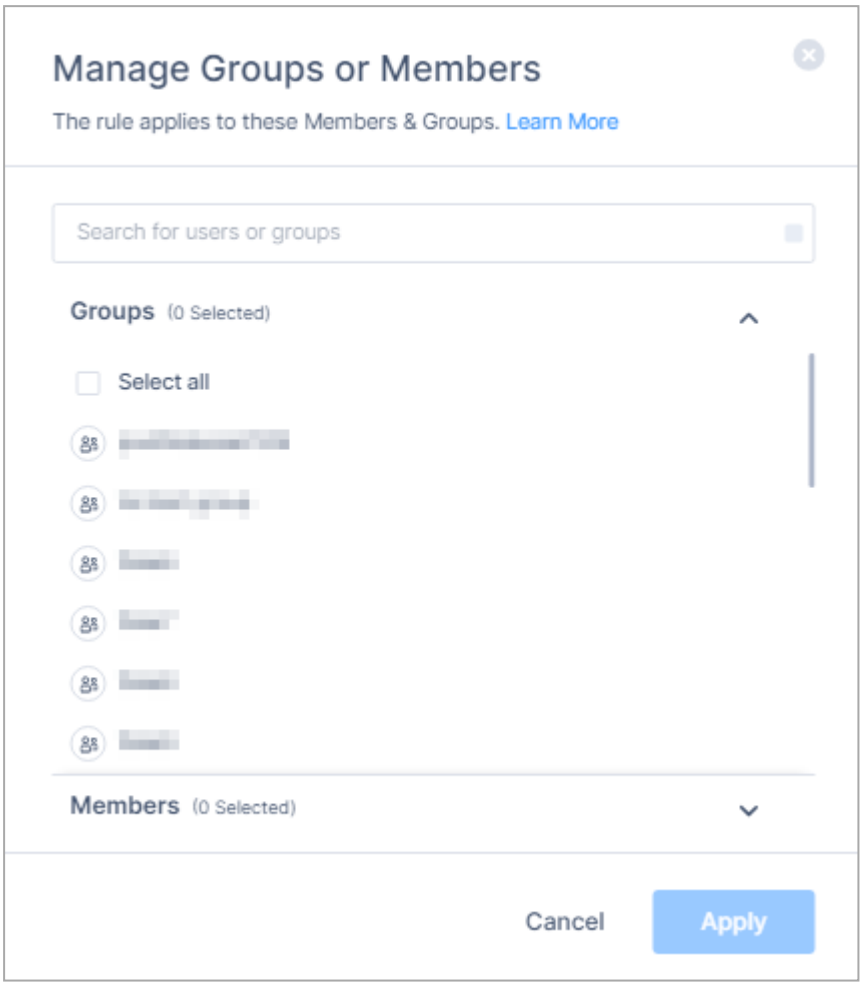



3. In the **Name** field, enter a name for the rule.
4. In the **Source** field, add user or group list to which you want to apply the rule. Default is **Any**.

a. Click **Any** > **Add Source**.

b. To add groups or members, select **Groups or Members**.

The **Manage Groups or Members** window appears.

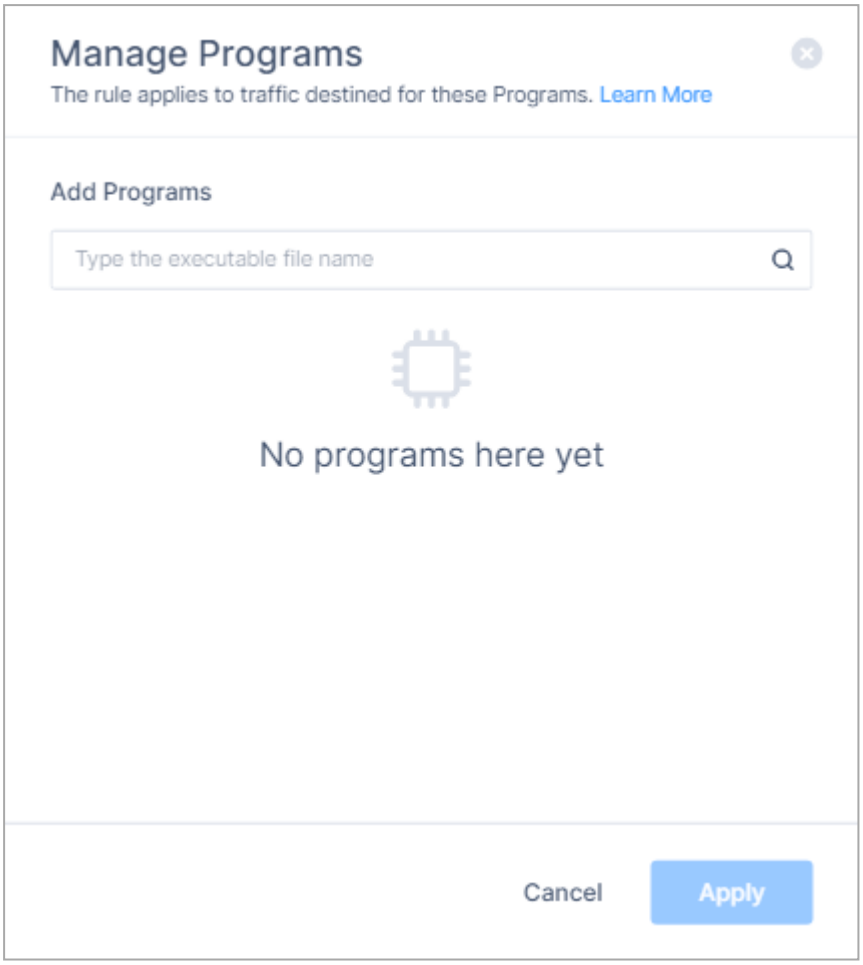



c. Select group(s) or member(s) from the list.

d. Click **Apply**.

e. To add programs, select **Programs**.

The **Manage Programs** window appears.




f. Enter the program name and press **Enter**.

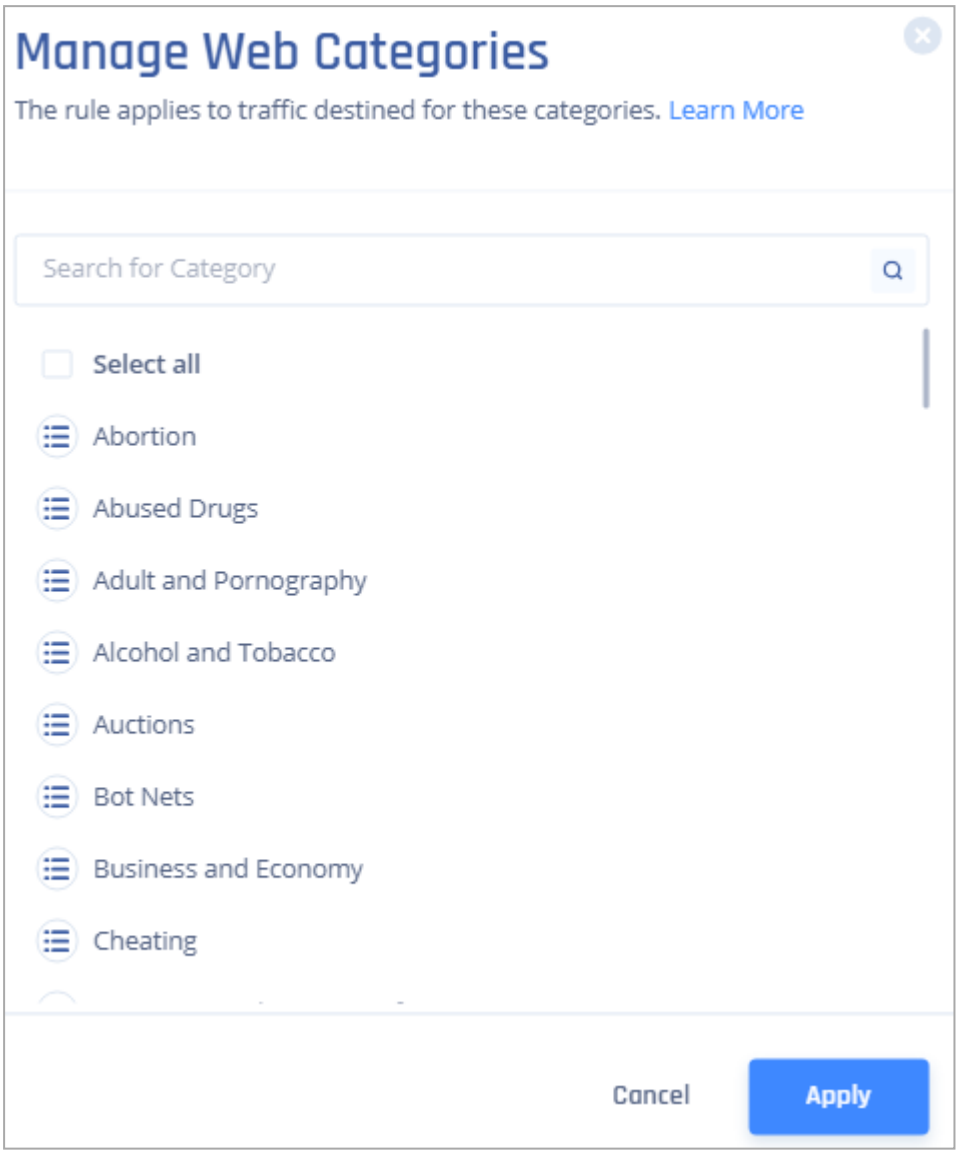
g. Click **Apply**.

5. In the **Destination** field, select the destination. Default is **Any**.

a. Click **Any** > **Add Destination.**

b. To add web categories, select **Web Categories**.

The **Manage Web Categories** window appears.

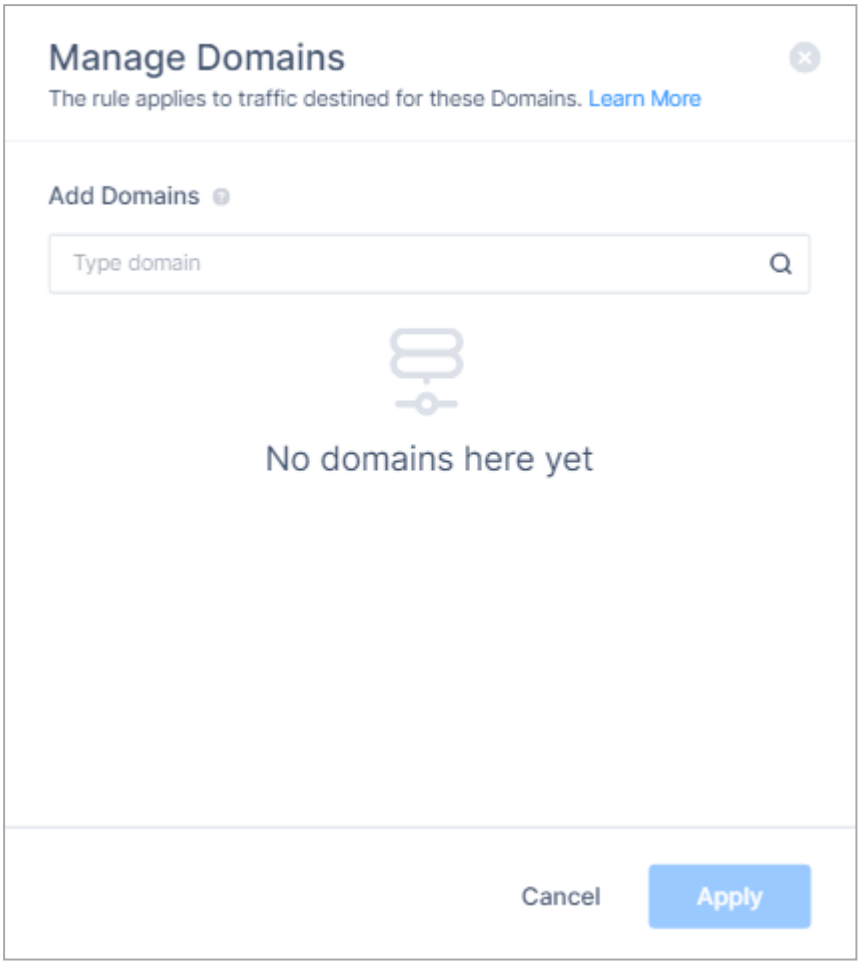



c. Select the categories from the list.

d. Click **Apply**.

e. To add domains, select **Domains**.

The **Manage Domains** window appears.

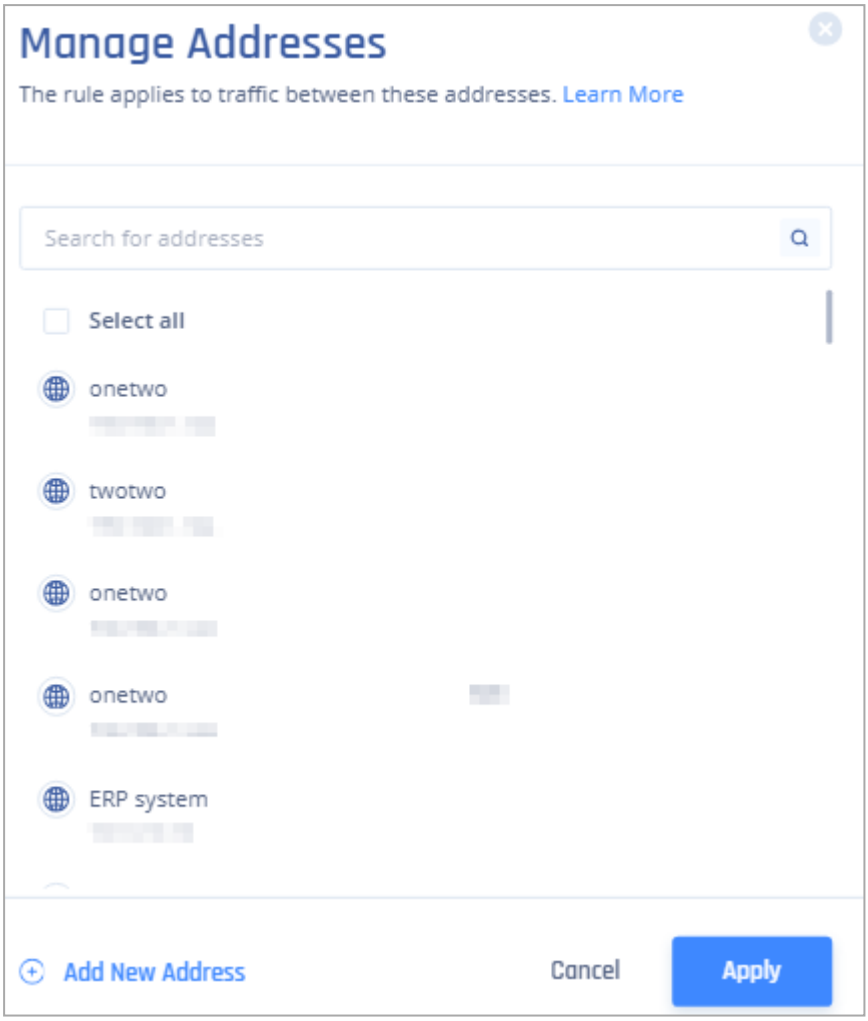



f. Enter the domain name and press **Enter**. For example, `google.com`.

g. Click **Apply**.

h. To add addresses, click **Addresses**.

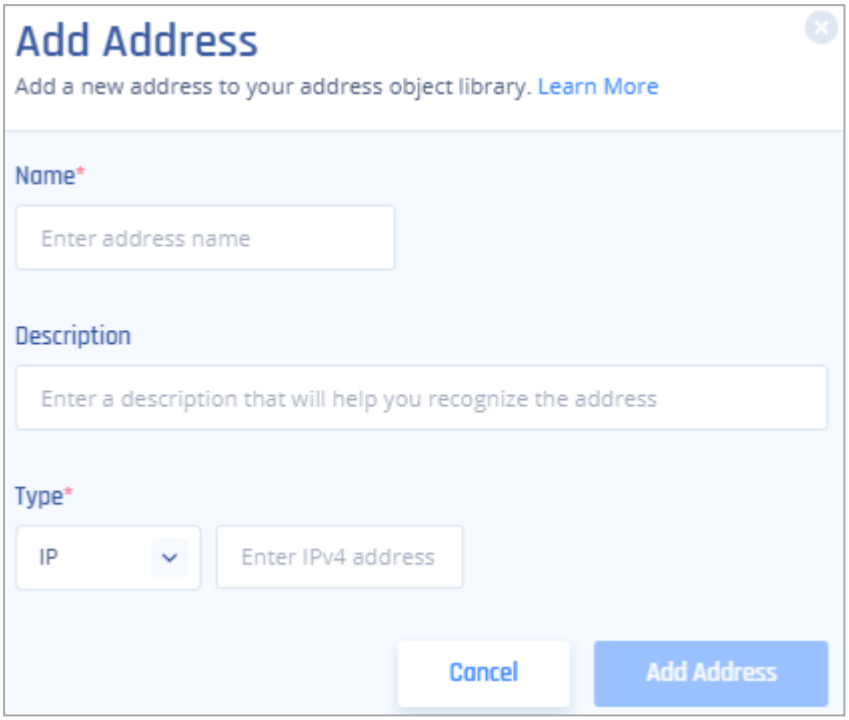
The **Manage Addresses** window appears.




i. Select the address from the list and click **Apply**.

j. To add address, click **Add New Address**.

The **Add Address** window appears.




k. In the **Name** field, enter address name.

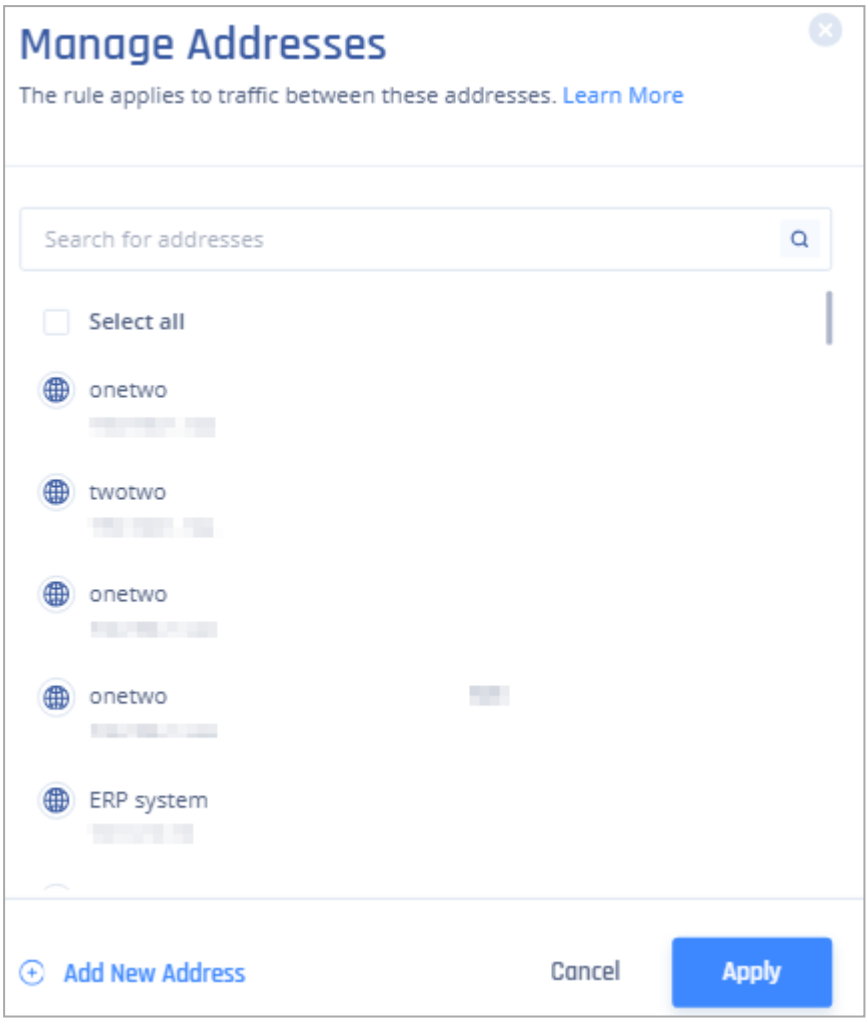
l. In the **Description** field, enter a description.

m. In the **Type** list, select **IP**, **Subnet**, **List**, or **FQDN**.

n. Enter a value, For example:

- For IP, enter the IPv4 address *139.1.1.1*.
- For subnet, enter *10.10.10.0/24*.
- For list, enter IP addresses separated by commas *172.16.254.1, 172.16.254.2*.
- For FQDN, enter the Fully Qualified Domain Name *www.example.com*.

o. Click **Add Address**.




p. Select the address from the list and click **Apply**.

q. Turn on the **Status** toggle button.

r. Click **Apply** in the bottom of the page.




s. Click **Apply**.

# Bypass Rules for Certificate Pinning

Certificate pinning is a security technique used by applications to ensure sever's certificate adheres to certain rules to enhance data security against potential threats. As a result, these applications may not recognize the Harmony SASE certificate as valid and blocks the connection.

Check Point recommends to use process name or domain to bypass the traffic to applications that use certificate pinning.

The table lists some of the popular applications that use certificate pinning and provides their domains to bypass:

| Application | Program | Domain |
|---|---|---|
| Adobe Suite (including Acrobat Reader, Creative Cloud and software updates) | N/A | Fill in these domain lists:<br>■ List 1<br>■ List 2 |
| Apple's iMessages, iTunes, App Store, Mail | N/A | ■ p24-keyvalueservice.icloud.com<br>■ apps.apple.com<br>■ itunes.apple.com<br>■ mzstatic.com<br>■ gs-loc.apple.com<br>■ gsa.apple.com<br>■ securemetrics.apple.com<br>■ swscan.apple.com<br>■ xp.apple.com<br>■ icloud.com<br>■ ppq.apple.com<br>■ akadns.net |

| Application | Program | Domain |
|---|---|---|
| AWS Console | N/A | ▪ console.aws.amazon.com<br>▪ docs.aws.amazon.com<br>▪ signin.aws.amazon.com<br>▪ signin.aws.amazon.com<br>▪ fls-na.amazon.com<br>▪ cdn.assets.as2.amazonaws.com<br>▪ aws-signin-website-assets.s3.amazonaws.com<br>▪ opfcaptcha-prod.s3.amazonaws.com<br>▪ d1dgtfo2wk29o4.cloudfront.net<br>▪ Images-na.ssl-images-amazon.com |
| Bitdefender | N/A | ▪ cdn.bitdefender.net<br>▪ download.bitdefender.com<br>▪ login.bitdefender.net<br>▪ login.bitdefender.com<br>▪ nimbus.bitdefender.net<br>▪ push.bitdefender.net<br>▪ upgrade.bitdefender.com |
| DropBox | ▪ **Windows** - dropbox.exe, dropboxupdate.exe<br>▪ **macOS** - com.getdropbox.dropbox | N/A |
| Evernote | evernote.exe | ▪ announce.evernote.com<br>▪ cd1. evernote.com<br>▪ evernote-a.akamaihd.net<br>▪ www.evernote.com |
| Google Drive | ▪ **Windows** - googledrivesync.exe, GoogleDriveFS.exe<br>▪ **macOS** - com.google.drivefs, com.google.drivefs.finderhelper.findersync | N/A |

| Application | Program | Domain |
|---|---|---|
| Google Services | N/A | ■ accounts.google.com<br>■ alt2-mtalk.google.com<br>■ android.clients.google.com<br>■ www.google.com<br>■ android.googleapis.com<br>■ cryptauthenrollment.googleapis.com<br>■ device-provisioning.googleapis.com<br>■ digitalassetlinks.googleapis.com<br>■ fcmconnection.googleapis.com<br>■ fcmtoken.googleapis.com<br>■ firebaseperusertopics-pa.googleapis.com<br>■ play.googleapis.com<br>■ semanticlocation-pa.googleapis.com<br>■ lh3.googleusercontent.com<br>■ play-lh.googleusercontent.com<br>■ gstatic.com<br>■ gvt1.com |
| Java Updates | N/A | ■ sjremetrics.java.com<br>■ javadl-esd-secure.oracle.com |
| LogMeIn | logmein.exe | Fill in this domain list. |
| Microsoft Defender | N/A | Fill in this domain list. |
| Microsoft Lync and Skype | N/A | ■ lync.com<br>■ az801095.vo.msecnd.net<br>■ i.s-microsoft.com |
| Microsoft Office365 | Configure within Office365:<br>Go to **Policy** > **URL & Cloud App Control** > **Advanced Settings**. | For outlook, add these domains:<br>■ office365.com<br>■ office.com |

| Application | Program | Domain |
|---|---|---|
| Microsoft OneDrive | N/A | ▪ cdn.funcaptcha.com<br>▪ fpt.live.com<br>▪ login.live.com<br>▪ odc.officeapps.live.com<br>▪ skyapi.policies.live.net<br>▪ signup.live.com<br>▪ skyapi.live.net<br>▪ pipe.aria.microsoft.com<br>▪ data.microsoft.com<br>▪ svc.ms<br>▪ msauth.net<br>▪ onedrive.com<br>▪ cdn.onenote.net |
| Microsoft Windows Store | N/A | ▪ eus-streaming-video-msn-com<br>▪ wns.windows.com<br>▪ live.com<br>▪ clientconfig.passport.net<br>▪ wustat.windows.com<br>▪ windowsupdate.com<br>▪ msftncsi.com<br>▪ microsoft.com |
| Microsoft Updates | N/A | ▪ login.live.com<br>▪ settings-win.data.microsoft.com<br>▪ vortex-win.data.microsoft.com<br>▪ delivery.mp.microsoft.com<br>▪ tsfe.trafficshaping.dsp.mp.microsoft.com<br>▪ update.microsoft.com<br>▪ sls.update.microsoft.com<br>login.microsoft.com |
| Slack | ▪ **Windows** - slack.exe<br>▪ **macOS** - com.tinyspeck.slackmacgap, com.tinyspeck.slackmacgap.helper | N/A |
| Spotify | N/A | spotify.com |

| Application | Program | Domain |
|---|---|---|
| Webex | atmrg.exe, wmlhost.exe, webexmta.exe, washost.exe | webex.com |
| Zoom | **Windows** - zoom.exe<br>**macOS** - us.zoom.xos | zoom.us |

## Default Bypass Rules

Harmony SASE provides a list of preconfigured bypass rules for applications that use certificate pinning.

