HARMONY

11 March 2025

HARMONY SASE

Administration Guide

CHECK POINT™

Check Point Copyright Notice

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.

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.

Patent Notice

Harmony SASE is protected by the following patents in the United States and elsewhere.
This page is intended to serve as notice under 35 U.S.C. § 287(a):
US10,440,762, US11,271,899, US11,502,993, US11,558,184, US11,777,718, US11,888,815, US12,010,132

Revision History

Date	Description
03 March 2025	Added: ■ *"Cisco Firepower" on page 201* ■ URL Aliasing for Zero-Trust Applications on Harmony SASE in *"Certificate Manager" on page 900* ■ Harmony SASE platform release notes for February 2025.
24 February 2025	Updated *"Managing a Network" on page 147*.
19 February 2025	Added *"SaaS API" on page 669*.
30 January 2025	Added Harmony SASE platform release notes for January 2025.
24 January 2025	Added *"MDM Deployment of the Harmony SASE MacOS Agent with Internet Security" on page 92*.
22 January 2025	■ Added *"Member Roles and Permissions" on page 53*. ■ Added release notes for: • Windows agent 11.2.1.2378 • Mac agent 11.2.1.3411
06 January 2025	Updated *"Regions and Point-of-Presence" on page 110*.
31 December 2024	■ Added *Resolving MDM Deployment Issues on MacOS*. ■ Added Harmony SASE platform release notes for December 2024.
23 December 2024	Added *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 221*.
05 December 2024	Added Harmony SASE Linux agent 10.0.0.879 release notes.
29 November 2024	Added Harmony SASE Android / Chromebook agent 8.1.2.3355 release notes.
27 November 2024	Added Harmony SASE platform release notes for November 2024.
12 November 2024	Added Harmony SASE Windows agent 11.1.0.2248 release notes.

Date	Description
03 November 2024	Added information about DenyUnauthenticatedBind.
30 October 2024	▪ Added Harmony SASE platform release notes for October 2024. ▪ Updated the commands for Silent Installation of macOS agent to address the macOS agent installation file name. See *"Deploying the Agent Using an MDM Application" on page 88*.
21 October 2024	Added: ▪ *"Harmony SASE Agent - Optimized Performance with Minimal Resource Impact" on page 104* ▪ Harmony SASE Windows agent 11.0.11.2205 release notes. ▪ Harmony SASE MacOS agent 11.0.10.2696 release notes.
01 October 2024	Added Harmony SASE Windows agent 11.0.10.2177 release notes.
30 September 2024	▪ Added support for a new client type - **Native**. See *"Adding an RDP Zero Trust Application" on page 617*. ▪ Added Harmony SASE platform release notes for September 2024.
25 September 2024	Added Harmony SASE Agent release notes: ▪ Android / Chromebook agent 8.1.0.3337 ▪ iOS agent 8.3.0.2600
16 September 2024	Added *"Data Residency" on page 33*.
30 August 2024	Added Harmony SASE platform release notes for August 2024.
28 August 2024	Added: ▪ Harmony SASE Agent release notes: • Windows - *"11.0.1.2083" on page 945* • macOS - *"11.0.1.2339" on page 948* ▪ *"Configuring Check Point Redundant IPsec Tunnel" on page 246*
09 August 2024	Added a new section for .msi installation flags for version 11.0 and above, to address the change in Windows agent installation file name. See *"Deploying the Agent Using an MDM Application" on page 88*.

Date	Description
07 August 2024	Added Harmony SASE MacOS agent 11.0.0.2227 release notes. See *Release Notes > Harmony SASE Agent > "MacOS" on page 948*.
01 August 2024	Added Harmony SASE Platform release notes for July 2024. See *Release Notes > Harmony SASE Administrator Portal > 2024 > "July" on page 941*.
31 July 2024	First release of the document in Check Point format.

Table of Contents

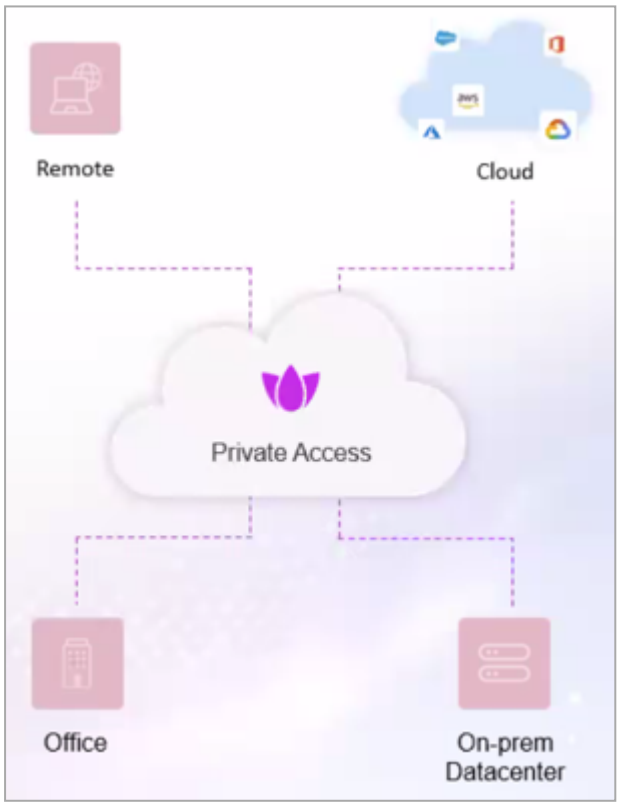
Introduction to Harmony SASE

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.

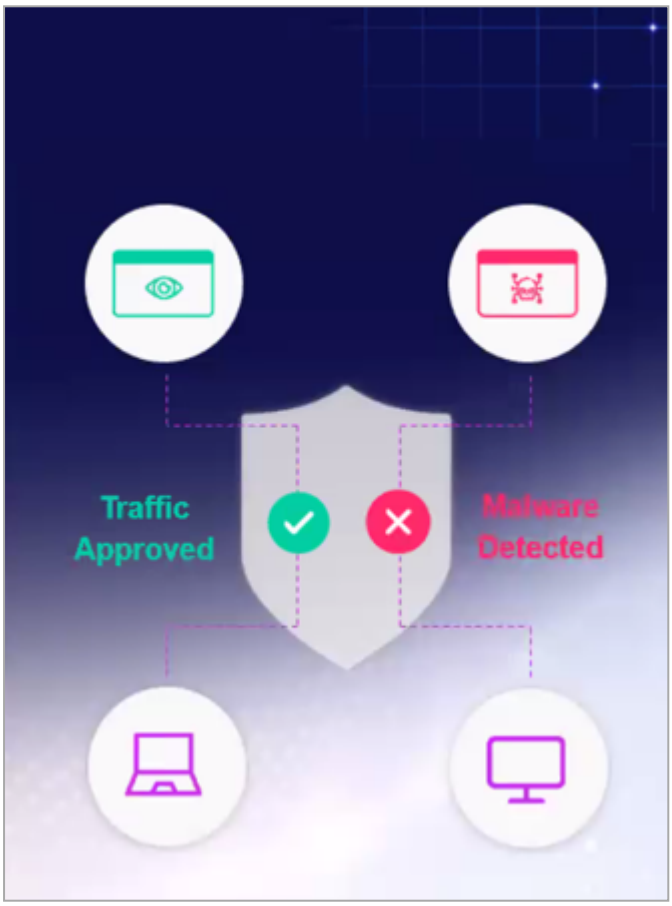


- Agentless access to only specific applications only to authorized members (also known as Application Access), for example, users with BYOD and contractors. The supported types of applications include:

Protocol	Sample Application
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.

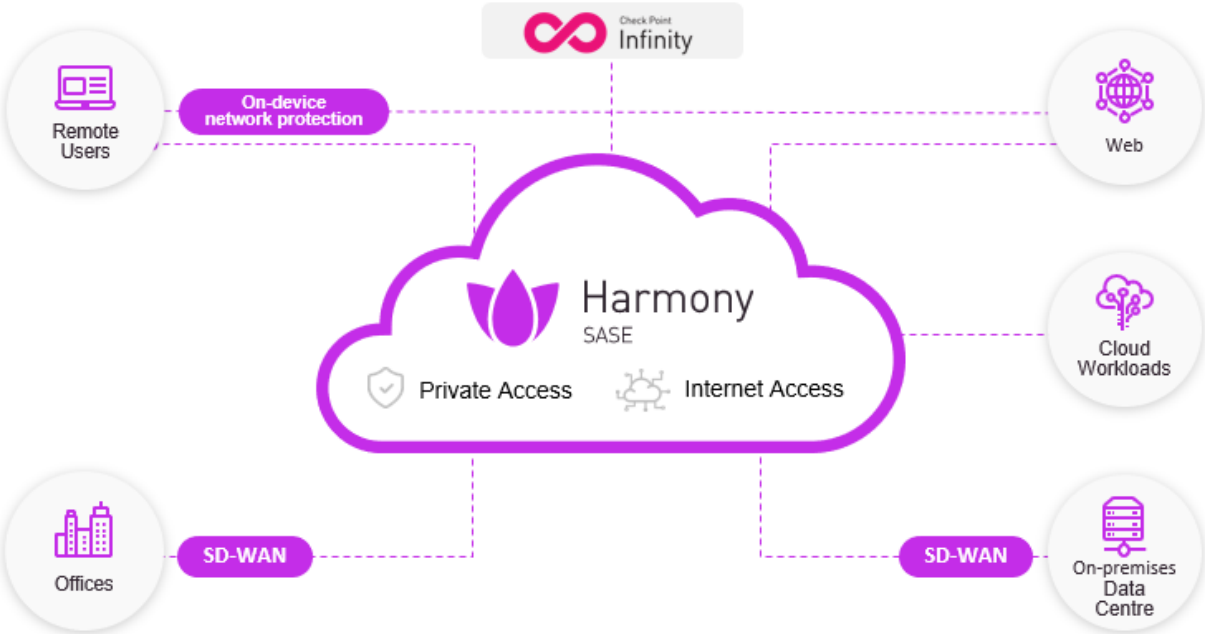
Supported Devices and Operating Systems

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.

Data Residency

For information on supported data residency, see sk182685.

API Support

You can use Harmony SASE API to create, manage, and control network security aspects, including networks, gateways, regions, tunnels, users, and groups.

For more information about Harmony SASE API, see app.swaggerhub.com.

Getting Started

To get started with Harmony SASE:

1. Access the Harmony SASE workspace:
   - If you use the Harmony SASE workspace in the Infinity Portal:
     a. *"Creating an Account in the Infinity Portal" on the next page*.
     b. *"Accessing the Harmony SASE Administrator Portal" on the next page*.
   - If you use the Harmony SASE (Perimeter 81) workspace:
     a. Create an account in the Harmony SASE portal.
     b. Activate the Perimeter 81 subscription.
2. Invite members.
3. To provide a secure private access:
   a. Define your network.
   b. "Firewall" on page 605
   c. Deploy the Harmony SASE Agent on members' devices.
4. To provide a secure application access:
   a. Define your network.
   b. Define the application.
   c. Create application access rule.
5. To provide a secure internet access:
   a. Define web filter rules.
   b. Define the bypass rules.
   c. Deploy the Harmony SASE Agent on members' devices.
6. Monitor:
   - Active sessions
   - Member activity
   - Web activity
   - Malware protection

- Admin activity
- Tunnel status
- Firewall events

Harmony SASE Workspace in the Infinity Portal

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.

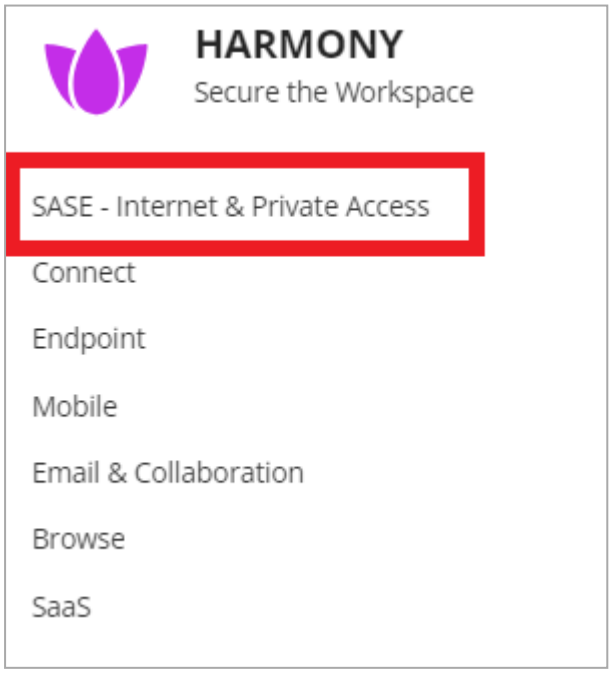
To create an Infinity Portal account, see the Infinity Portal Administration Guide.

Accessing the Harmony SASE Administrator Portal

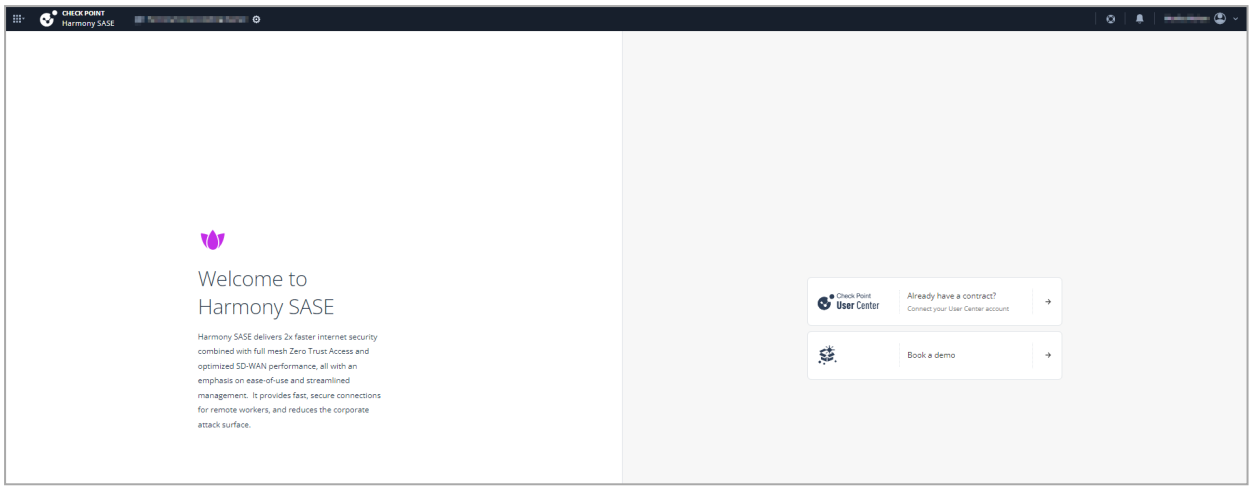
To access the Harmony SASE Administrator Portal:

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**.

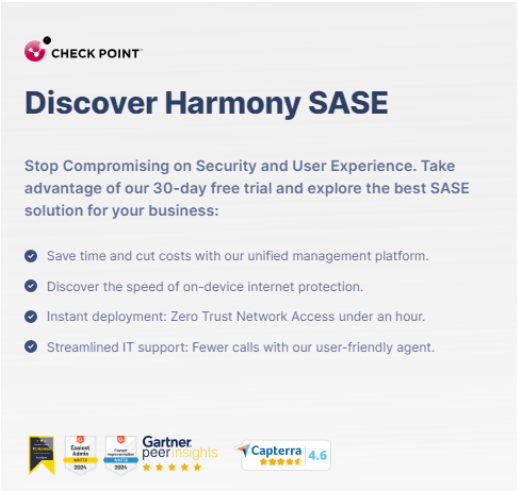


4. If you are accessing the portal for the first time, do one of these:

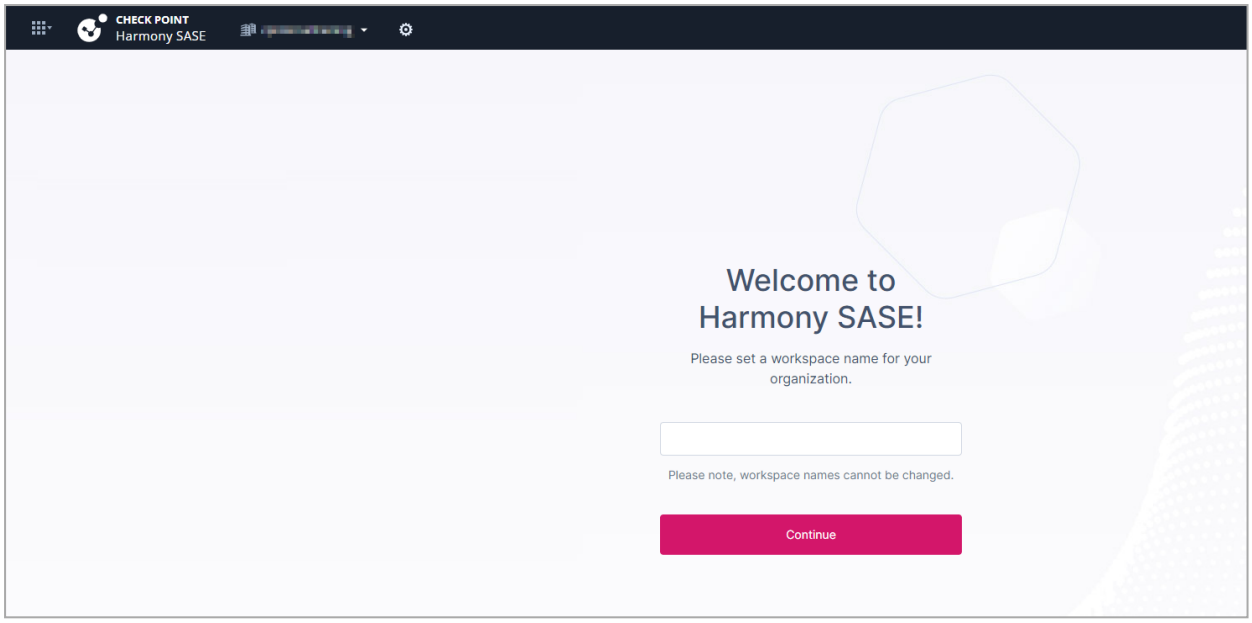


   - If you already have a Check Point contract, click **Already have a contract** to attach the contract to the product. For more information, see **Associated Accounts** in [Infinity Portal Administration Guide](#).
   - If you want to trial the product, click **Book a demo**.

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

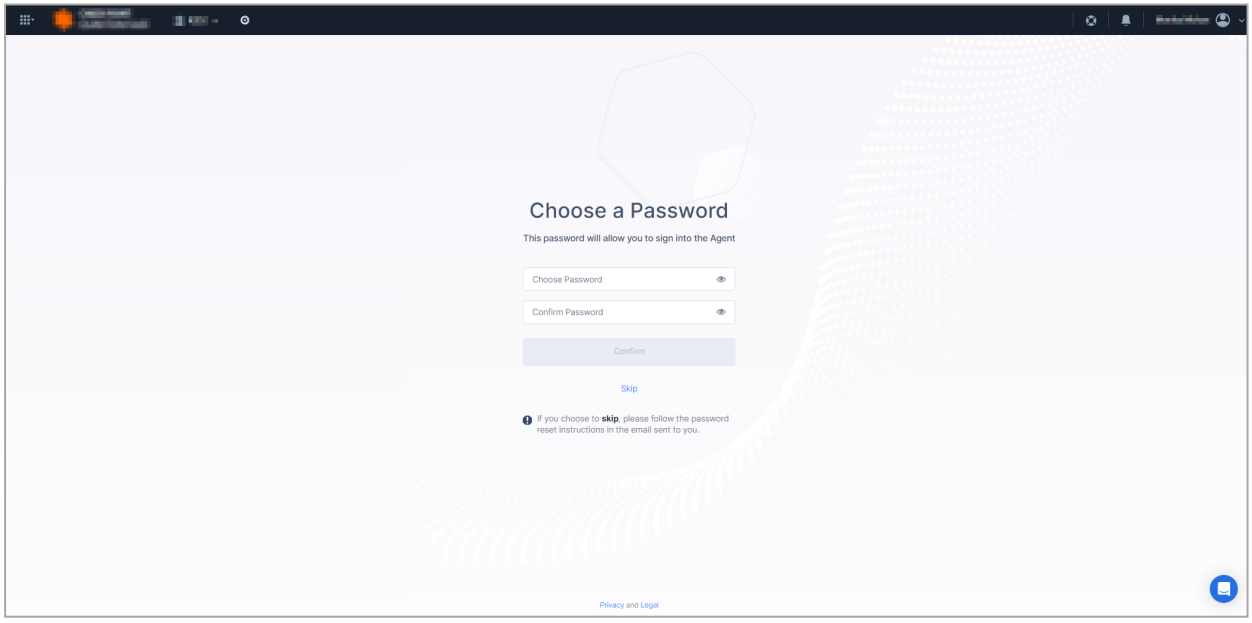


5. Once you fill and submit the form, or If you have already attached the contract with the product, the **Welcome to Harmony SASE** page appears.



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

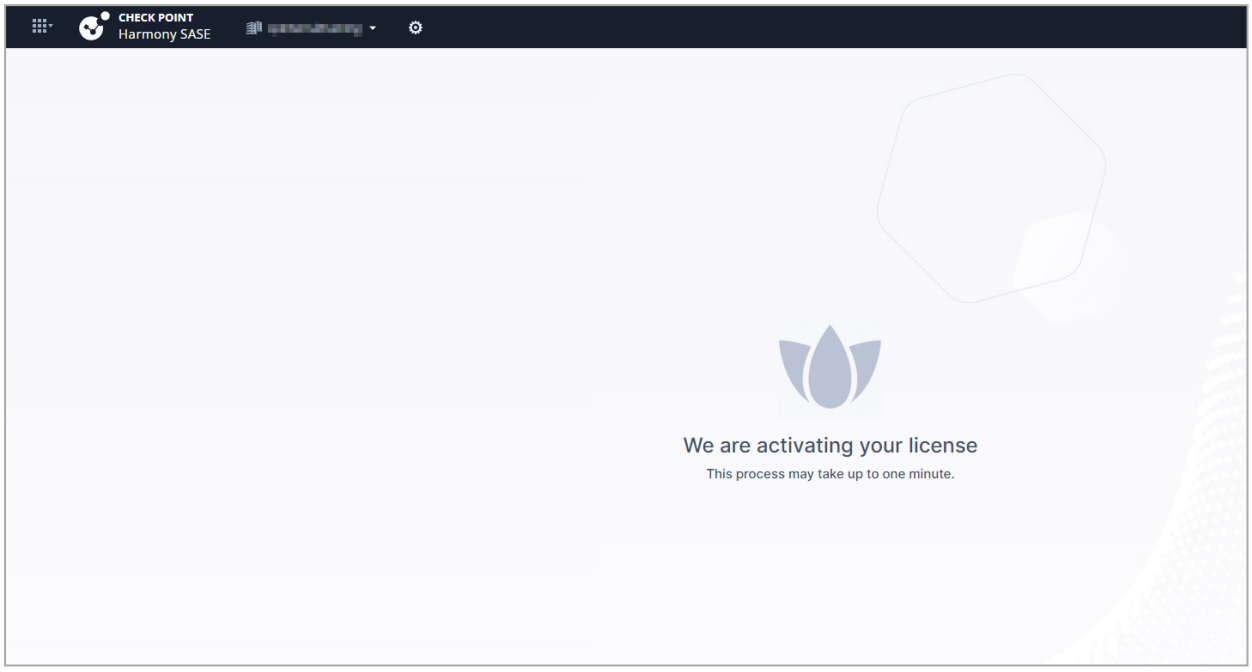
   b. Lower case letter

c. Number 0-9

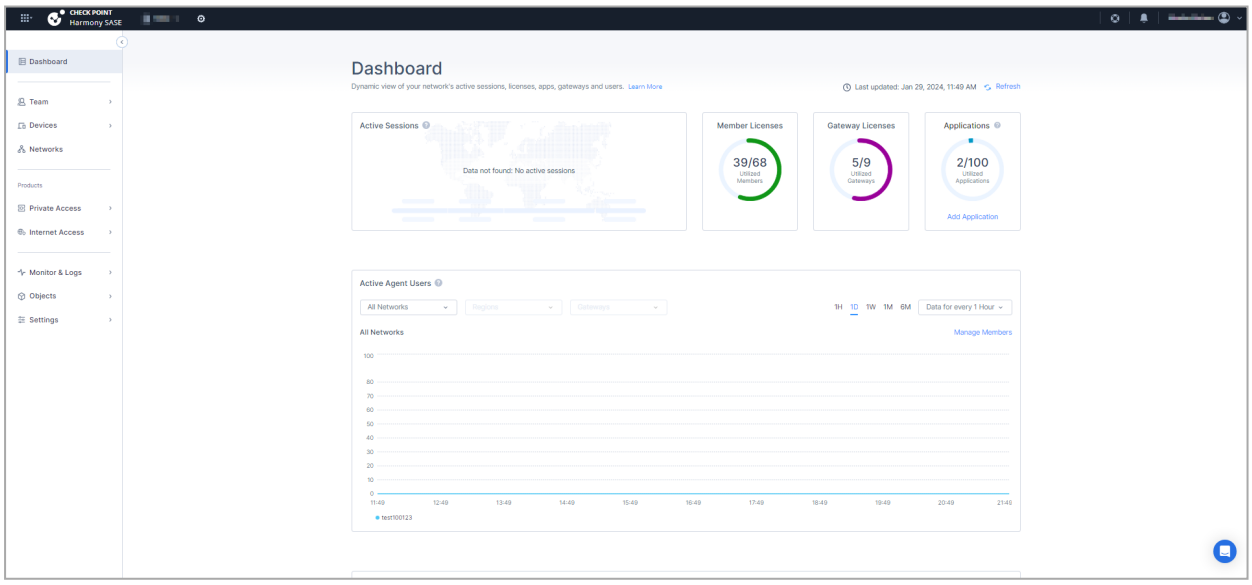
d. Character !*#%$

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.

Harmony SASE (Perimeter 81) Workspace

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.

Dashboard

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

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

Active Sessions

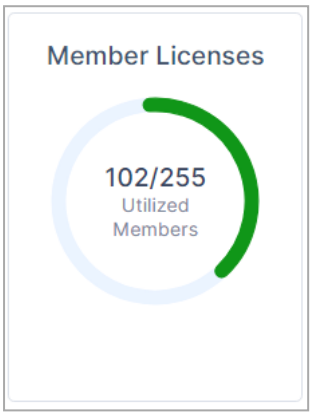
The **Active Sessions** widget shows:

- **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**.

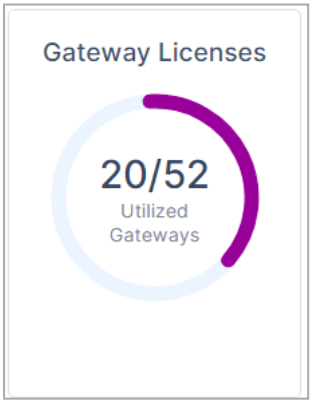
To view the detailed information, click **Expand**. The system redirects to the *"Active Sessions" on page 672* page.

Member Licenses



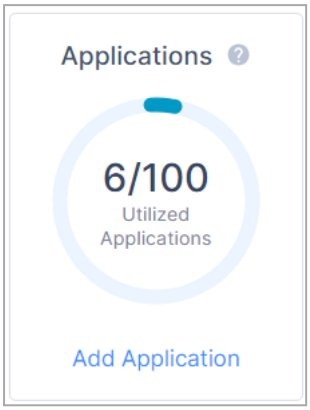
The **Member Licenses** widget shows the number of member licenses utilized out of the purchased licenses.

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 609*.

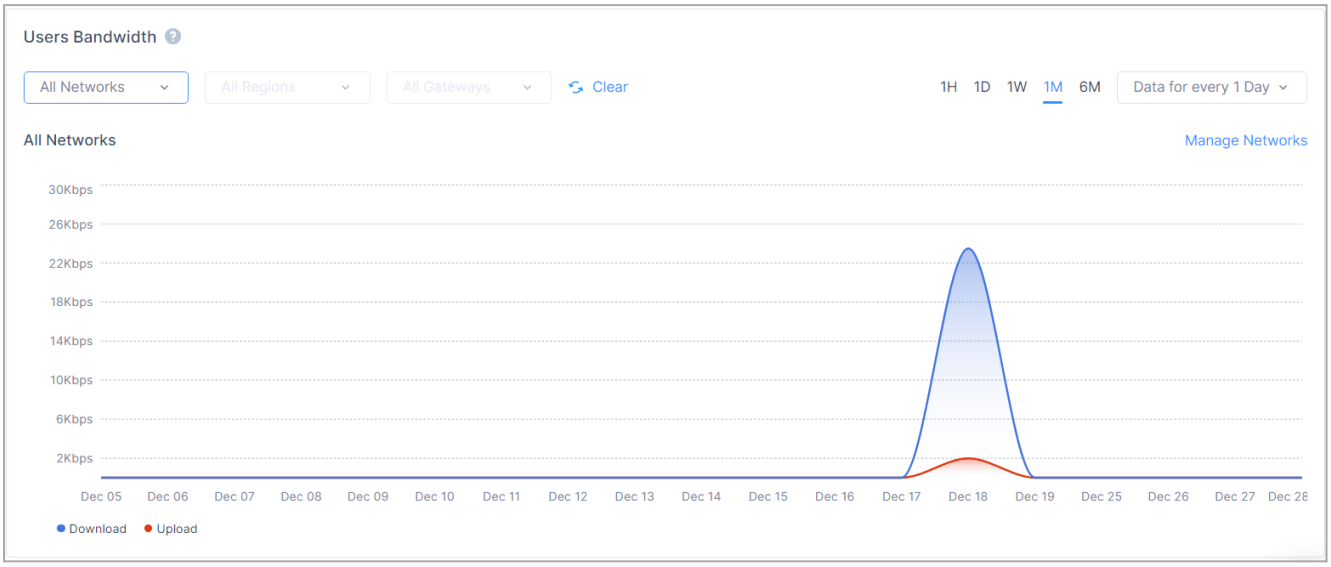
Active Agent Users

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

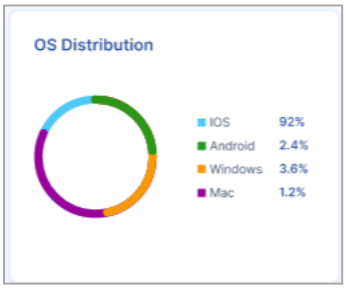


The **Users Bandwidth** widget shows the live and historical bandwidth used (upload and download) by members connected to the Harmony SASE Agent.

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

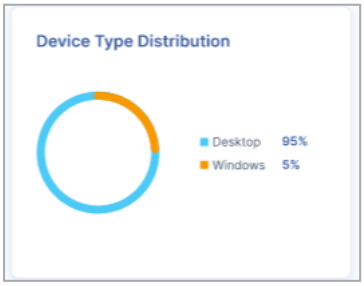
For a network and region, you can compare the data for up to three gateways.

OS Distribution



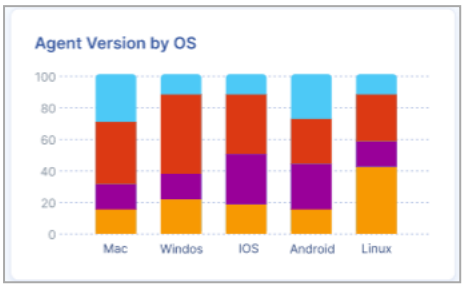
The **OS Distribution** widget shows the distribution of devices by operating systems.

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 50*
- *"Groups" on page 61*
- *"User Configuration Profiles" on page 64*

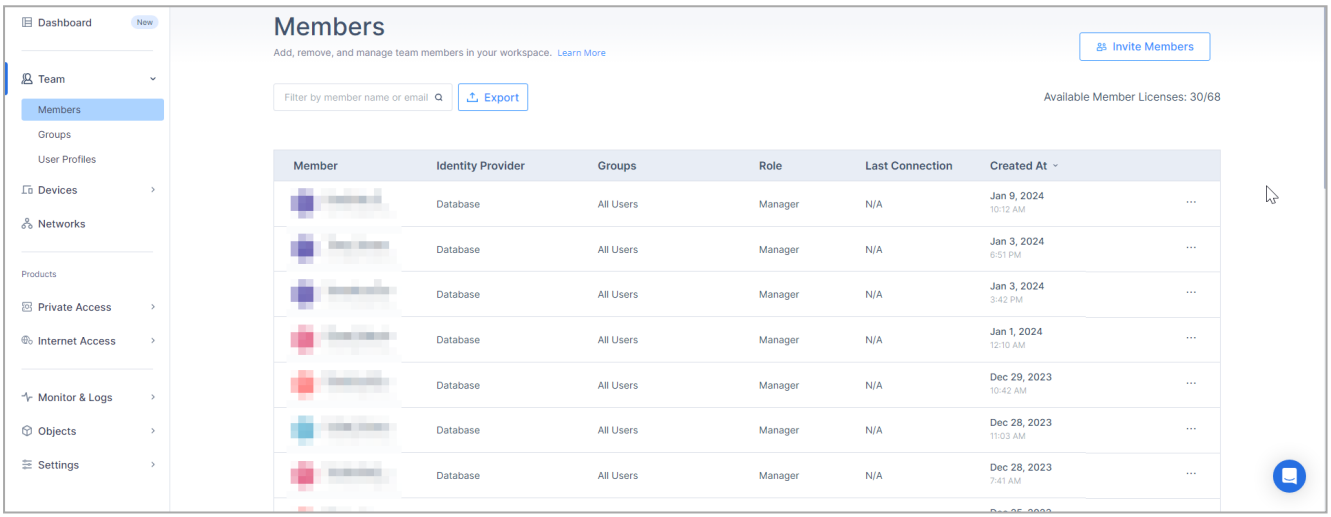
Members

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

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. **Database** means that the member is invited from the Harmony SASE Administrator Portal. See *"Invite Members" on page 52*.
Role	Role of the member: - **Admin** - Full privileges and permissions. - **Manager** - Manage networks, applications, members, groups, and monitor activity. - **User** - End-user that you want to provide safe private and internet access. For permissions associated with each role, see *"Member Roles and Permissions" on the next page*.
Groups	Group(s) to which the member is assigned.

Column	Description
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	⊖	✓	✓	✓	✓	⊖
User	⊖	⊖	⊖	⊖	⊖	⊖

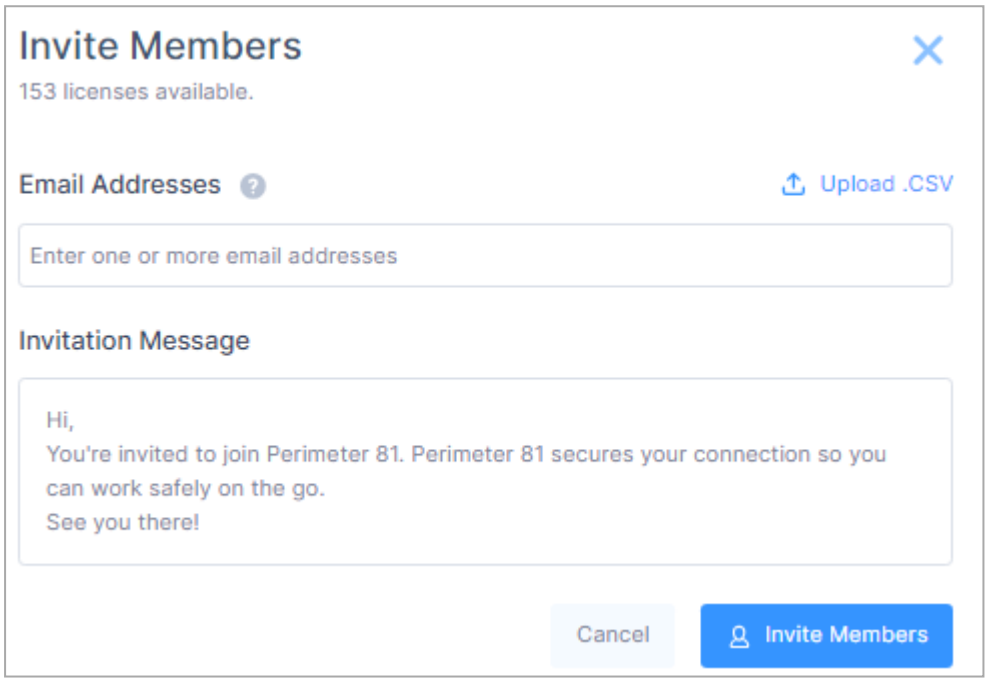
Invite Members

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 56*.

Inviting Members Using an Identity Provider

See *"Identity Providers" on page 727*.

Member Roles and Permissions

The predefined roles streamline administrative tasks by assigning specific permissions and restrictions to team members, ensuring operational efficiency and enhanced security.

Note - To change member role, see *"Managing Members" on page 56*.

Roles

- **Admin**
- **User Manager**
- **Network Manager**
- **Manager**
- **User**

Breakdown of Roles and Permissions

Role	Manage Licenses	Manage Members	Manage Networks	Manage Configuration	View Activities	Manage Billing
Admin	Yes	Yes	Yes	Yes	Yes	Yes
User Manager	No	Yes	No	No	No	No
Network Manager	No	No	Yes	No	No	No
Manager	No	Yes	Yes	Yes	Yes	Yes
User	No	No	No	No	No	No

Admin

The Admin role allows full access to configure system settings, manage users, and assign roles across the platform.

Permissions

- **User Management** - Full control over user roles and permissions.
- **Network Management** - Full access to network configurations, including creation and modification of networks.
- **Billing Management** - Access to billing information and subscription details.

- **System Configuration** - Modify system settings and integrations.
- **Activity Logs** - View all system activity logs.

User Manager

The User Manager role allows administrators to focus on managing members and device-related settings. This role is ideal for team members responsible for onboarding, monitoring, and managing user and device configurations.

Permissions

- **Access to Members and Devices interfaces**: Full visibility and control over user and device-related settings.
- **User Management**:
  - Invite and delete users.
  - Assign roles to users (except Admin and Billing roles).
- **Device Management**:
  - Configure device posture settings.
  - Manage user configuration profiles.
- **Activity Logs**: View logs related to Member Activity.

Restrictions

- No visibility or access to other administrative areas within the system.
- Cannot modify roles for Admin or Billing.
- Limited access strictly to member and device management.

Network Manager

The Network Manager role grants team members the ability to manage network configurations, including creating, updating, and deleting networks. This role is ideal for team members responsible for maintaining network infrastructure.

Permissions

- **Network Management**:
  - Access to all network management tools.
  - Create, modify, and delete networks, gateways, tunnels, and routes.
- **Activity Logs**: View logs associated with network activity.

Restrictions

- No access to other system management areas.
- Limited visibility especially to the network related configurations.

Manager

The Manager role allows managing network, member, and application configurations, with restricted access to billing and administrative functions.

Permissions

- **User Management** - Can manage user roles but cannot modify Admin or Billing roles.
- **Network Management** - Full access to manage network configurations.
- **System Configuration** - Modify application settings and user groupings.
- **Activity Logs** - View network and user activity logs.

Restrictions

- No access to Billing settings.
- Cannot assign or modify Admin roles.
- Limited access to administrative settings beyond network and member management.

User

The **User** role allows to access assigned Applications and the Downloads page.

Permissions

- **Use the System** - Access all the features necessary for their personal use of the platform.

Restrictions

- Cannot manage or configure other users, networks, or system settings.
- No visibility or access to other administrative areas within the system.
- No access to Billing settings or activity logs.
- Cannot modify roles for Admin or Billing.

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 72*.
6. To view the activity of a member, click the icon. The system redirects to the **Member Activity** page. See *"Member Activity" on page 673*.
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:

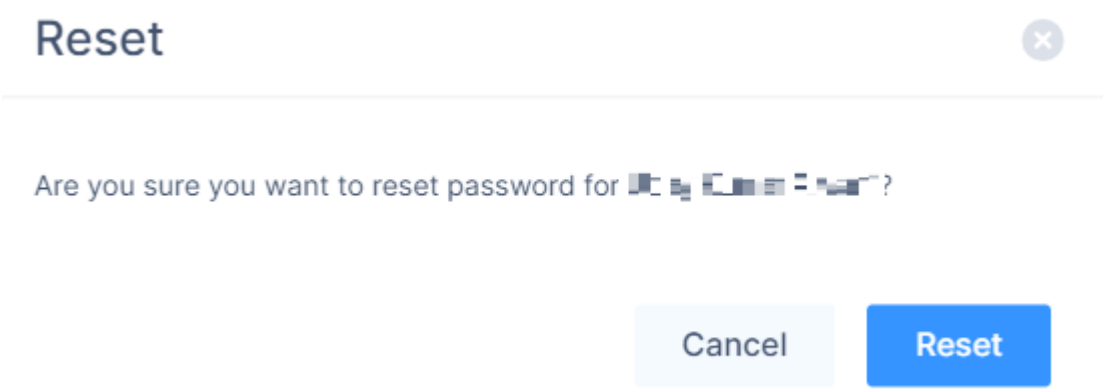
1. Access the Harmony SASE Administrator Portal.
2. Make sure *"Disable Sign-Out" on page 65* is enabled for the member or group.
3. Go to **Team** > **Members**.
4. Click the ··· icon in the last column for the member.
5. Click **Generate Sign-Out Code**.

   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.

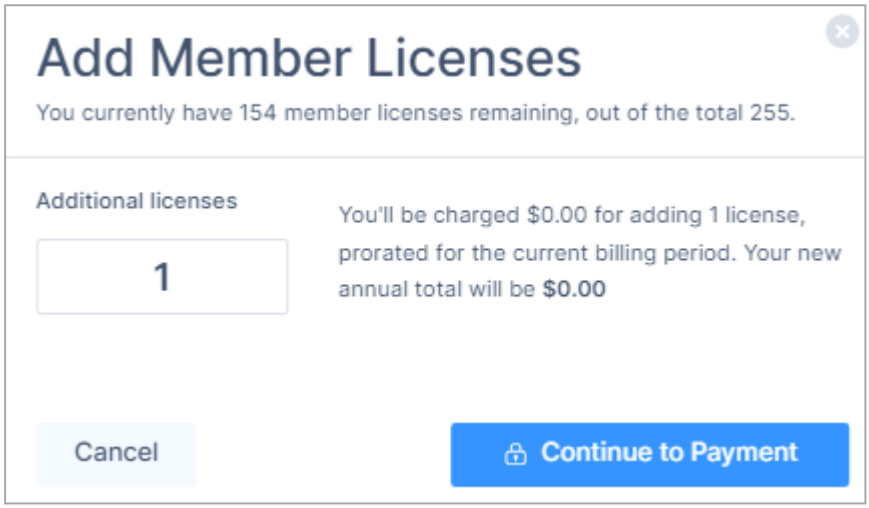
   The member receives a confirmation email for the Two-Factor Authentication reset and a link to re-activate it.

Adding Licenses

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

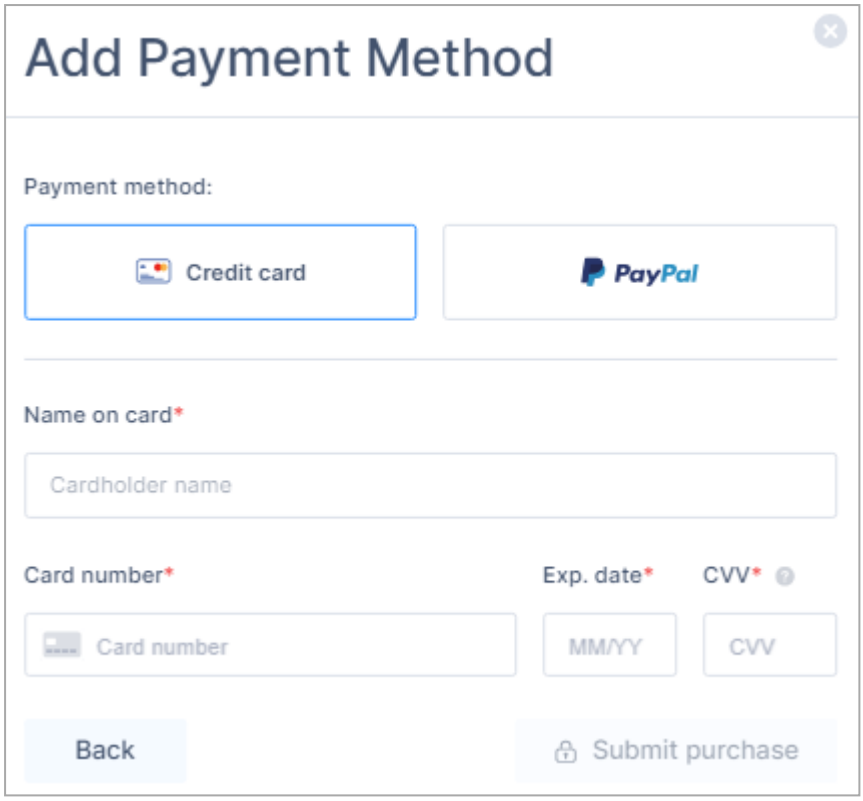
1. Access the Harmony SASE Administrator Portal and click **Team** > **Members**.
2. Click **Add Licenses**.

   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.



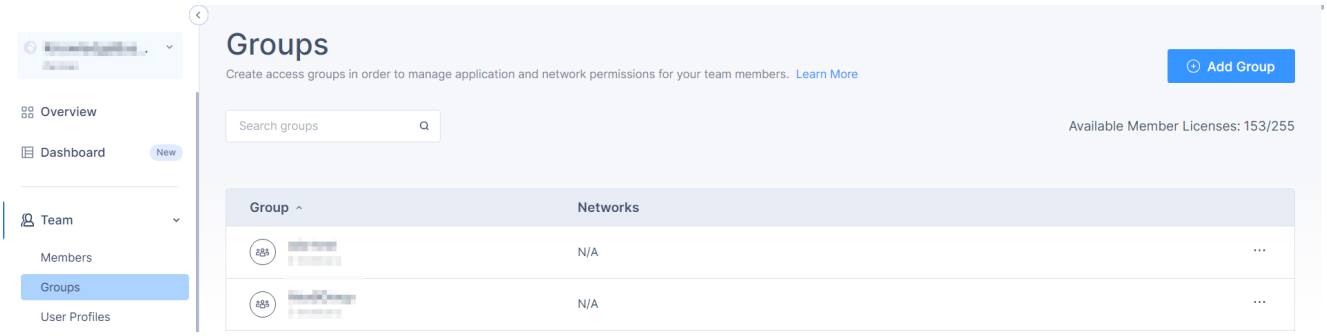
5. Enter the payment details and click **Submit purchase**.

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 642* 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**.



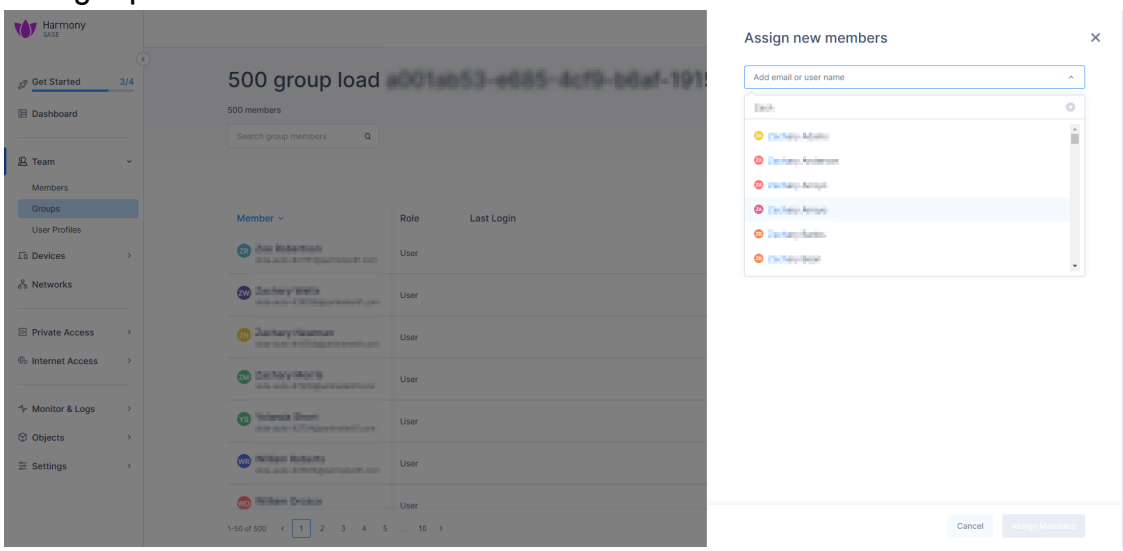
Column	Description
Group	Group name.
Networks	Name of the networks assigned to the group.

Creating a Group

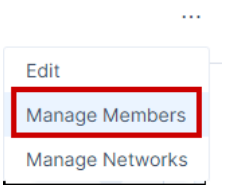
1. Access the Harmony SASE Administrator Portal and click **Team** > **Groups**.
2. Click **Add Group**.

   The **Create new group** window appears.

Note - You can search and select users in the **Assign new members** section in the right-pane.

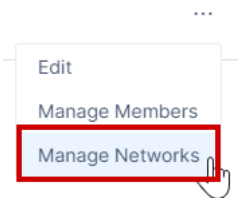


3. Enter the group name and click **Create Group**.
4. To add members to the group:
   a. Click the ··· icon in the last column of the group and then select **Manage Members**.



   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**.

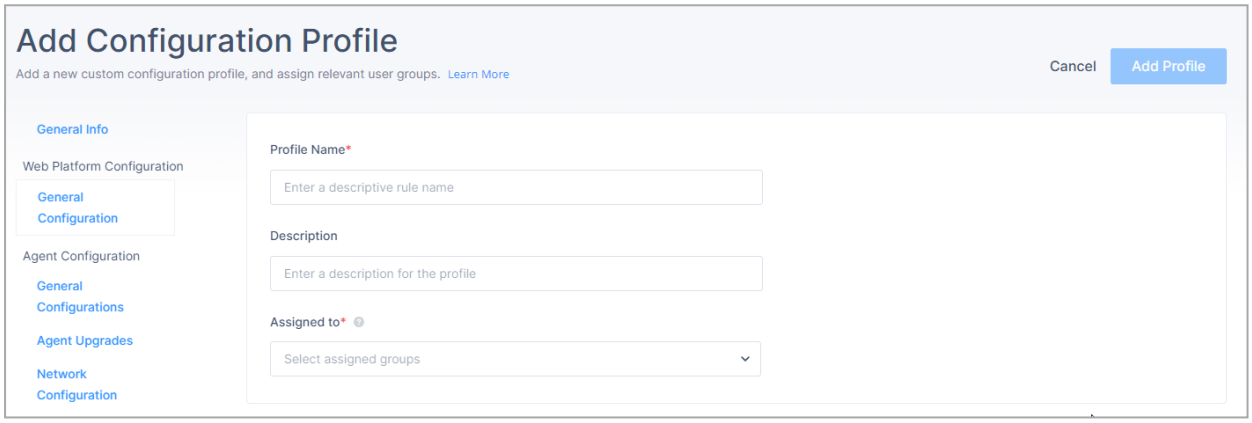
The members can access only the selected networks from the Harmony SASE Agent.

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.



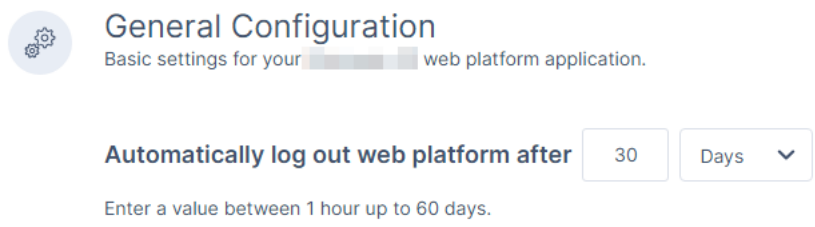
4. (Optional) In the **Description** field, enter a description for the profile.
5. In the **Assigned to** field, select the member groups.
6. Configure *"Web Platform Configuration" below* and *"Agent Configuration" on the next page*.
7. Click **Add Profile**.

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. 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 56*.
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. For more information about shared networks, see *" [DEPRECATED] Shared Gateways " on page 113*.

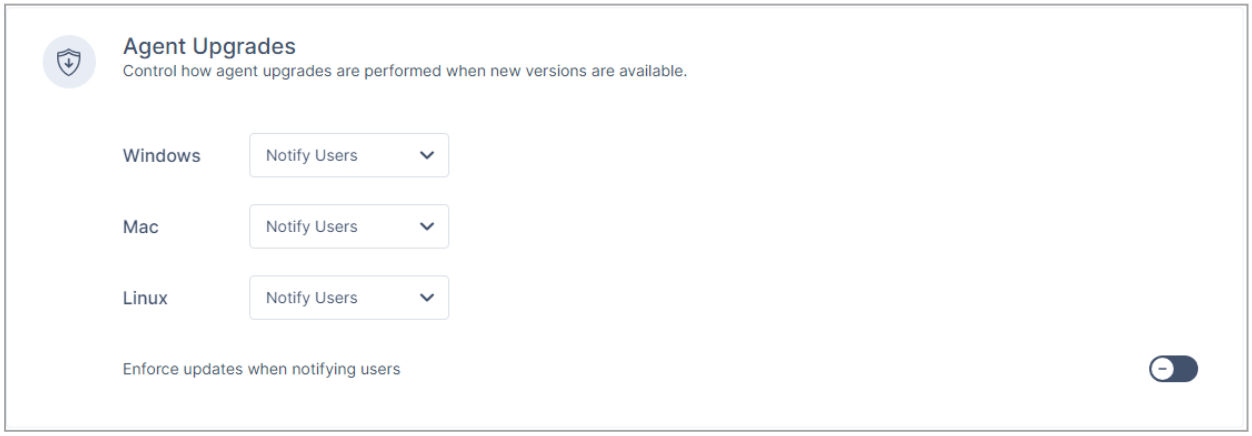
Setting	Description
Connect on Launch	Automatically starts the Harmony SASE Agent when the device starts and connects to the most recent network location. **Notes**: ▪ This setting applies only to Windows and macOS devices. ▪ The member can modify this setting from their device.
Connect / Disconnect Notification	Shows a pop-up notification on the device when the Harmony SASE Agent connection status changes. **Notes**: ▪ This setting applies only to Windows and macOS devices. ▪ 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 64*.
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. **To add trusted routers:** 1. Click **Add Trusted Router**. 2. In the **Name** field, enter the router name. 3. In the **Router MAC Address** field, enter the router MAC address. 4. Click **Add**. 5. To add multiple routers, repeat steps 1 to 4. 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. **To add trusted Wi-Fi network:** 1. Click **Add Wi-Fi Network**. 2. In the **Name** field, enter the SSID of the network. 3. Click **Add**. 4. To add multiple trusted Wi-Fi networks, repeat steps 1 to 3. 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.

Trusted Environment

Devices

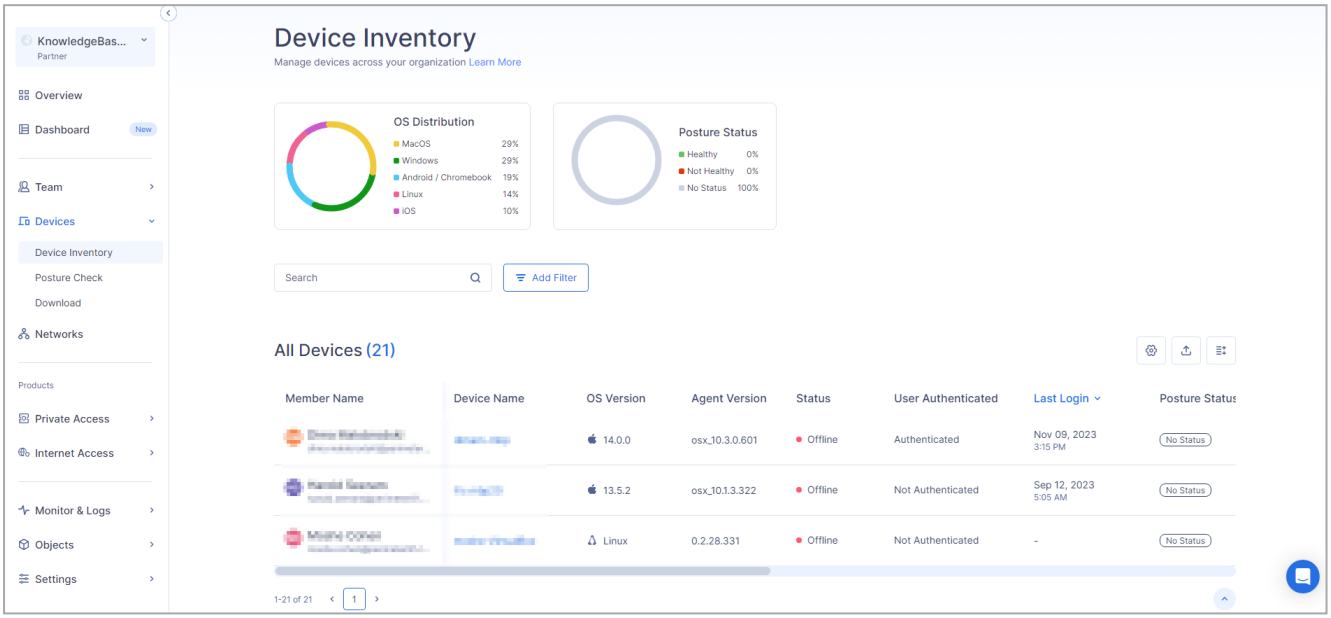
In the **Devices** page, you can:

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

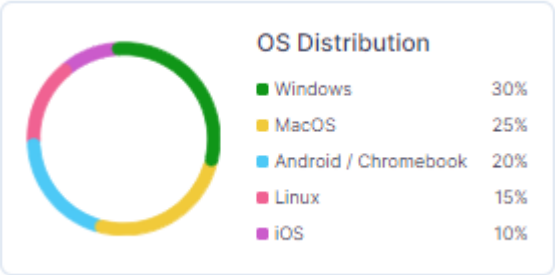
Device Inventory

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

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

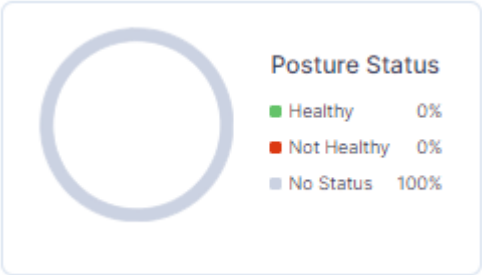


OS Distribution



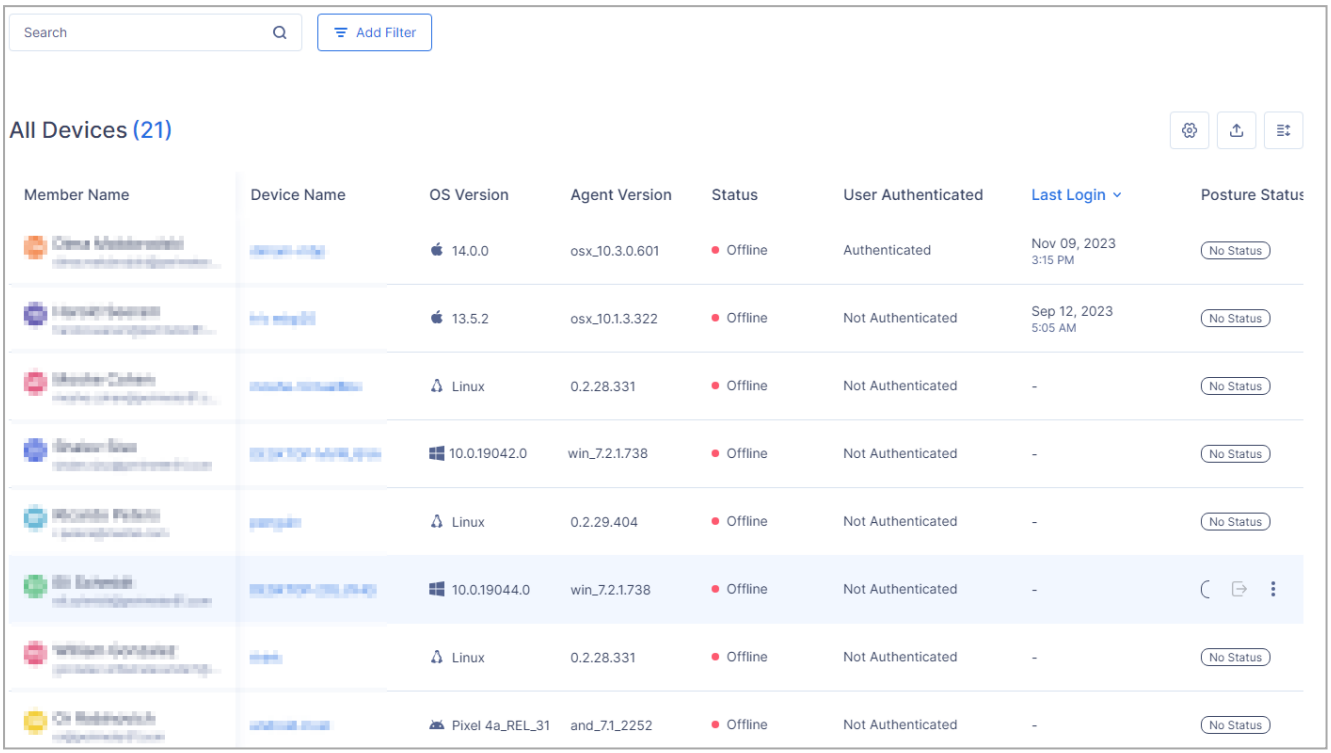
The **OS Distribution** widget shows the distribution of operating systems across devices by percentage.

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. ▪ **Online** - Agent is running and the user is signed in but not connected to the VPN. ▪ **Offline** - Device is turned off or not connected to the internet. ▪ **Connected** - Agent is connected to the VPN.
User Authenticated	User authentication status. ▪ **Authenticated** - User has signed in to the agent with valid credentials. ▪ **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. ▪ **Healthy** - Device is compliant with the DPC policy. ▪ **Not Healthy** - Device is not compliant with the DPC policy. ▪ **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. ▪ Desktop ▪ 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

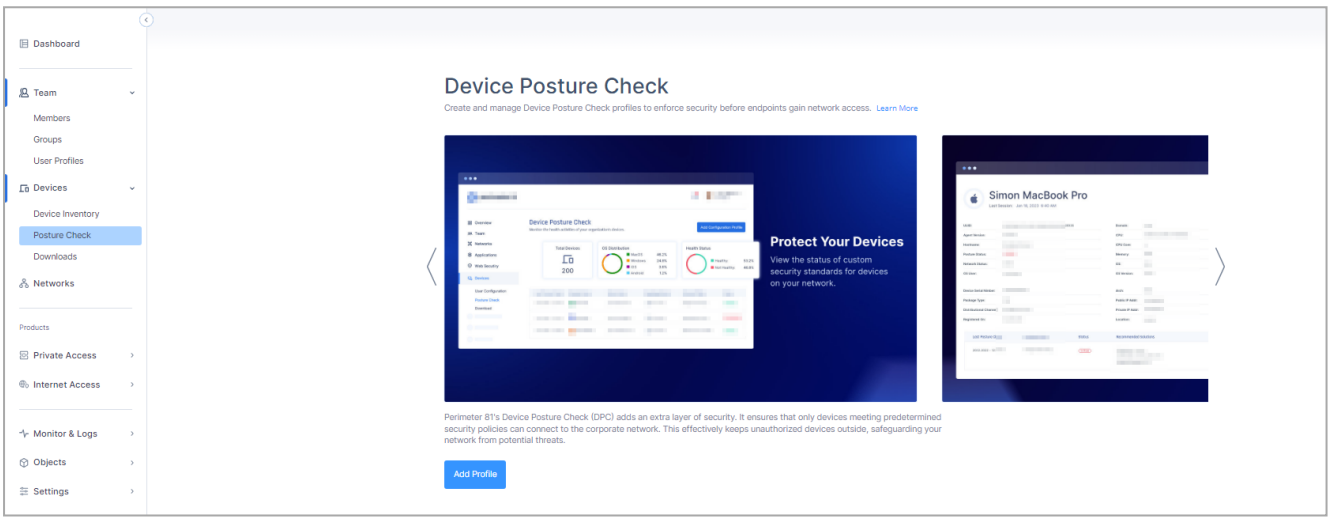
1. For the device you want to remove, scroll to the end of the row and click ⋮.
2. Go to **Actions** and click **Remove Device**.

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

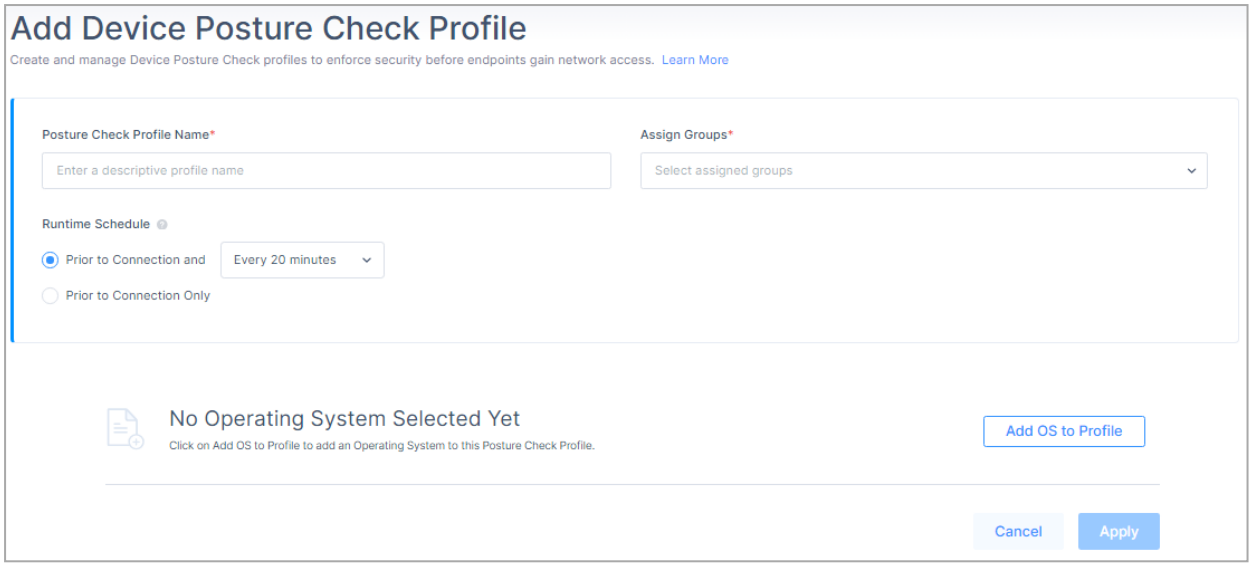
* The supported Anti-Virus software are:

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

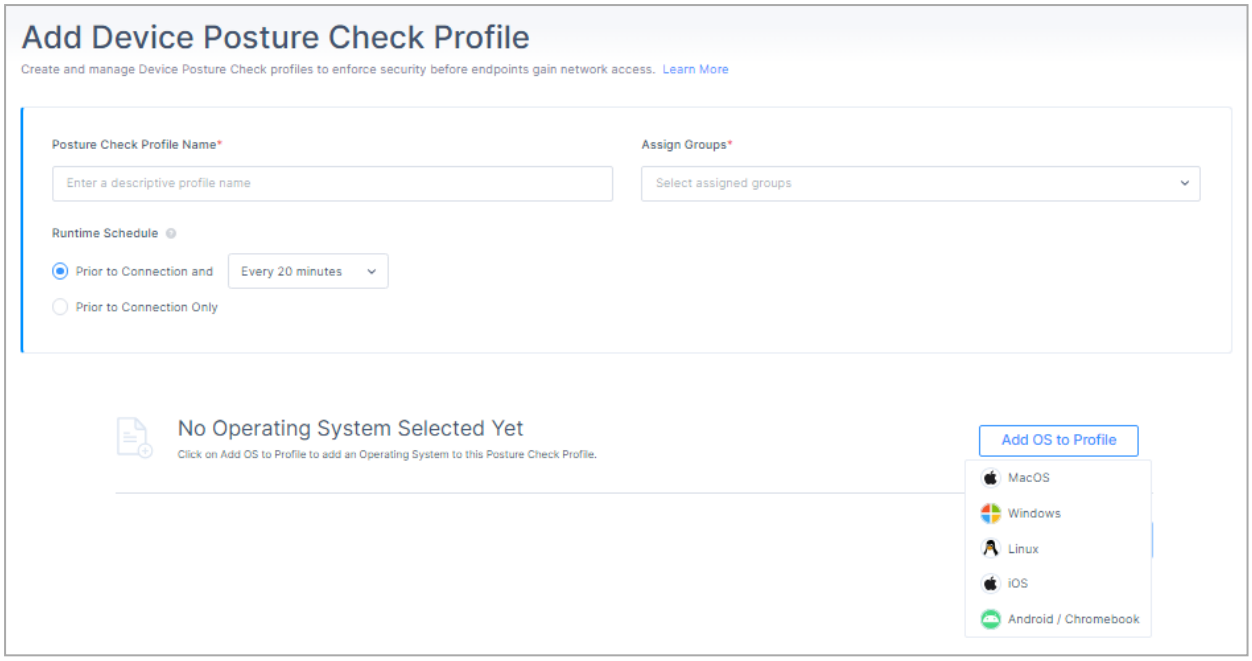
Specifying the Device Posture Check Requirements

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

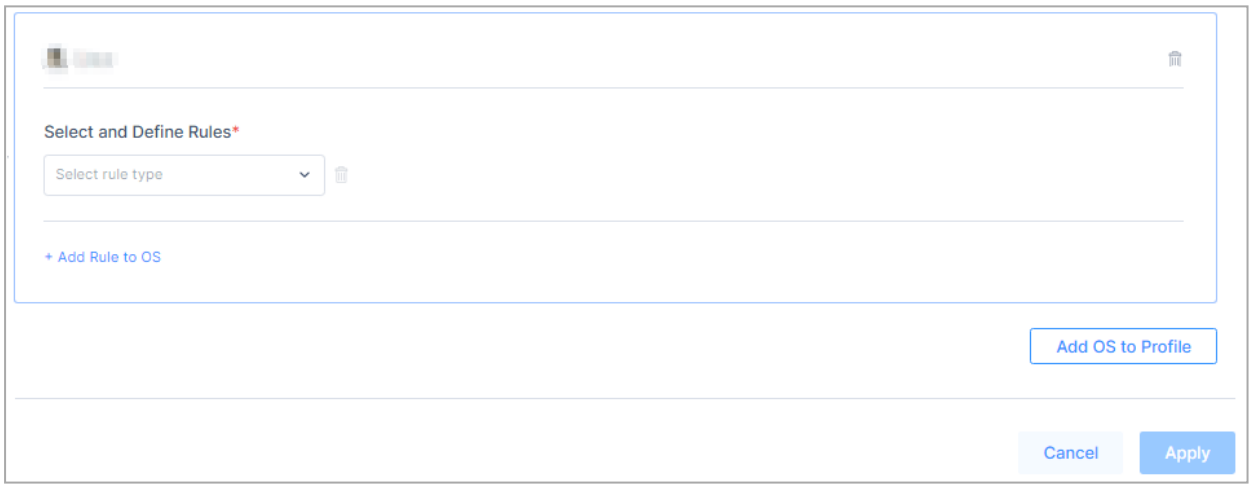
   The **Add Device Posture Check Profile** window appears.



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:

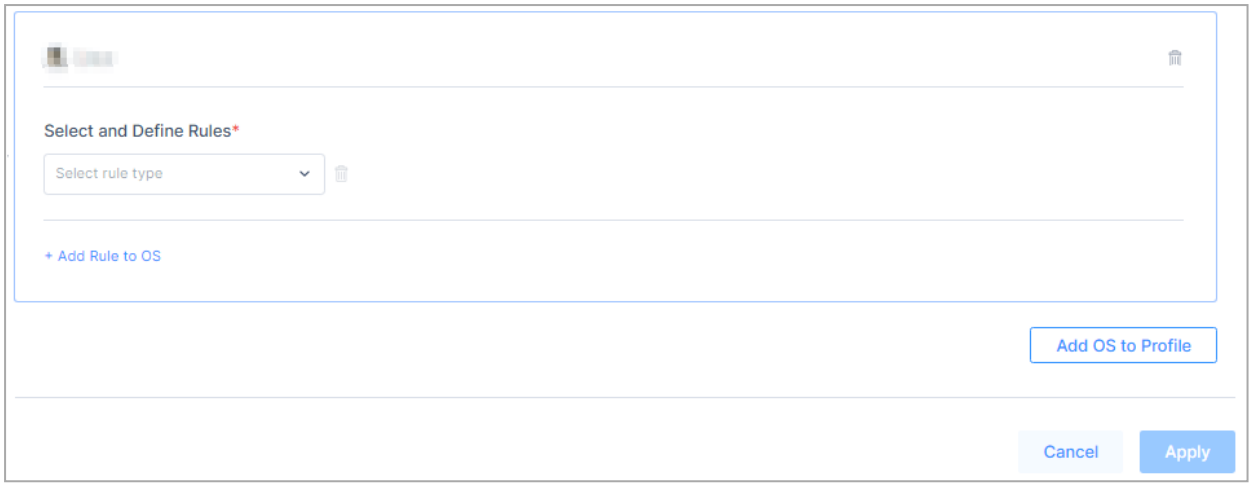


Posture Check Requirement	Description	Action
Anti-virus	Verifies if the specified Anti-Virus is installed, up-to-date and running.	Select the Anti-Virus software products from the list.
File Exists	Verifies if certain file exist or do not exist (banned) in the specified path.	Enter the path with forward 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`. 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`). ▪ (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: ▪ **Antivirus** ▪ **Firewall** ▪ **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: ▪ To allow mobile devices to access networks, select **Allow**. ▪ To block mobile devices from accessing networks, select **Deny**. ▪ 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.



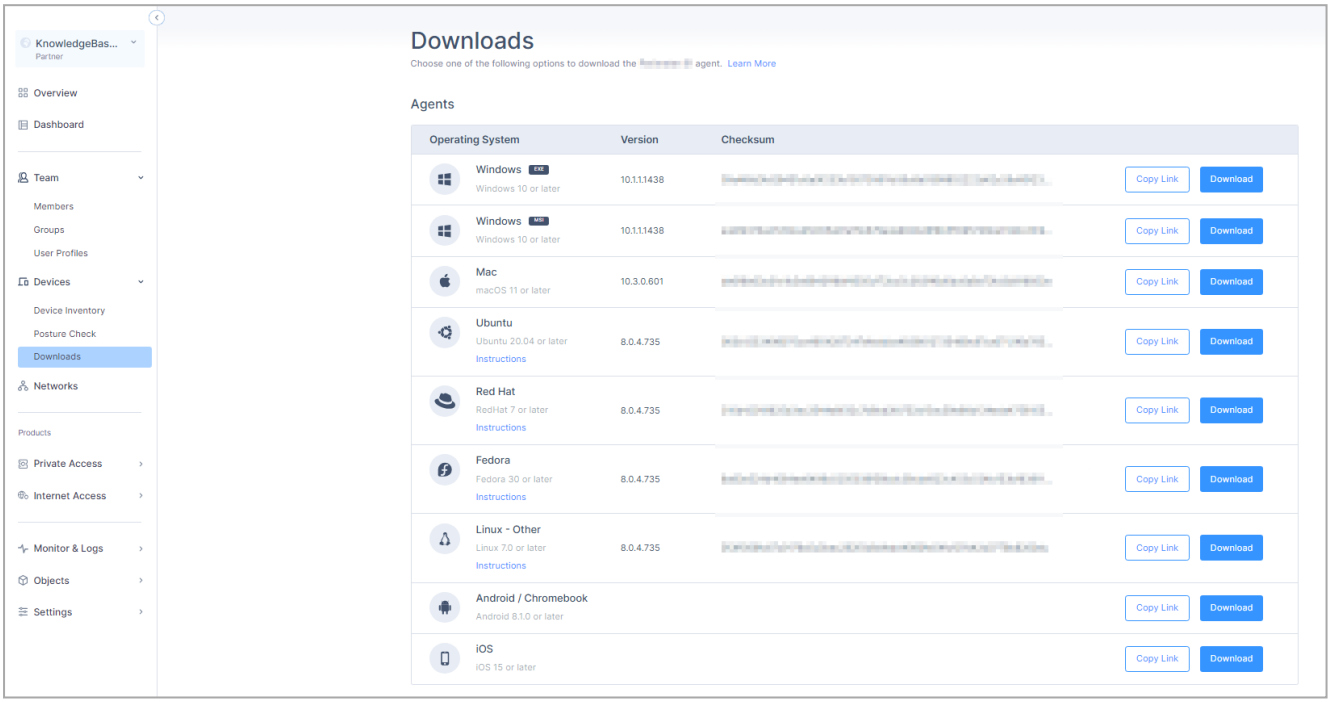
10. Click **Apply**.

    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 13 or later	Downloads a PKG file.
Ubuntu	Ubuntu 20.04 or later	Downloads a Deb file.
Red Hat	RedHat 8 or later	Downloads a RPM file.
Fedora	Fedora 40 or later	Downloads a RPM (Fedora) file.
Linux - Others	Linux 8.0 or later	Downloads a tar.xz file.
Android / Chromebook[1]	Android 12.1 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 94*.

- 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 87*.

Certificates

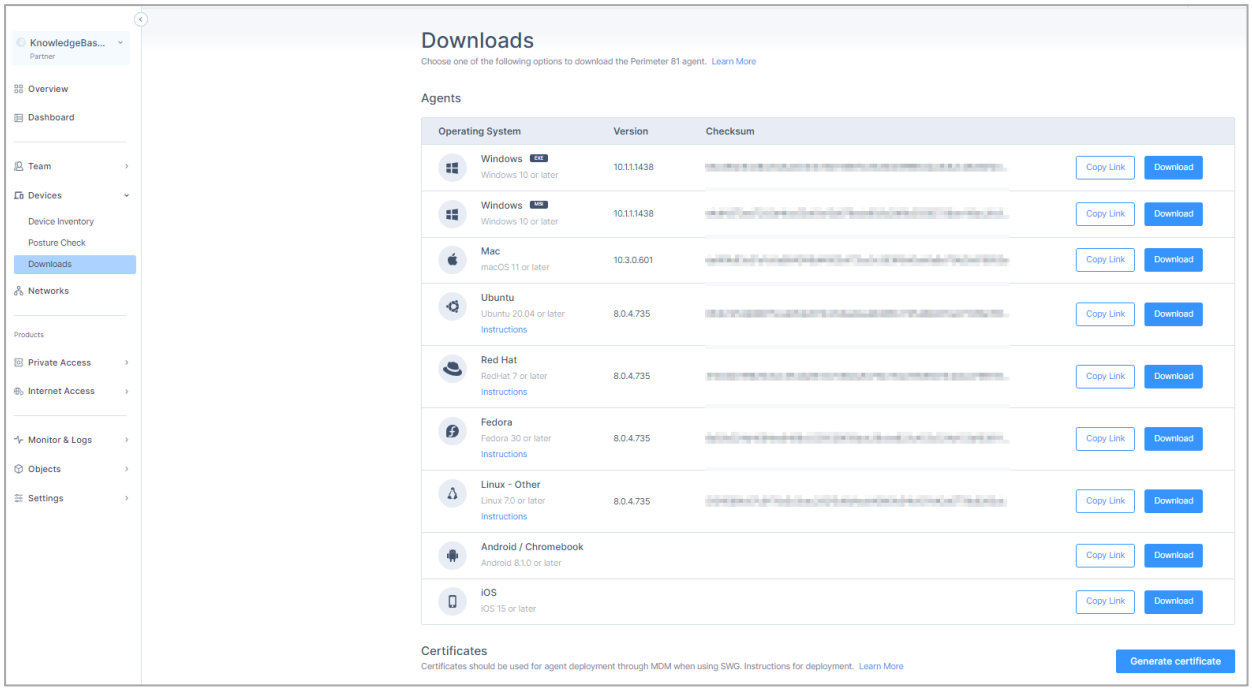
You can download Secure Web Gateway (SWG) root certificate and install it on macOS devices either manually or using an MDM application. The SWG root certificate is required for Internet Access.

Notes:

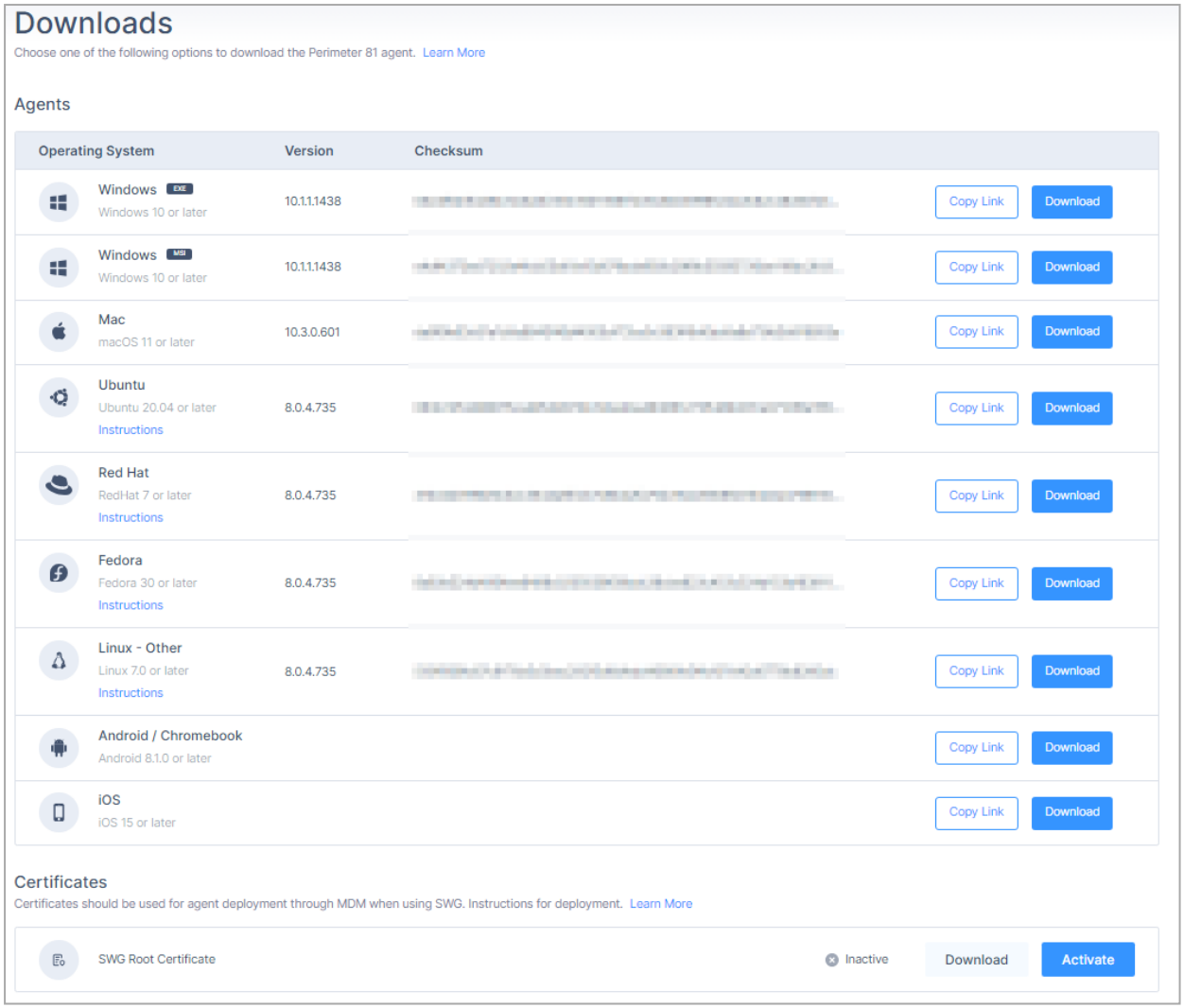
- It is supported only with the macOS Harmony SASE Agent version 10.4 and higher.
- The **Revoke** button is disabled. It will be supported in the future.

To download the SWG root certificate:

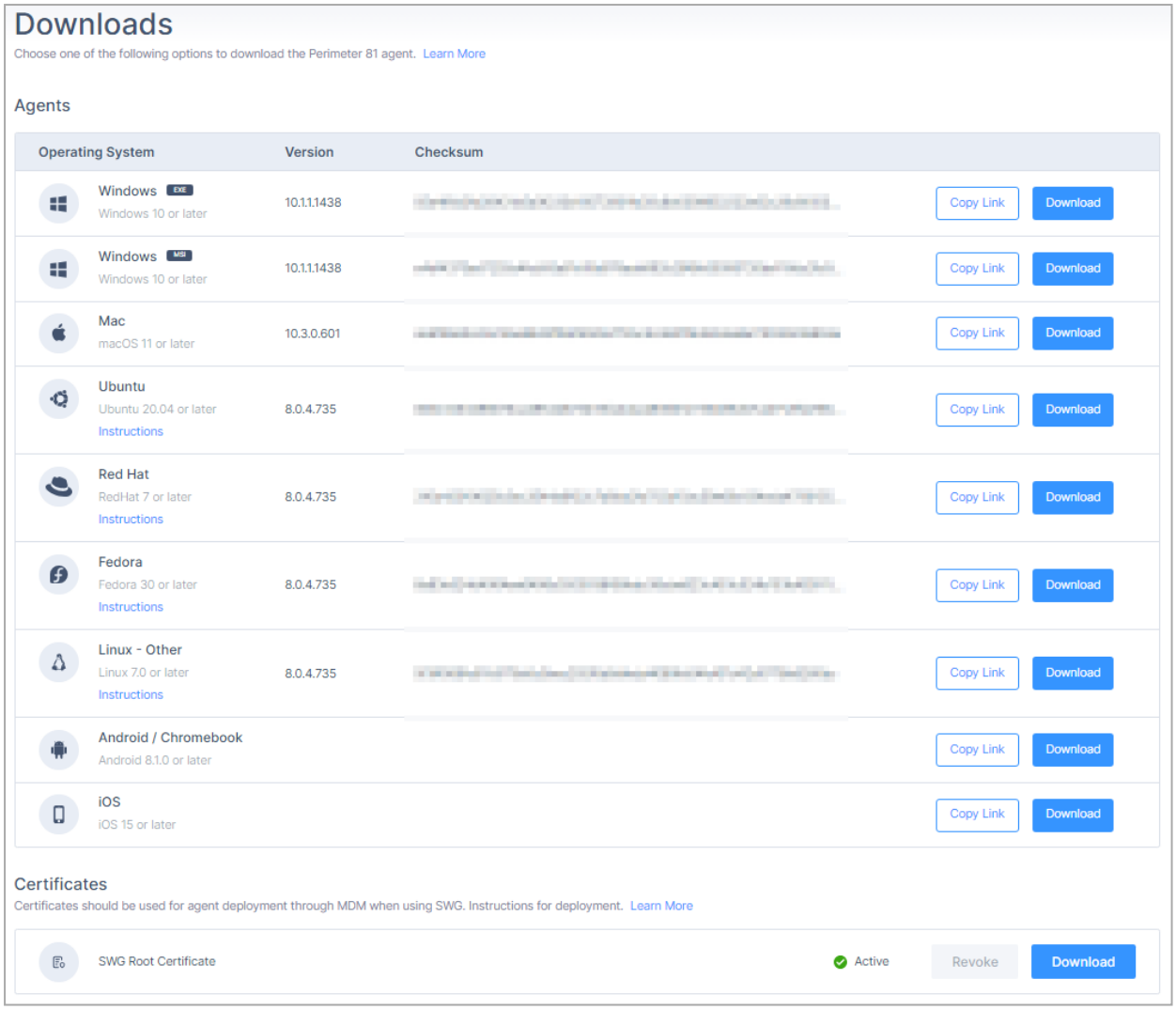
1. Access the Harmony SASE Administrator Portal and click **Devices** > **Downloads**.



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 52*

  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 / Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
Silent Installation	`msiexec /quiet /i Harmony_SASE_x.x.x.xxx.msi` To know the installation status after the silent installation, run: 1. `start /wait msiexec /quiet /i "Harmony_SASE_x.x.x.xxx.msi"` 2. `echo %errorlevel%`	`msiexec /quiet /i Perimeter81_x.x.x.xxx.msi` To know the installation status after the silent installation, run: 1. `start /wait msiexec /quiet /i "Perimeter81_x.x.x.xxx.msi"` 2. `echo %errorlevel%`	▪ **For version 11.0.10 and above**: `$ sudo installer -pkg Harmony_SASE_x.x.x.xxx.pkg -target /` ▪ **For legacy versions (up to 11.0.10)**: `$ sudo installer -pkg Perimeter81_x.x.x.xxx.pkg -target /` To change the agent permissions after the installation, run: 1. `$ sudo chown -R $(stat -f%Su /dev/console) "/Applications/Perimeter 81.app"`	

Operating System / Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):
			2. `$ chmod -R u=rwx "/Applications/Perimeter 81.app"`	

Pre-populating the tenant or workspace name	`msiexec /i "Harmony_SASE_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name"`	`msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name"`	`$ sudo defaults write com.perimeter81d workspace workspace_name`
			To remove pre-populated workspace/tenant name, run:
			`$ sudo defaults delete com.perimeter81d workspace`
			This is supported only with agent version 8.0.4.116 and higher.
				To pre-populae the workspace name, run:
				`/opt/Perimeter81/perimeter81 ctl set-prepopulate-tenant-id workspace_name`
				Replace "`workspace_name`" with your actual workspace

Pre-populating the data residency region	`msiexec /i "Harmony_SASE_x.x.x.xxx.msi" /quiet REGION="EU or US"` For `REGION`, add `"EU"` for Europe and `"US"` for America.	`msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet REGION="EU or US"` For `REGION`, add `"EU"` for Europe and `"US"` for America.	`$ sudo defaults write com.perimeter81d region "EU or US"` For `region`, add `"EU"` for Europe and `"US"` for America.	

Operating System Command for	Windows (.msi installation flags for versions 11.0 and above):	Windows (.msi installation flags for legacy versions (up to 11.0):	macOS	Linux (installation flags):

Pre-populating the tenant or workspace name and data residency region	`msiexec /i "Harmony_SASE_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name" REGION="EU or US"`
	For `REGION`, add `"EU"` for Europe and `"US"` for America.
		`msiexec /i "Perimeter81_x.x.x.xxx.msi" /quiet WORKSPACE="workspace_name" REGION="EU or US"`
		For `REGION`, add `"EU"` for Europe and `"US"` for America.
			To pre-populating the tenant or workspace name, run:
			`$ sudo defaults write com.perimeter81 d workspace workspace_name`
			To pre-populating the data residency region, run:
			`$ sudo defaults write com.perimeter81 d region "EU or US"`
			For `region`, add `"EU"` for Europe and `"US"` for America.	

Uninstallation	`msiexec /x "Harmony_SASE_x.x.x.xxx.msi"`	`msiexec /x "Perimeter81_x.x.x.xxx.msi"`	Run the uninstall script.	

MDM Deployment of the Harmony SASE MacOS Agent with Internet Security

The Harmony SASE system includes **Web Security** features. When Internet Security is enabled on the workspace, the system deploys a locally installed extension, content filter, and certificate to perform SSL decryption. These components are typically installed post-login, requiring user approval. Administrators can pre-deploy these configurations to eliminate the need for user approval and prevent potential misconfigurations of web security components.

Deploying the Agent through MDM

Downloading the Certificate

1. For information on how to download the certificate, see Downloads.
2. Once the certificate is downloaded, add it to the deployment through MDM.

Deploying the Content Filter and System Extension

- Download the .mobileconfig file and certificate for deployment through MDM:

  Harmony SASE.mobileconfig

- Alternatively, a Workspace Administrator can manually configure the Content Filter and System Extension for deployment through MDM.

  Note - Each vendor may assign different names to these values.

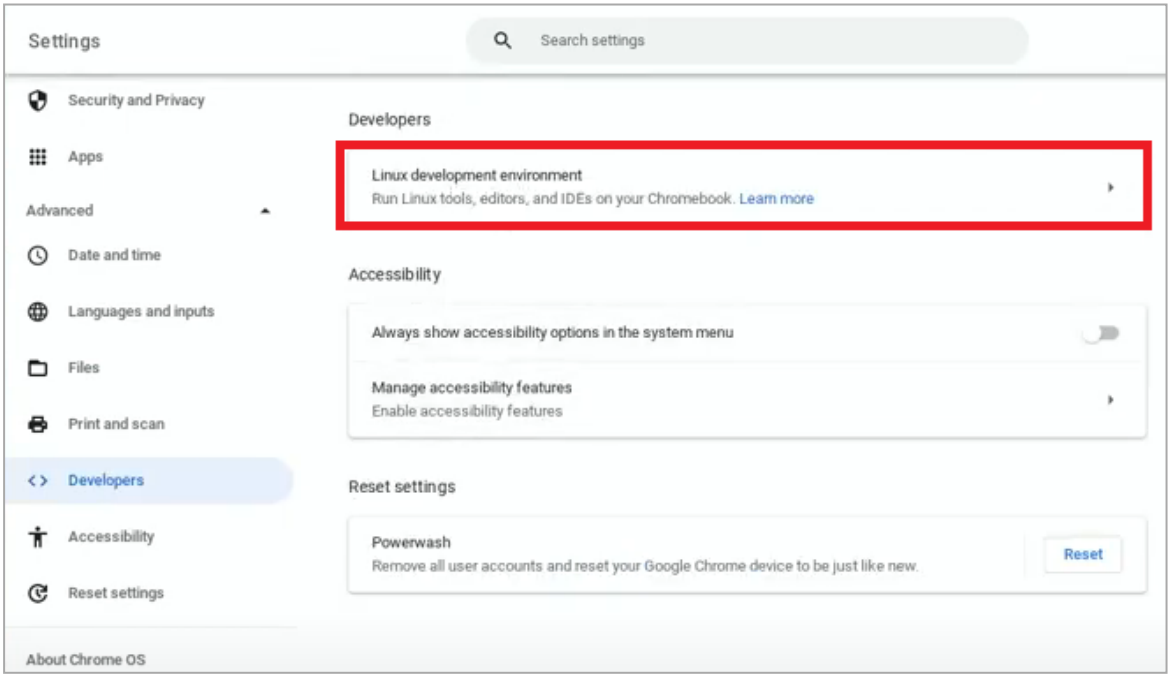
  - Deploy a **Content Filter**:
    - **Filter Type**: Plug-in
    - **Connection Name**: Harmony SASE
    - **Identifier**: com.safervpn.osx.smb
    - **Filter Webkit traffic**: Yes
    - **Filter Socket Traffic**: Yes
    - **Socket Filter Bundle ID**: com.safervpn.osx.smb
    - **Socket Requirement**: identifier "com.safervpn.osx.smb" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = "924635PD62"
    - **Filter Network Pockets**: Yes
    - **Pocket Bundle ID**: com.safervpn.osx.smb
    - **Packet Requirement**: identifier "com.safervpn.osx.smb" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = "924635PD62"
    - **Filter Grade**: Firewall

- Deploy a **System Extension**:
  - Navigate to where you add the VPN Payload Profiles and add a **MacOS** profile and context **Device Profile**.
  - **Allow User Overrides**: Yes
  - **Allowed System Extension Types**: Network
  - **Team ID**: 924635PD62
  - **Bundle Identifier**: com.safervpn.osx.smb.proxy

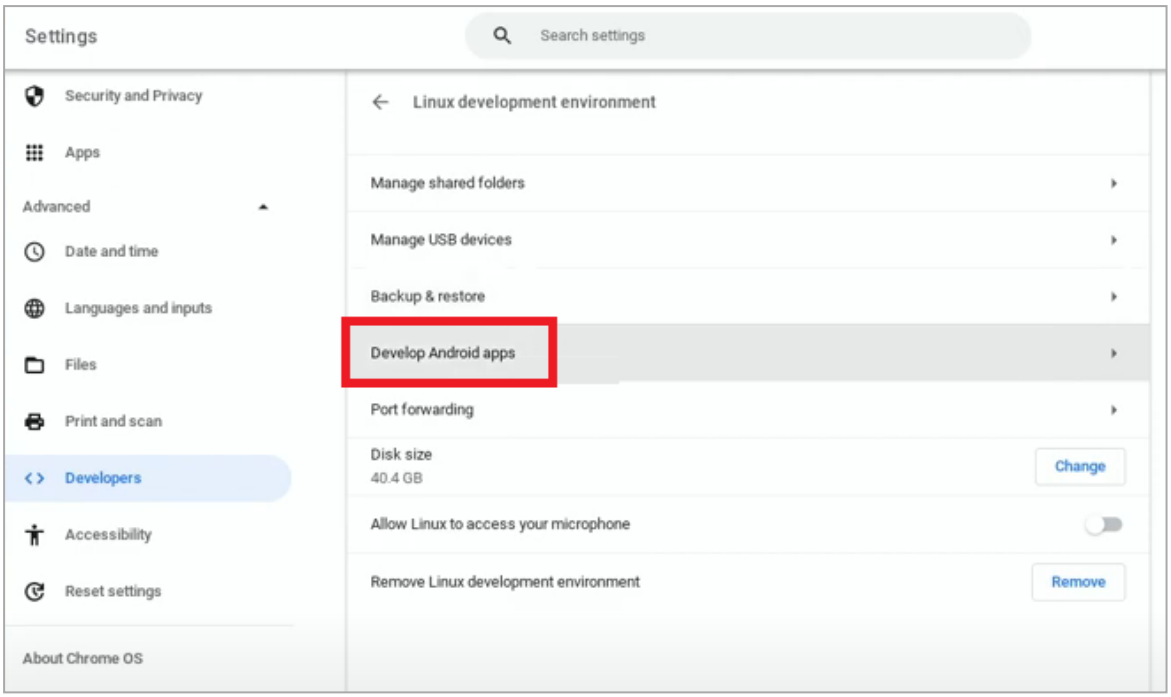
Installing Harmony SASE on Chromebook

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.

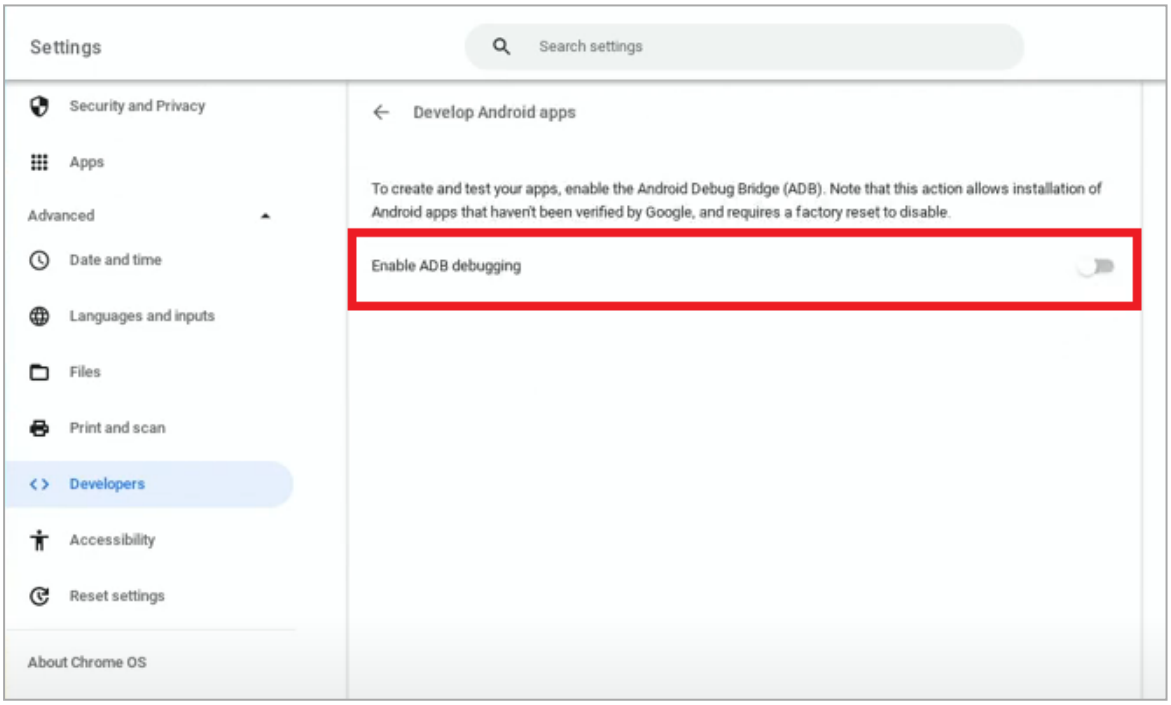
   The **Developer Mode** is enabled.
3. To enable **ADB debugging**:
   a. Go to **Settings** > **Advanced** > **Developers**.



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:

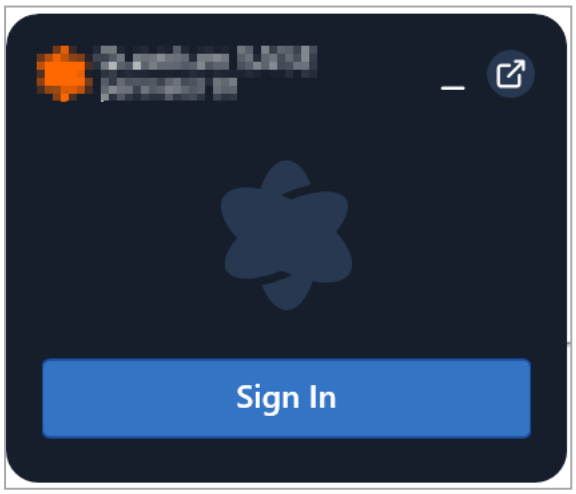
   ```
   df -h /boot/
   ```
9. Navigate to the file system `cd /dev/hda1` should be the default folder where the API file is located at.
10. To install Harmony SASE Agent, run:

    ```
    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**.

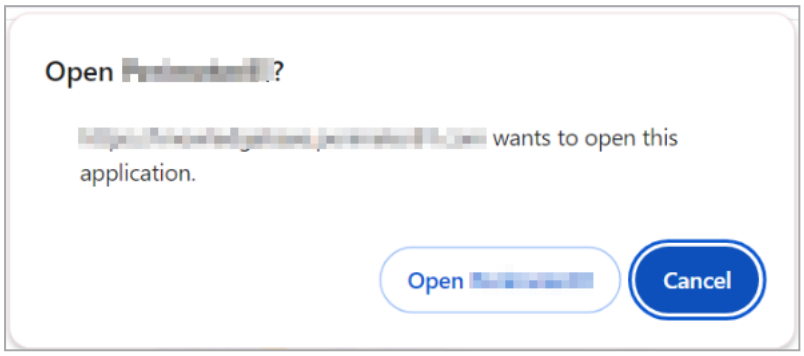
   

   The system opens a web browser for authentication.
3. In the **Workspace URL** field, enter the workspace URL and click **Continue**.
4. Enter your credentials and click **Sign In**.

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

A prompt appears.

5. Click **Open Harmony SASE**.

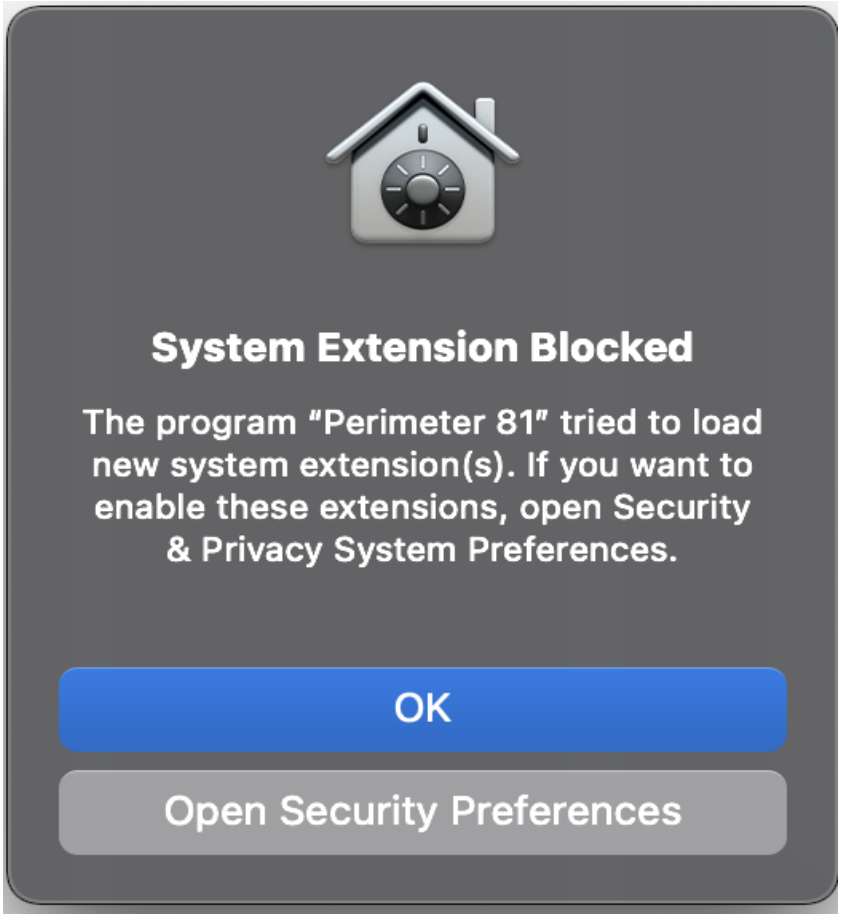


The Harmony SASE Agent opens and automatically connects to a **Network**.

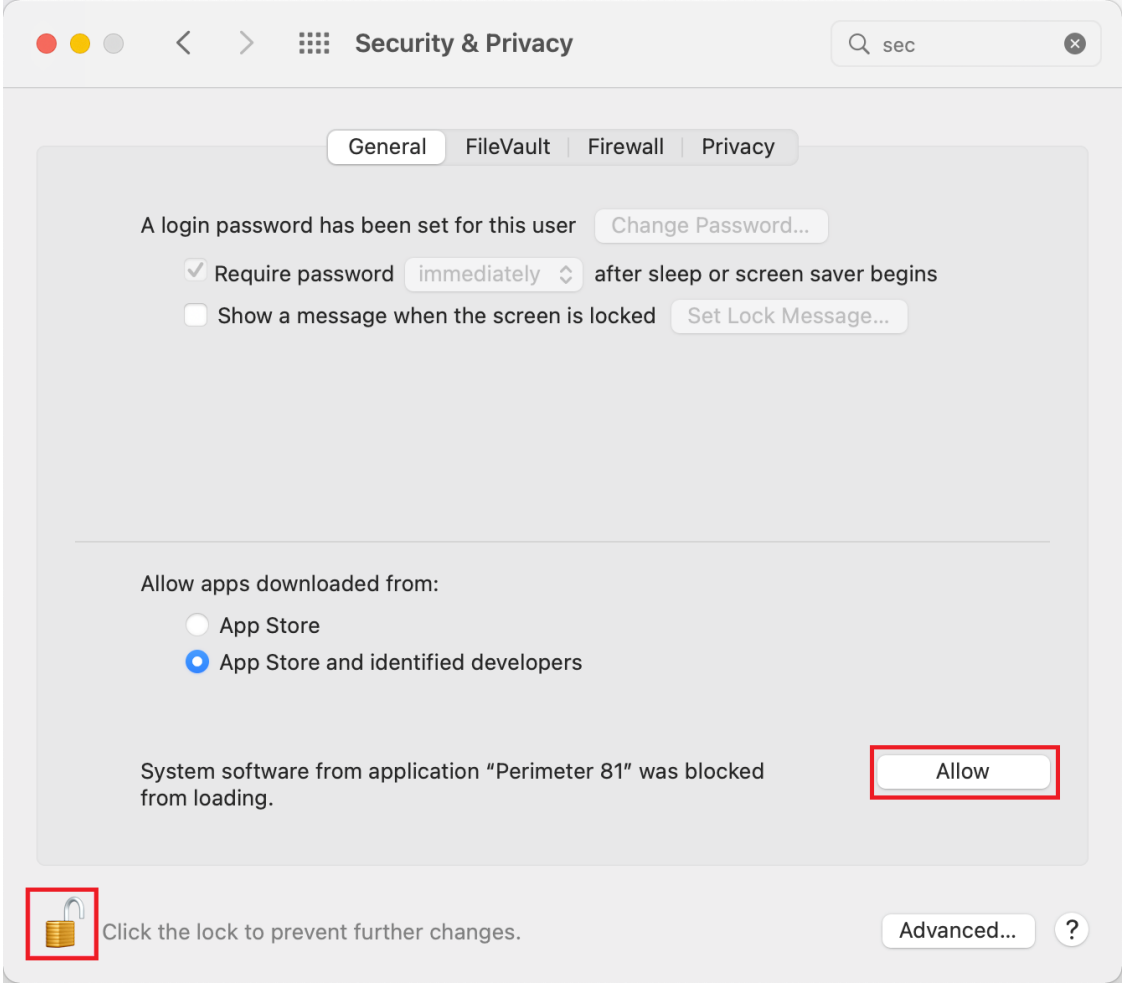
6. For macOS devices, if internet access is enabled, then do these (otherwise, skip the step):

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

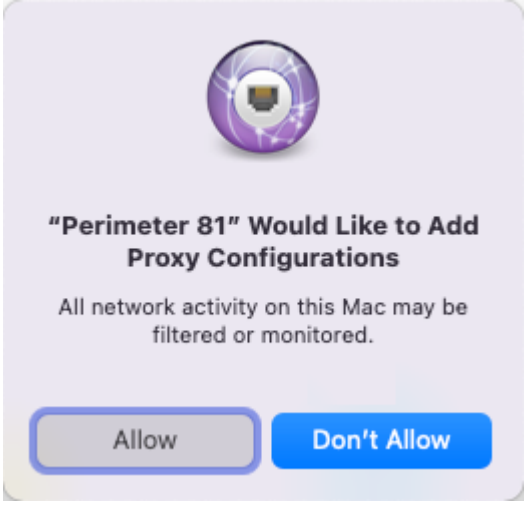
a. Click **Open Security Preferences**.



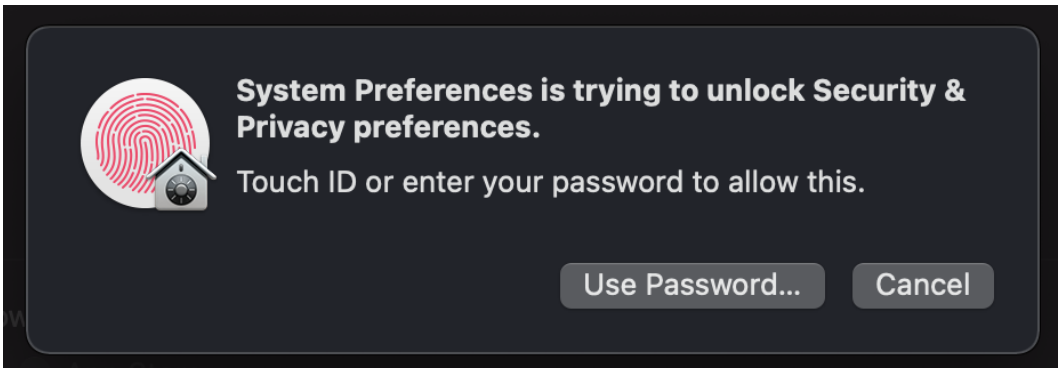
b. Click the lock icon at the bottom left and click **Allow**.



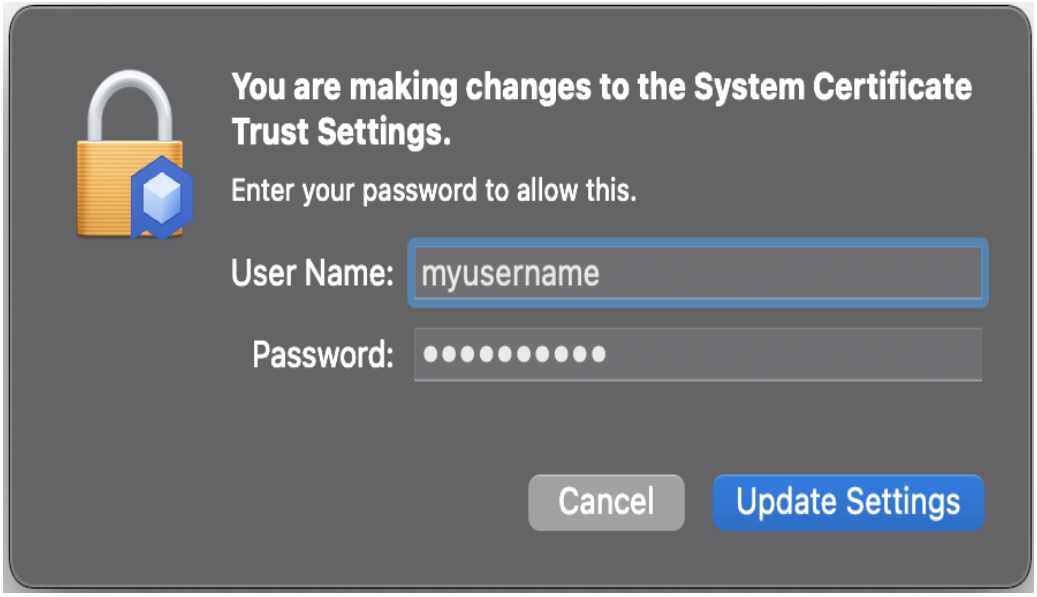
c. At this prompt, click **Allow**.



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. **Note** - Available only if the System Administrator has enabled it. See *"Agent Upgrades" on page 66*.
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. 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. **Note** - This option shows only the trusted networks added by the administrator. See *"Network Configuration" on page 67*.
Protocols tab	
Default	Automatically connects to the network using a protocol configured by the administrator. See *"Network Configuration" on page 67*.
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**.
10. To sign out of the agent, click the icon.

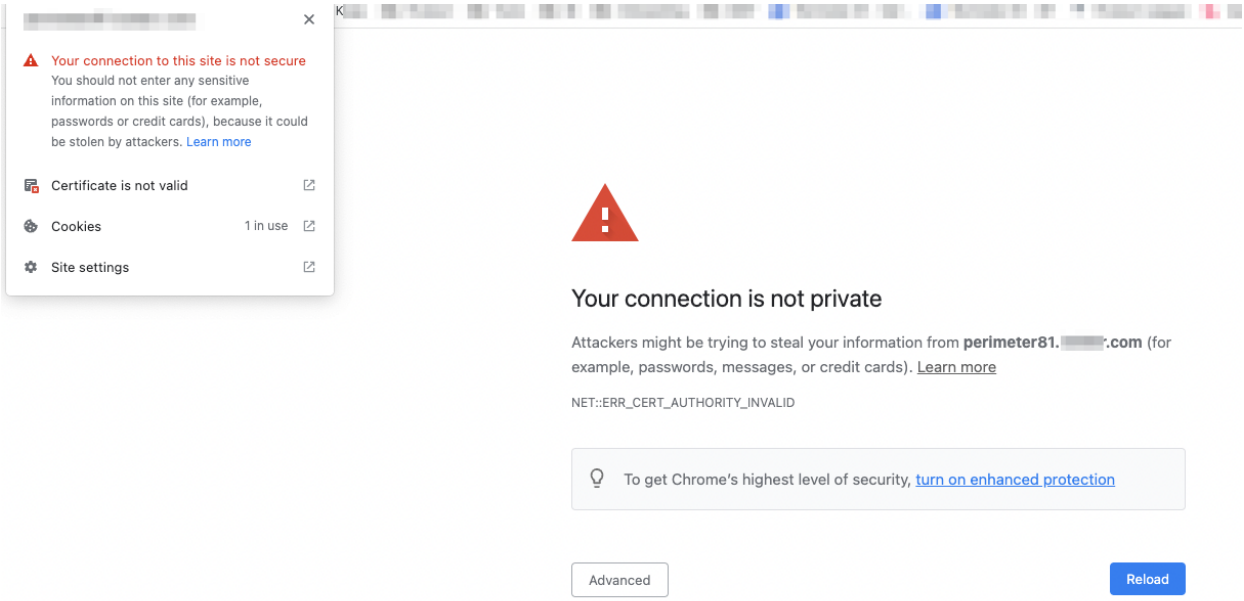
    If this option is disabled by the administrator, the agent prevents the member from signing out without a sign-out code. For more information, see *"Disable Sign-Out" on page 65*.

11. To exit the agent, click the icon. This disables the agent and stops the secure private and internet access.

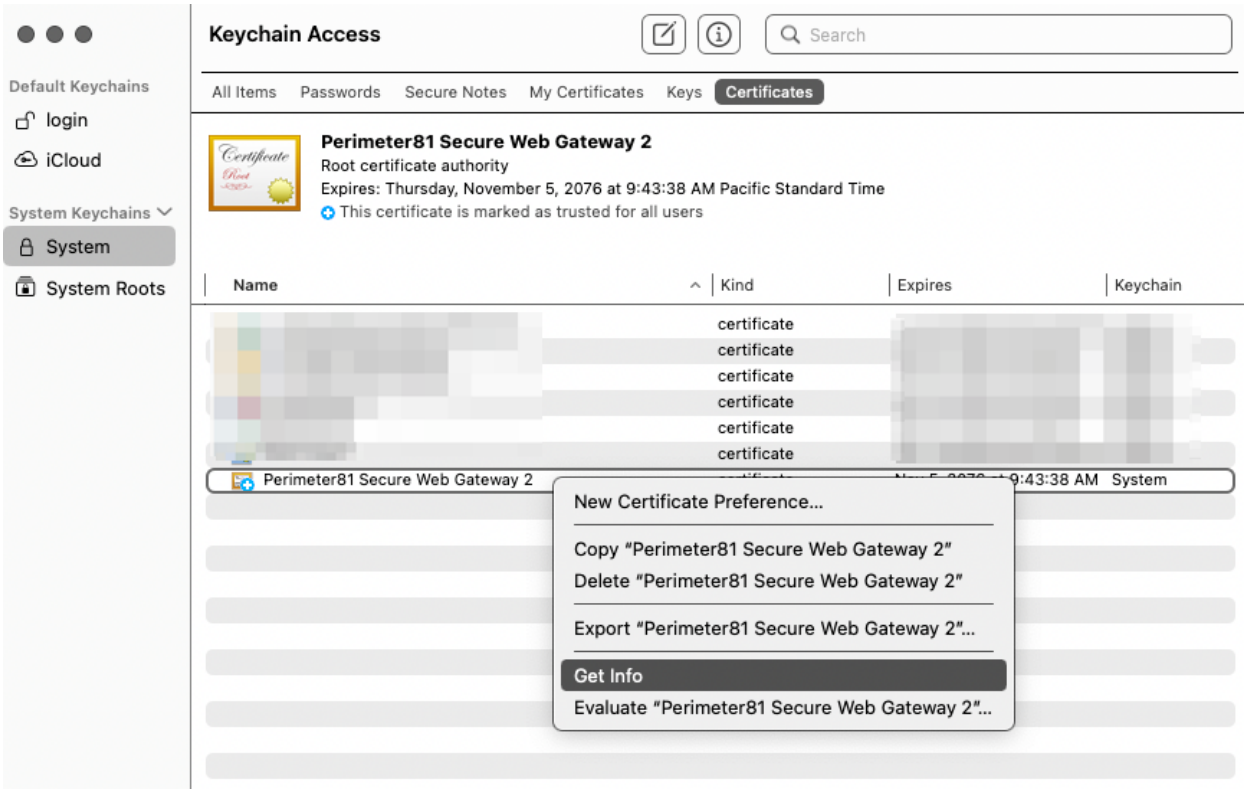
Troubleshooting System Extension Installation on macOS

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

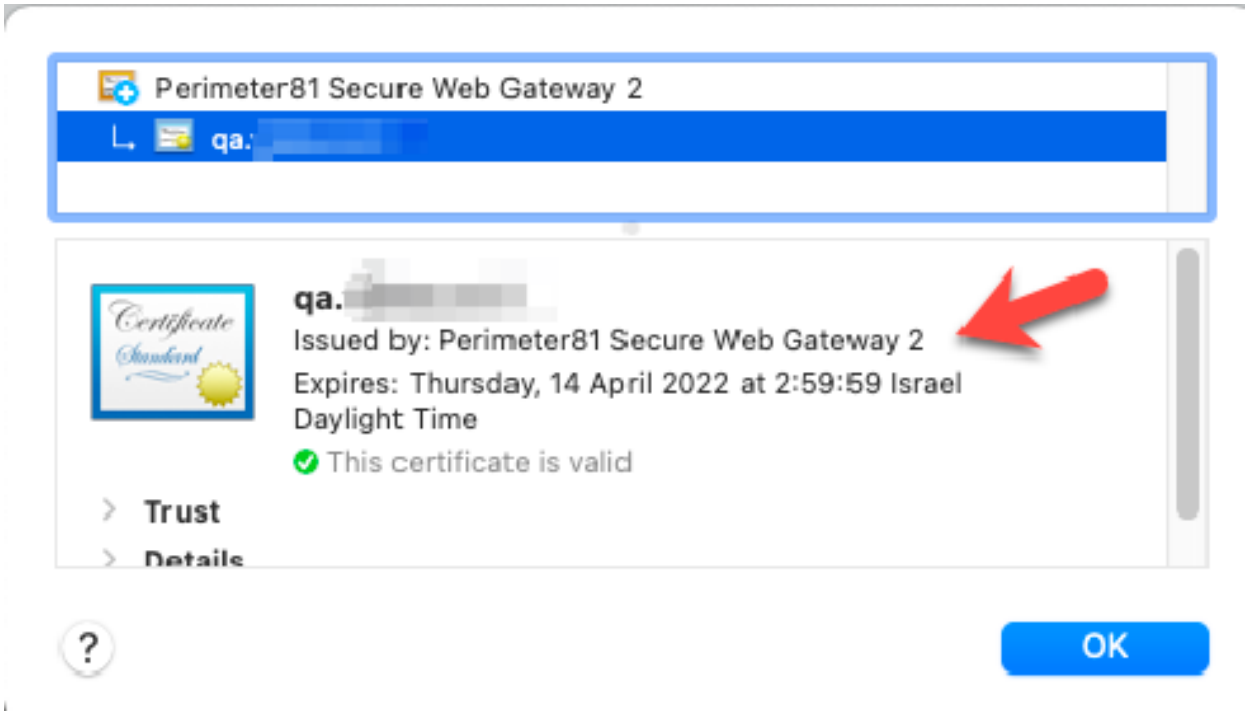
1. Sign out and sign in to the agent.
2. If the Secure Web Gateway certificate installation is blocked, then this error message appears.



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**.


Perimeter81 Secure Web Gateway 2
qa.
qa.
Issued by: Perimeter81 Secure Web Gateway 2
Expires: Thursday, 14 April 2022 at 2:59:59 Israel Daylight Time
This certificate is valid
Trust
Details
?
OK

Harmony SASE Agent - Optimized Performance with Minimal Resource Impact

Harmony SASE Agent is designed for optimal performance, ensuring your device stays fully operational while maintaining robust security. The agent uses minimal resources across all platforms, providing a smooth experience with little impact on system performance.

Performance Efficiency

- **Minimal CPU Usage**: Harmony SASE Agent is designed to use minimal CPU resources, enabling users to perform tasks without disruption, even during heavy network traffic.
- **Optimized Memory Usage**: The agent efficiently manages system memory, ensuring minimal resource consumption while maintaining high performance.

Windows 10 or higher

Resource	Typical Usage*
CPU Utilization	0-5%
Memory Consumption	Approximately 200 MB

macOS 11 or higher

Resource	Typical Usage*
CPU Utilization	0-5%
Memory Consumption	Approximately 400 MB

*The values above reflect typical usage during standard operations. However, resource consumption may temporarily increase during intensive tasks, such as heavy browsing or large file downloads.

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.

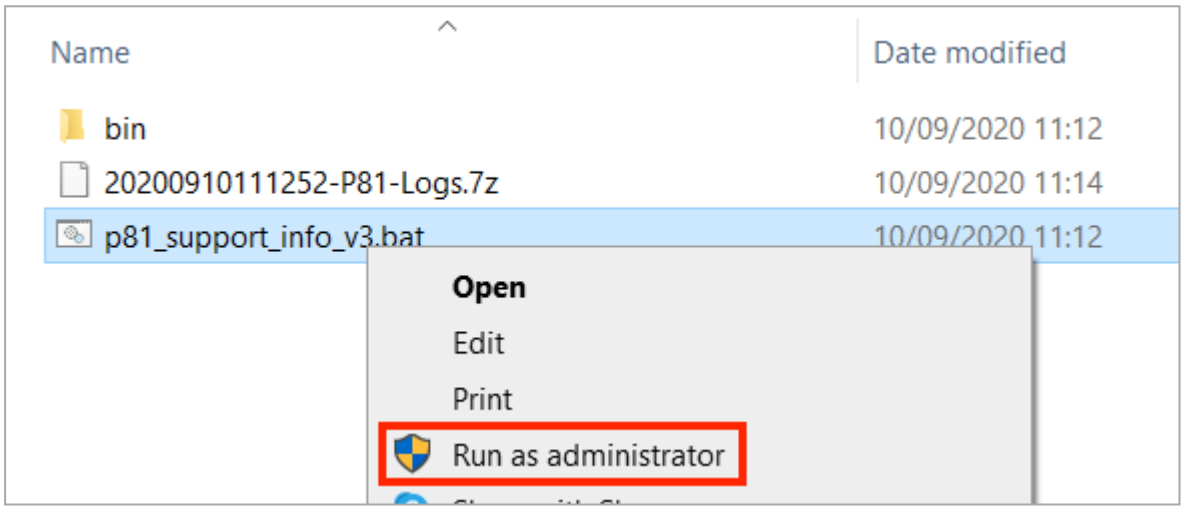
Collecting Logs Manually

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

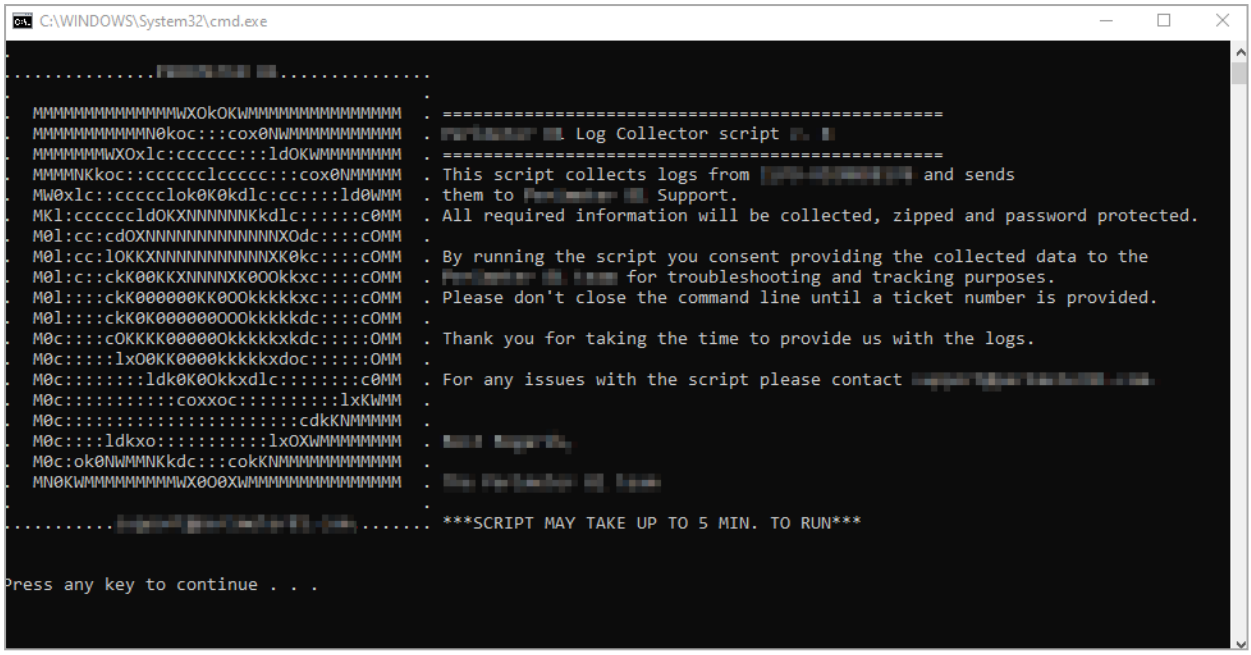
Note - This option is available only for the Perimeter 81 workspace accounts.

Windows

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



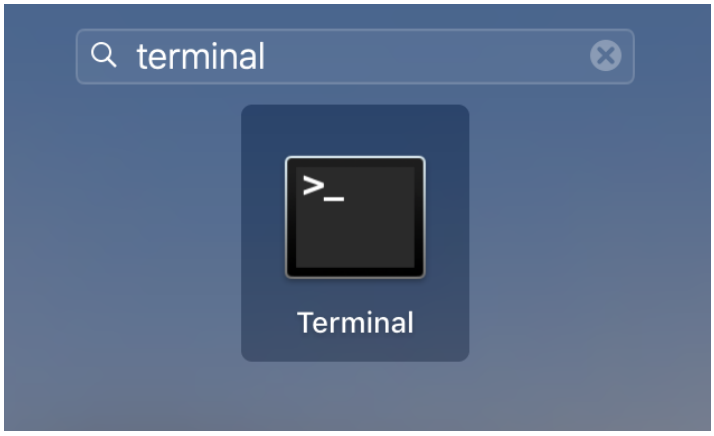
3. Provide your email, workspace name, and ticket number (if applicable). The system automatically sends the log files to *Check Point Support*.



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 the script file MacTroubleshooting.zip and extract it.
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 110*
- *"Gateways" on page 113*
- *"Tunnels" on page 116*

High-Level Procedure

"Defining a Network" on page 120.

"Adding a Tunnel" on page 126.

"Managing a Network" on page 147.

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

North America	EMEA	APAC	LATAM
▪ New Jersey 2, NJ, USA ▪ New York 2, NY, USA ▪ San Francisco, CA, USA ▪ Seattle, WA, USA ▪ Seattle 2, WA, USA ▪ Silicon Valley 2, CA, USA ▪ Toronto 2, Canada ▪ 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*.

Coming Soon

Zurich, Switzerland

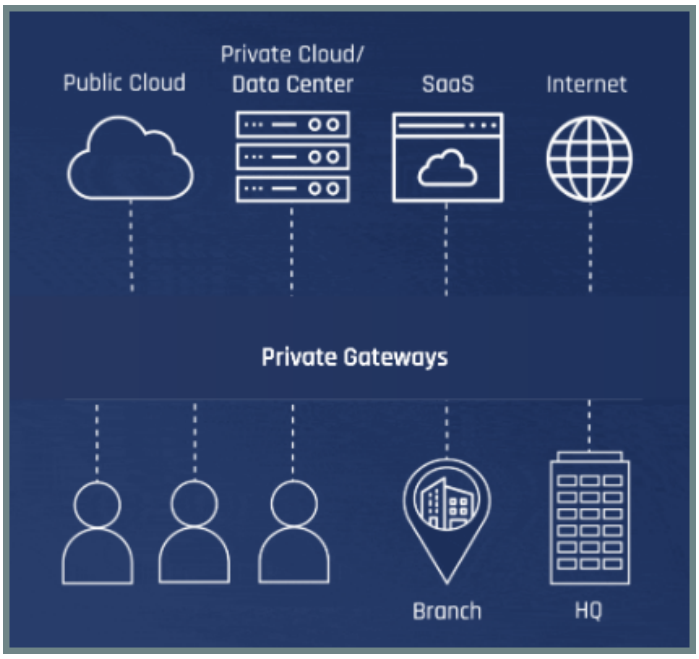
Gateways

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 65*.

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 page 118*

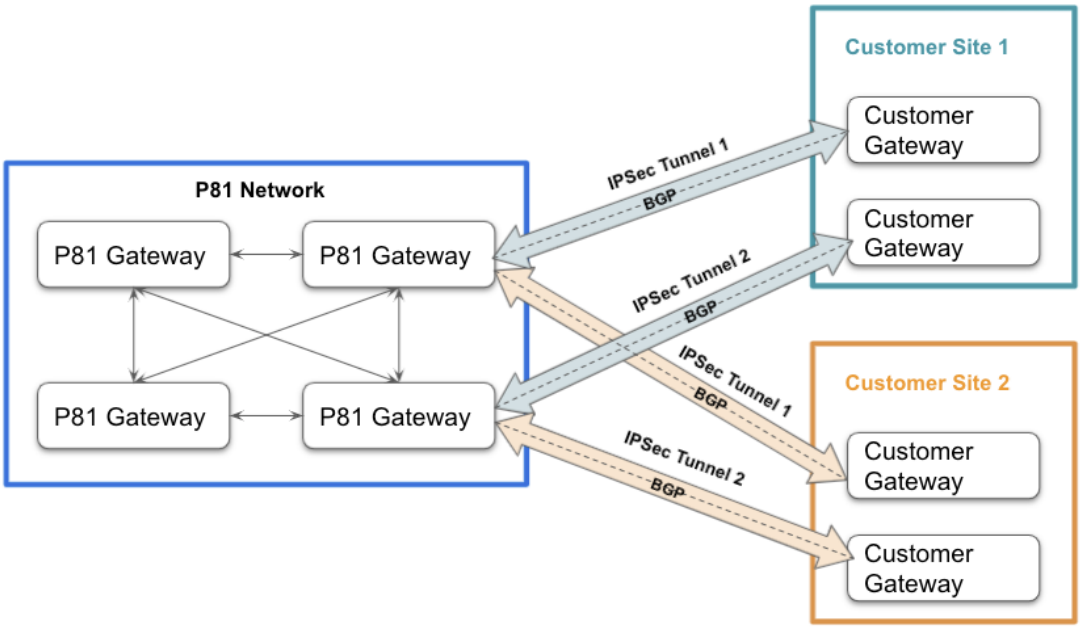
IPSec Site-2-Site VPN Tunnel

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.



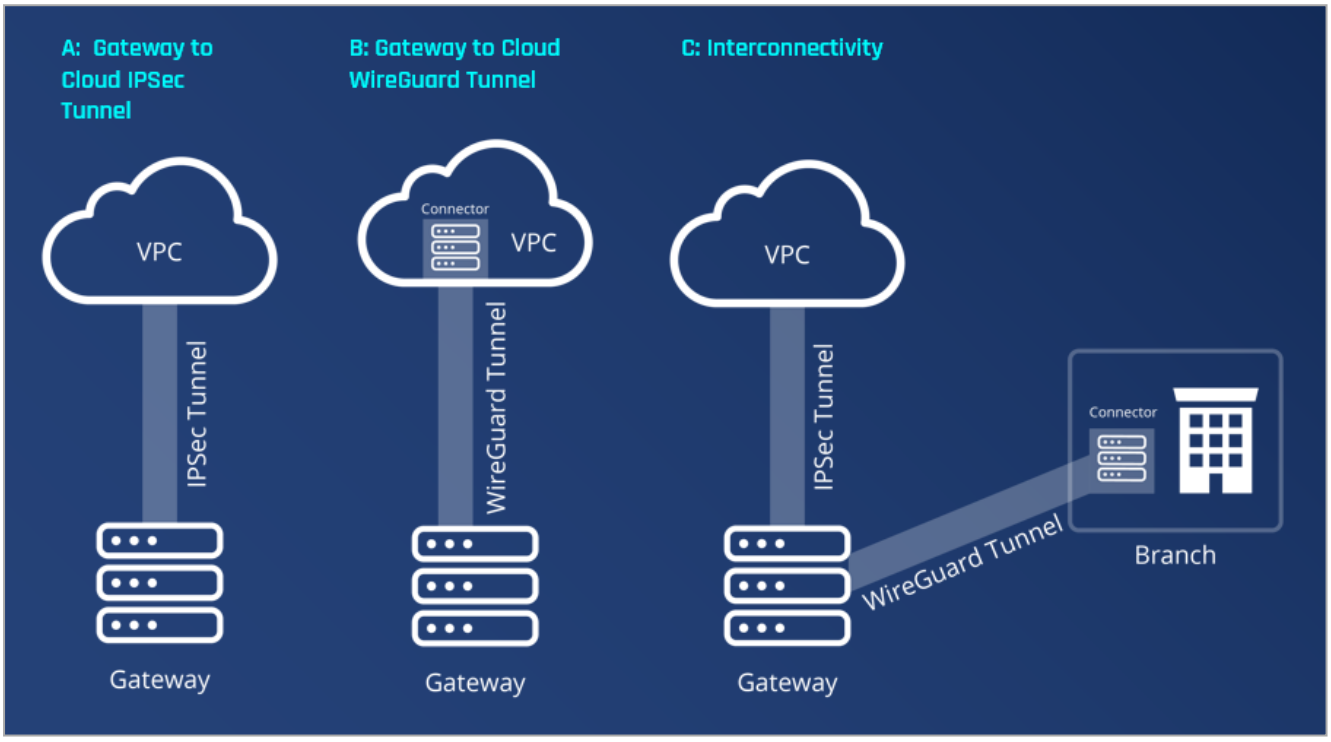
Best Practice - For redundancy, we recommend that you deploy the gateways in different regions depending on users' location.

To configure an IPSec Site-2-Site VPN Tunnel, see *"IPsec Site-to-Site VPN Tunnel" on page 127*.

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.

	Wireguard Connector	IPSec Tunnel
Site-to-Site Implementation	Wireguard	strongSwan
VPN Protocol	Wireguard	IKE
Internet Protocol	UDP	Any
Setup Environment	Linux	Any
Stability	High	High
Chipers Design Date	00's-10's	90's-00's
Code Length	4k	400k-60k lines

To configure a Wireguard connector, see *"WireGuard Connector Tunnel" on page 132*.

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 83*.
- 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.

To configure a OpenVPN Tunnel in the Harmony SASE Administrator Portal, see *"OpenVPN Tunnel" on page 138*.

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.

Creating a Network

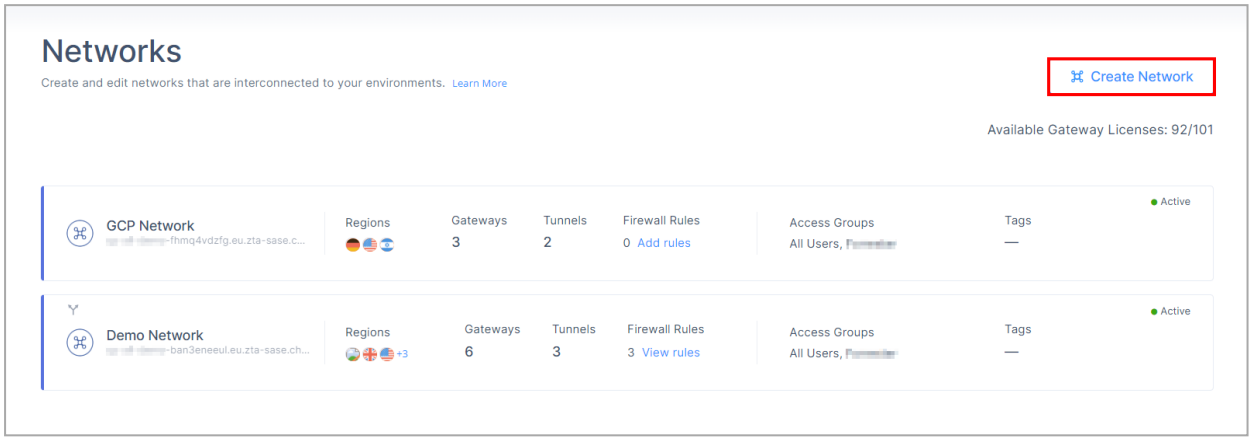
To protect the cloud infrastructure using Harmony SASE, you must define the network, add gateways, and create tunnels.

- Step 1 - Define a network
- Step 2 - Add a tunnel

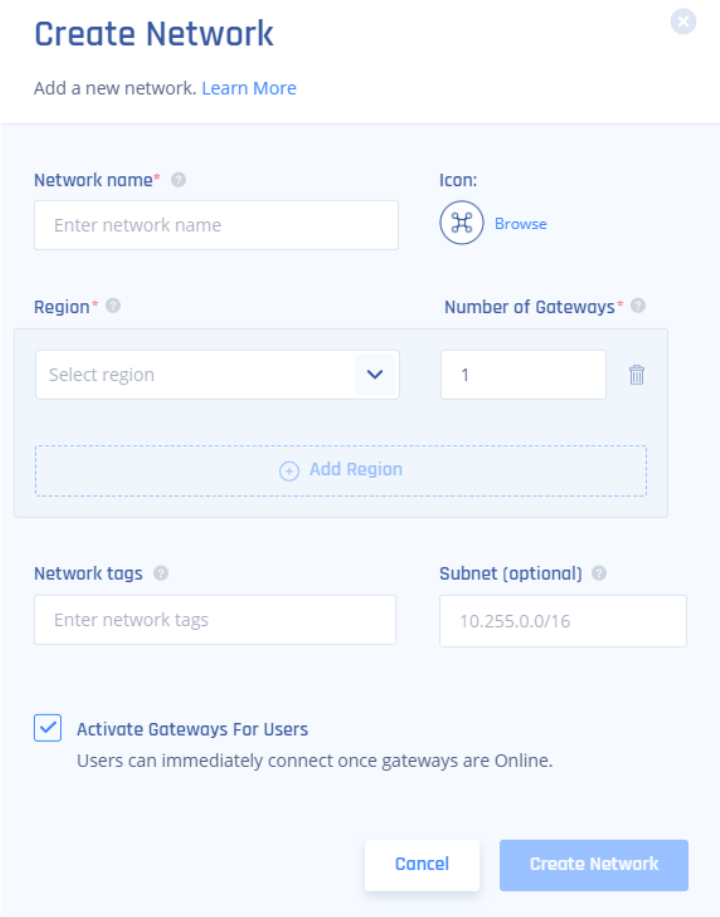
- Step 3 - Verify the tunnel setup
- Step 4 - Manage the network

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.

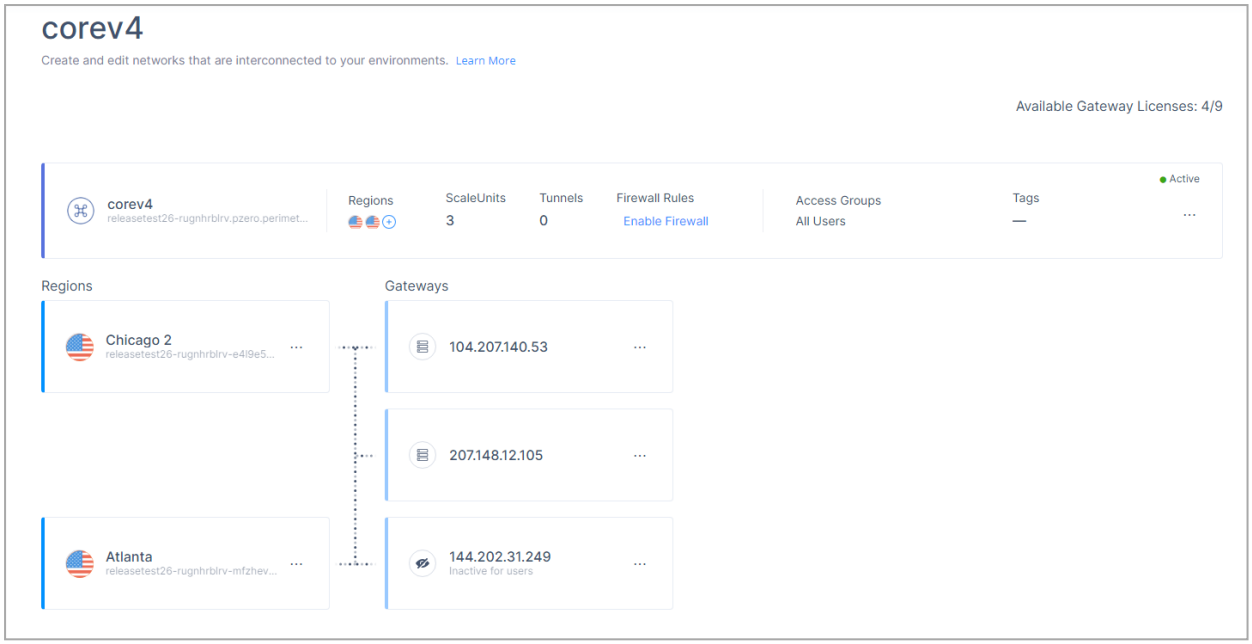
   Warning - You cannot change your subnet after you create your network. Make sure that the subnet does not overlap with your SD-WAN device's subnets.

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

5. Click **Create Network**.

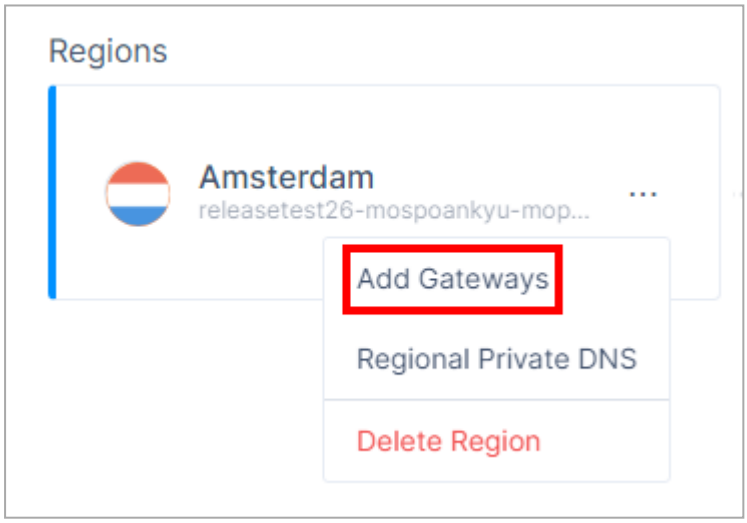
   The system creates the network and it is listed in the **Networks** page.

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

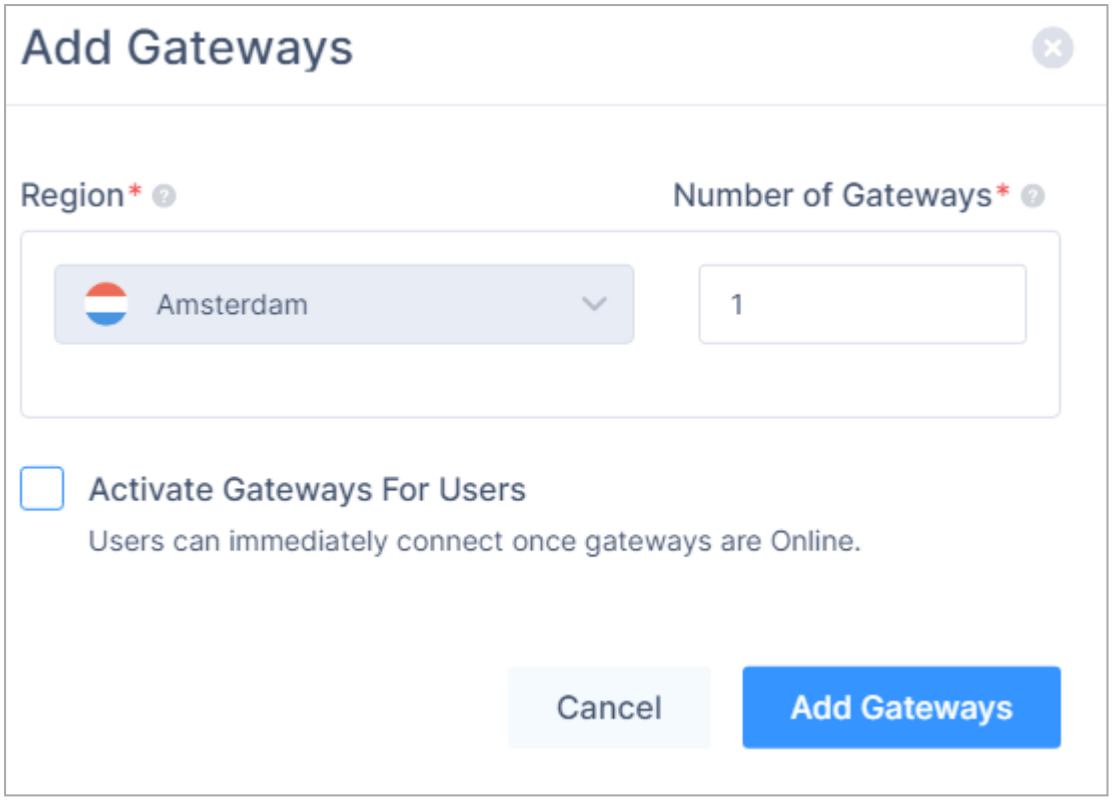


Adding Gateways to an Existing Network

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

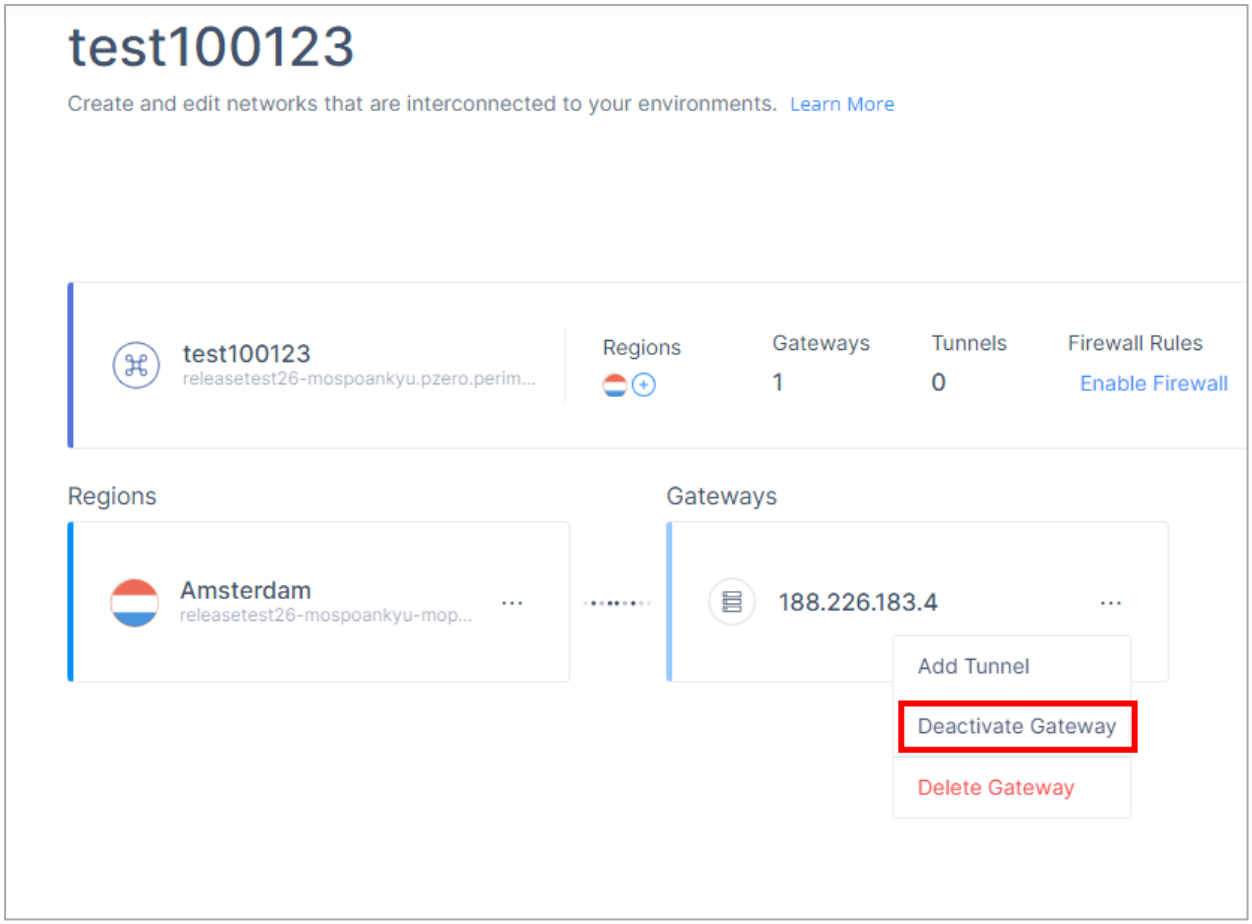
You can deactivate a gateway to block members from accessing the network resources (including Zero trust Applications) connected to the gateway. However, the gateway remains operational and configurable.

When you deactivate a gateway:

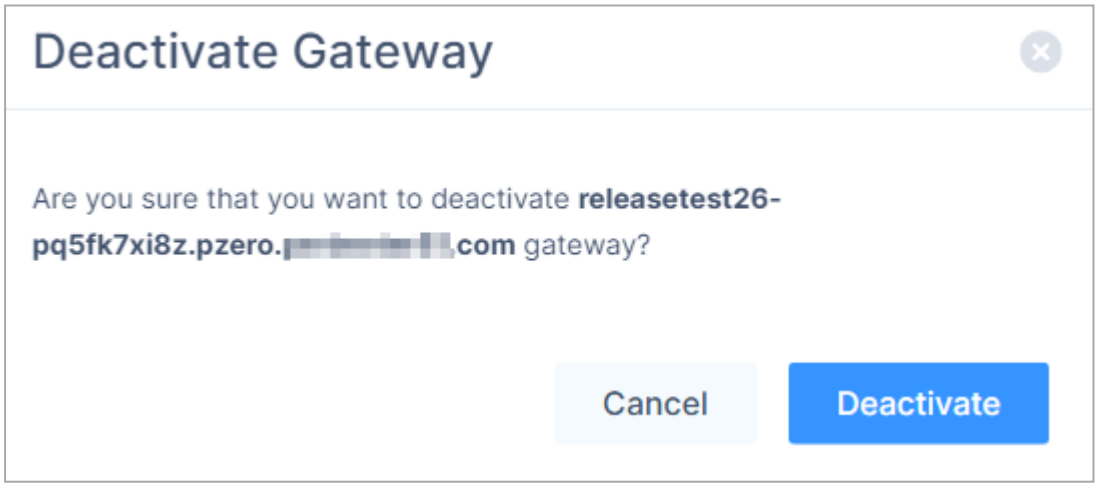
- Members and applications cannot connect to the gateway and are redirected to alternate gateways (if available).
- Members already connected to the gateway stay connected until they disconnect. After which, they are connected to an alternate gateway (if available).

To deactivate a gateway:

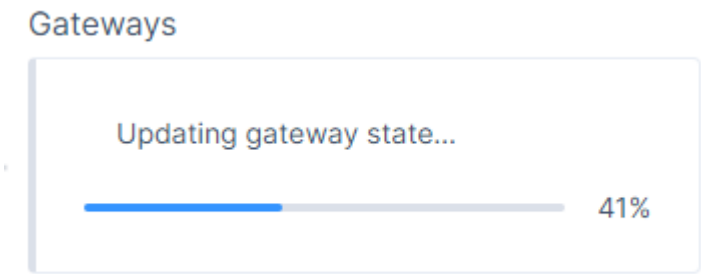
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· on your gateway and then click **Deactivate Gateway**.



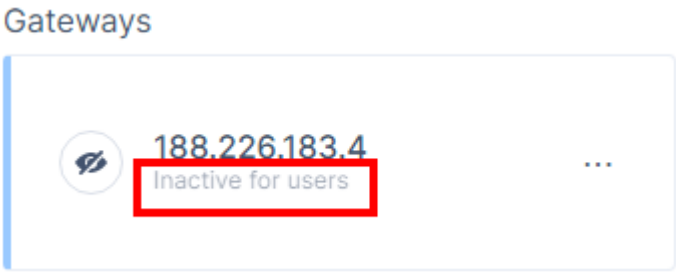
4. Click **Deactivate**.



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-to-Site VPN Tunnel" on page 127*
- *"WireGuard Connector Tunnel" on page 132*
- *"OpenVPN Tunnel" on page 138*

IPsec Site-to-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:

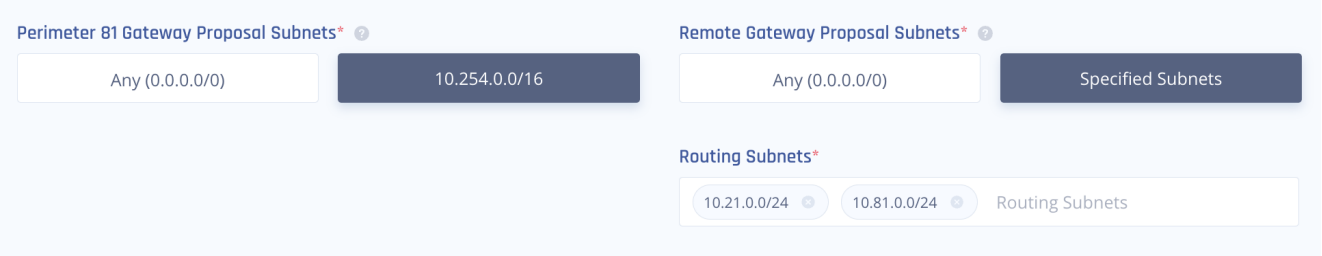
- **Harmony SASE Gateway Proposal Subnets**
- **Remote Gateway Proposal Subnets**
- **Tunnel Lifetime**
- **Dead Peer Detection (DPD)**
- **Encryption (Phase II)**

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

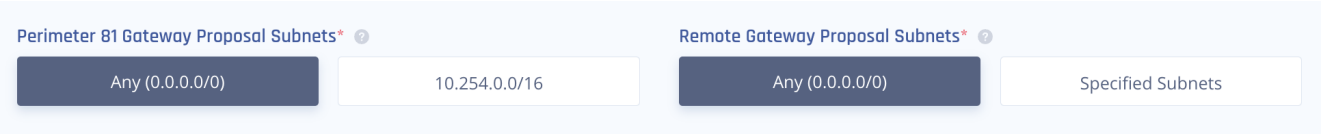
Policy-Based and Route-Based IPSec Connection

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" on page 181 ▪ "Check Point Firewall" on page 191 ▪ "Cisco Firepower" on page 201 ▪ "Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 221 ▪ "Configuring Check Point Redundant IPsec Tunnel" on page 246 ▪ "Cisco ASA Firewall" on page 271 ▪ "Cisco Meraki Router" on page 375 ▪ "FortiGate Next Generation Firewall" on page 305 ▪ "Juniper Networks ScreenOS Firewall" on page 309 ▪ "Juniper (JunOS) SRX Firewall" on page 315 ▪ "Palo Alto Firewall" on page 328 ▪ "pfSense Firewall" on page 335 ▪ "SonicWall Firewall" on page 341 ▪ "Sophos XG Firewall" on page 351 ▪ "UniFi USG Firewall" on page 357 ▪ "WatchGuard Firewall" on page 363 ▪ "Zyxel USG Firewall" on page 369	▪ "Cisco Meraki Router" on page 375 ▪ "D-Link DSR Series Router" on page 378 ▪ "DrayTek Vigor2862 Router" on page 385 ▪ "DrayTek Vigor3900 Router" on page 388 ▪ "EdgeMax Router" on page 395 ▪ "Linksys Router" on page 397 ▪ "Netgear BR500 Router" on page 401	**Single Tunnel** ▪ "AWS Virtual Gateway" on page 424 ▪ "AWS Transit Gateway" on page 443 ▪ "Google Cloud Platform" on page 556 ▪ "Azure Virtual Network Gateway" on page 491 **Redundant Tunnels** ▪ "AWS Redundant Tunnels - Virtual Private Gateway" on page 460 ▪ "AWS Redundant Tunnels - Transit Gateway" on page 474 ▪ "Google Cloud Platform (GCP) Redundant Tunnels" on page 568 ▪ "Azure Virtual Network Gateway Redundant Tunnels" on page 517 ▪ "Azure Virtual WAN Redundant Tunnels" on page 535 **Other Cloud Options** ▪ "Alibaba Cloud" on page 415 ▪ "Heroku Enterprise" on page 590 ▪ "IBM Cloud" on page 591

High-Level Procedure

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

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

On-premises		Cloud-based Resource
Firewall	**Router**	
▪ *"Barracuda Firewall" on page 181* ▪ *"Check Point Firewall" on page 191* ▪ *"Cisco Firepower" on page 201* ▪ *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 221* ▪ *"Configuring Check Point Redundant IPsec Tunnel" on page 246* ▪ *"Cisco ASA Firewall" on page 271* ▪ *"Cisco Meraki Router" on page 375* ▪ *"FortiGate Next Generation Firewall" on page 305* ▪ *"Juniper Networks ScreenOS Firewall" on page 309* ▪ *"Juniper (JunOS) SRX Firewall" on page 315* ▪ *"Palo Alto Firewall" on page 328* ▪ *"pfSense Firewall" on page 335* ▪ *"SonicWall Firewall" on page 341* ▪ *"Sophos XG Firewall" on page 351* ▪ *"UniFi USG Firewall" on page 357* ▪ *"WatchGuard Firewall" on page 363* ▪ *"Zyxel USG Firewall" on page 369*	▪ *"Cisco Meraki Router" on page 375* ▪ *"D-Link DSR Series Router" on page 378* ▪ *"DrayTek Vigor2862 Router" on page 385* ▪ *"DrayTek Vigor3900 Router" on page 388* ▪ *"EdgeMax Router" on page 395* ▪ *"Linksys Router" on page 397* ▪ *"Netgear BR500 Router" on page 401*	**Single Tunnel** ▪ *"AWS Virtual Gateway" on page 424* ▪ *"AWS Transit Gateway" on page 443* ▪ *"Google Cloud Platform" on page 556* ▪ *"Azure Virtual Network Gateway" on page 491* **Redundant Tunnels** ▪ *"AWS Redundant Tunnels - Virtual Private Gateway" on page 460* ▪ *"AWS Redundant Tunnels - Transit Gateway" on page 474* ▪ *"Google Cloud Platform (GCP) Redundant Tunnels" on page 568* ▪ *"Azure Virtual Network Gateway Redundant Tunnels" on page 517* ▪ *"Azure Virtual WAN Redundant Tunnels" on page 535* **Other Cloud Options** ▪ *"Alibaba Cloud" on page 415* ▪ *"Heroku Enterprise" on page 590* ▪ *"IBM Cloud" on page 591*

4. Verify the setup.

WireGuard Connector Tunnel

Prerequisites

A Linux machine with these specifications:

- **Kernel**: Any of these packages installed:
  - Ubuntu (Server/Desktop) 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS, 23.04
  - CentOS 7, or CentOS 8
  - REHL 7, REHL 8, or REHL 9 (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

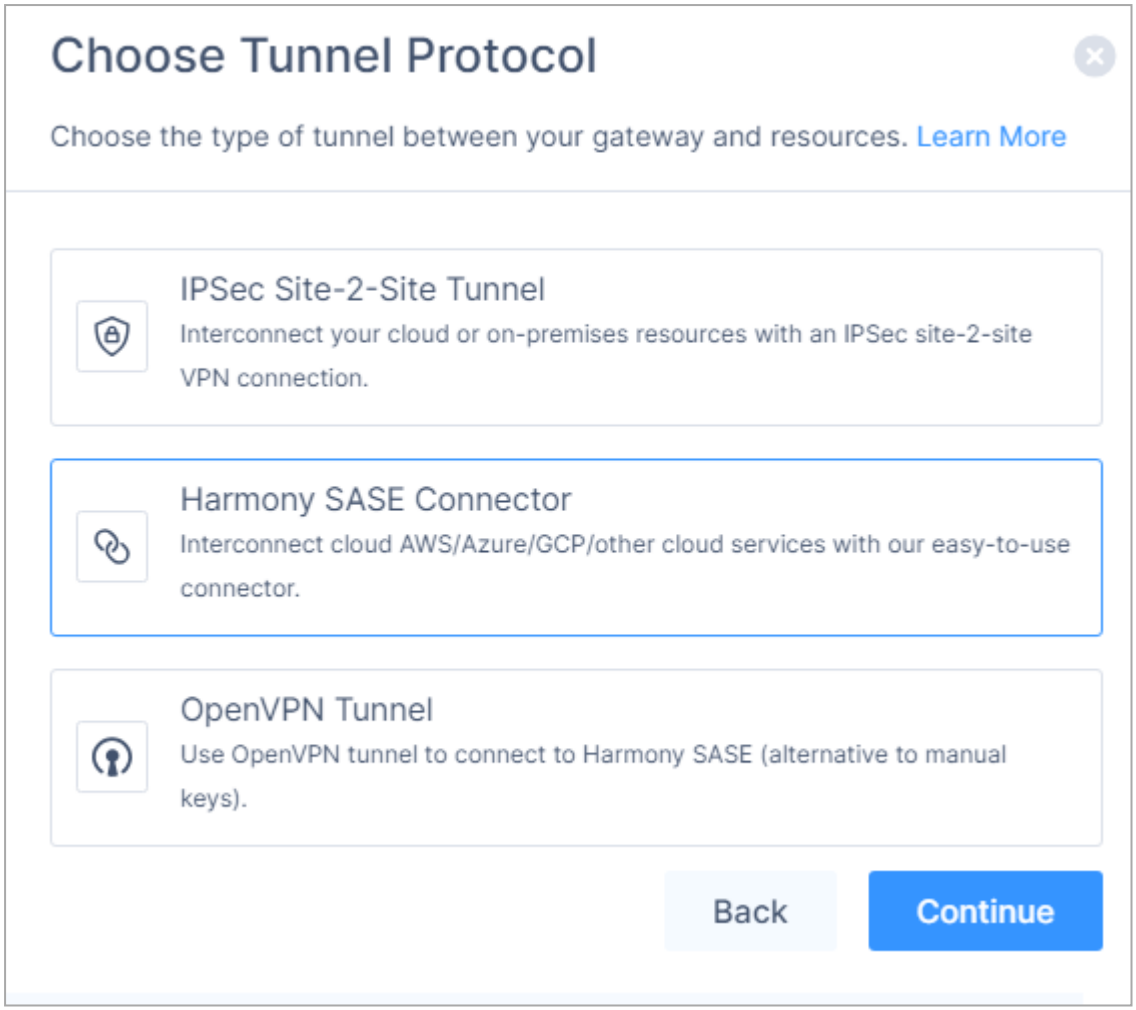
Note - For Linux deployed on a Windows host, enable virtualization on Windows BIOS.

Configuring a WireGuard Connector Tunnel

Configuring the Connector in the Harmony SASE Administrator Portal

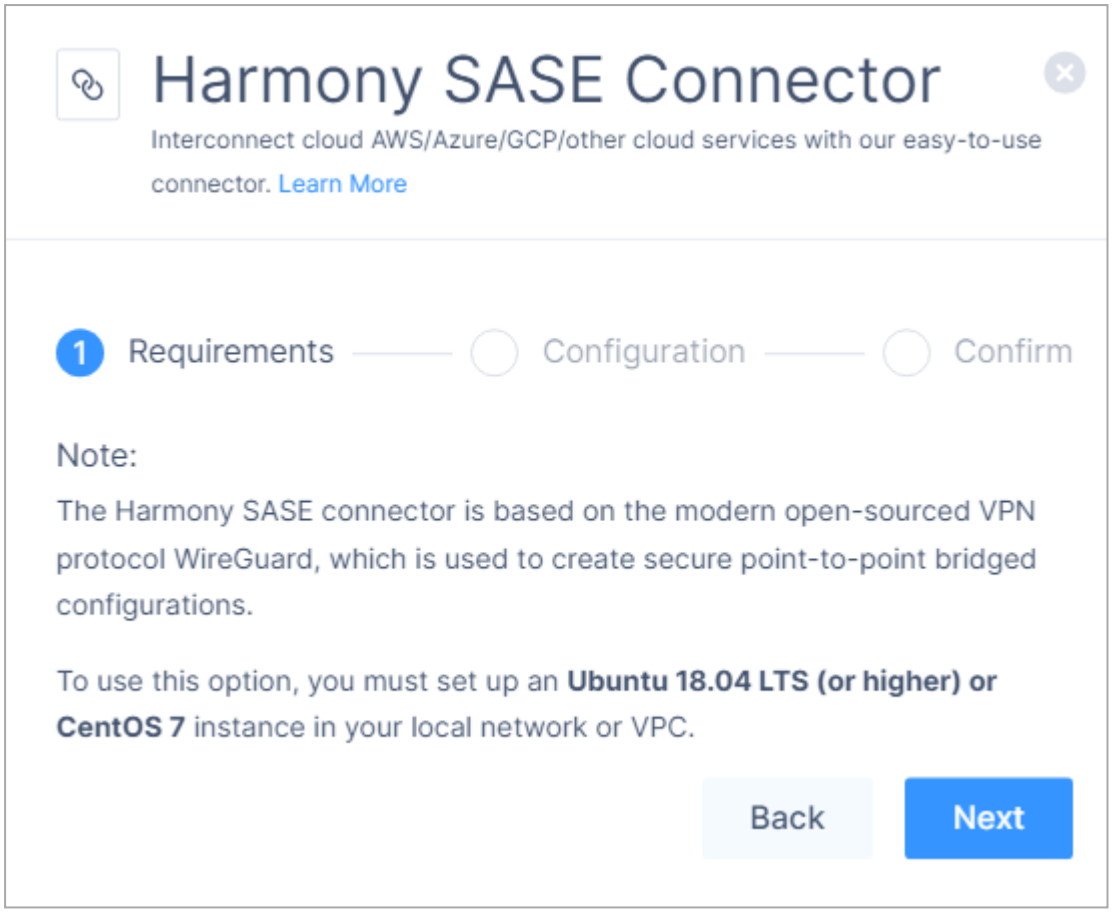
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. For the gateway to which you want to add the WireGuard Connector tunnel, click ··· and click **Add Tunnel**.

   The **Choose Tunnel Protocol** window appears.



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

   The **Harmony SASE Connector** window appears.

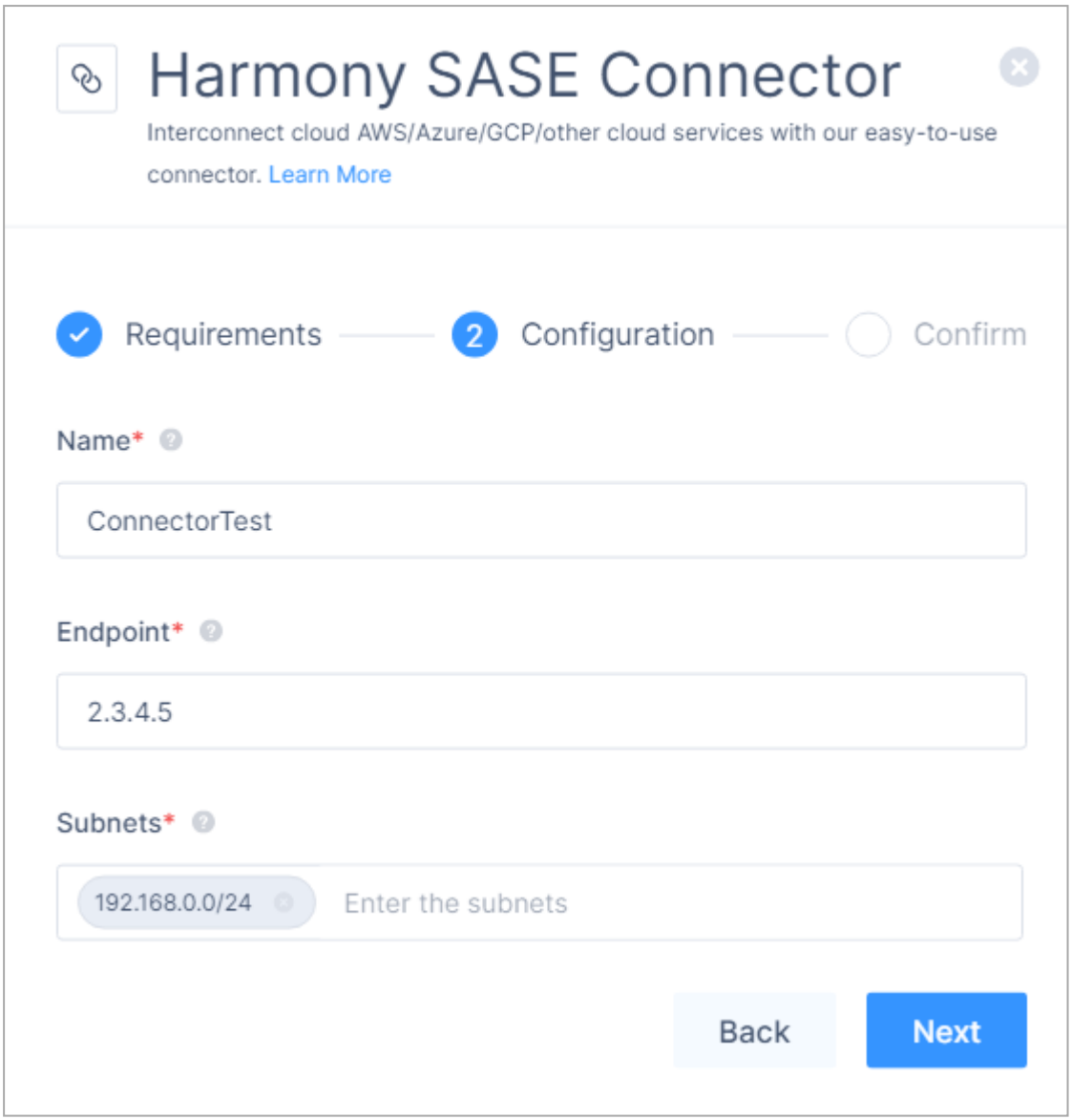


5. In the **Requirements** section, read the requirements and make sure they are met. Click **Next**.
6. In the **Configuration** section, enter these:
   a. **Name** - Name for the connector.
   b. **Endpoint** - IP address of the Linux server that has the WireGuard Connector installed.

      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**.

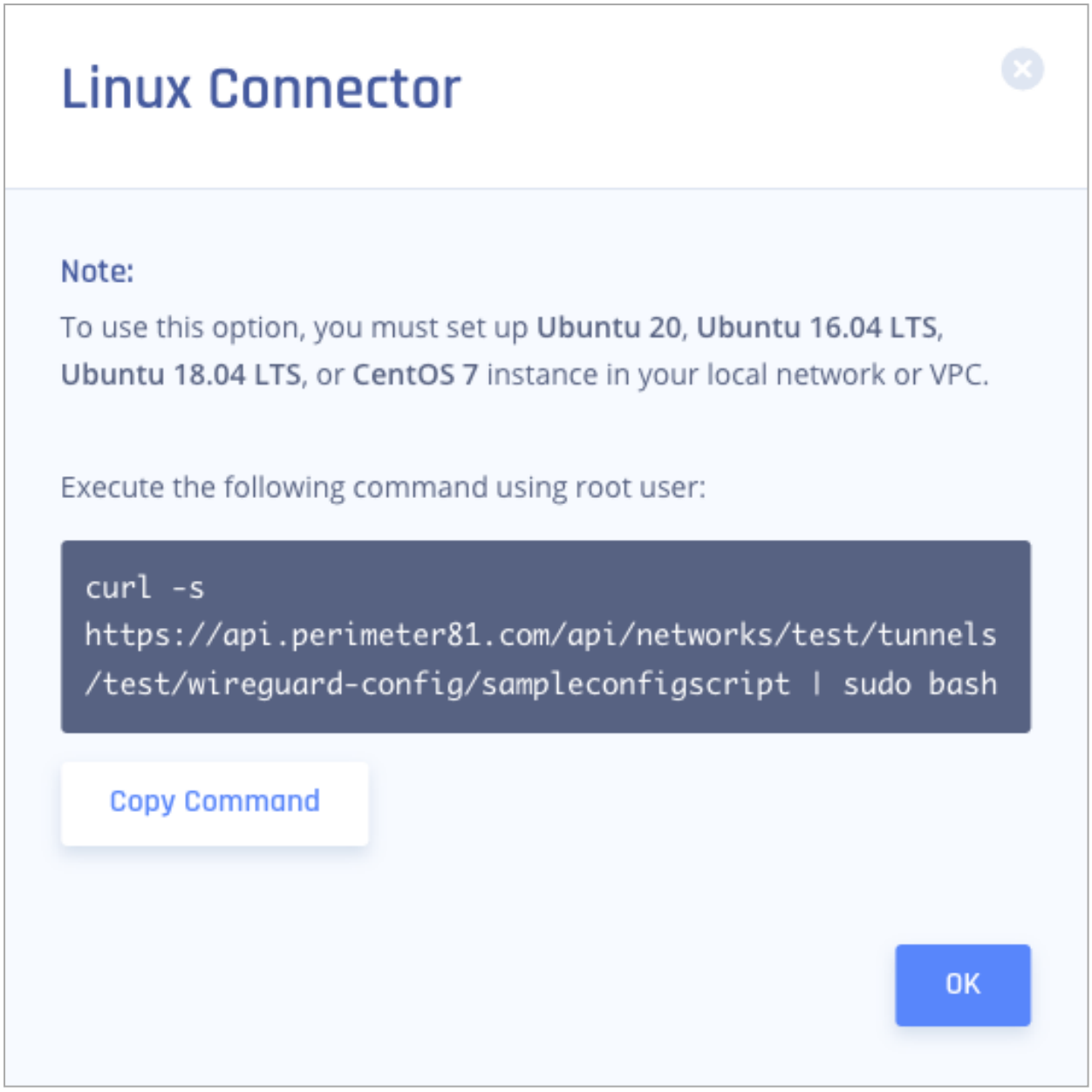
7. In the **Confirm** section, click **Apply**.

   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
```

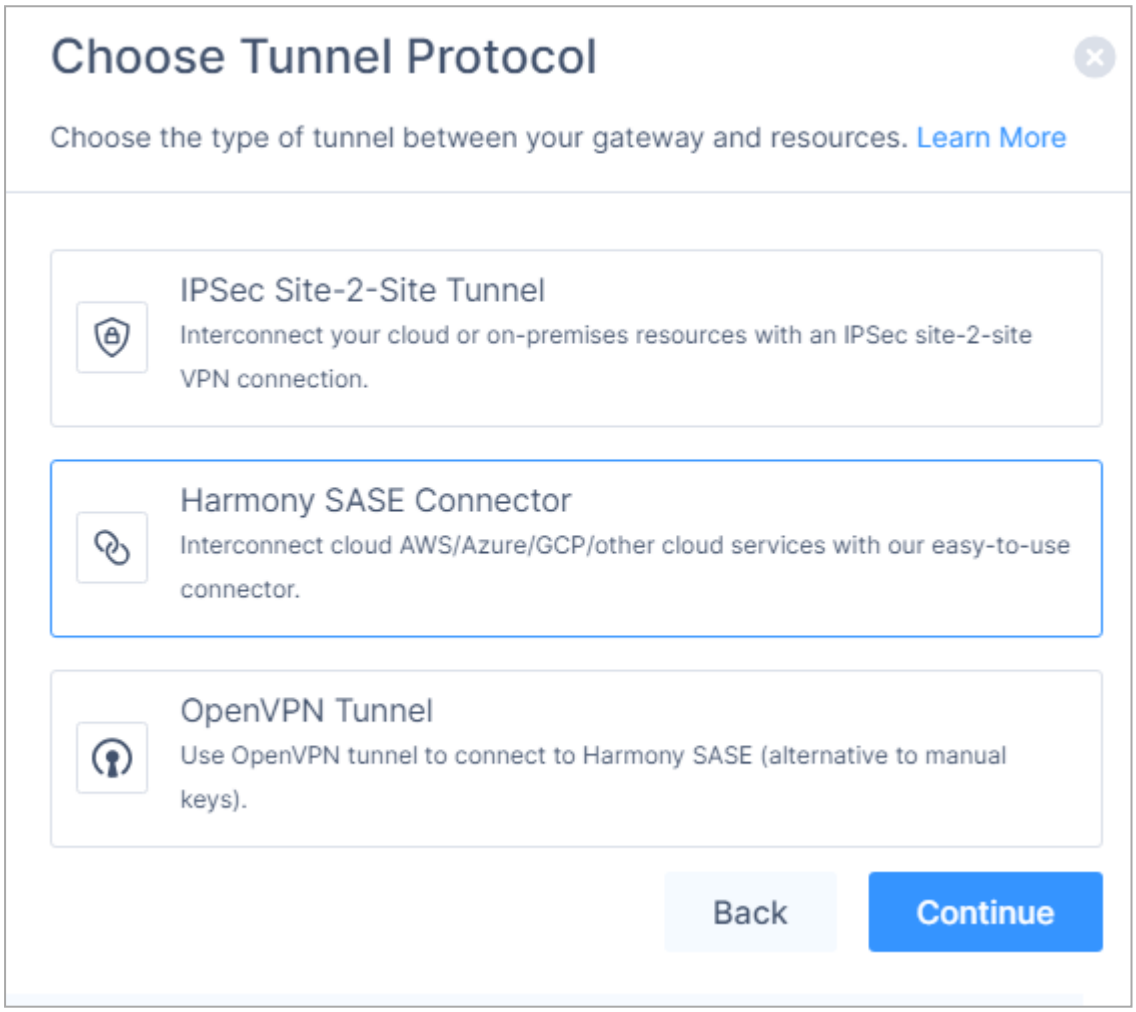
```
# Locate the WireGuard packages # (the output of this command will
show you all wireguard packages installed on the machine)
yum list installed | grep wireguard

# 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

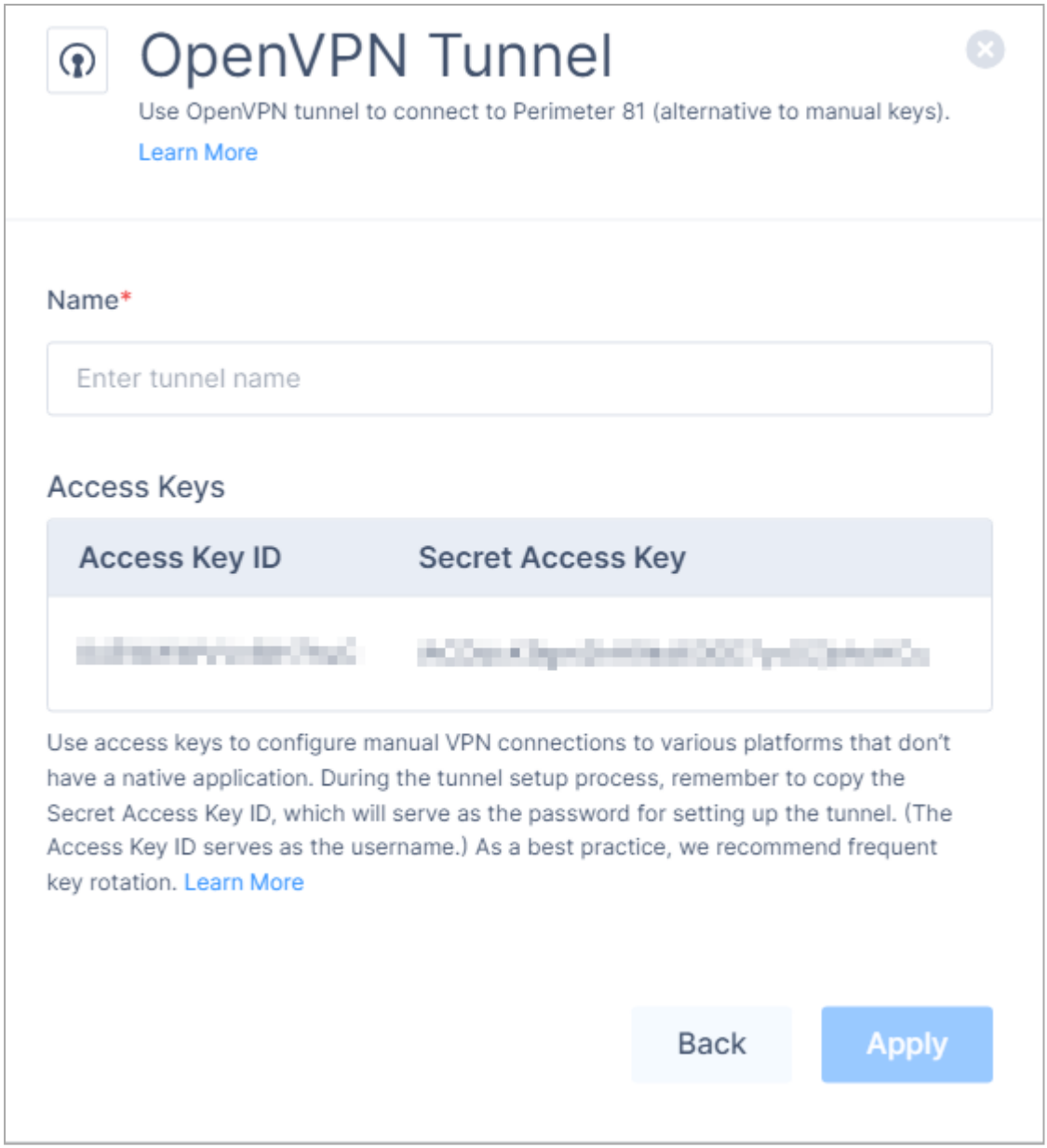
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. For the gateway to which you want to add the OpenVPN tunnel, click ··· and click **Add Tunnel**.

   The **Choose Tunnel Protocol** window appears.



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

   The **OpenVPN Tunnel** window appears.

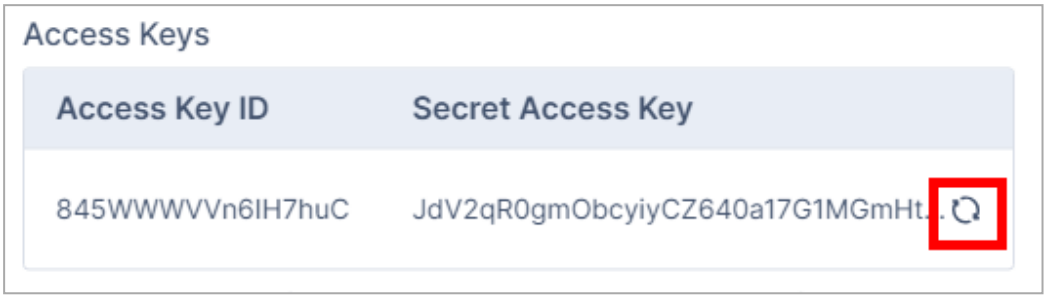


5. In the **Name** field, enter a name for the tunnel.
6. Save the **Access Keys** credentials.

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 .

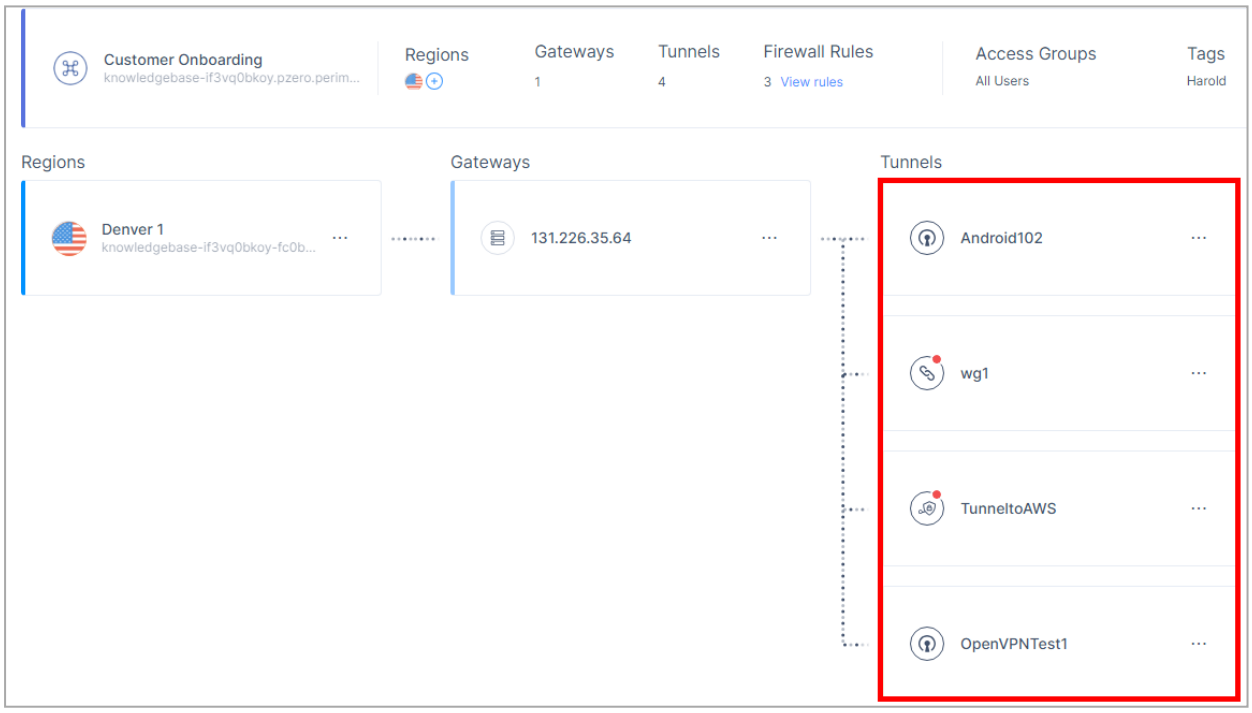


The system regenerates the **Access Key ID** and **Secret Access Key** values.

c. Click **Apply**.

7. Click **Apply**.

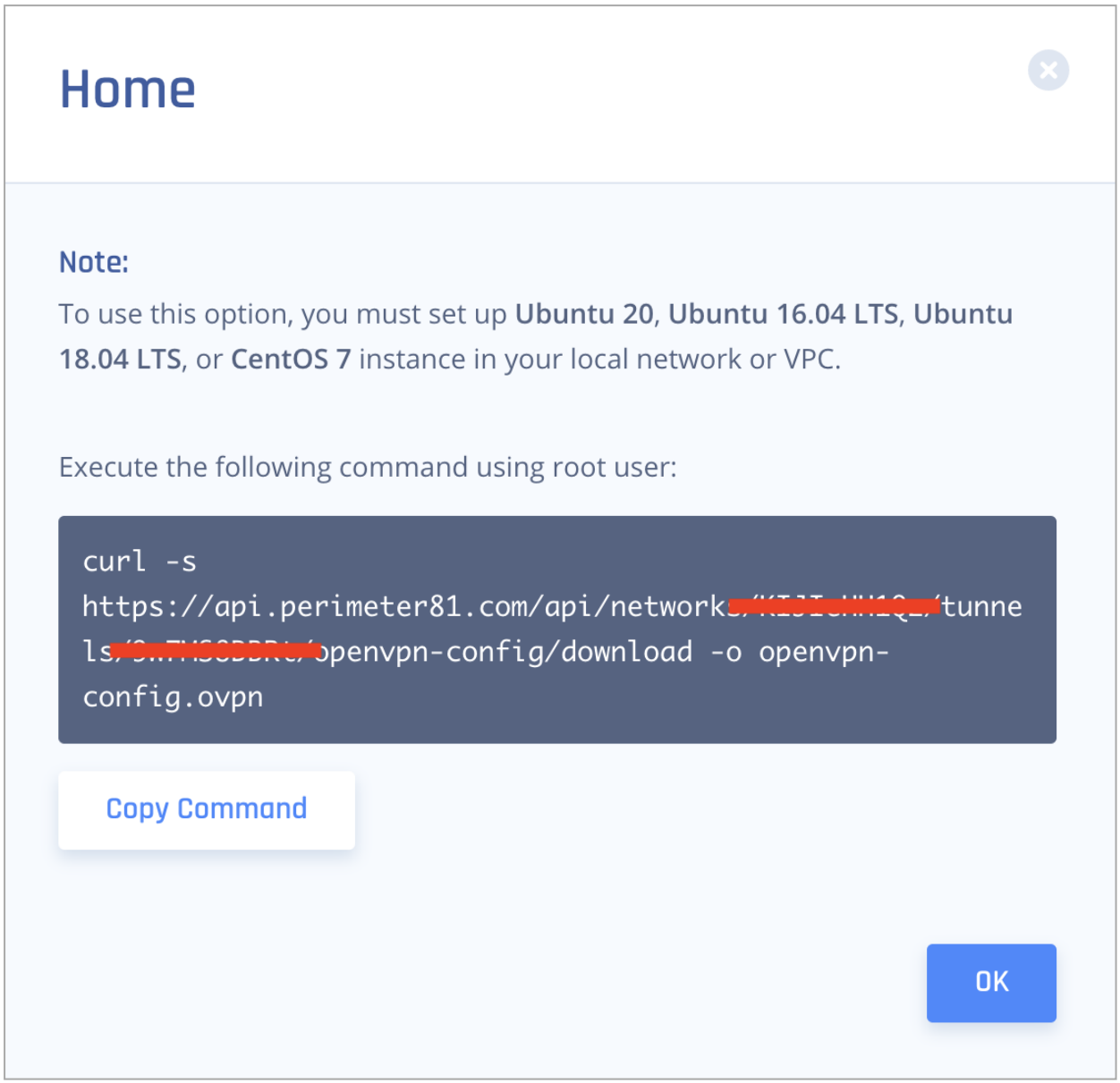
The system creates an OpenVPN tunnel and displays it in the **Tunnels** section.



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.