To view the default bypass rules, access **Harmony SASE** and click **Internet Access** > **Bypass Rules**. The default bypass rules disappear if you add new bypass rules.

| Rule Name | Default Status | Domains | Categories |
|---|---|---|---|
| Bypass sensitive traffic - Pre-configured | Disabled | N/A | Financial Services, Government, Health and Medicine, Legal |
| Bypass Microsoft updates - Pre-configured | Enabled | ■ login.live.com<br>■ settings-win.data.microsoft.com<br>■ vortex-win.data.microsoft.com<br>■ delivery.mp.microsoft.com<br>■ tsfe.trafficshaping.dsp.mp.microsoft.com<br>■ update.microsoft.com<br>■ sls.update.microsoft.com<br>■ login.microsoft.com | N/A |
| Bypass Adobe updates - Pre-configured | Enabled | ■ adobe.com<br>■ adobetag.com | N/A |

| Rule Name | Default Status | Domains | Categories |
|---|---|---|---|
| Bypass Java updates - Pre-configured | Enabled | ▪ sjremetrics.java.com<br>▪ javadl-esd-secure.oracle.com | N/A |
| Bypass Mozilla Firefox updates - Pre-configured | Enabled | download-installer.cdn.mozilla.net | N/A |
| Bypass AWS console - Pre-configured | Enabled | ▪ console.aws.amazon.com<br>▪ docs.aws.amazon.com<br>▪ signin.aws.amazon.com<br>▪ signin.aws.amazon.com<br>▪ fls-na.amazon.com<br>▪ cdn.assets.as2.amazonaws.com<br>▪ aws-signin-website-assets.s3.amazonaws.com<br>▪ opfcaptcha-prod.s3.amazonaws.com<br>▪ d1dgtfo2wk29o4.cloudfront.net<br>▪ Images-na.ssl-images-amazon.com | N/A |
| Bypass Dropbox - Pre-configured | Enabled | ▪ dropbox.com<br>▪ dropboxapi.com<br>▪ previews.dropboxusercontent.com<br>▪ mmp.getdropbox.com | N/A |

| Rule Name | Default Status | Domains | Categories |
|---|---|---|---|
| Bypass Google services - Pre-configured | Enabled | ■ accounts.google.com<br>■ alt2-mtalk.google.com<br>■ android.clients.google.com<br>■ www.google.com<br>■ android.googleapis.com<br>■ cryptauthenrollment.googleapis.com<br>■ device-provisioning.googleapis.com<br>■ digitalassetlinks.googleapis.com<br>■ fcmconnection.googleapis.com<br>■ fcmtoken.googleapis.com<br>■ firebaseperusertopics-pa.googleapis.com<br>■ play.googleapis.com<br>■ semanticlocation-pa.googleapis.com<br>■ lh3.googleusercontent.com<br>■ play-lh.googleusercontent.com<br>■ gstatic.com<br>■ gvt1.com | N/A |
| Bypass OneDrive - Pre-configured | Enabled | ■ cdn.funcaptcha.com<br>■ fpt.live.com<br>■ login.live.com<br>■ odc.officeapps.live.com<br>■ skyapi.policies.live.net<br>■ signup.live.com<br>■ skyapi.live.net<br>■ pipe.aria.microsoft.com<br>■ data.microsoft.com<br>■ svc.ms<br>■ msauth.net<br>■ onedrive.com<br>■ cdn.onenote.net | N/A |

| Rule Name | Default Status | Domains | Categories |
|---|---|---|---|
| Bypass LogMeIn - Pre-configured | Enabled | ■ cdngetgo.com<br>■ expertcity.com<br>■ getgo.com<br>■ getgocdn.com<br>■ getgoservices.com<br>■ getgoservices.net<br>■ go2assist.me<br>■ gofastchat.com<br>■ goto-rtc.com<br>■ gotoassist.com<br>■ gotoassist.at<br>■ gotoassist.me<br>■ gotomeet.me<br>■ gotomeet.at<br>■ gotomeet.me<br>■ gotomeeting.com<br>■ gotomypc.com<br>■ gotostage.com<br>■ gototraining.com<br>■ gotowebinar.com<br>■ helpme.net<br>■ accounts.logme.in<br>■ joingotomeeting.com<br>■ jointraining.com<br>■ joinwebinar.com<br>■ logmein.com<br>■ logmeininc.com<br>■ logmeinrescue.com | N/A |
| Bypass Microsoft Lync and Skype - Pre-configured | Enabled | ■ lync.com<br>■ az801095.vo.msecnd.net<br>■ i.s-microsoft.com | N/A |

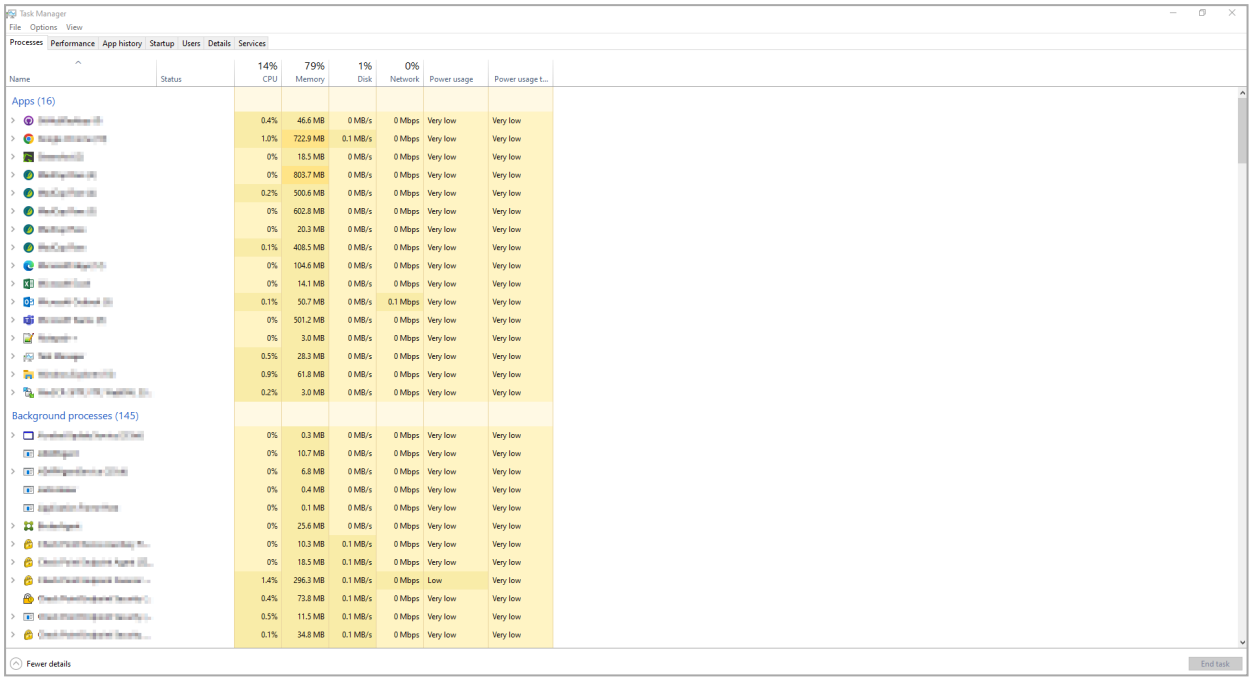
| Rule Name | Default Status | Domains | Categories |
|---|---|---|---|
| Bypass Apple services - Pre-configured | Enabled | ▪ p24-keyvalueservice.icloud.com<br>▪ apps.apple.com<br>▪ itunes.apple.com<br>▪ mzstatic.com<br>▪ gs-loc.apple.com<br>▪ gsa.apple.com<br>▪ securemetrics.apple.com<br>▪ swscan.apple.com<br>▪ xp.apple.com<br>▪ icloud.com<br>▪ ppq.apple.com<br>▪ akadns.net<br>▪ mail.me.com<br>▪ music.apple.com | N/A |
| Bypass Bitdefender services - Pre-configured | Enabled | ▪ cdn.bitdefender.net<br>▪ download.bitdefender.com<br>▪ login.bitdefender.net<br>▪ login.bitdefender.com<br>▪ nimbus.bitdefender.net<br>▪ push.bitdefender.net<br>▪ upgrade.bitdefender.com | N/A |
| Bypass Zoom - Pre-configured | Enabled | zoom.us | N/A |
| Bypass Webex - Pre-configured | Enabled | webex.com | N/A |
| Bypass Spotify - Pre-configured | Enabled | spotify.com | N/A |

## Finding the Process Name of an Application

You can use the process name to bypass the traffic to the application that uses certificate pinning.

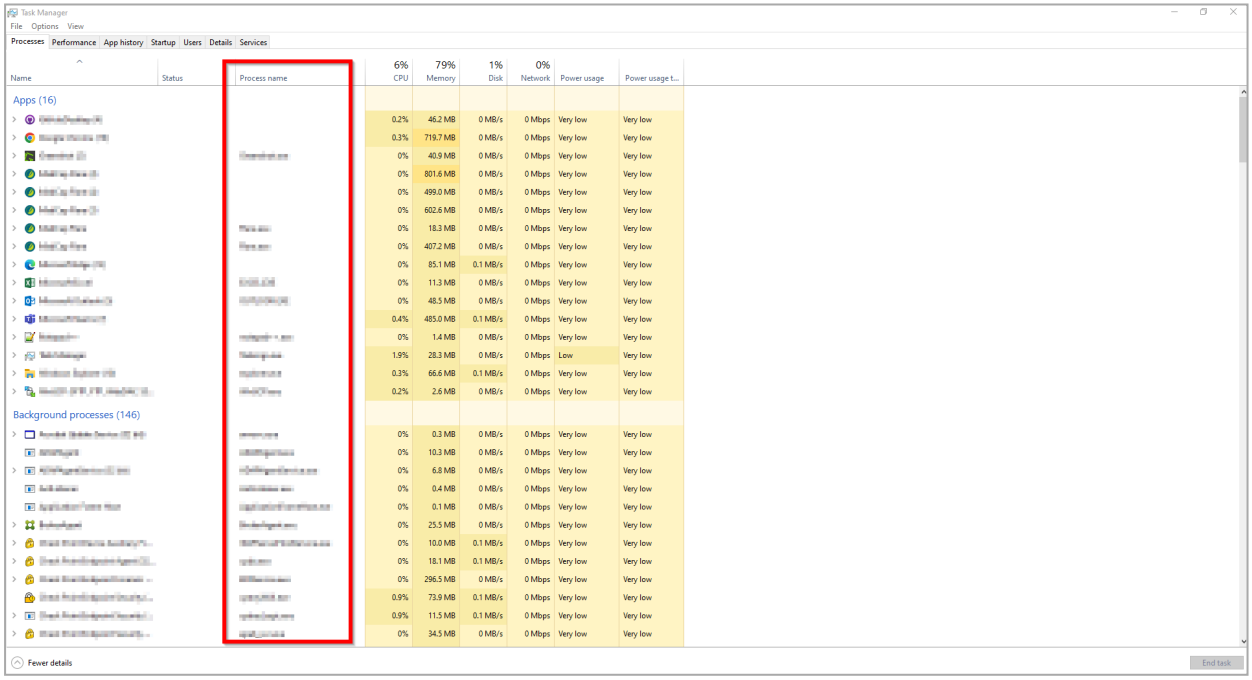
### To find the process name in Windows:

1. Open **Task Manager**.



2. Right-click any column in the **Processes** tab and select **Process name**.

   The **Process name** column appears in the table.



3. Search for your application and copy the process name.

**To find the process name in macOS, do one of these:**

- Go to **Activity Monitor**:
  a. Select the application's process.
  b. Click **View** and select **Inspect Process**.
  c. Go to **Sample** > **Binary Images**.
  d. Identify the process name from the first item in the list.
- Go to **Finder**:
  a. Navigate to the **Applications** folder.
  b. Select the application.
  c. Right-click the application and select **Show Package Contents**.
  d. Go to the **Contents** folder and open the **Info.plist** file.
  e. Find the process name next to the **CFBundleIdentifier** key.

**To find the process name in Linux:**

1. Run this command in the terminal:

   ```
   ps aux | grep <application_name>
   ```

   The process name is displayed in the second-to-last column of the output.

# Monitor & Logs

**Monitor & Logs** allows you to view:


- *"Active Sessions" on page 223*
- *"Member Activity" on page 224*
- *"Web Activity" on page 226*
- *"Malware Protection" on page 229*
- *"Admin Activity" on page 232*
- *"Tunnels Status" on page 236*
- *"Firewall Events" on page 237*

# Active Sessions

The **Active Sessions** page allows you to view the active user session details.

To view the **Active Sessions** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Active Sessions**.




| Column | Description |
|---|---|
| Member | Member name |
| Device | Name of device(s) logged in from. |
| Connection Type | Type of connection:<br>■ **app** - Member is connected to an application.<br>■ **agent** - Member is connected to the Harmony SASE Agent. |
| Start Time | Start date and time of the connection. |
| Duration | Duration of the connection. |
| Session Origin | Location of the connected network gateway.<br>For the Harmony SASE Agent, it shows the IP address. |
| Network | Connected network name. |
| Region | Connected network region. |
| Gateway | Harmony SASE gateway IP address. |

To select the columns required in the table, click the ⚙ icon and select the columns.

To export the data, click the ⬆ icon. The system downloads an archive file with the data in JSON and CSV file format.

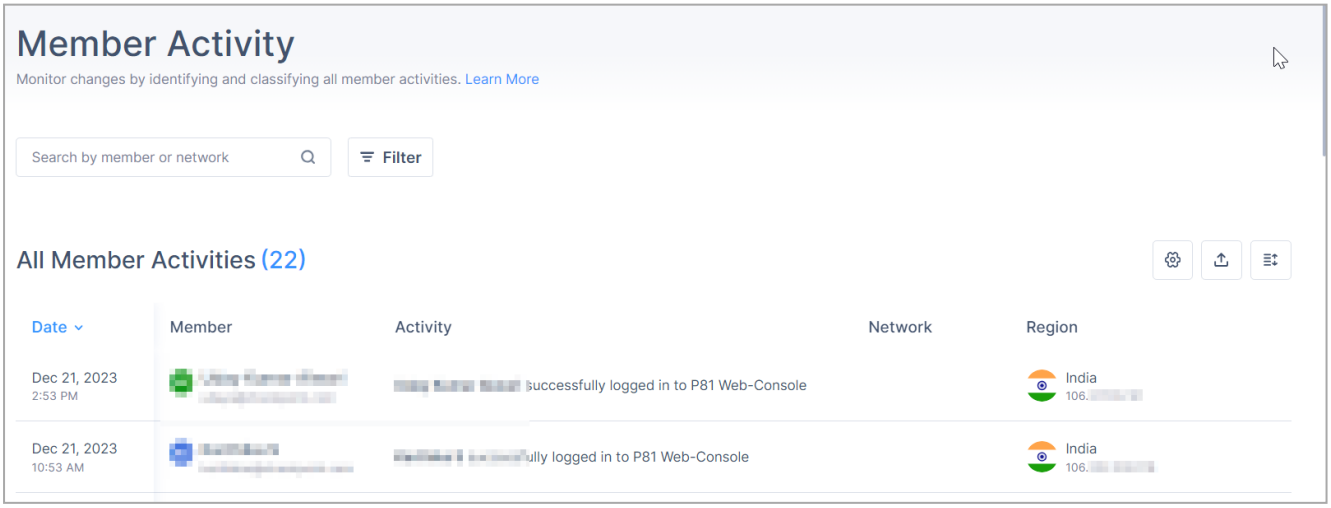
**Note** - You can export only the latest 1000 active sessions at a time.

# Member Activity

The **Member Activity** page allows you to view these member activities:

- **Application access**
  - Application authorization successful / failed
  - Application session started / ended
- **Login**
  - Login success / failed
  - Log out success / failed
  - Web console login success / fail
  - User blocked from web console
  - IP blocked from web console
  - Account blocked
  - Device registration success / fail
  - Device unregistration success / fail
  - Network login success / fail
  - Network logout
- Member accepted the invitation
- Support team login / logout

To view the **Member Activity** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Member Activity**.



| Column | Description |
|---|---|
| Date | Date and time of the activity. |
| Member | Member name. |
| Activity | Activity description. |
| Network | Connected network name. |
| Region | Region and gateway IP address of the connected session. |

To select the columns required in the table, click the icon and select the columns.

To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

**Note** - You can export data of only 1000 activities at a time.

# Web Activity

The **Web Activity** page shows:

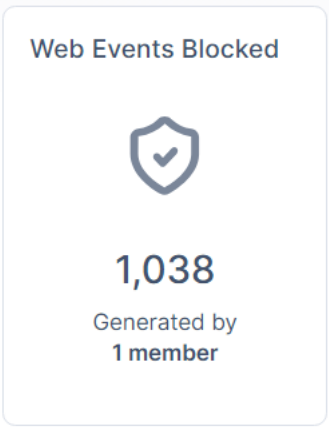
- *"Web Events Blocked" below*
- *"Top Web Categories" on the next page*
- *"Events Per User" on the next page*
- *"All Web Activities" on the next page*

To view the **Web Activity** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Web Activity**.

## Insights

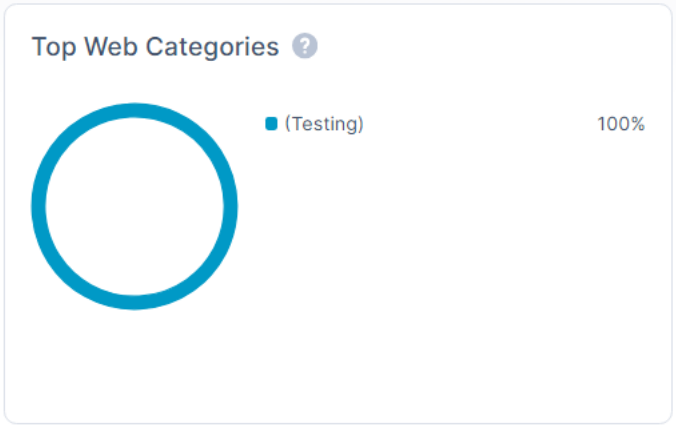
**Insights** shows the number of blocked web events, top web categories blocked, and top number of events blocked in the last 1 day, 7 days, and 30 days.

### Web Events Blocked



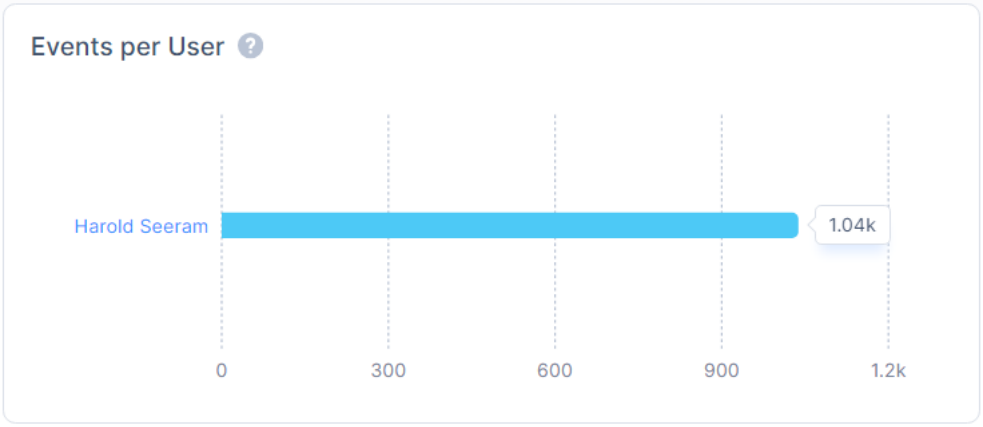

The **Web Events Blocked** widget shows the total number of URLs blocked in the selected time frame.

## Top Web Categories




The **Top Web Categories** widget shows the top five web categories blocked in the selected time frame.

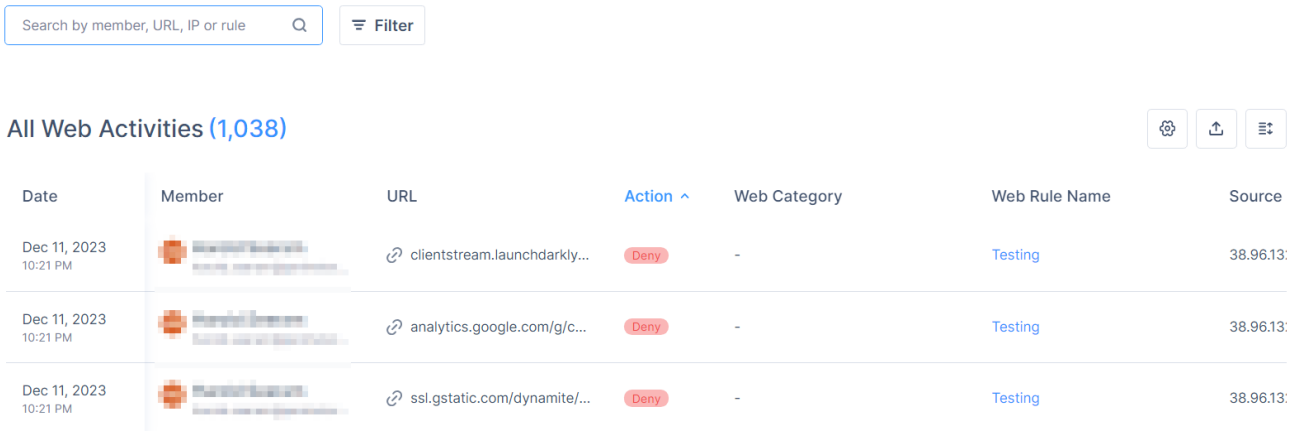
## Events Per User




The **Events per User** widget shows the top five users with the highest number of violations for web categories in the selected time frame.

# All Web Activities

**All Web Activities** shows a log of all the web traffic.




| Column | Description |
|---|---|
| Date | Date and time of the activity. |
| Member | Member name. |
| URL | Accessed URL. |
| Action | Action taken by Harmony SASE:<br>■ Deny - Member is denied access to the URL.<br>■ Warn - Member is warned before accessing URL. |
| Web category | Category name configured in the *"Web Filter Rules" on page 195*. |
| Web Rule Name | Web Rule name configured in the *"Web Filter Rules" on page 195*. |
| Source IP | IP address of the source. |
| Destination IP | IP address of the destination. |

To select the columns required in the table, click the ⚙ icon and select the columns.

To export the data, click the ⬆ icon. The system downloads an archive file with the data in JSON and CSV file format.

**Note** - You can export data of only 1000 activities at a time.

# Malware Protection

The **Malware Protection** page allows you to view:

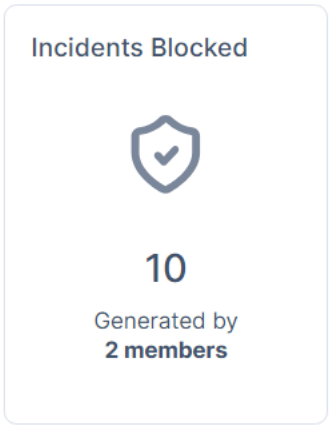
- *"Incidents Blocked" below*
- *"Malware Types" on the next page*
- *"Blocked Malware Per User" on the next page*
- *"All Malware Activities" on the next page*

To view the **Malware Protection** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Malware Protection**.

## Insights

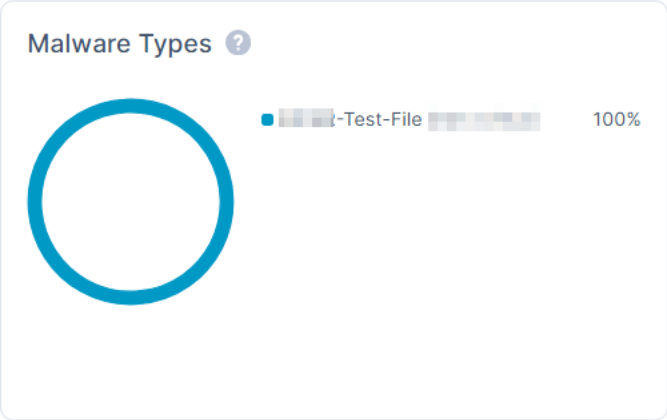
**Insights** shows the number of blocked malicious events, top malware types blocked, and top number of blocked events per user in the last 1 day, 7 days, and 30 days.

### Incidents Blocked



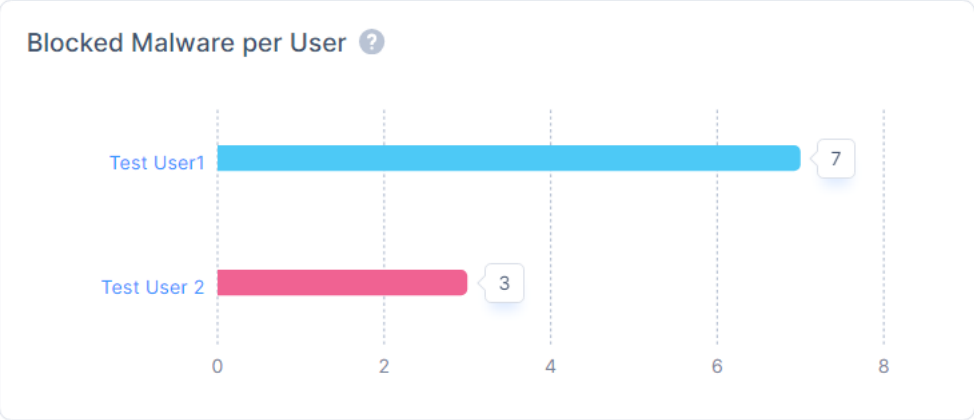

The **Incidents Blocked** widget shows the total number of blocked malicious files and URLs in the selected time frame.

## Malware Types




The **Malware Types** widget shows the top categories of malware blocked in the selected time frame.

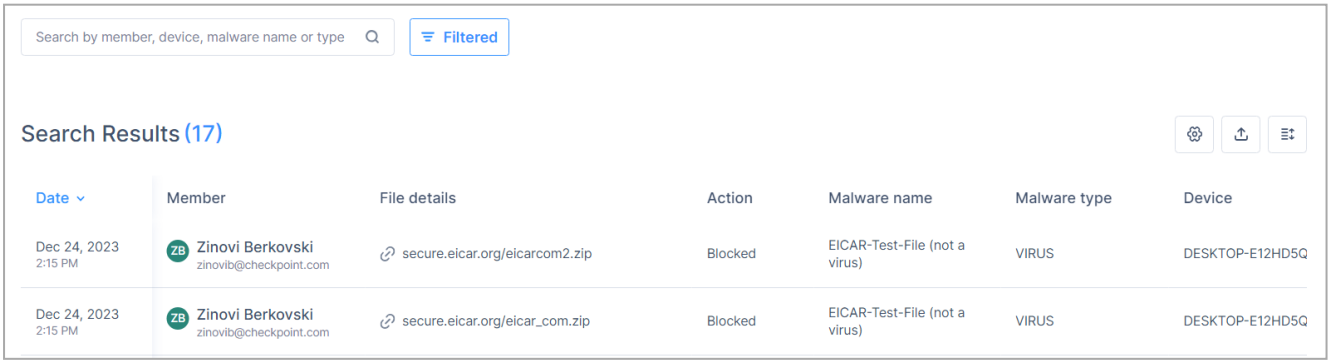
## Blocked Malware Per User




The **Blocked Malware per User** widget shows the users that have the highest number of incidents for blocked malicious files and URL in the selected time frame.

# All Malware Activities

**All Malware Activities** show a log of all the malware activities.



| Column | Description |
|---|---|
| Date | Date and time of the activity. |
| Member | Member name. |
| File Details | File URL. |
| Action | Action taken by Harmony SASE:<br>■ Blocked<br>■ Scan skipped |
| Malware name | Malware name. |
| Malware type | Malware type. |
| Device | Device from where the malware was detected. |

To select the columns required in the table, click the icon and select the columns.

To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

**Note** - You can export data of only 1000 activities at a time.

# Admin Activity

The **Admin Activity** page allows to you to view these administrator activities:

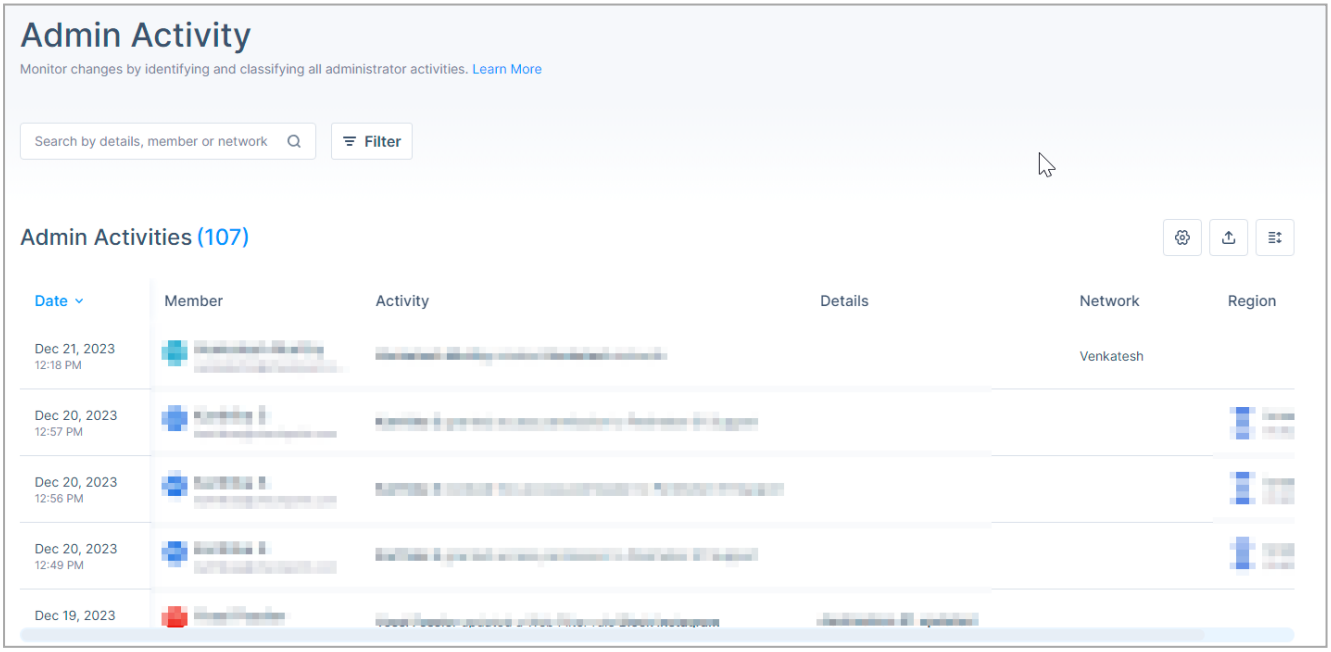
- Account unblocked
- Active sessions report exported
- API key created / deleted
- **Application Access**
    - Application created / deleted
    - Application creation failed
    - Application changed / enabled / disabled
    - Policy changed / created / deleted
- **Billing**
    - Application created / deleted
    - Subscription activated / cancelled / reactivated
    - Subscription plan changed
    - Payment method updated
- Bypass rule added / updated deleted / priority updated
- **Configuration Profile**
    - Configuration profile added / updated / deleted
    - Trusted wired network added / deleted / disabled / enabled
    - Trusted WiFi network added / deleted
- **Firewall**
    - Firewall rule added / updated / deleted
    - Firewall rule updated / update failed
    - Firewall rule priority updated
- Gateway license purchased / removed
- **Group**

- Group created / updated / deleted
- Group member added / deleted
- Group network added / delete

- **Identity Provider**
  - Identity Provider created / updated / disabled / deleted
  - SCIM integration enabled / disabled
  - SCIM token created
- Integration created / enabled / disabled / deleted
- **Members**
  - Member created / invited / updated / deleted
  - Member Profile updated
  - Exported members list
- Member license purchased / removed
- **Network**
  - Network created / updated / deleted / creation failed
  - Gateway created / deleted / restarted / state changed
  - Custom gateway created
  - Region created / deleted
  - Tunnel created / updated / deleted
  - DNS filtering updated / deleted
  - Private DNS updated / enabled / disabled
  - Regional private DNS updated / enabled / disabled
  - Custom network created / creation failed
  - Custom region created
  - Network Split Tunneling
  - Network groups changed
- **Objects**

    - Application created / deleted
    - Address updated / deleted / added
    - Service added / updated / deleted
    - Custom URL added / updated deleted
- Password reset / changed
- **Posture Check**
    - Posture profile created / updated / deleted
    - Posture profile check failed
- Role assigned to a member
- Support access granted / revoked
- Web activity report exported
- **Web Filter Rules**
    - Member license purchased / removed
    - Web filter rule added / updated / deleted
    - Web filter rules policy updated / priority changed / status changed

To view the **Admin Activity** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Admin Activity**.



| Column | Description |
|---|---|
| Date | Date and time of the activity. |
| Member | Member name. |
| Activity | Activity description. |
| Details | Change in the defined values for the activity. |
| Network | Connected network name. |
| Region | Region and gateway IP address of the connected session. |

To select the columns required in the table, click the icon and select the columns.

To export the data, click the icon. The system downloads an archive file with the data in JSON and CSV file format.

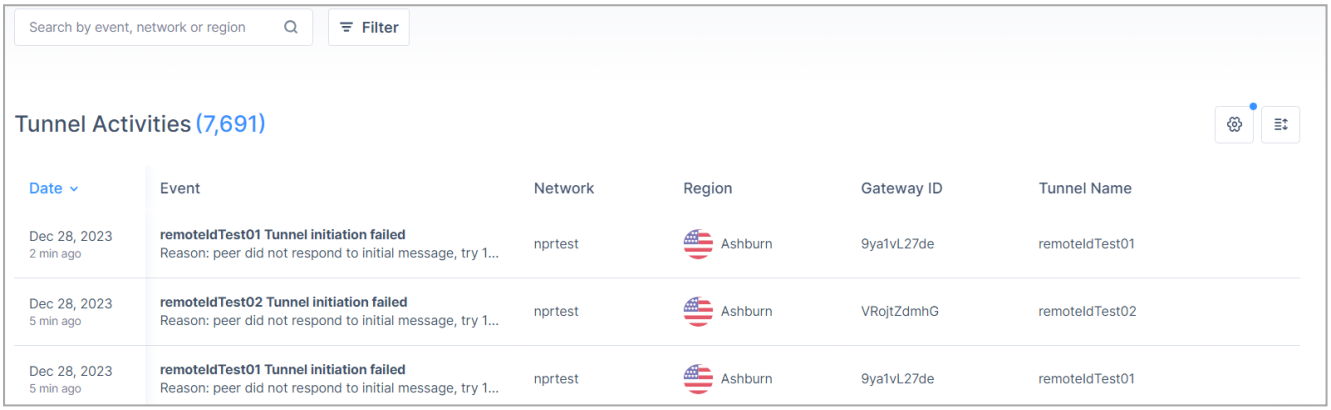
**Note** - You can export data of only 1000 activities at a time.

# Tunnels Status

The **Tunnels Status** page allows you to monitor the health of tunnels.

- Tunnel up / down
- Tunnel initialization failed

To view the **Tunnels Status** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Tunnels Status**.



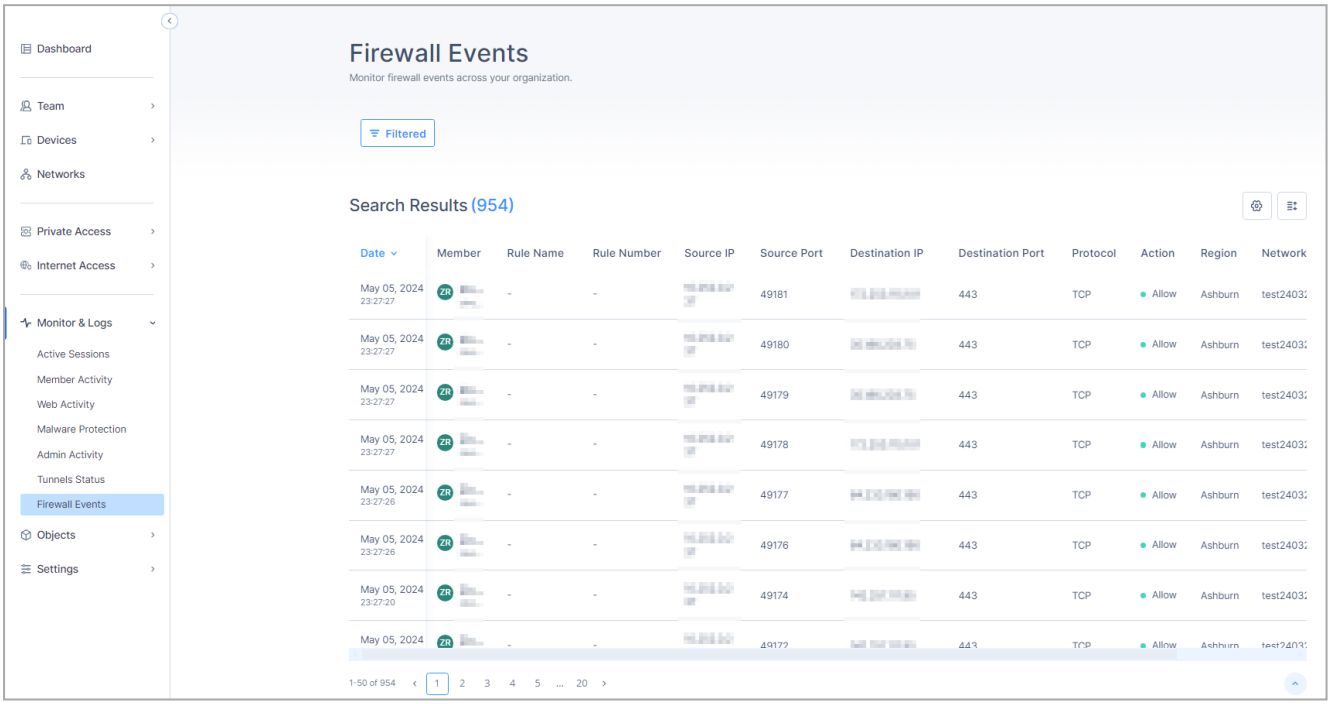

| Column | Description |
|---|---|
| Date | Date and time of the activity. |
| Event | Event type and the reason. |
| Network | Associated network. |
| Region | Region of the network. |
| Gateway ID | Harmony SASE gateway ID. |
| Tunnel Name | Tunnel name. |
| Tunnel Peer IP | Tunnel peer IP address. |
| Tunnel Source IP | Tunnel source IP address. |
| Tunnel Type | Tunnel type. |

To select the columns required in the table, click the ⚙ icon and select the columns.

# Firewall Events

The **Firewall Events** page allows you to monitor the firewall events.

To view the **Firewall Events** page, access the Harmony SASE Administrator Portal and click **Monitor & Logs** > **Firewall Events**.




| Column | Description |
|---|---|
| Date | Date and time of the activity. |
| Member | Member name. |
| Rule Name | Rule name configured in the *"Firewall" on page 160*. |
| Rule Number | Rule number configured in the *"Firewall" on page 160*. |
| Source IP | IP address of the source. |
| Source Port | Port number on the source IP. |
| Destination IP | IP address of the destination. |
| Destination Port | Port number on the destination IP. |

| Column | Description |
|---|---|
| Protocol | Communication protocol used for the network activity, for example, TCP, UDP, or ICMP. |
| Action | Action taken on the event:<br>■ Allow<br>■ Deny |
| Region | Region of the network. |
| Network | Associated network. |

To select the columns required in the table, click the icon and select the columns.

# Objects

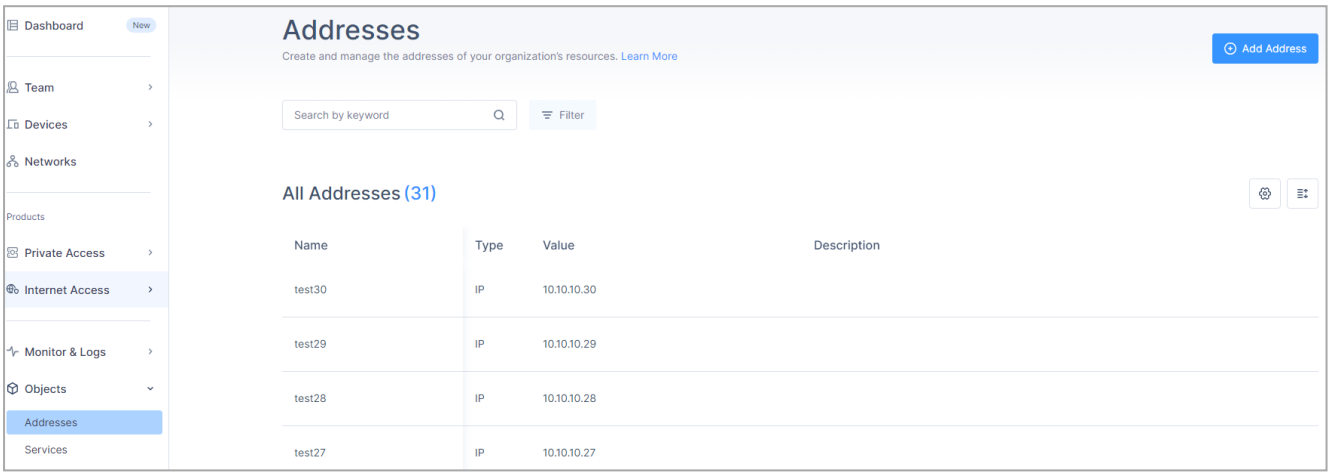
**Objects** allow you create:

- *"Addresses" on page 240*
- *"Services" on page 245*
- *"Custom URLs" on page 249*

# Addresses

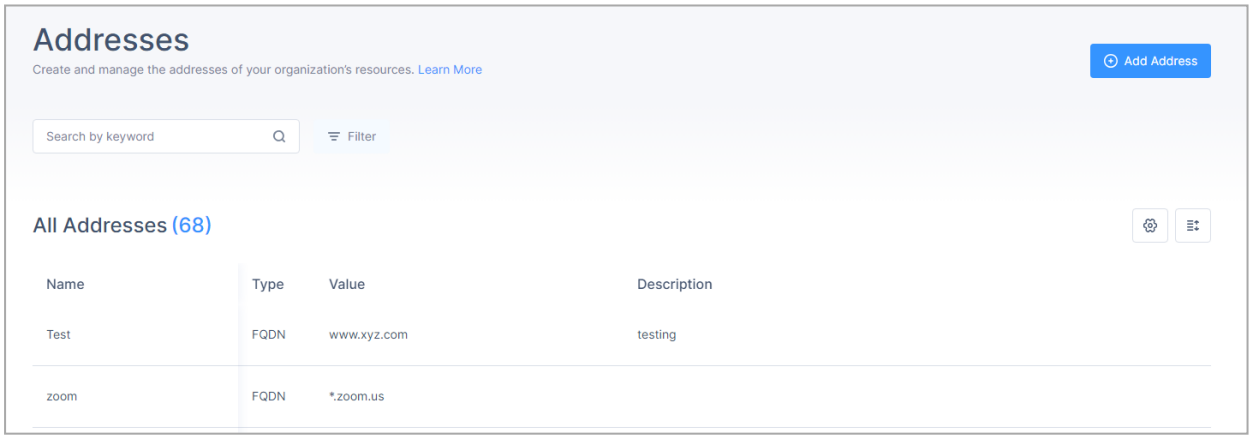
The **Address** object allows you manage the IP addresses and subnets that you use to define your network, firewall rules, application access rules and web filter rules.

To view the **Address** object, access the Harmony SASE Administrator Portal and click **Objects**.



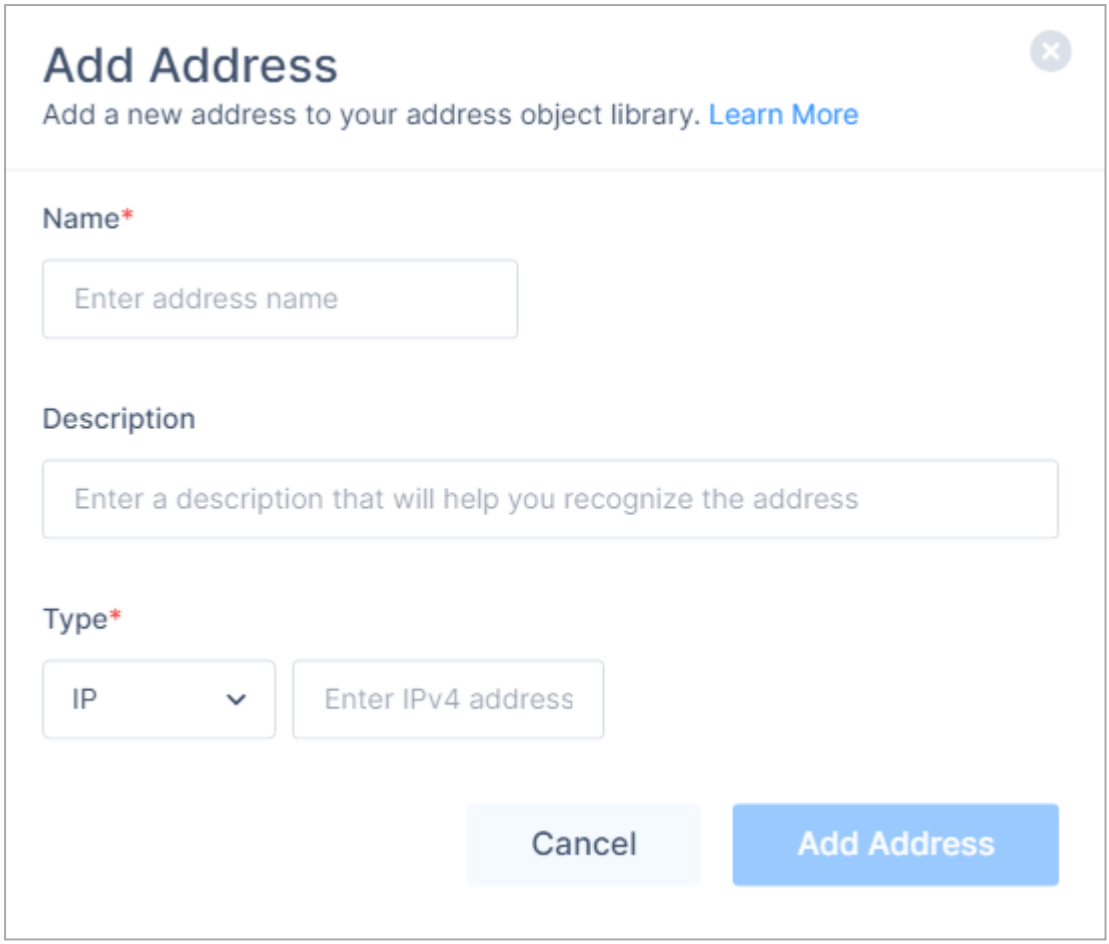

# Creating an Address Object

1. Access the Harmony SASE Administrator Portal and click **Objects** > **Addresses**.




2. Click **Add Address**.

   The **Add Address** window appears.




3. Enter these:
   a. **Name** - Name of the address object.
   b. (Optional) **Description**
   c. **Type** - Select the address type and enter the address value.
      - IP
      - Subnet
      - List
      - FQDN
4. Click **Add Address**.