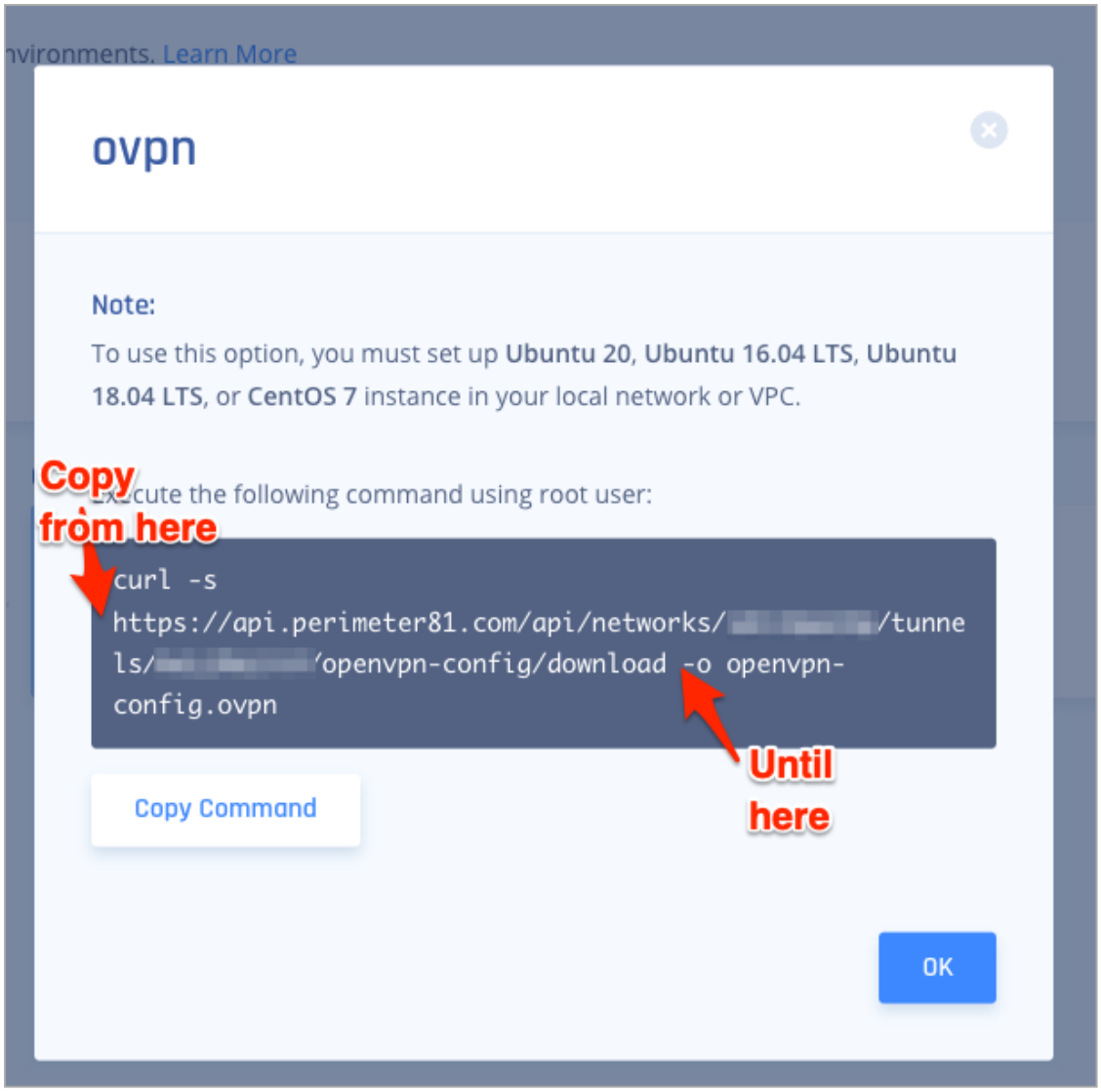
3. In the gateway where you added the OpenVPN tunnel, click ··· and then click **Configuration**.



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

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

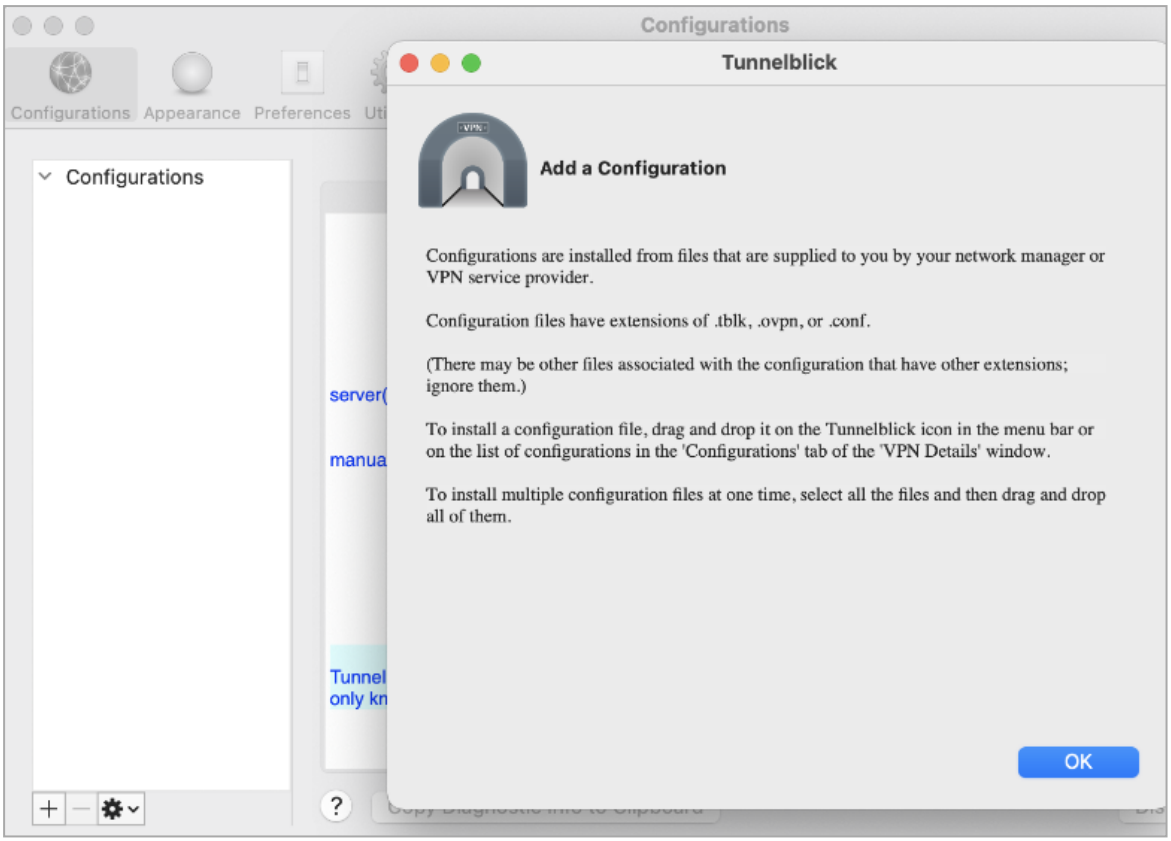
Note - If the device's operating system does not support a terminal window, copy the command from `https` until `download`. Paste the command in a browser address bar and press **Enter**. The system downloads the *saferx-openvpn-client.ovpn* configuration file.



5. On a macOS device:

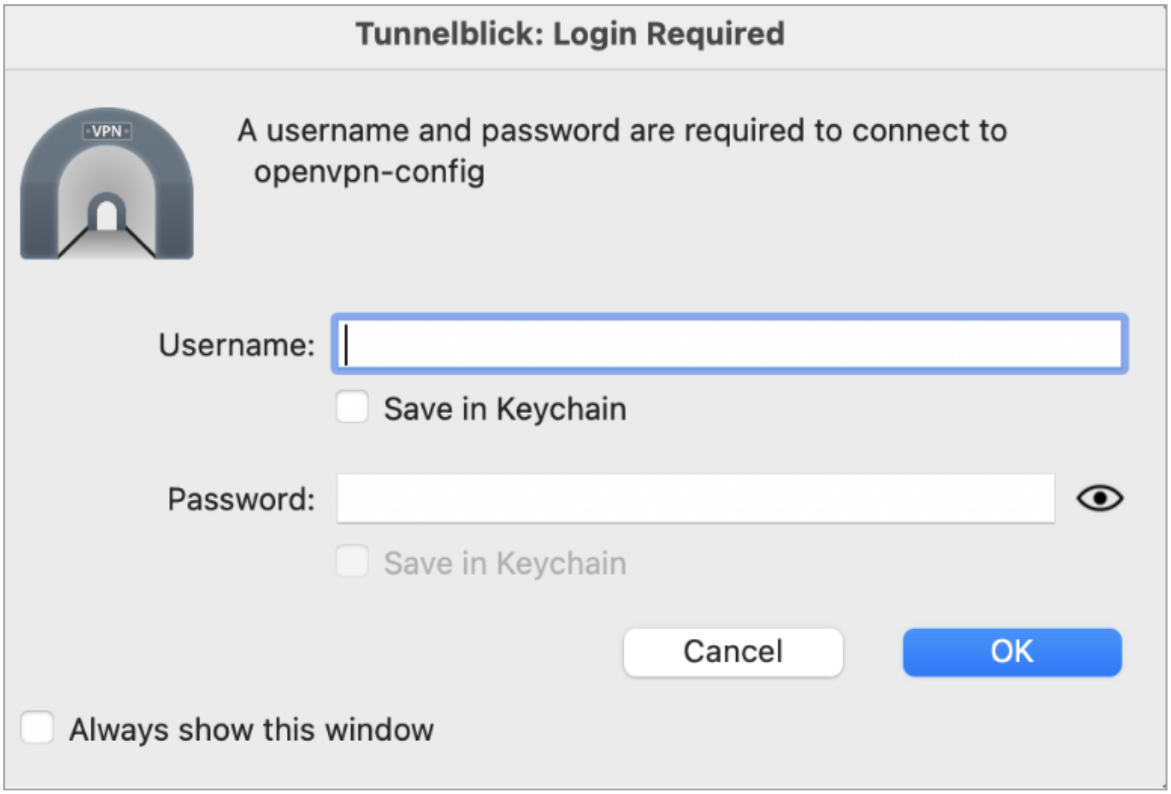
   a. Download and install a VPN client. Check Point recommends Tunnelblick VPN client.

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.

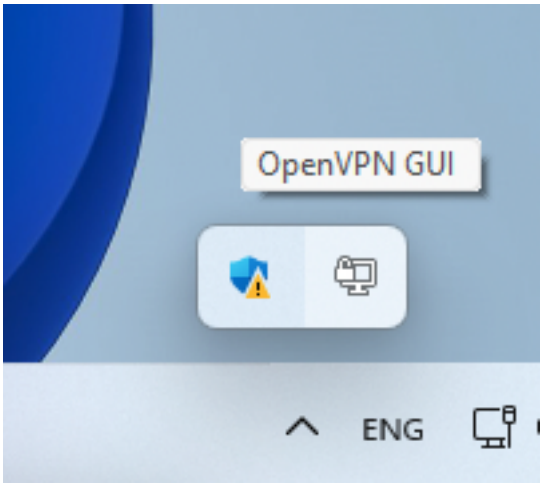


e. Click **OK**.

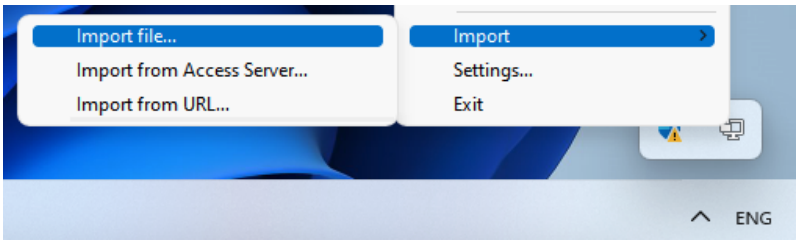
6. On a Windows device:

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...**

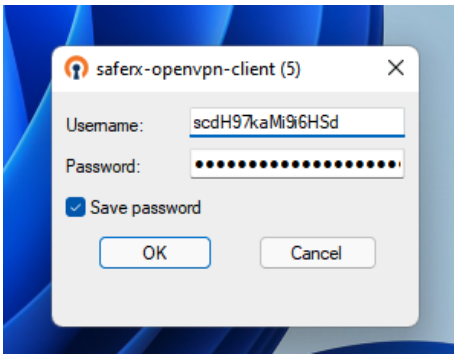


d. Select the downloaded file *saferx-openvpn-client.ovpn*

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 *6perimeter81$*, 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 138*.

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*.

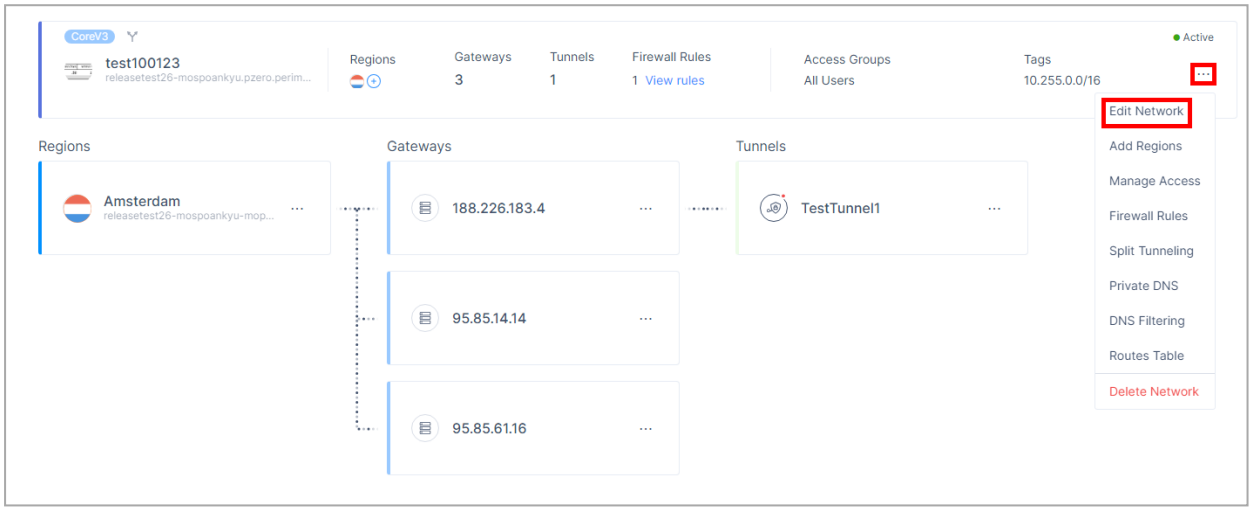
Verifying the Setup

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*.

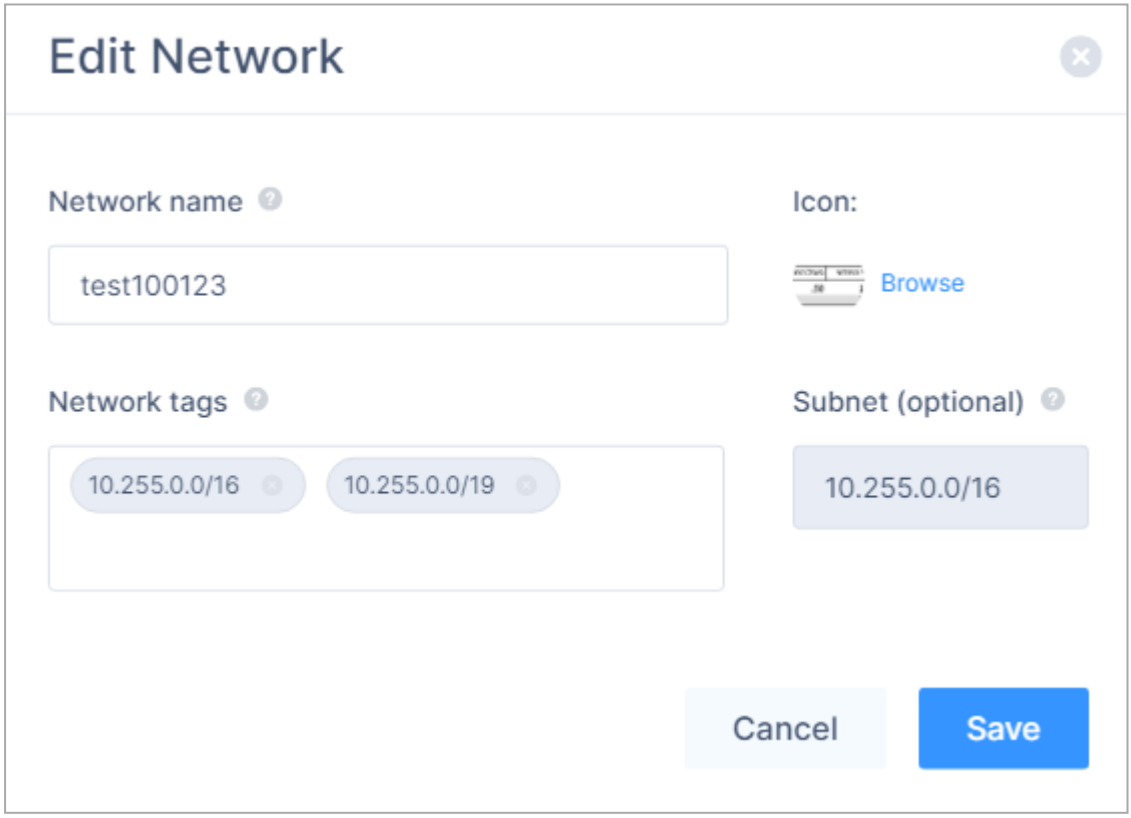
Managing a Network

Editing a Network

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



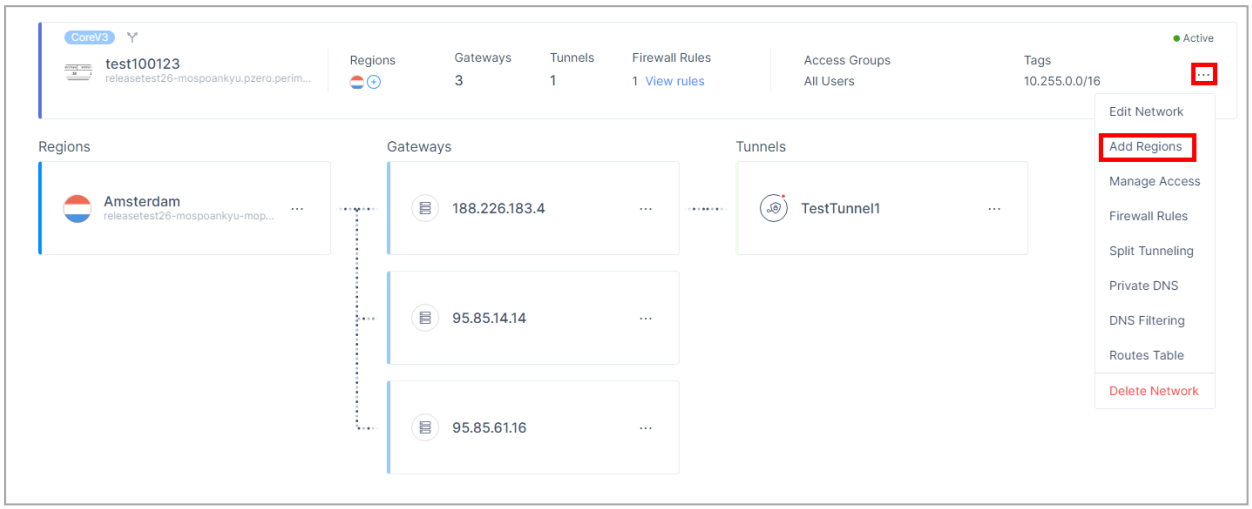
The **Edit Network** window appears.



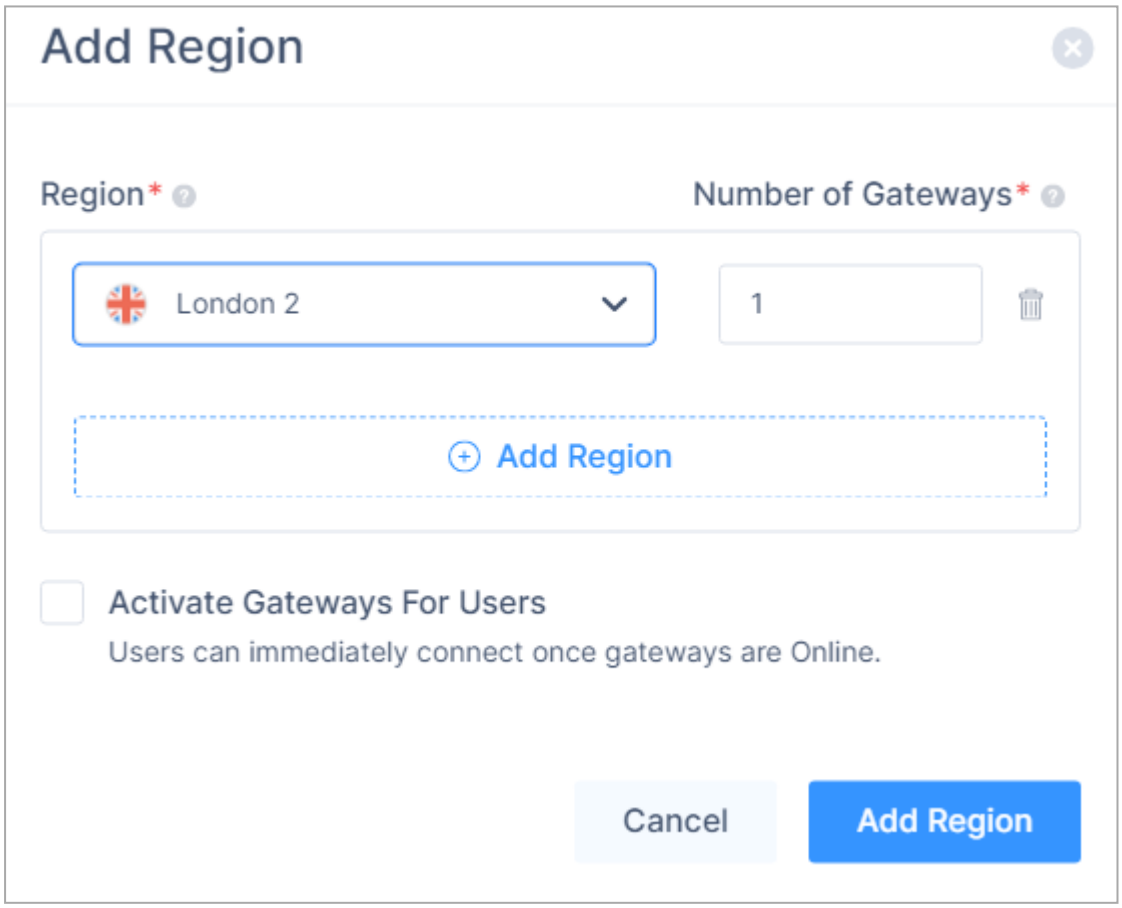
4. Make the required changes and click **Save**.

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.

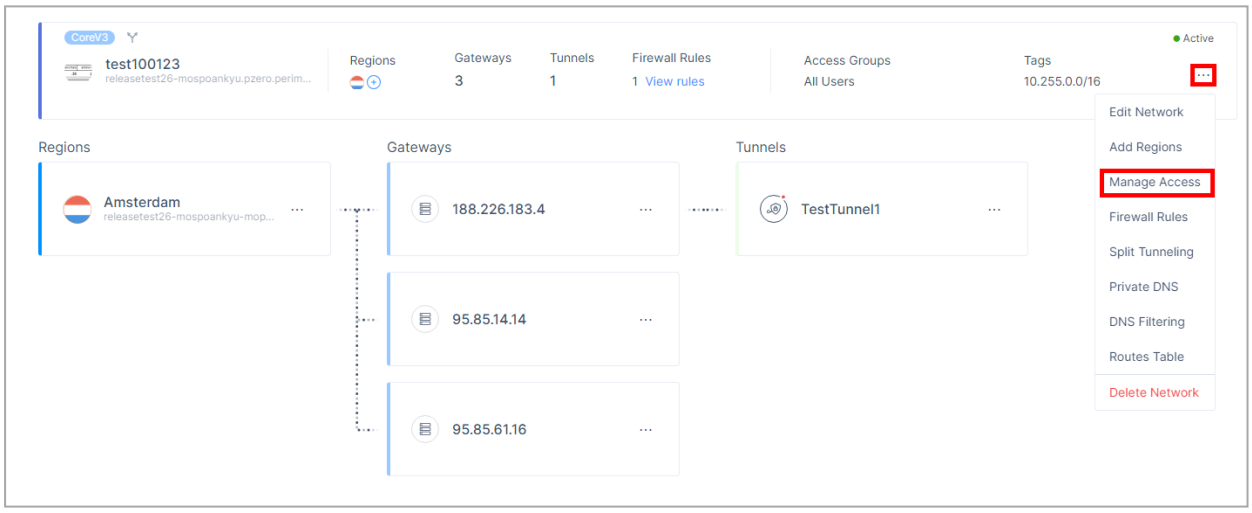
5. In the **Number of Gateways** field, enter the number of private gateways you want to deploy in the region.
6. To add another region, click **Add Region** and repeat steps 4 and 5.
7. To activate the gateway for users, select the **Activate Gateways For Users** checkbox.
8. Click **Add Region**.

Managing Access

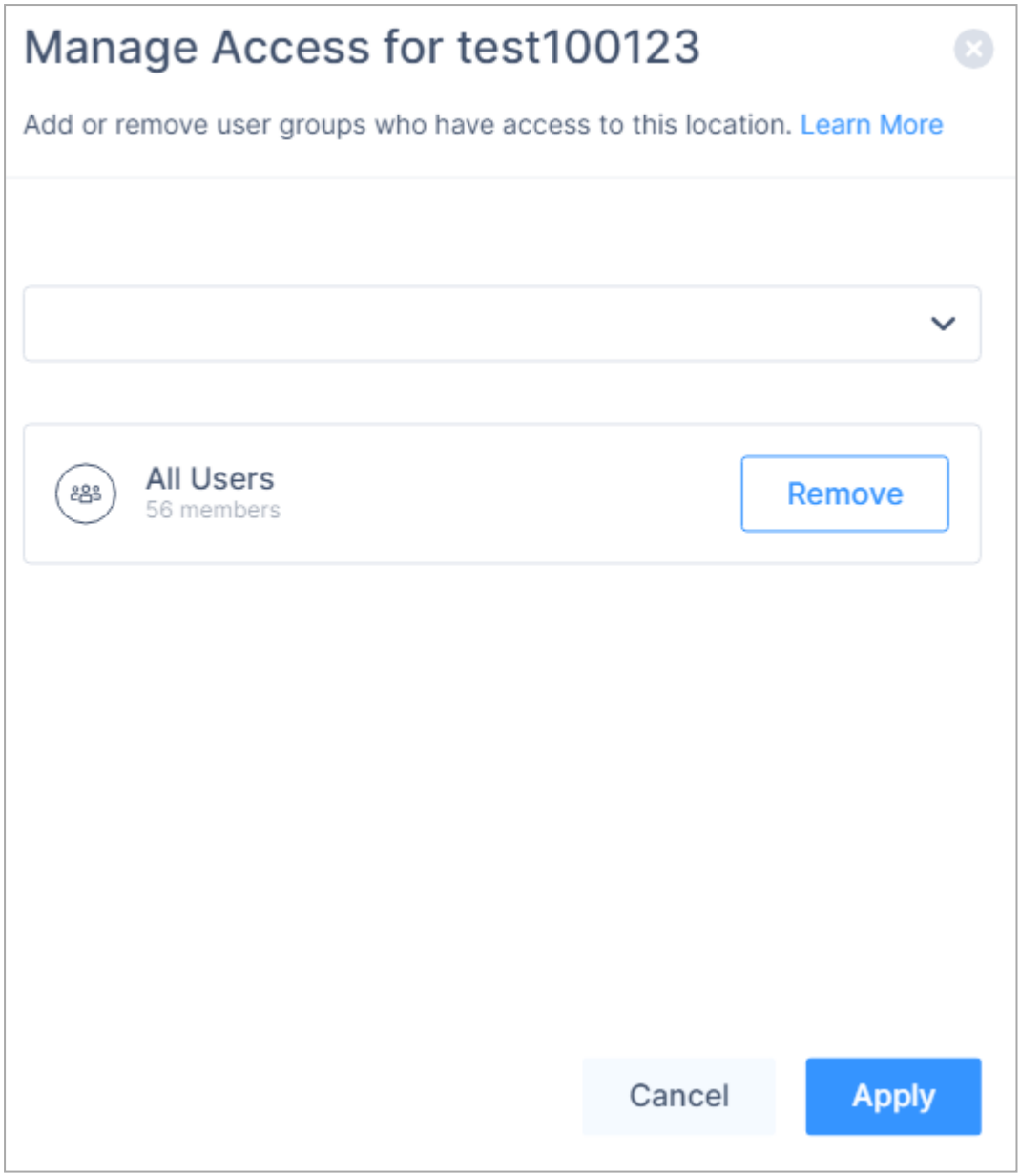
Manage Access allows you to select the member groups who can access the network.

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 605*.

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.

Private network traffic is always tunneled through the cloud, based on your network tunnels and routing table settings.

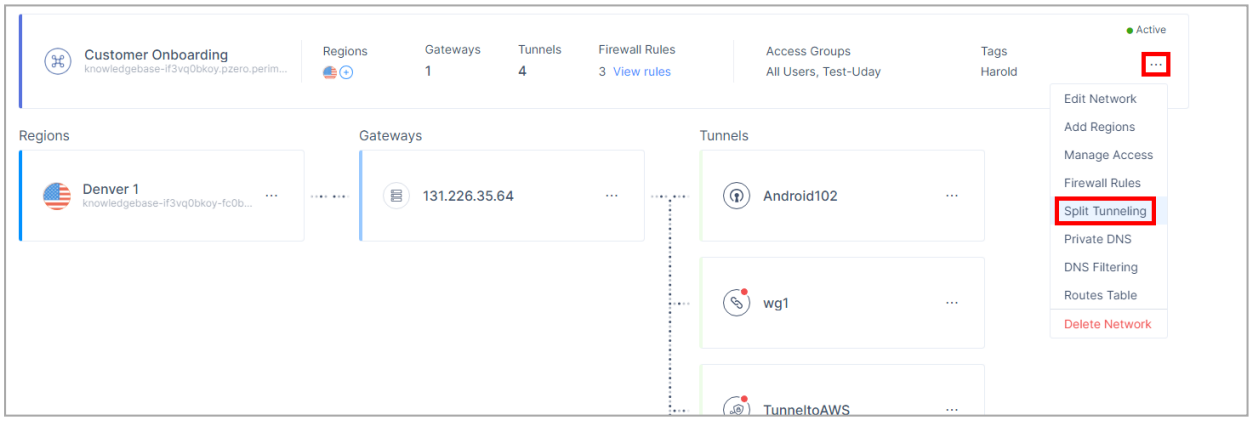
To route additional addresses through the Harmony SASE cloud, such as public cloud resources you wish to access through Harmony SASE using whitelisting, you must specify them manually.You also need to specify any addresses you want to exclude when routing all internet traffic through the tunnel.

Notes:

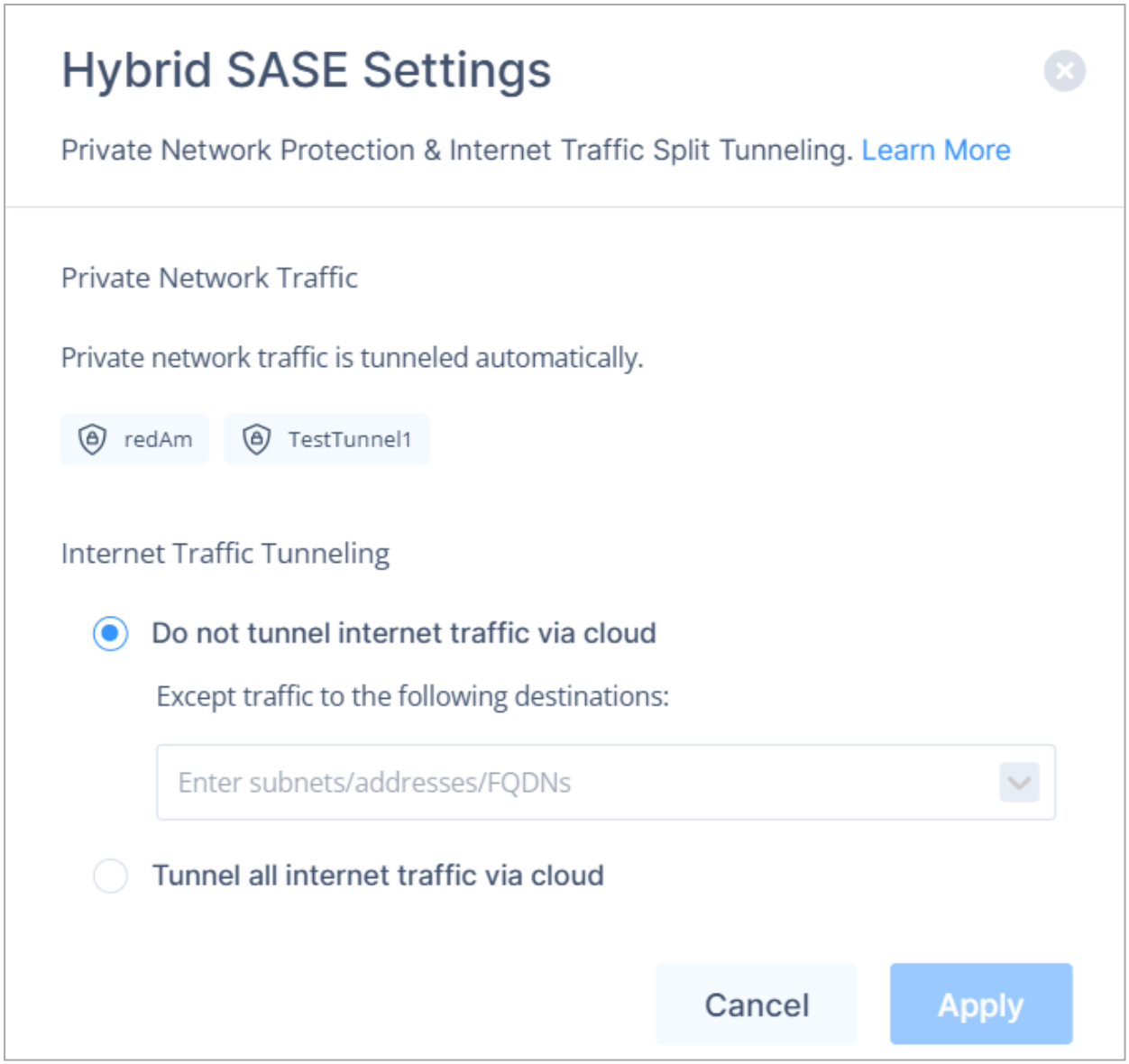
- Split tunneling by FQDN is supported only for Harmony SASE Agents 10.1.x and higher. With older agent versions, split tunneling by FQDN is ignored and reverts to full tunneling.
- The recommended setting is not to tunnel traffic internet through the cloud to minimize latency while keeping connectivity to private resources.

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 **Hybrid SASE Settings** window appears.



4. In the **Internet Traffic Tunneling** section, select one of these:

Item	Description
Do not tunnel internet traffic via cloud	Only private resources are tunneled through the VPN. All other traffic goes directly to the internet. This is the default setting. From the **Except traffic to the following destinations** list, select the addresses or IPs that should go through the tunnel.

Item	Description
Tunnel all internet traffic via cloud	All internet traffic is tunneled through the cloud, but you can exclude specific destinations from being tunneled. From the **Except traffic to the following destinations** list, select the addresses or IPs that should not go through the tunnel when all internet traffic is being tunneled.

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.

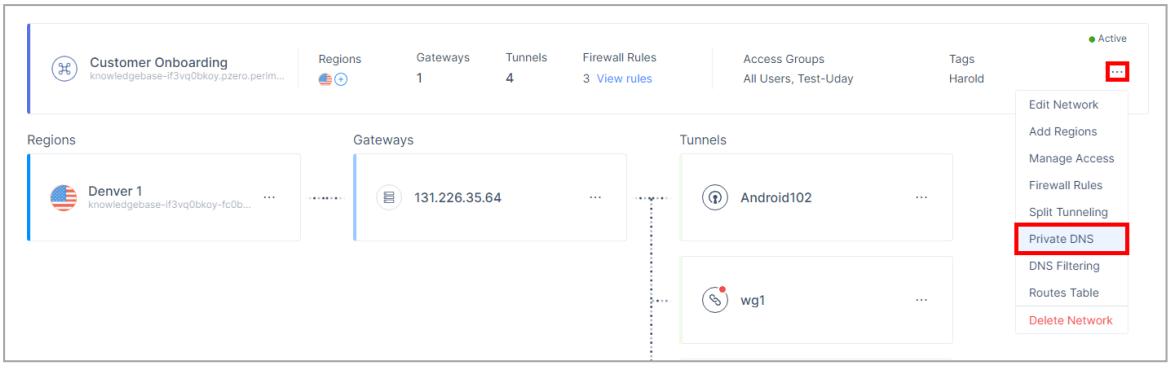
Notes -

- 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.

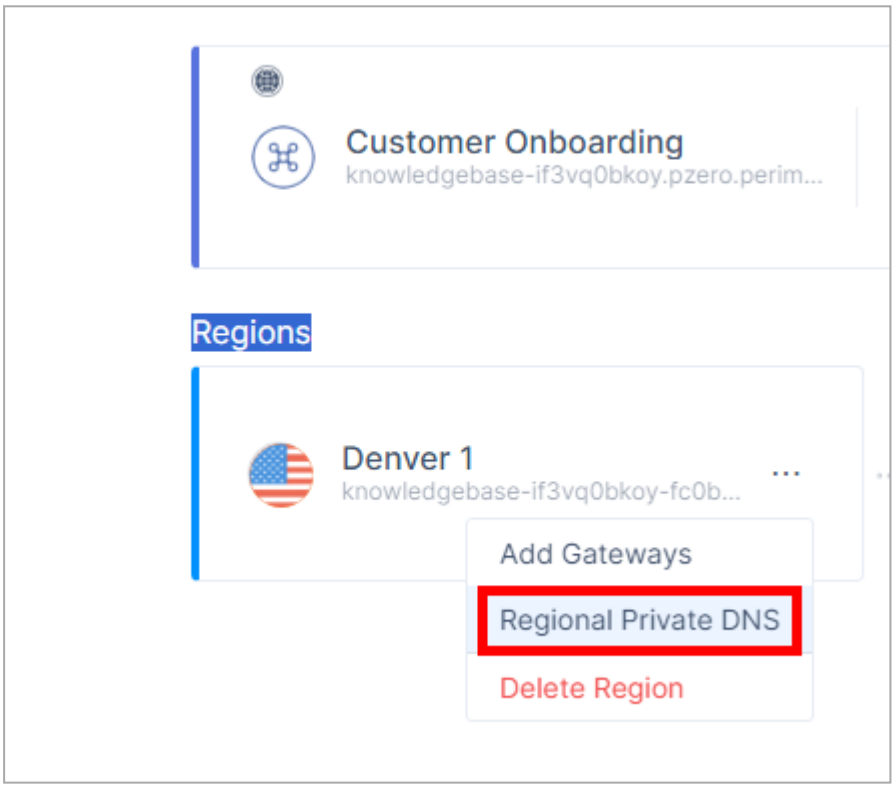
To configure a private DNS for a network:

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. To add a private DNS:

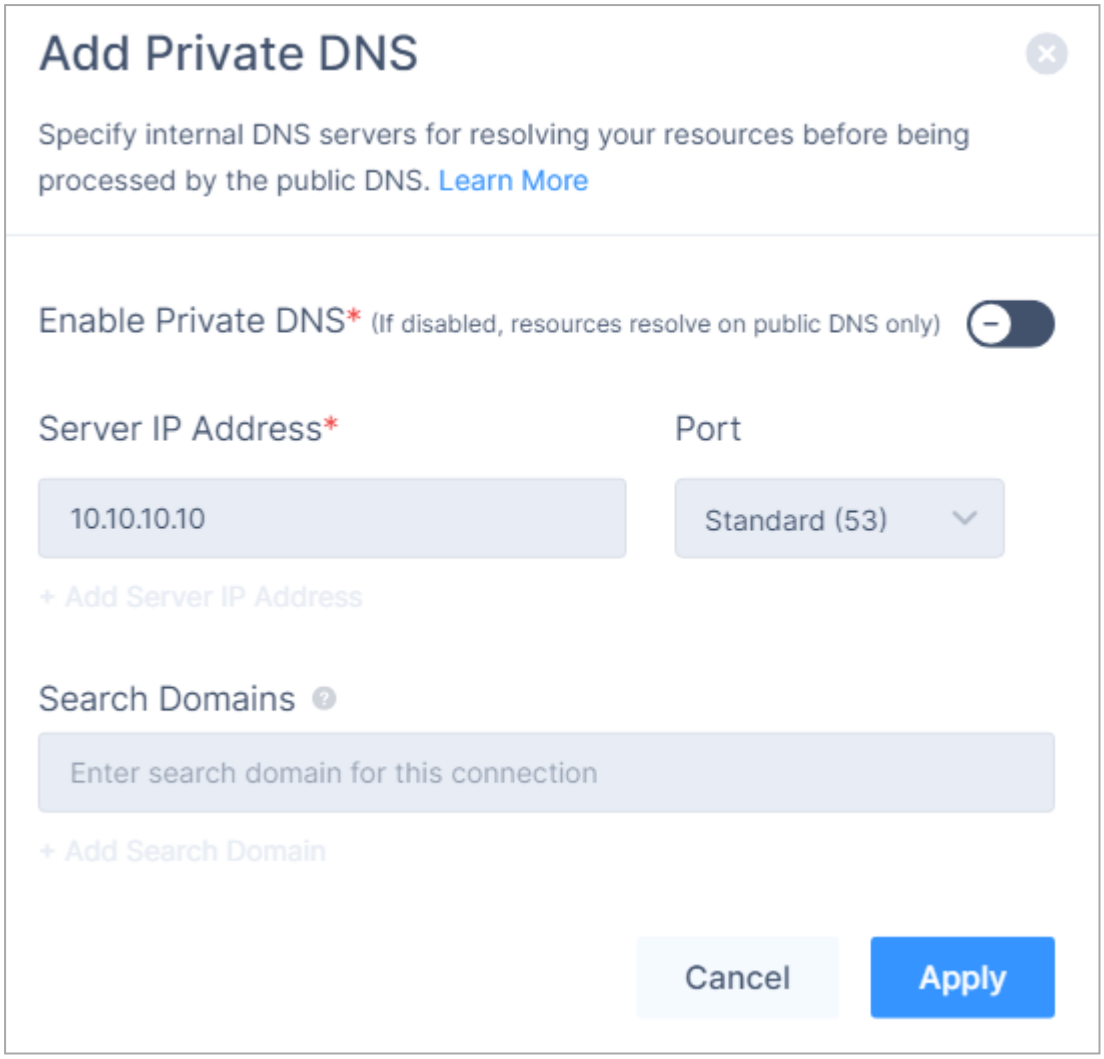
- For a network, click ··· and then click **Private DNS**.



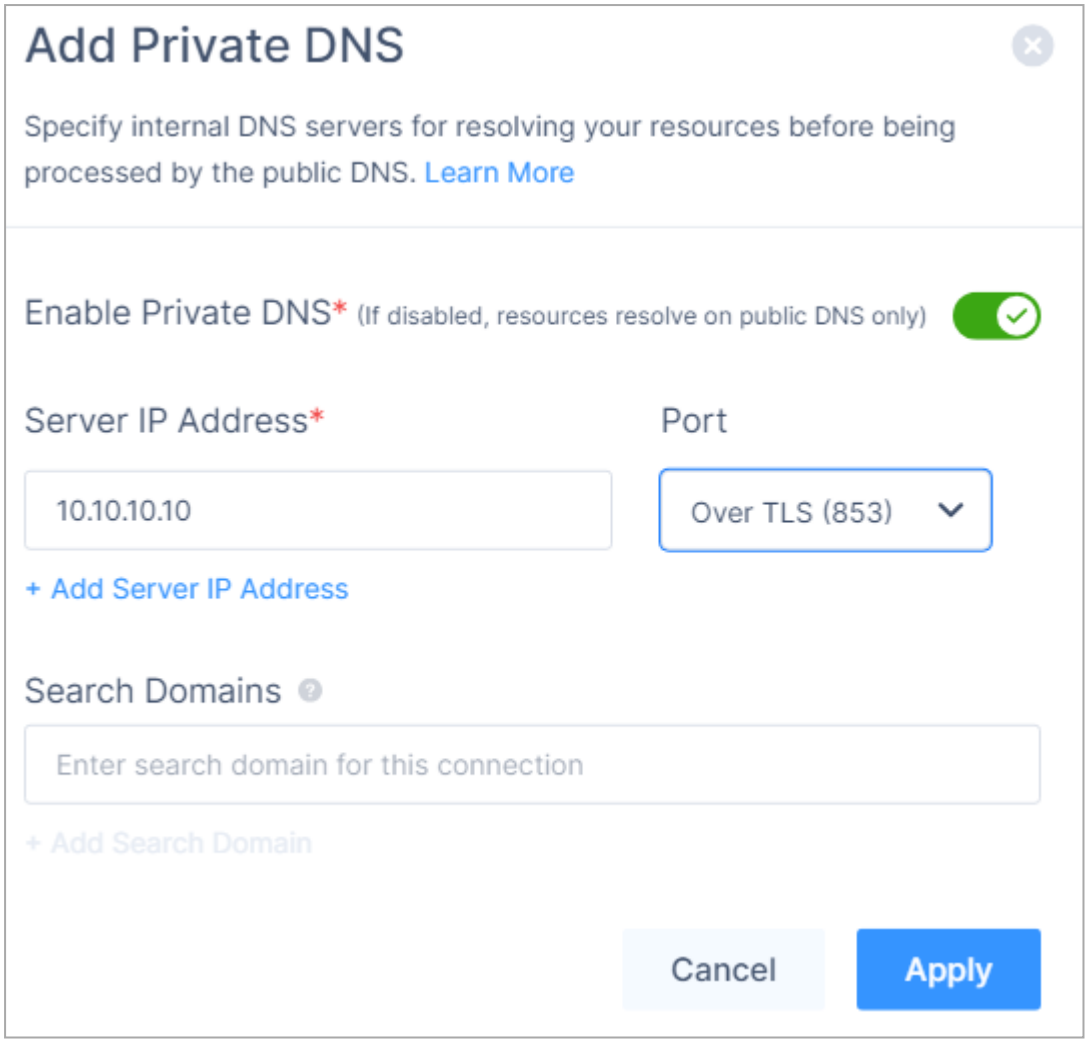
- For a region, in the **Regions** section, click ··· and then click **Regional Private DNS**.



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

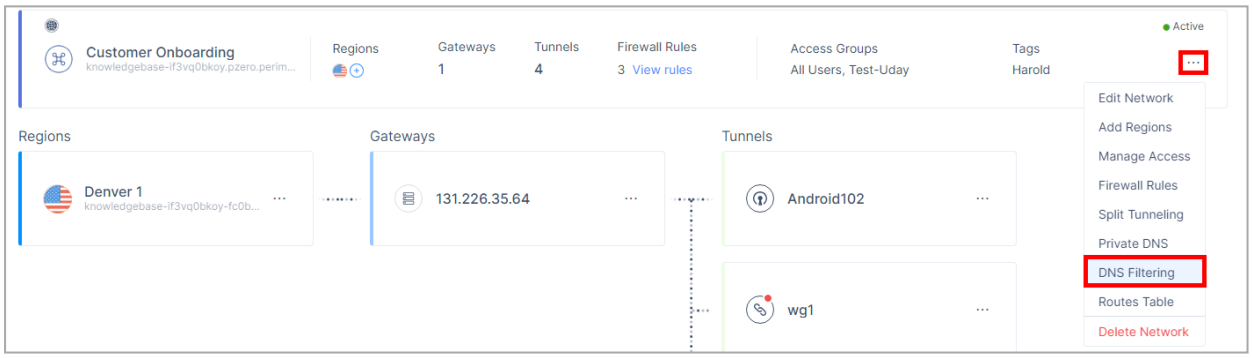
DNS Filtering allows you to manage internet access for members in your network by blocking or allowing websites using allow-list and block-list.

Best Practices -

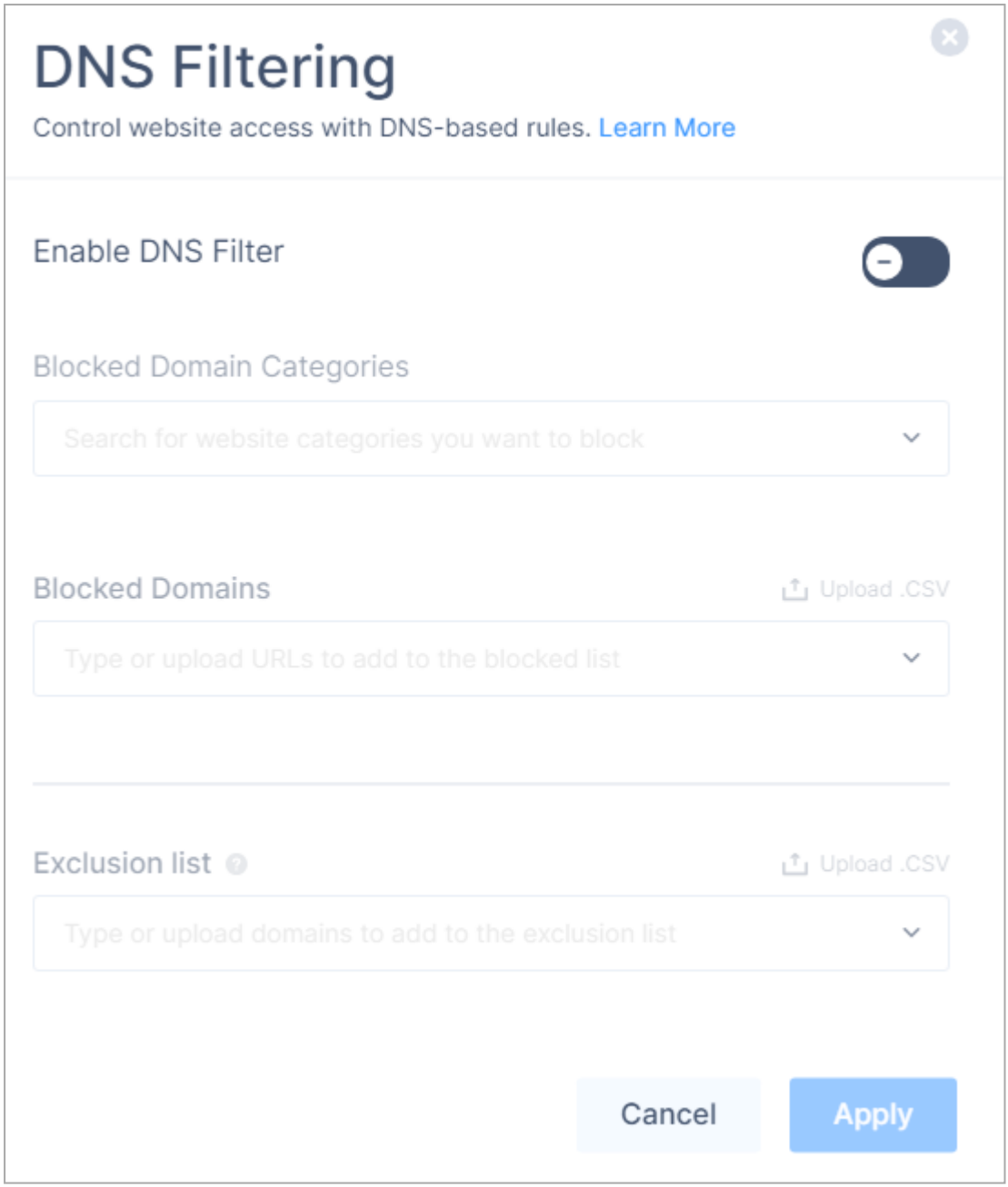
- Make sure that you have the list of URLs to block and allow.
- Make sure that the DNS filter settings work as expected.

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.

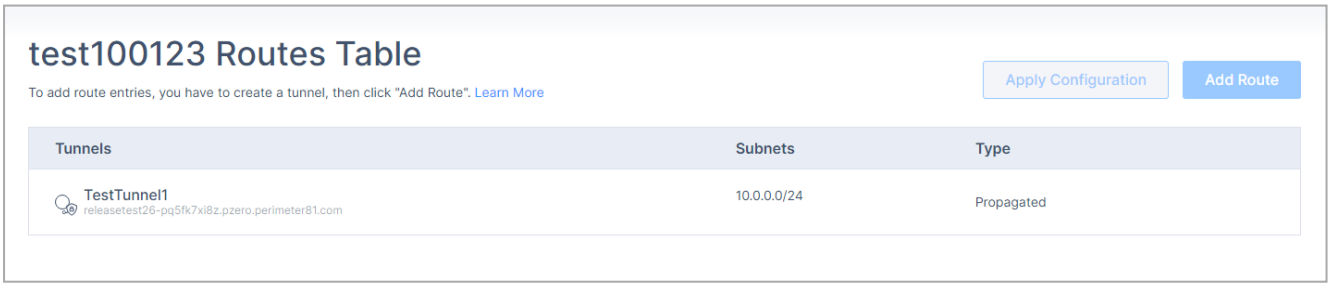
7. In the **Exclusion list** field, enter the URLs you want to exempt from the blocked domains list or upload a .CSV file with the domains.
8. Click **Apply**.

   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.

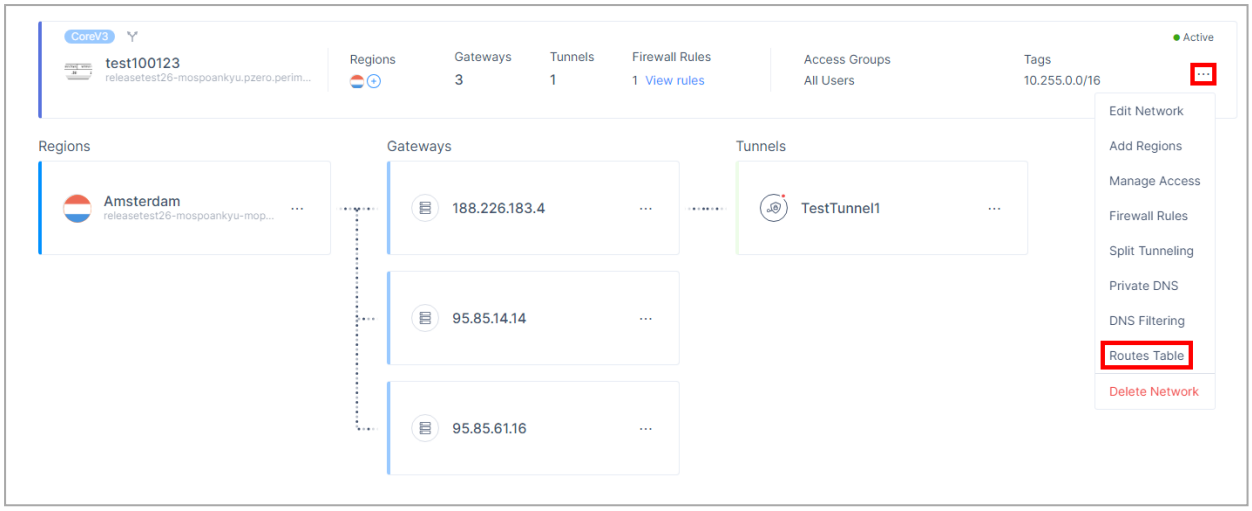
Routes Table

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

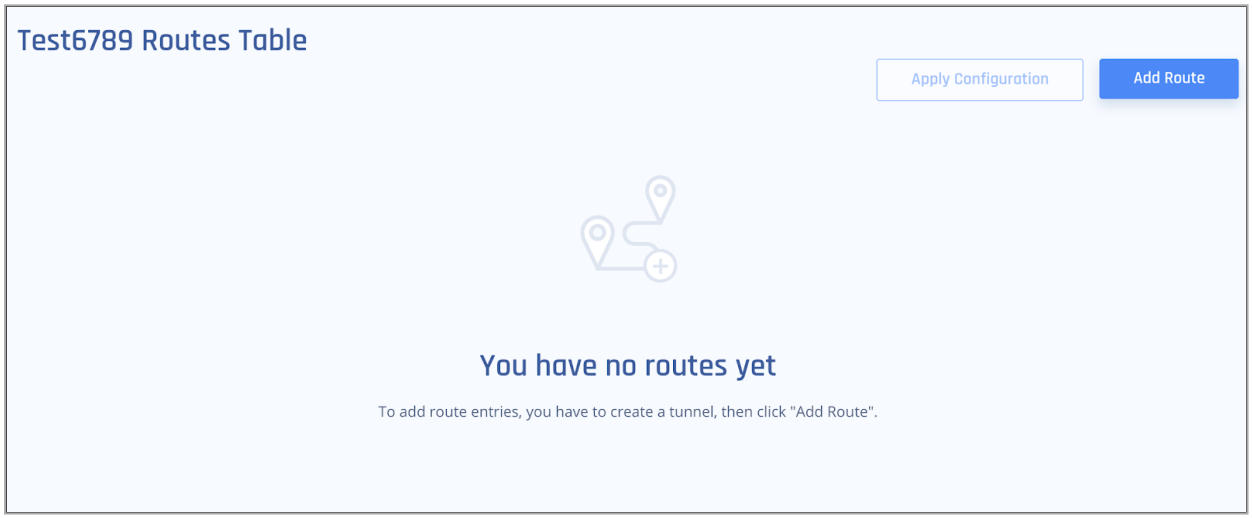


To add a new route to a tunnel in your network:

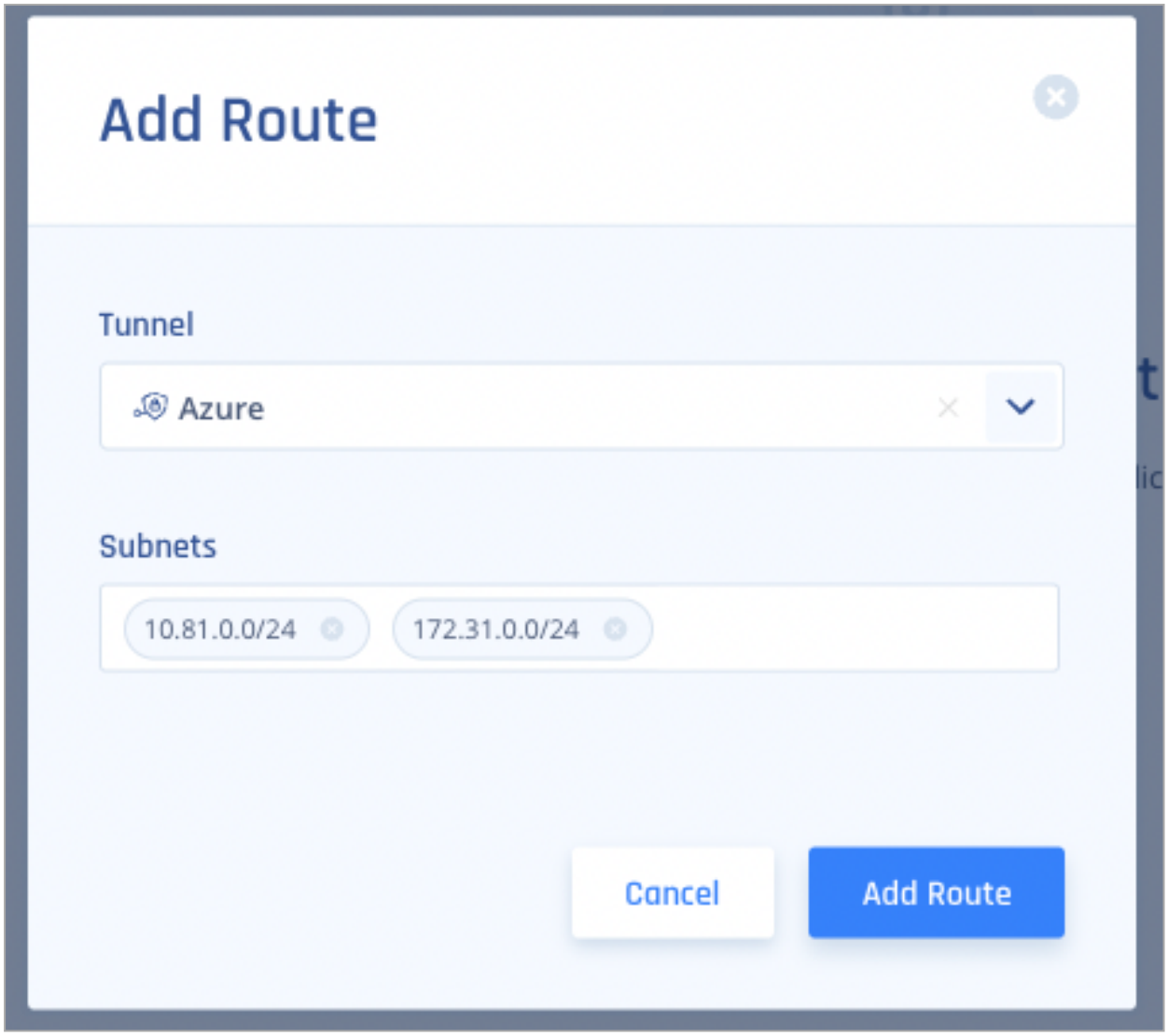
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· at the right end of the network and then select **Routes Table**.



4. Click **Add Route**.



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

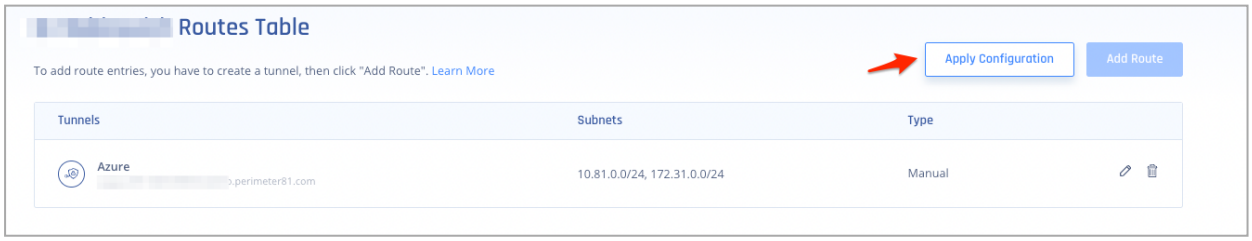


For cloud-based resources, enter these values for your vendor.

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

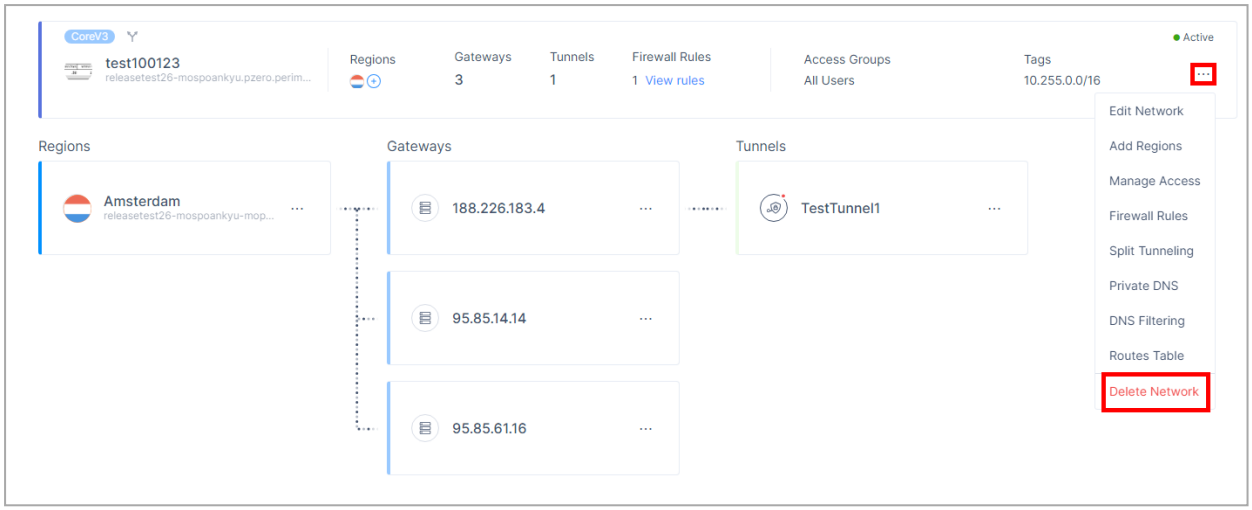
6. Click **Apply Configuration**.



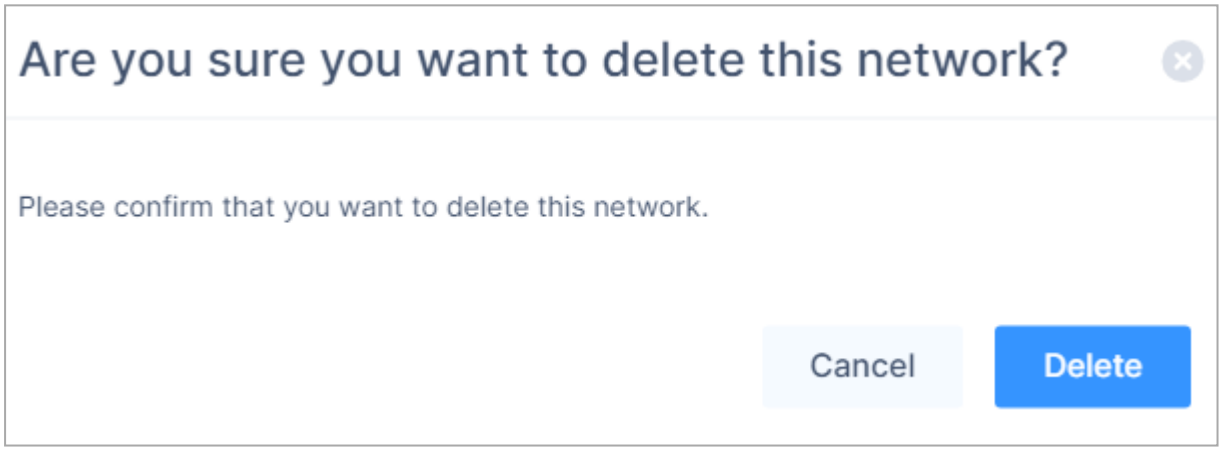
Deleting a Network

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

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



4. Click **Delete**.



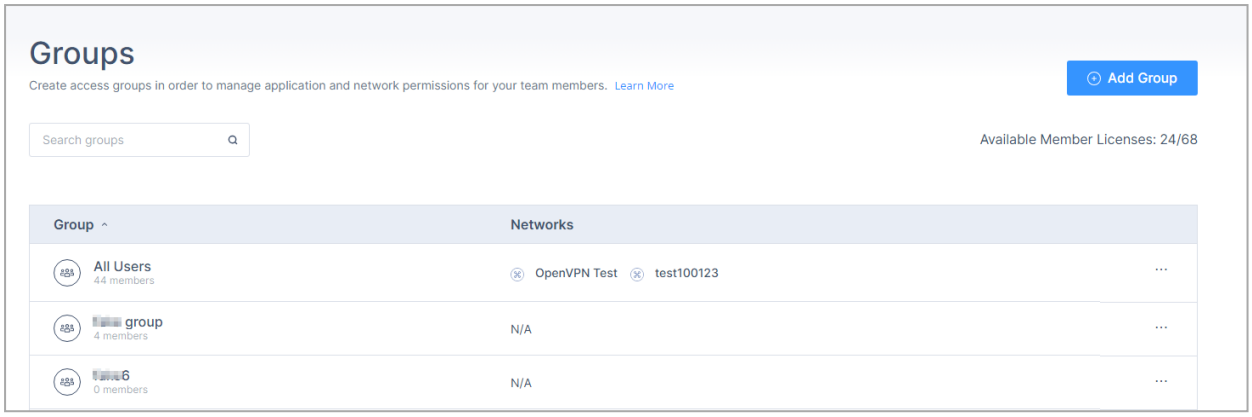
Segmenting Networks

Segmenting networks allows you to limit network access and provide customized member permissions. Harmony SASE uses Software-Defined Perimeter (SDP) to segment networks. For example, you can assign member groups to specific parts of a network or only to some of your SDPs.

To segment your network:

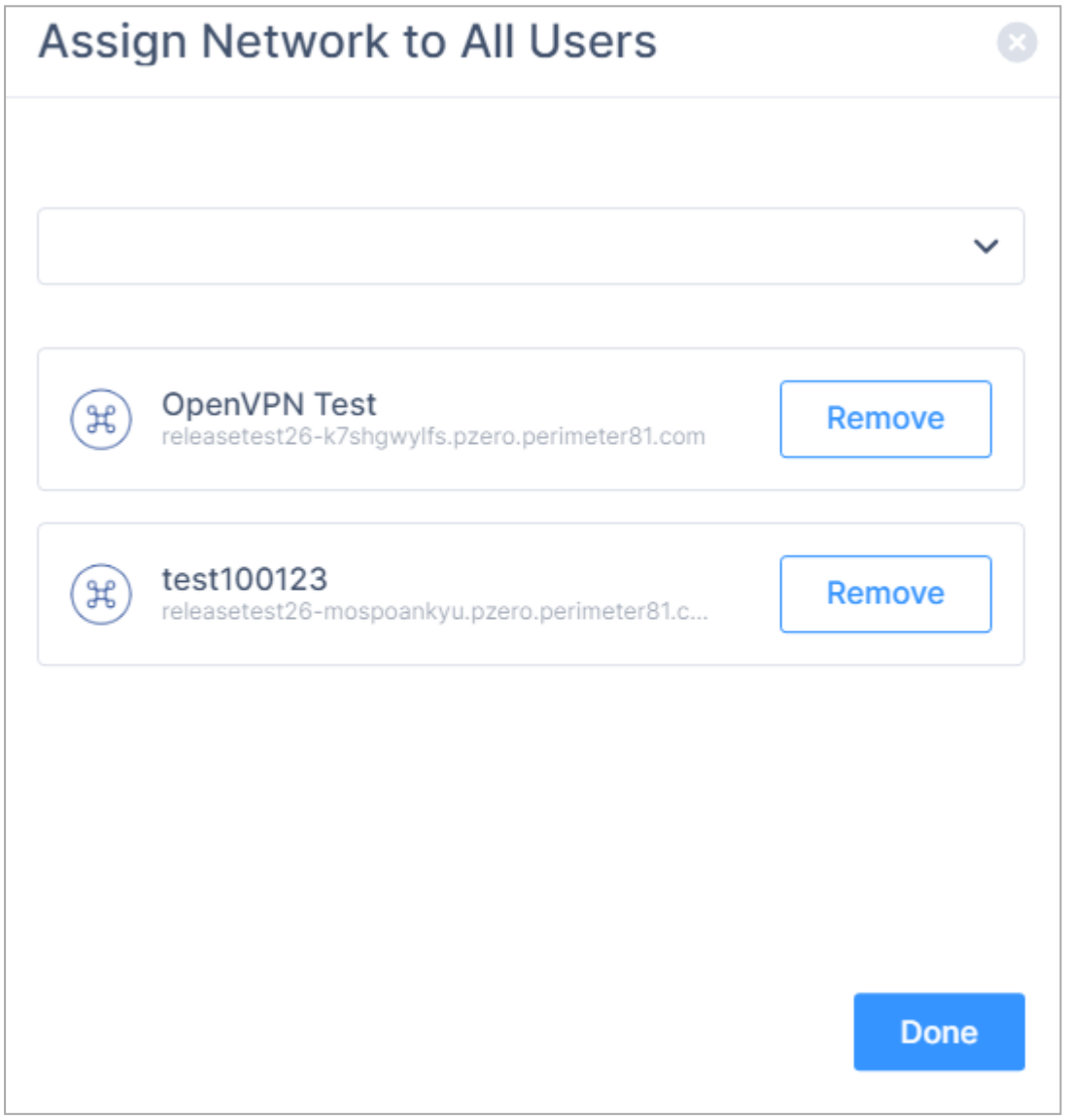
1. Access the Harmony SASE Administrator Portal and click **Team** > **Groups**.

   The **Groups** page appears.



2. Click ··· for the group you want to manage the network and then click **Manage Networks**.

   The **Assign Network to Group** window appears.



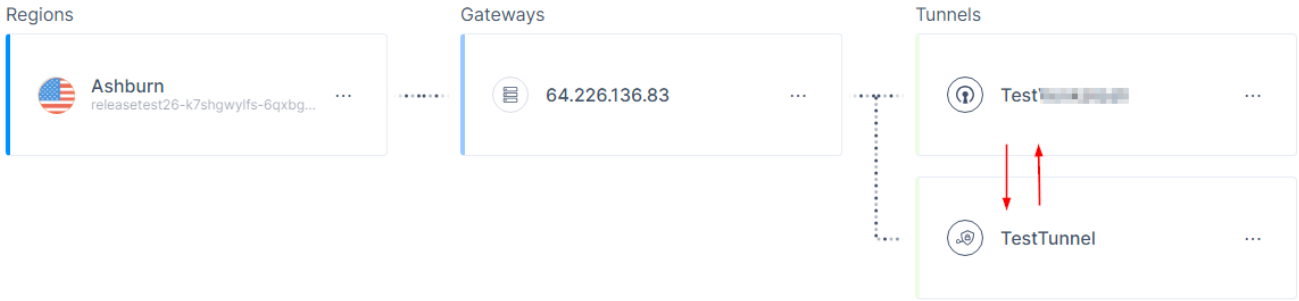
3. From the list, select the networks that the member group can access and click **Done**.

The members can access only the selected network locations when they log in to their client application.

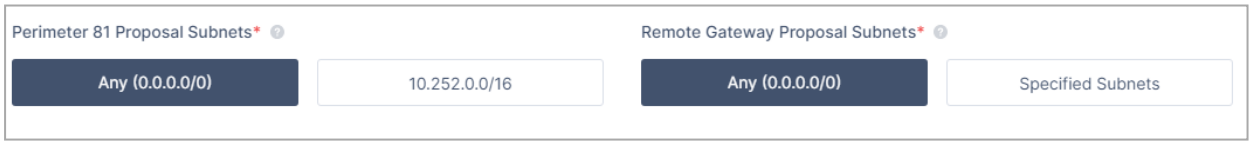
Interconnectivity (Cloud-Agnostic)

This chapter describes how to securely connect sites and cloud resources using Harmony SASE. When two sites are tunneled to your Harmony SASE network, they can securely communicate through this network without the Harmony SASE Agent.

IPSec Based Connections

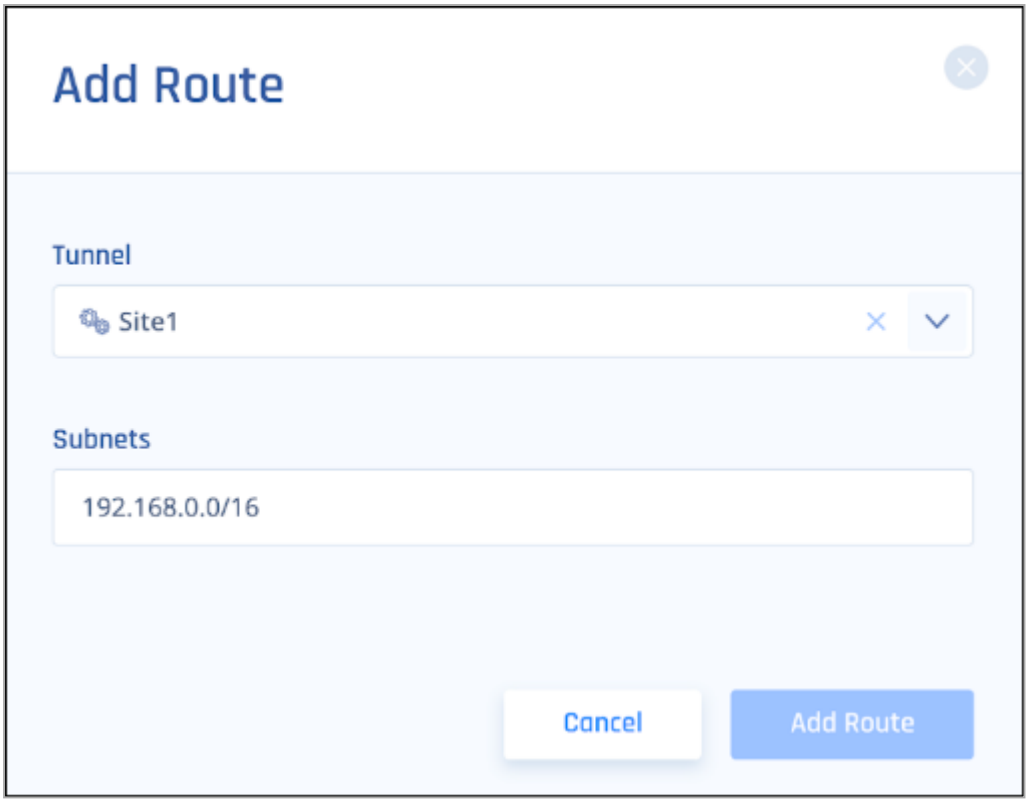


1. Make sure both tunnels are route-based. This means they do not rely on a specific internal subnet for a handshake between sites. Instead, a route is configured on each device's Route Table, to indicate which subnets to send through the tunnel.
2. In the Harmony SASE Administrator Portal, go to your network and set **Perimeter Proposal Subnets** and **Remote Gateway Proposal Subnets** to **ANY (0.0.0.0/0)** for both the tunnels.

   This may make the tunnel go down. Make sure the device you use supports route-based VPN. This means the tunnel is set up to **0.0.0.0/0** and a route is added separately.
3. Make sure the **Routes Table** in the Harmony SASE side has the routes of all of the configured sites.

   To add **Routes Table**, see Adding a route. In the **Subnets** field, add the routing to the internal LAN subnets behind each tunnel.



4. Go to the first site's Routes Table (Site1) and add a route to direct the traffic to the second site's LAN subnet, in addition to the route that indicates all Harmony SASE subnets (usually 10.255.0.0/16) to go through the IPSec Site-2-Site tunnel.
5. Go to the second site's Routes Table (Site2), and set up a static route for both the Harmony SASE LAN Subnet and Site1's LAN subnet to go through the IPSec Site-2-Site tunnel.

Policy-based IPSec Tunnels

To achieve interconnectivity in a Policy-based Site-to-Site environment:

1. Go to the first site's Routes Table (Site1), and ensure that there are two Phase II tunnels:
   - One from Site1's internal subnet to Harmony SASE's subnet.
   - Another from Site1's internal subnet to Site2's internal subnet.
2. Go to the second site's Routes Table (Site2), and ensure that there are two Phase II tunnels:
   - One from Site2's internal subnet to Harmony SASE's subnet.
   - Another from Site2's internal subnet to Site1's internal subnet.

Note - As this feature is not supported by most of the routers, Check Point recommends to use Route-based IPSec tunnels.

WireGuard Connector Based Connections

To establish a connection from one resource to another, you must reinstall the connector, as the default installation (Accessor mode) does not allow it.

1. Uninstall the connector.
   - Ubuntu

     ```
     # Locate the WireGuard packages (the output of this command
     is the full package name)
     dpkg -l | grep wireguard

     # Delete all packages found that are associated with
     WireGuard (replace pkg with the output from the previous
     command)
     apt-get remove --purge pkg
     ```

   - CentOS

     ```
     # Locate the WireGuard packages (the output of this command
     is the full package name)
     yum list installed | grep wireguard

     # Delete all packages found that are associated with
     WireGuard (replace pkg with the output from the previous
     command)
     yum remove pkg
     ```

2. Reboot the machine and execute the connector installation script (the curl command copied from the Harmony SASE Administrator Portal). For more information, see *"Installing the WireGuard Connector on a Linux Server" on page 135*.
3. At Stage 4, select **NO (n)**, which prevents access or mode installation.
4. To ensure that the default route for the Linux machine is not modified, select **N** for `"Do you want to route whole traffic through connector tunnel? [Y/N]"`.

   Note - In Full Tunnel Mode, the site's entire traffic is sent through the WireGuard connector and the entire firewall is placed behind the Harmony SASE secure network. To operate in this mode:
   a. Select **Y** to override the default route on the machine and forward the traffic through the connector.
   b. Ensure that the Router/Firewall on the network sends all of the route's traffic(0.0.0.0/0) through the internal IP of the WireGuard connector. Follow the instructions below if Linux machine is the router.

5. For `Do you want to enable IP forwarding (router mode)? [Y/N]:`
   - If the Linux server is acting as a firewall, router, or NAT device, select **Y**.
   - For any other device, select **N**.
6. Open the Route Table of the network in which the WireGuard connector is installed (usually your router or firewall).
7. Configure a static route to direct the traffic from your Harmony SASE LAN subnet (10.XXX.0.0/16) and your other desired remote subnet to the IP address of the machine hosting the connector.

   Open the Linux machine terminal that hosts the connector and run:

```
# Temporarily shut the connector down
wg-quick down wg0
# Open the connector's route table.
vi /etc/wireguard/wg0.conf
# Enter the subnets of the resources you'd like to communicate
with each other
set AllowedIPs = <Harmony SASE Subnet>, <Site1 Subnet>,< Site 2
Subnet>
# Turn the connector up
wg-quick up wg0
# Make sure that the desired change has taken place
wg show
```

Interconnectivity Using AWS EC2 Instance

For WireGuard connector installed over AWS EC2 instance, you must disable the source/destination checks.

To disable source/destination checks:

1. Log in to Amazon EC2 console.
2. In the navigation pane, click **Instances** and select the relevant instance.
3. Select **Actions**, **Networking**, **Change source/destination check**.
4. For **Source/destination checking** , select **Stop**.
5. Click **Save**.
6. If the instance has a secondary network interface:
   a. Go to **Networking** tab > **Network interfaces** and select the secondary network interface.

b. Select the interface ID and go to the **Network Interfaces** page.

c. Select **Actions**, **Change source/dest. check**.

d. Clear the **Enable** checkbox.

e. Click **Save**.

Integrating On-premises Firewall / Router or Cloud based Resources

High-Level Procedure

1. Make sure you have the required prerequisites.
2. For on-premises firewall and routers:

a. Configure the tunnel in the Harmony SASE Administrator Portal.

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

On-premises	
Firewall	**Router**
▪ *"Barracuda Firewall" on page 181* ▪ *"Check Point Firewall" on page 191* ▪ *"Cisco Firepower" on page 201* ▪ *"Configuring Check Point Cluster VIP Redundant IPsec Tunnel" on page 221* ▪ *"Configuring Check Point Redundant IPsec Tunnel" on page 246* ▪ *"Cisco ASA Firewall" on page 271* ▪ *"Cisco Meraki Router" on page 375* ▪ *"FortiGate Next Generation Firewall" on page 305* ▪ *"Juniper Networks ScreenOS Firewall" on page 309* ▪ *"Juniper (JunOS) SRX Firewall" on page 315* ▪ *"Palo Alto Firewall" on page 328* ▪ *"pfSense Firewall" on page 335* ▪ *"SonicWall Firewall" on page 341* ▪ *"Sophos XG Firewall" on page 351* ▪ *"UniFi USG Firewall" on page 357* ▪ *"WatchGuard Firewall" on page 363* ▪ *"Zyxel USG Firewall" on page 369*	▪ *"Cisco Meraki Router" on page 375* ▪ *"D-Link DSR Series Router" on page 378* ▪ *"DrayTek Vigor2862 Router" on page 385* ▪ *"DrayTek Vigor3900 Router" on page 388* ▪ *"EdgeMax Router" on page 395* ▪ *"Linksys Router" on page 397* ▪ *"Netgear BR500 Router" on page 401*

3. For cloud-based resource, configure any of these:

Single Tunnel

- *"AWS Virtual Gateway" on page 424*
- *"AWS Transit Gateway" on page 443*
- *"Google Cloud Platform" on page 556*
- *"Azure Virtual Network Gateway" on page 491*

Redundant Tunnels

- *"AWS Redundant Tunnels - Virtual Private Gateway" on page 460*
- *"AWS Redundant Tunnels - Transit Gateway" on page 474*
- *"Google Cloud Platform (GCP) Redundant Tunnels" on page 568*
- *"Azure Virtual Network Gateway Redundant Tunnels" on page 517*
- *"Azure Virtual WAN Redundant Tunnels" on page 535*

Other Cloud Options

- *"Alibaba Cloud" on page 415*
- *"Heroku Enterprise" on page 590*
- *"IBM Cloud" on page 591*

---

4. Verify the setup.

Prerequisites

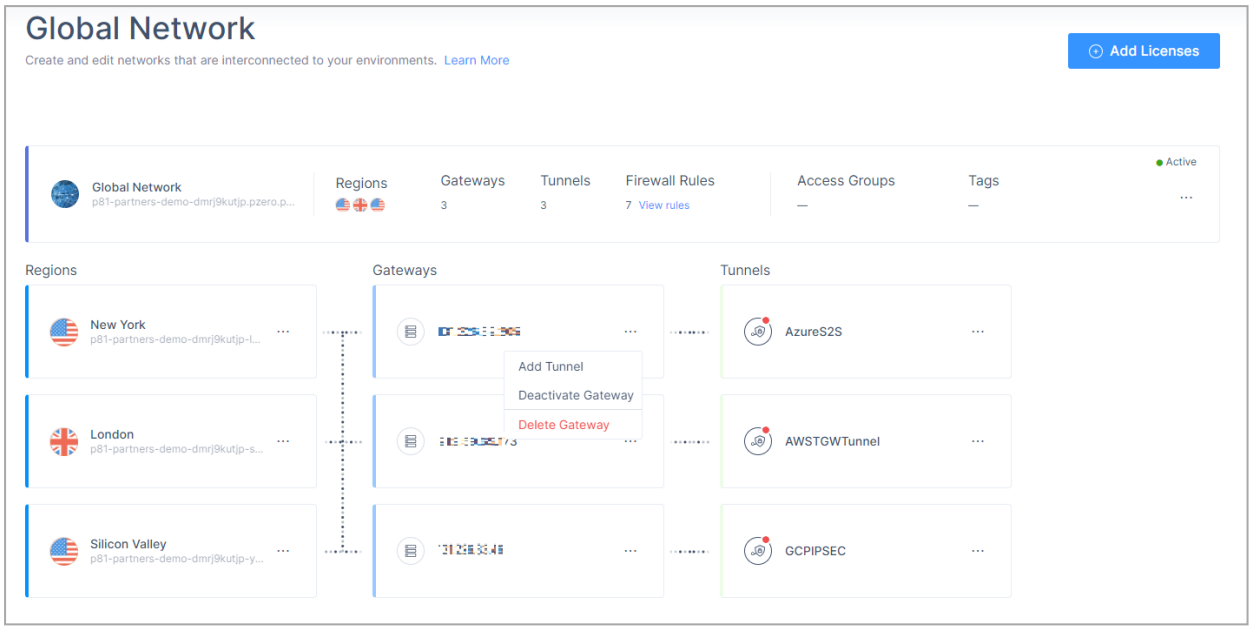
- Harmony SASE Administrator Portal account.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account with the Firewall/Router/Cloud Management Portal.

Configuring the Tunnel in the Harmony SASE Administrator Portal

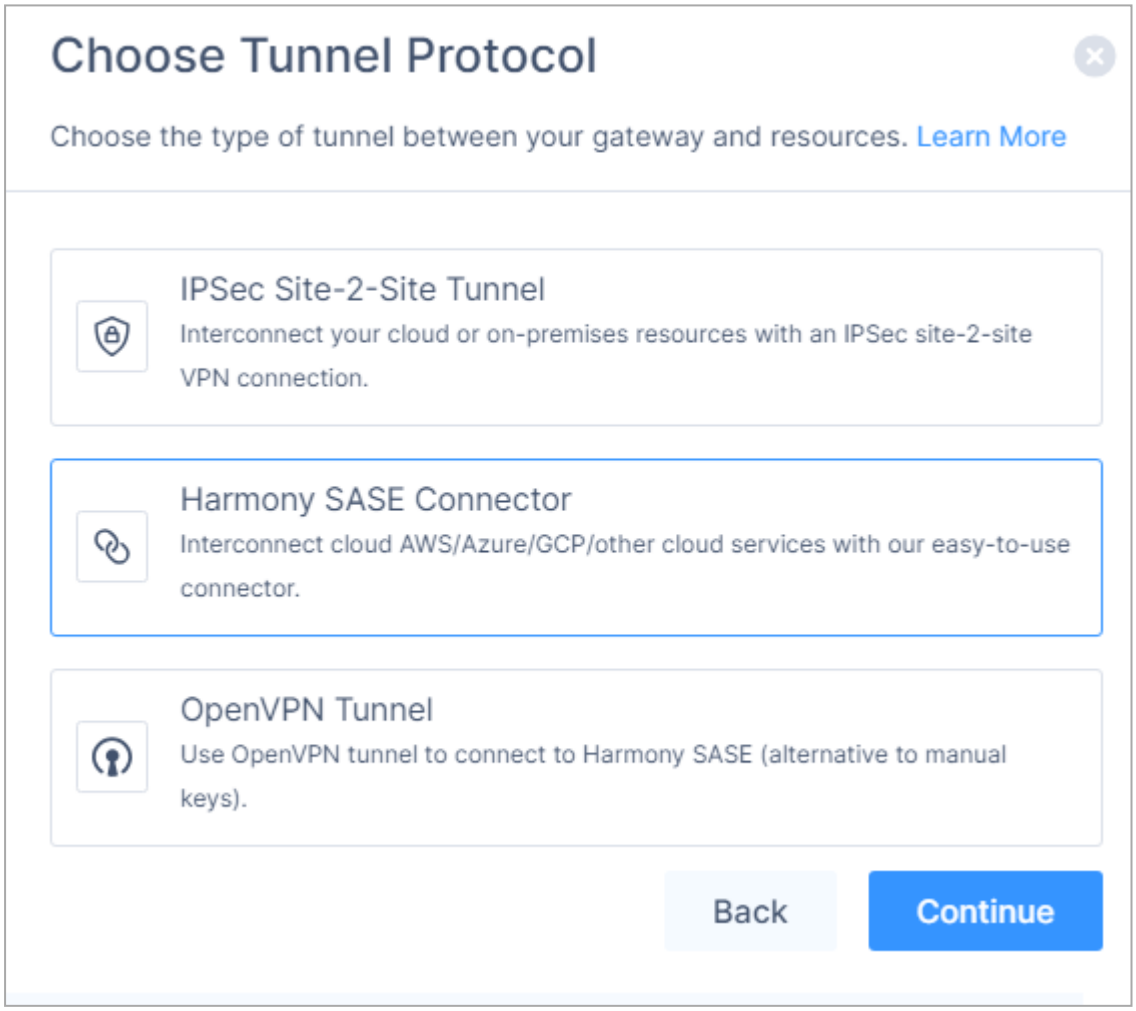
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.

3. Click ··· and select **Add Tunnel** for the gateway from which you want to add the IPSec Site-to-Site VPN tunnel.

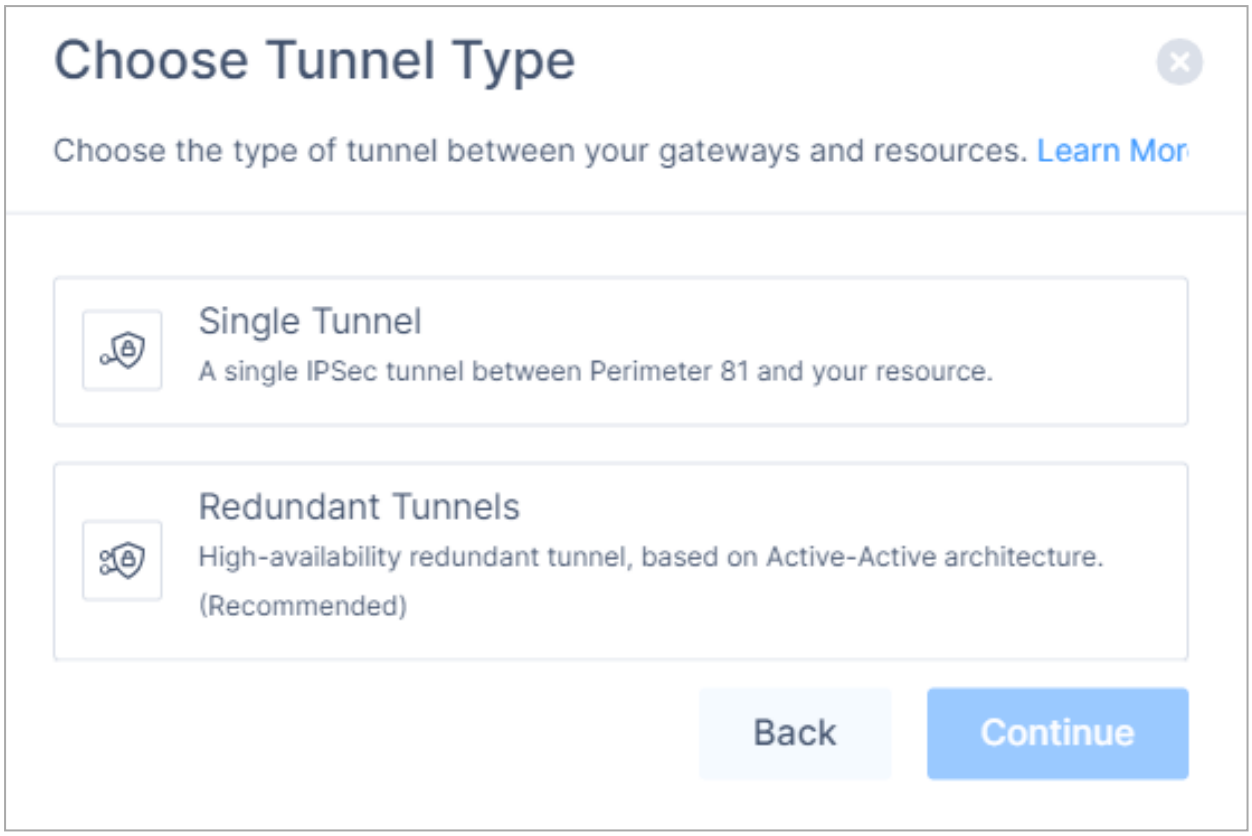
Note - Only a single dynamic IP IPSec tunnel is supported per each Cloud Gateway.



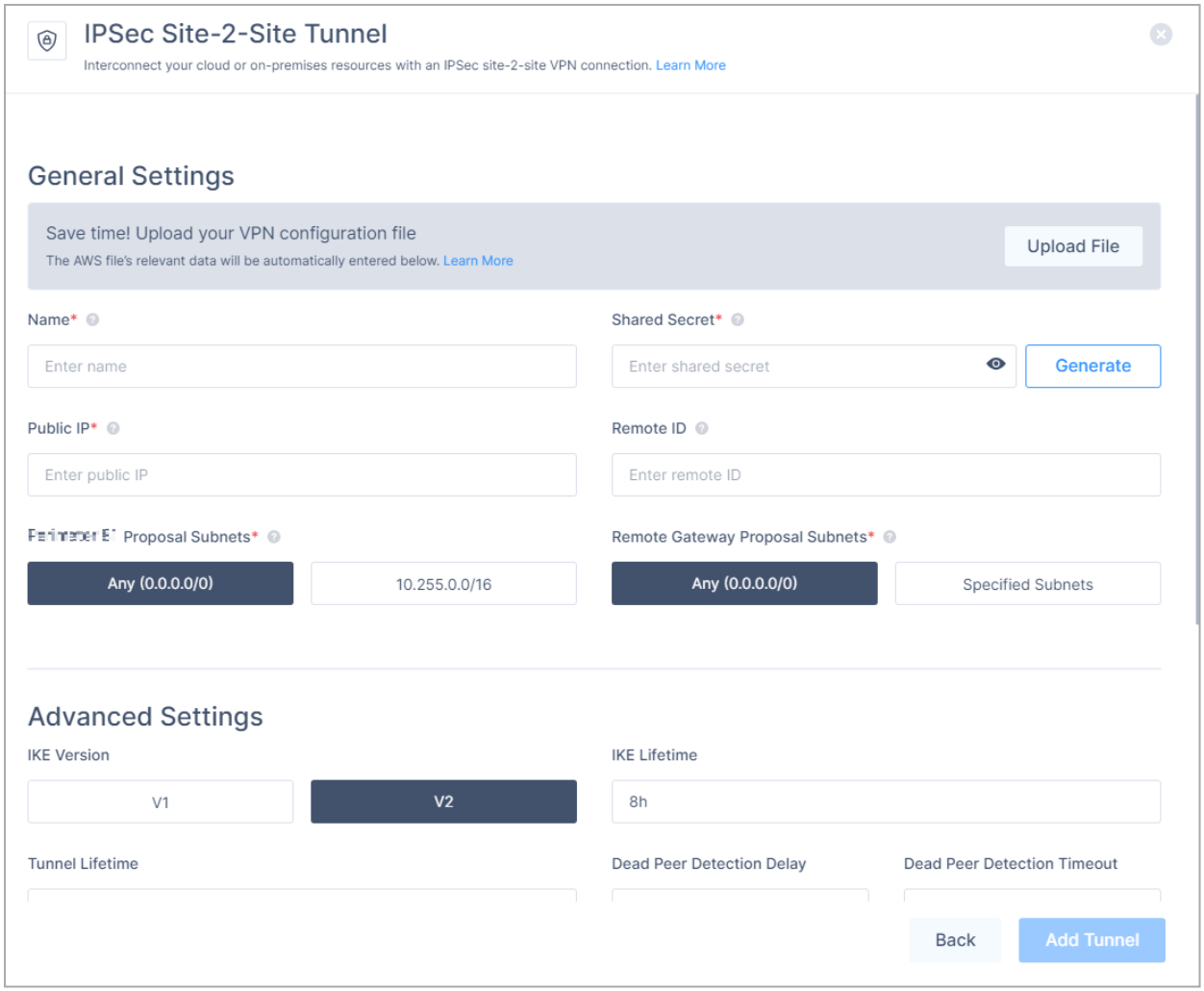
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



6. In the **General Settings** section, enter the relevant details:



Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Harmony SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"Barracuda Firewall" on page 181	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Barracuda Firewall Public WAN IP address.	Barracuda Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Barracuda internal LAN subnets.
"Check Point Firewall" on page 191	Name for the tunnel.	Enter the secret key specified in Check Point SmartConsole or click **Generate** to generate it.	Public or Egress IP address of Check Point Firewall	Public or Egress IP address of Check Point	Any (0.0.0.0)	Any (0.0.0.0)
"Cisco ASA Firewall" on page 271	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Cisco ASA Firewall Public WAN IP address.	Cisco ASA Firewall Public WAN IP address.	Any (0.0.0.0)	Any (0.0.0.0)

Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Harmony SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"Cisco Meraki Router" on page 375	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Cisco Meraki Router Public WAN IP address.	Cisco Meraki Router Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Cisco Meraki internal LAN subnets.
"D-Link DSR Series Router" on page 378	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	D-Link DSR Series Router Public WAN IP address.	D-Link DSR Series Router Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	D-Link DSR Series Router internal LAN subnets.
"DrayTek Vigor2862 Router" on page 385	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	DrayTek Vigor3900 Router Public WAN IP address.	DrayTek Vigor3900 Router Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	DrayTek Vigor internal LAN subnets.
"DrayTek Vigor3900 Router" on page 388	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	DrayTek Vigor2862 Router Public WAN IP address.	Name for the VPN profile on the DrayTek Vigor2862 Router.	Harmony SASE network subnet. The default is 10.255.0.0/16.	DrayTek Vigor internal LAN subnets.
"EdgeMax Router" on page 395	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	EdgeMax Router Public WAN IP address.	EdgeMax Router Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	EdgeMax internal LAN subnets.
"FortiGate Next Generation Firewall" on page 305	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	FortiGate Next Generation Firewall public IP address.	FortiGate Next Generation Firewall remote ID.	Harmony SASE network subnet. The default is 10.255.0.0/16.	FortiGate Next Generation Firewall internal LAN subnets.
"Linksys Router" on page 397	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Linksys public WAN IP address.	Linksys public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Linksys internal LAN subnets.
"Juniper Networks ScreenOS Firewall" on page 309	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Juniper Networks ScreenOS Firewall Public WAN IP address.	Juniper Networks ScreenOS Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Juniper Networks ScreenOS internal LAN subnets.
"Juniper (JunOS) SRX Firewall" on page 315	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Juniper SRX Firewall Public WAN IP address.	Juniper SRX Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Juniper Networks ScreenOS internal LAN subnets.

Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Harmony SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"Netgear BR500 Router" on page 401	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Netgear BR500 Router Public WAN IP address.	Netgear BR500 Router Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Netgear BR500 internal LAN subnets.
"Palo Alto Firewall" on page 328	Name for the tunnel.	Enter the secret key specified in the Palo Alto Management Portal.	External internal IP address of Palo Alto Firewall. You can obtain this from **Interfaces > Ethernet** in the Palo Alto Management Portal.	External internal IP address of Palo Alto Firewall. You can obtain this from **Interfaces > Ethernet** in the Palo Alto Management Portal. If NAT is configured, then enter the internal LAN IP address of the Palo Alto Firewall.	Any (0.0.0.0)	Any (0.0.0.0)
"pfSense Firewall" on page 335	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	pfSense Firewall Public WAN IP address.	pfSense Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	pfSense internal LAN subnets.
"SonicWall Firewall" on page 341	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	SonicWall Firewall Public WAN IP address.	SonicWall Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	SonicWall internal LAN subnets.
"Sophos XG Firewall" on page 351	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	Sophos XG Firewall Public WAN IP address.	Sophos XG Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Sophos XG internal LAN subnets.

Field Firewall/Router	Name	Shared Secret	Public IP [1]	Remote ID [2]	Harmony SASE Gateway Proposal Subnets [3]	Remote Gateway Proposal Subnets
"UniFi USG Firewall" on page 357	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	UniFi USG Firewall Public WAN IP address.	UniFi USG Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	UniFi USG internal LAN subnets.
"WatchGuard Firewall" on page 363	Name for the tunnel.	Enter a secret key or click **Generate** to generate it.	WatchGuard Firewall Public WAN IP address.	WatchGuard Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	WatchGuard internal LAN subnets.
"Zyxel USG Firewall" on page 369	Name for the tunnel.	Enter a secret key or click **Generate** to generate it	Zyxel USG Firewall Public WAN IP address.	Zyxel USG Firewall Public WAN IP address.	Harmony SASE network subnet. The default is 10.255.0.0/16.	Zyxel USG internal LAN subnets.

[1] For dynamic IP tunnels, enter 0.0.0.0

[2] For dynamic IP tunnels, do not enter 0.0.0.0

[3] For dynamic IP tunnels, do not select **Any (0.0.0.0/0)**

7. In the **Advanced Settings** section, enter the relevant details:

Field / Firewall/Router	IKE Version[1][2]	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Barracuda	V2	8h	1h	10s	30s	aes256	aes256	SHA	SHA	2	2
Check Point	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Cisco ASA	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Cisco Meraki	V1	8h	1h	10s	50s	aes256	aes256	sha1	sha1	5	5
D-Link DSR Series Router	V1	8h	1h	30s	10s	aes256	aes256	sha512	sha512	5	5
DrayTek Vigor2862	V2	8h	1h	30s	60s	aes256	aes256	sha1	sha1	2	2
DrayTek Vigor3900	V1	8h	1h	30s	60s	aes256	aes256	sha1	sha1	5	5
EdgeMax	V1	8h	1h	15s	30s	aes256	aes256	sha1	sha1	14	14
FortiGate Next Generation Firewall	V2	8h	1h	10s	30s	Default value	Default value	Default value	Default value	21	21
Linksys	V2	8h	1h	30s	10s	aes256	aes256	sha1	sha1	5	5
Juniper Networks ScreenOS	V1	8h	1h	10s	50s	aes256	aes256	sha1	sha1	5	5
Juniper Networks SRX	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Netgear BR500	V2	8h	1h	30s	10s	aes256	aes256	sha1	sha1	5	5
Palo Alto	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14

Field / Firewall/Router	IKE Version[1] [2]	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
pfSense	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
SonicWall	V2	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
Sophos XG	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	14	14
UniFi USG	V2	8h	8h	10s	30s	aes256	aes256	sha1	sha1	21	21
WatchGuard	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Zyxel USG	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14

[1] If **V2** is not supported, select **V1**.

[2] For dynamic IP tunnels, select **V2**.

8. Click **Add Tunnel**.

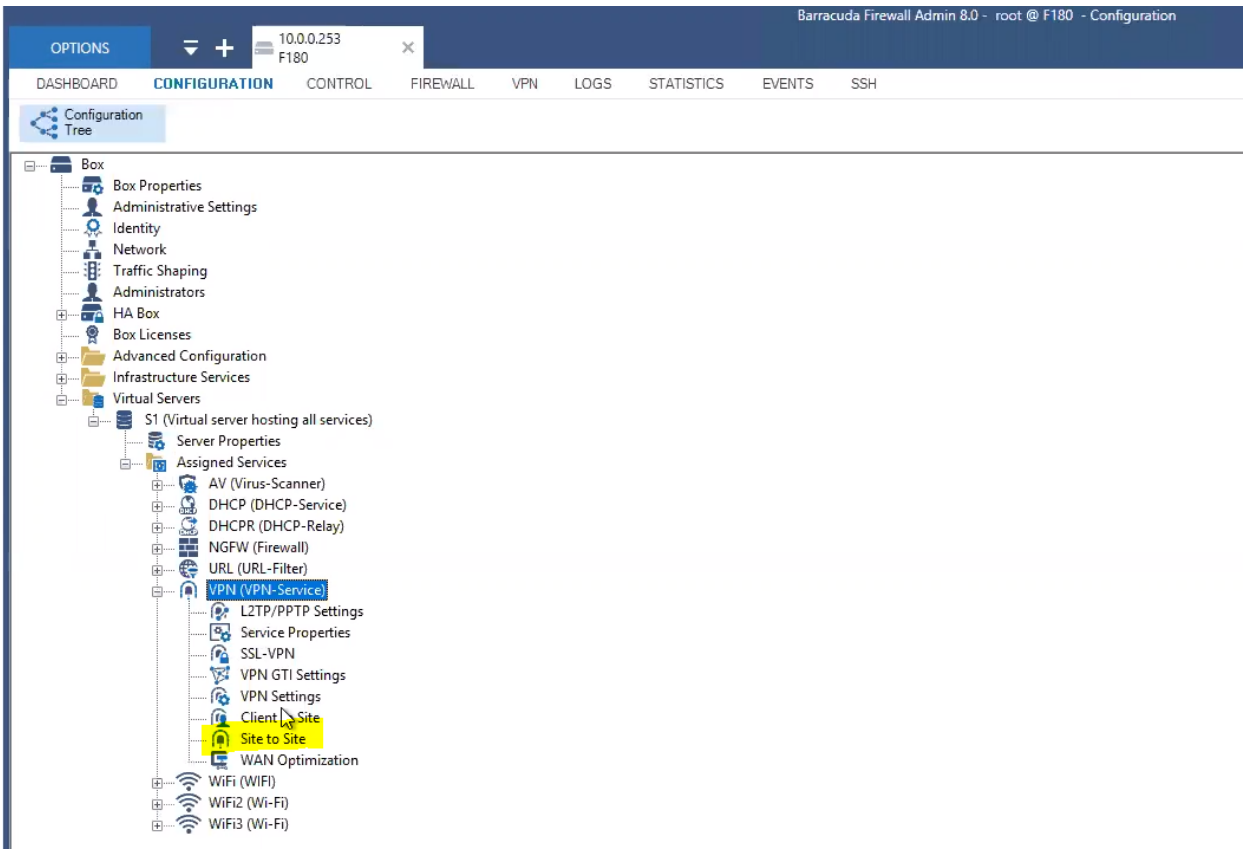
On-premises Firewall - Configuring the Tunnel in the Management Portal

Harmony SASE supports these on-premises firewall devices for the IPSec Site-2-Site VPN tunnel connection with the Harmony SASE gateway:

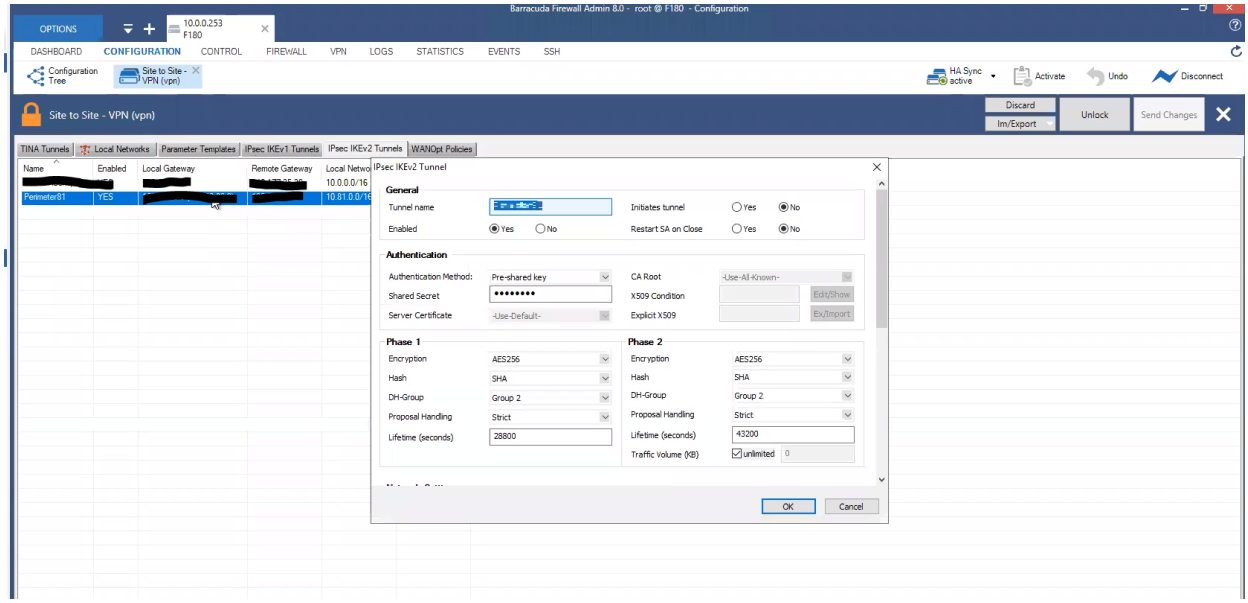
Barracuda Firewall

To configuring the tunnel in the Barracuda Management Portal:

1. Log in to the Barracuda Management Portal with the Administrator account.
2. From the top menu, click **Configuration > Virtual Servers > Your virtual server > Assigned Services > VPN (VPN-Service) > Site to Site**.



3. In the **IPsec IKEv2 Tunnels** tab, create a new tunnel:



a. In the **General** section:

   i. In the **Tunnel Name** field, enter a tunnel name.

   ii. Leave the rest of fields to default settings.

b. In the **Authentication** section:

   i. From the **Authentication Method** list, select Pre-shared key.

   ii. In the **Shared Secret** field, enter the same secret key that you specified in step **6** in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

   iii. Leave the rest of fields to default settings.

c. In the **Phase 1** section:

Field	Enter
Encryption	AES256
Hash	SHA
Diffie-Hellman Group	2
Proposal Handling	Strict
Lifetime	28800

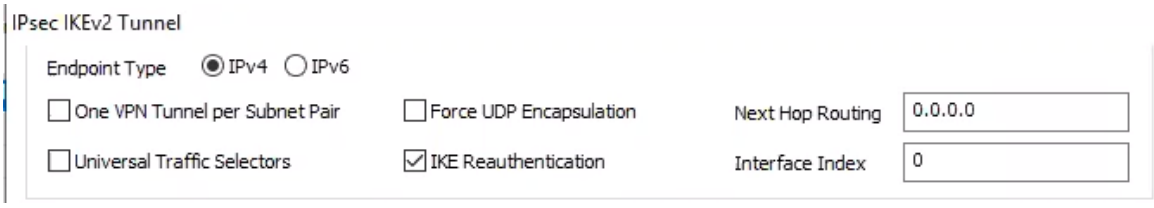
d. In the **Phase 2** section:

Field	Enter
Encryption	AES256
Hash	SHA
DH-Group	2
Proposal Handling	Strict
Lifetime	3600
Traffic Volume (KB)	Unlimited

4. Click **Configuration > Site to Site VPN (vpn)**:

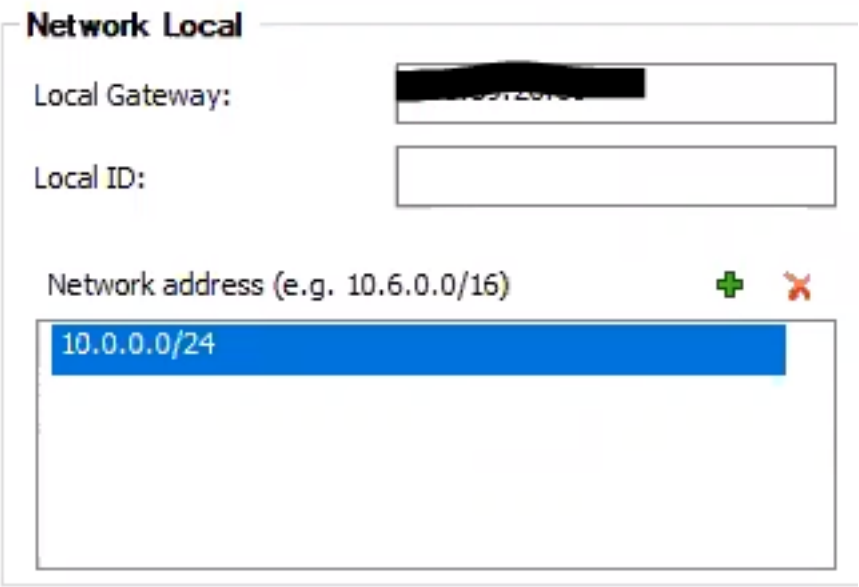
a. Create a new site-to-site VPN or edit an existing one.

b. In the **IPSec IKEv2 Tunnel** selection:



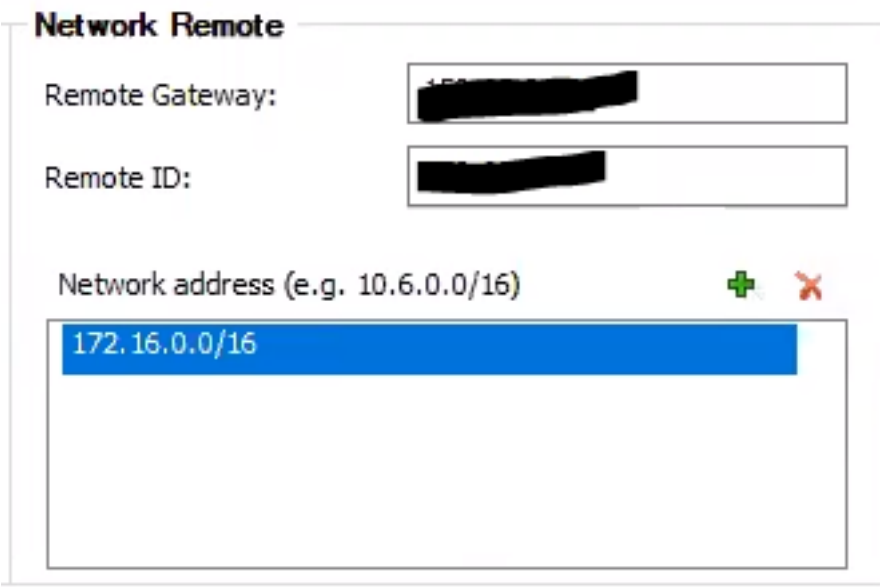
Field	Enter
Endpoint Type	IPv4
One VPN Tunnel per Subnet Pair	Clear
Universal Traffic Selectors	Clear
Force UDP Encapsulation	Clear
IKE Reauthentication	Select
Next Hop Routing	0.0.0.0
Interface Index	0

c. In the **Network Local** selection:



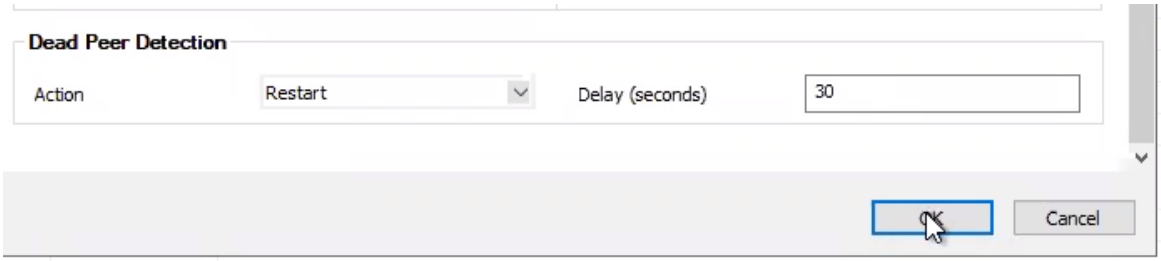
Field	Enter
Local Gateway	Barracuda Firewall Public IP address
Local ID	Barracuda Firewall Public IP address
Network address	Internal network subnets

d. In the **Network Remote** selection:



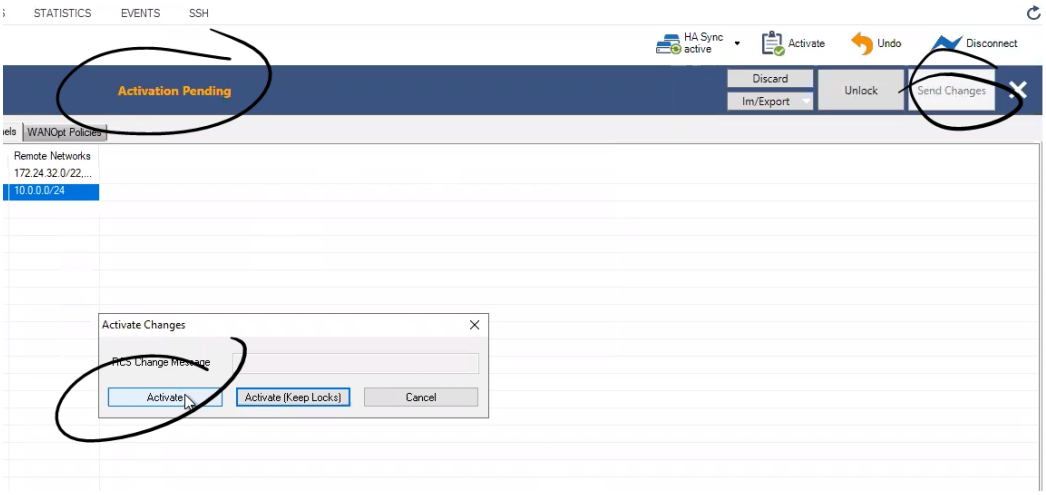
Field	Enter
Remote Gateway	Harmony SASE Public IP address
Remote ID	Harmony SASE Public IP address
Network address	Harmony SASE network subnets

e. In the **Dead Peer Detection** selection:



Field	Enter
Action	Restart
Delay (seconds)	30

f. Click **OK**.

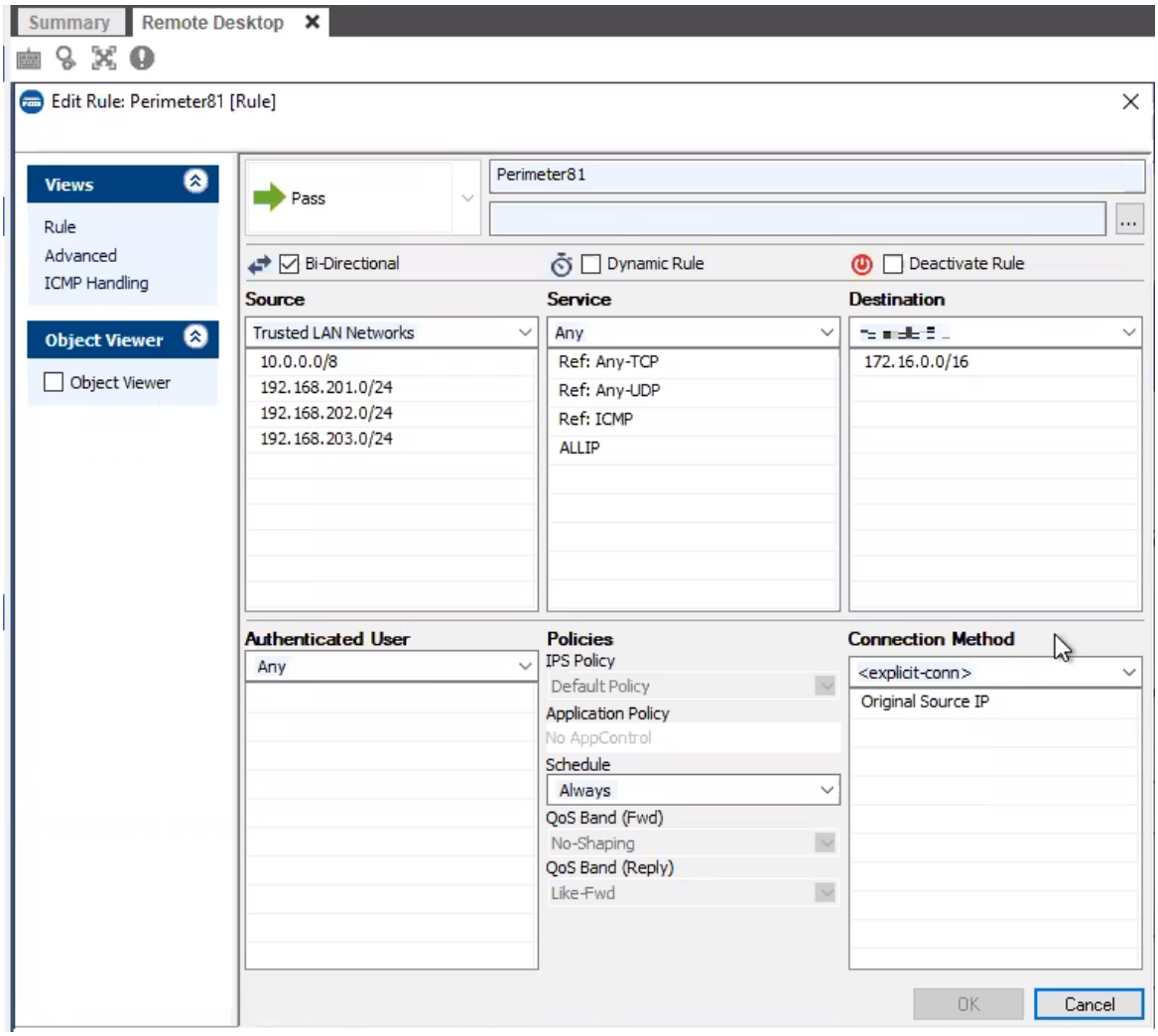


g. Click **Send Changes**.

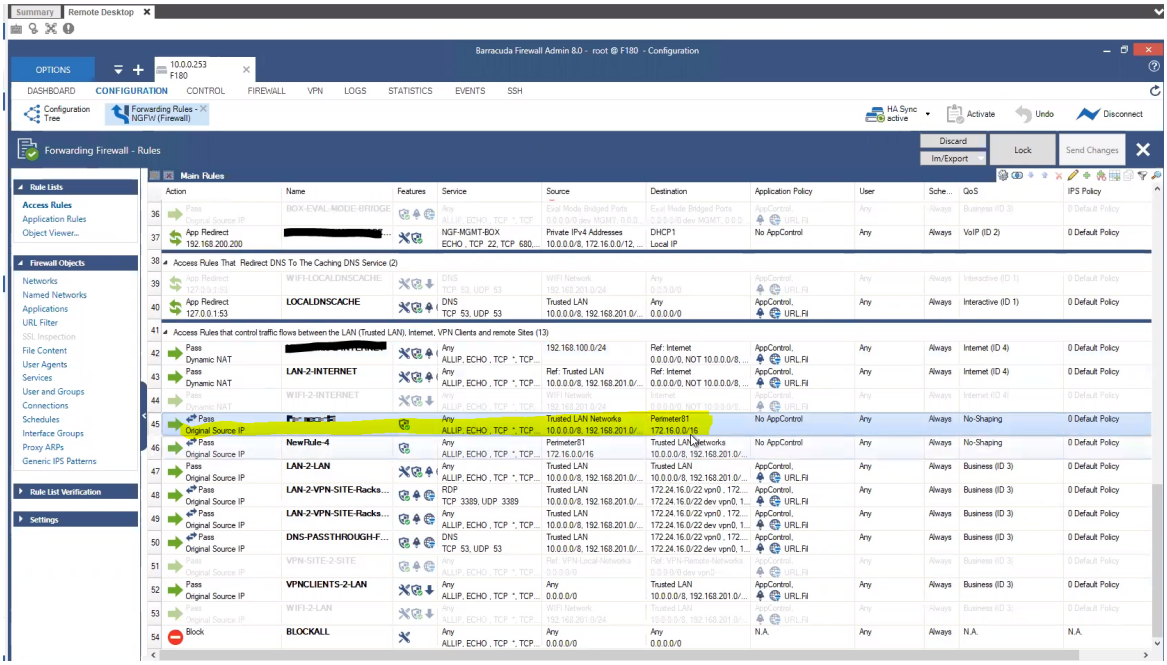
h. Click **Activate**.

5. Click **Firewall > Forwarding Rules**:

a. Add Harmony SASE gateway public IP address to the allow-list.

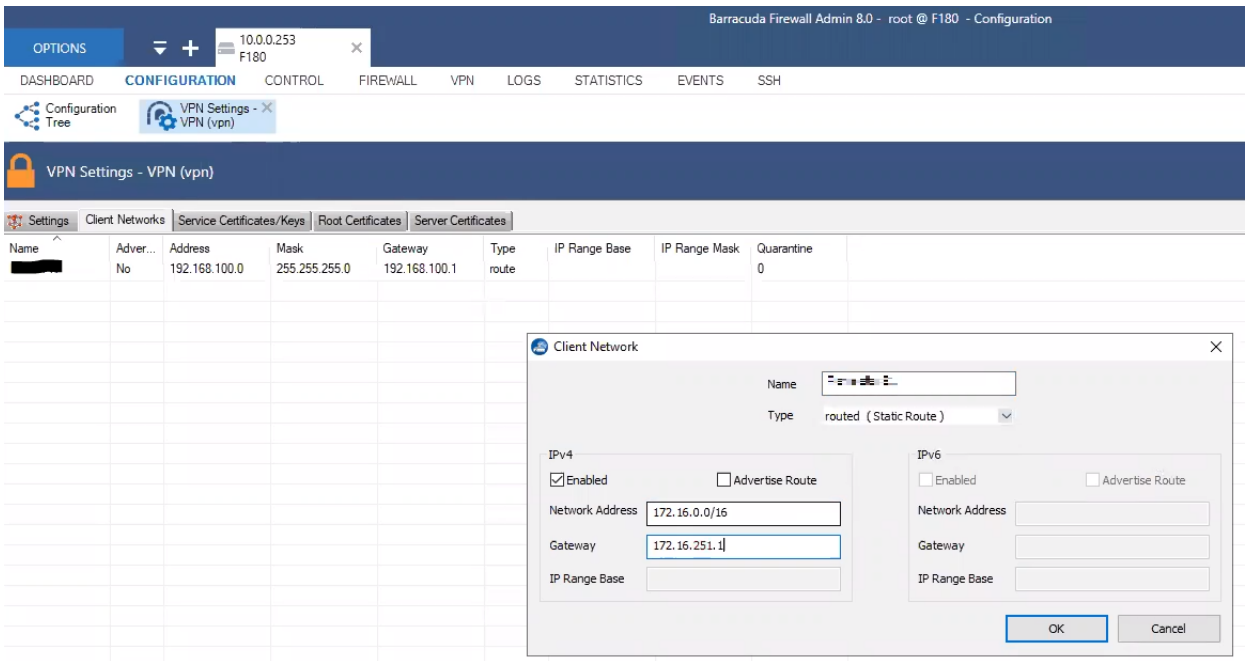


b. Ensure that the Harmony SASE gateway public IP address is listed under the firewall rules.



c. Add the static routes from the Harmony SASE subnet (10.XXX.0.0/16) to the local network and from the local network to the Harmony SASE subnet (10.XXX.0.0/16) through the VPN tunnel gateway.

6. Click **Configuration > Site to Site VPN (vpn)**:

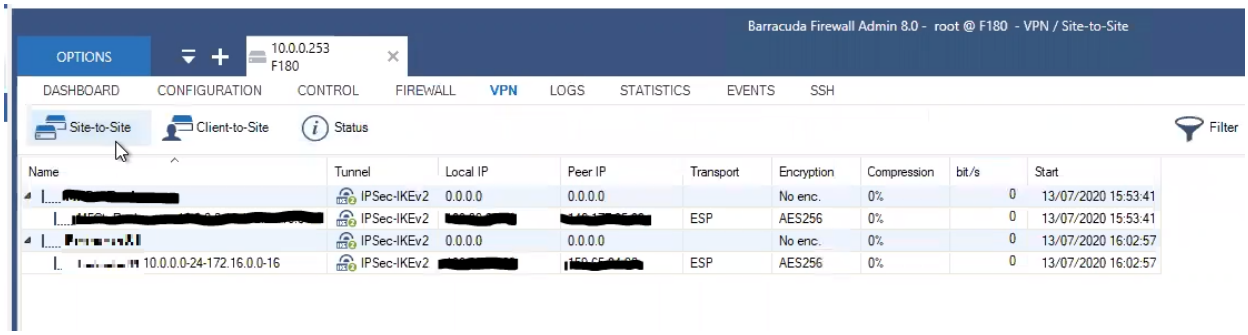


a. In the **Client Networks** tab:

Field	Enter
Network Address	172.xxx.0.0/16 (or relevant subnet0
Gateway	Local Barracuda IP address
Name	Tunnel name.

b. Click **OK**.

7. To verify that the tunnel is up, go to **VPN > Site-to-Site**. If the tunnel is listed in the table, then the tunnel is up.



Check Point Firewall

You can establish a Single Site-to-Site VPN tunnel between your Harmony SASE.

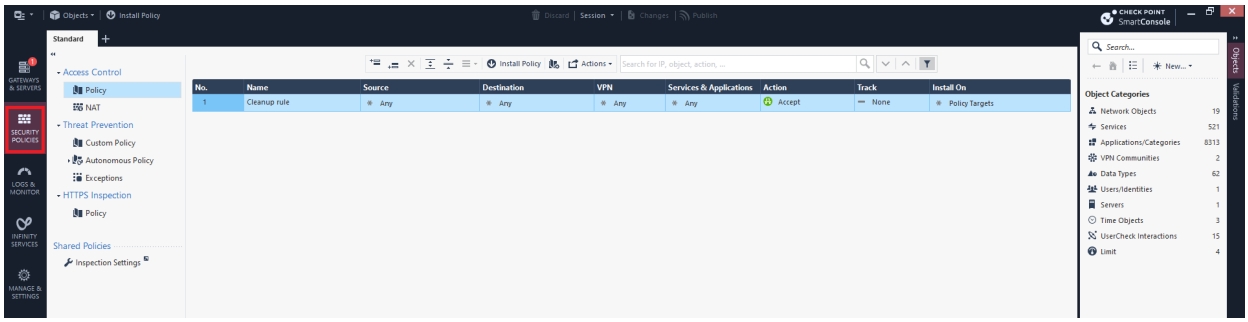
Pre-requisites

- Harmony SASE Administrator Portal account.
- Make sure that you have installed the Harmony SASE Agent on your device.
- Administrator account with Firewall/Router/Cloud Management Portal.

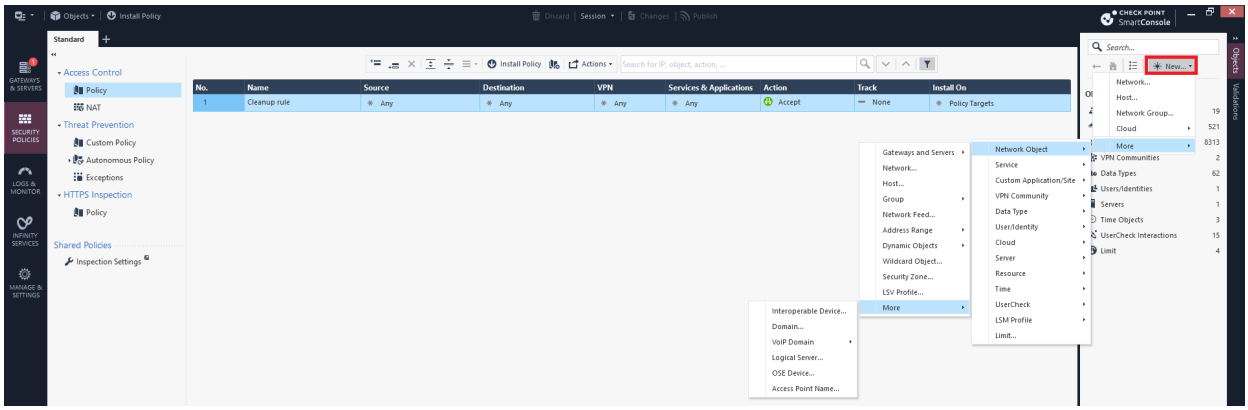
Configuration Steps

Creating Interoperable Device Object in the Check Point SmartConsole

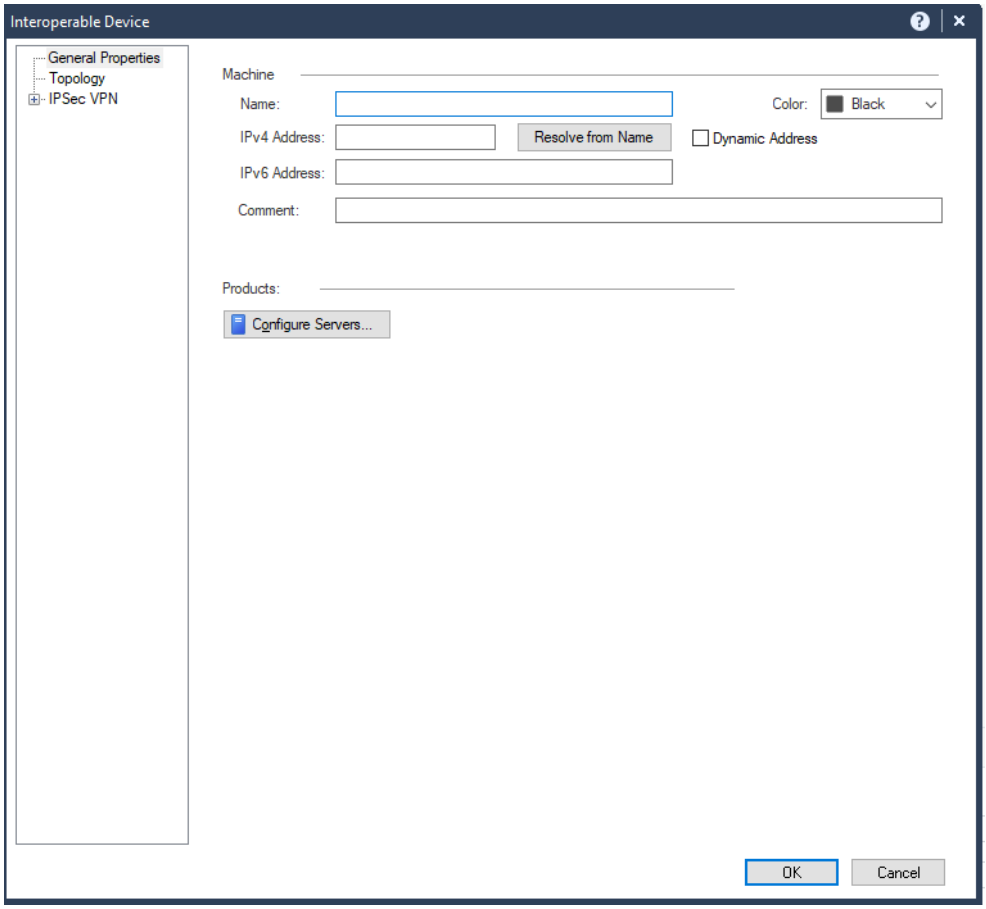
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



3. On the top right, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** window appears.



a. In the **Name** field, enter a name for Harmony SASE gateway.

b. In the **IPv4 Address** field, enter the Harmony SASE gateway public IP address.

   To find the Harmony SASE Gateway public IP Address:

   i. Access the Harmony SASE Administrator Portal and click **Networks**.

   ii. Select the network.

   iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

c. Click **OK**.

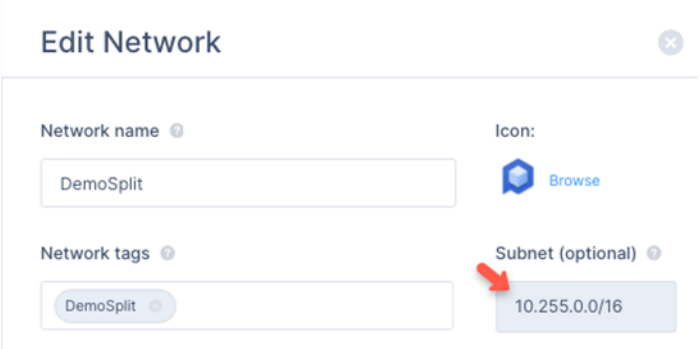
Adding Harmony SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object

1. Log in to the Harmony SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network. The default value is 10.255.0.0/16.
4. To verify:

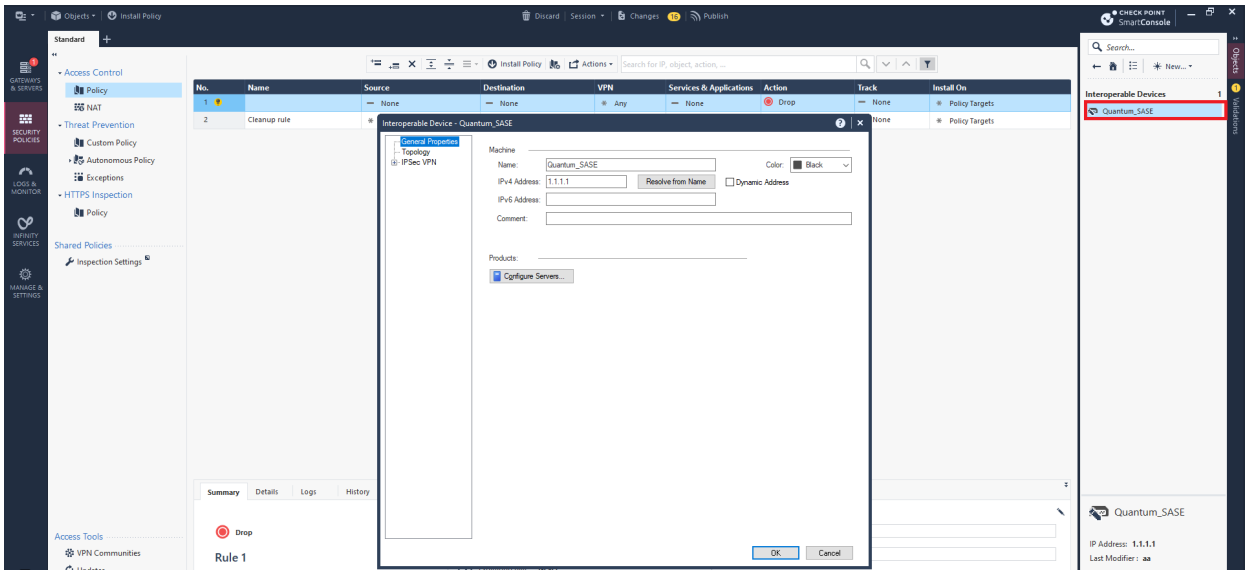
a. Select a network, scroll to the end of the row and click ··· .

b. Select **Edit Network.**

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.

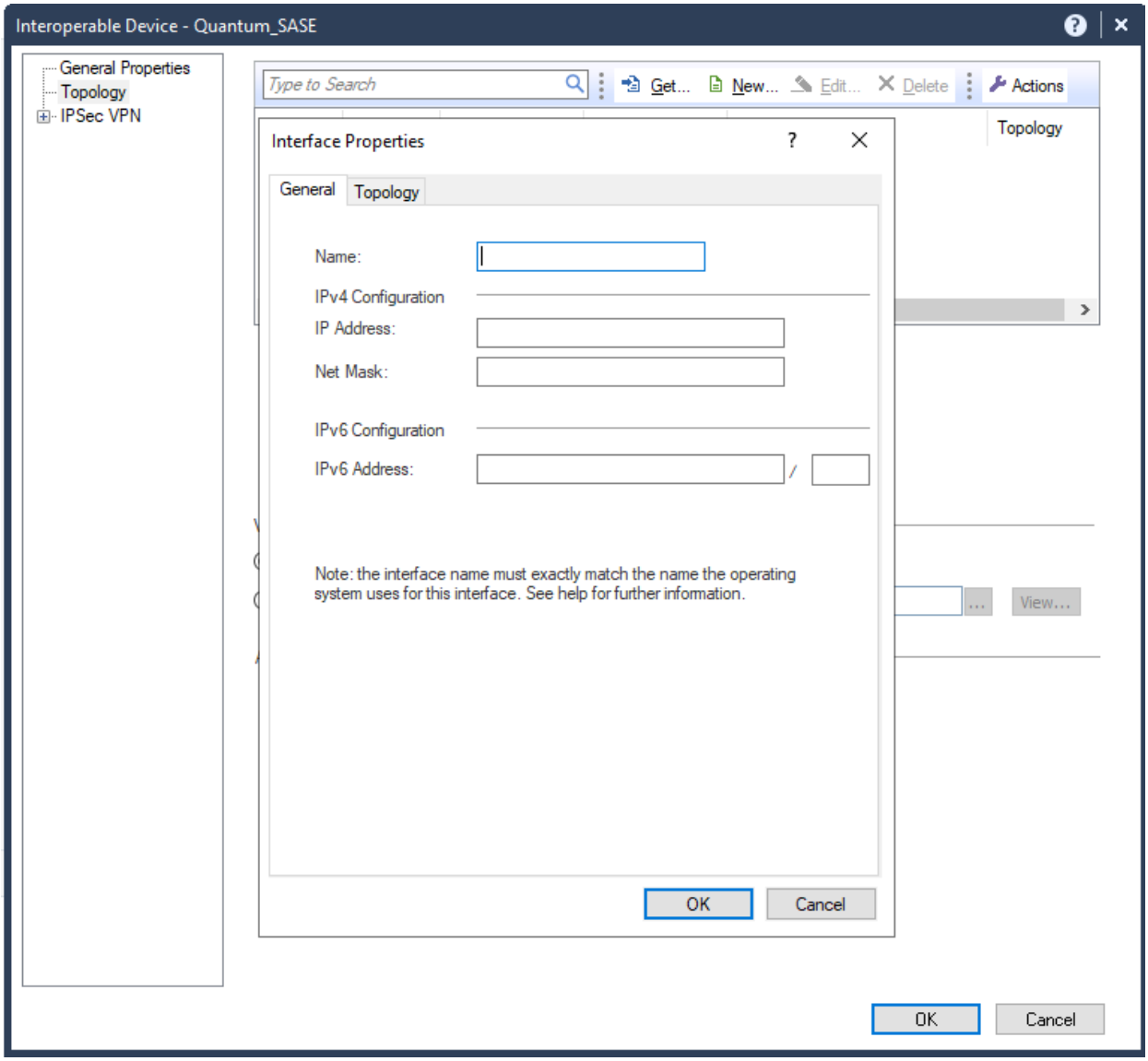


5. Open the network object that you created.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

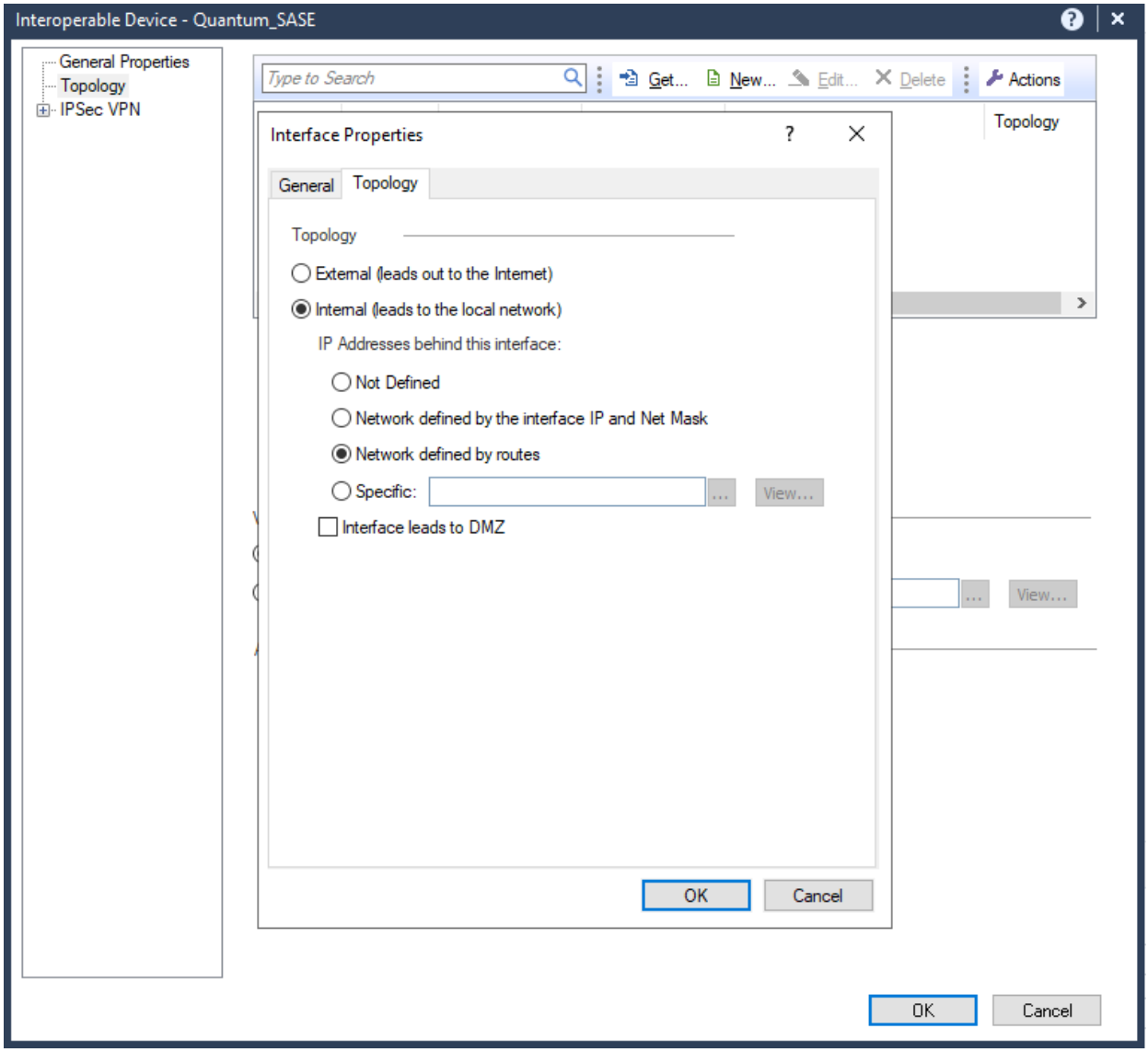
6. Click **Topology > New**.



7. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	10.255.0.0
Net Mask	255.255.0.0

8. In the **Topology** tab, select **Internal (leads to the local network)** and select **Network defined by the interface IP and Net Mask**.



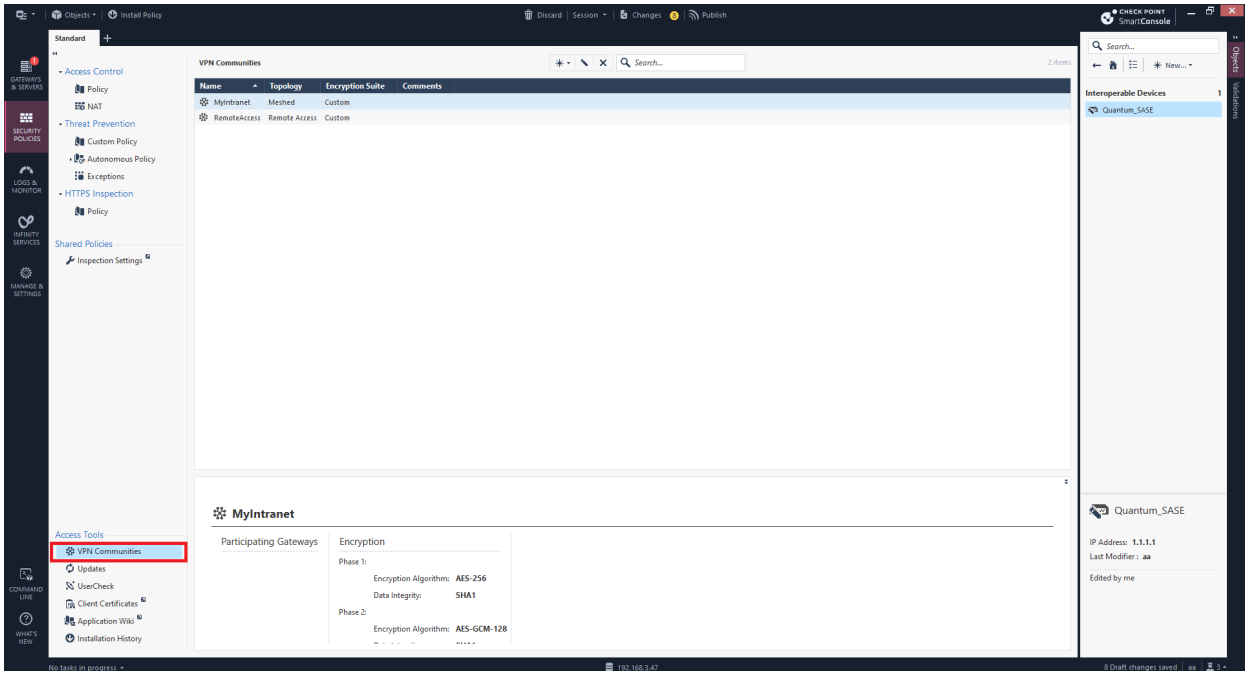
9. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	Public IP address of the Harmony SASE gateway.
Net Mask	255.255.255.255

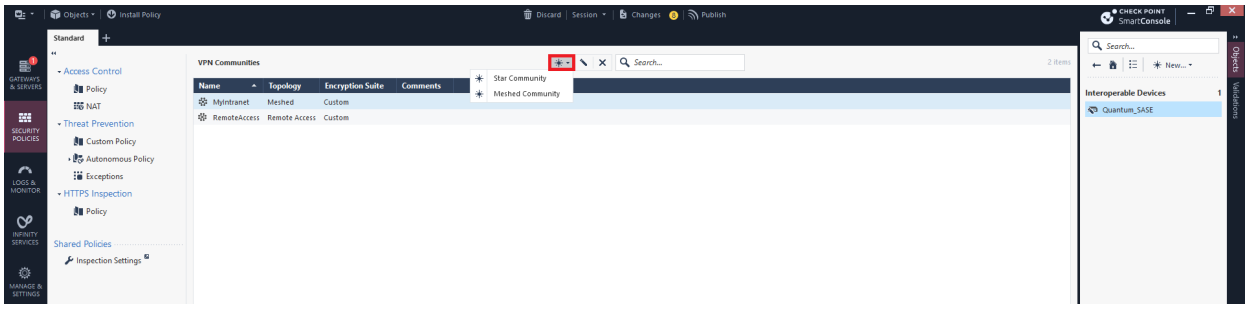
10. In the **Topology** tab, select **External (leads to the local Internet)**.
11. Click **OK**.
12. Click **OK**.
13. Publish and install the policy.

Creating VPN Start Community

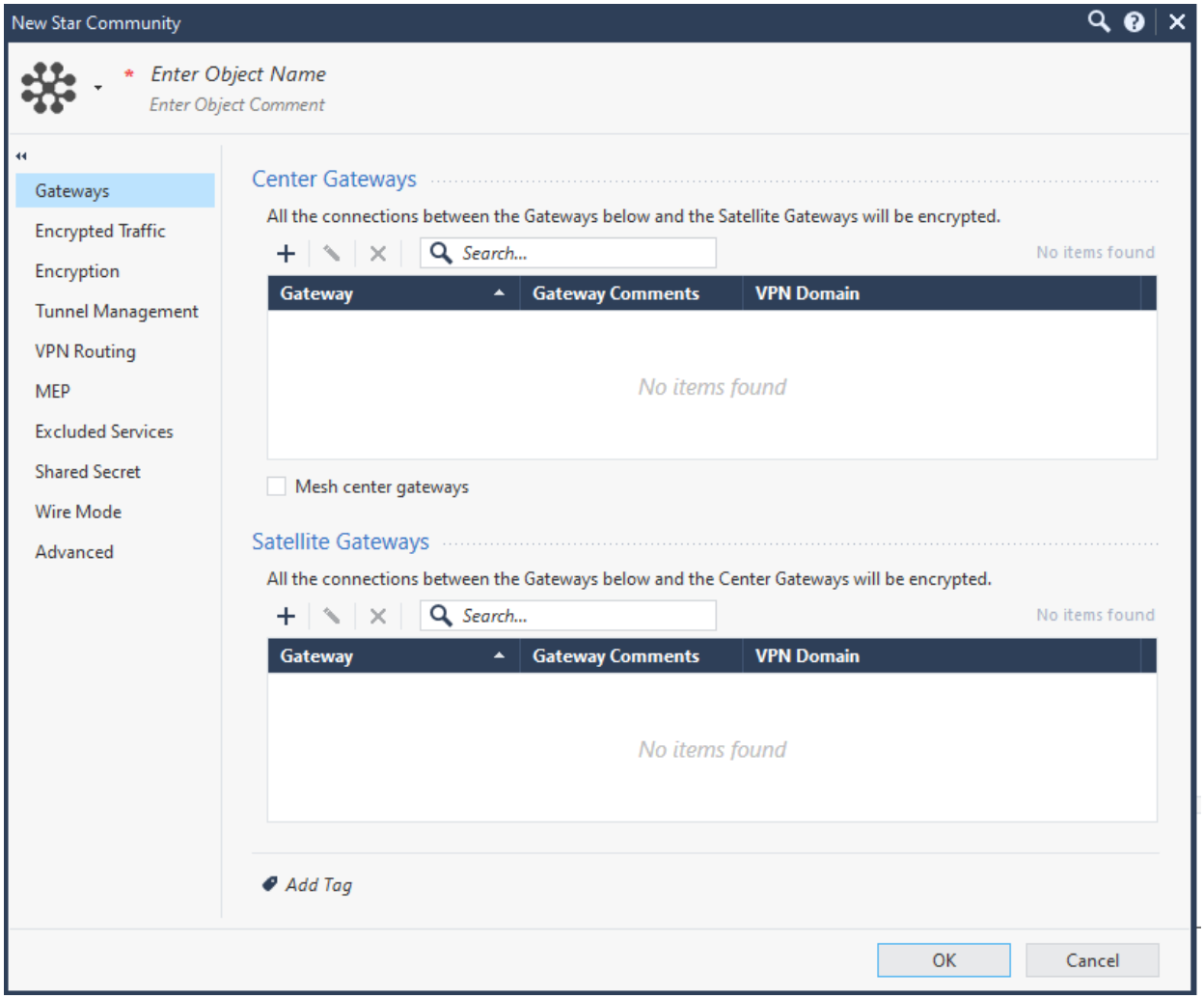
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools** > **VPN Communities**.



4. Click **New** and select **Star Community**.



The **New Star Community** window appears.



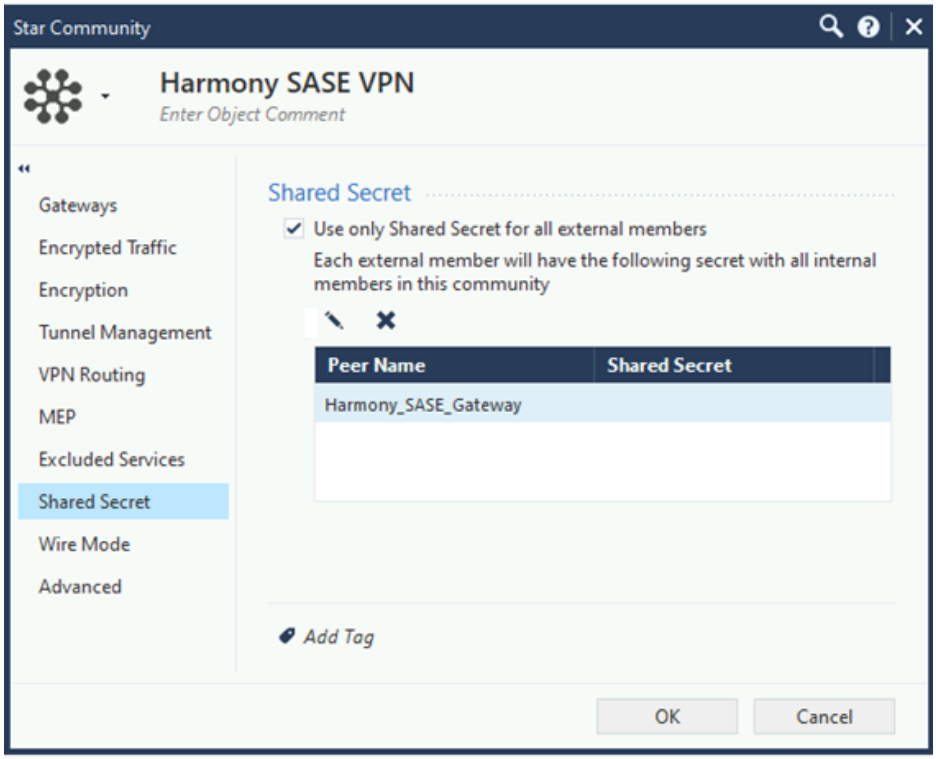
5. In the **Enter Object Name** field, enter an object name for the VPN Start Community, for example, Harmony SASE VPN.

6. Under **Center Gateways**, click + and add the Check Point gateway.

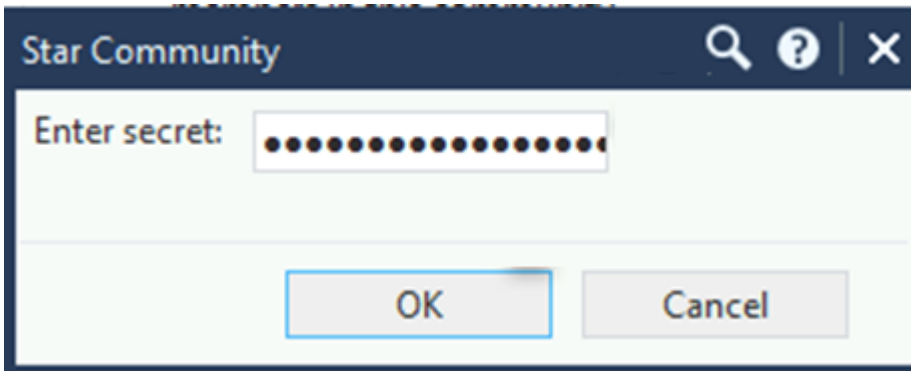
7. Under **Satellite Gateways**, click + and add the previously created Interoperable Device Object for the Harmony SASE gateway. See step 3.

8. Click **Shared Secret**.

9. To edit the shared key, click .



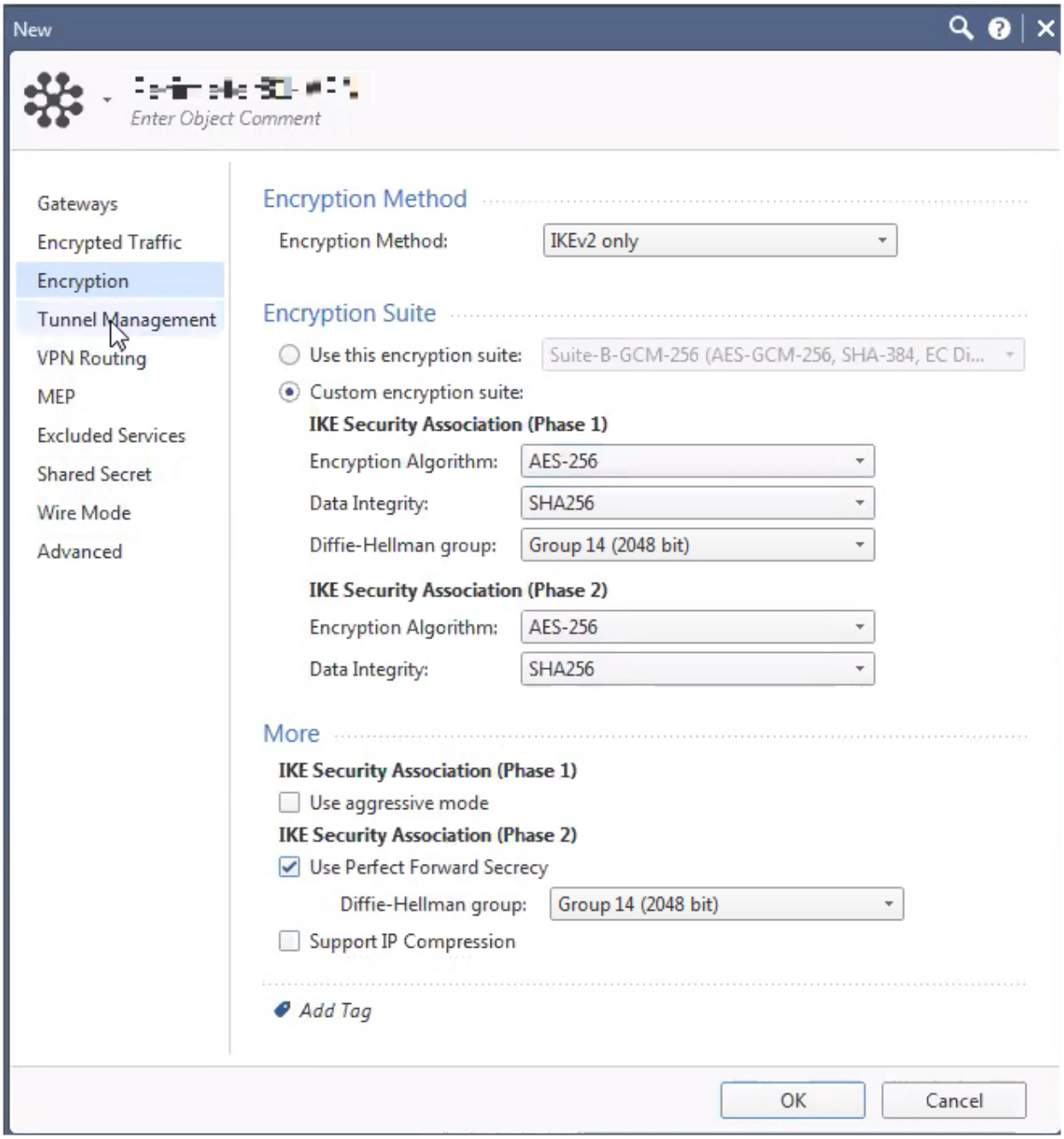
10. In the **Enter secret** field, enter an appropriate key. Make a note of it as it is used while configuring the tunnel in the Harmony SASE Administrator Portal.



Note - Check Point recommends that the share secret key is at least 20 characters in length.

11. Click **OK**.

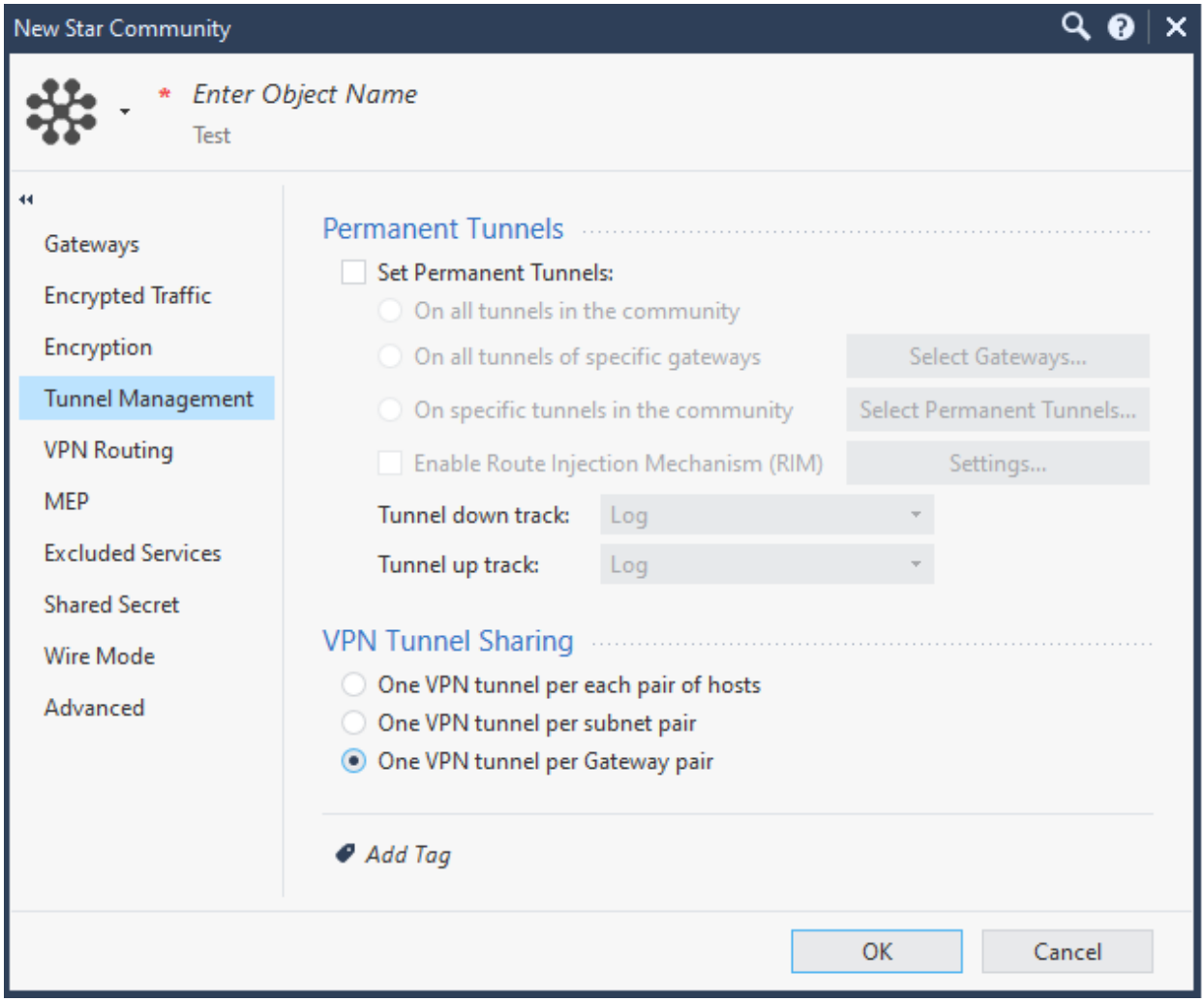
12. Click **Encryption**:



Field	Enter
Encryption Method	IKEv2 only
Custom encryption suite	
IKE Security Association (Phase 1)	
Encryption Algorithm	AES-256
Data Integrity	SHA256

Field	Enter
Diffie Hellman group	Group 14 (2048 bit)
IKE Security Association (Phase 2)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
More	
IKE Security Association (Phase 2)	
Use Perfect Forward Secrecy	
Diffie Hellman group	Group 14 (2048 bit)

13. Click **Tunnel Management** and under **VPN Tunnel Sharing**, select **One VPN tunnel per Gateway pair**.



Important - Make sure that you enter the remote subnets specified here in the Harmony SASE Administrator Portal. A mismatch can disconnect the tunnel.

14. Click **Advanced**.
    a. In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480.16**.
    b. In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security associations every (seconds)** field to **3600**.
15. Click **OK**.

Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the Harmony SASE Network 10.255.0.0/16 to specific destinations and services. Note that the network configuration may differ if you have not changed the default settings during Harmony SASE network creation. For testing purposes, you should initially allow any/any or allow before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

To configure the Tunnel in Harmony SASE Administrator Portal, see *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

To configure the Routes Table in Harmony SASE Administrator Portal, see Routes Table.

Cisco Firepower

You can establish a Site-to-Site VPN tunnel between your Harmony SASE and the Cisco Firepower device.

Pre-requisites

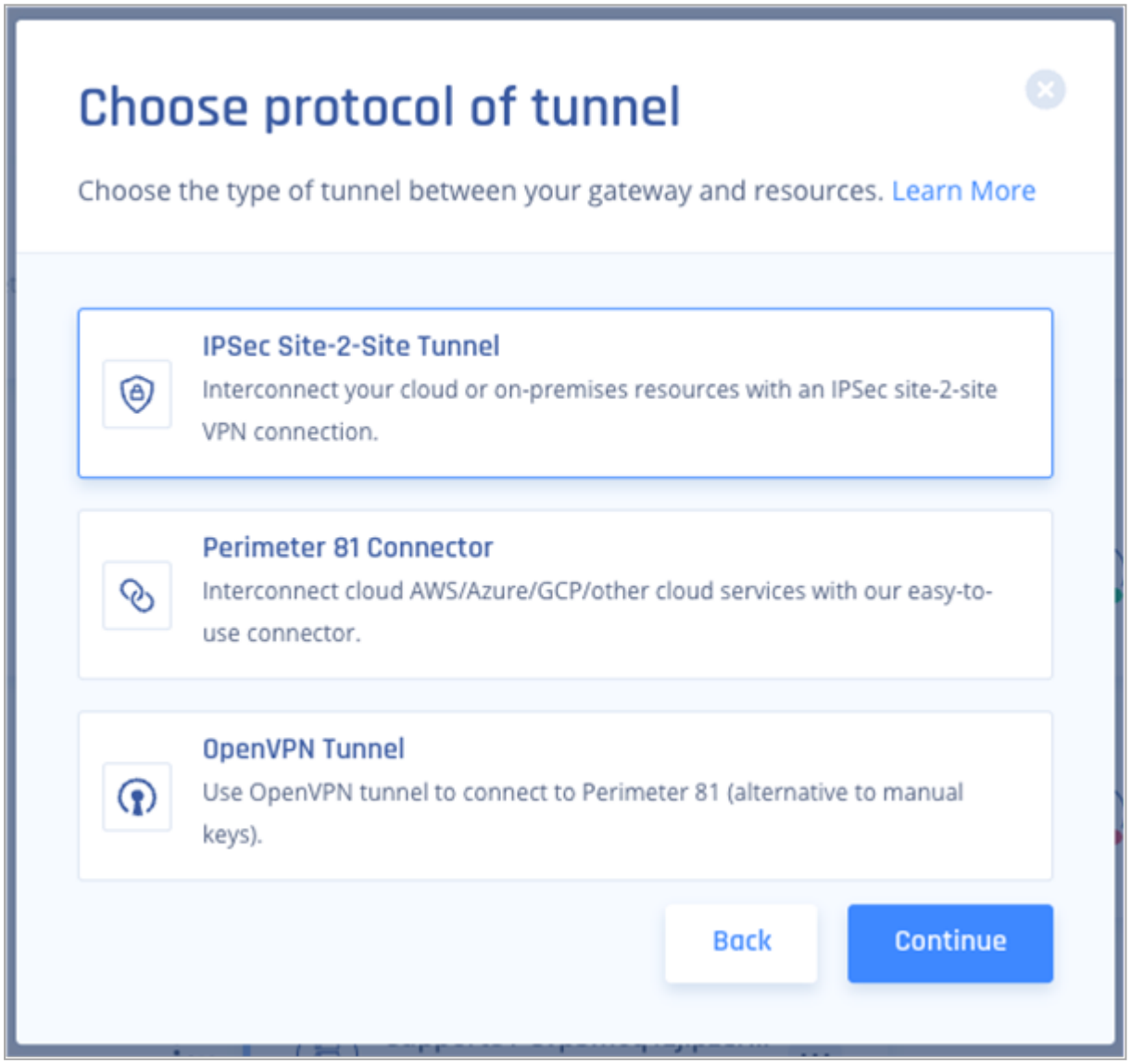
- Harmony SASE Administrator Portal account and a configured network.
- Make sure that you have installed the Harmony SASE Agent on your device.
- Active and licensed Cisco Firepower device with necessary administrative permissions.

Configuring IPsec Tunnel

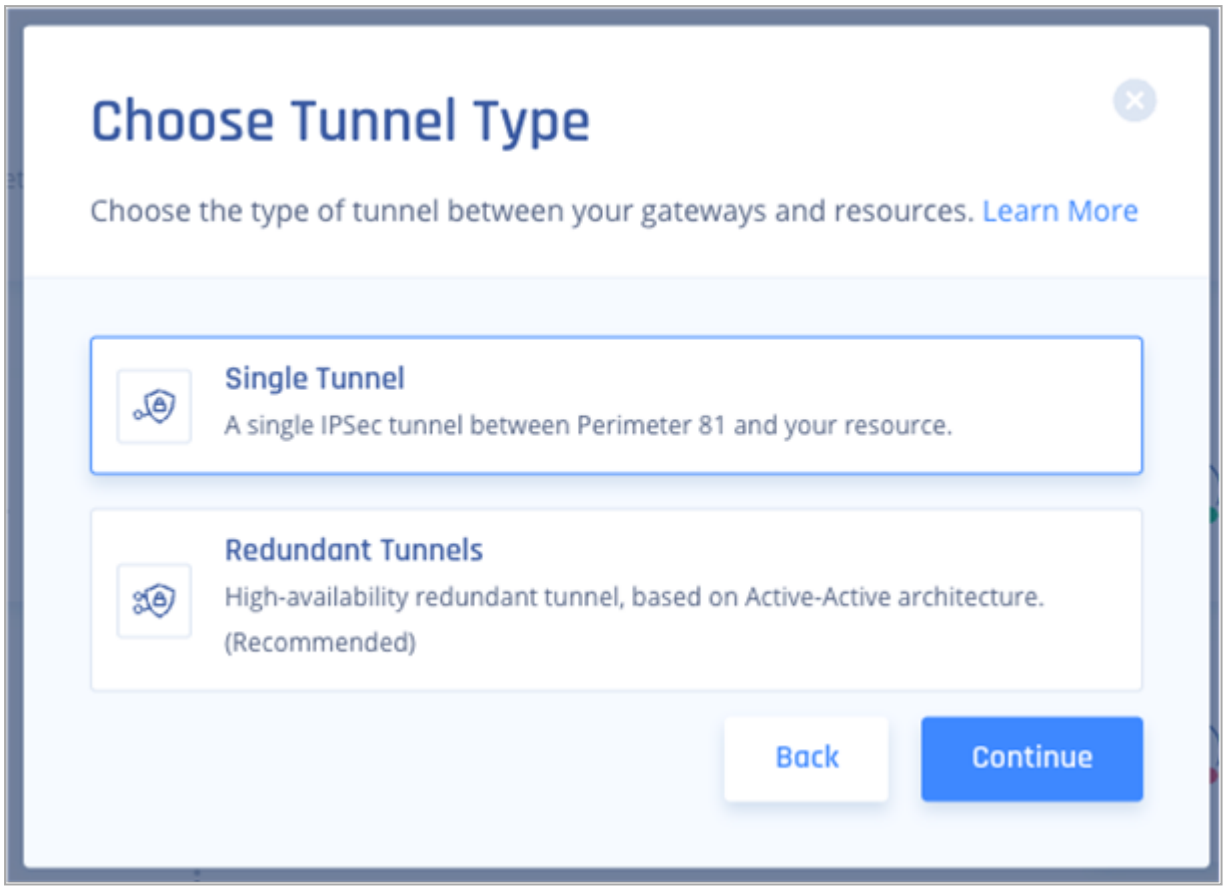
To configure an IPsec tunnel, do these:

1. Log in to the Harmony SASE Administrator Portal.
2. Click **Networks**.
3. Select the network from which you want to create the tunnel to the Cisco Firepower.
4. Click ··· and select **Add Tunnel**.

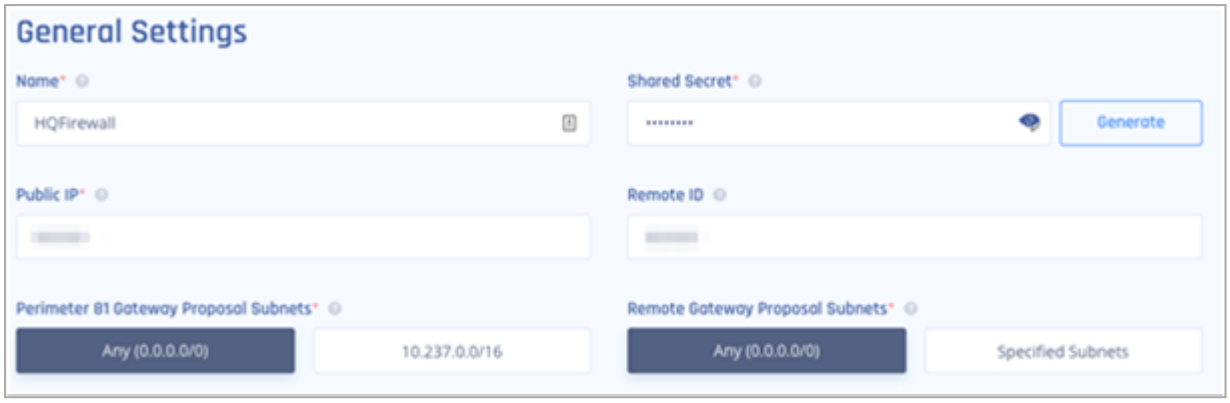
5. Select **IPSec Site-2-Site Tunnel** and click **Continue**.



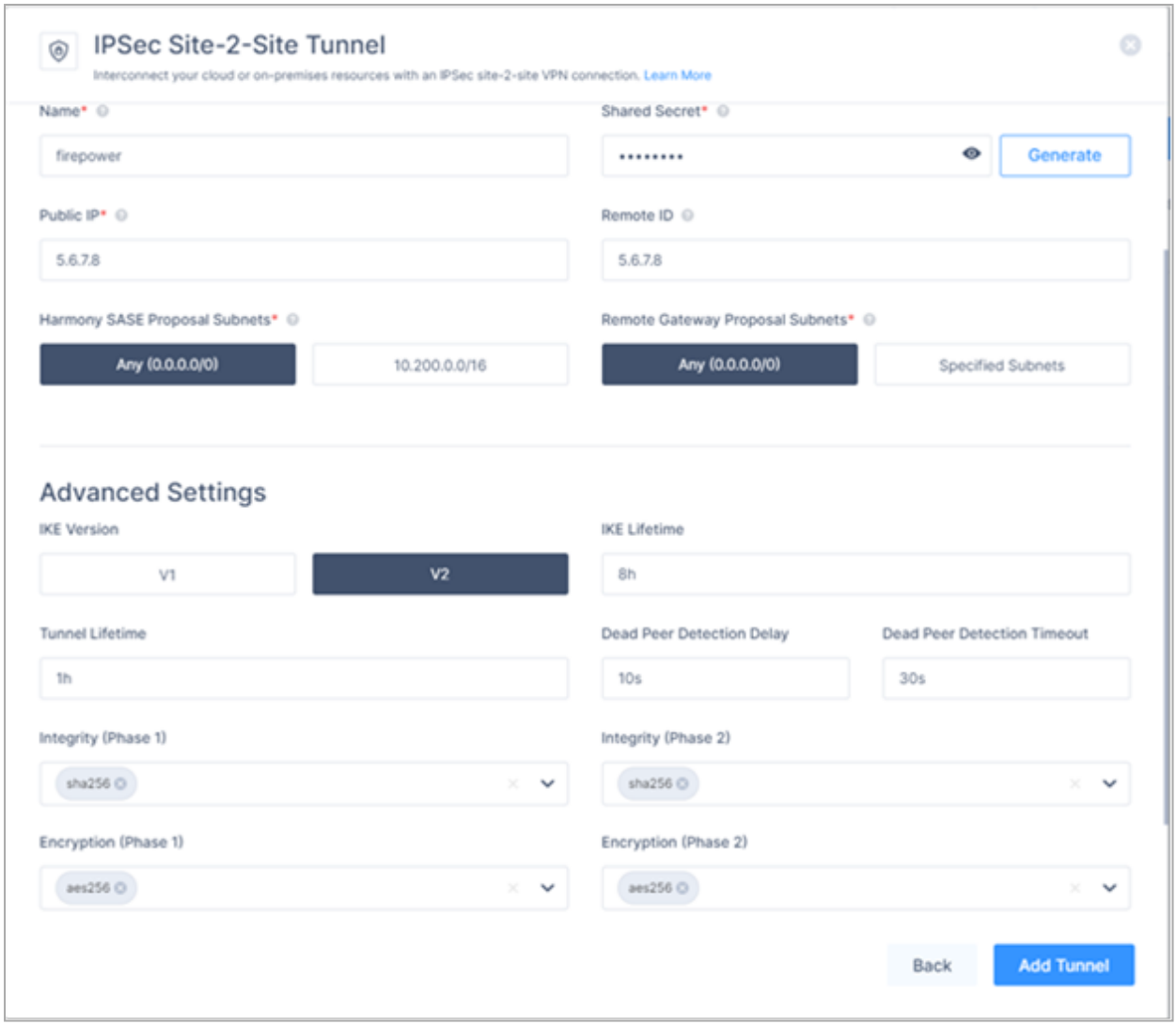
6. Select **Single Tunnel** and click **Continue**.



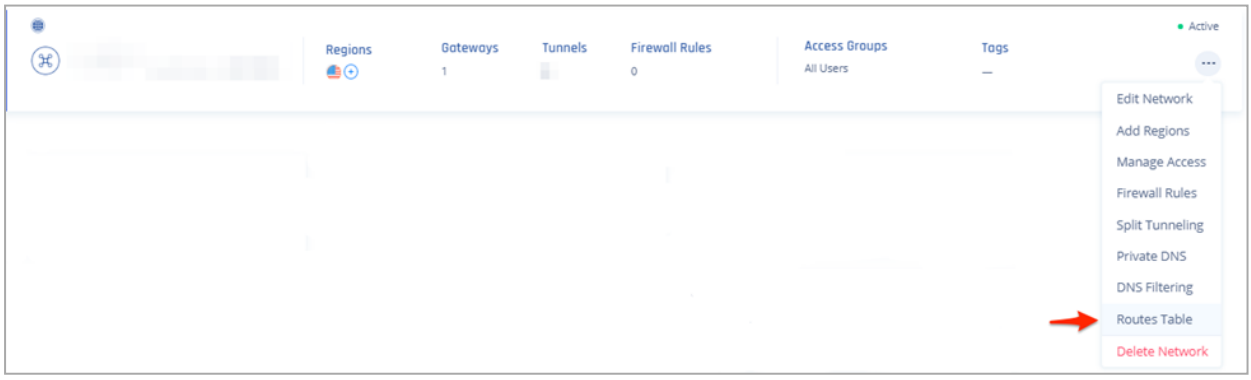
7. In the **General Settings** section:
   a. In the **Name** field, enter a name for the tunnel.
   b. In the **Shared Secret** field, enter a string or click **Generate**.
   c. In the **Public IP** field, enter the public IP of the Firepower device.
   d. In the **Remote ID** field, enter the remote ID of the Firepower device (this is same as Public IP unless the device is behind a NAT, then use the IP of the **outside** interface on the Firepower).
   e. In the **Harmony SASE Gateway Proposal Subnets** section, leave the default value, **Any (0.0.0.0/0)**.
   f. In the **Remote Gateway Proposal Subnets** section, leave the default value, **Any (0.0.0.0/0)**.



8. In the **Advanced Settings** section, specify these:
   - **IKE Version**: IKEv2
   - **IKE Lifetime**: 8h
   - **Tunnel Lifetime**: 1h
   - **Dead Peer Detection Delay**: 10s
   - **Dead Peer Detection Timeout**: 30s
   - **Encryption (Phase 1)**: aes256
   - **Encryption (Phase 2)**: aes256
   - **Integrity (Phase 1)**: sha256
   - **Integrity (Phase 2)**: sha256
   - **Diffie-Hellman Groups (Phase 1)**: 14
   - **Diffie-Hellman Groups (Phase 2)**: 14

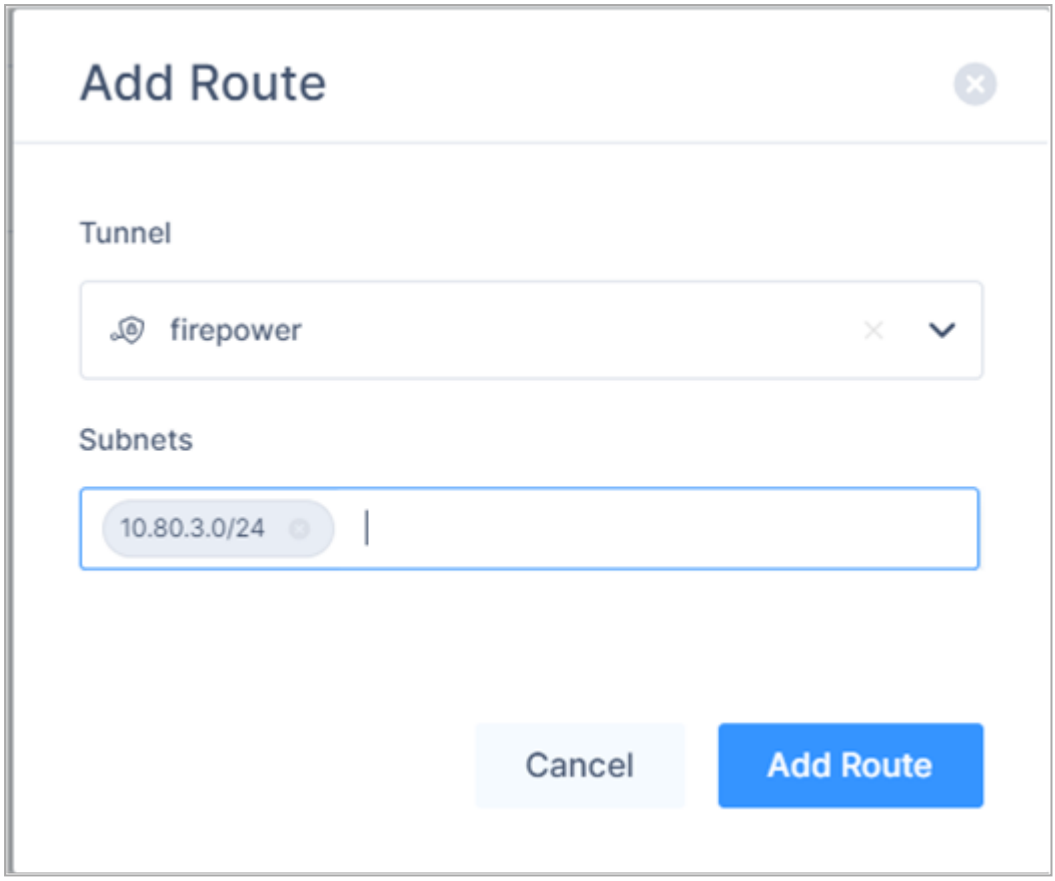


9. On your network, click ... and select **Routes Table**.

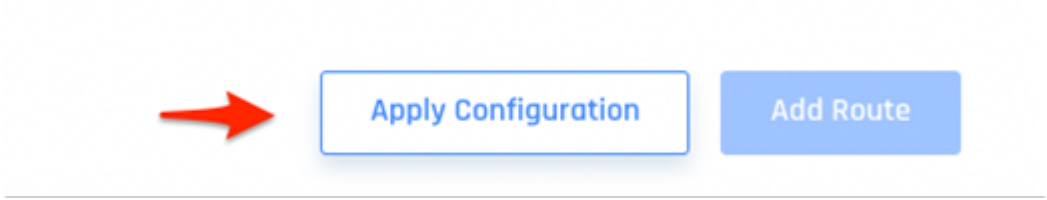


10. Click **Add Route**.

    The **Add Route** window appears.



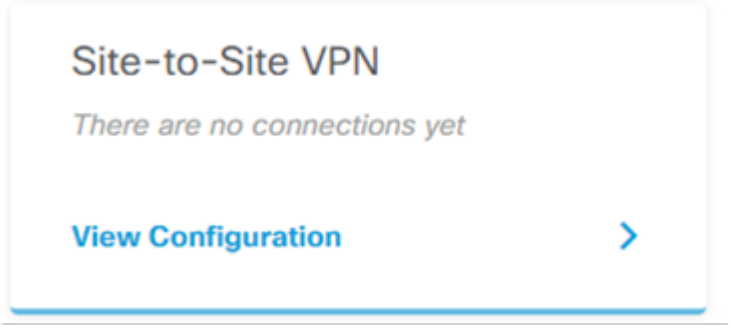
11. Verify the values entered in these:
    a. **Tunnel**
    b. **Subnet**
12. Click **Add Route**.
13. Click **Apply Configuration**.



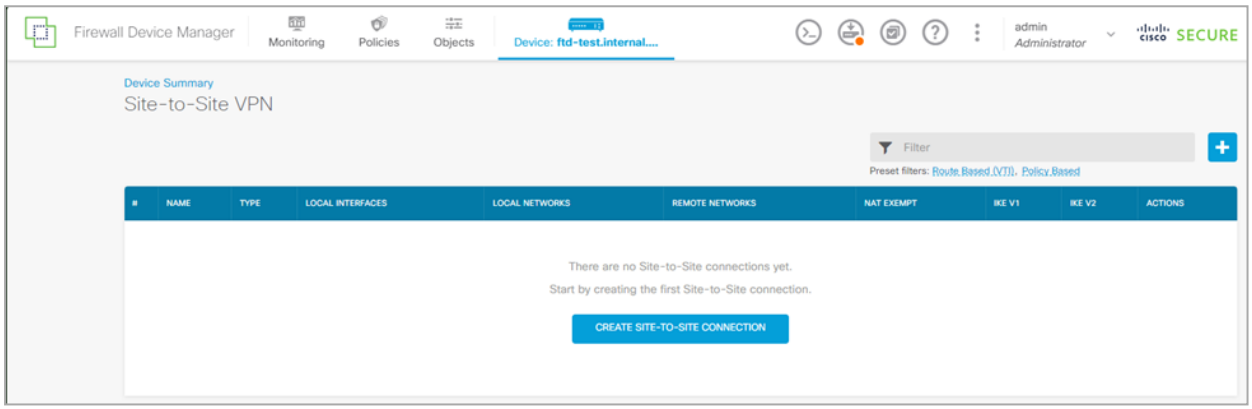
Configuring the Tunnel in Cisco Firepower

1. Login to your Cisco Firepower web console.
2. Select your device.

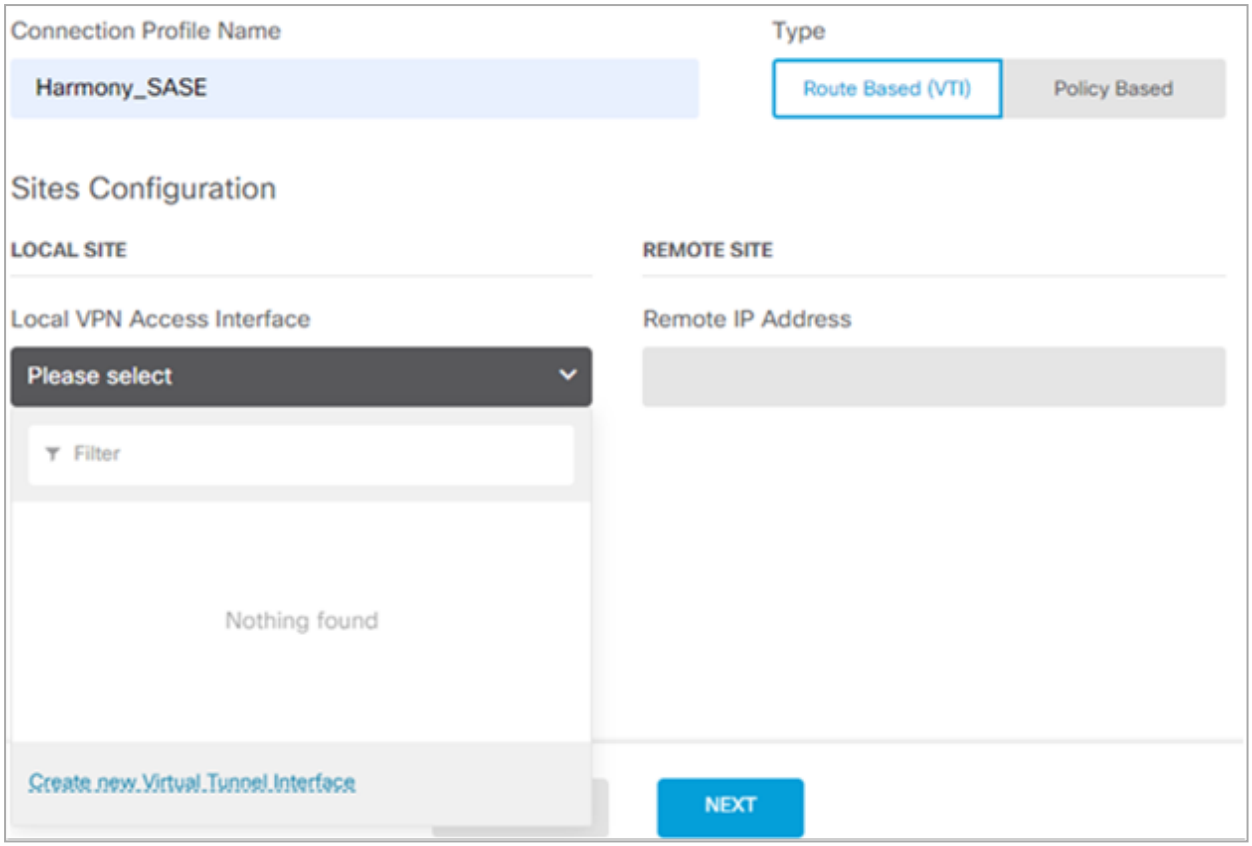
3. Go to Site-to-Site VPN configuration and click **View Configuration**.



4. Click + to create a Site-to-Site Connection.



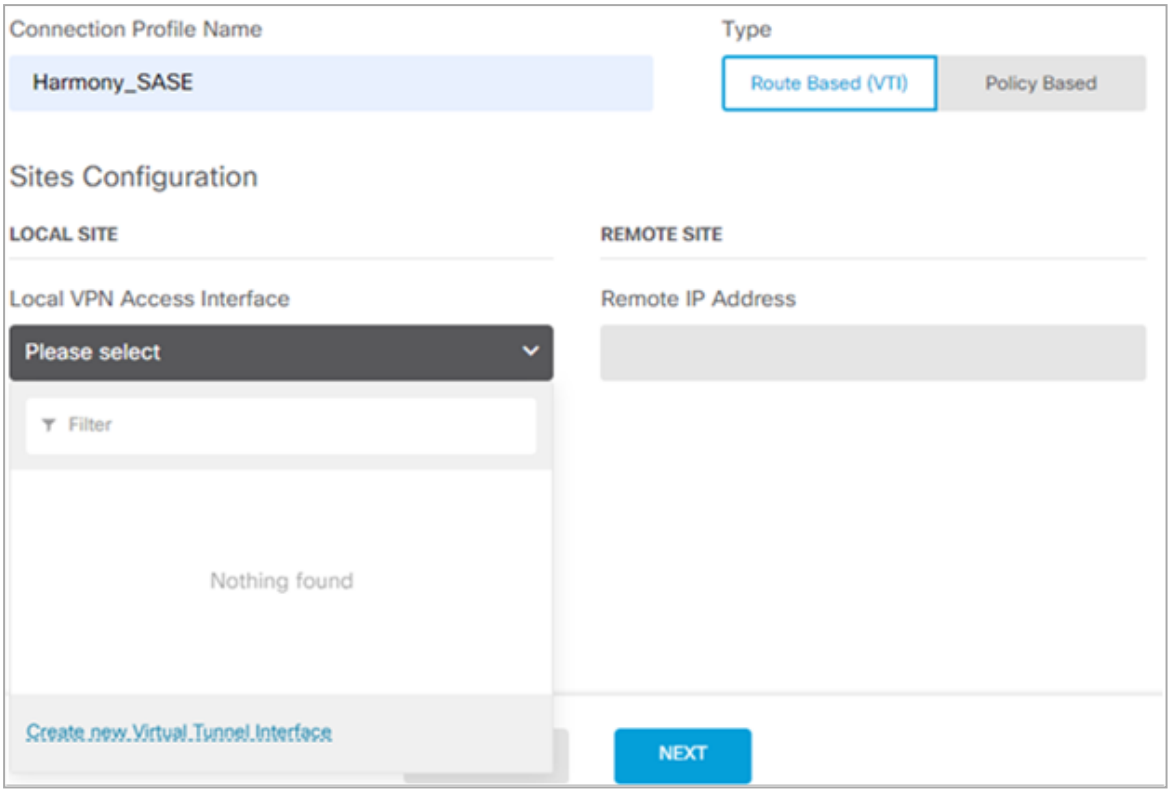
5. Specify these:



a. In the **Connection Profile Name** field, enter a name for your connection.

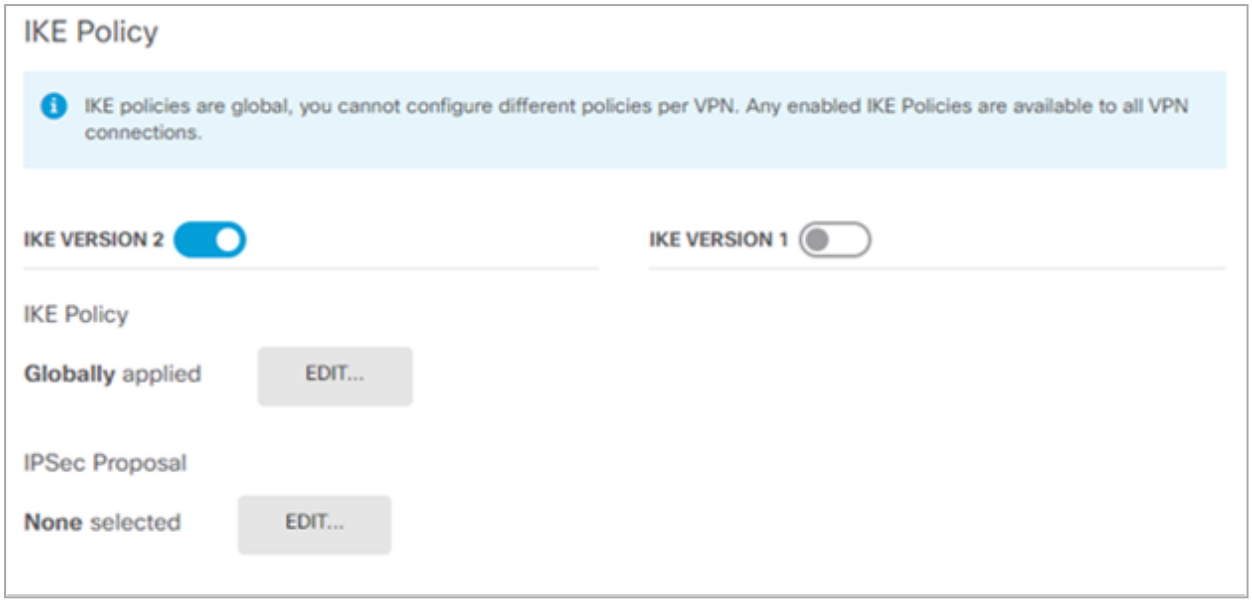
b. In the **Type** section, select **Route Based (VTI)**.

c. Expand **Local VPN Access Interface**, and click **Create new Virtual Tunnel Interface**.

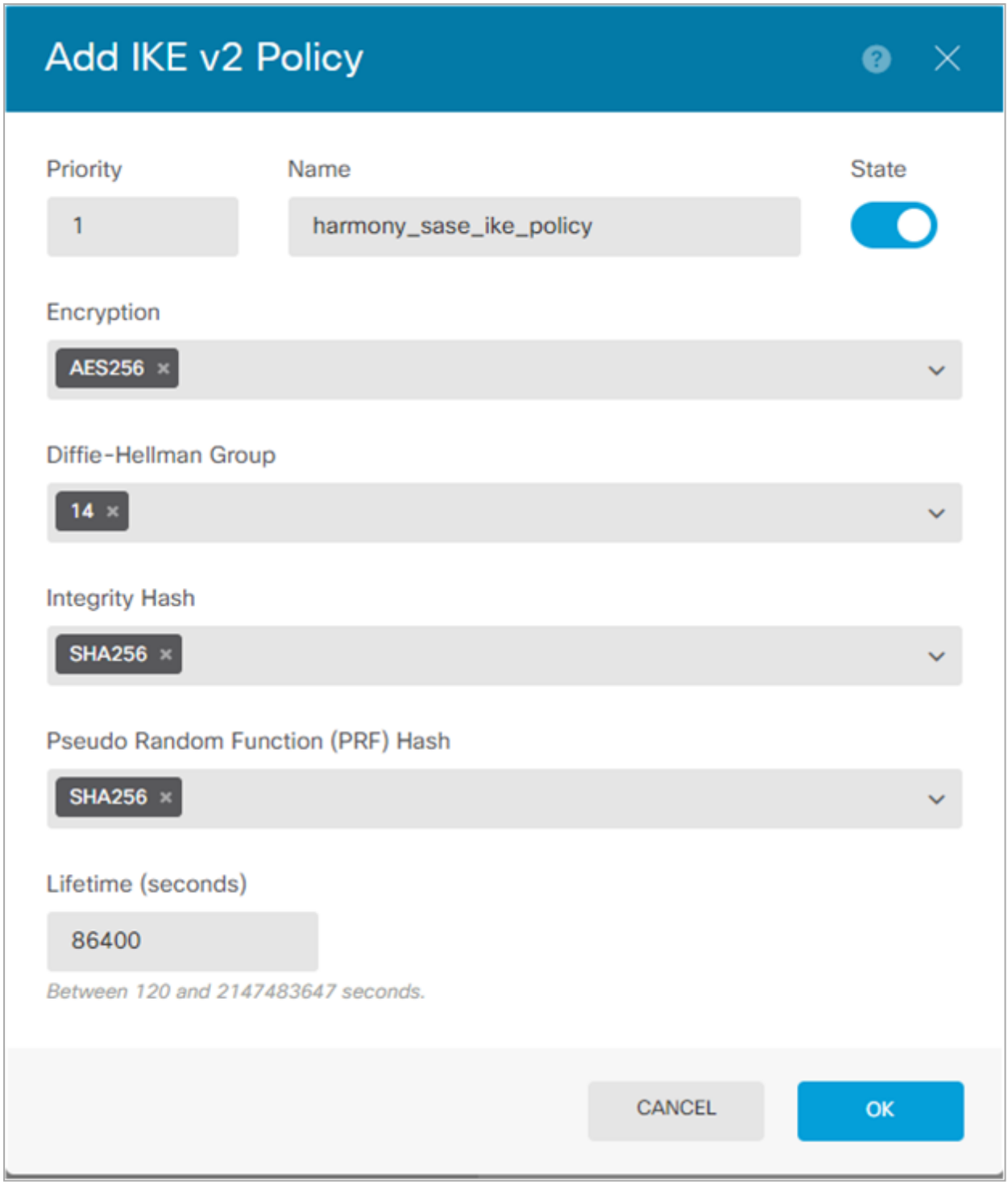


The **Create Virtual Tunnel Interface** window appears.

6. Enter a name for your VTI adapter, for example, harmony_sase_vti.
7. Turn on the **Status** toggle button.
8. Enter a tunnel ID.
9. Set the source to your outside interface.
10. Set the IP and Subnet Mask to `169.254.2.122 / 255.255.255.252`
11. Click **OK**.
12. From the **Create Virtual Tunnel Interface** list, select the newly created VTI object.
13. In the **Remote IP Address** field, enter your Harmony SASE gateway IP address (found in your Harmony SASE Admin Panel).
14. Click **Next**.



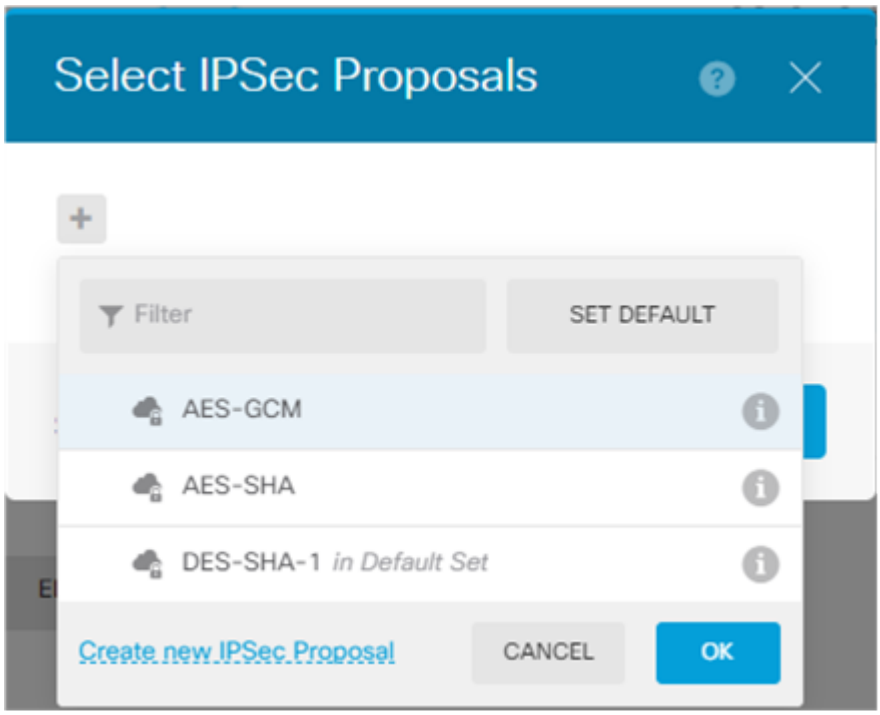
15. Make sure **IKE VERSION 2** is enabled.
16. In the **IKE Policy** section, for **Globally applied**, click **Edit**.
17. Create a new policy with the settings that match the Phase 1 settings on the Harmony SASE side. Specify these:



- **Priority**
- **Name**
- **State** - Enable
- **Encryption**: AES256
- **Diffie-Hellman Group**: 14

- **Integrity Hash**: SHA256
- **Pseudo Random Function (PRF) Hash**: SHA256
- **Lifetime**: 28800

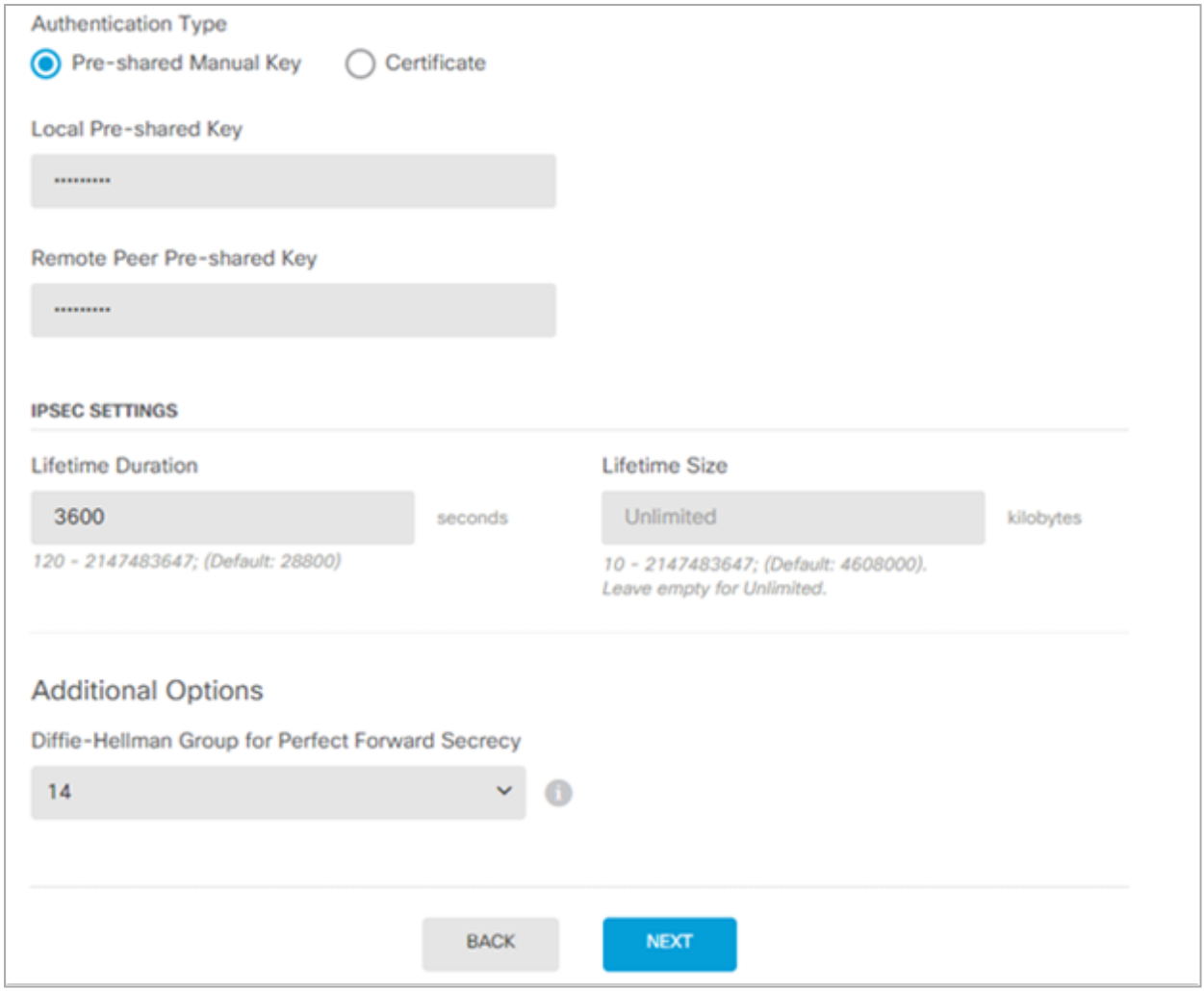
18. Click **OK**.
19. Click **Edit by IPSec Proposal**.



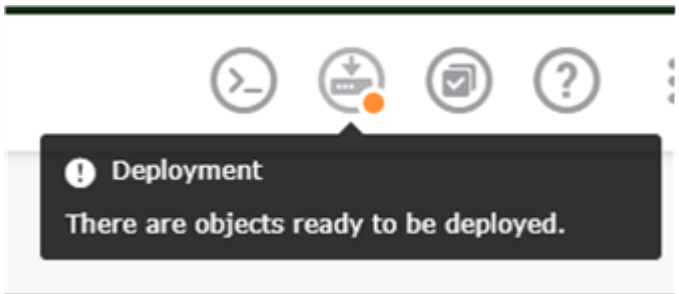
20. Click **Create new IPSec Proposal**.
21. Specify these:
    a. **Name**
    b. **Encryption**: AES256
    c. **Integrity Hash**: SHA256

    Note - Select the Encryption and Integrity Hash to match the Harmony SASE side for Phase 2.

22. Click **OK**.
23. In the **Authentication Type** section, select **Pre-shared Manual Key**.



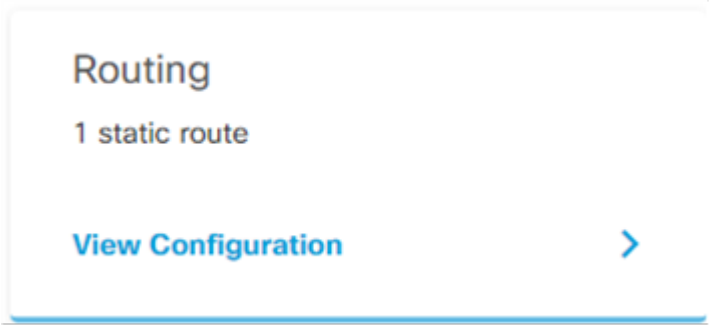
24. In the **Local Pre-shared Key** and **Remote Peer Pre-shared Key** fields, enter the Pre-shared Key that you created on the Harmony SASE portal.
25. In the **Lifetime Duration** field, enter **3600**.
26. In the **Diffie-Hellman Group for Perfect Forward Secrecy** field, enter **14**.
27. Click **Next**.
28. Click **Finish**.
29. Click  to deploy changes to apply the new tunnel.



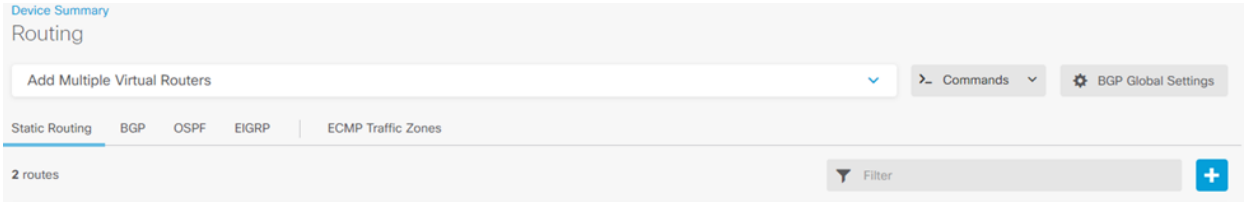
Configuring the Static Route in the Cisco Firepower

1. Select your device.

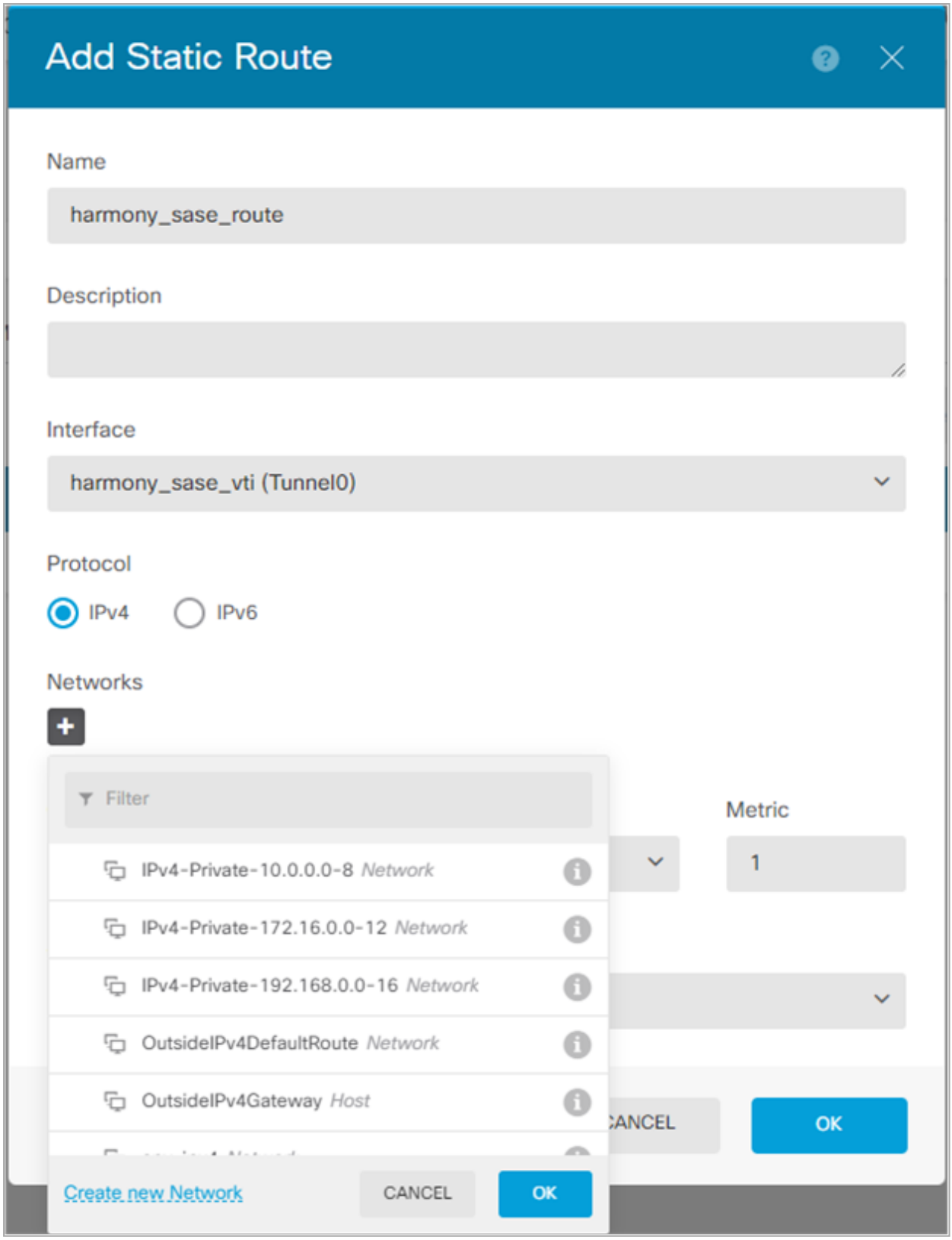
2. In the **Routing** section, click **View Configuration**.



3. Click + to add a new static route.



The **Add Static Route** window appears.



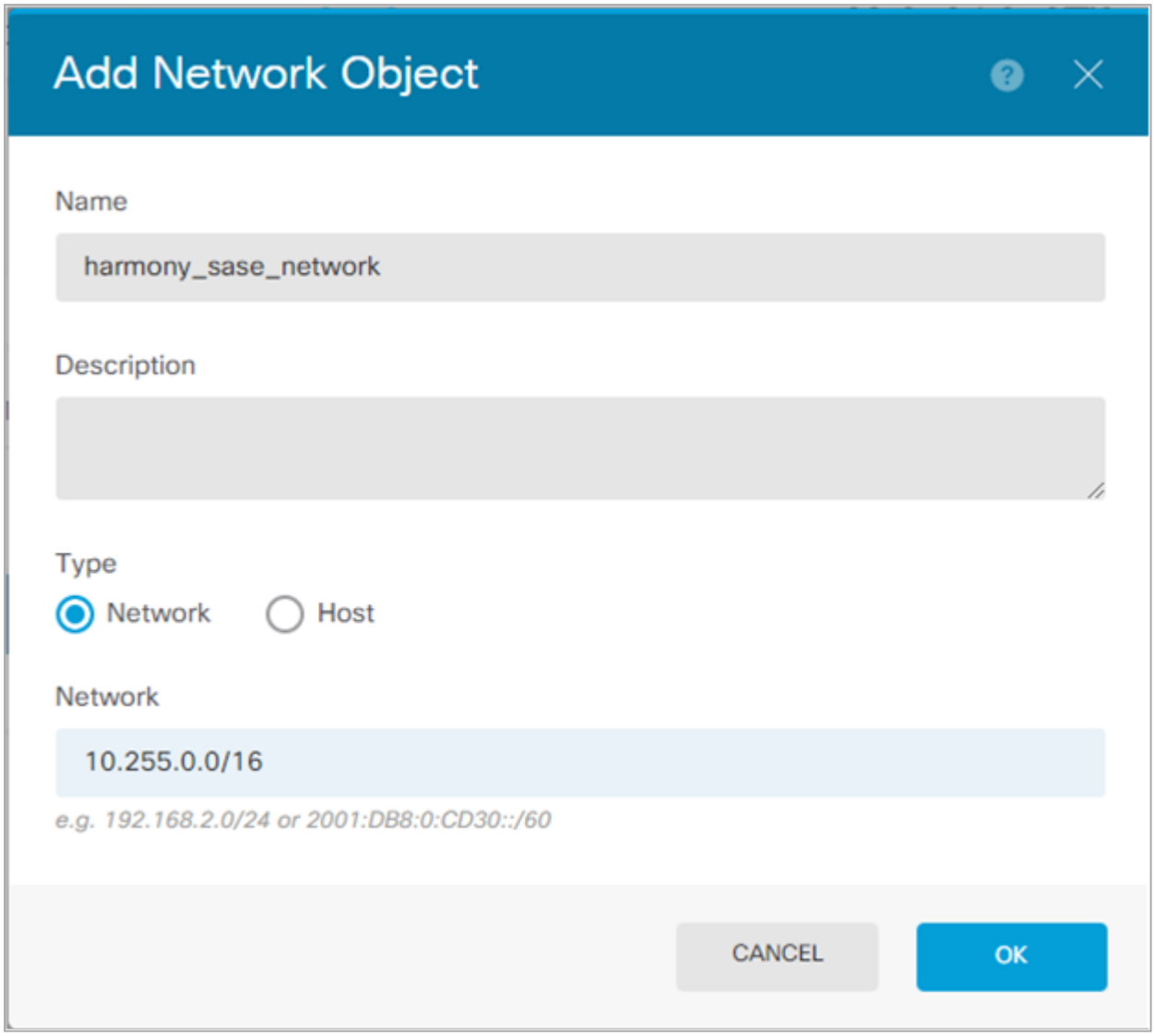
4. In the **Name** field, enter a name for your static route.
5. In the **Description** field, enter a description.

6. From the **Interface** list, select the interface you created in [Configuring the Tunnel in the Cisco Firepower](#) step 6.

7. In the **Networks** section, click  .

8. Click **Create new Network**.

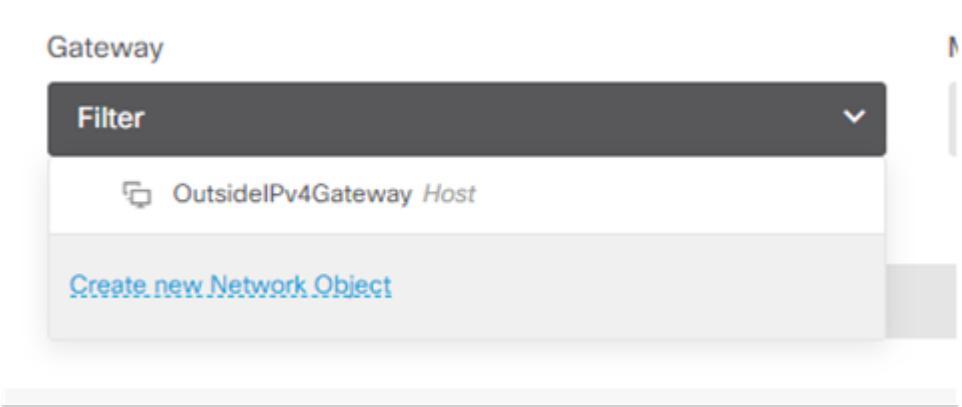
   The **Add Network Object** window appears.



9. Specify these:
   - **Name**
   - **Description**
   - **Type** - Network
   - **Network** - 10.255.0.0/16 (default)

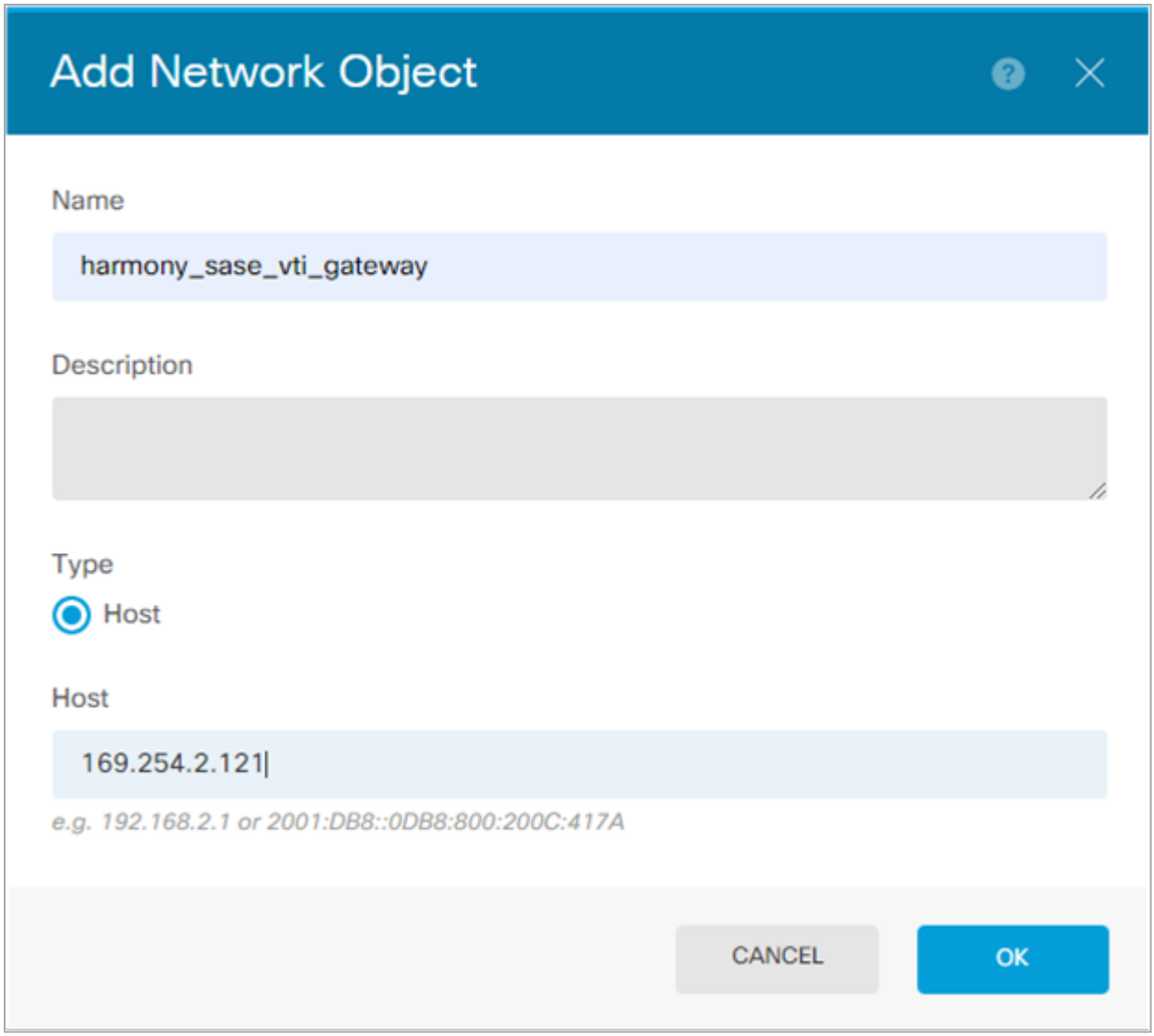
10. Click **OK**.

11. In the **Networks** section, click + .
12. Select the object you just created.
13. In the **Gateway** section, click **Create new Network Object**.



The **Add Network Object** window appears.

14. Specify these:



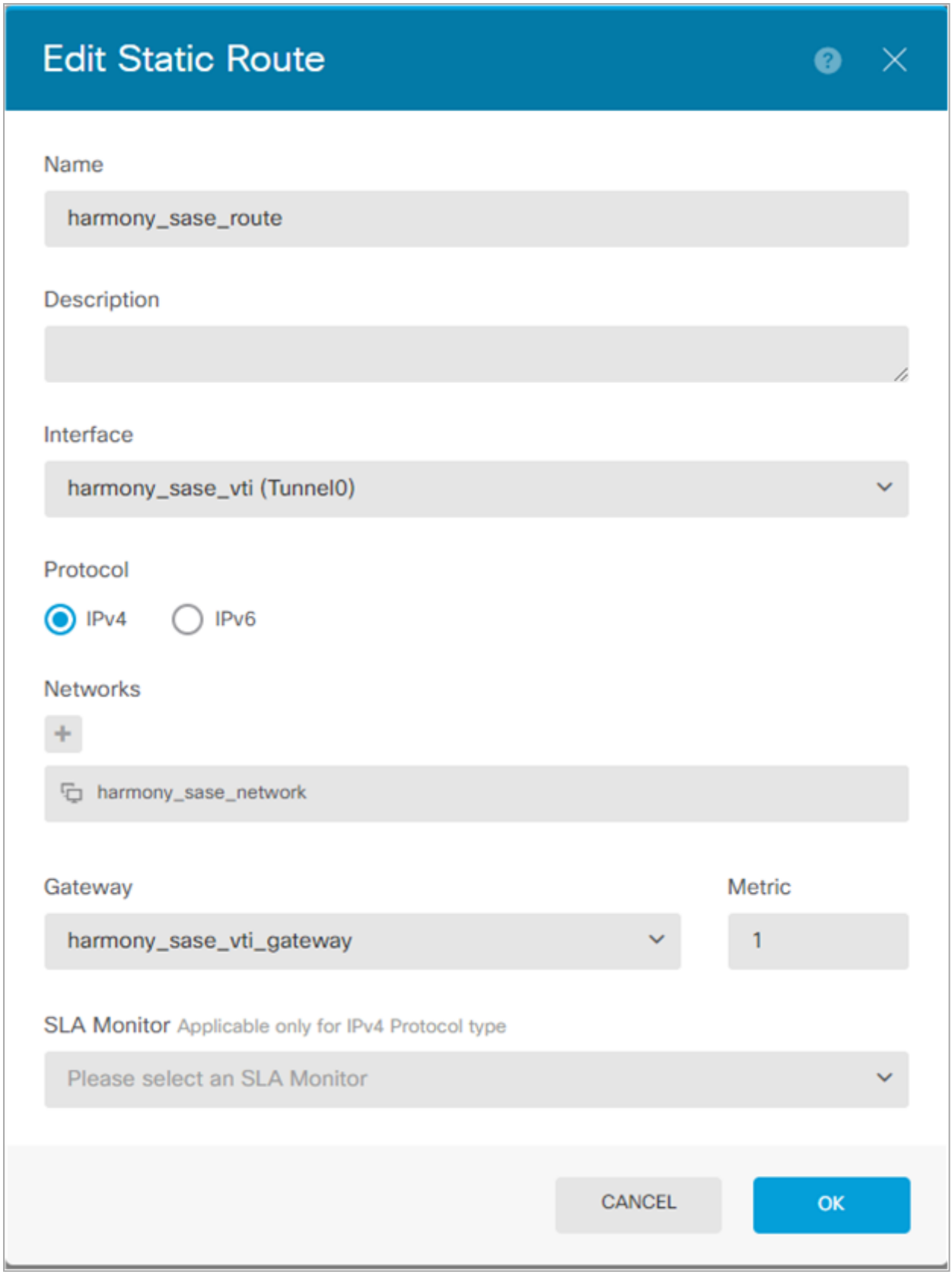
a. Name. For example, harmony_sase_vti_gateway

b. Description

c. Type - Host

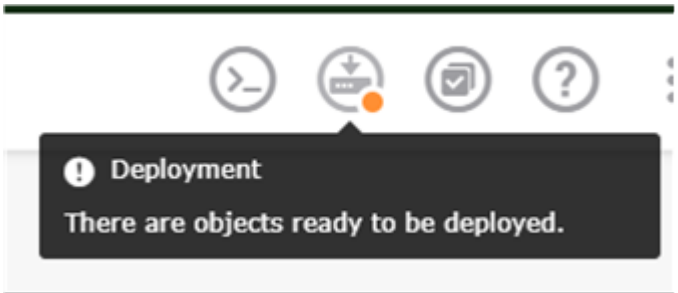
d. Network - 169.254.2.121 (this is the corresponding side of your VTI adapter)

15. Click **OK**.



The new route is added.

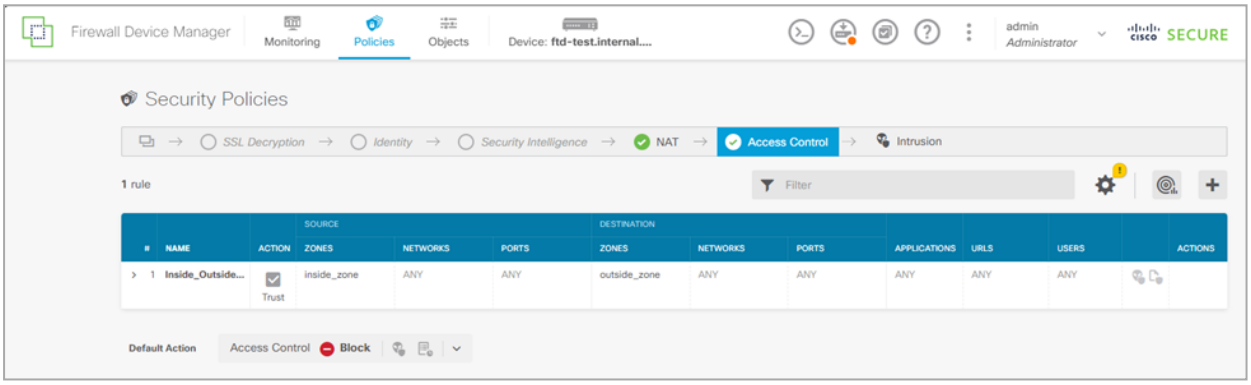
16. Click  to deploy changes to apply the new route.



Configuring Firepower Policies Allowing Traffic Flow

To configure Cisco Firepower policies to allow traffic to flow:

1. Go to **Policies** and click + to add a new access rule.



2. Configure either 1 bidirectional rule or 2 unidirectional rules.

   For example: Creating a single bidirectional rule.

   a. Enter an order number. Make sure this rule is not after a block rule that affects this traffic.

   b. Enter a title. For example, harmony_sase_allow.

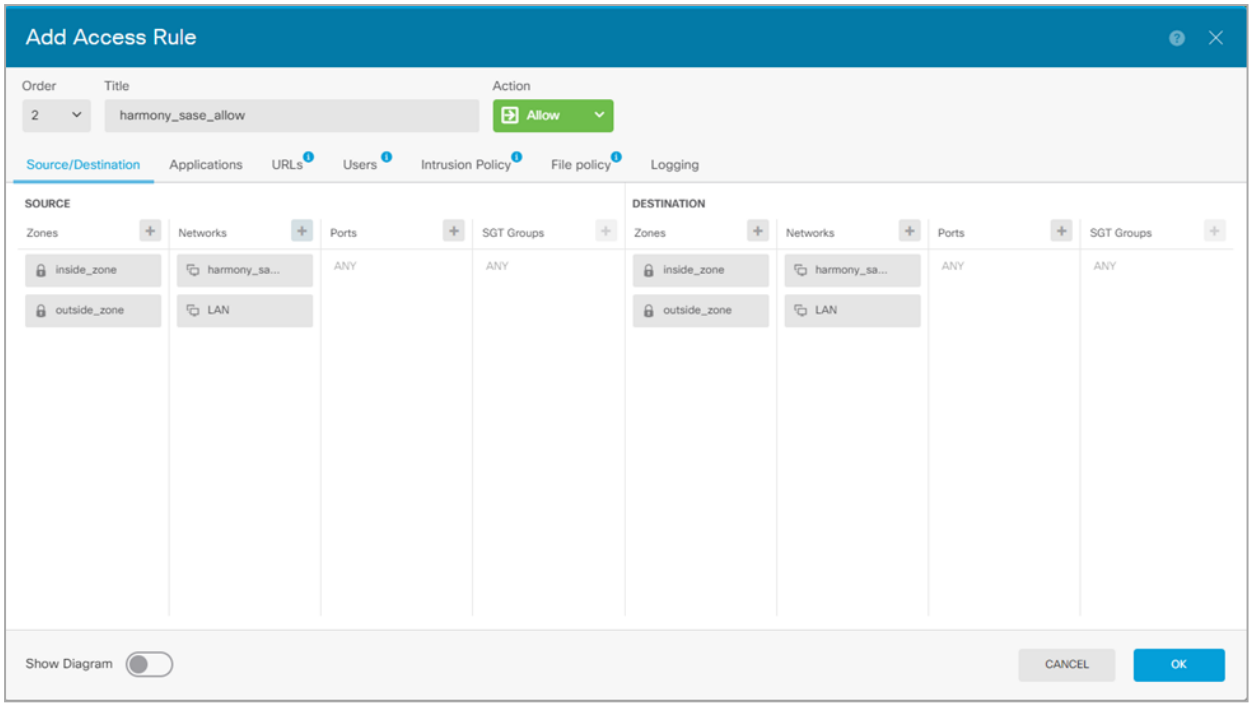
   c. Set your Source zones and Networks.

   d. Add an entry for inside_zone and outside_zone.

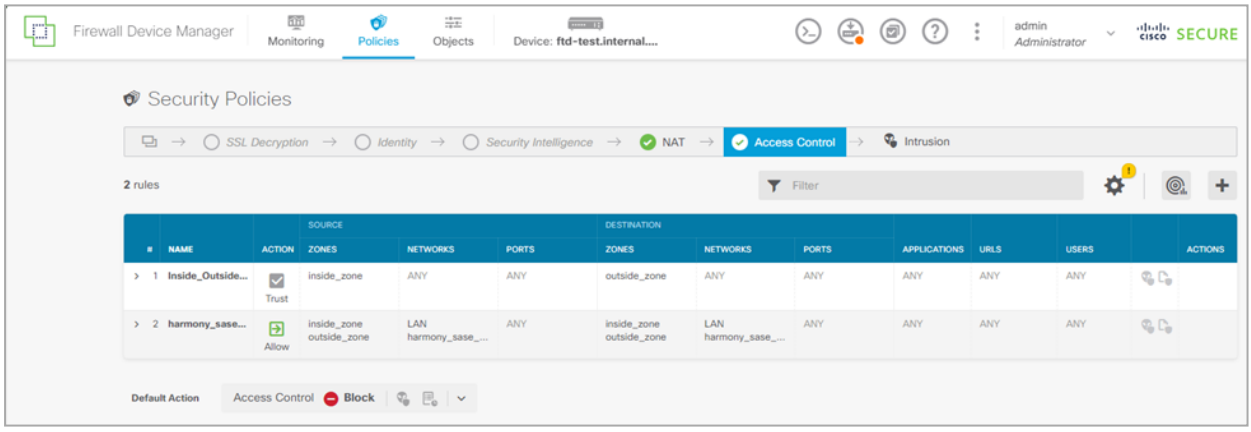
   e. Add a network entry for your harmony_sase_network object.

   f. Repeat the same for the Destination.

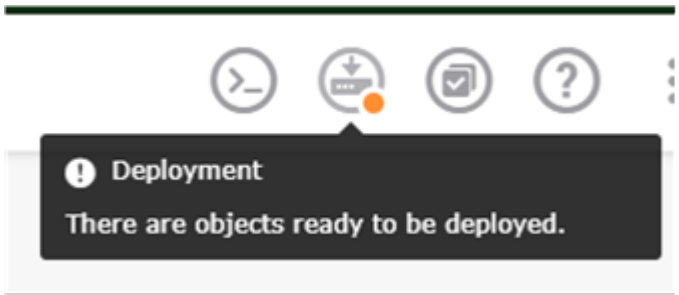
3. Click **OK**.



Once you add the rule, the table should display:



4. Click  to deploy changes to apply the new route.



Configuring Check Point Cluster VIP Redundant IPsec Tunnel

This topic explains how to establish a redundant Site-to-Site tunnel between your Harmony SASE Network and Check Point Firewall cluster VIP.

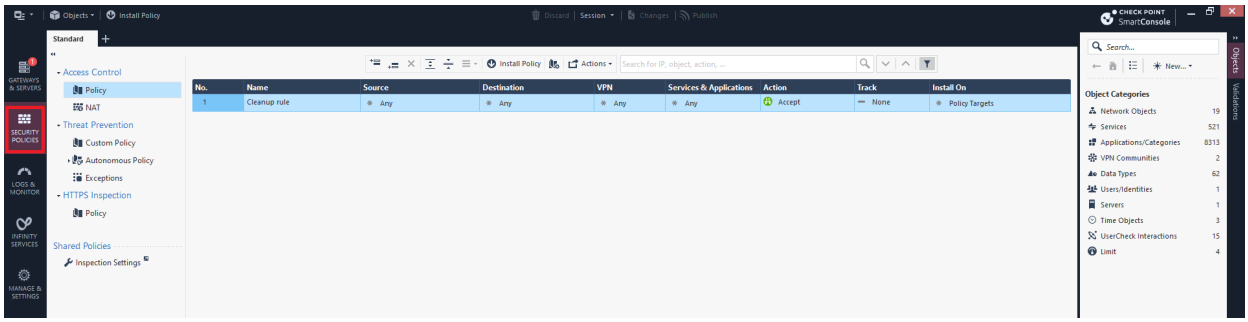
Pre-requisites

- Harmony SASE Administrator Portal account.
- Device with Harmony SASE Agent installed.
- Administrator account with Firewall, Router, and Cloud Management Portal.
- A cluster of two Quantum gateways, behind a single VIP.
- Configuration with ISP redundancy PMTR-68991 is not supported.

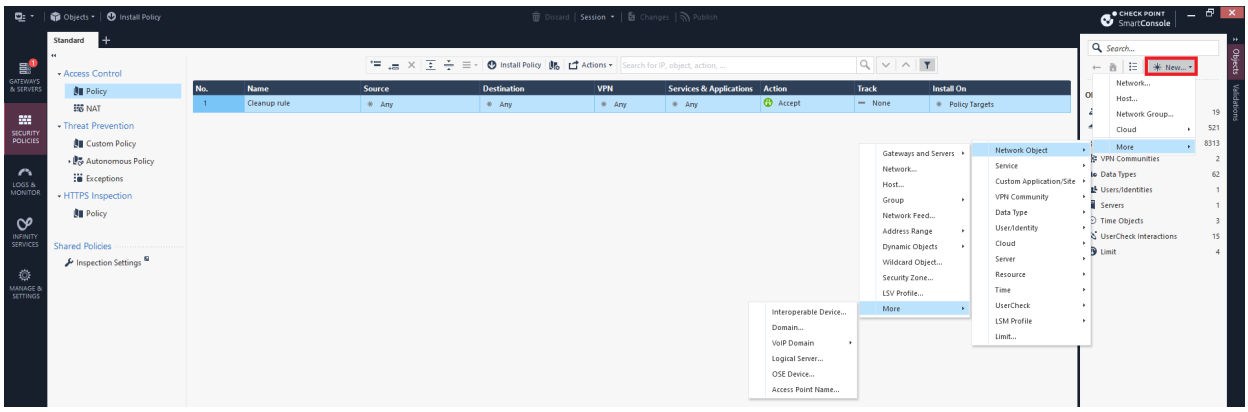
Part 1 - Configuration in SmartConsole

Step 1: Creating Interoperable Device Object in the Check Point SmartConsole

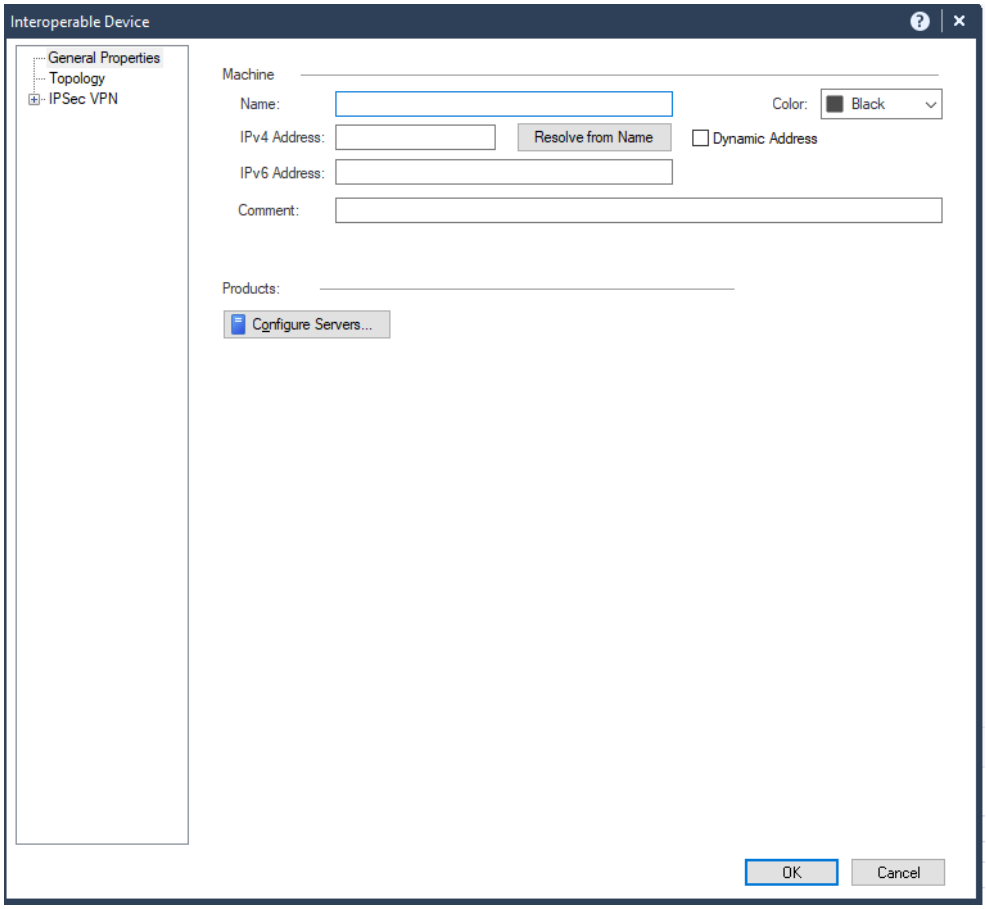
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



3. In the Objects pane, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** window appears.



a. In the **Name** field, enter a name for the Harmony SASE gateway, for example, Harmony_SASE_Gateway.

b. In the **IPv4 Address** field, enter the Harmony SASE gateway public IP address.

   To find the Harmony SASE Gateway public IP Address:

   i. Access the Harmony SASE Administrator Portal and click **Networks**.

   ii. Select the network.

   iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

c. Click **OK**.

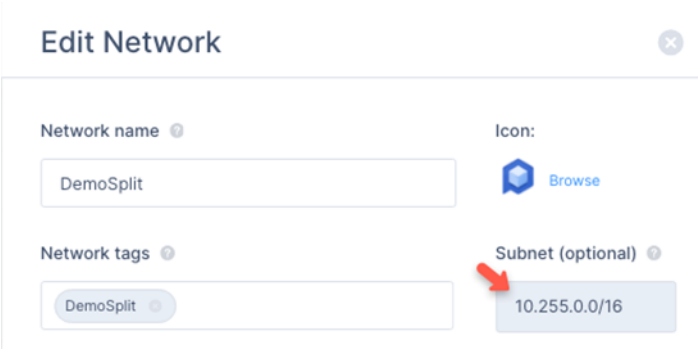
Step 2: Adding Harmony SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object

1. Log in to the Harmony SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network:

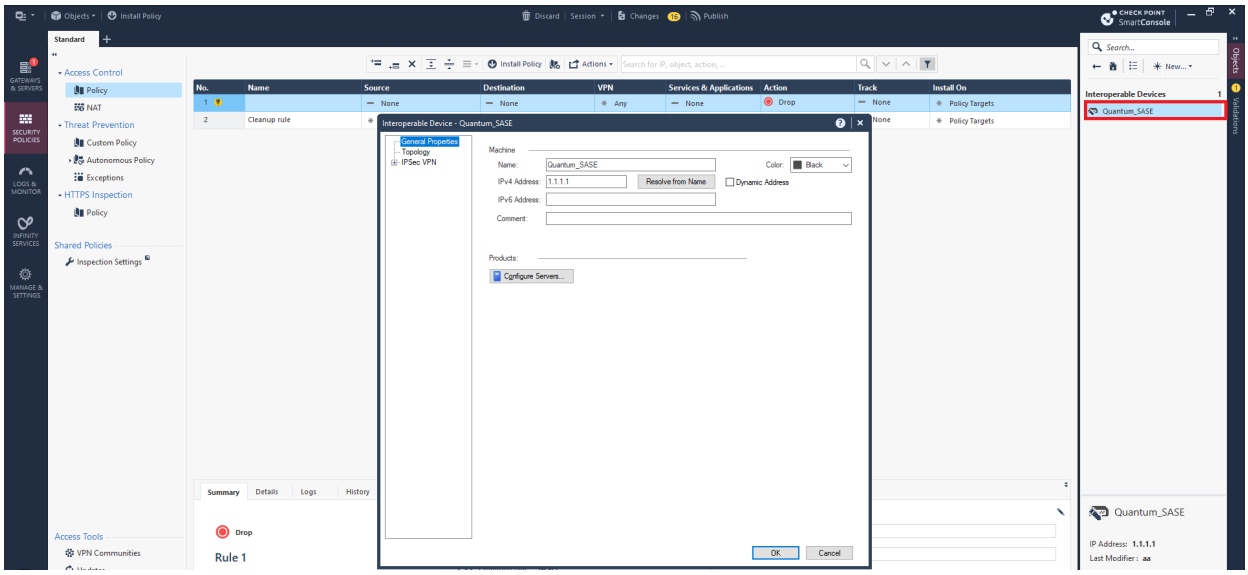
a. Select a network, scroll to the end of the row and click ··· .

b. Select **Edit Network.**

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.

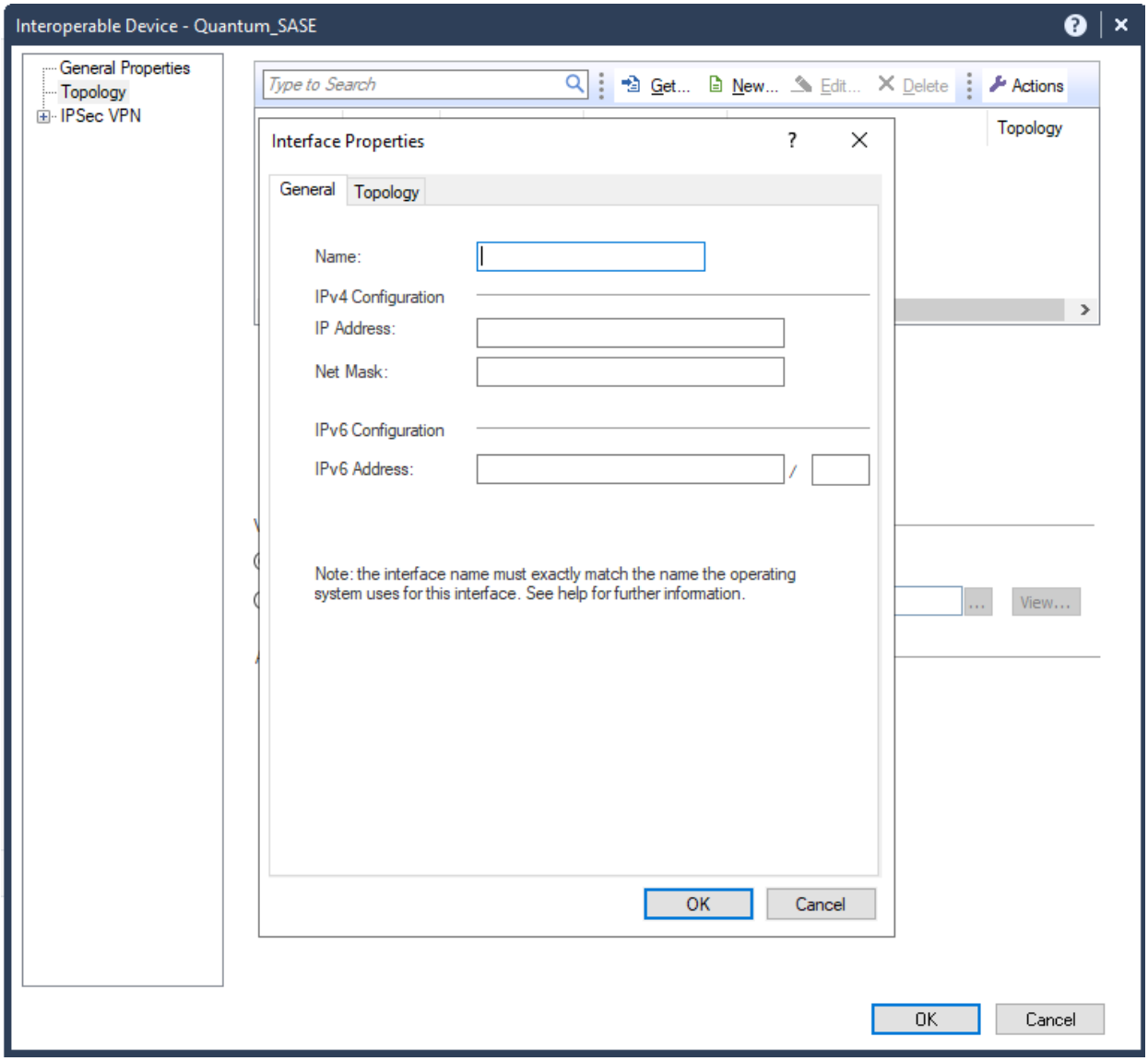


4. Open the network object that you created.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

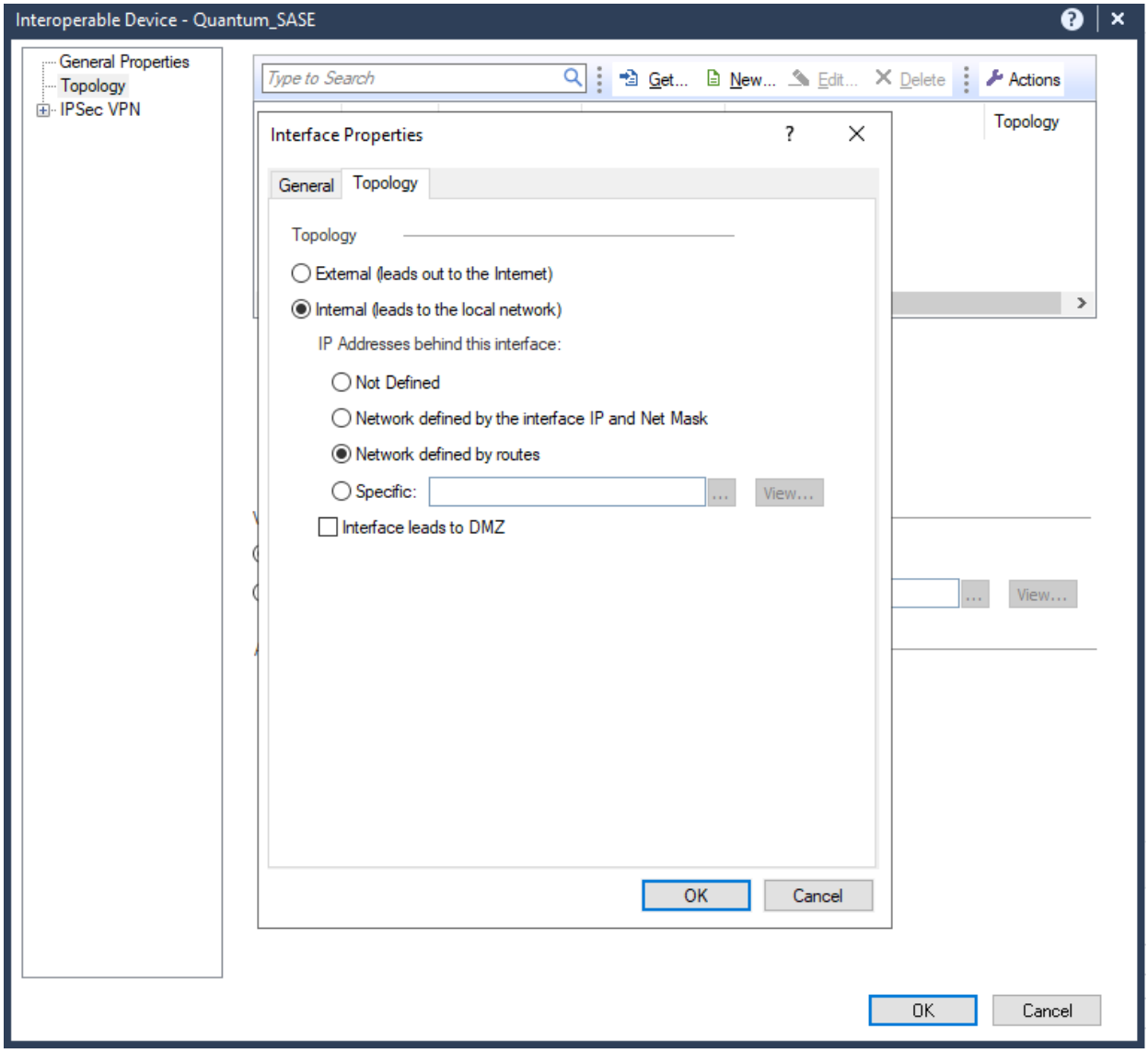
5. Click **Topology > New**.



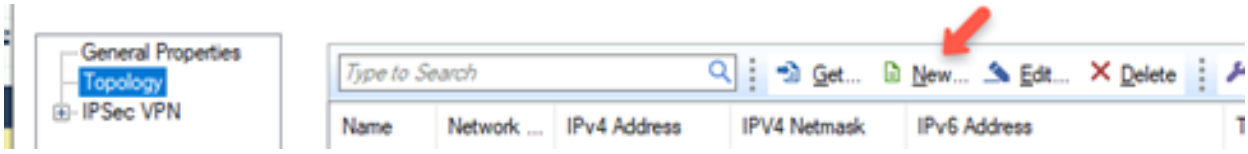
6. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	10.255.0.0
Net Mask	255.255.0.0

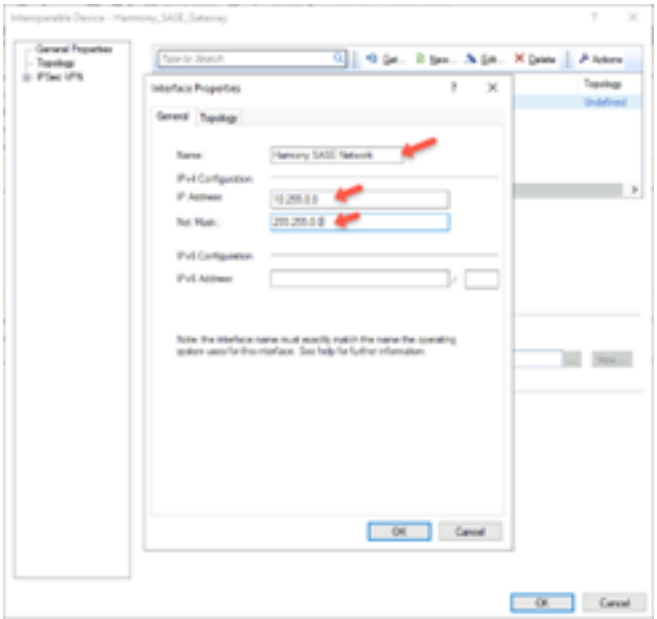
7. In the **Topology** tab, select **Internal (leads to the local network)** and select **Network defined by the interface IP and Net Mask**.



8. Click **OK**.
9. Click **Topology** > **New**.

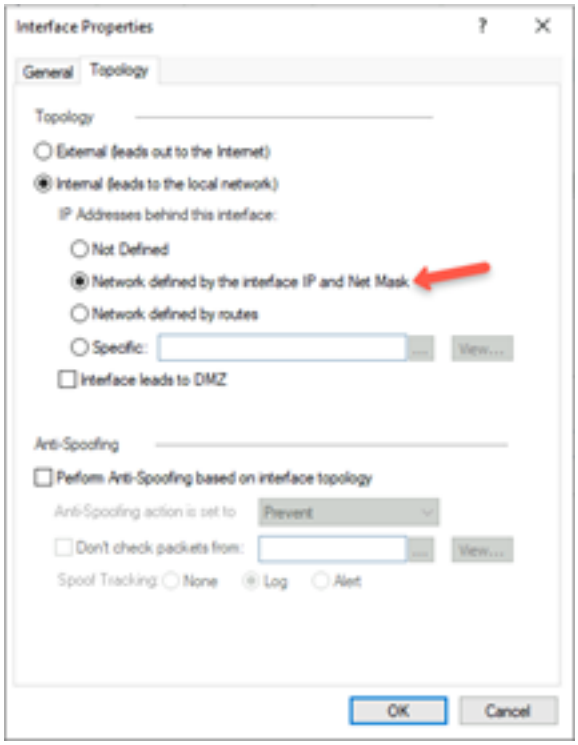


10. In the **General** tab:



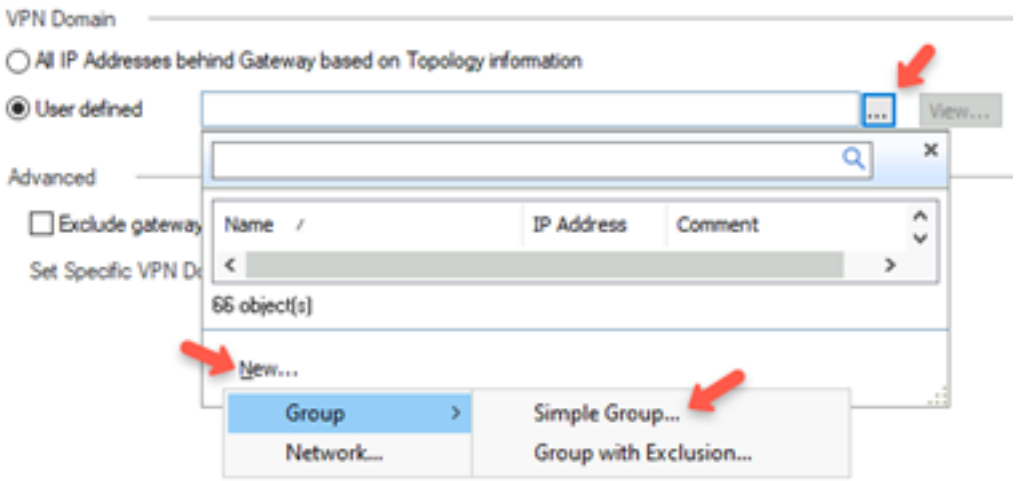
Field	Enter
Name	Name for the topology.
IP Address	Public IP address of the Harmony SASE gateway.
Net Mask	255.255.255.255

11. In the **Topology** tab, select **External (leads to the local Internet)**.



12. Click **OK**.

13. Click **Topology** > **New**.
14. In the **General** tab, enter these:
    a. **Name** - Name for the topology, for example, Harmony_SASE_Gateway.
    b. **IP Address** - Public IP address of the Harmony SASE gateway.
    c. **Net Mask** - 255.255.255.255
15. Click the **Topology** tab.
16. Select **External (leads out to the internet)**.
17. Click **OK**.
18. In the **VPN Domain** section, select User defined and click ··· .
19. Click **New** and go to **Group** > **Simple Group**.



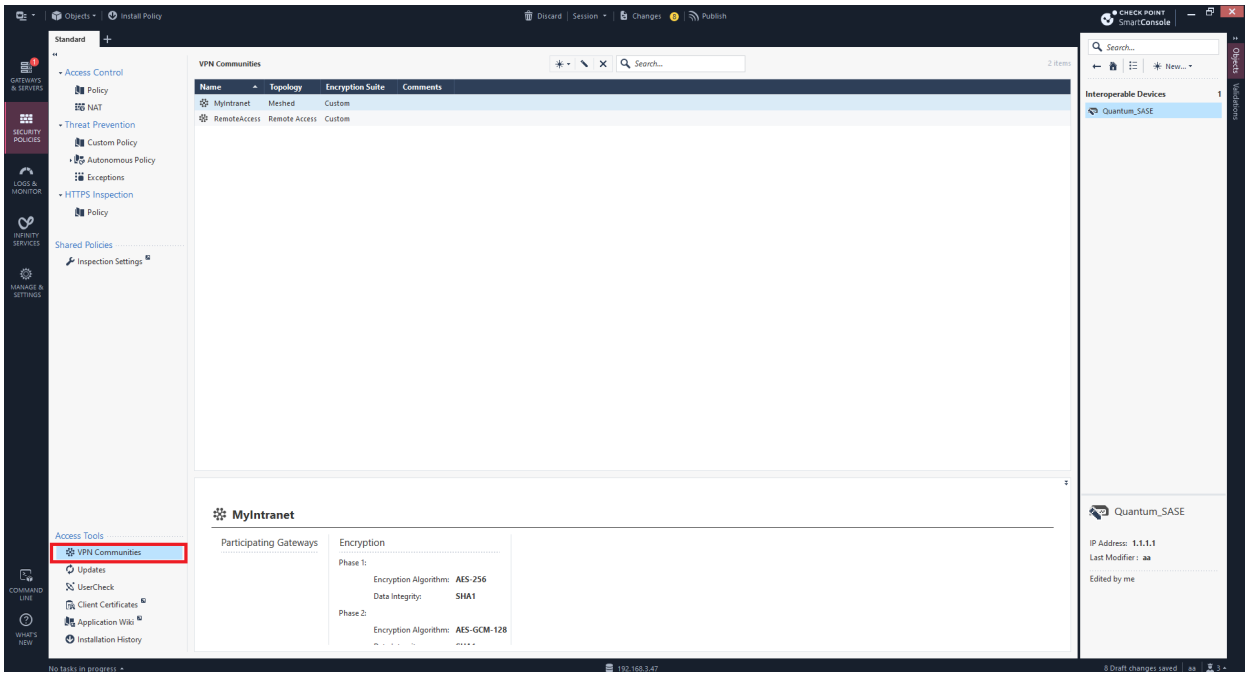
The **New Network Group** window appears.

20. In the **Enter Object Comment** field, enter a name, for example, HSASE_VTI, and click **OK**.

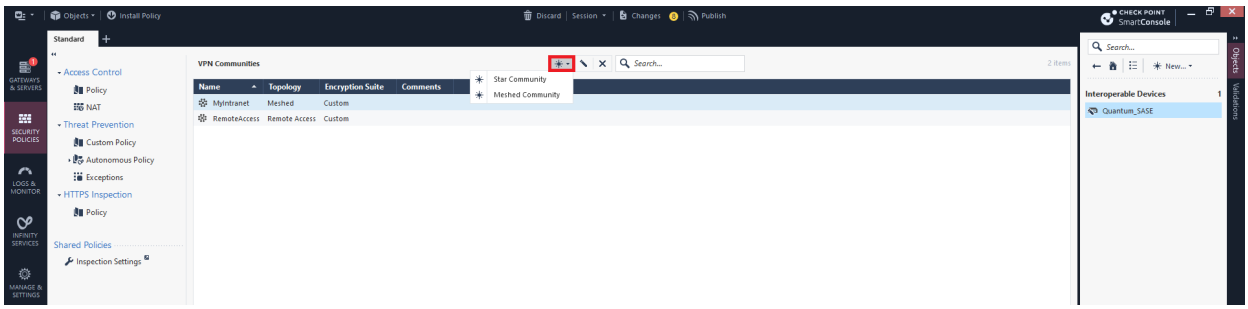
21. For the other Harmony SASE Gateway and Check Point Gateway, follow the same procedure in **Creating Interoperable Device Objects in the Check Point SmartConsole** and **Adding Harmony SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object sections**.
22. Publish and install the policy.

Step 3: Creating VPN Start Community

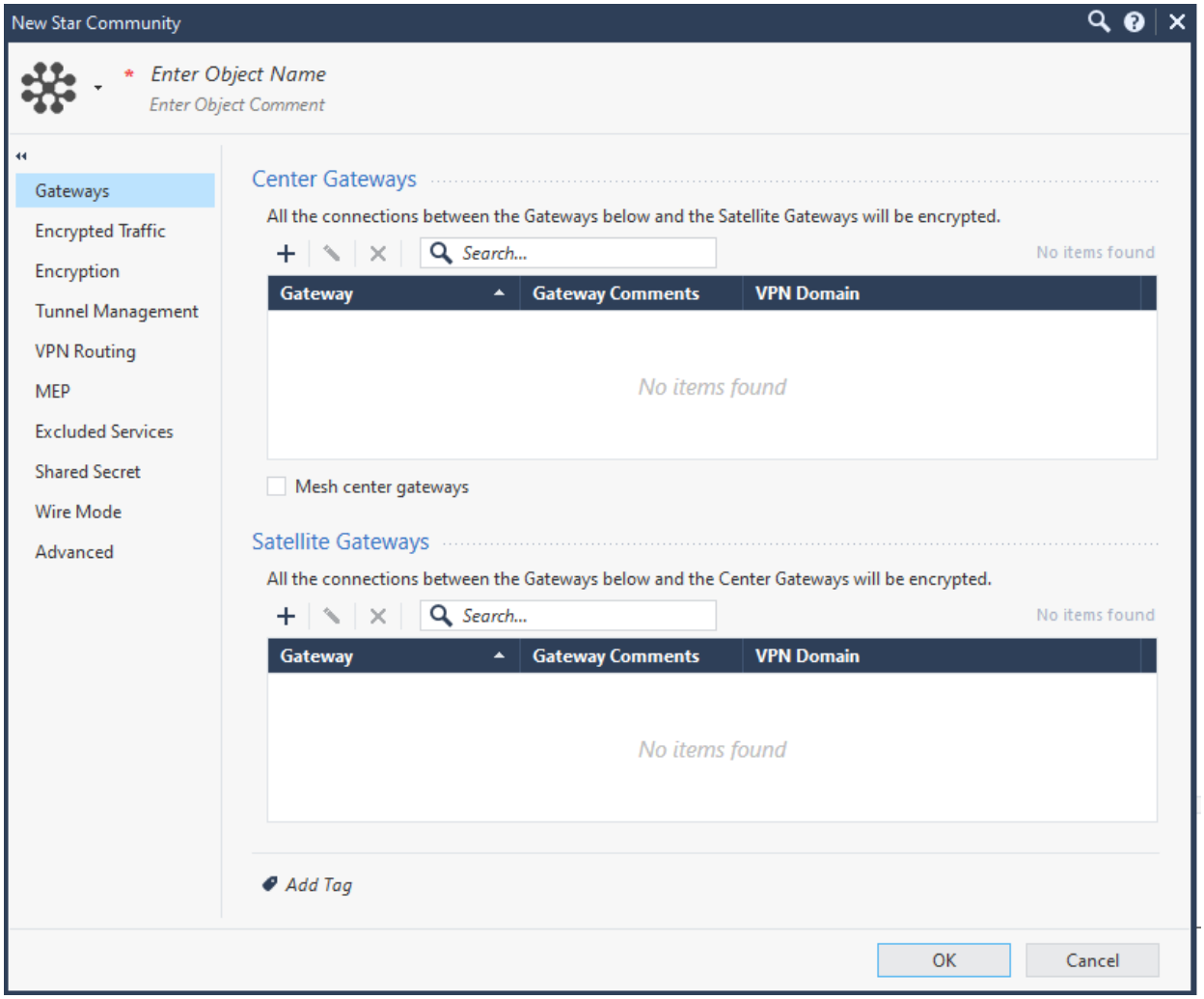
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools** > **VPN Communities**.



4. Select an object, click **New** and go to **More** > **VPN Community** > **Star Community**.



The **New Star Community** window appears.

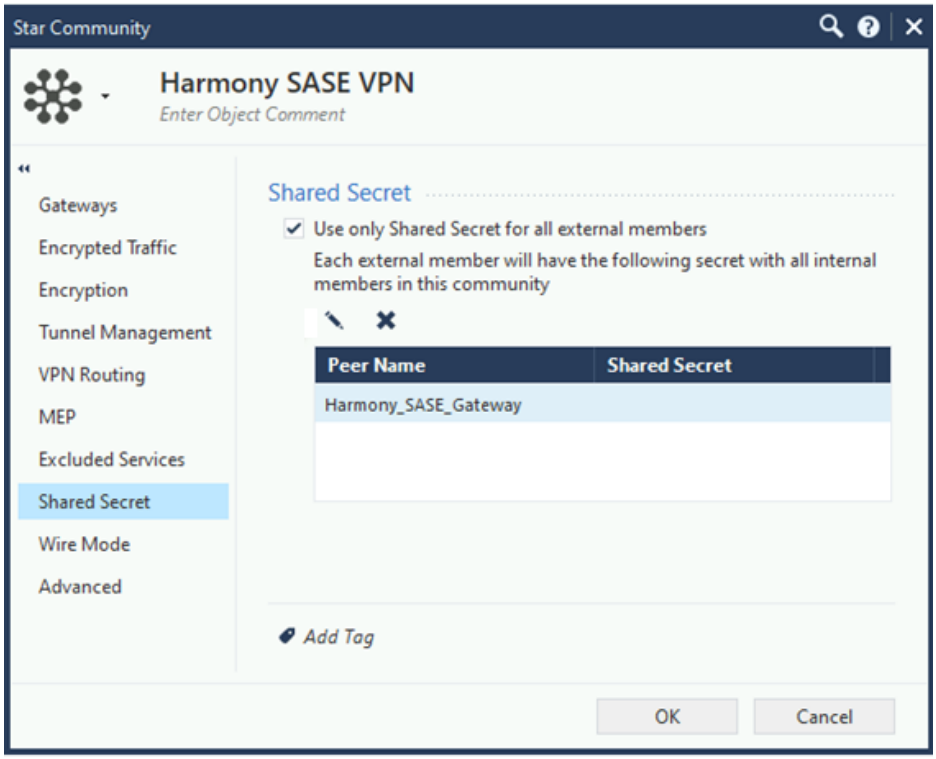


5. In the **Enter Object Name** field, enter an object name for the VPN Start Community, for example, Harmony_SASE_VPN.

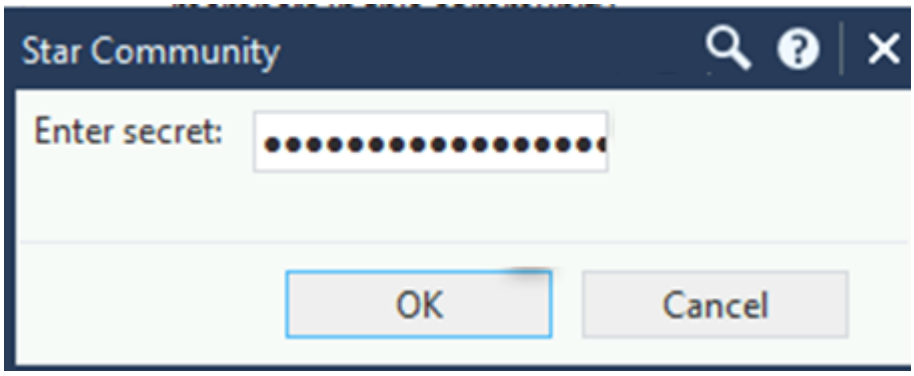
6. Under **Center Gateways**, click + and add the Check Point Gateway.

7. Under **Satellite Gateways**, click + and add the Interoperable Device Object created for the Check Point Gateway. See Step 1.

8. Go to **Shared Secret** and click to edit the shared key.



9. In the **Enter secret** field, enter an appropriate key.

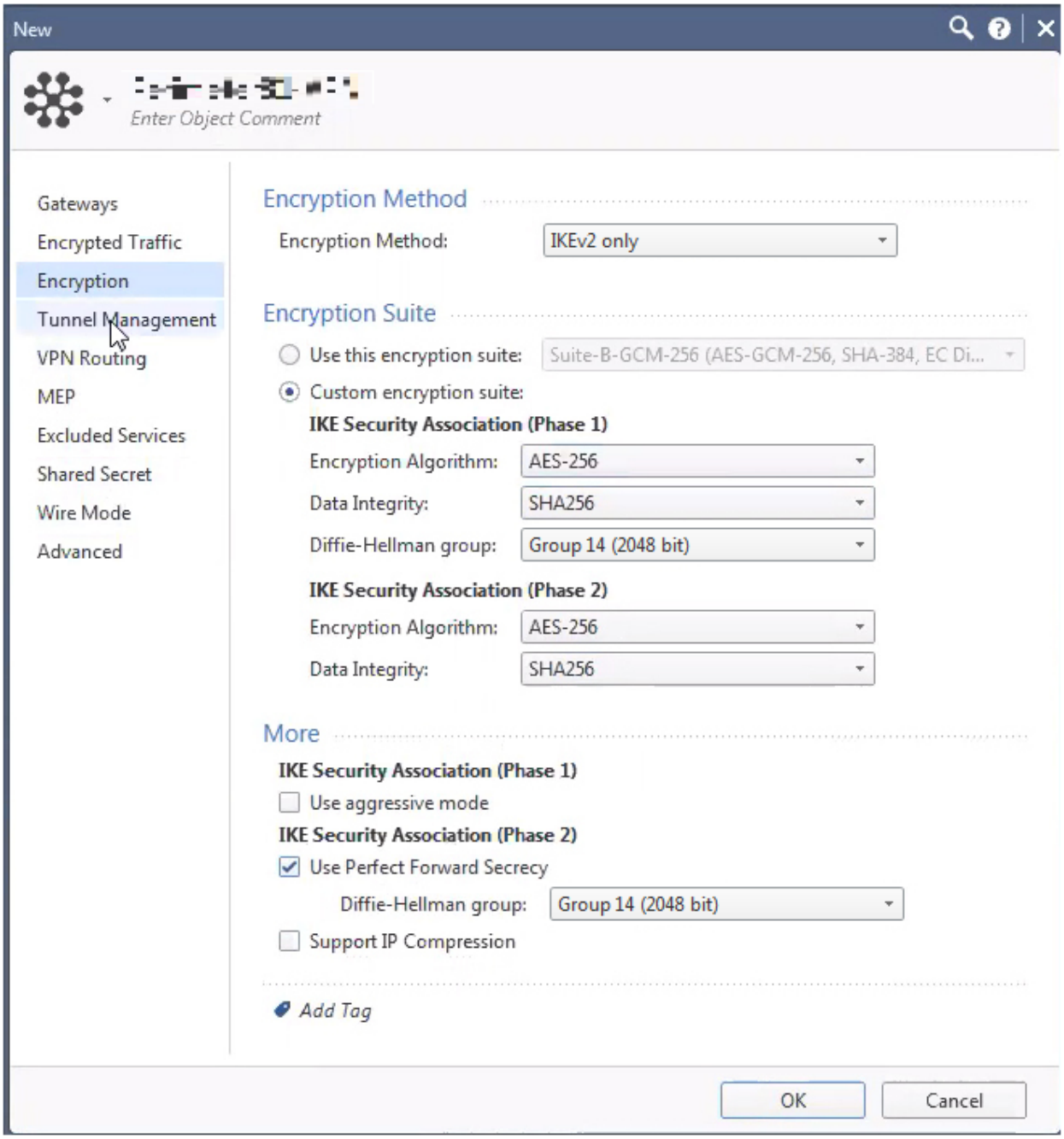


Notes:

- Copy the key as it is required while configuring the IPsec Tunnel in the Harmony SASE Administrator Portal.
- Check Point recommends that the share secret key is at least 20 characters in length.

10. Click **OK**.

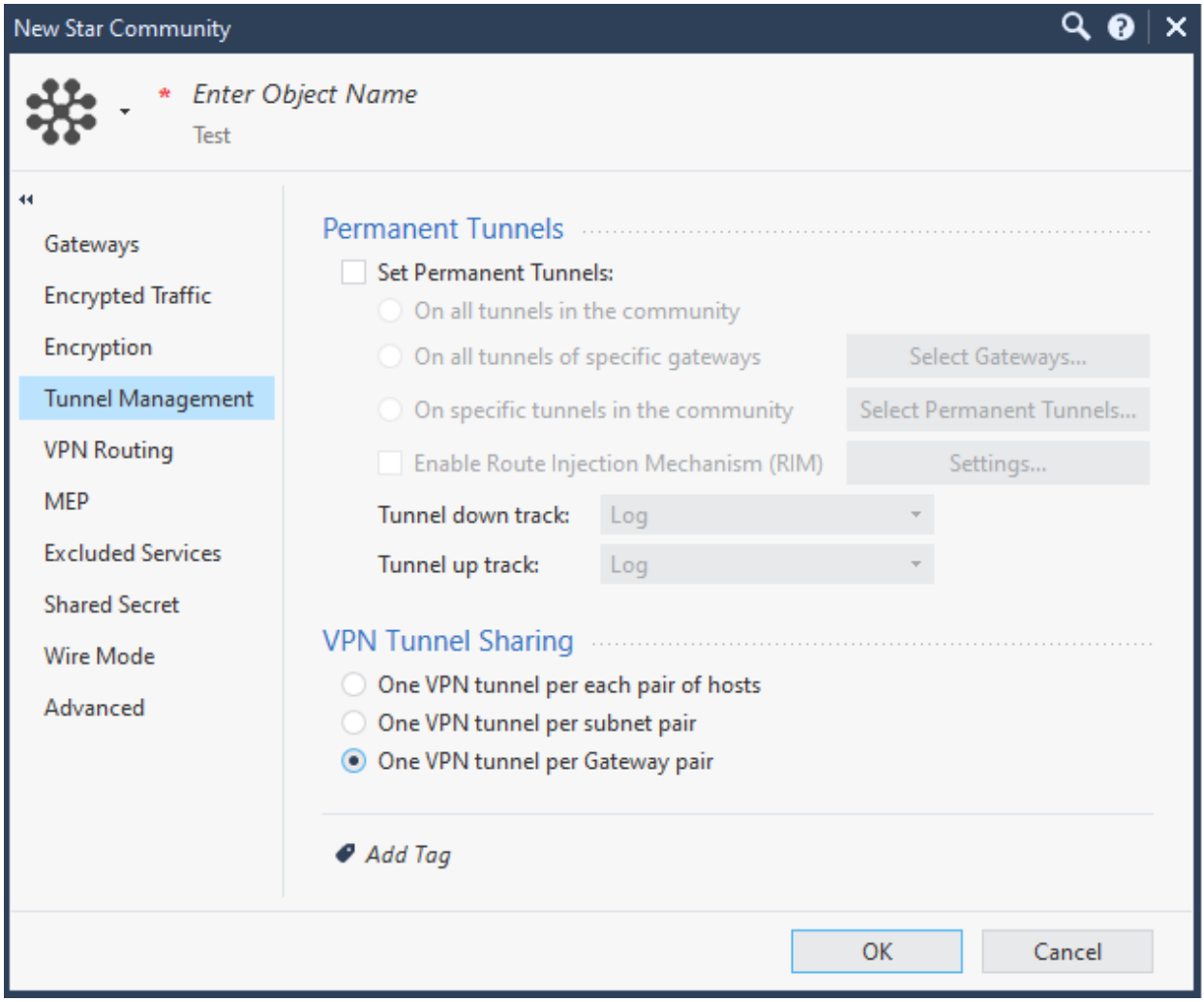
11. From the left navigation pane, click **Encryption** and do these:



Field	Enter
Encryption Method	IKEv2 only
Custom encryption suite	
IKE Security Association (Phase 1)	
Encryption Algorithm	AES-256
Data Integrity	SHA256

Field	Enter
Diffie Hellman group	Group 14 (2048 bit)
IKE Security Association (Phase 2)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
More	
IKE Security Association (Phase 2)	
Use Perfect Forward Secrecy	
Diffie Hellman group	Group 14 (2048 bit)

12. Click **Tunnel Management** and under **VPN Tunnel Sharing**, select **One VPN tunnel per Gateway pair**.



Important - Make sure that you enter the remote subnets specified here in the Harmony SASE Administrator Portal. A mismatch can disconnect the tunnel.

13. Click **Advanced**.
    a. In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480**.
    b. In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security associations every (seconds)** field to **3600**.
14. Click **OK**.
15. Publish and install the policy.

Step 4: Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the Harmony SASE Network 10.255.0.0/16 to specific destinations and services. Note that the network configuration may differ if you have not changed the default settings during Harmony SASE network creation. For testing purposes, you should initially allow any/any or allow before making the firewall policy more restrictive.

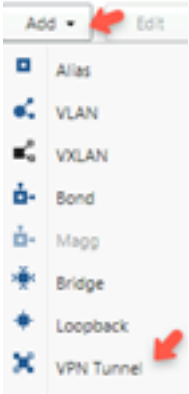
   Note - The network configuration differs if you have not changed the default settings during Harmony SASE network creation. For testing purposes, you should initially allow any/any or allow ping before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

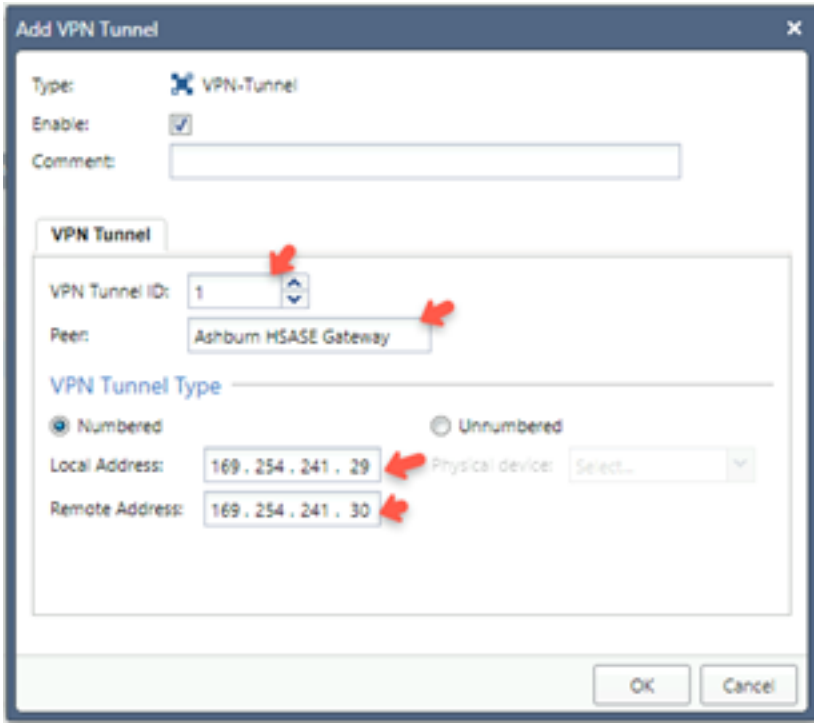
Step 5: Configuring VPN Tunnel Interface and BGP Configuration

1. Log in to the Check Point Gaia Portal of the first Check Point Gateway.
2. Click **Network Interfaces**.
3. From the **Add** list, select **VPN Tunnel**.



The **Add VPN Tunnel** page appears.

4. Enter these:



   a. **VPN Tunnel ID** - Select a unique ID.

   b. **Peer** - Name of the interoperable device previously created for the first Harmony SASE Gateway.

   c. **VPN Tunnel Type** - Numbered.

   d. **Local Address** - Internal address for the Quantum Gateway (within 169.254.x.x/30 ranges).

   e. **Remote Address** - Internal address for the Harmony SASE Gateway (within 169.254.x.x/30 ranges, corresponding to the above).

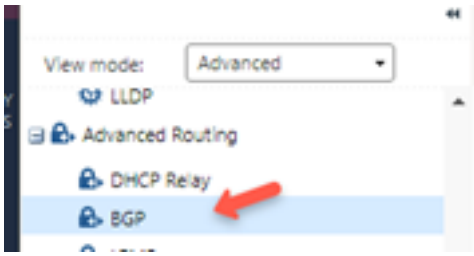
5. Click **OK**.

6. Repeat steps 3 through 5 and create the second VPN Tunnel.

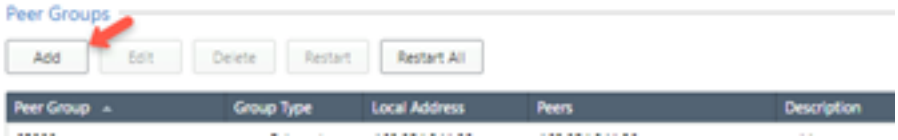
7. Perform steps 1 through 6 on the second Check Point Gateway Gaia Portal.
8. Log in to the Check Point SmartConsole.
9. Open the Gateway Cluster Properties.
10. Go to **Network Management**.
11. From the **Get Interfaces** List, select **Ger interfaces Without Topology**.
12. Once the two VPN Tunnel Interfaces are added, click the first tunnel interface.
13. Go to **General**.
14. In the **IPv4** field, add the Virtual IP (VIP) that matches the member IP addresses.
15. Repeat steps 12 through 14 on the second tunnel interface.
16. Publish and install the policy.

Step 6: Configuring BGP Configuration

1. Log in to the Check Point Gaia Portal of the first Check Point Gateway.
2. Go to **Advanced Routing** and select **BGP**.

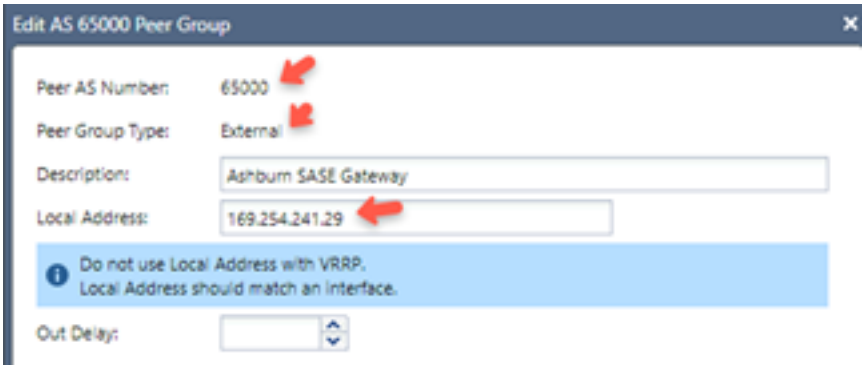


3. In the **Peer Groups** section, click **Add**.



4. Enter these:
   a. **Peer AS Number** - The AS Number of the Harmony SASE network. If not set already, enter **65000**.
   b. **Peer Group Type** - External.

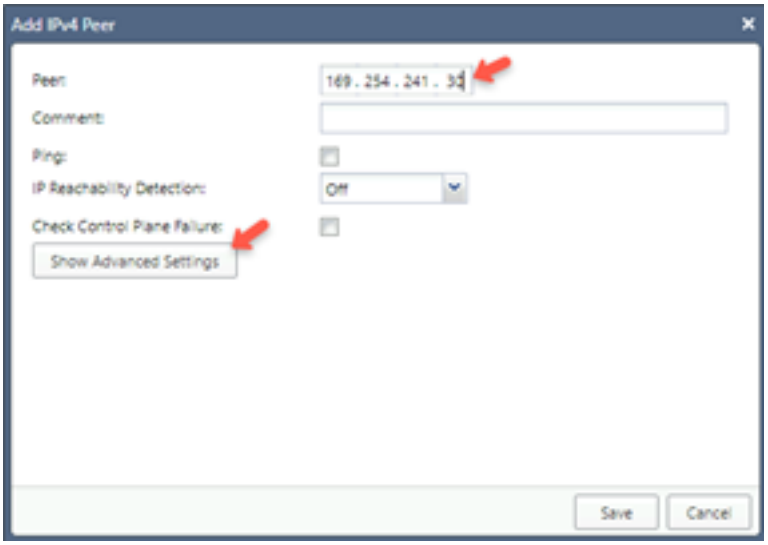
c. **Local Address** - The local address entered in the Configuring VPN Tunnel Interface section step 14.



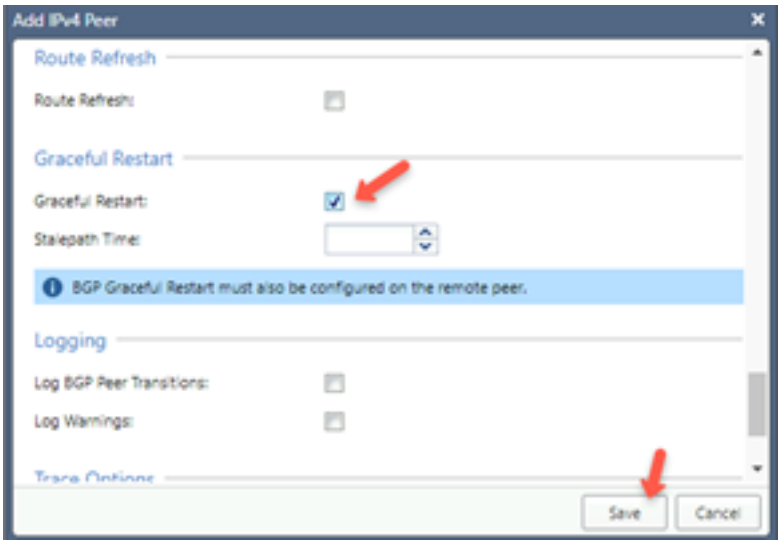
5. Click **Add Peers**.

6. Enter these:

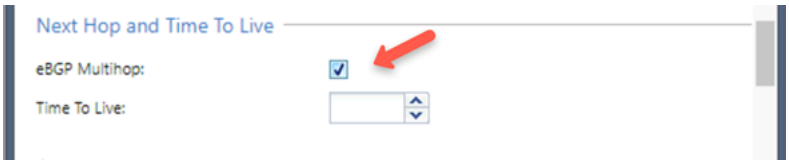
   a. In the **Peer** field, enter the Remote Address set under the VTI configuration in Step 4 and click **Show Advanced Settings**.



b. Select the **Graceful Restart** checkbox.

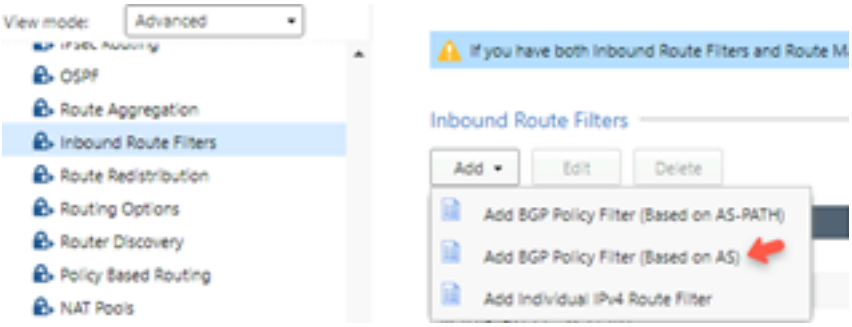


c. Select the **eBGP Multihop** checkbox and click **Save**.



Note - Without Multihop enabled,the BGP session cannot be established.

7. Repeat step 6 and add the address of the second interface remote address.
8. From the **View mode** list, select **Advanced Routing** and click **Inbound Route Filter**.
9. From the **Add** list, select **Add BGP Policy Filter (Based on AS)**.



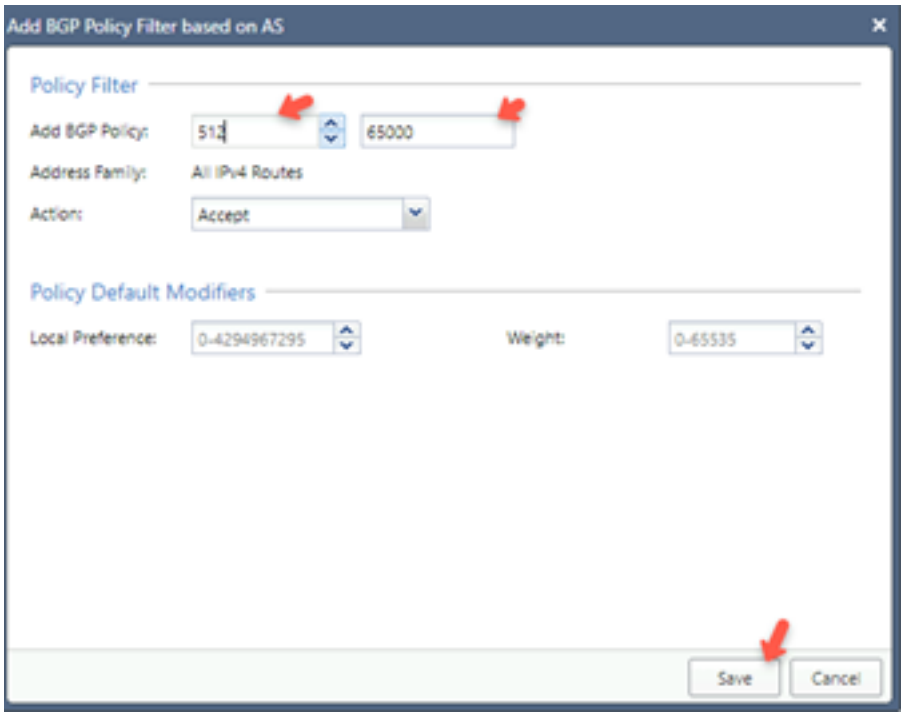
The **Add BGP Policy Filter based on AS** window appears.

10. Specify these:

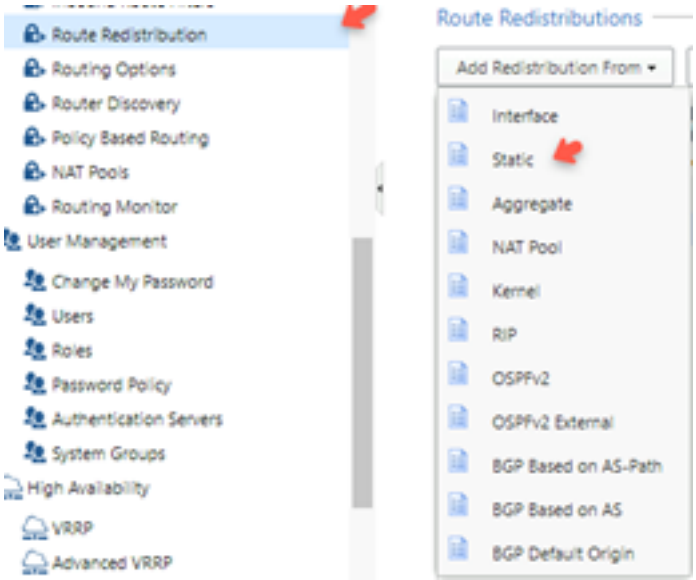
a. **Add BGP Policy** - Set a number from the available range.

b. **AS Number** - Set the AS Number of the Harmony SASE Network.

c. **Action** - Accept



11. Click **Save**.
12. From the **View mode** list, select **Advanced Routing**, click **Route Redistribution**.
13. From the list, select **Add Redistribution From**.
14. Select **Static**.



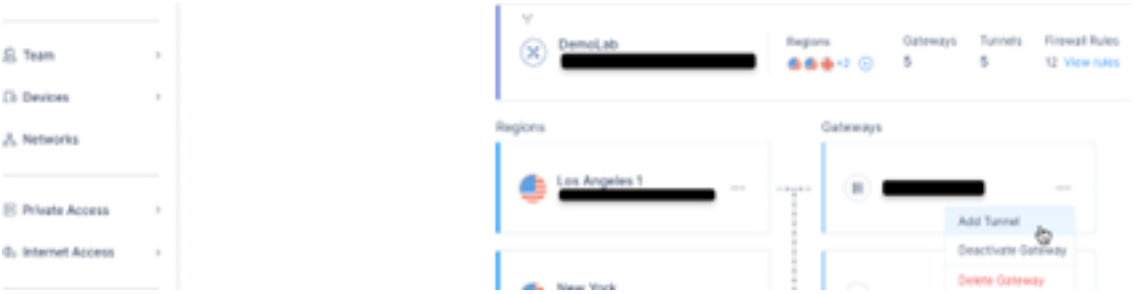
Note - For BGP, no routes are accepted from a peer by default. You must configure an explicit Inbound BGP Route Filter to accept a BGP route from a peer.

15. Repeat the steps for the second Check PointGateway Gaia Portal.

Part 2 - Configuration in Harmony SASE Administrator Portal

Step 1: Configuring Tunnel and Routes Table

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· .
4. Select **Add Tunnel** for the gateway from which you want to add the IPSec Site-2-Site VPN tunnel.

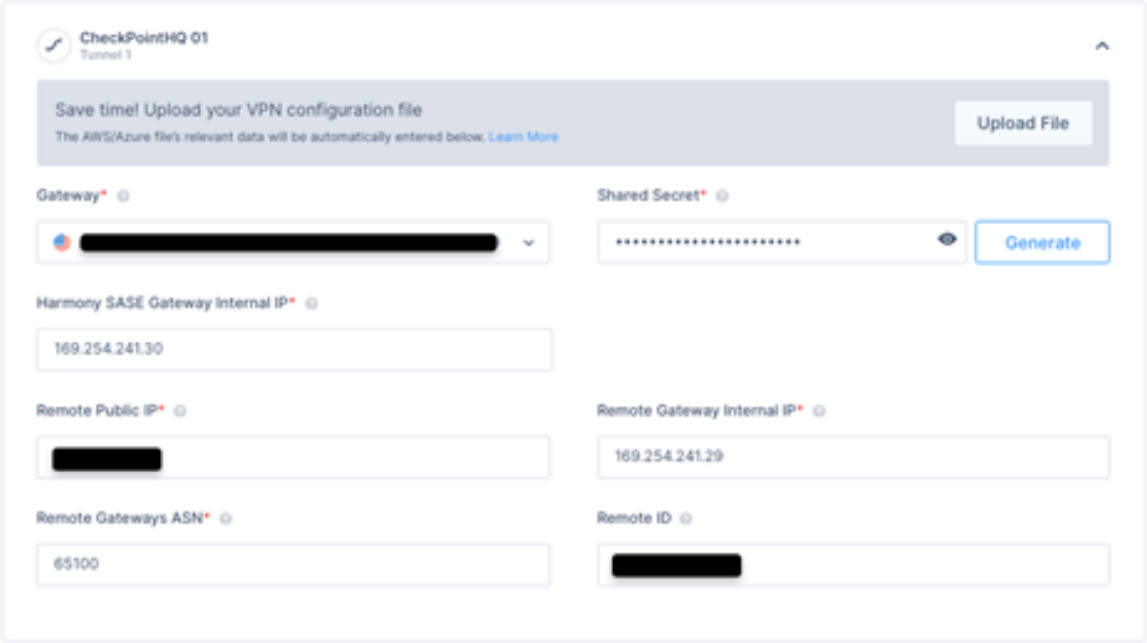


   a. Click **IPSec Site-2-Site Tunnel** and click **Continue**.

b. Click **Redundant Tunnels** and click **Continue**.

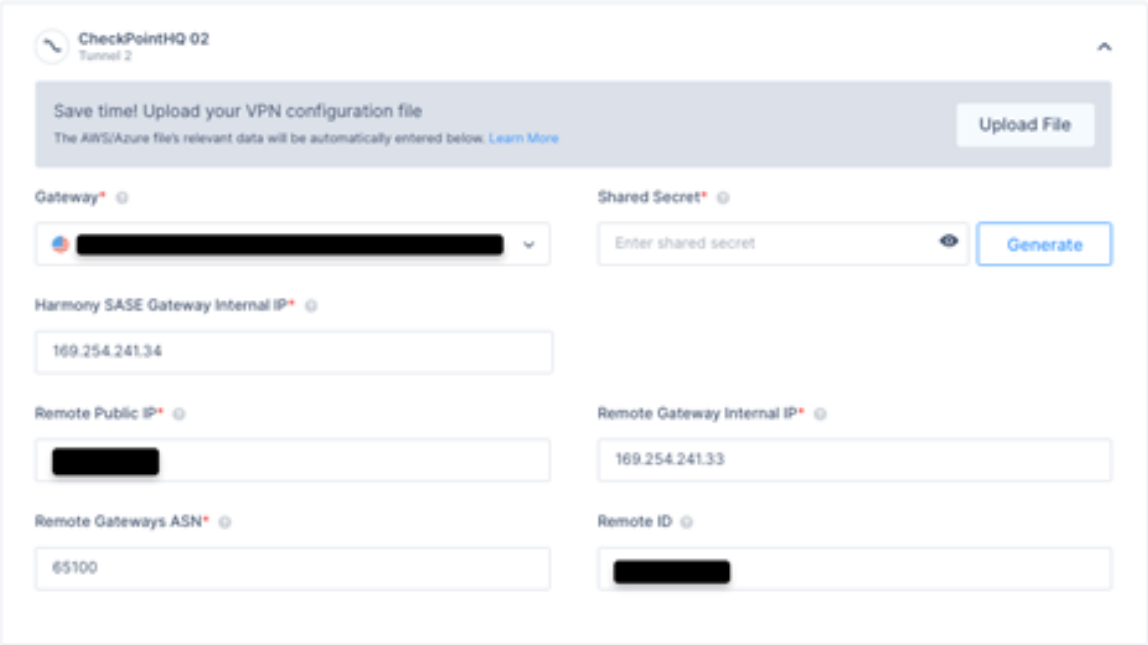
c. In the **Tunnel name** field, enter a logical name.

d. Expand Tunnel 1 and specify these:



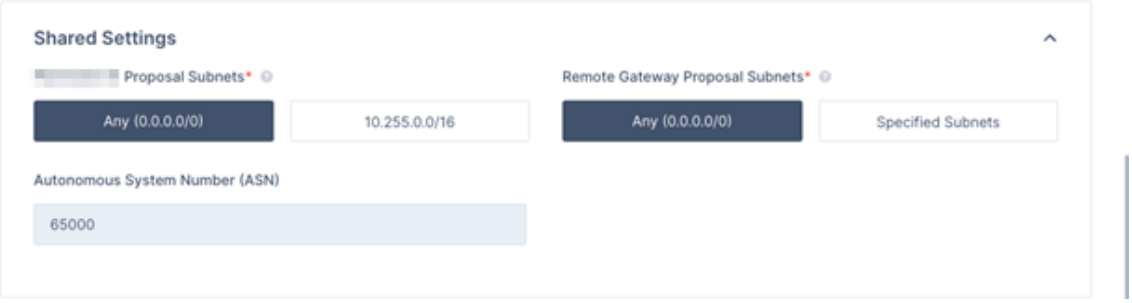
- **Shared Secret** - The value previously set on the first start policy.
- **Harmony SASE Gateway Internal IP** - The remote address of the first Check Point Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the first Quantum Gateway.
- **Remote Gateway Internal IP** - The VIP of the first VTI interface.
- **Remote Gateways ASN** - The ASN of the first Quantum Gateway.
- **Remote ID** - The router ID of the first Quantum Gateway used under the BGP settings above.

e. Expand Tunnel 2 and specify these:



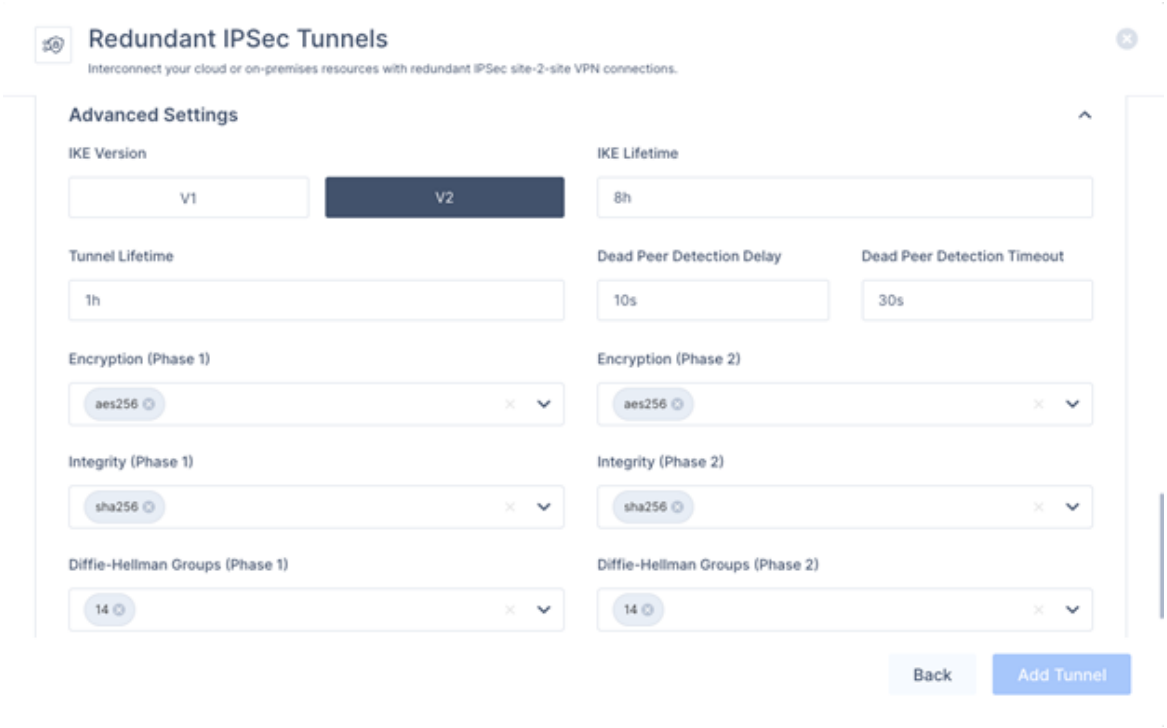
- **Gateway** - Select the second Harmony SASE Gateway for the tunnel.
- **Shared Secret** - The value previously set on the second star policy.
- **Harmony SASE Gateway Internal IP** - The remote address of the second Quantum Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the second Quantum Gateway.
- **Remote Gateway Internal IP** - The VIP of the second VTI interface.
- **Remote Gateways ASN** - The ASN of the second Quantum Gateway.
- **Remote ID** - The router ID of the second Quantum Gateway used under the BGP settings above.

f. Expand **Shared Settings** and specify these:



- **Harmony SASE Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Remote Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Autonomous System Number (ASN)** - Default value is **65000**, if not set, enter the AS Number for the Harmony SASE network.

g. In the **Advanced Settings** section, specify these:



- **IKE Version**: V2
- **IKE Lifetime**: 8h
- **Tunnel Lifetime**: 1h
- **Dead Peer Detection Delay**: 10s
- **Dead Peer Detection Timeout**: 30s
- **Encryption(Phase 1)**: aes256
- **Encryption(Phase 2)**: aes256
- **Integrity (Phase 1)**: sha256
- **Integrity (Phase 2)**: sha256
- **Diffie-Hellman Groups (Phase 1)**: 14
- **Diffie-Hellman Groups (Phase 2)**: 14

h. Click **Add Tunnel**.

5. Select **Routes Table**:

a. Click **Add Route**.

The **Add Route** window appears.

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

c. Click **Apply Configuration**.

Step 2: Verifying the Setup

Once you complete the above steps, your tunnel should be active.

1. Verify the setup in the Harmony SASE Administrator Portal:

   a. Click **Networks**.

   b. Locate the tunnel you create, and check the tunnel status.

   It should indicate that the tunnel is **Up**, signifying a successful connection.

2. Verify the setup in the Harmony SASE Agent:

   a. Connect to your network using the Harmony SASE Agent.

   b. Access one of the resources in your environment.

Configuring Check Point Redundant IPsec Tunnel

This topic explains how to establish a single Site-to-Site tunnel between your Harmony SASE Network and Check Point Firewall.

Pre-requisites

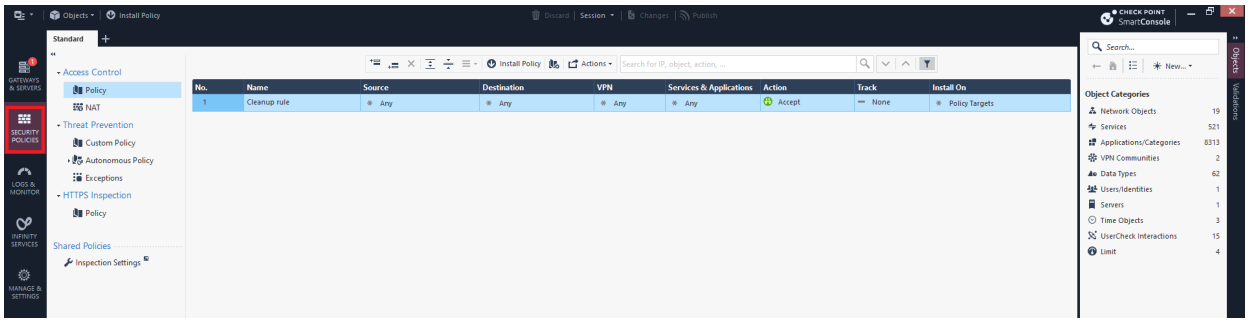
- Harmony SASE Administrator Portal account.
- Device with Harmony SASE Agent installed.
- Administrator account with Firewall, Router, and Cloud Management Portal.

- A cluster of two Quantum gateways, each with a public IP.
- Configuration with ISP redundancy PMTR-68991 is not supported.

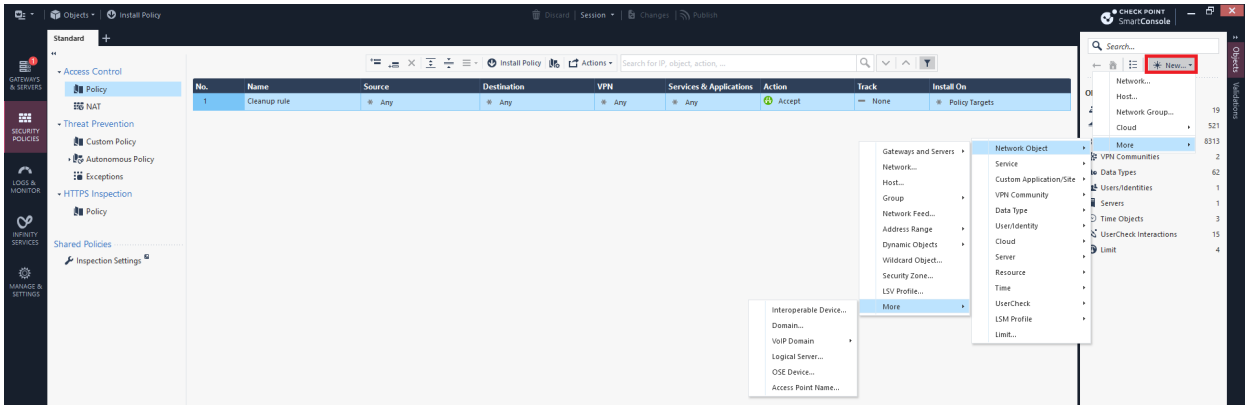
Part 1 - Configuration in SmartConsole

Step 1: Creating Interoperable Device Object in the Check Point SmartConsole

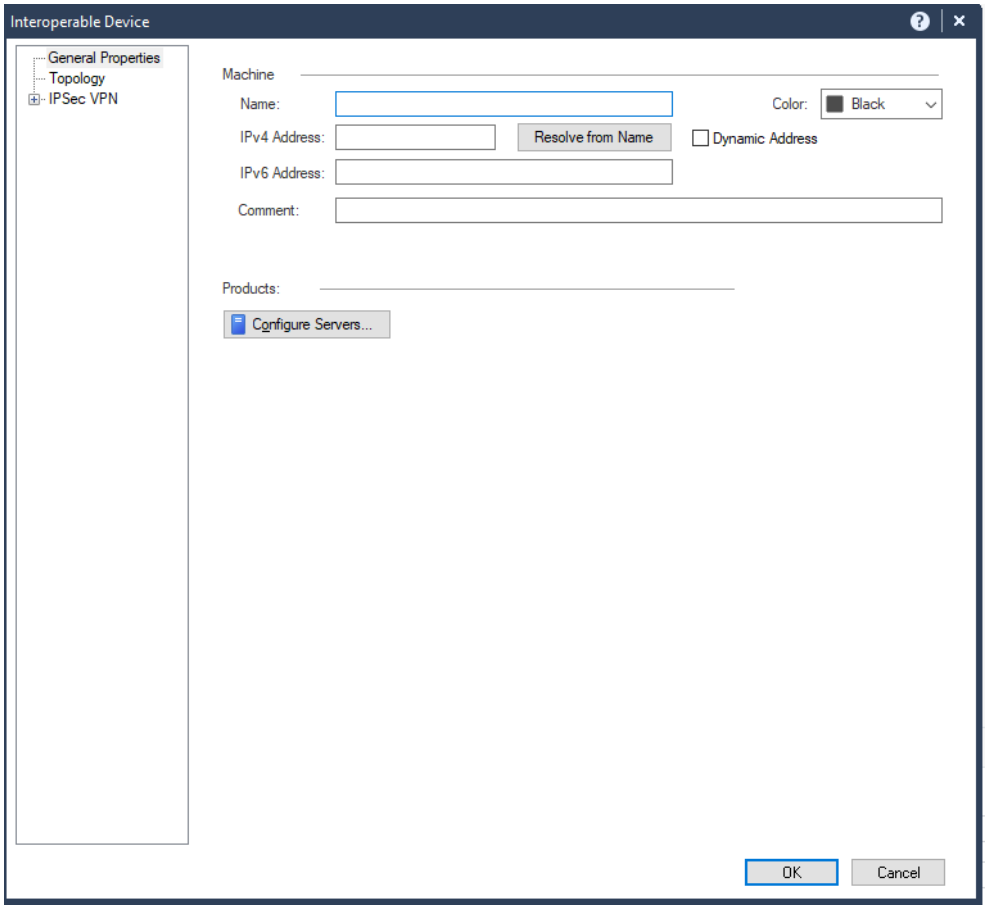
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.



3. In the Objects pane, click **New** and select **More > Network Object > More > Interoperable Device**.



The **Interoperable Device** window appears.



a. In the **Name** field, enter a name for the Harmony SASE gateway, for example, Harmony_SASE_Gateway.

b. In the **IPv4 Address** field, enter the Harmony SASE gateway public IP address.

   To find the Harmony SASE Gateway public IP Address:

   i. Access the Harmony SASE Administrator Portal and click **Networks**.

   ii. Select the network.

   iii. Go to the **Gateways** section to find the Public IP address for setting up the single IPsec tunnel.

c. Click **OK**.

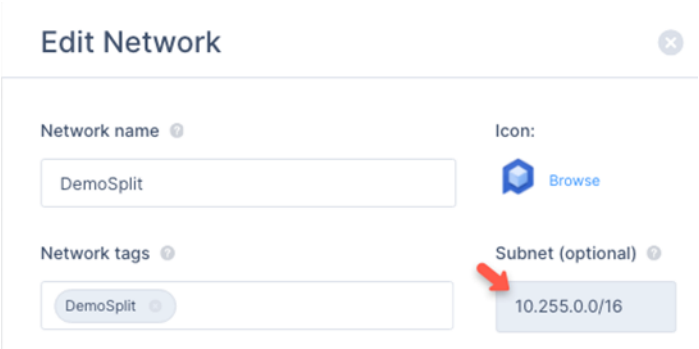
Step 2: Adding Harmony SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object

1. Log in to the Harmony SASE Administrator Portal.
2. Click **Networks**.
3. Verify the assigned network:

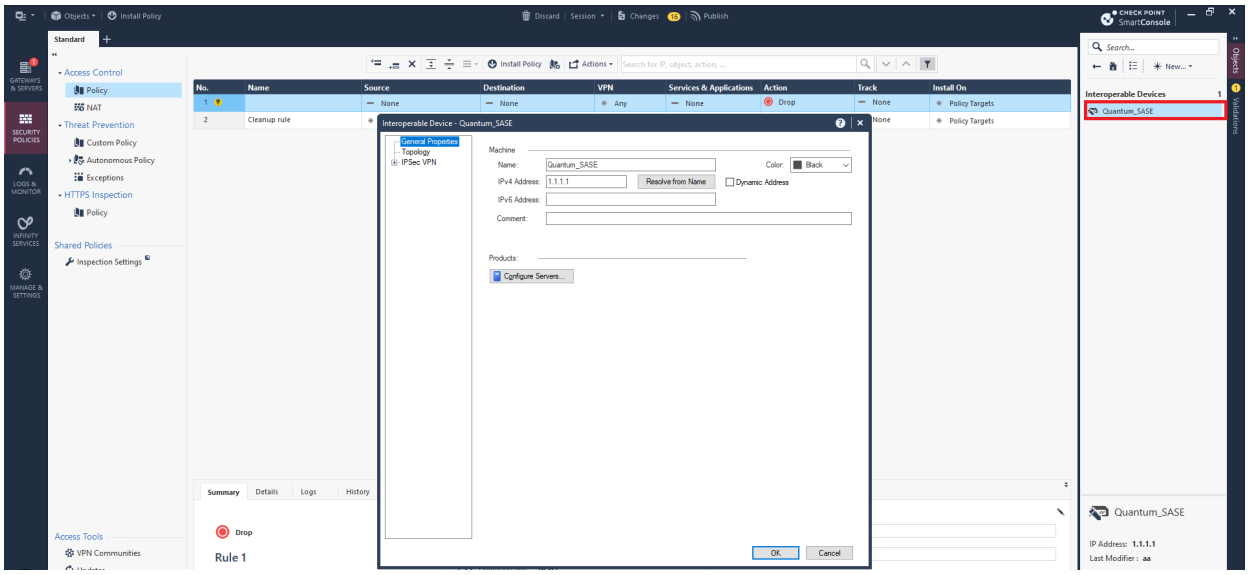
a. Select a network, scroll to the end of the row and click ··· .

b. Select **Edit Network.**

c. In the **Edit Network** section, check the **Subnet** field to verify the assigned network. The default value is 10.255.0.0/16.

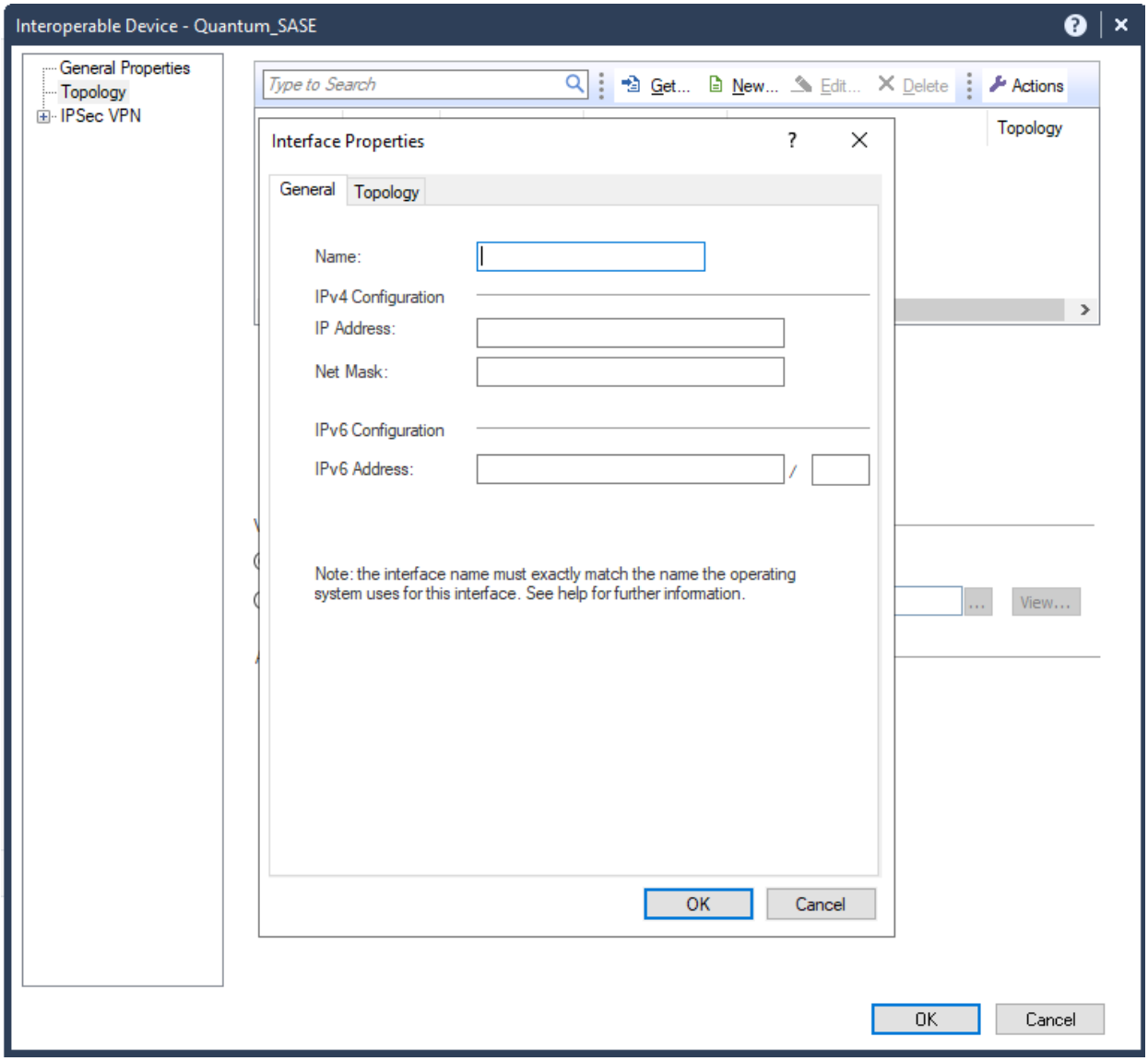


4. Open the network object that you created.



Note - If the gateway is configured with an interface topology that includes a network range or a group overlapping with the encryption domain of the remote VPN peer, incoming decrypted traffic may be seen as coming from the wrong interface. This could trigger anti-spoofing measures, causing traffic to be dropped. To create an anti-spoofing exception, see sk151774.

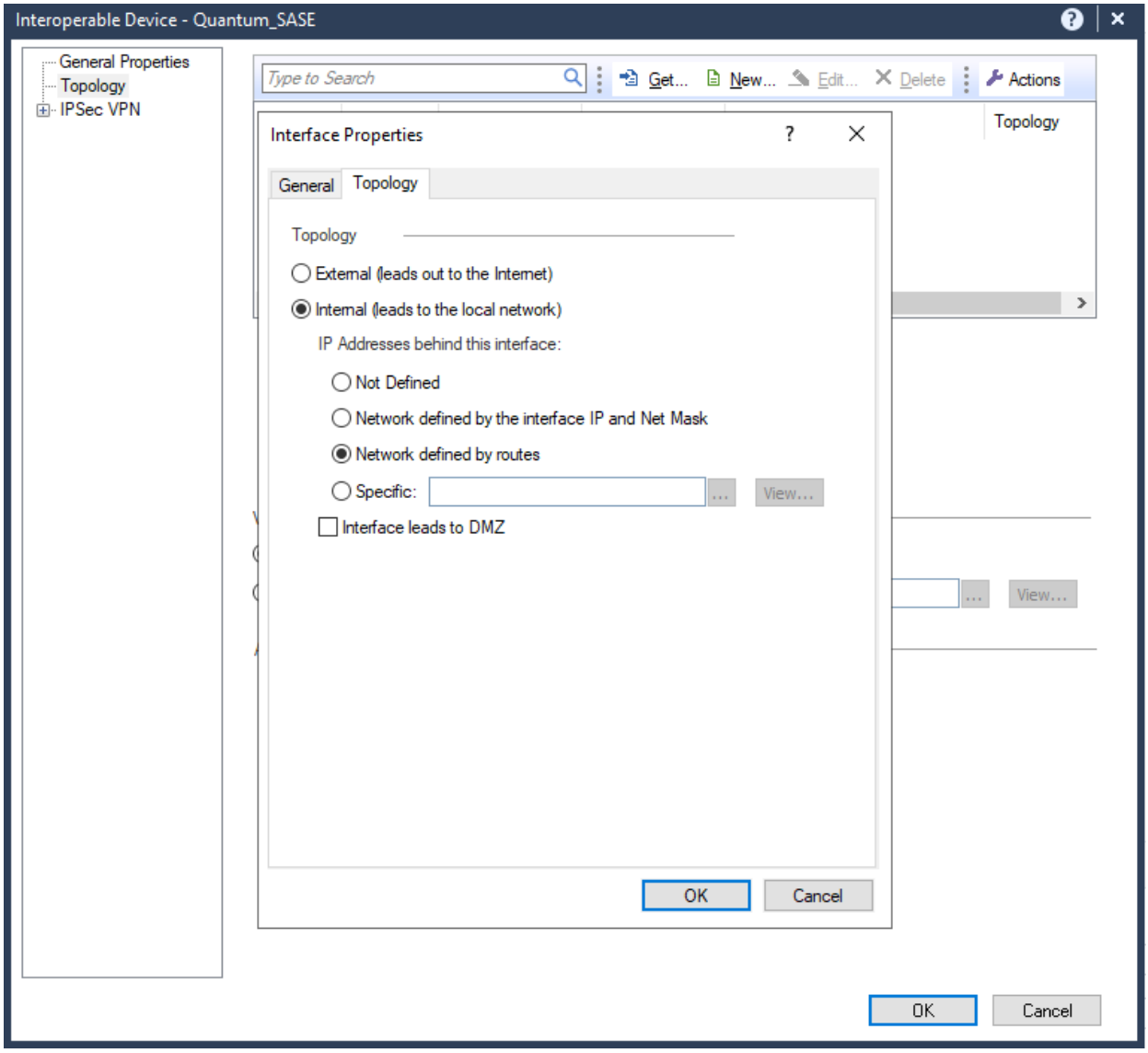
5. Click **Topology > New**.



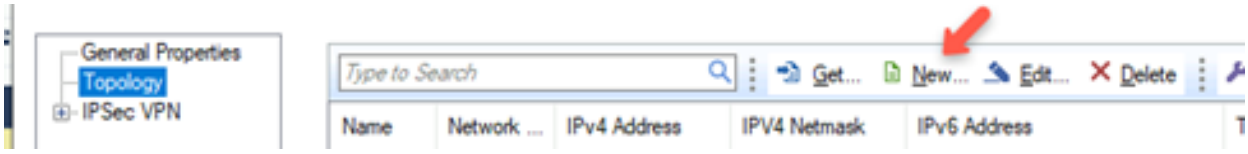
6. In the **General** tab:

Field	Enter
Name	Name for the topology.
IP Address	10.255.0.0
Net Mask	255.255.0.0

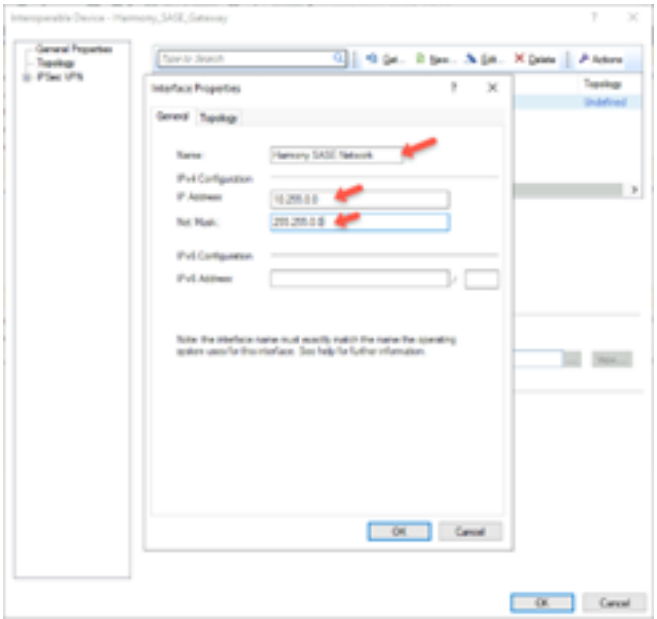
7. In the **Topology** tab, select **Internal (leads to the local network)** and select **Network defined by the interface IP and Net Mask**.



8. Click **OK**.
9. Click **Topology** > **New**.

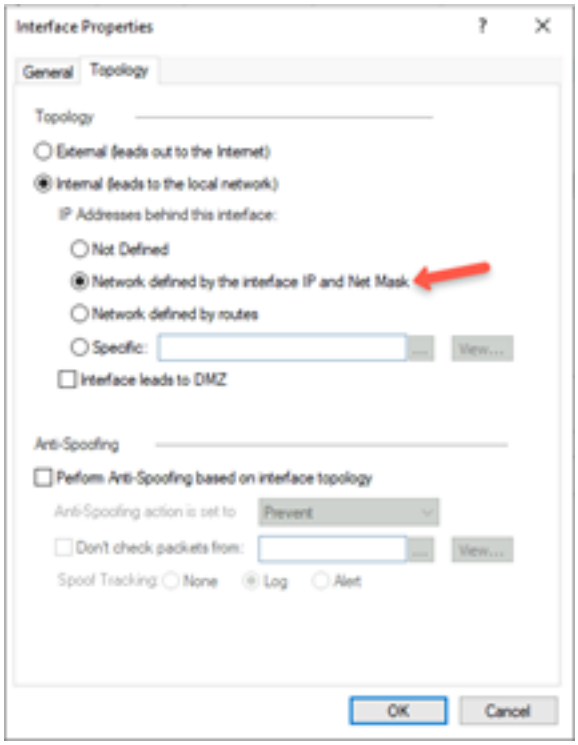


10. In the **General** tab:



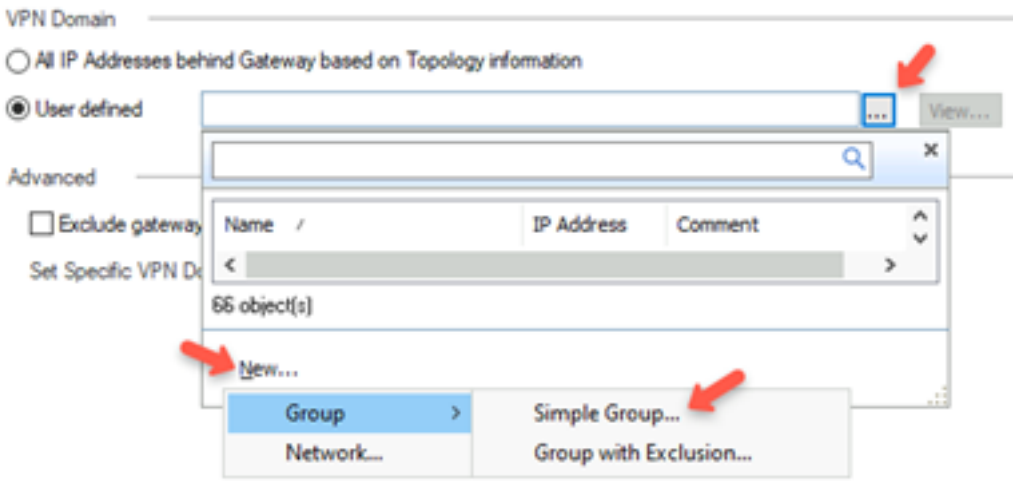
Field	Enter
Name	Name for the topology.
IP Address	Public IP address of the Harmony SASE gateway.
Net Mask	255.255.255.255

11. In the **Topology** tab, select **External (leads to the local Internet)**.



12. Click **OK**.

13. Click **Topology** > **New**.
14. In the **General** tab, enter these:
    a. **Name** - Name for the topology, for example, Harmony_SASE_Gateway.
    b. **IP Address** - Public IP address of the Harmony SASE gateway.
    c. **Net Mask** - 255.255.255.255
15. Click the **Topology** tab.
16. Select **External (leads out to the internet)**.
17. Click **OK**.
18. In the **VPN Domain** section, select User defined and click ··· .
19. Click **New** and go to **Group** > **Simple Group**.



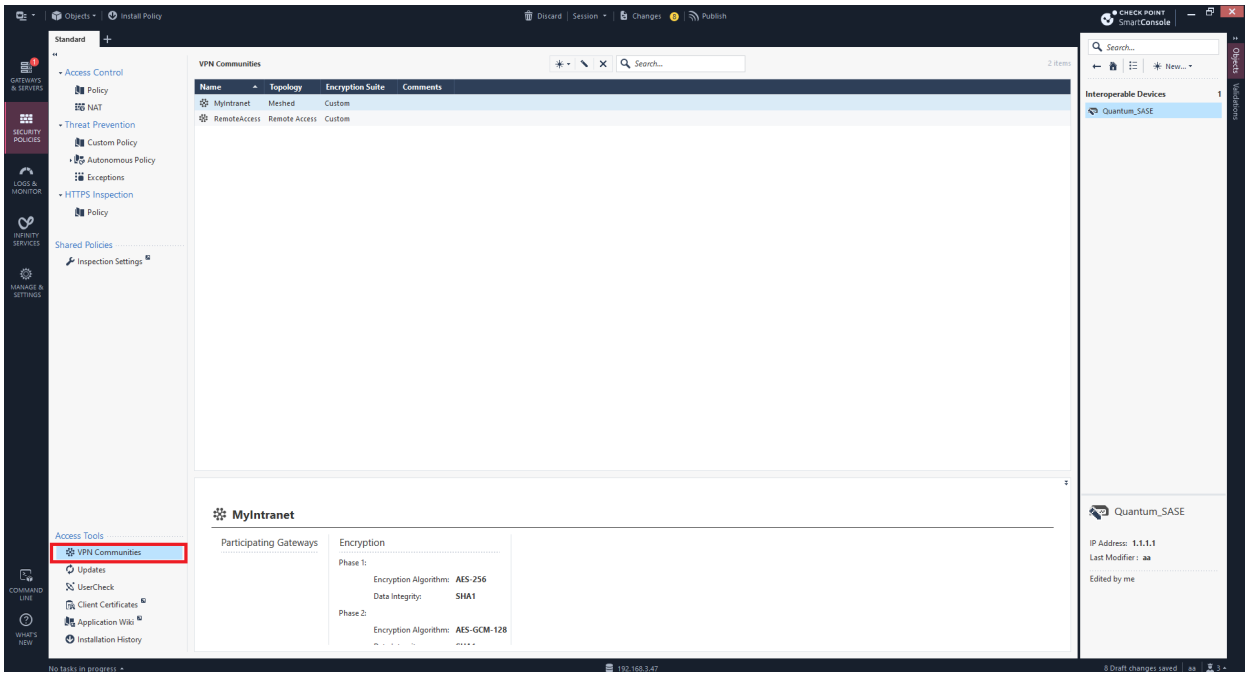
The **New Network Group** window appears.

20. In the **Enter Object Comment** field, enter a name, for example, HSASE_VTI, and click **OK**.

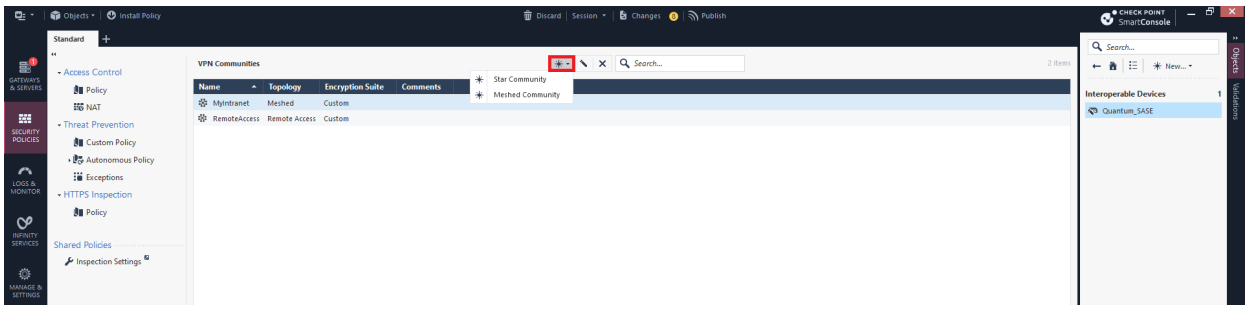
21. For the other Harmony SASE Gateway and Check Point Gateway, follow the same procedure in **Creating Interoperable Device Objects in the Check Point SmartConsole** and **Adding Harmony SASE Gateway IP Address and Remote Subnet To The Interoperable Device Object sections**.
22. Publish and install the policy.

Step 3: Creating VPN Start Community

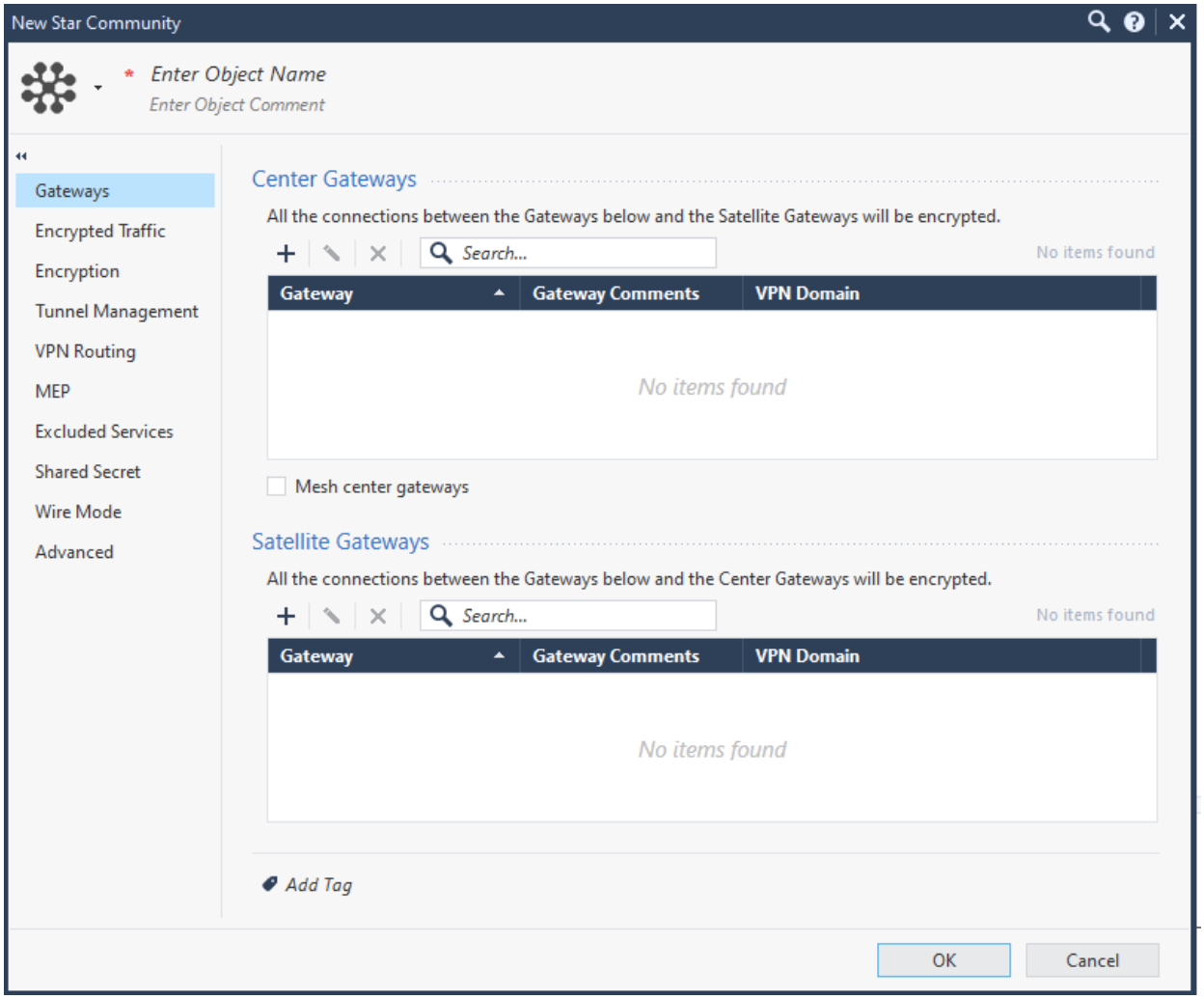
1. Log in to the Check Point SmartConsole.
2. Click **Security Policies**.
3. Go to **Access Tools** > **VPN Communities**.



4. Select an object, click **New** and go to **More** > **VPN Community** > **Star Community**.



The **New Star Community** window appears.

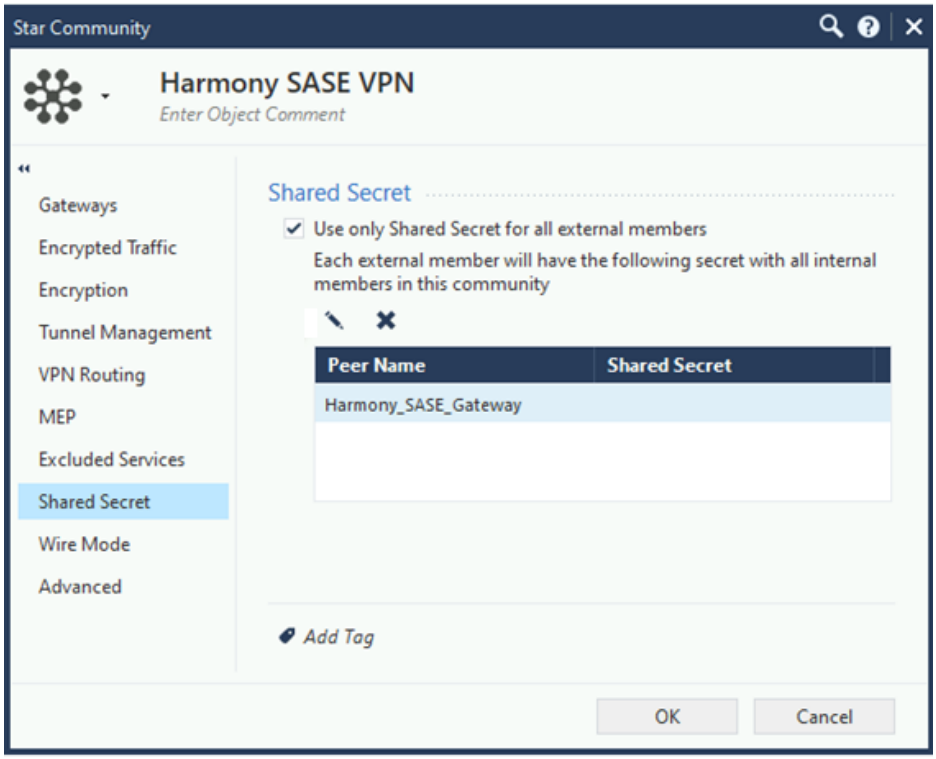


5. In the **Enter Object Name** field, enter an object name for the VPN Start Community, for example, Harmony_SASE_VPN.

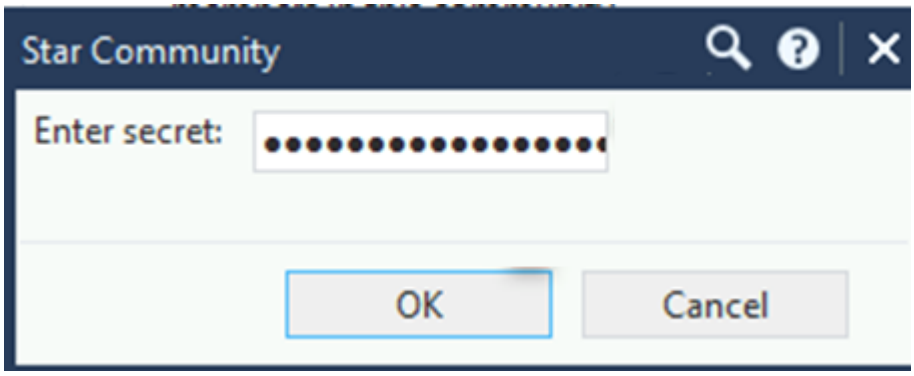
6. Under **Center Gateways**, click + and add the Check Point Gateway.

7. Under **Satellite Gateways**, click + and add the Interoperable Device Object created for the Check Point Gateway. See Step 1.

8. Go to **Shared Secret** and click to edit the shared key.



9. In the **Enter secret** field, enter an appropriate key.

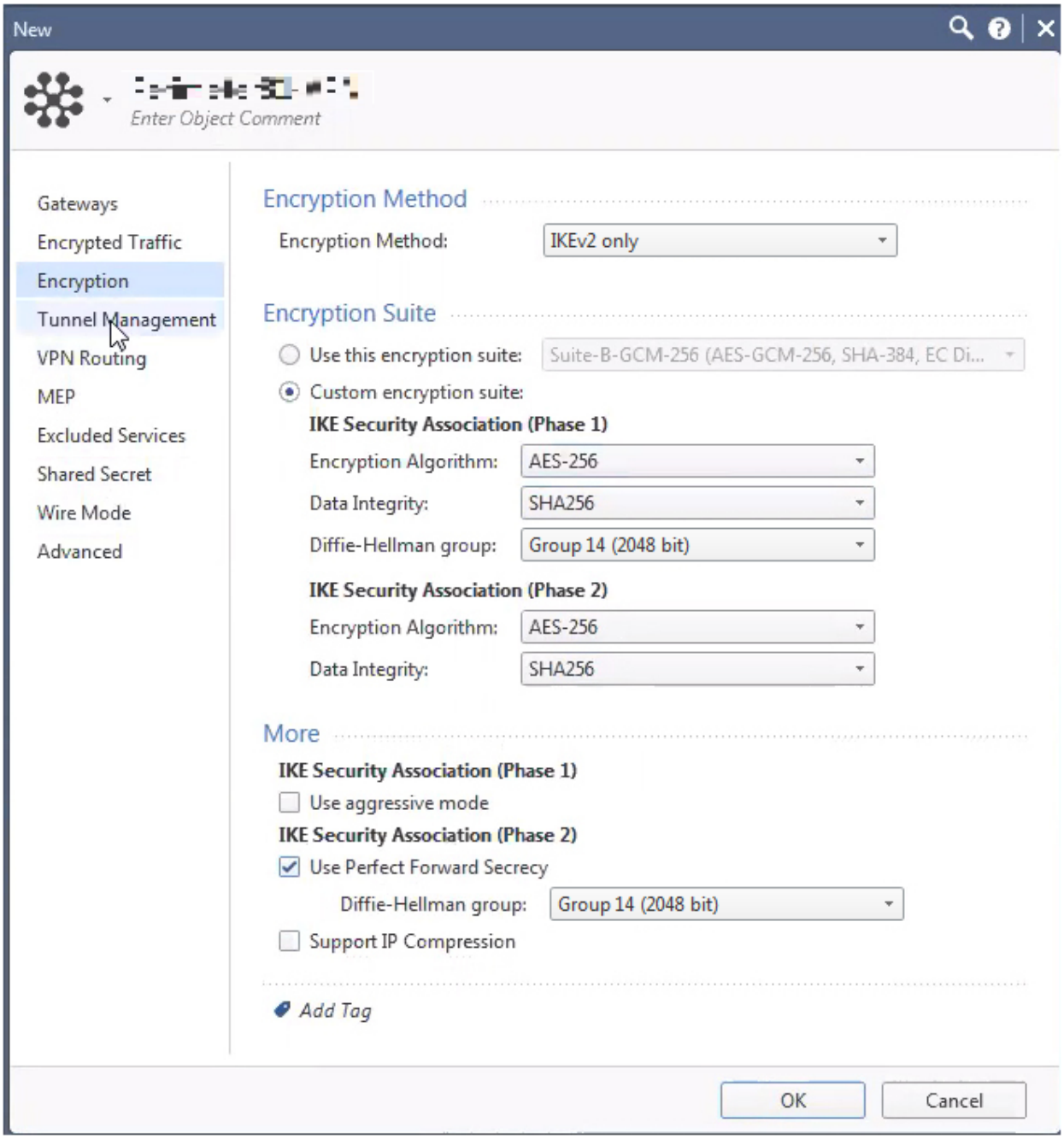


Notes:

- Copy the key as it is required while configuring the IPsec Tunnel in the Harmony SASE Administrator Portal.
- Check Point recommends that the share secret key is at least 20 characters in length.

10. Click **OK**.

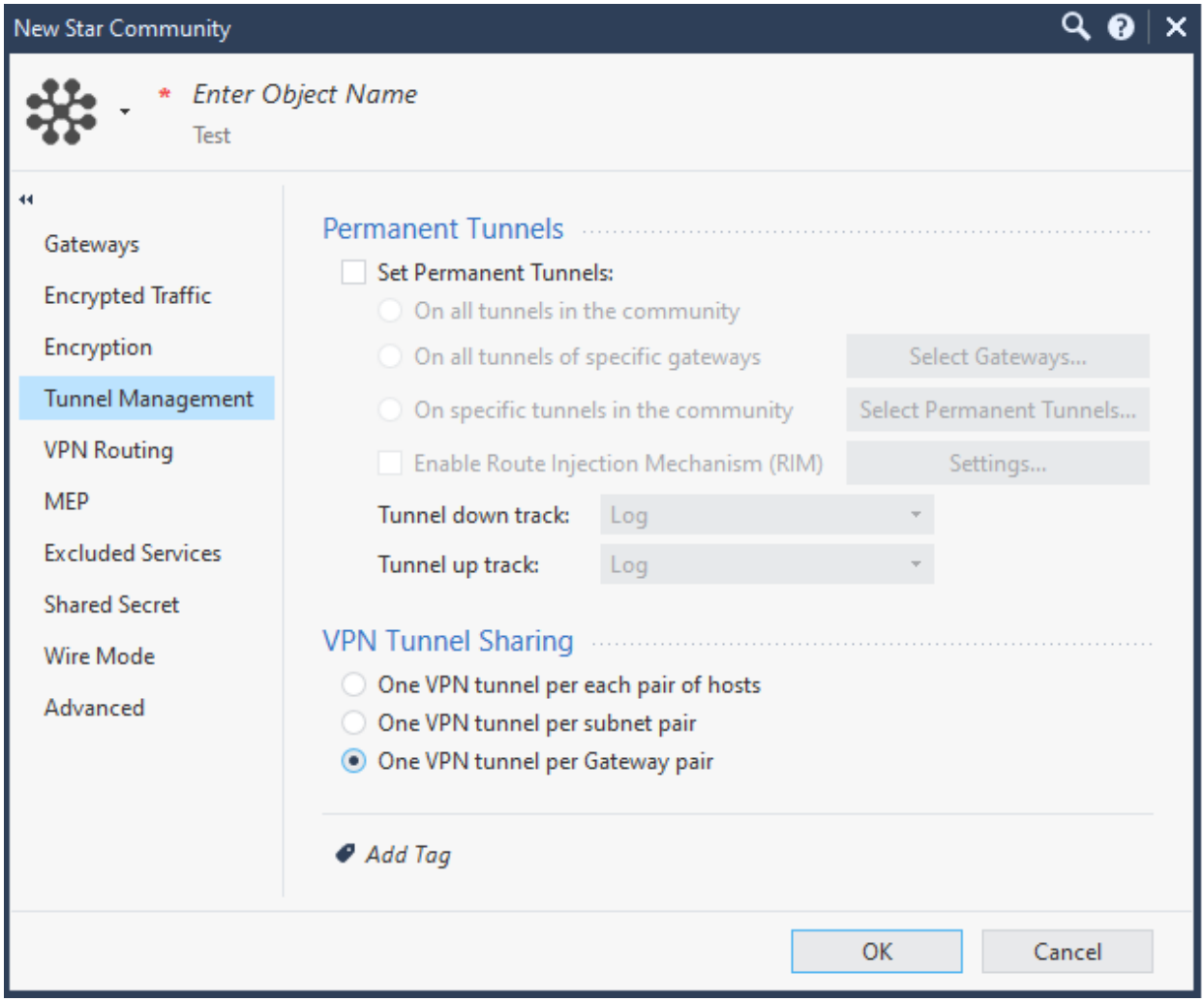
11. From the left navigation pane, click **Encryption** and do these:



Field	Enter
Encryption Method	IKEv2 only
Custom encryption suite	
IKE Security Association (Phase 1)	
Encryption Algorithm	AES-256
Data Integrity	SHA256

Field	Enter
Diffie Hellman group	Group 14 (2048 bit)
IKE Security Association (Phase 2)	
Encryption Algorithm	AES-256
Data Integrity	SHA256
More	
IKE Security Association (Phase 2)	
Use Perfect Forward Secrecy	
Diffie Hellman group	Group 14 (2048 bit)

12. Click **Tunnel Management** and under **VPN Tunnel Sharing**, select **One VPN tunnel per Gateway pair**.



Important - Make sure that you enter the remote subnets specified here in the Harmony SASE Administrator Portal. A mismatch can disconnect the tunnel.

13. Click **Advanced**.
    a. In the **IKE (Phase 1)** section, set the **Renegotiate IKE security associations every (minutes)** field to **480**.
    b. In the **IPsec (Phase 2)** section, set the **Renegotiate IPsec security associations every (seconds)** field to **3600**.
14. Click **OK**.
15. Repeat steps 1 to 17 for the other Check Point Gateway and Harmony SASE Gateway.
16. Publish and install the policy.

Step 4: Additional settings in Check Point SmartConsole

1. To set up a Check Point firewall policy, add a rule for VPN traffic for the specific VPN Domain in the Check Point SmartConsole.

   In the example below, we have created a policy to allow traffic from the Harmony SASE Network 10.255.0.0/16 to specific destinations and services. Note that the network configuration may differ if you have not changed the default settings during Harmony SASE network creation. For testing purposes, you should initially allow any/any or allow before making the firewall policy more restrictive.

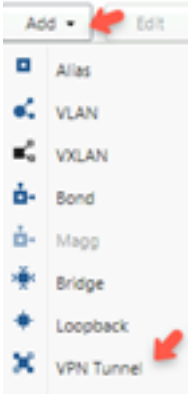
   Note - The network configuration differs if you have not changed the default settings during Harmony SASE network creation. For testing purposes, you should initially allow any/any or allow ping before making the firewall policy more restrictive.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	P81 Basic AD Ingress	n_10.255.0.0_16	AD_Servers	vpn_StarP81	ActiveDirectorySvcs Active Directory DCE-RPC Protocol	Accept	Log Accounting	Policy Targets
2	P81 Basic RDP Ingress	n_10.255.0.0_16	RDP_Farm	vpn_StarP81	Remote_Desktop_Pr...	Accept	Log Accounting	Policy Targets

2. Publish and install the policy.

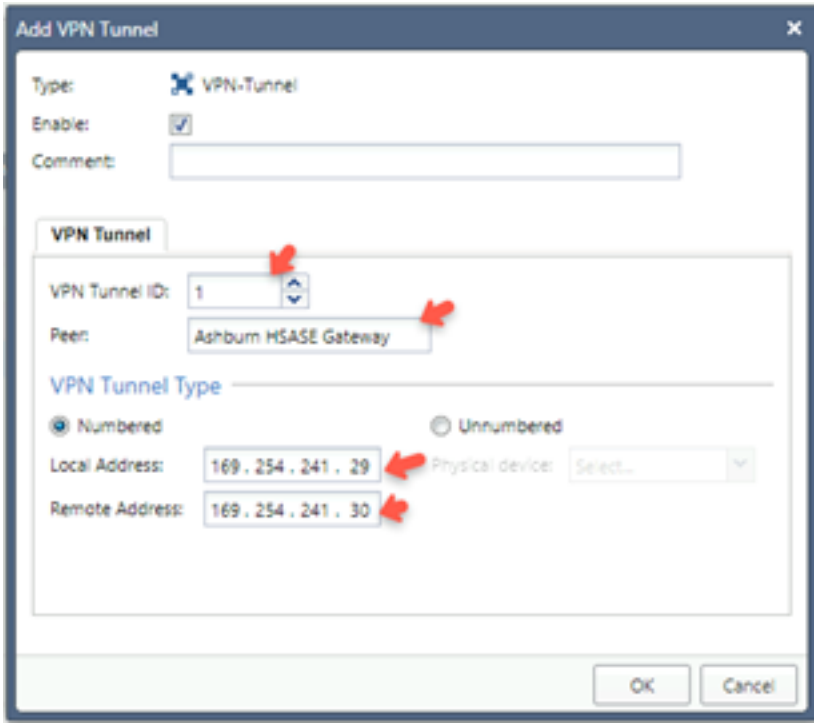
Step 5: Configuring VPN Tunnel Interface and BGP Configuration

1. Log in to the Check Point Gaia Portal of the first Check Point Gateway.
2. Click **Network Interfaces**.
3. From the **Add** list, select **VPN Tunnel**.



The **Add VPN Tunnel** page appears.

4. Enter these:



   a. **VPN Tunnel ID** - Select a unique ID.

   b. **Peer** - Name of the interoperable device previously created for the first Harmony SASE Gateway.

   c. **VPN Tunnel Type** - Numbered.

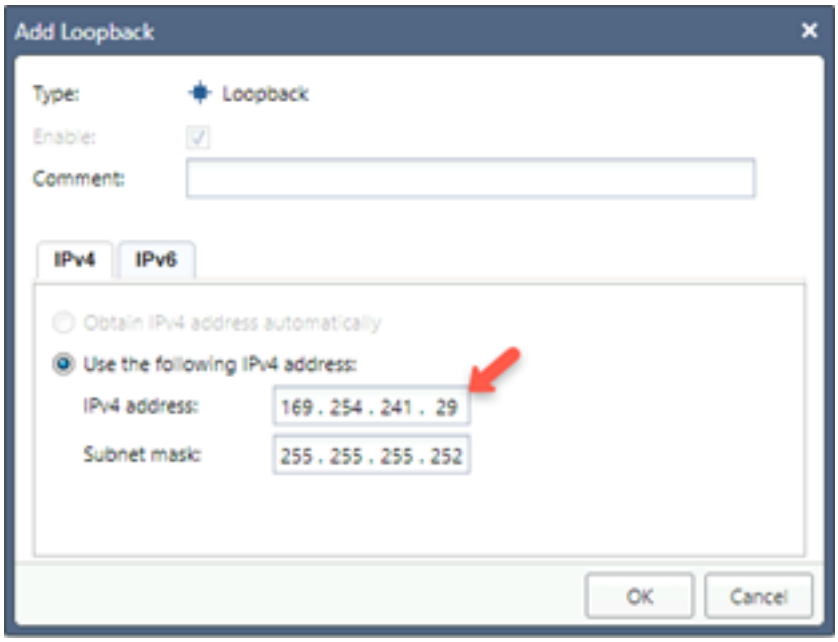
   d. **Local Address** - Internal address for the Quantum Gateway (within 169.254.x.x/30 ranges).

   e. **Remote Address** - Internal address for the Harmony SASE Gateway (within 169.254.x.x/30 ranges, corresponding to the above).

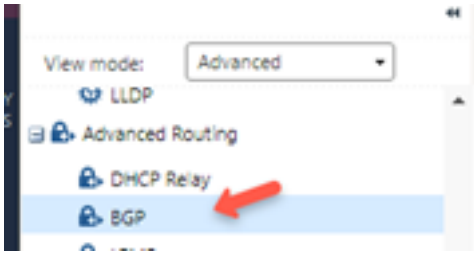
5. Click **OK**.

6. Click **Network Interfaces**, **Add** > **Loopback**.

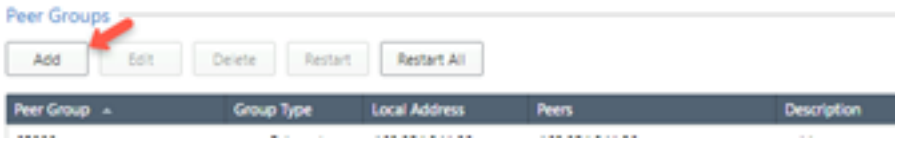
7. Select **Use the following IPV4 address**.



8. In the **IPv4** field, enter the Local Address entered in step 4 and click **OK**.
9. Go to **Advanced Routing** and select **BGP**.



10. In the **Peer Groups** section, click **Add**.

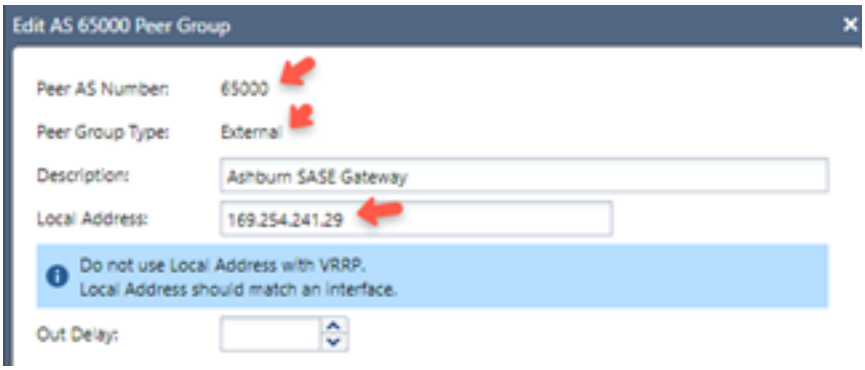


11. Enter these:

    a. **Peer AS Number** - The AS Number of the Harmony SASE network. If not set already, enter 65000.

    b. **Peer Group Type** - External.

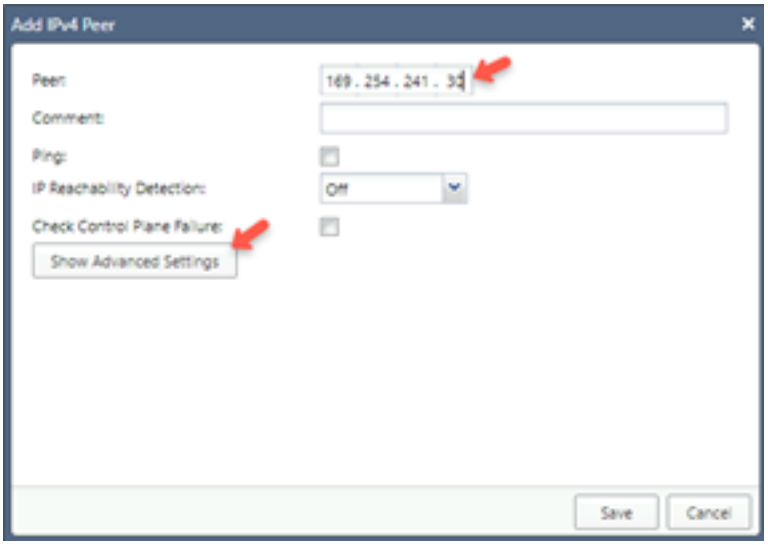
c. **Local Address** - The local address entered in the VTI configuration section Step 4.



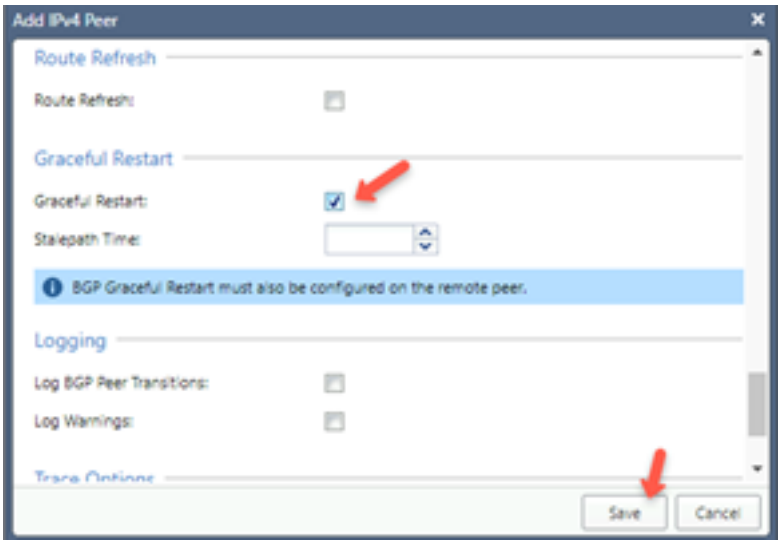
12. Click **Add Peers**.

13. Enter these:

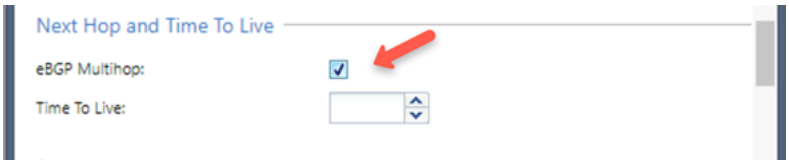
    a. In the **Peer** field, enter the Remote Address set under the VTI configuration in Step 4 and click **Show Advanced Settings**.



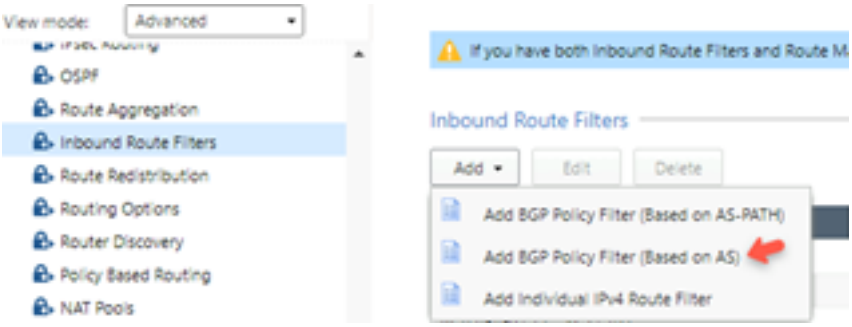
b. Select the **Graceful Restart** checkbox.



c. Select the **eBGP Multihop** checkbox and click **Save**.



14. From the **View mode** list, select **Advanced Routing** and click **Inbound Route Filter**.
15. From the **Add** list, select **Add BGP Policy Filter (Based on AS)**.



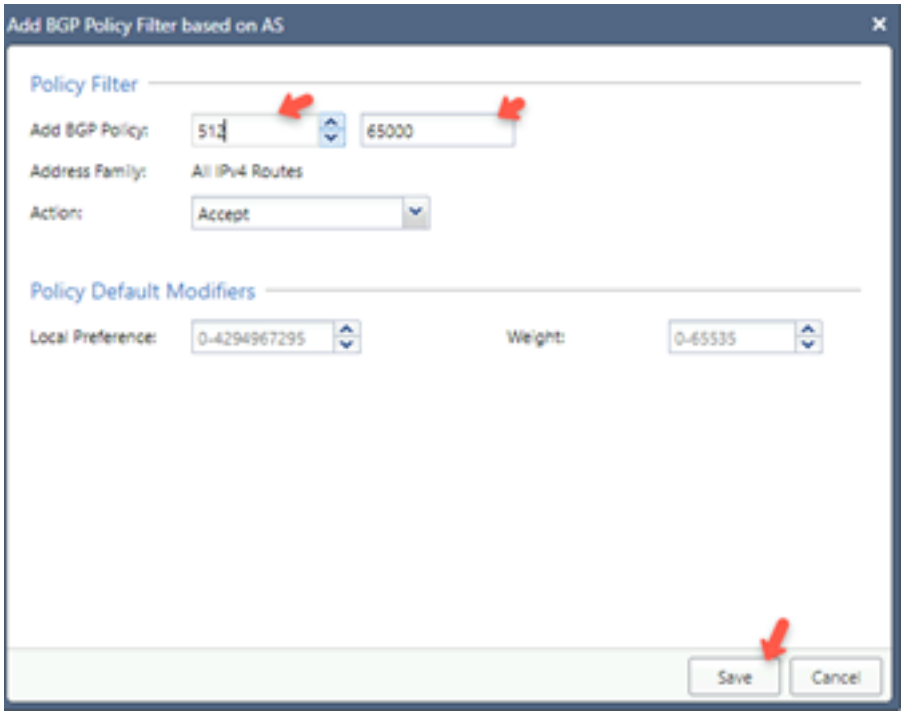
The **Add BGP Policy Filter based on AS** window appears.

16. Specify these:

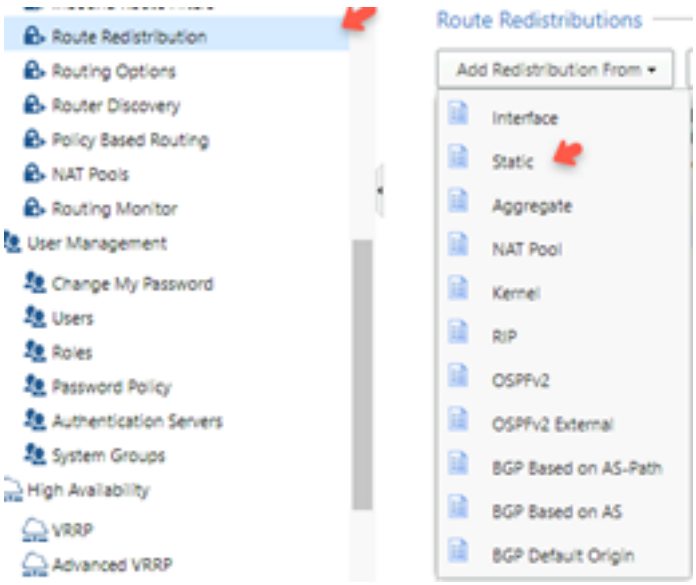
    a. **Add BGP Policy** - Set a number from the available range.

    b. **AS Number** - Set the AS Number of the Harmony SASE Network.

    c. **Action** - Accept



17. Click **Save**.
18. From the **View mode** list, select **Advanced Routing**, click **Route Redistribution**.
19. From the list, select **Add Redistribution From**.
20. Select **Static**.



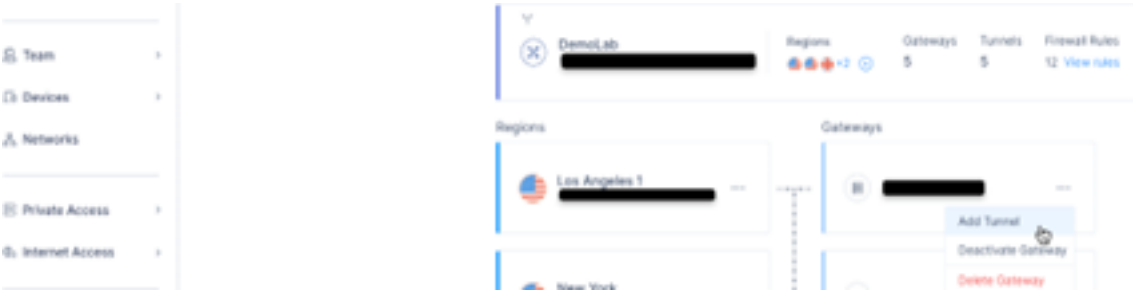
Note - For BGP, no routes are accepted from a peer by default. You must configure an explicit Inbound BGP Route Filter to accept a BGP route from a peer.

21. Repeat the steps for the second Check Point Gateway and Harmony SASE Gateway. Use a different 169.254.x.x/30 range for the local and remote peer IP addresses.

Part 2 - Configuration in Harmony SASE Administrator Portal

Step 1: Configuring Tunnel and Routes Table

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Select the network.
3. Click ··· .
4. Select **Add Tunnel** for the gateway from which you want to add the IPSec Site-2-Site VPN tunnel.

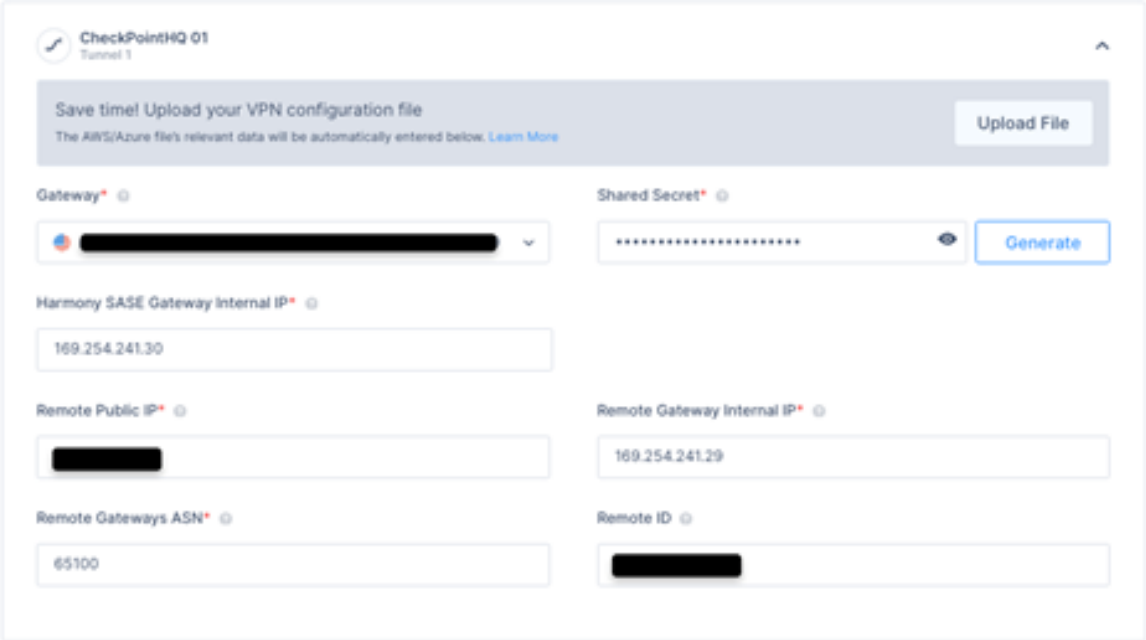


a. Click **IPSec Site-2-Site Tunnel** and click **Continue**.

b. Click **Redundant Tunnels** and click **Continue**.

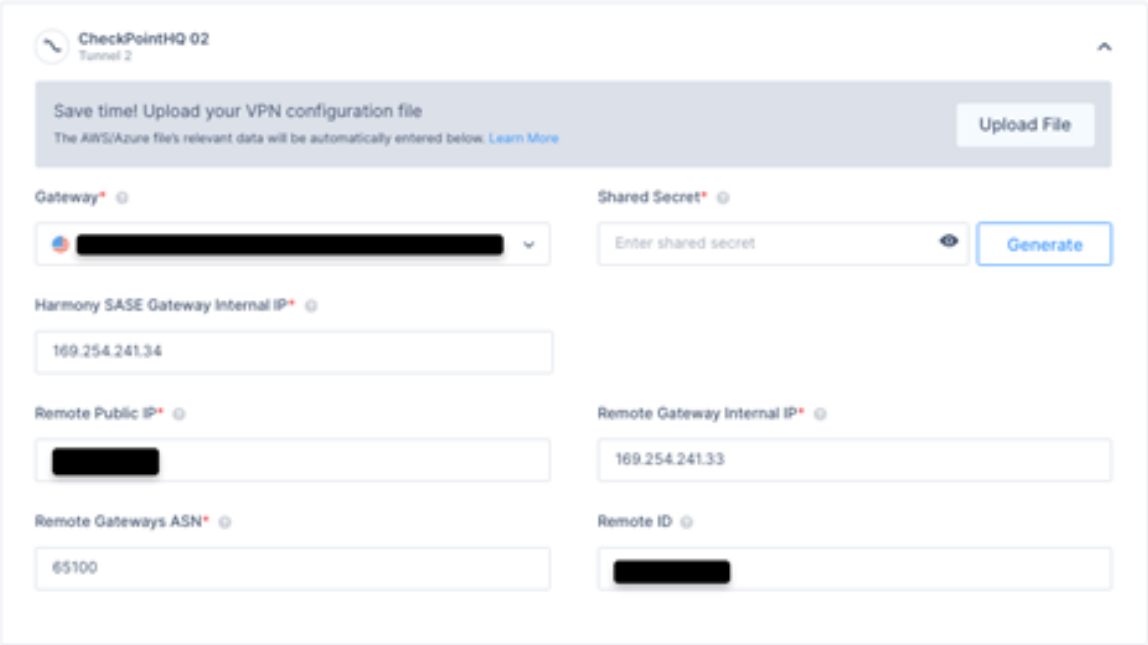
c. In the **Tunnel name** field, enter a logical name.

d. Expand Tunnel 1 and specify these:



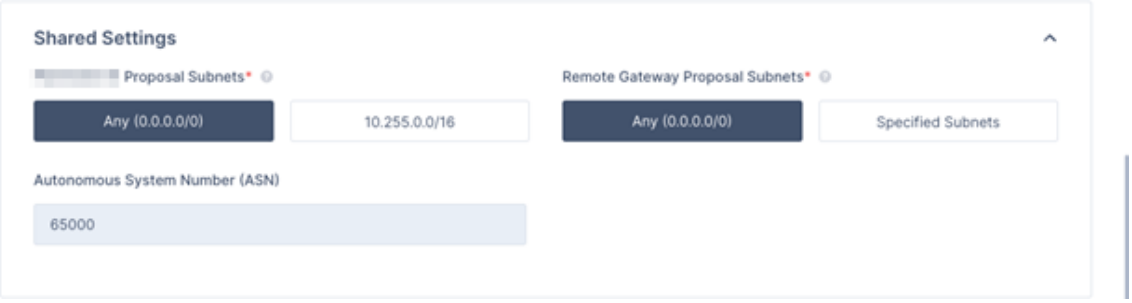
- **Shared Secret** - The value previously set on the first start policy.
- **Harmony SASE Gateway Internal IP** - The remote address of the first Check Point Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the first Quantum Gateway.
- **Remote Gateway Internal IP** - The local address of the first Quantum Gateway used under the VTI settings.
- **Remote Gateways ASN** - The ASN of the first Quantum Gateway.
- **Remote ID** - The router ID of the first Quantum Gateway used under the BGP settings above.

e. Expand Tunnel 2 and specify these:



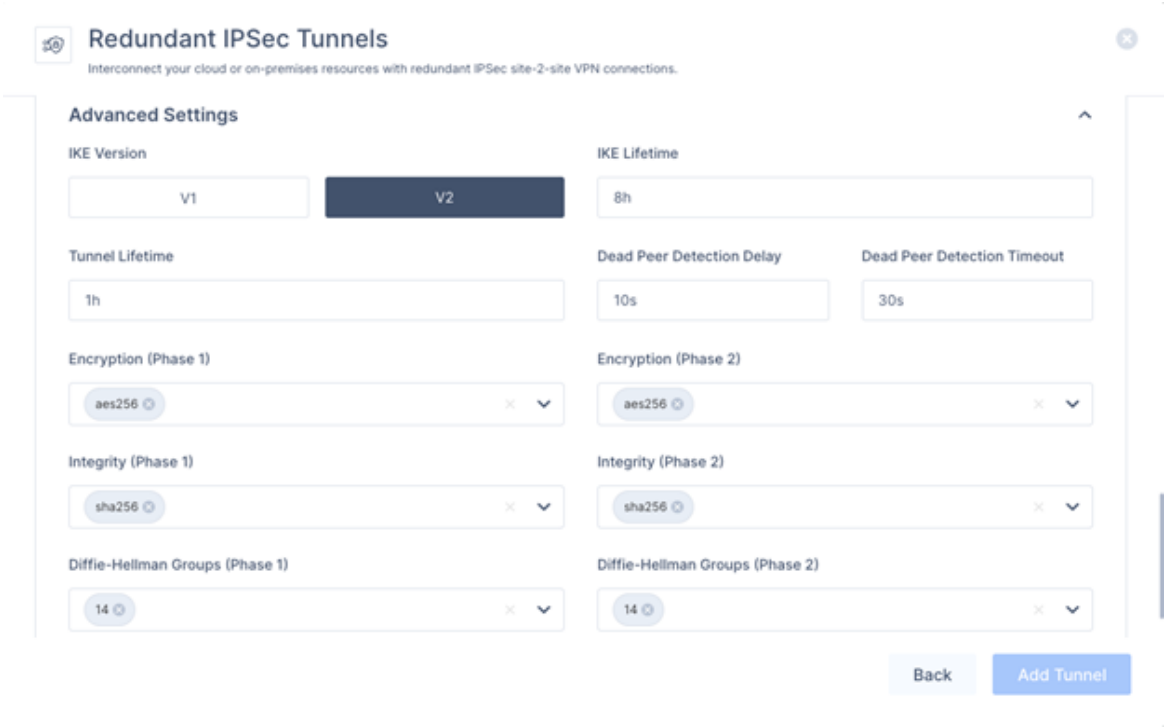
- **Gateway** - Select the second Harmony SASE Gateway for the tunnel.
- **Shared Secret** - The value previously set on the second star policy.
- **Harmony SASE Gateway Internal IP** - The remote address of the second Quantum Gateway used under the VTI settings.
- **Remote Public IP** - The public IP of the second Quantum Gateway.
- **Remote Gateway Internal IP** -The local address of the second Quantum Gateway used under the VTI settings.
- **Remote Gateways ASN** - The ASN of the second Quantum Gateway.
- **Remote ID** - The router ID of the second Quantum Gateway used under the BGP settings above.

f. Expand **Shared Settings** and specify these:



- **Harmony SASE Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Remote Gateway Proposal Subnets** - Leave **Any (0.0.0.0/0)** selected.
- **Autonomous System Number (ASN)** - Default value is **65000**, if not set, enter the AS Number for the Harmony SASE network.

g. In the **Advanced Settings** section, specify these:



- **IKE Version**: V2
- **IKE Lifetime**: 8h
- **Tunnel Lifetime**: 1h
- **Dead Peer Detection Delay**: 10s
- **Dead Peer Detection Timeout**: 30s
- **Encryption(Phase 1)**: aes256
- **Encryption(Phase 2)**: aes256
- **Integrity (Phase 1)**: sha256
- **Integrity (Phase 2)**: sha256
- **Diffie-Hellman Groups (Phase 1)**: 14
- **Diffie-Hellman Groups (Phase 2)**: 14

h. Click **Add Tunnel**.

5. Select **Routes Table**:

a. Click **Add Route**.

The **Add Route** window appears.

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

c. Click **Apply Configuration**.

Step 2: Verifying the Setup

Once you complete the above steps, your tunnel should be active.

1. Verify the setup in the Harmony SASE Administrator Portal:

   a. Click **Networks**.

   b. Locate the tunnel you create, and check the tunnel status.

   It should indicate that the tunnel is **Up**, signifying a successful connection.

2. Verify the setup in the Harmony SASE Agent:

   a. Connect to your network using the Harmony SASE Agent.

   b. Access one of the resources in your environment.

Cisco ASA Firewall

You can configure the tunnel in the Cisco Adaptive security Appliance (ASA) firewall either using CLI or ASDM.

To configure the tunnel in Cisco ASA firewall through CLI:

1. Connect to the firewall through SSH with the privilege-15-level account and then enter the enable mode. For example, using PuTTY.