   The system creates the address and displays it in the **Addresses** page.

# Managing Addresses

1. Access the Harmony SASE Administrator Portal and click **Objects** > **Addresses**.
2. Hover over the address and do one of these:

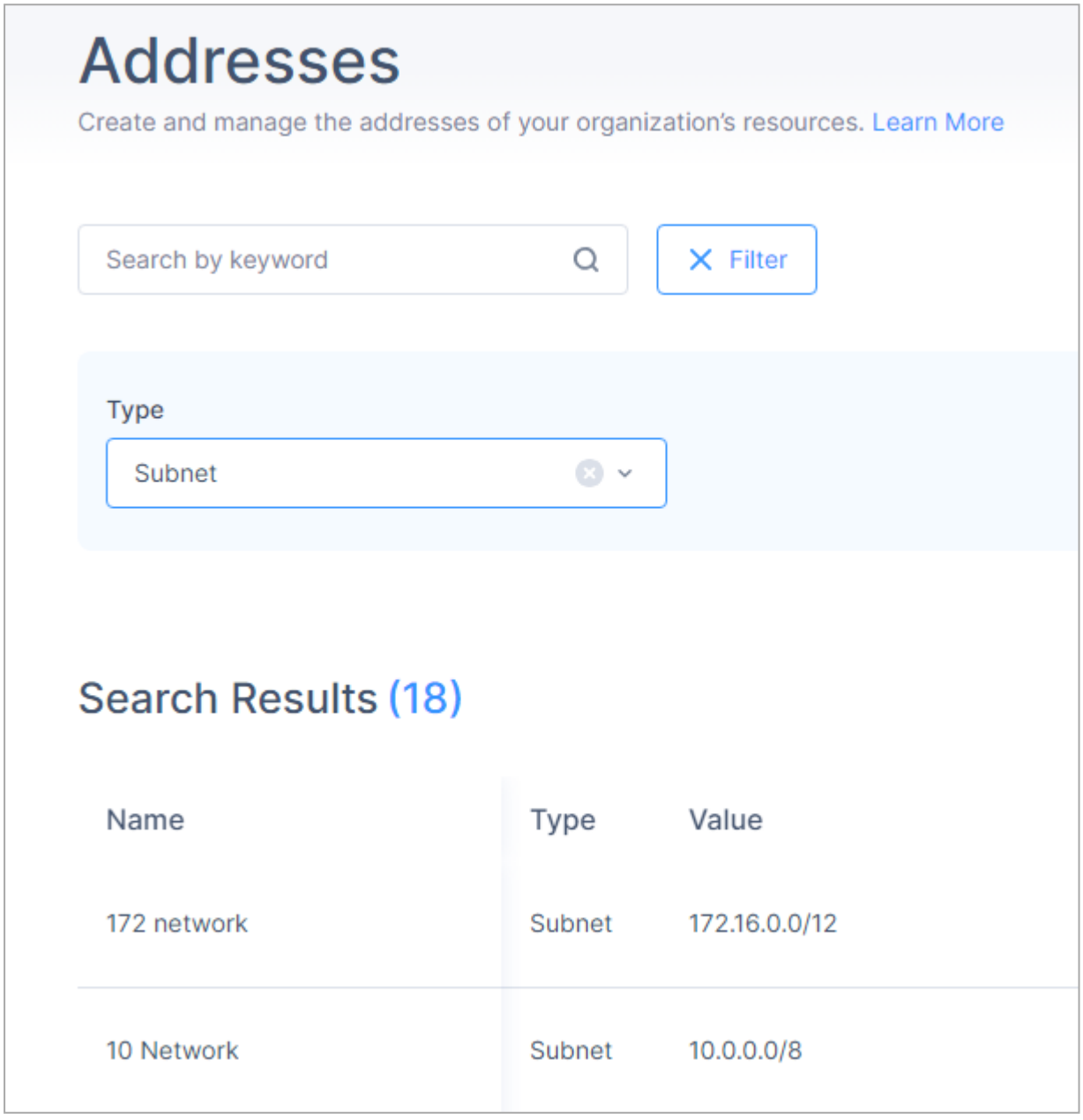
- To edit, click .

  Make the required changes and click **Apply**.

- To delete, click and then click **Delete**.

- To duplicate, click .

3. To search for an address, enter the address name in the **Search** box.
4. To filter the addresses by their **Type**, click **Filter** and select the address **Type**.




5. To edit the **Addresses** table settings, click .
6. To edit the number of addresses displayed in the table, click .

# FQDN-based Firewall Objects

FQDN-based firewall objects allows you to use FQDN as objects in firewall rules. You can use FQND object for services with dynamic IP address and use DNS to eliminate the requirement to manually update the IP address of services.

## FQDN Wildcards

You can use the FQDN wildcard support to specify sub-domains. For example, **.example.com* includes all sub-domains, such as *sales.example.com*, *support.example.com* and so on.

## Multi-Level Sub-domains

FQDN objects support multi-level subdomains, up to 5 levels.

For example, *one.two.three.four.five.example.com*

## Important Considerations

- The firewall supports a total of 100 FQDN objects.

  Examples:

  - **One** FQDN object per rule, across **100x rules**, or:
  - **100x** FQDN objects contained in a **single rule**.
- FQDN objects can contain a maximum of 1000 domains per account.

  Examples:

  - **Ten** FQDN objects containing **100x domains**, or:
  - **100x** FQDN objects containing **ten domains** each.

## Limitations

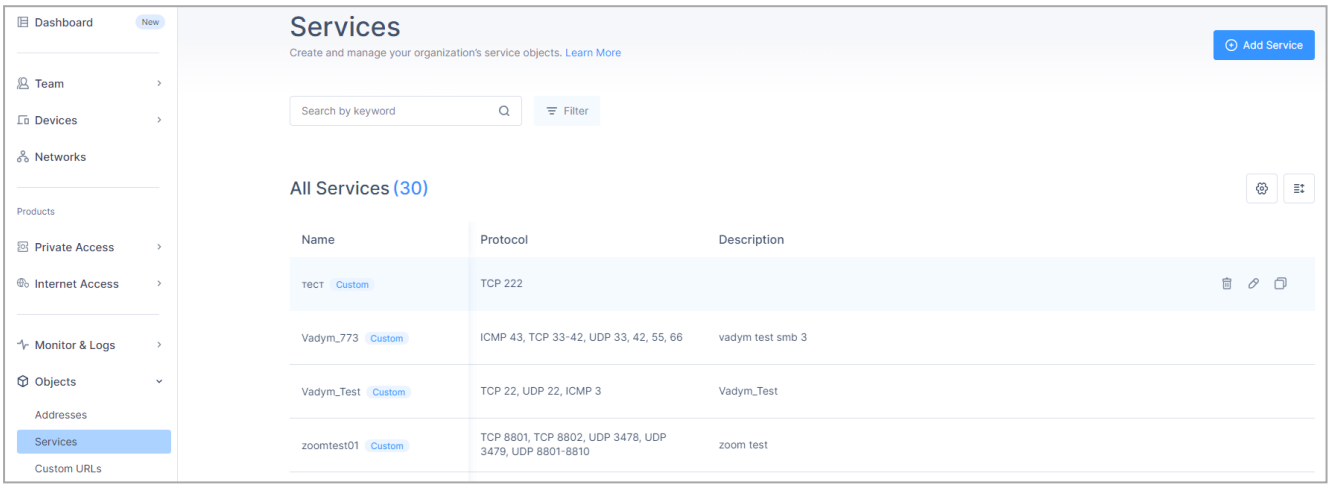
- FQDN firewall rules may be bypassed by using an IP.
- CDN is not permitted, only FQDN.
- If you have two or more FQDNs sharing the same IP, both are affected by the Firewall rule. For example, if you block one FQDN, another resource sharing the same IP is also be blocked.
- Limited compatibility with services supported by multiple FQDN (for example, websites).
- No compatibility with DNS load balancers as they return different IPs for each query.
- The browser and local DNS cache take priority over FQDN Firewall rules.

- No compatibility with third-party DNS services, for example, DoH (The admin must enforce user VPN interface DNS).

# Services

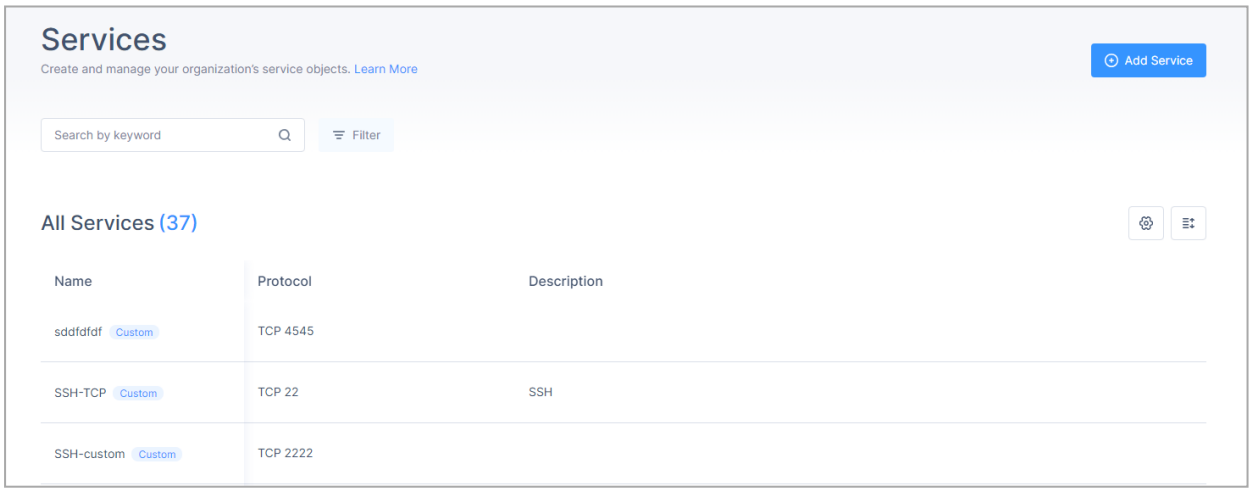
The **Services** object allows you to define the applications that you want to allow access to. These services belong to the Layer 4 of the OSI model with protocol and port combinations. For example, protocol TCP port 80 or protocol UDP port 53.

To view the **Service** object, access the Harmony SASE Administrator Portal and click **Objects**.



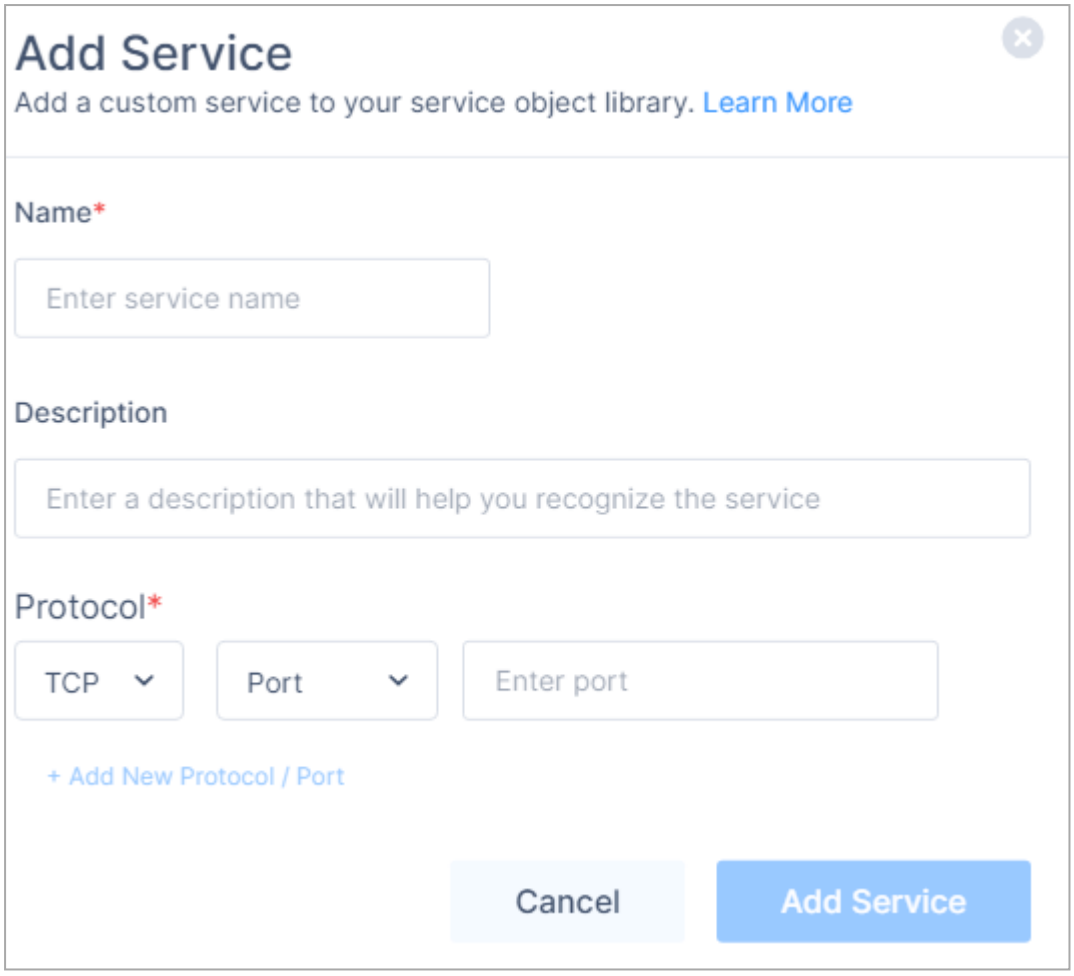

## Creating a Service Object

1. Access the Harmony SASE Administrator Portal and click **Objects** > **Services**.



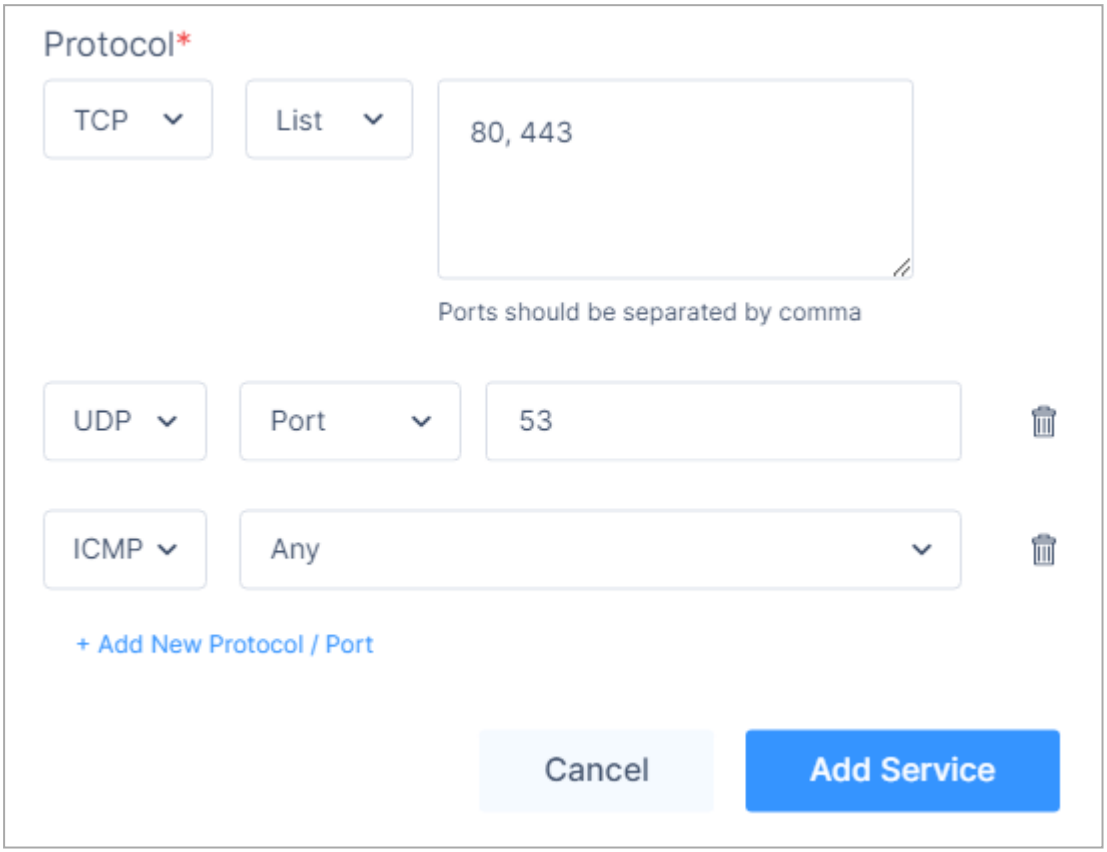

2. Click **Add Service**.

   The **Add Service** window appears.




3. In the **Name** field, enter the name of the service object.
4. (Optional) **Description**
5. In the **Protocol** section:

a. Select the protocol type:
   - TCP
   - UDP
   - IDMP




b. Select how you want to define the protocol:
   - Range - A range of port numbers.
   - Port - A single port number.
   - List - A list of port numbers.

c. Enter the protocol values.

6. To add a new protocol/port pair to the service, click **Add New Protocol / Port**.

   You can combine multiple protocol/port pairs in a single service.

7. Click **Add Service**.

   The system creates the service and displays it in the **Services** page.

# Managing Services

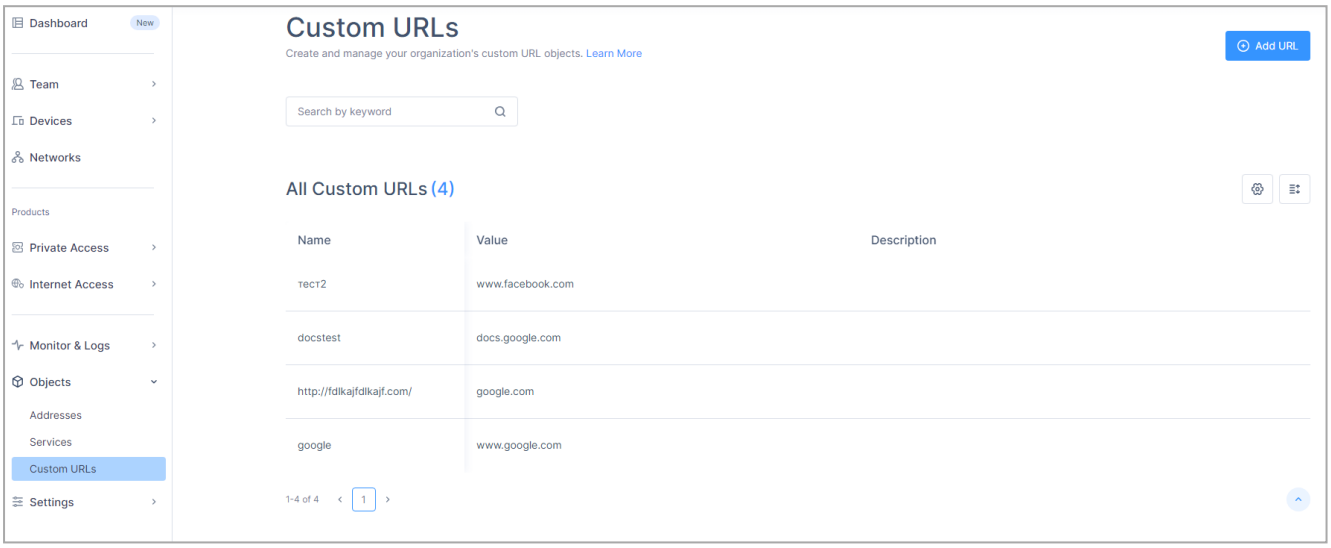
1. Access the Harmony SASE Administrator Portal and click **Objects** > **Services**.
2. Hover over the service and do one of these:
   - To edit, click .

     Make the required changes and click **Apply**.
   - To delete, click and then click **Delete**.
   - To duplicate, click .
3. To search for a service, enter the service name in the **Search** box.
4. To filter the services by their **Protocol**, click **Filter** and select the protocol.
5. To edit the **Services** table settings, click .
6. To edit the number of services displayed in the table, click .

# Custom URLs

The **Custom URL** object allows you to specify a URL's specific path in Web Filter Rules.

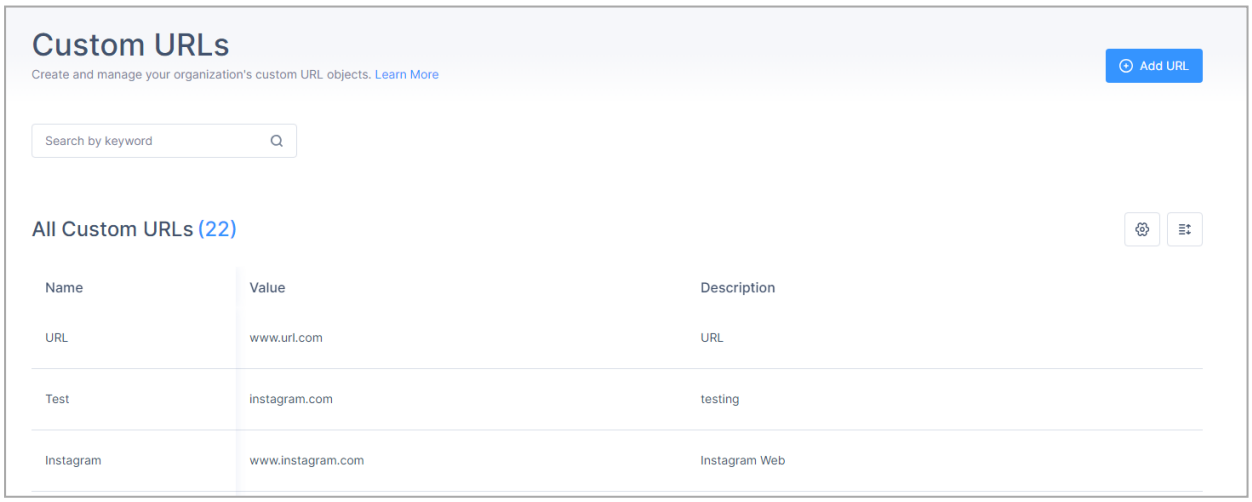
To view the **Custom URL** object, access the Harmony SASE Administrator Portal and click **Objects**.




## Creating a Custom URL Object

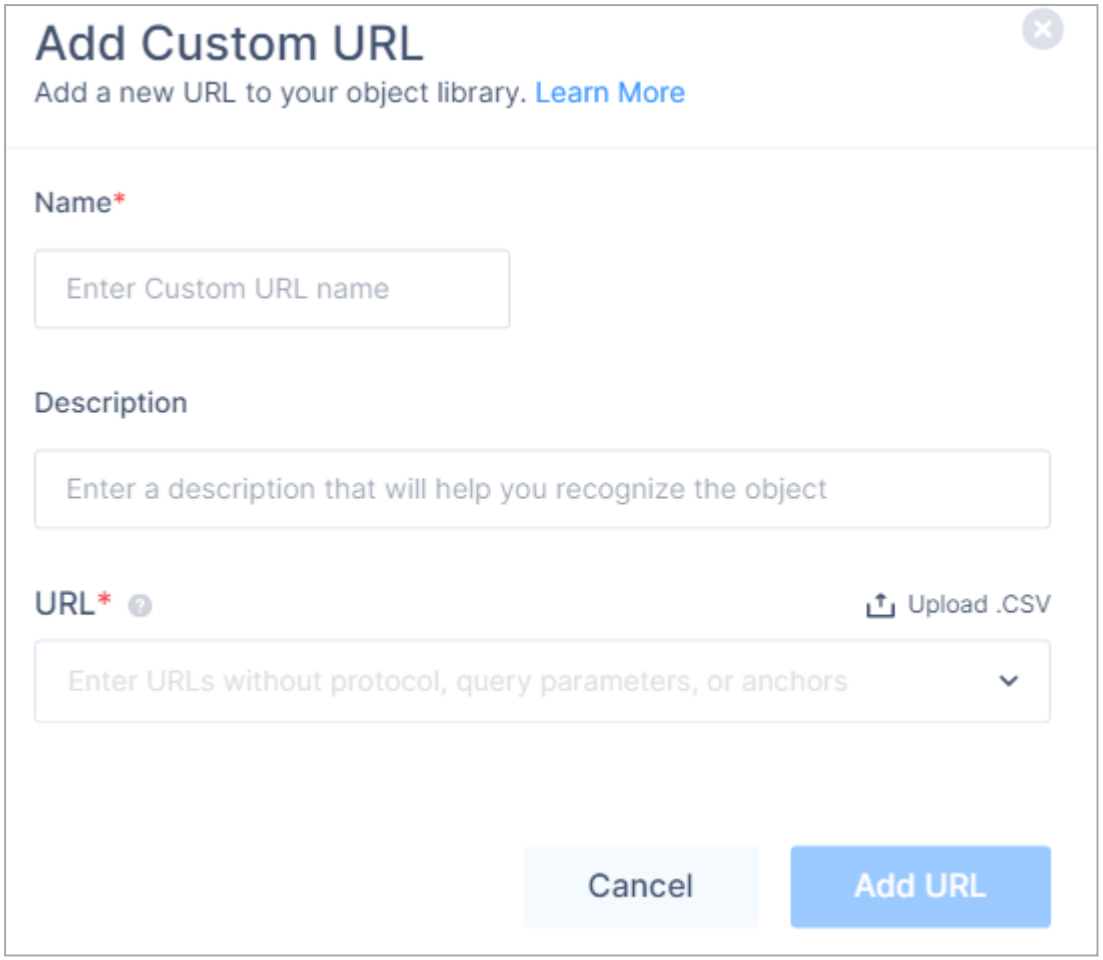
1. Access the Harmony SASE Administrator Portal and click **Objects** > **Custom URLs**.

   The **Custom URLs** page appears.




2. Click **Add URL**.

   The **Add Custom URL** window appears.




3. Enter these:
   a. **Name** - Name of the custom URL.
   b. (Optional) **Description**
4. In the **URL** field, enter the list of URLs or upload a .CSV file with the list of URLs.

   Do not add any protocols (http:// , https://) , query parameters (?) or anchors (#).
5. Click **Add URL**.

   The system creates the URL and displays it in the **Custom URLs** page.

# Managing Custom URLs

1. Access the Harmony SASE Administrator Portal and click **Objects** > **Custom URLs**.
2. Hover over the URL and do one of these:
   - To edit, click .

     Make the required changes and click **Apply**.

- To delete, click and then click **Delete**.

  **Note** - The delete and edit options are disabled if the custom URL is used in a web filter rule.
  Before you delete the URL, remove its references from the web filter rules.

- To duplicate, click .

3. To search for a URL, enter the URL name in the **Search** box.
4. To edit the **Custom URLs** table settings, click .
5. To edit the number of URLs displayed in the table, click .

# Settings

From the **Settings** tab you can configure:

- *"Integrations" on page 253*
- *"Identity Providers" on page 278*
- *"Two-Factor Authentication" on page 279*
- *"Certificate Manager" on page 282*
- *"Support Access" on page 285*

# Integrations

## Security Information and Event Management (SIEM) Integrations

Harmony SASE allows you to export logs to these third-party SIEM applications:

- *"Splunk Cloud" below*
- *"Microsoft Sentinel" on page 258*
- *"Amazon S3" on page 262*

## Professional Services Automation (PSA) Integrations

Integrate Perimeter 81 with ConnectWise Manage to automate the billing process.

- *"ConnectWise PSA" on page 271*

**Note** - This is available only for the accounts in the Perimeter 81 workspace.

## Splunk Cloud

Splunk Cloud allows you to search, analyze and view data collated from various systems in your IT infrastructure.

### Integrating Splunk Cloud

#### Step 1 - Setting Up the HTTP Event Collector

The HTTP Event Collector (HEC) allows you send data and application events to a Splunk deployment over HTTP and HTTPS protocols. You can use HEC to generate a token and use it to configure a log library with data in a specific format. This eliminates the requirement for a Splunk forwarder when you send application events.

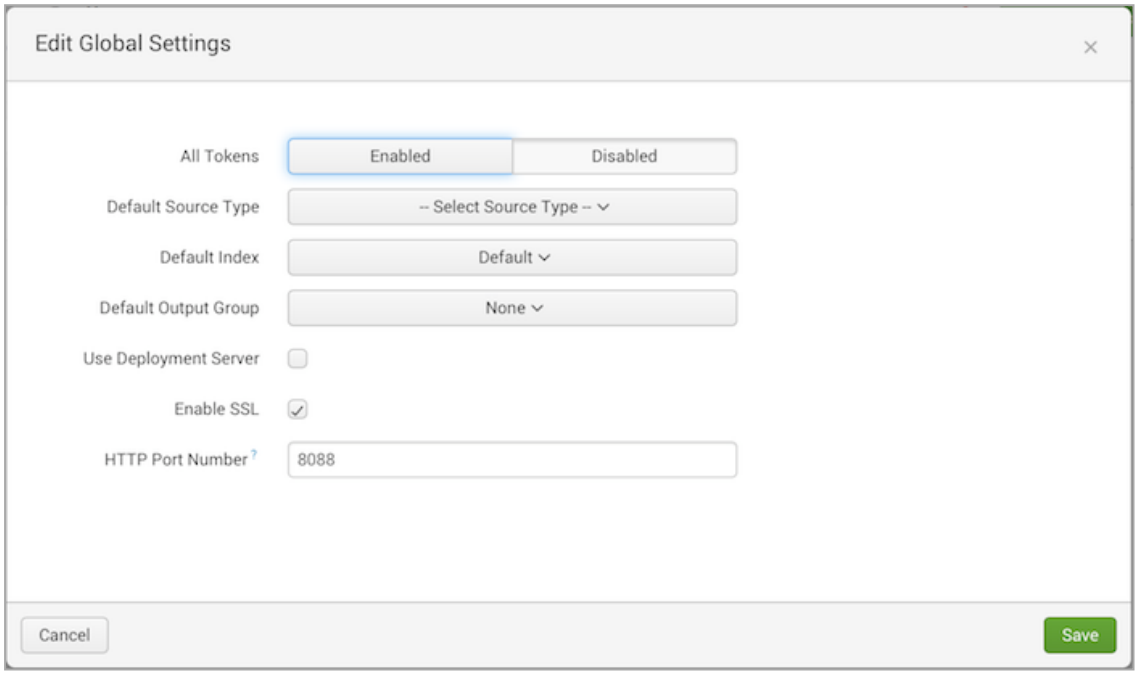
#### Step 2 - Enabling an HTTP Event Collector

When you enable HEC, applications use the HEC tokens to send data to HEC, eliminating the requirement for Splunk credentials in your application or supported files.

**Note** - If you have managed Splunk, contact Splunk customer support for assistance.

**To enable an HTTP Event Collector:**

1. Log in to the Splunk web portal.
2. Click **Settings** > **Data Inputs**.
3. Click **HTTP Event Collector**.
4. Click **Global Settings**.




5. In the **All Tokens** field, select **Enabled**.
6. To enable communication over HTTPs, select the **Enable SSL**checkbox.

   **Note** - It is enabled by default. You can disable it only through Splunk Enterprise.

7. Click **Save**.

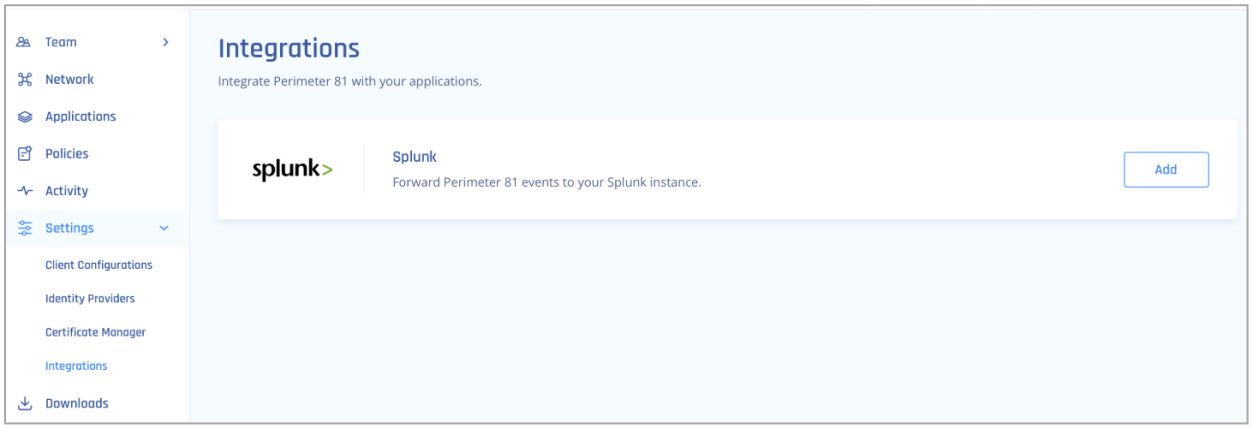
**Step 3 - Creating an Event Collector Token**

1. Log in to the Splunk web portal.
2. Go to **Settings** > **Add Data**.
3. Click **Monitor**.
4. Click **HTTP Event Collector**.
5. In the **Name** field, enter a name for the token.
6. Make sure indexer acknowledgment is disabled for this token.
7. Click **Next**.

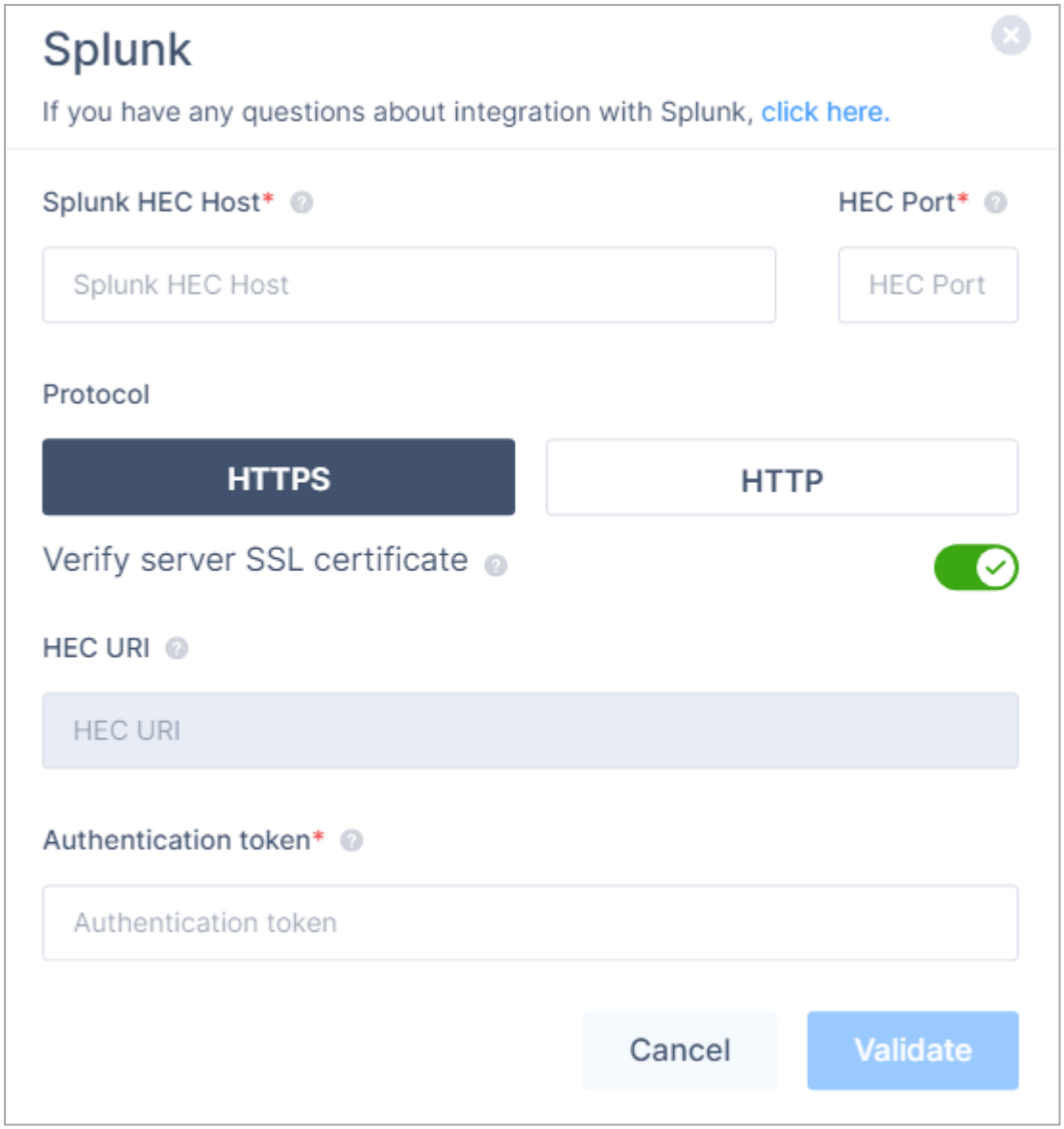
8. Click **Review**.
9. Verify the settings.
10. Click **Submit**.

## Configuring the Splunk Integration in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **SIEM integrations** section, in the **Splunk** row, click **Add**.




3. Enter these:




| Item | Description |
|---|---|
| **Splunk HEC Host** | Enter an appropriate value according to your Splunk tier.<br>Replace {hostname} with your Splunk server hostname.<br>■ Splunk Cloud (paid): inputs-<host><br>■ Splunk Cloud (free-trial): <host> ORinputs.<host> |
| **HEC Port** | ■ Splunk Cloud free trial: 8088<br>■ Splunk Cloud paid: 443 |
| **Protocol** | ■ Splunk Cloud free trial: HTTP<br>■ Splunk Cloud paid: HTTPS |

| Item | Description |
|---|---|
| (For HTTPS only) **Verify server SSL certificate**: | ■ If you are using a self-signed certificate disable SSL verification.<br>■ If you are using a CA-signed certificate make sure to enable it. |
| **HEC URI** | Value is automatically populated. |
| **Authentication token** | Enter the token generated in the Splunk web portal. |

4. Click **Validate**.

## Troubleshooting

This table shows the status codes 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 | Make sure you entered a valid token. |
| 403 | Forbidden | Invalid token | Make sure you entered a valid token. |
| 500 | Internal Error | Internal server error | Contact *Check Point Support*. |
| 503 | Service Unavailable | Server is busy | There are too many requests pending in the Splunk server queue. Try again later. |
| 400 | Bad Request | Data channel is missing | Edit the token at the Splunk web portal and make sure the Indexer Acknowledgement is disabled. |
| 400 | Bad Request | Error in handling indexed fields | Contact *Check Point Support* . |

# Microsoft Sentinel

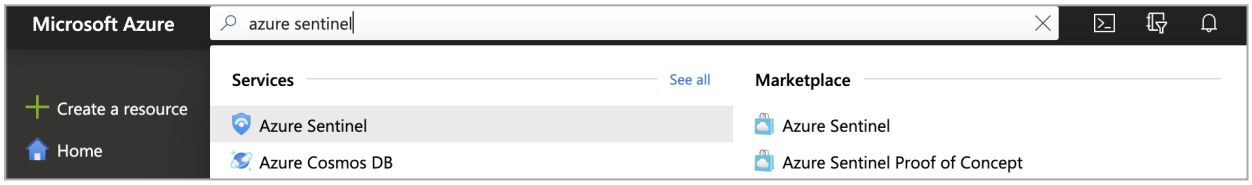
Microsoft Sentinel (formerly Azure Sentinel) is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. It delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

## Configuring the Integration in the Microsoft Azure Portal

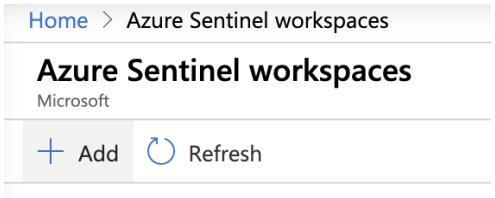
### Step 1 - Setting up a Log Analytics Workspace

**Note** - If you are using an existing log analytics workspace, skip this section.

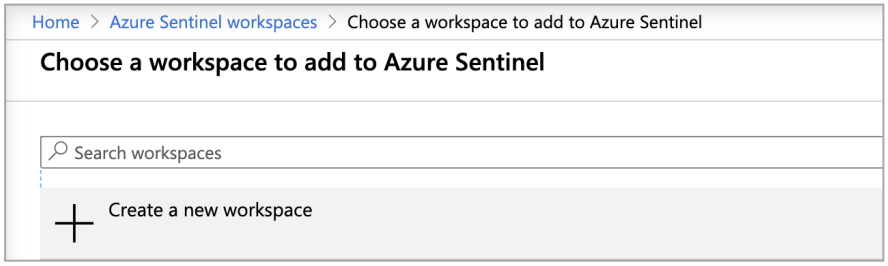
1. Log in to the Microsoft Azure portal.
2. Search for **Azure Sentinel** and select it.



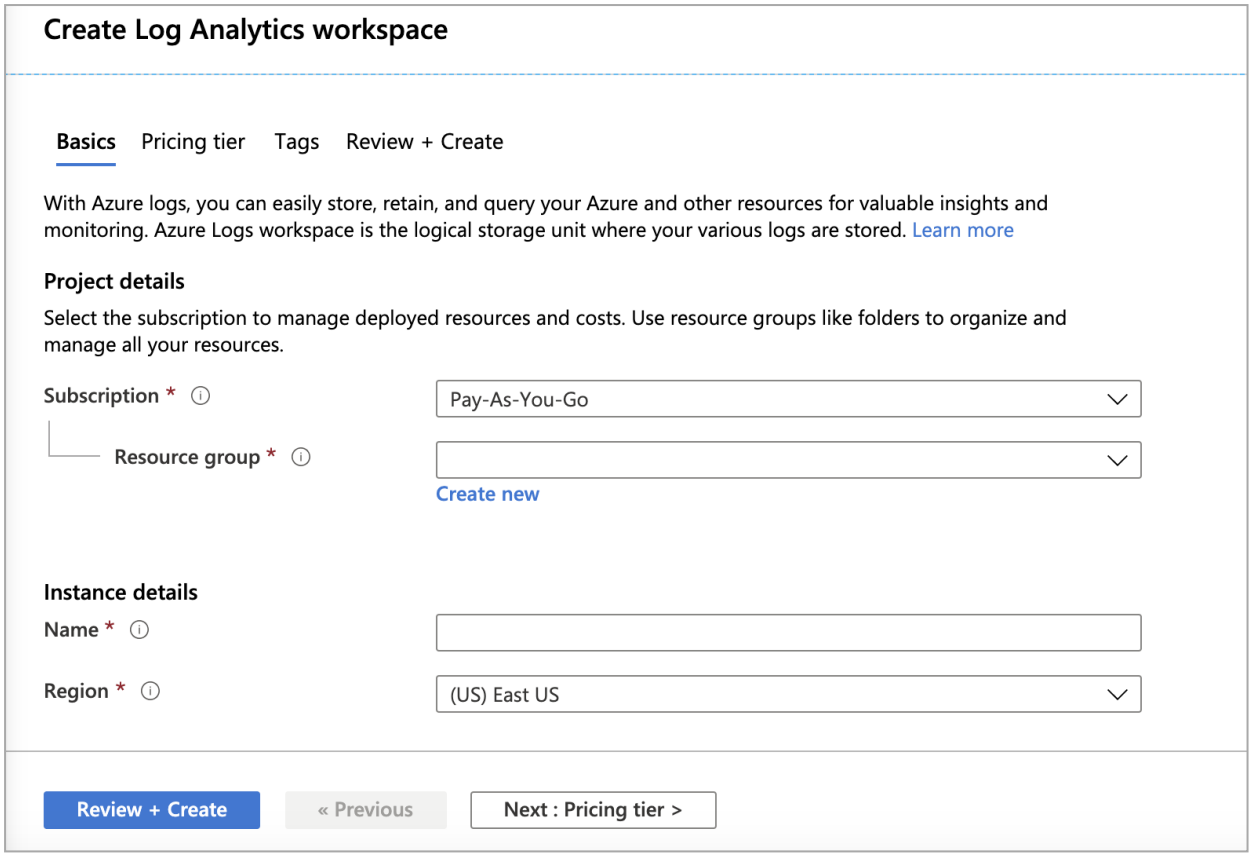

3. Click **Add**.




4. Click **Create a new workspace**.



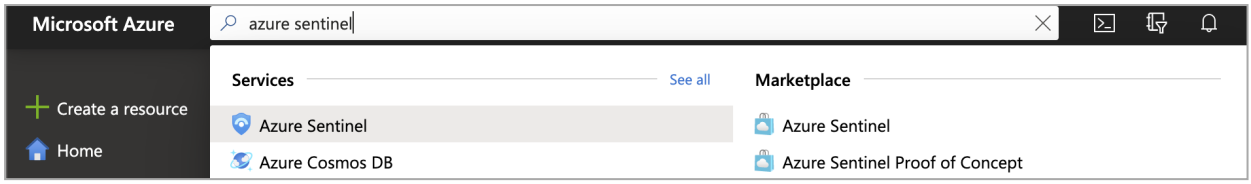

The **Create Log Analytics workspace** window appears.



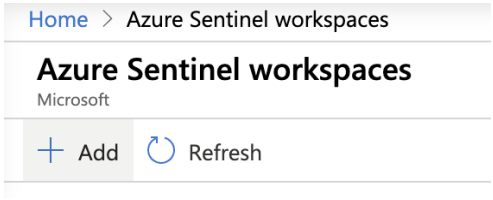

5. Enter these:
   a. **Subscription** - A subscription according to your business needs.
      - **Resource group** - Associate the log analytics workspace with the appropriate business unit.
   b. **Name** - Name of the workspace. It must contain minimum four characters (alphabets, numerals and hyphen) up to 63. Make sure hyphen is not the first or last character.
   c. **Region**: Physical location of the server generating the event collector. Select according to pricing and business requirement.
   d. **(Optional)** Review the pricing tiers and set appropriate tags for the workspace.
6. Click **Review + Create**.

### Step 2 - Linking the Log Analytics Workspace to Microsoft Sentinel

1. Log in to the Microsoft Azure portal.
2. Search for **Azure Sentinel** and select it.



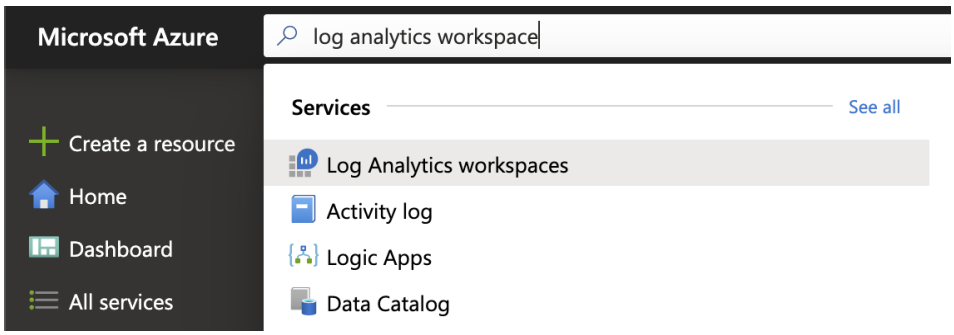

3. Click **Add**.



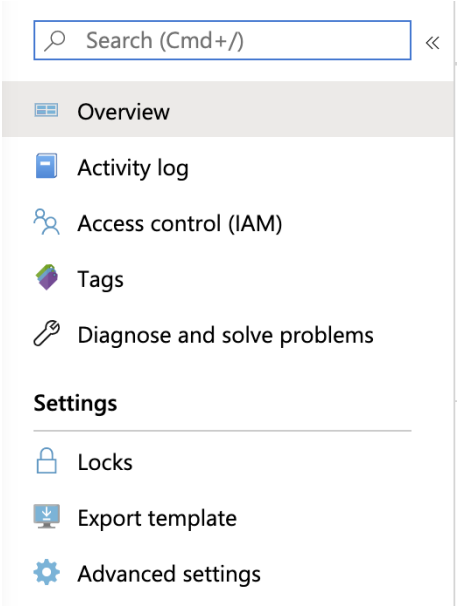

4. Select the Log Analytics Workspace that you have created or an existing one that you want to utilize.

### Step 3 - Finding your Log Analytics Workspace ID and Primary Key

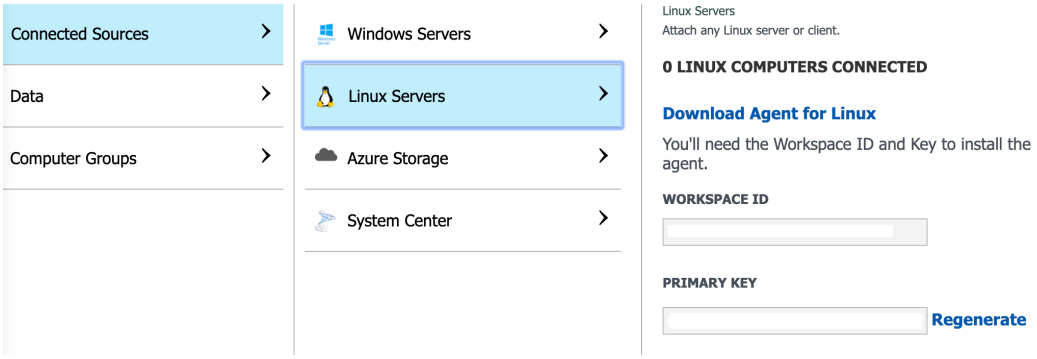
1. Log in to the Microsoft Azure portal.
2. Search for **Log Analytics Workspace** and select it.