2. Create a tunnel profile and proposal with the values specified in the Harmony SASE Administrator Portal. Run:

```
crypto ipsec ikev2 ipsec-proposal Tun-Prop
 protocol esp encryption aes-256
 protocol esp integrity sha-512

crypto ipsec profile Tun-Prof
 set ikev2 ipsec-proposal Tun-Prop
 set pfs group21
 set security-association lifetime seconds 3600
```

3. Create a crypto policy with the values specified in the Harmony SASE Administrator Portal. Run:

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha512
 group 21
 prf sha512
 lifetime seconds 28800
crypto ikev2 enable outside
```

4. Select IPsec IKEv2 Tunnels and create a new tunnel with the values specified in the Harmony SASE Administrator Portal. Run:

```
group-policy Tun-Grp-Pol internal
group-policy Tun-Grp-Pol attributes
 vpn-tunnel-protocol ikev2

tunnel-group 131.226.X.X type ipsec-l2l
tunnel-group 131.226.X.X general-attributes
 default-group-policy Tun-Grp-Pol
tunnel-group 131.226.X.X ipsec-attributes
 ikev2 remote-authentication pre-shared-key SuperSecret
 ikev2 local-authentication pre-shared-key SuperSecret
```

5. Create your Virtual Tunnel Interface (VTI). Please be sure to use the IP address in the text. Run:

```
interface Tunnel1
 nameif P81_131.226.X.X
 ip address 169.254.2.122 255.255.255.252
 tunnel source interface outside
```

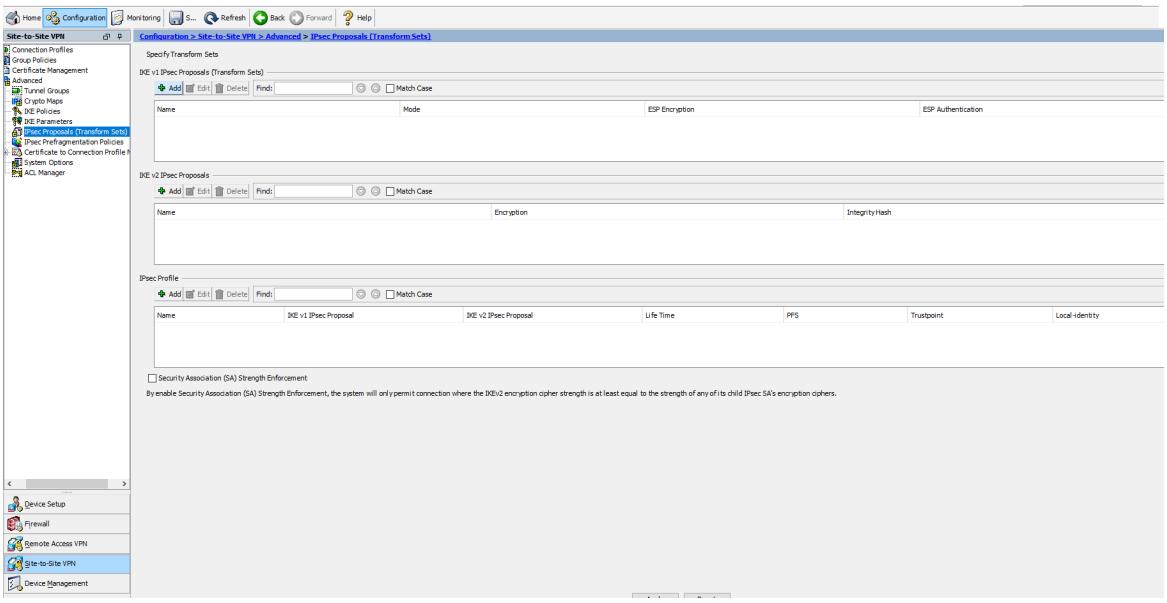
```
tunnel destination 131.226.X.X
tunnel mode ipsec ipv4
tunnel protection ipsec profile Tun-Prof
```

6. Create a route back to the Harmony SASE subnet. Run:

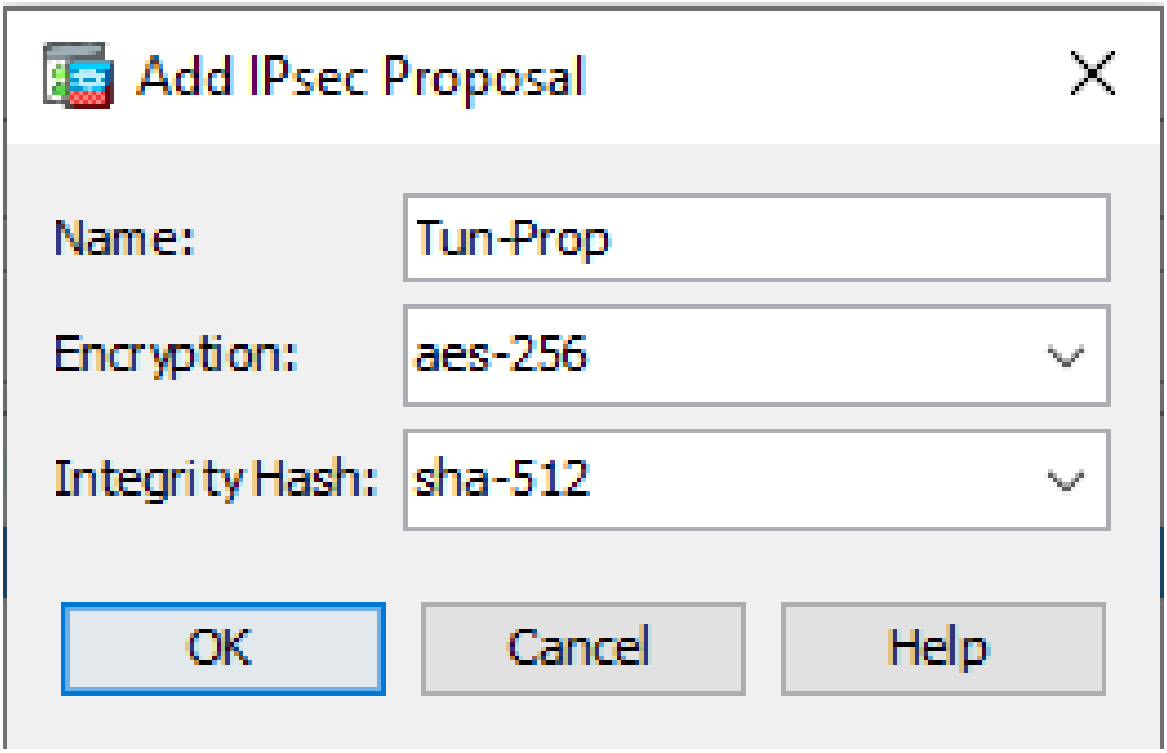
```
route P81_131.226.X.X 10.255.0.0 255.255.0.0 169.254.2.121 1
```

To configure the tunnel with Cisco ASA firewall through Adaptive Security Device Manager (ASDM):

1. Log in to the firewall using ASDM.
2. Create a tunnel profile and proposal with the values specified in the Harmony SASE Administrator Portal:
   a. Click **Configuration > Site-to-site VPN > Advanced > IPsec Proposals (Transform Sets)**.

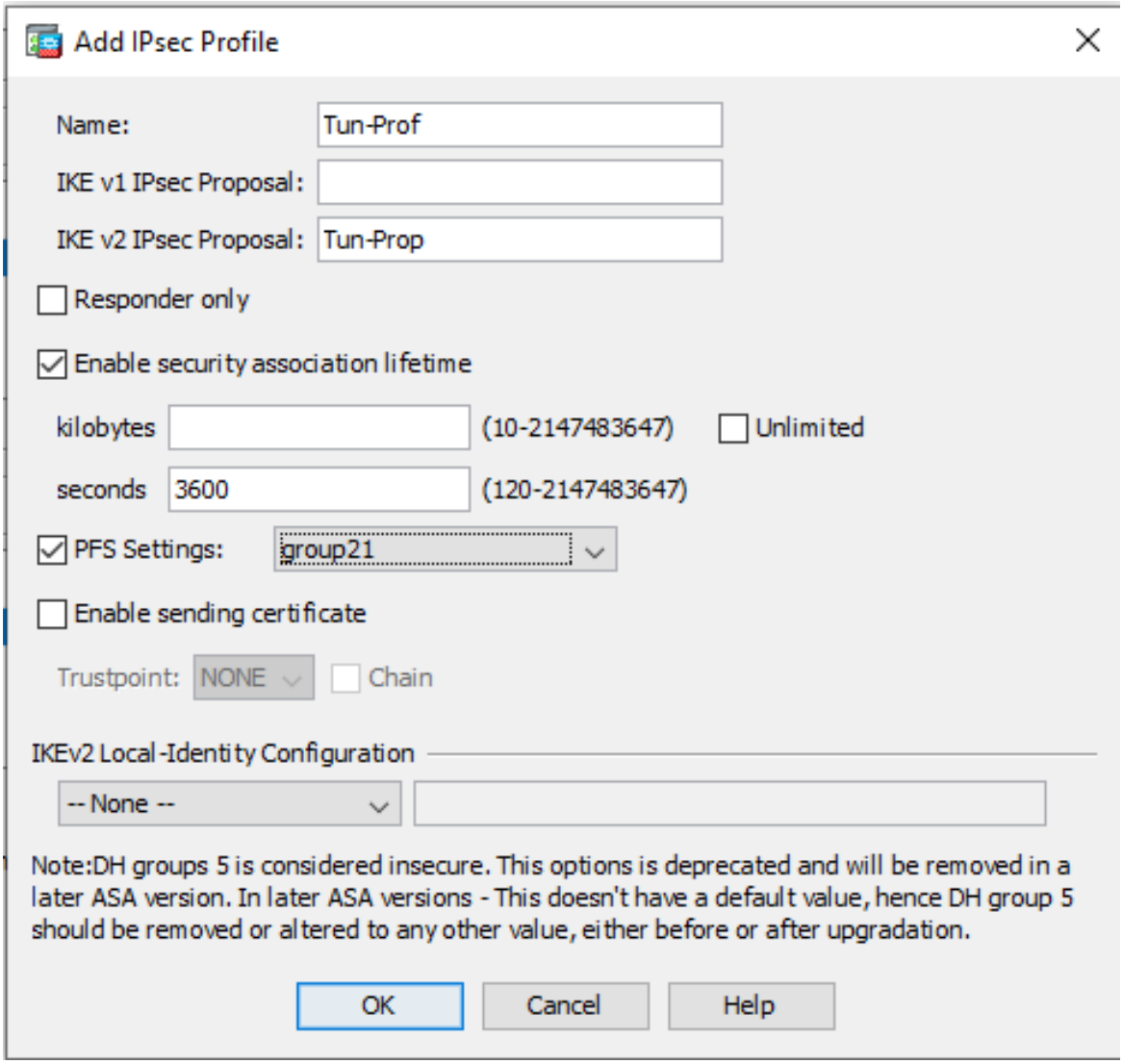


b. In the **IKE v2 IPsec Proposals** section, click **Add**:



Field	Enter
Name	Tun-Prop
Encryption	aes-256
Integrity Hash	sha-512

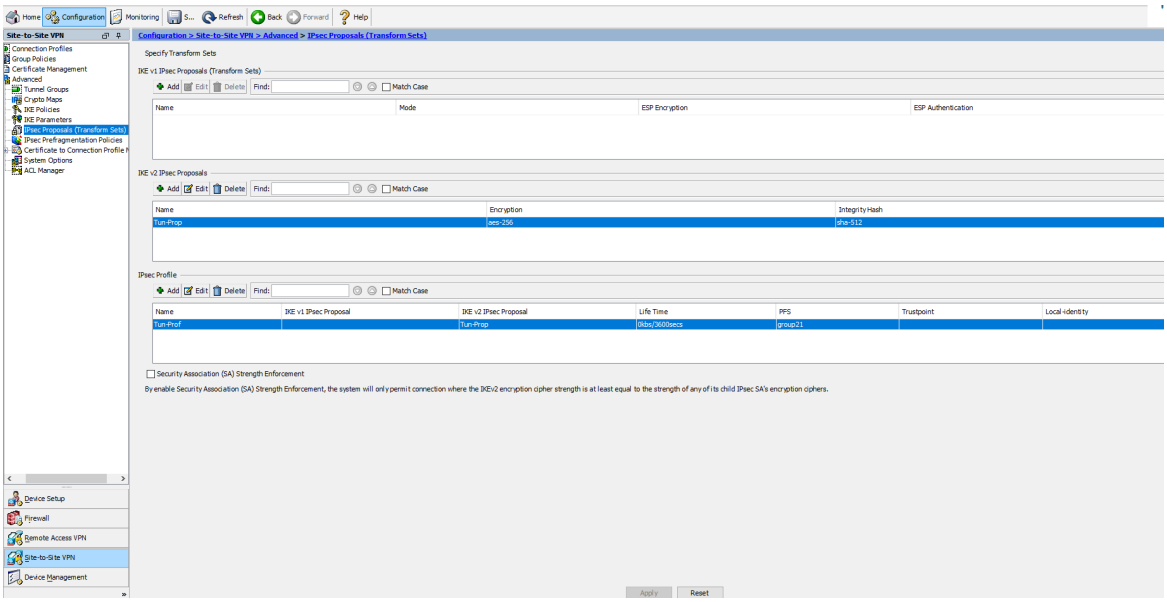
In the **IPsec Profile** section, click **Add**:



Field	Enter
Name	Tun-Prop
IKE v2 IPsec Proposal	Tun-Prop
Enable security association lifetime	Select and leave **kilobytes** blank.
Seconds	3600

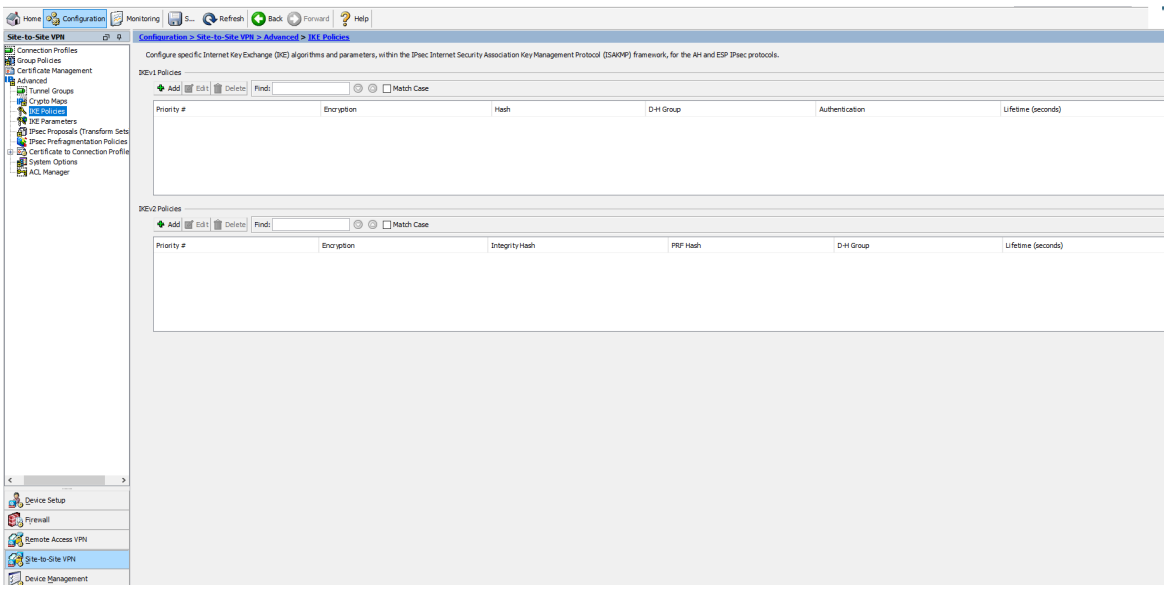
c. Click **OK**.

d. Click **Apply** and **Save**.

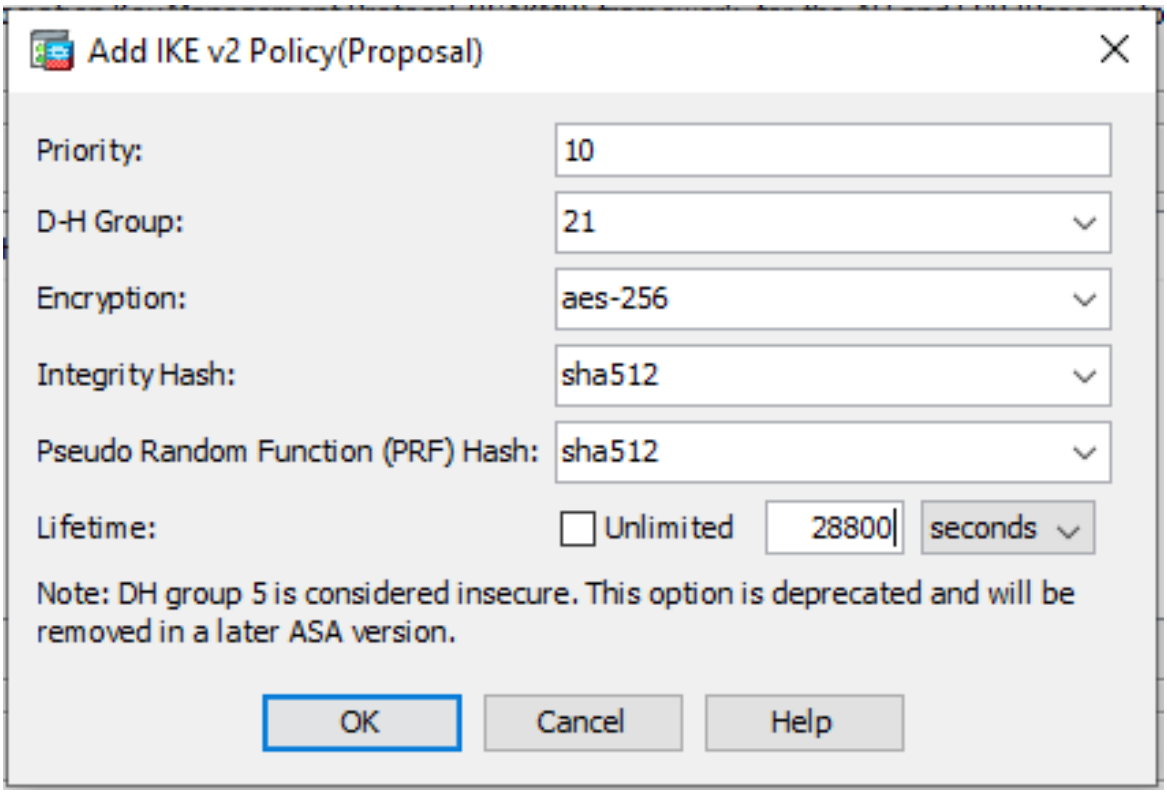


3. Create a crypto policy with the values specified in the Harmony SASE Administrator Portal:

   a. Go to **Configuration > Site-to-Site VPN > Advanced > IKE Policies**.



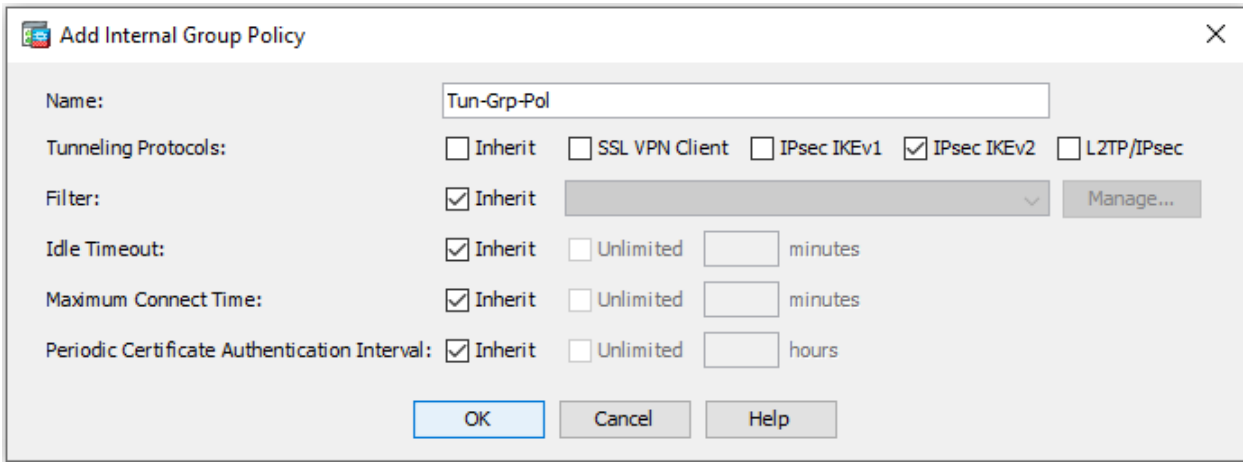
b. In the **IKEv2 Policies** section, click **Add**:



Field	Enter
Priority	10
D-H Group	21
Encryption	AES-256
Integrity Hash	sha256
Pseud0-Random Function (PRF) Hash	sha256
Lifetime	28800 seconds

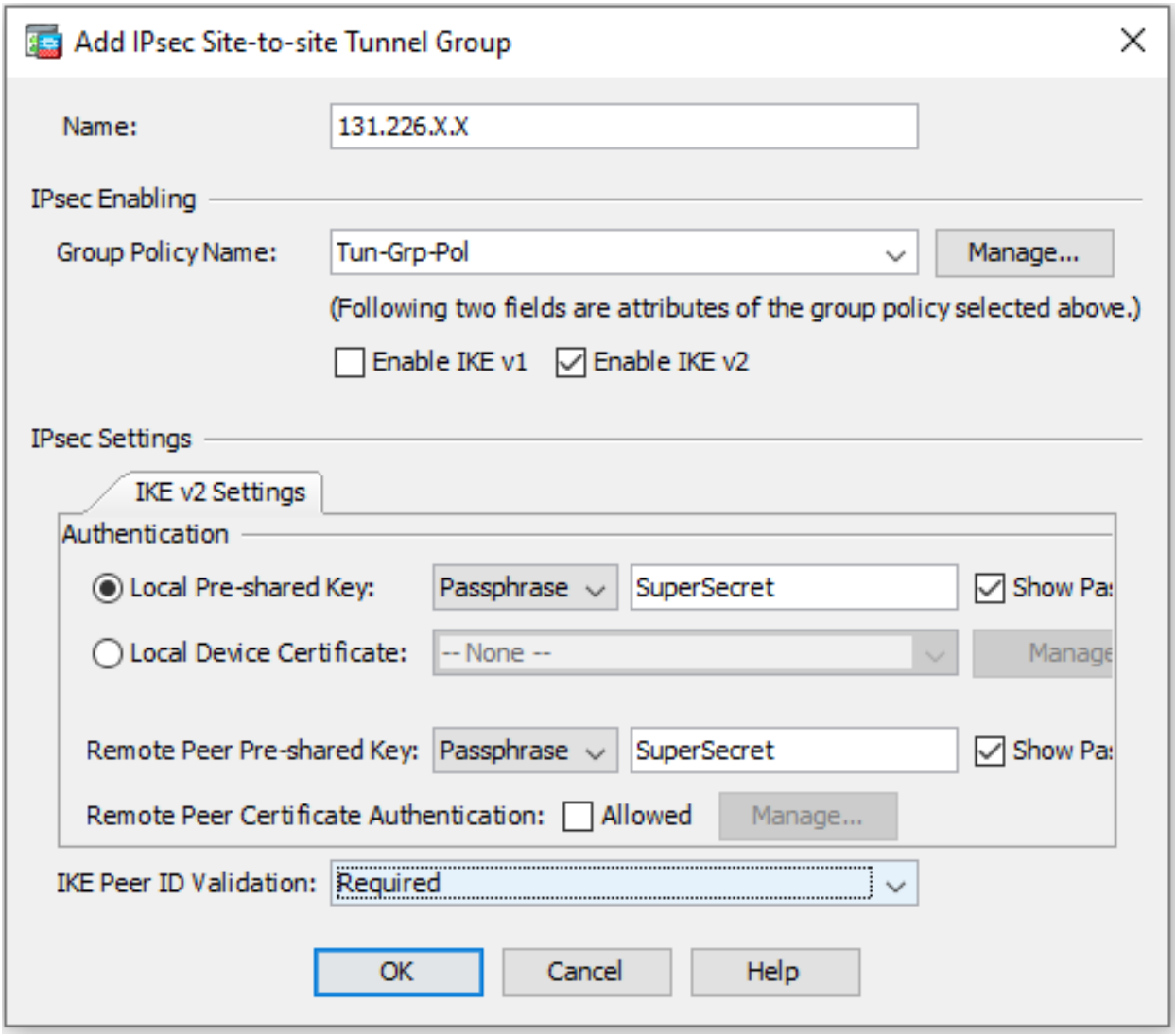
c. Click **OK**.

4. Go to **Configuration > Site-to-Site VPN > Group Policies** and click **Add**:



Field	Enter
Name	Tun-Prop
Tunneling Protocols	IPsec IKEv2

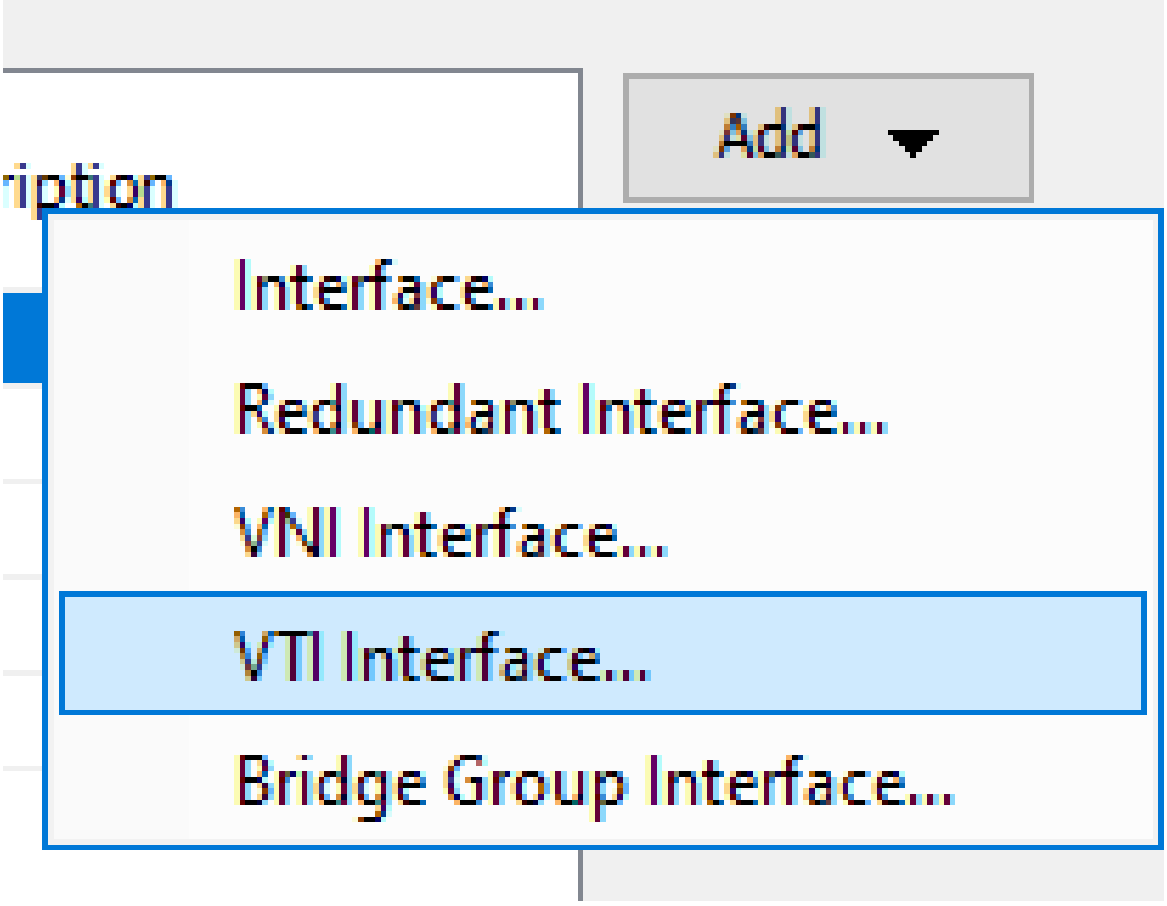
5. Go to **Configuration > Site-to-Site VPN > Advanced > Tunnel Groups** and click **Add**:



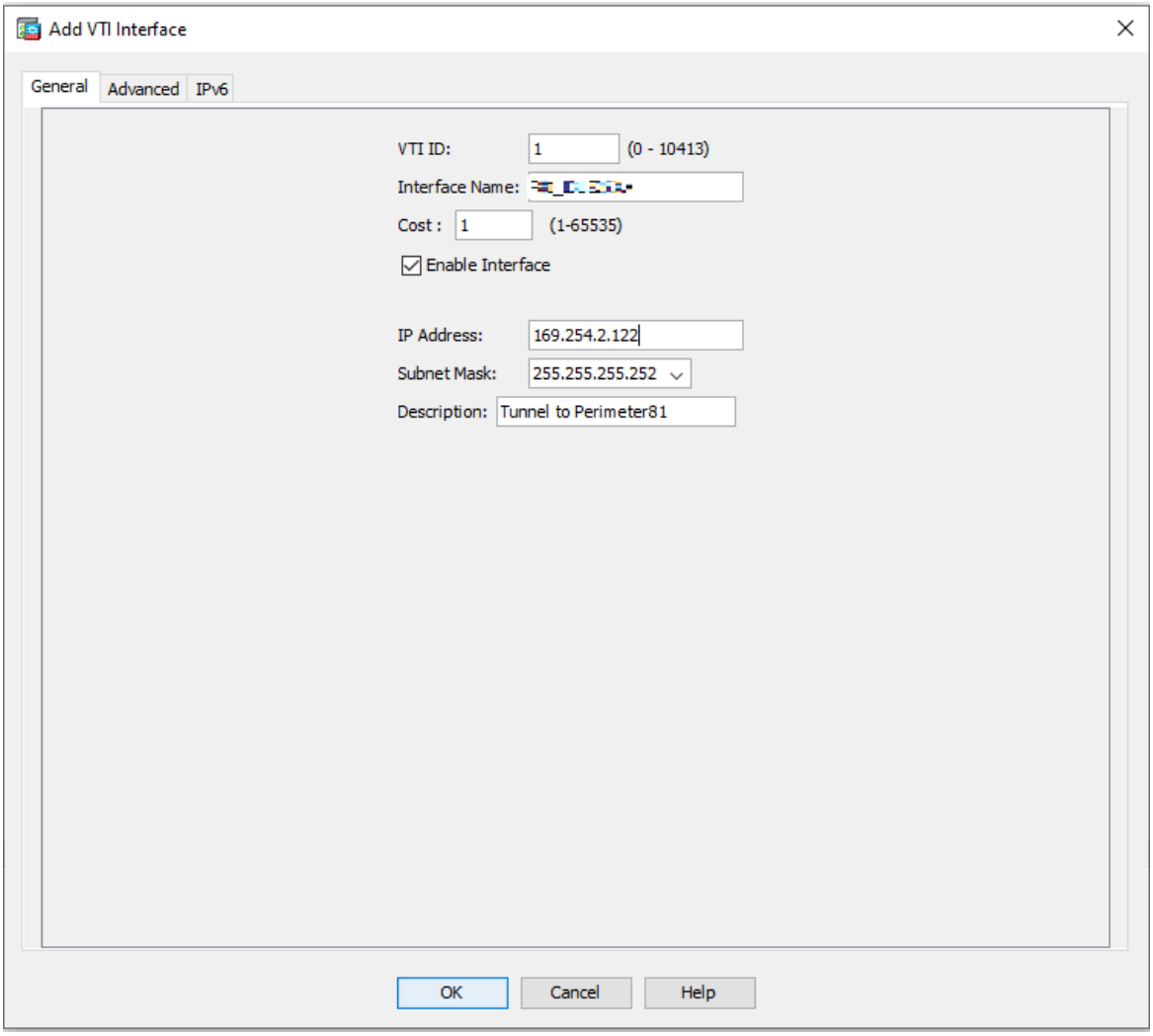
Field	Enter
Name	131.226.x.x. Make sure this is same value specified in the Harmony SASE Administrator Portal.
Group Policy Name	Tun-Grp-Pol
Local Pre-Shared Key	Secret key specified in the Harmony SASE Administrator Portal.
Remote Pre-Shared Key	Secret key specified in the Harmony SASE Administrator Portal.

6. Go to **Configuration > Device Setup > Interface Settings > Interfaces** and click **Add**.

a. Select **VTI Interface**:

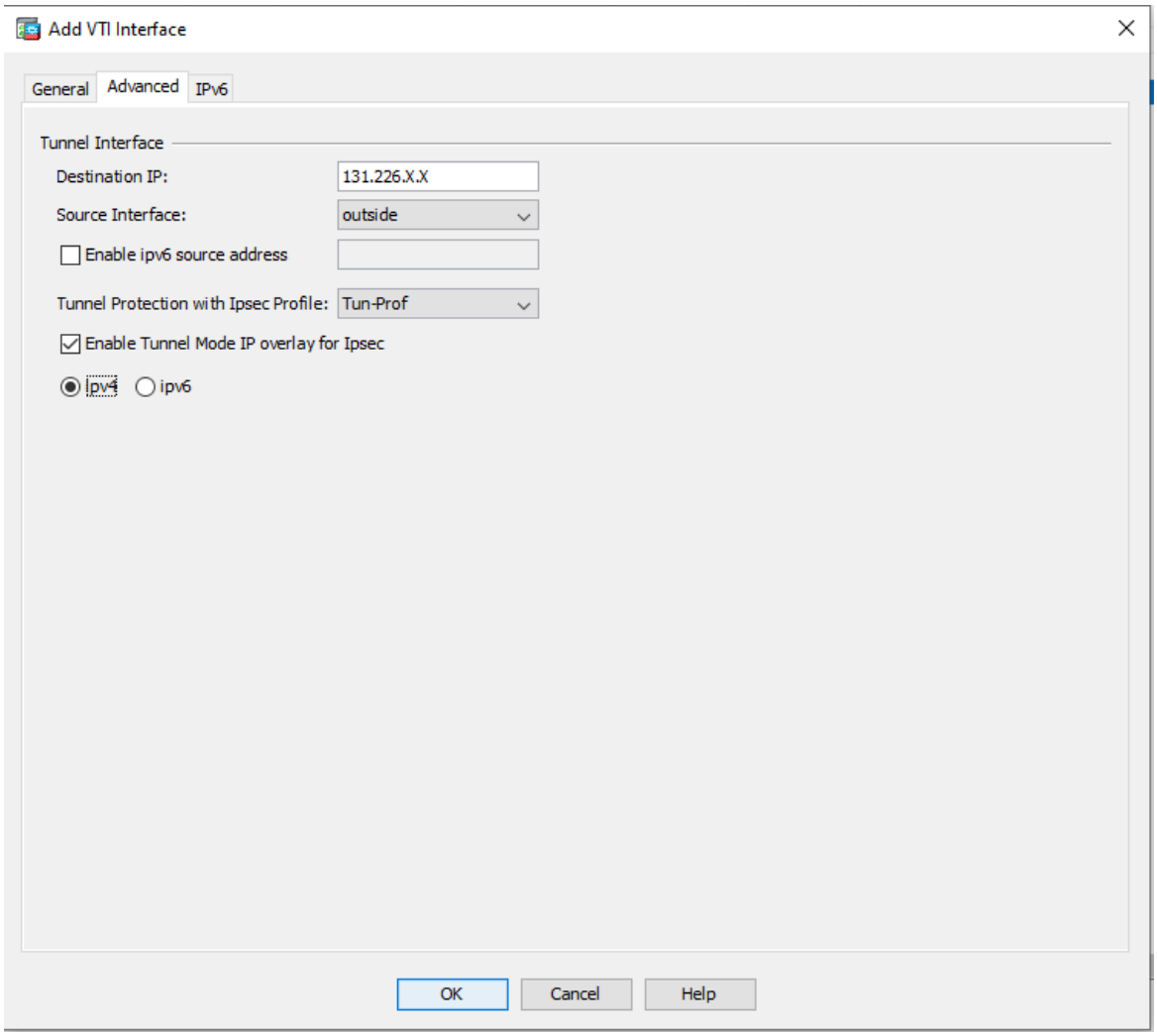


b. In the **General** tab:



Field	Enter
VTI ID	1
Interface Name	Name for the interface.
IP Address	169.254.2.122
Subnet Mask	255.255.255.252
Description	Tunnel to Harmony SASE.

c. In the **Advanced** tab:

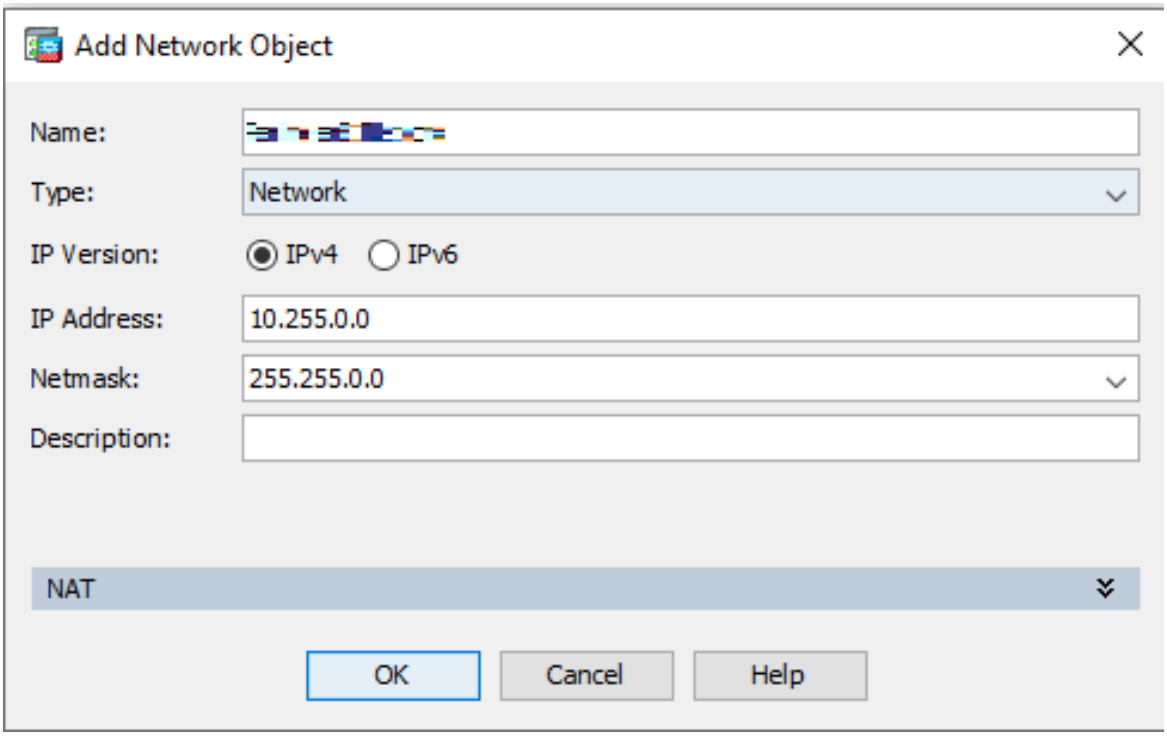


Field	Enter
Destination IP	131.226.x.x. Public IP address of Harmony SASE gateway.
Source Interface	Name for your outside interface.
Tunnel Protection with Ipsec Profile	Tun-Prof
Enable Tunnel Mode IP overlay for Ipsec	Select and select **ipv4**.

7. Create a route back to the Harmony SASE subnet:

a. Go to **Configuration > Firewall > Objects > Network Objects/Groups**.

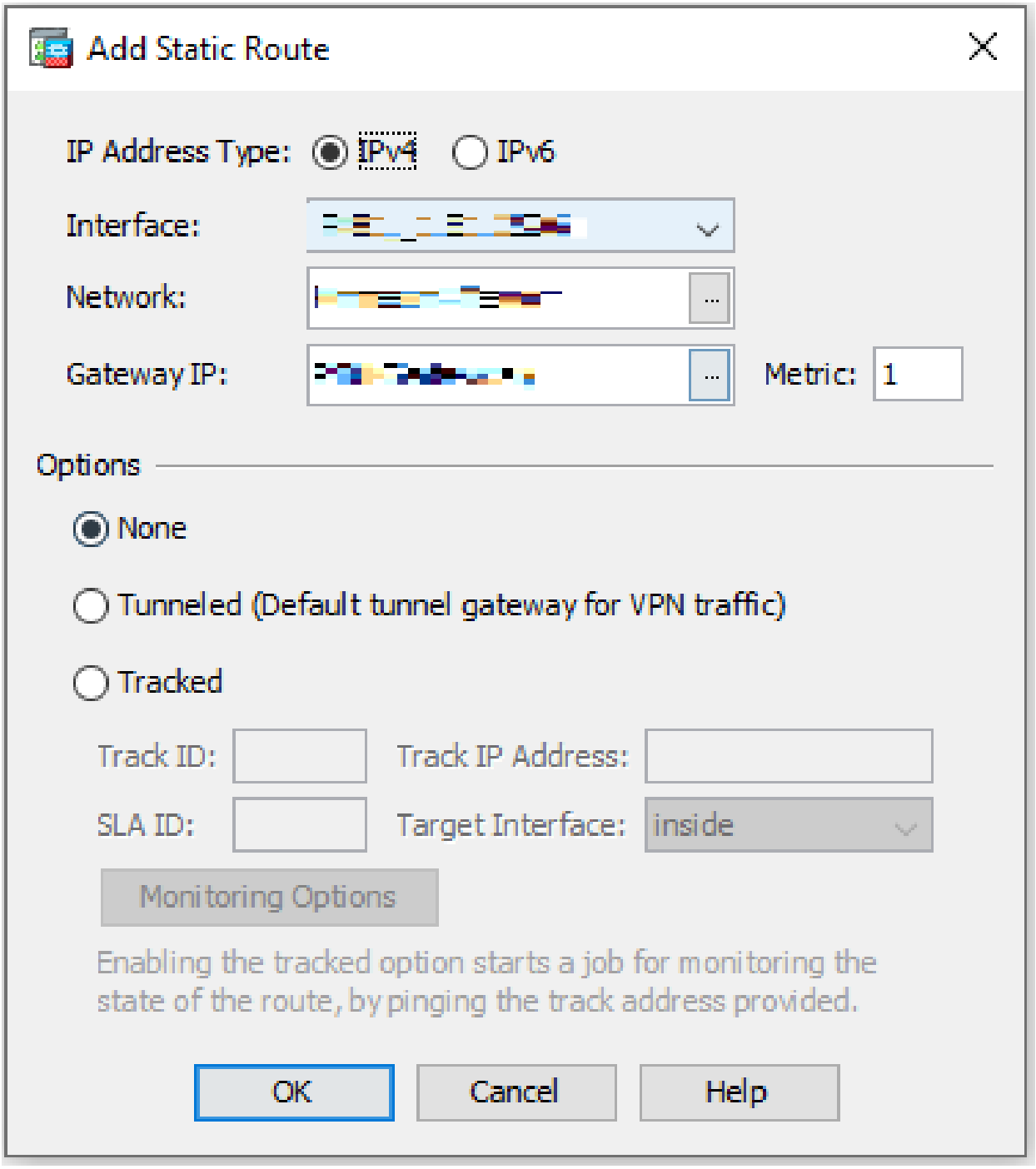
b. Clicking **Add > Network Object**:



Field	Enter
Name	Name for the object.
Type	Host
IP Version	IPv4
IP Address	169.254.2.121

c. Click **OK**.

8. Go to **Configuration > Device Setup > Routing > Static Routes** and then click Add:

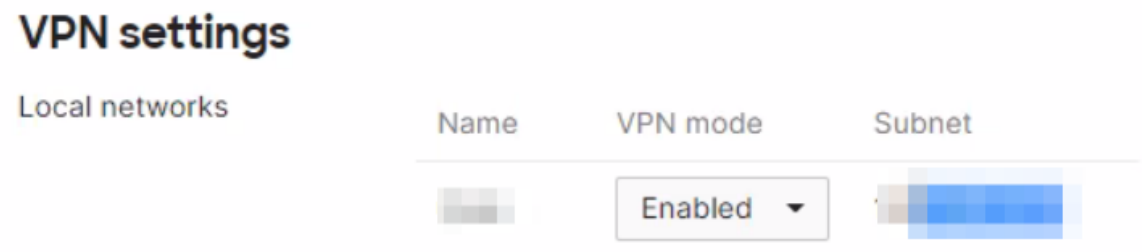


Field	Enter
IP address Type	IPv4
Interface	Interface that you created for the setup.
Network	Network that you created for the setup.
Gateway IP	Gateway that you created for the setup.

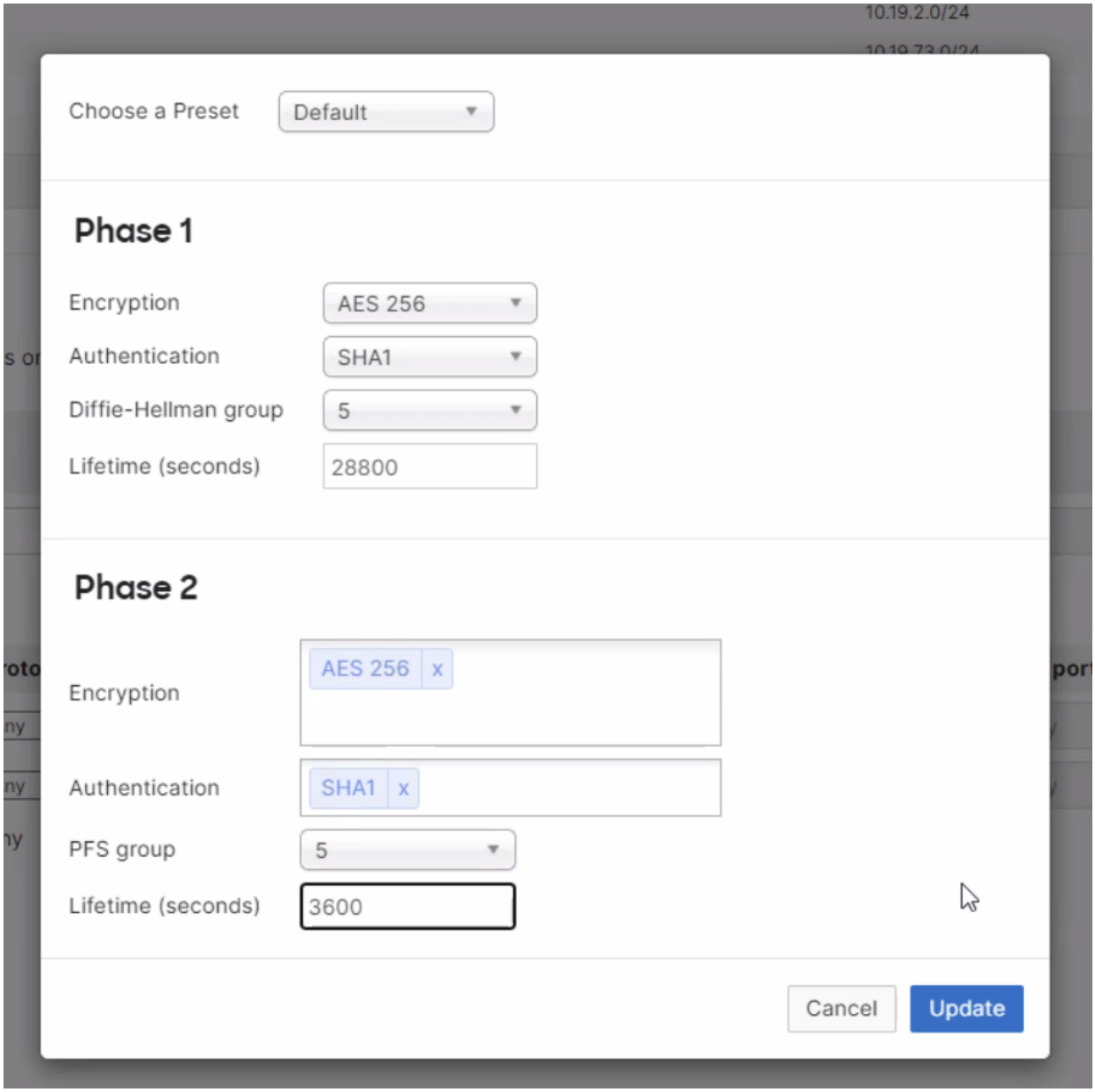
Cisco Meraki Router

To configure the tunnel in the Cisco Meraki Management Portal:

1. Log in to the Cisco Meraki Management Portal with the Administrator account.
2. Go to **Security Appliance > Configure > Site-to-site VPN**.
3. Make sure that the local LAN you want t connect from the Harmony SASE network is participating in the VPN.



4. Scroll down to the **Non-Meraki VPN peers** section.
5. Click **Add a peer**:



Field	Enter
Name	Name for the remote device or VPN.
IKE Version	IKEv1
Public Ip	Public IP address of the Harmony SASE gateway.
Remote ID	Public IP address of the Harmony SASE gateway.
Private subnets	Harmony SASE network subnets. Default is 10.255.0.0/16.
Preshared secret key	Secret key specified in the Harmony SASE Administrator Portal.

Field	Enter
IPsec Policy to use	Custom
Phase 1	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	28800
Phase 2	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	3600

6. Click **Update**.
7. Edit the router rules to allow the traffic through the Harmony SASE tunnel. These rules apply to inbound and/or outbound VPN traffic from all MX appliances in the organization that participate in site-to-site VPN.

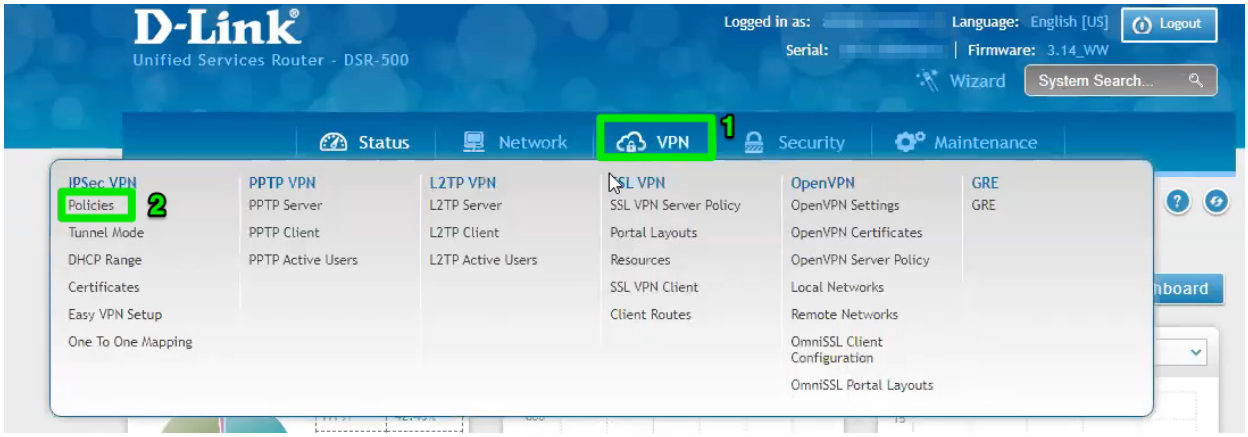
   To create a rule, got to **Security Appliance > Configure > Site-to-site VPN**, in the **Site-to-site firewall** section, select **Add a rule**.

   For reference, see the Layer 3 firewall rules.

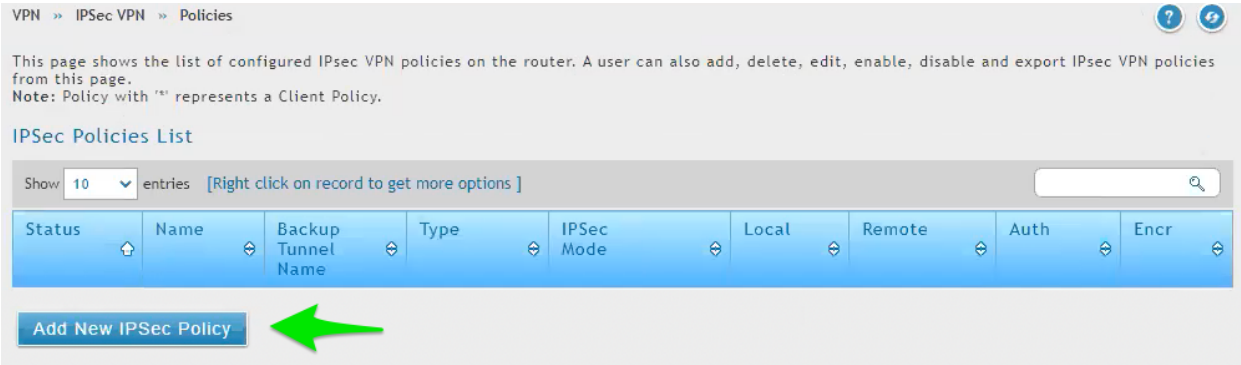
D-Link DSR Series Router

To configure the tunnel in the D-Link DSR Series Router Management Portal:

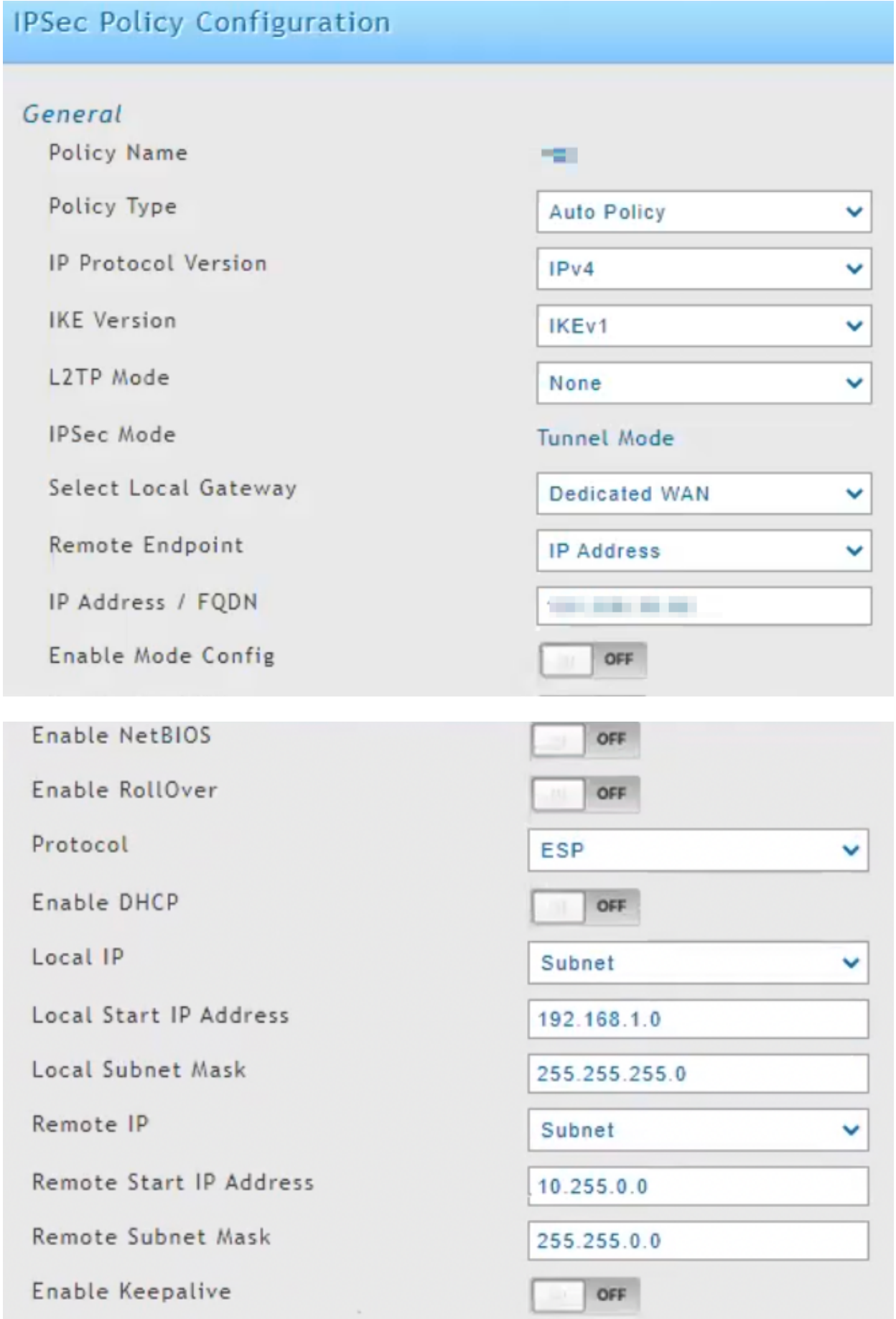
1. Log in to the D-Link DSR Series Router Management Portal with the Administrator.
2. Click **VPN**.



3. Click **IPSec VPN > Policies**.
4. Click **Add New IPSec Policy**.

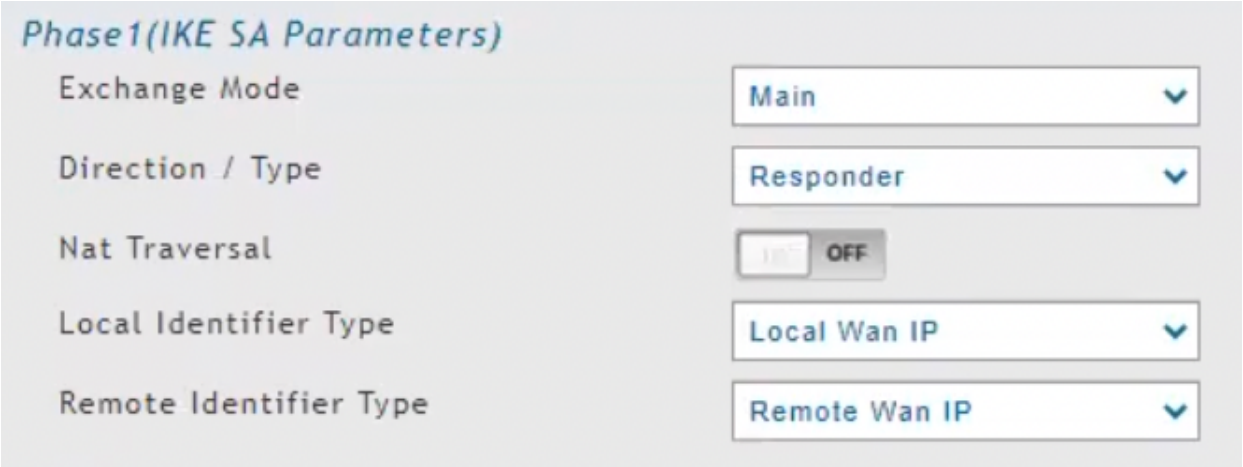


5. In the **General** section:


IPSec Policy Configuration
General
Policy Name
Policy Type
Auto Policy
IP Protocol Version
IPv4
IKE Version
IKEv1
L2TP Mode
None
IPSec Mode
Tunnel Mode
Select Local Gateway
Dedicated WAN
Remote Endpoint
IP Address
IP Address / FQDN
Enable Mode Config
OFF
Enable NetBIOS
OFF
Enable RollOver
OFF
Protocol
ESP
Enable DHCP
OFF
Local IP
Subnet
Local Start IP Address
192.168.1.0
Local Subnet Mask
255.255.255.0
Remote IP
Subnet
Remote Start IP Address
10.255.0.0
Remote Subnet Mask
255.255.0.0
Enable Keepalive
OFF

Field	Enter
Policy Name	Name for the policy.
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address/FQDN	Public IP address of the Harmony SASE gateway.
Enable Config Mode	Off
Enable NetBIOS	Off
Enable RollOver	Off
Protocol	ESP
Enable DHCP	Off
Local IP	Subnet
Local Start IP Address	Your local subnet
Local Subnet Mask	Matching subnet mask
Remote IP	Subnet
Remote Start IP Address	10.255.0.0
Remote Subnet Mask	255.255.0.0
Enable Keepalive	Off

6. In the **Phase1 (IKE SA Parameters)** section:



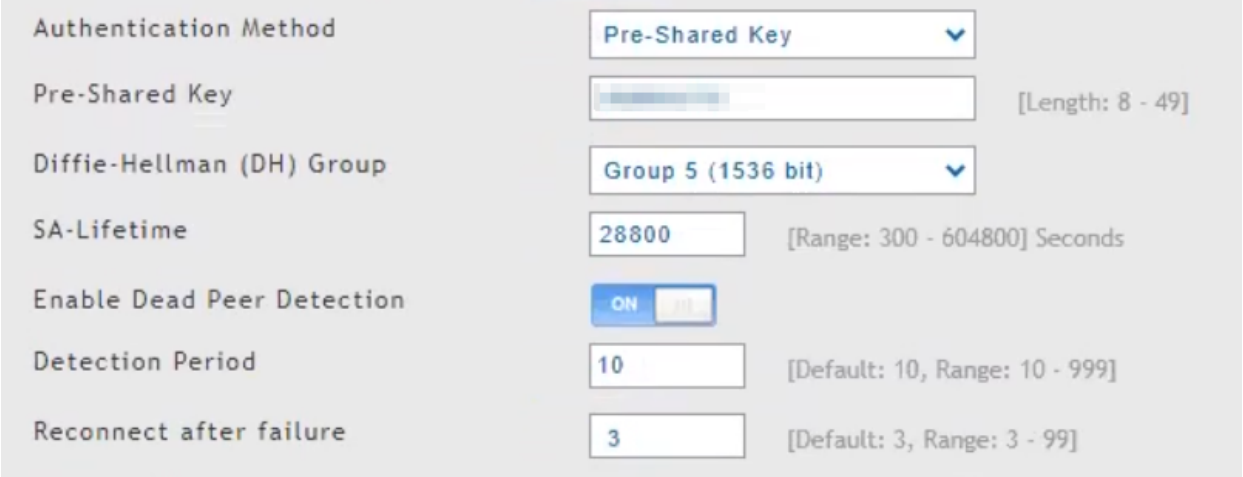
Field	Enter
Exchange Mode	Main
Direction/Type	Responder
NAT Traversal	Off
Local Identifier Type	Local Wan IP
Remote Identifier Type	Remote Wan IP

7. In the **Encryption Algorithm** section:

Field	Enter
DES	Off
AES-128	Off
AES-256	On
Blowfish	Off

Field	Enter
3DES	Off
AES-192	Off

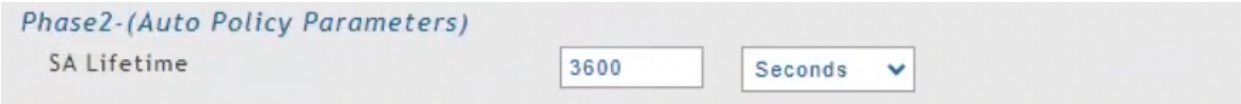
8. In the **Authentication Algorithm** section:



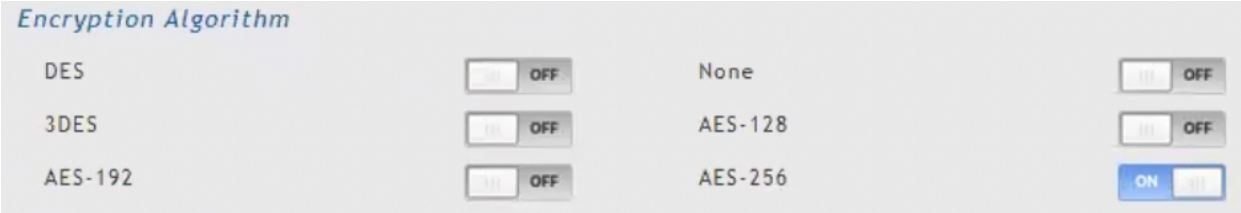
Field	Enter
MD5	Off
SHA2-256	Off
SHA2-512	On
Authentication Method	Pre-Shared Key
Pre-Shared Key	Secret key specified in the Harmony SASE Administrator Portal.
Diffie-Hellman (DH) Group	Group 5
SA-Lifetime	28800

Field	Enter
Enable dead Peer Detection	On
Detection Period	10
Reconnect after failure	3

9. In the **Phase2 - (Auto Policy Parameters)** section, in the **SA Lifetime** field, enter **3600 seconds**.



10. In the **Encryption Algorithm** section:



Field	Enter
DES	Off
3DES	Off
AES-192	Off
None	Off
AES-128	Off
AES-256	On

11. In the **Integrity Algorithm** section:

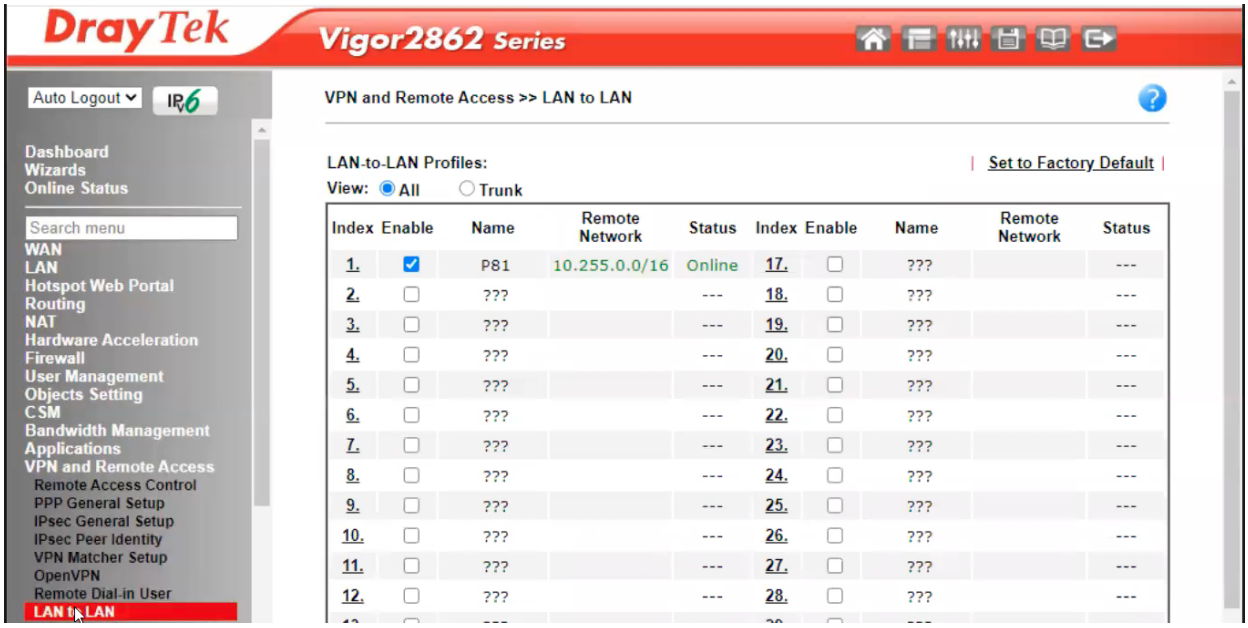
Field	Enter
MD5	Off
SHA-224	Off
SHA2-384	Off
PFS Key Group	On
SHA-1	Off
SHA2-256	Off
SHA2-512	On

12. Click **Save**.

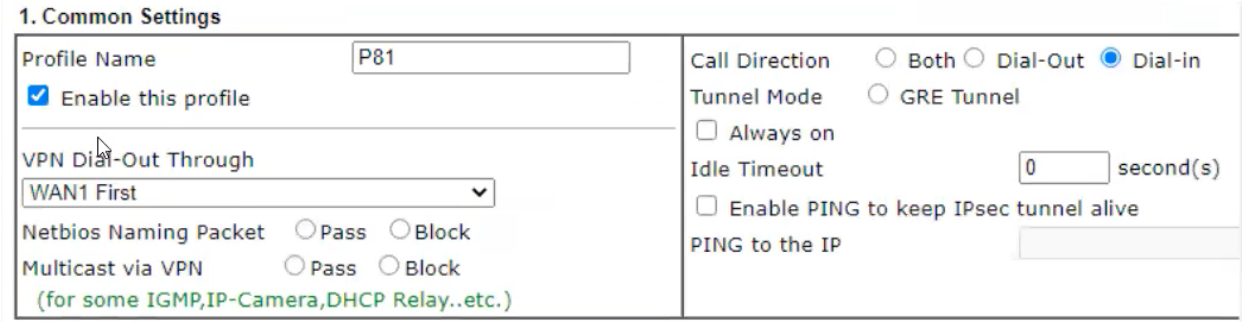
DrayTek Vigor2862 Router

To configure the tunnel in the DrayTek Vigor2862 Management Portal:

1. Log in to the DrayTek Vigor2862 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **LAN to LAN** and create a new profile.

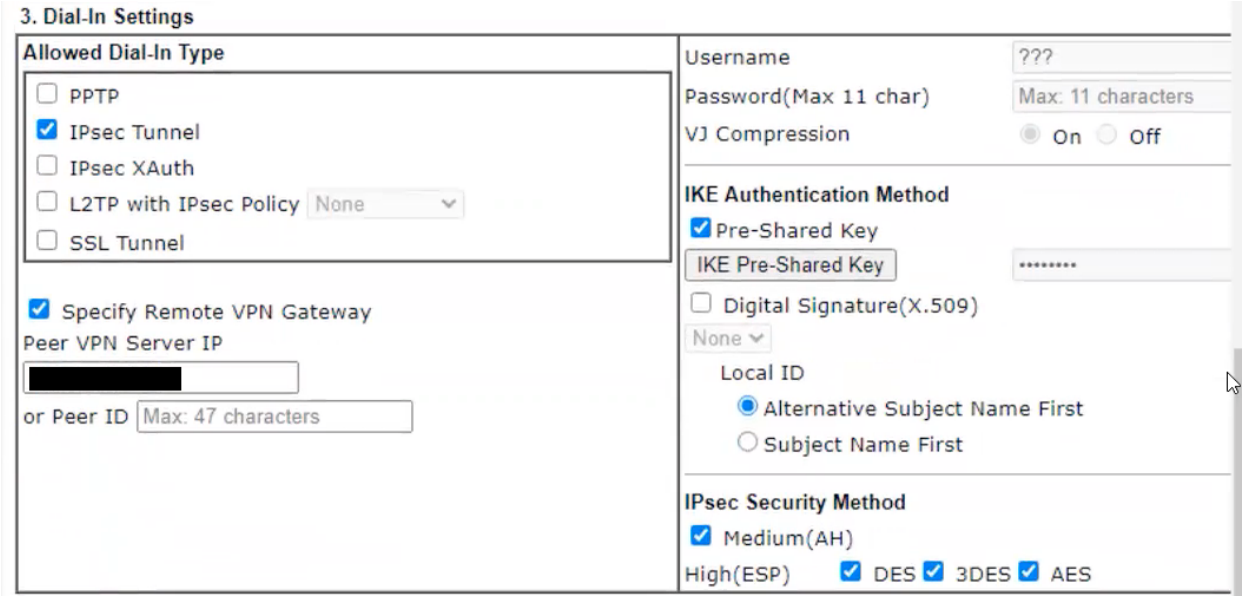


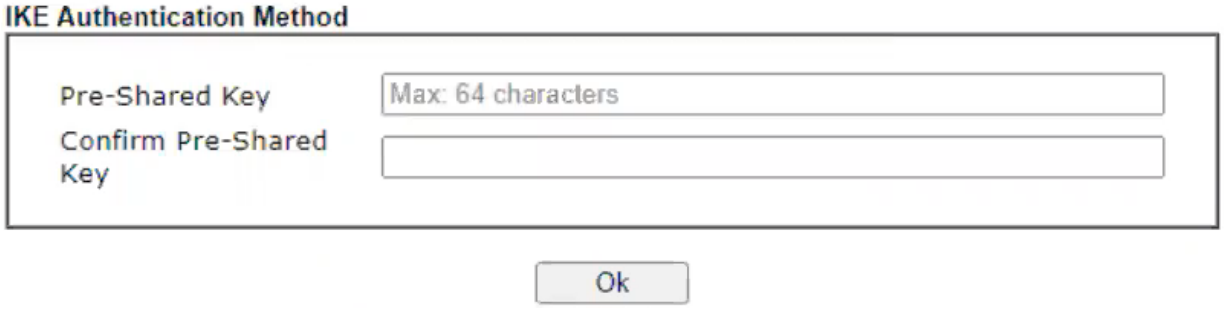
4. In the **Custom Settings** tab:



Field	Enter
Profile Name	Name for the profile. For example, Harmony SASE.
Enable this profile	Select
VPN Dial-Out Through	Your WAN interface.
Call Direction	Dial-in
Idle Timeout	0

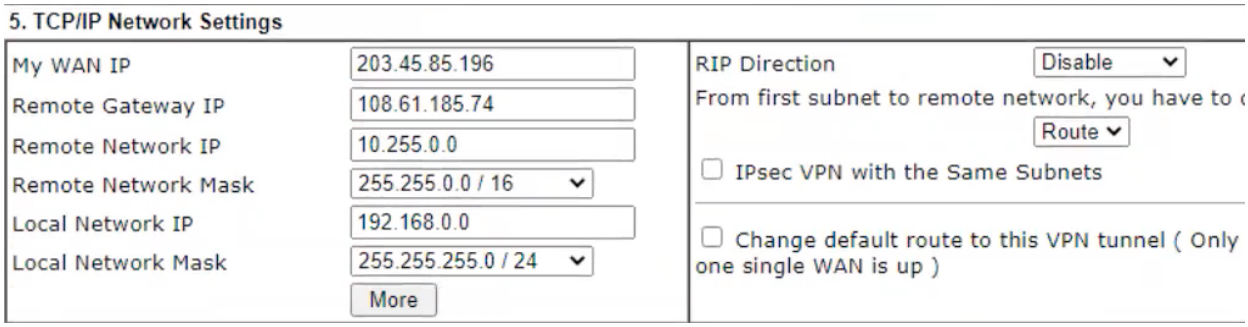
5. In the **Dial-In Settings**tab:





Field	Enter
Allowed Dial-In Type	IPsec Tunnel
Specify Remote VPN Gateway	Public IP address of the Harmony SASE gateway.
Pre-Shared Key	Select and click **IKE Pre-Shared Key** and enter the secret key specified in the Harmony SASE Administrator Portal.

6. In the **TCP/IP Network Settings** tab:

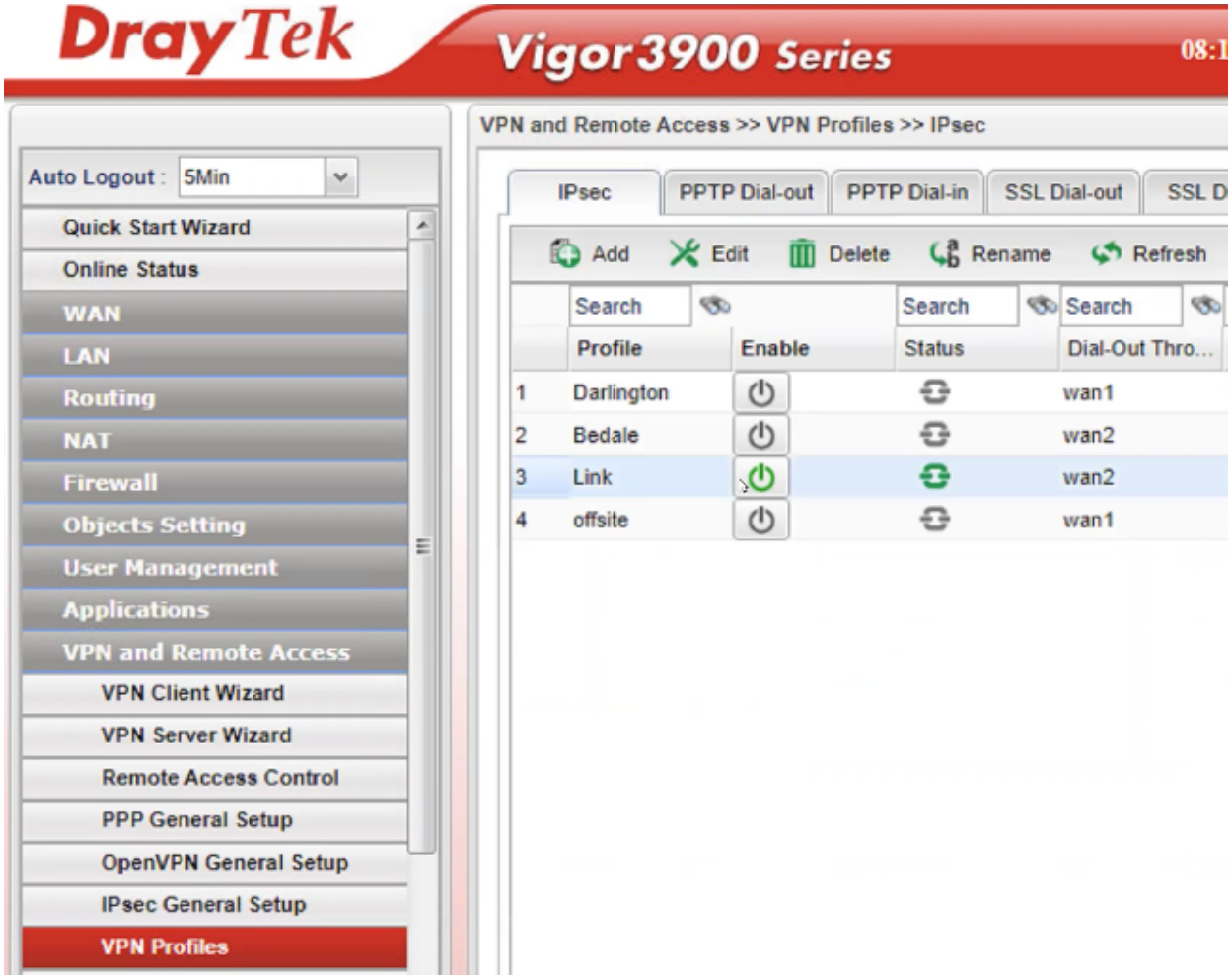


Field	Enter
My WAN IP	Your WAN interface's default IP address.
Remote Gateway IP	Public IP address of the Harmony SASE gateway.
Remote Network IP	Harmony SASE network subnet.
Local Network IP	Your LAN subnnet.

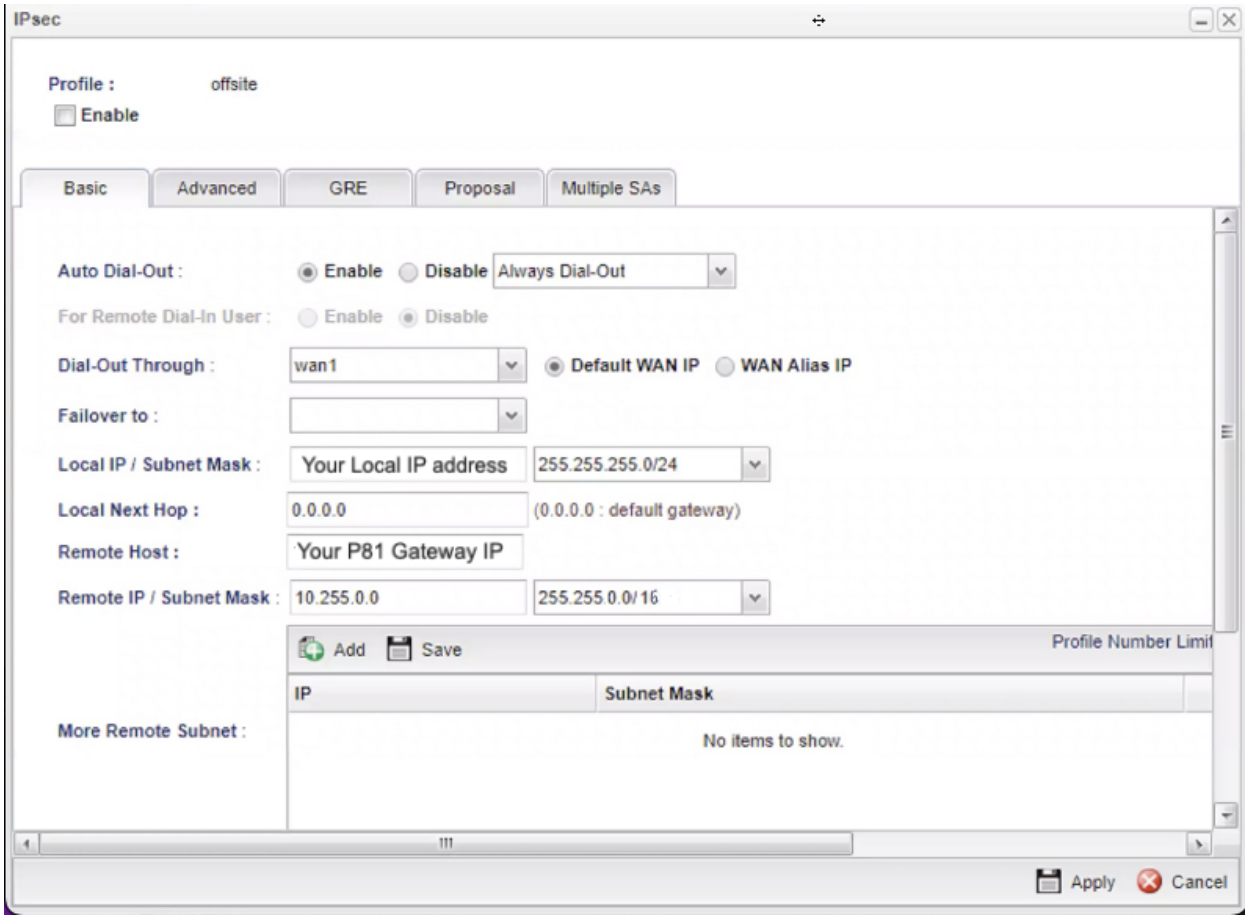
DrayTek Vigor3900 Router

To configure the tunnel in the DrayTek Vigor3900 Management Portal:

1. Log in to the DrayTek Vigor3900 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **VPN Profiles** and click **Add**.



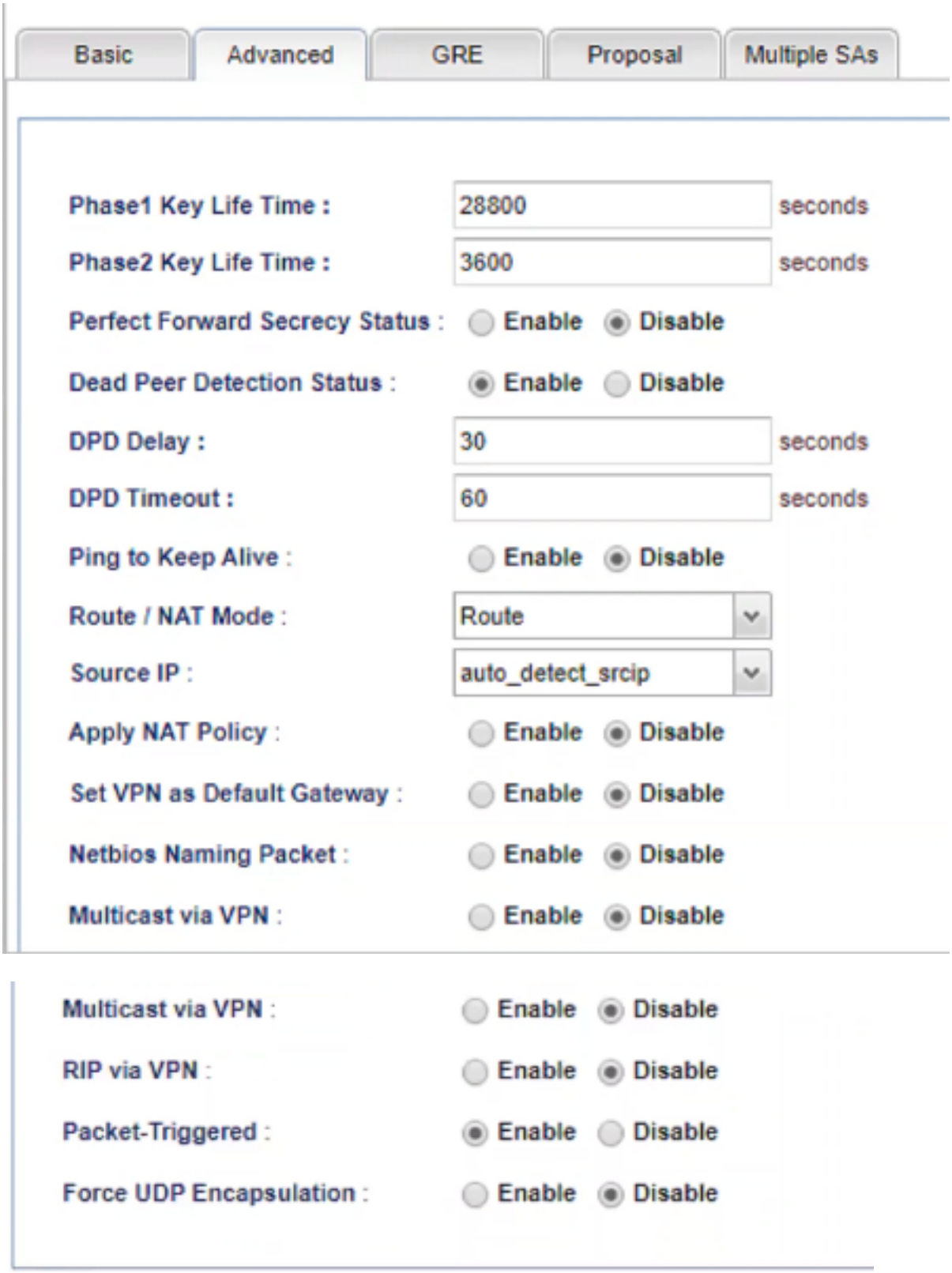
4. In the **Basic** tab:



Field	Enter
Auto Dial-Out	Enable; Always Dial-Out
Dial-Out Through	Your WAN interface; Default WAN IP
Failover	Blank
Local IP / Subnet Mask	Your router external IP address and subnets.
Remote Host	Public IP address of the Harmony SASE gateway.

Field	Enter
Remote IP / Subnet Mask	Default is 10.255.0.0 and 255.255.0.0/16. If you modified these in the Harmony SASE Administrator Portal, enter the modified values.
IKE Protocol	IKEv1
IKE Phase 1	Main Mode
Auth Type	PSK
Pre-shared Key	Secret key specified in the Harmony SASE Administrator Portal.
Security Protocol	ESP

5. In the **Advanced** tab:



Field	Enter
Phase 1 Key Lifetime	28800 seconds

Field	Enter
Phase 2 Key Lifetime	3600 seconds
Perfect Forward Secrecy Status	Enable
DPD Status	Enable
DPD Delay	30 seconds
DPD Timeout	60 seconds
Ping to Keep Alive	Disable
Route/NAT Mode	Route
Source IP	Auto-detect
Apply NAT Policy	Disable
Set VPN Default Gateway	Disable
Netbios Naming Packet	Disable
Multicast via VPN	Disable
RIP via Triggered	Enable
Packet Triggered	Enable
Force UDP Encapsulation	Disable

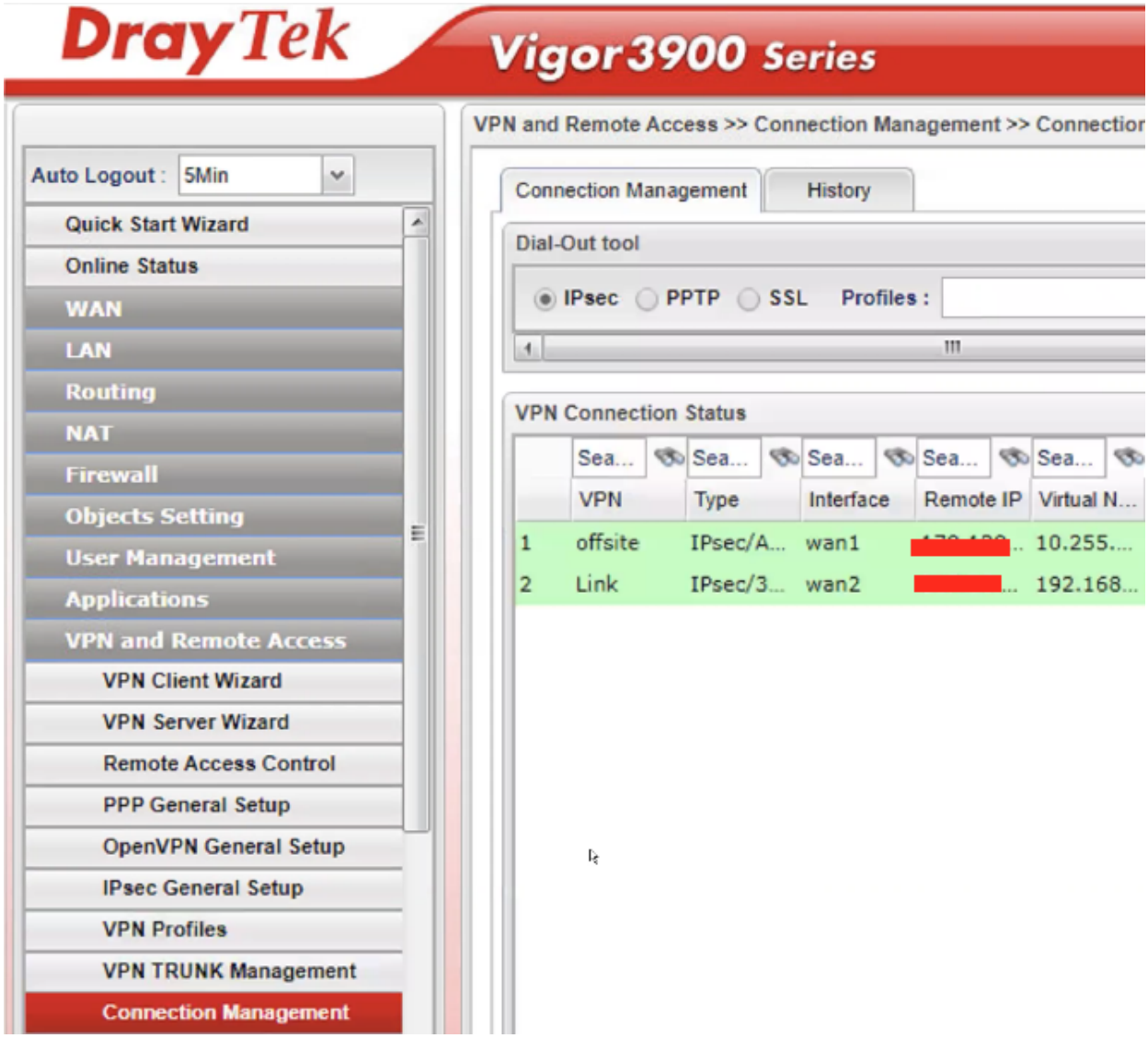
6. In the **GRE** tab:

Field	Enter
Enable GRE Function	Disable
Auto Generate GRE Key	Enable

7. In the **Proposal** tab:

Field	Enter
IKE Phase 1 Proposal	AES 256 G2
IKE Phase 1 Authentication	SHA1
IKE Phase 2 Proposal	AES 256 with auth
IKE Phase 2 Authentication	SHA1
Accepted Proposal	Accept

8. Click **Apply**.
9. To verify if the tunnel is up, from the left pane, click **Connection Management** and check if the profile is listed and highlighted in Green.



EdgeMax Router

To configure the tunnel in the EdgeMax Router through CLI:

1. Connect to the router through SSH and then enter the configuration mode. For example, using PuTTY.
2. Enable the **auto-firewall-nat-exclude** feature which automatically creates the IPsec firewall/NAT policies in the iptables firewall. Run:

```
set vpn ipsec auto-firewall-nat-exclude enable
```

3. Create IKE / Phase 1 (P1) Security Associations (SAs). Run:

```
set vpn ipsec ike-group FOO0 lifetime 28800
set vpn ipsec ike-group FOO0 proposal 1 dh-group 14
set vpn ipsec ike-group FOO0 proposal 1 encryption aes256
set vpn ipsec ike-group FOO0 proposal 1 hash sha1
set vpn ipsec ike-group FOO0 dead-peer-detection interval 15
set vpn ipsec ike-group FOO0 dead-peer-detection timeout 30
```

4. Create the ESP / Phase 2 (P2) SAs and enable Perfect Forward Secrecy (PFS). Run:

```
set vpn ipsec esp-group FOO0 lifetime 3600
set vpn ipsec esp-group FOO0 pfs enable
set vpn ipsec esp-group FOO0 proposal 1 encryption aes256
set vpn ipsec esp-group FOO0 proposal 1 hash sha1
```

5. Define the remote peering address. Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication mode pre-shared-secret
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication pre-shared-secret <secret key from Quantum SASE
Administrator Portal>
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
description ipsec
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
local-address <Your Edgerouter WAN IP>
```

6. Link the SAs created above to the remote peer and bind the VPN to a virtual tunnel interface (vti0). Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
ike-group FOO0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti bind vti0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti esp-group FOO0
```

7. Configure the virtual tunnel interface (vti0) and assign an internal IP address that is not used in any site. Run:

```
set interfaces vti vti0 address 192.168.20.20/32
```

8. Create a static route for the Harmony SASE subnet (the default is 10.255.0.0/16). Run:

```
set protocols static interface-route 10.255.0.0/16 next-hop-
interface vti0
```

9. Commit the changes and save the configuration. Run:

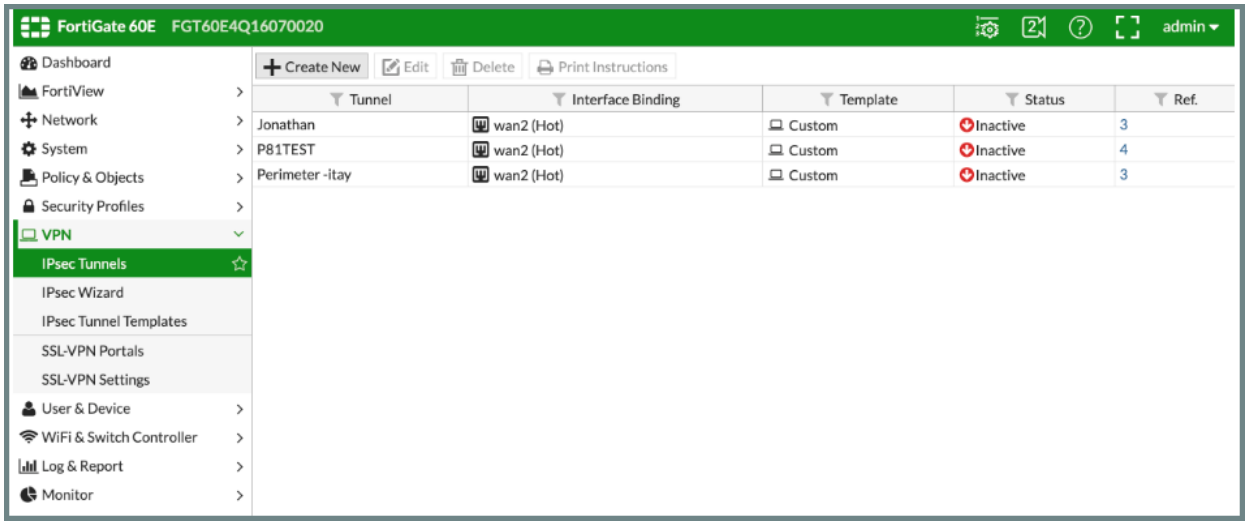
```
commit ; save
```

10. In the EdgeMax Management portal, go **VPN - site to site connection**.
11. Verify that the peer associated with the gateway IP address obtained from Harmony SASE has:
    - **Remote subnet**: 10.255.0.0/16 (or the local Harmony SASE gateway that you selected)
    - **Local subnet**: All the subnet range (CIDR) of your LAN devices

FortiGate Next Generation Firewall

To configure the tunnel in the FortiGate Next Generation Firewall Management Portal:

1. Log in to the FortiGate Next Generation Firewall Management Portal.
2. Go to **VPN > IPSec Tunnels**.

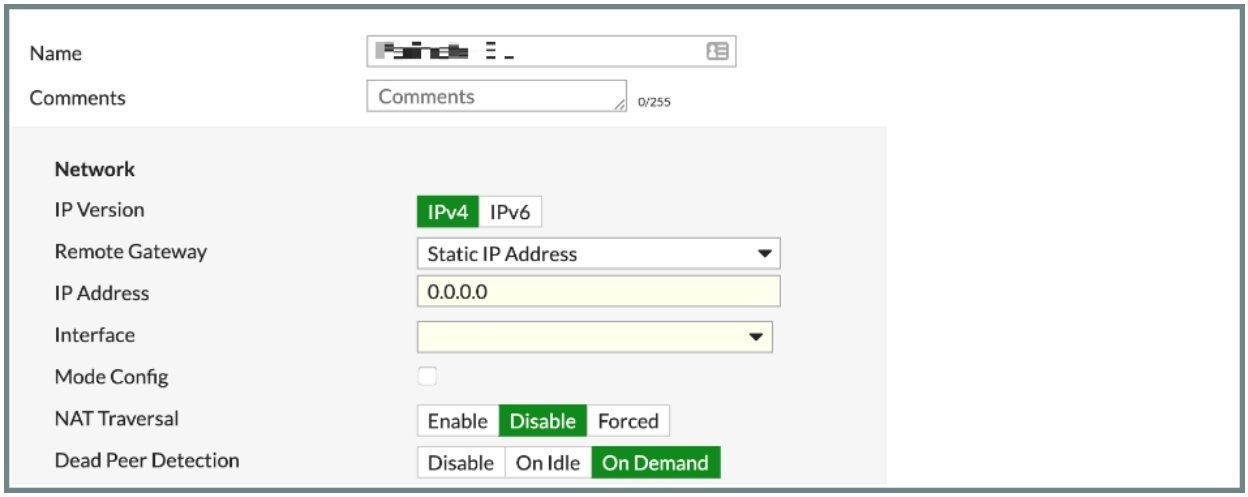


3. Click **Create New**.

   The **VPN Creation Wizard** window appears.

4. In the **Name** field, enter a name for the tunnel.

5. Set **Template Type** to **Custom**.
6. Click **Next**.



7. In the **Network** section:

Field	Enter
IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	Public IP address of the location server.
Interface	Your WAN interface.
Mode Config	Clear
NAT Traversal	Disable **Note** - If the tunnel stops to respond while its status is active, change the settings to **Enable**.
Dead Peer Detection	On-Demand

8. In the **Authentication** section:

Field	Enter
Method	Pre-shared key
Pre-shared Key	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

Field	Enter
IKE Version	2
Mode	Main (ID Protection).

9. In the **Phase 1 Proposal** section:

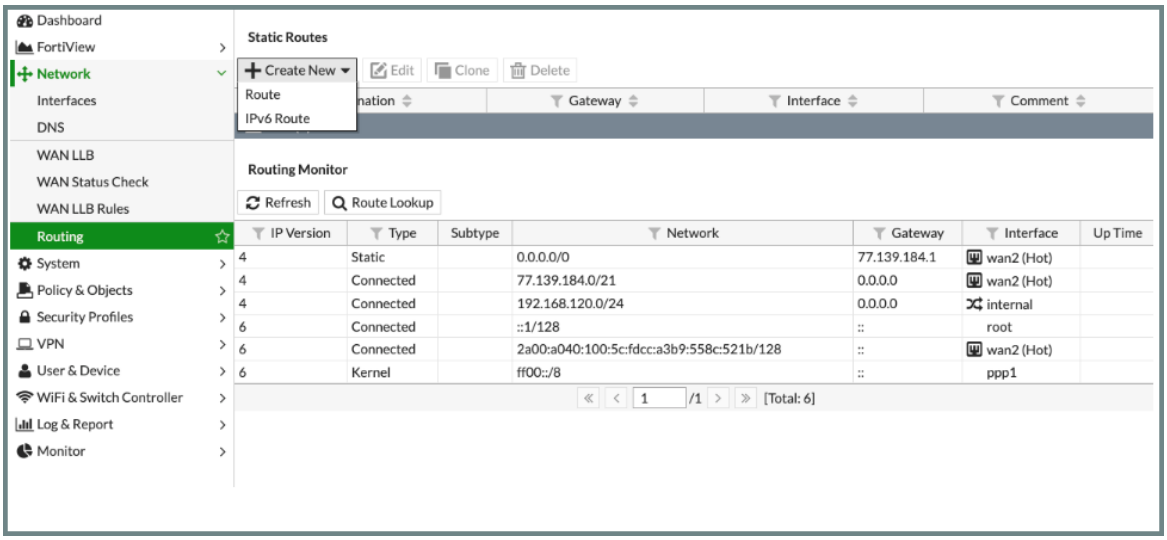
Field	Enter
Encryption	AES256
Authentication	SHA256
Diffie-Hellman Group	21
Key Lifetime (seconds)	28800
Local ID	Blank
XAUTH	Blank

10. In the **Phase 2 Selectors (+Advanced)** section:

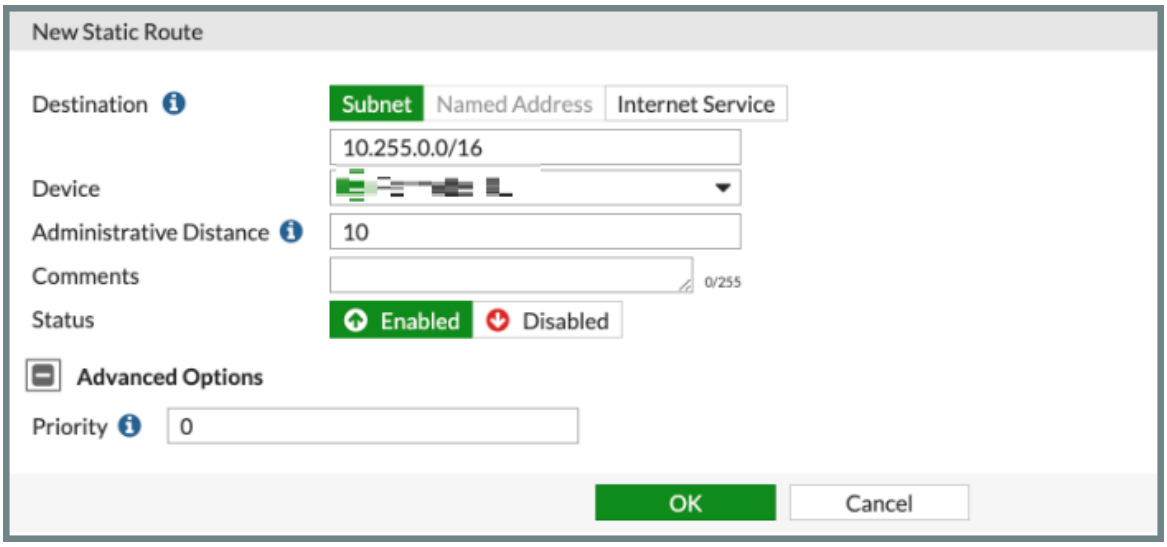
Field	Enter
Name	Harmony SASE
Local Address	Your local network subnet
Remote Address	Harmony SASE network subnet (10.255.0.0/255.255.0.0)
Enable Replay Detection	Select
Enable Perfect Forward Secrecy (PFS)	Select
Diffie-Gellman Group	21
Encryption	AES256
Authentication	SHA256
Local Port	Select
remote Port	Select

Field	Enter
Protocol	Select
Key Lifetime	Seconds
Seconds	3600

11. Add static routes from the Harmony SASE subnet (10.256.0.0/16) to the local network and vice versa through the VPN tunnel gateway:
    a. Click **Network > Routing**.
    b. Click **Create new** and select **Route**.
    c. In the **Destination** field, enter 10.255.0.0/16.
    d. From the **Device** list, select **Harmony SASE**.
    e. Click **OK**.
12. Add firewall rules to allow traffic from the Harmony SASE subnet (10.255.0.0/16) to your local network or services:
    a. Go to **Policy & Objects > IPv4 Policy**.



b. Click **Create New** and enter these:



Field	Enter
Name	Harmony SASE
Incoming Interface	Harmony SASE
Outgoing Interface	Your local network object.
Source	All
Destination	All
Schedule	Always
Service	All
NAT	Disabled

Leave the rest of the fields to default settings.

c. Click **OK**.

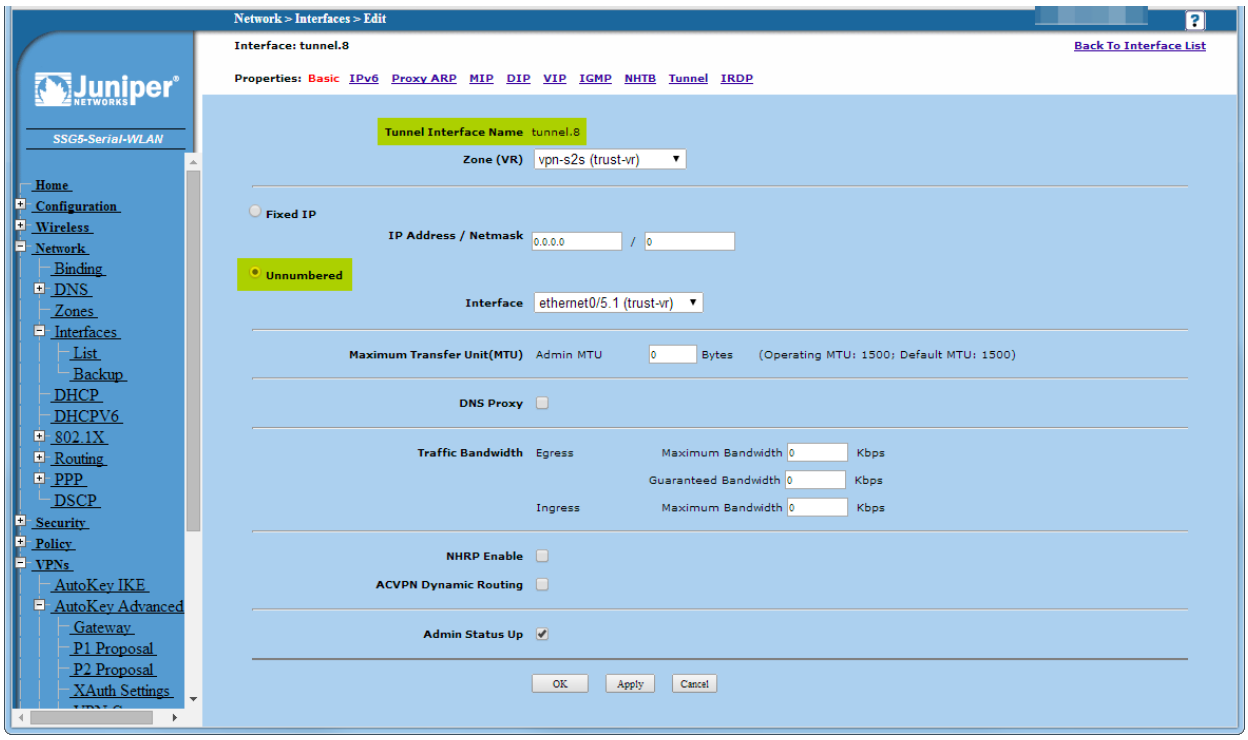
13. To verify that the tunnel is up, go to **VPN > IPSec Tunnels**. If the tunnel is listed in the table, then the tunnel is up.

Juniper Networks ScreenOS Firewall

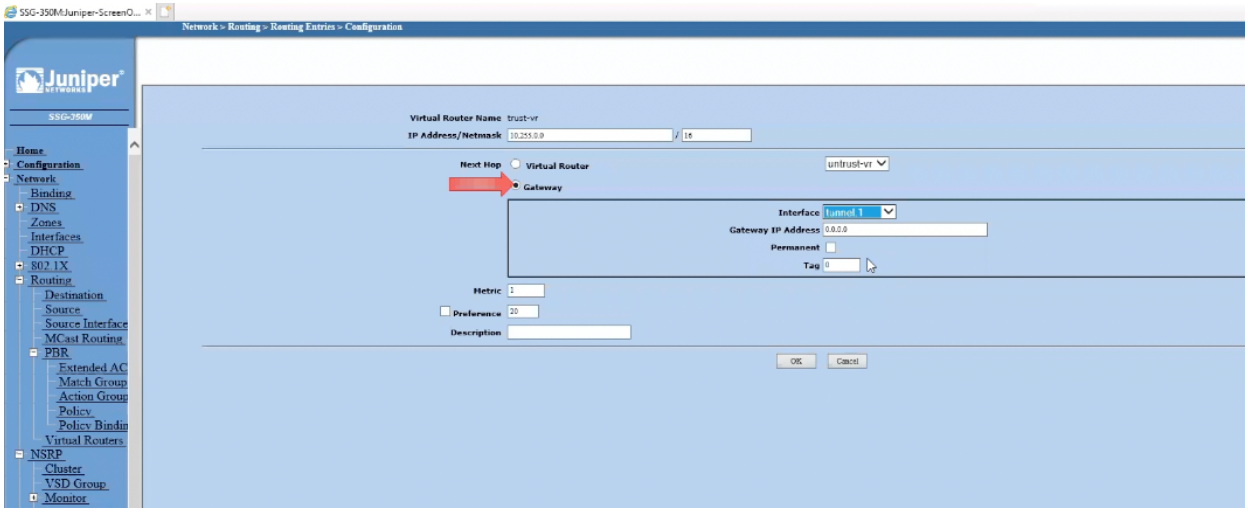
To configure the tunnel in the Juniper Networks ScreenOS Management Portal:

1. Log in to the Juniper Networks ScreenOS Management Portal with the Administrator account.

2. From the left pane. go to **Network > Interfaces**.
3. Create a new **Unnumbered** tunnel interface.



4. From the left pane, go to **Network > Routing > Source**:

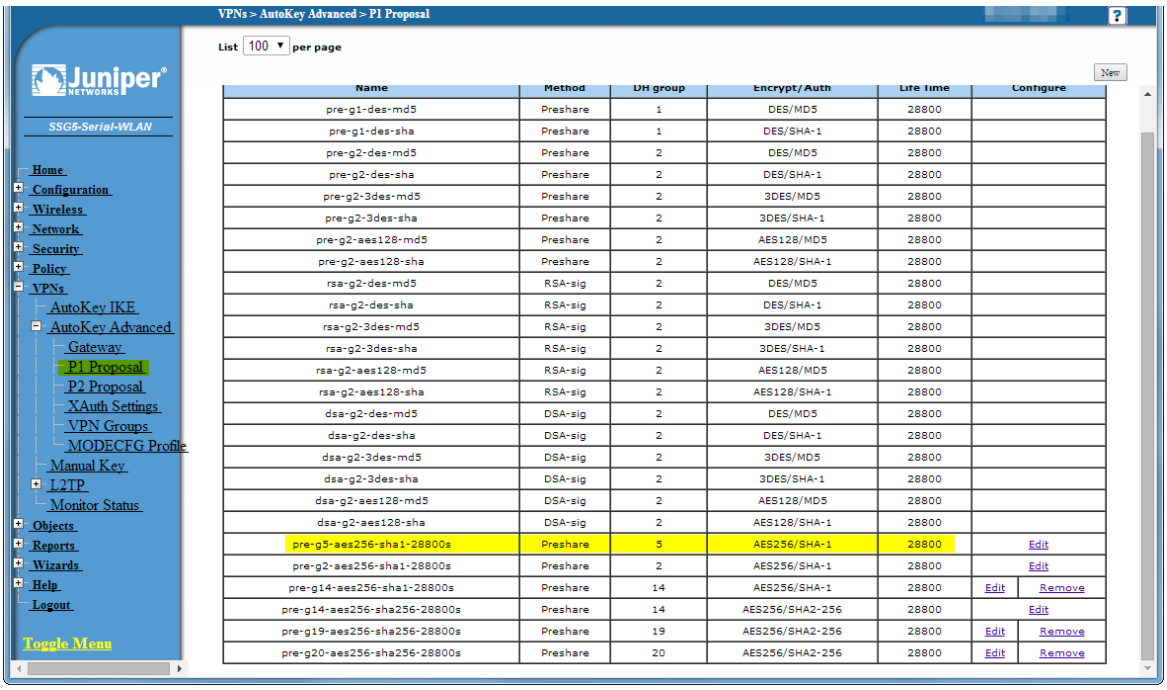


   a. Select an appropriate zone and click **New**.
   b. In the **IP Address/Netmask** field, enter the Harmony SASE network subnet.
   c. For **Next Hop**, select **gateway**.
   d. Click **OK**.

5. From the left pane, click **VPN**:

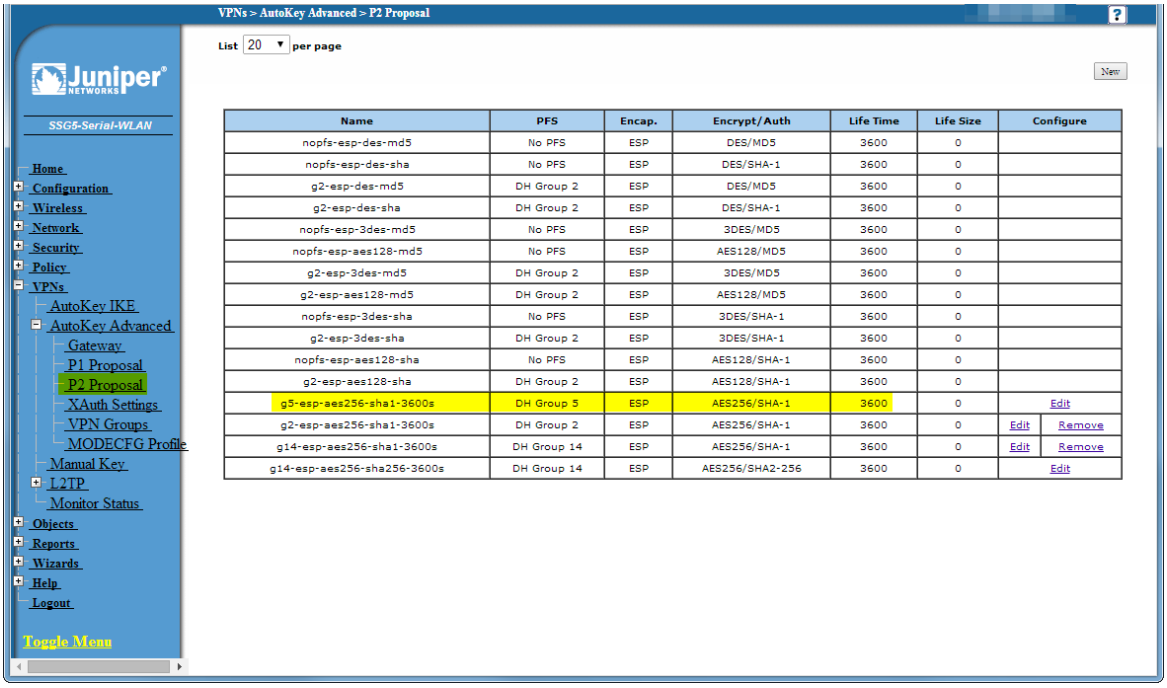
a. Select **AutoKey Advanced**.

b. Verify that the **PI Proposal** is listed as shown in the following graphic.



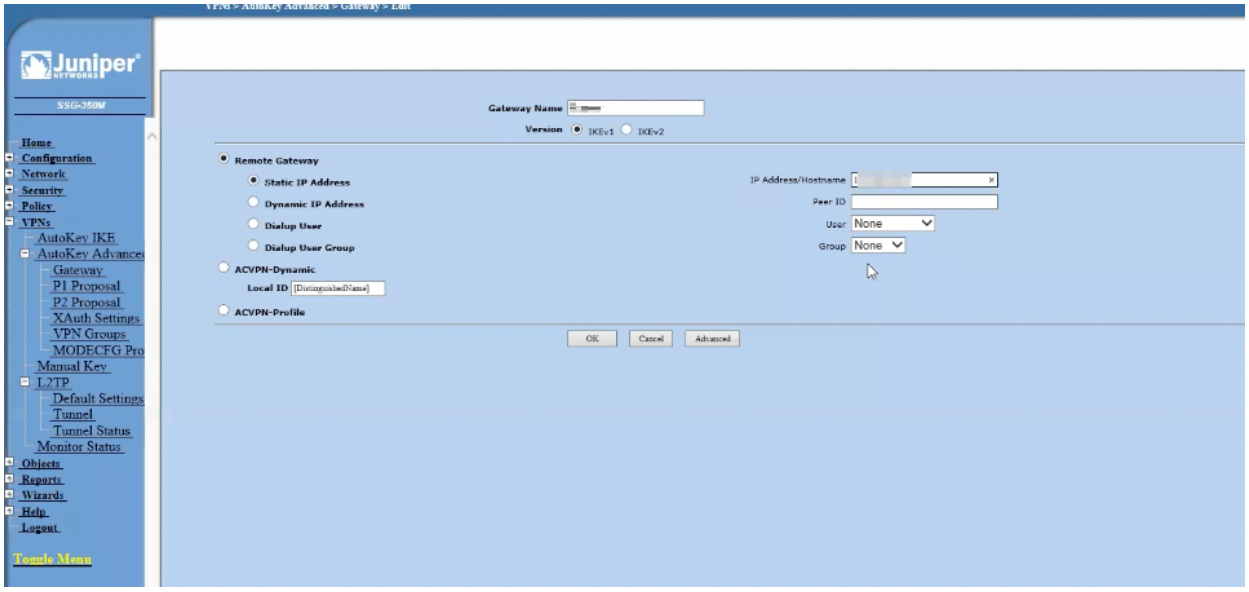
Name	Method	DH group	Encrypt/Auth	Life Time	Configure	
pre-g1-des-md5	Preshare	1	DES/MD5	28800		
pre-g1-des-sha	Preshare	1	DES/SHA-1	28800		
pre-g2-des-md5	Preshare	2	DES/MD5	28800		
pre-g2-des-sha	Preshare	2	DES/SHA-1	28800		
pre-g2-3des-md5	Preshare	2	3DES/MD5	28800		
pre-g2-3des-sha	Preshare	2	3DES/SHA-1	28800		
pre-g2-aes128-md5	Preshare	2	AES128/MD5	28800		
pre-g2-aes128-sha	Preshare	2	AES128/SHA-1	28800		
rsa-g2-des-md5	RSA-sig	2	DES/MD5	28800		
rsa-g2-des-sha	RSA-sig	2	DES/SHA-1	28800		
rsa-g2-3des-md5	RSA-sig	2	3DES/MD5	28800		
rsa-g2-3des-sha	RSA-sig	2	3DES/SHA-1	28800		
rsa-g2-aes128-md5	RSA-sig	2	AES128/MD5	28800		
rsa-g2-aes128-sha	RSA-sig	2	AES128/SHA-1	28800		
dsa-g2-des-md5	DSA-sig	2	DES/MD5	28800		
dsa-g2-des-sha	DSA-sig	2	DES/SHA-1	28800		
dsa-g2-3des-md5	DSA-sig	2	3DES/MD5	28800		
dsa-g2-3des-sha	DSA-sig	2	3DES/SHA-1	28800		
dsa-g2-aes128-md5	DSA-sig	2	AES128/MD5	28800		
dsa-g2-aes128-sha	DSA-sig	2	AES128/SHA-1	28800		
pre-g5-aes256-sha1-28800s	Preshare	5	AES256/SHA-1	28800	Edit	
pre-g2-aes256-sha1-28800s	Preshare	2	AES256/SHA-1	28800	Edit	
pre-g14-aes256-sha1-28800s	Preshare	14	AES256/SHA-1	28800	Edit	Remove
pre-g14-aes256-sha256-28800s	Preshare	14	AES256/SHA2-256	28800	Edit	
pre-g19-aes256-sha256-28800s	Preshare	19	AES256/SHA2-256	28800	Edit	Remove
pre-g20-aes256-sha256-28800s	Preshare	20	AES256/SHA2-256	28800	Edit	Remove

c. Go to **P2 Proposal** and ensure the proposal is listed as shown in the following graphic.



Name	PFS	Encap.	Encrypt/Auth	Life Time	Life Size	Configure	
nopfs-esp-des-md5	No PFS	ESP	DES/MD5	3600	0		
nopfs-esp-des-sha	No PFS	ESP	DES/SHA-1	3600	0		
g2-esp-des-md5	DH Group 2	ESP	DES/MD5	3600	0		
g2-esp-des-sha	DH Group 2	ESP	DES/SHA-1	3600	0		
nopfs-esp-3des-md5	No PFS	ESP	3DES/MD5	3600	0		
nopfs-esp-aes128-md5	No PFS	ESP	AES128/MD5	3600	0		
g2-esp-3des-md5	DH Group 2	ESP	3DES/MD5	3600	0		
g2-esp-aes128-md5	DH Group 2	ESP	AES128/MD5	3600	0		
nopfs-esp-3des-sha	No PFS	ESP	3DES/SHA-1	3600	0		
g2-esp-3des-sha	DH Group 2	ESP	3DES/SHA-1	3600	0		
nopfs-esp-aes128-sha	No PFS	ESP	AES128/SHA-1	3600	0		
g2-esp-aes128-sha	DH Group 2	ESP	AES128/SHA-1	3600	0		
g5-esp-aes256-sha1-3600s	DH Group 5	ESP	AES256/SHA-1	3600	0	Edit	
g2-esp-aes256-sha1-3600s	DH Group 2	ESP	AES256/SHA-1	3600	0	Edit	Remove
g14-esp-aes256-sha1-3600s	DH Group 14	ESP	AES256/SHA-1	3600	0	Edit	Remove
g14-esp-aes256-sha256-3600s	DH Group 14	ESP	AES256/SHA2-256	3600	0	Edit	

6. From the left pane, click **Gateway**:

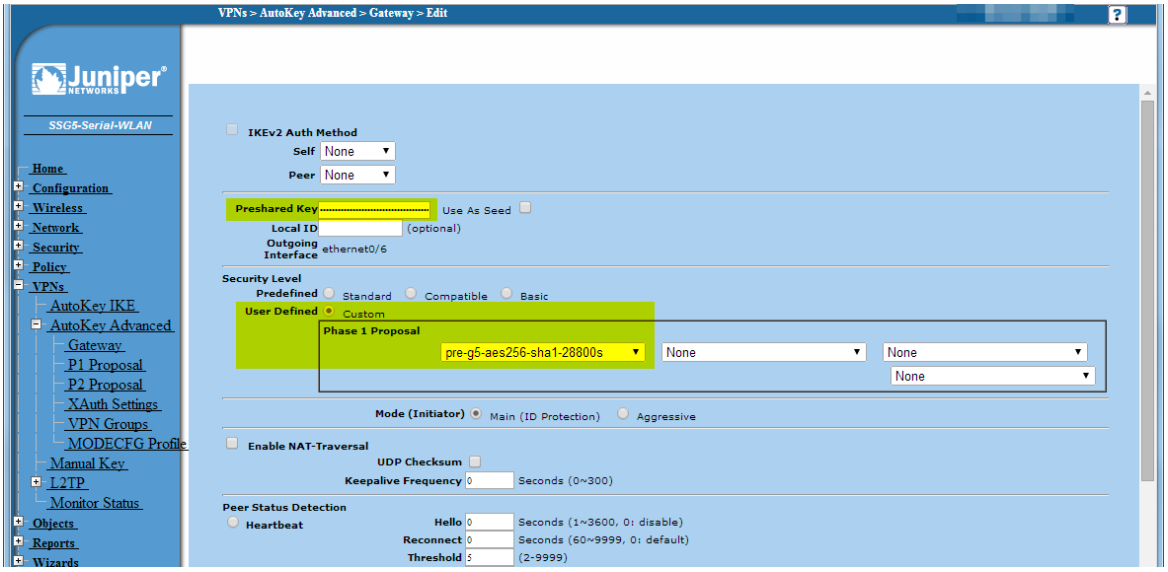


a. In the **Gateway Name** field, enter a name for the gateway.

b. Select **Remote Gateway** and then select **Static IP Address**.

c. In the **IP Address/Hostname** field, enter the public IP address of Harmony SASE gateway.

d. Click **Advanced**:

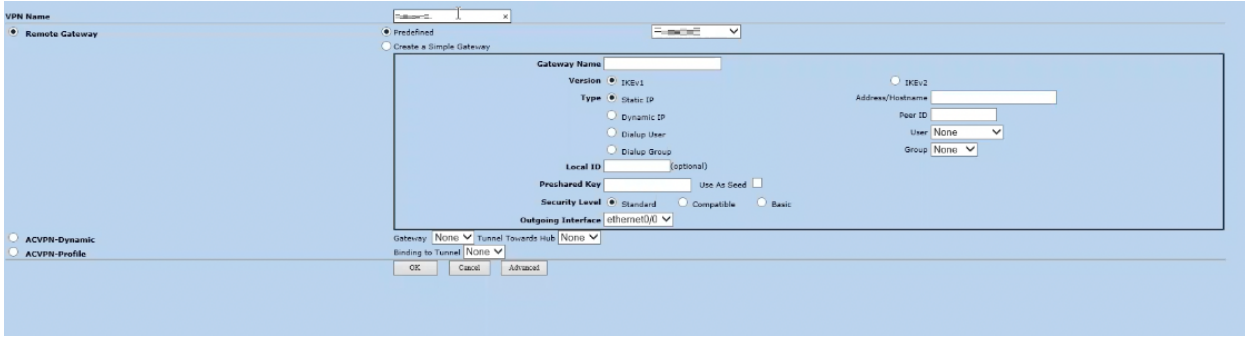


i. In the **Preshared Key** field, enter the secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

ii. In the **Security Level** section, select **Custom** and from the **Phase 1 Proposal** list, select **pre-g5-aes256-sha1-28800s**.

iii. Enable **DPD** and set **DPD Interval** to **10s** and **DPD Retry** to **5s**.

7. From the left pane, click **VPN > Autokey IKE**:

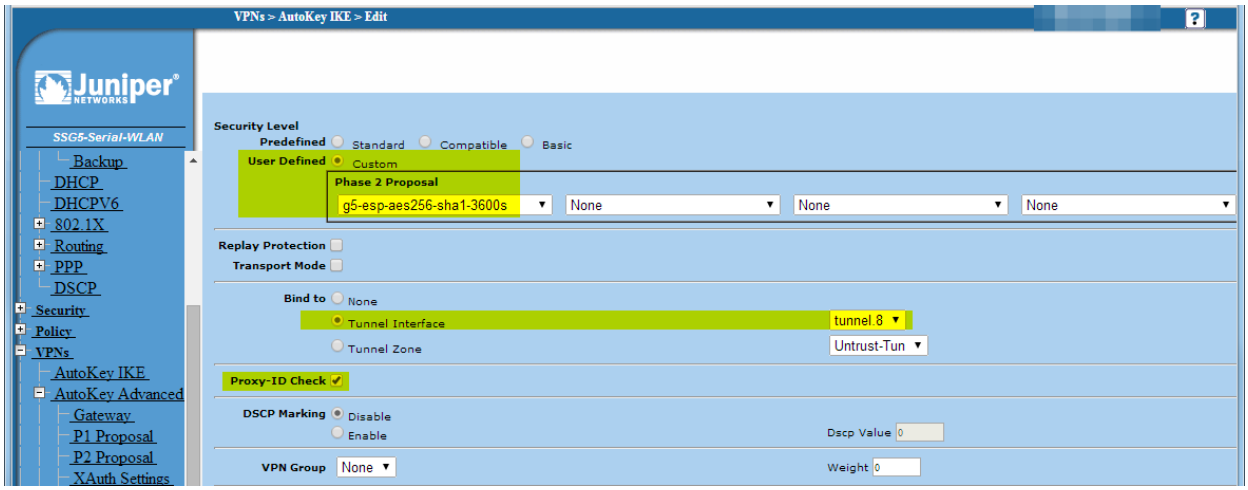


a. In the **VPN Name** field, enter a name for the VPN. For example, Harmony SASE.

b. Select **Remote Gateway** and then select **Predefined**.

c. Select the AutoKey Advanced Gateway that you created in the previous step.

8. From the left pane, click **VPN > Advanced**:

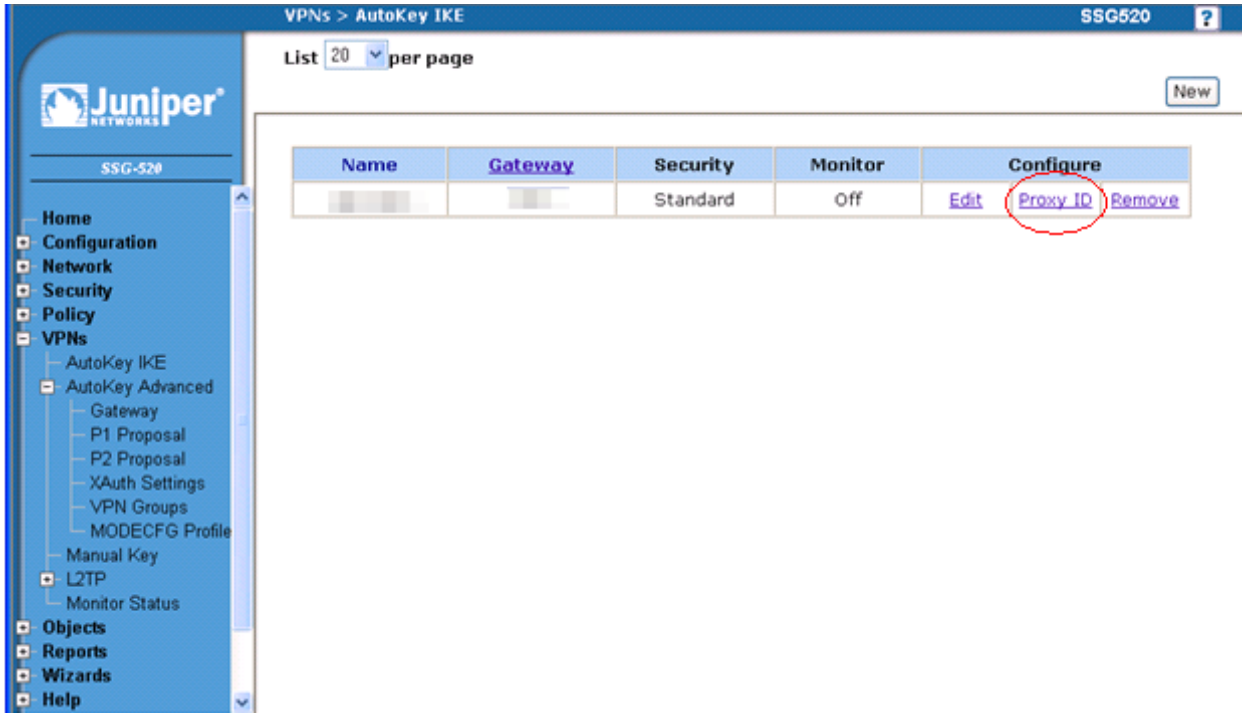


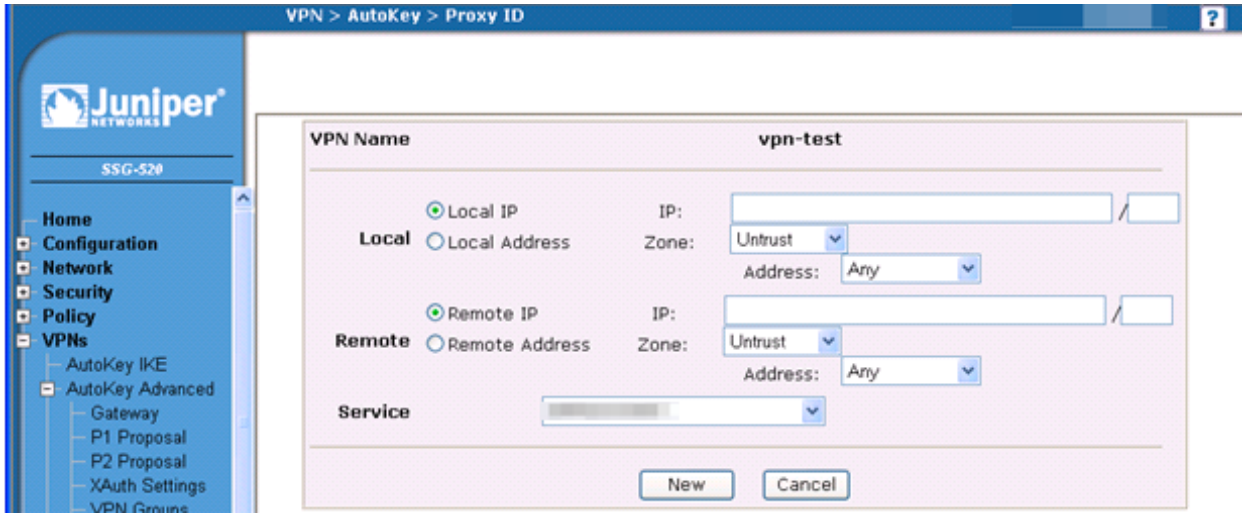
a. In the **Security Level** section, select **Custom** and from the **Phase 2 Proposal** list, select **g5-aes256-sha1-3600s**.

b. In the **Bind to** section, click **Tunnel Interface** and select the tunnel interface you created in step 3.

c. Select the **Proxy-ID Check** checkbox.

9. From the left pane, click **VPN > Autokey IKE**, configure **Proxy ID** with these details:





Field	Enter
Local proxy ID	Your local LAN subnet. For example, 192.168.120.0/24.
Remote Proxy ID	Harmony SASE network subnet. The default is 10.255.0.0./16.
Service	Any

Juniper (JunOS) SRX Firewall

To configure the tunnel with Juniper SRX firewall through CLI:

Note - To configure the tunnel in the Juniper SRX Management Portal, see Juniper VPN configuration generator.

1. Connect to the firewall through SSH. For example, using PuTTY.
2. Create a tunnel interface. Run:

   Note - Do not assign an IP address but make sure it's enabled for layer 3 communication.

   ```
   set interfaces st0 unit 0 family inet
   ```

3. Set up the IKE Proposal. Run:

   ```
   set security ike proposal QS description Perimeter81-SRXTunnel

   set security ike proposal QS authentication-method pre-shared-
   keys

   set security ike proposal QS dh-group group14

   set security ike proposal QS authentication-algorithm sha-256

   set security ike proposal QS encryption-algorithm aes-256-cbc

   set security ike proposal QS lifetime-seconds 28800
   ```

4. Set up the IKE policy configuration. Run:

   ```
   set security ike policy QS-policy proposals p81

   set security ike policy QS-policy pre-shared-key ascii-text
   <Secret_key_from_Quantum SASE Administrator Portal>
   ```

5. Set up the IKE gateway configuration. Run:

   ```
   set security ike gateway QS-ike-gateway ike-policy QS-policy
   ```

```
set security ike gateway QS-ike-gateway address <Public IP
address of Quantum SASE gatewy>

set security ike gateway QS-ike-gateway local-identity inet
<Locak IP address of the firewall>

set security ike gateway QS-ike-gateway external-interface ge-
0/0/0

set security ike gateway QS-ike-gateway version v1-only
```

6. Set up the IPSec proposal. Run:

```
set security ipsec proposal QS-proposal description Perimeter81

set security ipsec proposal QS-proposal protocol esp

set security ipsec proposal QS-proposal authentication-algorithm
hmac-sha-256-128

set security ipsec proposal QS-proposal encryption-algorithm aes-
256-cbc

set security ipsec proposal QS-proposal lifetime-seconds 3600
```

7. Set up the IPSec policy configuration. Run:

```
set security ipsec policy ipsec-QS-policy perfect-forward-secrecy
keys group14

set security ipsec policy ipsec-QS-policy proposals QS-proposal
```

8. Bind your tunnel interface and apply the configuration. Run:

```
set security ipsec vpn QS-ipsec bind-interface st0.0

set security ipsec vpn QS-ipsec ike gateway p81-ike-gateway

set security ipsec vpn QS-ipsec ike ipsec-policy ipsec-p81-policy
```

```
set security ipsec vpn QS-ipsec establish-tunnels on-traffic
immediately

set security address-book global address QS_internal
10.255.0.0/16
```

Note - To establish the tunnel only upon active traffic or set the firewall to the only to respond when the traffic is initiated from Harmony SASE (never initiate a tunnel), set firewall to the **Responder-Only** mode.

9. Set firewall security policies. Run:

Note - If the tunnel interface is in a trusted zone or a zone that allows all the traffic, then skip this step. Otherwise, modify the parameters in the following commands according to your network topology.
In the following example, all the traffic from **icmp** and **ssh** from zone **vpn** with a source address of 10.255.0.0/16 to any address in zone **trust** is allowed.

```
set security policies from-zone vpn to-zone trust policy vpn-
internal match source-address QS_internal

set security policies from-zone vpn to-zone trust policy vpn-
internal match destination-address any

set security policies from-zone vpn to-zone trust policy vpn-
internal match application junos-icmp-all

set security policies from-zone vpn to-zone trust policy vpn-
internal match application junos-ssh

set security policies from-zone vpn to-zone trust policy vpn-
internal then permit
```

10. Set host inbound services. Allow services to the firewall interfaces and your public facing interface. Run:

```
set security zones security-zone vpn interfaces st0.0 host-
inbound-traffic system-services ike

set security zones security-zone untrust interfaces ge-0/0/0.0
host-inbound-traffic system-services ike
```

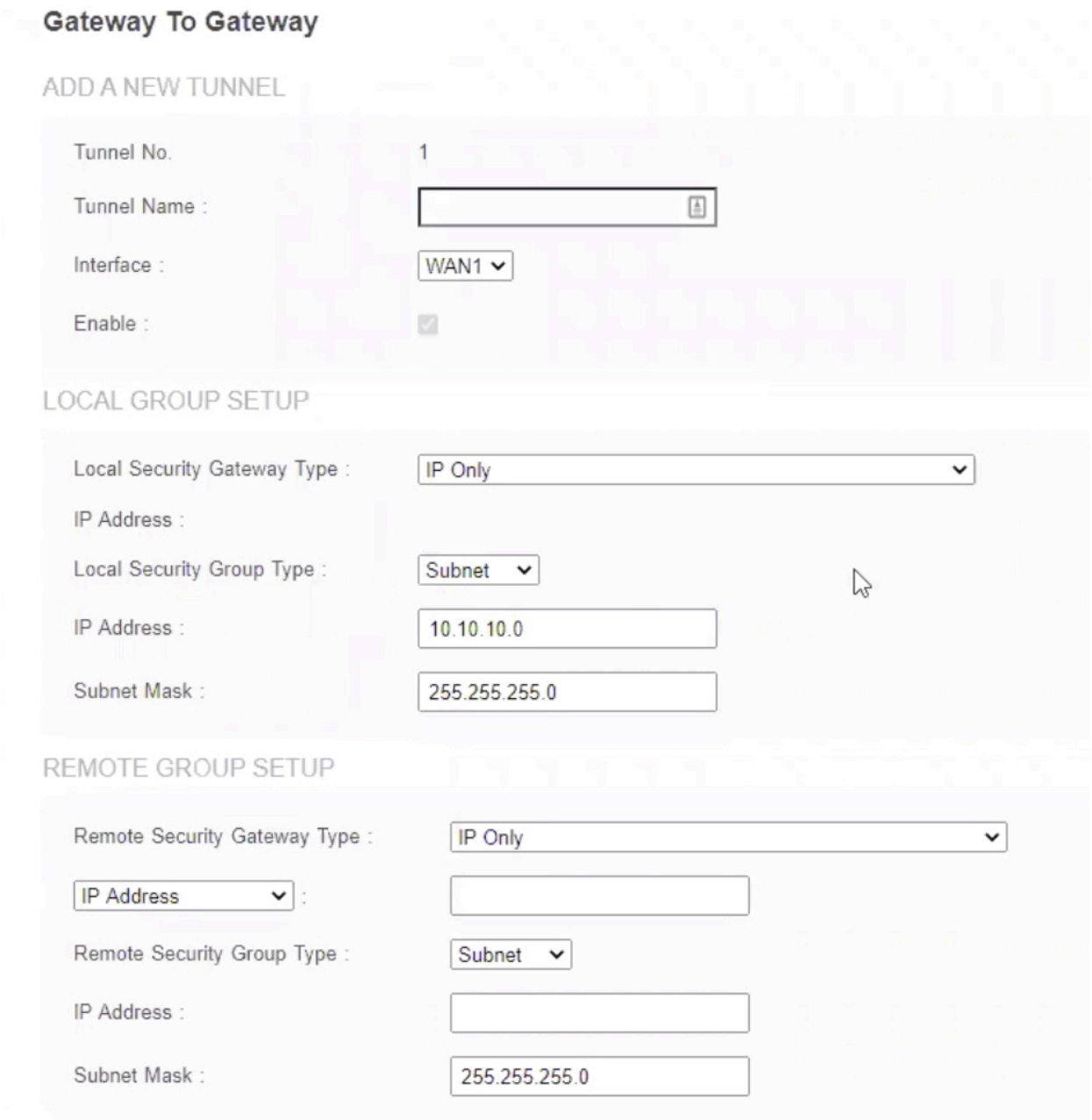
11. Define a static route to Harmony SASE network. Run:

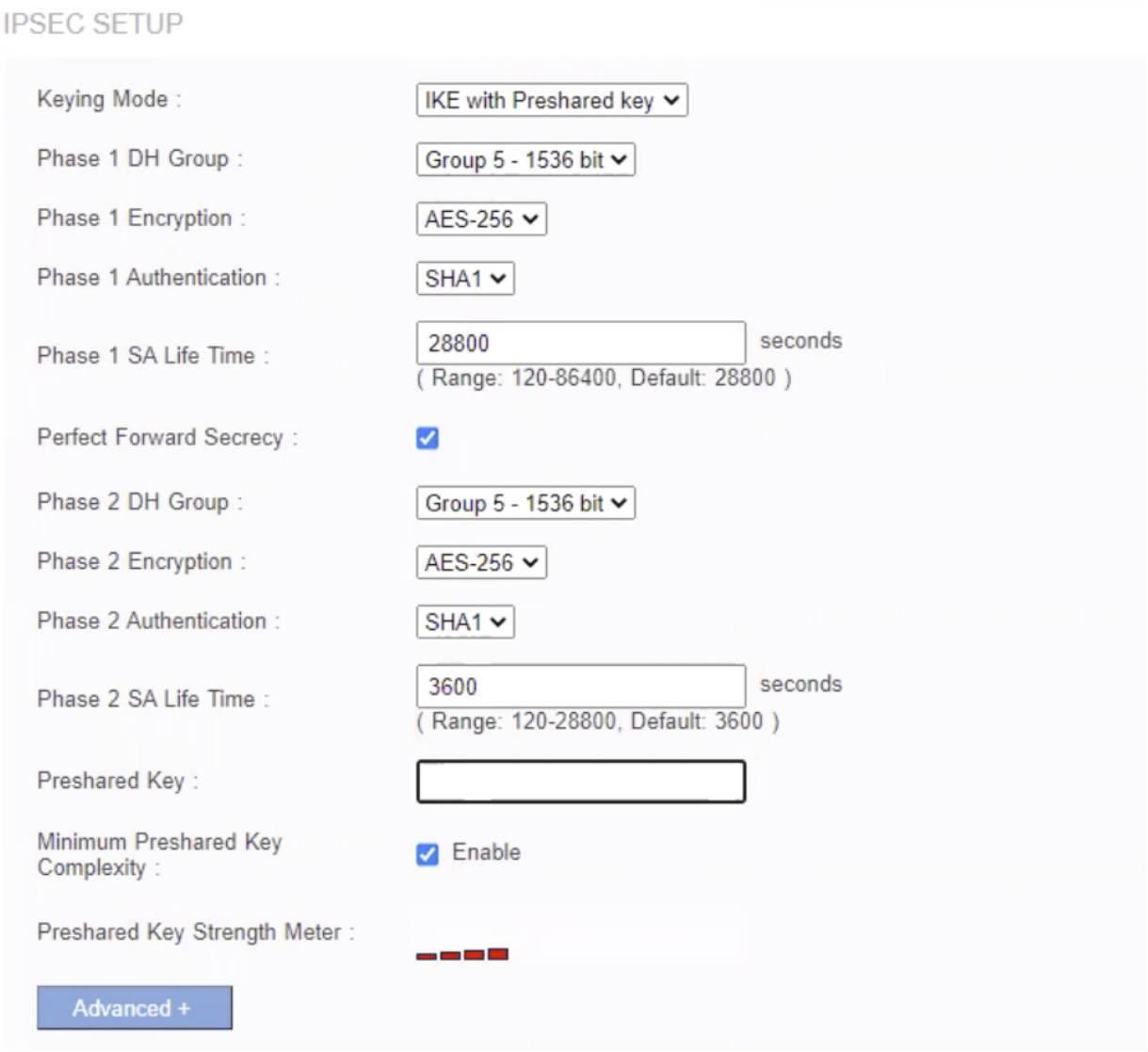
```
set routing-options static route 10.255.0.0/16 next-hop st0.0
```

Linksys Router

To configure the tunnel in the Linksys Management Portal:

1. Log in to the Linksys Management Portal with the Administrator account.
2. From the left panel, go to **VPN > Gateway to Gateway**.



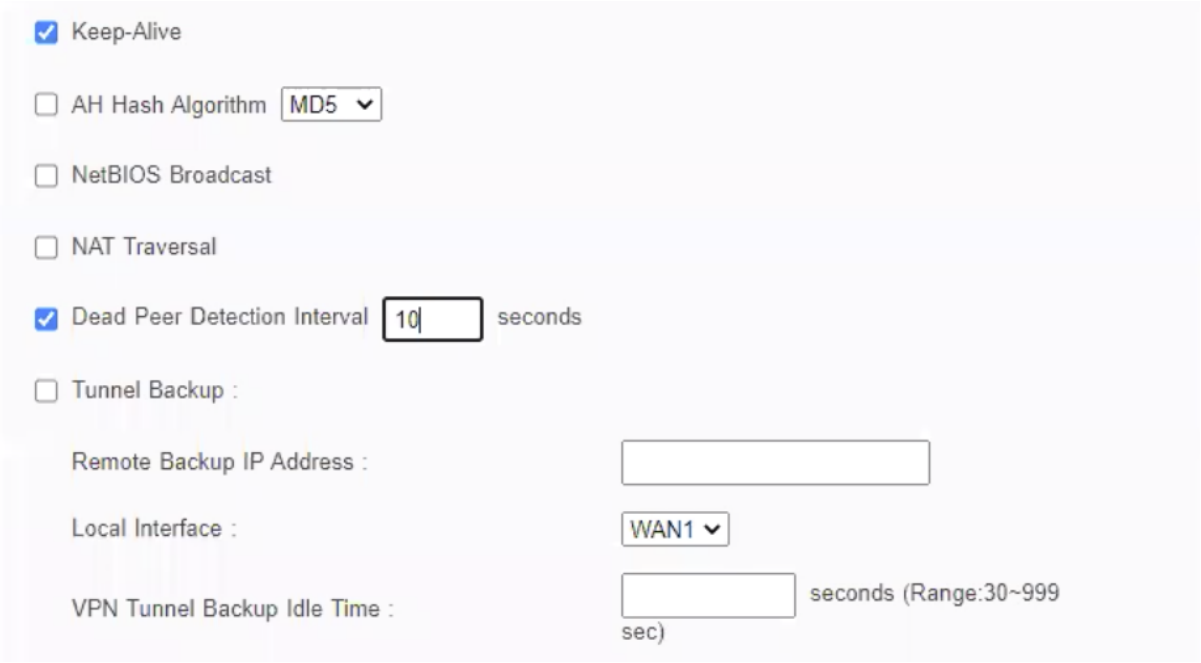


3. Enter these:

Field	Enter
Add a New Tunnel	
Tunnel Name	Name for the tunnel.
Interface	WAN1
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	Linksys external IP address.

Field	Enter
Local Security Group Type	Subnet
IP Address	Linksys local IP address.
Subnet Mask	Linksys subnet mask.
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	Public IP address of Harmony SASE gateway.
Remote Security group Type	Subnet
IP Address	10.255.0.0
Subnet Mask	255.255.0.0
IPSec Setup	
Keying Mode	IKE with PSK
Phase 1 DHG	Group 5
Phase 1 Encryption	aes256
Phase 1 Authentication	sha1
Phase 1 SA Lifetime	28800
Perfect Forward Secrecy	Selected
Phase 2 DHG	Group 5
Phase 1 Encryption	aes256
Phase 2 Authentication	sha1
Phase 2 SA Lifetime	3600
Preshared Key	Secret key specified in the Harmony SASE Administrator Portal.

4. Click **Advanced**:



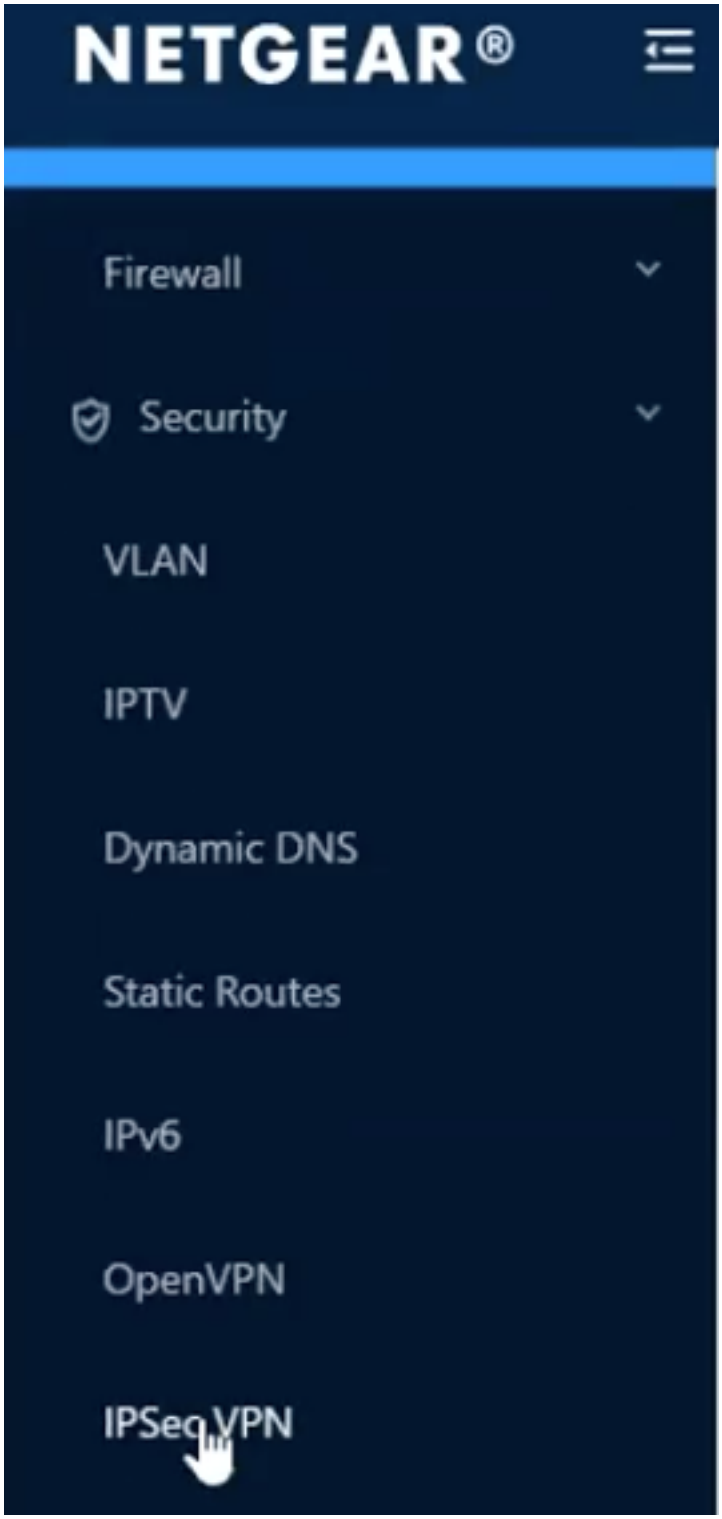
a. Select the **Keep-Alive** checkbox.

b. Select the **Dead Peer Detection Interval** checkbox and enter **10** seconds.

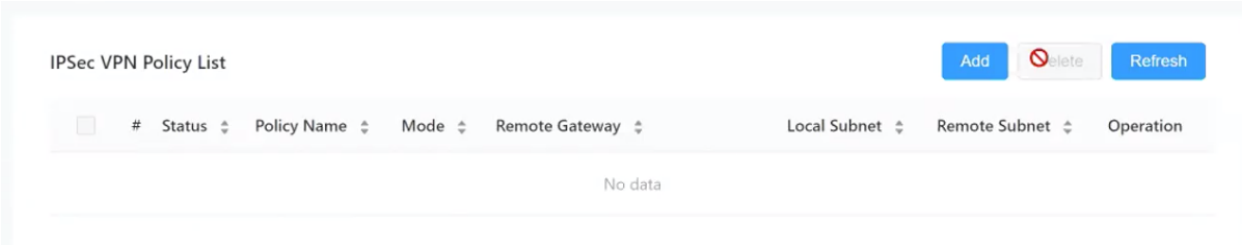
Netgear BR500 Router

To configure the tunnel in the Netgear BR500 Management Portal:

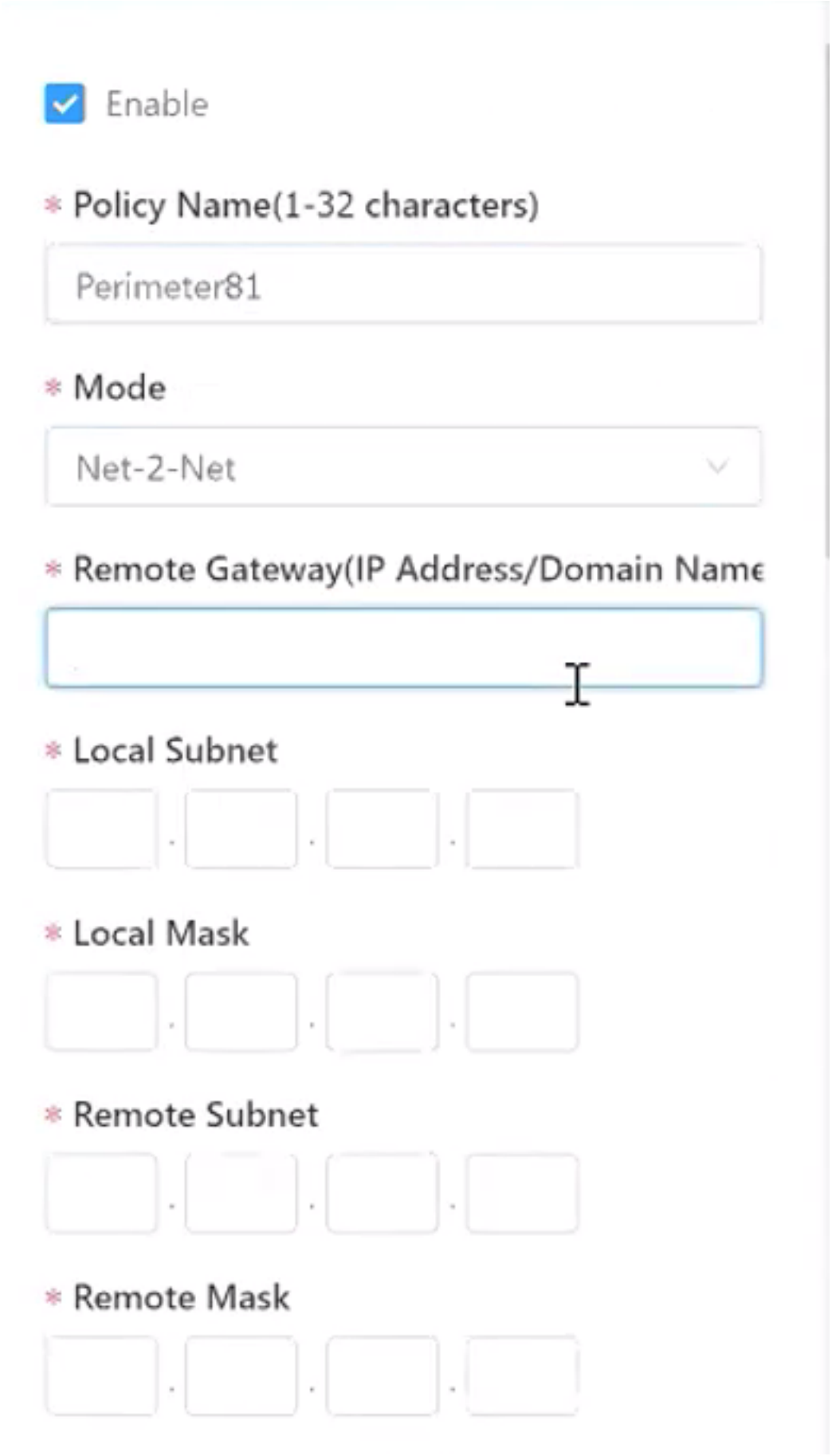
1. Log in to the Netgear BR500 Management Portal with the Administrator account.
2. From the left panel, go to **Security > IPSec VPN**.

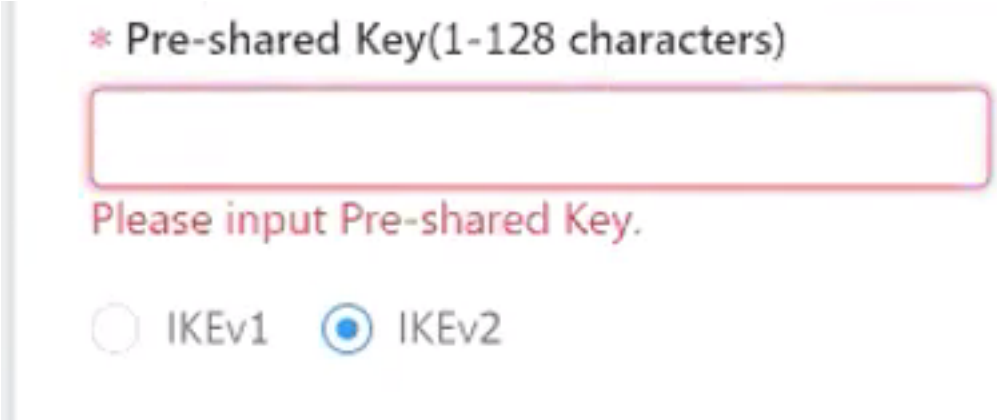

NETGEAR®
Firewall
Security
VLAN
IPTV
Dynamic DNS
Static Routes
IPv6
OpenVPN
IPSec VPN

3. Click **Add**.



4. Enter these:


Enable
* Policy Name(1-32 characters)
Perimeter81
* Mode
Net-2-Net
* Remote Gateway(IP Address/Domain Name
* Local Subnet
* Local Mask
* Remote Subnet
* Remote Mask



Field	Enter
Policy Name	Name for the policy.
Mode	Net-2-Net
Remote Gateway IP	Public IP address of the Harmony SASE gateway.
Local Subnet and Local Mask	You LAN subnet and subnet mask.
Remote Subnet	Harmony SASE network subnets. Default is 10.255.0.0/16.
Remote Mask	255.255.0.0
Pre-shared Key (1-128 characters)	Secret key specified in the Harmony SASEAdministrator Portal and **IKEv2**.

5. In the **Advanced Settings** section:

Advanced Settings

Phase-1 Settings

Proposal	sha1-aes256-dh5
Proposal	---
Proposal	---
Proposal	---

Exchange Mode

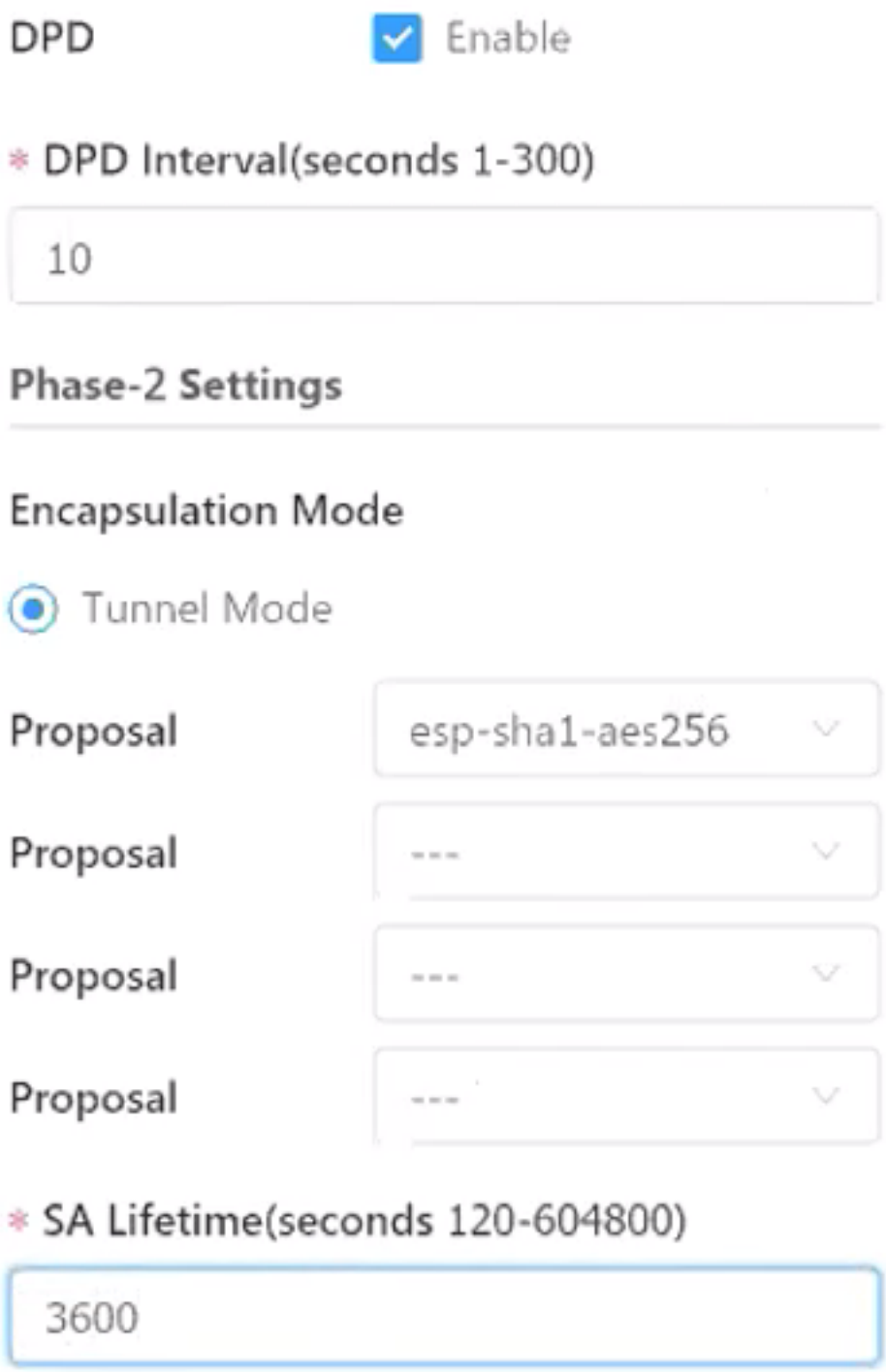
(•) Main Mode

Negotiation Mode

(•) Initiator Mode ( ) Responder Mode

* **SA Lifetime(seconds 60-604800)**

28800



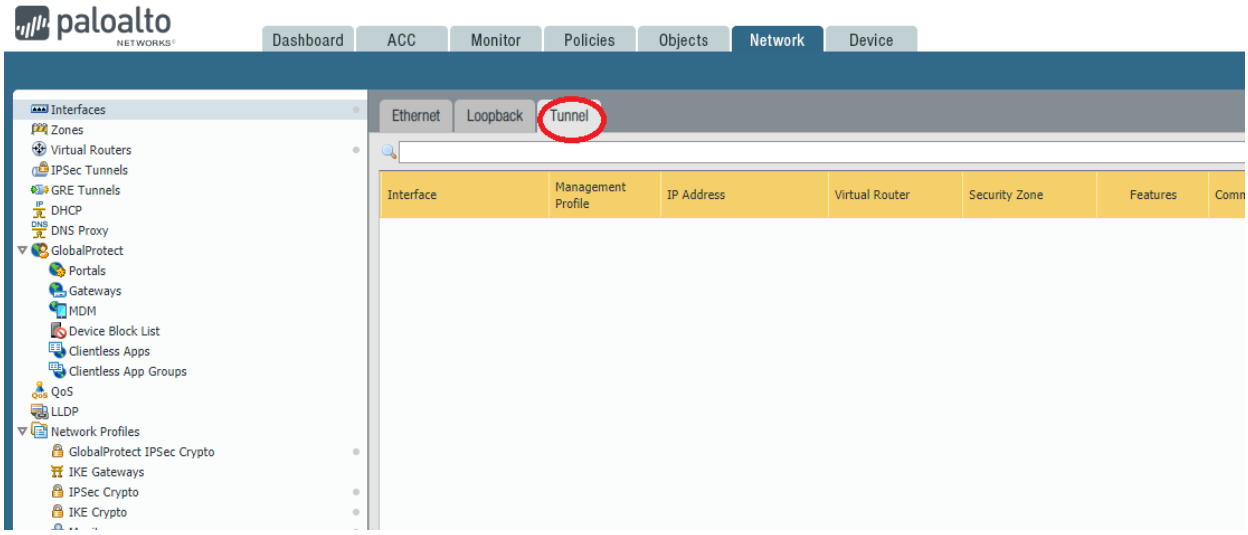
Field	Enter
Phase 1 Proposal	sha1-aes256-dh5
Exchange Mode	Main Mode
Negotiation Mode	Initiator Mode

Field	Enter
Phase I SA Lifetime seconds	28800
DPD	Enable
DPD Interval	10 seconds
Phase II Encapsulation Mode	Tunnel Mode
Phase II SA Lifetime seconds	3600

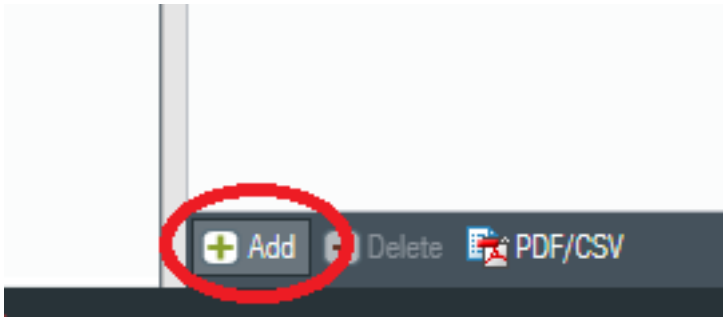
Palo Alto Firewall

To configure the tunnel in the Palo Alto Management Portal:

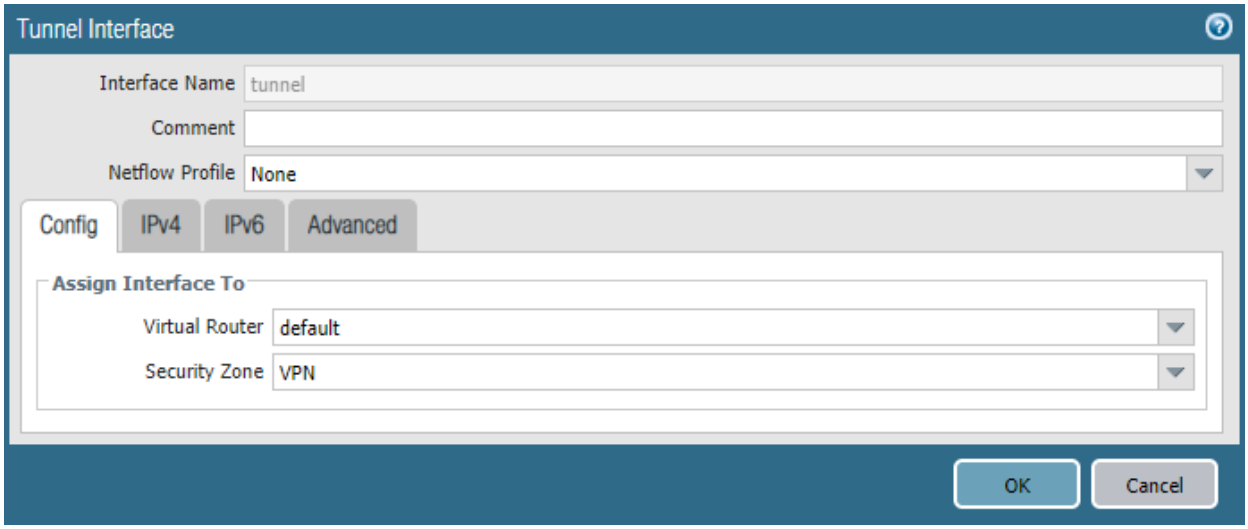
1. Log in to the Palo Alto Management Portal with the Administrator account.
2. Go to **Interfaces** and click the **Tunnel** tab.



3. Click **Add**.



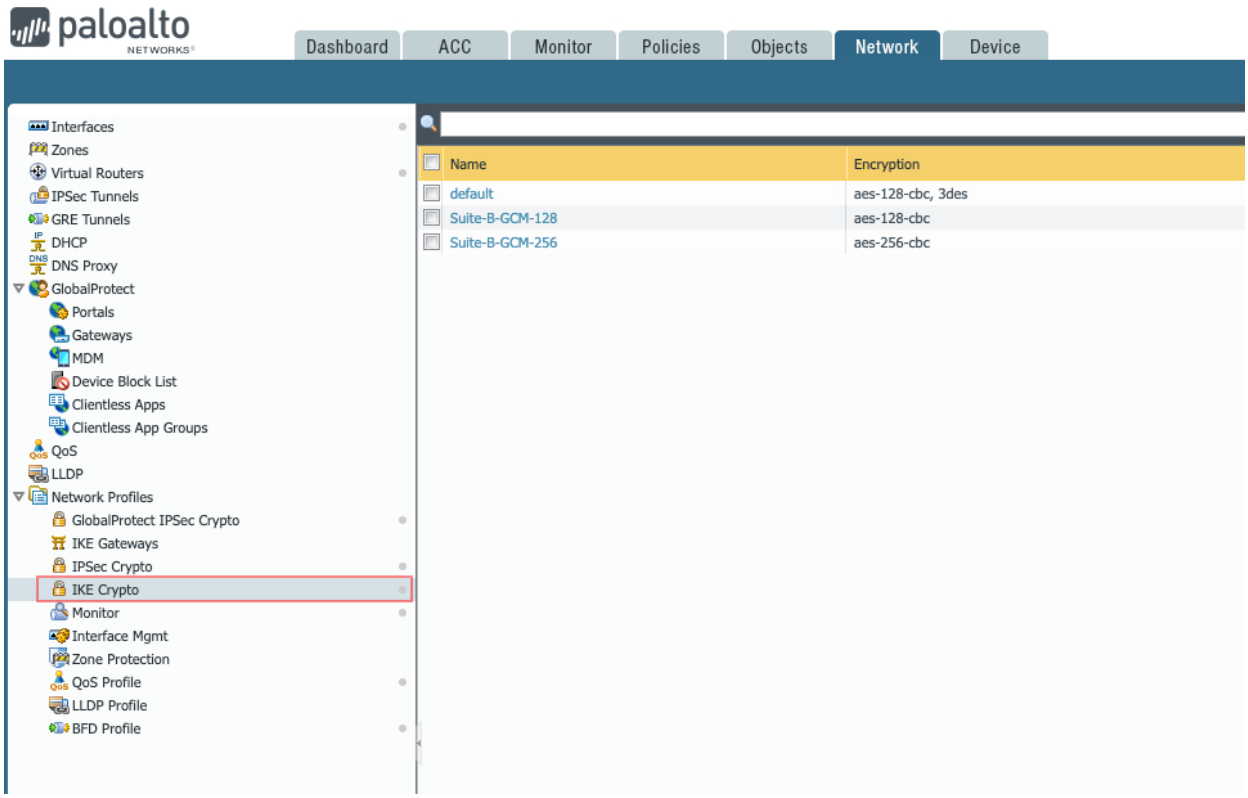
The **Tunnel Interface** window appears.



4. From the **Virtual Router** list, select the virtual router for the tunnel interface.
5. From the **Security Zone** list, select a zone for the tunnel interface

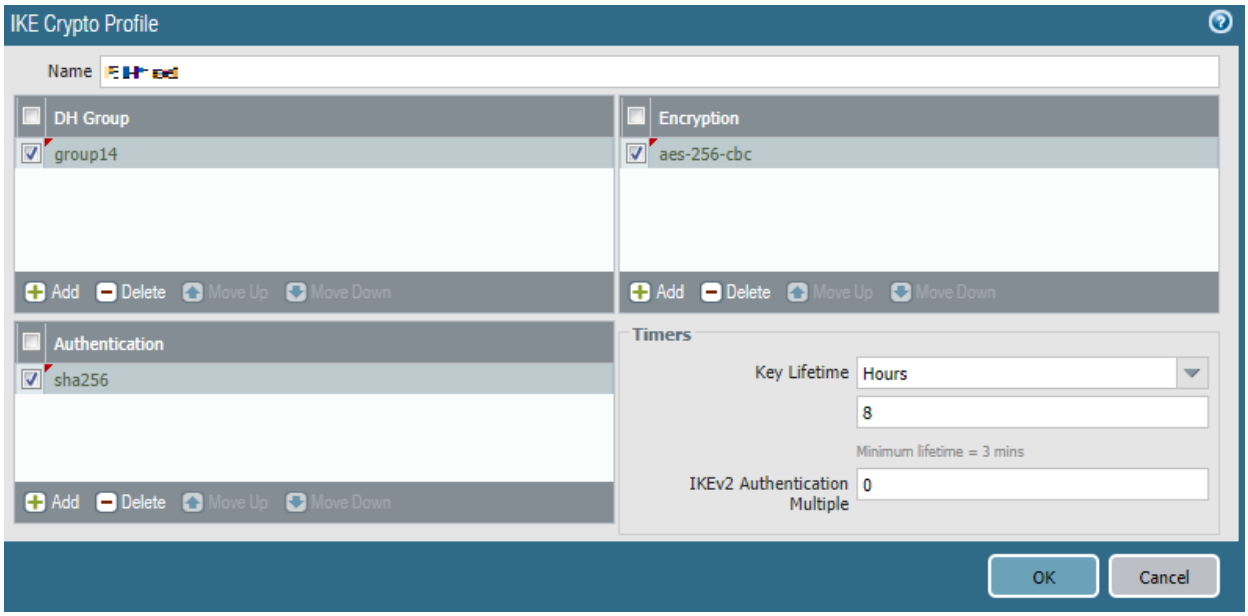
   Note - Configure a new zone for the tunnel interface for granular control of traffic ingress and egress through the tunnel. If the tunnel interface zone is different from the zone where the traffic originates or departs, then configure a policy to allow the traffic from the source zone to the tunnel interface zone.

6. Click **OK**.
7. Go to **Network Profiles > IKE Crypto**.



8. In the **Networks** tab, click **Add**.

The **IKE Crypto Profile** window appears.

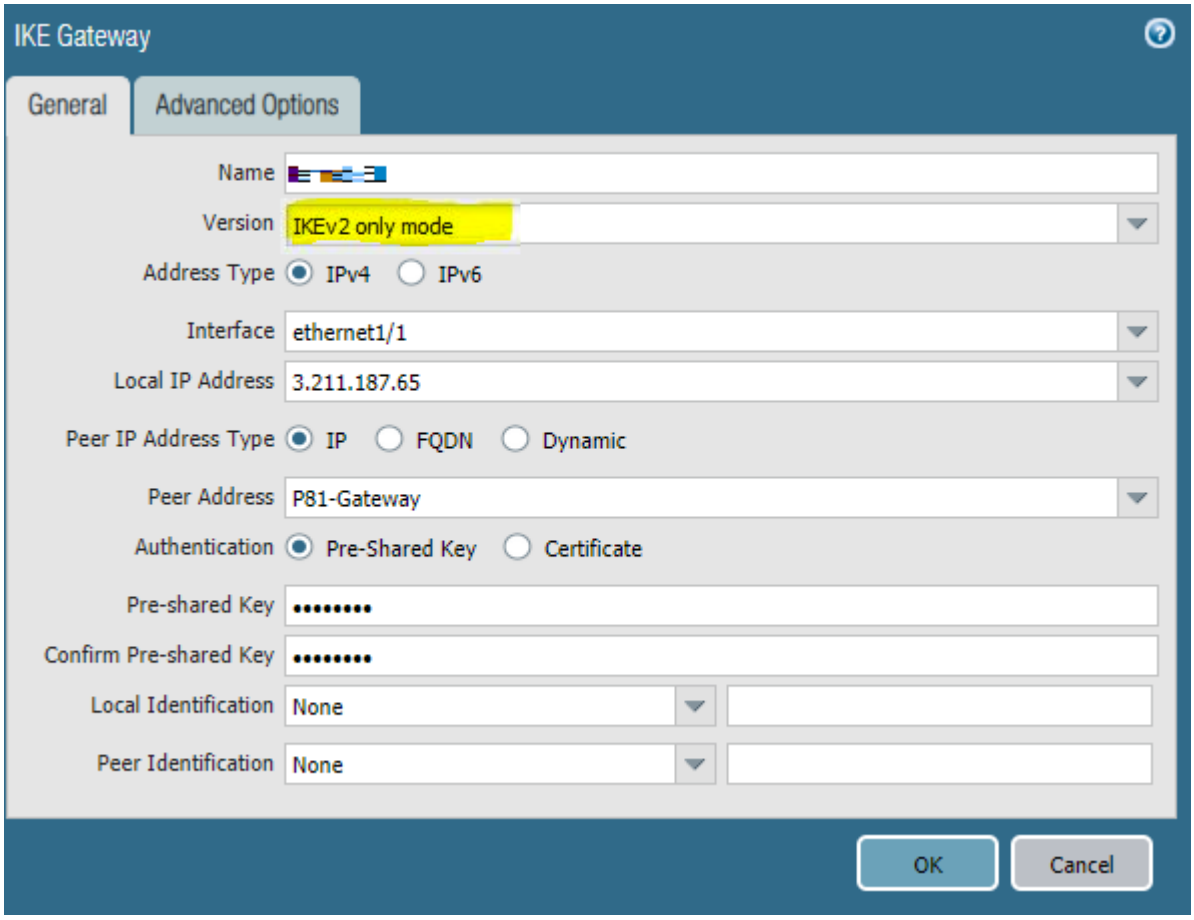


9. Enter these:

Field	Enter
Name	Name for the profile.
DH Group	14
Encryption	aes-256-cbc
Authentication	sha256
Key Lifetime	8 Hours
IKEv2 Authentication Multiple	0

10. Go to **Network Profiles > IKE Gateways**.
11. In the **Networks** tab, click **Add**.

    The **IKE Gateway** window appears.



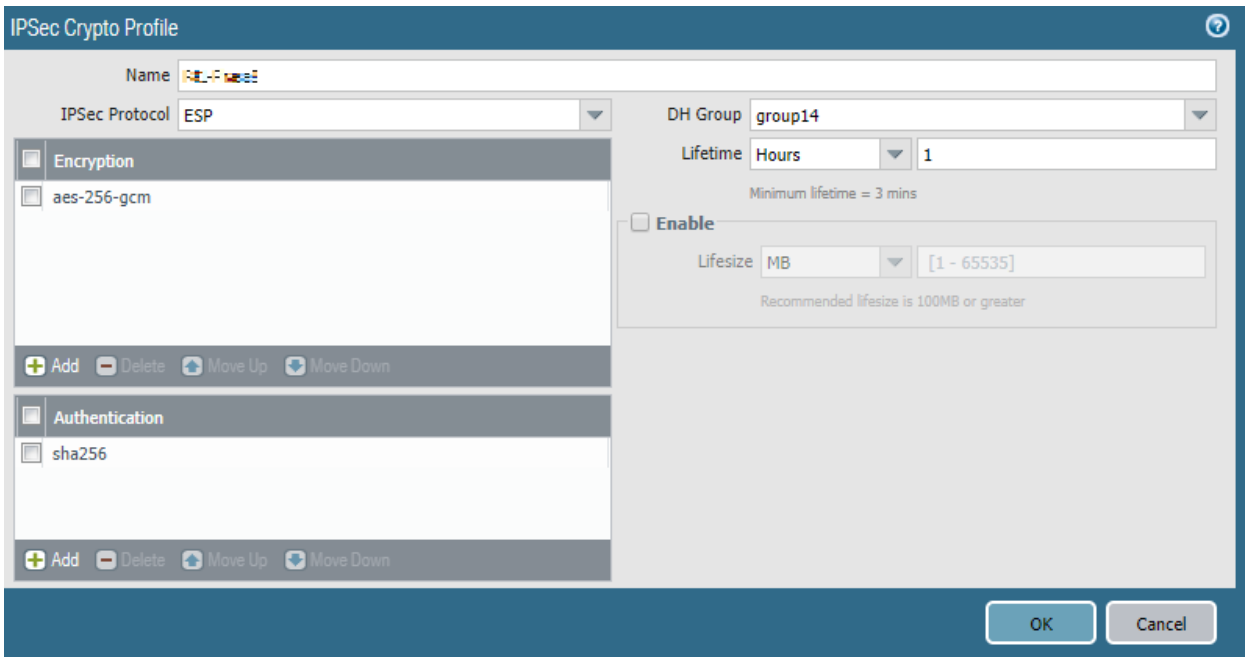
12. In the **General** tab:

Field	Enter
Name	Name for the gateway.
Version	IKEv2 only mode. If the firewall does not support IKEv2 , select IKEv1.
Address	IPv4
Interface	External interface connected to the internet.
Local IP Address	External IP address.
Peer IP Address Type	IP
Peer Address	Public IP address of the Harmony SASE gateway.
Authentication	Pre-Shared Key
Pre-shared Key	An alphanumeric string. Make a note of the key.

Field	Enter
Local Identification	None
Peer Identification	None

13. Click **OK**.
14. Go to **Network Profiles > IPSec Crypto**.
15. In the **Networks** tab, click **Add**.

    The **IPSec Crypto Profile** window appears.



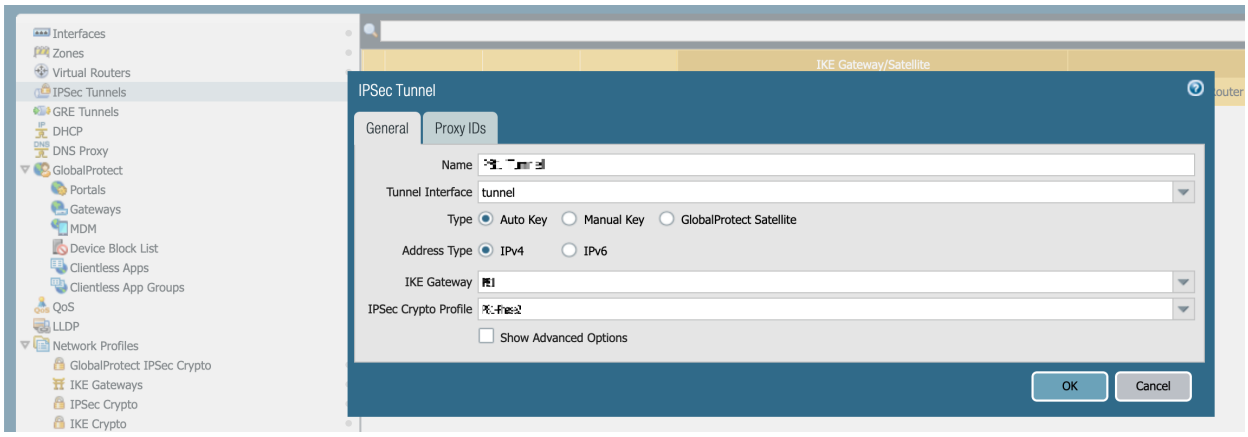
16. Enter these:

Field	Enter
Name	Name for the profile.
IPSec Protocol	ESP
DH Group	14
Encryption	aes-256-cbc
Lifetime	1 hour
Authentication	sha256

17. Click **OK**.

18. Click **IPSec Tunnels**.
19. In the **Networks** tab, click **Add**.

    The **IPSec Tunnel** window appears.

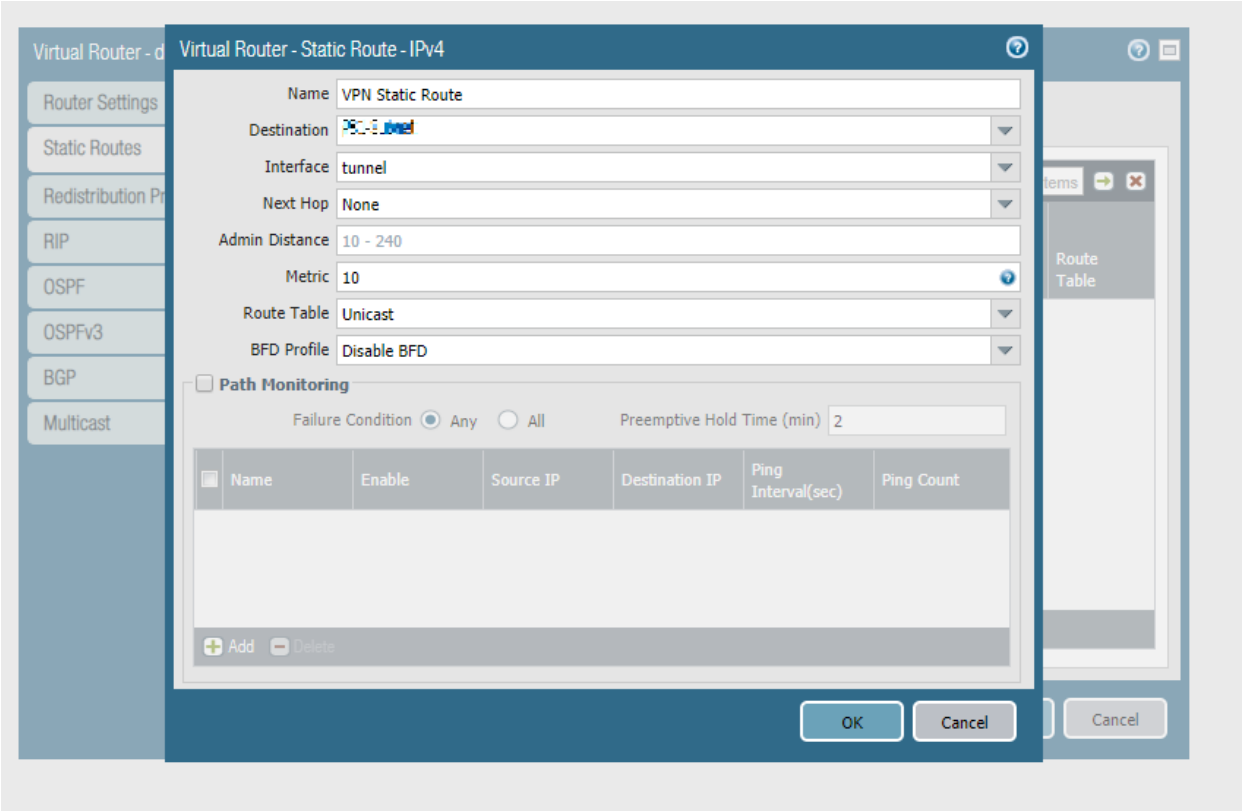


20. Enter these:

Field	Enter
Name	Name for the tunnel.
Tunnel Interface	An appropriate interface.
Type	Auto Key
Address	IPv4
IKE Gateway	Gateway that was defined previously.
IPSec Crypto Profile	Profile that was defined previously.

21. Click **Virtual Routers**.
22. Click **Static Routes** and click **Add**.

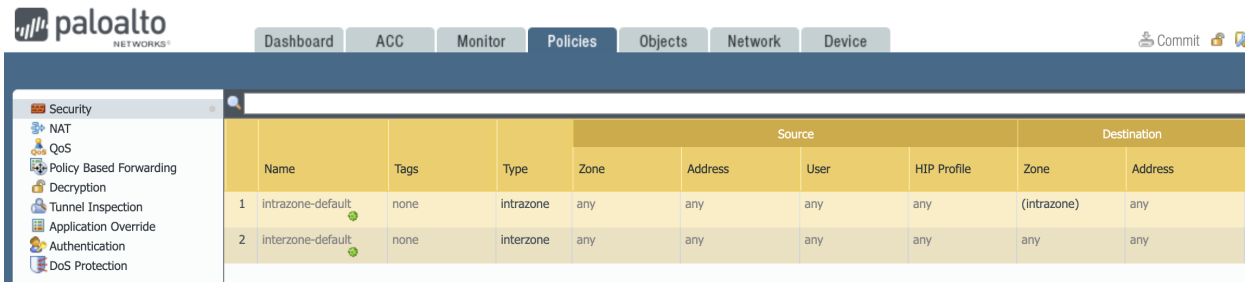
    The **Virtual Router - Static Route - IPv4** window appears.



23. Enter these:

Field	Enter
Name	Name for the static route.
Destination	Harmony SASE subnet.
Interface	An appropriate interface.
Next Hop	None
Metric	10
Route Table	Unicast
BFD Profile	Disable BFD

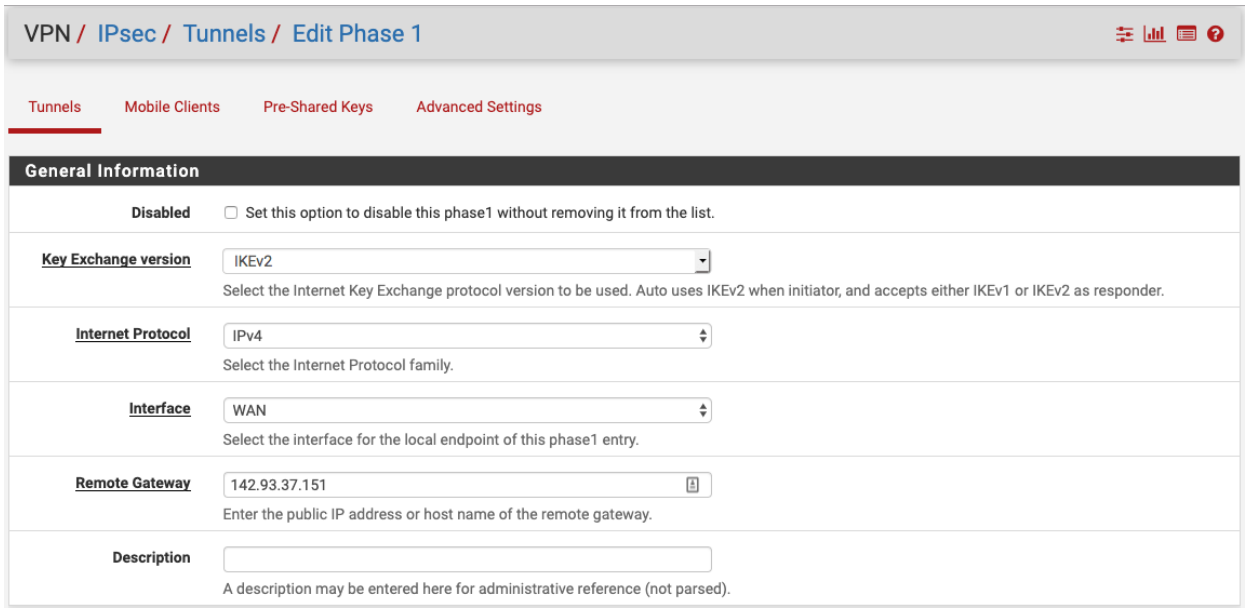
24. Go to **Network Profiles > IKE Crypto**.
25. Click the **Policies** tab. By default, IKE negotiation and IPSec/ESP packets are allowed. If they are not, create an appropriate rule.



pfSense Firewall

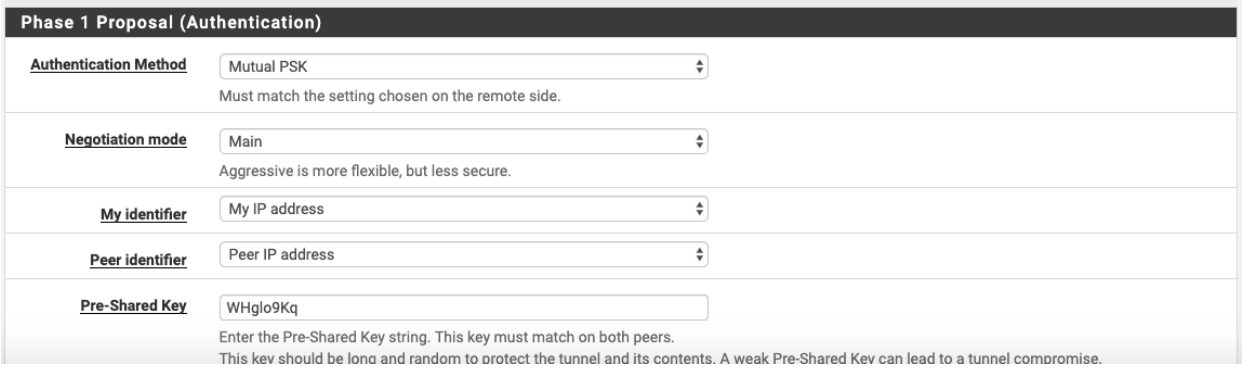
To configure the tunnel in the pfSense Management Portal:

1. Log in to the pfSense Management Portal with the Administrator account.
2. Go to **VPN > IPsec**.
3. Click **+Add P1**.
4. In the **General Information** section:



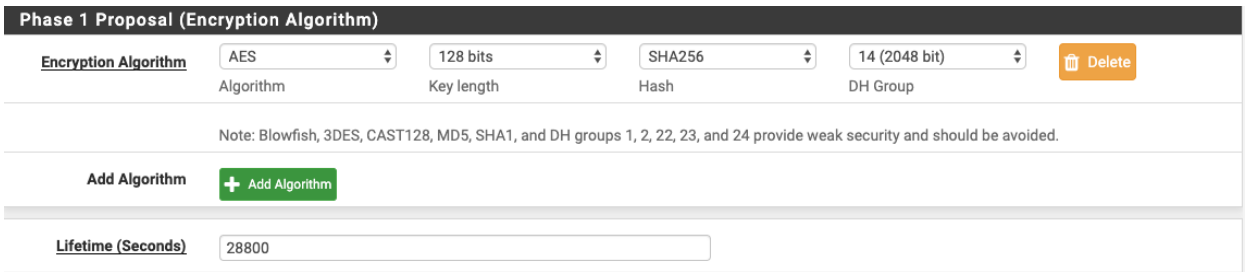
Field	Enter
Key Exchange version	IKEv2 if supported. Otherwise IKEv1.
Internet Protocol	IPv4
Interface	WAN
Remote Gateway	Public IP address of the Harmony SASE gateway.

5. In the **Phase 1 Proposal (Authentication)** section:



Field	Enter
Authentication Method	Mutual PSK
Negotiation Mode	Main
My Identifier	My IP Address **Note** - For Dynamic-IP Tunnel, select **Distinguished Name** and enter the predefined Remote ID.
Peer Identifier	Peer IP Address
Pre-Shared Key	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171* .

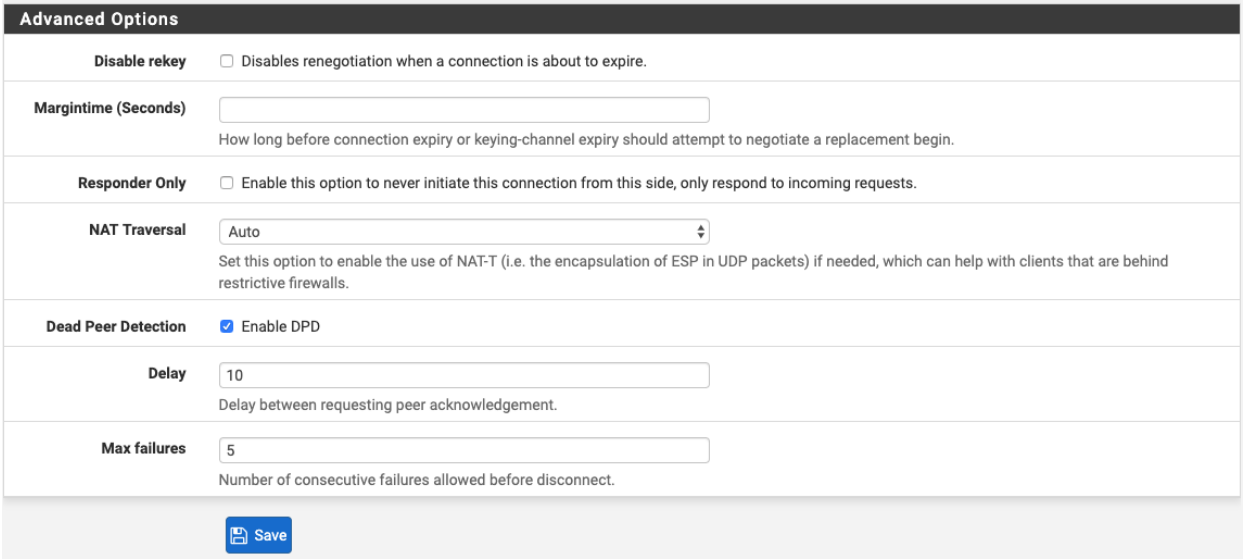
6. In the **Phase 1 Proposal (Encryption Algorithm)** section:



Field	Enter
Algorithm	AES
Key Length	256 bits
HASH	SHA256
DH Group	14

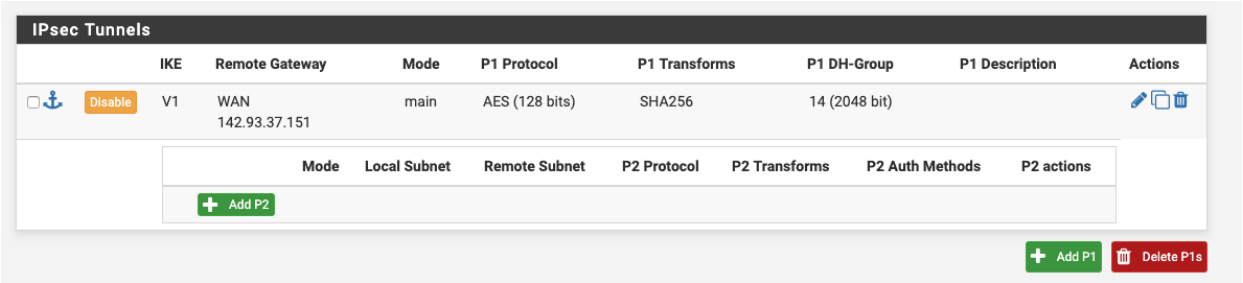
Field	Enter
Lifetime (Seconds)	28800

7. In the **Advanced Options** section:

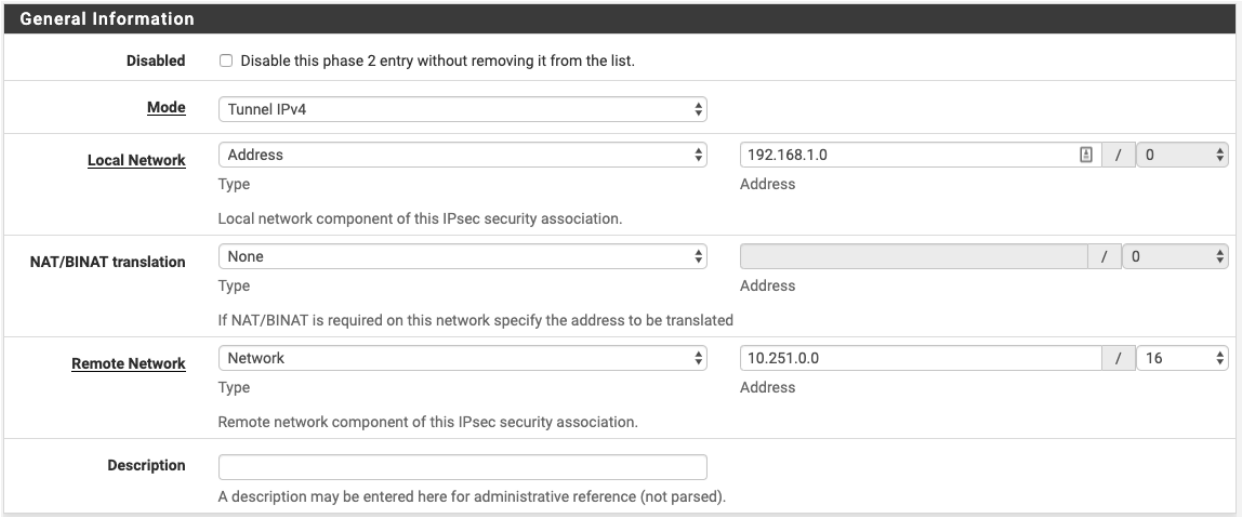


Field	Enter
Disable rekey	Clear
Margintime (Seconds)	Blank
Responder Only	Clear
NAT Traversal	Auto
Dead Peer Detection	Select
Delay	10
Max failures	5

8. Click **Save**.
9. Click **+Add P2**.

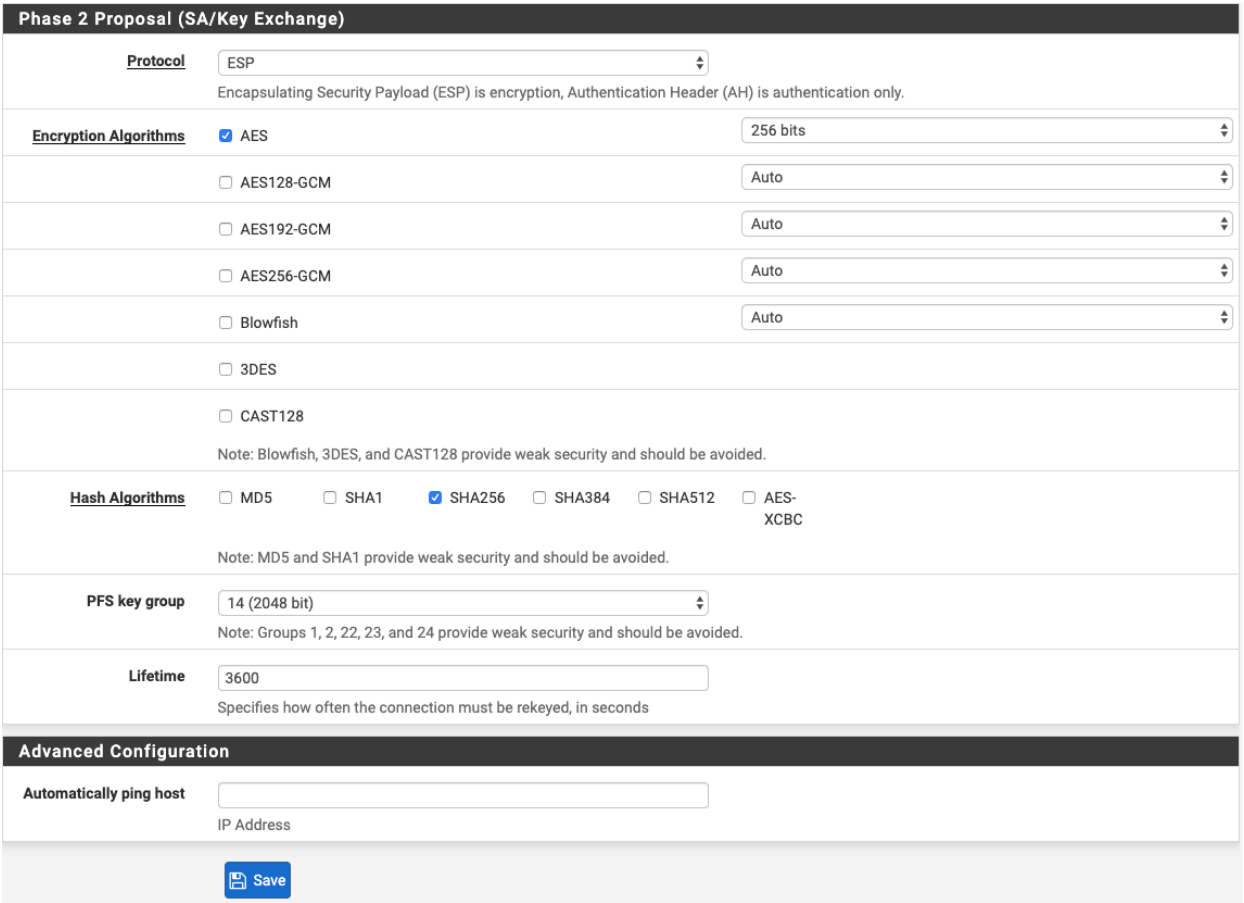


10. In the **General Information** section:



Field	Enter
Mode	Tunnel IPv4
Local Network Type	Network
Local Network Address	Your local LAN network subnet.
Remote Network Type	Network
Remote Network Address	Harmony SASE remote network subnet.

11. In the **Phase 2 Proposal (SA/Key Exchange)** section:

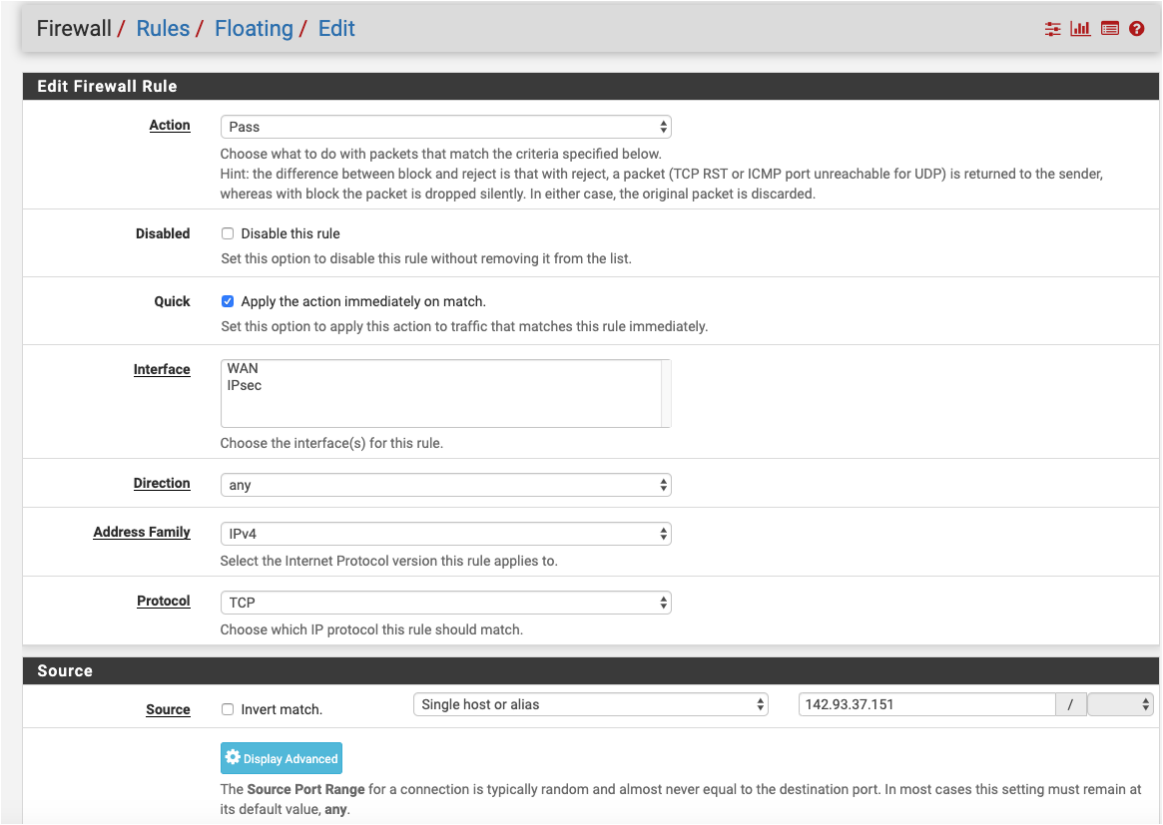


Field	Enter
Protocol	ESP
Encryption Algorithm	AES 256 bits
Hash Algorithm	SHA256
PFS Key Group	14

12. Click **Save**.
13. (Optional) Configure firewall rules:

a. Go to **Firewall > Rules**.

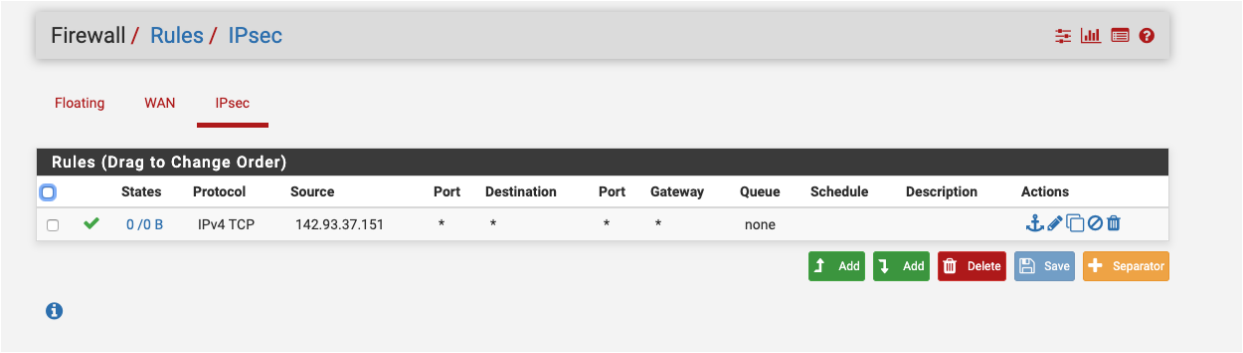
b. Under **IPSEC**, add a new rule:



Field	Enter
Action	Pass
Quick	Mark v
Interface	WAN and IPSEC
Source	Public IP address of Harmony SASE gateway
Destination	Any or an external IP address.

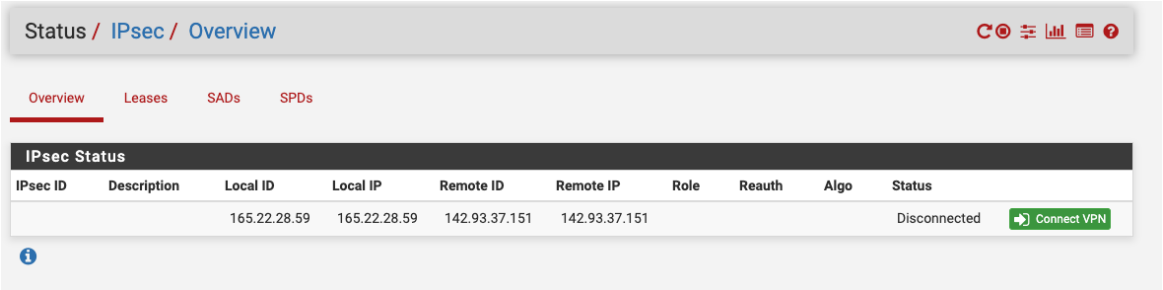
c. Click **Save**.

14. Under **IPSEC**, add a new rule:



Field	Enter
Action	Pass
Source	Public IP address of Harmony SASE gateway
Destination	Any or an external IP address.

15. Click **Save**.
16. Click **Apply Changes**.
17. Activate the tunnel:
    a. From the **Menu Bar**, click **Status > IPsec**.

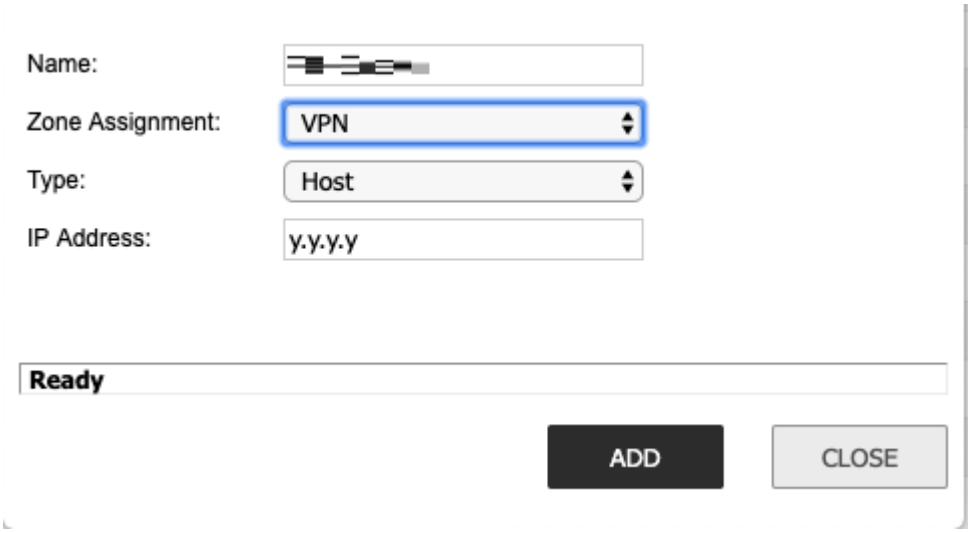


    b. Click **Connect VPN** for the tunnel to Harmony SASE gateway.

SonicWall Firewall

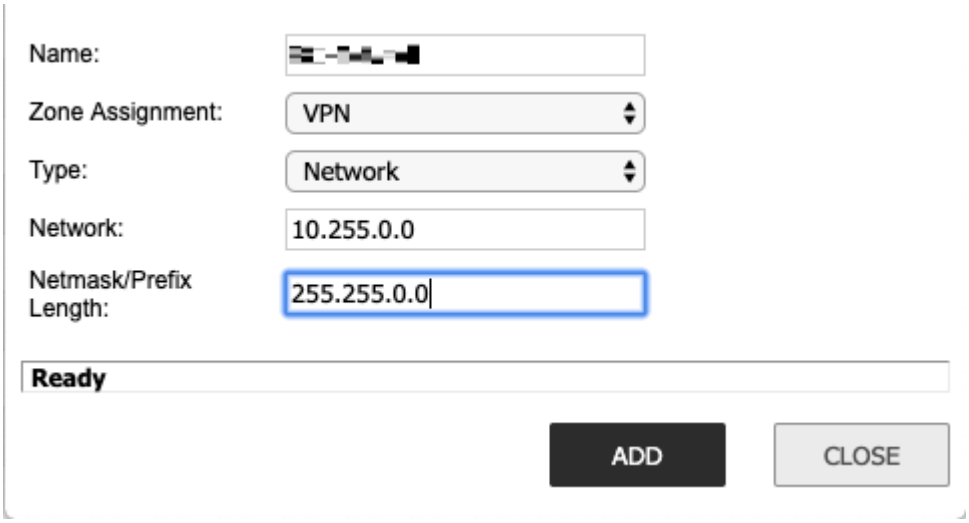
To configure the tunnel in the SonicWall Management Portal:

1. Log in to the SonicWall Management Portal with the Administrator account.
2. Go to **Objects > Address Objects**.
3. Add a gateway object:



Field	Enter
Name	Name for the gateway object.
Zone Assignment	VPN
Type	Host
IP Address	Public IP address of Harmony SASE gateway.

4. Click **Add**.
5. Add a network object:



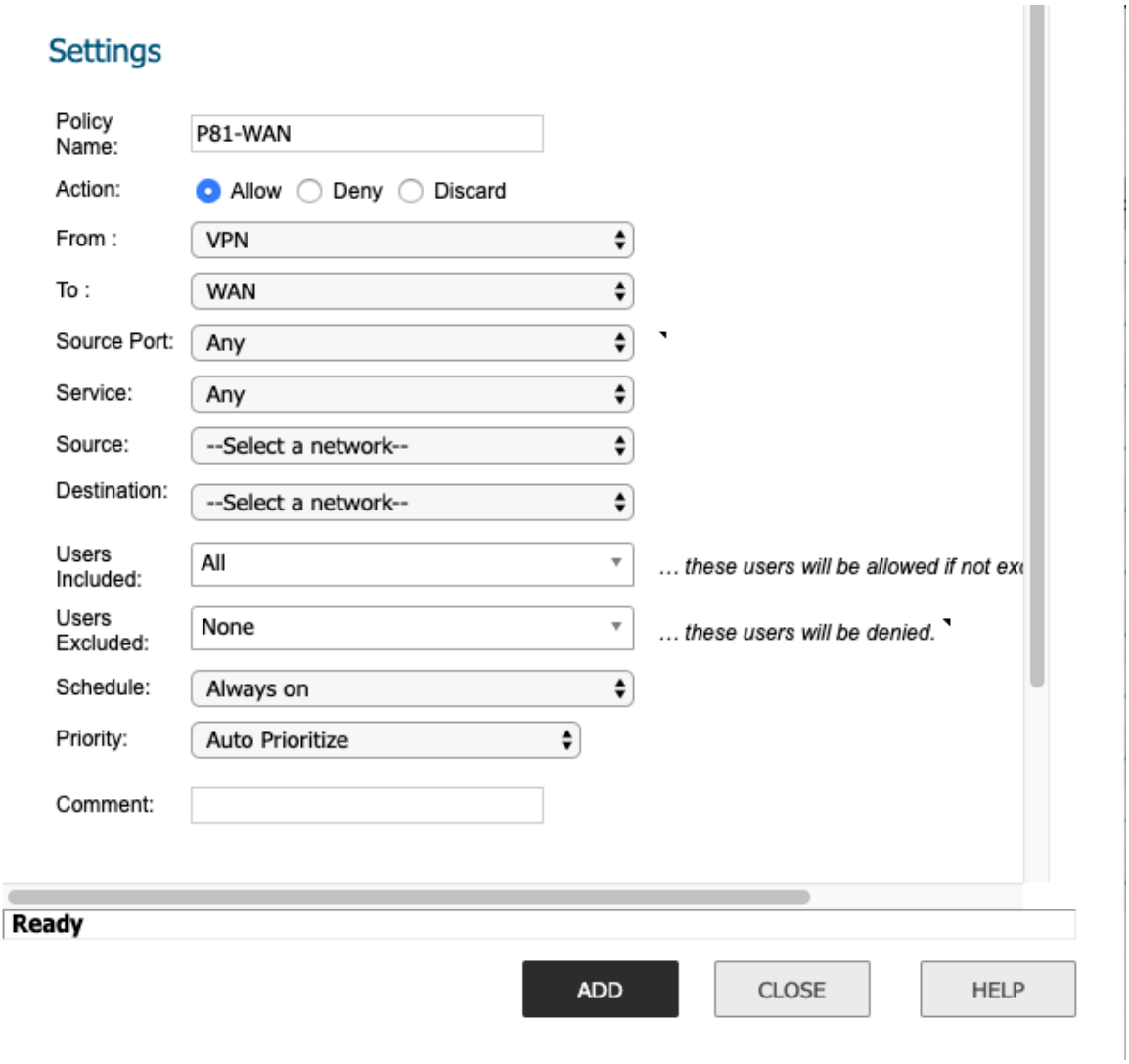
Field	Enter
Name	Name for the network object.
Zone Assignment	VPN
Type	Host
Network	Public IP address of Harmony SASE gateway.
Netmask/Prefix length	Harmony SASE subnet mask (255.255.255.0)

6. Click **Add**.
7. Configure firewall policies from VPN to WAN:

a. Go to **Policy > Rules**.

b. Click **Add**.

The **Settings** window appears.



c. Enter these:

Field	Enter
Policy Name	Name for the firewall policy.
Action	Allow
From	VPN
To	WAN
Source Port	Any
Service	Any
Source	Harmony SASE gateway object.
Destination	Your external internet interface object.

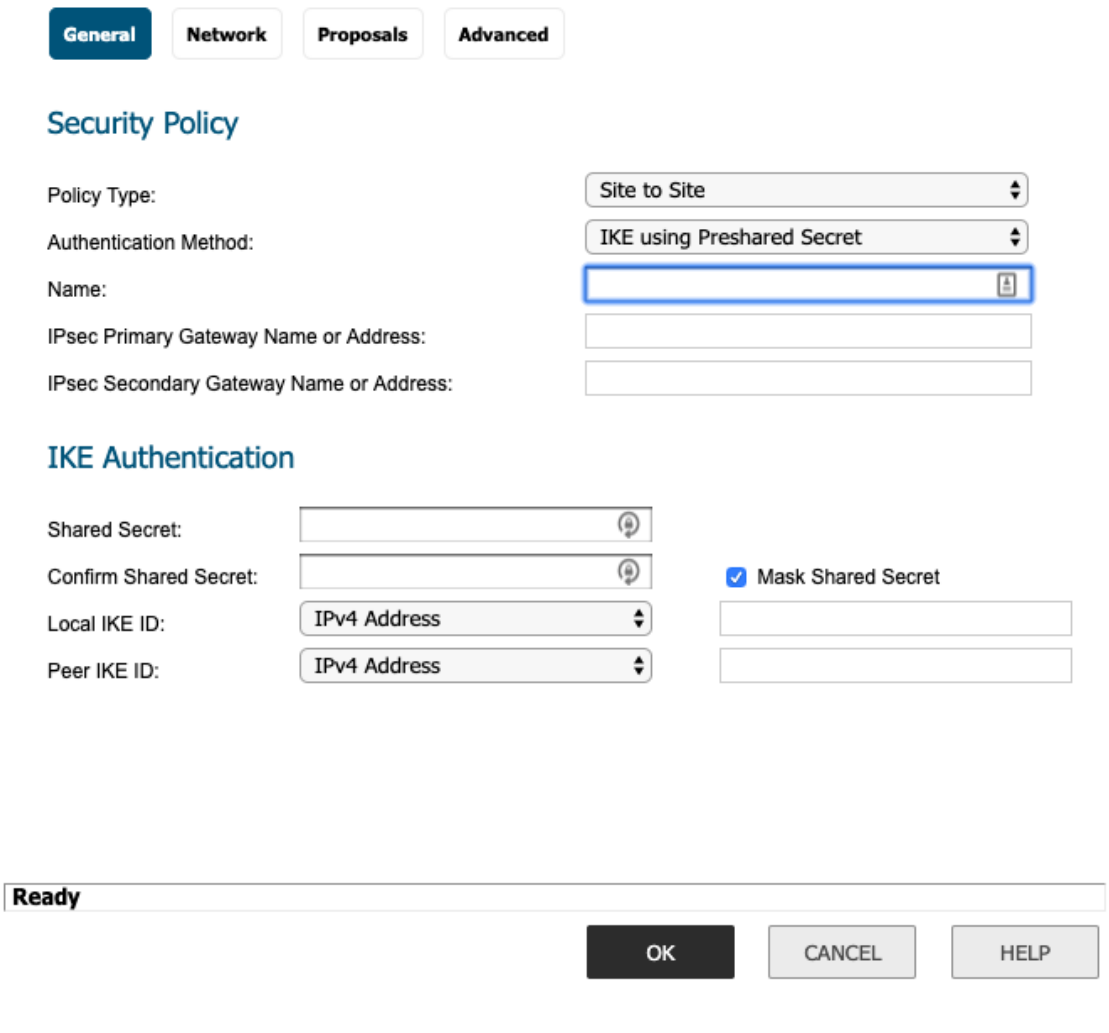
d. Click **Add**.

8. Create a site-to-site connection:

a. Click **VPN**.

b. In the **Base Settings** section, click **VPN Policy**.

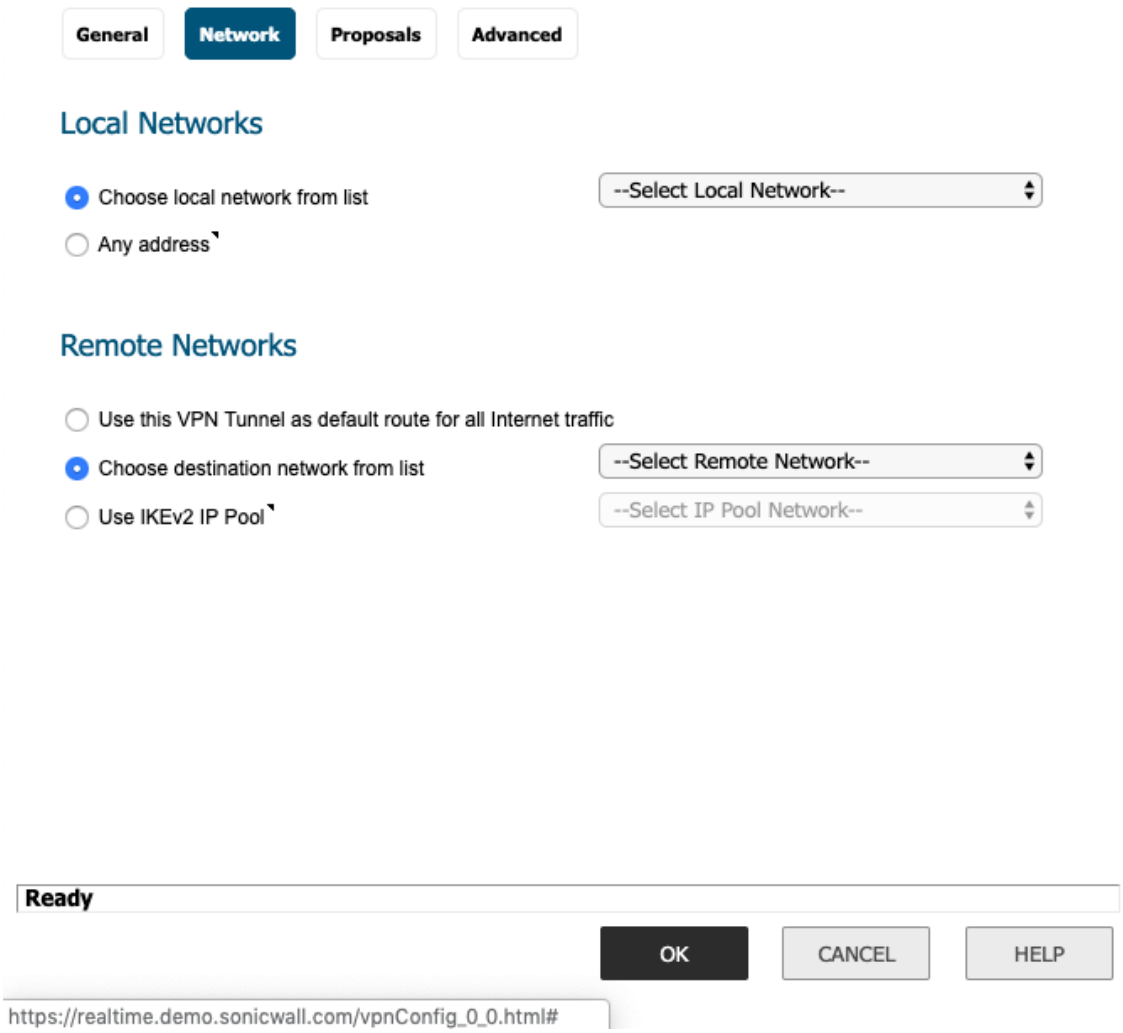
c. In the **General** tab, enter these:



Field	Enter
Security Policy	
Policy Type	Site to Site
Authentication Method	IKE using Preshared Secret
Name	Name for the site-to-site connection.
IPsec primary Gateway Name or Address	Public IP address of Harmony SASE gateway.
IPsec Secondary Gateway Name or Address	Blank

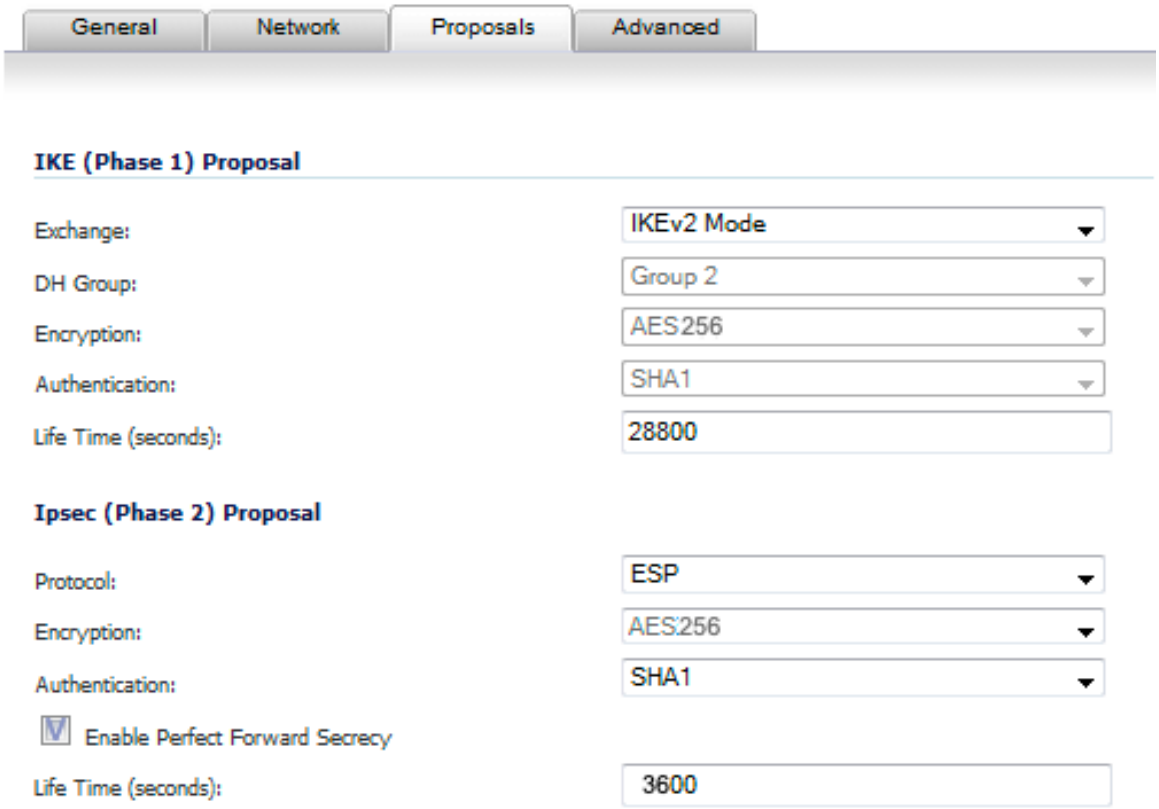
Field	Enter
Service	Any
Source	Harmony SASE gateway object.
Destination	Your external internet interface object.
IKE Authentication	
Shared Secret	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.
Confirm Secret	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.
Local IKE ID	IPv4 Address and your local external internet address.
Peer IKE ID	IPv4 Address and the public IP address of Harmony SASE gateway.

d. In the **Network** tab, enter these:



Field	Enter
Local Networks	
Choose a local network from the list	Your local LAN network.
IKE Authentication	
Choose destination network from the list	Harmony SASE network object.

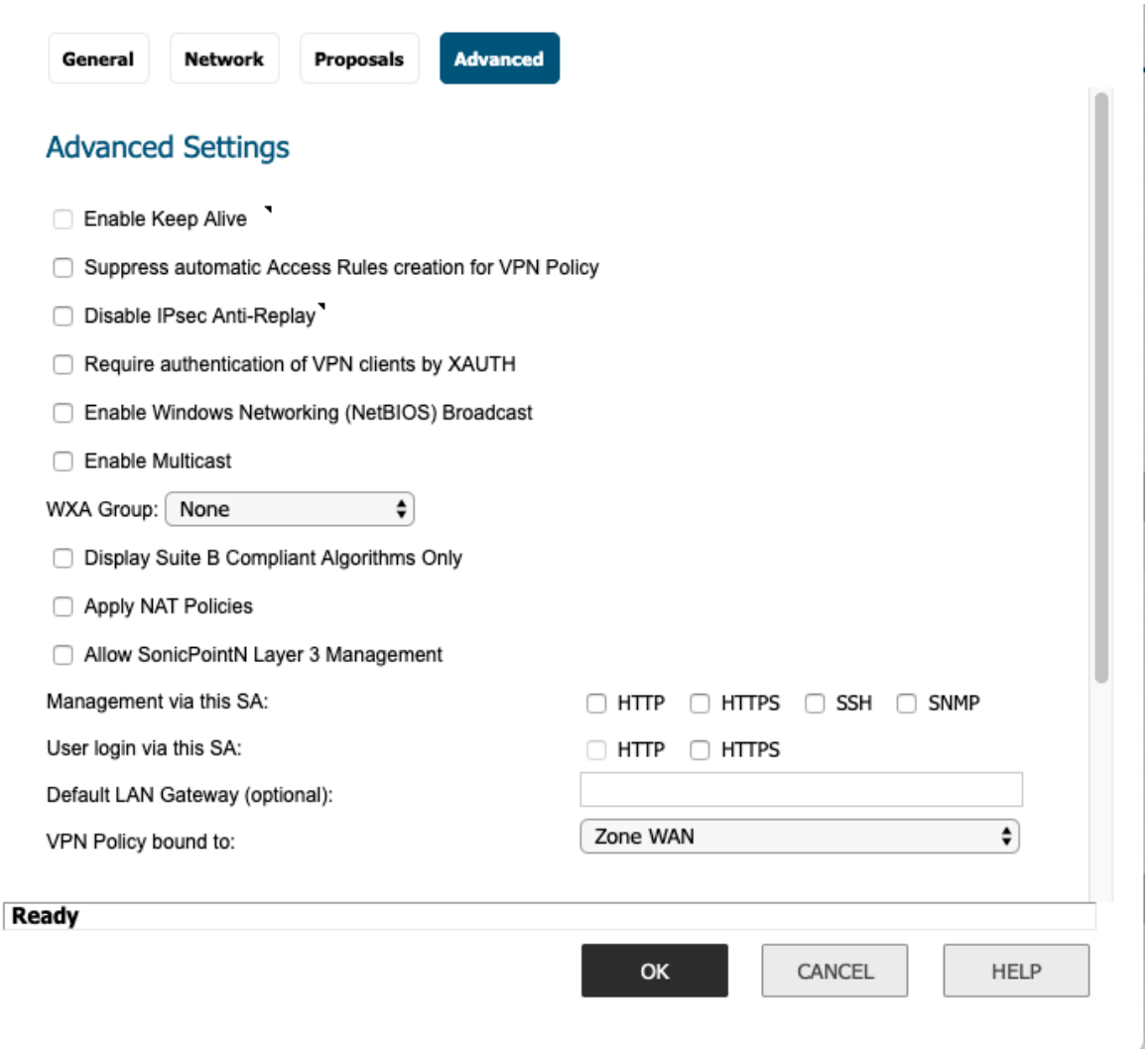
e. In the **Proposals** tab, enter these:



Field	Enter
IKE (Phase 1) Proposal	
Exchange	IKEv2 Mode
DH Group	Group 2
Encryption	AES-256
Authentication	SHA1
Life Time (seconds)	28800
IKE (Phase 2) Proposal	
Protocol	ESP
Encryption	AES-256
Authentication	SHA1

Field	Enter
Enable Perfect Forward Security	Select
DH Group	Group 2
Life Time (seconds)	3600

f. In the **Advanced Settings** tab, select the **Enable Keep Alive** checkbox.



g. Click **OK**.

h. Make sure the change is committed to SonicWall. In the **VPN Policies** screen, make sure that the new VPN policy is enabled.

   You can select the **Play** (▶) button to the right of the **Currently Active VPN Tunnels** to view whether the tunnel is up or not.

   If the tunnel is not up, navigate to the **Event Logs** and check the logs for errors in the new VPN policy.

Sophos XG Firewall

To configure the tunnel in the Sophos XG Management Portal:

1. Log in to the Sophos XG Management Portal with the Administrator account.
2. Add a local and remote LAN object:
   a. Go to **Hosts and Services > IP Host**, click **Add** and enter these:

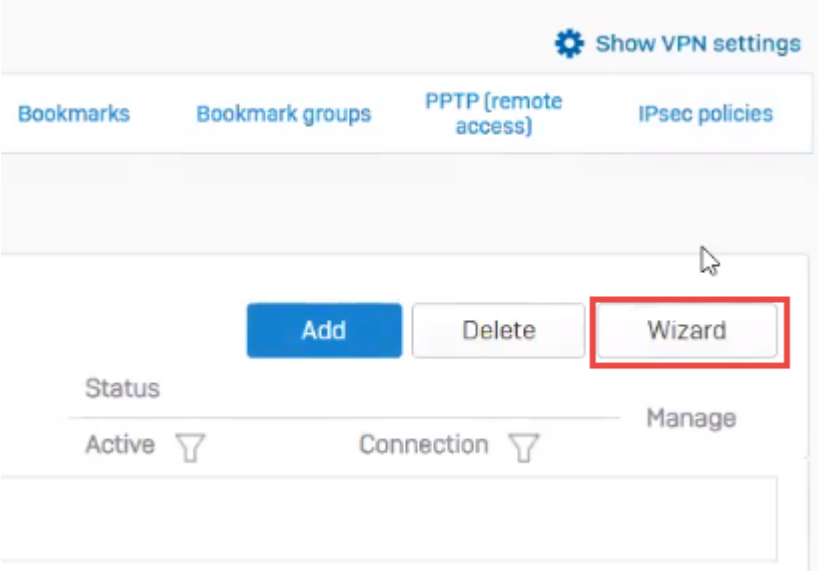
Field	Enter
Name	Name for the object.
IP Family	IPv4
Type	Network
IP Address	Your local network and subnet.

   b. Repeat step a to add a remote LAN object:

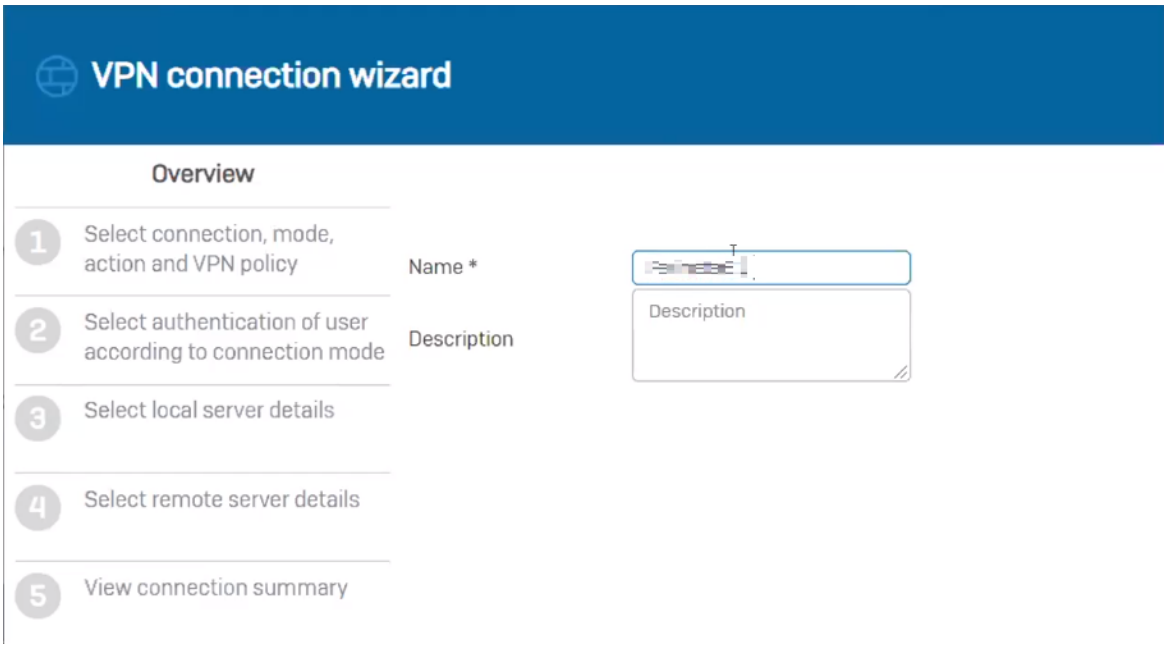
Field	Enter
Name	Name for the object.
IP Family	IPv4
Type	Network
IP Address	Your remote network and subnet.

3. Create an IPsec VPN connection:

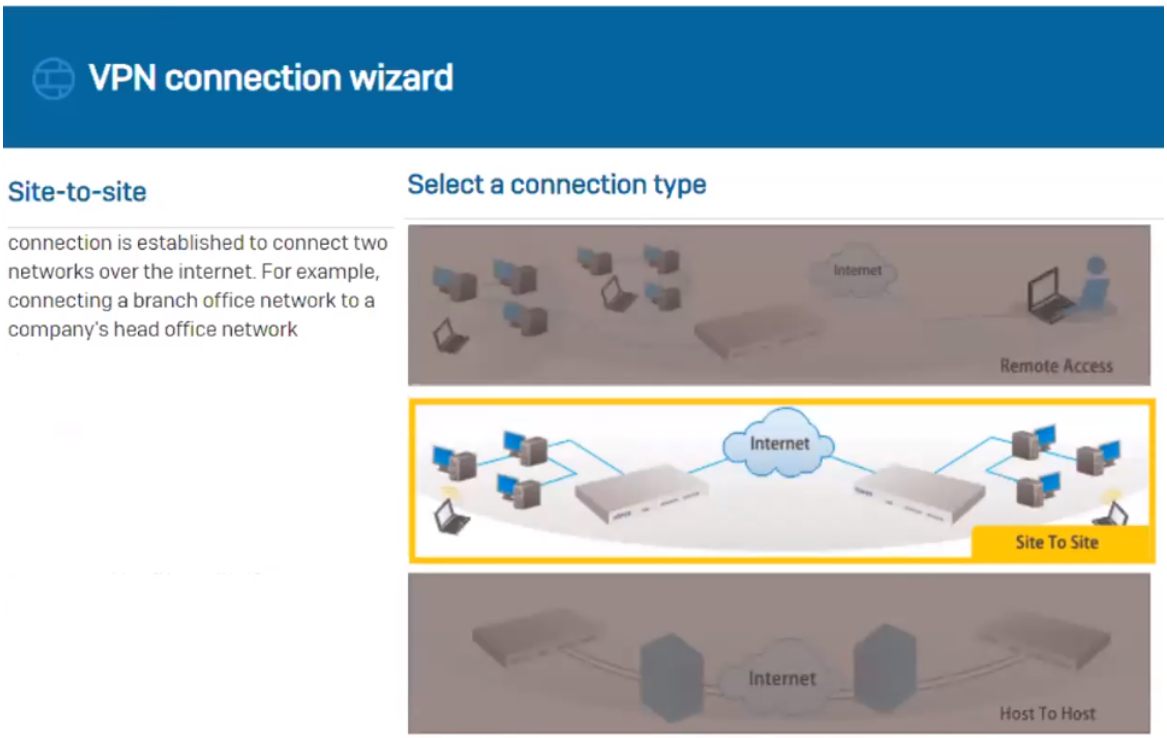
a. Go to **VPN > IPsec Connections** and select **Wizard**.



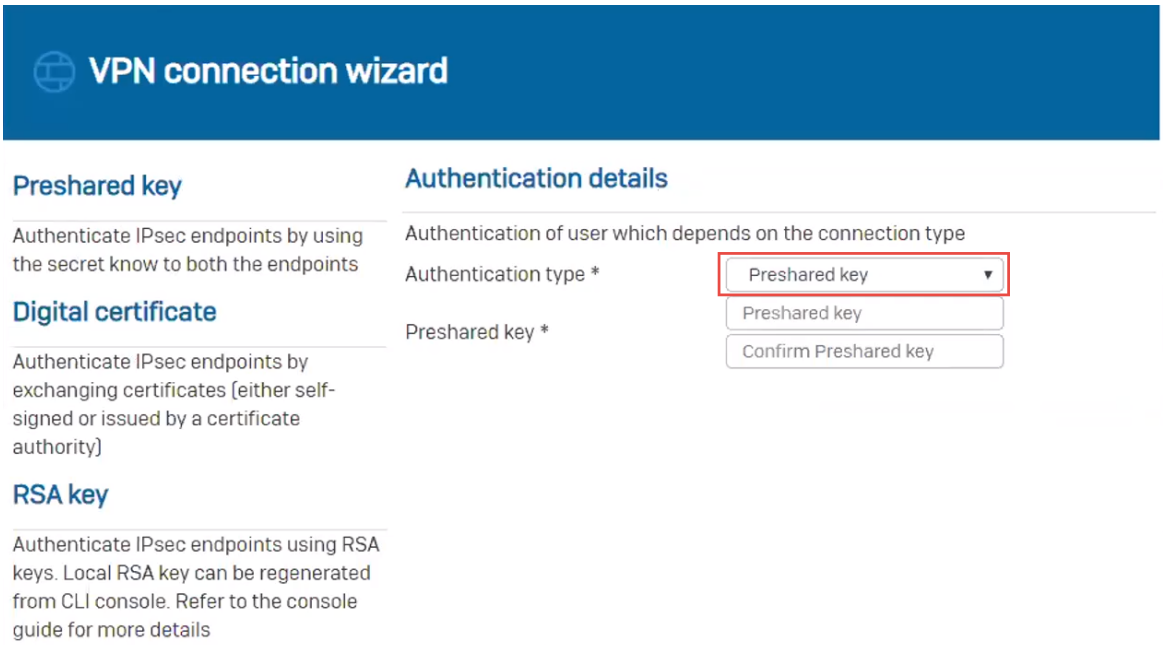
b. In the **Name** field, enter a name for the connection, and click **Start**.



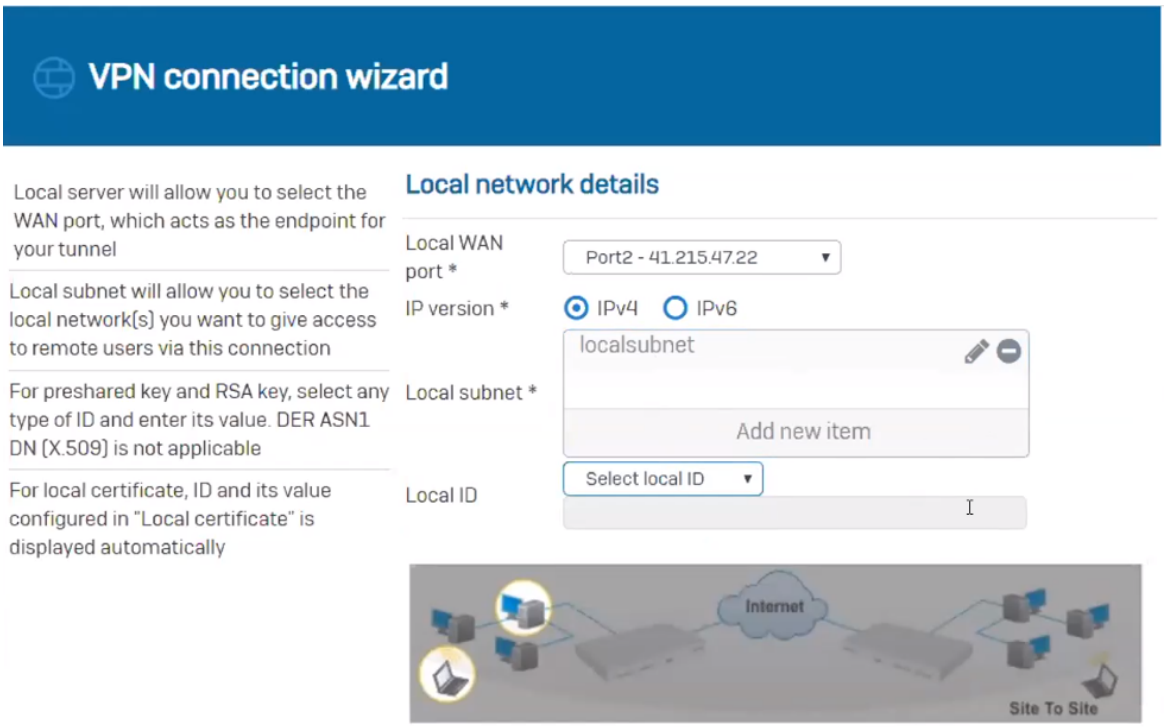
c. For **Select a connection type**, select **Site To Site** and select **Head Office**.



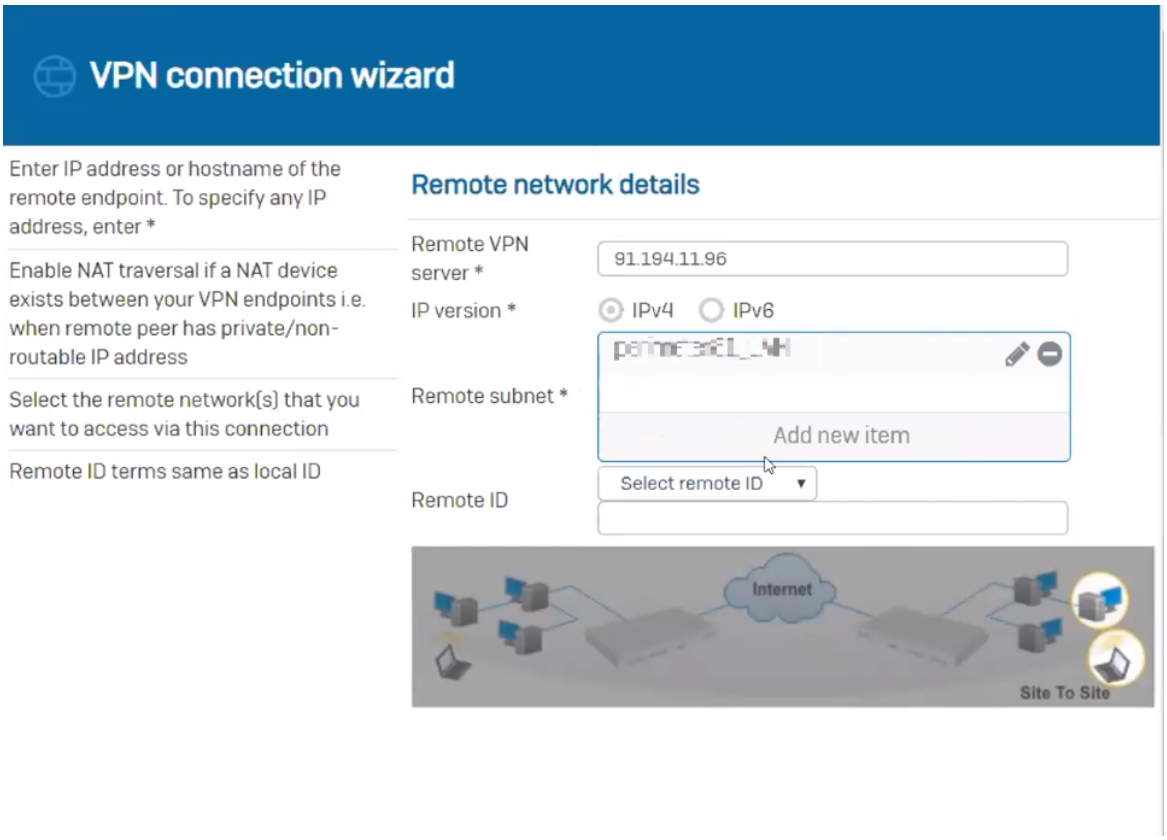
d. From the **Authentication type** list, select **Preshared key**.



e. In the **Local subnet** field, enter the local LAN created earlier in the procedure.



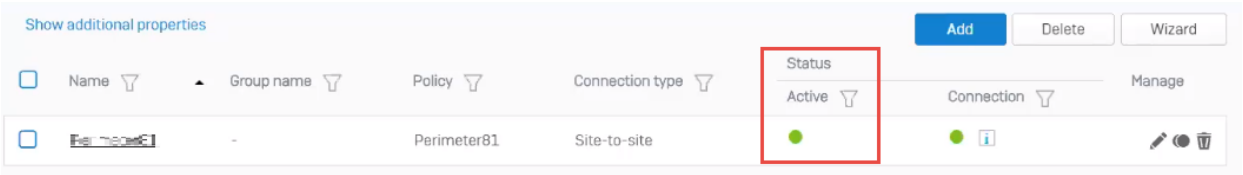
f. In the **Remote subnet** field, enter the remote LAN created earlier in the procedure.



g. From the **User Authentication** list, select **Disabled**.

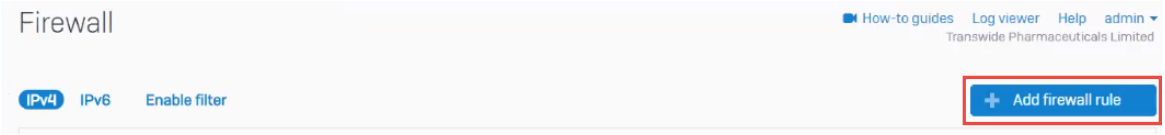
h. Review the IPSec connection summary and click **Finish**.

4. Set **Status** to **Active**.

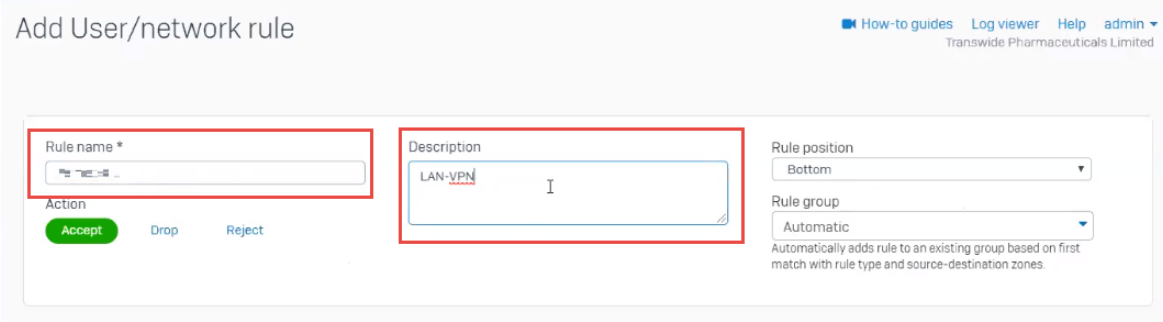


5. Add two firewall rules to allow the VPN traffic:

a. Click **Firewall** and click **Add Firewall Rule**.

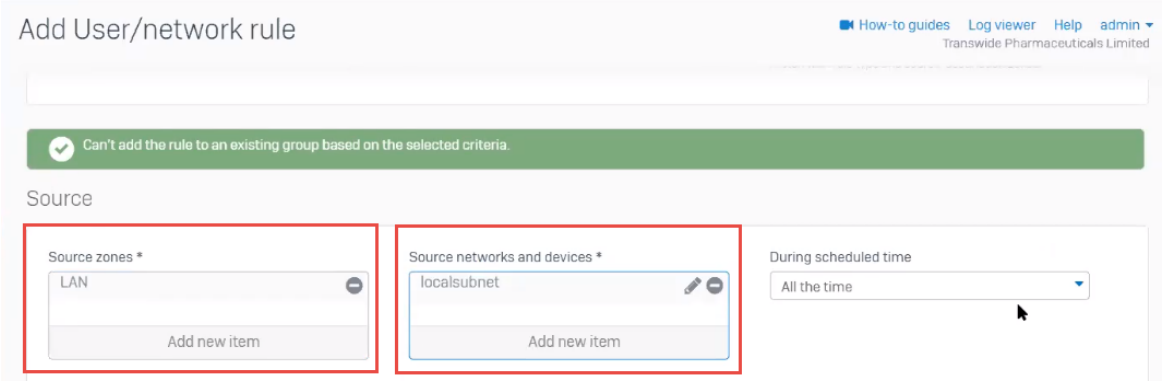


b. In the **Name** field, enter a name for the rule.



c. In the **Description** field, enter **LAN-VPN**.

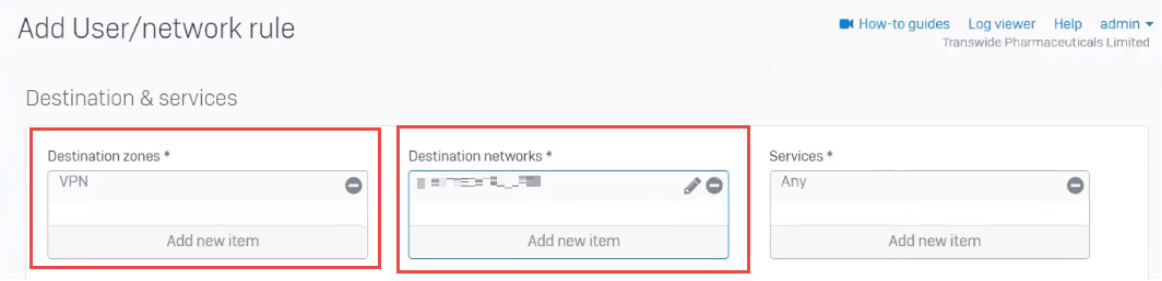
d. In the **Source** section:



i. In the **Source zones** field, enter **LAN**.

ii. In the **Source network and devices** field, enter **local subnet**.

e. In the **Destination &services** section:



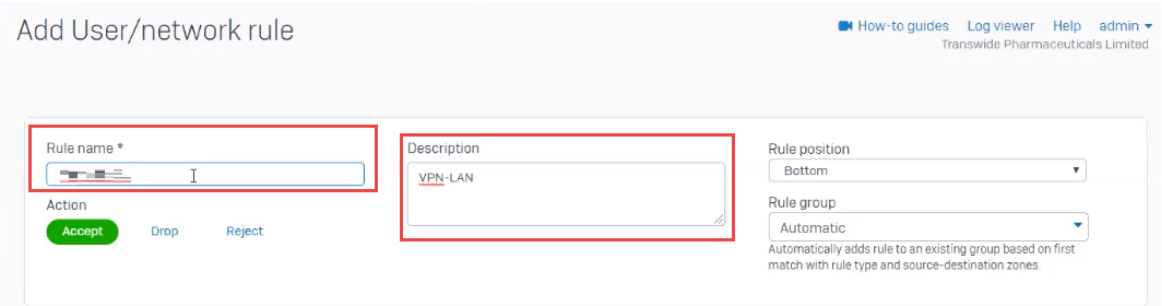
i. In the **Destination zones** field, enter **VPN**.

ii. In the **Destination networks** field, enter **Harmony SASE_LAN**.

f. Click **Save**.

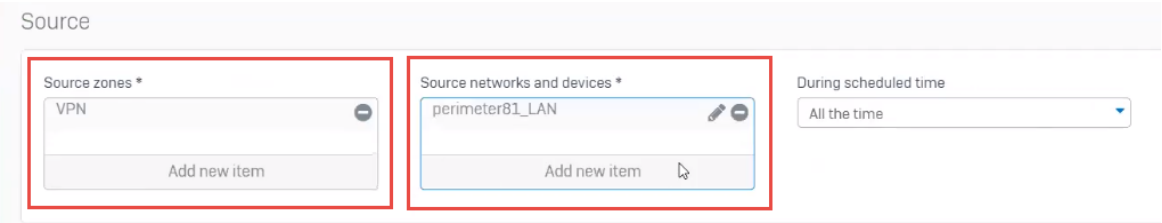
g. Add the second firewall, click **Firewall** and click **Add Firewall Rule**.

h. In the **Name** field, enter a name for the rule.



i. In the **Description** field, enter **VPN-LAN**.

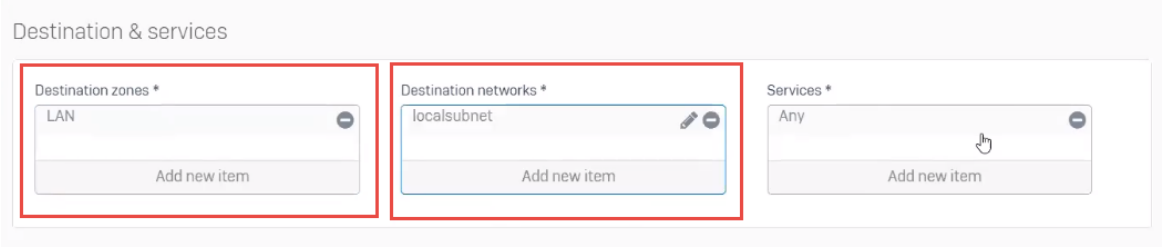
j. In the **Source** section:



i. In the **Source zones** field, enter **VPN**.

ii. In the **Source network and devices** field, enter **Harmony SASE_LAN**.

k. In the **Destination &services** section:



i. In the **Destination zones** field, enter **LAN**.

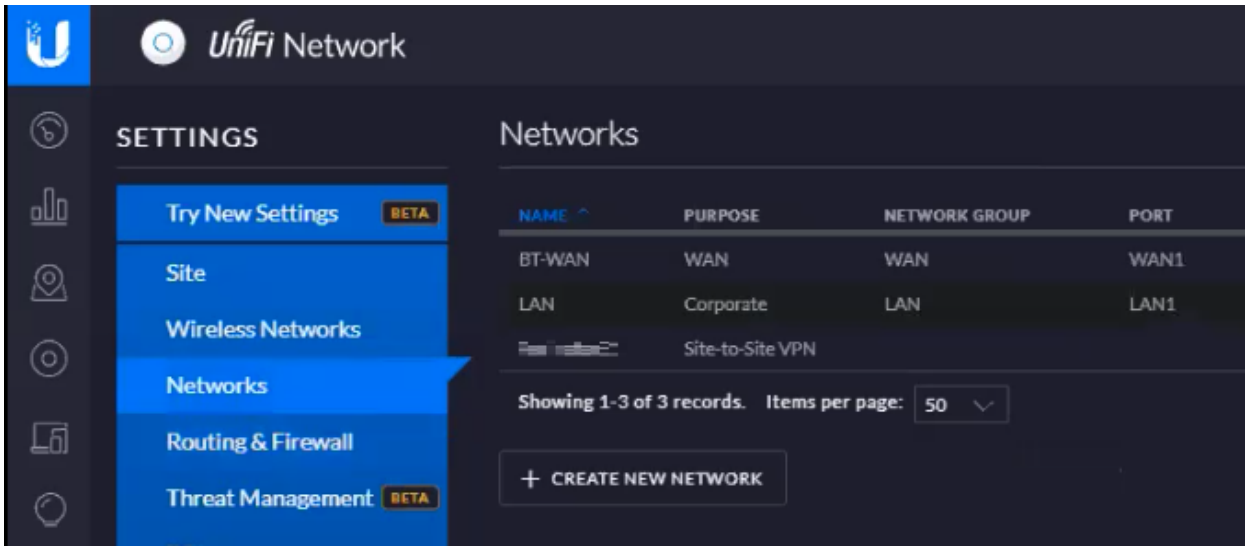
ii. In the **Destination networks** field, enter **local subnet**.

l. Click **Save**.

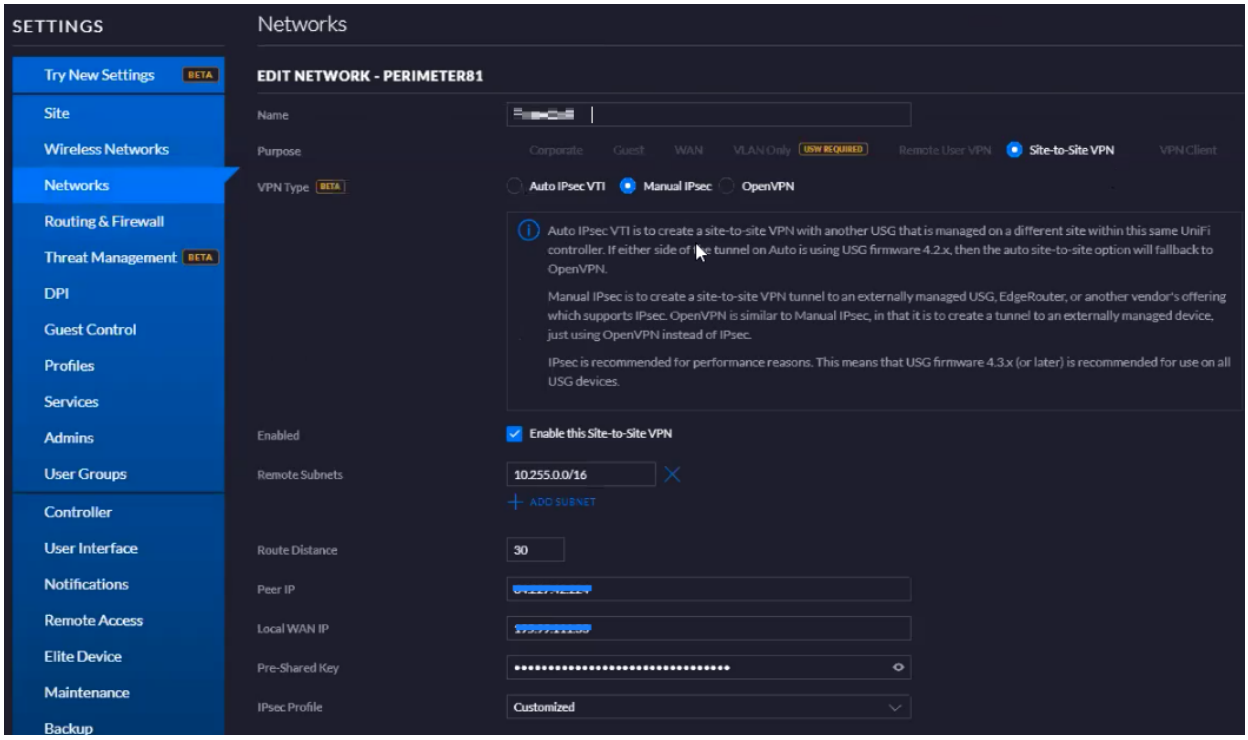
UniFi USG Firewall

To configure the tunnel in the UniFi USG Management Portal:

1. Log in to the UniFi USG Management Portal with the Administrator account.
2. Click **Networks** and then click **Create New Network**.



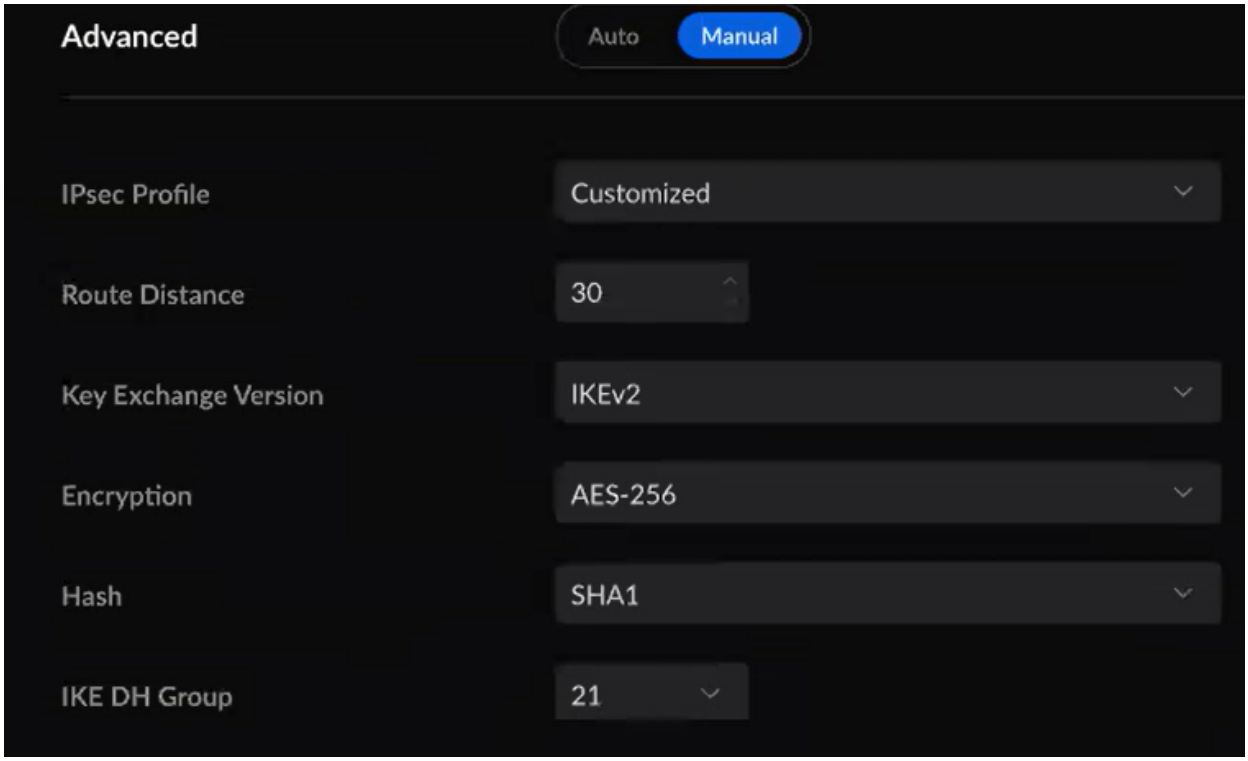
3. Click **Site to Site VPN > Manual IPSec**.



4. Enter these:

Field	Enter
Name	Name for the network.
Purpose	Site-to-Site VPN
VPN Type	Manual IPSec
Enabled	Select the Enable this Site-toSite VPN checkbox.
Remote Subnets	Harmony SASE subnet. The default is 10.255.0.0/16.
Peer IP	Public IP address of the location server.
Local WAN IP	Public IP address of the UniFi USG firewall.
Pre-shared key	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

5. In the **Advanced Options** section:



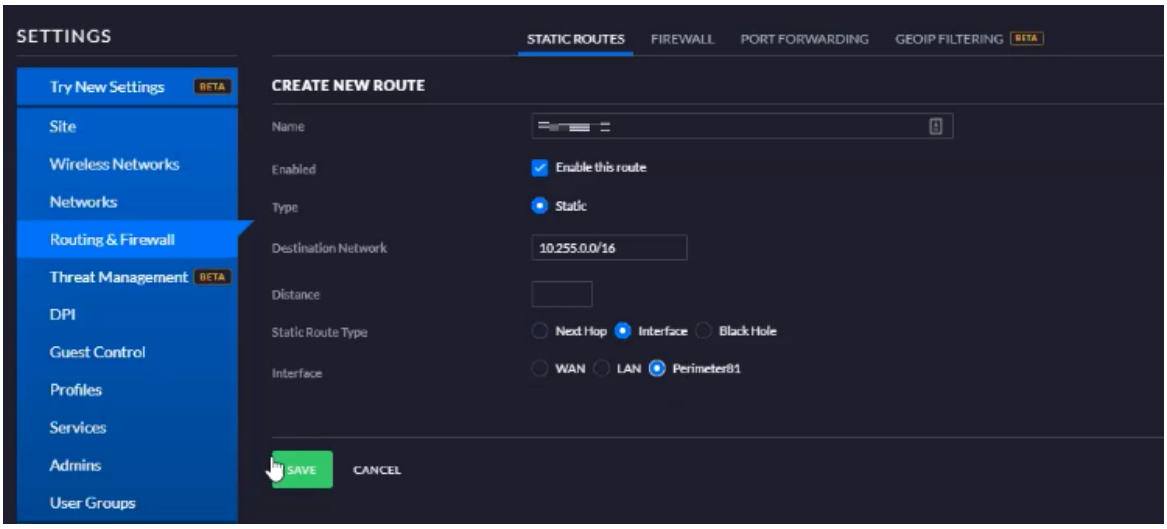
Field	Enter
IPsec Profile	Customized
Route Distance	30
Key Exchange version	IKEv2
Encryption	AES-256
Hash	SHA1
IKE DH Group	21
PFS	Enable
Dynamic Routing	Disable[1]

[1] To create a Route-Based IPSEC Site-to-Site connection between Harmony SASE and your Ubiquiti network:

a. Set **Dynamic Routing** to **Enable** .
b. Add any other subnet specified in **Remote Subnets** and make sure that a reverse traffic route is created under **Static Routes** in the UniFi USG firewall for each connected subnet to route through the Harmony SASE Interface.
c. In the Harmony SASE Administrator Portal, change **Harmony SASE Gateway Proposal Subnets** and **Remote Gateway Proposal Subnets** to **Any (0.0.0.0/0)**.
d. Create separate static routing in Harmony SASE. For more information, see <TBD_Cross-ref to site-connection overview>.

6. Add static routes from Harmony SASE subnet (10.255.0.0/16) to the local network and vice versa through the VPN gateway:

   a. Go to **Routing & Firewall > Static Routes > Create New Route**.

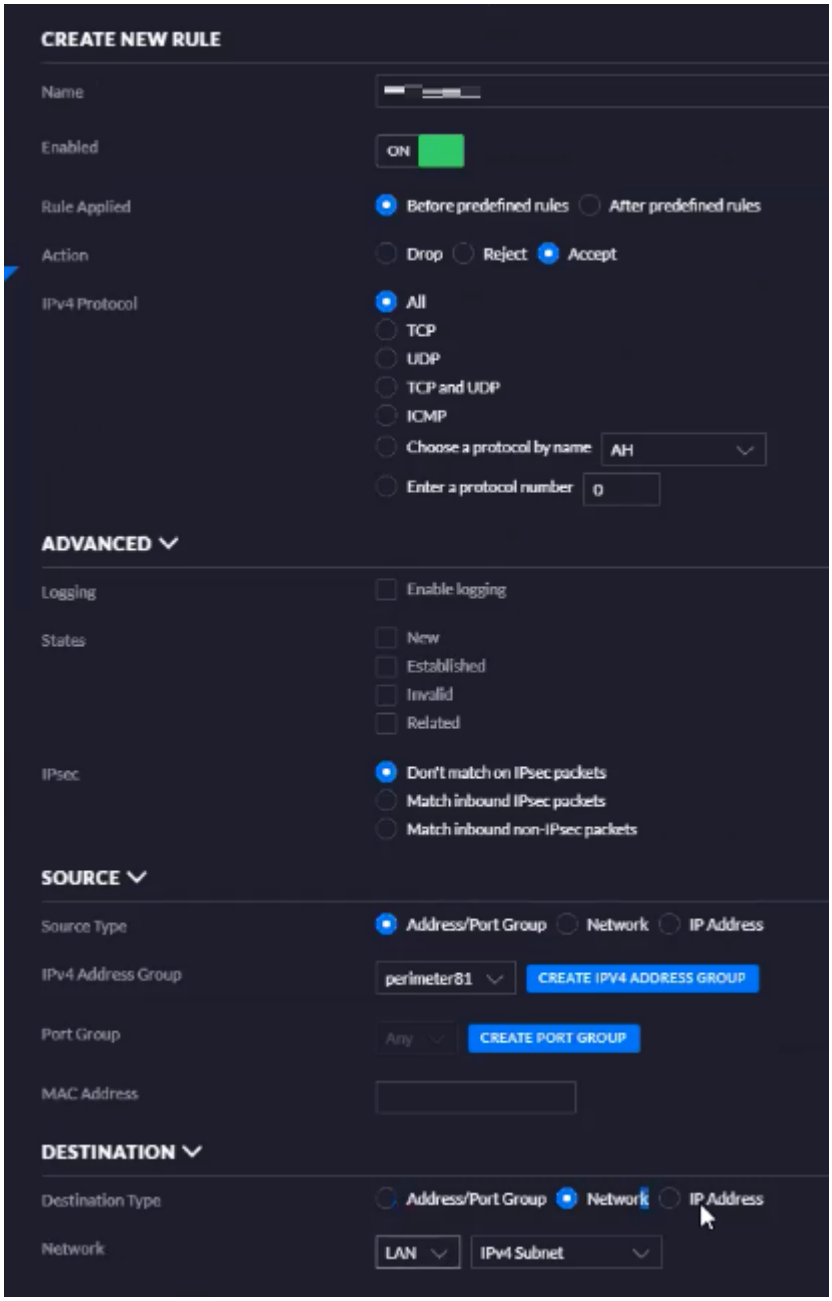


b. Enter these:

Field	Enter
Name	Name for the static route.
Enabled	Select the Enable this route checkbox.
Type	Static
Destination Network	Harmony SASE subnet. The default is 10.255.0.0/16.
Static Route Type	Interface
Interface	Select the interface created in the previous procedure.

c. Click **Save**.

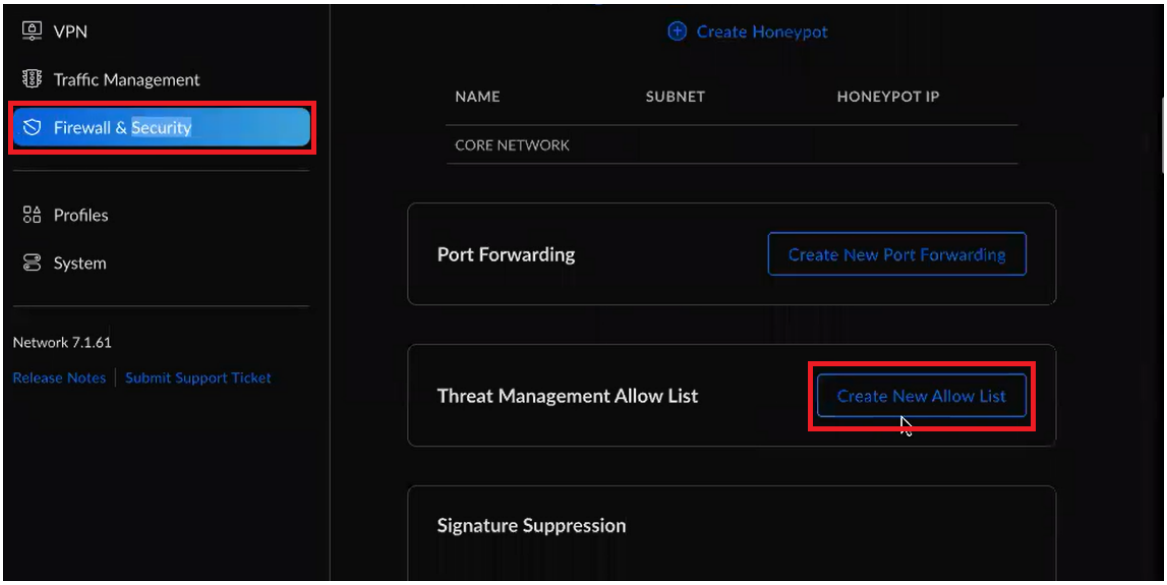
7. Create a firewall rule to allow traffic from Harmony SASE subnet to the LAN network.



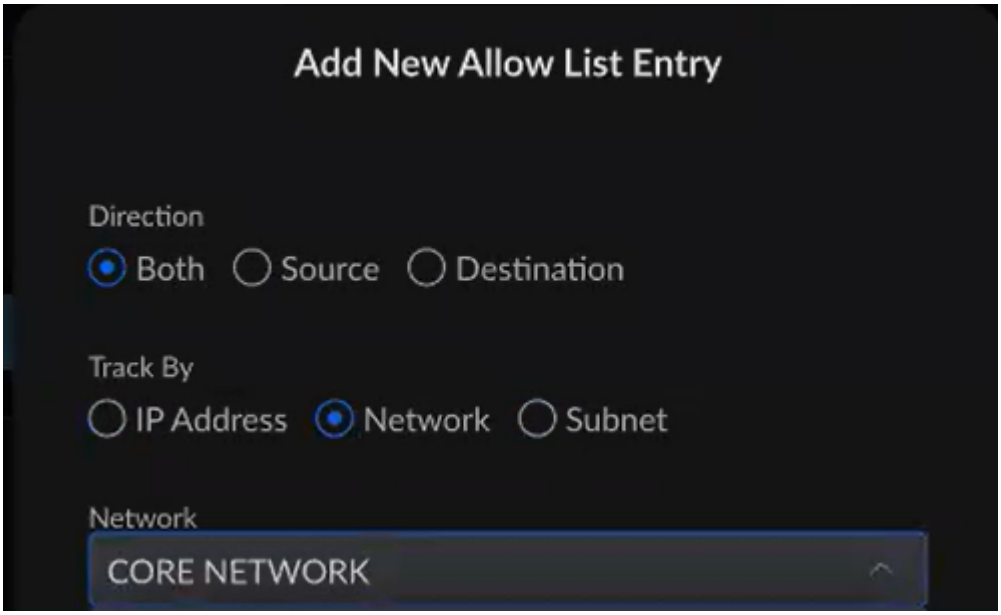
8. If you have enabled IPS/IDS on the UniFi USG firewall, then to establish a tunnel between the Harmony SASE network and UniFi USG firewall version 7 and later, create an exception in your Threat detection system:

a. Click the **Firewall & Security** tab.

b. Click **Create New Allow List**.



c. Select the site-to-site network that you created for this setup.

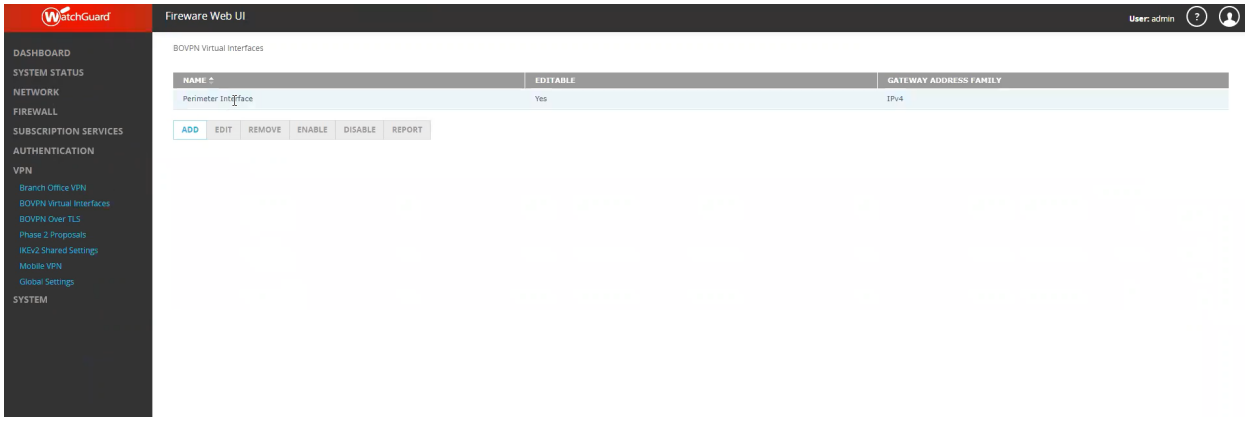


d. Save your changes.

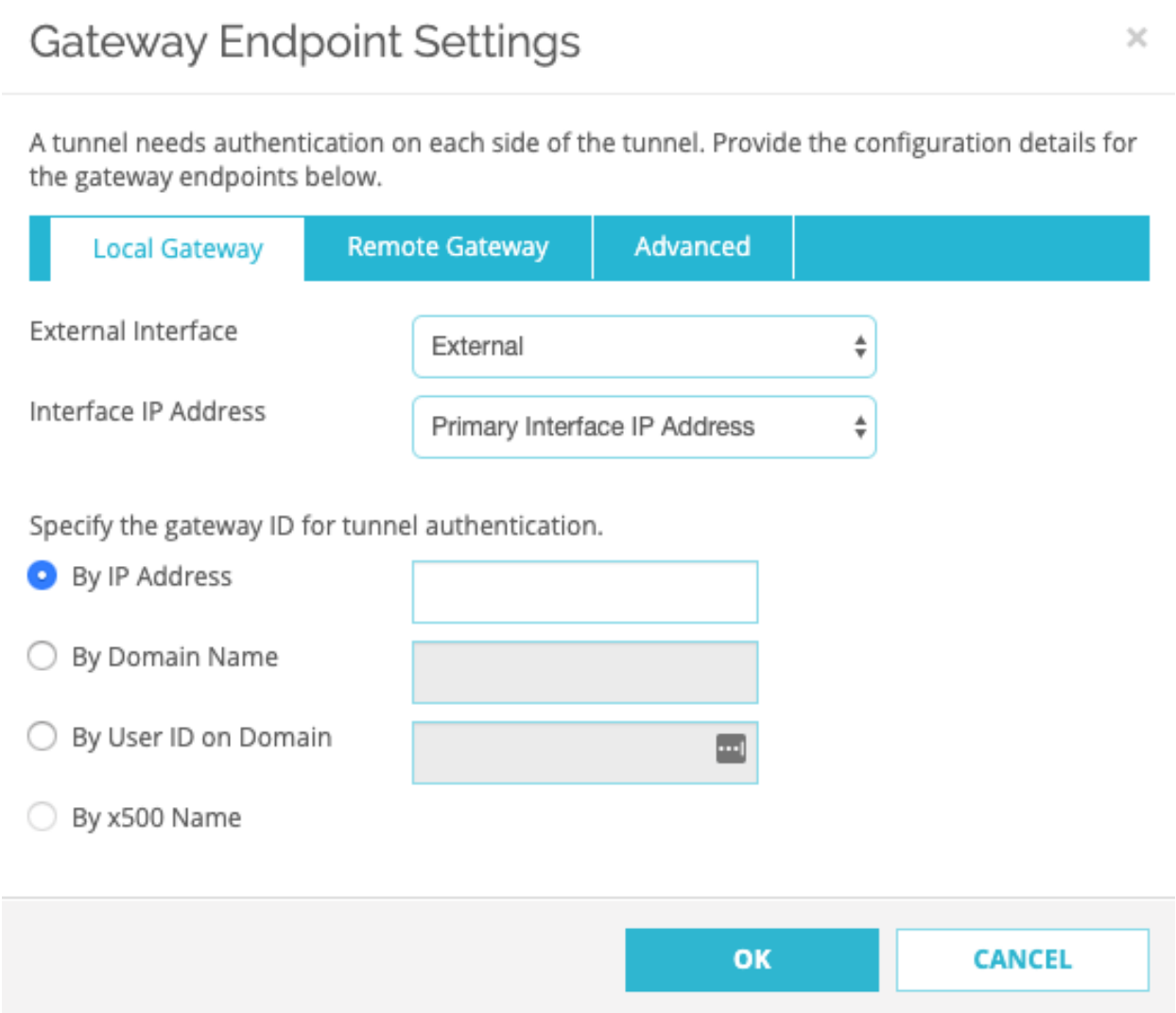
WatchGuard Firewall

To configure the tunnel in the WatchGuard Management Portal:

1. Log in to the WatchGuard Management Portal with the Administrator account.
2. From the left pane, click **VPN > BOVPN Virtual Interfaces**.
3. Click **Add**.



4. In the **Remote Endpoint Type** section, select **Cloud VPN or Third-Party Gateway**.
5. In the **Gateway Address Family** section, select **IPv4 Addresses**.
6. In the **Gateway Settings** section, enter the secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.
7. In the **Local Gateway** tab:

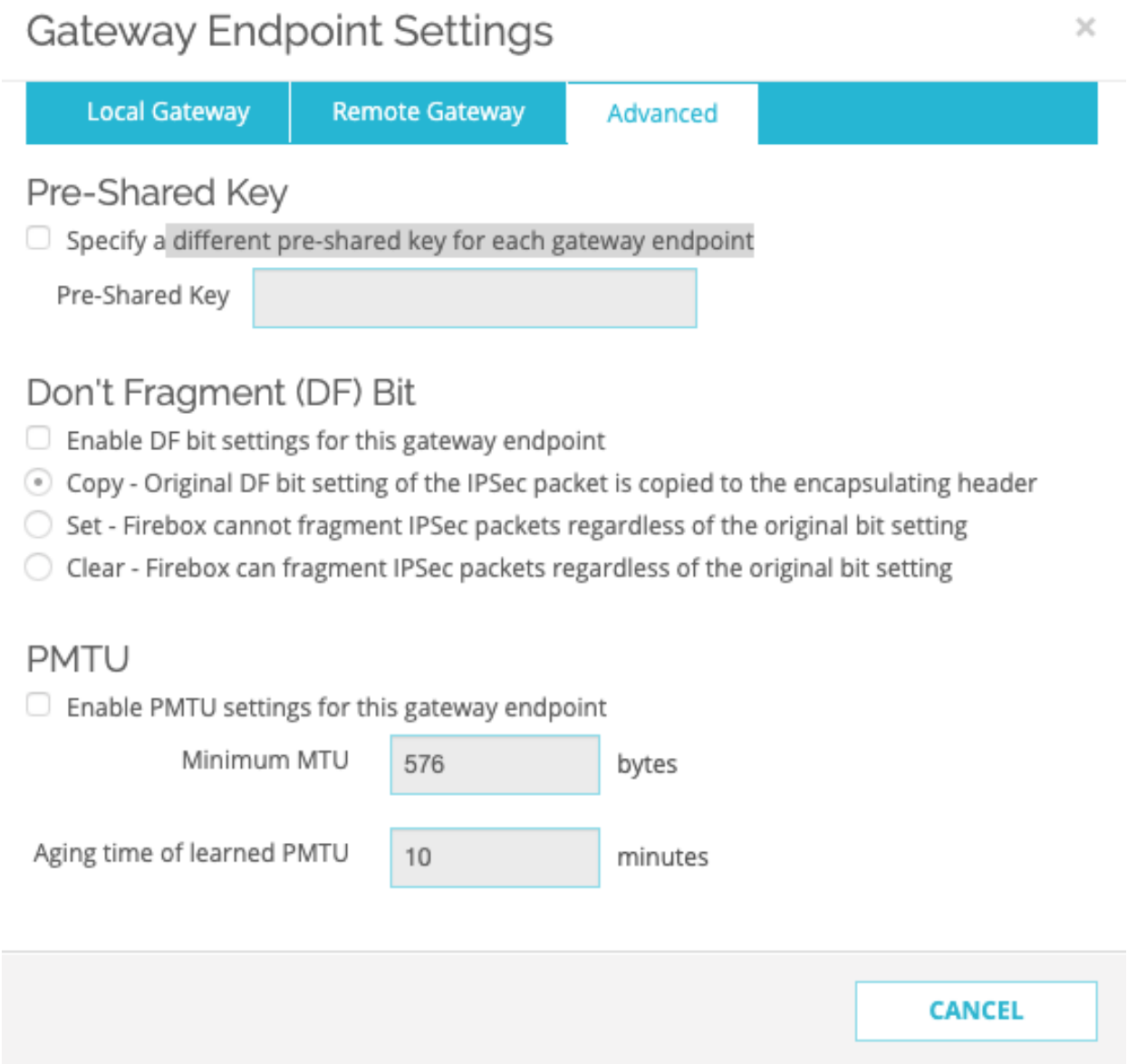


Field	Enter
External Interface	External
Interface IP Address	Primary Interface IP Address
Specify the gateway ID for tunnel authentication	
By IP Address	WatchGuard firewall local IP address.

8. In the **Remote Gateway** tab:

Field	Enter
Static IP Address	WatchGuard firewall IP address.
By IP Address	WatchGuard firewall IP address.

9. In the **Advanced** tab:



Field	Enter
Pre-Shared Key	
Specify a different pre-shared key for each gateway endpoint	Select the checkbox.
Pre-Shared Key	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

Leave rest of the fields with the default values.

10. In the **Phase 1 Settings** tab:

Field	Enter
Version	IKEV2
Mode	Main
NAT Traversal	Select
Keep-alive interval	Select
IKE Keep-alive	30 seconds
Message Interval	30 seconds
Max failures	5
Dead Peer Detection (RFC3706)	Select
Traffic idle timeout	20 seconds
Max retries	5

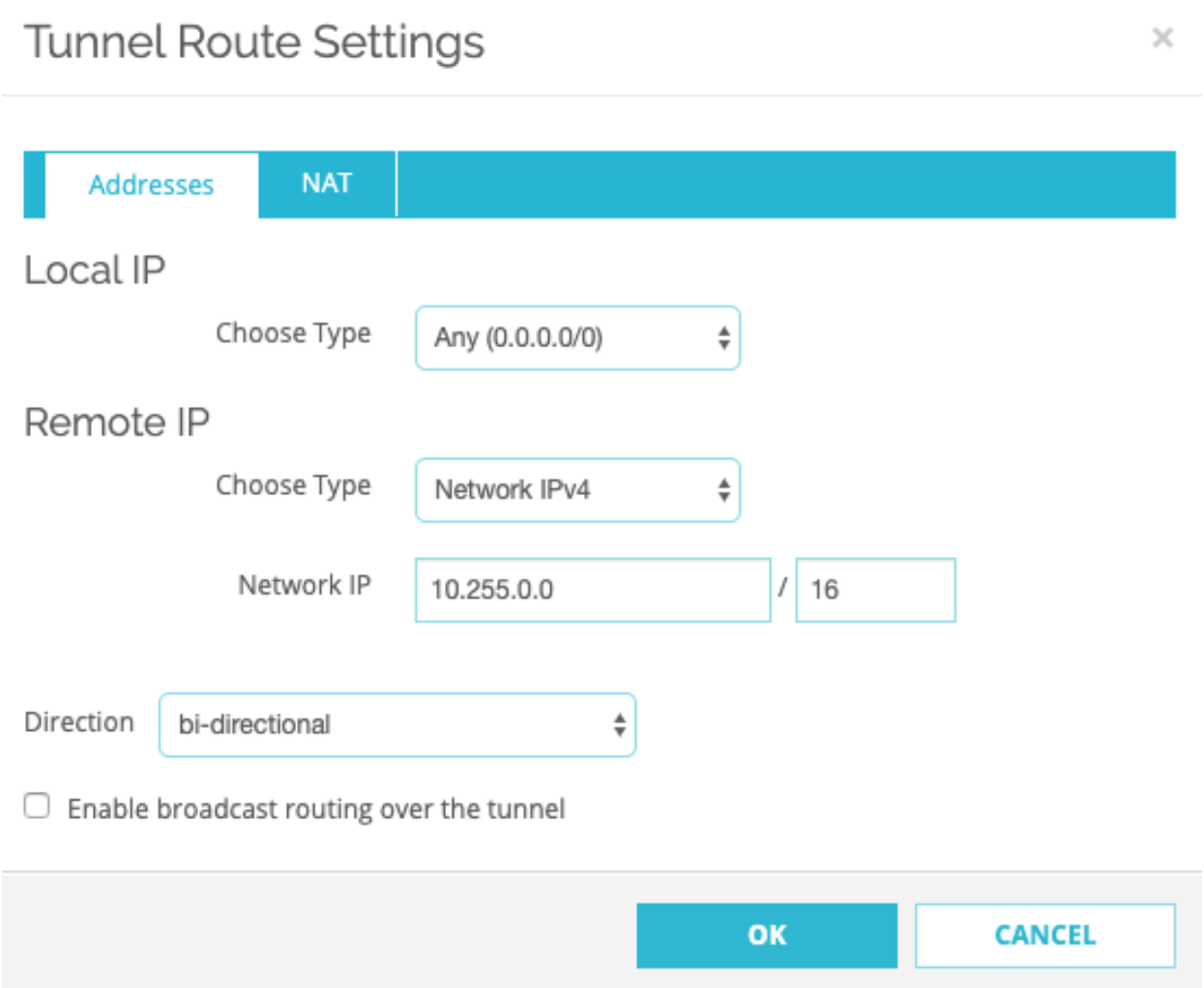
11. Click **OK**.
12. Go to **Transform Settings**, click **Add** and enter these:

Field	Enter
Authentication	SHA2-256
Encryption	AES(256-bit)
SA Life	8 hours
Key Group	Diffie-Hellman Group 14

13. In the **BOVPN Virtual Interfaces** page, in the **Tunnel** section, click **Add** and enter these:

Field	Enter
Name	Name for the tunnel.
Gateway	Firewall that you created for this setup.

14. Go to tab **Addresses** tab, click **Add** and enter these:



Field	Enter
Local IP	ANY (0.0.0.0/0)
Remote IP	Harmony SASE network remote IP address. The default is 10.255.0.0./16.
Direction	bi-directional
Key Group	Diffie-Hellman Group 14

Leave rest of the fields with the default values.

15. Go to **Phase 2 Settings**:

    a. Select the checkbox next to **Enable Perfect Forward Secrecy** next to and select **Diffie-Hellman Group 14**.

b. In the **IPSec Proposals** section, select **ESP-AES256-SHA256** and click **Add**.

   Leave rest of the fields with the default values.

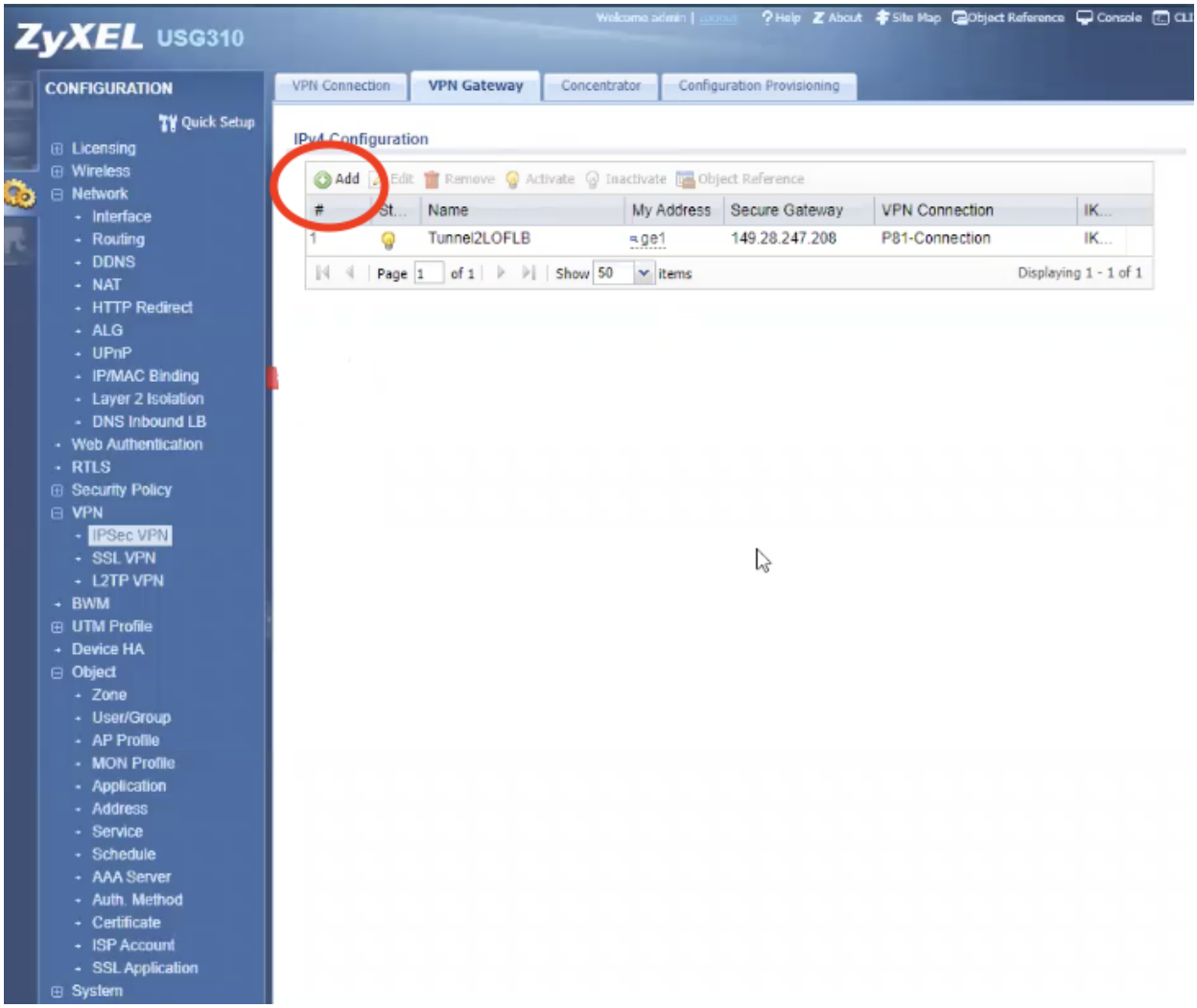
c. Click **Save**.

16. To verify whether the tunnel is up, go to **System Status > VPN Statistics > Branch Office VPN**. If the tunnel is up, the tunnel is listed under **Tunnels**.

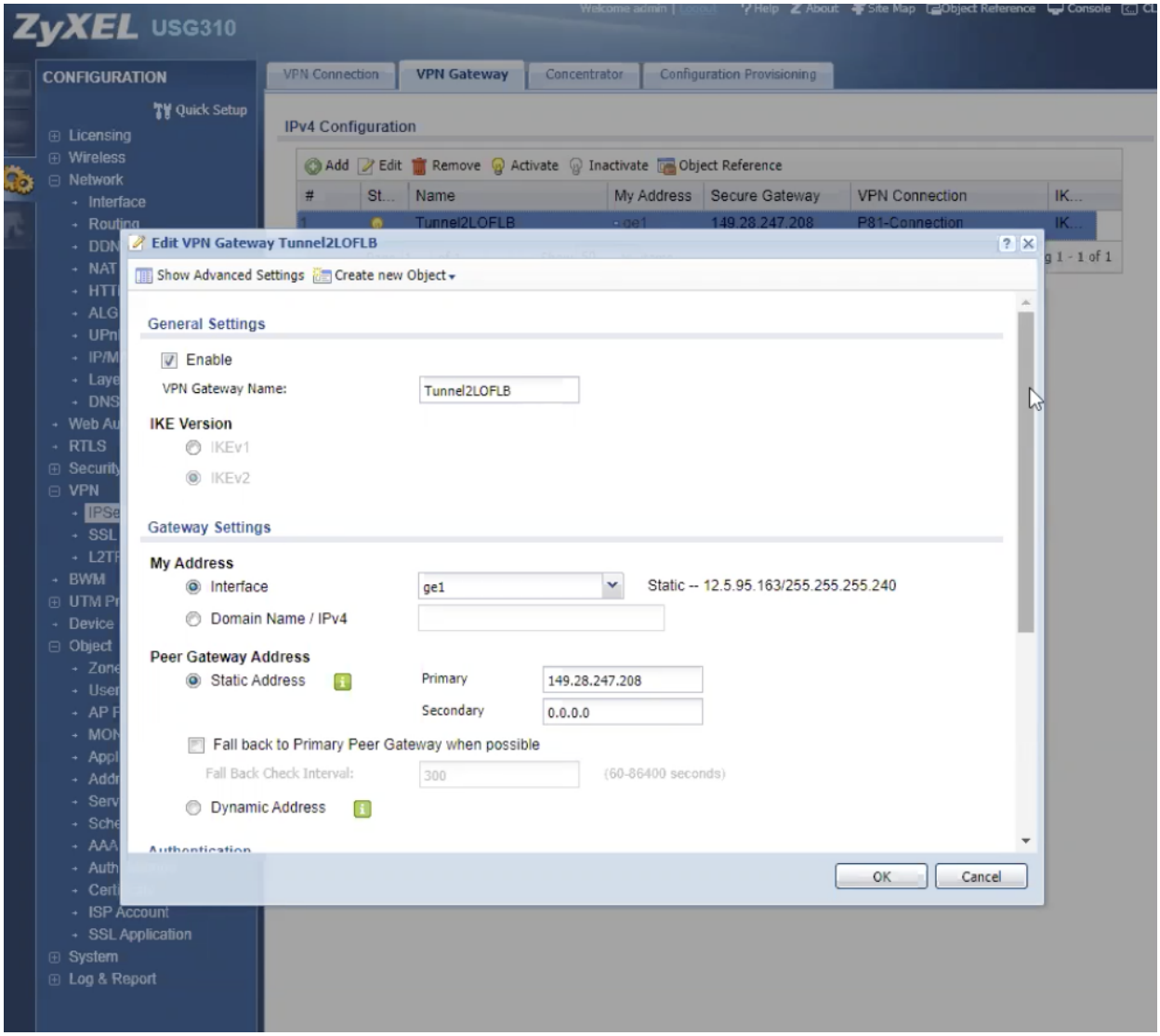
Zyxel USG Firewall

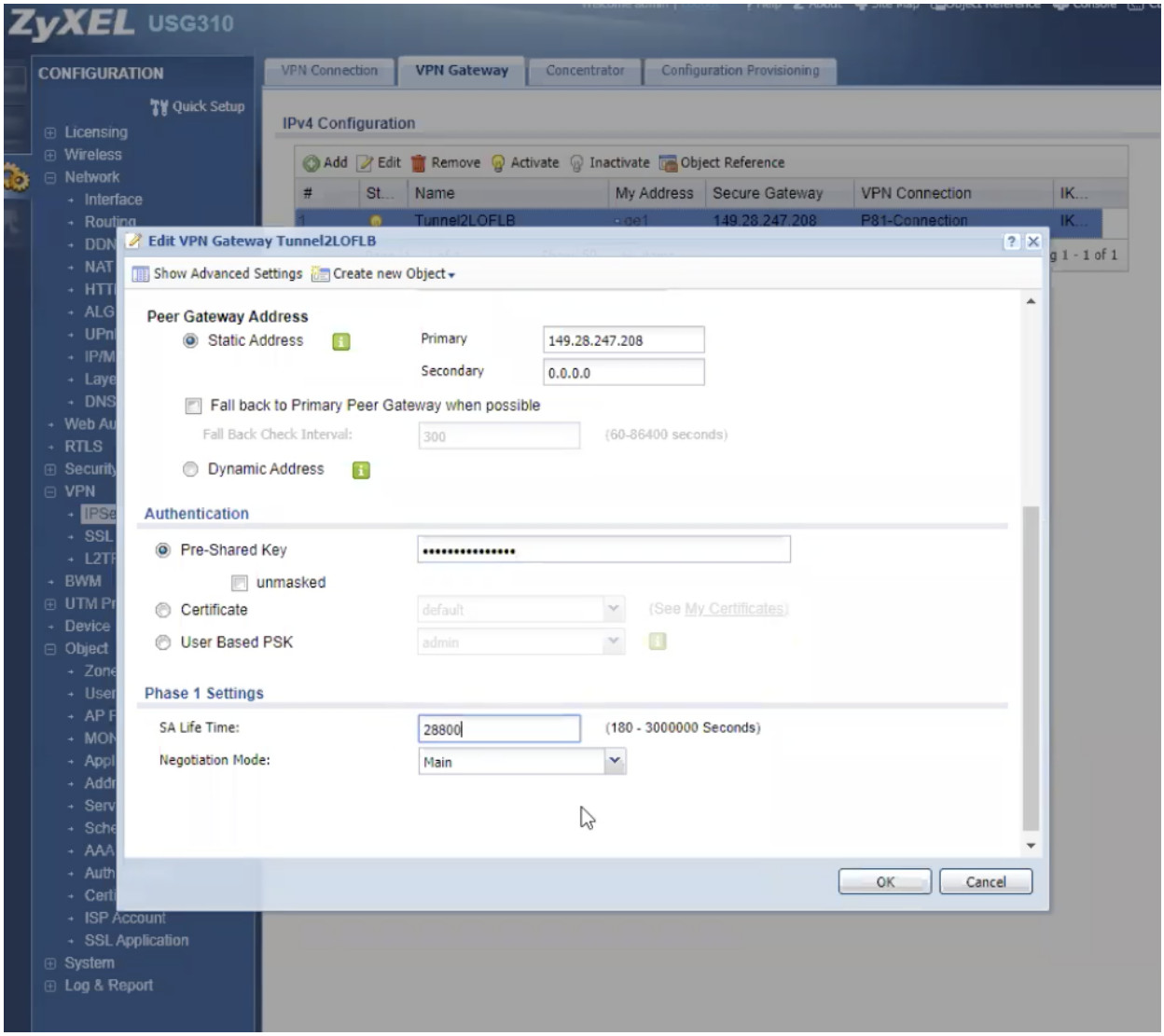
To configure the tunnel in the Zyxel USG Management Portal:

1. Log in to the Zyxel USG Management Portal.
2. Go to **Configuration > VPN > IPSec VPN**.



3. In the **VPN Gateway** tab, click **Add**.
4. In the **General settings** section:
   a. Select the **Enable** checkbox.
   b. In the **VPN Gateway Name** field, enter a name for the gateway.
5. In the **Gateway Settings** section:

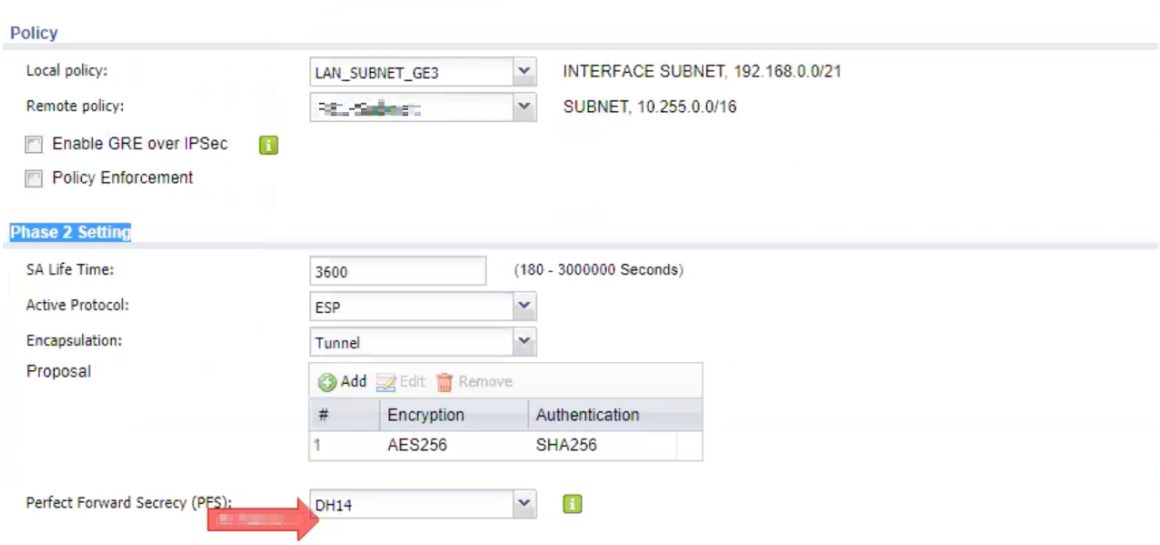

ZyXEL USG310
CONFIGURATION
Quick Setup
Licensing
Wireless
Network
Interface
Routing
VPN
IPSec
SSL
L2TP
BWM
Device
Object
ISP Account
SSL Application
System
Log & Report
VPN Connection
VPN Gateway
Concentrator
Configuration Provisioning
IPv4 Configuration
Add
Edit
Remove
Activate
Inactivate
Object Reference
Name
My Address
Secure Gateway
VPN Connection
Tunnel2LOFLB
149.28.247.208
P81-Connection
Edit VPN Gateway Tunnel2LOFLB
Show Advanced Settings
Create new Object
General Settings
Enable
VPN Gateway Name:
Tunnel2LOFLB
IKE Version
IKEv1
IKEv2
Gateway Settings
My Address
Interface
ge1
Static -- 12.5.95.163/255.255.255.240
Domain Name / IPv4
Peer Gateway Address
Static Address
Primary
149.28.247.208
Secondary
0.0.0.0
Fall back to Primary Peer Gateway when possible
Fall Back Check Interval:
300
(60-86400 seconds)
Dynamic Address
OK
Cancel



Field	Enter
My Address	
Interface	You WAN interface.
Peer gateway Address	
Static Address Primary	Public IP address of Harmony SASE gateway.
Static Address Secondary	0.0.0.0
Authentication	
Pre-Shared Key	Secret key specified in *"Configuring the Tunnel in the Harmony SASE Administrator Portal" on page 171*.

Field	Enter
Phase 1 Settings	
SA Life Time	28800
Negotiation Mode	Main

6. Click **OK**.
7. Add a VPN tunnel:
   a. Go to **Configuration > VPN > IPSec VPN**.
   b. In the **VPN Connection** tab, click **Add**.
   c. Enable and enter a rule name.
   d. Select **Site-to-Site** and select the created VPN gateway.
   e. Set the local policy to your LAN subnet and the remote policy to your Harmony SASE subnet.



   f. Select **Create new Object** and choose **IPv4 Address**.

      Note - Check if the IP address of the remote subnet does not already exist on the local subnet to avoid a double IP address configuration. The remote subnet must match the local subnet to reach the local network.

   g. Select **Show Advanced Settings** and make sure that the **Encryption** and **Authentication** in **Phase 2 Setting** are the same as the **Phase 1 Setting**.

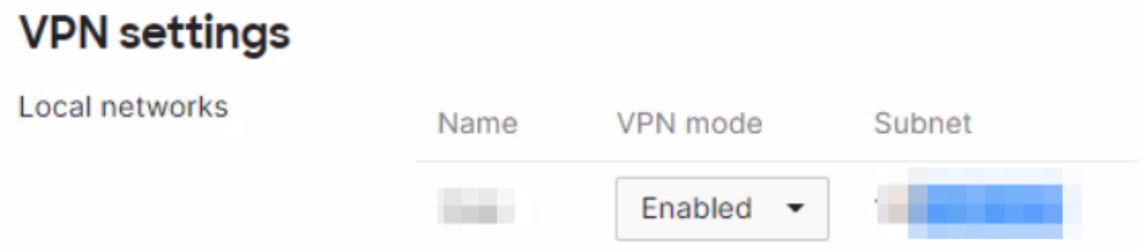
On-premises Router - Configuring the Tunnel in the Management Portal

Harmony SASE supports these on-premises router devices for the IPSec Site-2-Site VPN tunnel connection with the Harmony SASE gateway:

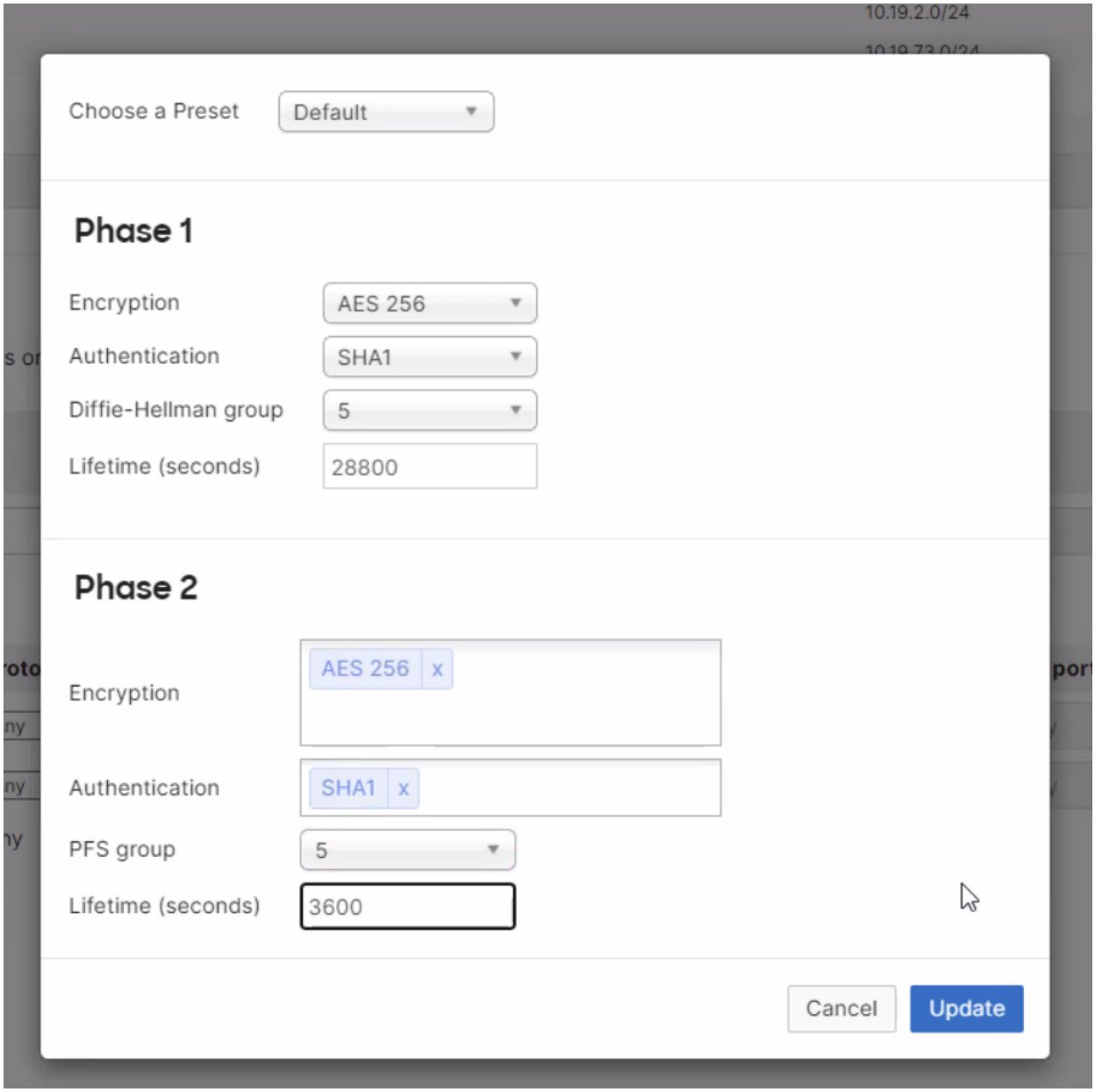
Cisco Meraki Router

To configure the tunnel in the Cisco Meraki Management Portal:

1. Log in to the Cisco Meraki Management Portal with the Administrator account.
2. Go to **Security Appliance > Configure > Site-to-site VPN**.
3. Make sure that the local LAN you want t connect from the Harmony SASE network is participating in the VPN.



4. Scroll down to the **Non-Meraki VPN peers** section.
5. Click **Add a peer**:



Field	Enter
Name	Name for the remote device or VPN.
IKE Version	IKEv1
Public Ip	Public IP address of the Harmony SASE gateway.
Remote ID	Public IP address of the Harmony SASE gateway.
Private subnets	Harmony SASE network subnets. Default is 10.255.0.0/16.
Preshared secret key	Secret key specified in the Harmony SASE Administrator Portal.

Field	Enter
IPsec Policy to use	Custom
Phase 1	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	28800
Phase 2	
Encryption	AES-256
Authentication	SHA1
Diffie-Hellman group	5
Lifetime (seconds)	3600

6. Click **Update**.
7. Edit the router rules to allow the traffic through the Harmony SASE tunnel. These rules apply to inbound and/or outbound VPN traffic from all MX appliances in the organization that participate in site-to-site VPN.

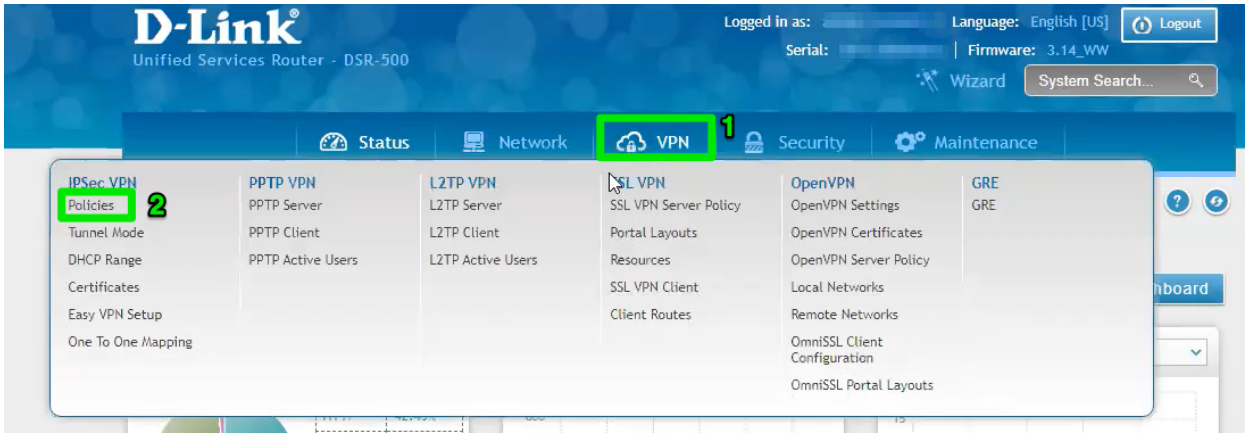
   To create a rule, got to **Security Appliance > Configure > Site-to-site VPN**, in the **Site-to-site firewall** section, select **Add a rule**.

   For reference, see the Layer 3 firewall rules.

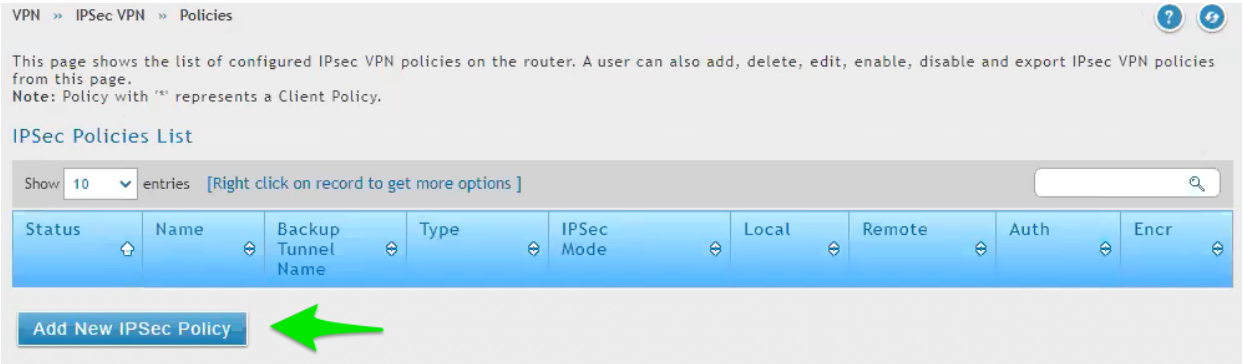
D-Link DSR Series Router

To configure the tunnel in the D-Link DSR Series Router Management Portal:

1. Log in to the D-Link DSR Series Router Management Portal with the Administrator.
2. Click **VPN**.



3. Click **IPSec VPN > Policies**.
4. Click **Add New IPSec Policy**.



5. In the **General** section:

IPSec Policy Configuration

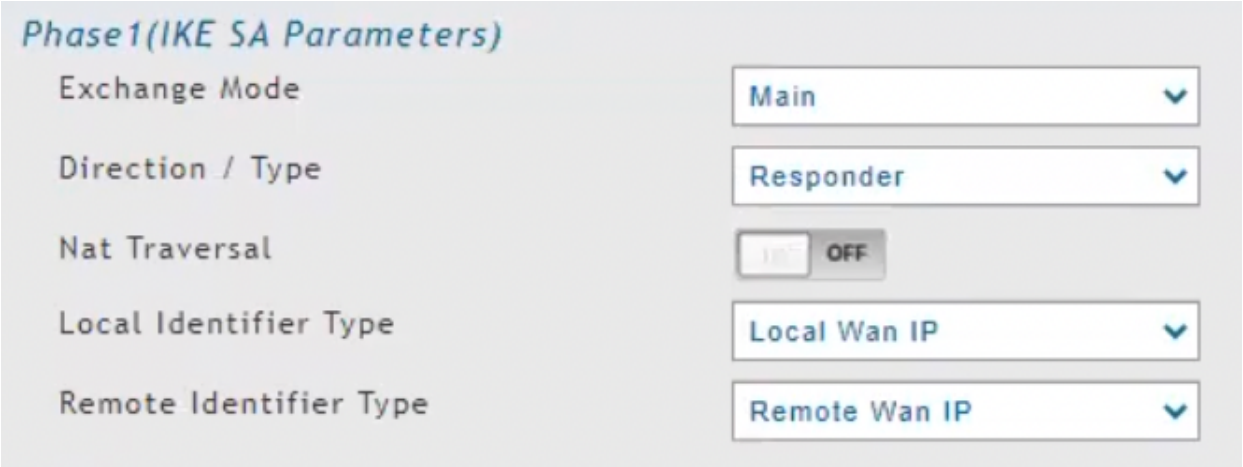
General

Policy Name	
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local Gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address / FQDN	
Enable Mode Config	OFF

Enable NetBIOS	OFF
Enable RollOver	OFF
Protocol	ESP
Enable DHCP	OFF
Local IP	Subnet
Local Start IP Address	192.168.1.0
Local Subnet Mask	255.255.255.0
Remote IP	Subnet
Remote Start IP Address	10.255.0.0
Remote Subnet Mask	255.255.0.0
Enable Keepalive	OFF

Field	Enter
Policy Name	Name for the policy.
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address/FQDN	Public IP address of the Harmony SASE gateway.
Enable Config Mode	Off
Enable NetBIOS	Off
Enable RollOver	Off
Protocol	ESP
Enable DHCP	Off
Local IP	Subnet
Local Start IP Address	Your local subnet
Local Subnet Mask	Matching subnet mask
Remote IP	Subnet
Remote Start IP Address	10.255.0.0
Remote Subnet Mask	255.255.0.0
Enable Keepalive	Off

6. In the **Phase1 (IKE SA Parameters)** section:



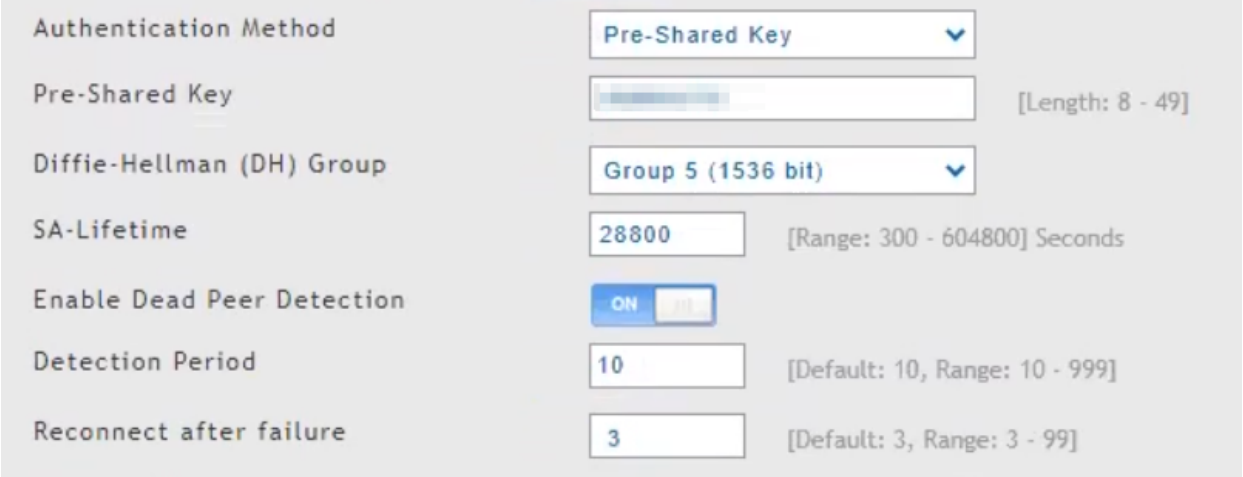
Field	Enter
Exchange Mode	Main
Direction/Type	Responder
NAT Traversal	Off
Local Identifier Type	Local Wan IP
Remote Identifier Type	Remote Wan IP

7. In the **Encryption Algorithm** section:

Field	Enter
DES	Off
AES-128	Off
AES-256	On
Blowfish	Off

Field	Enter
3DES	Off
AES-192	Off

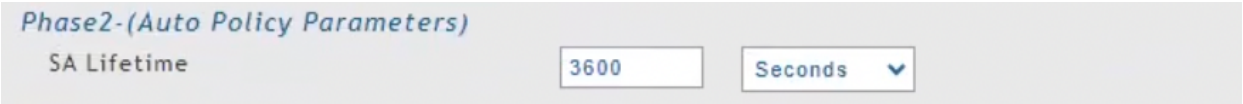
8. In the **Authentication Algorithm** section:



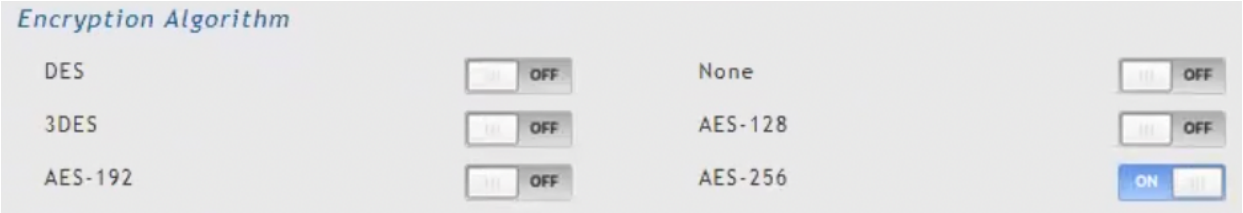
Field	Enter
MD5	Off
SHA2-256	Off
SHA2-512	On
Authentication Method	Pre-Shared Key
Pre-Shared Key	Secret key specified in the Harmony SASE Administrator Portal.
Diffie-Hellman (DH) Group	Group 5
SA-Lifetime	28800

Field	Enter
Enable dead Peer Detection	On
Detection Period	10
Reconnect after failure	3

9. In the **Phase2 - (Auto Policy Parameters)** section, in the **SA Lifetime** field, enter **3600 seconds**.



10. In the **Encryption Algorithm** section:



Field	Enter
DES	Off
3DES	Off
AES-192	Off
None	Off
AES-128	Off
AES-256	On

11. In the **Integrity Algorithm** section:

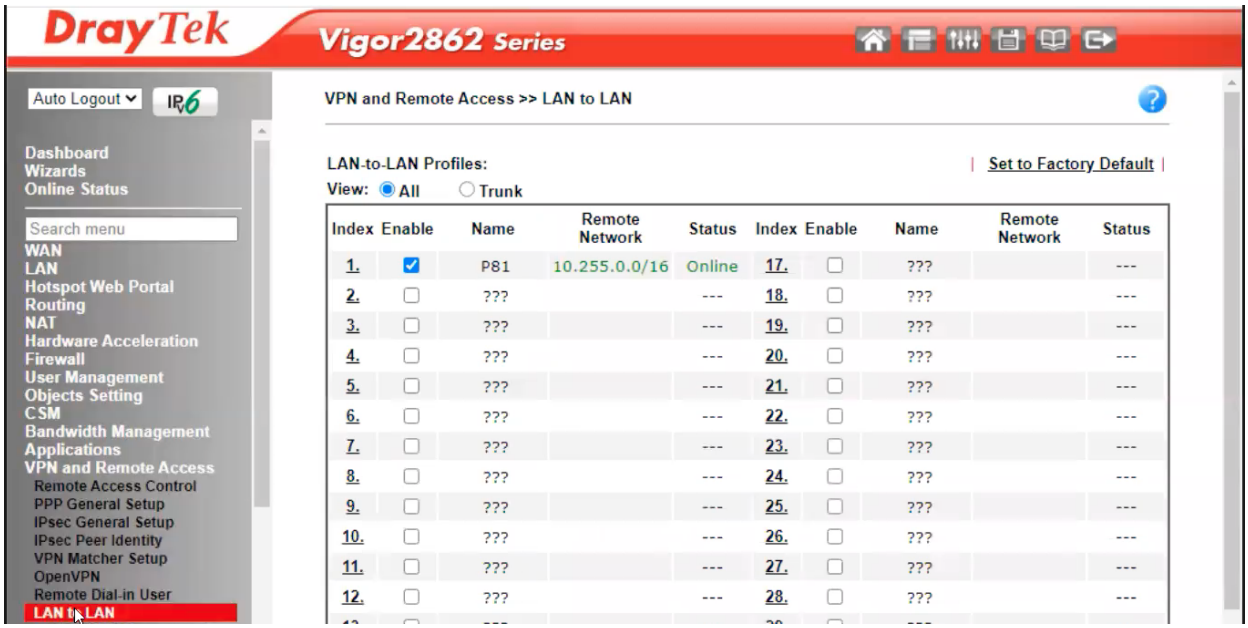
Field	Enter
MD5	Off
SHA-224	Off
SHA2-384	Off
PFS Key Group	On
SHA-1	Off
SHA2-256	Off
SHA2-512	On

12. Click **Save**.

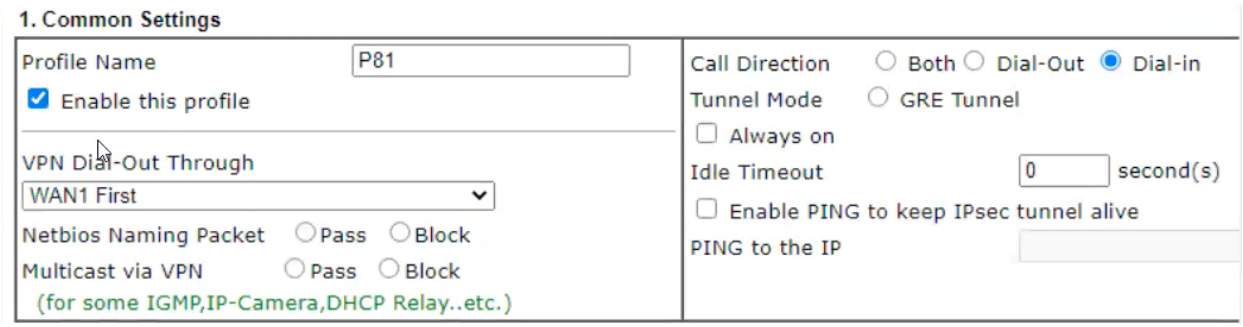
DrayTek Vigor2862 Router

To configure the tunnel in the DrayTek Vigor2862 Management Portal:

1. Log in to the DrayTek Vigor2862 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **LAN to LAN** and create a new profile.



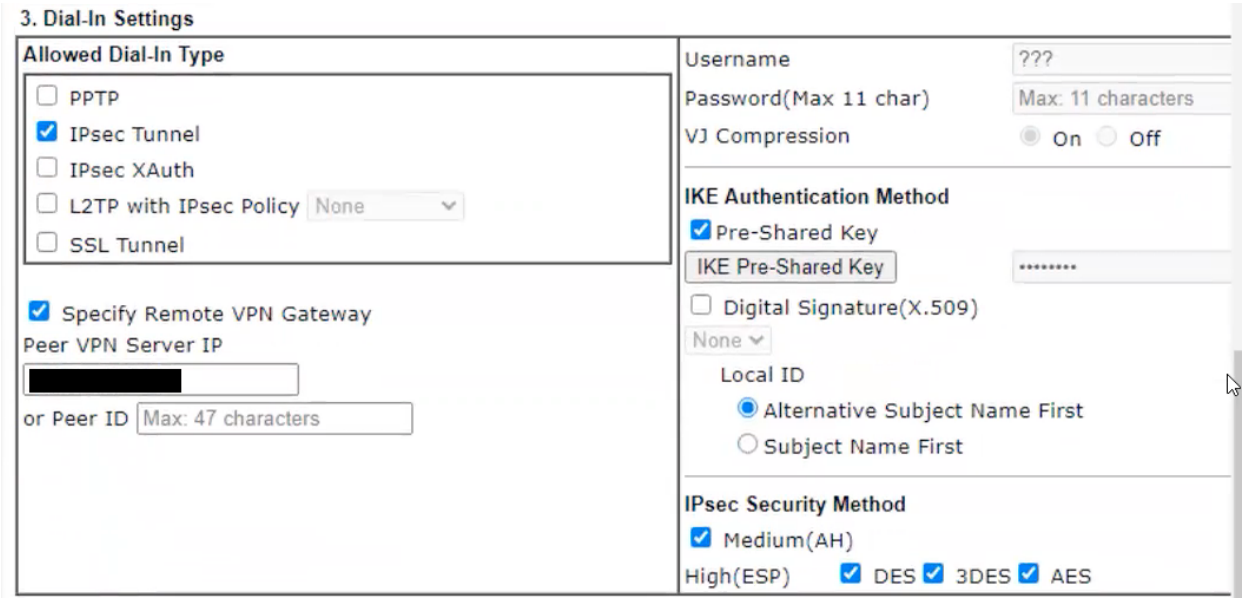
4. In the **Custom Settings** tab:

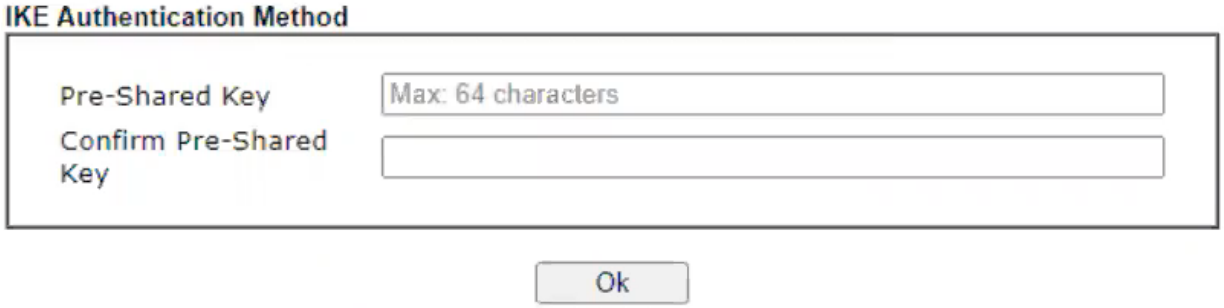


Field	Enter
Profile Name	Name for the profile. For example, Harmony SASE.
Enable this profile	Select
VPN Dial-Out Through	Your WAN interface.
Call Direction	Dial-in

Field	Enter
Idle Timeout	0

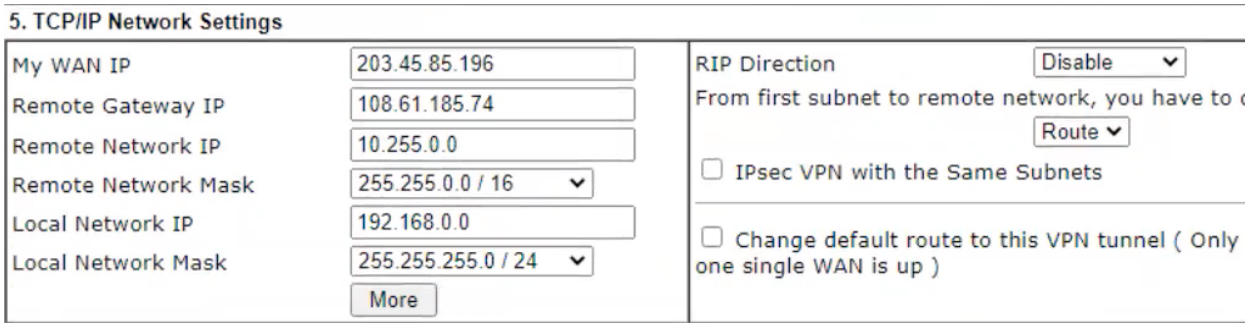
5. In the **Dial-In Settings**tab:





Field	Enter
Allowed Dial-In Type	IPsec Tunnel
Specify Remote VPN Gateway	Public IP address of the Harmony SASE gateway.
Pre-Shared Key	Select and click **IKE Pre-Shared Key** and enter the secret key specified in the Harmony SASE Administrator Portal.

6. In the **TCP/IP Network Settings** tab:

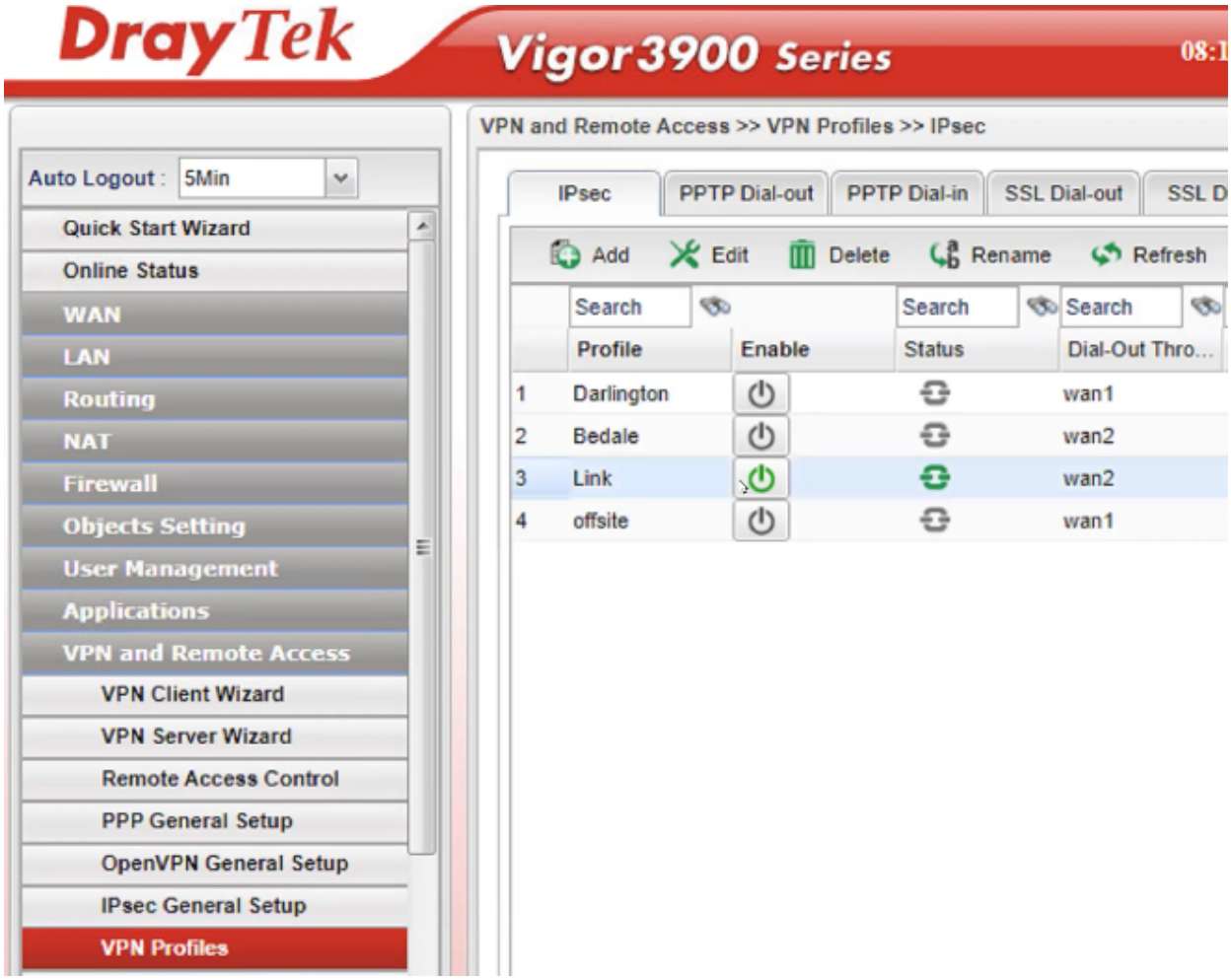


Field	Enter
My WAN IP	Your WAN interface's default IP address.
Remote Gateway IP	Public IP address of the Harmony SASE gateway.
Remote Network IP	Harmony SASE network subnet.
Local Network IP	Your LAN subnnet.

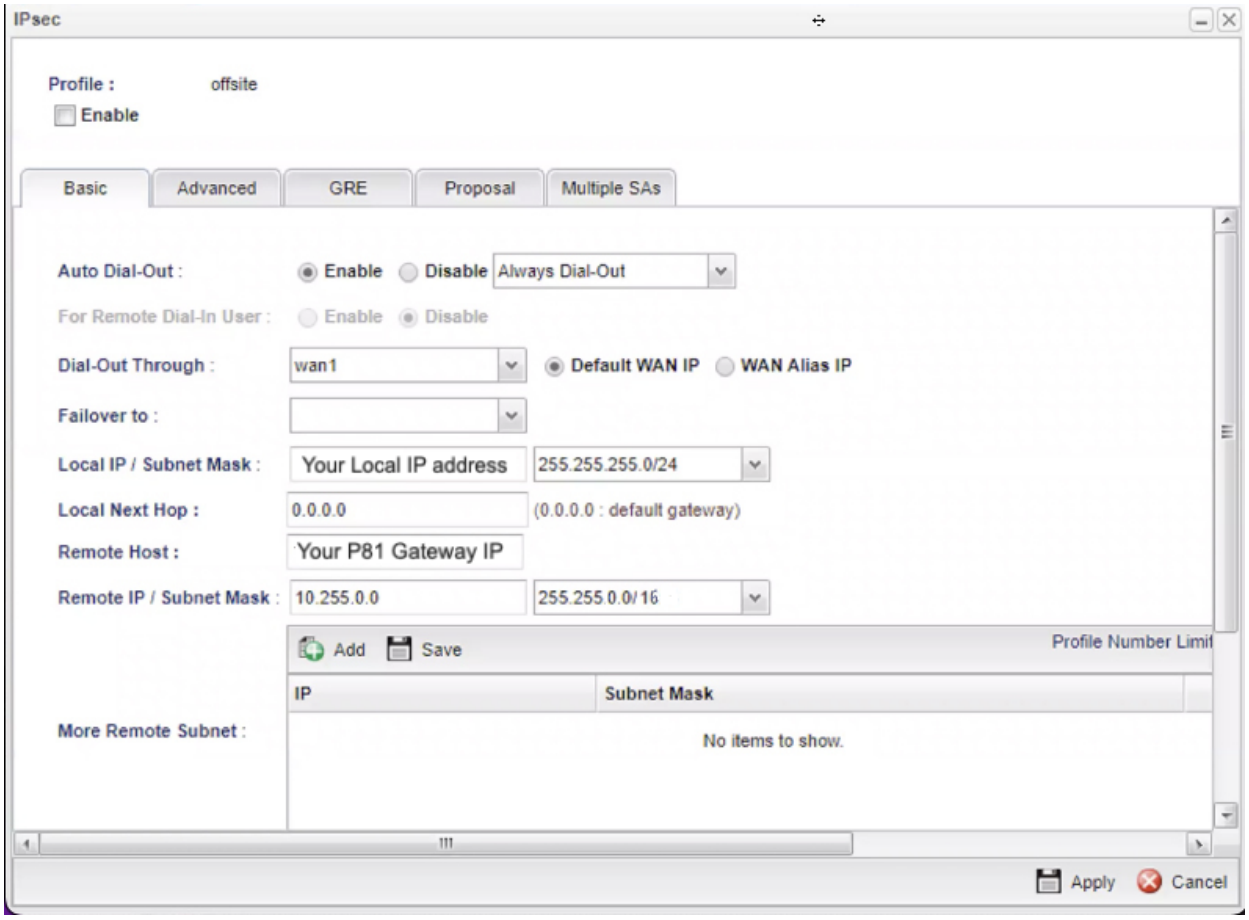
DrayTek Vigor3900 Router

To configure the tunnel in the DrayTek Vigor3900 Management Portal:

1. Log in to the DrayTek Vigor3900 Management Portal with the Administrator account.
2. From the left panel, go to **VPN and Remote Access**.
3. Click **VPN Profiles** and click **Add**.



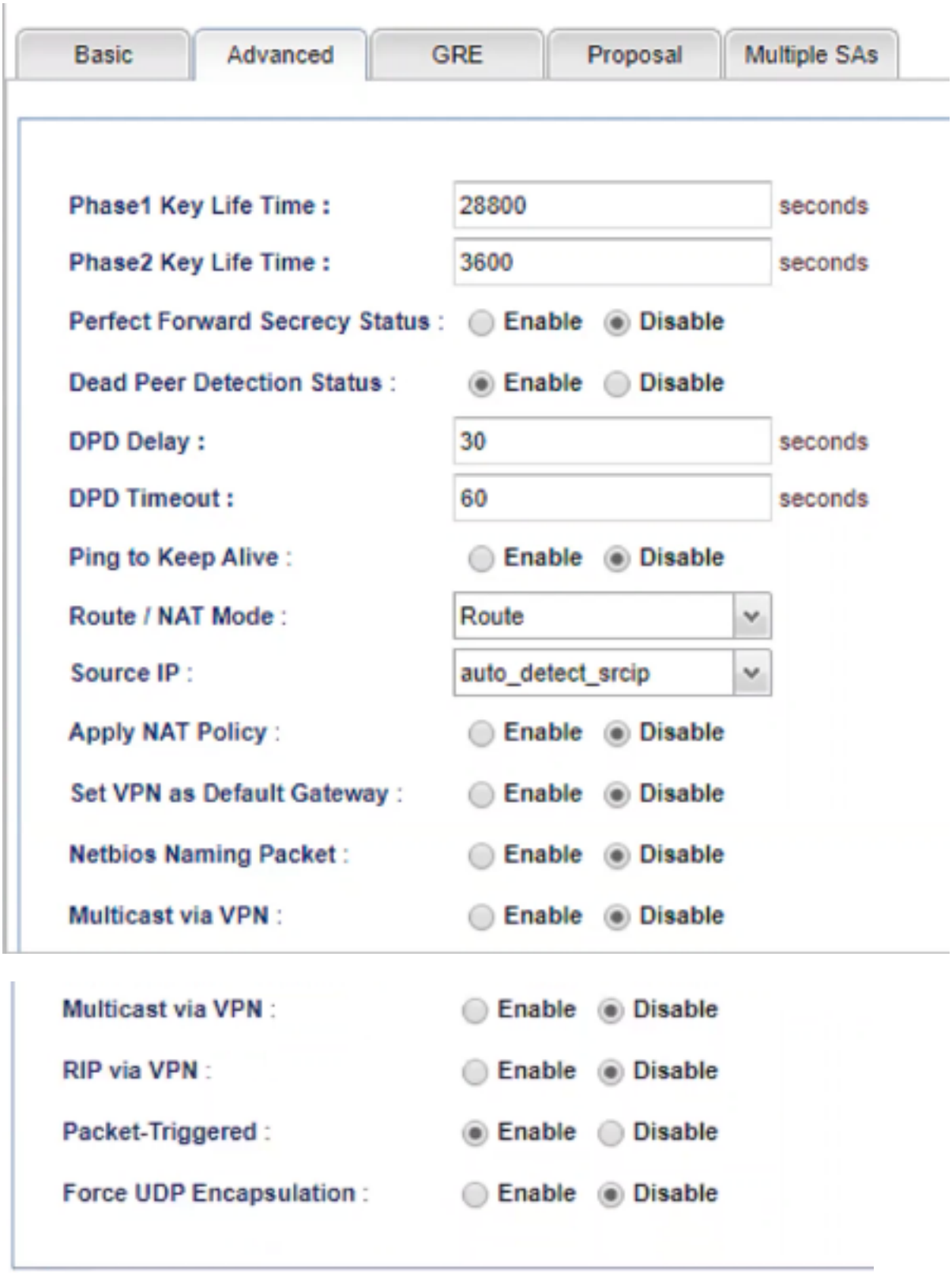
4. In the **Basic** tab:



Field	Enter
Auto Dial-Out	Enable; Always Dial-Out
Dial-Out Through	Your WAN interface; Default WAN IP
Failover	Blank
Local IP / Subnet Mask	Your router external IP address and subnets.
Remote Host	Public IP address of the Harmony SASE gateway.

Field	Enter
Remote IP / Subnet Mask	Default is 10.255.0.0 and 255.255.0.0/16. If you modified these in the Harmony SASE Administrator Portal, enter the modified values.
IKE Protocol	IKEv1
IKE Phase 1	Main Mode
Auth Type	PSK
Pre-shared Key	Secret key specified in the Harmony SASE Administrator Portal.
Security Protocol	ESP

5. In the **Advanced** tab:



Field	Enter
Phase 1 Key Lifetime	28800 seconds

Field	Enter
Phase 2 Key Lifetime	3600 seconds
Perfect Forward Secrecy Status	Enable
DPD Status	Enable
DPD Delay	30 seconds
DPD Timeout	60 seconds
Ping to Keep Alive	Disable
Route/NAT Mode	Route
Source IP	Auto-detect
Apply NAT Policy	Disable
Set VPN Default Gateway	Disable
Netbios Naming Packet	Disable
Multicast via VPN	Disable
RIP via Triggered	Enable
Packet Triggered	Enable
Force UDP Encapsulation	Disable

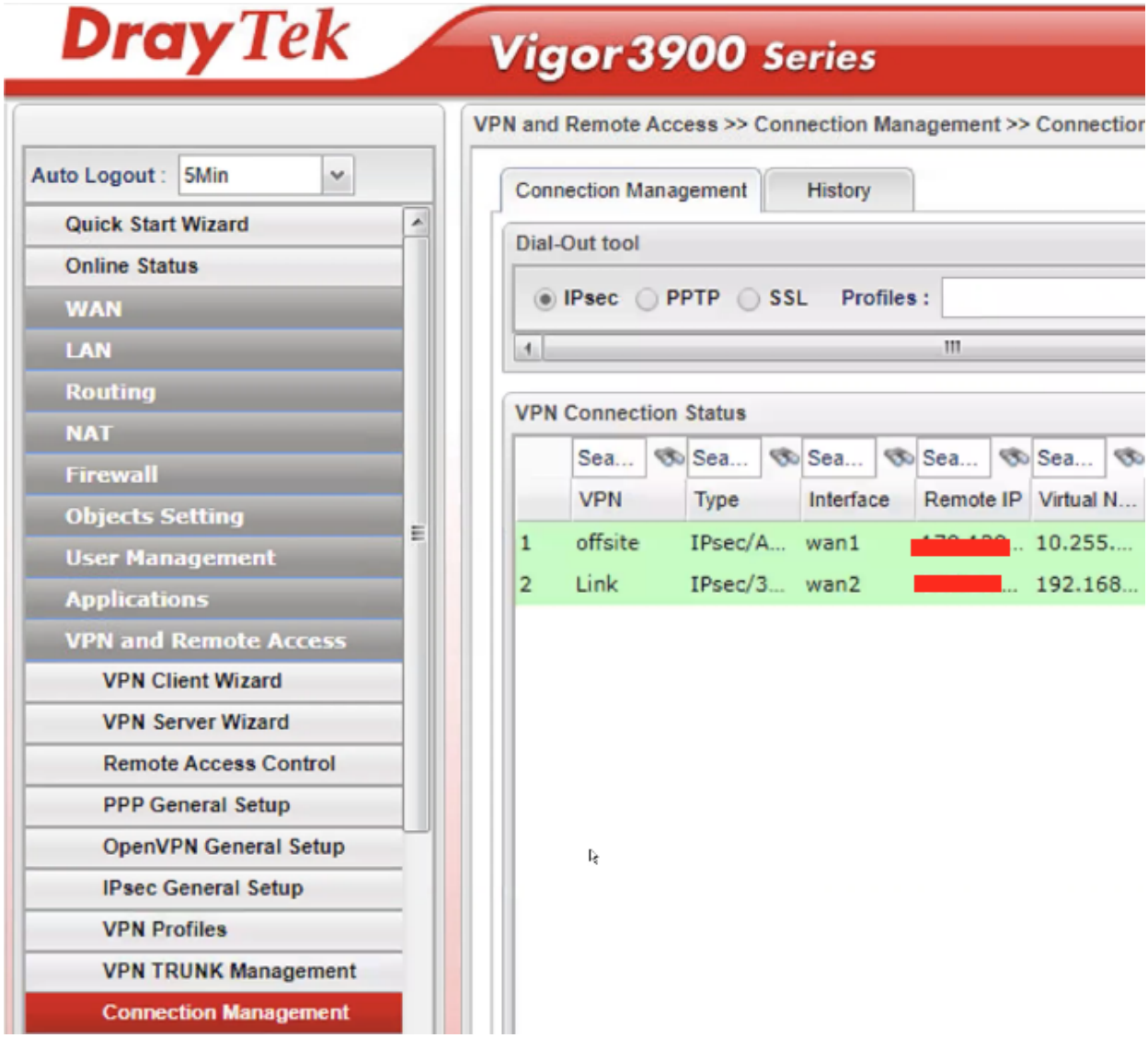
6. In the **GRE** tab:

Field	Enter
Enable GRE Function	Disable
Auto Generate GRE Key	Enable

7. In the **Proposal** tab:

Field	Enter
IKE Phase 1 Proposal	AES 256 G2
IKE Phase 1 Authentication	SHA1
IKE Phase 2 Proposal	AES 256 with auth
IKE Phase 2 Authentication	SHA1
Accepted Proposal	Accept

8. Click **Apply**.
9. To verify if the tunnel is up, from the left pane, click **Connection Management** and check if the profile is listed and highlighted in Green.


DrayTek
Vigor3900 Series
VPN and Remote Access >> Connection Management >> Connectior
Auto Logout : 5Min
Quick Start Wizard
Online Status
WAN
LAN
Routing
NAT
Firewall
Objects Setting
User Management
Applications
VPN and Remote Access
VPN Client Wizard
VPN Server Wizard
Remote Access Control
PPP General Setup
OpenVPN General Setup
IPsec General Setup
VPN Profiles
VPN TRUNK Management
Connection Management
Connection Management
History
Dial-Out tool
IPsec
PPTP
SSL
Profiles :
VPN Connection Status
VPN
Type
Interface
Remote IP
Virtual N...
1
offsite
IPsec/A...
wan1
10.255....
2
Link
IPsec/3...
wan2
192.168...

EdgeMax Router

To configure the tunnel in the EdgeMax Router through CLI:

1. Connect to the router through SSH and then enter the configuration mode. For example, using PuTTY.
2. Enable the **auto-firewall-nat-exclude** feature which automatically creates the IPsec firewall/NAT policies in the iptables firewall. Run:

```
set vpn ipsec auto-firewall-nat-exclude enable
```

3. Create IKE / Phase 1 (P1) Security Associations (SAs). Run:

```
set vpn ipsec ike-group FOO0 lifetime 28800
set vpn ipsec ike-group FOO0 proposal 1 dh-group 14
set vpn ipsec ike-group FOO0 proposal 1 encryption aes256
set vpn ipsec ike-group FOO0 proposal 1 hash sha1
set vpn ipsec ike-group FOO0 dead-peer-detection interval 15
set vpn ipsec ike-group FOO0 dead-peer-detection timeout 30
```

4. Create the ESP / Phase 2 (P2) SAs and enable Perfect Forward Secrecy (PFS). Run:

```
set vpn ipsec esp-group FOO0 lifetime 3600
set vpn ipsec esp-group FOO0 pfs enable
set vpn ipsec esp-group FOO0 proposal 1 encryption aes256
set vpn ipsec esp-group FOO0 proposal 1 hash sha1
```

5. Define the remote peering address. Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication mode pre-shared-secret
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
authentication pre-shared-secret <secret key from Quantum SASE
Administrator Portal>
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
description ipsec
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
local-address <Your Edgerouter WAN IP>
```

6. Link the SAs created above to the remote peer and bind the VPN to a virtual tunnel interface (vti0). Run:

```
set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
ike-group FOO0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti bind vti0
 set vpn ipsec site-to-site peer <Your Perimeter81 Gateway IP>
vti esp-group FOO0
```

7. Configure the virtual tunnel interface (vti0) and assign an internal IP address that is not used in any site. Run:

```
set interfaces vti vti0 address 192.168.20.20/32
```

8. Create a static route for the Harmony SASE subnet (the default is 10.255.0.0/16). Run:

```
set protocols static interface-route 10.255.0.0/16 next-hop-
interface vti0
```

9. Commit the changes and save the configuration. Run:

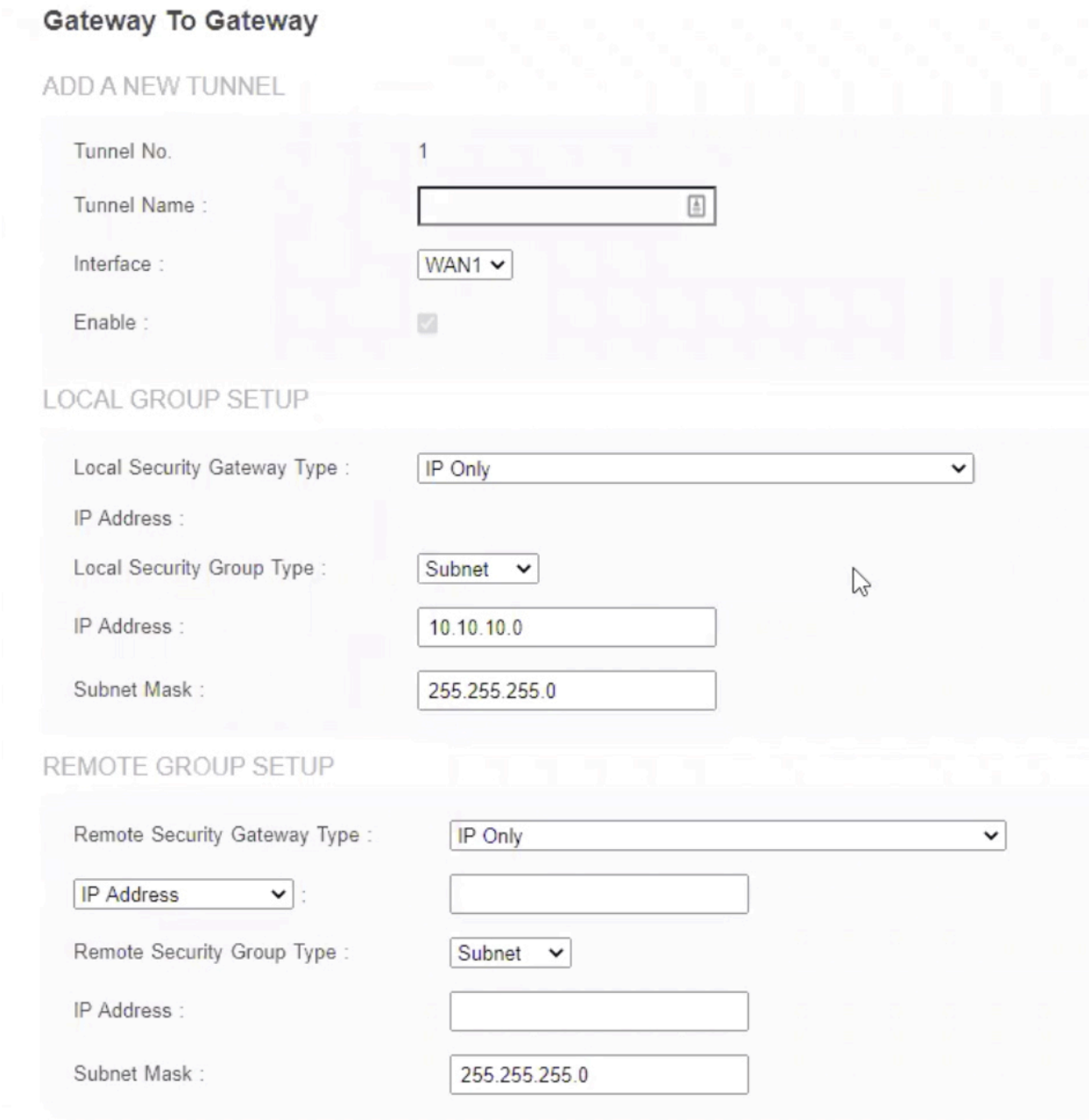
```
commit ; save
```

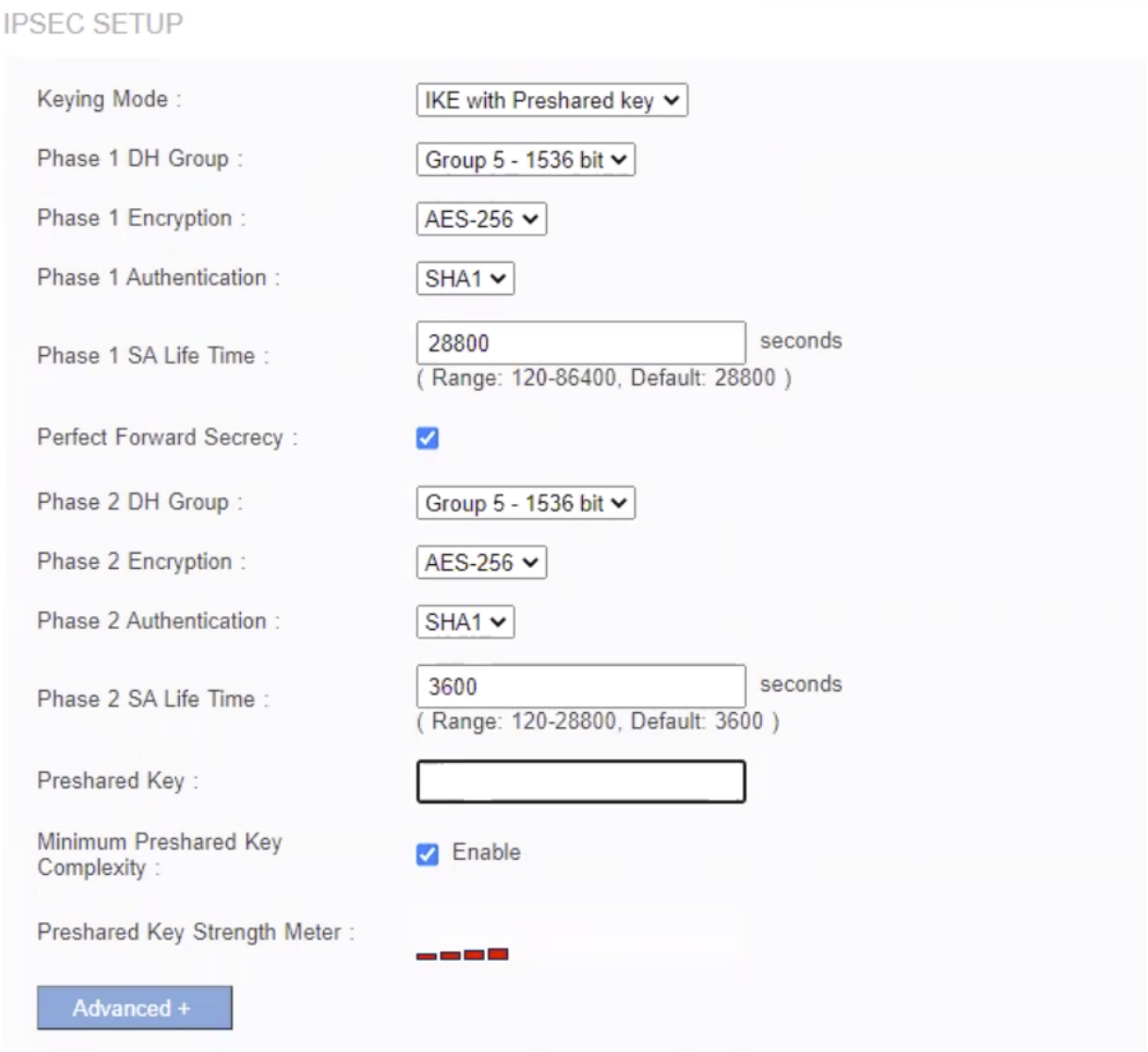
10. In the EdgeMax Management portal, go **VPN - site to site connection**.
11. Verify that the peer associated with the gateway IP address obtained from Harmony SASE has:
    - **Remote subnet**: 10.255.0.0/16 (or the local Harmony SASE gateway that you selected)
    - **Local subnet**: All the subnet range (CIDR) of your LAN devices

Linksys Router

To configure the tunnel in the Linksys Management Portal:

1. Log in to the Linksys Management Portal with the Administrator account.
2. From the left panel, go to **VPN > Gateway to Gateway**.



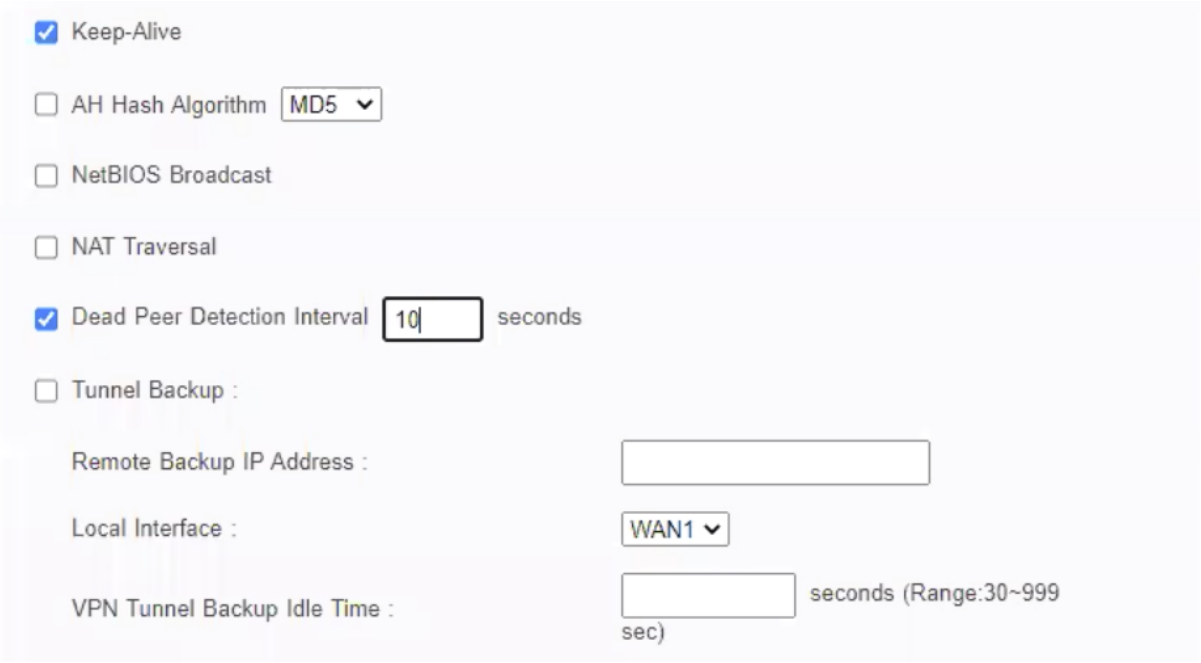


3. Enter these:

Field	Enter
Add a New Tunnel	
Tunnel Name	Name for the tunnel.
Interface	WAN1
Local Group Setup	
Local Security Gateway Type	IP Only
IP Address	Linksys external IP address.

Field	Enter
Local Security Group Type	Subnet
IP Address	Linksys local IP address.
Subnet Mask	Linksys subnet mask.
Remote Group Setup	
Remote Security Gateway Type	IP Only
IP Address	Public IP address of Harmony SASE gateway.
Remote Security group Type	Subnet
IP Address	10.255.0.0
Subnet Mask	255.255.0.0
IPSec Setup	
Keying Mode	IKE with PSK
Phase 1 DHG	Group 5
Phase 1 Encryption	aes256
Phase 1 Authentication	sha1
Phase 1 SA Lifetime	28800
Perfect Forward Secrecy	Selected
Phase 2 DHG	Group 5
Phase 1 Encryption	aes256
Phase 2 Authentication	sha1
Phase 2 SA Lifetime	3600
Preshared Key	Secret key specified in the Harmony SASE Administrator Portal.

4. Click **Advanced**:



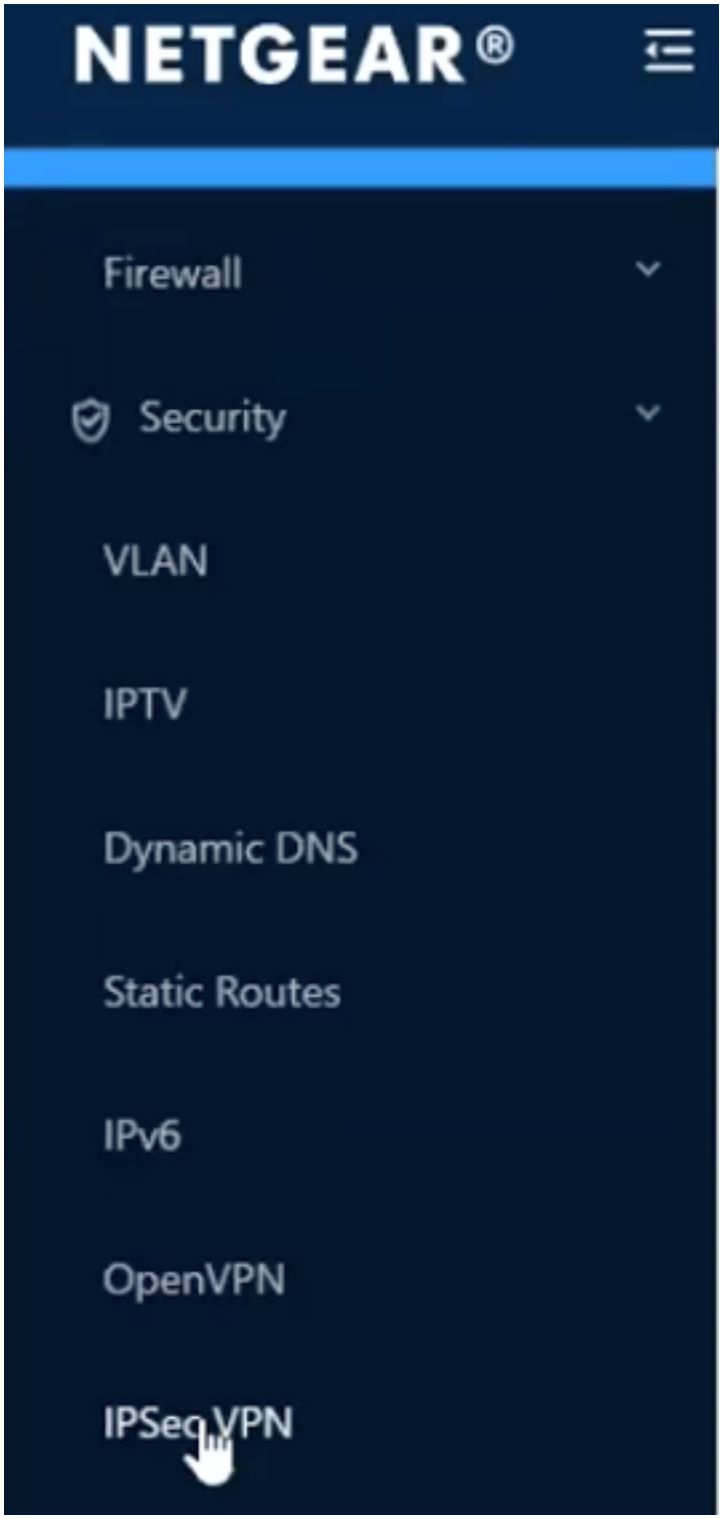
a. Select the **Keep-Alive** checkbox.

b. Select the **Dead Peer Detection Interval** checkbox and enter **10** seconds.

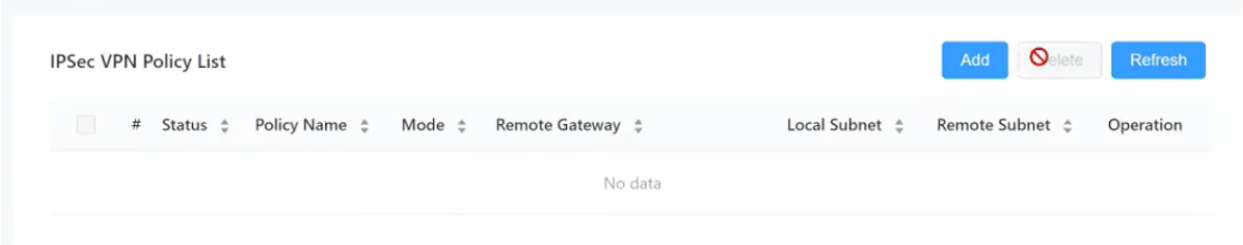
Netgear BR500 Router

To configure the tunnel in the Netgear BR500 Management Portal:

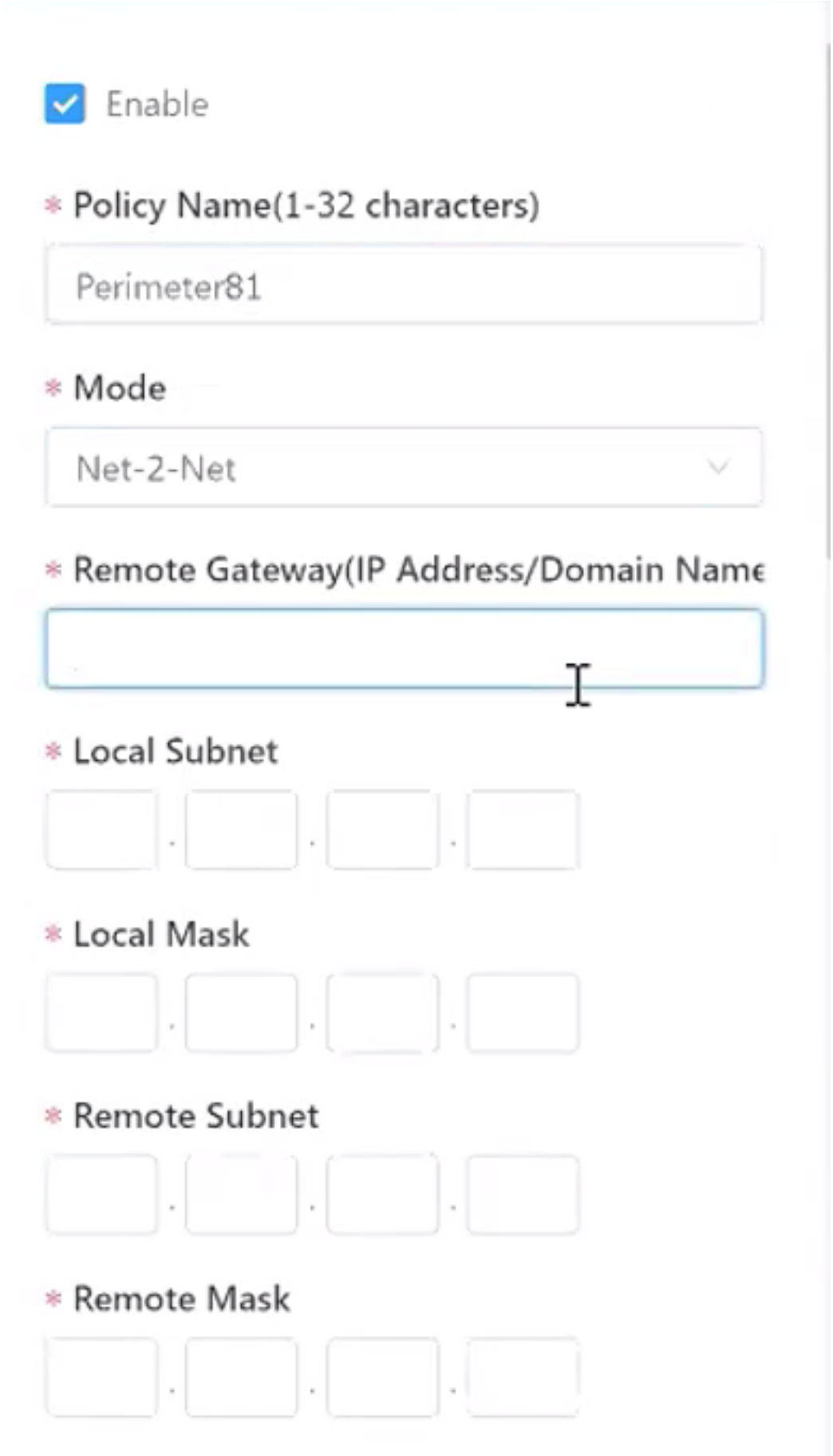
1. Log in to the Netgear BR500 Management Portal with the Administrator account.
2. From the left panel, go to **Security > IPSec VPN**.

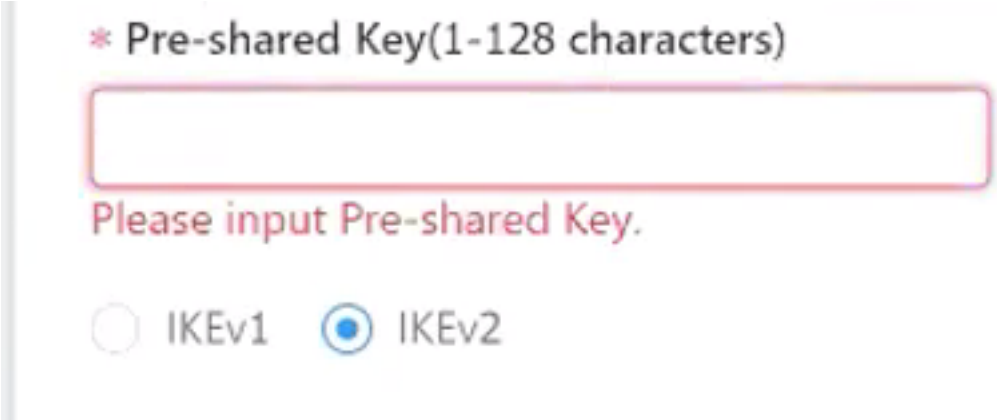


3. Click **Add**.



4. Enter these:


Enable
* Policy Name(1-32 characters)
Perimeter81
* Mode
Net-2-Net
* Remote Gateway(IP Address/Domain Name
* Local Subnet
* Local Mask
* Remote Subnet
* Remote Mask



Field	Enter
Policy Name	Name for the policy.
Mode	Net-2-Net
Remote Gateway IP	Public IP address of the Harmony SASE gateway.
Local Subnet and Local Mask	You LAN subnet and subnet mask.
Remote Subnet	Harmony SASE network subnets. Default is 10.255.0.0/16.
Remote Mask	255.255.0.0
Pre-shared Key (1-128 characters)	Secret key specified in the Harmony SASEAdministrator Portal and **IKEv2**.

5. In the **Advanced Settings** section:

Advanced Settings

Phase-1 Settings

Proposal	sha1-aes256-dh5
Proposal	---
Proposal	---
Proposal	---

Exchange Mode

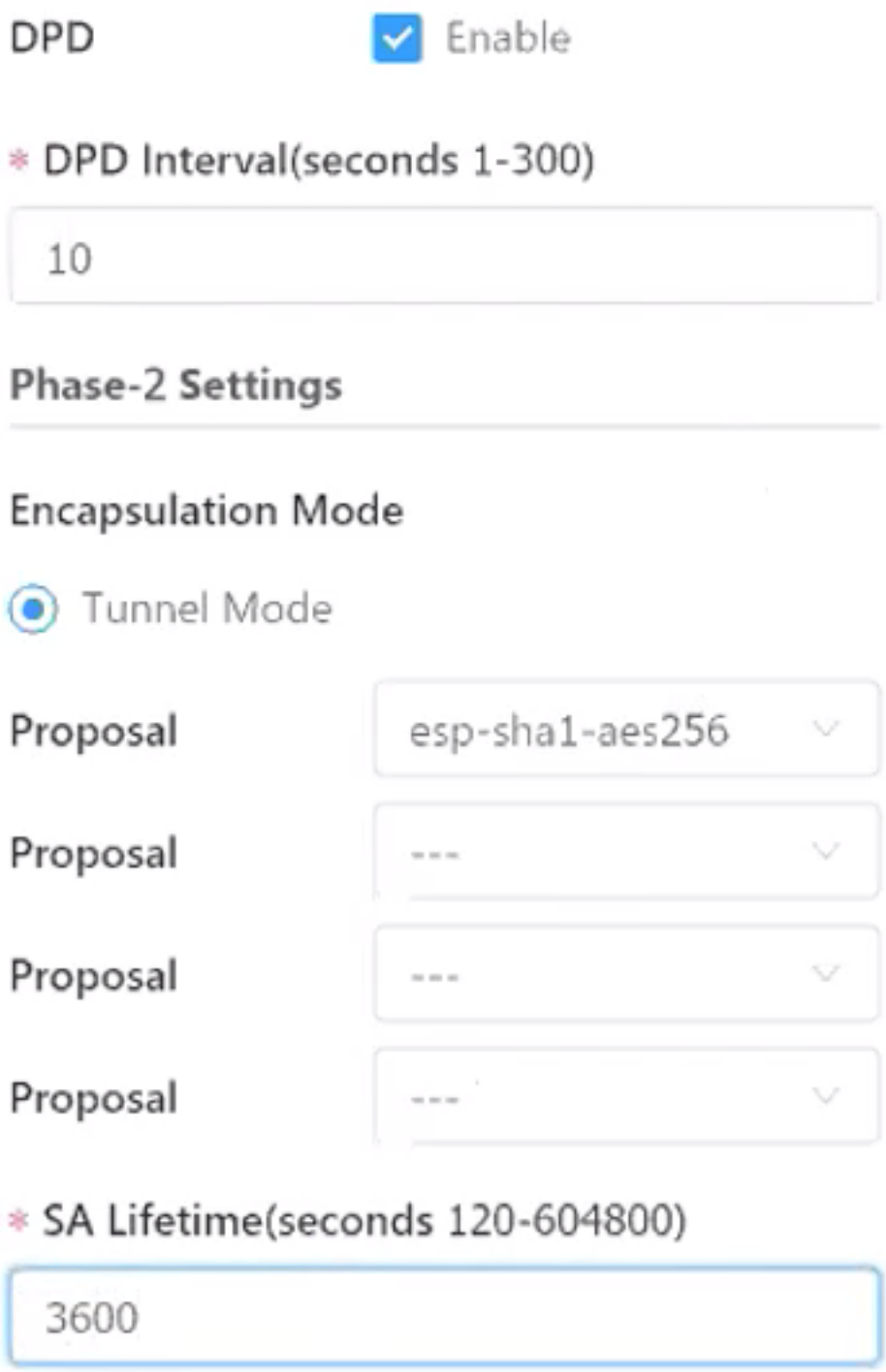
Main Mode

Negotiation Mode

Initiator Mode Responder Mode

* SA Lifetime(seconds 60-604800)

28800



Field	Enter
Phase 1 Proposal	sha1-aes256-dh5
Exchange Mode	Main Mode
Negotiation Mode	Initiator Mode

Field	Enter
Phase I SA Lifetime seconds	28800
DPD	Enable
DPD Interval	10 seconds
Phase II Encapsulation Mode	Tunnel Mode
Phase II SA Lifetime seconds	3600

Configuring the Cloud-based Resources

High-Level Procedure

1. *"Prerequisites" on page 171*
2. For a cloud-based resource, configure any of these:

   Single Tunnel
   - *"AWS Virtual Gateway" on page 424*
   - *"AWS Transit Gateway" on page 443*
   - *"Google Cloud Platform" on page 556*
   - *"Azure Virtual Network Gateway" on page 491*

   Redundant Tunnels
   - *"AWS Redundant Tunnels - Virtual Private Gateway" on page 460*
   - *"AWS Redundant Tunnels - Transit Gateway" on page 474*
   - *"Google Cloud Platform (GCP) Redundant Tunnels" on page 568*
   - *"Azure Virtual Network Gateway Redundant Tunnels" on page 517*
   - *"Azure Virtual WAN Redundant Tunnels" on page 535*

   Other Cloud Options
   - *"Alibaba Cloud" on page 415*
   - *"Heroku Enterprise" on page 590*
   - *"IBM Cloud" on page 591*

3. *"Verifying the Setup" on page 603*.

Using the Configuration File for Tunnel Configuration

You can upload a configuration file generated from the cloud-based resource management portal containing the configuration settings into the Harmony SASE Administrator Portal. This eliminates the manual configuration in the Harmony SASE Administrator Portal.

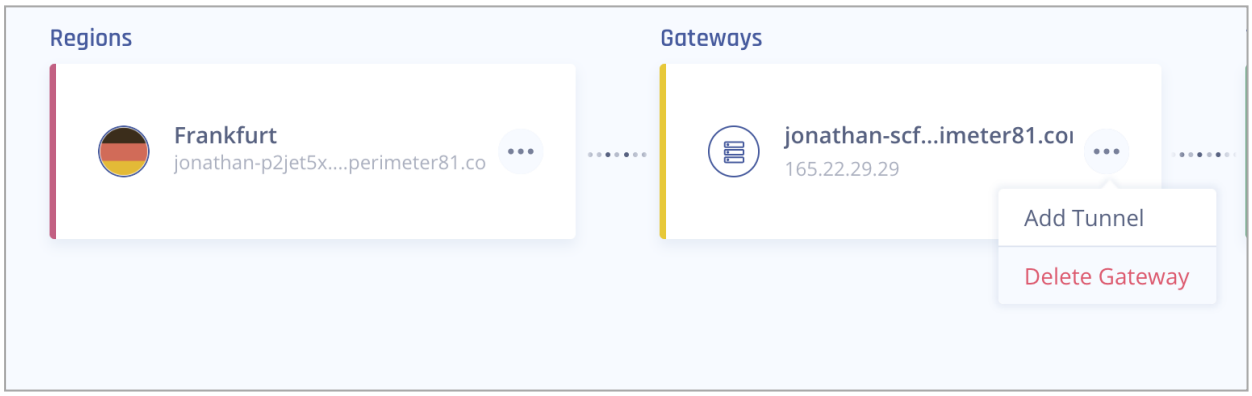
The cloud-based resources that support a configuration file are:

- *"AWS Transit Gateway" on page 443*
- *"AWS Virtual Gateway" on page 424*
- *"AWS Redundant Tunnels - Transit Gateway" on page 474*
- *"AWS Redundant Tunnels - Virtual Private Gateway" on page 460*
- *"Azure Virtual Network Gateway" on page 491*

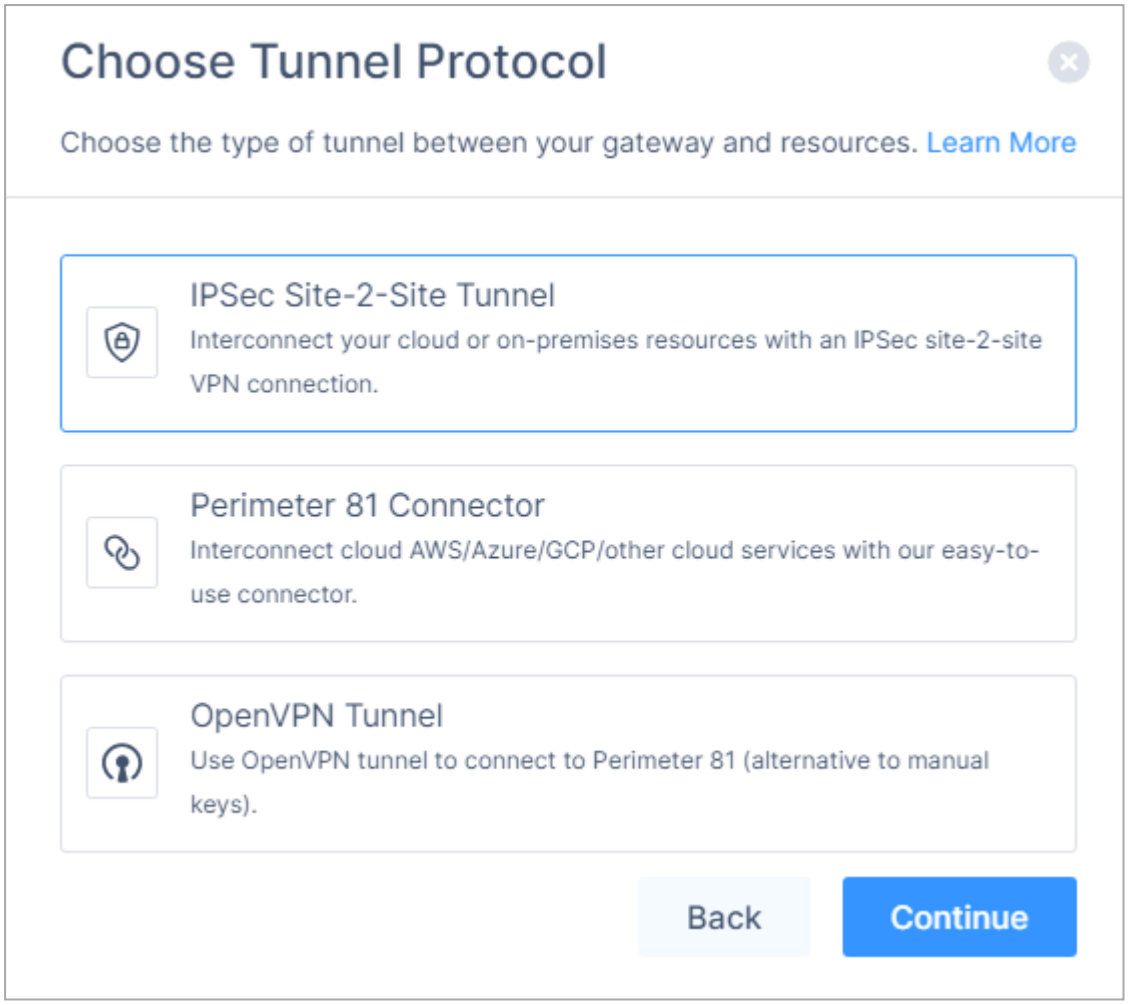
Uploading the Configuration File in the Harmony SASE Administrator Portal

After you download the configuration file from the cloud-based resource management portal, upload the file in the Harmony SASE Administrator Portal.