3. Select the workspace you connected to Microsoft Sentinel.
4. In the **Settings** section, click **Advanced settings**.

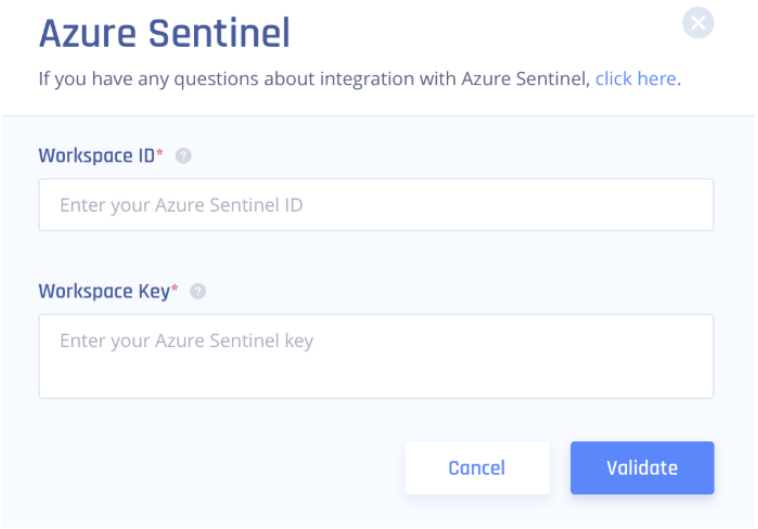



5. Click **Connected Sources** > **Linux Servers** and then copy the **Workspace ID** and the **Primary Key**.




## Configuring the Microsoft Sentinel Integration in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **SIEM integrations** section, in the **Microsoft Sentinel** row, click **Add**.
3. In the **Workspace ID** field, enter the Log Analytics **Workspace ID** from the above section.
4. In the **Workspace Key** field, enter the Log Analytics **Primary Key** from the above section.




5. Click **Validate**.

### Troubleshooting

| Status Message | Action Required |
|---|---|
| Success | None. |
| SENTINEL_INACTIVE_CUSTOMER | The workspace has been deactivated. |
| SENTINEL_INVALID_CUSTOMER_ID | Make sure you have entered the correct customer ID. |
| SENTINEL_INVALID_AUTHORIZATION | The service failed to authenticate the request. Verify that the workspace ID and connection key are valid. |

## Amazon S3

Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance.

### Prerequisites

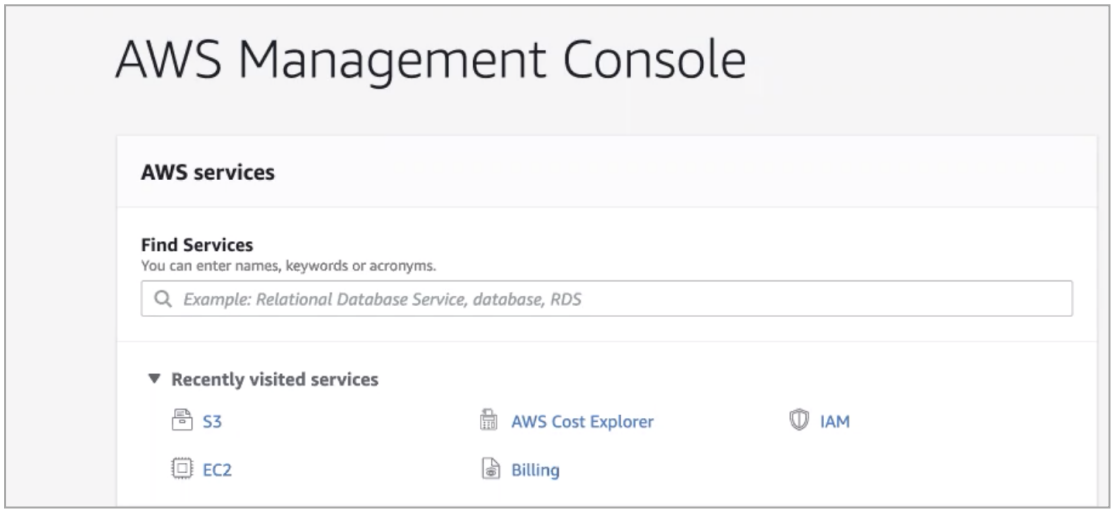
- Ensure that the IAM user has the necessary permissions to access the S3 bucket.
- Harmony SASE uses these IP addresses to deliver SIEM logs:
  - 44.198.227.127
  - 44.199.0.186

- 107.23.141.112
- 54.85.165.134
- 23.20.83.77
- 50.19.134.176

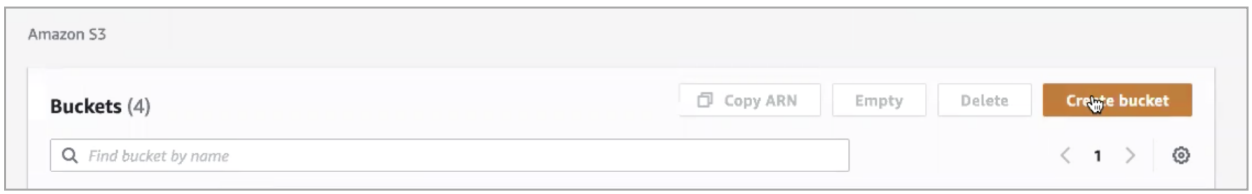
## Configuring the Integration in the AWS Management Console

### Step 1 - Creating a New Bucket

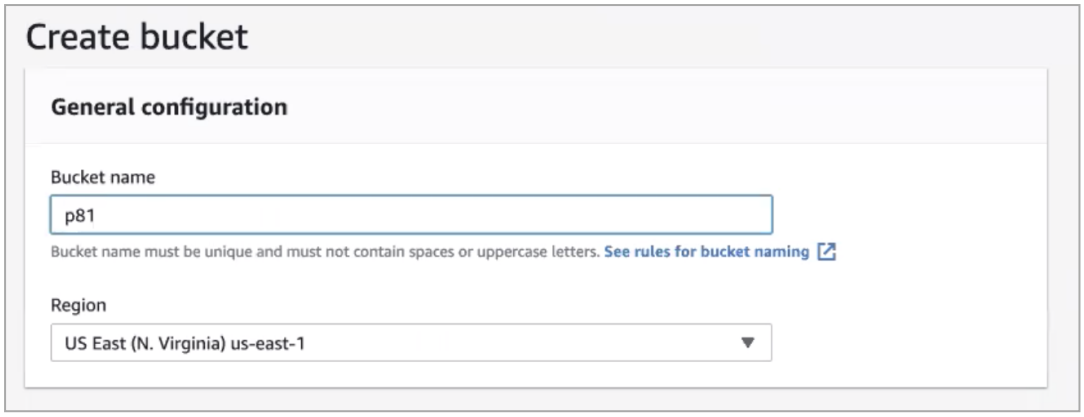
1. Log in to the AWS Management Console.
2. Go to **AWS Services** and select **S3**.




3. Click **Create Bucket**.




The **Create bucket** window appears.

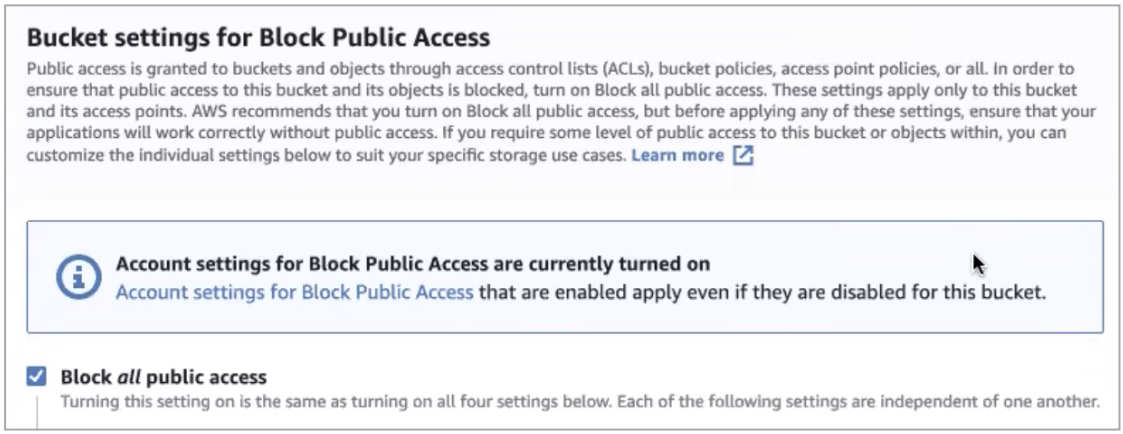



4. In the **Bucket name** field, enter the name of the bucket.

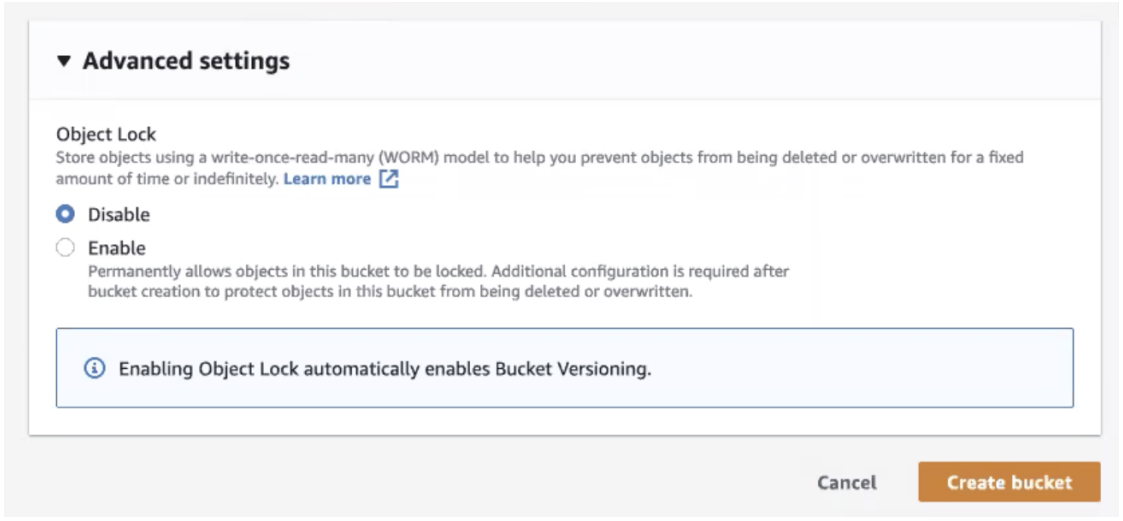
   The name must contain alphabets only. Hypen (-) and period (.) are not supported.

5. In the **Region** field, enter the region where Amazon S3 creates buckets. Select the AWS region geographically nearest to you.

6. Select or clear the **Block all public access** checkbox according to your company policy. It is selected by default.




7. In **Advanced settings** > **Object Lock**, select **Disable**.



8. Click **Create bucket**.

### Step 2 - Creating a New IAM Policy

**Important** - You can 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 Harmony SASE bucket. If you grant full access, skip this procedure.

1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Policies** tab and click **Create policy**.
4. Paste this snippet as a JSON file. Replace `test` with the bucket name.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test"
        },
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test/*"
        }
    ]
}
```

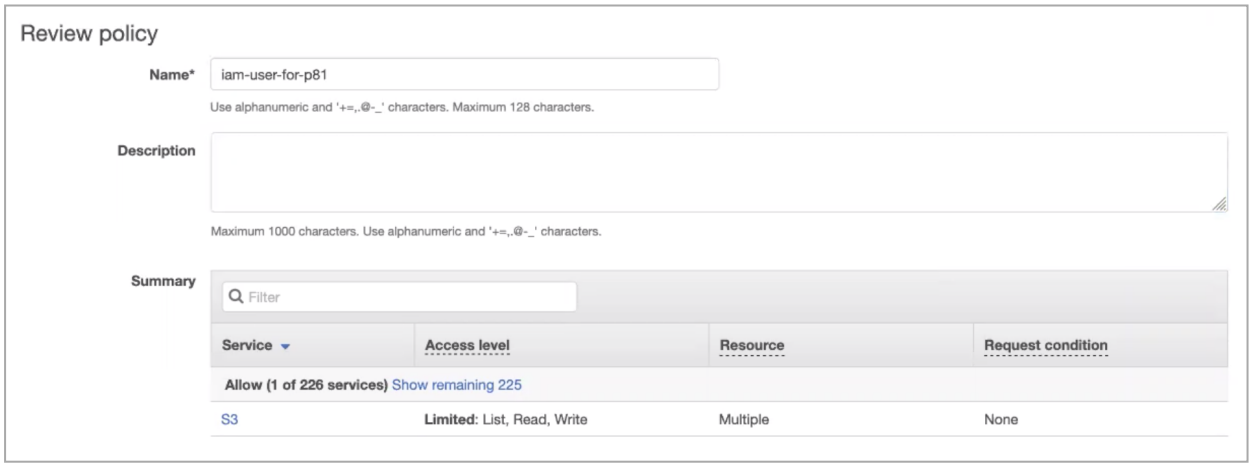


**Important** - For a full list of permissions granted, see permissions. To restrict the list of permissions, add the highlighted text to the syntax.