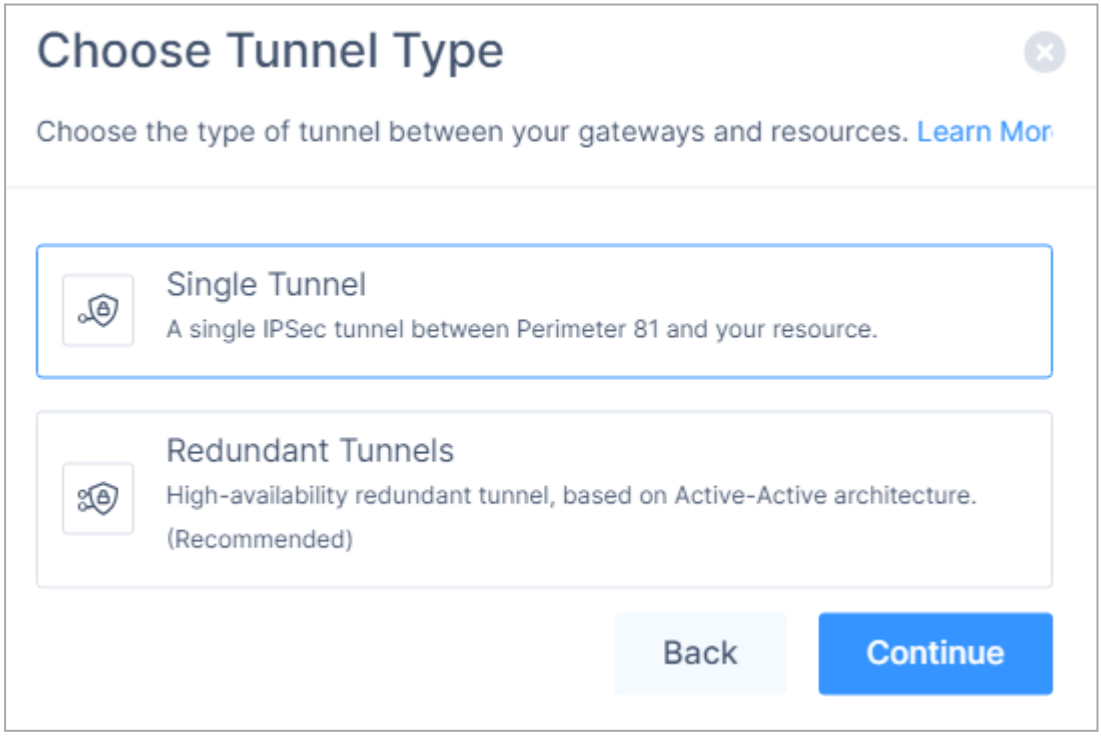
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



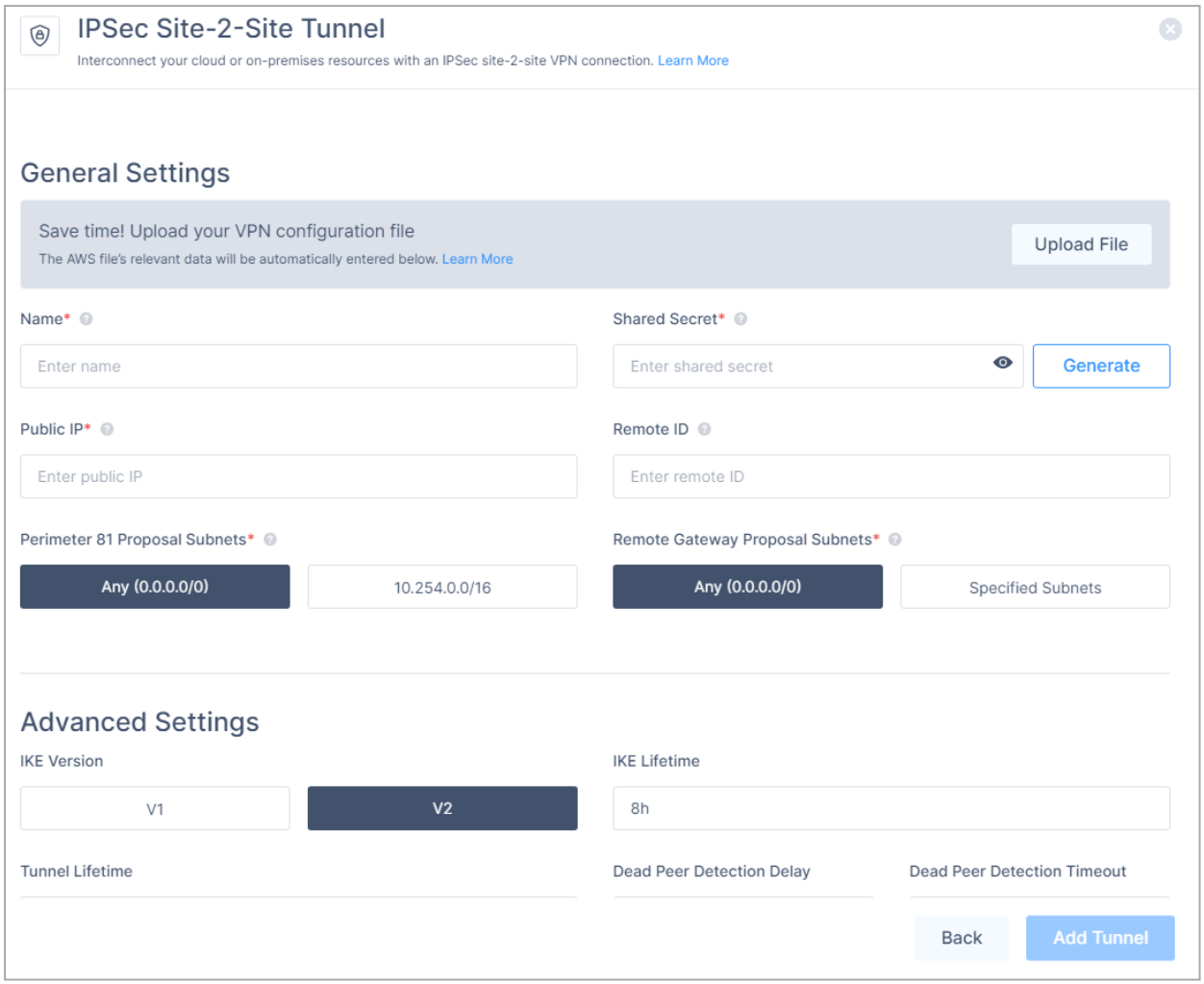
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



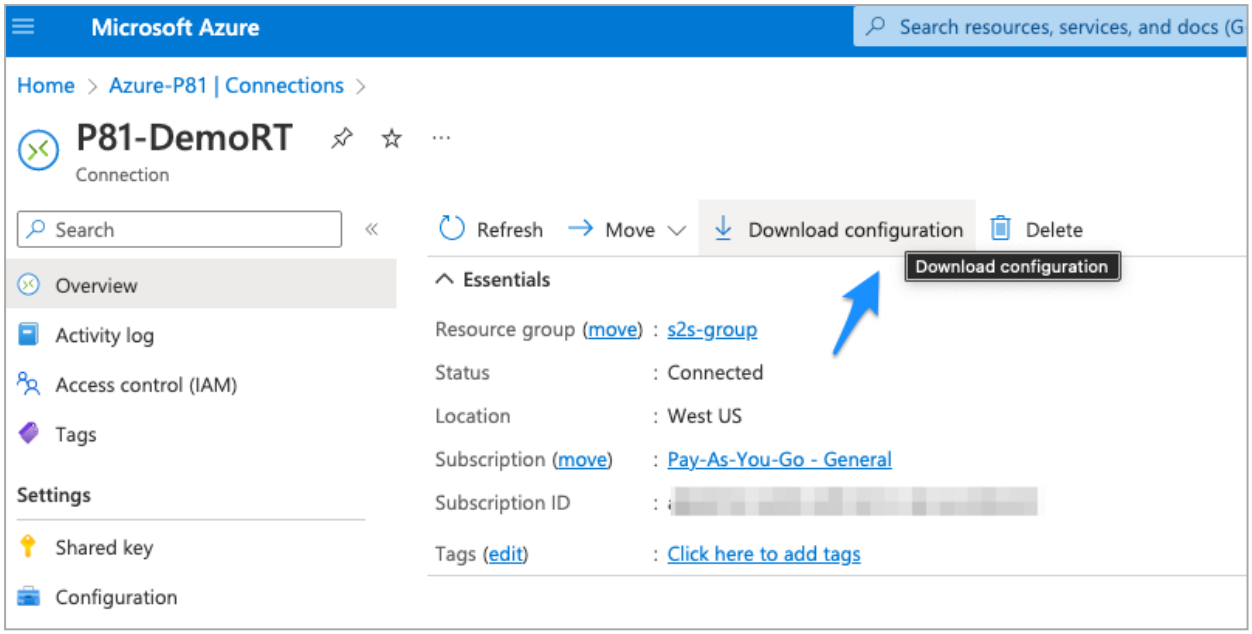
The **IPSec Site-2-Site Tunnel** window appears.



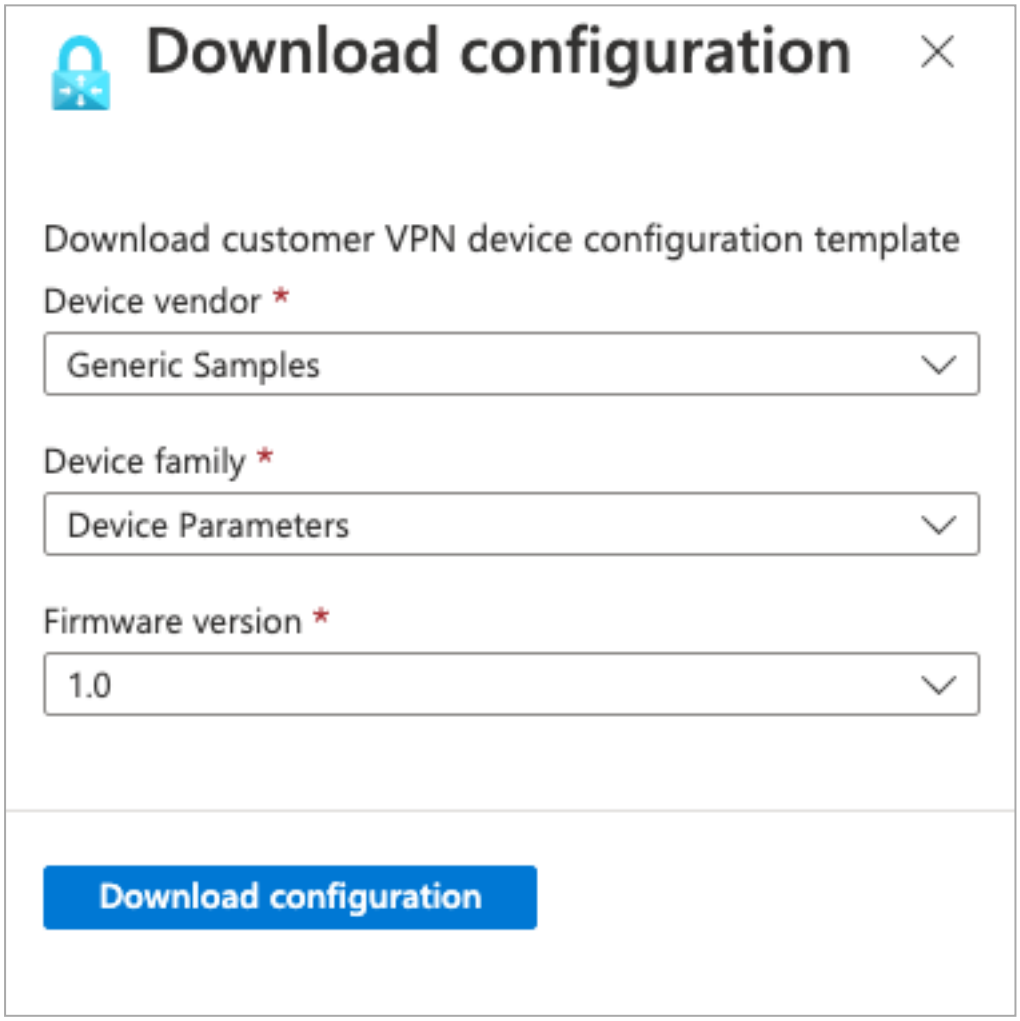
6. In the **General Settings** section, click **Upload File**.

Microsoft Azure

1. Access the Azure Management Portal and set up your Site-to-Site tunnel. For instructions, see *"Azure Virtual Network Gateway" on page 491*.
2. Go to your Virtual network gateway, click **Connections** and select your Harmony SASE connection.
3. Go to **Overview** and click **Download configuration**.



The **Download configuration** window appears.



4. Enter these:

a. **Device vendor** - Generic Samples.

b. **Device family** - Device Parameters.

c. **Firmware version** - 1.0.

5. Click **Download Configuration**.

   The system downloads the configuration file.

Tunnel Values

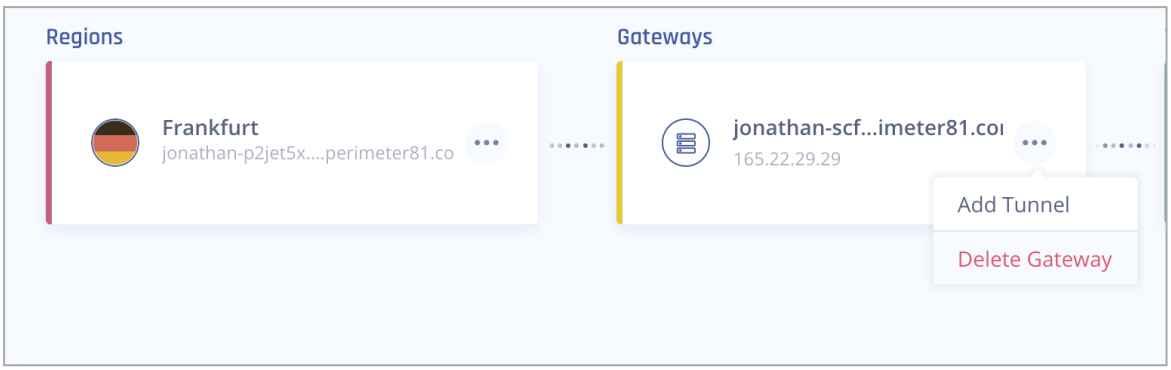
The tunnel values extracted from the configuration file are:

- **General Settings**:
  - Shared Secret (Pre-Shared Key)
  - Harmony SASE Gateway internal IP
  - Remote Public IP
  - Remote ID
  - Remote Gateway internal IP
  - Remote Gateway ASN (for redundant tunnels)
- **Advanced Settings**:
  - IKE Version
  - IKE Lifetime
  - Tunnel Lifetime
  - Dead Peer Detection Delay
  - Dead Peer Detection Timeout
  - Cipher Suites (Azure Only)

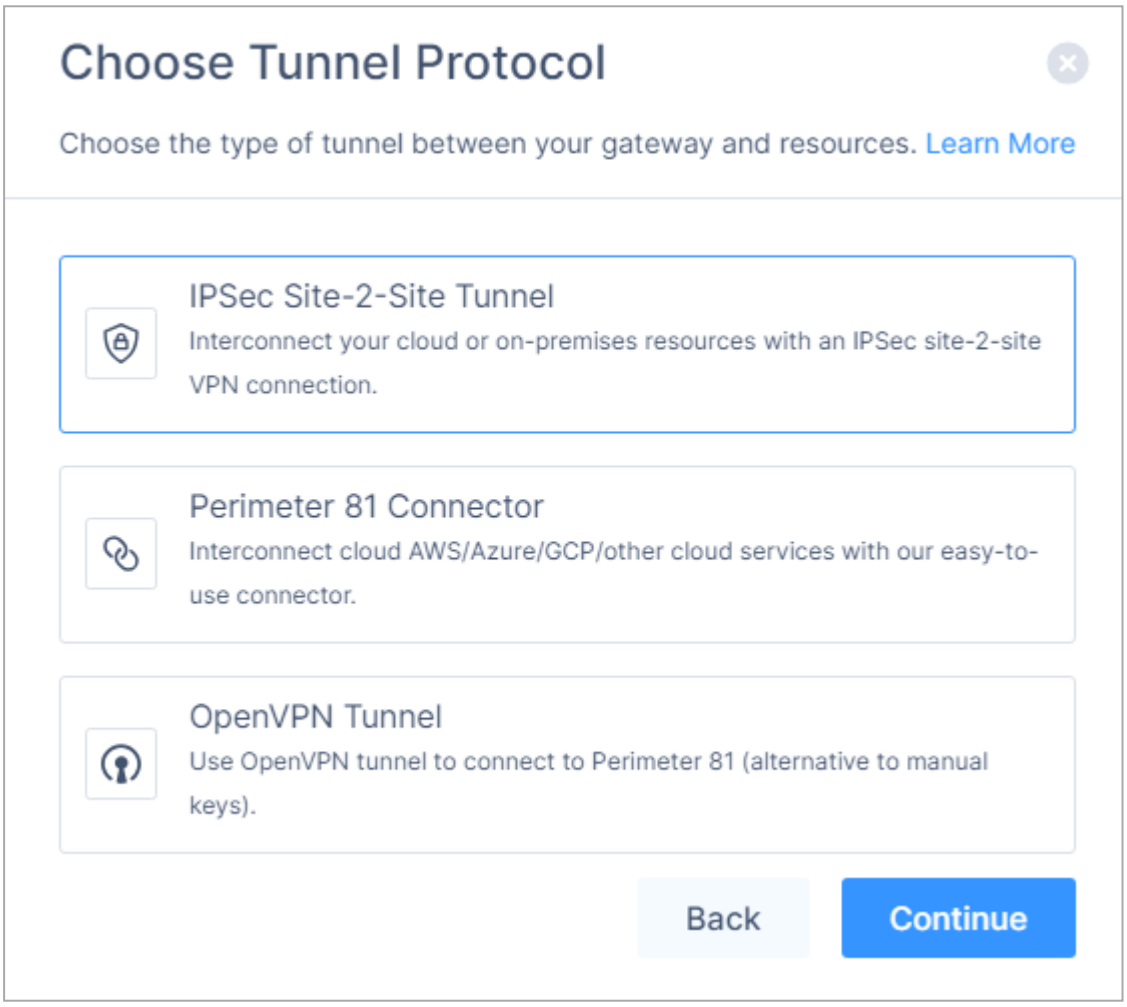
Uploading the Configuration File in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.

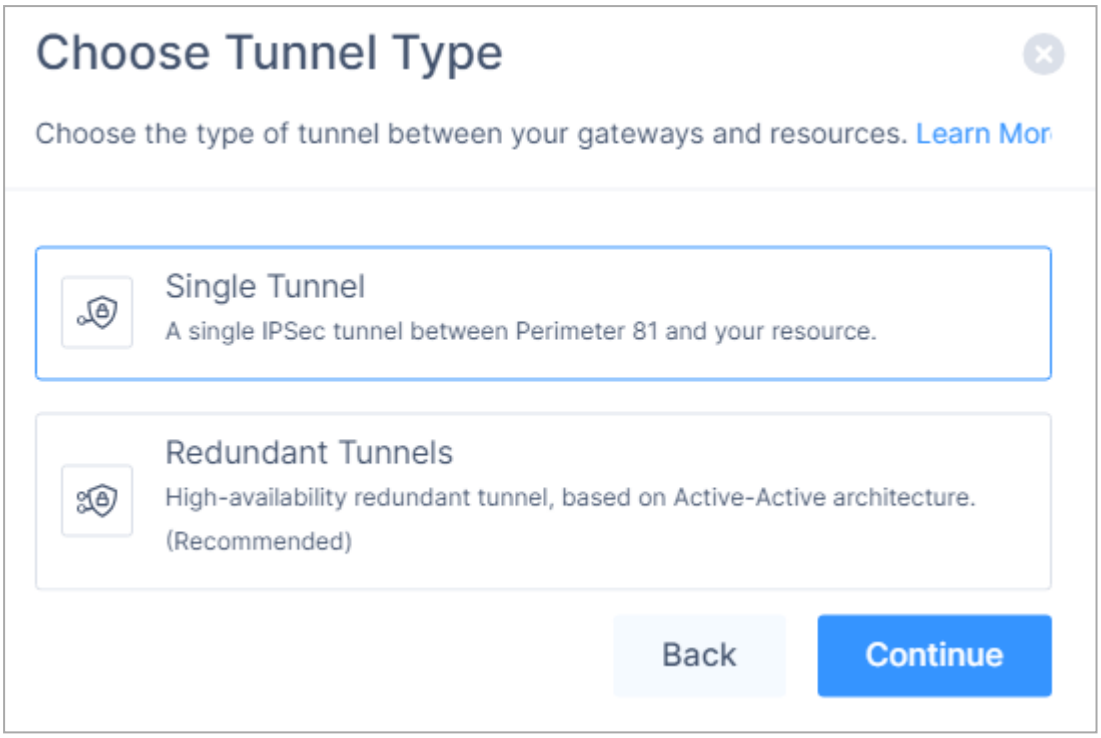
3. In the required gateway, click ··· > **Add Tunnel**.



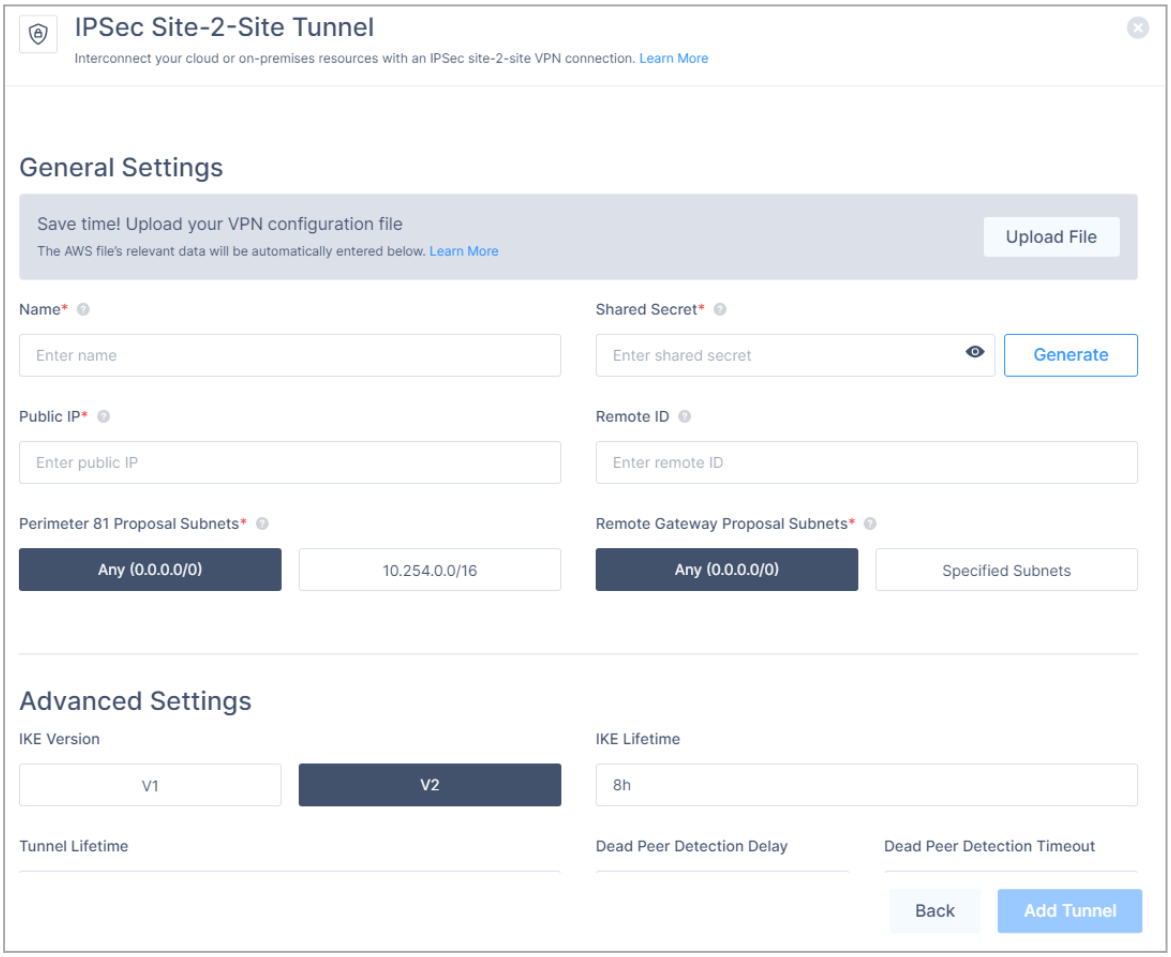
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, click **Upload File**.

Alibaba Cloud

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

Step 1 - Configurations in Alibaba Cloud

Setting Up a Tunnel

1. Access the VPC console.
2. In the **Management Platform** on the left side, click **VPN** > **IPsec Connections**.
3. Select a region.
4. In the **IPsec Connections** page, click **Create IPsec Connection**.
5. In the **Create IPsec Connection** page, configure the IPsec-VPN connection with the following information:
   a. **Name** - Name of the IPsec-VPN connection.
   b. **VPN Gateway** - Select the VPN Gateway to connect. If there are no gateways, create a new gateway.
   c. **Customer Gateway** - Select the customer gateway to connect. If none exists, create a new one for the Harmony SASE gateway public IP address.
   d. **Local Network** - CIDR block of the VPC to be connected with the on-premises data center. This parameter is used for phase two negotiation.
   e. **Remote Network** - CIDR block of the on-premises data center to be connected with the VPC. This parameter is used for phase two negotiation (if you do not select a specific subnet).

      Harmony SASE default value is **10.255.0.0/16**.
   f. **Effective Immediately** - Yes.

g. **Advanced Configuration** - IKE Configurations

   i. **Pre-Shared Key** - Pre-shared key used for the authentication between the VPN Gateway and the customer gateway. By default, it is an automatically generated value. However, you can also specify a pre-shared key. This key should be used also in the Harmony SASE side.

   ii. **Version** - IKEv1

   iii. **Negotiation Mode** - Main mode

   iv. **Encryption Algorithm** - aes256

   v. **Encryption Algorithm** - sha1

   vi. **DH Group** - group2

   vii. **SA Life Cycle (seconds)** - SA lifecycle for phase one negotiation. The default value is 86,400 seconds.

   viii. **LocalId** - Local VPN Gateway public IP address

   ix. **RemoteId** - Harmony SASE gateway public IP address

h. **Advanced Configuration**: **IPSec Configurations**

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

i. **Health Check** - Optional

6. Click **OK**.

Setting Access Rules in Alibaba Security Groups

1. Access the VPC console and go to your security group associated with your server.
2. Add Allow rule with 10.255.0.0/16 object to the desired ports.

Setting Routes in Alibaba Cloud

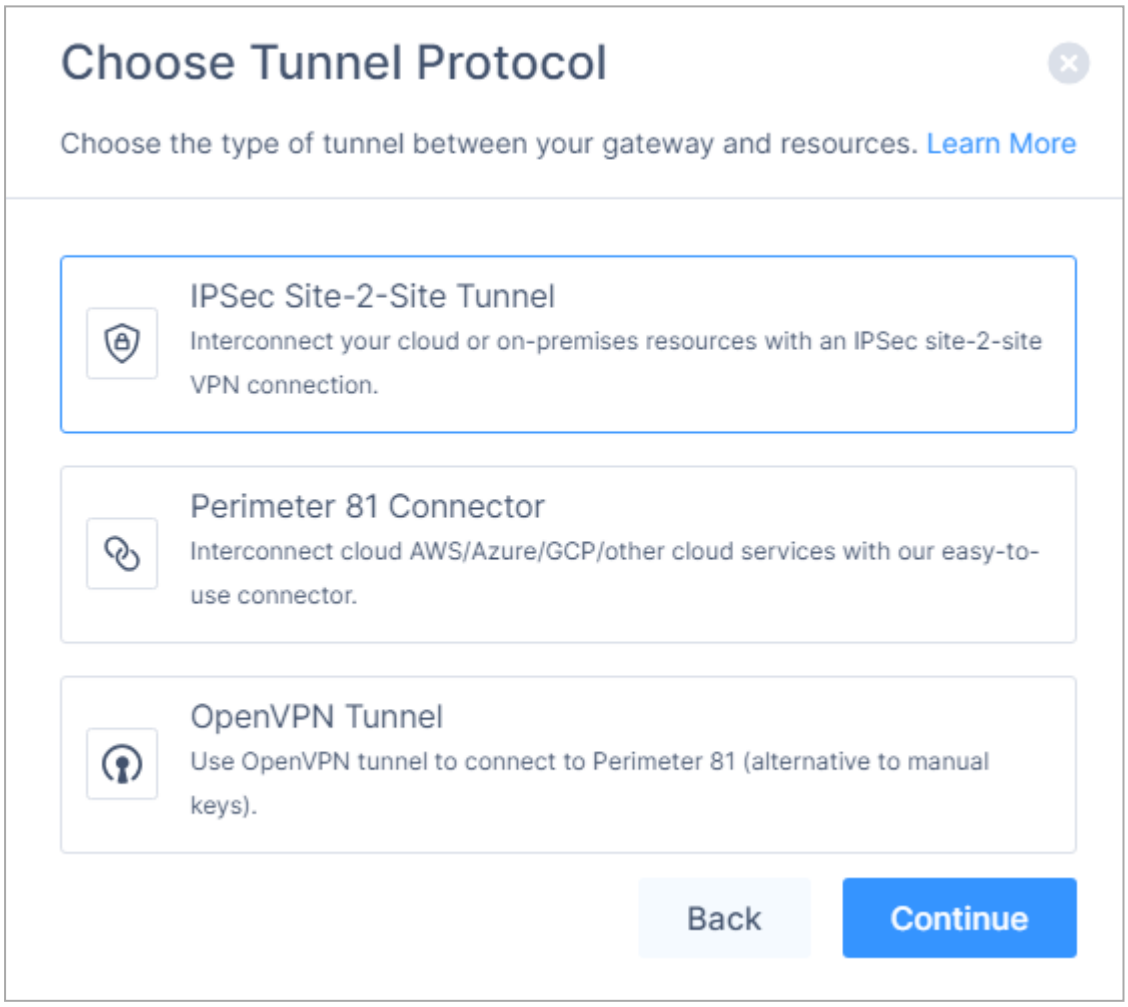
1. Access the VPC console and go to your VPN.
2. Click **Route Tables**.
3. Add this route under the System route table or on your custom route table:

   10.255.0.0/16.

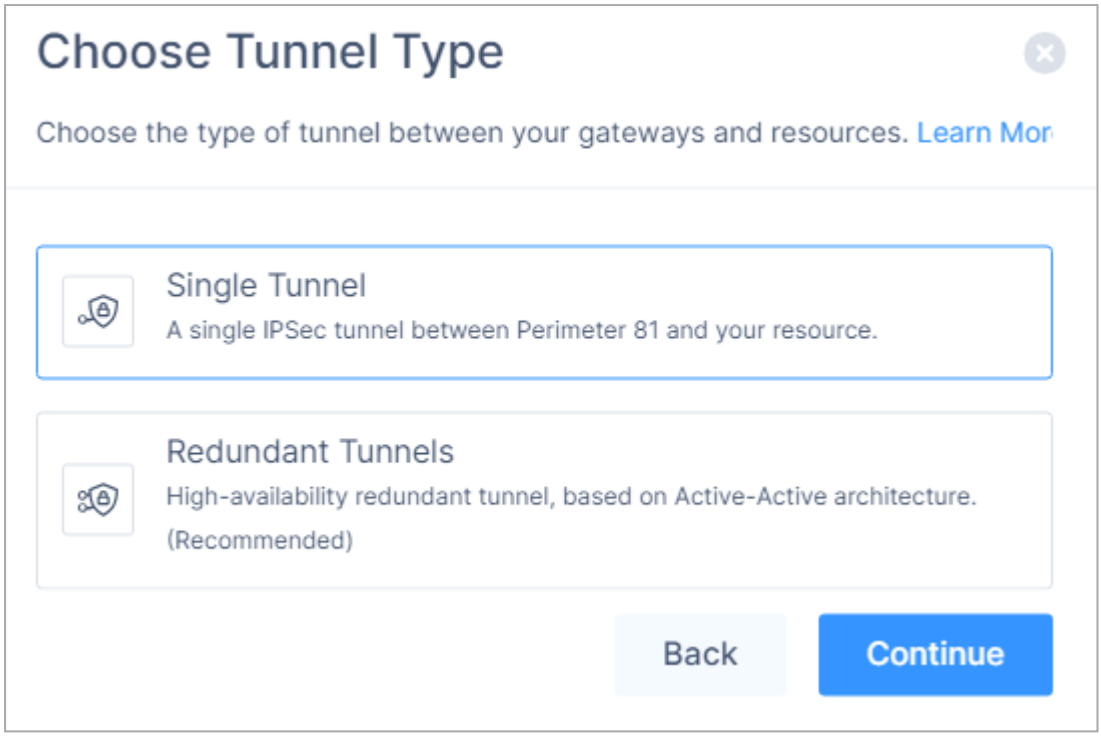
Step 2 - Creating the Tunnel in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.

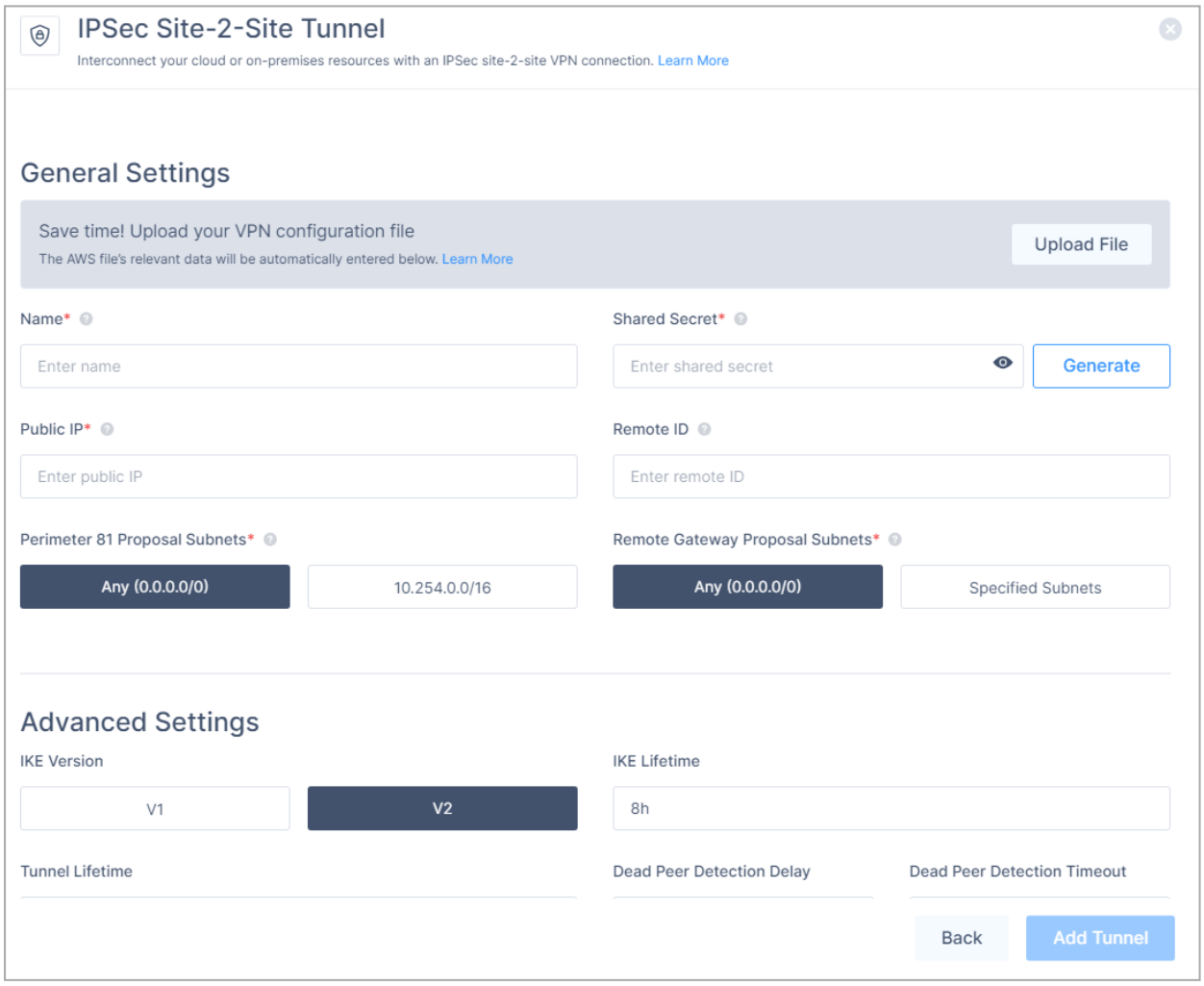
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, enter these:
    a. **Name** - Name of the tunnel.
    b. **Shared Secret** - Shared secret you set in VPC console.
    c. **Public IP** and **Remote ID**: Enter Alibaba VPN Gateway Public IP address.
    d. In **Perimeter 81 Gateway Proposal Subnets**, select **Any** or **Specific Subnet**.

e. In **Remote Gateway Proposal Subnets**, enter your VPC console subnet/s.

f. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha 512	sha 512	21	21
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha 512	sha 512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha 512	sha 512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes 256	aes 256	sha 512	sha 512	21	21
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes 256	aes 256	sha 512	sha 512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes 256	aes 256	sha 512	sha 512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes 256	aes 256	sha 1	sha 1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes 256	aes 256	sha 256	sha 256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

7. Click **Add Tunnel**.

AWS Virtual Gateway

This chapter describes the process to establish a Site-to-Site IPsec tunnel between your Harmony SASE network and your AWS environment.

Use this configuration if your connection is intended for a single Virtual Private Cloud (VPC).

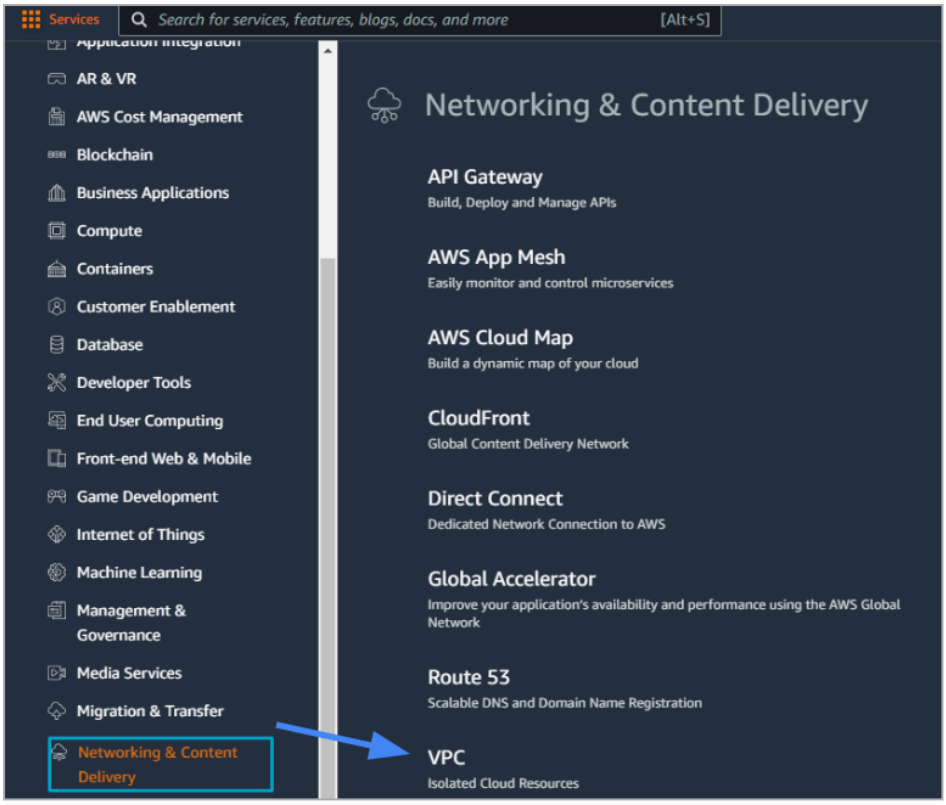
If you have multiple VPCs, see *"AWS Transit Gateway" on page 443*.

Prerequisites

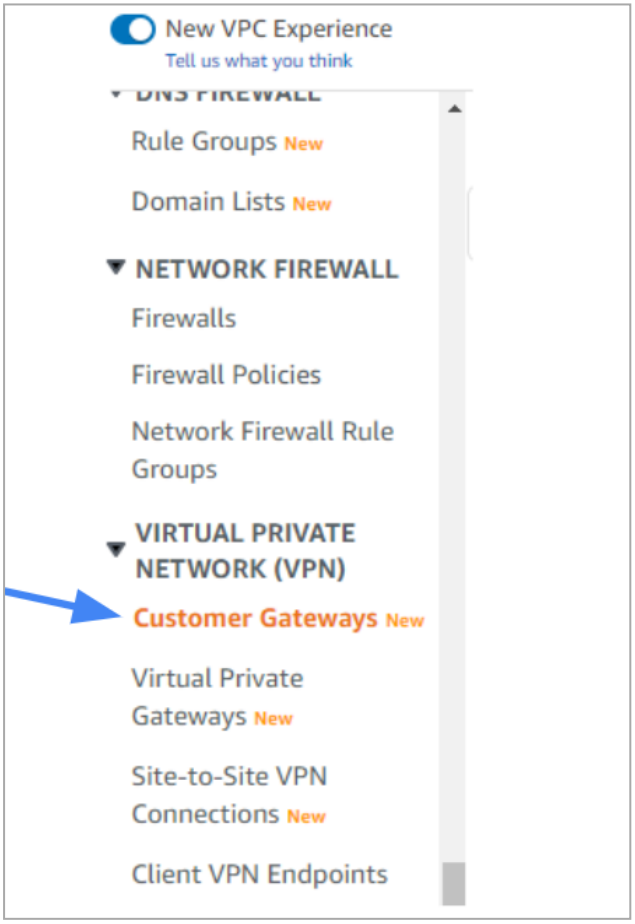
- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

Step 1 - Configuring the Tunnel in the AWS Management Console

1. Access the AWS Management console and go to the **VPC** section.
2. In the **Services** section, scroll down to **Networking & Content Delivery** and select **VPC**.



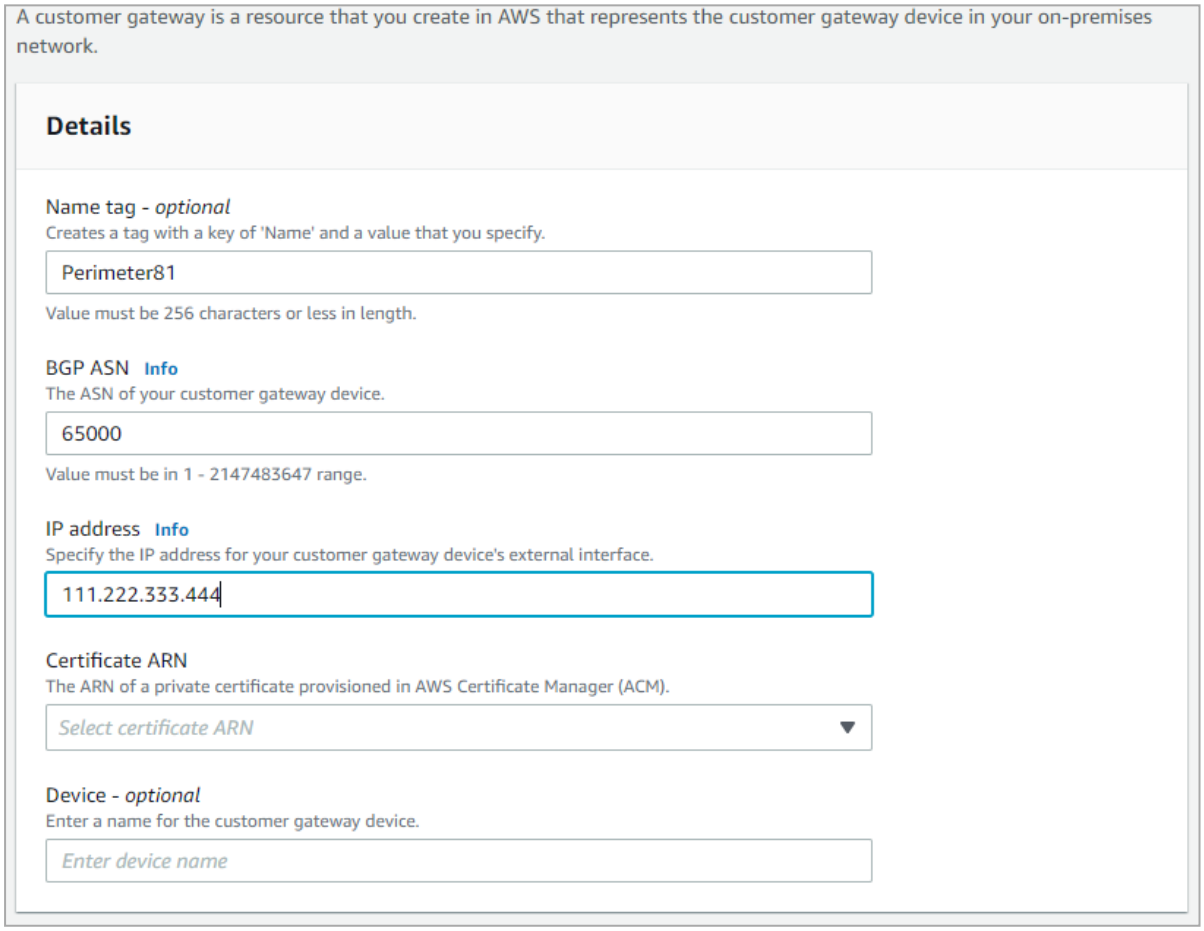
3. In the left menu **Virtual Private Network (VPN)** section, click **Customer Gateways**.



4. Click **Create Customer Gateway**.
5. Click **static** routing.
6. Enter the IP Address of the Harmony SASE Gateway. To get the IP Address, go to the Harmony SASE Administrator Portal and see the **Networks** page.

7. Select **Create Customer Gateway**.

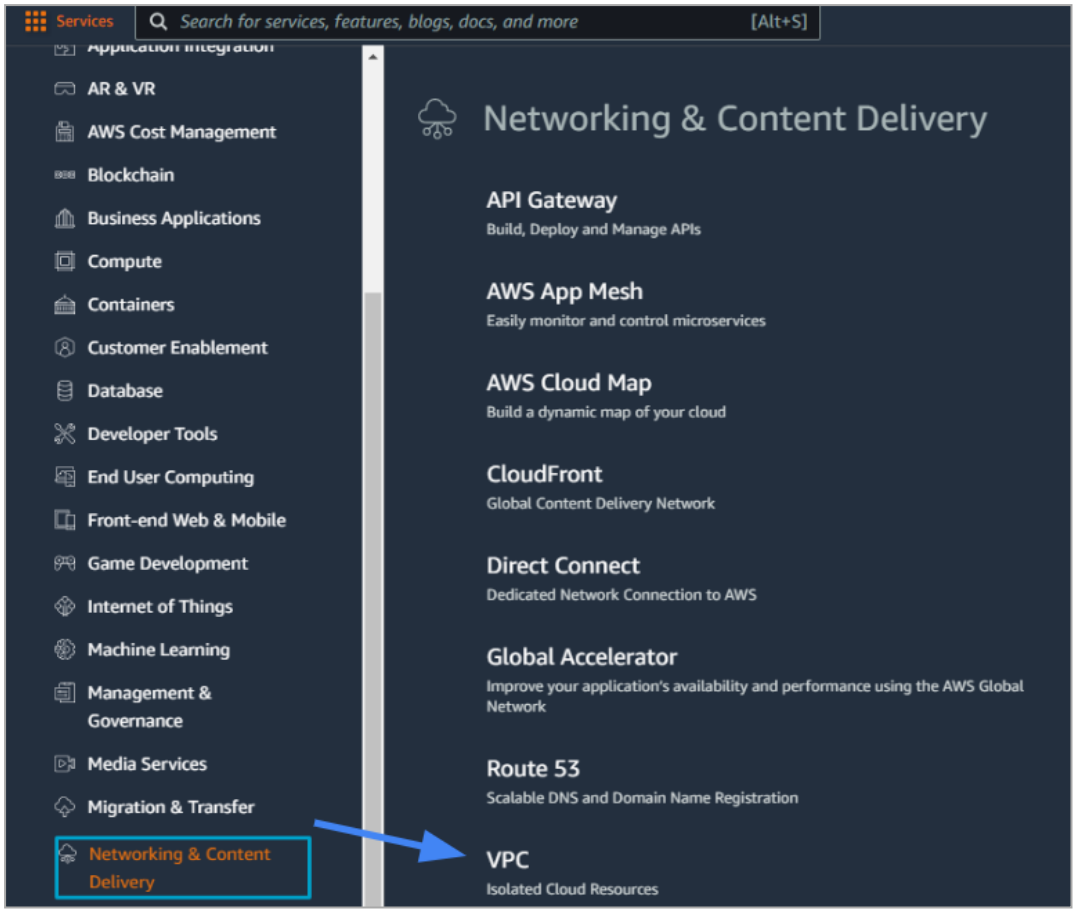
   A message displays to indicate that the gateway was created successfully.



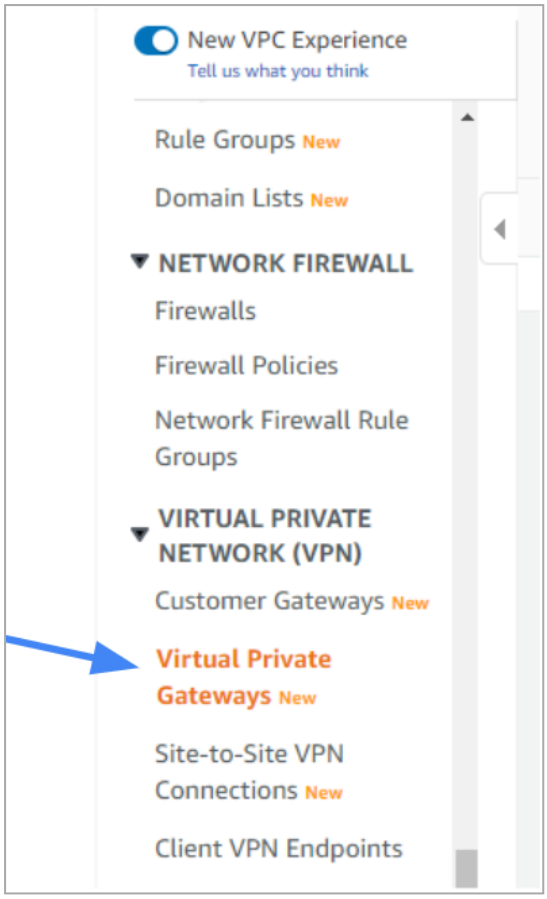
Configuring a Virtual Private Gateway

Important - If you already have a virtual private gateway attached to your VPC, skip this section and continue with *"Creating a Virtual Private Network Connection" on page 431*.

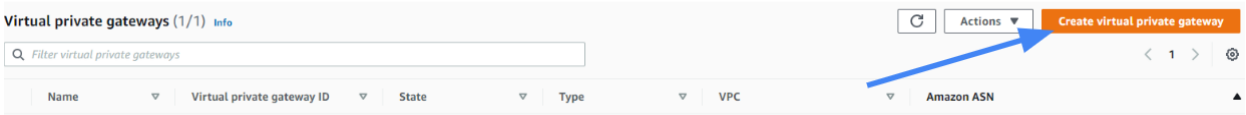
1. Access the AWS Management console and go to **Services**, scroll down to **Networking & Content Delivery** and click **VPC**.



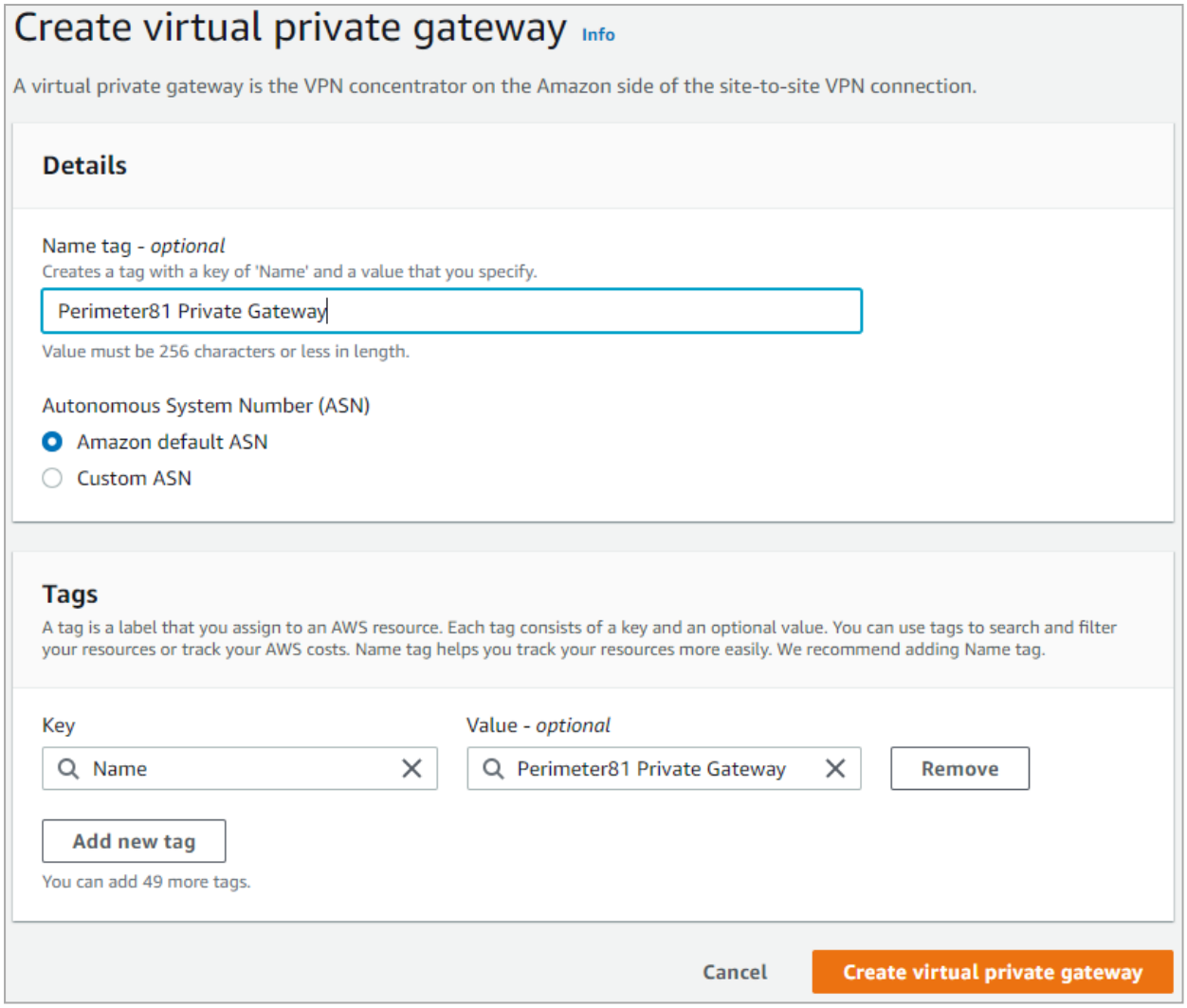
2. On the left menu, go to **Virtual Private Network (VPN)** > **Virtual Private Gateways**.



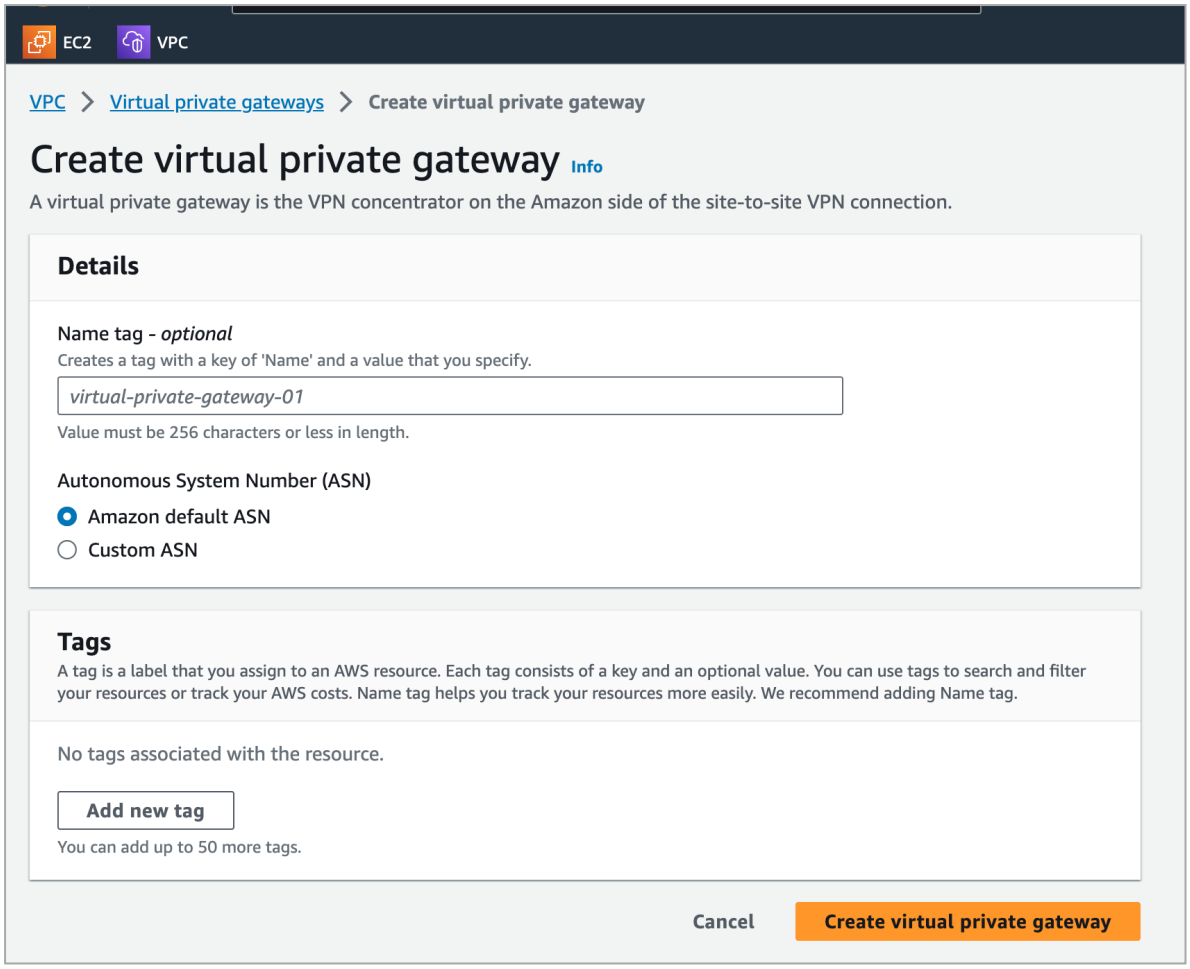
3. Click **Create Virtual Private Gateway**.



The **Create virtual private gateway** window appears.

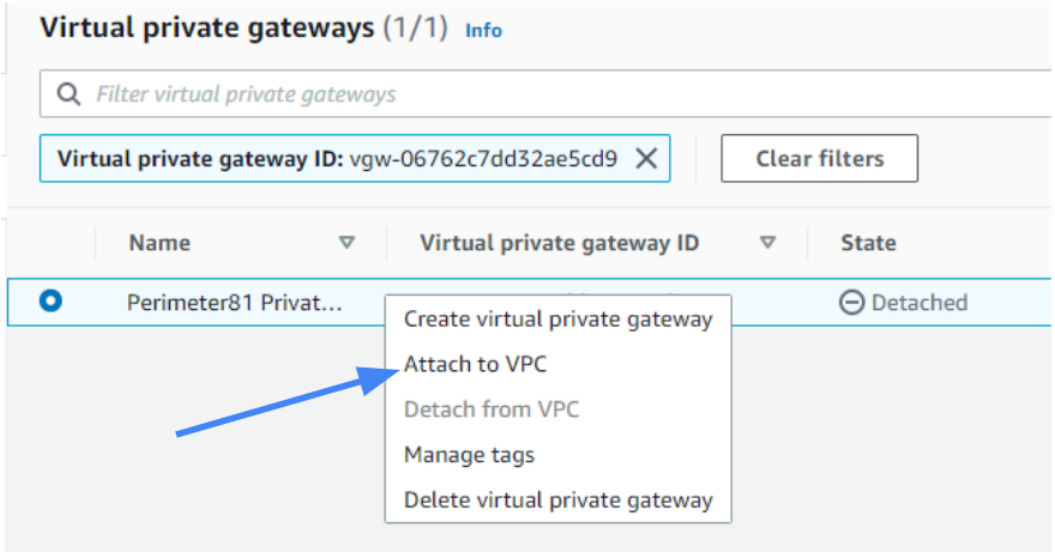


4. In the **Name** field, enter the name of the gateway, for example US_HQ.
5. In the **ASN** field, click **Amazon default ASN**.
6. Click **Create virtual private gateway**.



The systems displays a message that the virtual Private Gateway was created successfully.

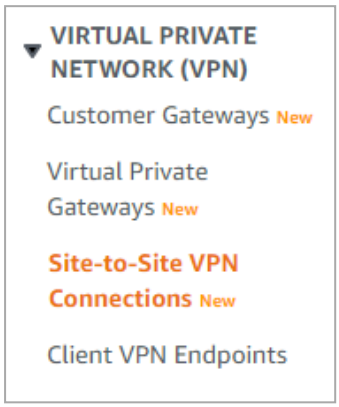
7. Select the newly created gateway and click **Actions**. On the context menu, select **Attach to VPC**.



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

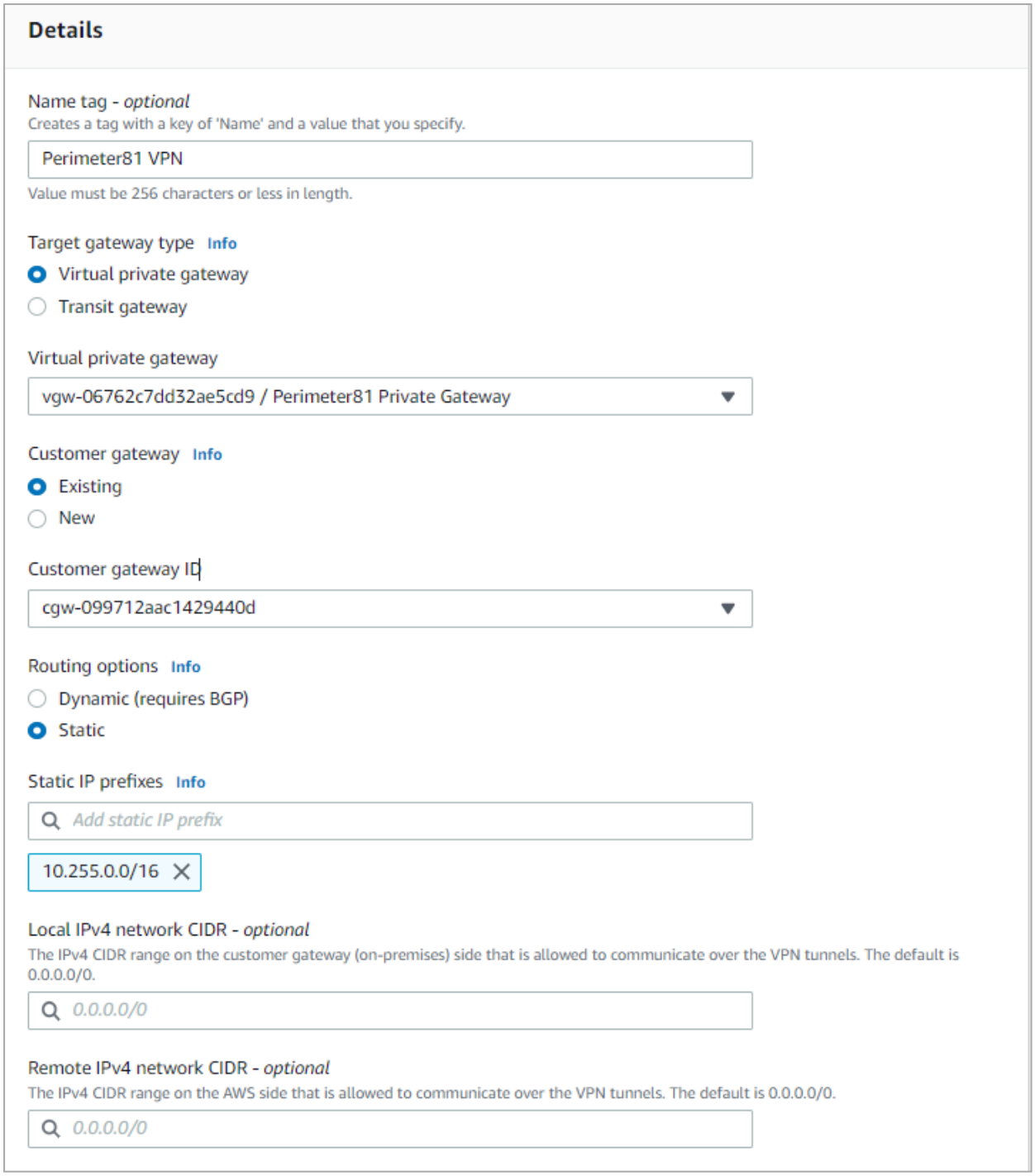
Creating a Virtual Private Network Connection

1. Access the AWS Management console and go to **Services**, scroll down to **Networking & Content Delivery** and click **VPC**.
2. On the left menu, go to **Virtual Private Network** > **Site-to-SiteVPN Connections**.



3. Click **Create VPN Connection**.

The **Create VPN Connection** window appears.



4. In the **Name** field, enter the name tag (for example, US_HQ).
5. In the **Target gateway type** field, click **Virtual private gateway**.
6. In the **Customer gateway** field, click **Existing**.
7. From the **Customer gateway ID** list, select the **Customer Gateway** that you have created.
8. In the **Routing Options** field, select **Static**.

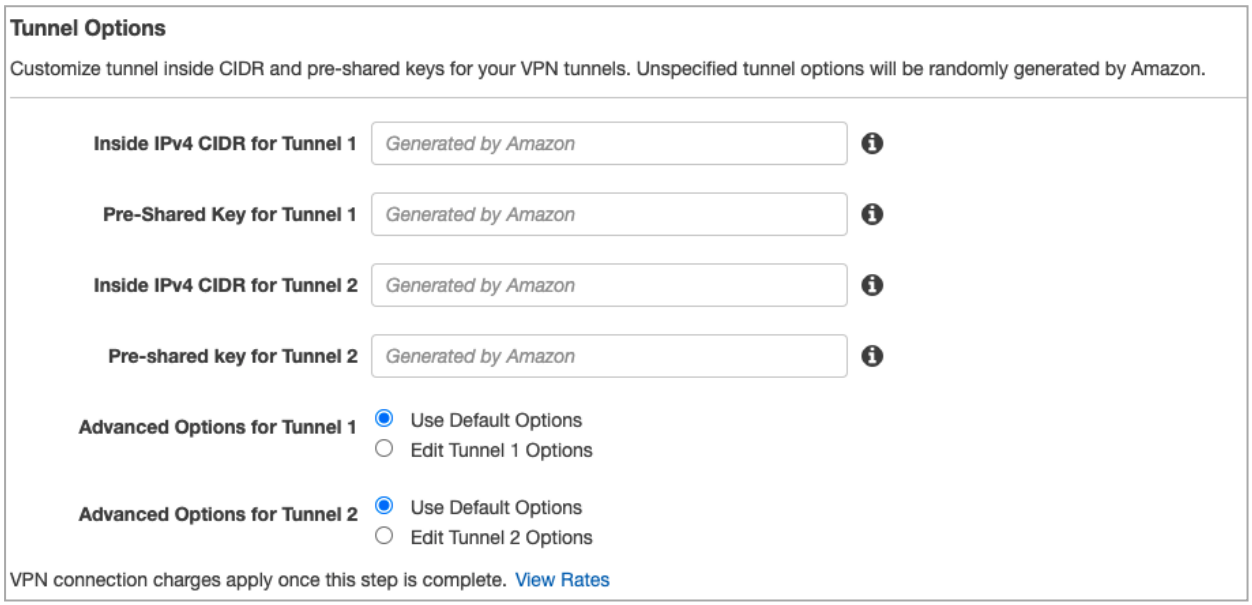
9. In the **Static IP prefixes** field, enter your Harmony SASE network subnet (Usually 10.255.0.0/16).

   Important - This address might differ if you have not chosen the default subnet mask for your tunnel.

10. In **Tunnel Options** section:

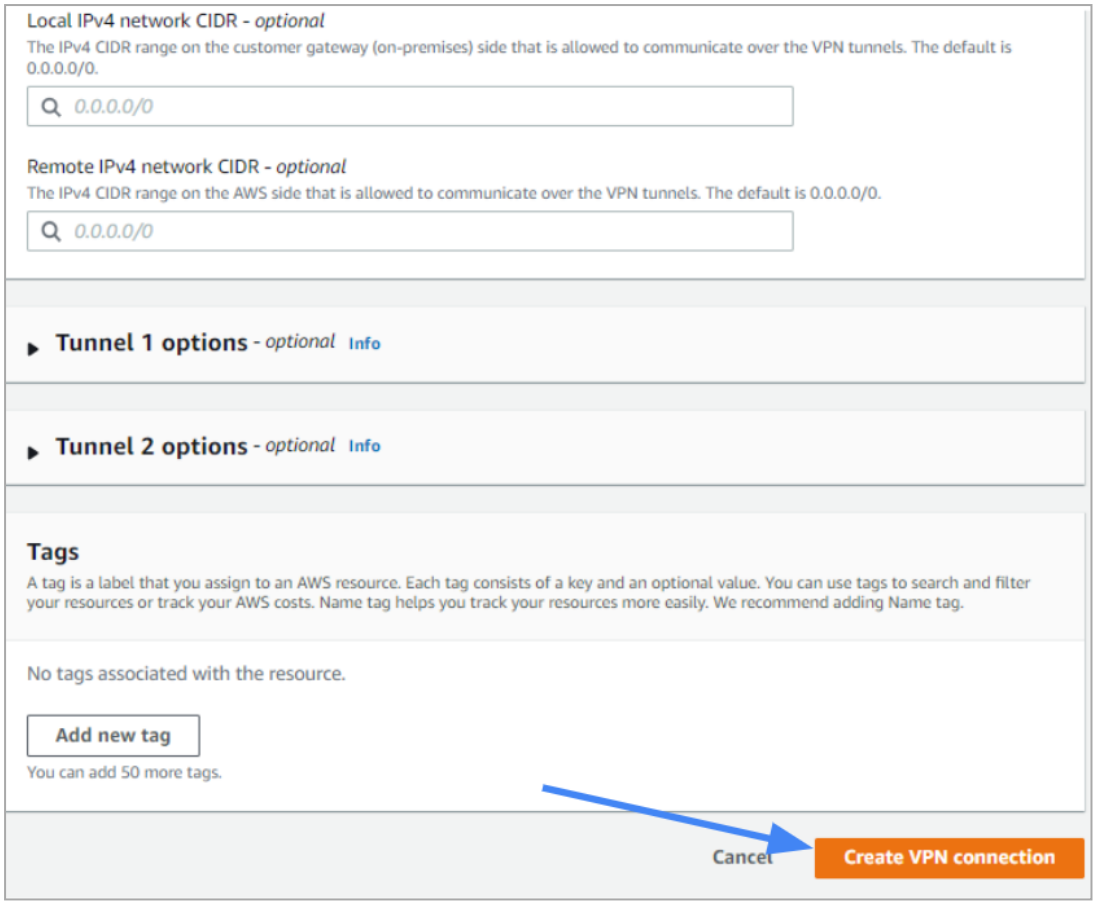
    a. In **Advanced Options**, select **Edit Tunnel Options**.

    b. In **DPD timeout**, set the value to **60**.



   Note - AWS supports various types of encryption and hash formats for both the tunnels. If the tunnel options are set to default (as shown below) it accepts any encryption suite you want for the handshake with Harmony SASE. In this screen, you can also select the inside subnets you want to connect through the tunnel.

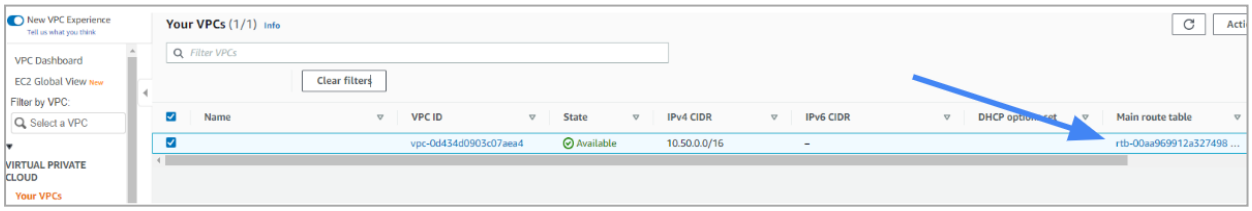
11. Click **Create VPN connection**.



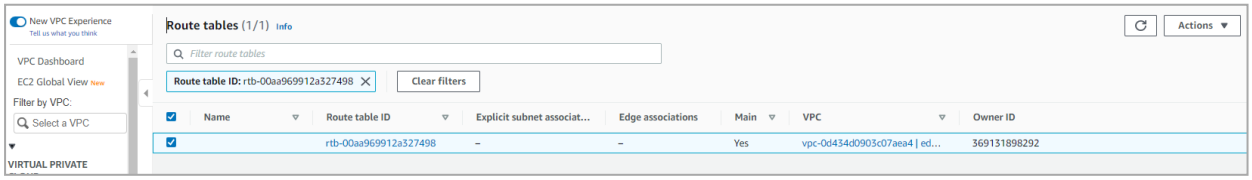
The system displays a message that a VPN Connection Request was created successfully.

Configuring the Routing Rules to the Default Gateway

1. Access the AWS Management console and go to the **VPC** section.
2. Enter the Route table associated with your VPC.

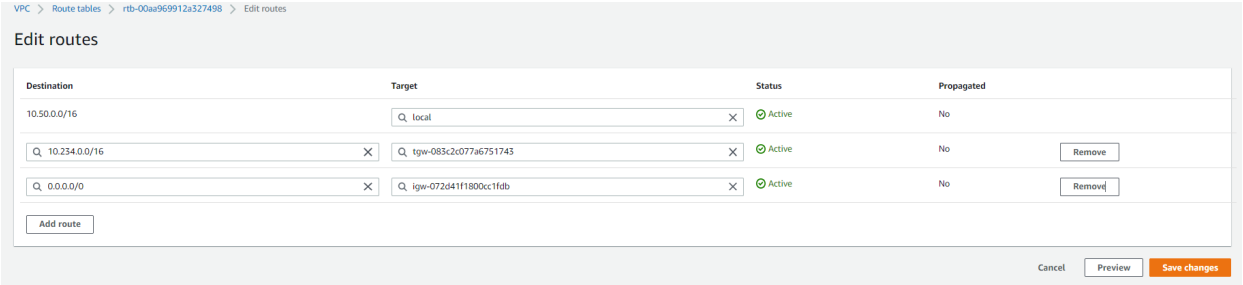


3. In the **Route Tables** menu option, select the routing table associated with the VPC you have created for the tunnel.



4. Click **Edit**.

The **Edit routes** window appears.



5. Add the new static routes for these subnets:

   a. In the **Destination** field, enter your Harmony SASE network subnet listed in the Harmony SASE Administrator Portal (**Networks** > **Gateway** > **Settings**)

   Usually 10.255.0.0/16

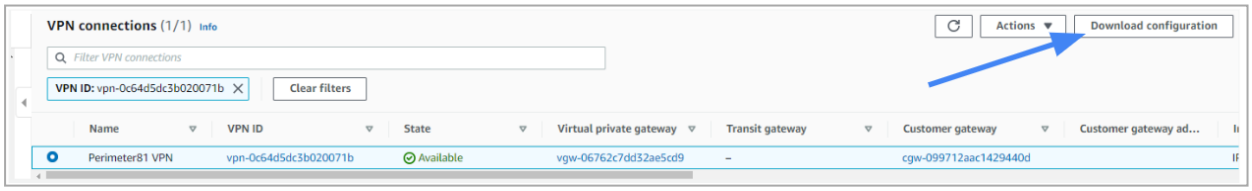
   b. In the **Target** field, enter your new VPN Gateway ID as the target (it appears under the subcategory Virtual Private Gateway).

6. Click **Save changes**.

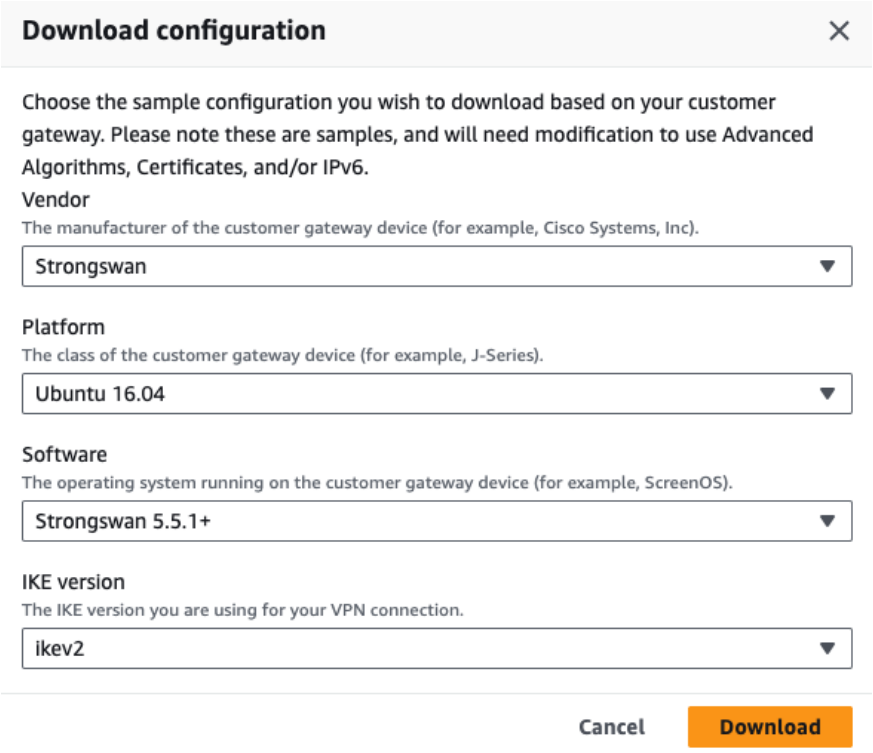
Note - If you have a customized security group associated with your VPC, configure your AWS security groups to allow all traffic from Harmony SASE subnets (usually 10.255.0.0/16) or allow only particular traffic using the port and IP restrictions.

Configuring the Tunnel

1. Access the AWS Management console and go to **Site-to-Site VPN Connections** and click **Download configuration**.

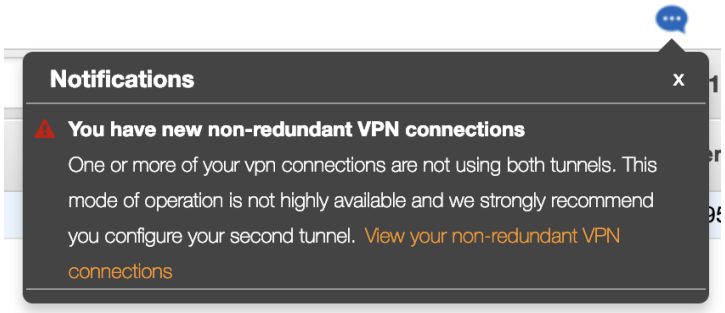


The **Download configuration** window appears.



2. Enter these:
   a. **Vendor** - Strongswan
   b. **Platform** - Ubuntu 16.04
   c. **Software** - Strongswan version.
   d. **Ike version** - Ikev2
3. Click **Download**.

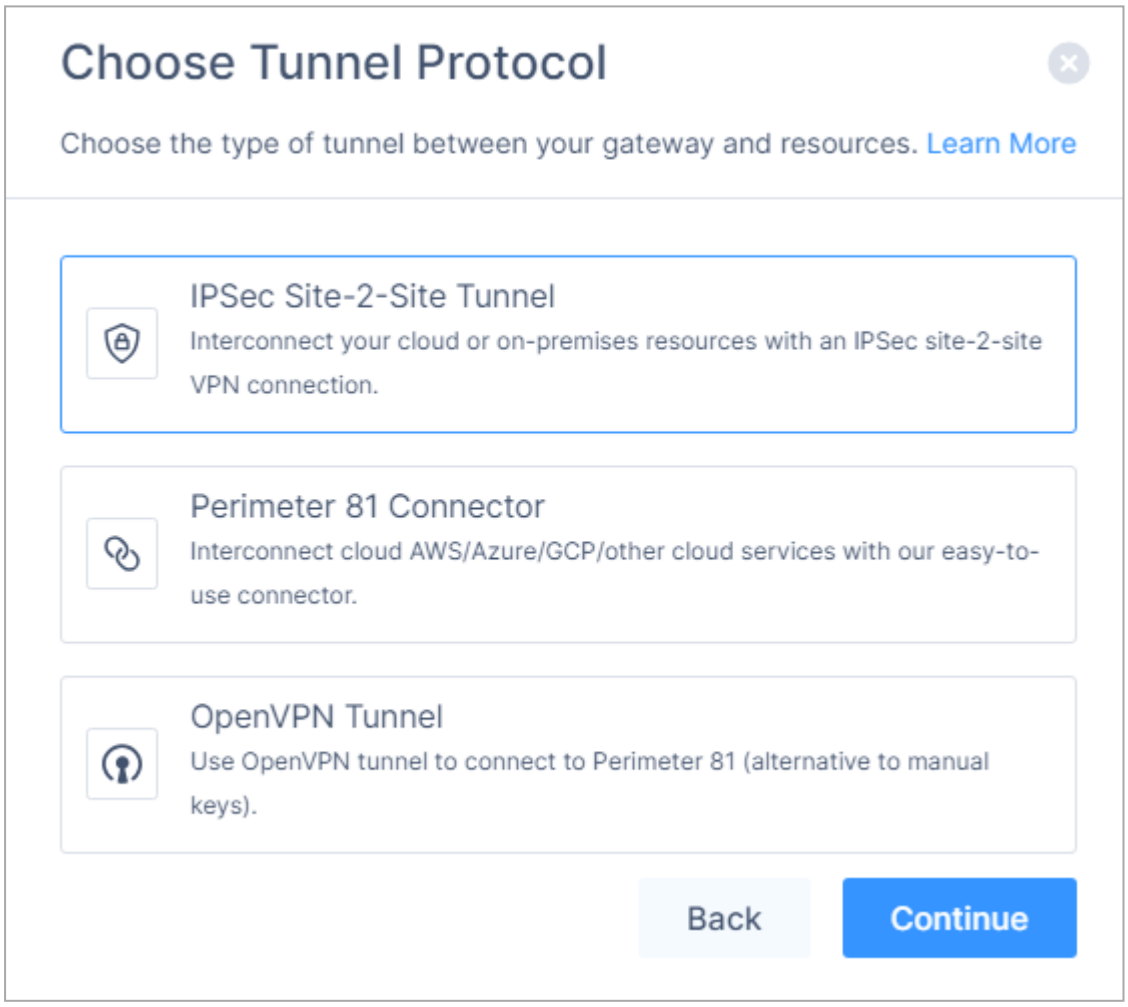
Important - When you examine the configuration file, you may notice that AWS has created two separate tunnels for the same VPN connection, however Harmony SASE utilizes only one of them.
We recommend you to use the one that appears first in the file.



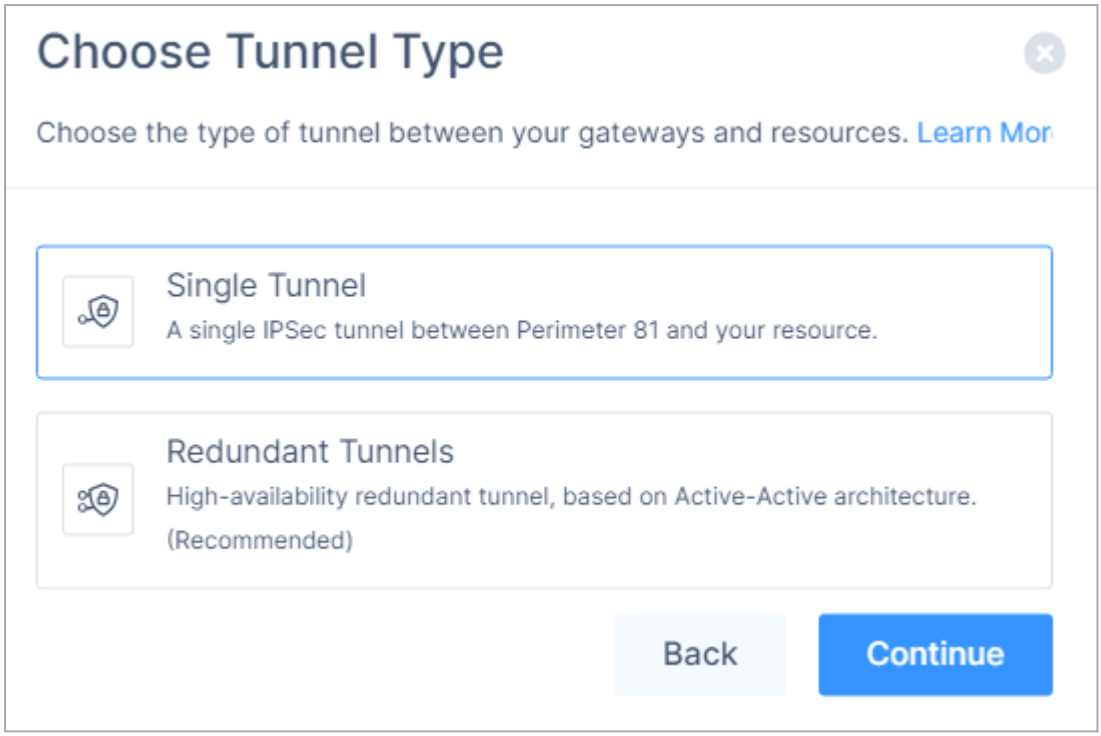
Step 2 - Creating the Tunnel in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.

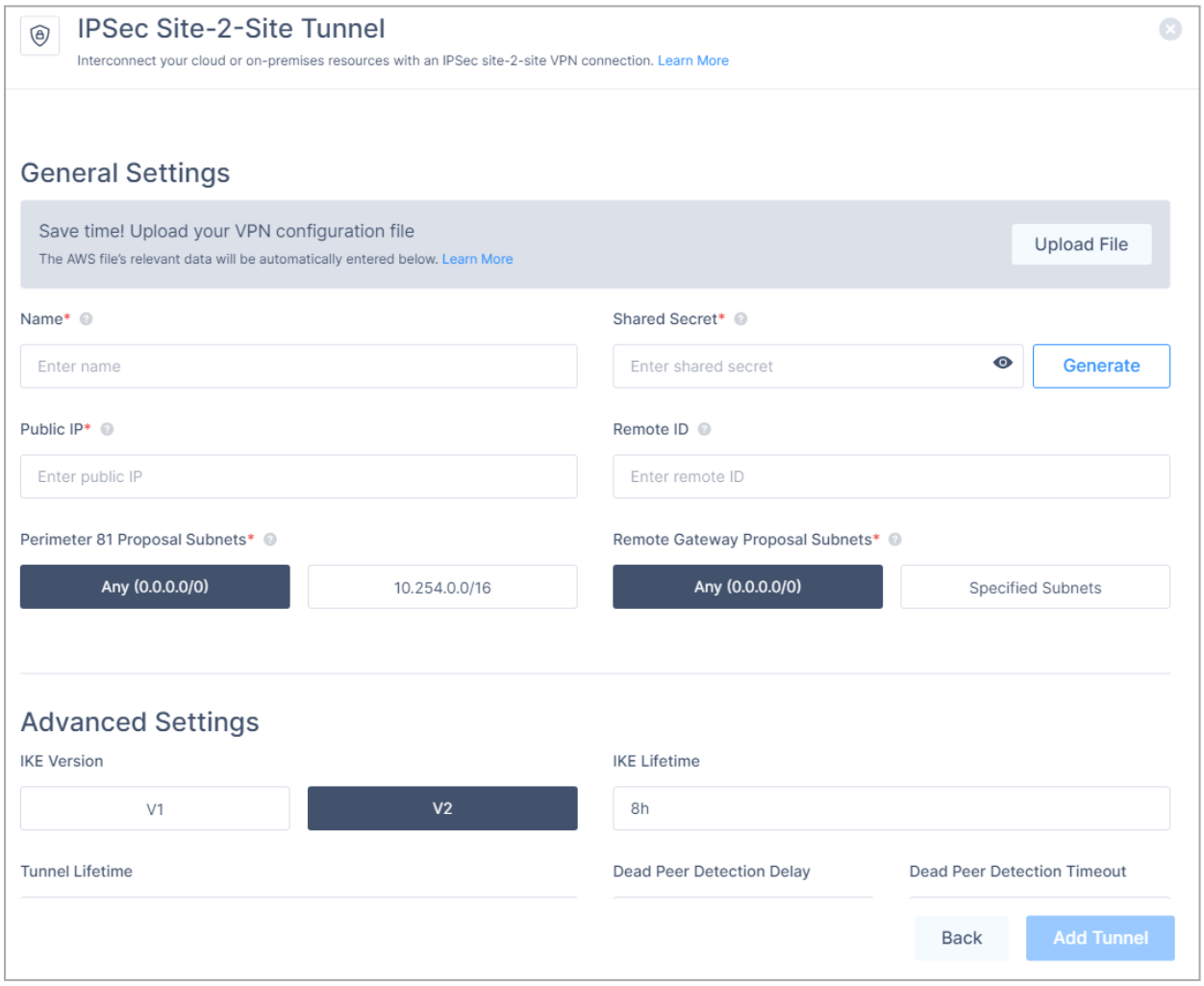
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. To automatically populate the tunnel configuration values, in the **General Settings** section, click **Upload File** and upload the configuration file downloaded from the AWS Management console.

7. For manual configuration, open the configuration file you downloaded and copy the below values and paste it for **Public IP**, **Remote ID** (both identical), and **Shared Secret**.

```
Outside IP Addresses:
  - Customer Gateway                    : 45.[redacted].73
  - Virtual Private Gateway             : 13.[redacted]109

Inside IP Addresses
  - Customer Gateway                    : 169.254.241.30/30
```

Perimeter81 Gateway

Remote Public IP and ID

```
IPSec Tunnel #1
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
The address of the external interface for your customer gateway must be a static address.
Your customer gateway may reside behind a device performing network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to unblock UDP port 4500.
| If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.
  - IKE version             : IKEv2
  - Authentication Method   : Pre-Shared Key
  - Pre-Shared Key          : CYyjvw[redacted]3hGT2
  - Authentication Algorithm : sha1
  - Encryption Algorithm    : aes-128-cbc
  - Lifetime                : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Diffie-Hellman          : Group 2
```

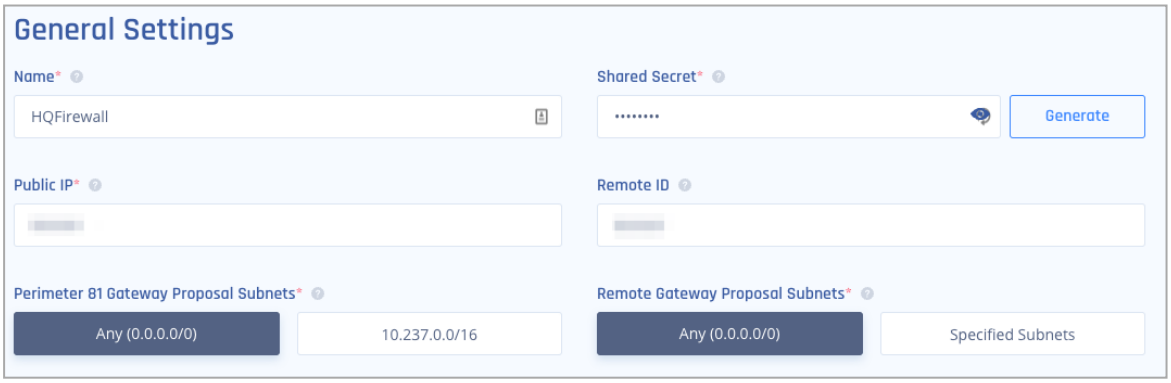
Shared key

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

   a. **Name** - Name of the tunnel.

   b. **Perimeter 81 Gateway Proposal Subnets** - **Any (0.0.0.0/0)**.

   c. **Remote Gateway Proposal Subnets** - **Any (0.0.0.0/0)**.



9. In the **Advanced Settings** section, enter the information for your tunnel type:

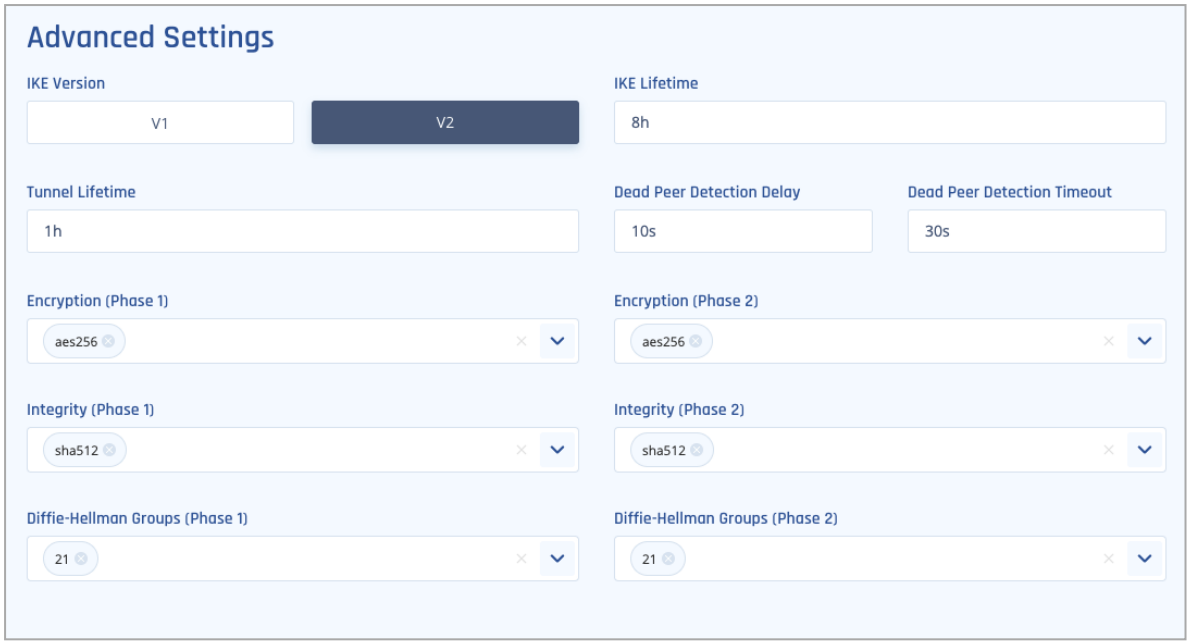
Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

Make sure to verify the tunnel settings under section 3 in the configuration.



10. Click **Add Tunnel**.

AWS Transit Gateway

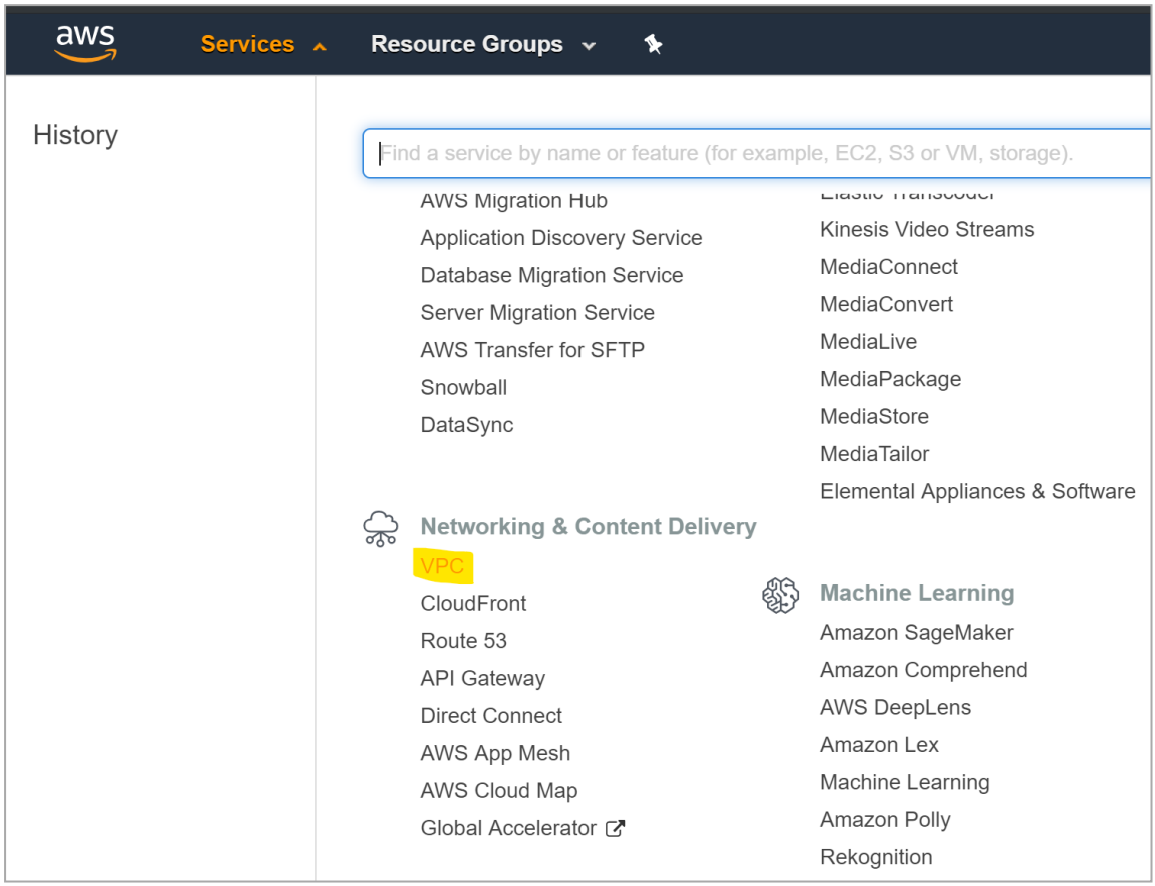
Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

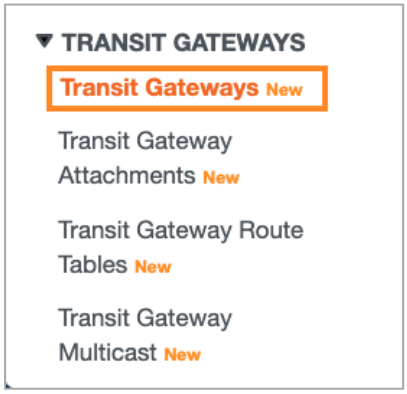
Step 1 - Configurations in the AWS Management Console

Creating the Transit Gateway and Transit Gateway Attachments

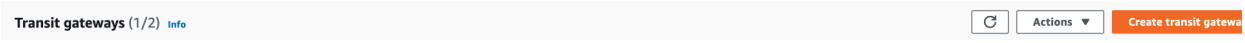
1. Access the AWS Management console and go to the **VPC** section.



2. On the left pane, click **Transit Gateways**.



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



The **Create transit gateway attachment** page appears.

4. In the **Name tag** field, enter a name of the Transit Gateway.

   Keep the default values for rest of the fields.

5. Click **Create transit gateway**.

Creating the Transit Gateway Attachments

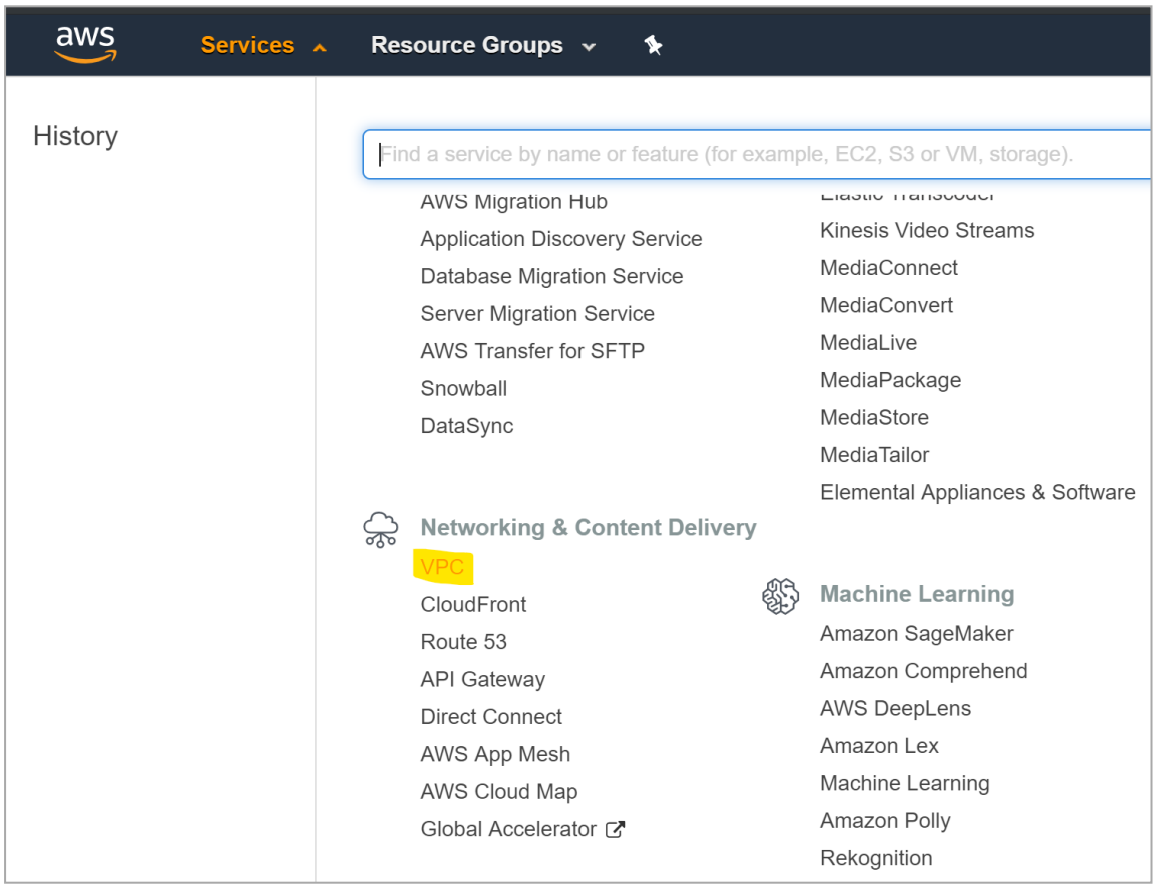
You can create an attachment for VPCs, other VPNs, and other Peered Transit Gateways located on another AWS region. All connected attachments can communicate with each other as defined in the Transit Gateway's routes.

A single VPC attachment connects one VPC to the Transit Gateway. You may connect multiple VPC attachments to a single Transit Gateway.

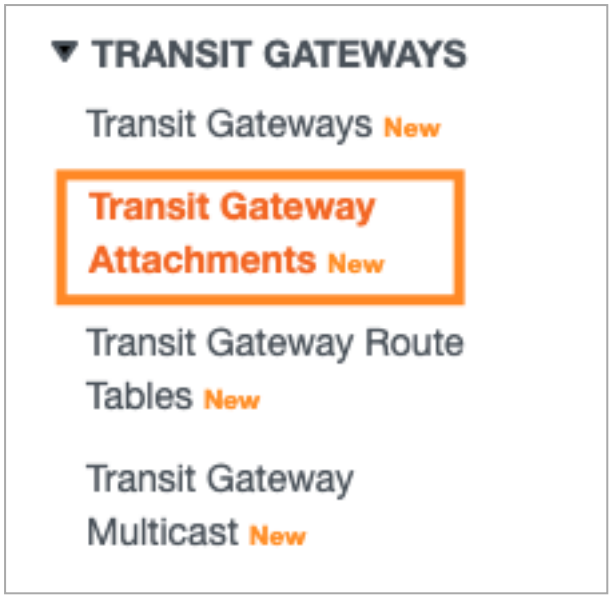
Creating the Transit Gateway VPC Attachments

Note - If you already have a Transit Gateway Attachment to your VPC, skip this procedure and go to *"Creating the Transit Gateway VPN Attachment" on page 449*.

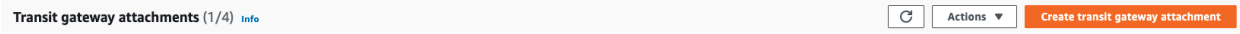
1. Access the AWS Management console and go to the **VPC** section.



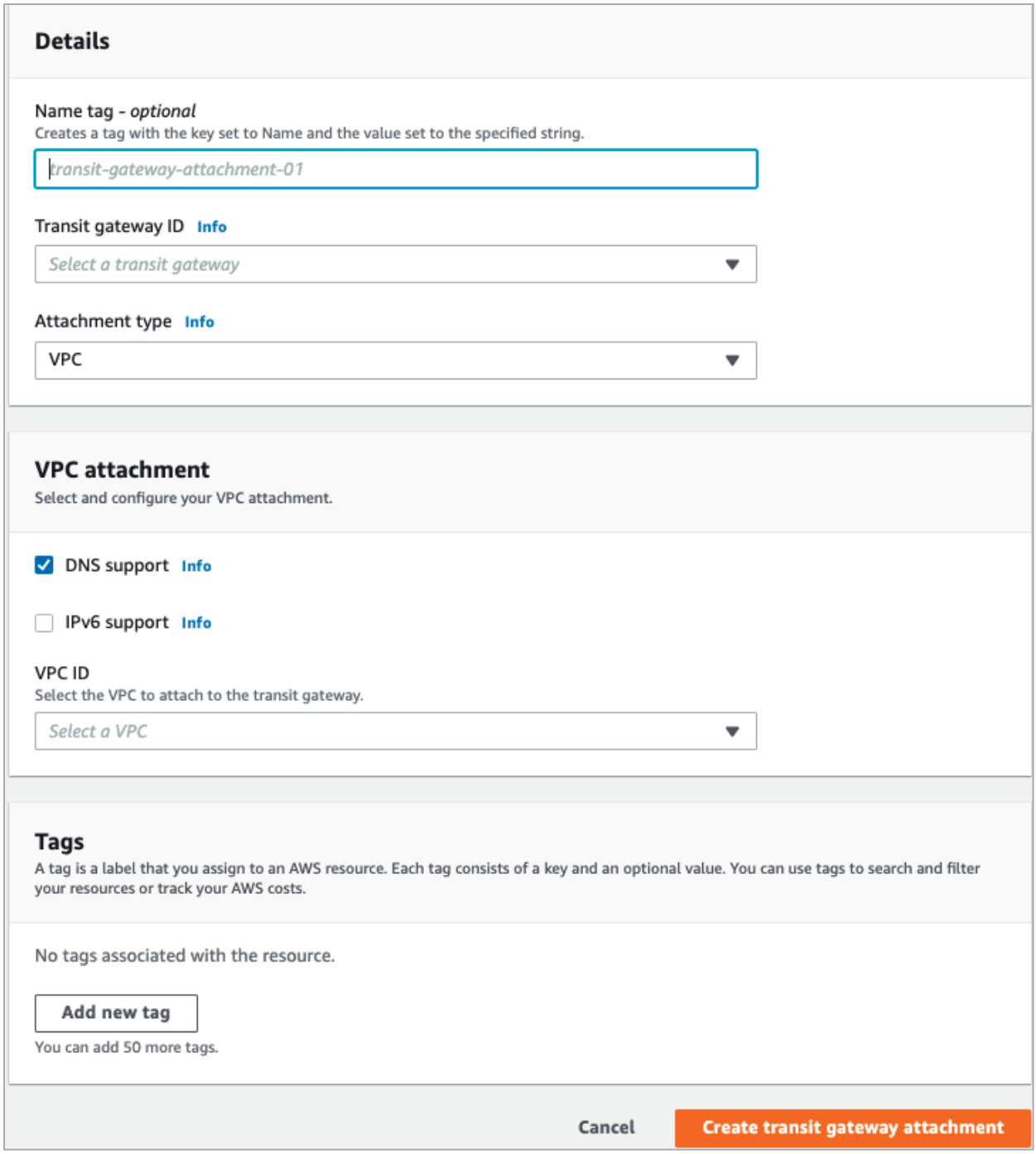
2. On the left pane, click **Transit Gateway Attachments**.



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



The **Create transit gateway attachment** page appears.



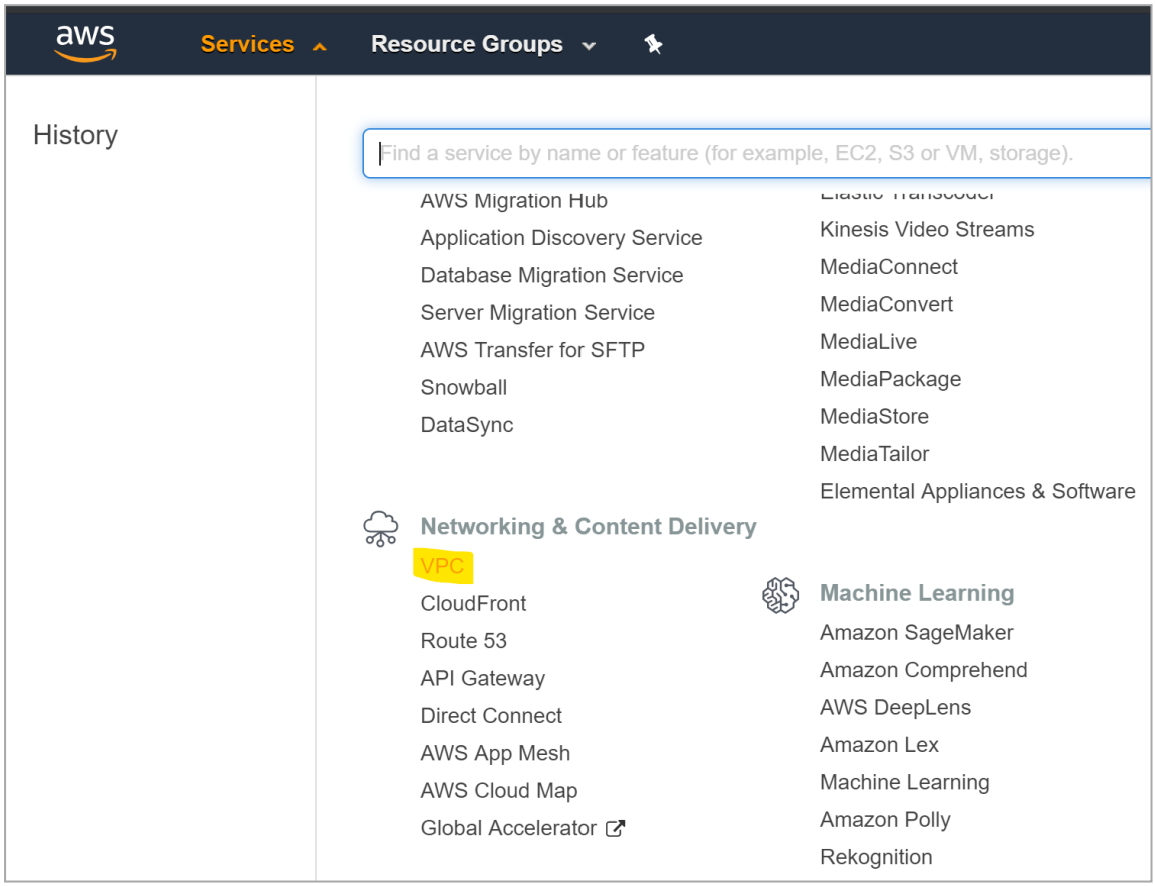
4. Enter these:
   a. **Name Tag** - Name of the Transit Gateway Attachment.
   b. **Transit gateway ID** - Select the newly created Transit gateway.
   c. **Attachment Type** - VPC
   d. **VPC ID** - Select the relevant VPC.

      Keep the default values for rest of the fields.
5. Click **Create transit gateway attachment**.

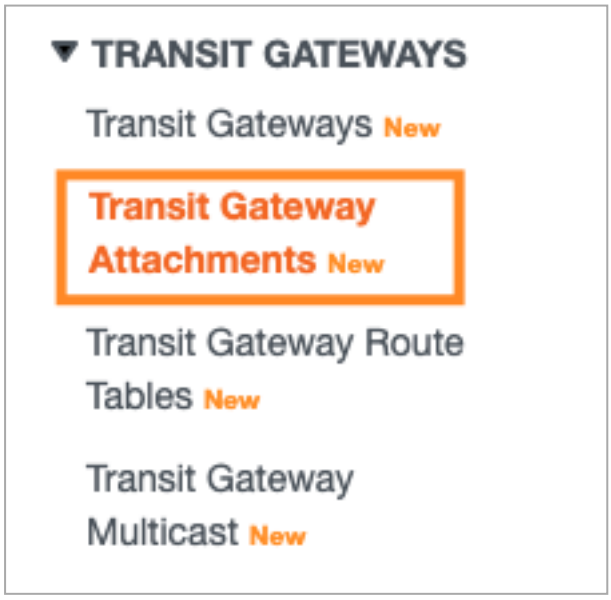
Note - Repeat the above procedure for each of the VPCs that you want to access to.

Creating the Transit Gateway VPN Attachment

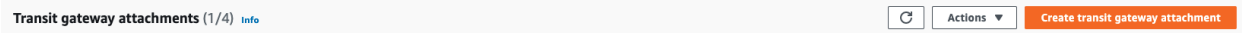
1. Access the AWS Management console and go to the **VPC** section.



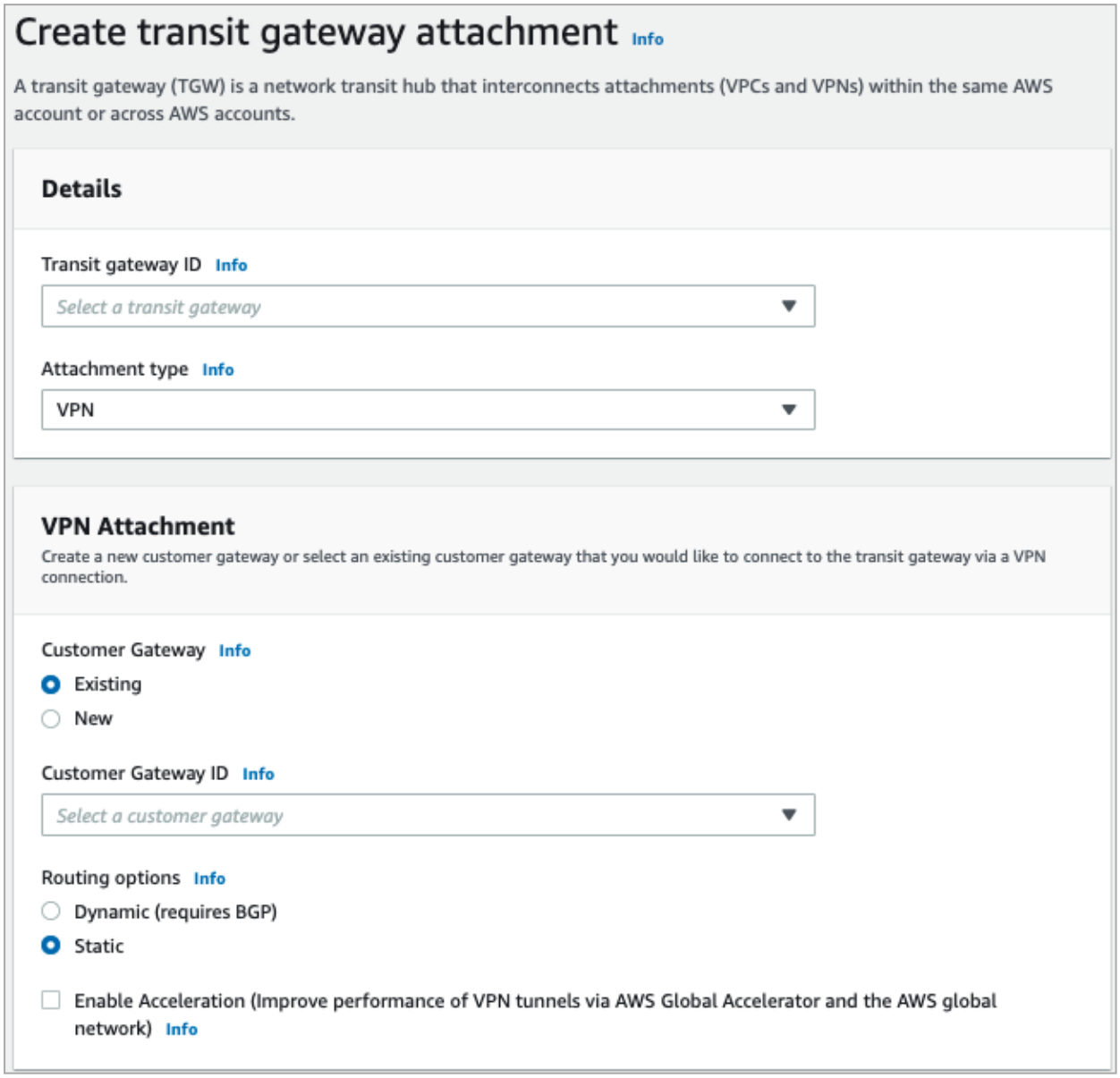
2. On the left pane, click **Transit Gateway Attachments**.



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



The **Create transit gateway attachment** page appears.



4. Enter these:

   a. **Transit gateway ID** - Select the newly created Transit gateway.

   b. **Attachment Type** - VPN

   c. **Customer Gateway** - New

d. **IP address** - IP address of the relevant Gateway in the Harmony SASE Administrator Portal.

e. **BGP ASN** - Keep the default value.

f. **Routing Options** - Static

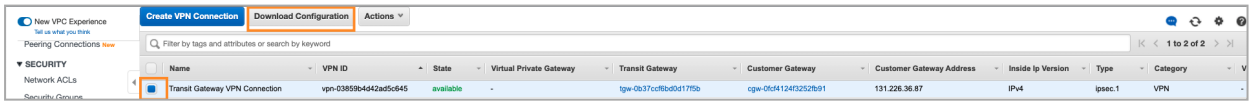
Keep the default values for rest of the fields.

5. Click **Create transit gateway attachment**.

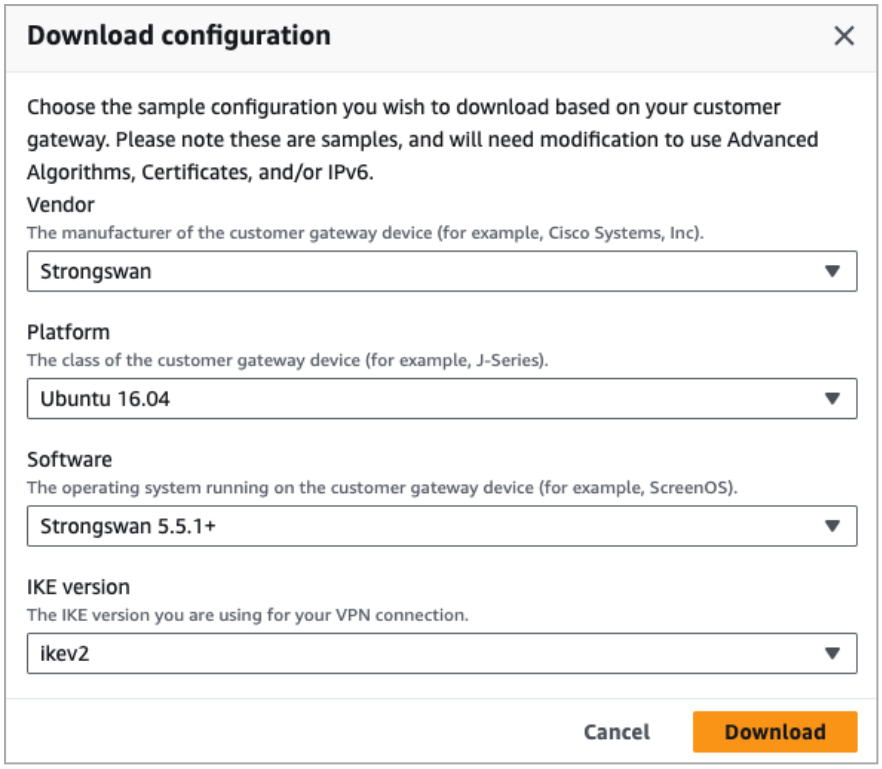
Configuring the Tunnel

1. Access the AWS Management console and on the left pane, in the **Virtual Private Network (VPN)** section, click **Site-to-Site VPN Connections**.

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



The **Download configuration** window appears.



4. Enter these:
   a. **Vendor** - Strongswan
   b. **Platform** - Ubuntu version
   c. **Software** - Strongswan version
   d. **Ike version** - Ikev2
5. Click **Download**.

Configuring the Routing

1. Access the AWS Management console and go to the **VPC** section.
2. In the **Transit Gateways** section, select **Transit Gateway Route Tables**.

3. Select the relevant Transit Gateway Route Table.
4. If your routes do not propagate automatically:

a. At the bottom, click **Propagations**.

b. Verify that all of the Transit Gateway Attachments are included.

> **Note** - If any of the Transit Gateway Attachments is missing a route, click **Create propagation** and add the missing route.

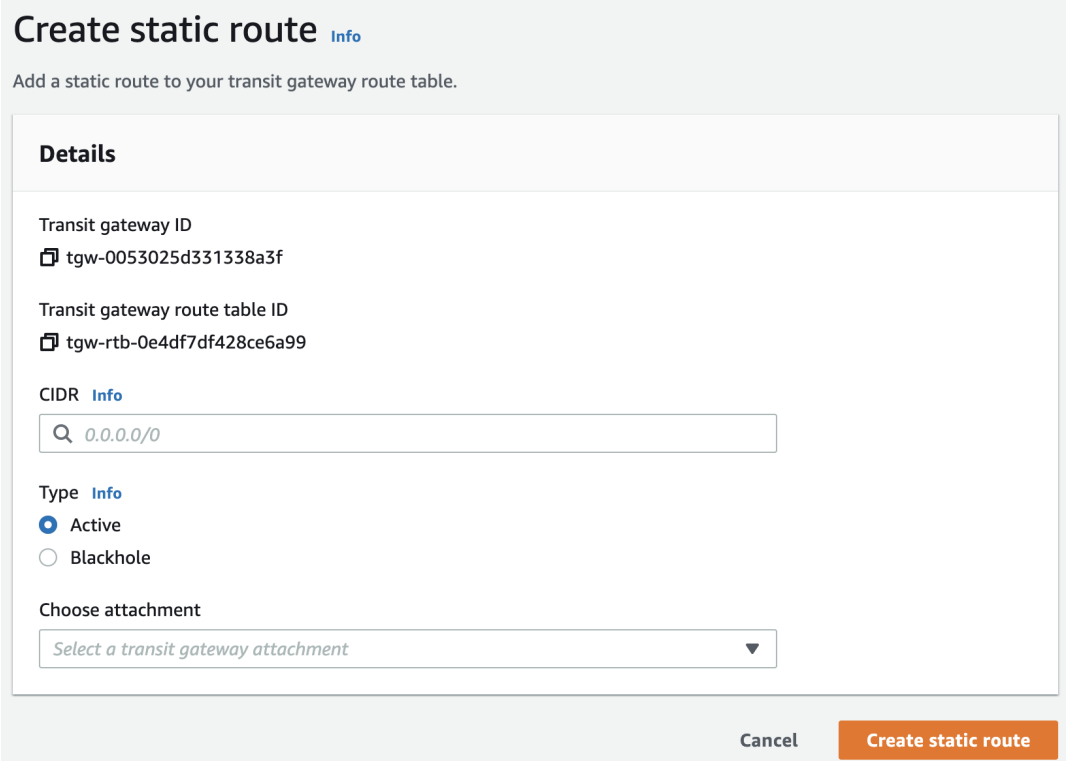
c. At the bottom, click **Associations**.

d. Verify that all of the Transit Gateway Attachments are included (same as the previous step).

> **Note** - If any of the Transit Gateway Attachments is missing a route, click **Create propagation** and add the missing route.

e. At the bottom, click **Routes**.

The **Create static route** window appears.



f. In the **CIDR** field, enter your Harmony SASE subnet. To find your Harmony SASE network subnet:

   i. Go to the Harmony SASE Administrator Portal > **Networks** page.

   ii. In your network, click ··· next to your network.

   iii. Click **Edit Network**.

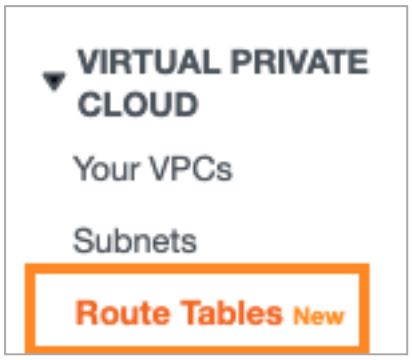
   iv. Copy the **Subnet** value.

g. Select **Type** as **Active**.

h. From the **Choose attachment** list, select the VPN attachment.

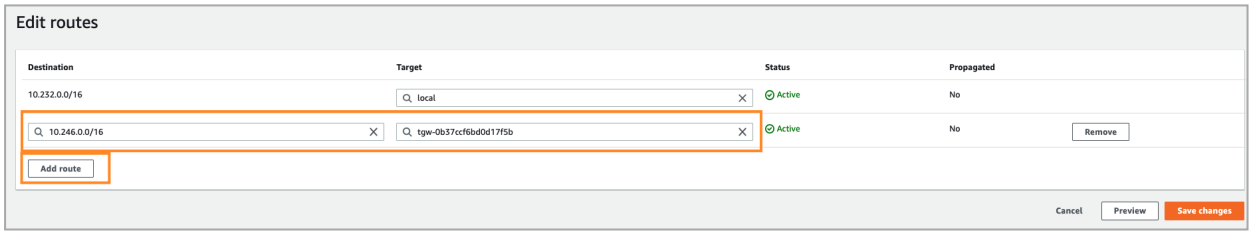
i. Click **Create static route**.

5. In the left pane, in the **Virtual Private Cloud** section, click **Route Tables**.



6. Select the Route Table for one of the attached VPCs.
7. At the bottom, click **Routes**.
8. Click **Edit Routes**.

   The **Edit routes** window appears.



9. Click **Add route**.
10. Enter these:

    a. **Destination** - Your Harmony SASE subnet. To find your Harmony SASE network subnet, see step 4f above.

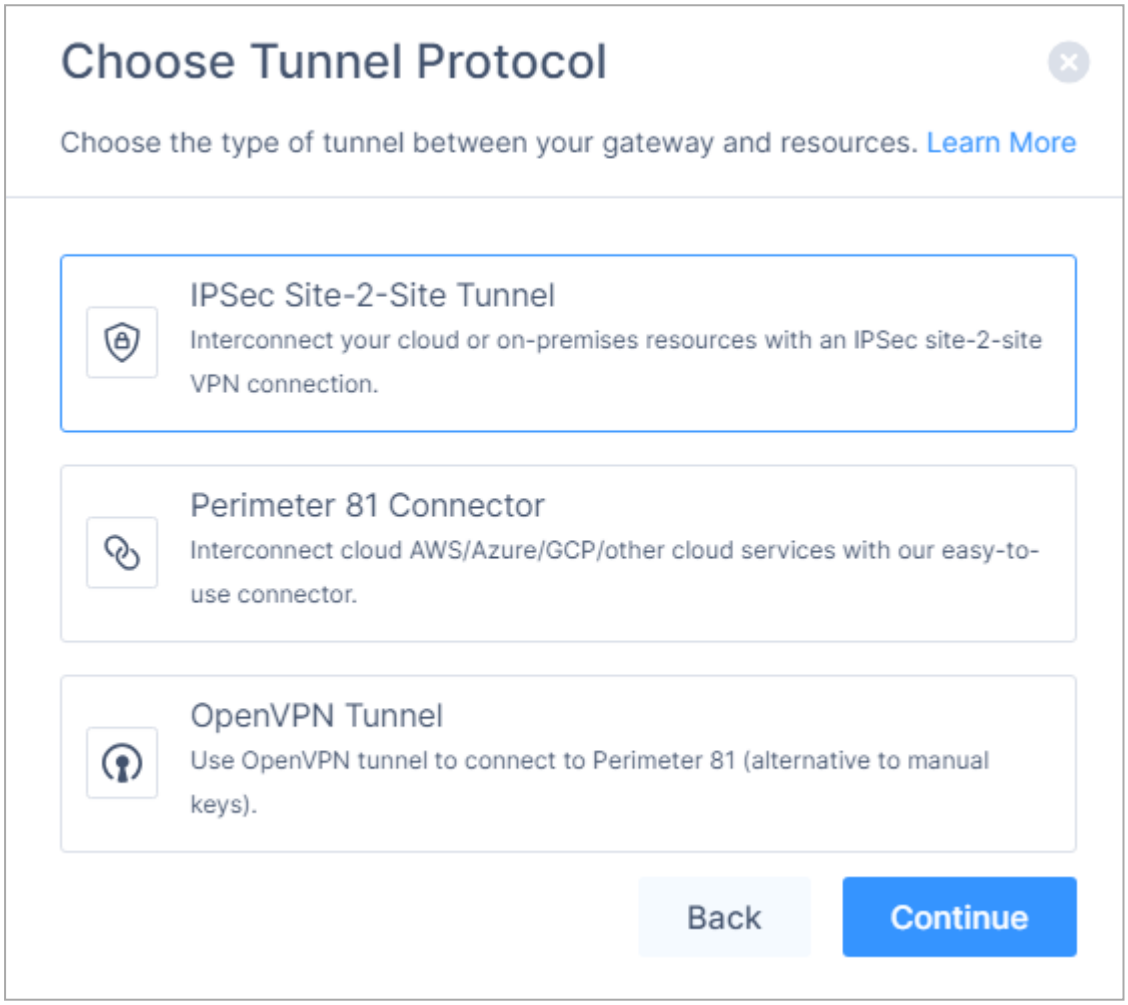
    b. **Target** - Select Transit Gateway and pick the relevant Transit Gateway.

11. Click **Save changes**.

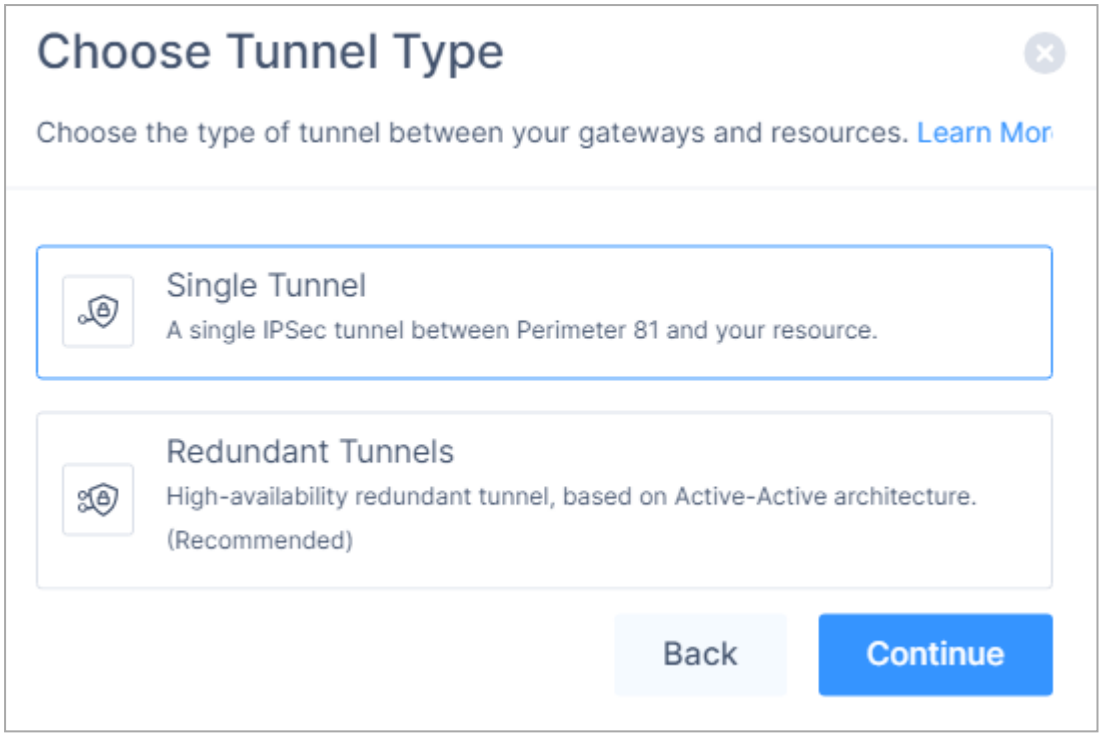
Step 2 - Creating the Tunnel in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.

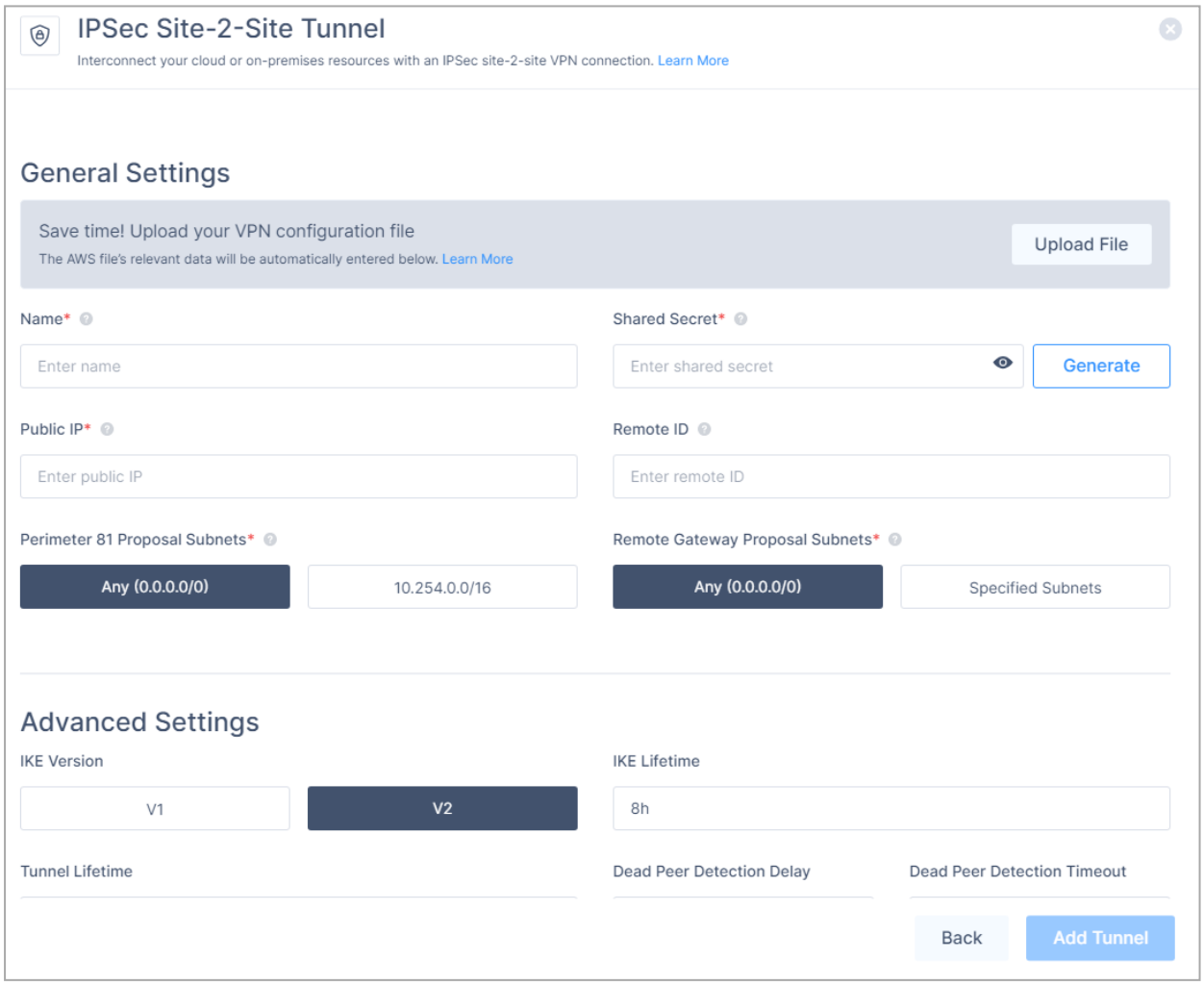
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. To automatically populate the tunnel configuration values, in the **General Settings** section, click **Upload File** and upload the configuration file downloaded from the AWS Management console.

7. For manual configuration, open the configuration file you downloaded and copy and paste these attributes.

   a. **Shared Secret** - Paste the value marked in yellow. Omit the quotation marks.

   b. **Public IP & Remote ID** - Paste the IP address marked in red. This is your AWS external IP address.

```
4) Create a new file at /etc/ipsec.secrets if it doesn't already exist, and append this
line to the file (be mindful of the spacing!). This value authenticates the tunnel
endpoints:
185.253.69.17 18.16.10.253 : PSK "QzquwHAcOTfLR0yuKRVrqSAbO"
```

   c. **Perimeter 81 Gateway Proposal Subnets** - 0.0.0.0/0.

   d. **Remote Gateway Proposal Subnets** - 0.0.0.0/0.

8. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

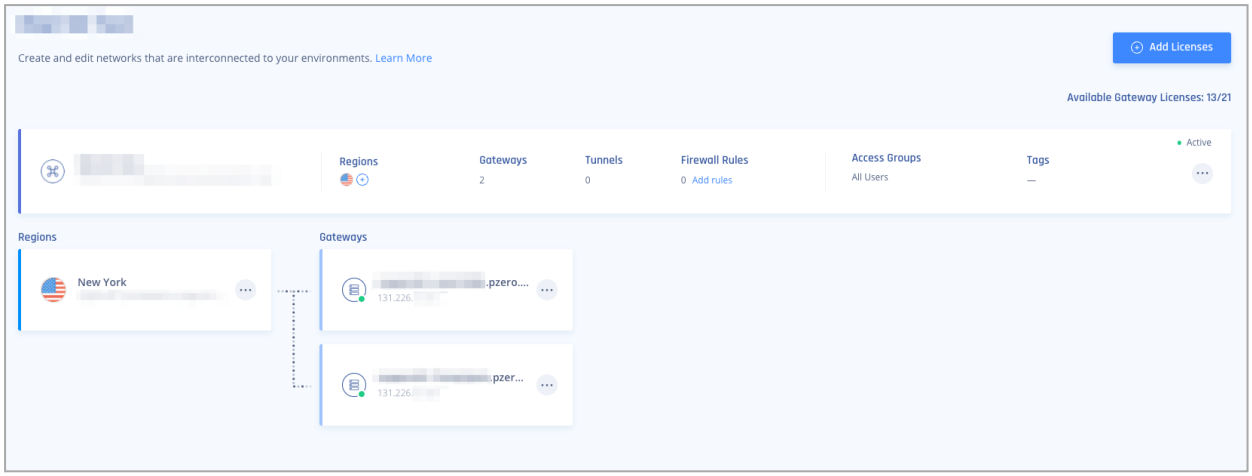
9. Click **Add Tunnel**.

AWS Redundant Tunnels - Virtual Private Gateway

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Harmony SASE network must have at least two different gateways in the same network.



Notes -

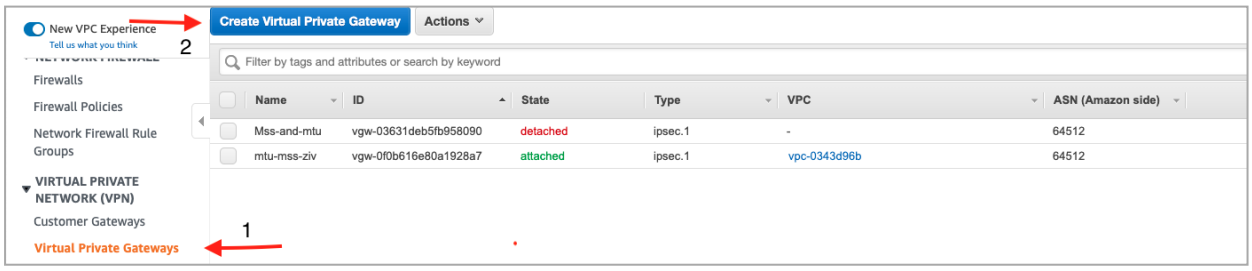
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the AWS Management Console

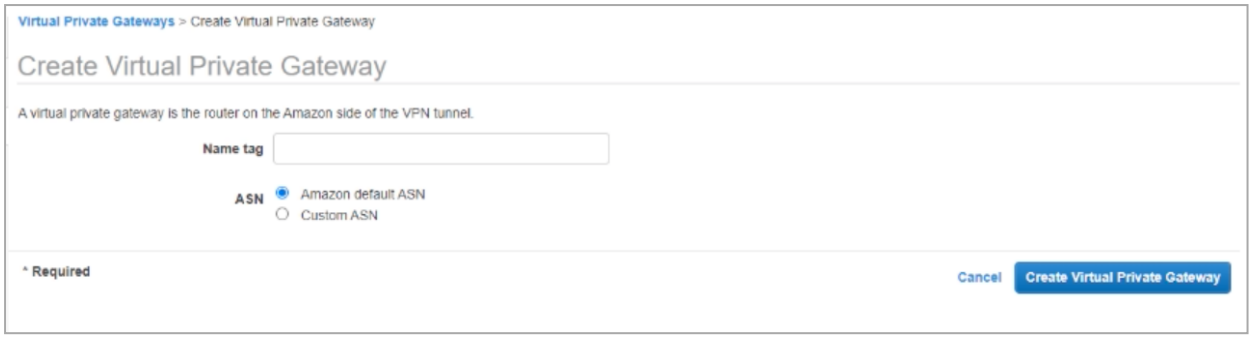
Creating a Virtual Private Gateway

Note - If you already have a Virtual Private Gateway in your AWS region, skip this procedure.

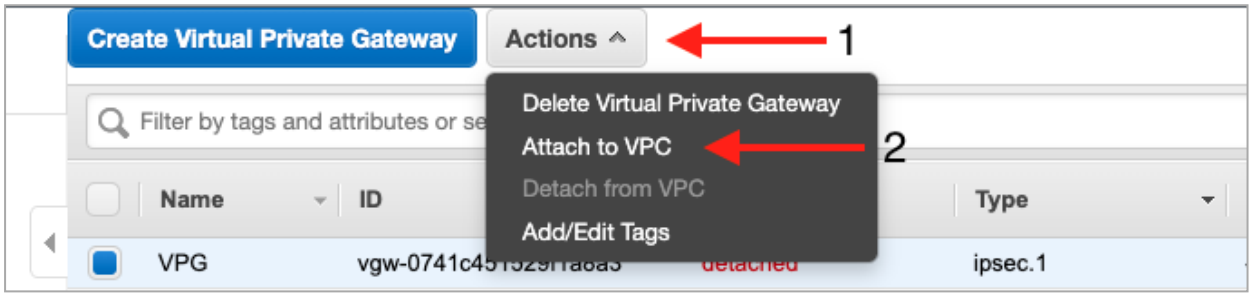
1. Access the AWS Management Console and go to the **VIRTUAL PRIVATE NETWORK (VPN)** section.
2. Click **Virtual Private Gateways** > **Create Virtual Private Gateway**.



3. Create the Virtual Private Gateway with the default settings.



4. Select the newly created Virtual Private Gateway and on the top, click **Actions** > **Attach to VPC**.



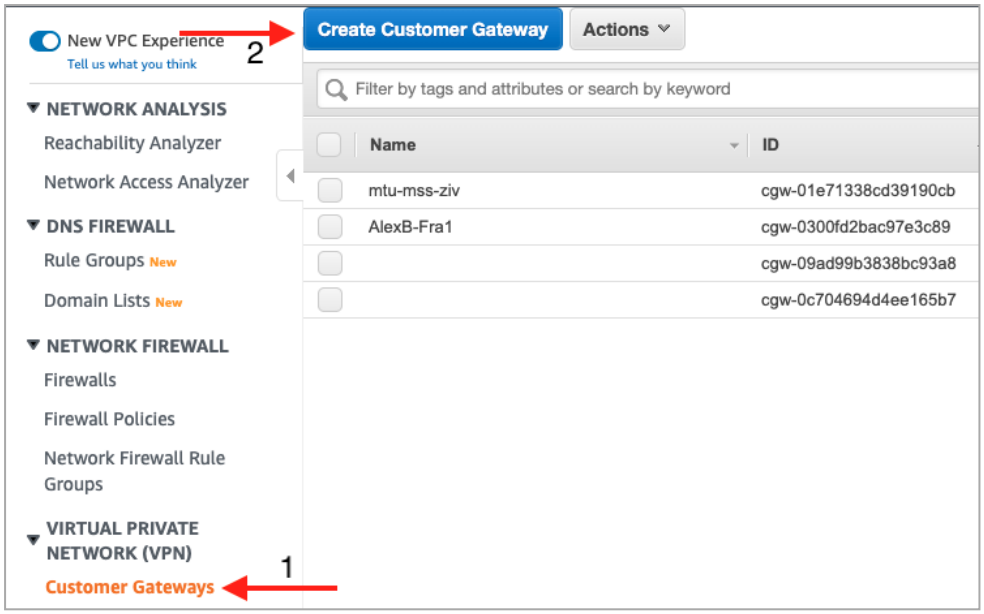
The **Attach to VPC** window appears.

5. From the **VPC** drop-down list, select the relevant VPC.

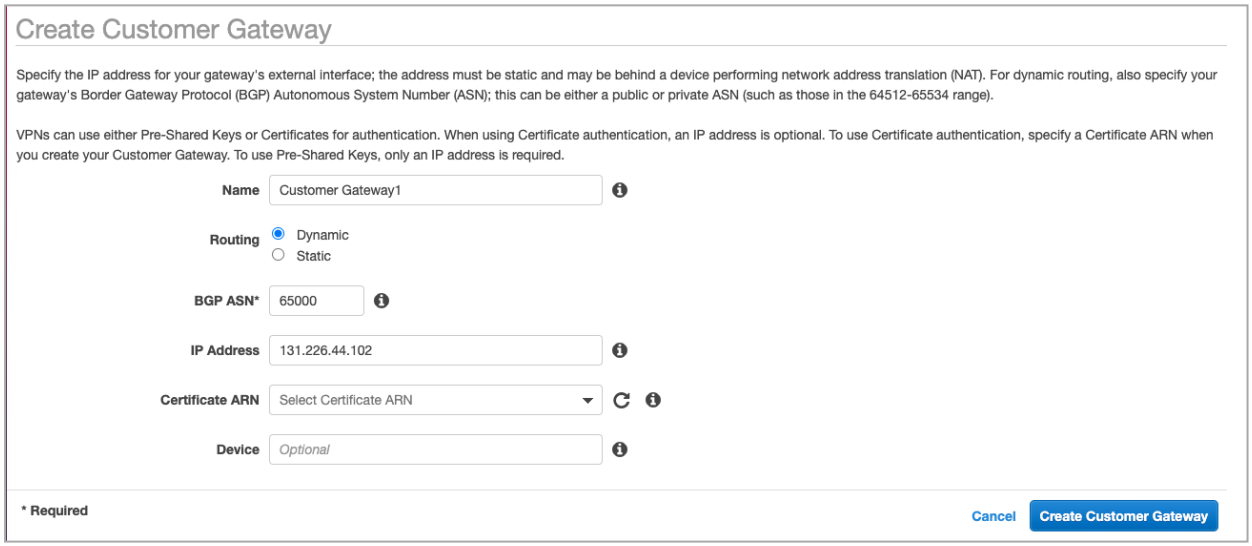
6. Click **Yes, Attach**.

Creating Two Customer Gateways

1. Access the AWS Management Console and go to the **VIRTUAL PRIVATE NETWORK (VPN)** section.
2. Click **Customer Gateway** > **Create Customer Gateway**.



The **Create Customer Gateway** window appears.



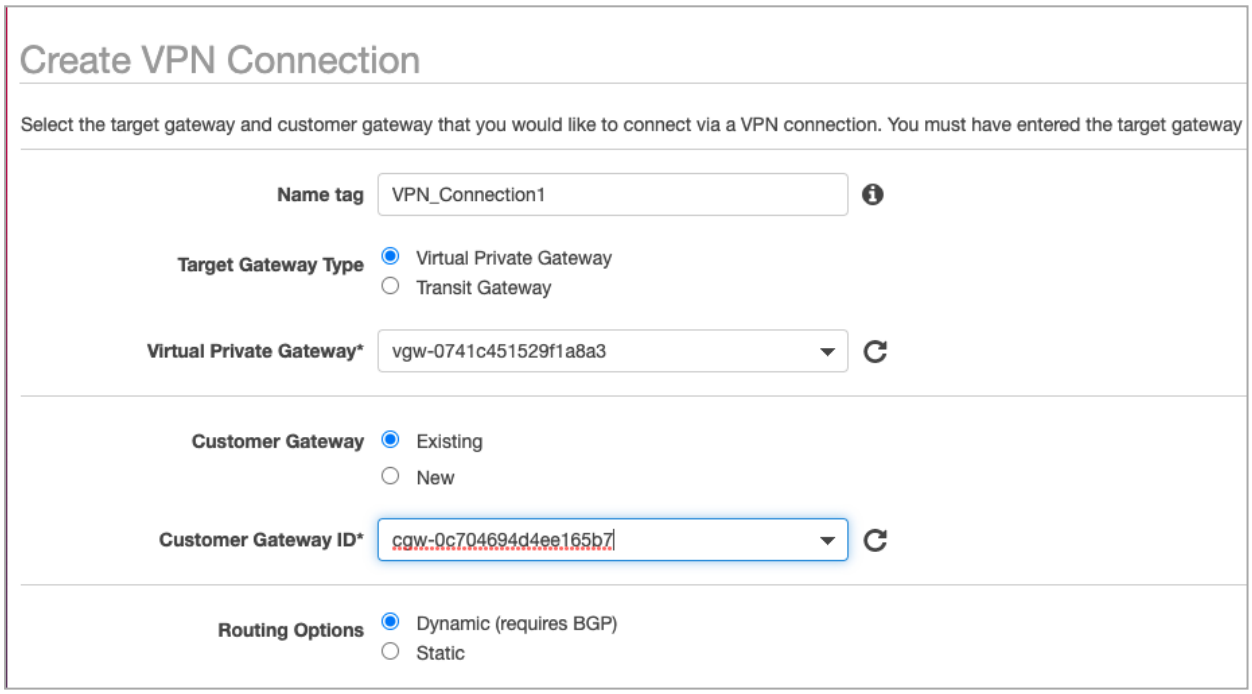
3. Enter these:
   a. **Name** - Name of the gateway.
   b. **Routing** - Dynamic.
   c. **IP Address** - IP address of the first Harmony SASE gateway.
   d. **BGP ASN** - ASN for the Harmony SASE gateway. Keep it as 65000.
4. Click **Create Customer Gateway**.
5. To create the second customer gateway, repeat steps 1- 4.

   In the **IP Address** field, enter the IP address of the second Harmony SASE gateway.

Creating Two Site-to-Site VPN Connections

1. Access the AWS Management Console.
2. In your AWS VPC, in the **VIRTUAL PRIVATE NETWORK(VPN)** section, click **Site-to-Site VPN Connections** > **Create VPN Connection**.

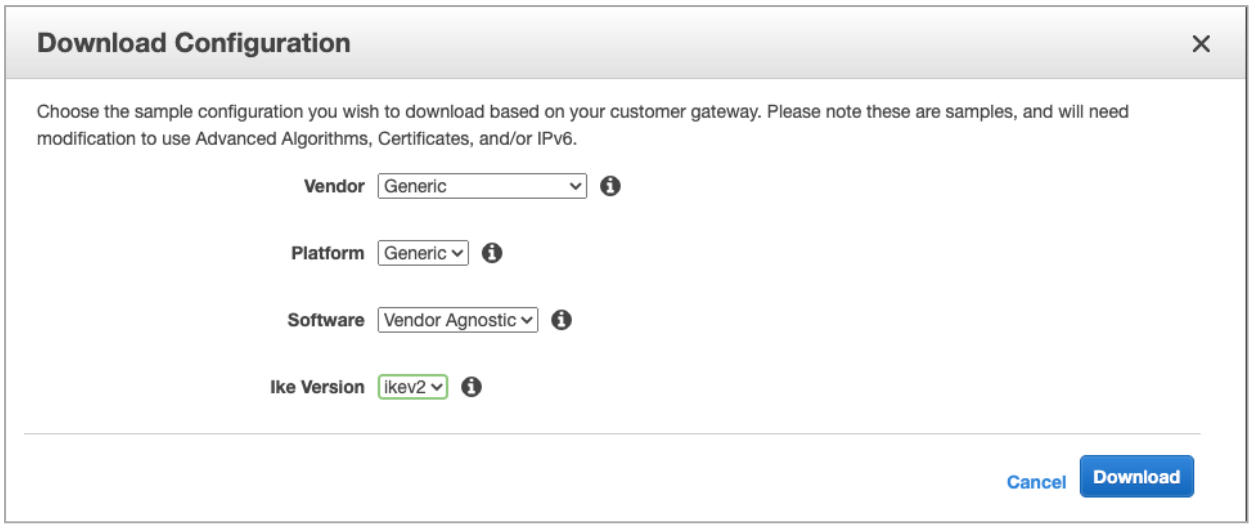
The **Create VPN Connection** window appears.



3. Enter these:
   a. **Target Gateway Type** - Virtual Private Gateway.
   b. **Virtual Private Gateway** - Select the first Virtual Private Gateway created.
   c. **Customer Gateway** - Existing.
   d. **Customer Gateway ID** - Select the first Customer Gateway created.
   e. **Routing Options** - Dynamic (requires BGP).

   Keep the other options to default.
4. Click **Download Configuration**.

The **Download configuration** window appears.

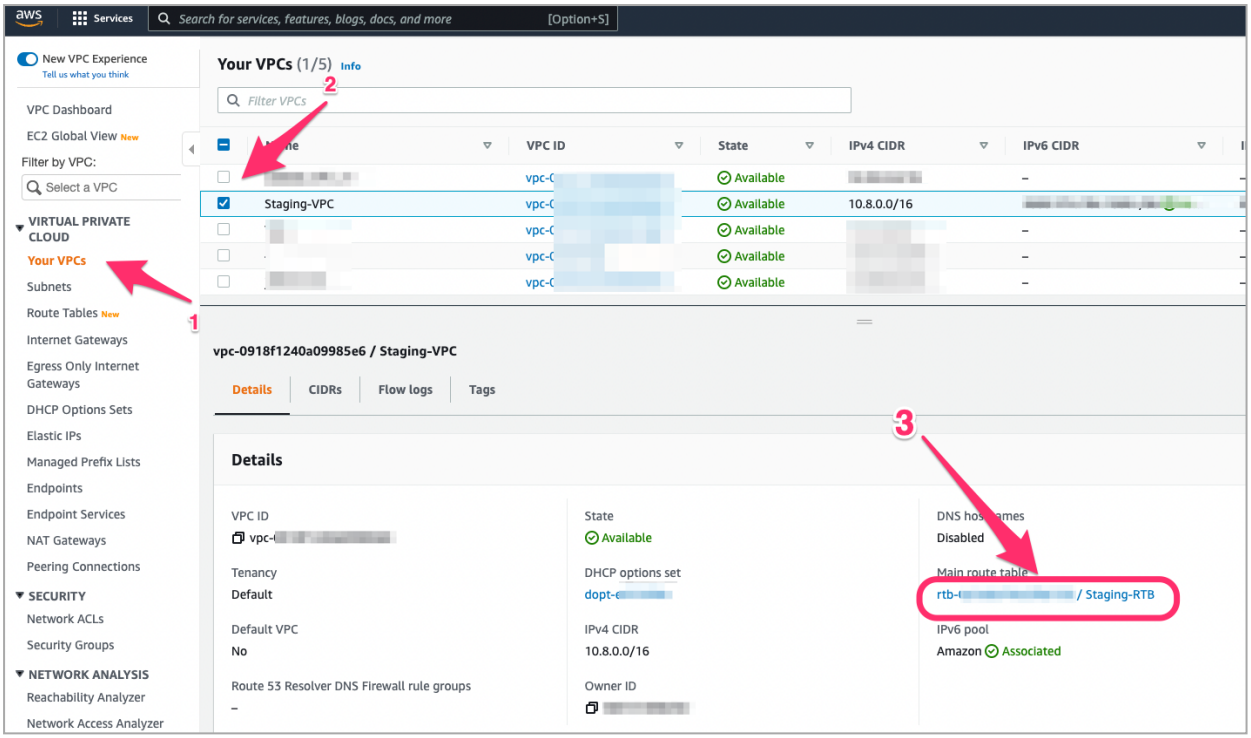


5. Enter these:
   a. **Vendor** - Generic
   b. **Platform** - Generic
   c. **Software** - Vendor Agnostic
   d. **Ike version** - Ikev2
6. Click **Download**.

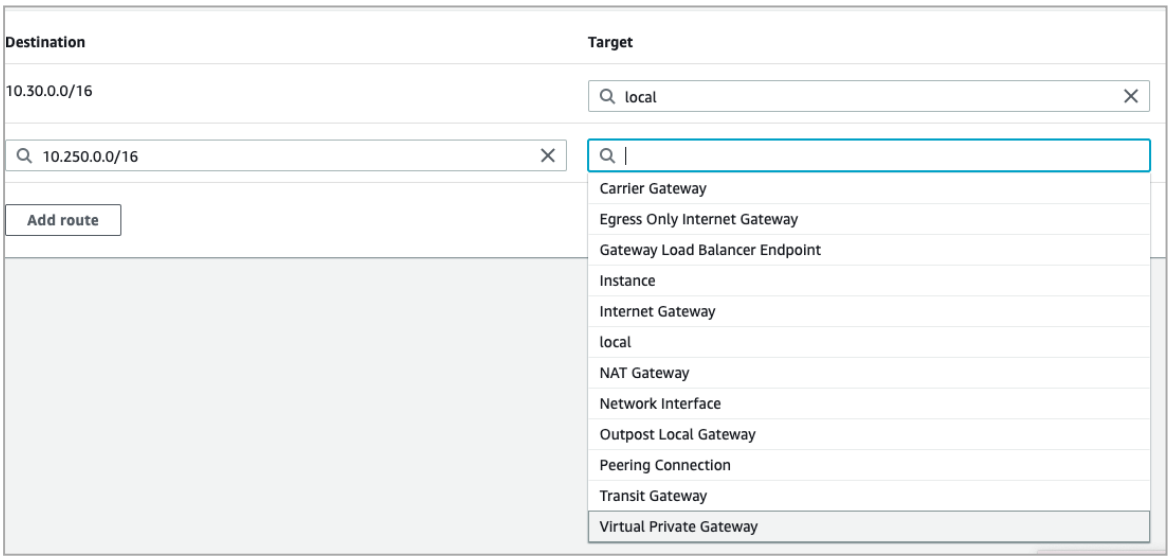
   The system downloads the file. Rename the file as *Tunnel1.txt*.
7. Repeat steps 1-6 for the second Customer Gateway.
8. Rename the second downloaded file as *Tunnel2.txt*.

Creating Static Routes

1. Access the AWS Management Console and Go to **VPC**.
2. Select the corresponding VPC attached to the Virtual Private Gateway and then select the **Main Route Table** for the VPC.



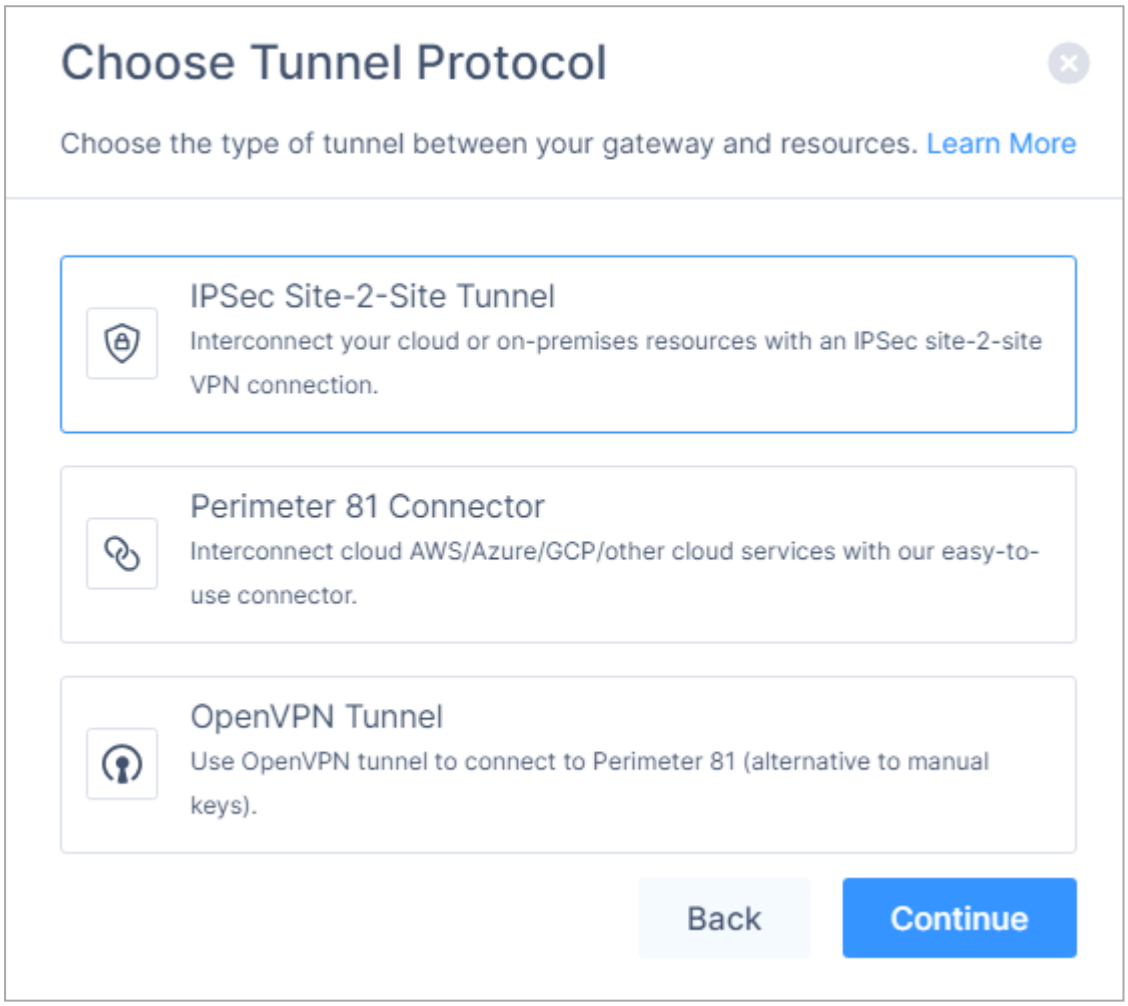
3. Edit the main Route Table for the VPC:
   a. In the **Destination** column, add the subnet mask of your Harmony SASE network.
   b. In the **Target** column, select **Virtual Private Gateway** (Route for reverse traffic).



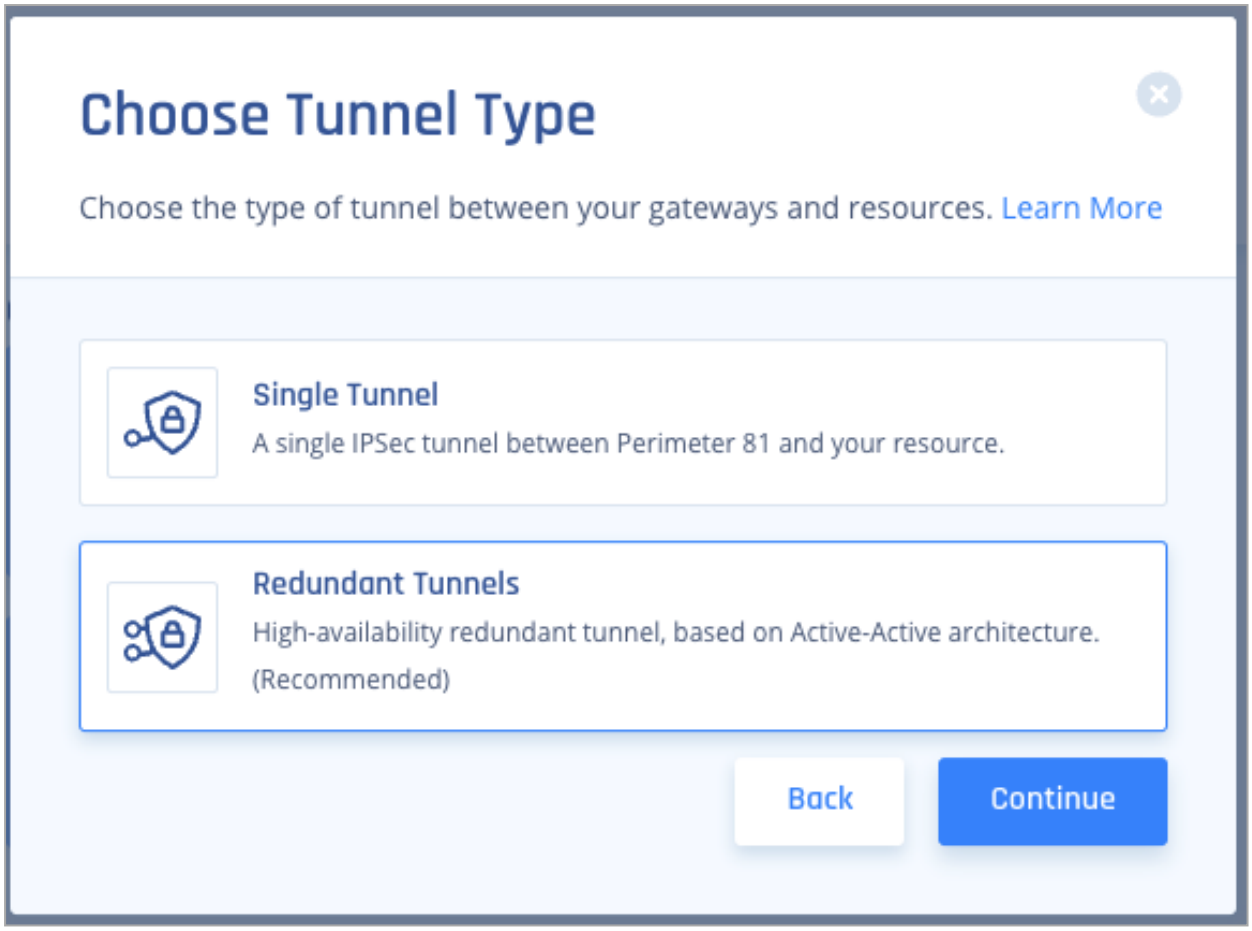
Note - If this is not the Main Route Table for the VPC, locate each subnet associated with the VPC and add the reverse route for the Harmony SASE internal subnet range.

Step 2 - Creating the Tunnels in the Harmony SASE Administrator Portal

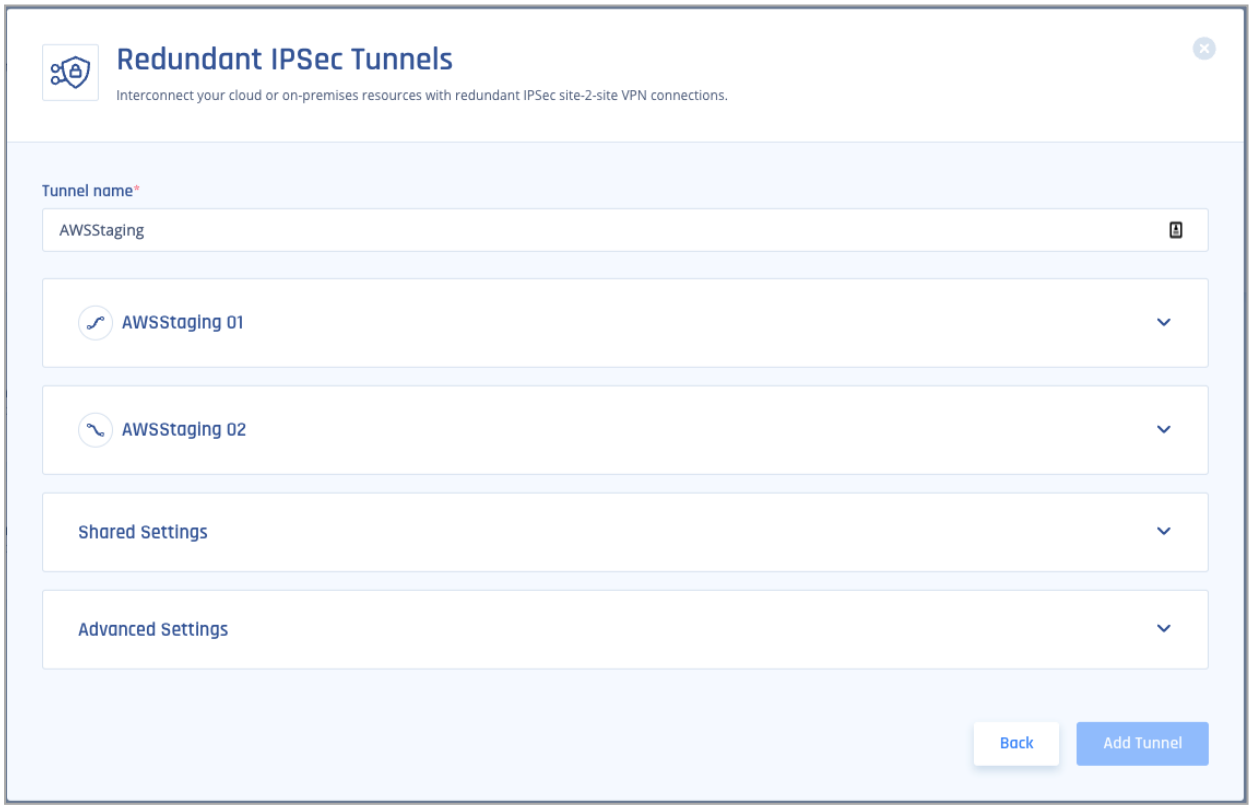
1. Access the Harmony SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.



6. For the first tunnel:

   a. Expand the **Tunnel 01** drop-down.

   b. To automatically populate the tunnel configuration values, click **Upload File** and upload Tunnel_1.txt file.

   c. For manual configuration, copy the values from Tunnel_1.txt file as shown below.

   a. **Shared Secret** - Pre-Shared Key

```
IPSec Tunnel #1
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
The address of the external interface for your customer gateway must be a static address.
Your customer gateway may reside behind a device performing network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to unblock UDP port 4500.
| If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.
  - IKE version          : IKEv2
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : CYyjwv[redacted]3hGT2
  - Authentication Algorithm : sha1
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Diffie-Hellman           : Group 2
```

Shared key

   b. **Harmony SASE gateway Internal IP** - Inside IP Addresses of Customer Gateway.

   c. **Remote Public IP & Remote ID** - Outside IP Addresses of Virtual Private Gateway.

   d. **Remote Gateway internal IP** - Inside IP Addresses of Virtual Private Gateway. The IP on the AWS side has a subnet (/30), discard it when pasting.

   e. **Remote Gateway ASN** - BGP Configuration Options of Virtual Private Gateway ASN from the file.

```
Outside IP Addresses:
  - Customer Gateway                    : 45.[redacted].73
  - Virtual Private Gateway             : 13.[redacted]109

Inside IP Addresses
  - Customer Gateway                     : 169.254.241.30/30
  - Virtual Private Gateway             : 169.254.241.29/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes

#4: Border Gateway Protocol (BGP) Configuration:

The Border Gateway Protocol (BGPv4) is used within the tunnel, between the inside
IP addresses, to exchange routes from the VPC to your home network. Each
BGP router has an Autonomous System Number (ASN). Your ASN was provided
to AWS when the Customer Gateway was created.

BGP Configuration Options:
  - Customer Gateway ASN           : 65000
  - Virtual Private  Gateway ASN          : 64512
  - Neighbor IP Address                     : 169.254.241.29
  - Neighbor Hold Time       : 30

Configure BGP to announce routes to the Virtual Private Gateway. The gateway
will announce prefixes to your customer gateway based upon the prefix you
assigned to the VPC at creation time.
```

Perimeter81 Gateway

Remote Public IP and ID

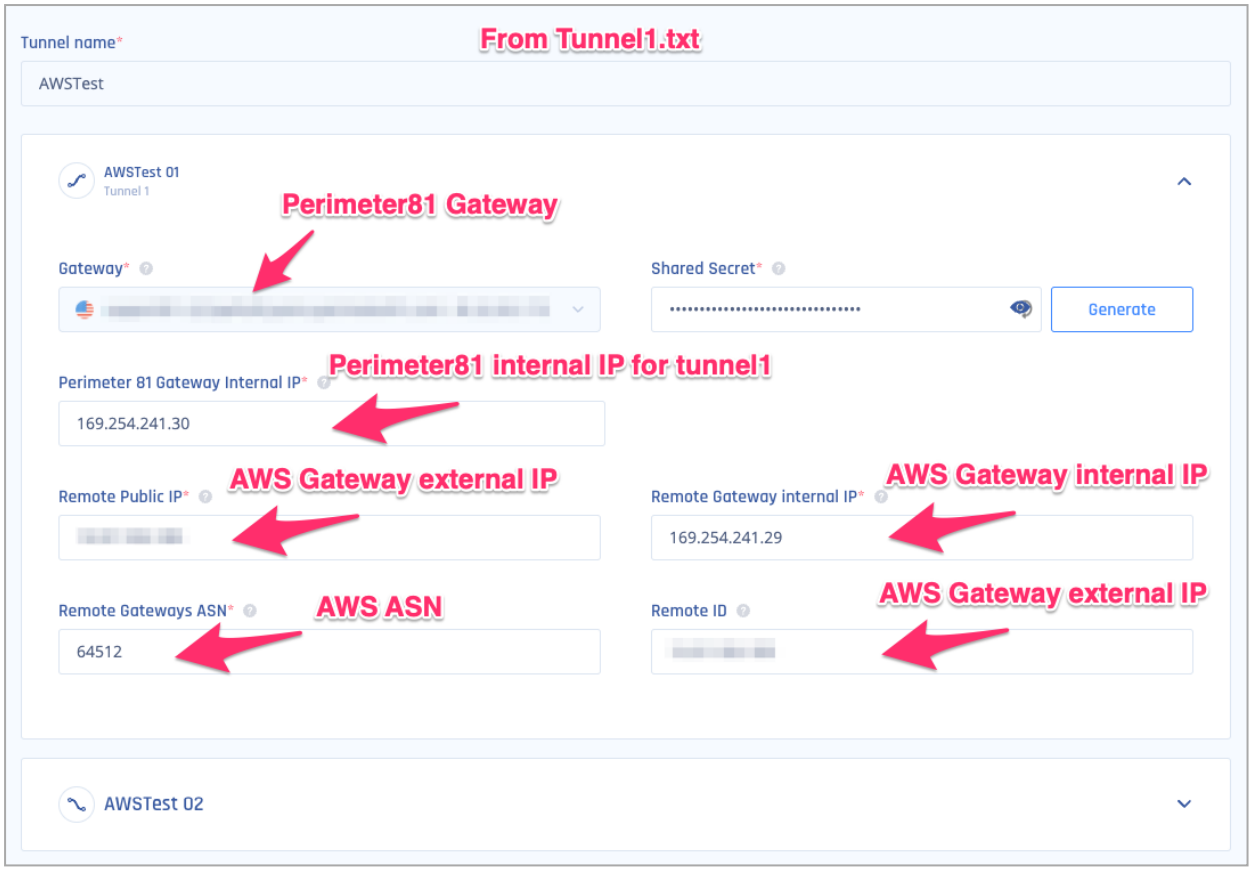
Perimeter81 Gateway internal IP

Remote Gateway internal IP

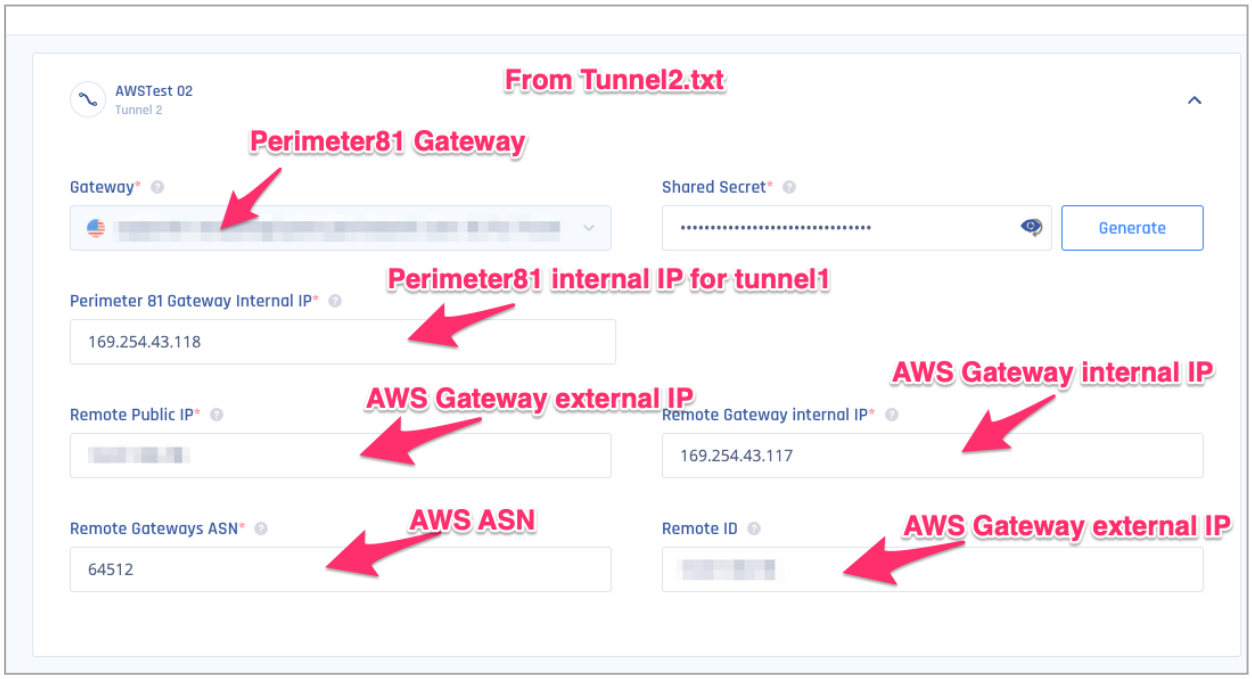
Perimeter81 ASN

AWS ASN

7. Enter the above copied values:



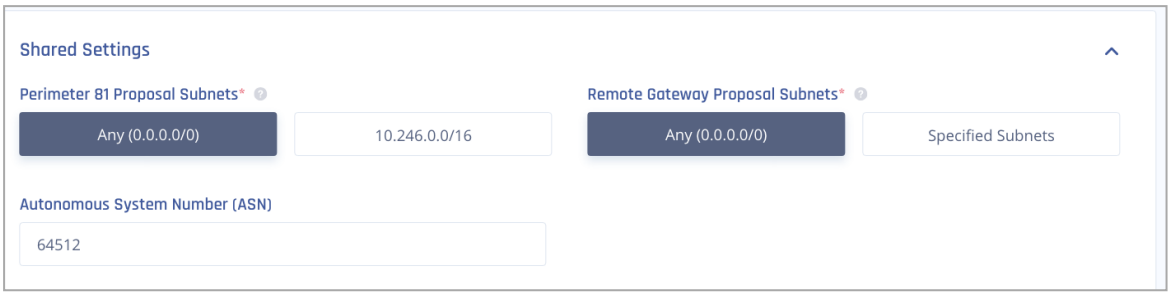
8. For the second tunnel, expand the **Tunnel 02** drop-down and repeat step 6 with the values from *Tunnel_2.txt* file.



9. In the **Shared Settings** section:

a. In the **Proposal Subnets** field, select **Any(0.0.0.0/0)** for both sides.

b. The **ASN** number should be the same as the Customer Gateway ASN you configured on the AWS Management console.



10. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

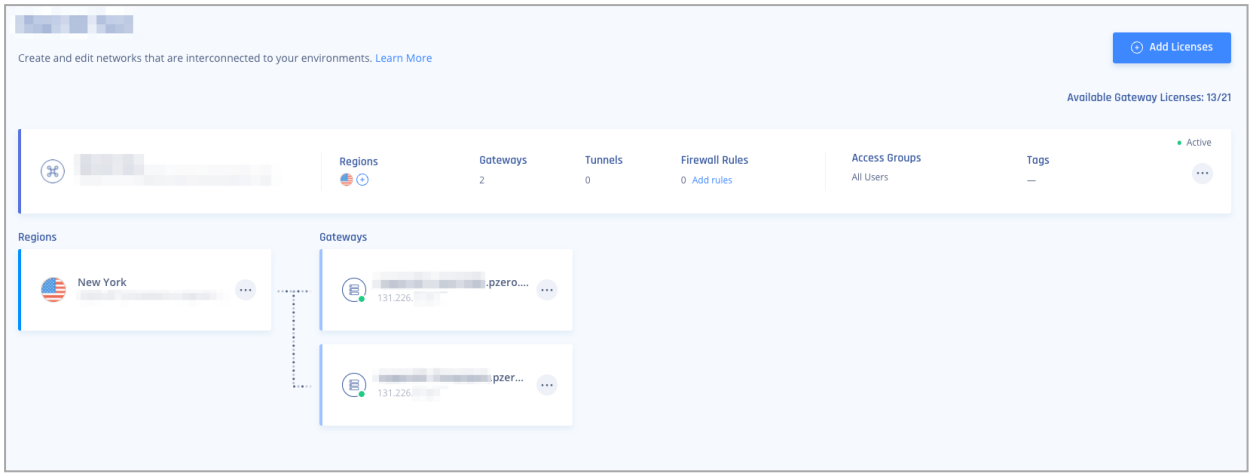
11. Click **Add Tunnel**.

AWS Redundant Tunnels - Transit Gateway

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Harmony SASE network must have at least two different gateways in the same network.



Notes -

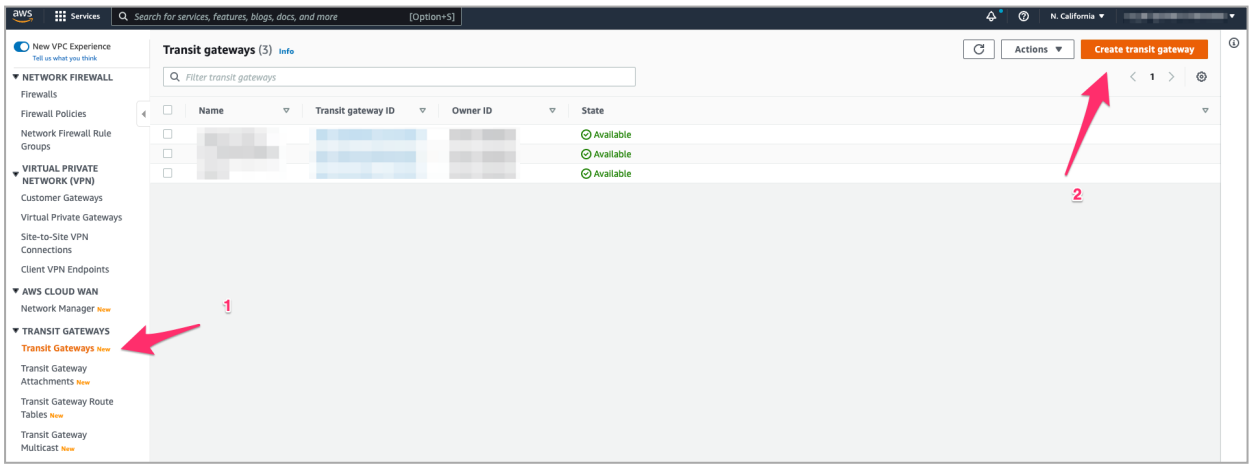
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the AWS Management Console

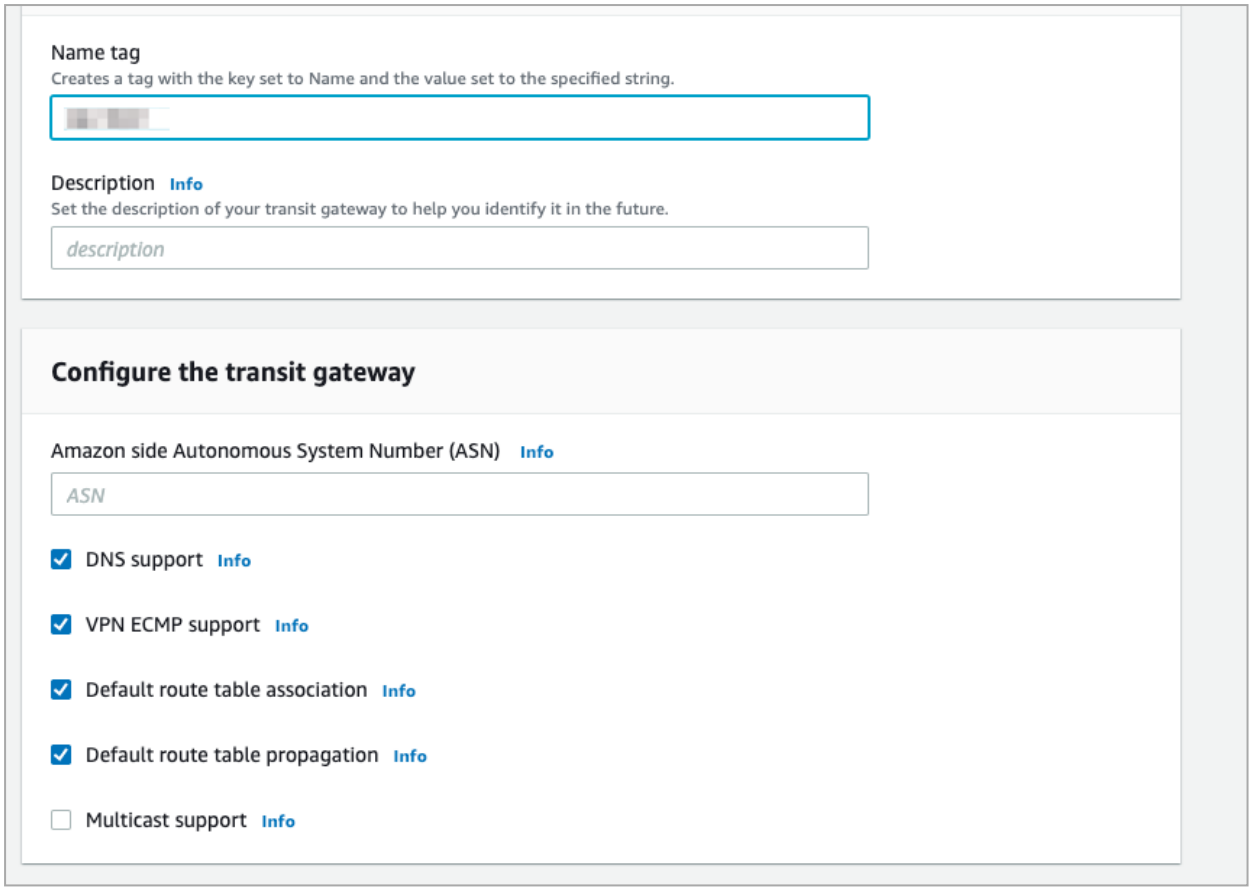
Creating a Transit Gateway

Note - If you already have a Transit Gateway in your AWS region, skip this procedure.

1. Access the AWS Management Console and go to the **TRANSIT GATEWAYS** section.
2. Click **Transit Gateway** > **Create transit Gateway**.



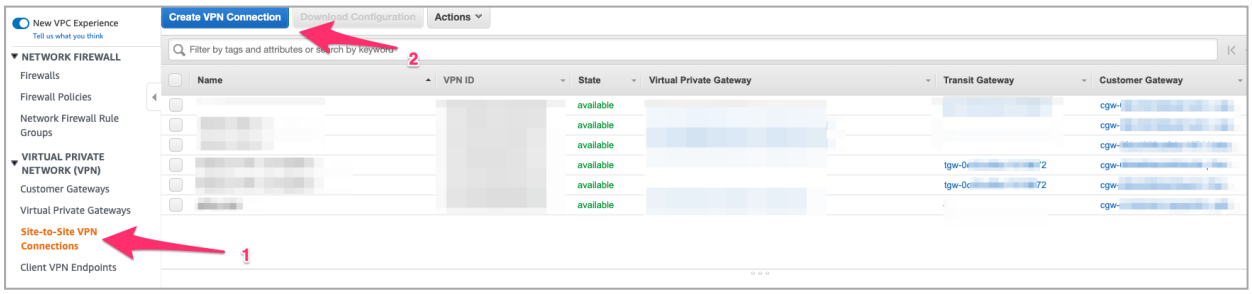
3. Create the Transit Gateway with the default settings.



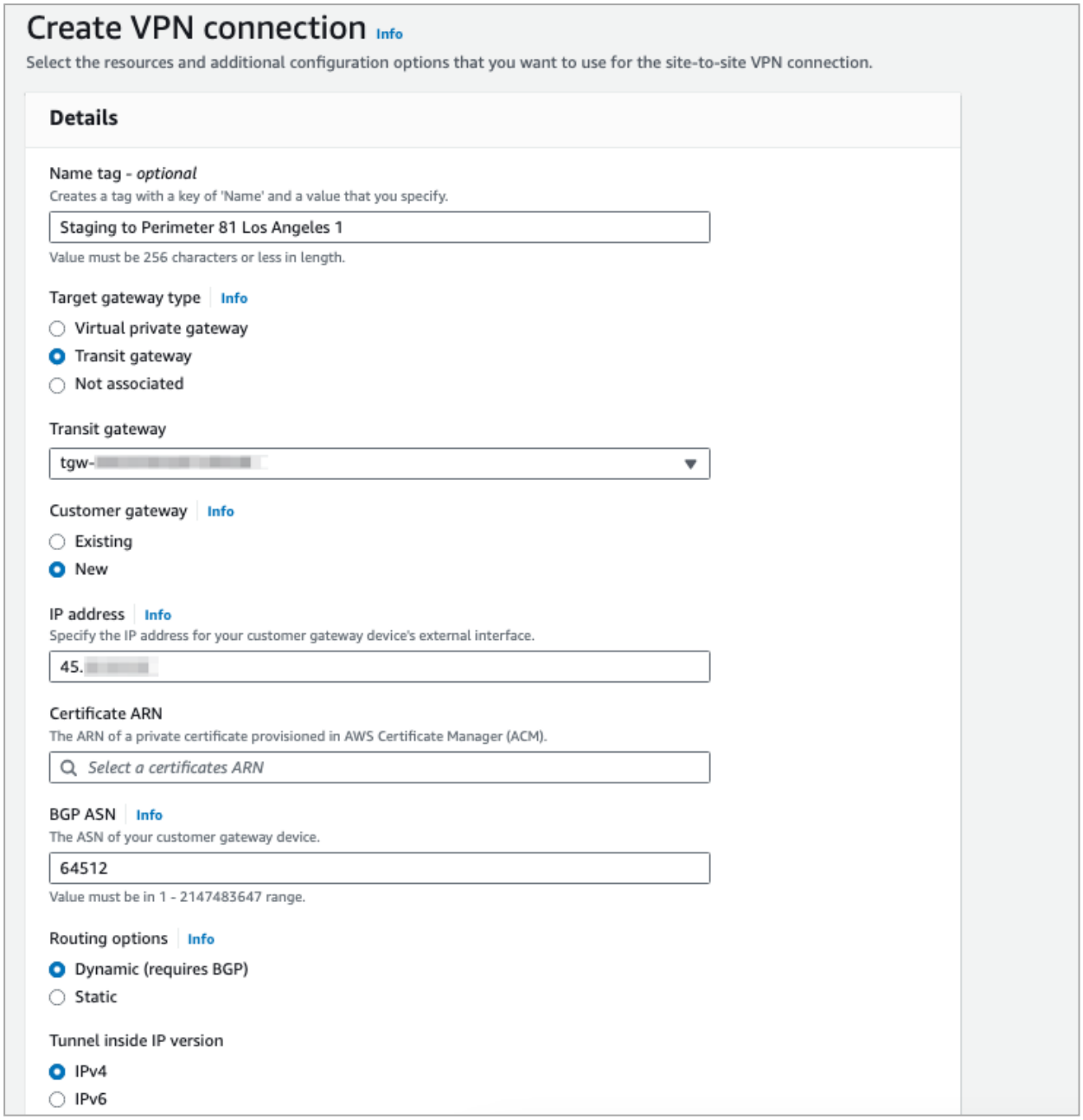
4. In the **VPC** section, go to **Transit Gateway Attachments** and create a Transit Gateway Attachment for your VPC.

Creating Two Site-to-Site VPN Connections

1. Access the AWS Management Console and go to your **AWS VPC** > **VIRTUAL PRIVATE NETWORK(VPN)** section.
2. Click **Site-to-Site VPN Connections** > **Create VPN Connection**.



The **Create VPN connection** window appears.



3. Enter these:

   a. **Transit Gateway** - Transit gateway you created.

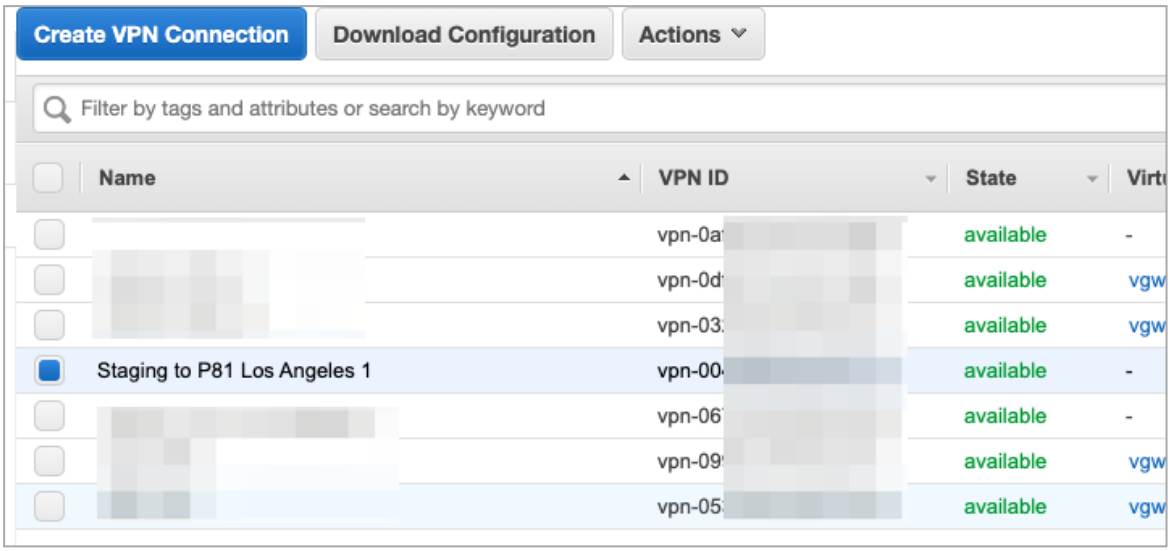
   b. **Customer gateway** - New.

   c. **IP address** - IP address of the first Harmony SASE gateway.

   d. **BGP ASN** - ASN you plan to use for the Harmony SASE network. The default is 64512.