```
{
"Version" : "2012-10-17",
"Statement" : [
{
"Effect" : "Allow" ,
"Action" : [
"s3:ListBucket",
"s3:GetBucketLocation"
],
"Resource" : ["${aws_s3_bucket.pm81-logs.arn}"]
},
{
"Effect" : "Allow" ,
"Action" : [
"s3:PutObject" ,
"s3:GetObject" ,
"s3:DeleteObject" ],
"Resource" : ["${aws_s3_bucket.pm81-logs.arn}/*" ]
}
]}
```

5. Click **Review policy**.

   The **Review policy** window appears.

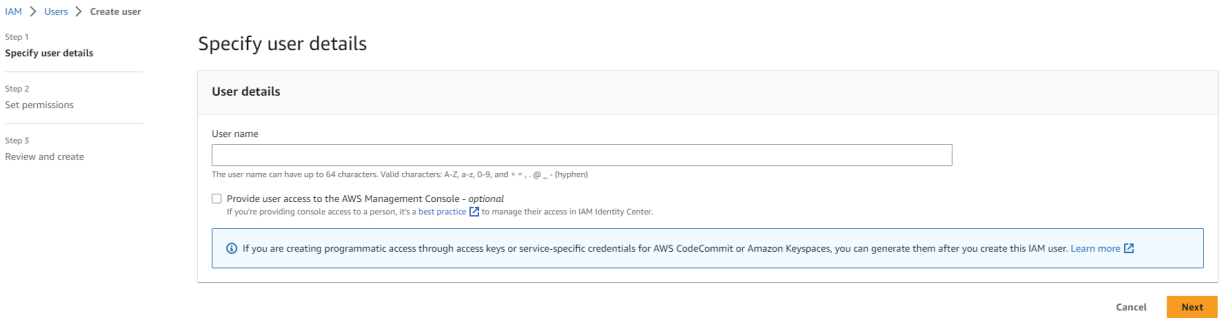



6. Enter these:
   a. **Name**: Name of the policy.
   b. (Optional) **Description**
7. Click **Create policy**.

## Step 3 - Creating an AWS User

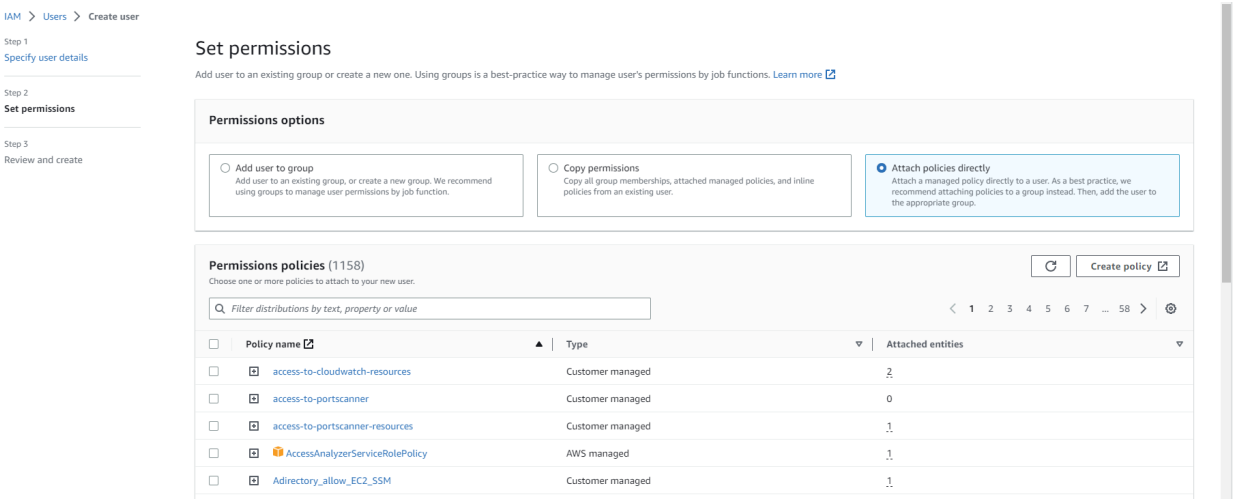
1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Users** tab and click **Create user**.
4. In the **Username** field, enter a name.

   Click **Next**.




5. Click **Attach policies directly** and select the policy you created earlier.

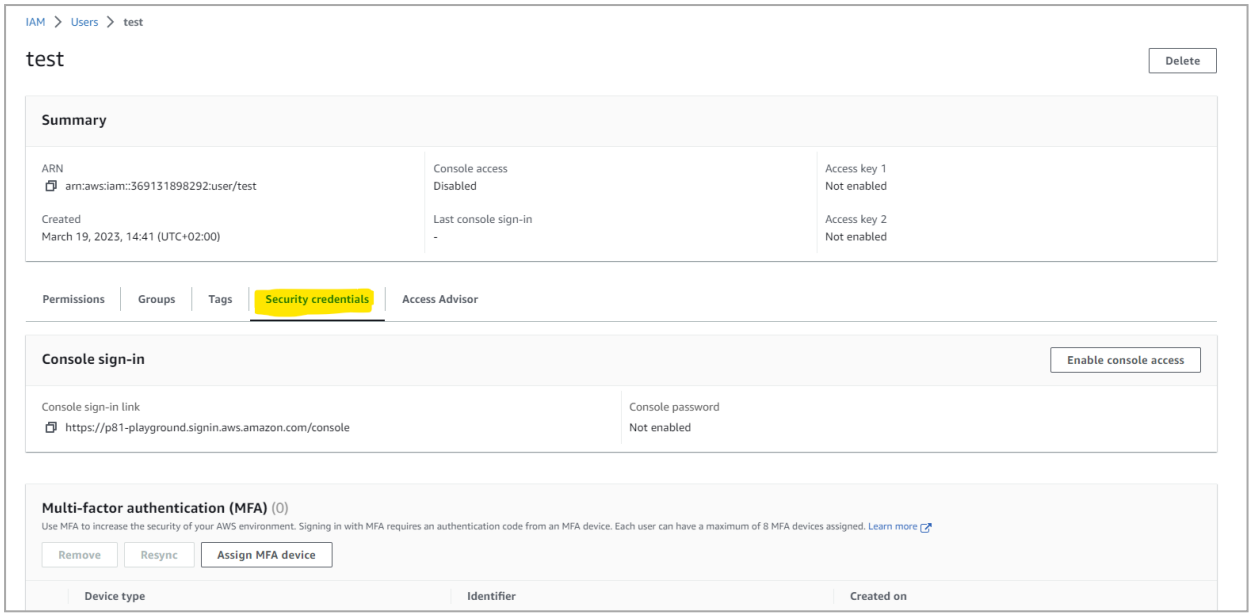
   If you have granted full access, then select the S3 full access AWS managed policy.



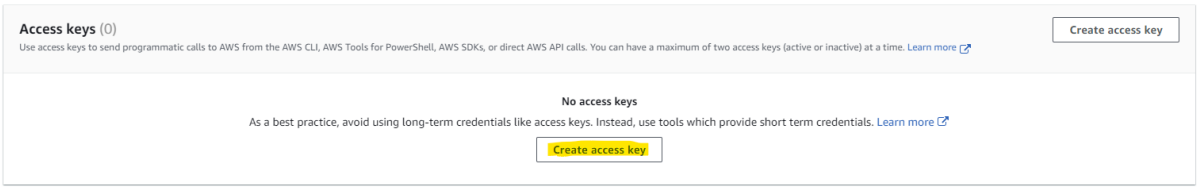

6. Click **Next**.

## Step 4 - Creating an AWS Access Key

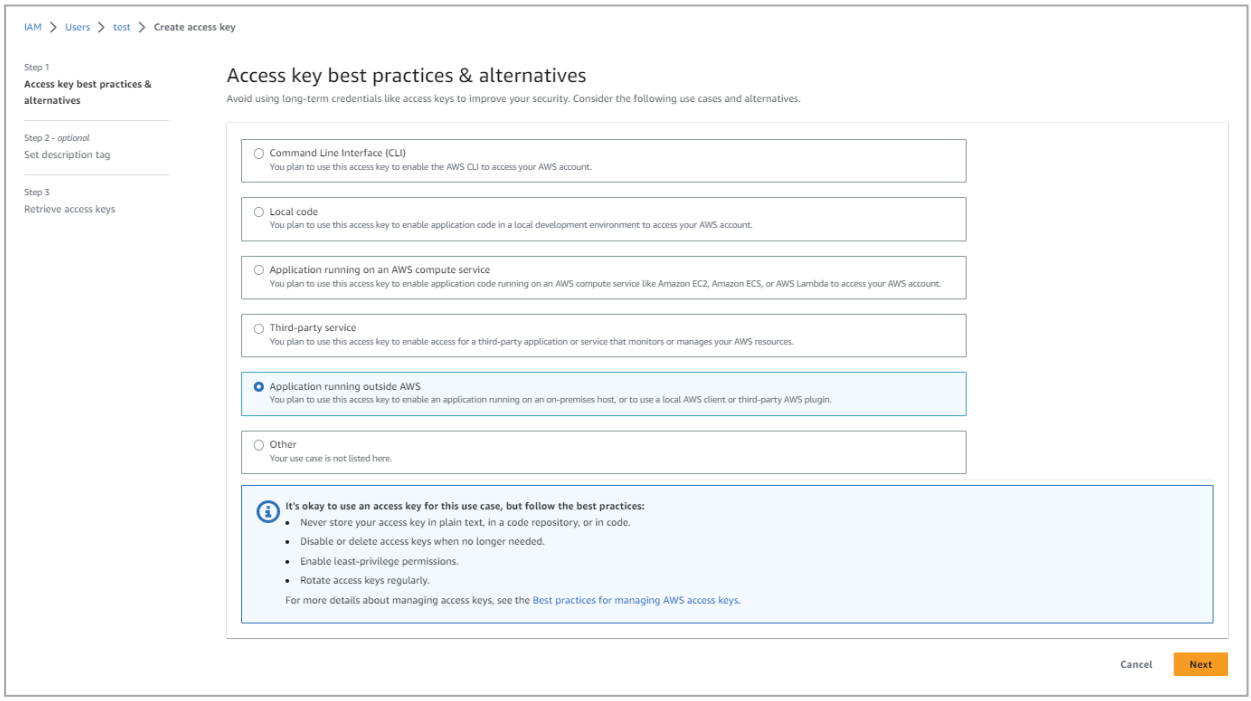
1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Users** tab and select the user you have created.
4. Click the **Security credentials** tab.




5. Scroll down to **Access keys** and click **Create access key**.

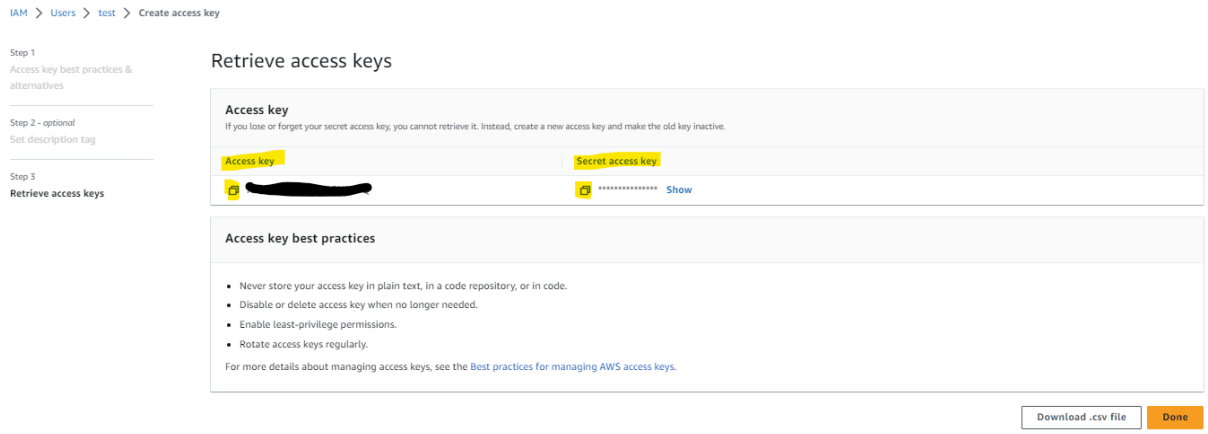



6. Select **Application running outside AWS** and click **Next**.




7. Select **Create access key**.
8. Description tag is optional.

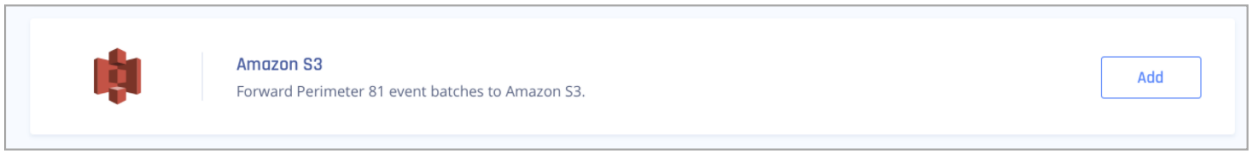
9. Copy the **Secret access key** and the **Access key**.



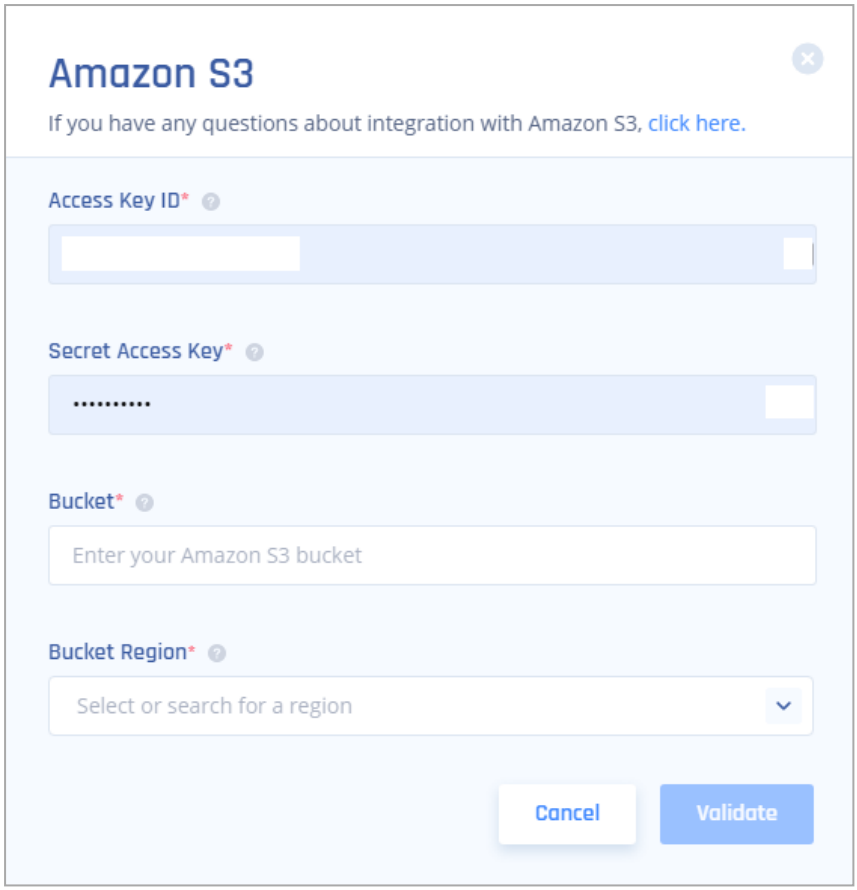

10. Click **Done**.

## Configuring the Amazon S3 Integration in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **SIEM integrations** section, in the **Amazon S3** row, click **Add**.




The **Amazon S3** window appears.




3. In the **Access Key ID** field, enter the **Access key** copied from AWS console.
4. In the **Secret Access Key** field, enter the **Secret access key** copied from AWS console.
5. In the **Bucket** field, enter the Amazon S3 bucket name (for example in this case, arn:aws:s3:::test, the bucket name is test)
6. In the **Bucket region** field, enter the region selected when you created the Amazon S3 bucket.
7. Click **Validate**.

## Troubleshooting

| Status message | Action required |
|---|---|
| Success | None |
| S3_INVALID_ ACCESS_KEY_ID | Make sure you copied the correct access key ID. |
| S3_INVALID_ SECRET_ACCESS_ KEY | Make sure you copied the correct secret access key. |

| Status message | Action required |
|---|---|
| S3_INVALID_ BUCKET | Make sure the Bucket name in Harmony SASE matched the Bucket name in Amazon S3 (case sensitive). |
| S3_ACCESS_ DENIED_BUCKET | The IAM user does not have the required access permissions to the bucket. Make sure to attach the appropriate policy. |

# ConnectWise PSA

ConnectWise PSA allows Managed Service Providers (MSPs) to streamline the billing process through automation with ConnectWise Manager.

It can receive product catalog and usage data from Perimeter 81 and automate customer invoices.

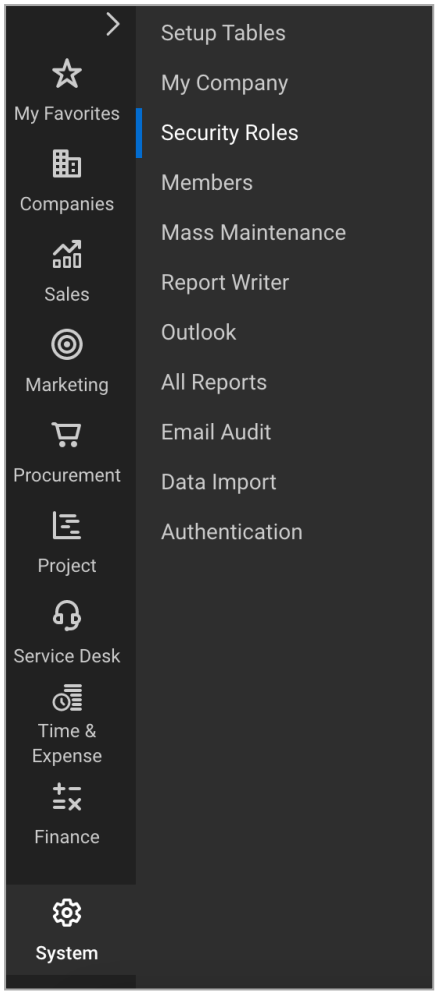
**Note** - This is available only for the accounts in the Perimeter 81 workspace.

## Generating API Key in ConnectWise PSA

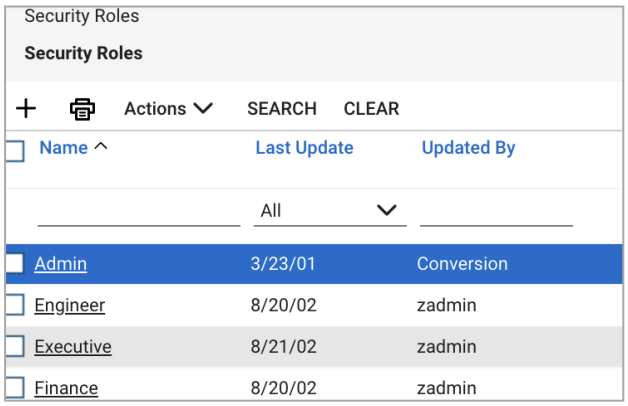
Harmony SASE uses an API key to authenticate the ConnectWise PSA integration.

**To generate the API key in ConnectWise PSA:**

1. Log in to the ConnectWise PSA portal.
2. Go to **System** > **Security Roles**.




3. Select the role for this integration.




4. Set these permissions:

   a. **Companies > Company Maintenance > Inquire Level= All**



b. **Finance** > **Agreements** > **Inquire Level=All**

c. **Finance** > **Agreements** > **Add Level=All**




d. **Procurement** > **Product Catalog** > **Inquire Level= All**

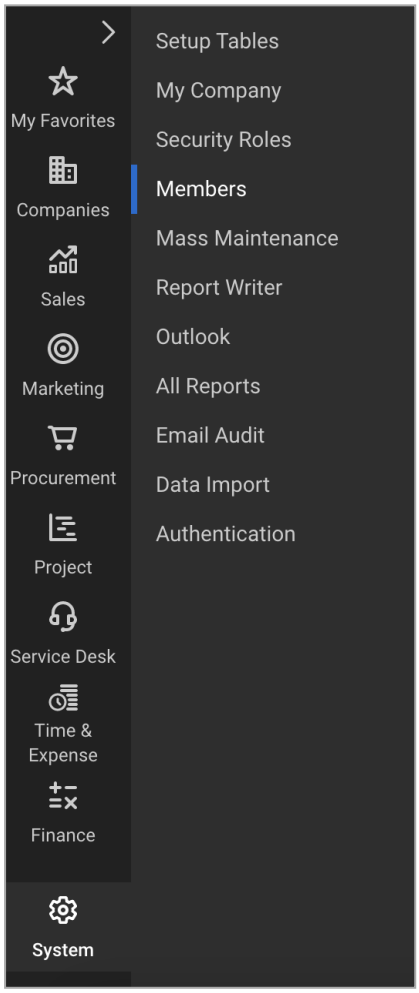
e. **Procurement** > **Product Catalog** > **Add Level= All**



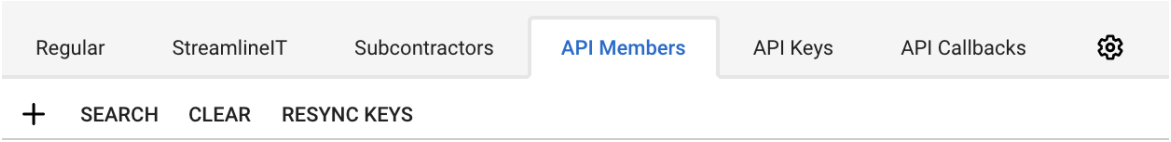

f. **System** > **Table setup** > **Inquire Level= All**



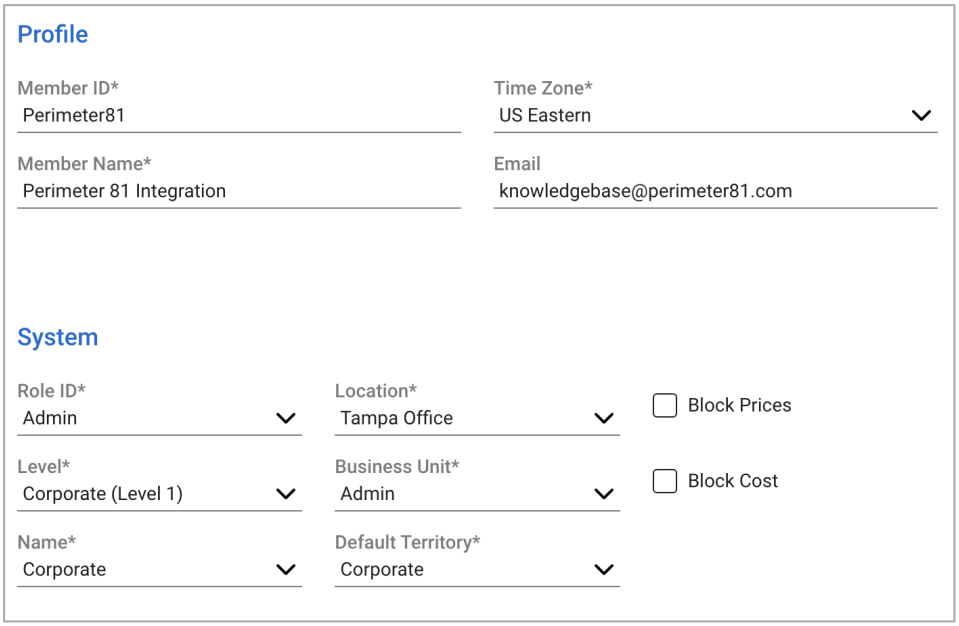

5. Click **Save**.
6. To generate the API key, from the **System** menu, click **Members**.



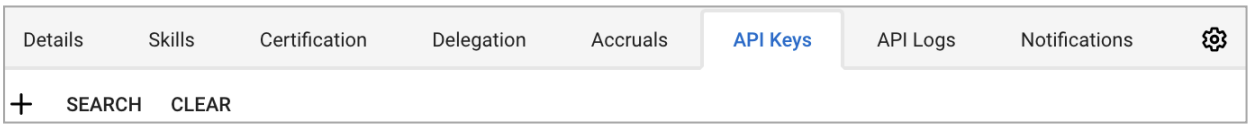

7. To add an API membership for Perimeter 81, click **API Members** tab and then click **+**.



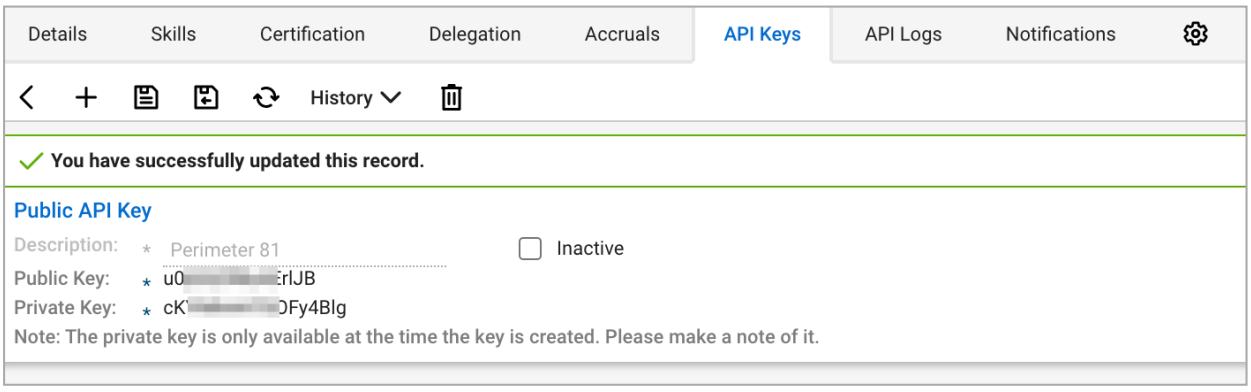

8. Enter the member details and click **Save**.




9. Select the newly created membership from the list of members, and then click the **API Keys** tab.




10. Create a new API key pair.



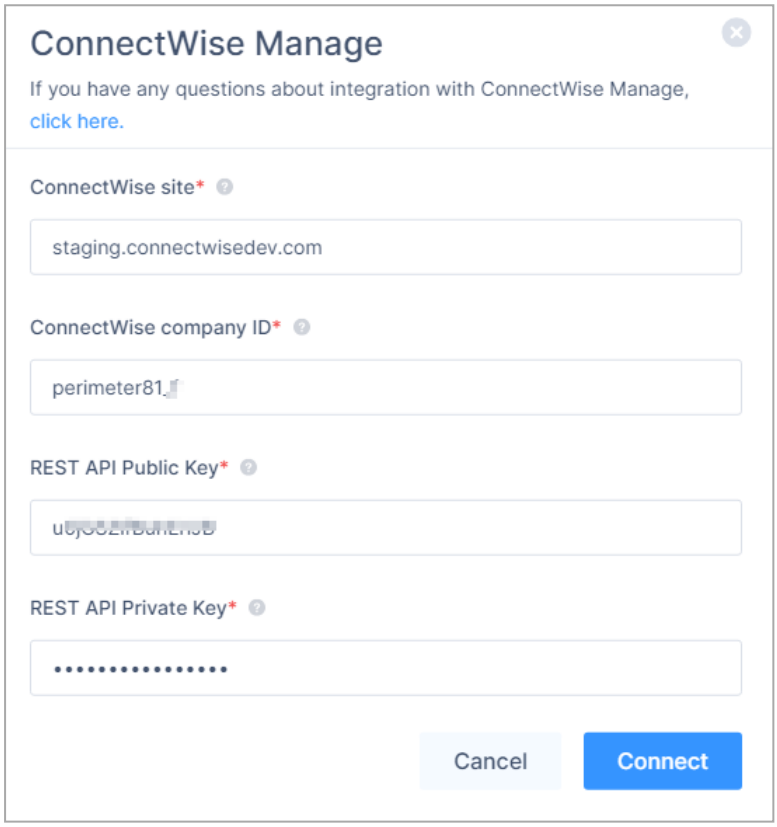

11. Copy the public and private keys.

## Configuring the Integration in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **PSA integrations** section, in the **ConnectWise Manage** row, click **Add**.




3. Enter these:




| Item | Description |
|---|---|
| ConnectWise site | URL of the ConnectWise PSA portal login screen. |
| ConnectWise company ID | Company ID registered with ConnectWise PSA portal. |
| REST API Public Key | API Public Key generated in the ConnectWise PSA portal. |
| REST API Private Key | API Public Key generated in the ConnectWise PSA portal. |

4. Click **Connect**.

   The *Successfully connected to ConnectWise Manage* message appears.

5. Click **Apply**.

   The *ConnectWise integration has been configured successfully* message appears.

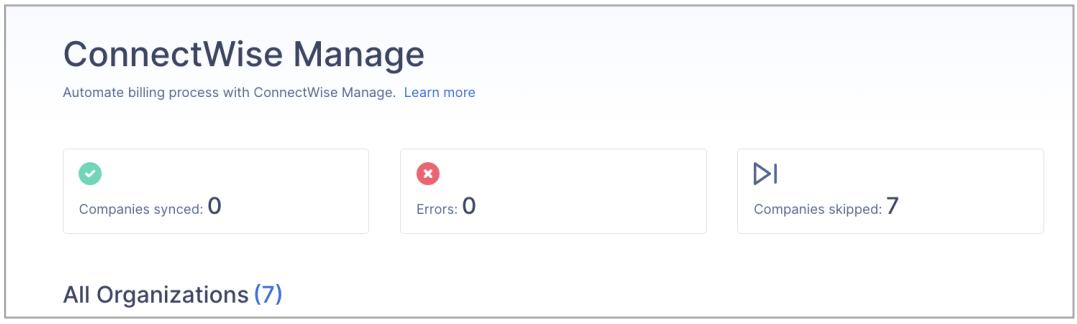
   After a successful integration, the Harmony SASE product catalog is synchronized with ConnectWise PSA.

## Mapping Customers and Agreements

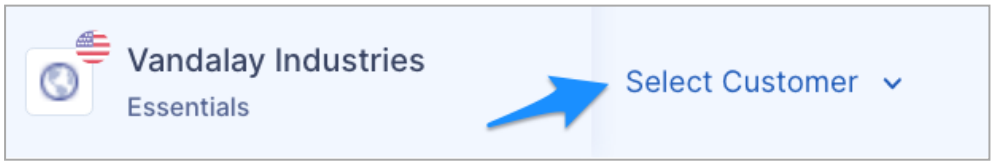
1. Access the Harmony SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **PSA integrations** section, in the **ConnectWise Manage** row, click **Manage**.



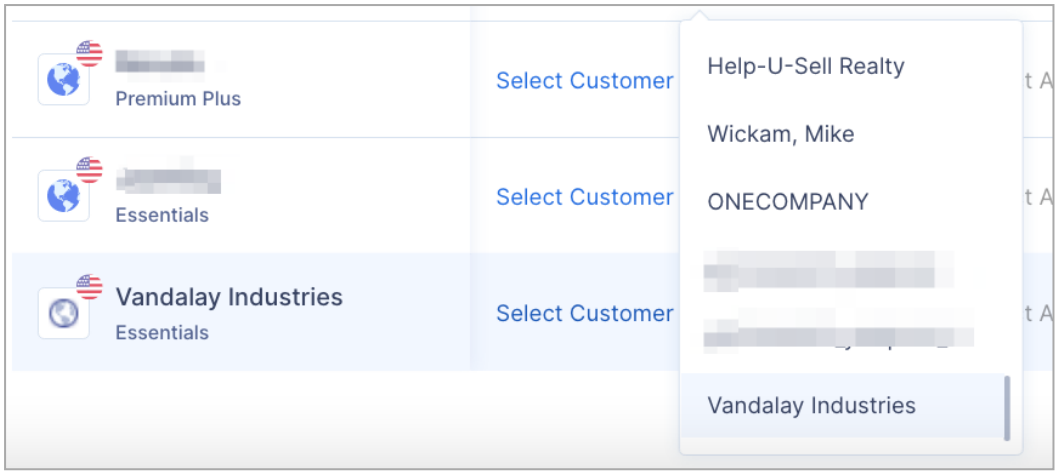

   The **ConnectWise Manage** page appears that displays all the organizations you manage in Perimeter 81.



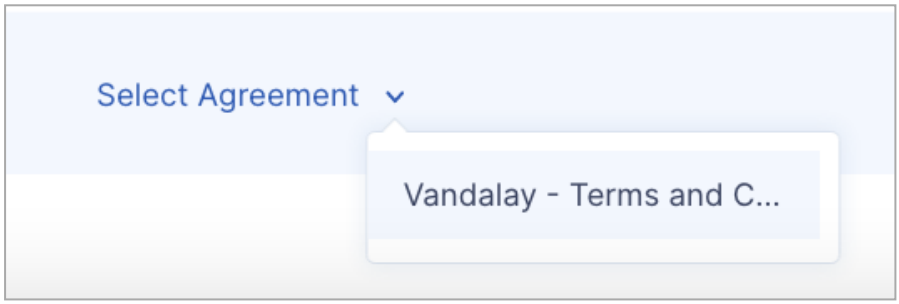

3. For the organization you want to sync with ConnectWise Manage, click **Select Customer**.