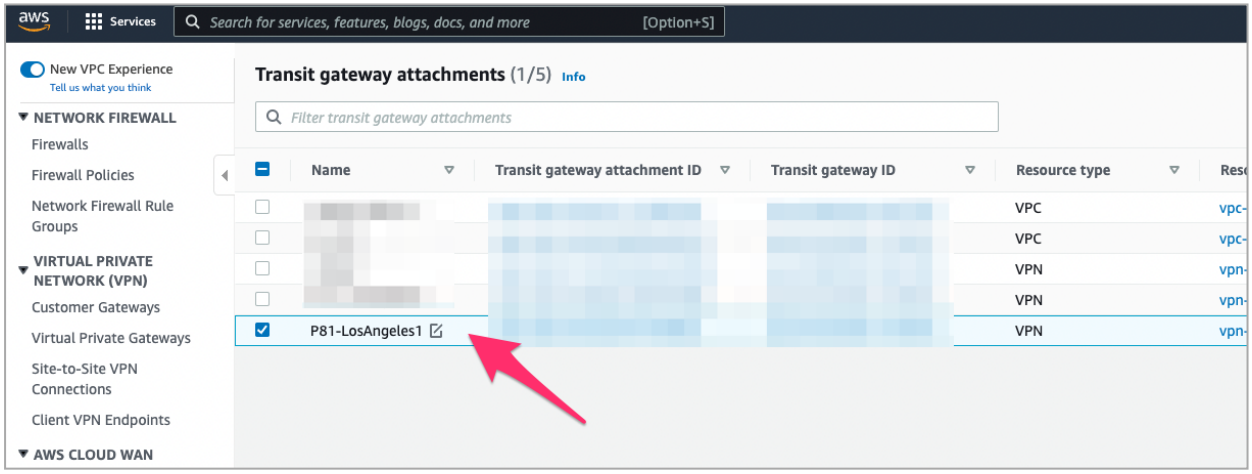
e. **Routing options** - Dynamic (requires BGP).

(Recommended) Use suitable naming conventions so that you can locate and distinguish between the connections later.

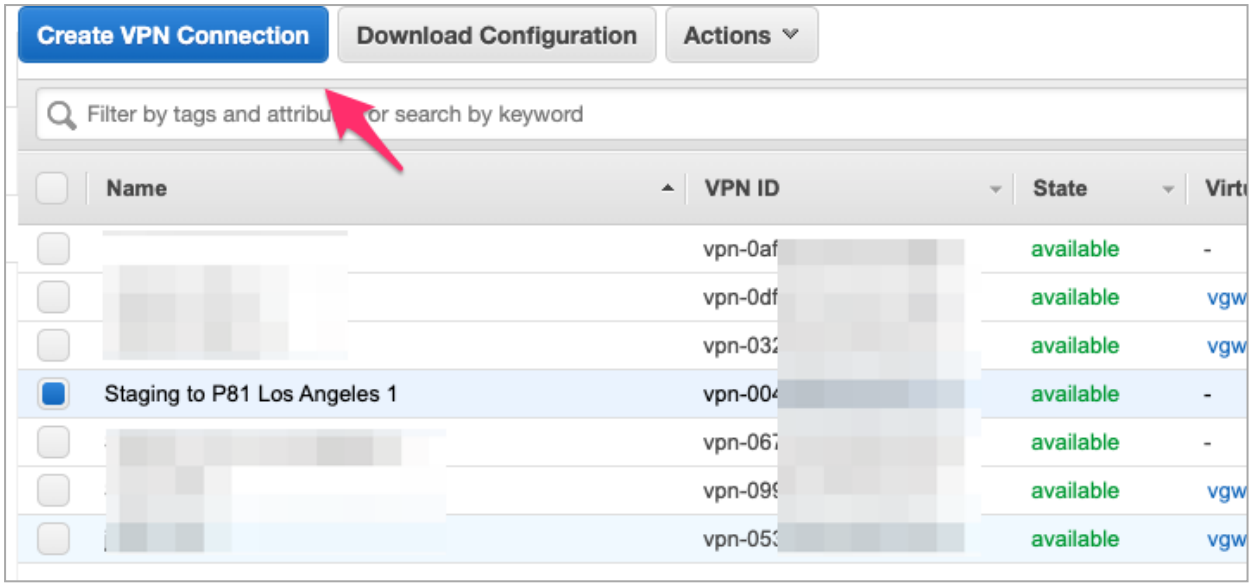


4. In the **TRANSIT GATEWAYS** section, go to **Transit Gateway attachments** and find the Transit Gateway Attachment you created.

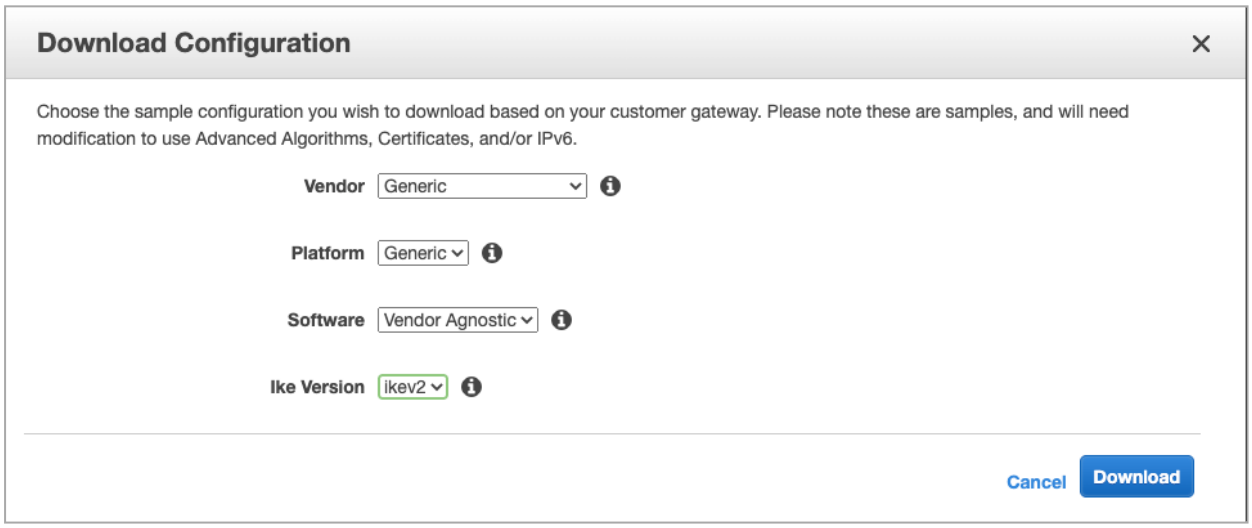
   Rename it with a meaningful name.



5. Go back to **Site-to-Site VPN Connections**, select the VPN connection you created, and then click **Download Configuration**.

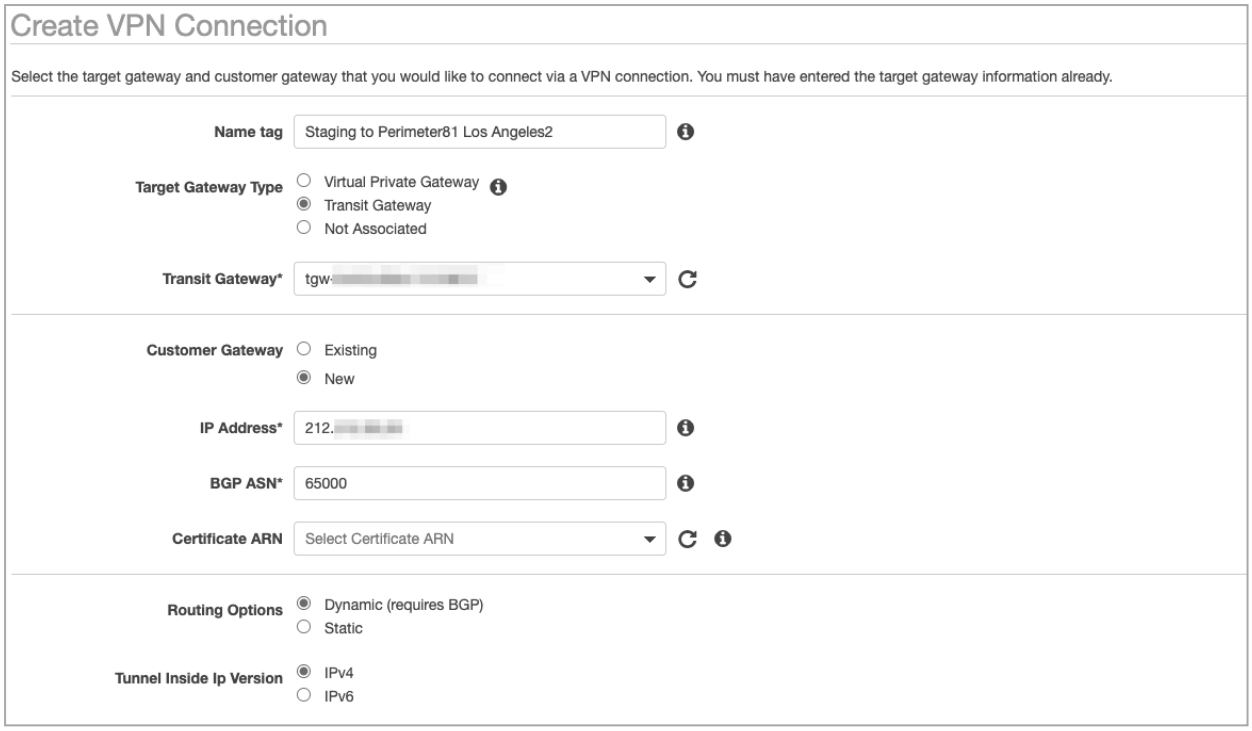


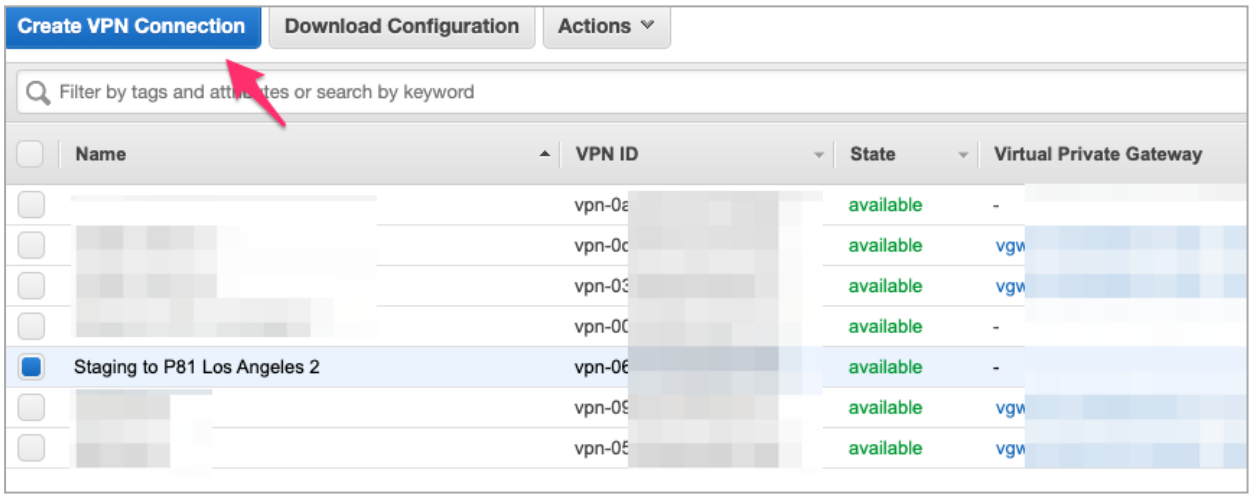
The **Download configuration** window appears.



6. Enter these:
   a. **Vendor** - Generic
   b. **Platform** - Generic
   c. **Software** - Vendor Agnostic
   d. **Ike version** - Ikev2
7. Click **Download**.

   The system downloads the file. Rename the file as *Tunnel1.txt*.
8. Repeat steps 1-7 for the other Site-to-Site Tunnel with the IP address of the second Harmony SASE gateway.

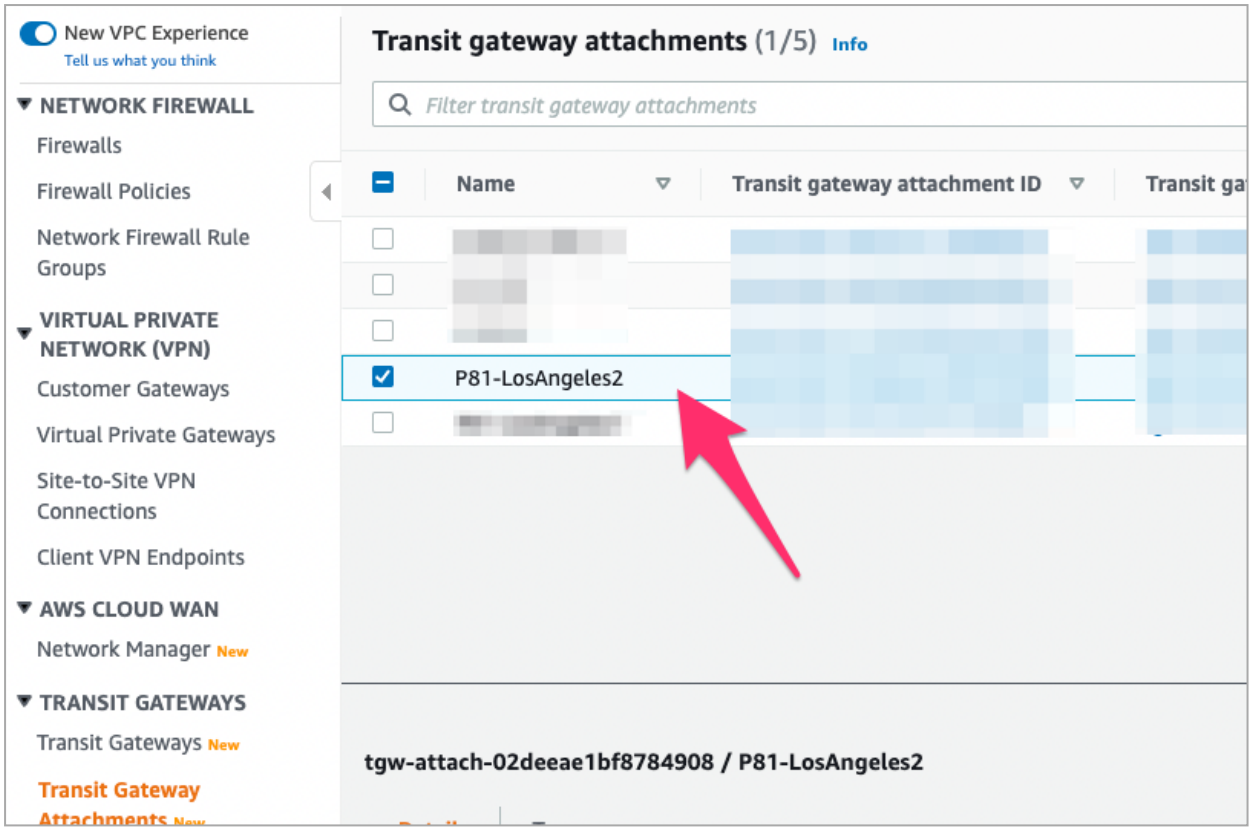




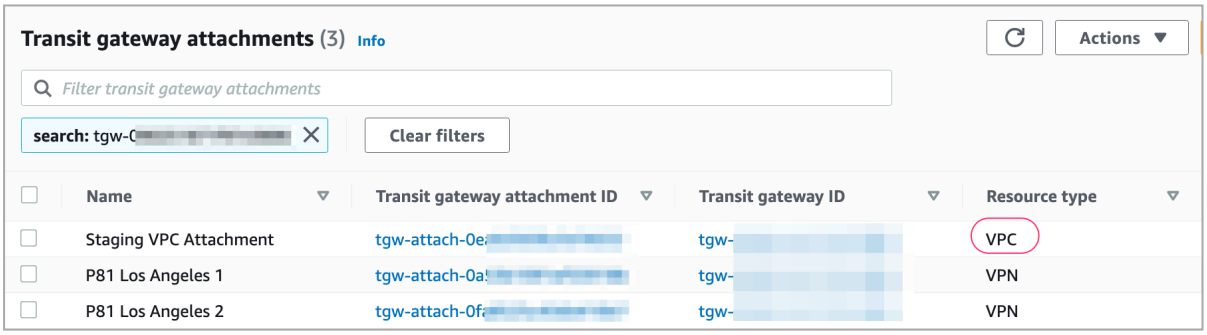
9. Rename the second downloaded file as *Tunnel2.txt*.

10. In the **TRANSIT GATEWAYS** section, go to **Transit Gateway attachments** and find the Transit Gateway Attachment you created.

    Rename it with a meaningful name.

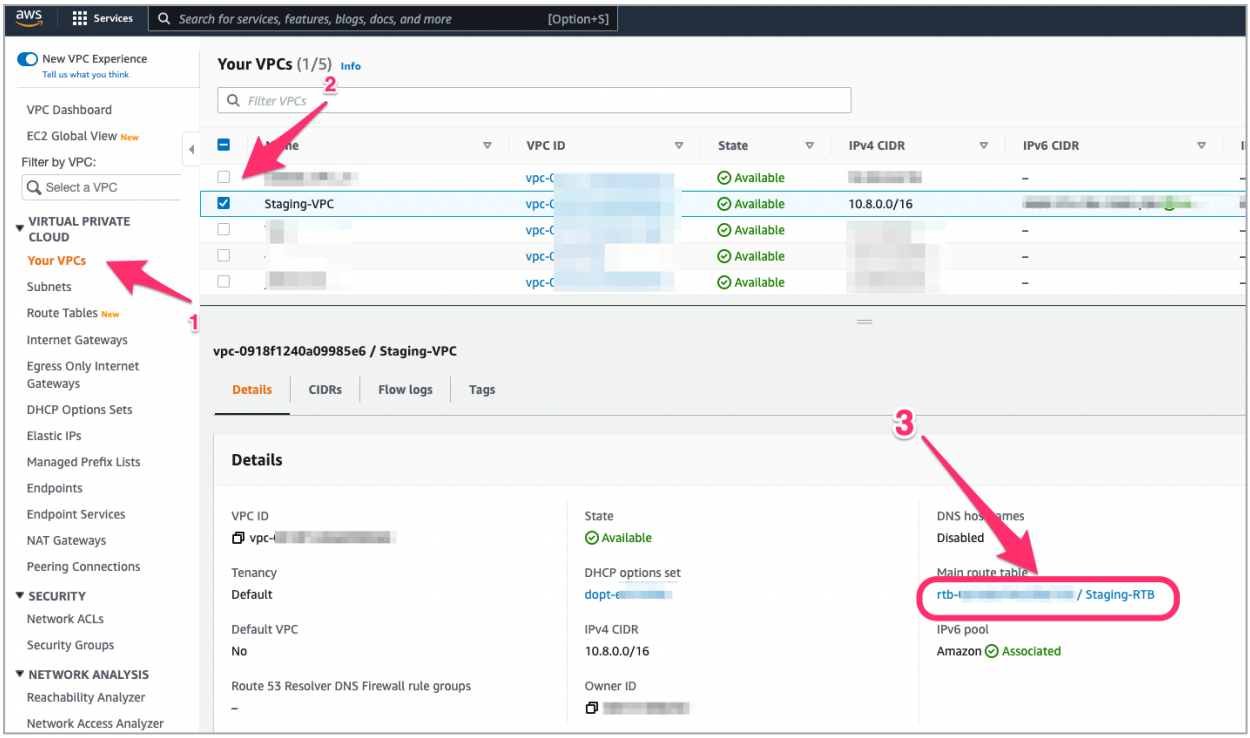


Note - To access your VPC through the redundant connection, you must have a VPC Attachment connected to the Transit gateway.



Creating Static Routes

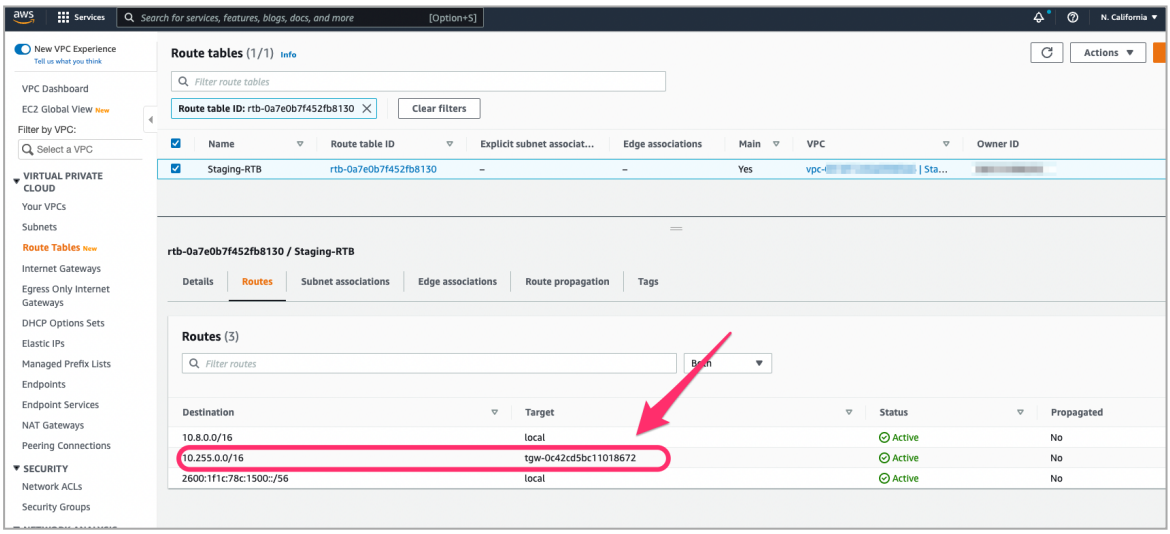
1. Access the AWS Management Console and go to **VPC**.
2. Select the corresponding VPC attached to the Transit Gateway and then select the **Main Route Table** for the VPC.



3. Edit the main Route Table for the VPC:

   a. In the **Destination** column, add the subnet mask of your Harmony SASE network.

   b. In the **Target** column, select **Transit Gateway** (Route for reverse traffic).



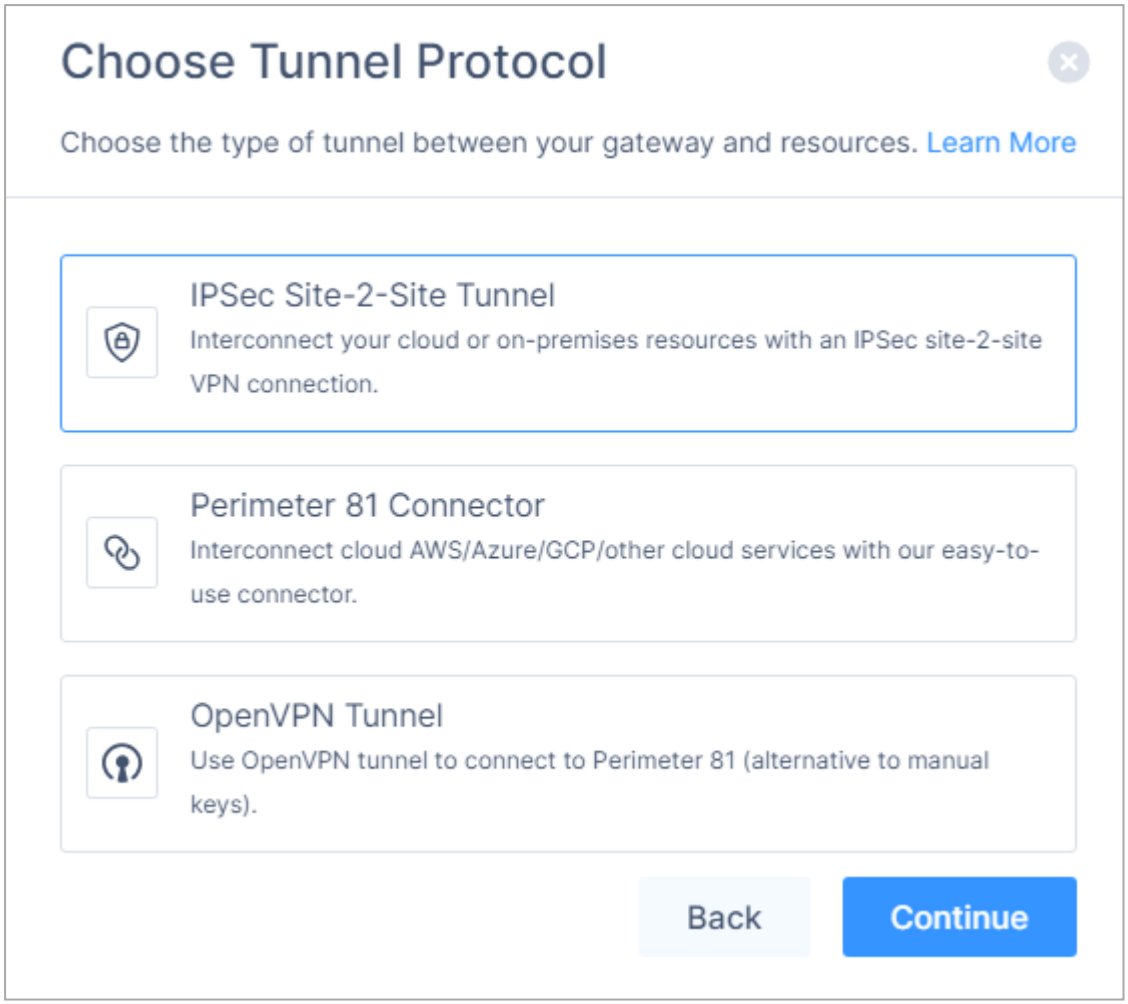
Note - If this is not the Main Route Table for the VPC, locate each subnet associated with the VPC and add the reverse route for the Harmony SASE internal subnet range.

Step 2 - Creating the Tunnels in the Harmony SASE Administrator Portal

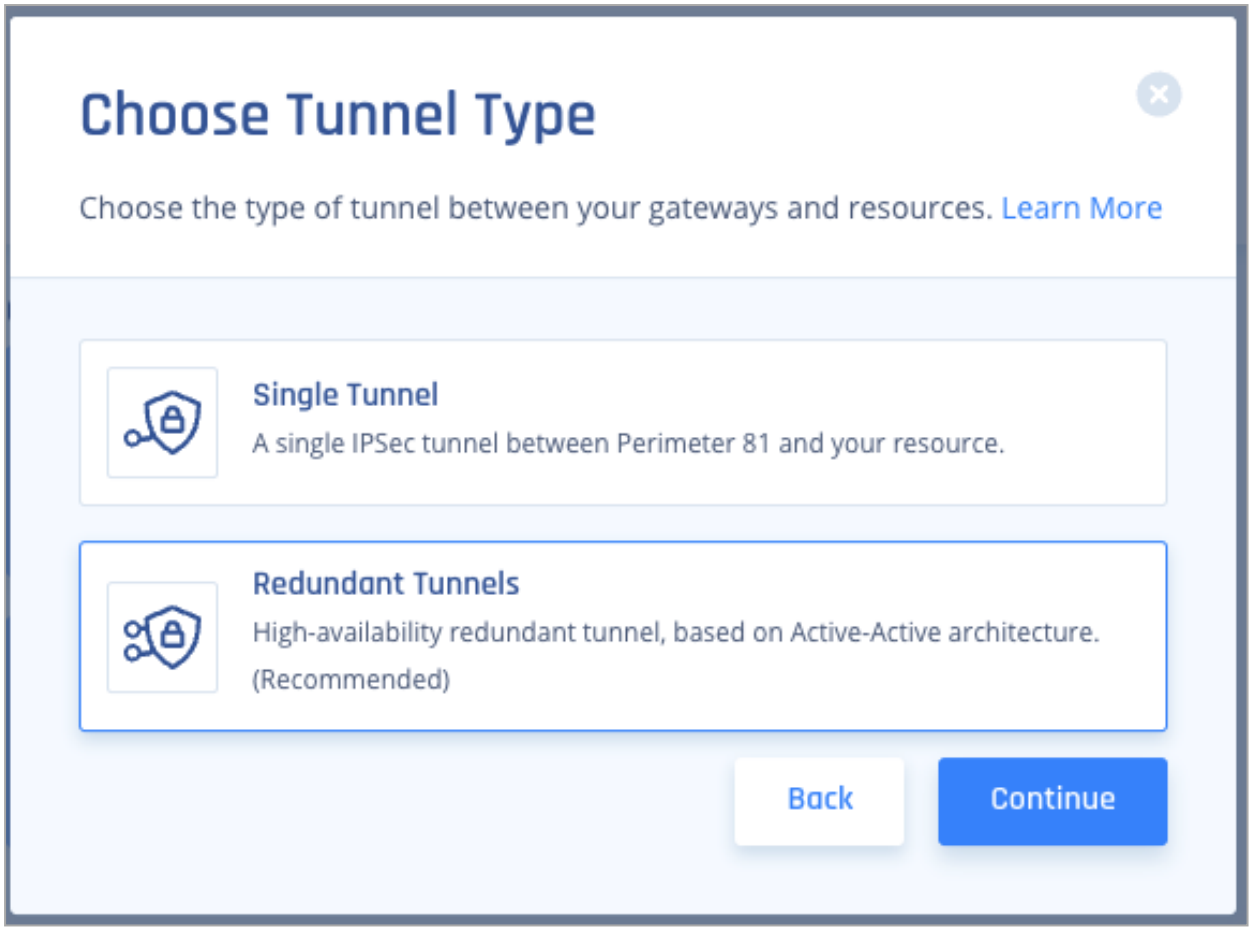
1. Access the Harmony SASEAdministrator Portal and click **Networks**.

2. Click the network where you want to create the tunnel.

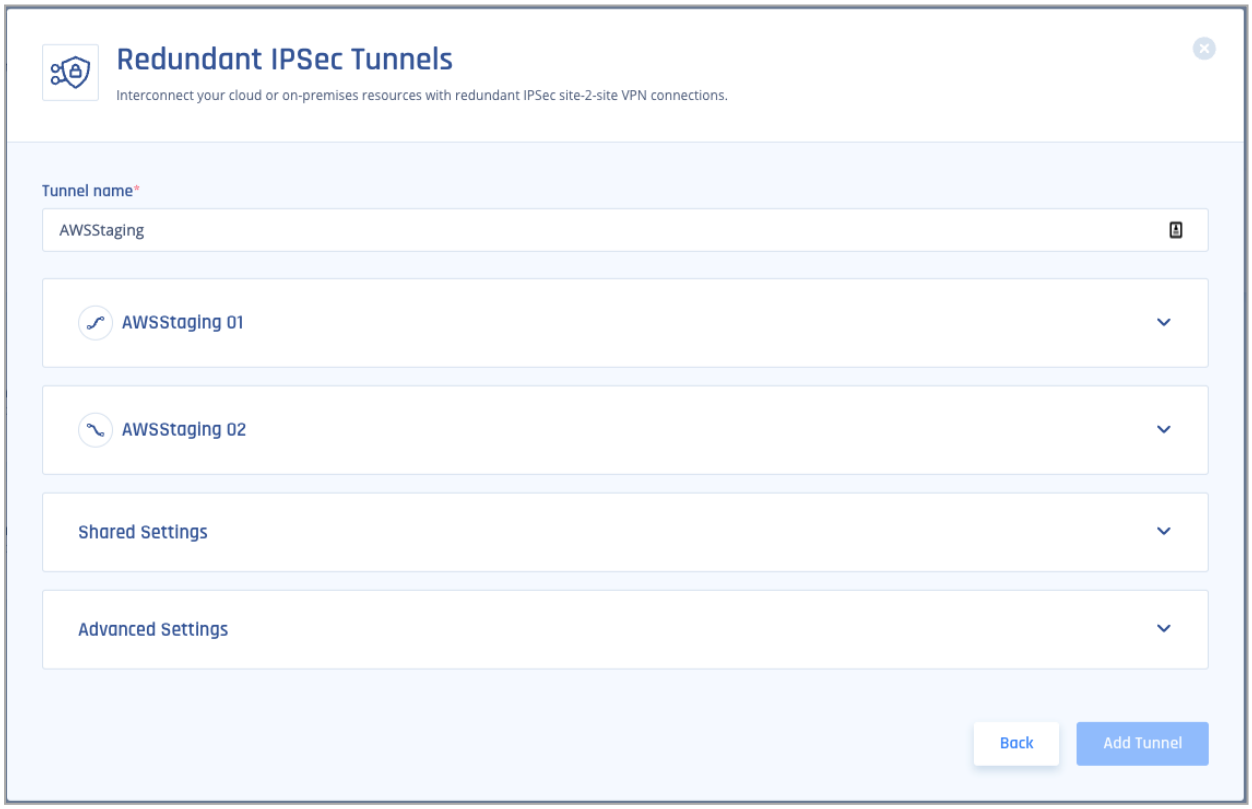
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.



6. For the first tunnel:
    a. Expand the **Tunnel 01** drop-down.
    b. To automatically populate the tunnel configuration values, click **Upload File** and upload Tunnel_1.txt file.

c. For manual configuration, copy the values from Tunnel_1.txt file as shown below.

i. **Shared Secret** - Pre-Shared Key

```
IPSec Tunnel #1
================================================================================
#1: Internet Key Exchange Configuration

Configure the IKE SA as follows:
Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and DH Group 2.
Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2, and DH Group 14.
You will need to modify these sample configuration files to take advantage of AES256, SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
NOTE: If you customized tunnel options when creating or modifying your VPN connection, you may need to modify these sample configurations to match the custom settings for your tunnels.

Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
The address of the external interface for your customer gateway must be a static address.
Your customer gateway may reside behind a device performing network address translation (NAT).
To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to unblock UDP port 4500.
| If not behind NAT, and you are not using an Accelerated VPN, we recommend disabling NAT-T. If you are using an Accelerated VPN, make sure that NAT-T is enabled.
  - IKE version           : IKEv2
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : CYyjwv[redacted]3hGT2
  - Authentication Algorithm : sha1
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Diffie-Hellman           : Group 2
```

Shared key

ii. **Harmony SASE gateway Internal IP** - Inside IP Addresses of Customer Gateway.

iii. **Remote Public IP & Remote ID** - Outside IP Addresses of Virtual Private Gateway.

iv. **Remote Gateway internal IP** - Inside IP Addresses of Virtual Private Gateway. The IP on the AWS side has a subnet (/30), discard it when pasting.

v. **Remote Gateway ASN** - BGP Configuration Options of Virtual Private Gateway ASN from the file.

```
Outside IP Addresses:
  - Customer Gateway                        : 45.[redacted].73
  - Virtual Private Gateway                 : 13.[redacted]109

Inside IP Addresses
  - Customer Gateway                         : 169.254.241.30/30
  - Virtual Private Gateway                 : 169.254.241.29/30

Configure your tunnel to fragment at the optimal size:
  - Tunnel interface MTU     : 1436 bytes

#4: Border Gateway Protocol (BGP) Configuration:

The Border Gateway Protocol (BGPv4) is used within the tunnel, between the inside
IP addresses, to exchange routes from the VPC to your home network. Each
BGP router has an Autonomous System Number (ASN). Your ASN was provided
to AWS when the Customer Gateway was created.

BGP Configuration Options:
  - Customer Gateway ASN            : 65000
  - Virtual Private  Gateway ASN          : 64512
  - Neighbor IP Address                     : 169.254.241.29
  - Neighbor Hold Time       : 30

Configure BGP to announce routes to the Virtual Private Gateway. The gateway
will announce prefixes to your customer gateway based upon the prefix you
assigned to the VPC at creation time.
```

Perimeter81 Gateway

Remote Public IP and ID

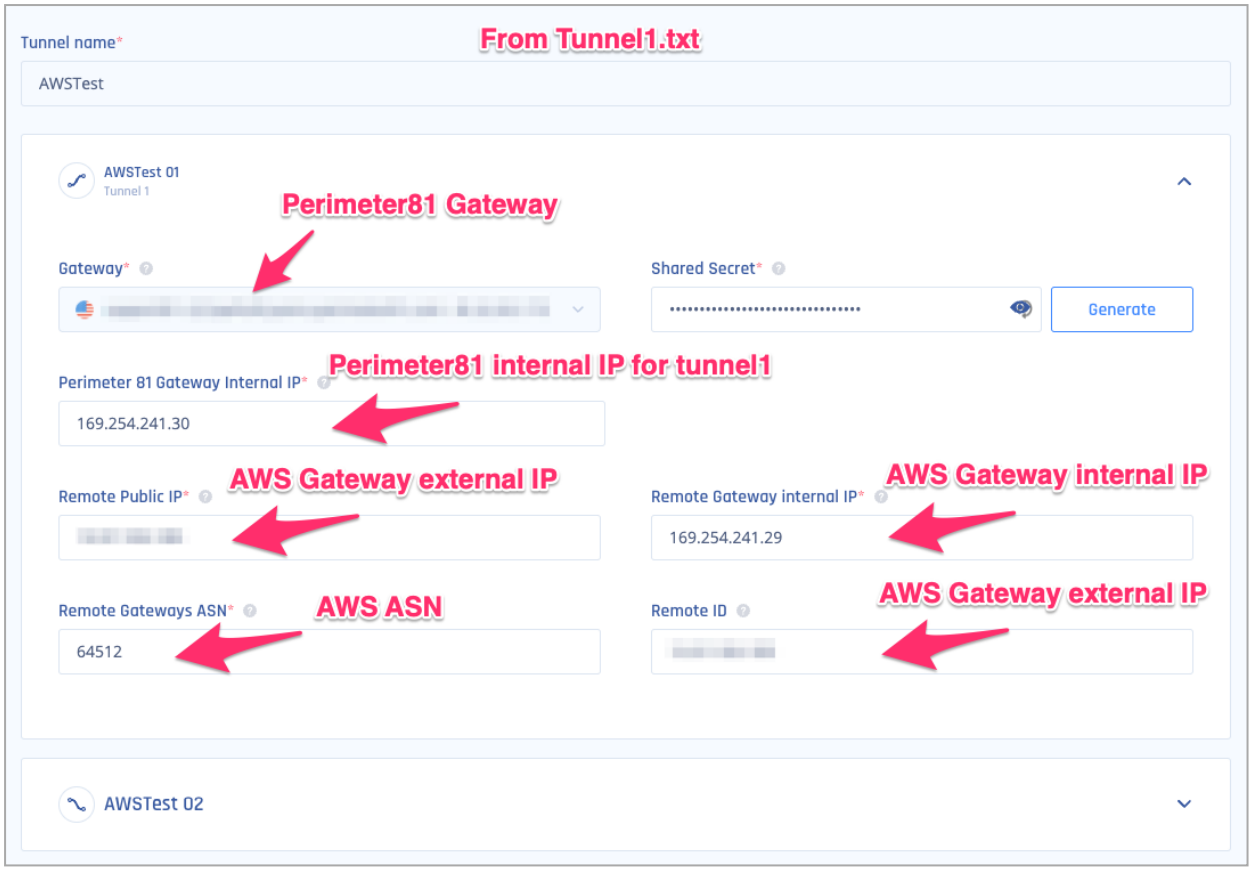
Perimeter81 Gateway internal IP

Remote Gateway internal IP

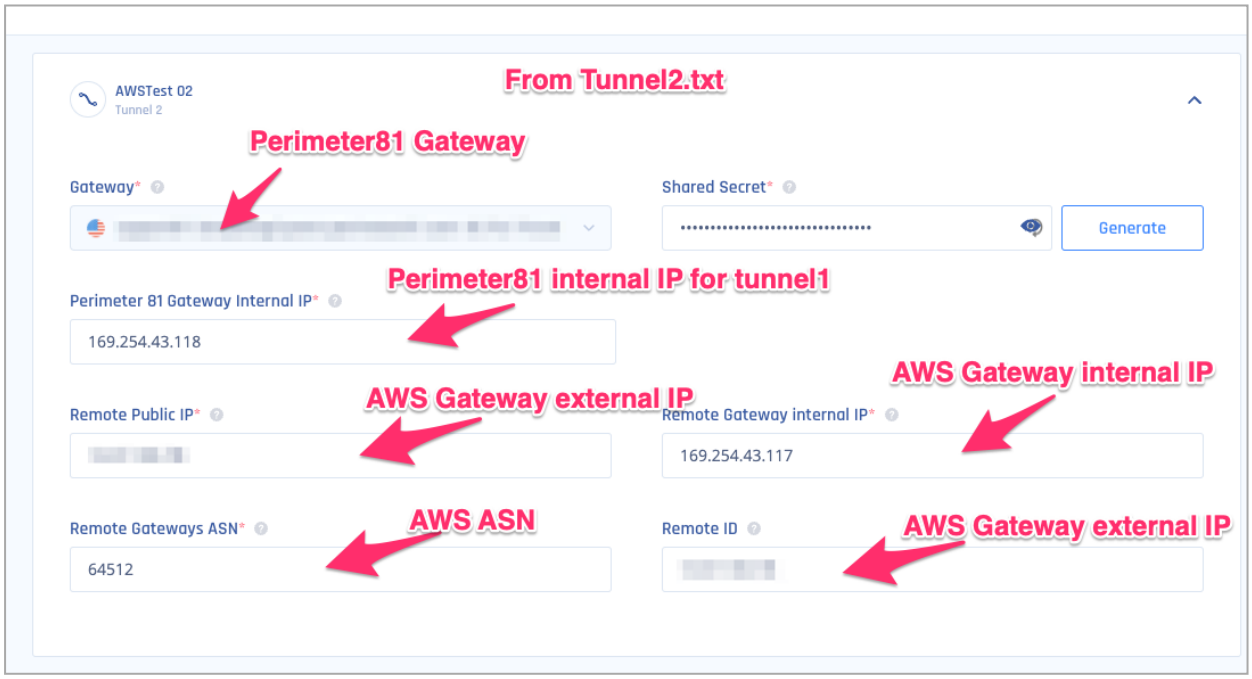
Perimeter81 ASN

AWS ASN

7. Enter the above copied values.



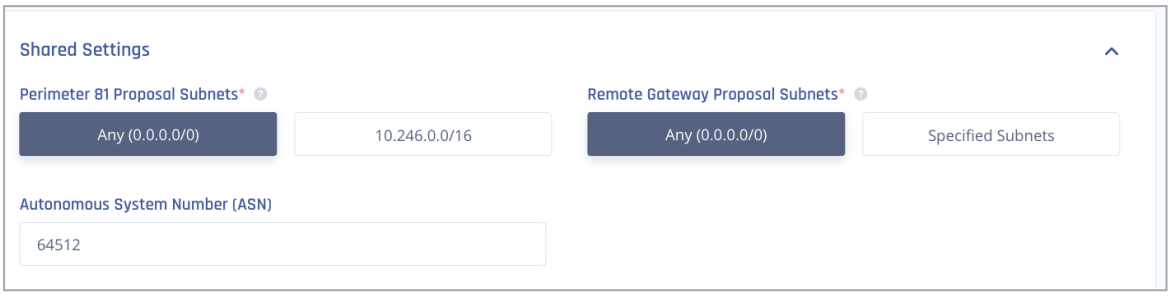
8. For the second tunnel, expand the **Tunnel 02** drop-down and repeat step 6 with the values from *Tunnel_2.txt* file.



9. In the **Shared Settings** section:

a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.

b. The **ASN** number should be the same as the Customer Gateway ASN you configured on the AWS Management console.



10. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

11. Click **Add Tunnel**.

Azure Virtual Network Gateway

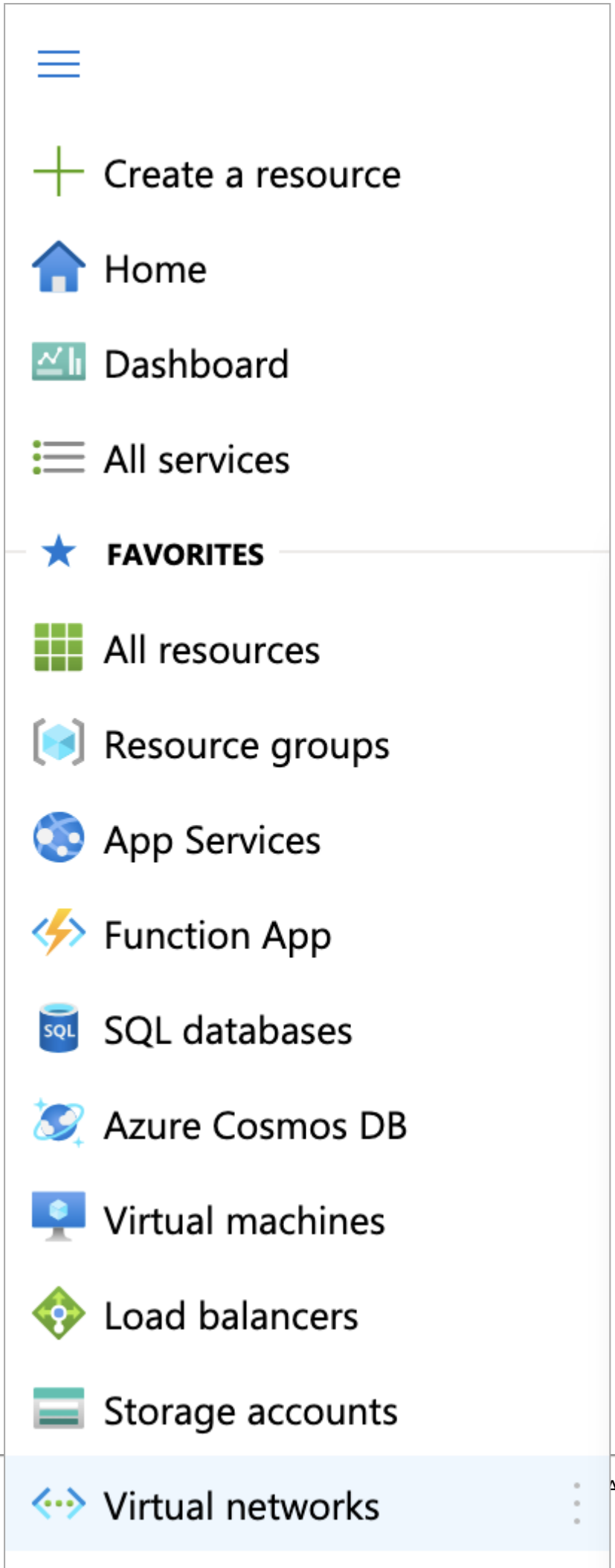
Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

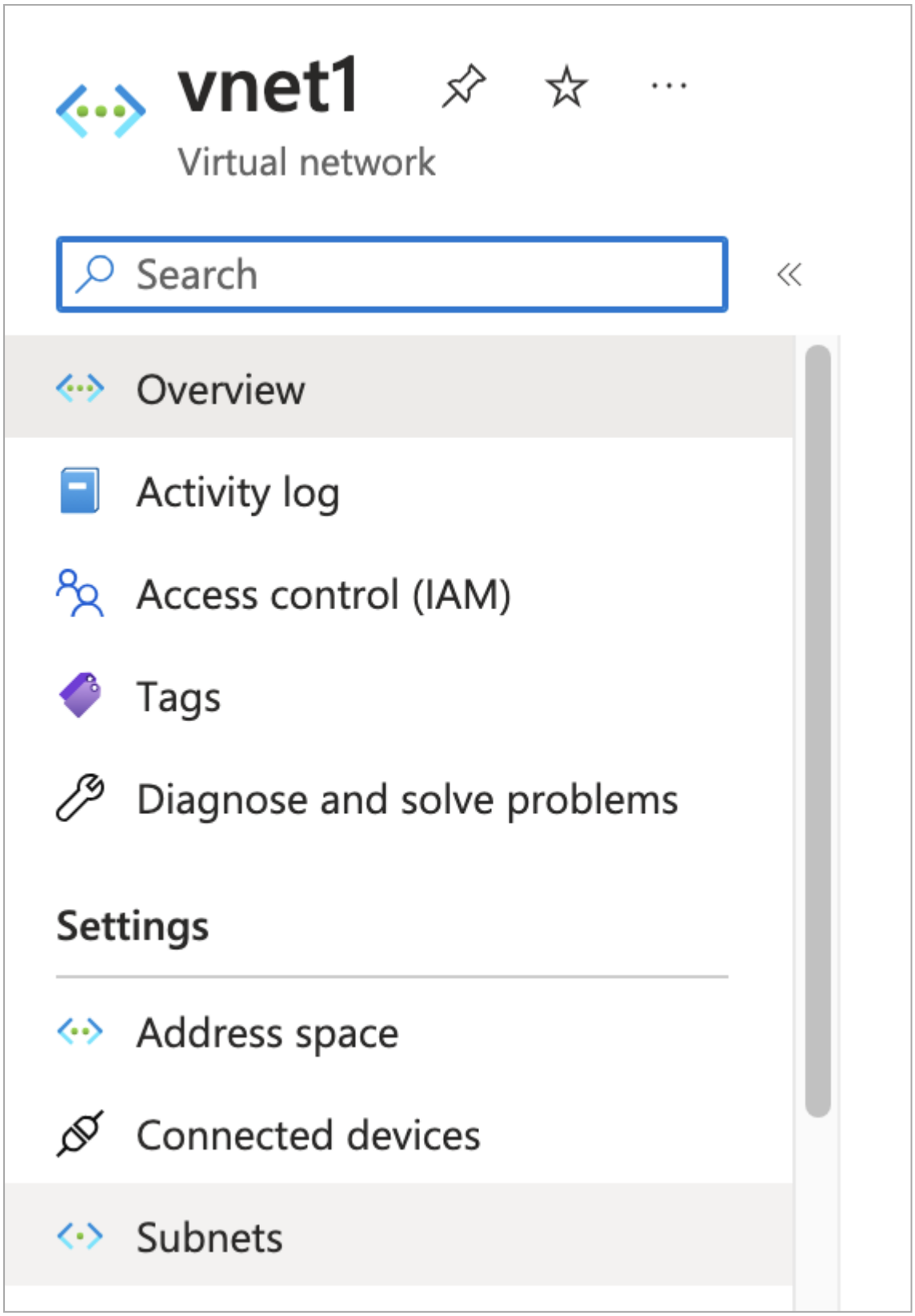
Step 1 - Configurations in the Azure Management Portal

Creating a Gateway Subnet

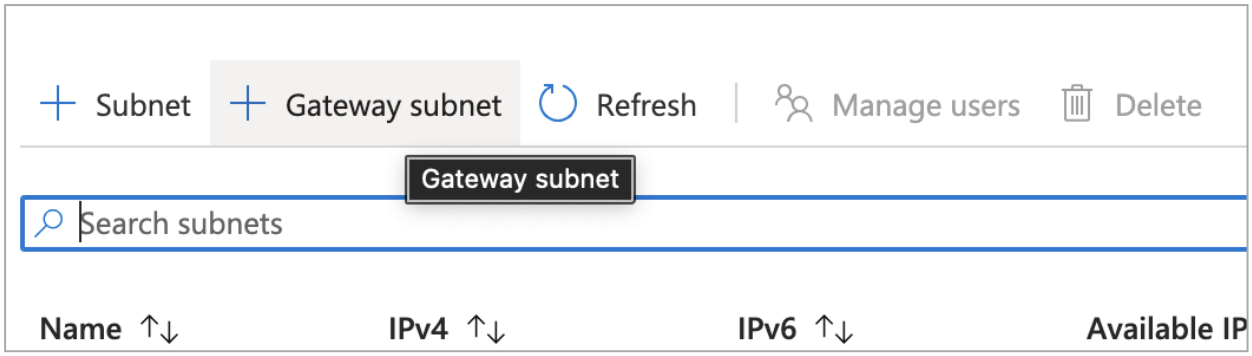
1. Access the Azure Management Portal and go to **Virtual networks**.


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks

2. Click the virtual network to which you wan to create the gateway and click **Subnets**.



3. Click **+ Gateway subnet**. The system populates the subnet name as **Gateway subnet** by default.



4. (Optional) Adjust the auto-filled Address range values. This subnet is used for the Virtual Gateway only.

   If this range is not auto-filled:

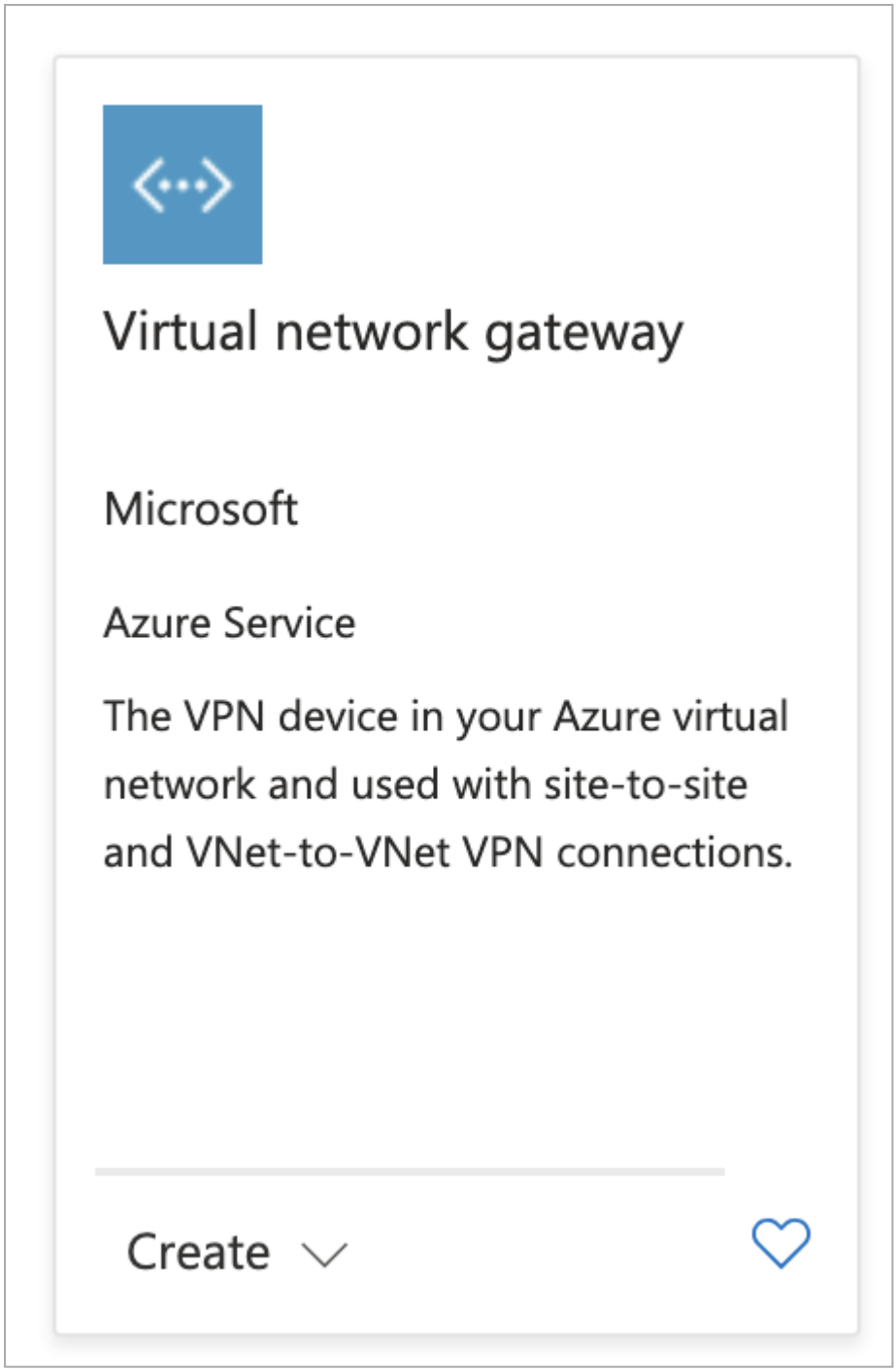
   a. Go to address space and click **+Add**.

   b. Select a random /27 bit mask subnet space. For example, 10.1.255.0/27.

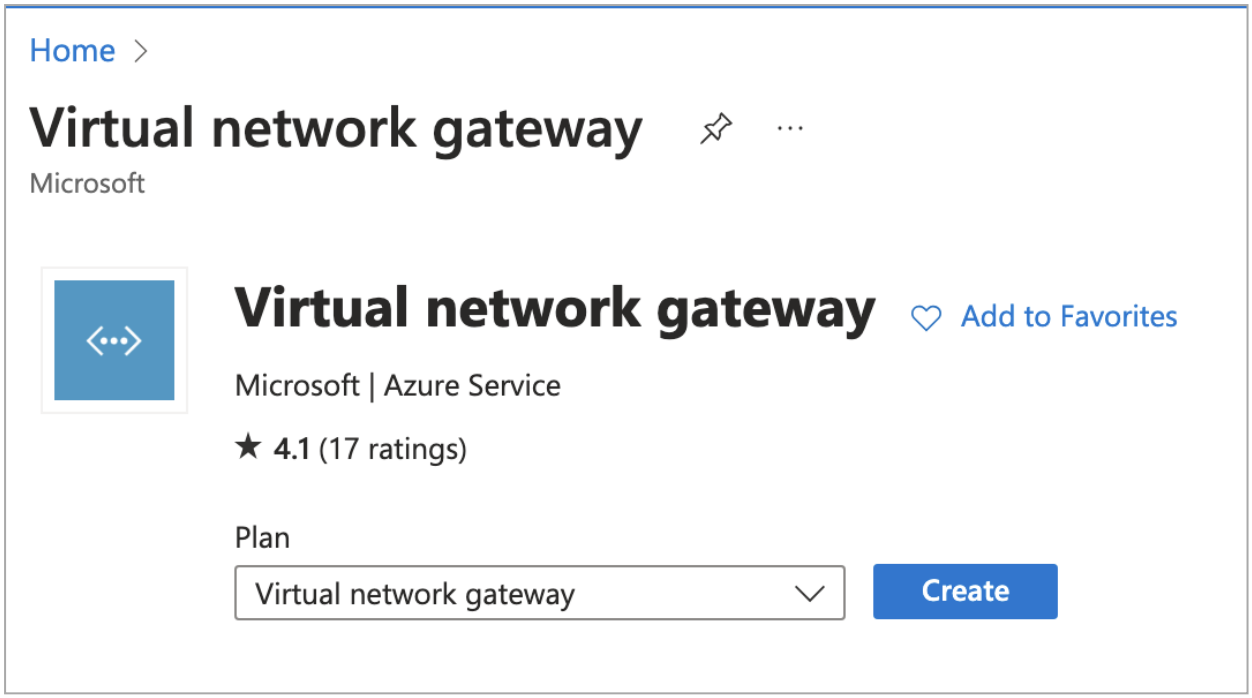
Creating a Virtual Network Gateway

1. Access the Azure Management Portal and click **+Create a resource**.

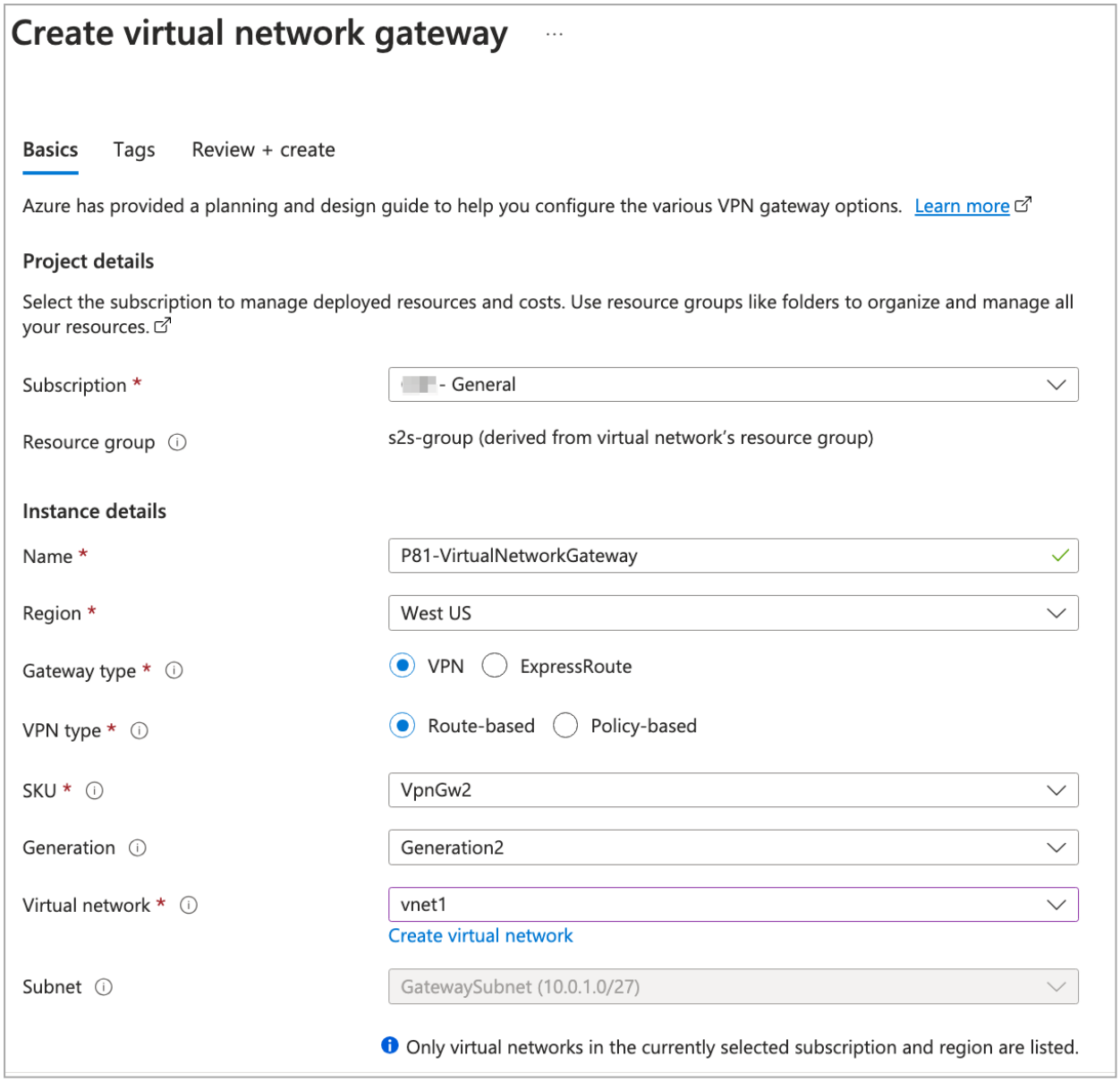
2. Search for **Virtual Network Gateway** and click it in the search results.



3. Click **Create**.



4. The **Create virtual network gateway** window appears.



5. Enter these:
   a. **Name** - Name of the gateway.
   b. **Region** - Region where your resources are located.
   c. **Gateway type** - VPN.
   d. **SKU** - Select the gateway SKU from the list. The SKUs listed depends on the selected VPN.

e. **Virtual network** - The Virtual network that contains the resources you want to reach through the tunnel.

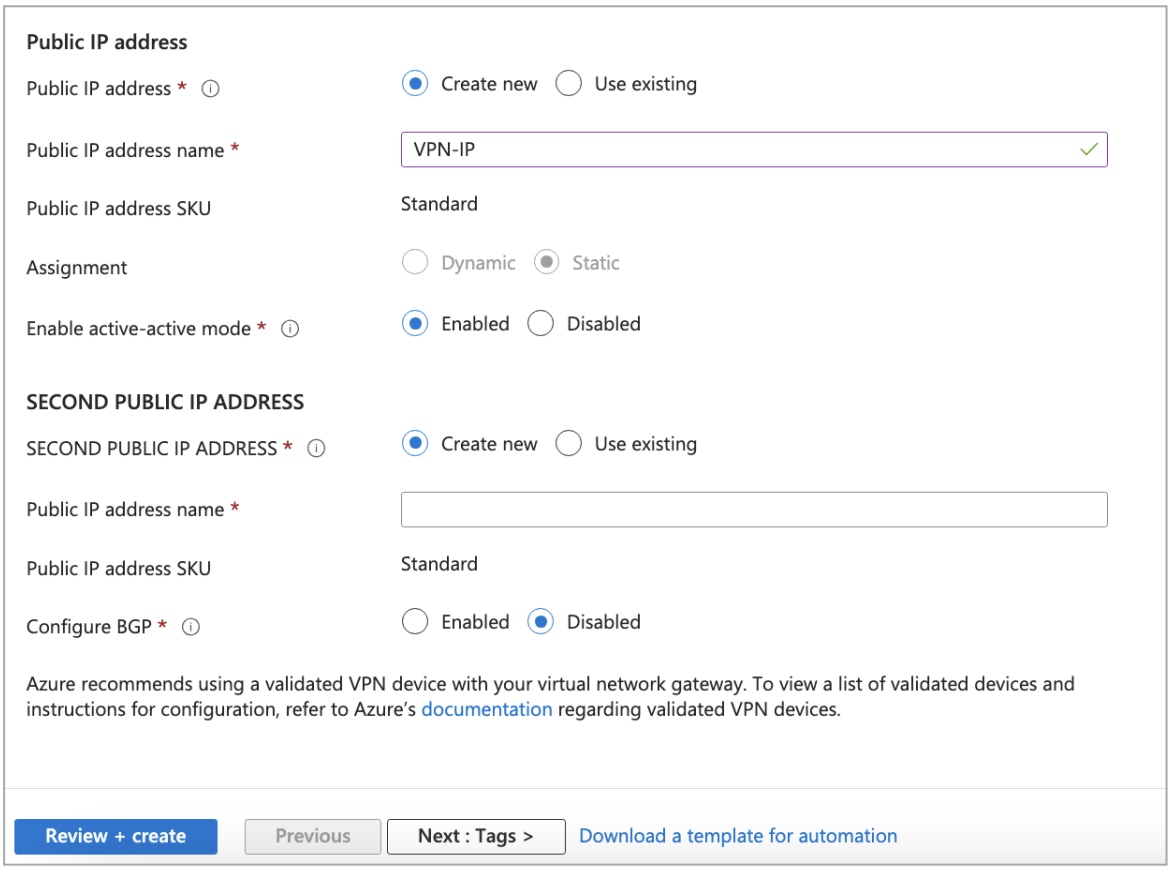
   The **Choose a virtual network** page appears.

   Note - If you do not see your VNet, make sure your virtual network is located in the selected **Region**.

f. **Subnet** - Subnet range for your virtual network.

   This setting appears only when you create a gateway subnet for your virtual network for the first time.

g. **Public IP address** - Click **Create New** or choose an existing IP used by your organization.



h. **Enable active-active mode** - Disabled.

i. **Configure BGP** - Disabled.

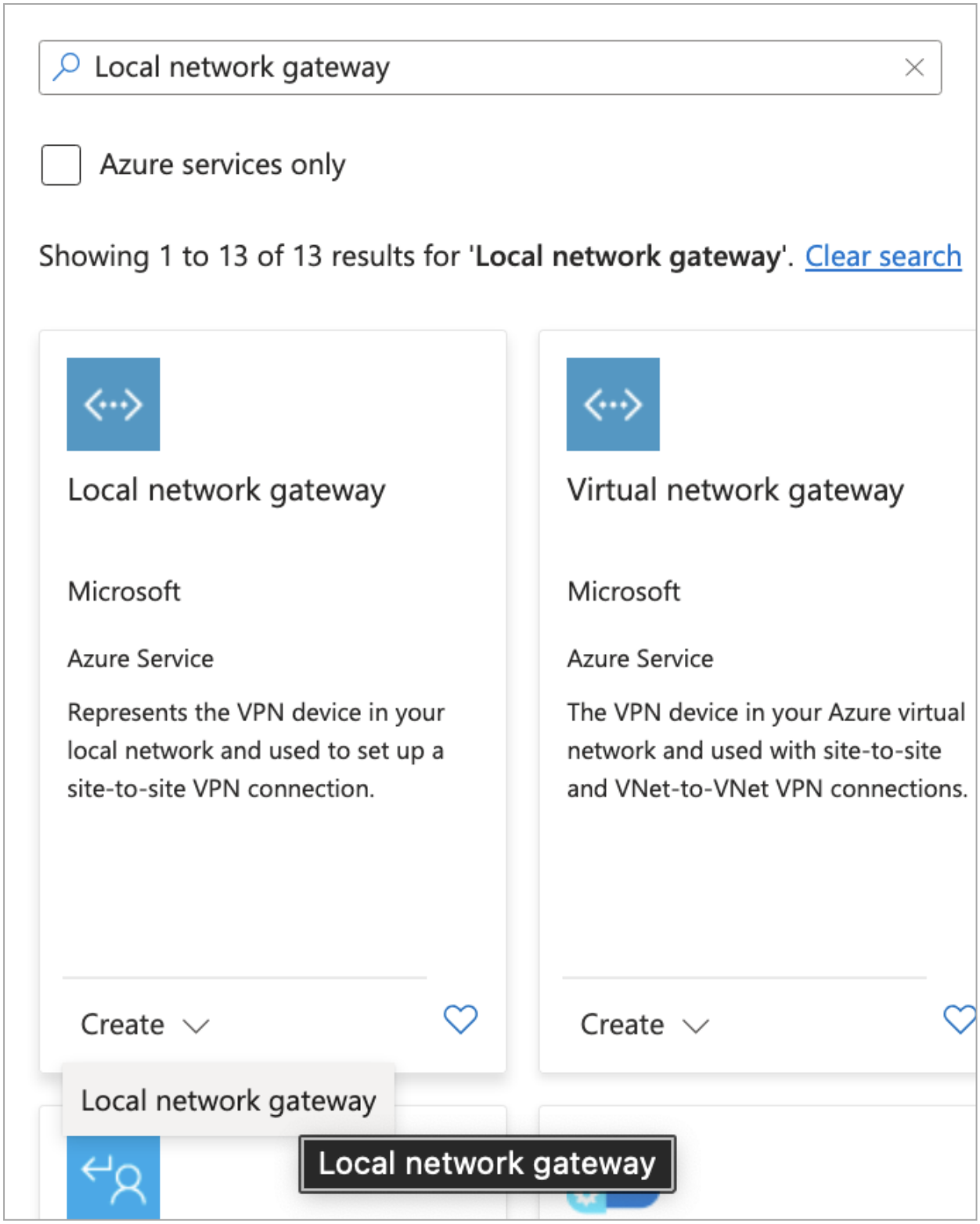
j. Click **Review+create**.

   The system starts to create the VPN gateway and it may take up to 45 minutes to complete.

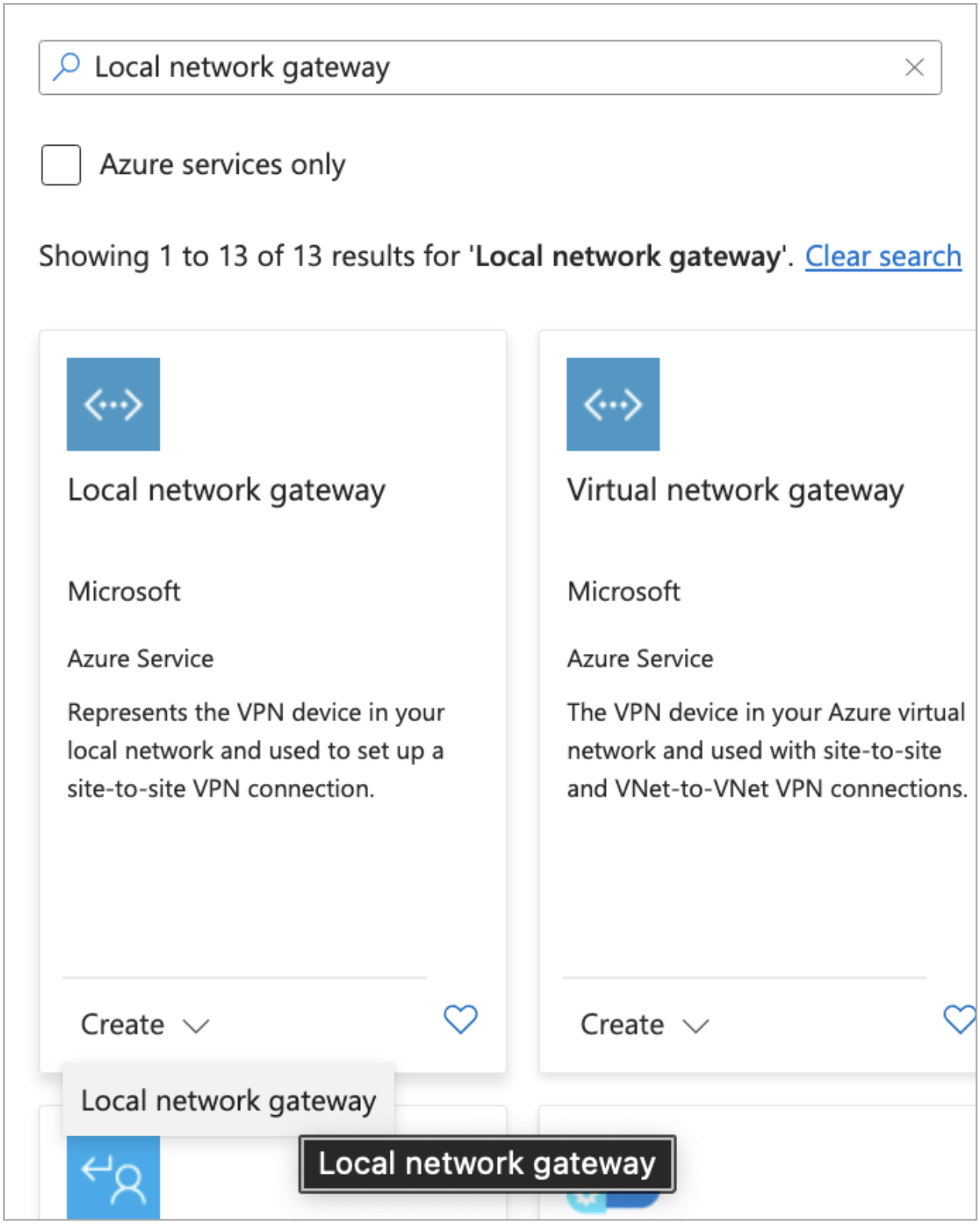
Creating a Local Network Gateway

1. Access the Azure Management Portal and click **+Create a resource**.

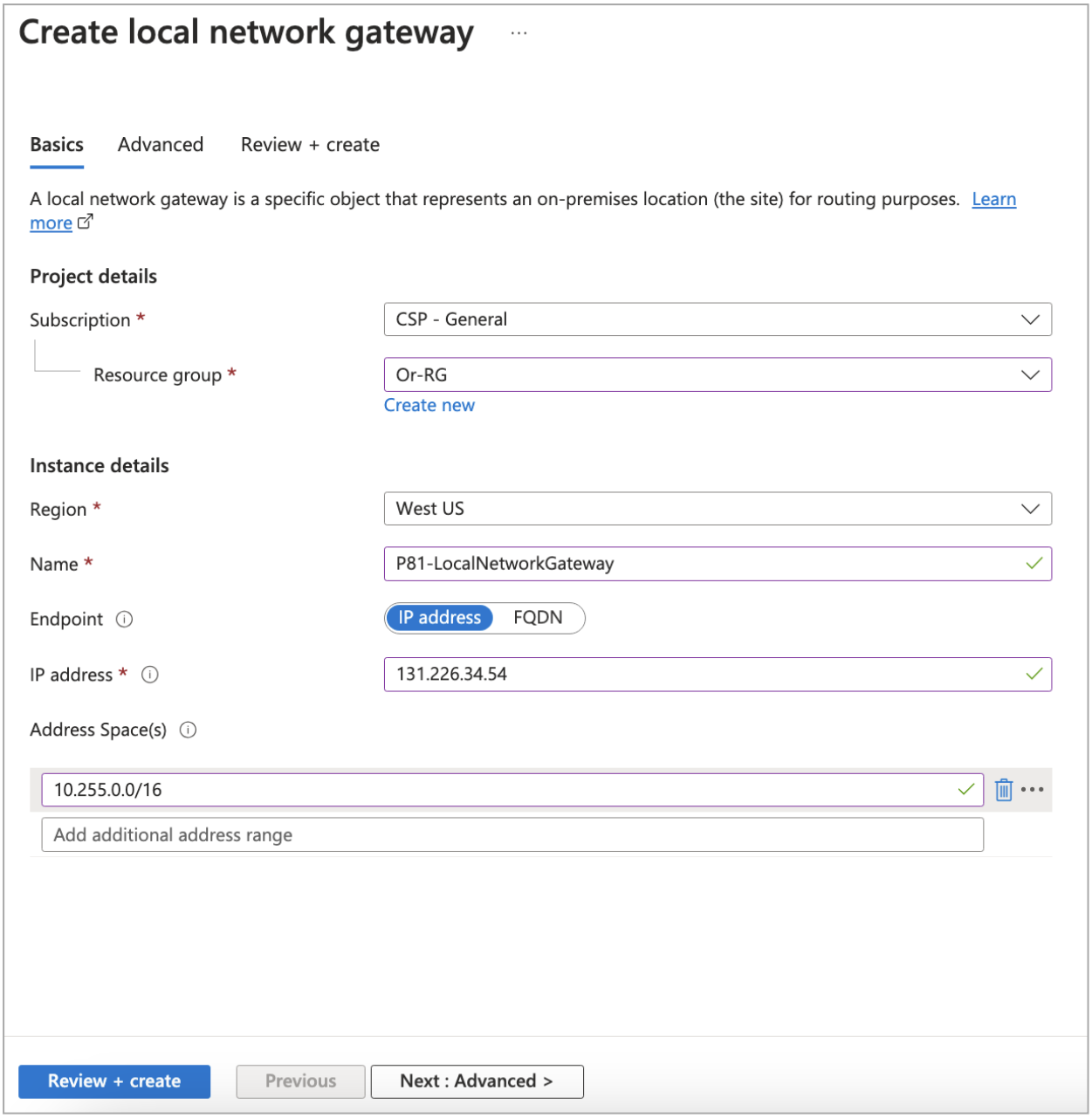
2. Search for **Local network gateway** and click it in the search results.



3. Click **Create**.



The **Create local network gateway** page appears.



4. Enter these:
   a. **Name** - Name of your gateway.
   b. **IP address** - IP address of your Harmony SASE gateway.

c. **Address Space** - Harmony SASE subnet.

   Make sure that these ranges do not overlap with other networks' ranges that you want to connect to.

d. **Subscription** - Verify that the value is correct.

e. **Resource Group** - Select the resource group that you want to use. Create a new resource group or select one that you have already created.

f. **Location** - Select the location where this object is created.

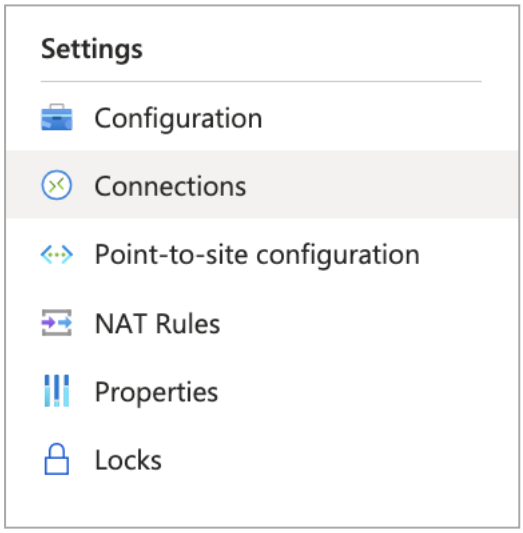
   (Optional) Select the location in which your Virtual Network resides.

g. **SKU** - Select the gateway SKU from the list. The SKUs listed depends on the selected VPN.

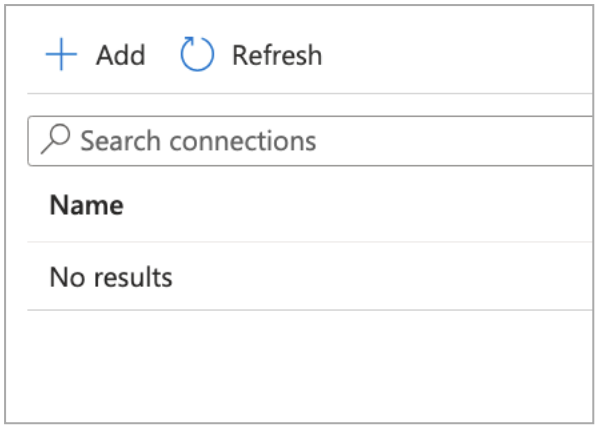
5. Click **Create**.

Creating the IPSecTunnel Connection

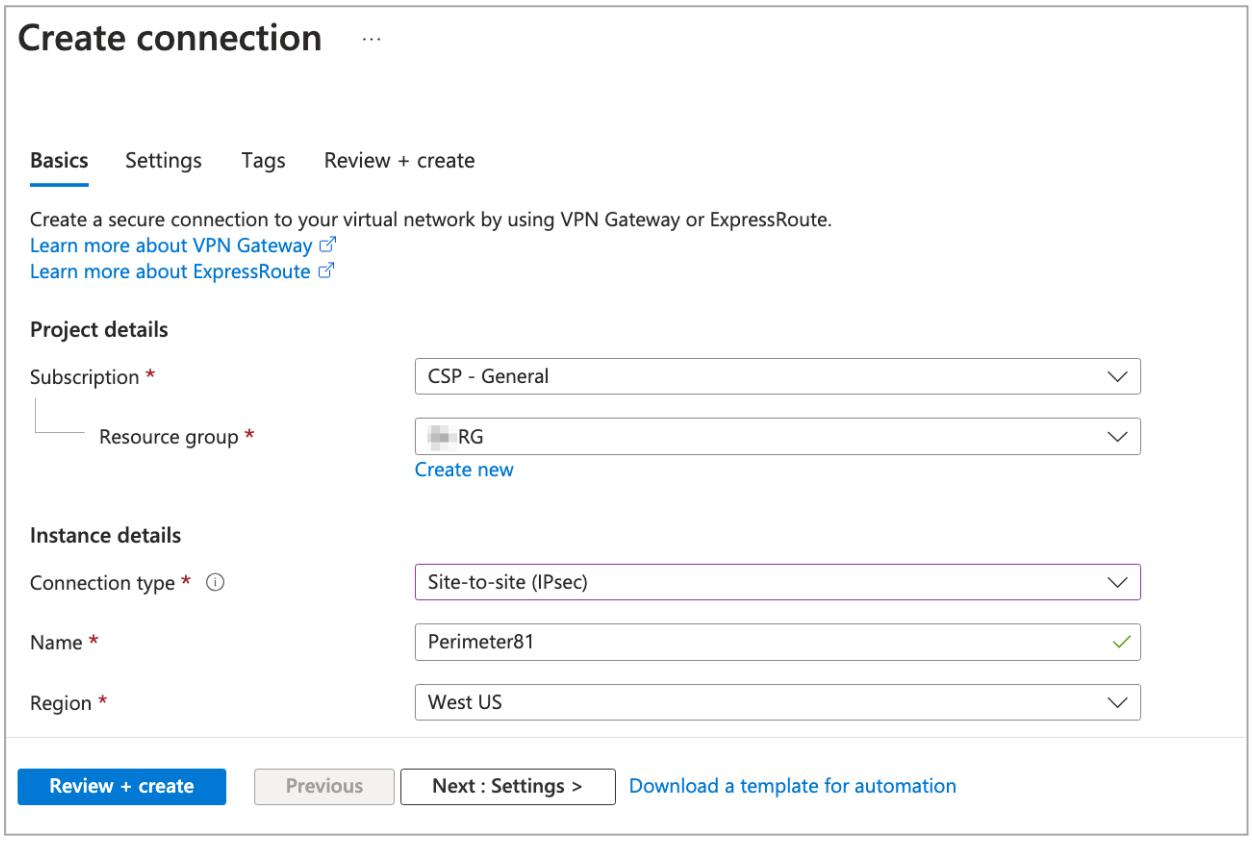
1. Access the Azure Management Portal and go to your **Virtual Network Gateway** page.
2. Go to **Settings** and click **Connections**.



3. Click **+Add**.

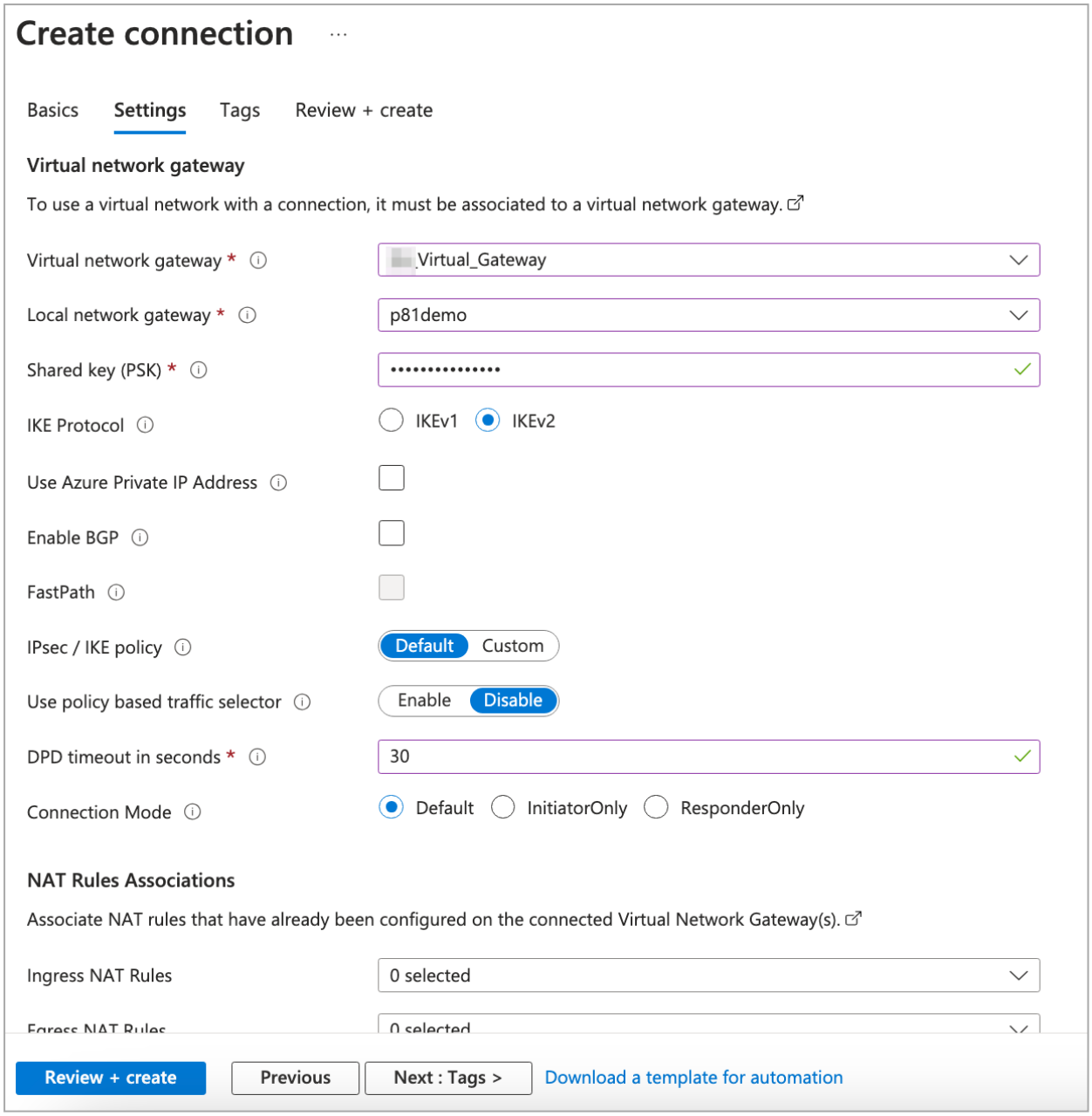


The **Create connection** window appears.



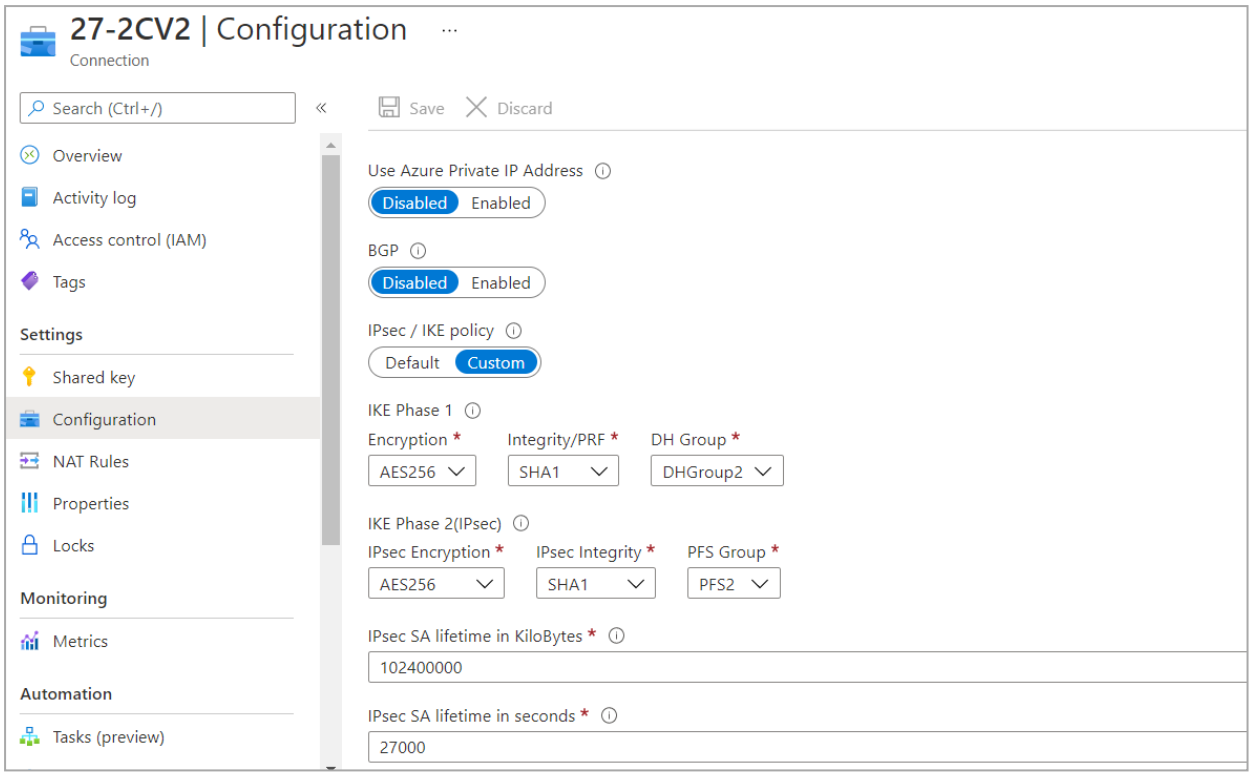
4. In the **Basics** tab, enter these:
   a. **Connection type** - Site-to-site (IPSec).
   b. **Name** - Name of the connection.
5. Click **Next: Settings >**.

   The **Settings** tab appears.

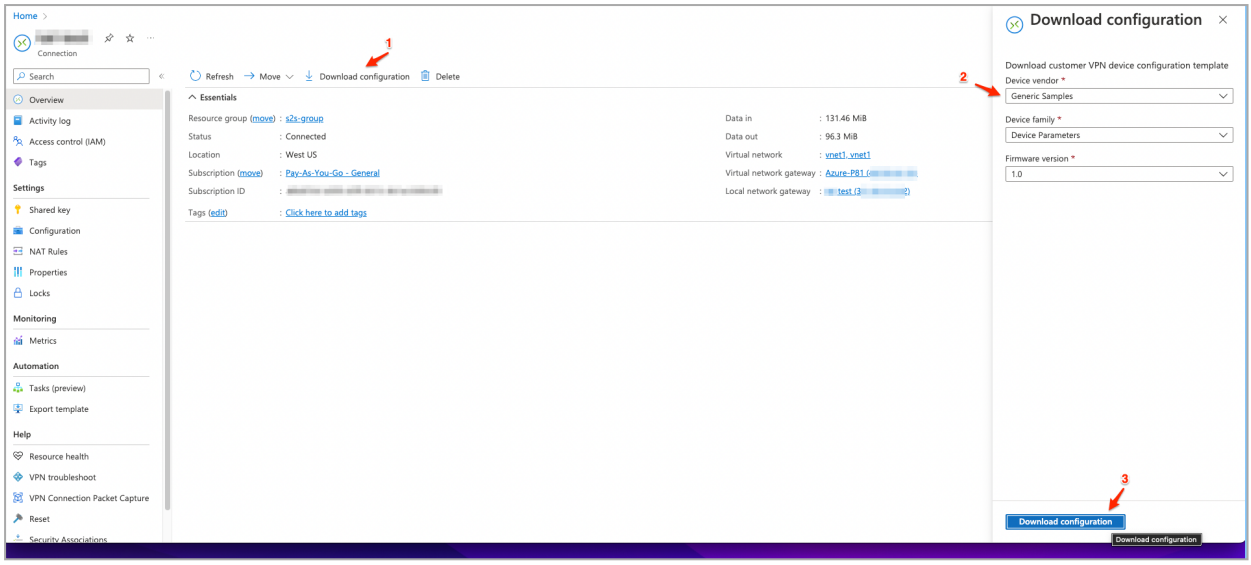


6. Enter these:
   a. **Virtual network gateway** - IP address you receive from Azure. The value is static.
   b. **Local network gateway** - Local network gateway (your Harmony SASE network address) which you have created. The value is static.
   c. **Shared Key (PSK)** - Create a unique key value. This must match with the key value used for the Harmony SASE tunnel.
   d. **IKE Protocol** - IKev2.
   e. **DPD timeout in seconds** - 30
7. Click **Review + Create** to create your connection.
8. Select the connection you just created and click **configuration**.

The **Configuration** window appears.



9. Enter these:
   a. **IPsec / IKE policy** - Select **Custom** and use these values to align with the values set in Harmony SASE tunnel settings.
      i. **Encryption** - AES256
      ii. **Integrity/PRF** - SHA1
      iii. **DH Group** - DHGroup2
      iv. **IPsec Encryption** - AES256
      v. **IPsec Integrity** - SHA1
      vi. **PFS Group** - PFS2
      vii. **IPsec SA lifetime in KiloBytes** - 102400000
      viii. **IPsec SA lifetime in seconds** - 27000
10. Go to **Overview** > **Download configuration**.

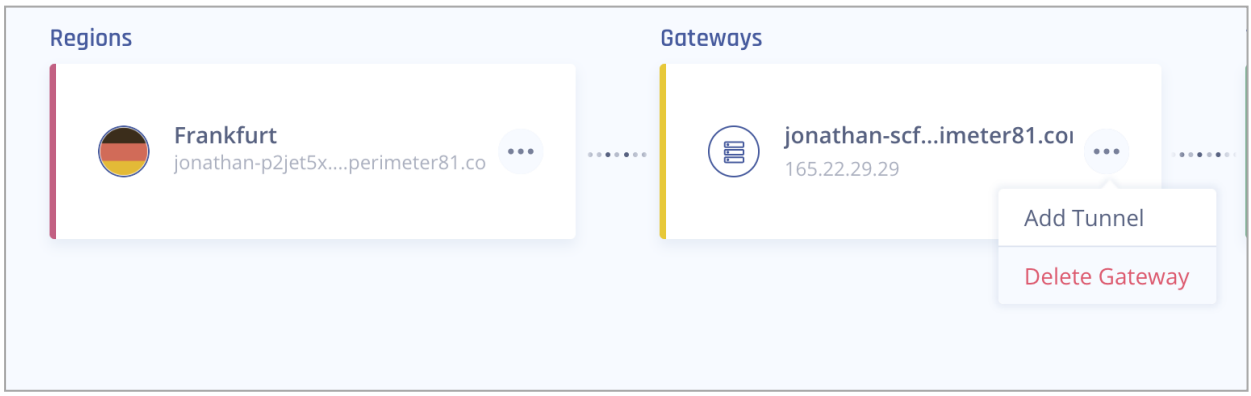


11. Enter these:
    a. **Device vendor** - Generic Samples
    b. **Device family** - Device Parameters
    c. **Firmware version** - 1.0
12. Click **Download Configuration**.

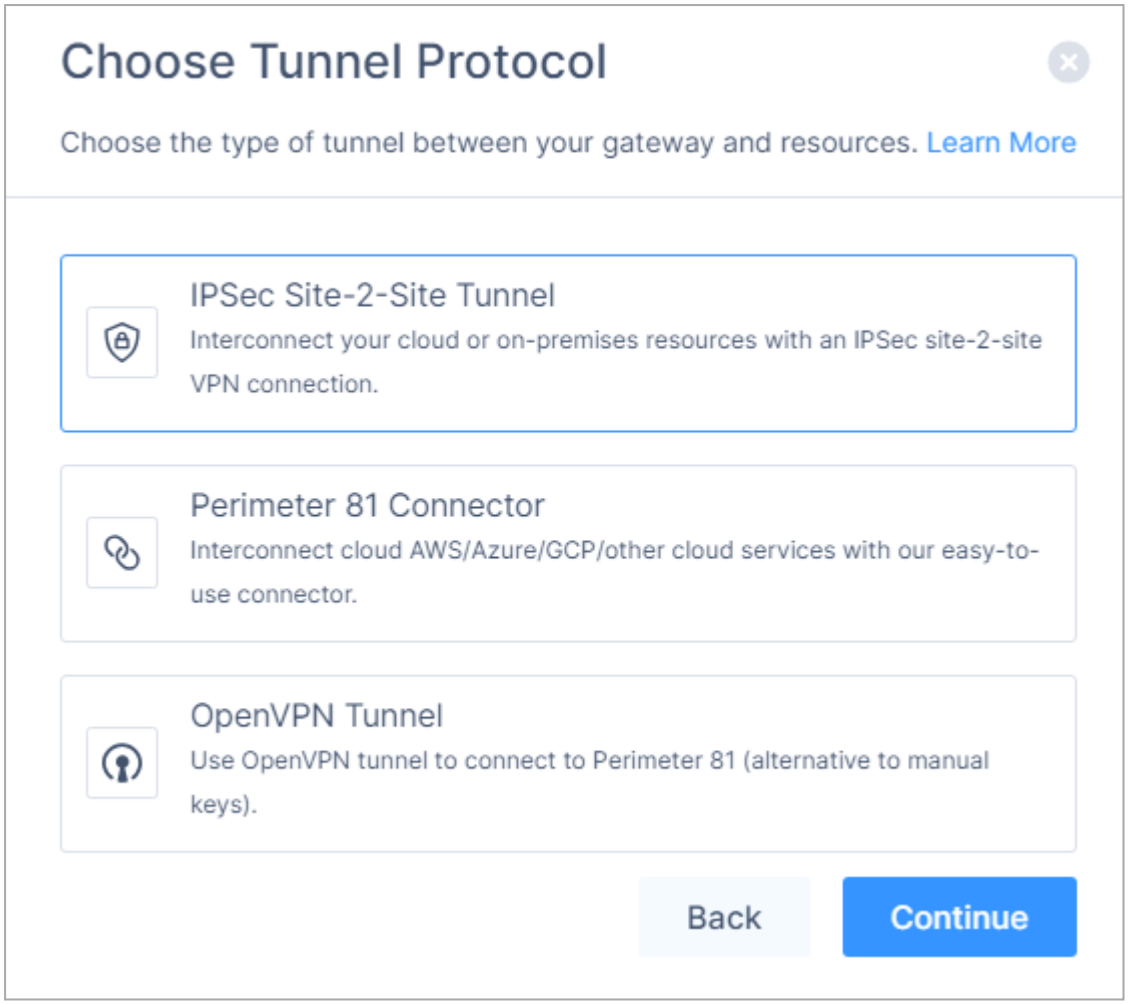
    The system downloads the configuration file.

Step 2 - Creating the Tunnel in the Harmony SASE Administrator Portal

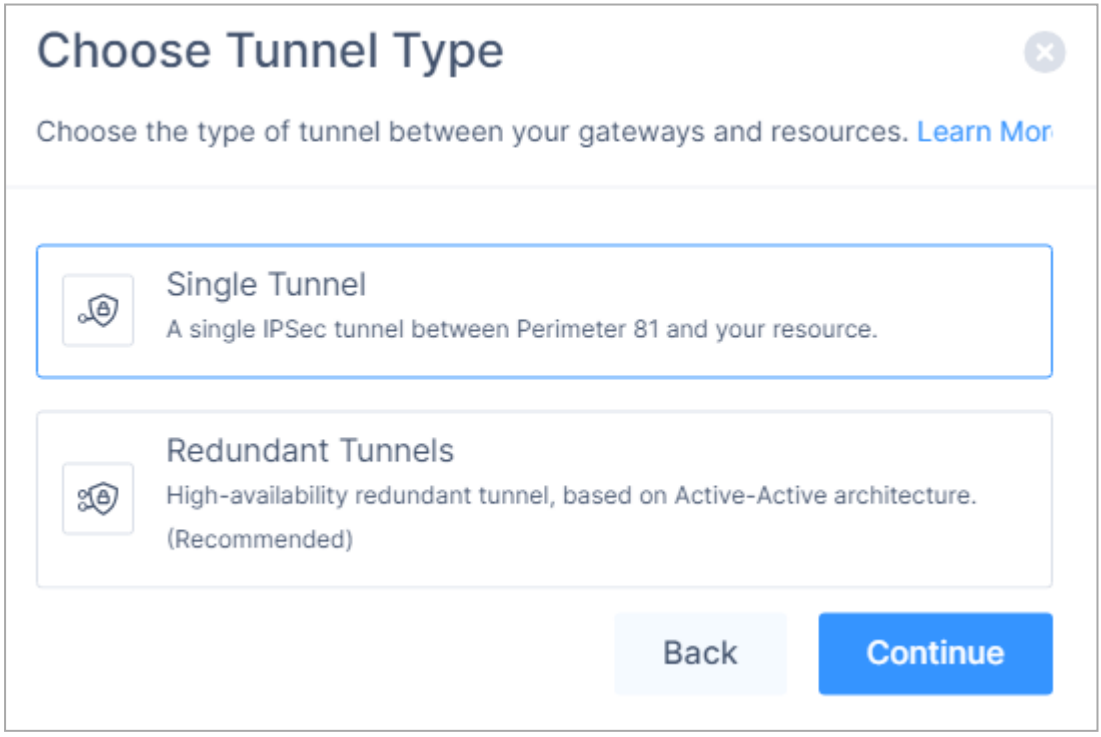
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



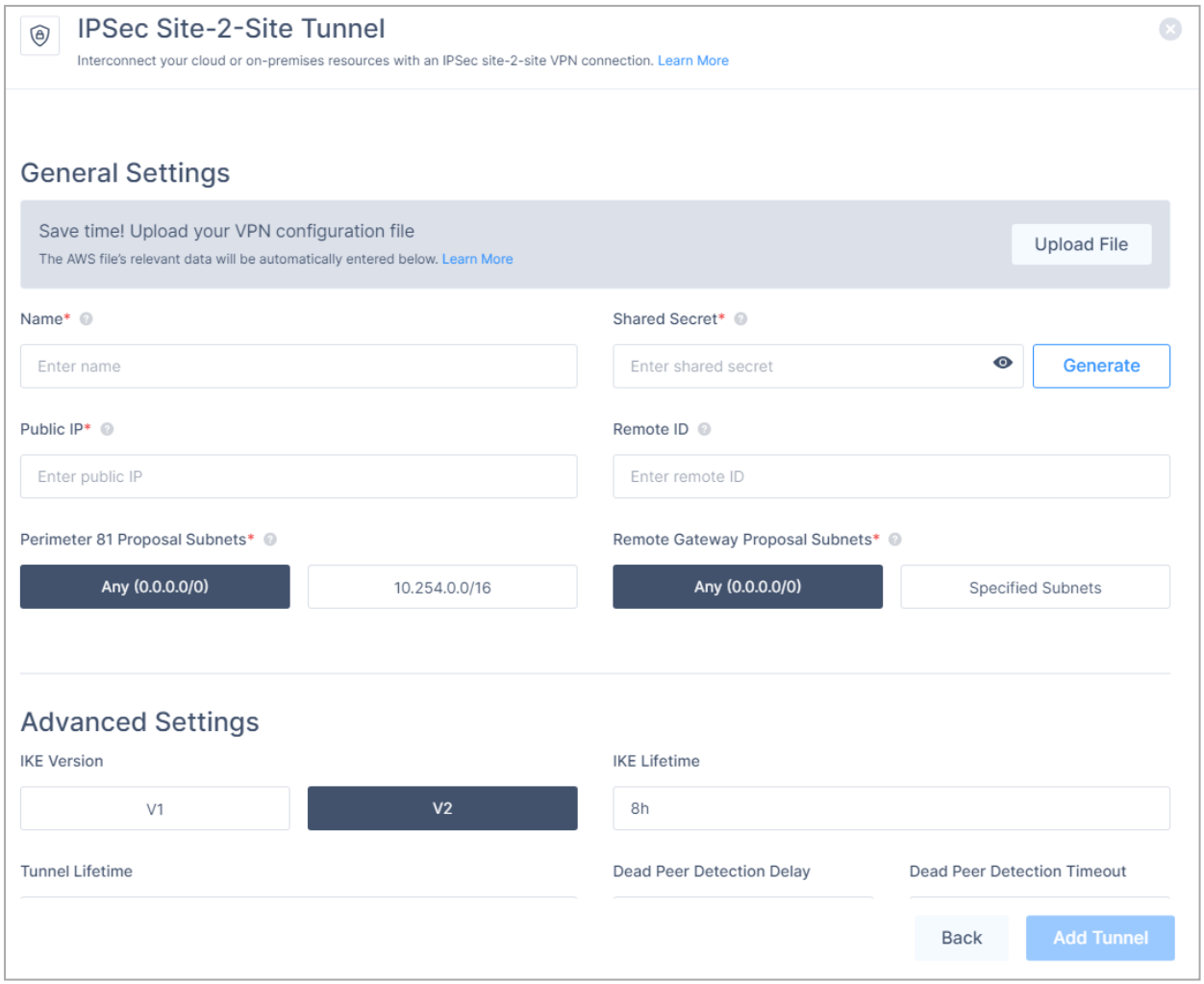
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. To automatically populate the tunnel configuration values, in the **General Settings** section, click **Upload File** and upload the configuration file downloaded from the Azure Management Portal.
7. For manual configuration, in the **General Settings** section, enter these:
   a. **Name** - Name of the tunnel.
   b. **Shared Secret** - Shared secret you set in the Azure Management Portal.
   c. **Public IP** - Public IP address of the Azure Virtual network gateway.
   d. **Remote ID** - Remote ID of Azure Virtual network gateway.
   e. **Perimeter 81 Gateway Proposal Subnets** - Any (0.0.0.0/0).
   f. **Remote Gateway Proposal Subnets** - Any (0.0.0.0/).
8. To enter the details in **Advanced Settings** section, open the configuration file downloaded from the Azure Management Portal and refer the

   [2] IPsec/IKE parameters.

```
! [2] IPsec/IKE parameters
!
!   > IKE version:                IKEv2
!     + Encryption algorithm:     aes-cbc-256
!     + Integrityalgorithm:       sha1
!     + Diffie-Hellman group:     2
!     + SA lifetime (seconds):    3600
!     + Pre-shared key:           MyKeyIsGr8!
!     + UsePolicyBasedTS:         False
!
!   > IPsec
!     + Encryption algorithm:     esp-gcm 256
!     + Integrity algorithm:      sha1
!     + PFS Group:                2
!     + SA lifetime (seconds):    27000
```

9. Enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

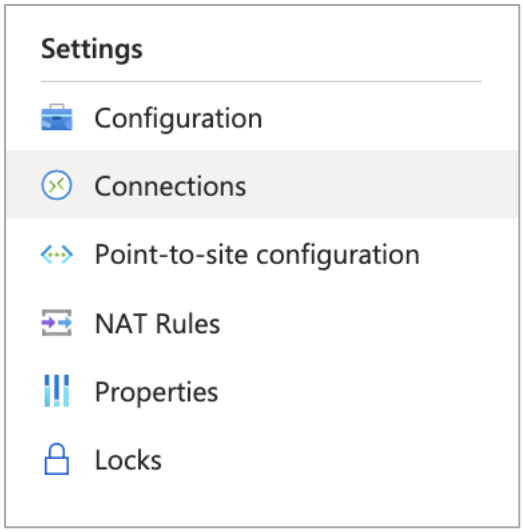
Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

10. Click **Add Tunnel**.

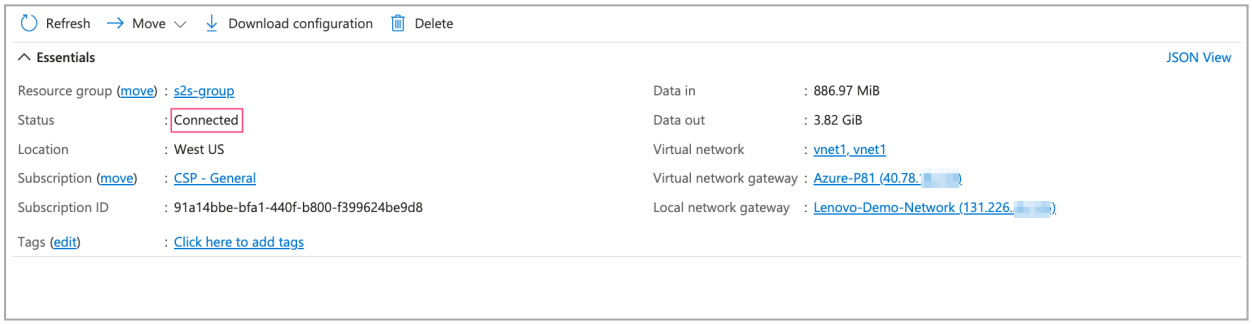
Verifying the VPN Connection in the Azure Management Portal

1. Access the Azure Management Portal and go to your **Virtual Network Gateway** page.
2. Go to **Settings** and click **Connections**.



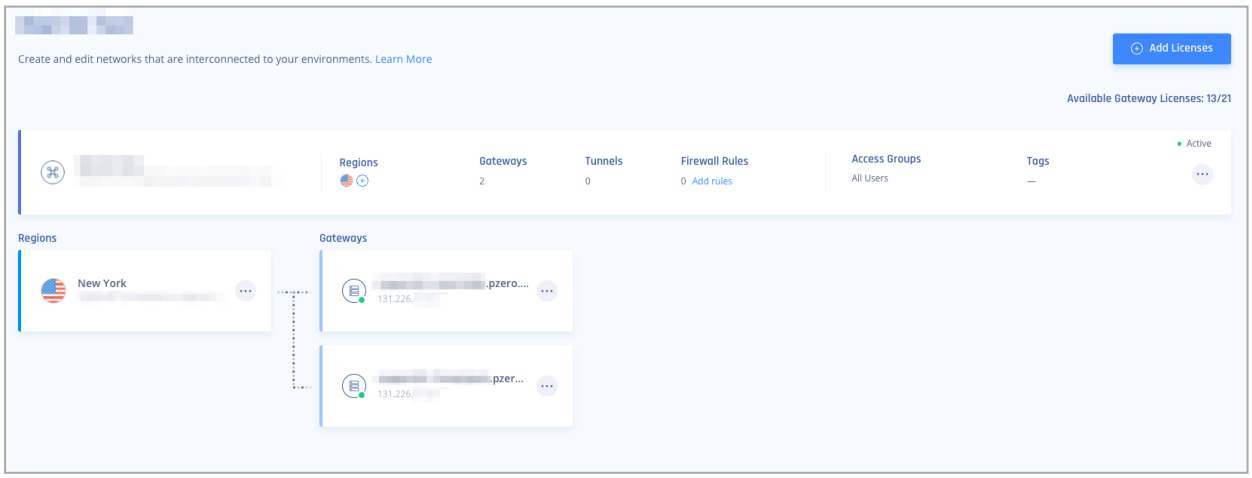
3. In the connection you created, click the **Overview** tab.

   Make sure that the **Status** is **Connected** and that there is data coming in (**Data in**) and going out (**Data out**).



Azure Virtual Network Gateway Redundant Tunnels

- Your Harmony SASE network must have at least two different gateways in the same network.



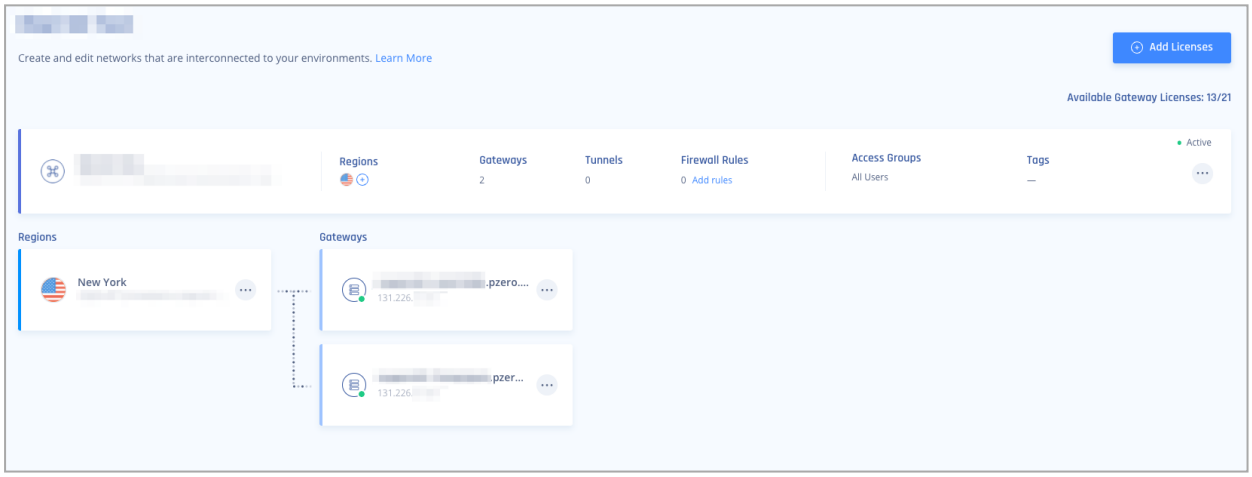
Notes -

- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Azure Redundant Tunnels - Virtual Network Gateway

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.
- Your Harmony SASE network must have at least two different gateways in the same network.

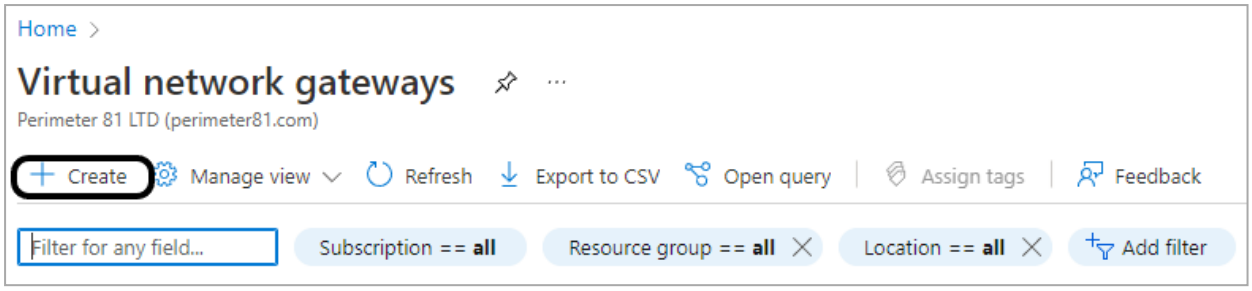


Notes -

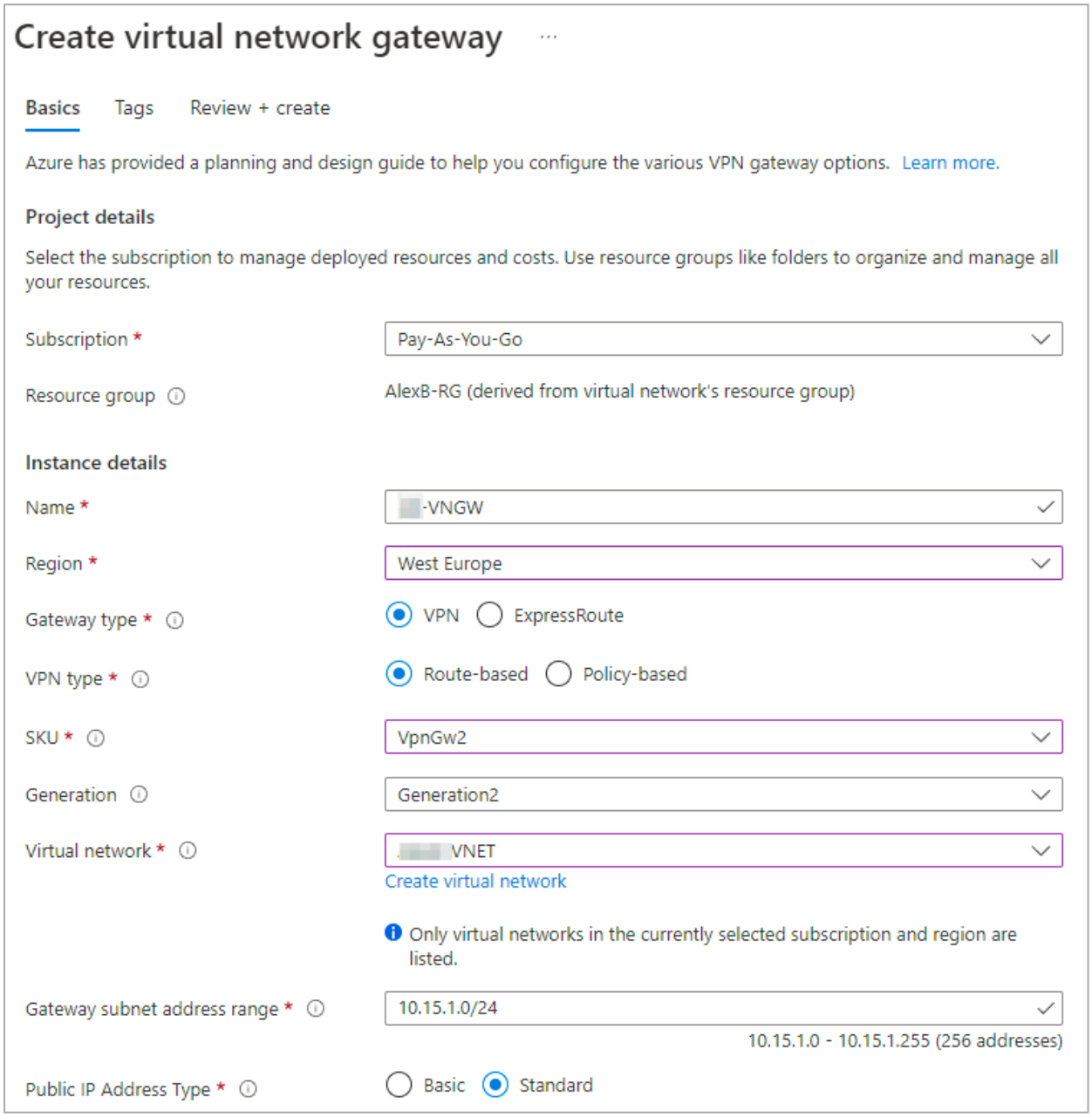
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the Azure Management Portal

1. Access the Azure Management Portal and go to **Virtual network gateways**.
2. Click **+Create**.



The **Create virtual network gateway** window appears.



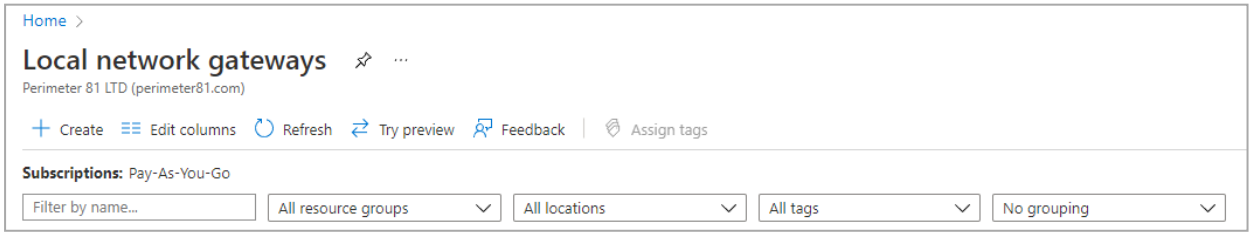
3. Enter these:

Item	Value
Name	Name of the gateway.
Region	Region where your resources are located.
Gateway type	VPN
VPN type	Route-Based
SKU	Select based on your preference and requirements.
Virtual network	Select the relevant VNET.
Gateway subnet address range	(If not filled automatically) Address range reserved for your Azure gateway.
Public IP address	Create new or select existing.
Enable active-active mode	Enabled
Second Public IP Address	Create new or select existing.
Configure BGP	Enabled
ASN	Leave default or configure based on your preference.
Custom Azure APIPA BGP IP address	Leave as empty.

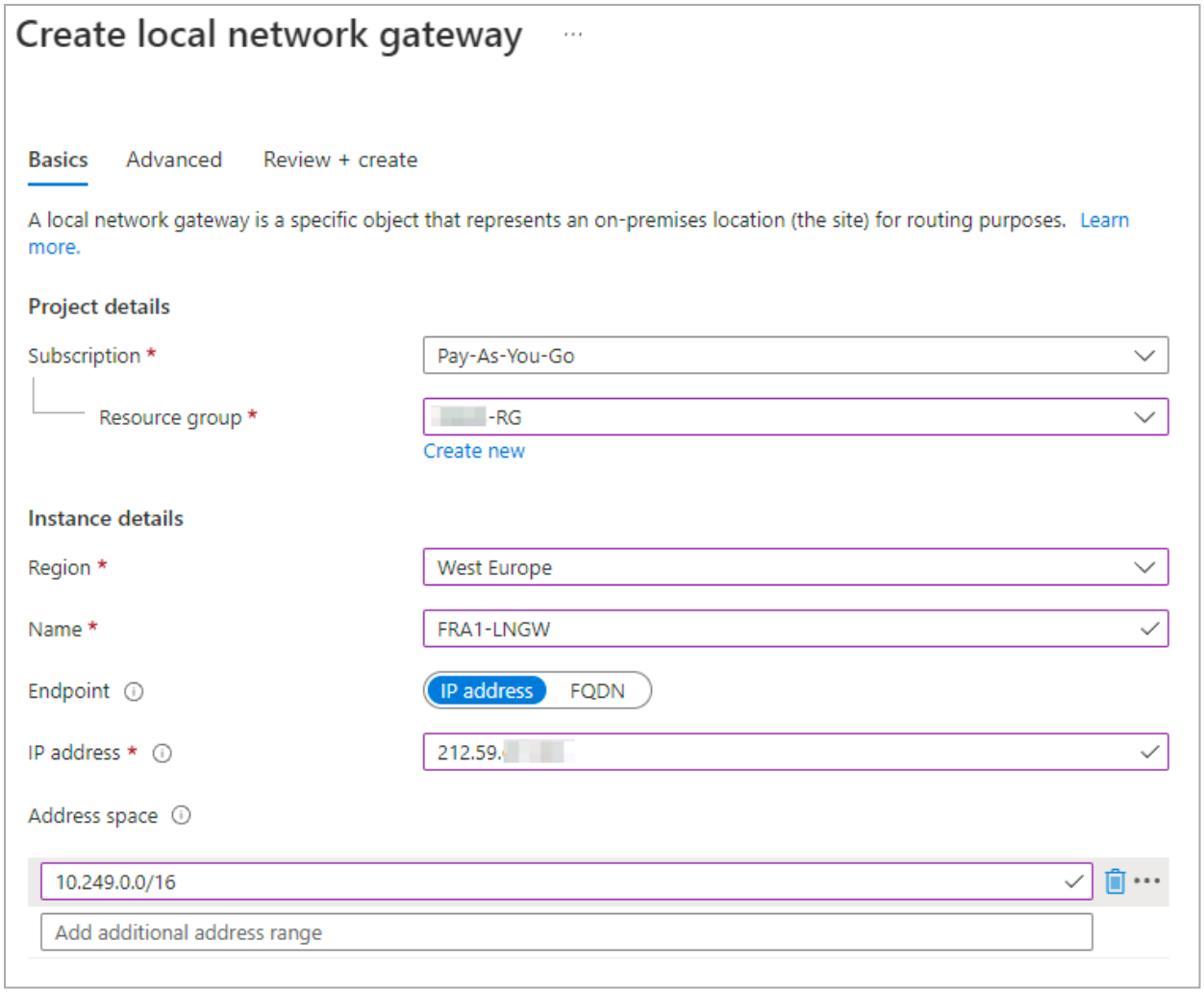
Creating Local Network Gateways

You must create two local network gateways, one for each of your Harmony SASE gateways.

1. Access the Azure Management Portal and go to **Local network gateways**.
2. Click **+Create**.



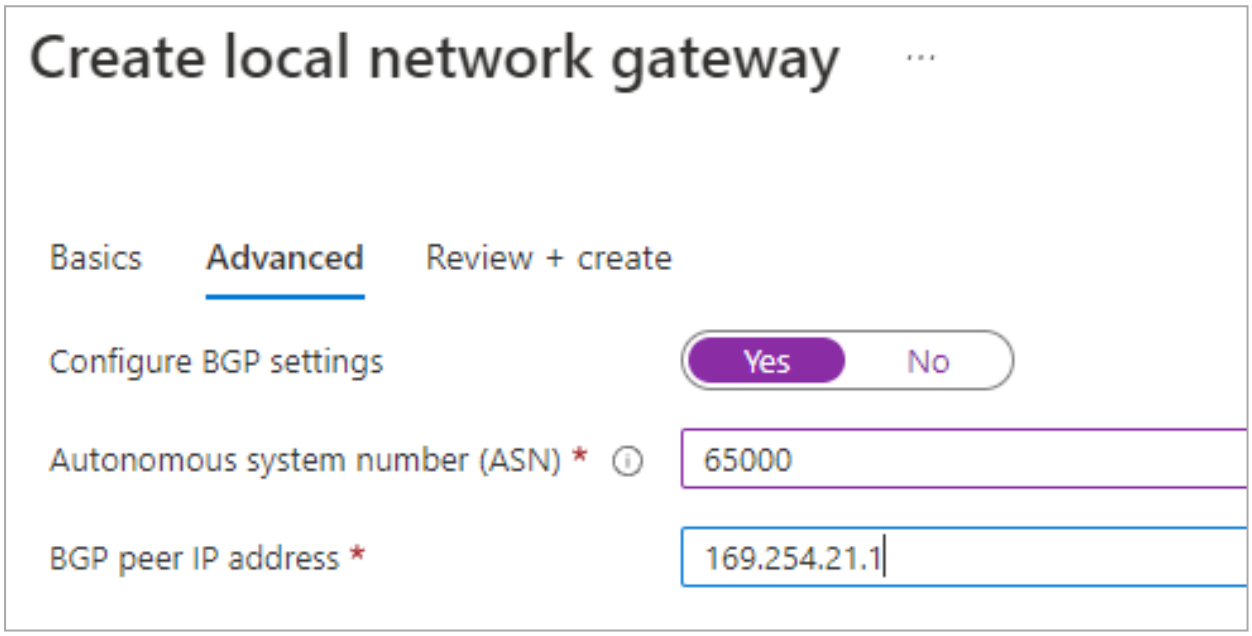
The **Create local network gateway** window appears.



3. Enter these:

Item	Value
Basics tab	
Resource group	Select the relevant resource group.
Region	Region where your resources are located.
Name	Name of the gateway.
Endpoint	IP address
IP address	Public IP address of the gateway in the Harmony SASE Administrator Portal.
Address Space	Subnet value of the network in the Harmony SASE Administrator Portal.

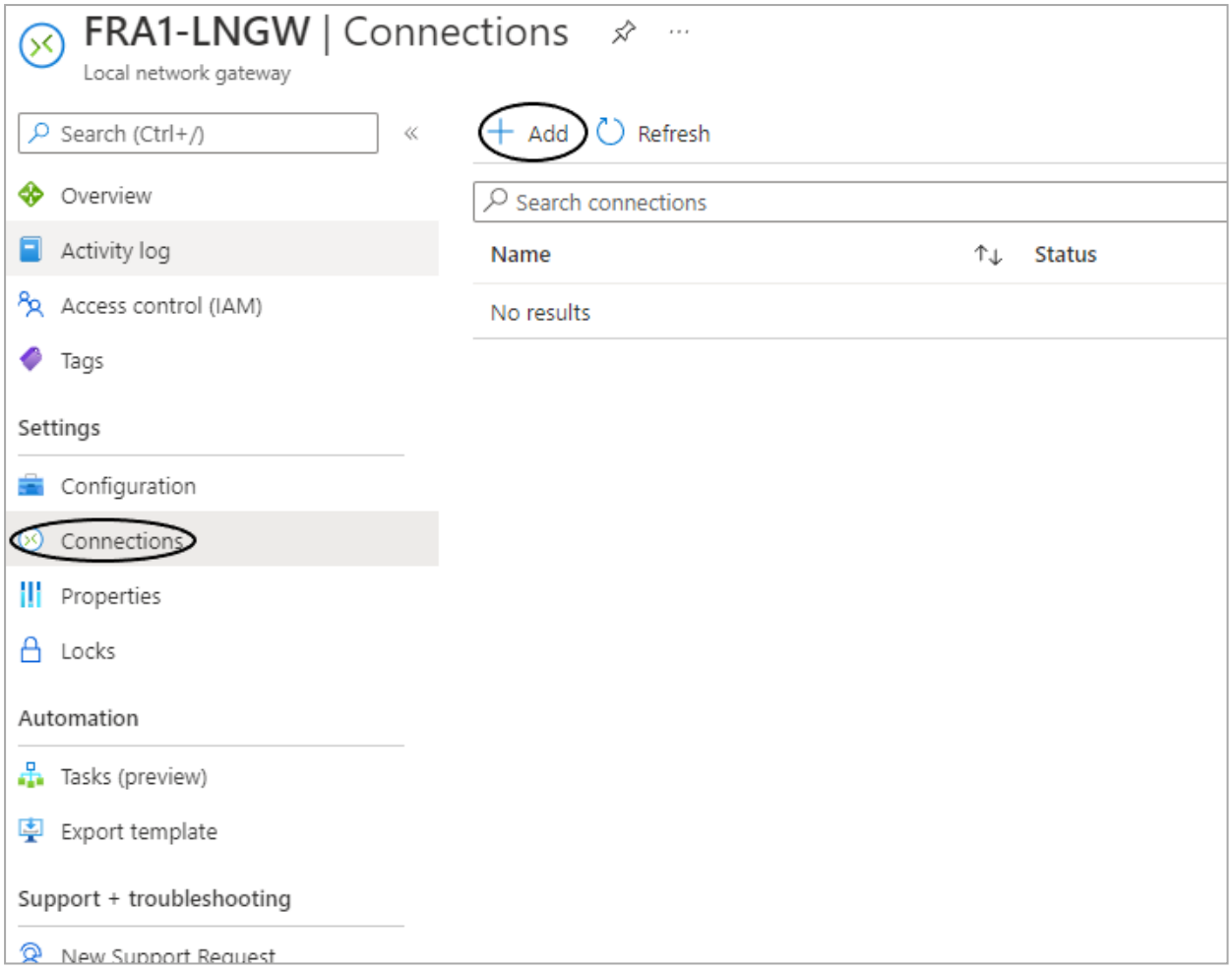
Item	Value
Advanced tab	
Configure BGP settings	Yes
ASN	Leave default or select a value from the permitted range.
BGP peer IP address	Any address from the permitted range.



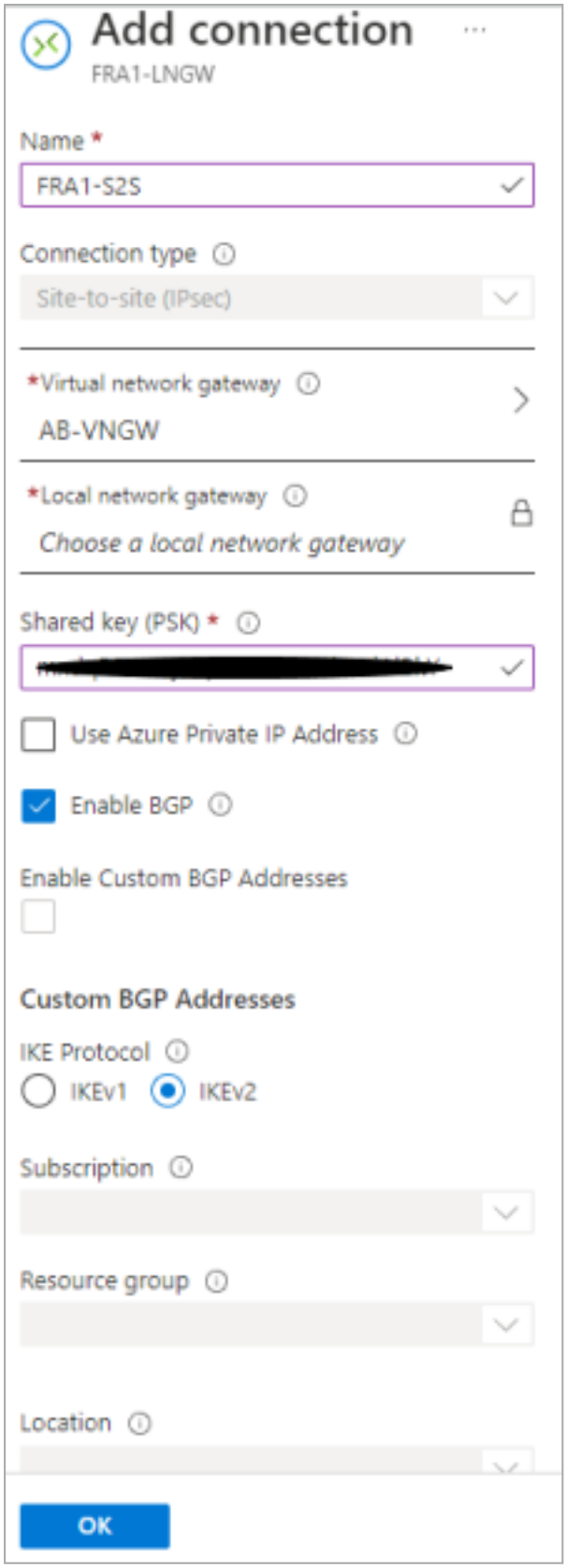
4. Repeat the above steps to create the second local network gateway.

Creating a Connection

1. Access the Azure Management Portal and go to your local network gateway and click **Connections**.
2. Click **+Add**.



The **Add connection** window appears.

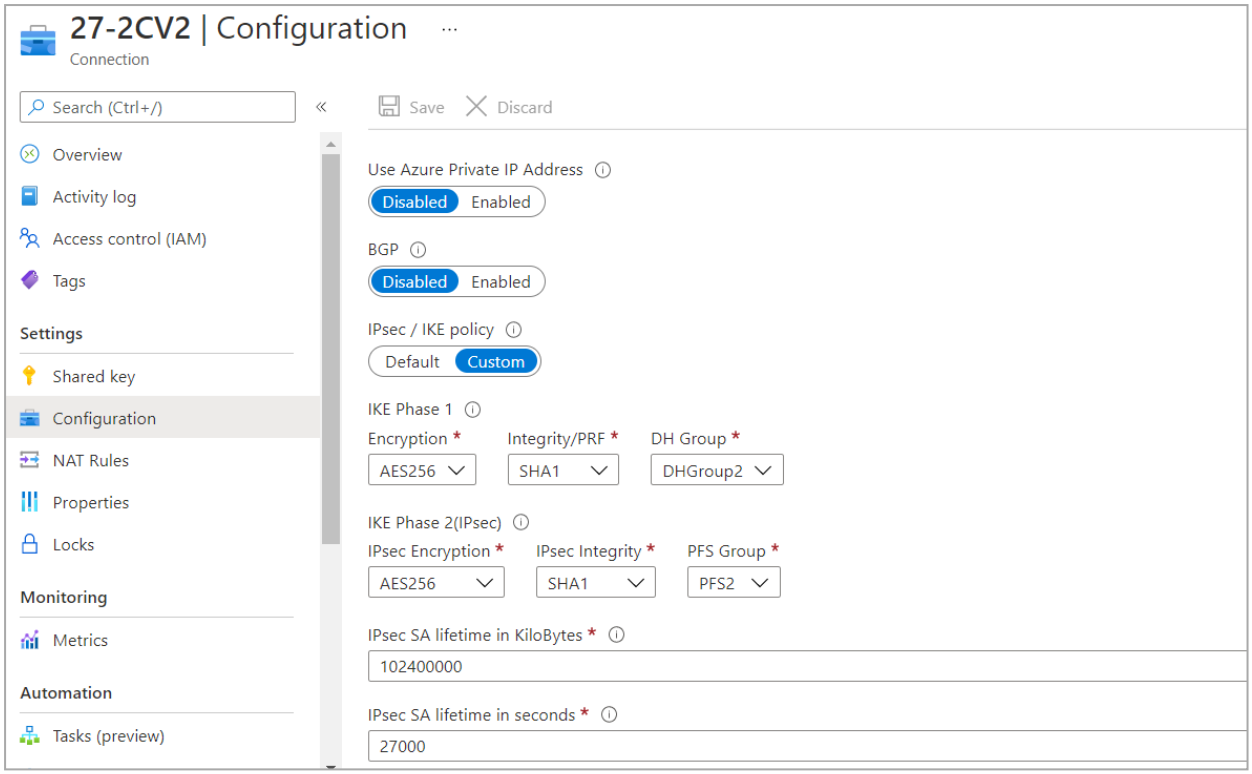


3. Enter these:

Item	Value
Name	Name of the connection.
Virtual Private Gateway	Select the first Virtual Private Gateway you created.
Local network gateway	Field is locked for editing.
Shared key (PSK)	Generate a key on the Harmony SASE side, or on a different PSK generating application. The key must only contain numbers, letters, underscore (_) and period (.).
Use Azure Private IP Address	Leave as cleared.
Enable BGP	Select the checkbox.
IKE Protocol	IKEv2

4. Click **OK**.
5. Open the connection you just created and click **Configuration**.

   The **Configuration** window appears.

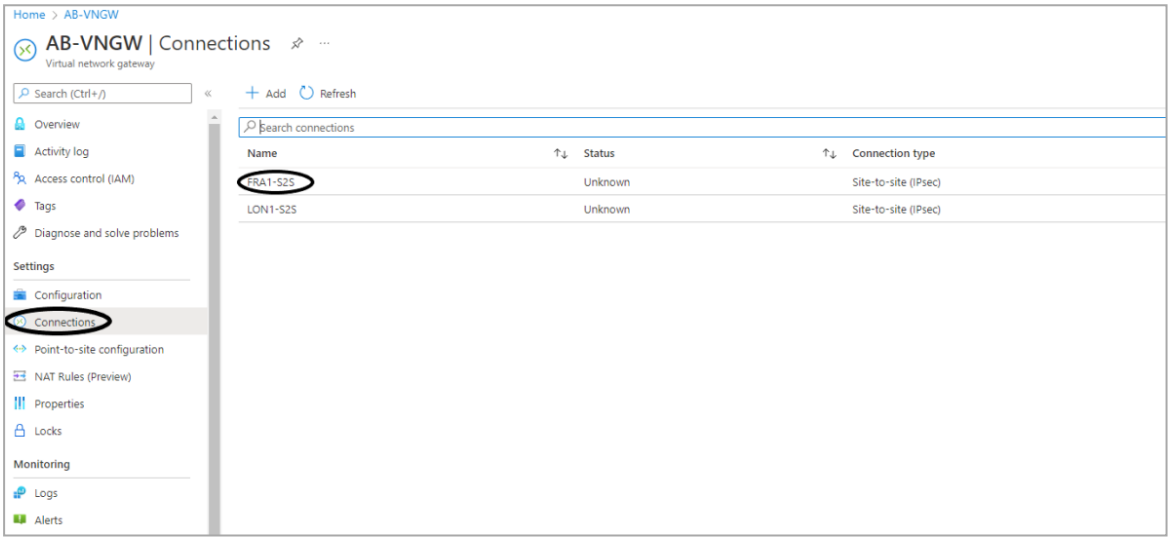


6. In the **IPsec / IKE policy** field, select **Custom** and enter these (same values are set for the tunnel in the Harmony SASE Administrator Portal:

Item	Value
Encryption	AES256
Integrity/ PRF	SHA1
DH Group	DHGroup2
IPsec Encryption	AES256
IPsec Integrity	SHA1
PFS Group	PFS2
IPsec SA lifetime in KiloBytes	102400000

Item	Value
IPsec SA lifetime in seconds	27000

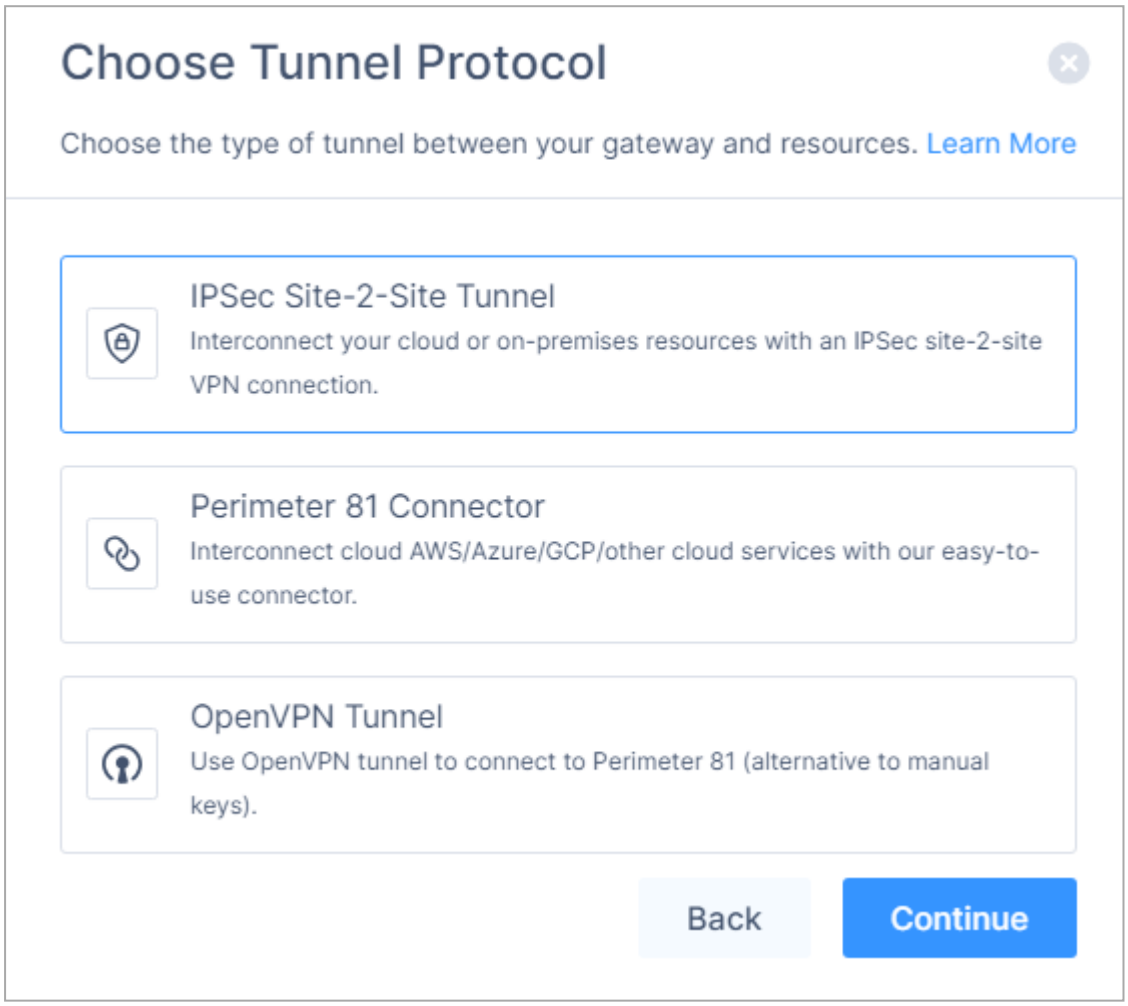
7. Repeat the above steps to create a connection for the second local network gateway.
8. Download the tunnel configuration for the first connection:
   a. Go to your **Virtual network gateway** > **Settings** > **Connections** and click on your first connection.



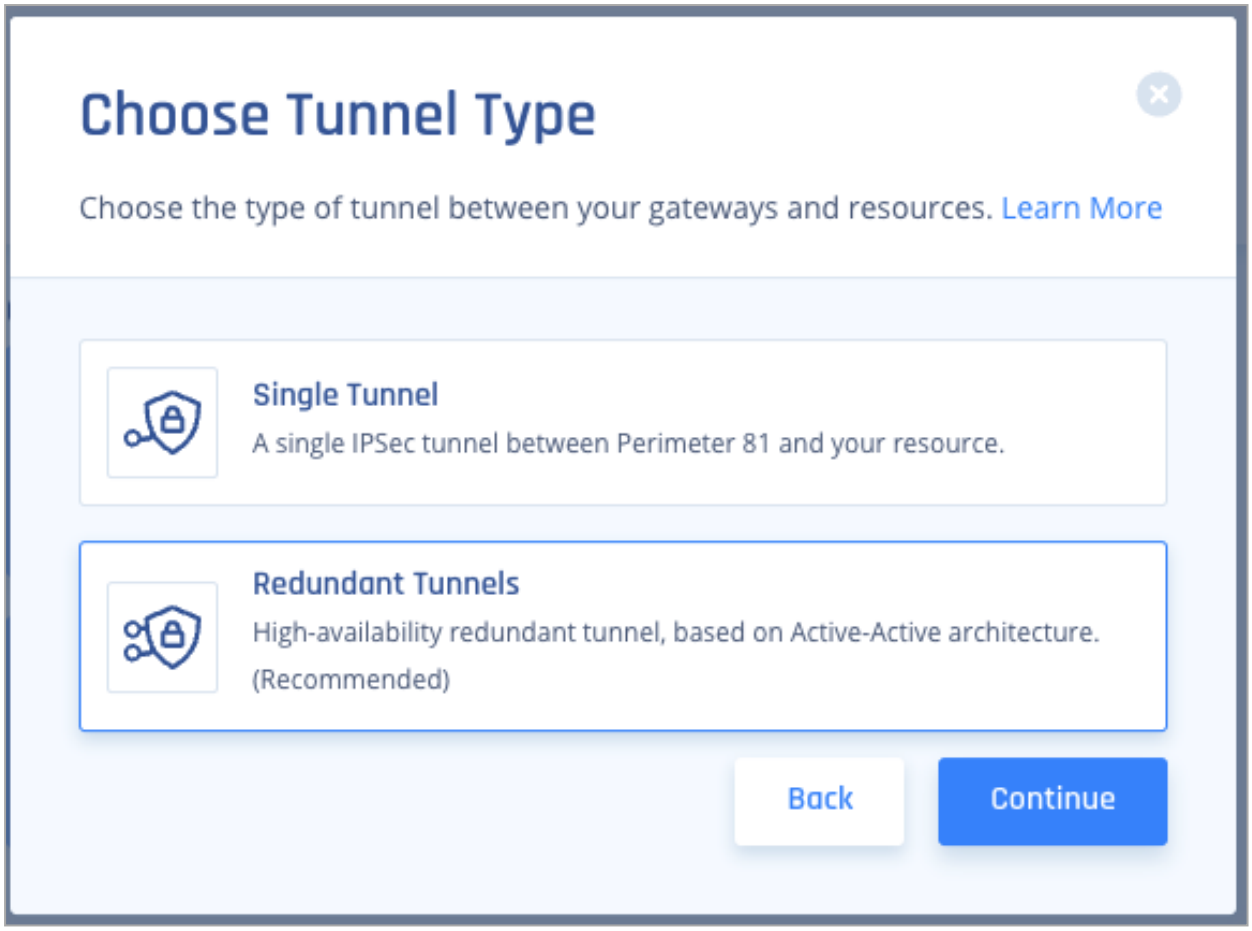
   b. Click **Download configurations**.
   c. Enter these:
      i. **Device vendor** - Generic Samples
      ii. **Device family** - Device Parameters
      iii. **Firmware version** - 1.0
   d. Click **Download configuration**.

Step 2 - Creating the Tunnels in the Harmony SASE Administrator Portal

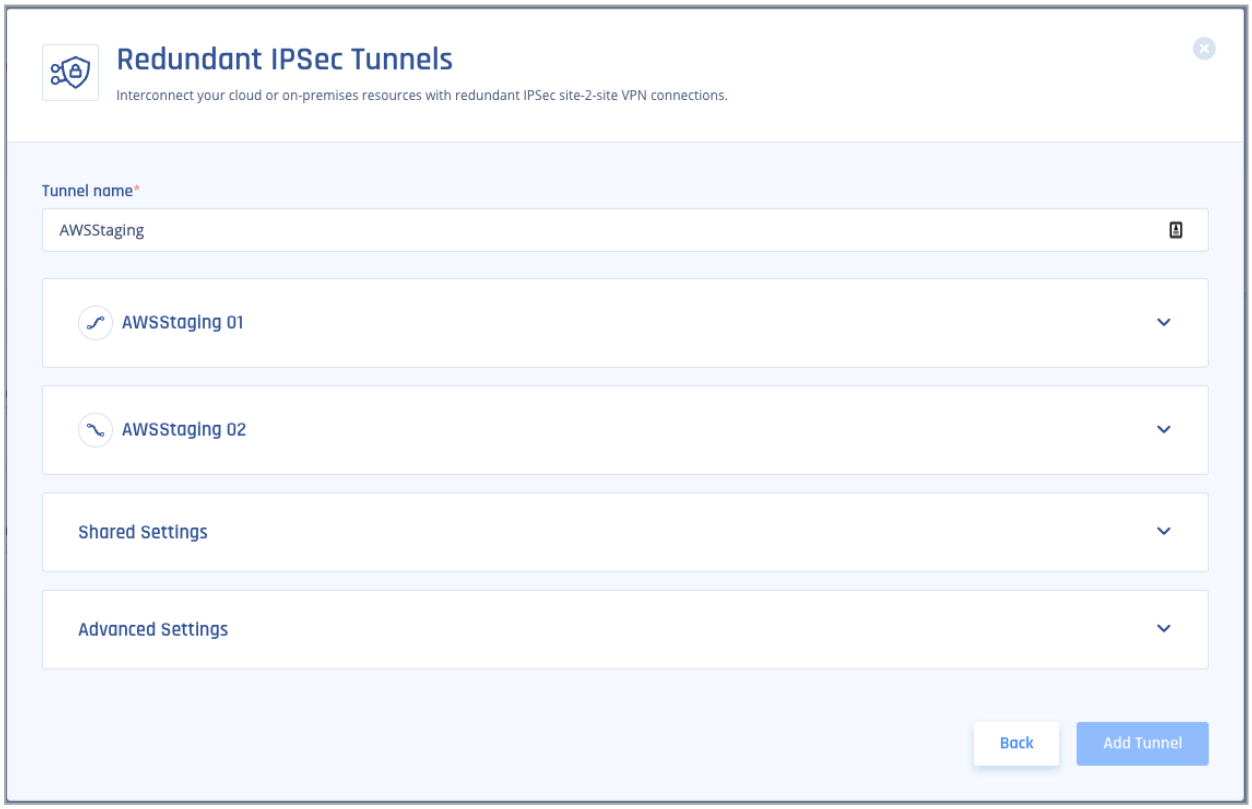
1. Access the Harmony SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.



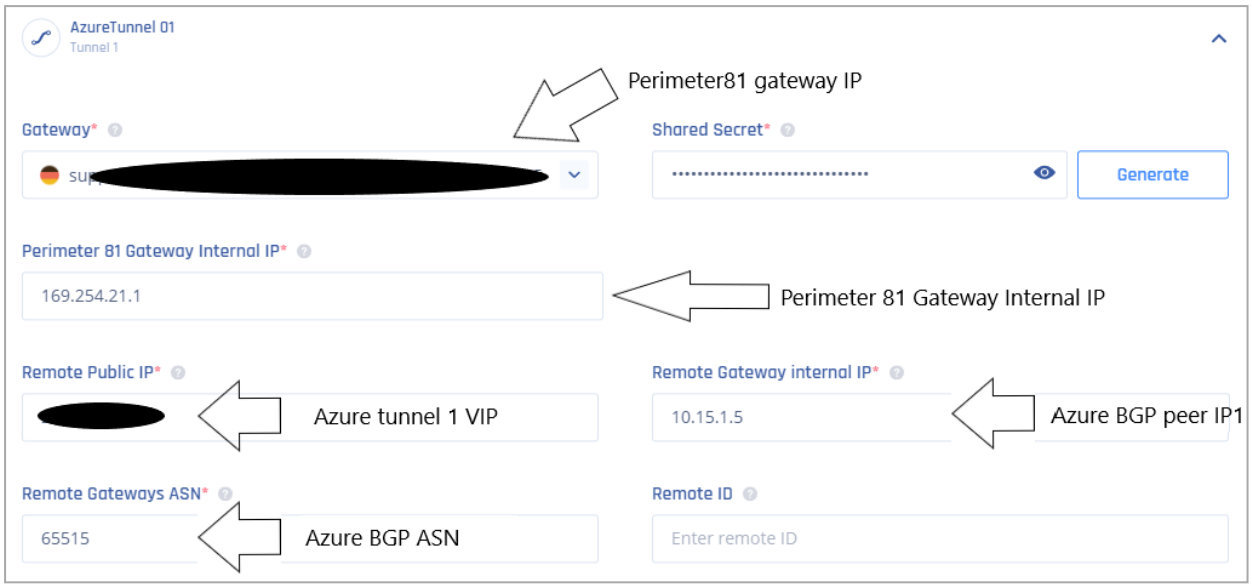
6. Copy the values for the first tunnel from the downloaded configuration file:

```
!   > On-premises VPN IP:
!   > On-premises address prefixes:
!     + CIDR: 10.243.0.0/16
!       - Prefix:   10.243.0.0
!       - Netmask:  255.255.0.0
!       - Wildcard: 0.0.255.255
!
! [2] IPsec/IKE parameters
!
!   > IKE version:              IKEv2
!     + Encryption algorithm:   aes-cbc-256
!     + Integrityalgorithm:     sha1
!     + Diffie-Hellman group:   2
!     + SA lifetime (seconds):  3600
!     + Pre-shared key:
!     + UsePolicyBasedTS:       False
!
!   > IPsec
!     + Encryption algorithm:   esp-gcm 256
!     + Integrity algorithm:
!     + PFS Group:              none
!     + SA lifetime (seconds):  3600
!
! [3] BGP parameters - Azure VPN gateway
!
!   > Azure virtual network
!     + Enable BGP:             True
!     + Azure BGP ASN:          65515
!     + BGP peer IP1:           10.15.1.5
!     + BGP peer IP2:           10.15.1.4
!     + BGP tunnel 1 VIP:
!     + BGP tunnel 2 VIP:
!   > On-premises network / LNG
!     + On premises BGP ASN:    65000
!     + On premises BGP IP:     169.254.21.1
!
```

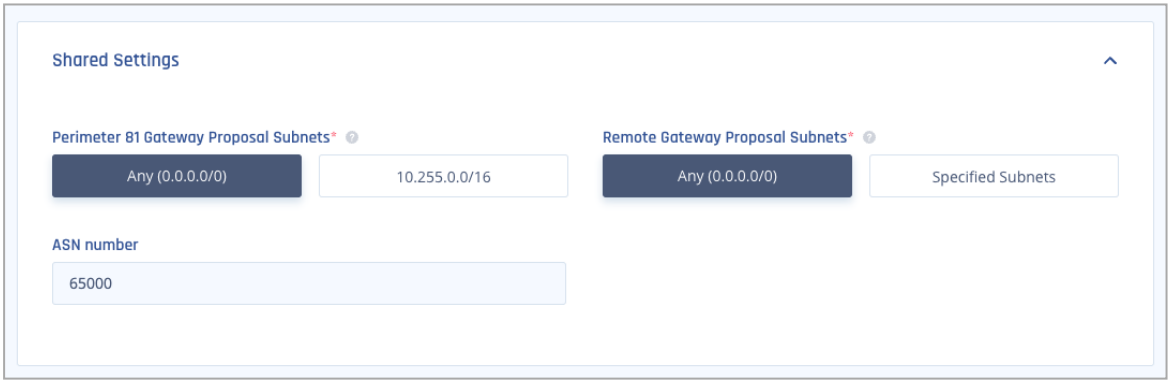
Perimeter 81 gateway IP
Pre-Shared Key
Remote Gateways ASN
Remote Gateway internal IP1
Remote Gateway internal IP2
Remote Public IP1
Remote Public IP2
Perimeter81 ASN
Perimeter 81 Gateway Internal IP

Item	Value
Shared Secret	Pre-Shared Key
Harmony SASE gateway Internal IP	Inside IP Addresses of Customer Gateway
Remote Public IP & Remote ID	Outside IP Addresses of Virtual Private Gateway
Remote Gateway internal IP	Inside IP Addresses of Virtual Private Gateway
Remote Gateway ASN	BGP Configuration Options of Virtual Private Gateway ASN

In the Harmony SASE Administrator Portal, enter the values for Tunnel 1 as:



7. Repeat step 6 for the second tunnel.
8. In the **Shared Settings** section:
   a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.
   b. **ASN** number must be the same for the Harmony SASE side.



9. In the **Advanced Settings** section, enter the information for your tunnel type (unless you have configured customer settings on the Azure side):

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

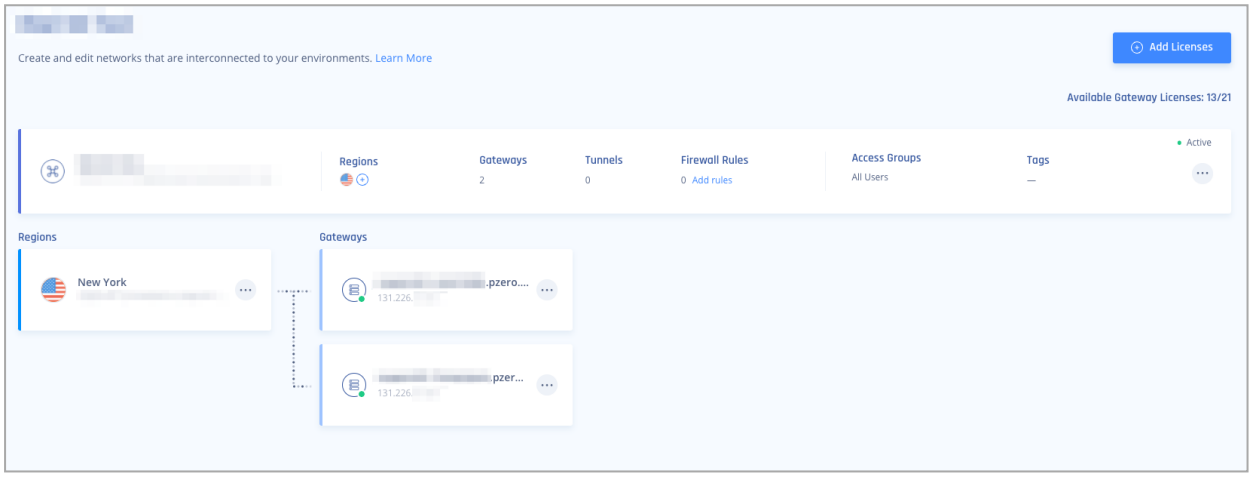
[1] Suggested values. For other supported ciphers, see this Google article.

10. Click **Add Tunnel**.

Azure Virtual WAN Redundant Tunnels

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.
- Your Harmony SASE network must have at least two different gateways in the same network.



Notes -

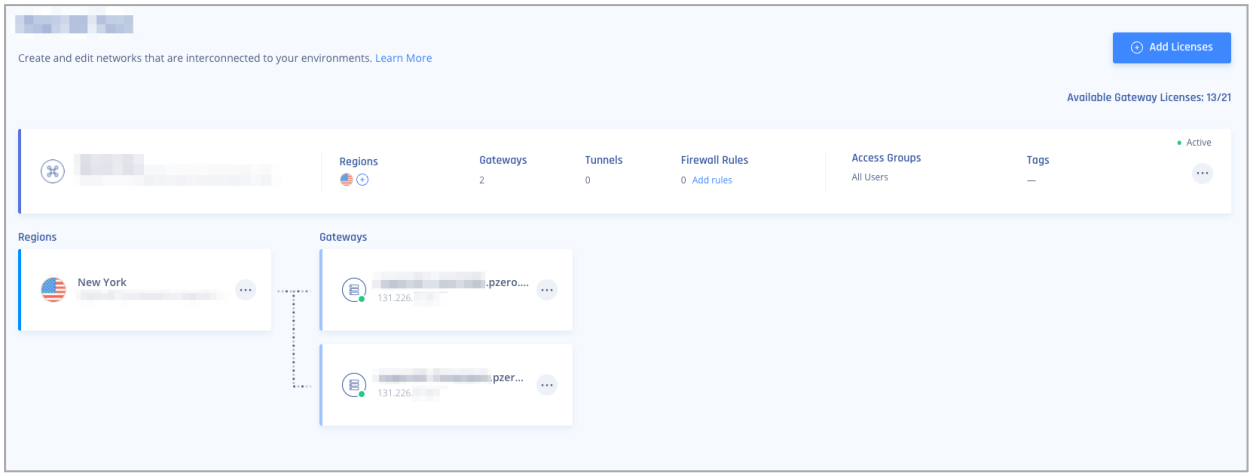
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Azure Redundant Tunnels - Virtual WAN

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Harmony SASE network must have at least two different gateways in the same network.

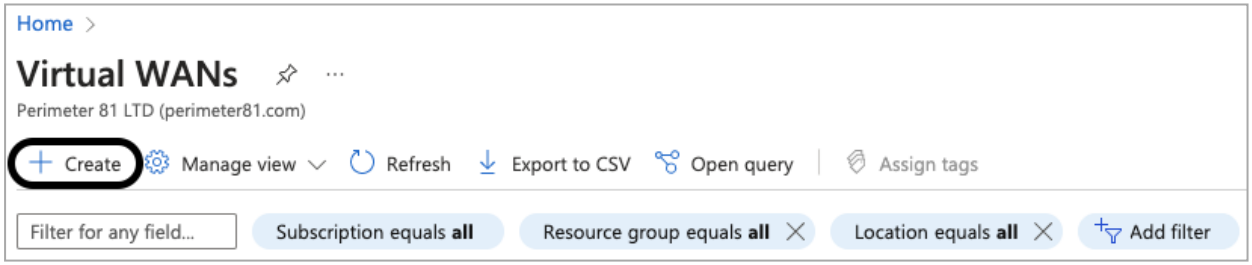


Notes -

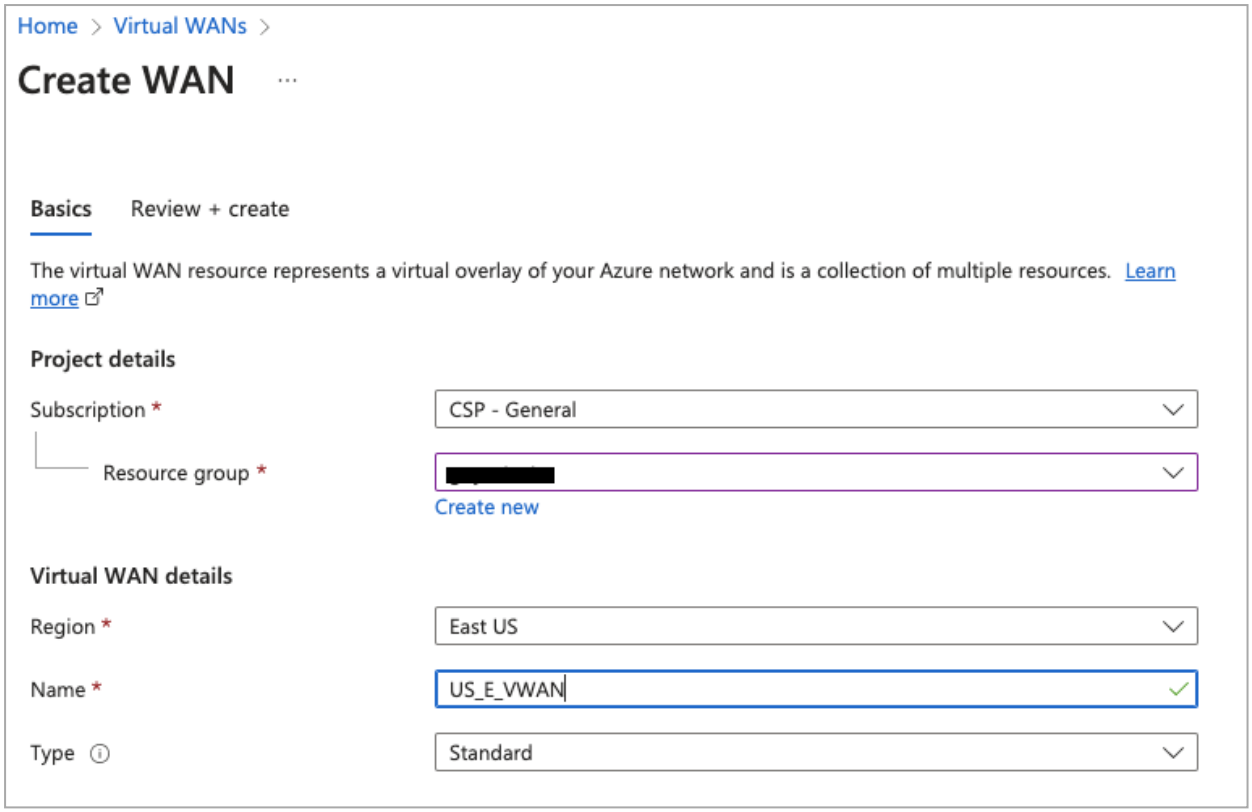
- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the Azure Management Portal

1. Access the Azure Management Portal and go to **Virtual WANs** and click **+Create**.



The **Create WAN** window appears.



2. In the **Basics** tab, enter these:

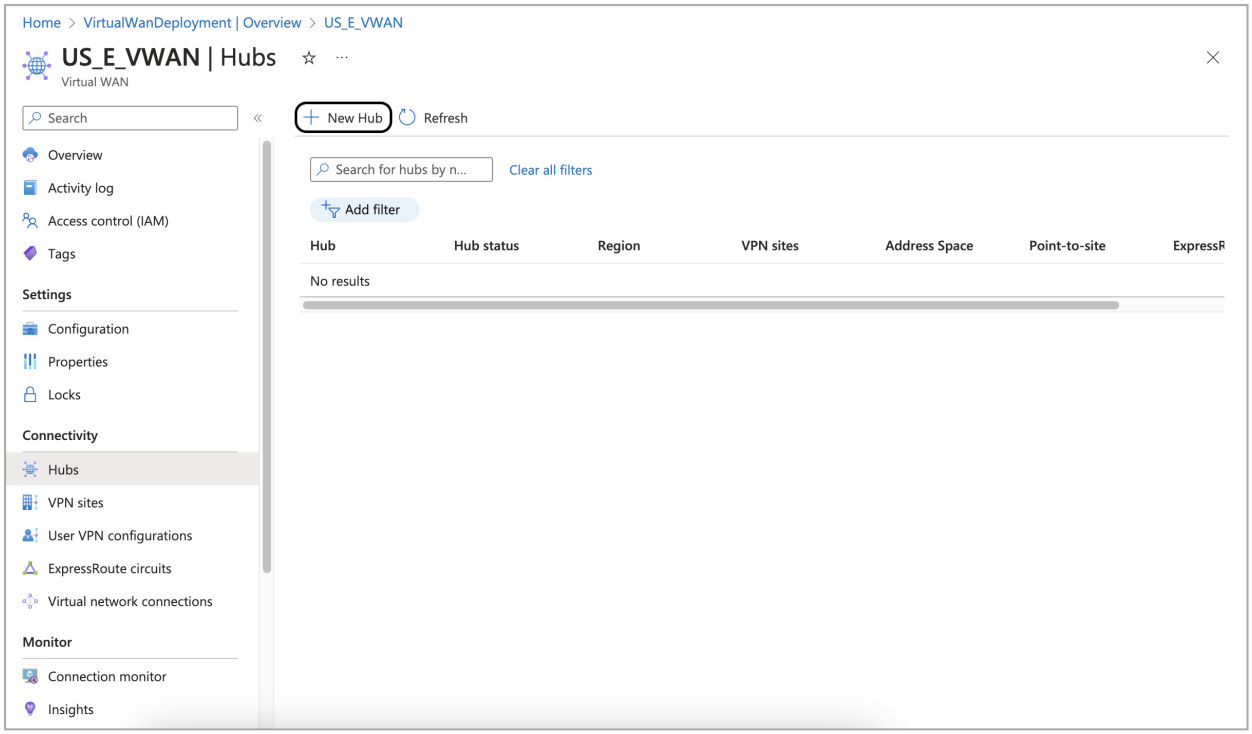
Item	Value
Subscription	Select the relevant subscription and resource group.
Region	Region where your resources are located.
Name	Name of the virtual WAN.
Type	Standard

3. Click **Review+create**.
4. Click **Create**.

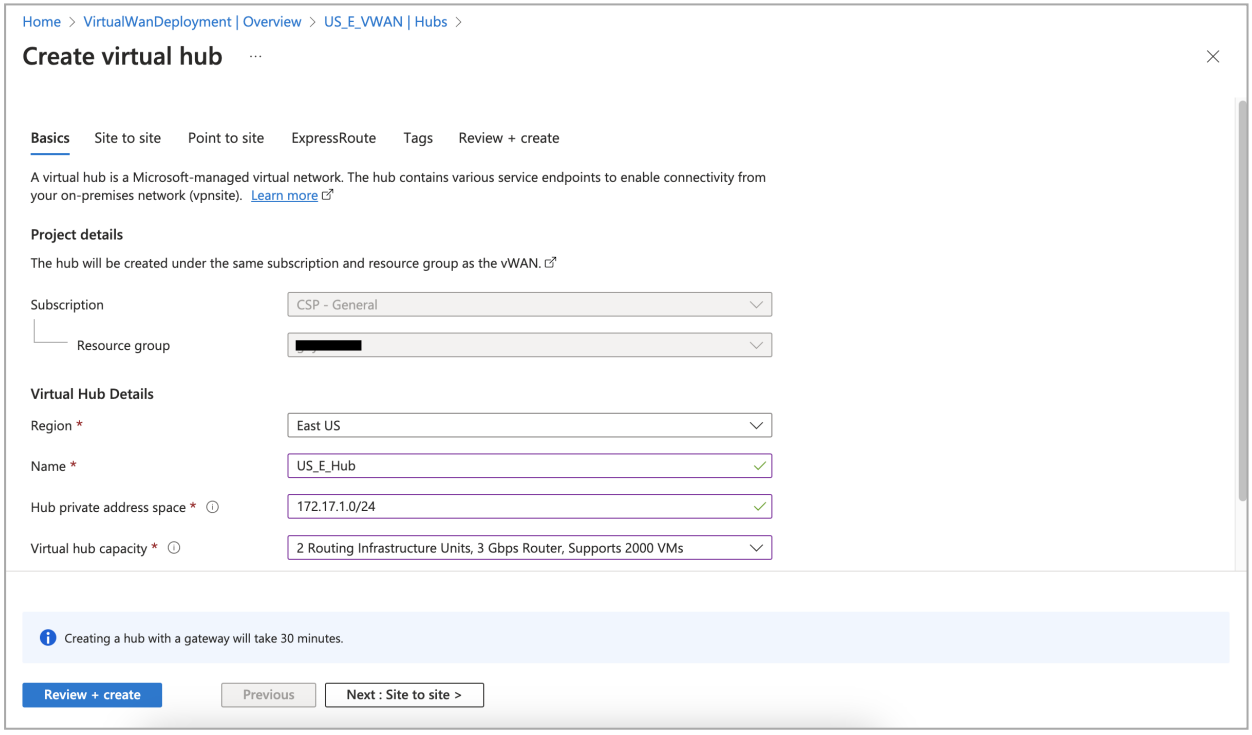
Creating a Virtual Hub

Note - If you already have a virtual hub in your Azure region, skip this step.

1. Access the Azure Management Portal and go to the Virtual WAN you created and from the left pane, click **Hubs** > **+New Hub**.



The **Create virtual hub** window appears.



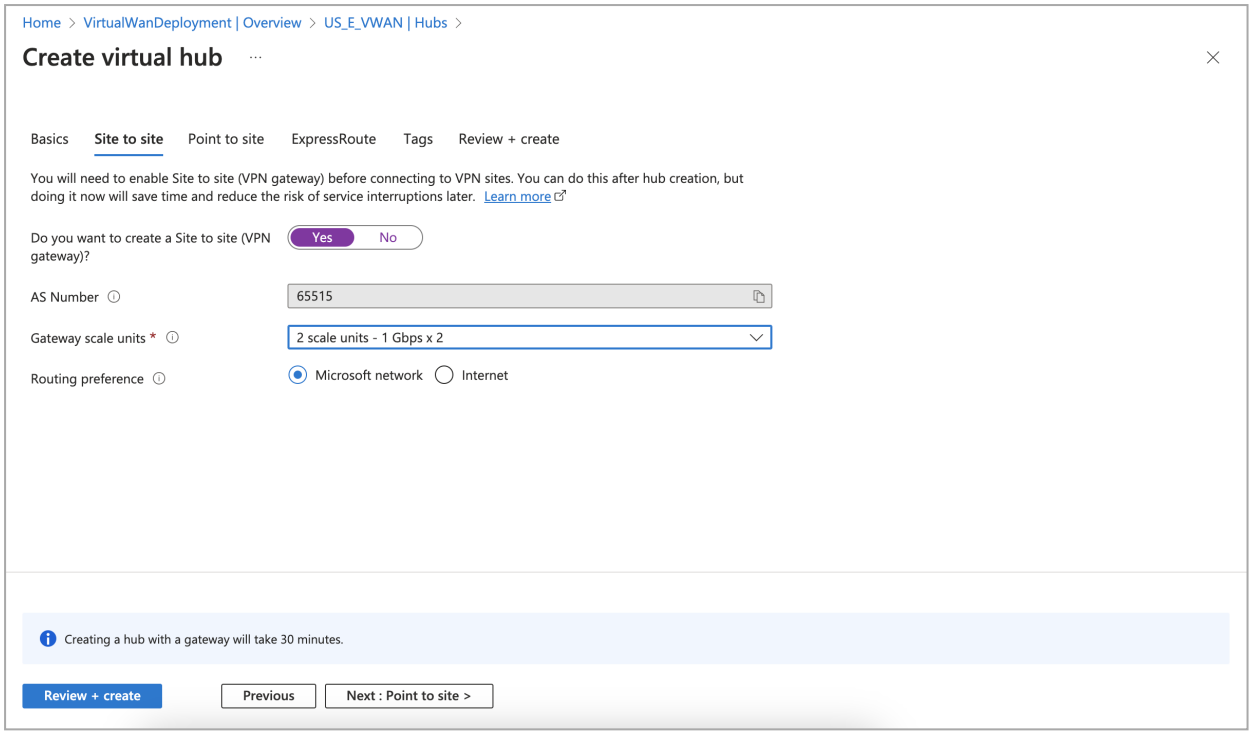
2. In the **Basics** tab, enter these:

Item	Value
Region	Region where your resources are located.

Item	Value
Name	Name of the virtual hub.
Endpoint	IP Address
Hub private address space	Select a CIDR range that does not overlap with any existing CIDR (/24 range is the minimal one).
Address Space	Subnet value of the network in the Harmony SASEAdministrator Portal.
Virtual hub capacity	Select a value according to the maximum number of VMs to be connected through this hub.

3. In the **Site to site** tab, enter these:

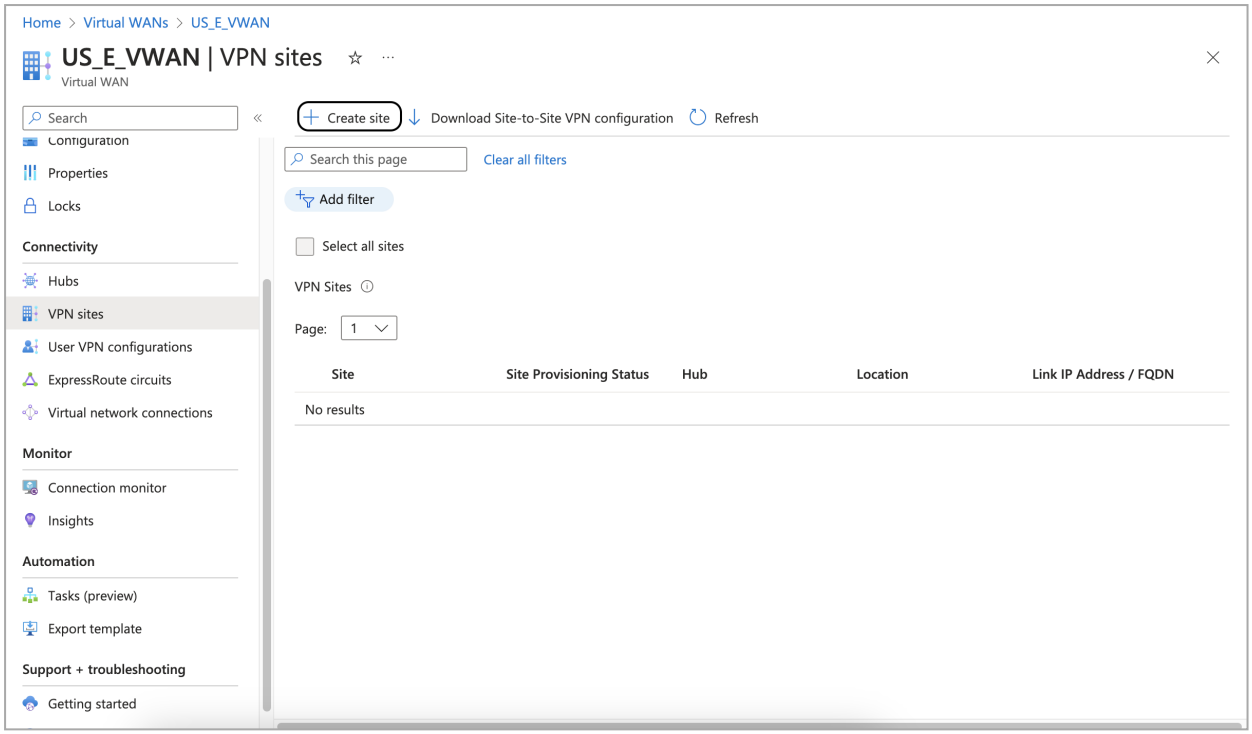
Item	Value
Create a Site to site (VPN gateway)	Yes
Gateway scale units	Select the required value from the list.
Routing preference	Microsoft network



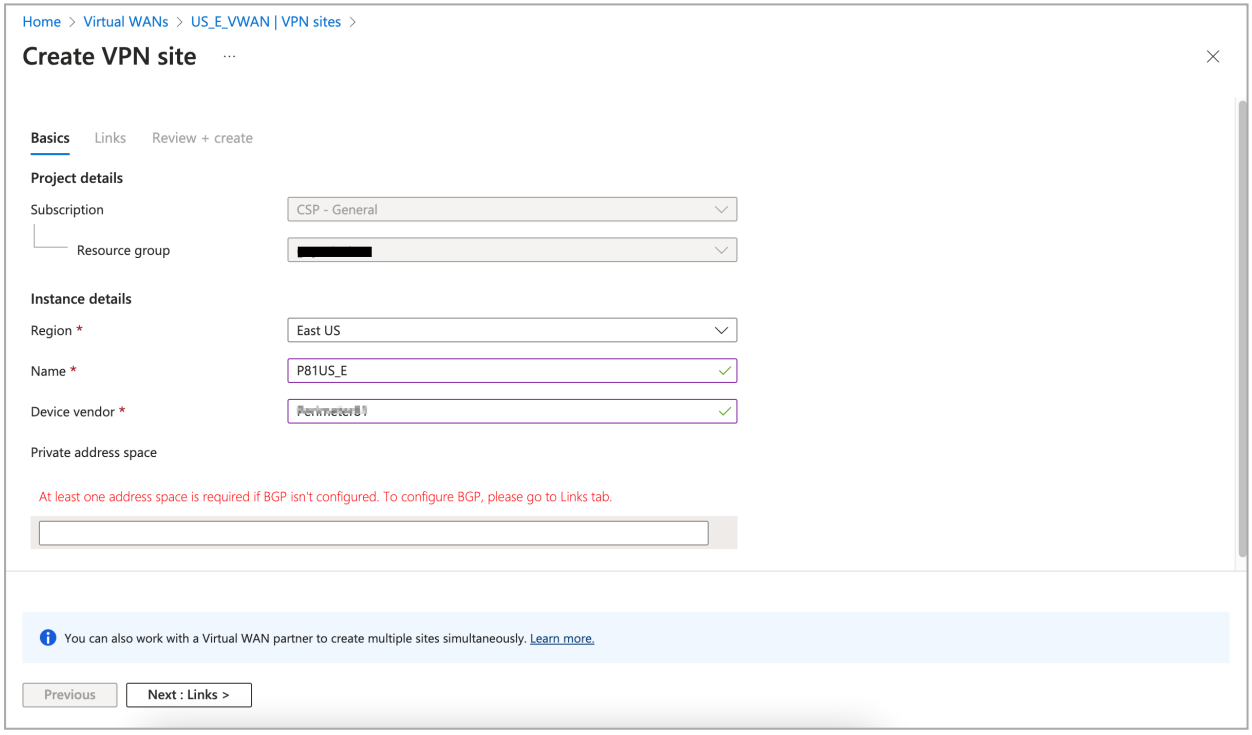
4. Click **Review+create**.
5. Click **Create**.

Creating a Site

1. Access the Azure Management Portal and go to the Virtual WAN you created, and from the left pane, select **VPN sites**.
2. Click **+Create site**.



The **Create VPN site** window appears.



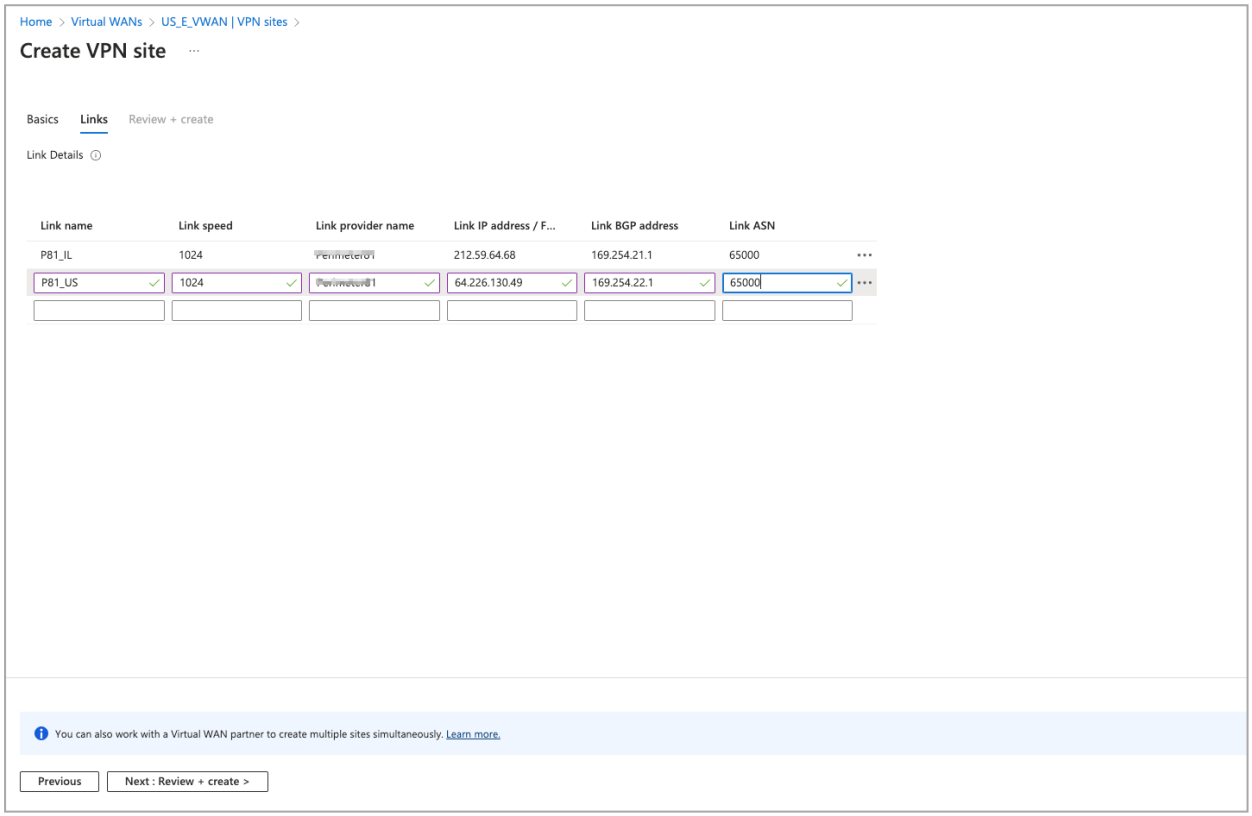
3. In the **Basics** tab, enter these:

Item	Value
Region	Region where your resources are located.

Item	Value
Name	Name of the VPN site.
Device vendor	Harmony SASE
Private address space	Leave as empty.

4. Click **Next:Links**.

   The **Links** tab appears.

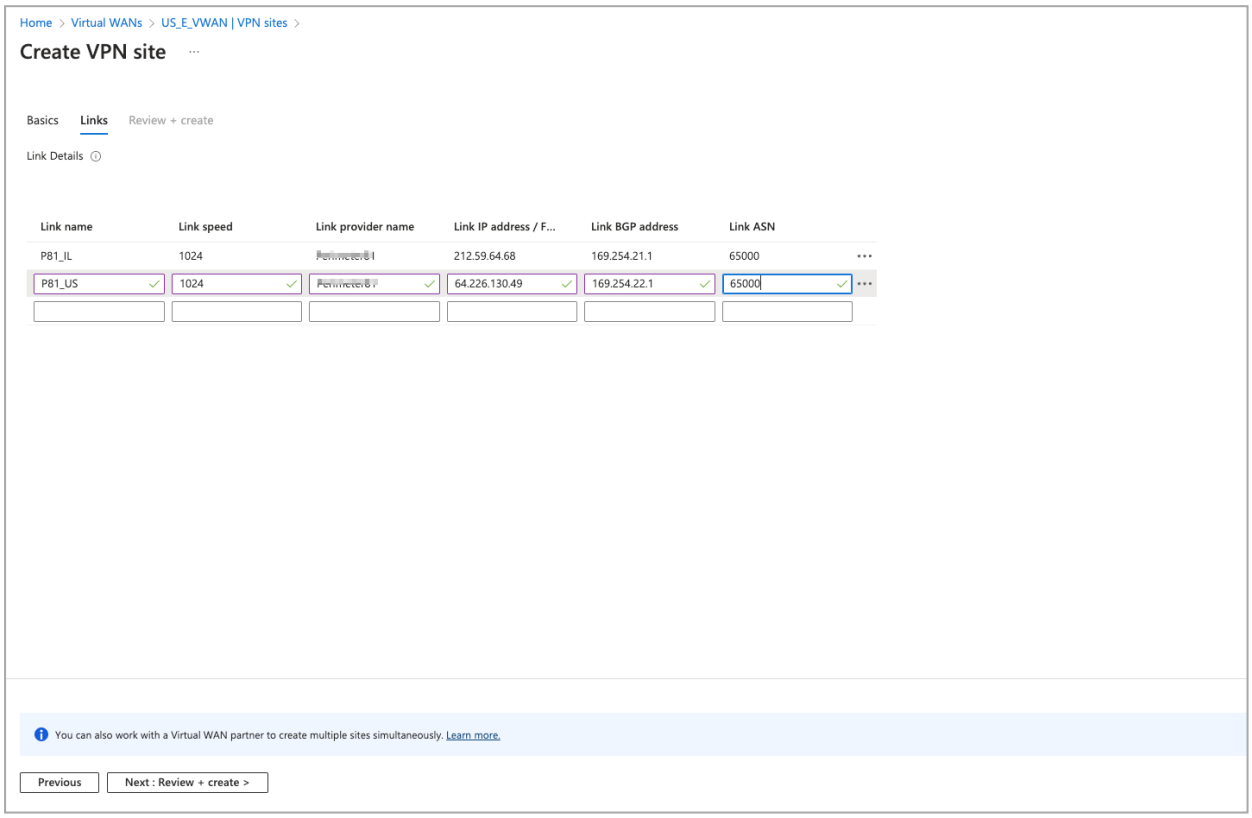


5. Enter these:

Item	Value
Link name	Name of the link that connects to the first Harmony SASE gateway.
Link speed	1024
Link provider name	Harmony SASE
Link IP address	IP address of the first Harmony SASE gateway.

Item	Value
Link BGP address	Any address in the permitted range.
Link ASN	ASN for your Harmony SASE network.

6. Repeat the above step to link the second Harmony SASE gateway.

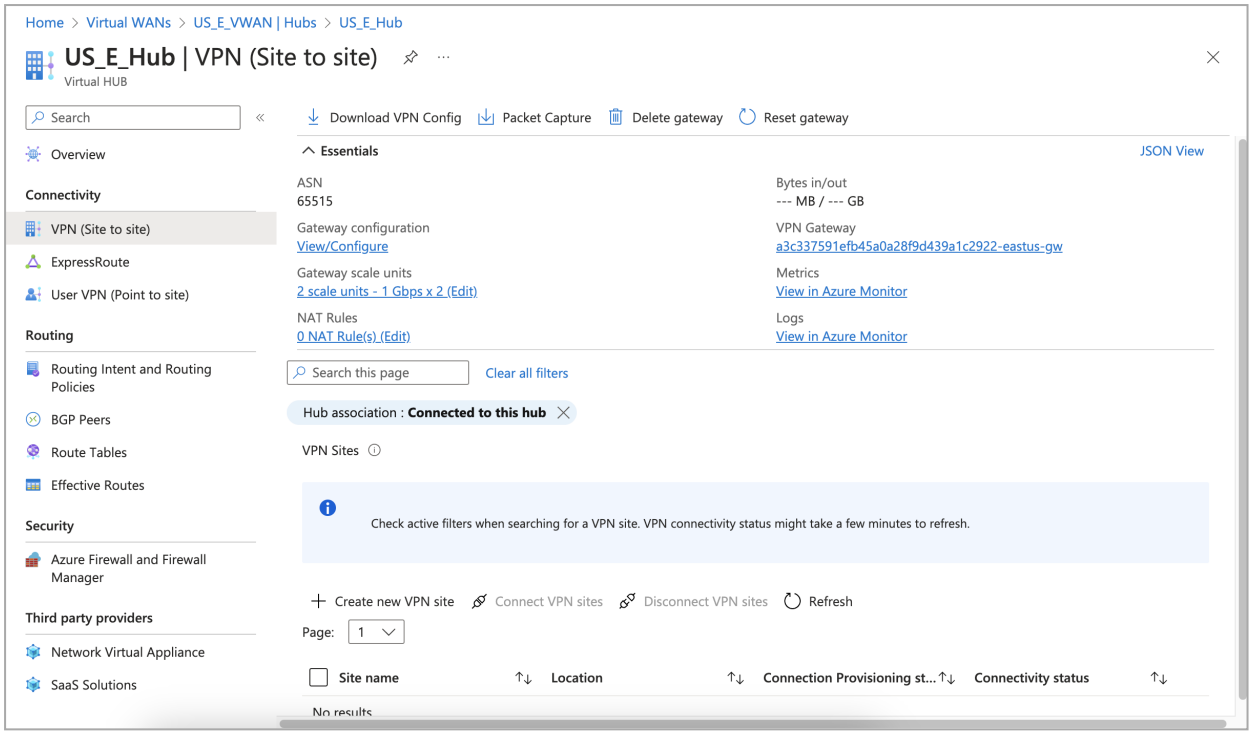


7. Click **Review+create**.
8. Click **Create**.

Connecting the Site to your Virtual Hub

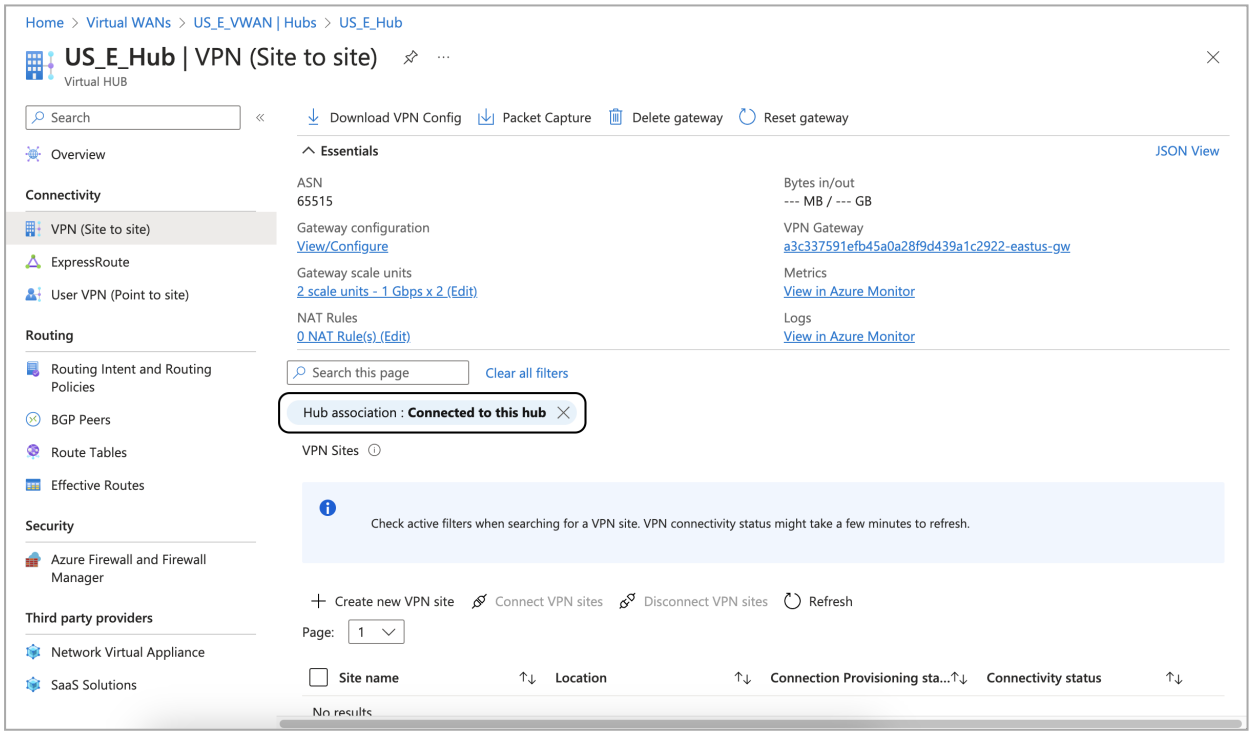
1. Access the Azure Management Portal and go to the Virtual WAN you created, and from the left pane, click **Hubs**.
2. Click the virtual hub you created.