4. Select the corresponding account on ConnectWise Manage.

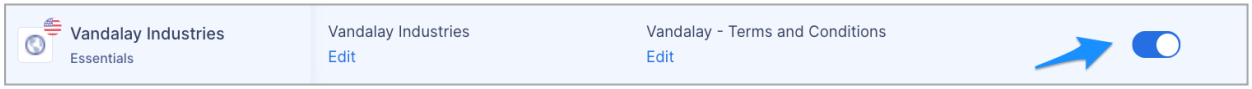



5. Select the ConnectWise Manage agreement that you have with your customer.




6. After you map customers and agreements, enable synchronization for each customer.

   Customers selected for synchronization are synchronized automatically every hour.



# Identity Providers

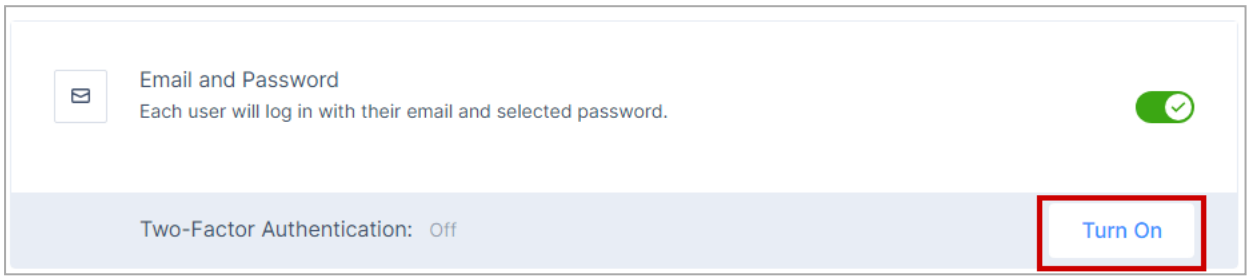
Harmony SASE supports integration with these third-party Identity Providers (IDP) to identify members and allow Single Sign-On (SSO) when logging in with the Harmony SASE Agent.

- SAML 2.0
  - *Generic SAML*
  - *Active Directory Federation Services (AD FS)*
  - *Auth0*
  - *OneLogin*
  - *PingOne for Enterprise*
  - *PingFederate*
  - *Rippling*
  - *JumpCloud*
  - *Okta with SAML*
- Google Workspace
  - *Google Applications with SAML 2.0*
  - *Google Services*
- Microsoft Azure
  - *Azure Active Directory (SAML 2.0)*
  - *Azure Active Director (Enterprise Application)*
  - *Azure Active Director (App Registration)*
- SCIM
  - *Okta (SCIM)*
  - *Azure Active Directory (SCIM)*
- *On-Premises Active Directory*

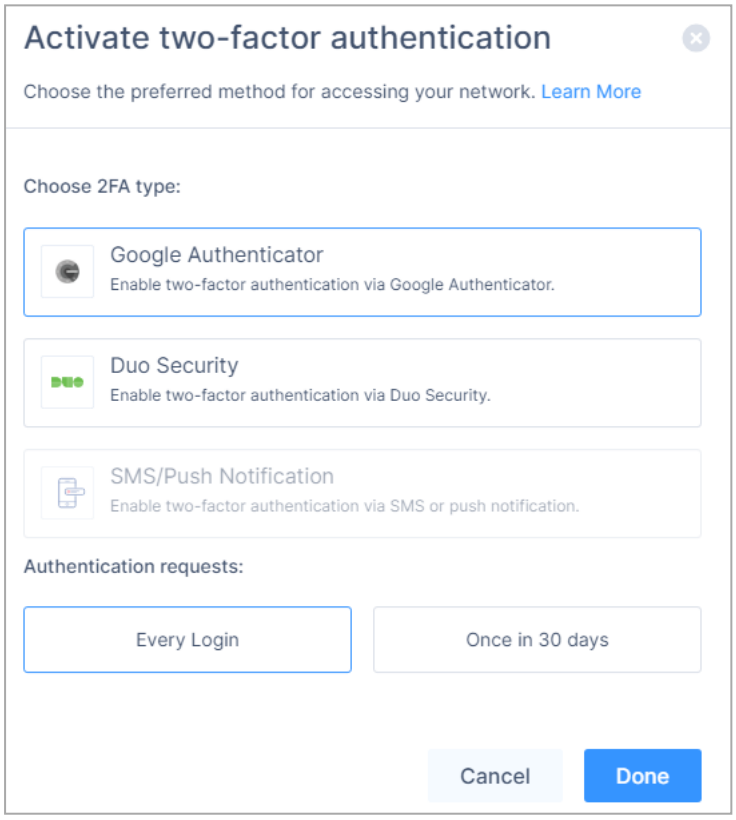
# Two-Factor Authentication

## Activating Two-Factor Authentication

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Identity Providers**.
2. For the Identity Provider for which you want to activate 2FA, click **Turn On** for **Two-Factor Authentication**.




3. In the **Choose 2FA type** section, select the authentication type:



- Google Authenticator
- Duo Security
  - Enter the details in the **Integration key**, **API hostname**, and **Secret key** fields. See *"Configuring Duo Security for Two-Factor Authentication" below*.
- SMS/Push Notification

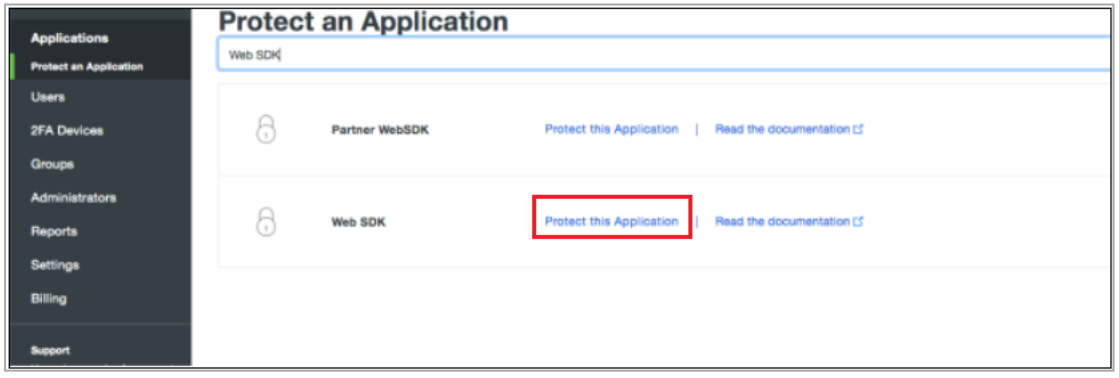
4. In the **Authentication requests** section, select the frequency of authentication:
   - Every Login
   - Once in 30 days
5. Click **Done**.

### Configuring Duo Security for Two-Factor Authentication

1. Log in to the Duo Security Management Portal.
2. Go to **Applications** and click **Protect an Application**.

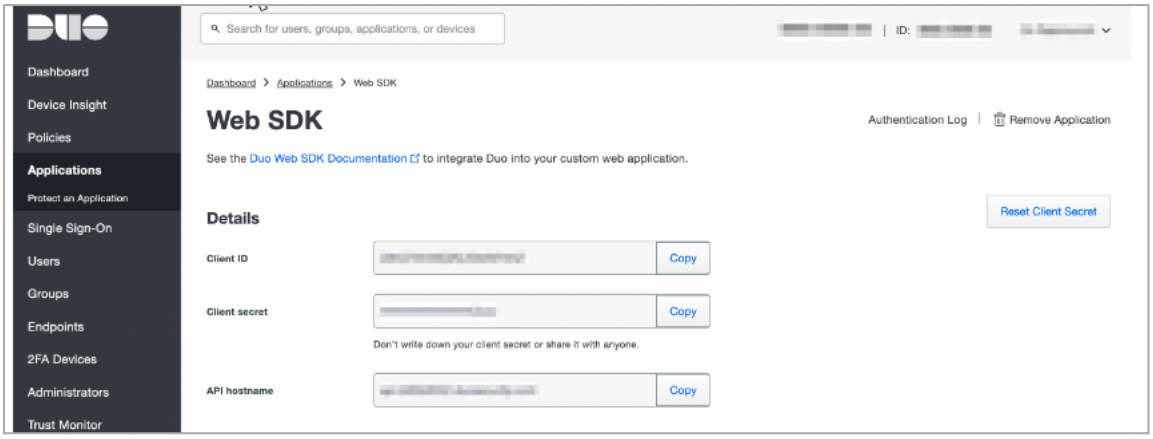



3. Search for **Web SDK** and click **Protect this Application** for **Web SDK**.

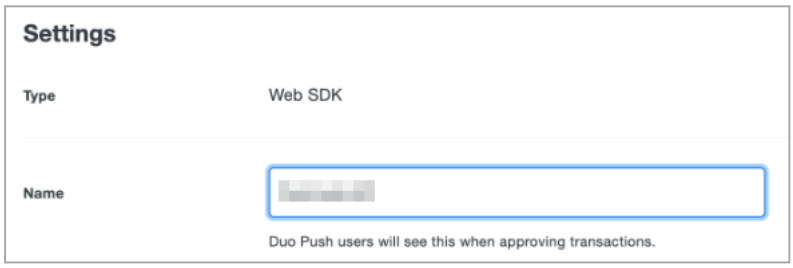



The system creates the application.

4. In the **Details** section, copy the **Client ID**, **Client secret**, and **API hostname**.

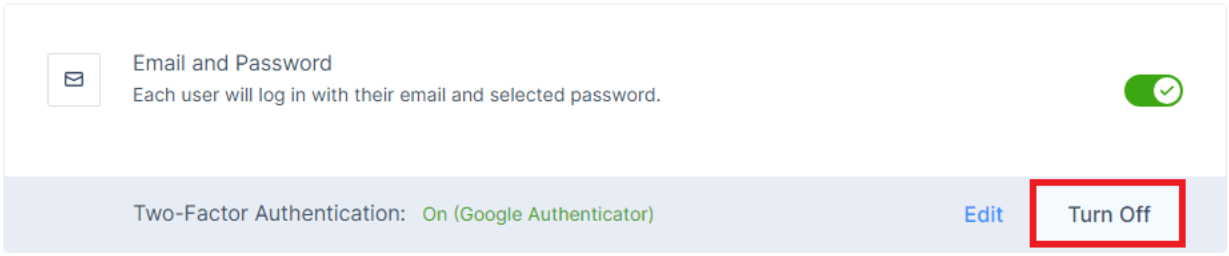



5. (Optional) Scroll down to **Settings** and in the **Name** field, change the name of the application.

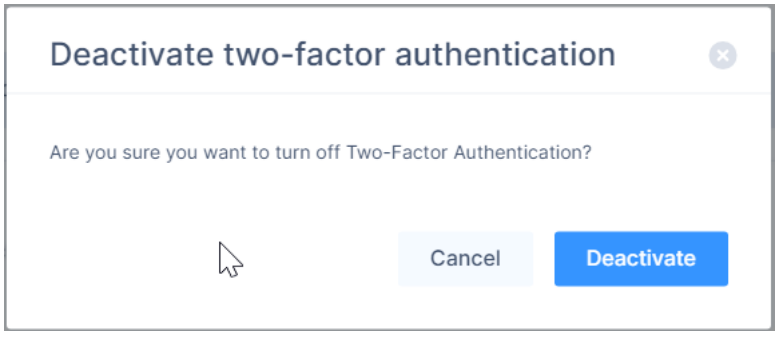



## Deactivating Two-Factor Authentication

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Identity Providers**.
2. For the Identity Provider for which you want to deactivate 2FA, click **Turn Off** for **Two-Factor Authentication**.




3. Click **Deactivate** in the confirmation pop-up that appears.



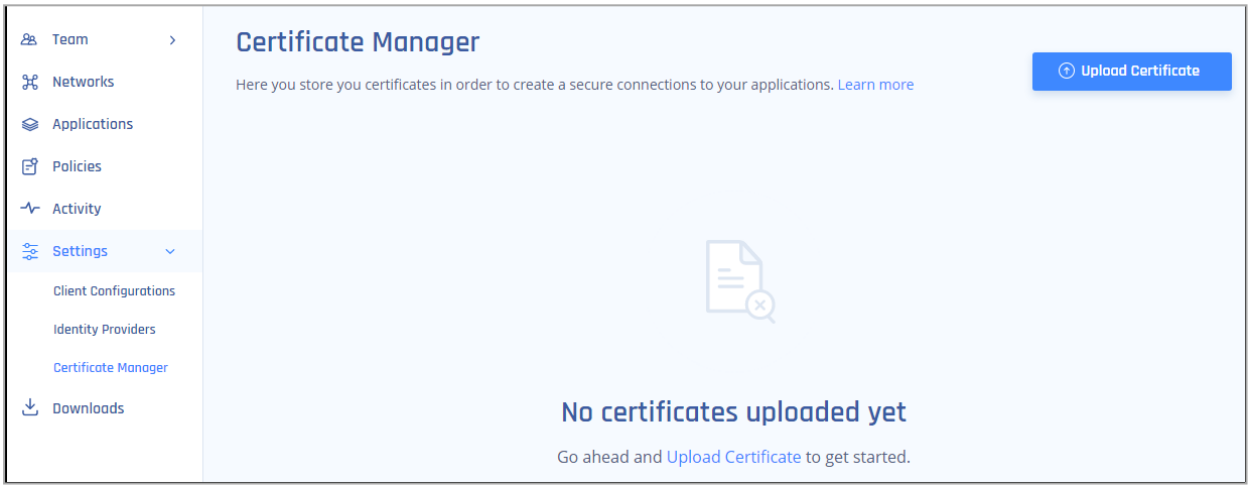
# Certificate Manager

**Certificate Manager** allows to upload the application domain SSL certificate. This certificate is required to configure URL Alias for members to access the applications.

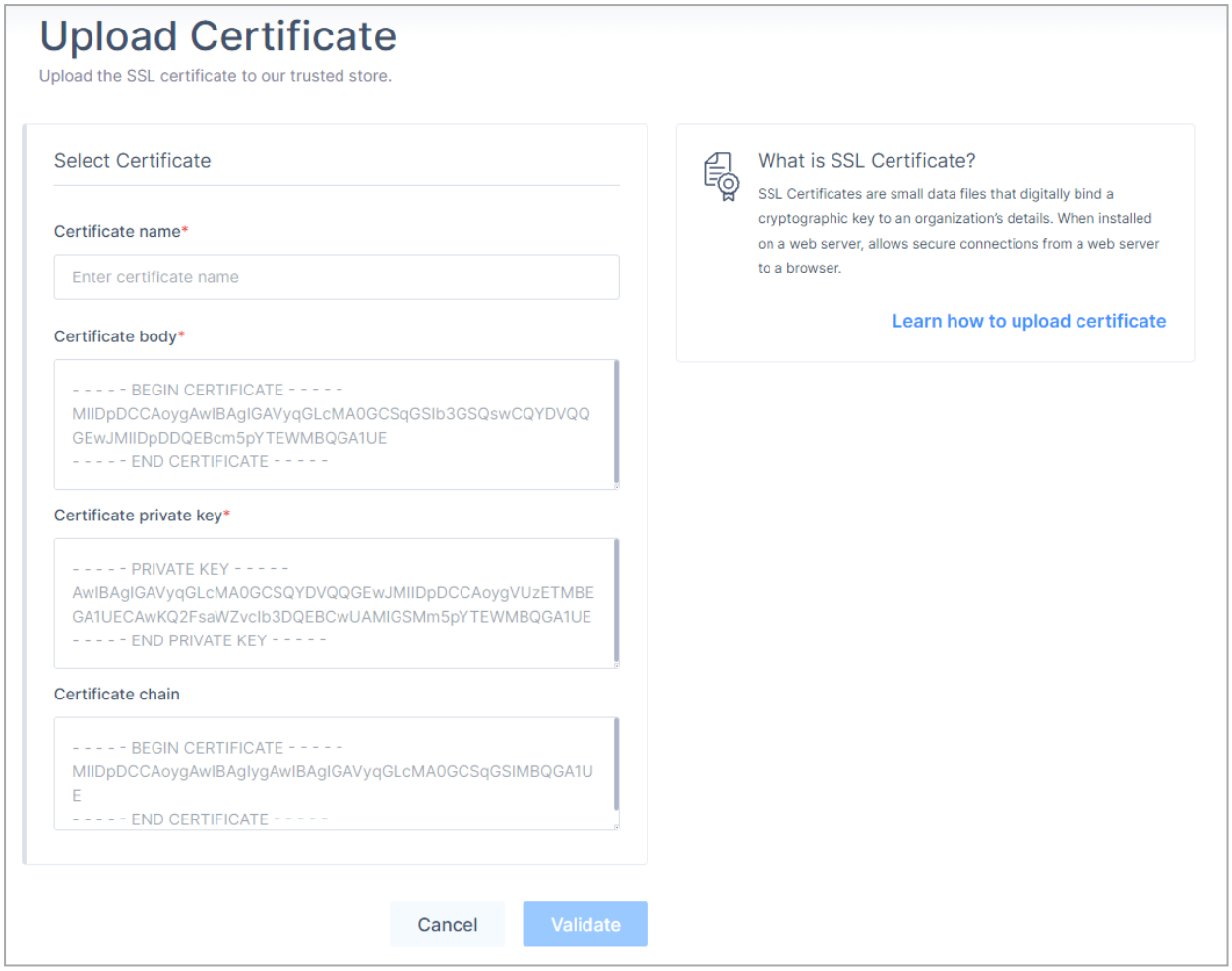
A domain-validated certificate (DV) is an X.509 digital certificate used for Transport Layer Security (TLS). The domain name of the applicant is validated by providing control over a DNS domain.

**To upload application domain certificates:**

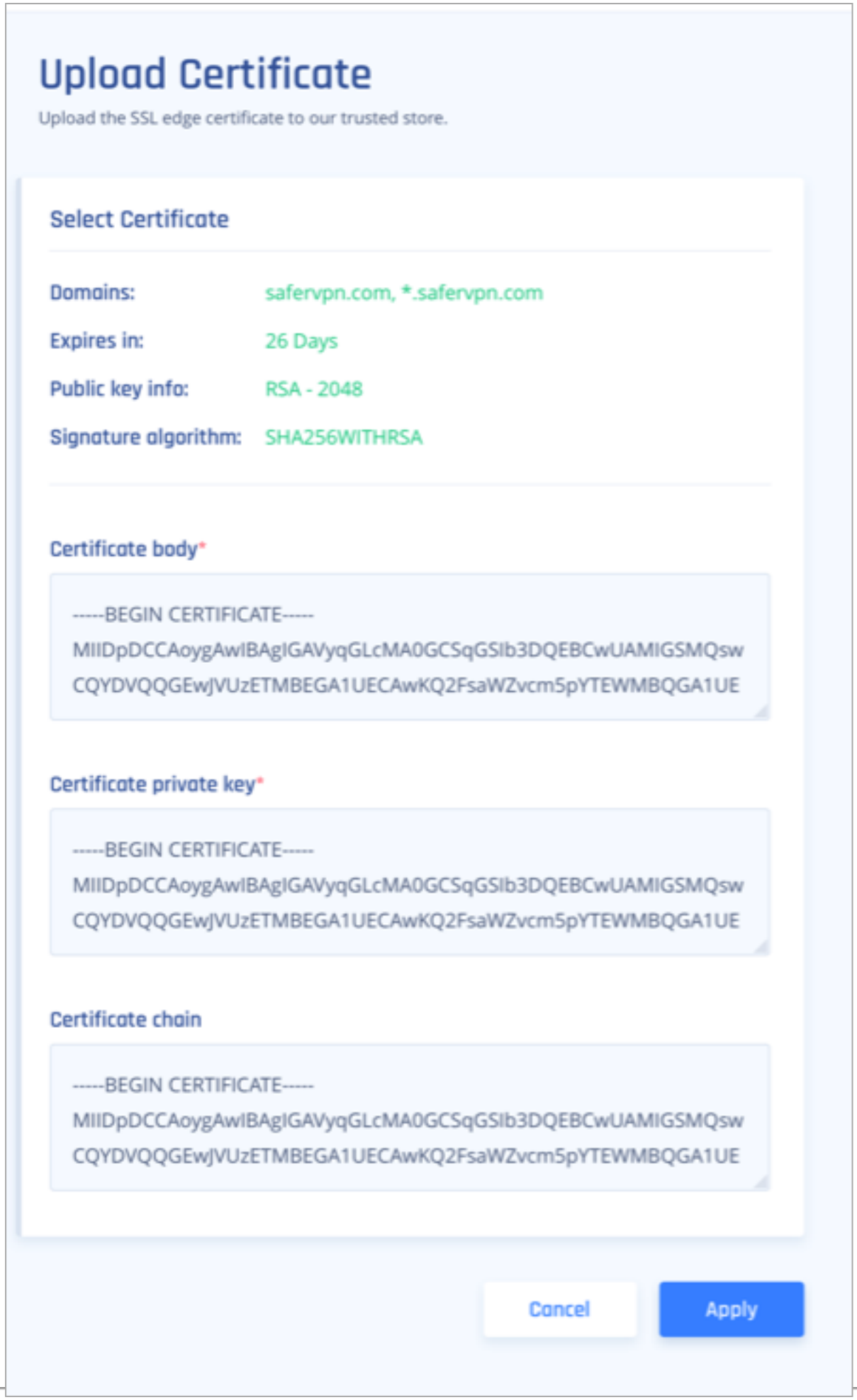
1. Access the Harmony SASE Administrator Portal and click **Settings** > **Certification Manager**.
2. Click **Upload Certificate**.




The **Upload Certificate** window appears.




3. Enter these:
    a. **Certificate name**
    b. **Certificate body**
    c. **Certificate private key**
    d. **Certificate chain**
4. Click **Validate** to ensure this certificate is correct.
5. Click **Apply**.


Upload Certificate
Upload the SSL edge certificate to our trusted store.
Select Certificate
Domains:
safervpn.com, *.safervpn.com
Expires in:
26 Days
Public key info:
RSA - 2048
Signature algorithm:
SHA256WITHRSA
Certificate body*
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Certificate private key*
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Certificate chain
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAVyqGLcMA0GCSqGSIb3DQEBCwUAMIGSMQsw
CQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
Cancel
Apply

# Support Access

The **Support Access** page allows you to assign Support Access role to Harmony SASE support engineer. This allows the Harmony SASE support engineer to temporarily access your tenant without credentials for troubleshooting purposes.

You can grant Support Access role to only one member or a group at a time.

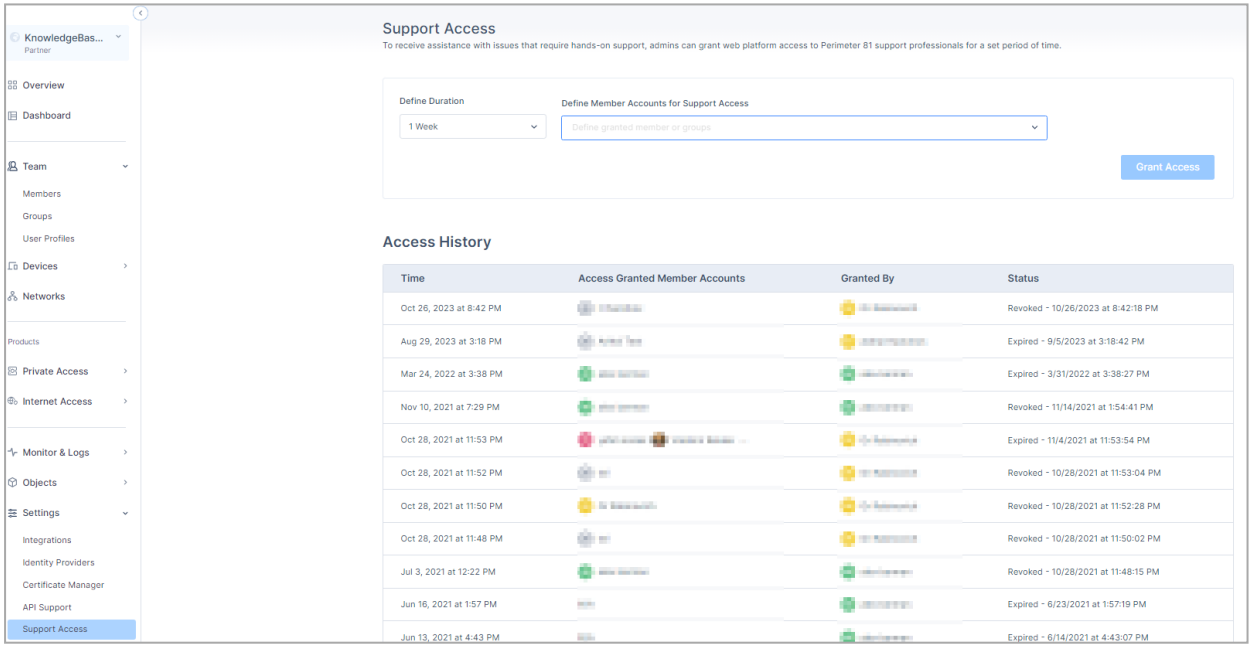
**Notes -**

- You do not require an additional user license to enable the Support Access role.
- When a Harmony SASE support engineer access your tenant, is it logged in *"Member Activity" on page 224*.
  For Premium or Enterprise plans, the logs can be sent to the SIEM or Splunk instance.

## Granting the Support Access Role

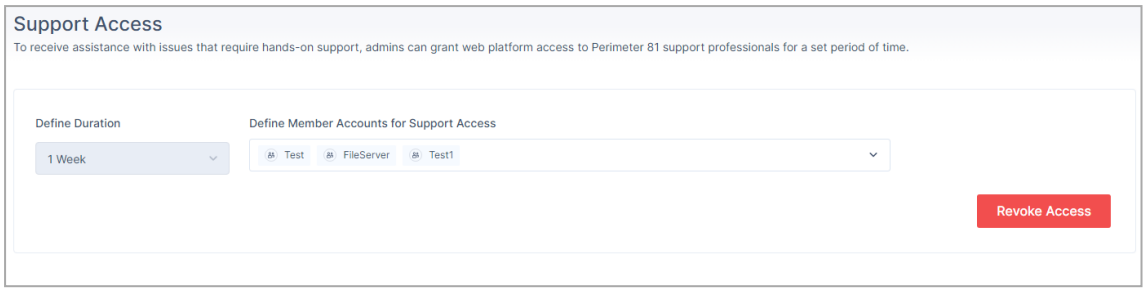
1. Access the Harmony SASE Administrator Portal and click **Settings** > **Support Access**.

   The **Support Access** page appears.




2. From the **Define Duration** list, select the time duration for which Support Access role is valid.
3. From the **Define Member Accounts for Support Access** list, select the member or member groups for the Support Access role.
4. Click **Grant Access**.

5. To revoke the current Support Access role, click **Revoke Access**.




# Access History

The **Access History** table shows the history of members and groups with the Support Access role.

| Item | Description |
|---|---|
| Time | Time when the Support Access role was granted, revoked or expired. |
| Access Granted Member Accounts | Members and member groups assigned with the Support Access role. |
| Granted By | Owner that granted the Support Access role. |
| Status | Status of the Support Access role.<br>■ Active<br>■ Revoked<br>■ Expired |