   The **Hub** page appears.
3. From the left pane, in the **Connectivity** section, click **VPN (Site to site)**.

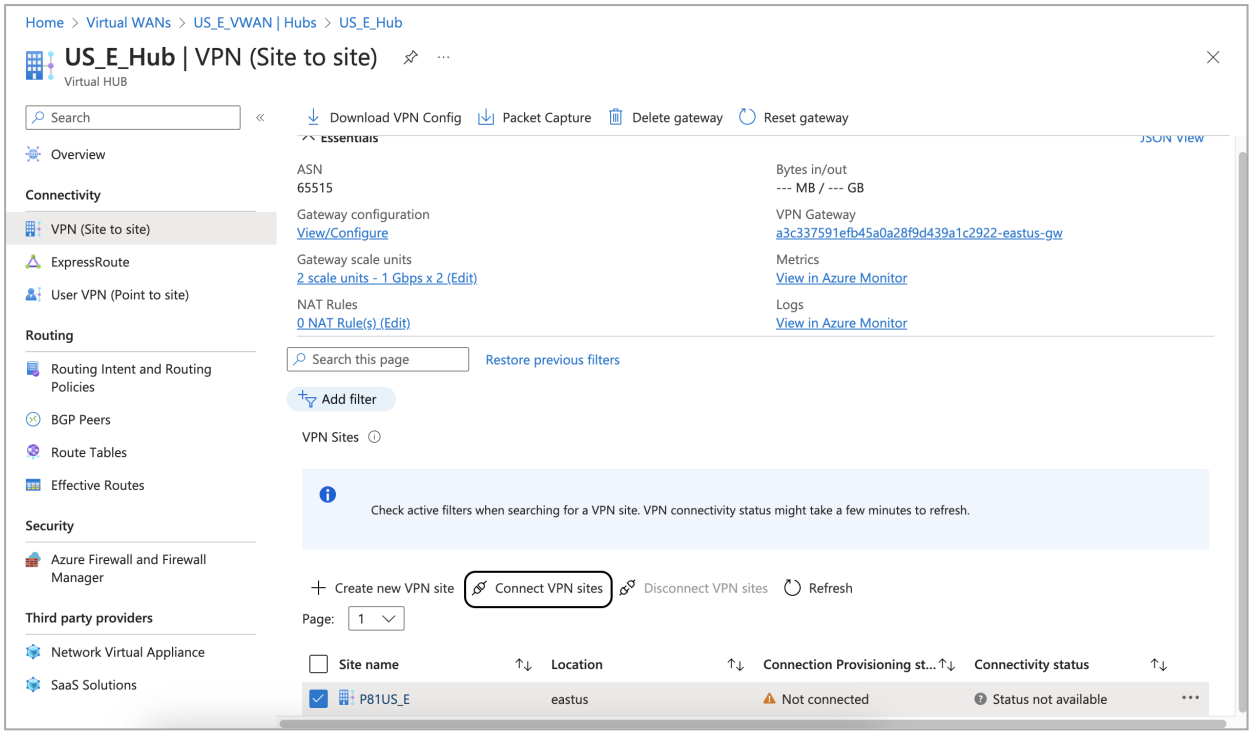


The **VPN (Site to site)** page appears.

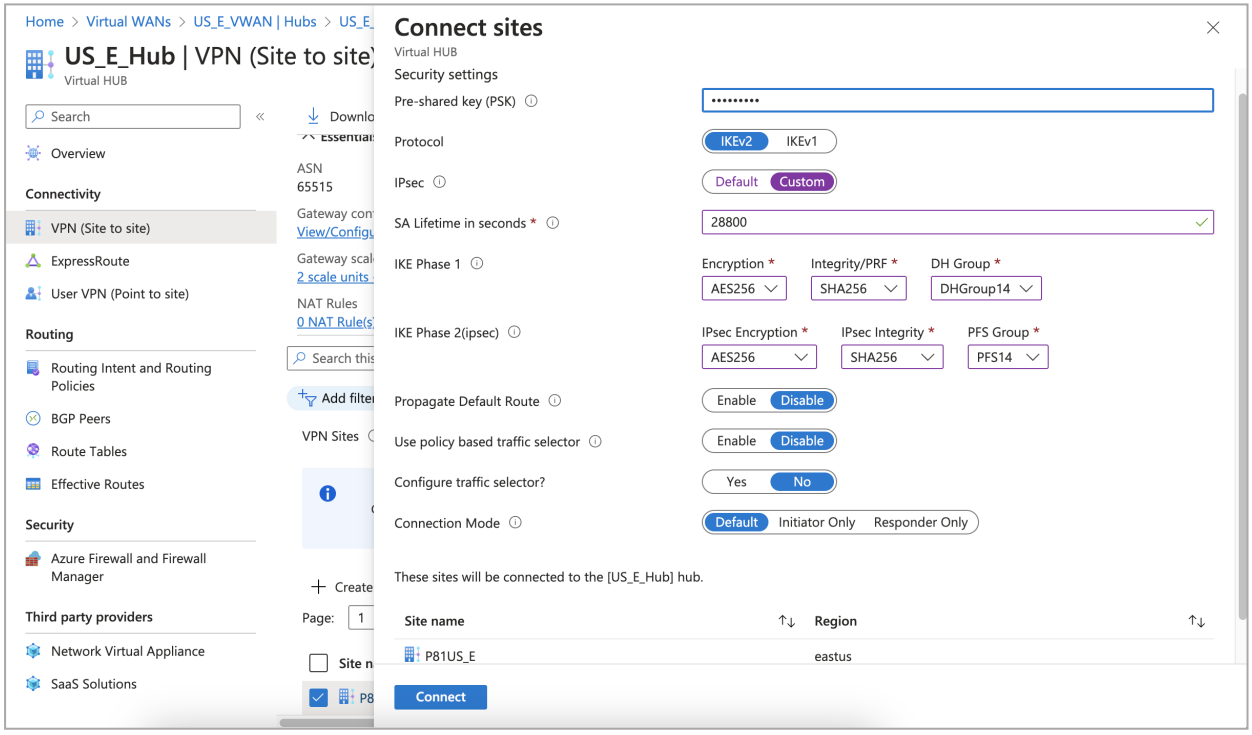
4. Clear the filter to view your site in the list.



5. Select the checkbox next to the created site and click **Connect VPN Sites**.



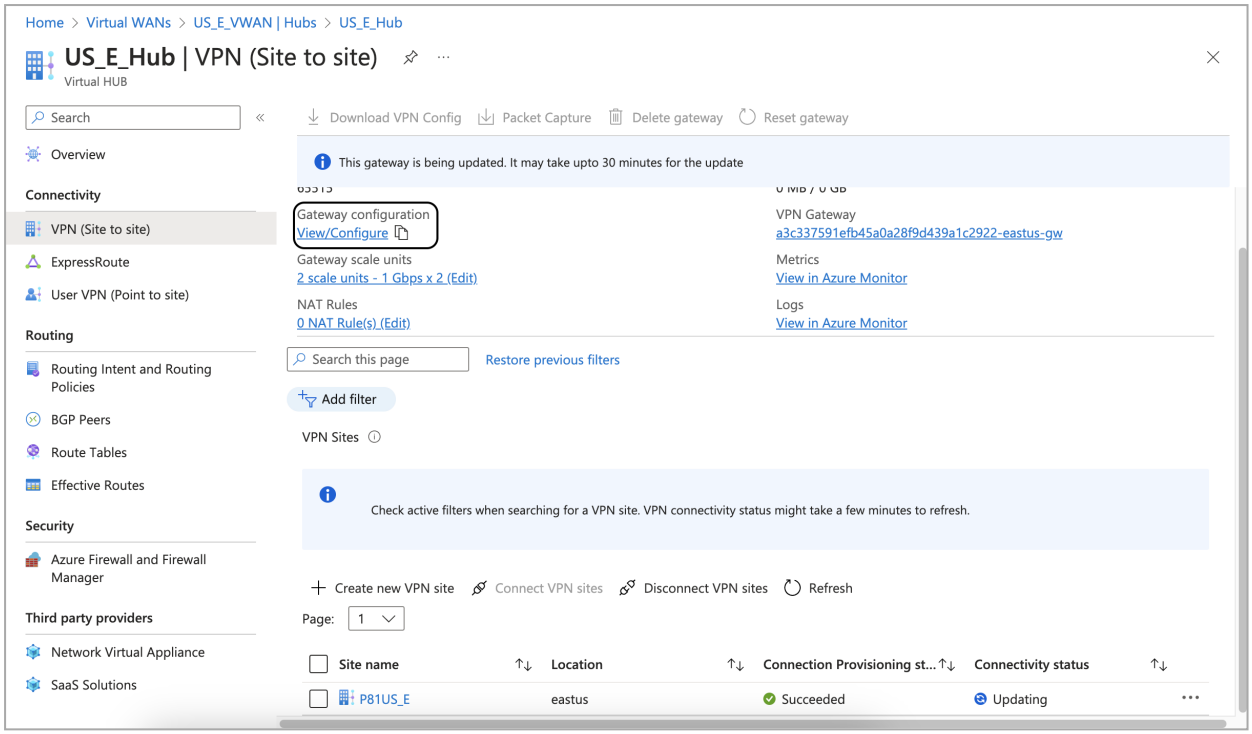
The **Connect sites** window appears.



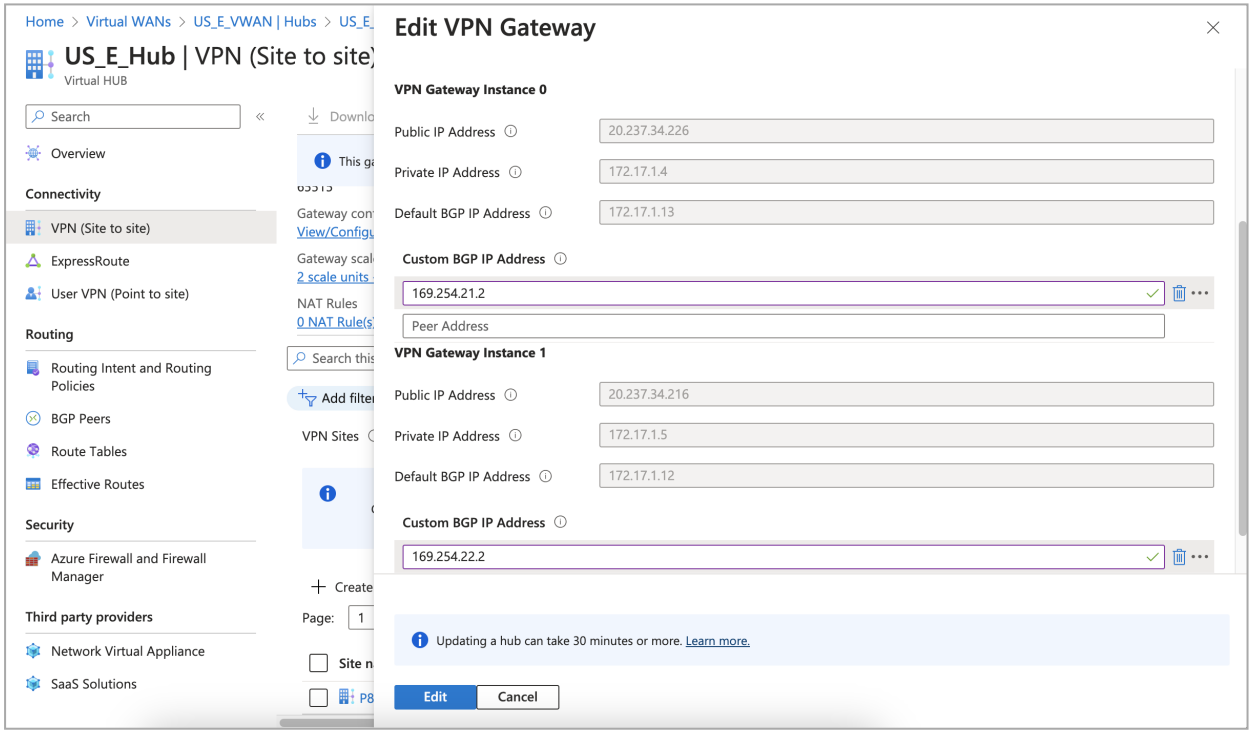
6. Enter these:

Item	Value
Pre-shared key (PSK)	Pre-shared key for this connection.
Protocol	IKEv2
IPsec	Custom
SA Lifetime in seconds	28800
IKE Phase 1	
Encryption	AES256
Integrity/PRF	SHA256
DH Group	DHGroup14
IKE Phase 2(ipsec)	
IPsecEncryption	AES256
IPsec Integrity	SHA256
PFS Group	PFS14
Propagate Default Route	Disable
Use policy based traffic selector	Disable
Configure traffic selector	No
Connection Mode	Default

7. Go to the **VPN (Site to site)** window and click **View/Configure** to configure the gateway.

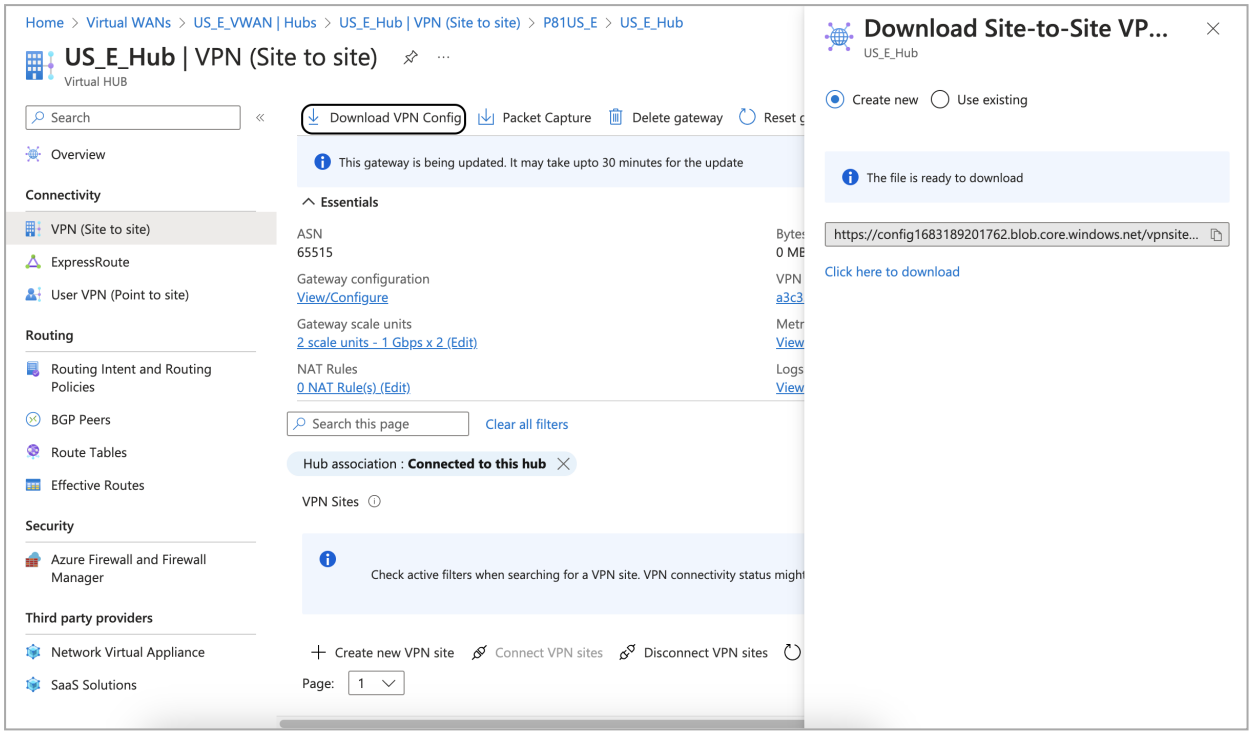


The **Edit VPN Gateway** window appears.



8. In the **VPN Gateway Instance 0** section, set the **Custom BGP IP Address** to the same network range as the BGP address for the first link.
9. In the **VPN Gateway Instance 1** section, set the **Custom BGP IP Address** to the same network range as the BGP address for the second link.
10. Click **Edit** and then **Confirm**.

11. Go to the **VPN (Site to site)** window and click **Download VPN Config** to download the configuration.

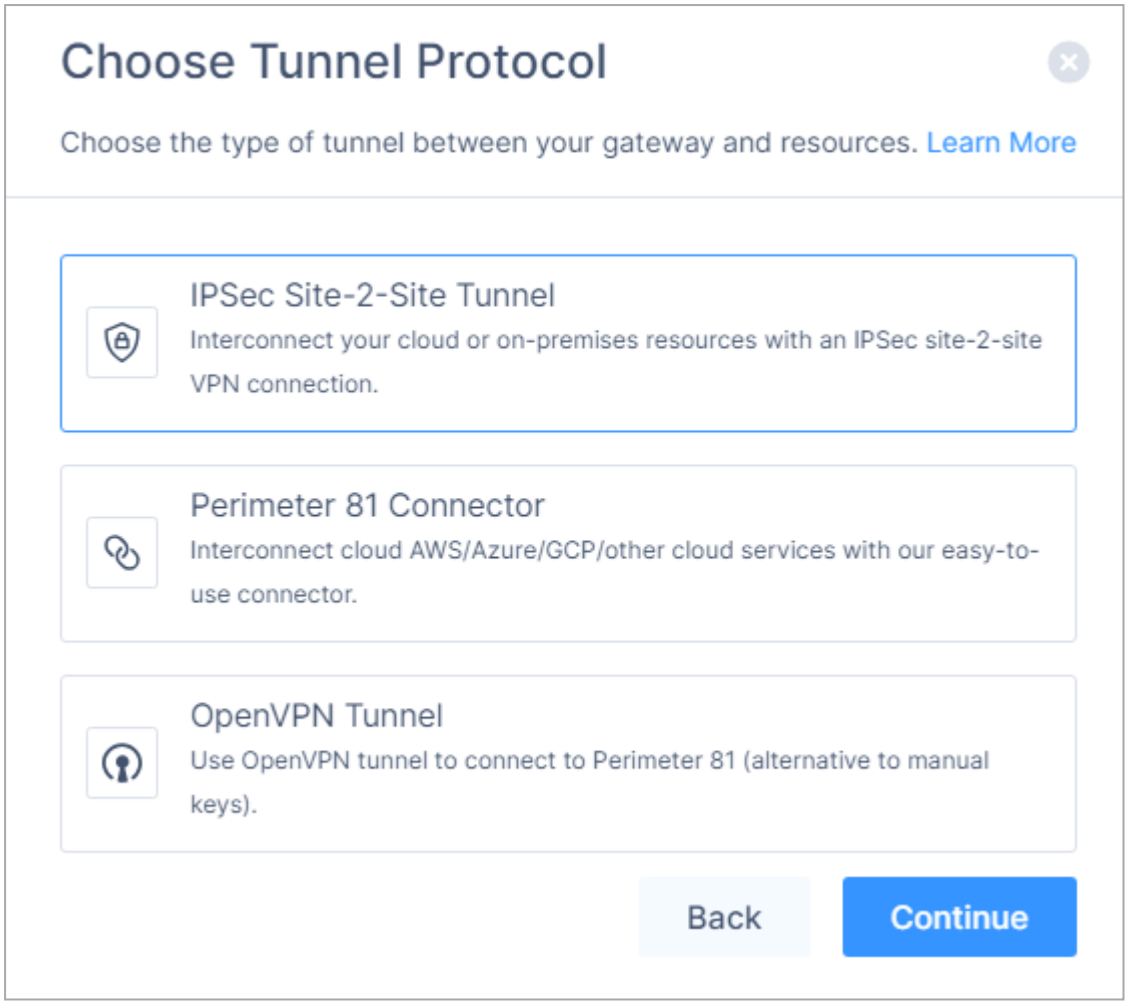


12. Click the download link.

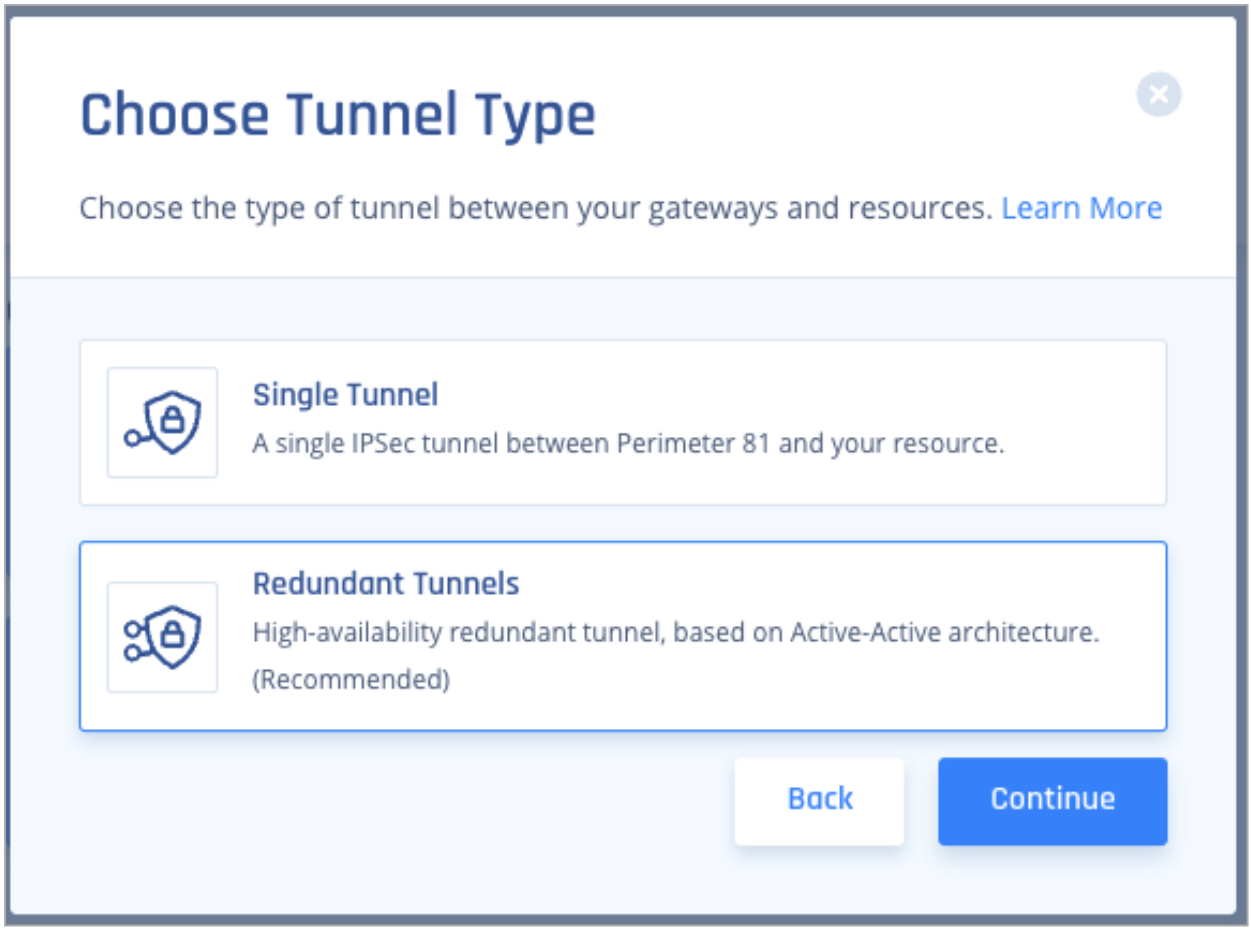
    The system downloads the configuration file.

Step 2 - Creating the Tunnels in the Harmony SASE Administrator Portal

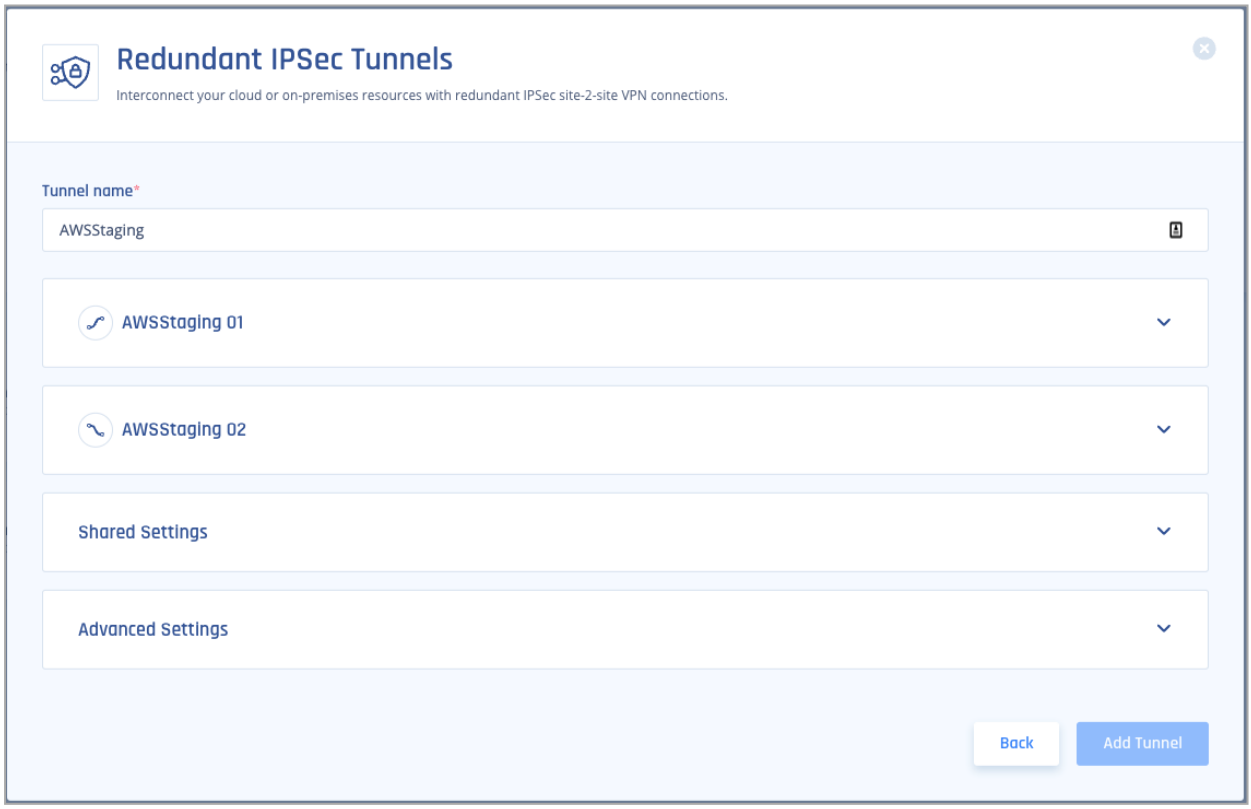
1. Access the Harmony SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



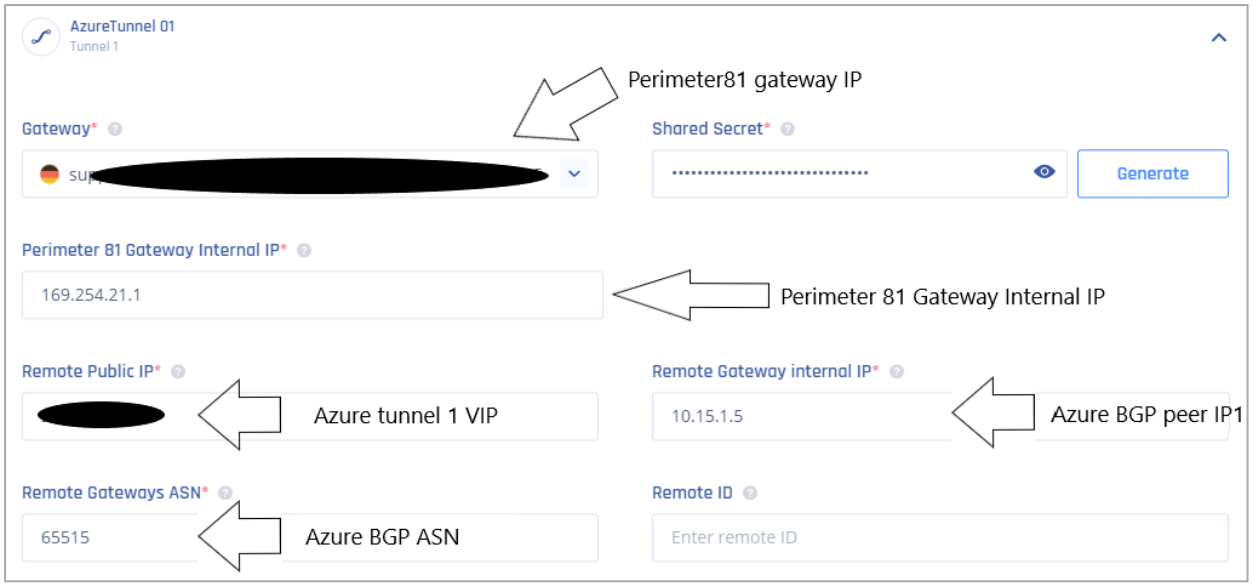
The **Redundant IPSec Tunnels** window appears.



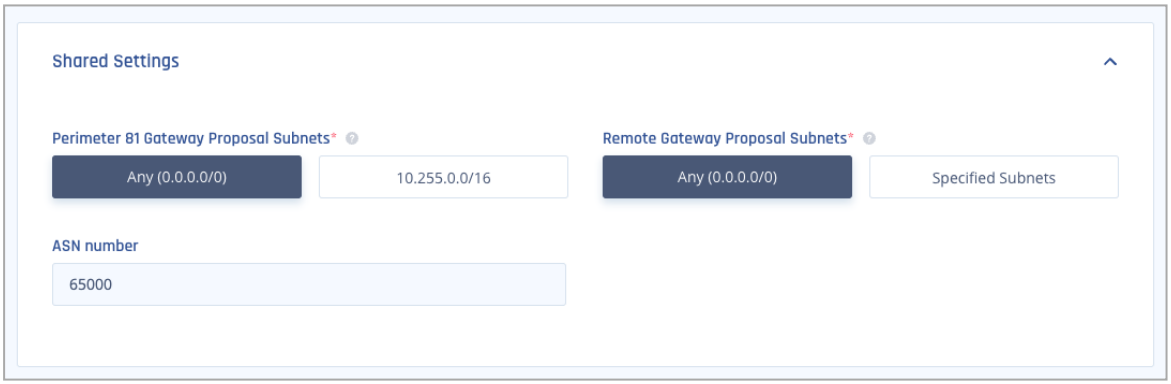
6. Copy the values for the first tunnel from the downloaded configuration file:

Item	Value
Shared Secret	PSK
Harmony SASE gateway Internal IP	Inside IP Addresses of Customer Gateway
Remote Public IP & Remote ID	Public IP Addresses of **VPN Gateway Instance 0**.
Remote Gateway internal IP	BGPPeeringAddress of **VPN Gateway Instance 0**
Remote Gateway ASN	Azure ASN

In the Harmony SASE Administrator Portal, enter the values for Tunnel 1 as:



7. Repeat step 6 for the second tunnel.
8. In the **Shared Settings** section:
   a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.
   b. **ASN** number must be the same for the Harmony SASE side.



9. In the **Advanced Settings** section, enter the information for your tunnel type (unless you have configured customer settings on the Azure side):

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

10. Click **Add Tunnel**.

Google Cloud Platform

This chapter describes the procedure to establish a Site-to-Site IPsec tunnel between your Harmony SASE network and Google Cloud Platform (GCP).

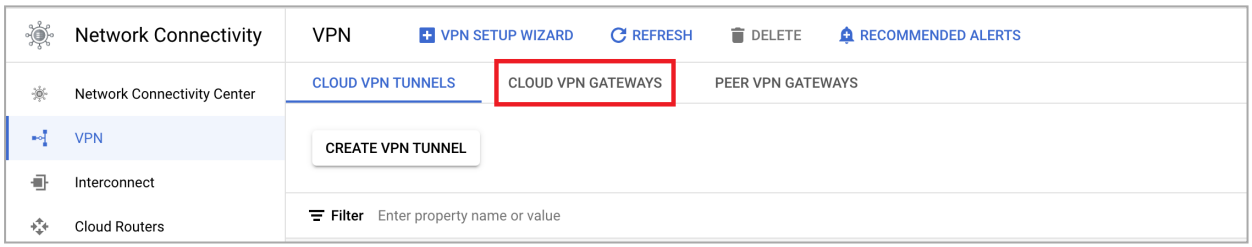
Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

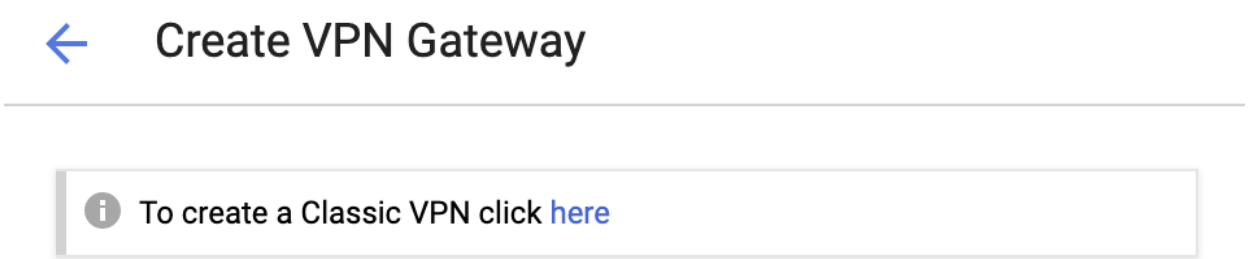
Step 1 - Configurations in the GCP Console

Creating a Virtual Private Gateway

1. Access the GCP console and go to **Network Connectivity**.
2. In the left menu, click **VPN**.
3. Click **Cloud VPN Gateways** > **Create VPN gateway**.

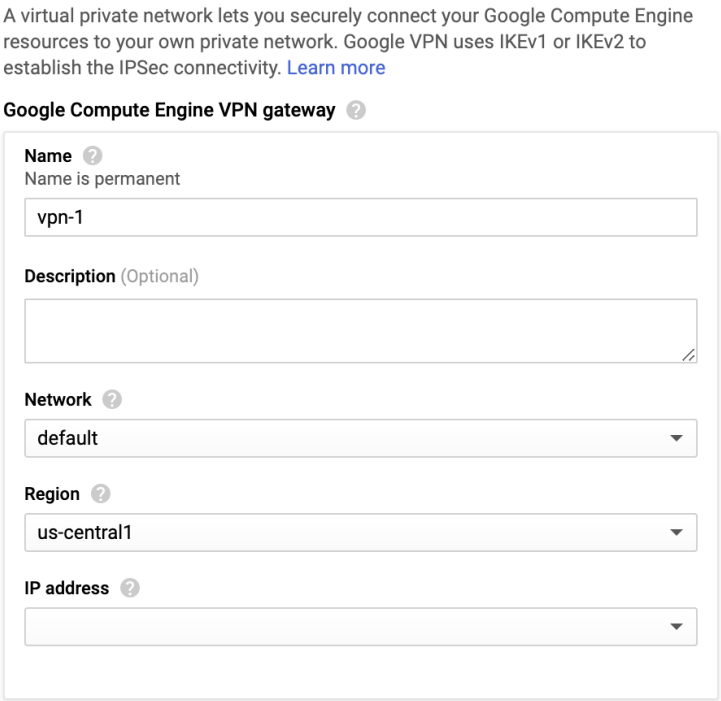


4. Click the link to create Classic VPN.



5. Enter these:
   i. **Name** - Name of the gateway.
   ii. **Network** - Select **default** or a specific VPC.

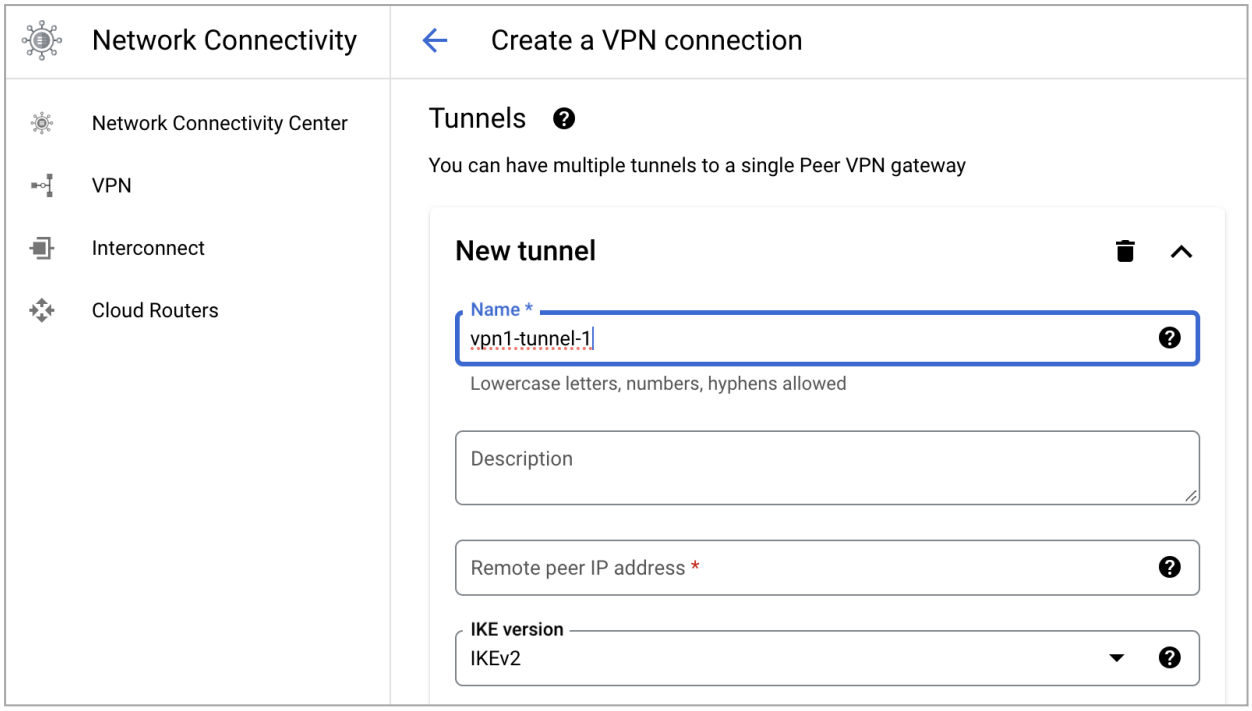
iii. **Region** - Select the region where your resources are located.



iv. **IP address** - Create an IP address to connect your gateway and click **Reserve**.

Creating a Tunnel

1. Access the GCP console and go to **Network Connectivity**.
2. In the left menu, click **VPN**.
3. Click **Cloud VPN Tunnels** > **Create VPN tunnel**.
4. Enter these:



i. **Name** - Name of the tunnel.

ii. **Remote peer IP address** - IP address of your Harmony SASE Gateway.

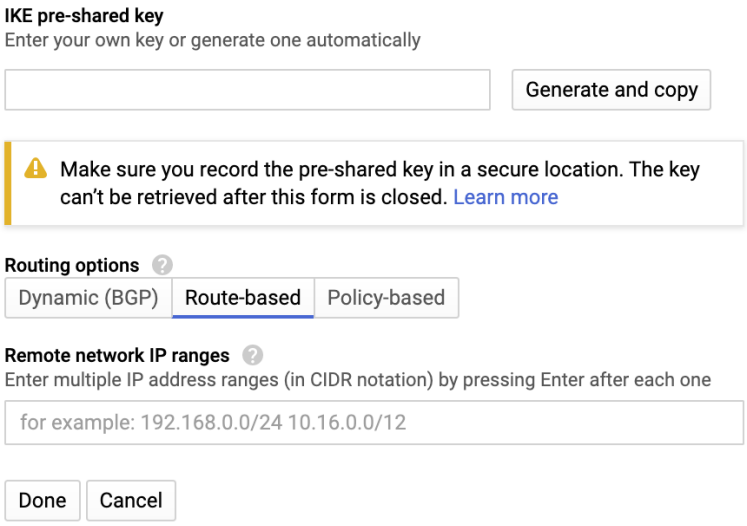
To obtain this, go to the Harmony SASEAdministrator Portal > **Networks** and select the network that contains the gateway to which you wan to create a tunnel.

iii. **IKE Version** - IKEv2

iv. **IKE pre-shared key** - Click **Generate and copy** or select a key of your own and note it down.

v. **Routing options** - Route-based

vi. **Remote network IP ranges** - 10.255.0.0/16 (unless customized)



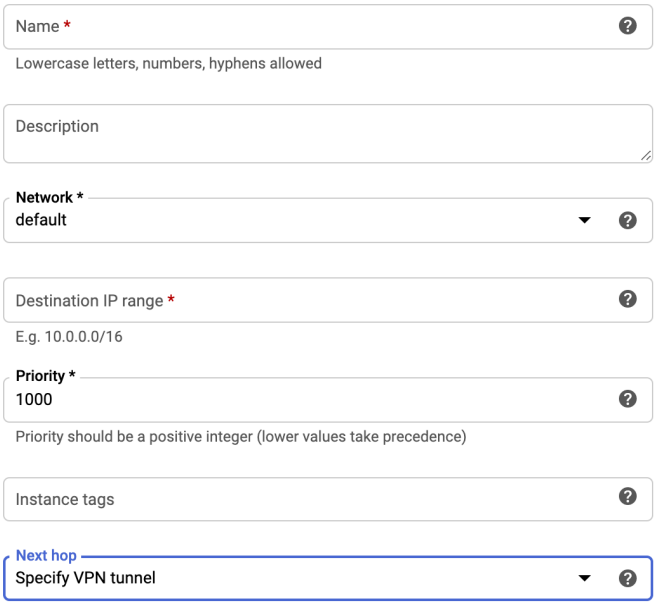
5. Click **Done** and then **Create**.

Configuring the Routing Rules to the VPC Network

1. Access the GCP console and go to the **VPC Network** section.
2. In the left menu, click **Routes**.

3. Click **Create Route Rule**.
4. Enter these:
   a. **Name** - Name of the VPN gateway.
   b. **Network** - Select the VPC network that contains the instances served by the VPN gateway. This must be the same network selected in the previous steps.
   c. **Destination IP range** - 10.255.0.0/16 (or customized)
   d. **Priority** - 1000
   e. **Next hop** - Select **Specify VPN Tunnel**.

f. **Next hop VPN tunnel** - Select the VPN tunnel you created in the previous steps.



5. Click **Create**.

Allowing Incoming Connections from Harmony SASE Local Network Using Firewall Rules

1. Access the GCP console and go to the **VPC Network** section.
2. In the left menu, click **Firewall rules**.

3. Click **Create Firewall Rule**.

Name
Name is permanent

lowercase, no spaces

Description (Optional)

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Stackdriver. Learn more

On
Off

Network

default

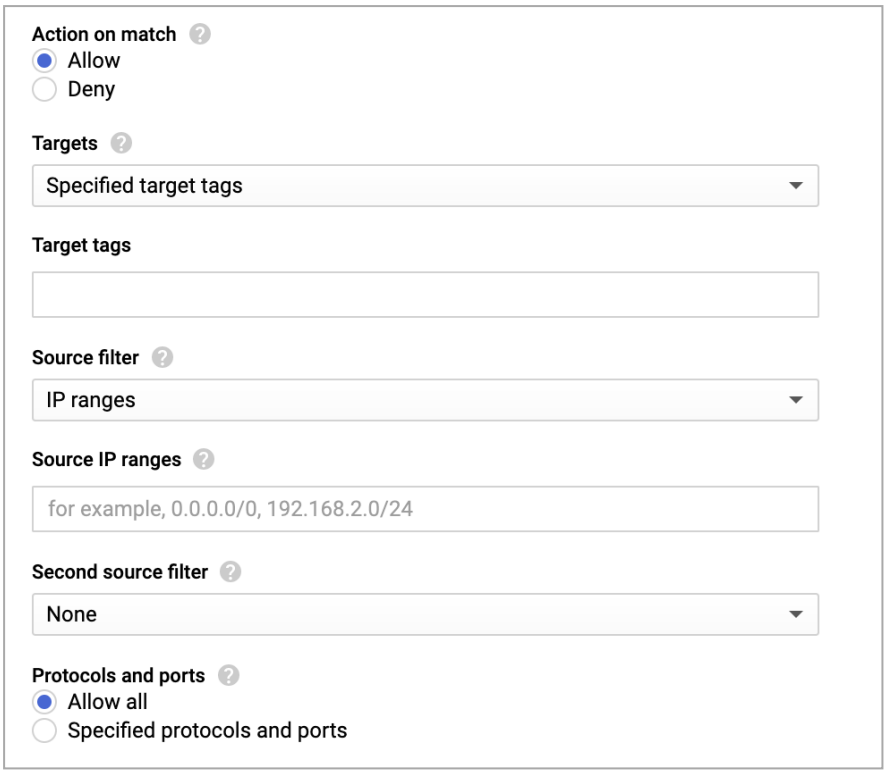
Priority
Priority can be 0 - 65535 Check priority of other firewall rules

1000

Direction of traffic
Ingress
Egress

4. Enter these:
   a. **Name** - Name of the rule.
   b. **Logs** - Off
   c. **Network** - Select the VPC network that contains the instances served by the VPN gateway. This must be the same network selected in the previous steps.
   d. **Priority** - 1000
   e. **Direction of traffic** - Ingress.

f. **Action on match** - Allow



g. (Optional) **Target tags**

h. **Source filter** - IP ranges

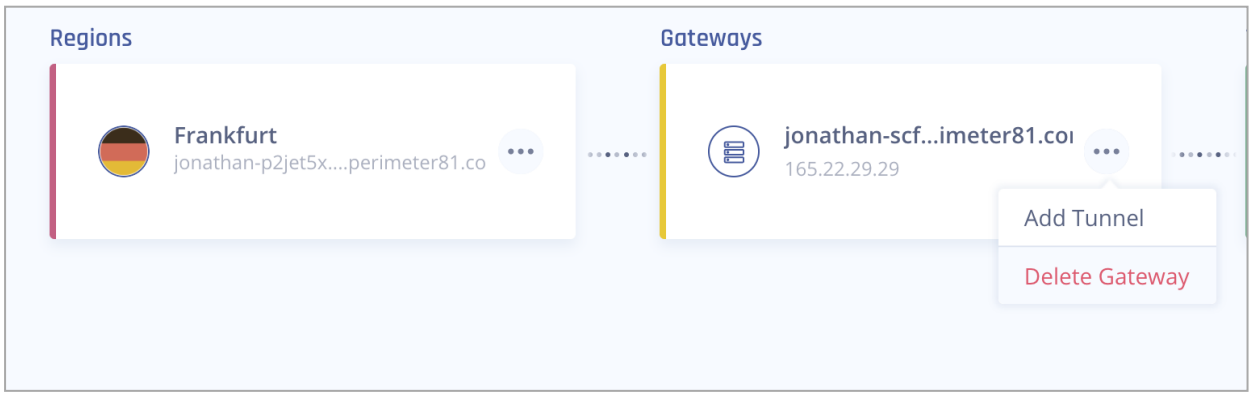
i. **Source IP ranges** - 10.255.0.0/16 (unless customized)

j. **Second source filter** - None

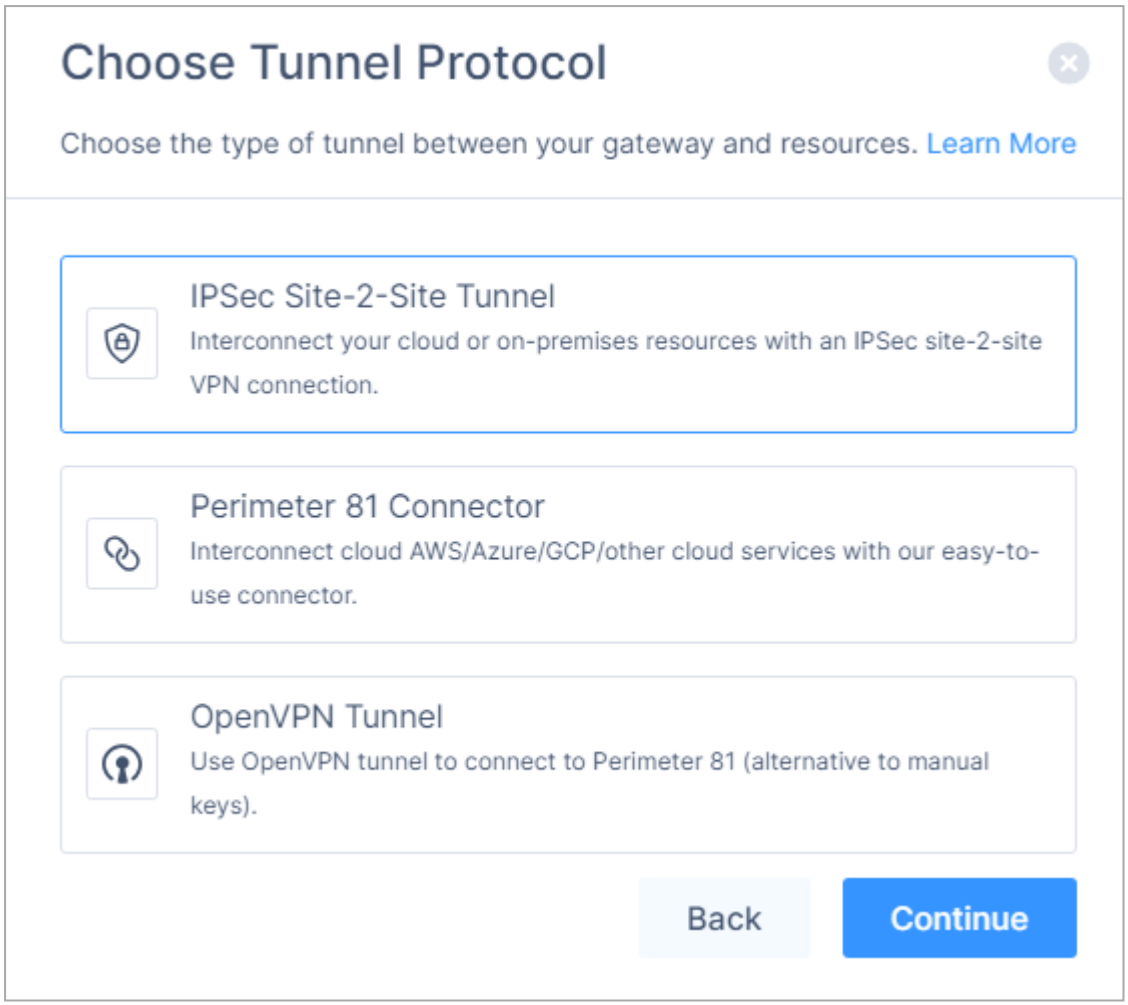
k. **Protocols and ports** - Allow all

Step 2 - Creating the Tunnel in the Harmony SASE Administrator Portal

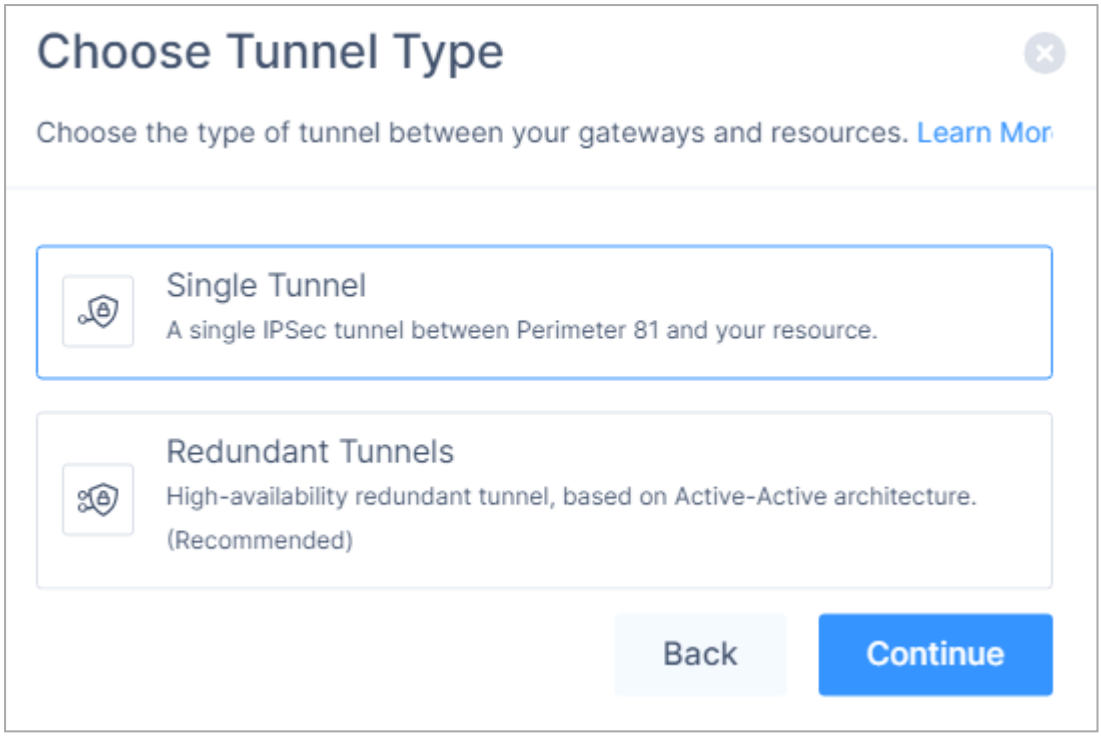
1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.



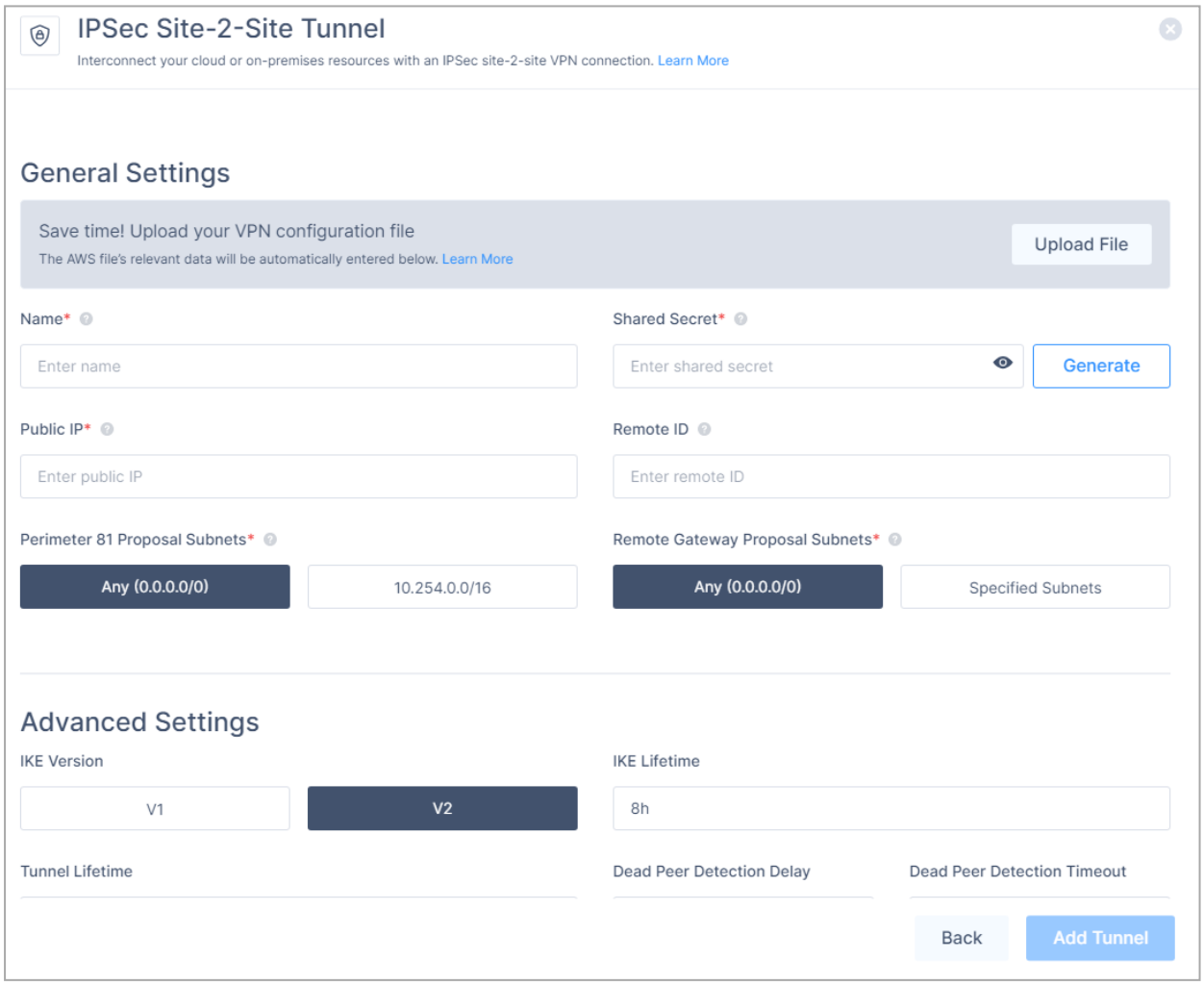
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



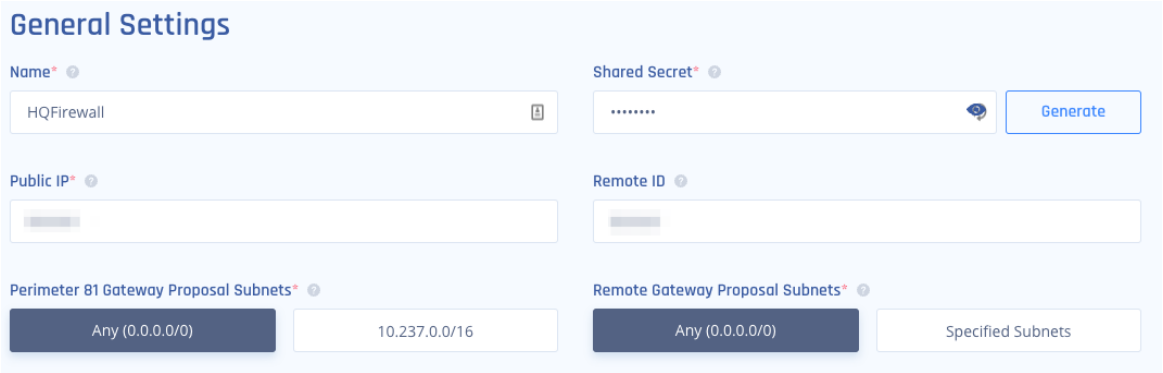
5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, enter these:
   a. **Name** - Name of the tunnel.
   b. **Harmony SASE Gateway Proposal Subnets** - Any (0.0.0.0/0)
   c. **Remote Gateway Proposal Subnets** - Any (0.0.0.0/0)



7. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

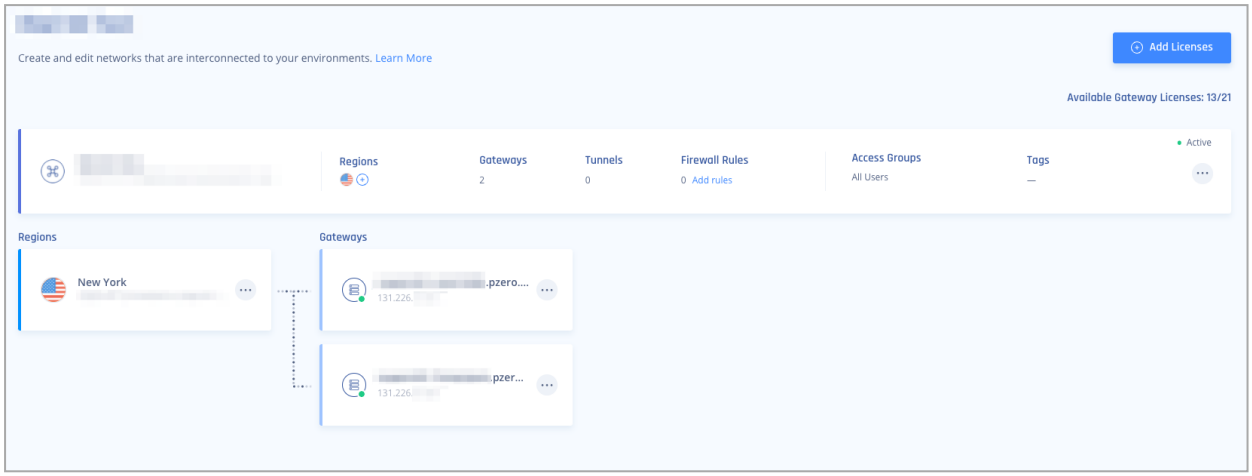
8. Click **Add Tunnel**.

Google Cloud Platform (GCP) Redundant Tunnels

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

- Your Harmony SASE network must have at least two different gateways in the same network.



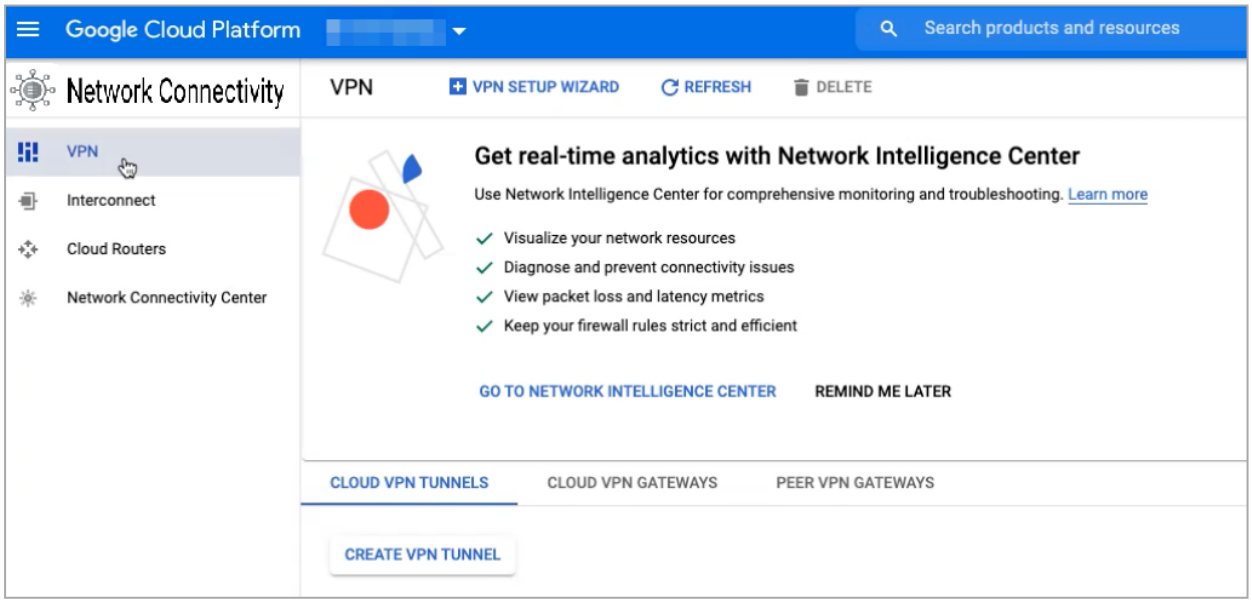
Notes -

- You can deploy the gateways in two separate regions for comprehensive ISP redundancy.
- You can scale up the network. Adding another region does not affect the connection.

Step 1 - Configurations in the GCP Console

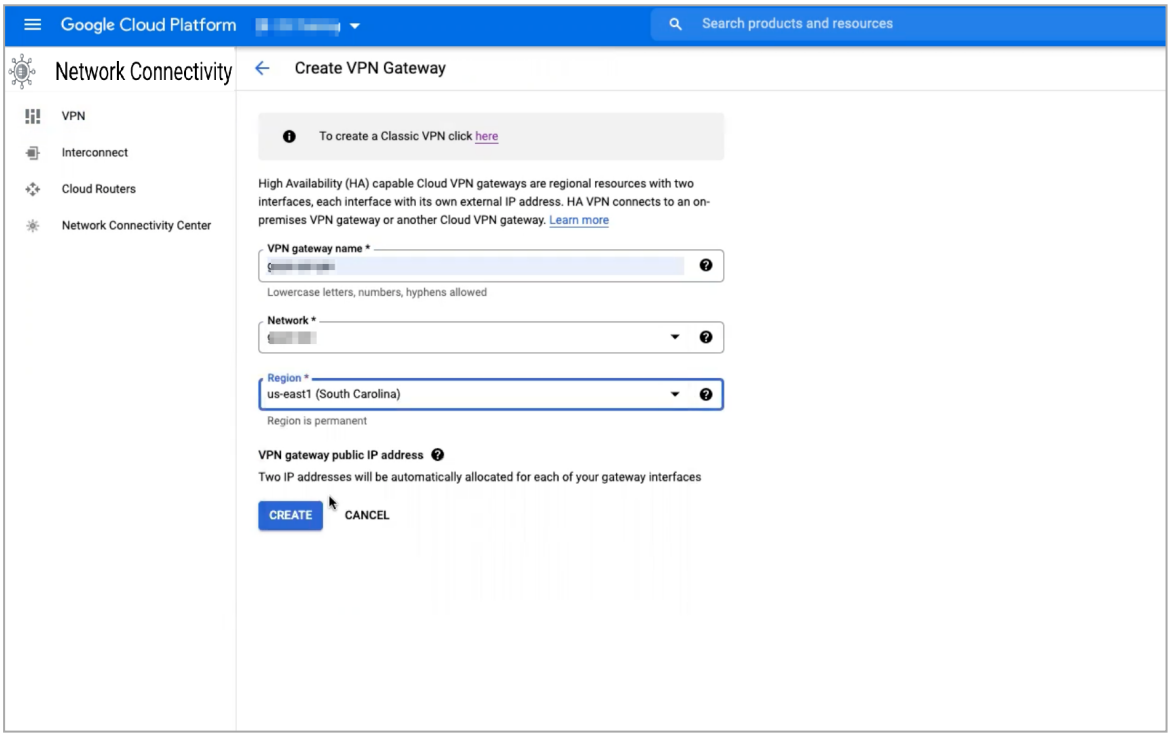
Creating a VPN Gateway

1. Access the GCP console and in the **Network Connectivity** section, click **VPN**.



2. Click **Cloud VPN Gateways** > **Create VPN Gateway**.

3. Enter these:
   a. **Name** - Name of the gateway.
   b. **Network** - GCP network you want to access through Harmony SASE.
   c. **Region** - Region where your resources are located.

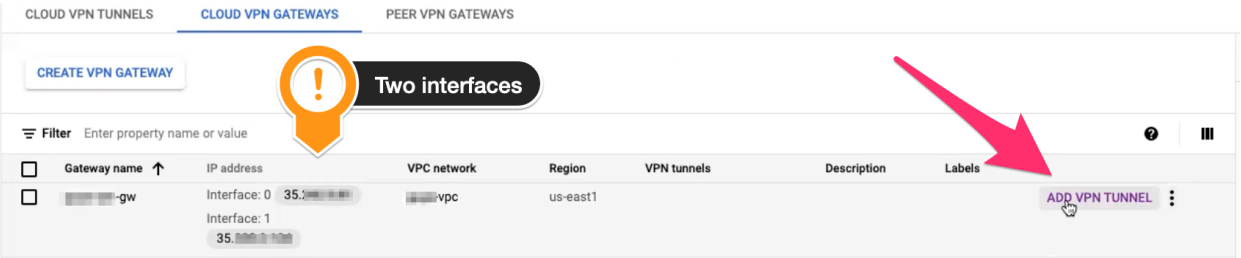


4. Click **Create**.

   The system creates two interfaces, **Interface 0** and **Interface 1**.

Adding a Redundant VPN Tunnel

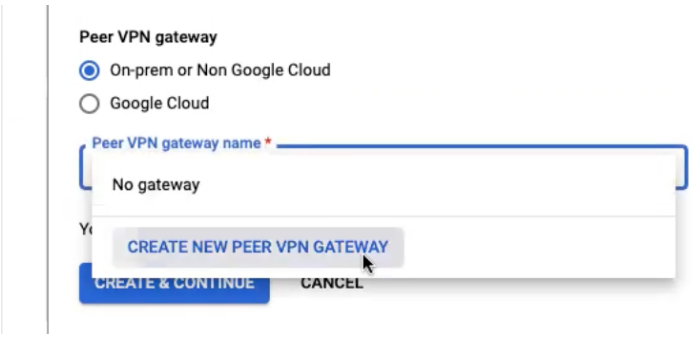
1. Access the GCP console and go to the VPN gateway you created and click **Add VPN Tunnel**.



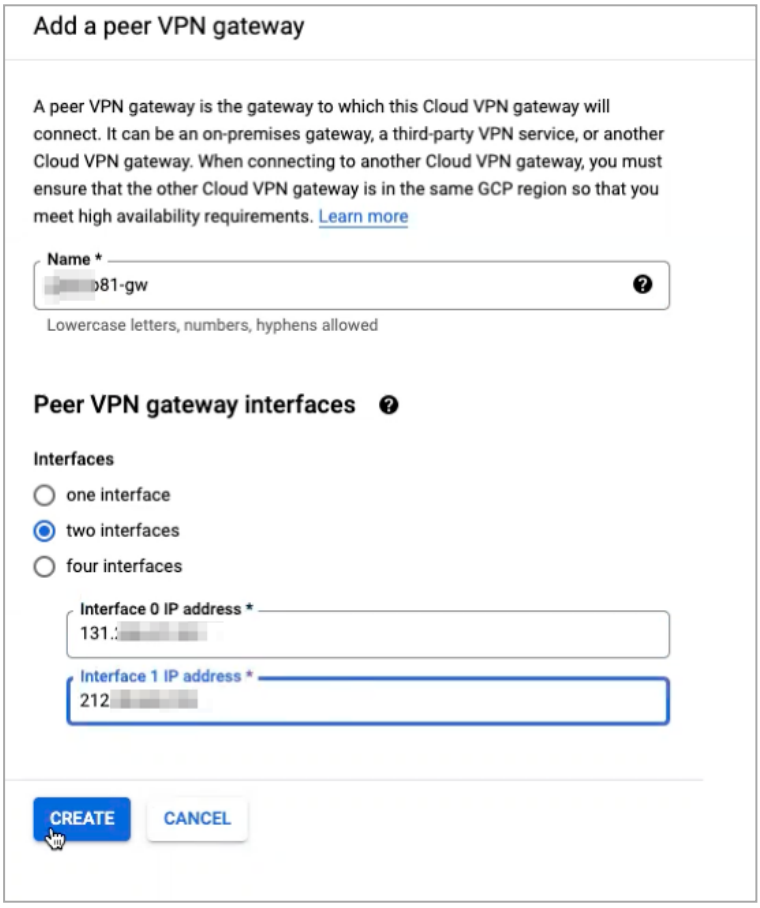
2. Enter these:

a. **Peer VPN gateway** - On-prem or Non-Google Cloud.

b. Click the drop-down menu in **Peer VPN gateway name** and select **Create new peer VPN gateway**.



The **Add a peer VPN gateway** window appears.



c. In the **Name** field, enter the name of the peer VPN gateway that represents the setup at the Harmony SASE side.

d. In the **Peer VPN gateway interfaces** section, select **two interfaces**.

e. In the**Interface 0 IP address** field, enter the IP address of the first Harmony SASE gateway.

f. In the**Interface 1 IP address** field, enter the IP address of the second Harmony SASE gateway.

g. Click **Create**.

h. In the **High availability** section, select **Create a pair of VPN tunnels**.

i. In the **Routing options** section, click the **Cloud Router** drop-down menu, and select **Create a new router**.

   The Cloud router in GCP manages your BGP ASN routes.

   I. Name your Cloud router.

   II. Set **Google ASN** to 65111 (This can be any value. Note this value as it is required to configure the tunnel in the Harmony SASE Administrator Portal).

      Following steps are optional. Perform them only if you have a peered VPC to reach through the tunnel:

      i. In **Advertised routes**, select **Create custom routes**.

      ii. Select Advertise all subnets visible to the Cloud Router.

      iii. In **Custom ranges**, click **Add Custom Route**.

      iv. In **New custom route**, enter the network CIDR for the peered VPC and click **Done**.

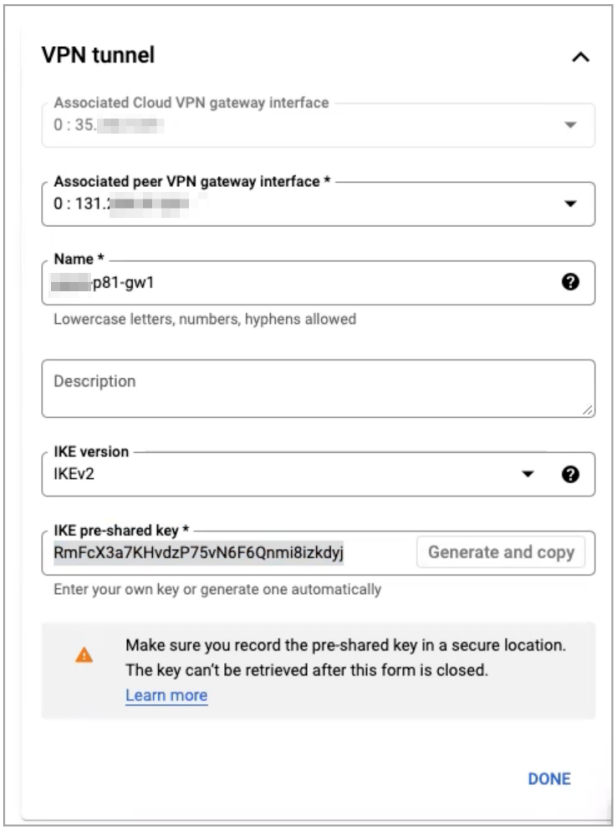
      v. Repeat the last two steps for each range you need to route through the tunnel.

   III. Click **Create**.

j. In the **VPN tunnel** section, select the first VPN tunnel and name it according to the gateway you created in Harmony SASE.

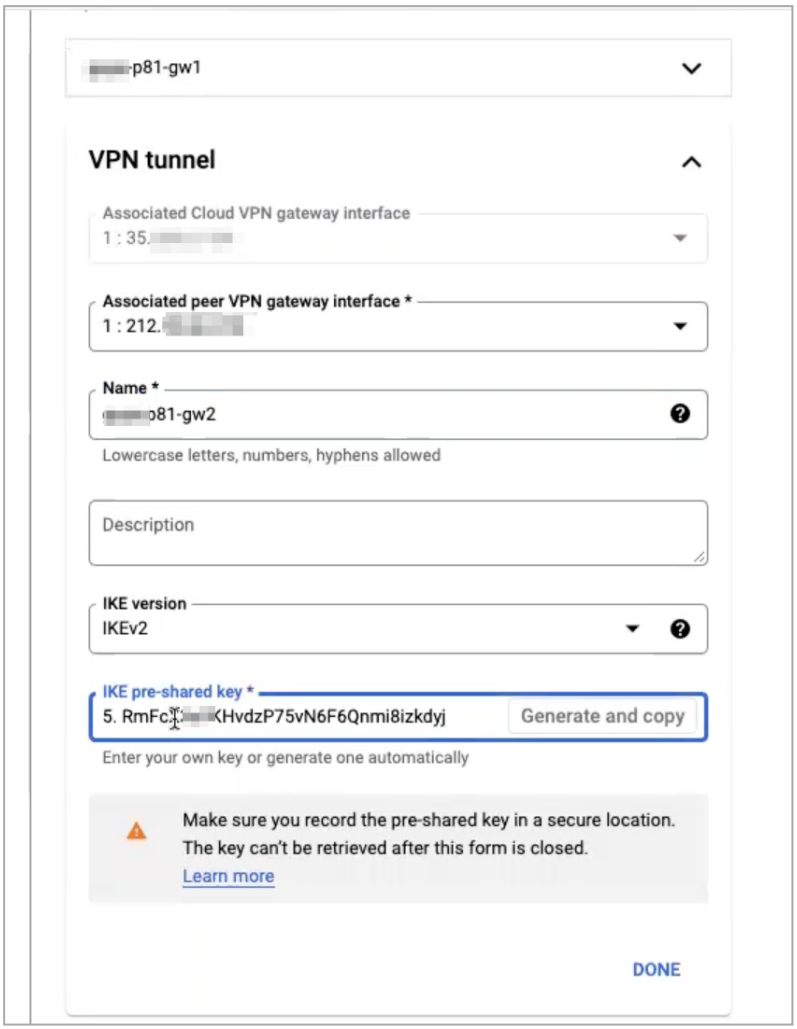
   i. In the **IKE pre-shared key** field, click **Generate and copy**.

   Special characters except dot (.) and underscore (_) are not allowed.



k. Select the second VPN tunnel and name it according to the gateway you created in Harmony SASE.

   i. In the **IKE pre-shared key** field, paste the IKE pre-shared key you copied in the previous step.



   Note - This IKE Pre-shared key is used later to establish a handshake between the sites.

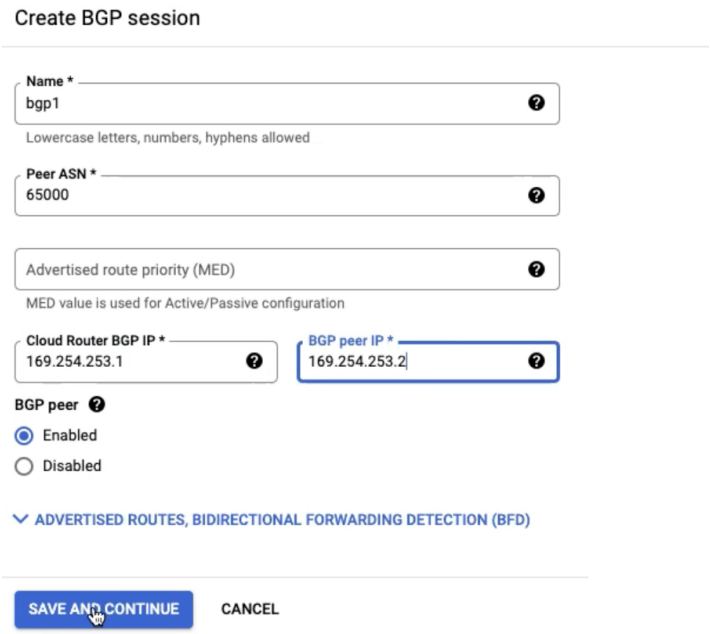
   ii. Click **Done**.

l. Click **Create and continue**.

Configuring Border Gateway Protocol (BGP) Routes

1. Access the GCP console and go to the tunnel where you want to configure the route and click **Configure**.

2. For Tunnel 1, set the BGP routes according to this image.

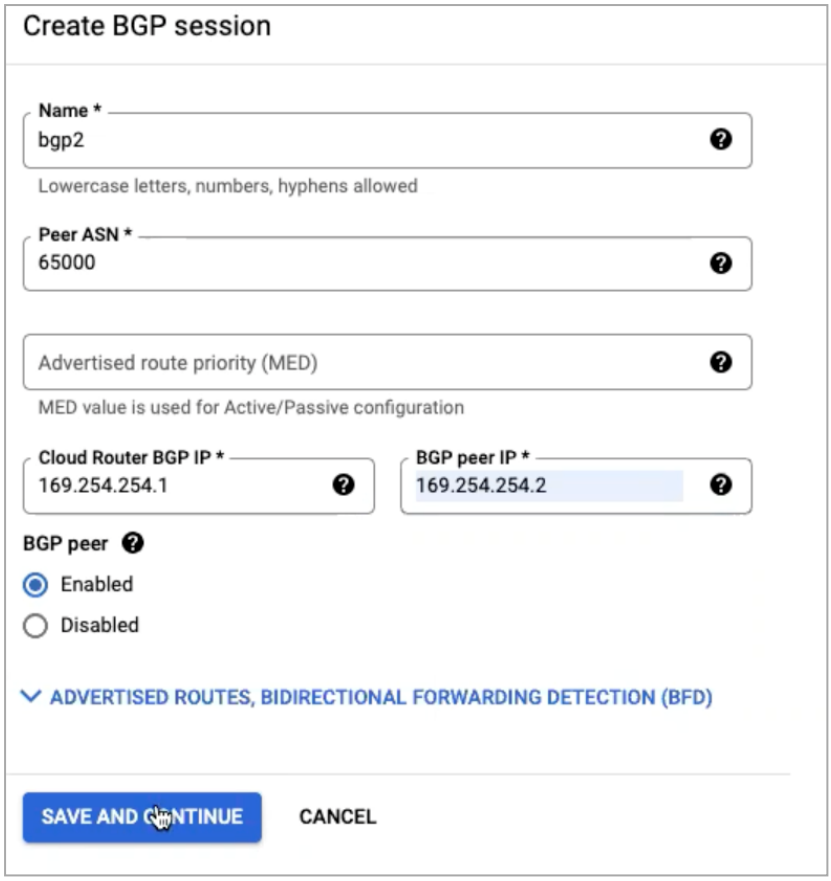


   a. In the **Peer ASN** field, set the value as 65000. It represents the BGP route for Harmony SASE.

   b. For **Cloud Router BGP IP** and **BGP peer IP** fields, select a unique Link-local address.

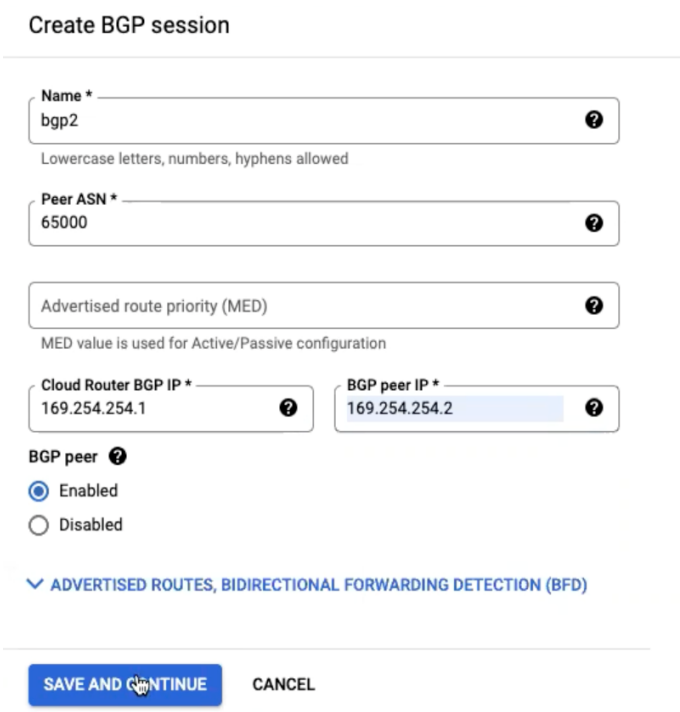
3. Click **Save and Continue**.

4. For Tunnel 2, set the BGP routes according to this image.

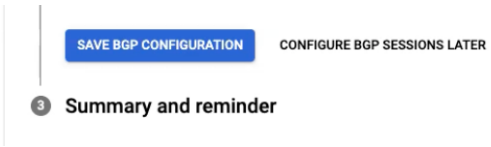


a. In the **Peer ASN** field, set the value as 65000. It represents the BGP route for Harmony SASE.

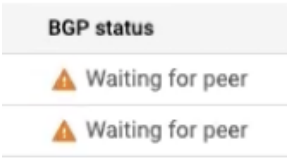
b. For **Cloud Router BGP IP** and **BGP peer IP** fields, select a unique Link-local address.



5. Click **Save and Continue**.
6. Click **Save BGP Configuration**.



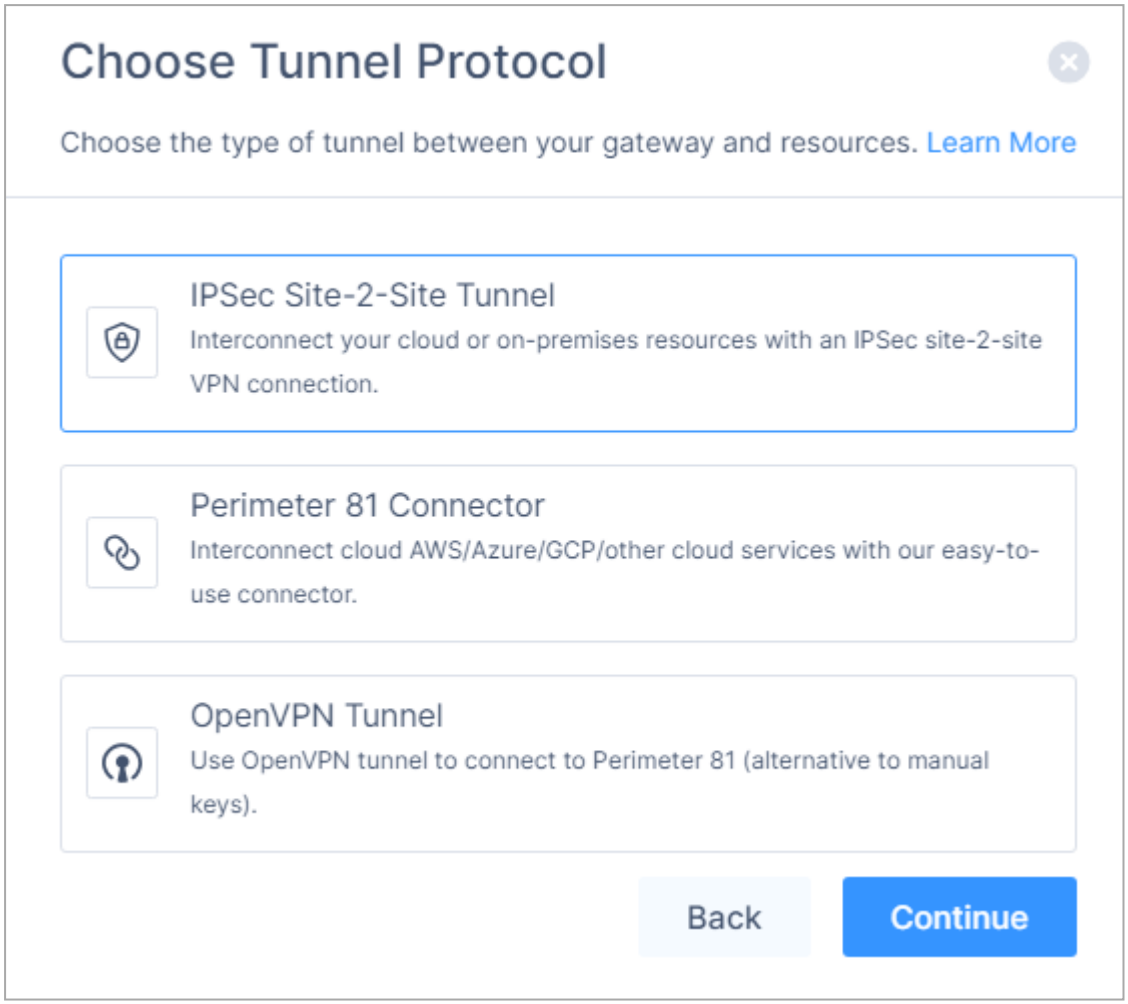
When the tunnel setup is complete, the **BGP status** is displayed as **Waiting for peer** until the tunnels are setup in Harmony SASE.



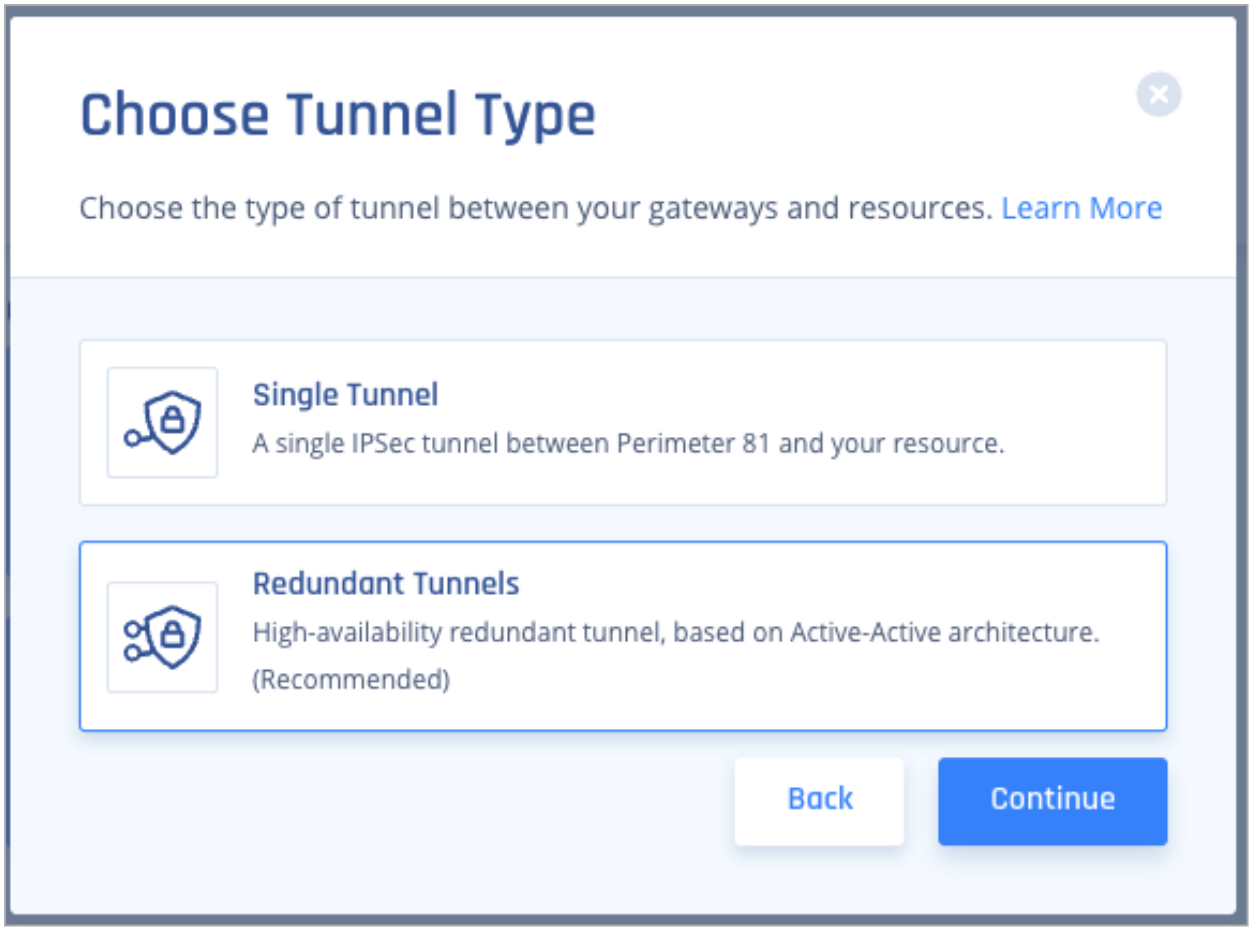
Step 2 - Creating the Tunnels in the Harmony SASE Administrator Portal

1. Access the Harmony SASEAdministrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.

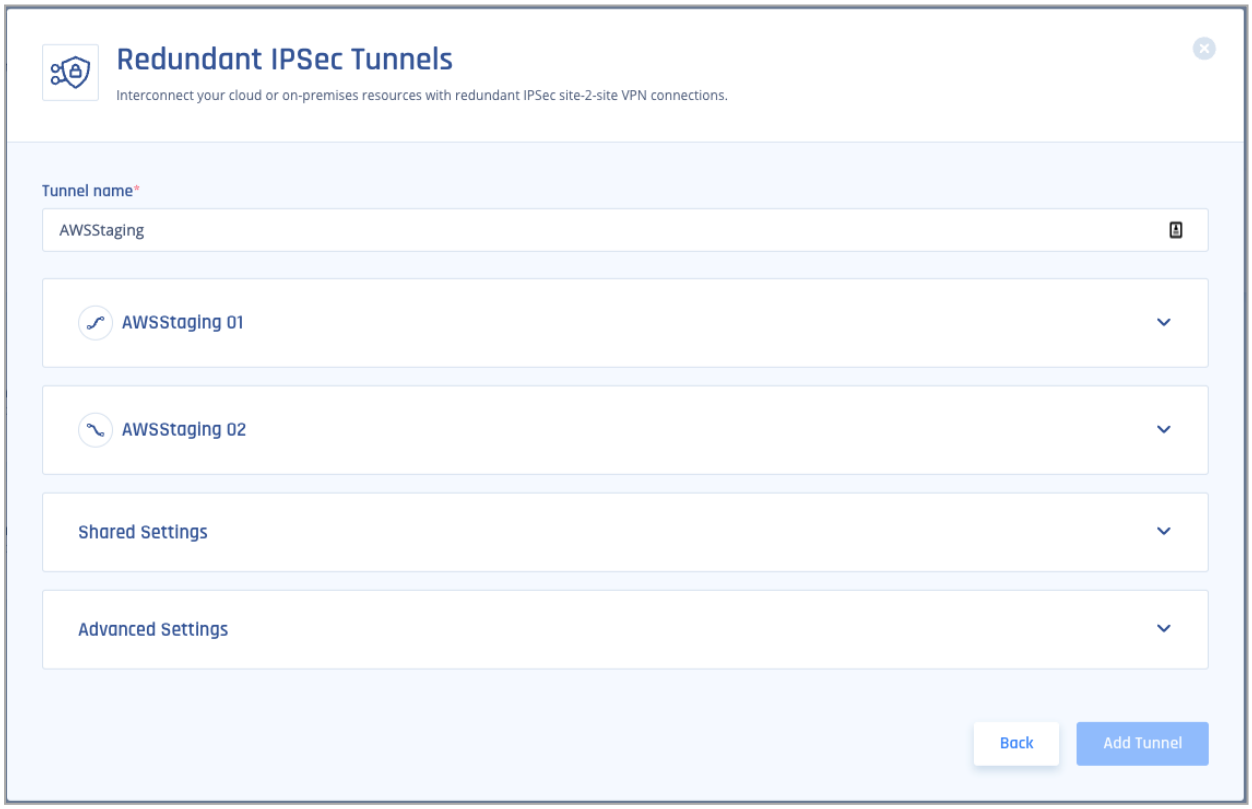
3. In one of the gateways, click ··· > **Add Tunnel**.
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Select **Redundant Tunnels** and click **Continue**.



The **Redundant IPSec Tunnels** window appears.

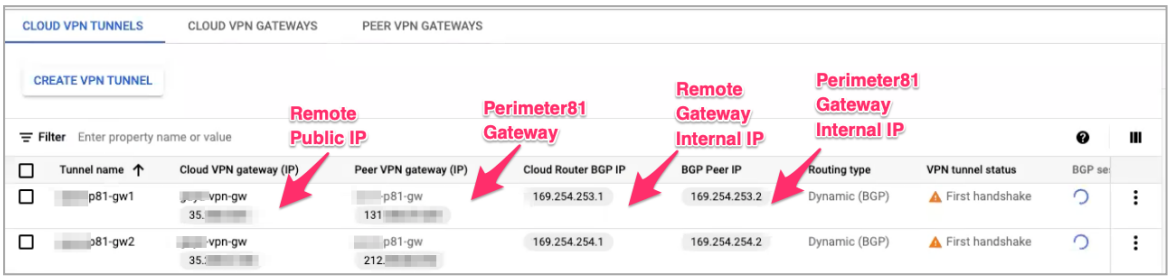


6. In the **General Settings** section:

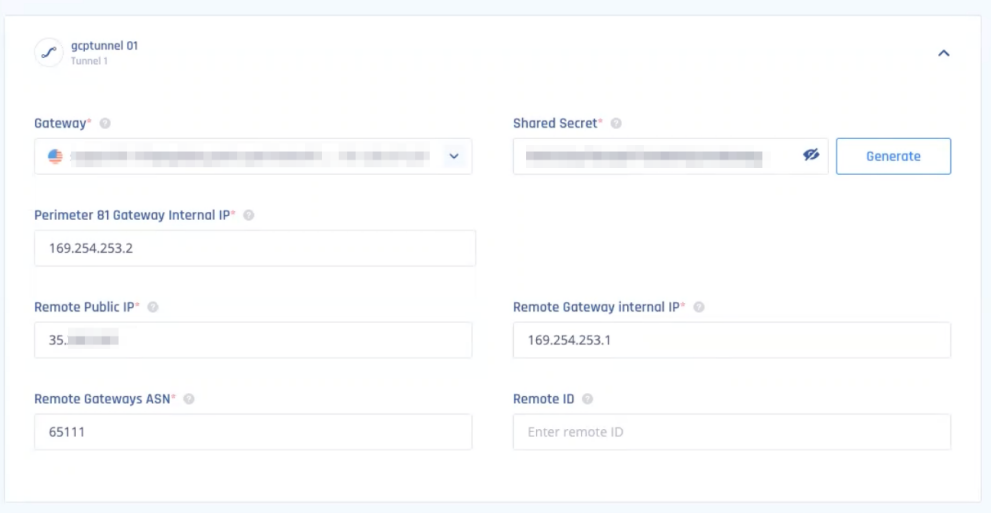
   a. In the **Name** field, enter a name for your tunnel.

   b. In your GCP console, in **Network Connectivity** > **VPN**, copy and paste the values for Tunnel 1 and Tunnel 2 according to the image below.

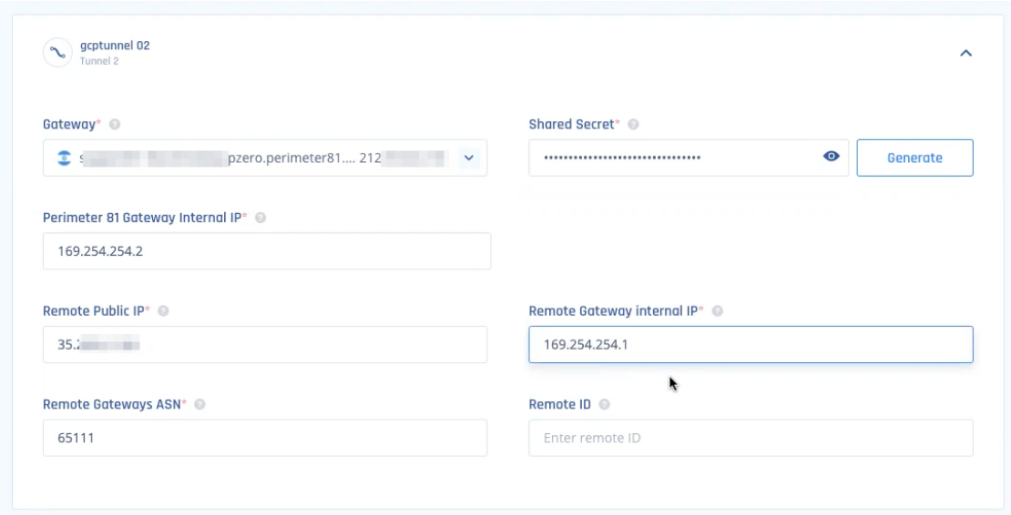
   Enter **ASN** value as 65111 for both tunnels.



Example - Tunnel 1



Example - Tunnel 2

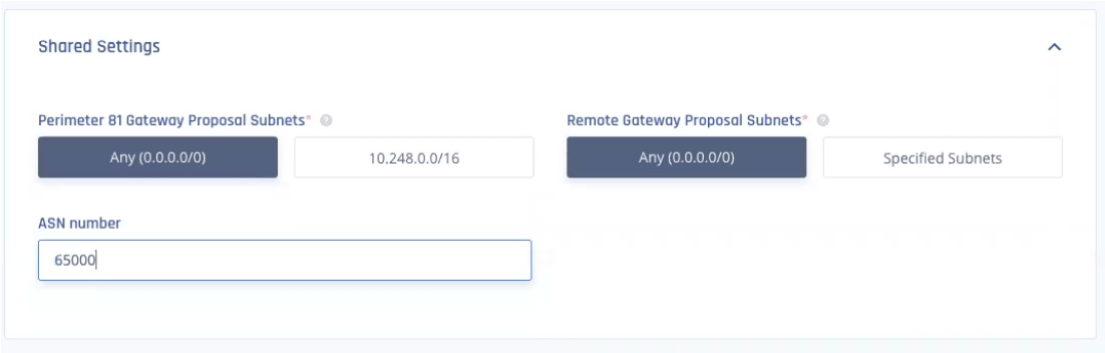


7. In the **Shared Settings** section:

a. In **Proposal Subnets**, select **Any(0.0.0.0/0)** for both sides.

b. Set **ASN** as 65000.

Warning - You cannot edit the ASN in Harmony SASE after you create the tunnel.



8. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

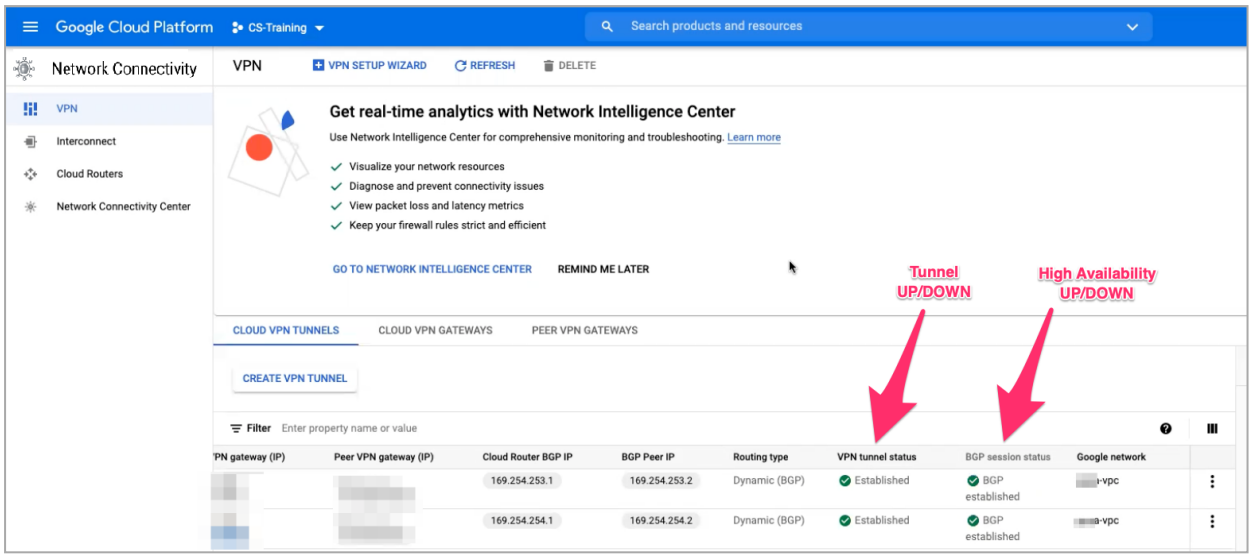
[1] Suggested values. For other supported ciphers, see this Google article.

9. Click **Add Tunnel**.

Verifying the Setup in GCP Console

1. Access the GCP console and go to **Network Connectivity** > **VPN**.
2. Verify that the **VPN tunnel status** and **BGP session status** appears with a green tick

mark.

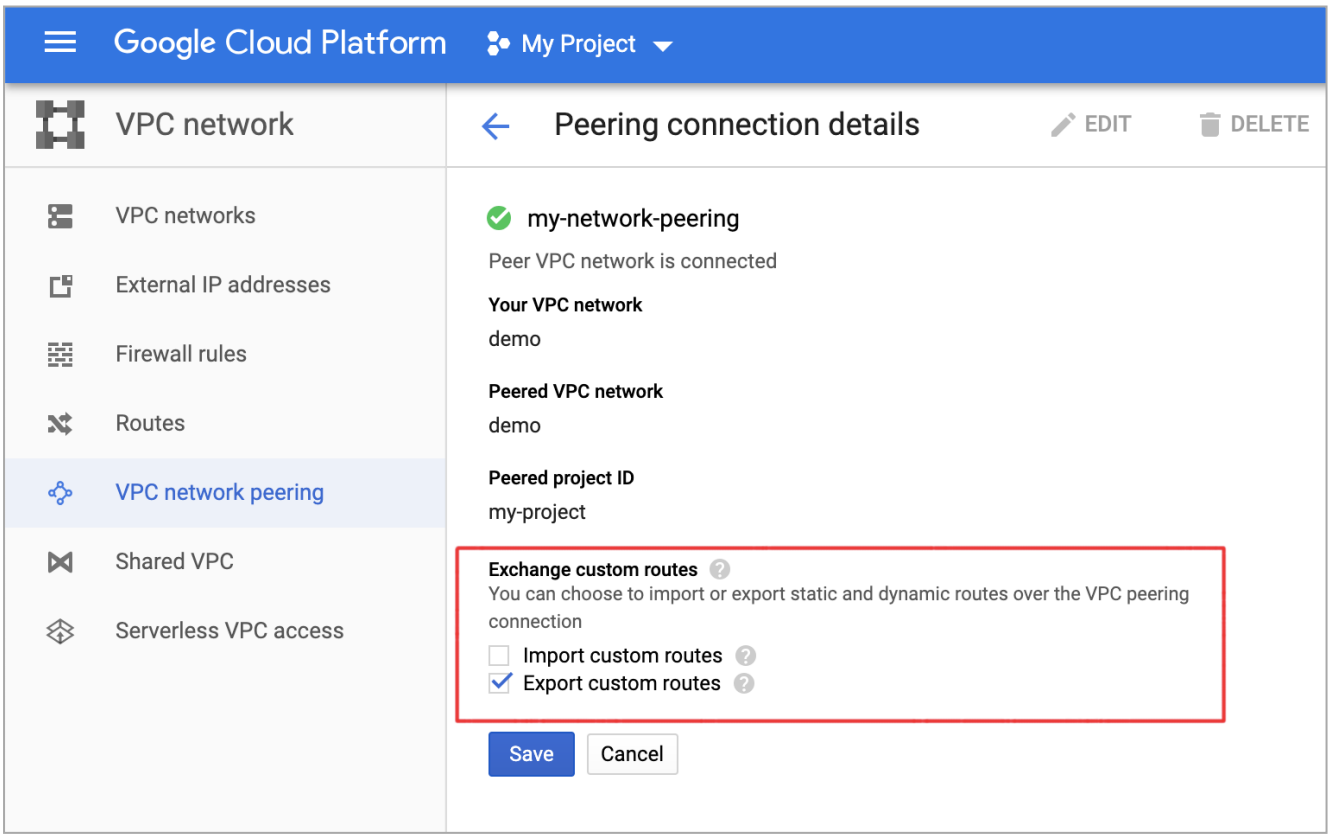


Google Cloud VPC Peering

VPC peering allows you to connect Harmony SASE with Google Cloud Platform by exporting the route of your Harmony SASE network to the VPC.

With VPC peering, you need only a single tunnel from Harmony SASE to the shared Google Cloud VPC. The other peered VPC recognizes the Harmony SASE subnets by having its route in their routing table.

Export the custom routes from your shared VPC.



Google Cloud DNS

You can integrate Google Cloud's Private Zone/Private DNS feature with Harmony SASE gateway. This enables you to utilize the capabilities of private DNS zones, that allows resolution of external records.

Prerequisites

- Google Cloud Platform (GCP) project
- VPC Network (you can create one or use Google's predefined subnets)
- Site-to-Site VPN tunnel to the VPC from Harmony SASE

Enabling Private DNS with Harmony SASE Gateway

To allow administrator to expose Google Cloud DNS through a private IP within one or multiple networks defined in your VPC through GUI/Web Interface, do this:

1. Log in to Google Cloud Platform.
2. Go to **Networking** > **Network services** > **Cloud DNS**.
3. Click the **DNS Server Policies** tab.
4. Click **Create Policy**.

   The **Create a DNS policy** page appears.
5. In the **Name** field, enter a name for the DNS policy. Use lowercase and no space.
6. In the **Description** field, add a description.
7. In the **Logs** section, select one of these:
   - **On**
   - **Off**
8. In the **Inbound query forwarding** section, select **On**.
9. In the **Alternate DNS servers** section, from the **Networks list**, select all desired networks.
10. Click **Create**.

    The system generates a private IP address that you can use to configure Private DNS in Harmony SASE Administrator Portal.
11. Install Google Cloud Software Development Kit (SDK).
12. To authenticate or initialize your gcloud CLI environment, run:

    ```
    gcloud auth login
    ```

13. To create an inbound server policy for DNS, run:

    ```
    gcloud dns policies create {{NAME}} --description=
    {{DESCRIPTION}} --networks={{VPC_NETWORK_LIST}} --enable-
    inbound-forwarding
    ```

    where, `{{NAME}}` is the name for the policy, `{{DESCRIPTION}}` is the description of the policy, and `{{VPC_NETWORK_LIST}}` is the comma separated list of VPC networks (not subnets).

    For example:

    ```
    ops-vlad:~ vbekker$ gcloud dns policies create inbounddnsvlad --
    description=inboundDNSVlad --networks=vladvpc --enable-inbound-
    forwarding
    Created Policy
    [https://dns.googleapis.com/dns/v1/projects/vladgcp/policies/inbo
    unddnsvlad].
    {
      "description": "inboundDNSVlad",
      "enableInboundForwarding": true,
      "enableLogging": false,
      "id": "8199820556025819315",
      "kind": "dns#policy",
      "name": "inbounddnsvlad",
      "networks": [
        {
          "kind": "dns#policyNetwork",
          "networkUrl":
    "https://compute.googleapis.com/compute/v1/projects/vladgcp/globa
    l/networks/vladvpc"
        }
      ]
    }
    ```

14. Validate the setup by performing the successful DNS lookup from the gateway directly to the server and also to DNS forwarder.

    For example:

- Directly querying the name server:

```
vlad@vodFpGngx3:~$ dig www.vpcdnszone.com  @192.168.128.2

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.vpcdnszone.com
@192.168.128.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51251
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.vpcdnszone.com.        IN    A

;; ANSWER SECTION:
www.vpcdnszone.com.    300    IN    A    192.168.128.50

;; Query time: 161 msec
;; SERVER: 192.168.128.2#53(192.168.128.2)
;; WHEN: Fri Mar 05 00:11:01 UTC 2021
;; MSG SIZE  rcvd: 63
```

- Through local forwarder:

```
vlad@vodFpGngx3:~$ dig www.vpcdnszone.com

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> www.vpcdnszone.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46053
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.vpcdnszone.com.        IN    A

;; ANSWER SECTION:
www.vpcdnszone.com.    300    IN    A    192.168.128.50

;; Query time: 156 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Mar 05 01:38:15 UTC 2021
;; MSG SIZE  rcvd: 70
```

15. Enable Private DNS on the network in Harmony SASE Administration Guide. For more information on how to enable, see Private DNS.

Heroku Enterprise

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

Configuration Steps

After you obtain your private Harmony SASE gateway, to set up a VPN gateway for the Private Space, run:

```
* Shell
```

```
Copy ```
heroku spaces:vpn:connect \
```

```
     --name   perimeter81 \   --ip   PUBLIC_IP_OF_YOUR_VPN_GATEWAY
\   --cidrs     '10.255.248.0/21'   \   --space   SPACE
```

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

```
* Shell

Copy ```
heroku   spaces  :vpn  :wait   --space    SPACE   perimeter81
```

When the gateway is ready, to get the configuration, run:

```
* Shell

Copy ```
heroku   spaces  :vpn  :info   --space    SPACE   perimeter81
```

The above command returns a table that contains all the details you need to configure Harmony SASE.

Sample output:

```
* Text
Copy ```
heroku spaces:vpn:info --space SPACE perimeter81
=== SPACE VPNs
VPN Tunnel  Customer Gateway  VPN Gateway    Pre-shared Key
Routable Subnets  IKE Version
__________  _________________  _____________ _______________
________________  ___________
Tunnel 1 52.91.173.226 34.203.187.158 abcdef12345     10.0.0.0 /16 1
Tunnel 2 52.91.173.226 34.227.70.143 123456abcdef    10.0.0.0 /16 1
```

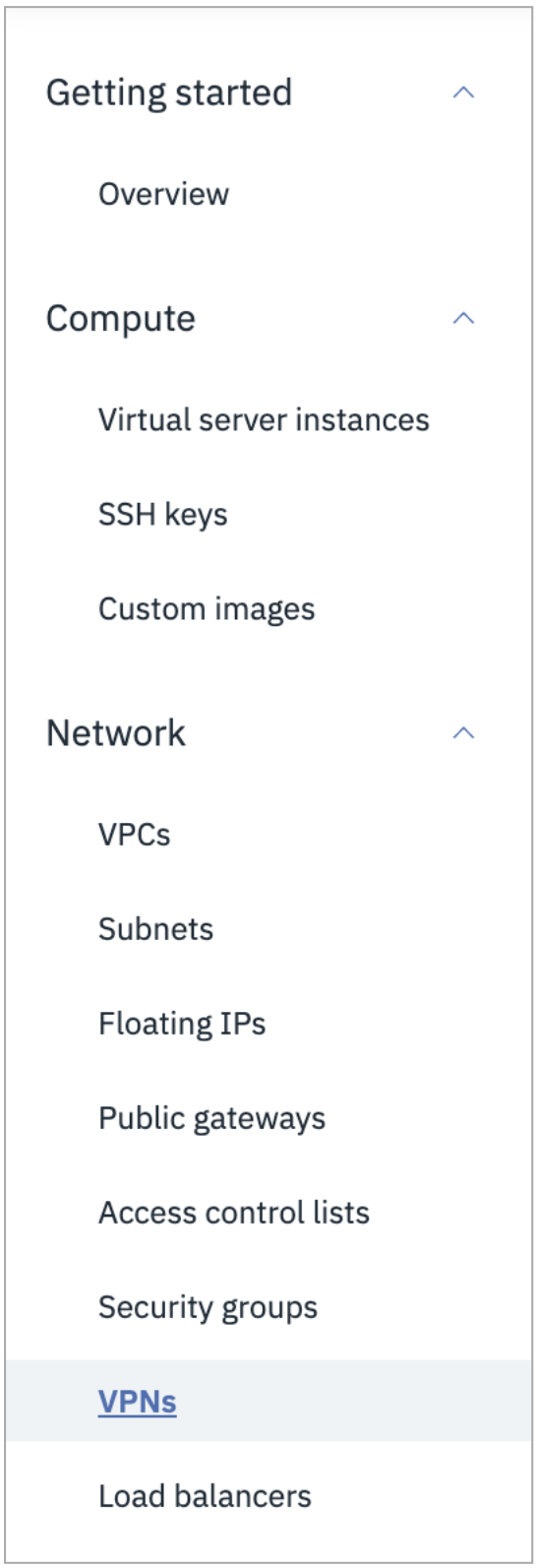
IBM Cloud

Prerequisites

- An active Harmony SASE Administrator Portal account and network.
- Make sure you have installed the Harmony SASE Agent on your devices.
- Administrator account in the Firewall/ Router/ Cloud Management Portal.

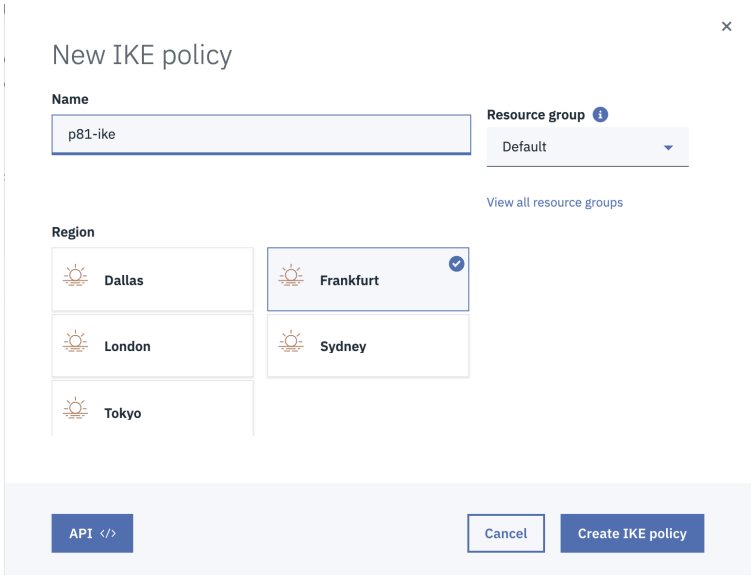
Step 1 - Configuring a VPN Gateway at the IBM Cloud Console

1. Access the IBM Cloud Console and open the **VPC** section and go to **Network** > **VPNs**.



2. Go to the **IKE policies** tab and click **New IKE policy**.

3. The **New IKE policy** window appears.

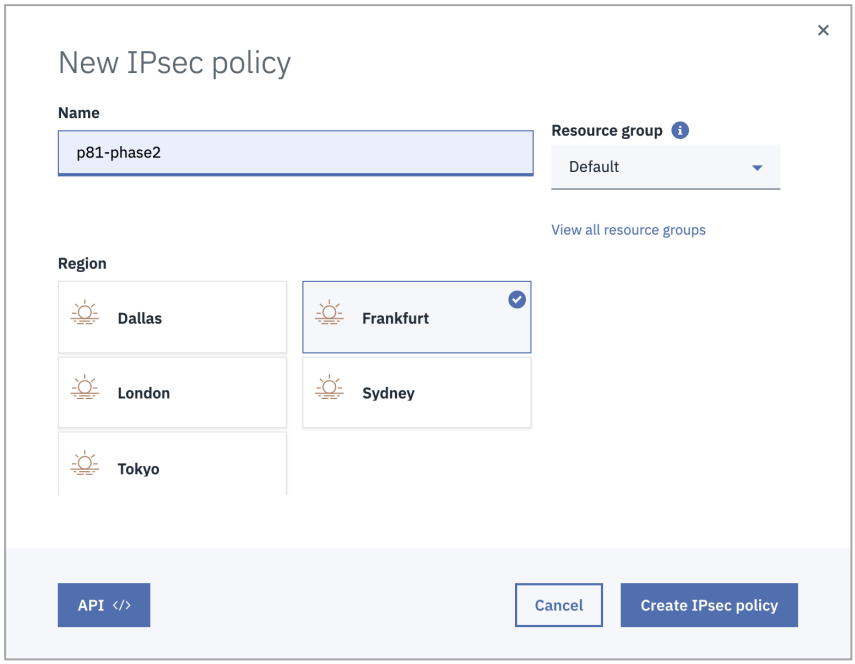


4. Enter these:
   a. **Name** - Name of the policy.
   b. **Resource group**
   c. **Region** - Region in which the VPC is located.
5. Click **Create IKE policy**.

   The system creates the IKE policy.
6. Click ··· and then **Edit**.
7. Enter these:
   a. **IKE Version** - 1
   b. **DH Group** - 2
   c. **Authentication** - sha256
   d. **Key Lifetime** - 28800
   e. **Encryption** - aes256
8. Click **Save IKE policy**.

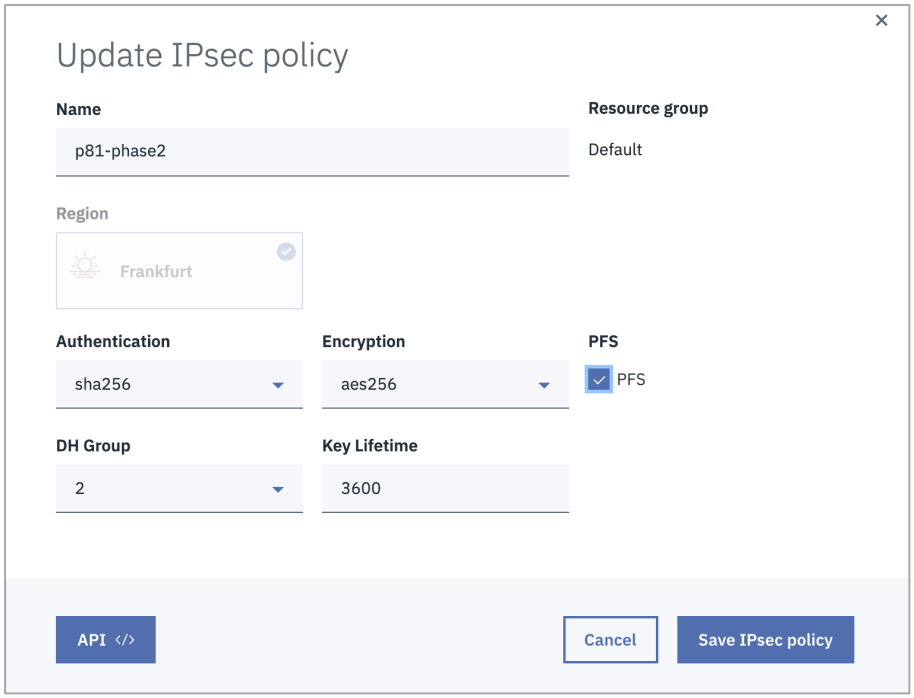
9. Go to the **IPSec Policies** tab and click **New IPSec Policy**.

   The **New IPSec policy** window appears.



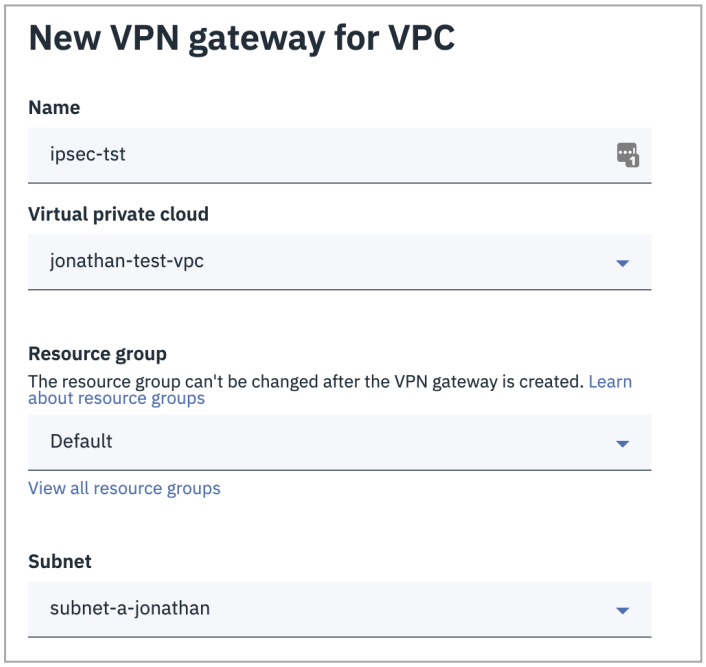
10. Enter these:
    a. **Name** - Name of the policy.
    b. **Resource group**
    c. **Region** - Region in which the VPC is located.
11. Click **Create IPSec policy**.

    The system creates the IPSec policy.
12. Click ··· and then **Edit**.
13. Enter these:
    a. **Authentication** - sha256
    b. **Encryption** - aes256
    c. **PFS** - Select the checkbox.
    d. **DH Group** - 2
    e. **Key Lifetime** - 3600
14. Click **Save IPSec policy**.



15. Go to the **VPN gateways** tab and click **New VPN gateway**.

    The **New VPN gateway for VPC** window appears.



16. Enter these:

    a. **Name** - Name of the VPN gateway.

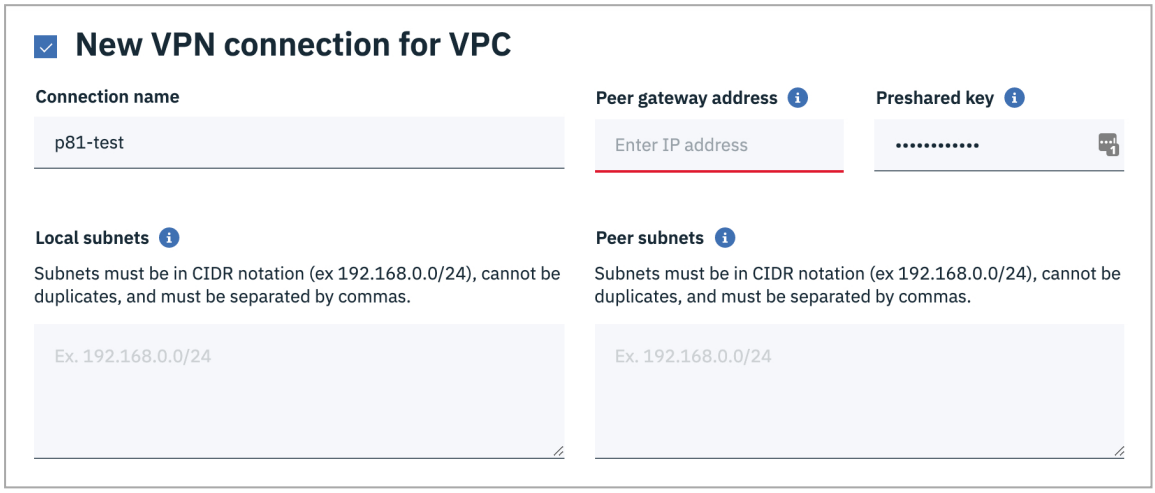
    b. **Virtual private cloud** - Select the required cloud.

c. **Resource group** - Select the resource group.

d. **Subnet** - Select the required subnet.

17. Select **New VPN Connection for VPC**.

    The **New VPN connection for VPC** window appears.



18. Enter these:

    a. **Connection name** - Name of the VPN connection.

    b. **Peer gateway address** - IP address of your Harmony SASE gateway.

    c. **Preshared key** - A string with at least 8 characters that contains upper-case letters and numbers.

    d. **Local subnets** - Specify one or more subnets in the VPC you want to connect.

    e. **Peer subnets** - 10.255.0.0/16 (Unless you have custom configurations or multiple tunnels to the same Harmony SASE gateway).

    f. **Dead peer detection action** - Restart

    g. **Interval** - 10 seconds

    h. **Timeout** - 30 seconds

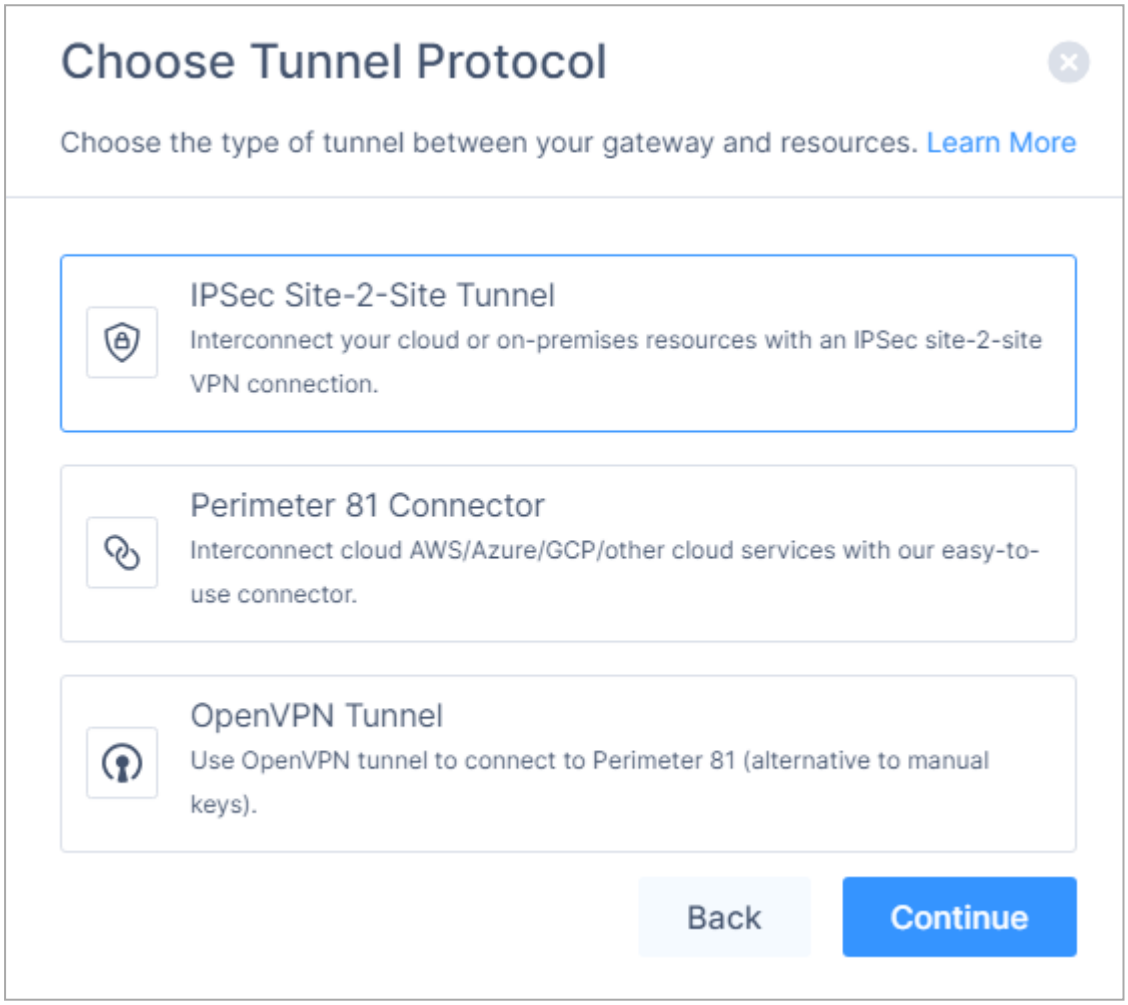
    i. **IKE policy** - Select the IKE policy created earlier.

    j. **IPSec policy** - Select the IPSec policy created earlier.

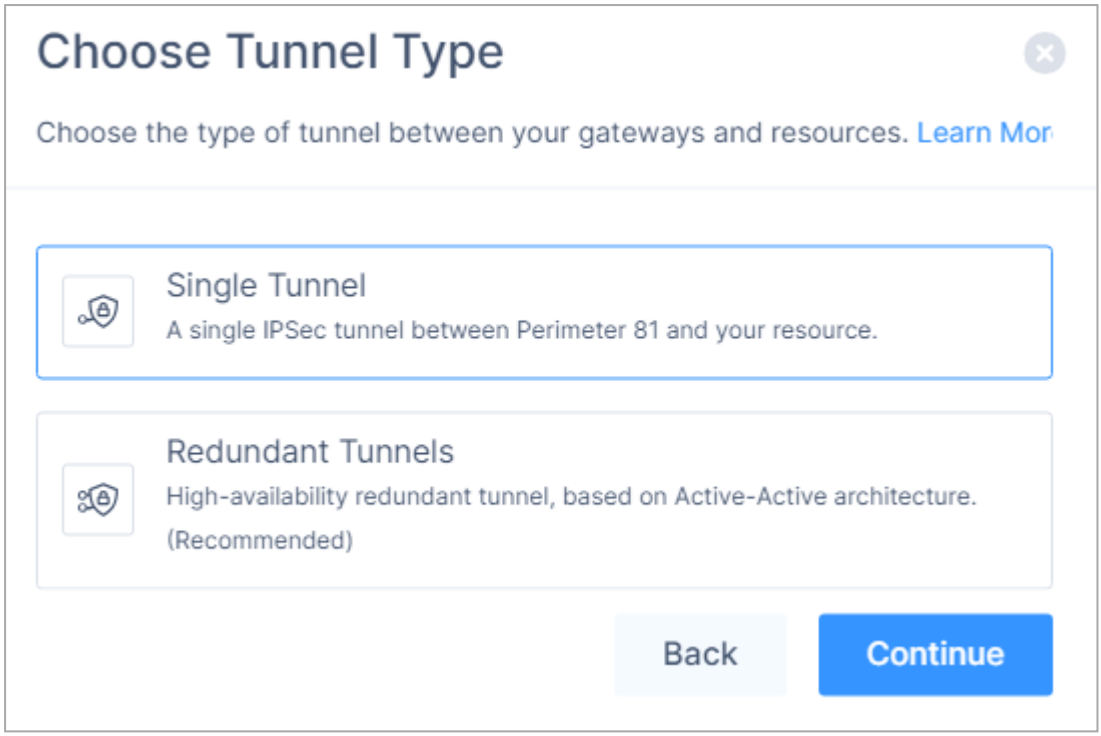
Step 2 - Creating the Tunnel in the Harmony SASE Administrator Portal

1. Access the Harmony SASE Administrator Portal and click **Networks**.
2. Click the network where you want to create the tunnel.
3. In the required gateway, click ··· > **Add Tunnel**.

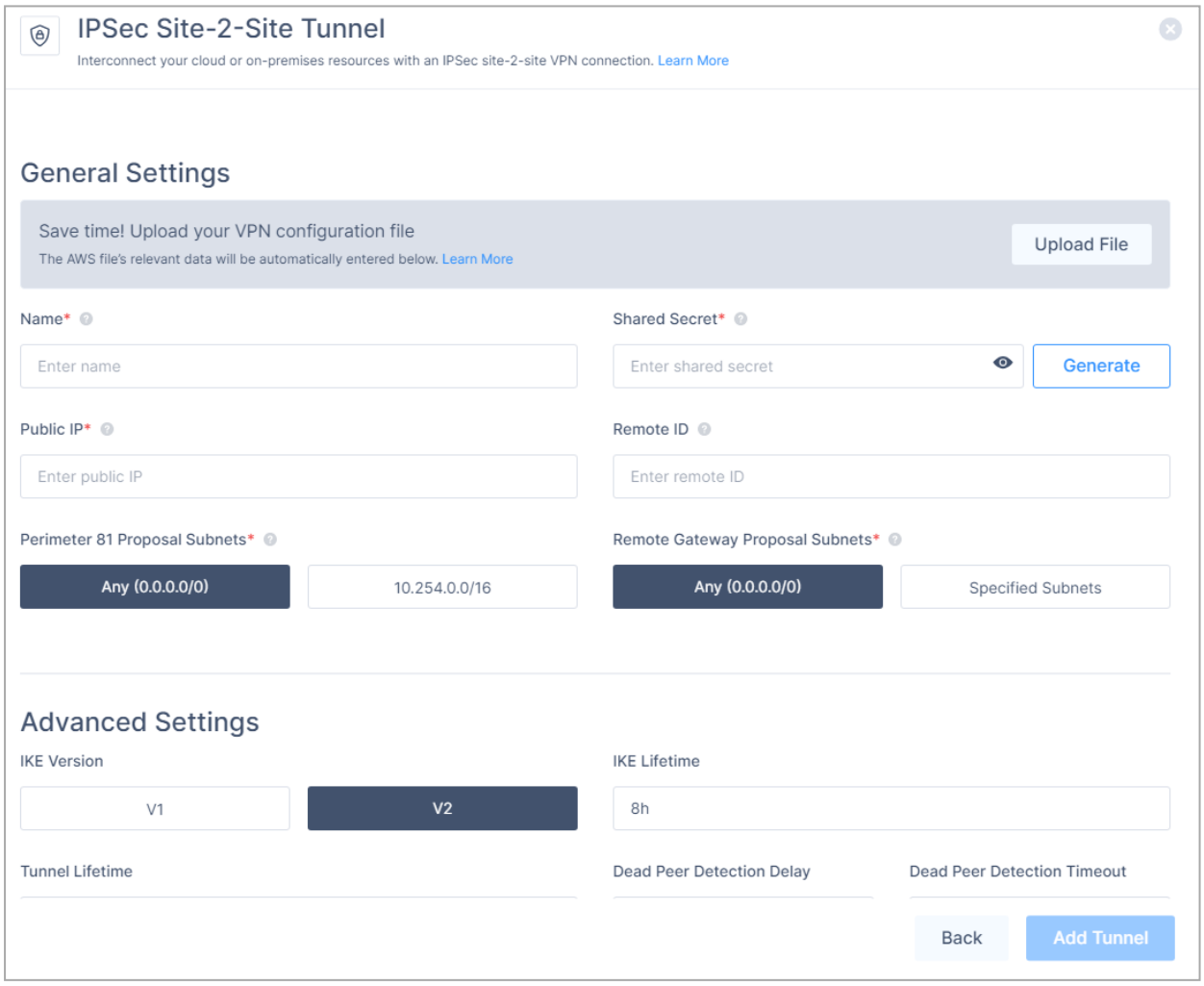
4. Click **IPSec Site-2-Site Tunnel** and click **Continue**.



5. Click **Single Tunnel** and click **Continue**.



The **IPSec Site-2-Site Tunnel** window appears.



6. In the **General Settings** section, enter these:
   a. **Name** - Name of the tunnel.
   b. **Public IP** - IP address of the VPN Gateway defined in the IBM Cloud console.
   c. **Remote ID** - Identical to Remote IP.
   d. **Shared Secret** - Preshared key in the IBM Cloud console.
   e. **Perimeter 81 Gateway Proposal Subnets** - 10.255.0.0/16 or the value defined in the IBM Cloud console.
   f. **Remote Gateway Proposal Subnets** - Subnets in the VPC that you want to connect.
7. In the **Advanced Settings** section, enter the information for your tunnel type:

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Amazon AWS											
Single Tunnel - AWS Virtual Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Virtual Private Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels - AWS Transit Gateway	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Google Cloud Platform											

Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Single Tunnel [1]	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Redundant Tunnels	V2	8h	1h	10s	30s	aes256	aes256	sha512	sha512	21	21
Microsoft Azure											
Single Tunnel - Azure Virtual Network Gateway	V2	3600s	27000s	10s	45s	aes256	aes256	sha1	sha1	2	2
Redundant Tunnels - Virtual Network Gateway	V2	9h	9h	10s	30s	aes256	aes256	sha1	sha1	2	2

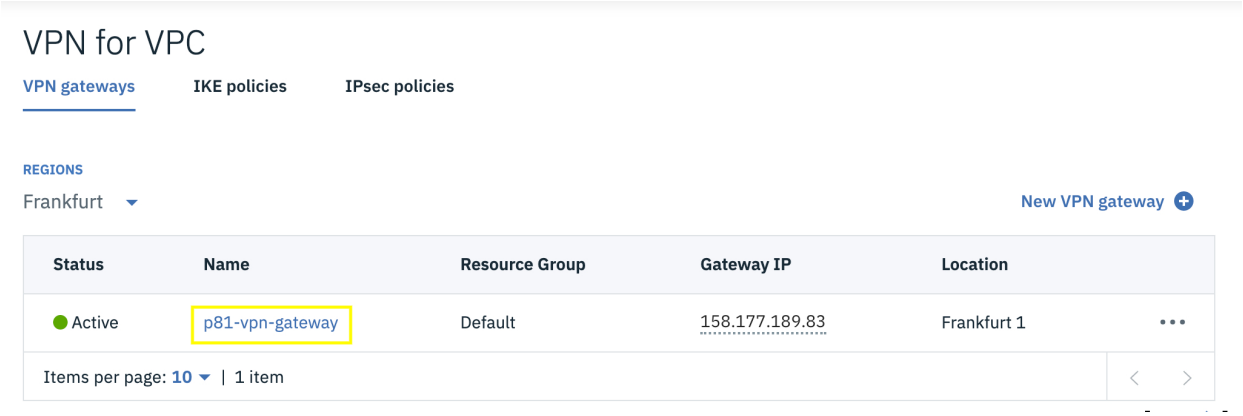
Field / Cloud Vendor	IKE Version	IKE Lifetime	Tunnel Lifetime	Dead Peer Detection Delay	Dead Peer Detection Timeout	Encryption (Phase 1)	Encryption (Phase 2)	Integrity (Phase 1)	Integrity (Phase 2)	Diffie Hellman Groups (Phase 1)	Diffie Hellman Groups (Phase 2)
Redundant Tunnels - Virtual WAN	V2	8h	1h	10s	30s	aes256	aes256	sha256	sha256	14	14
Other tunnel types											
Alibaba Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha1	sha1	2	2
IBM Cloud	V1	8h	1h	10s	30s	aes256	aes256	sha256	sha256	21	21

[1] Suggested values. For other supported ciphers, see this Google article.

8. Click **Add Tunnel**.

Verifying the Setup in IBM Cloud Console

1. Access the IBM Cloud console and go to the **VPN gateways** tab.
2. Select the name of the VPN Gateway associated with the tunnel.



3. Scroll down and click **View all connections**.

   Verify whether the tunnel **Status** as active.

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*.

Private Access

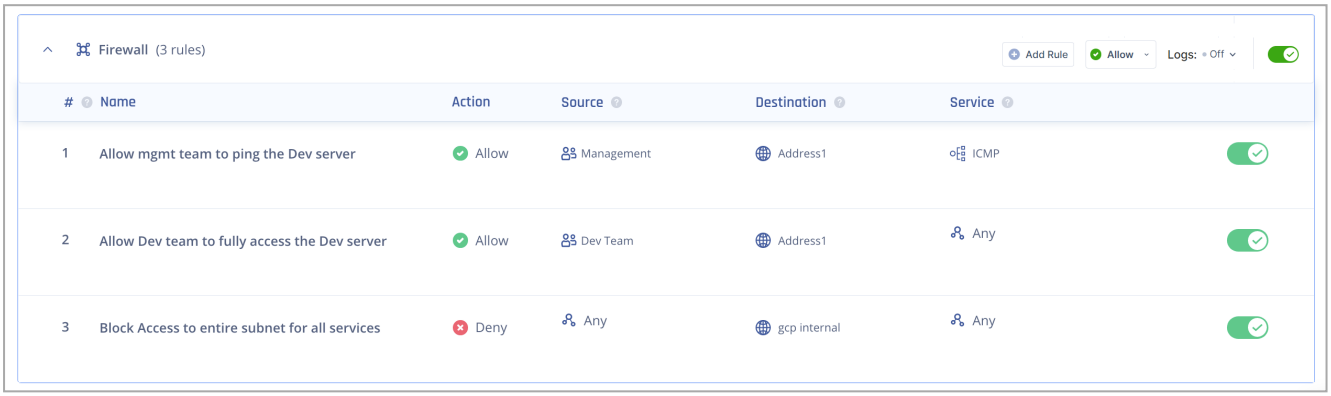
Private Access allows you to:

- 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**.



Note - Contact your account manager to request firewall logging functionality.

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 126*.

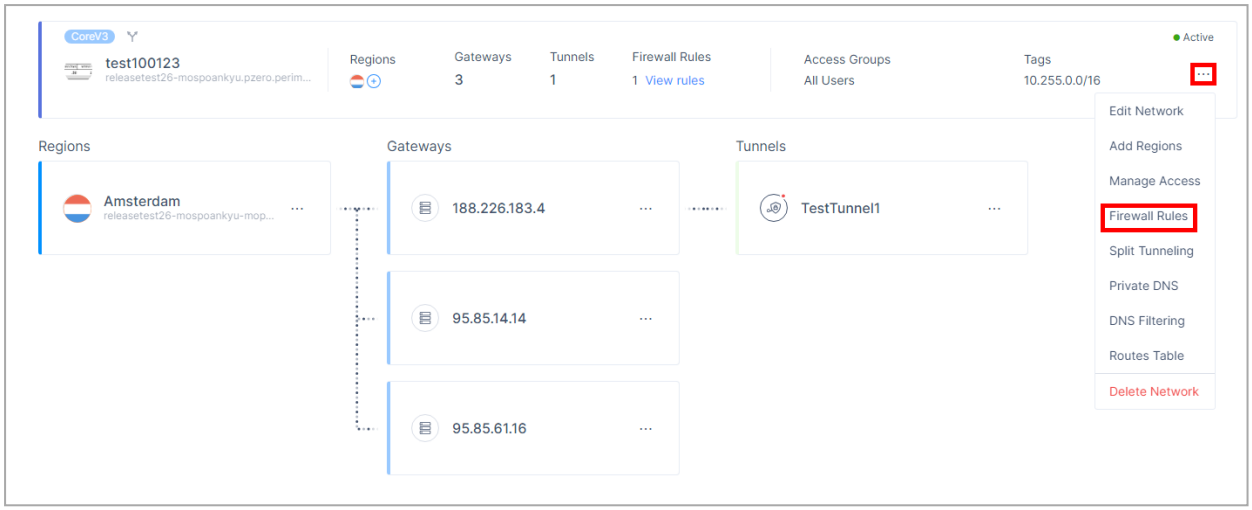
Access Rules Order

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.

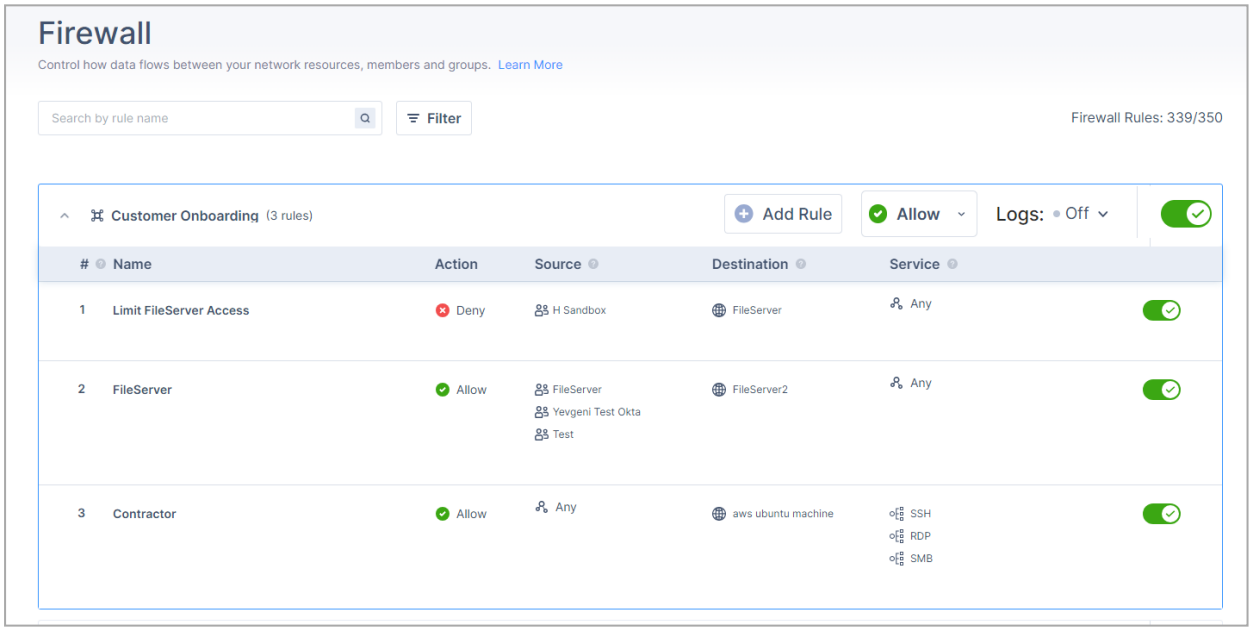
Creating a Firewall Access Rule

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**.

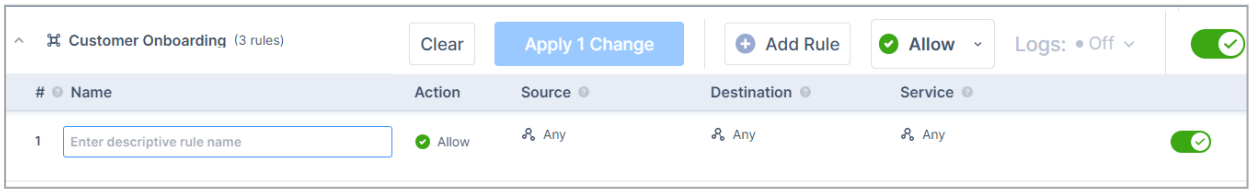


The **Firewall** page appears.



4. Click **Add Rule**.

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



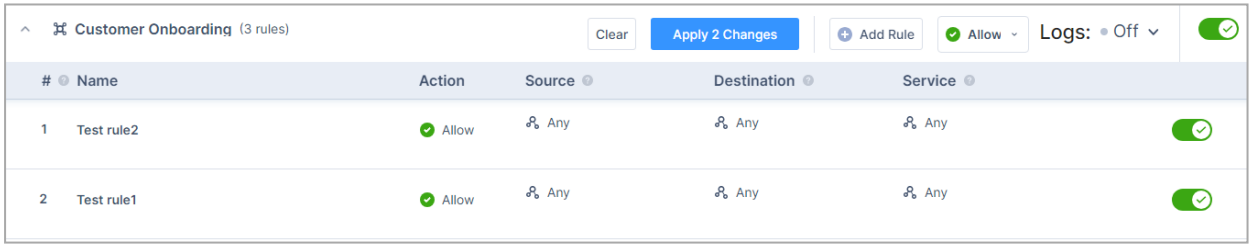
5. In the **Name** field, enter a name that describes the rule.
6. From the **Action** list, select the action type:

- **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

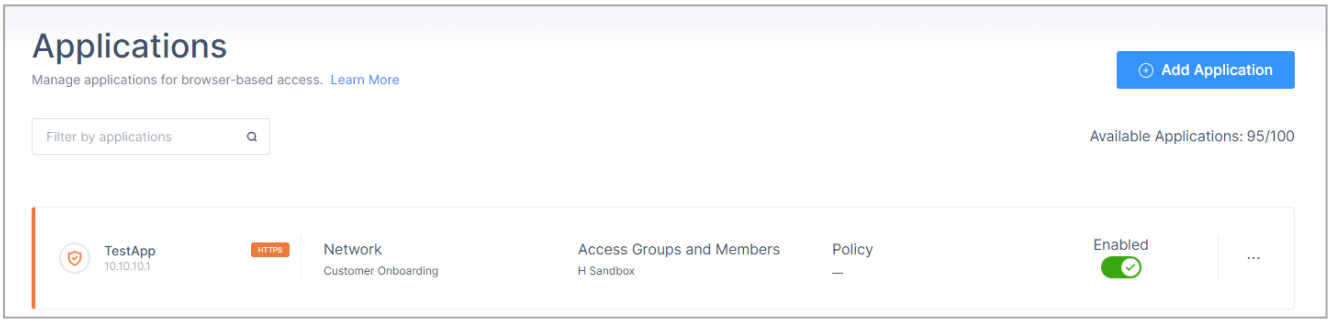
Applications

The **Applications** page allows to you add your web-applications and offer an agent-less access to these applications through customized protocols.

The supported application protocols are:

Protocol	Sample Application
HTTP/HTTPS	Bitbucket
RDP	My Desktop
SSH	Staging Web Server
VNC	Build PC

To view the **Applications** page, access the Harmony SASEAdministrator 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.

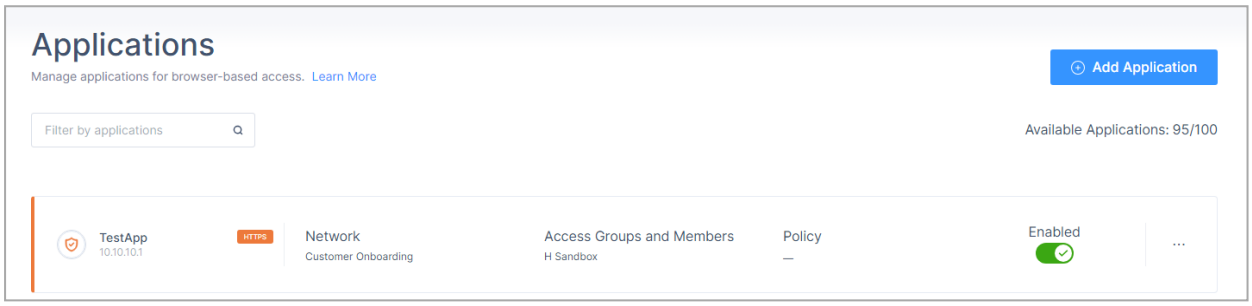
Note - To provide secure access for public SaaS applications, such as Microsoft Office 365, Gmail and so on, use the Harmony SASE Agent.

Prerequisites

1. Define your network with IPSec or Harmony SASE Connector tunnel. See *"Networks" on page 109*.
2. Verify that the application is accessible through the Harmony SASE Agent.

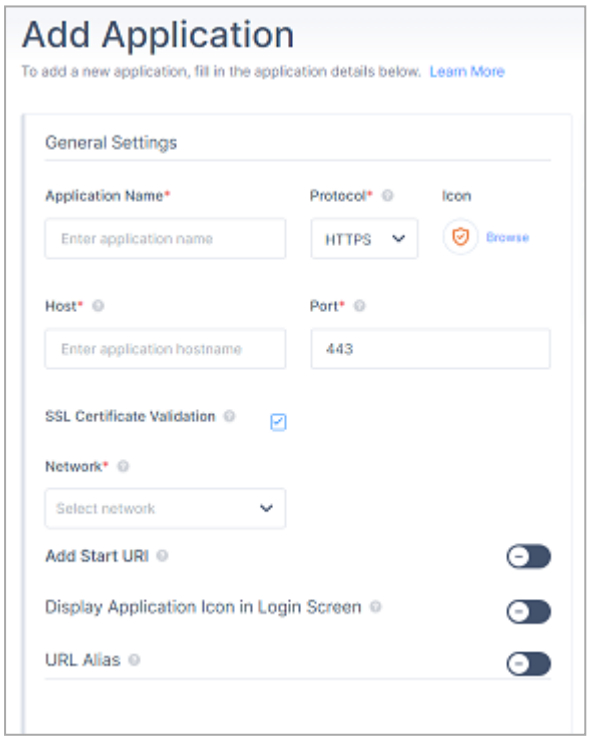
Adding an Application

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



2. Click **Add Application**.

   The **Add application** window appears.

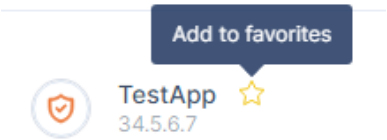


3. Select the application type:

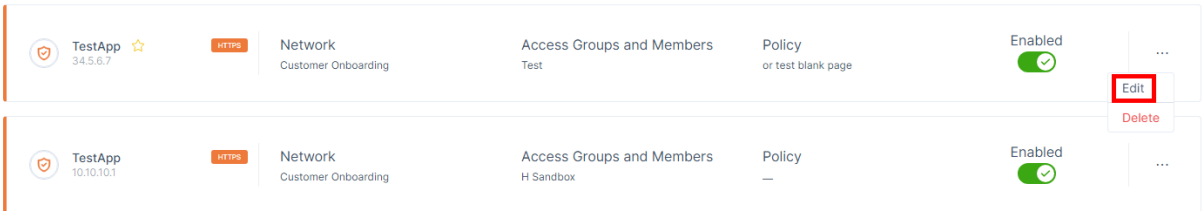
- HTTP/HTTPS application
- RDP application
- SSH application
- VNC application

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.



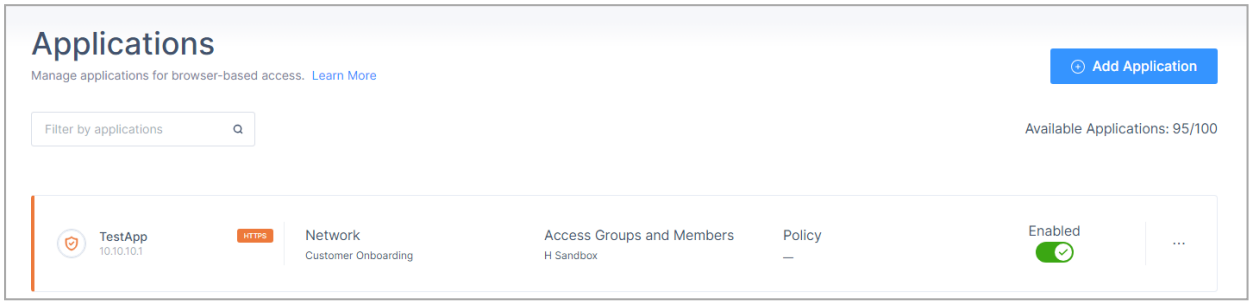
5. To edit the application details, click ··· and then click **Edit**.



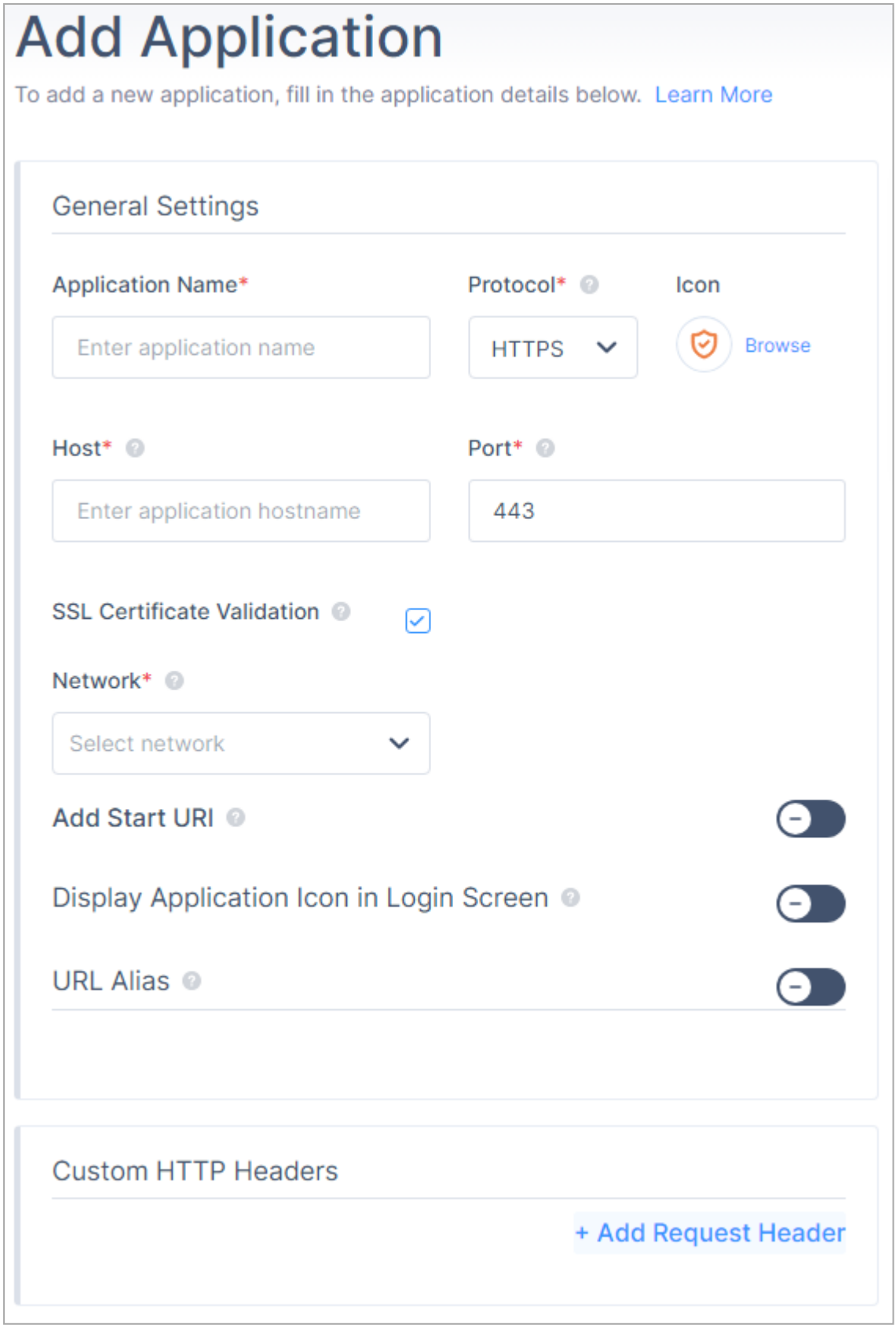
6. Make the required changes and click **Apply**.
7. For members to access the application, see *"Providing Application Access to Members" on page 636*.

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.

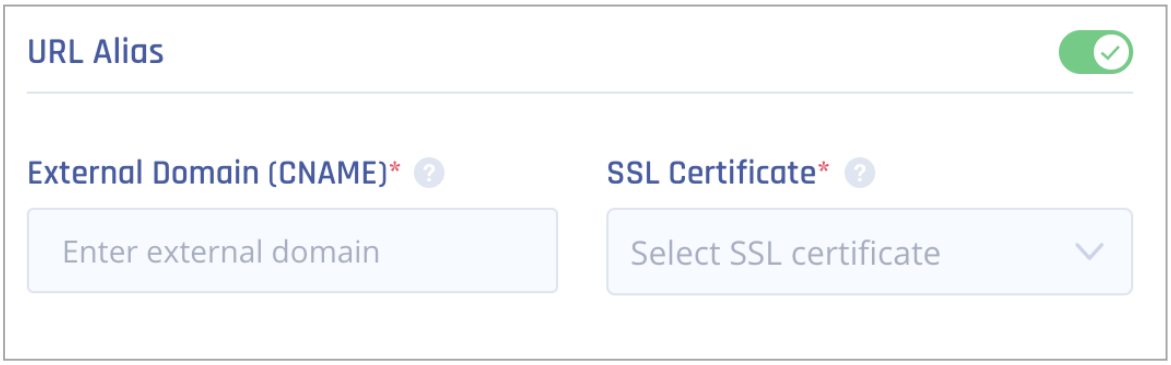
h. (Optional) **Add Start URI** - Subpath to which the system must redirect after the member launches the application.

   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.

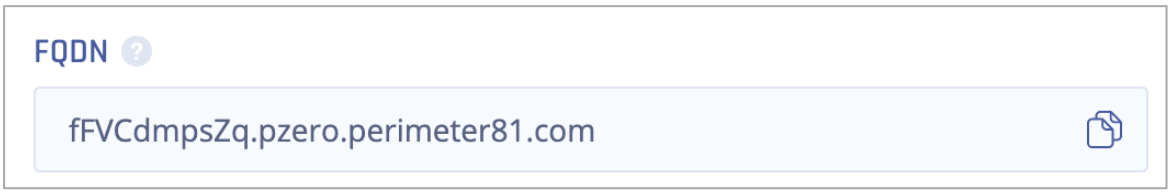


k. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

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).

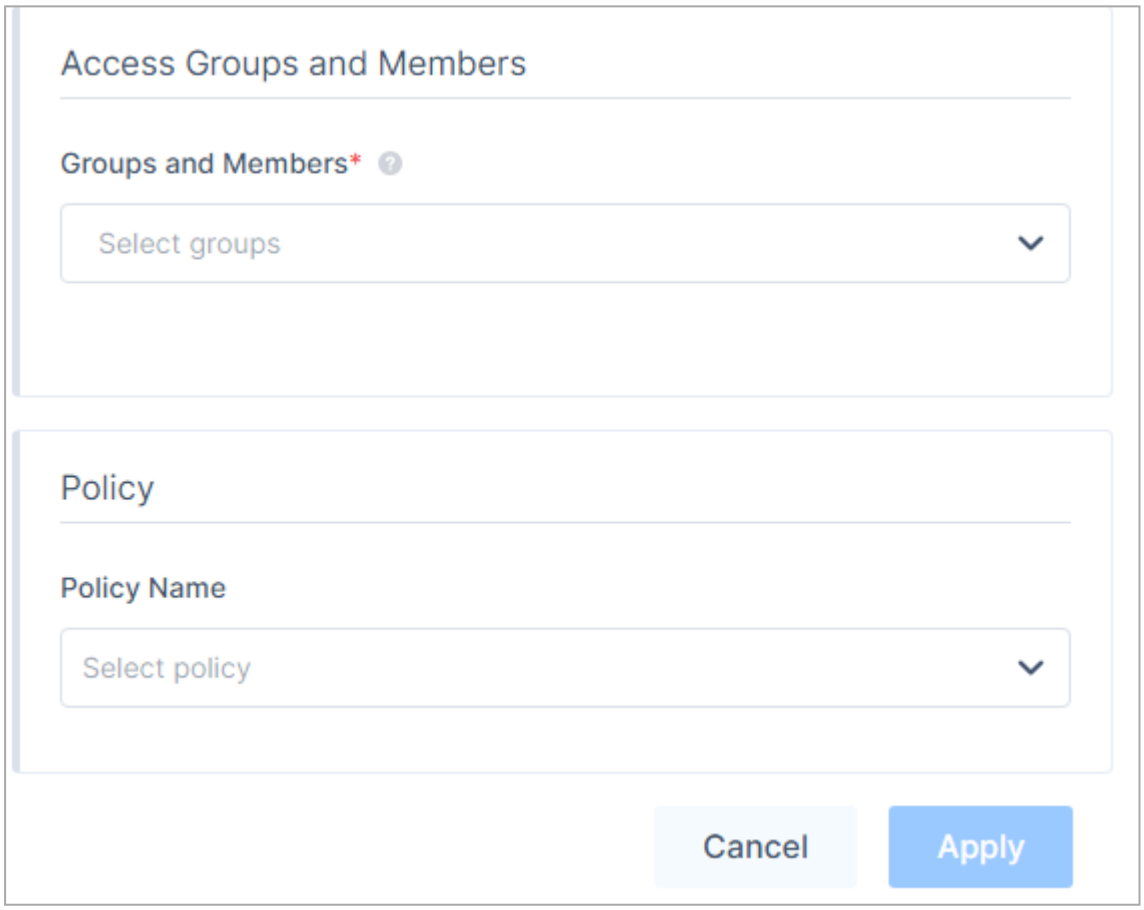
Under your domain, use the CNAME specified in the previous step and point it to the application FQDN. The FQDN appears in the application settings after you click Apply.



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

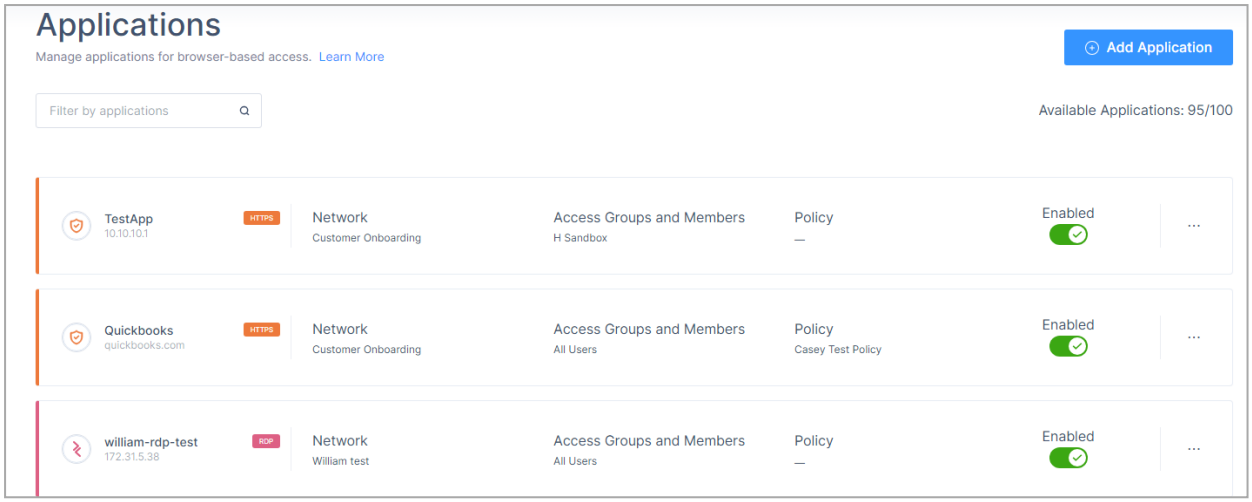
Mandatory if you have specified DNS in the **Host** field.

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 *"Providing Application Access to Members" on page 636*.

Adding an RDP Zero Trust Application

Harmony SASE allows you to create an RDP Zero Trust Application (ZTA) as either:

- Web Client Type - A browser-based solution providing convenient and quick remote desktop access without installation.
- Native Client Type - A locally installed application offering robust performance and advanced features for remote desktop access.

For networks created or upgraded after September 2024, the administrators can configure a property in the IdP Attribute for Host and/or Port fields, that allows each member to access the dedicated RDP server. For more information, see *"RDP Server Access Based on IdP" on page 623*.

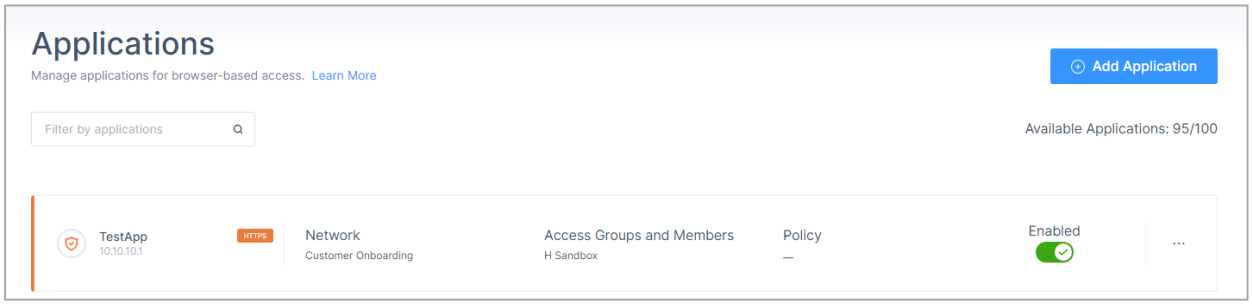
Prerequisite

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

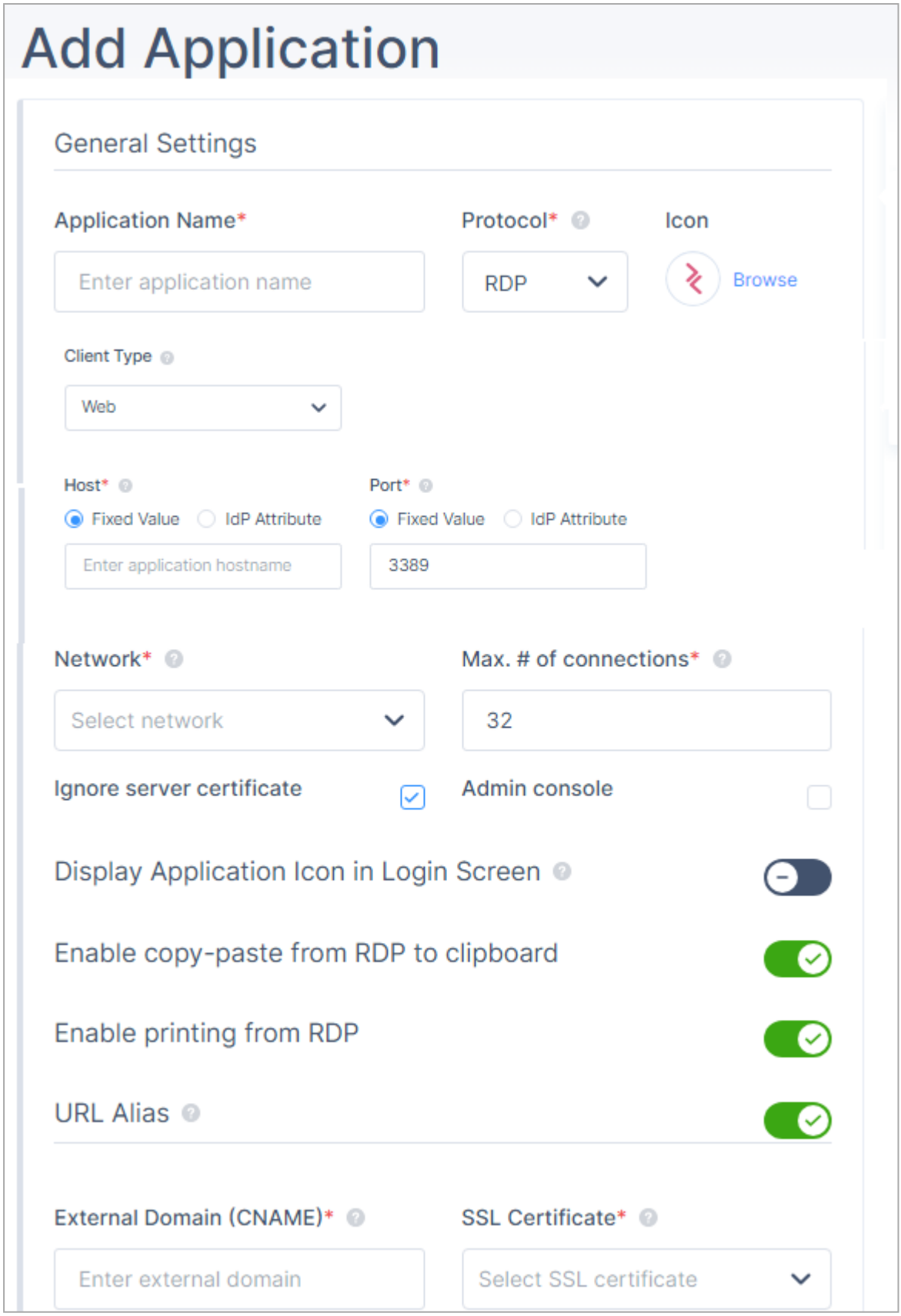
Adding an RDP ZTA

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. **Client Type** - Select one of these:

- **Web**
- **Native**

Note - For Native Client Type, these are the supported clients: Windows 10, Windows 11, Android, iOS, Mac, with latest MSTSC or MSRDC applications from Microsoft.

e. **Host** - Internal IP address of the server to which you want to connect. Select one of these and enter the value:

- **Fixed Value** - A predefined, unchanging value set by the administrator.
- **IdP Attribute** - Information provided by the Identity Provider during user authentication. For more information, see *"RDP Server Access Based on IdP" on page 623*.

Notes:

- IdP Attribute:
  - This feature is available only for networks created after September 2024. To use it for existing networks, contact *Check Point Support*.
  - This feature is supported only for Active Directory/LDAP and Azure Active Directory IdPs.
  - The administrator must store the hostname and/or port number in the IdP for each member.

f. **Port** - Select one of these and enter the value:

- **Fixed Value** - 3389
- **IdP Attribute**

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

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

Note - Disabled when you select **Client Type** as **Native**.

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

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

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

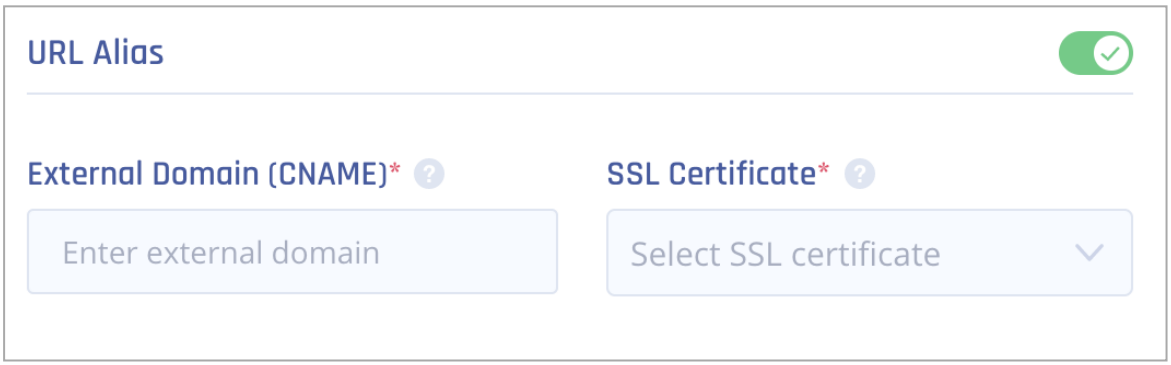
Note - Disabled when you select **Client Type** as **Native**.

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

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

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

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

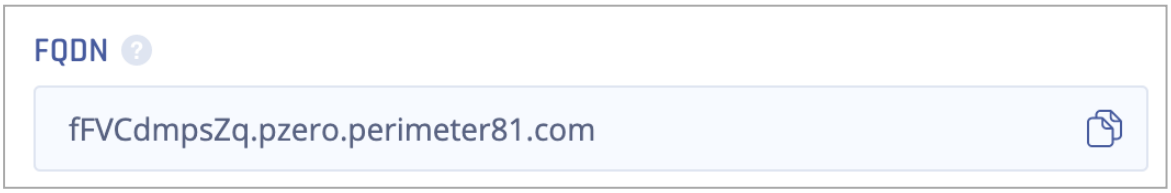


o. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

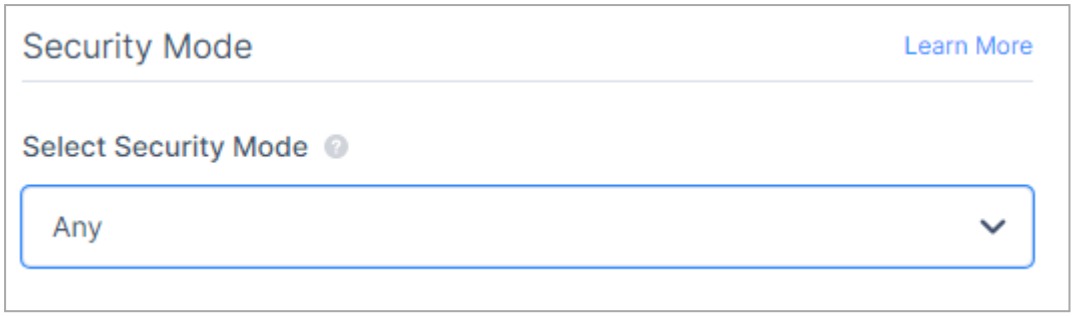
p. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

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

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



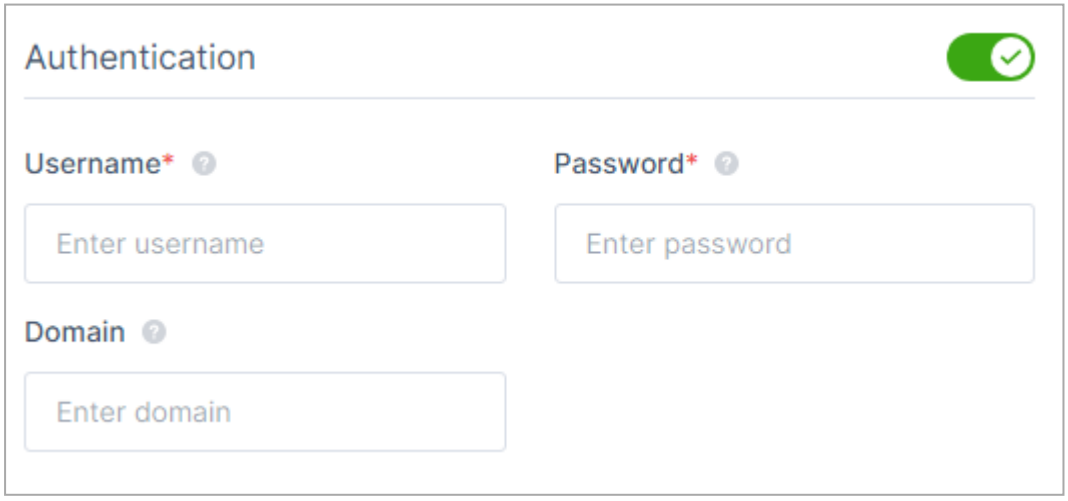
4. From the **Select Security Mode** list, select a security mode. It indicates the encryption and authentication mode.



- **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.

Note - Disabled when you select **Client Type** as **Native**.

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



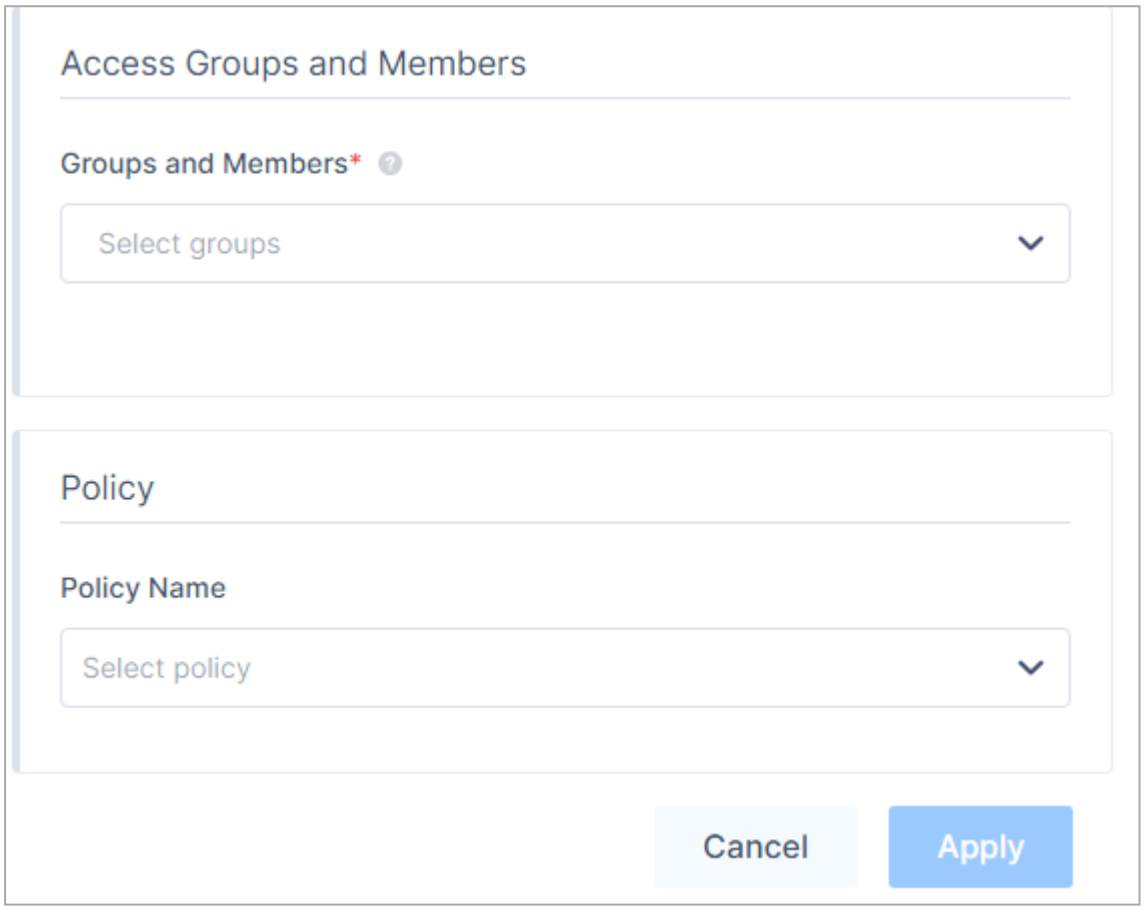
a. **Username** and **Password** - Credentials of the server.

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

Notes:

- If you disable **Authentication**, then the member must enter the credentials when accessing the application.
- This section is disabled when you select **Client Type** as **Native**.

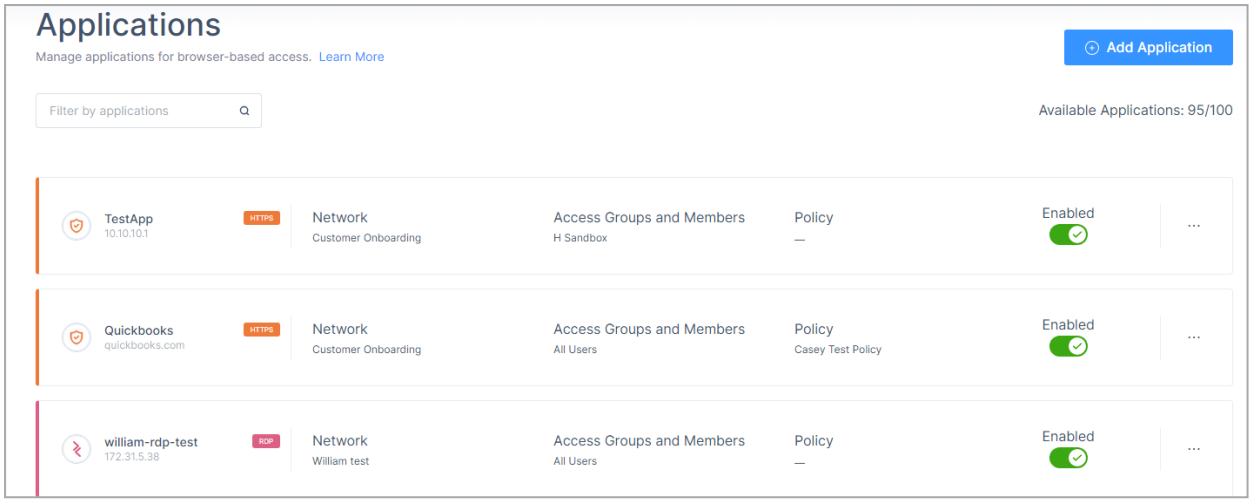
6. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.



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 *"Providing Application Access to Members" on page 636*.

RDP Server Access Based on IdP

For the RDP Zero Trust Application, the administrators can configure a property in the IdP Attribute for Host and/or Port fields, that allows each member to access the dedicated RDP server.

Notes:

- Hostname must be an IP address or Fully Qualified Domain Name(FQDN).
- The administrator must store the hostname and/or port number in the IdP to redirect the member to the appropriate RDP server.
- For the list of supported IdP Attribute properties, see Microsoft Graph User Properties.
- Custom properties are not supported.
- For Azure AD, make sure to configure the Azure application to have these permissions:
  - `Directory.Read.All`
  - `User.Read`

  For more information, see *"Microsoft Entra ID (formerly Azure AD) (Enterprise Application)" on page 815*.
- To map the AD/LDAP attributes to the property name in AD/LDAP, see Map AD/LDAP Profile Attributes to Auth0 User Profile.

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

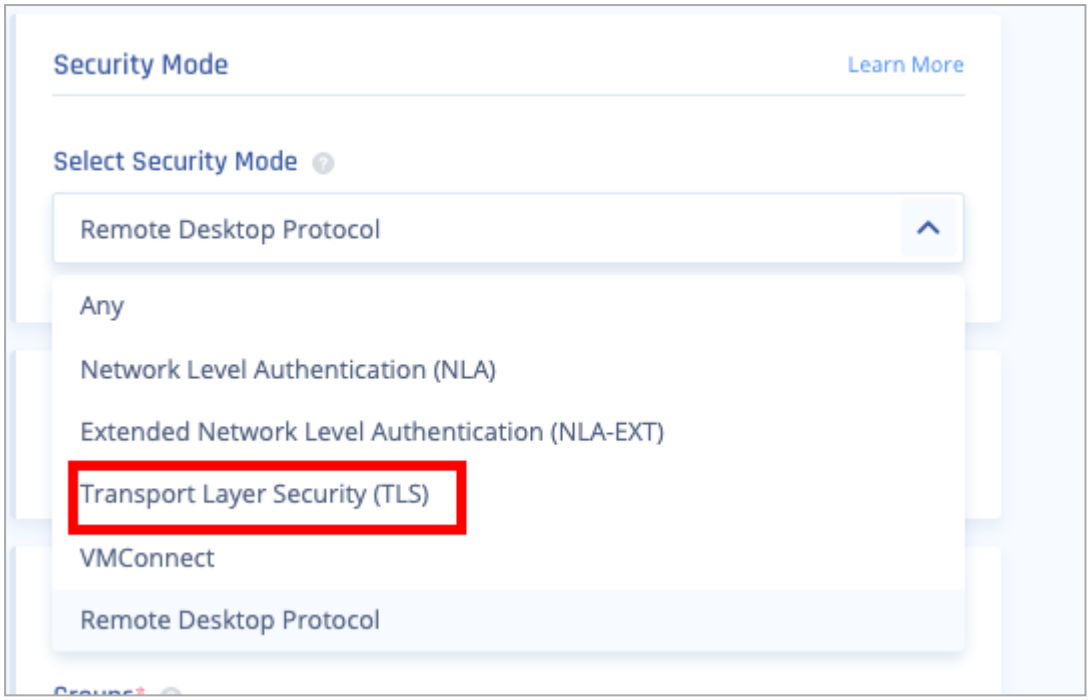
1. Open the **Registry Editor**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp**
3. Select **SecurityLayer** and change the value to **0**.
4. Reboot the machine.

Troubleshooting

Upstream Error

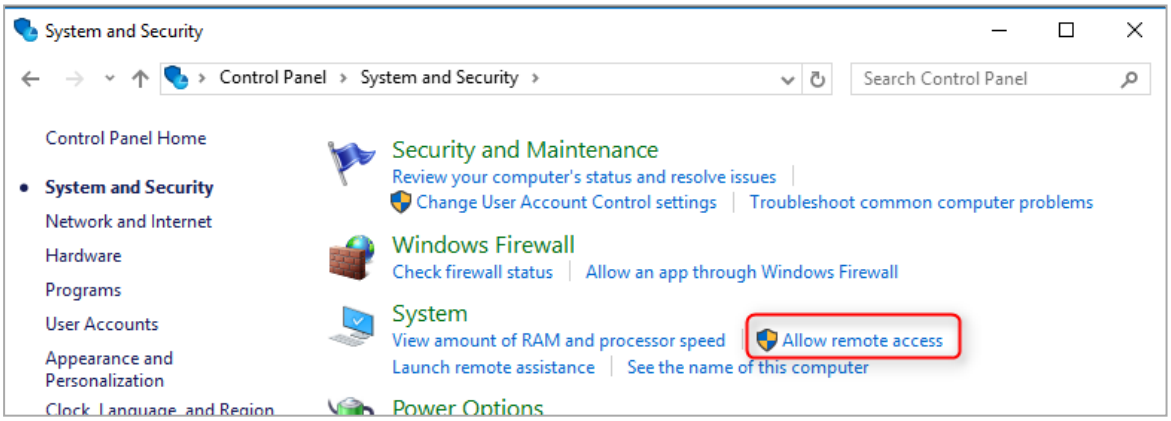
1. If **Authentication** is enabled (see Authentication), verify the credentials.

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



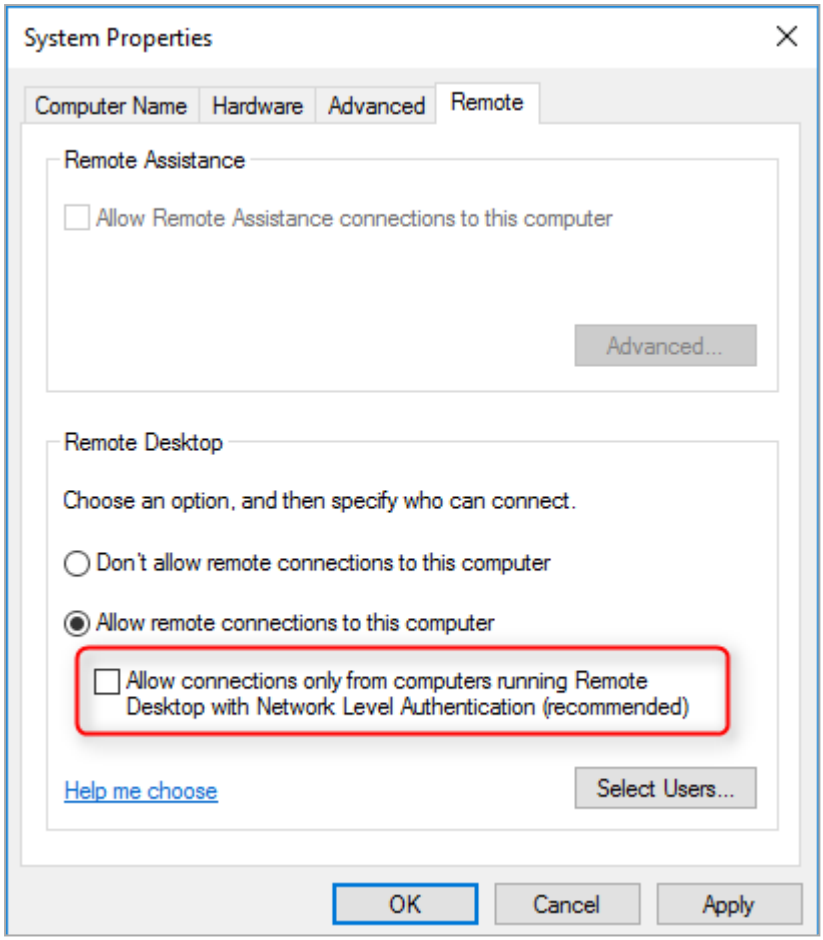
Additional Troubleshooting Steps

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**.

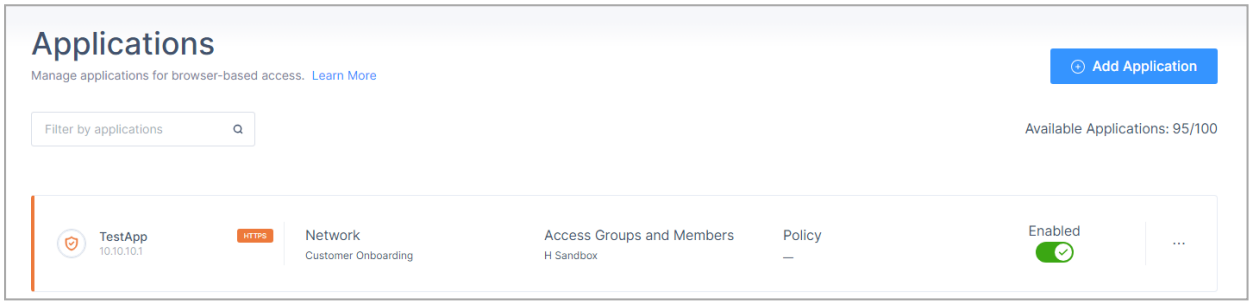
Adding a SSH Zero Trust Application

Prerequisite

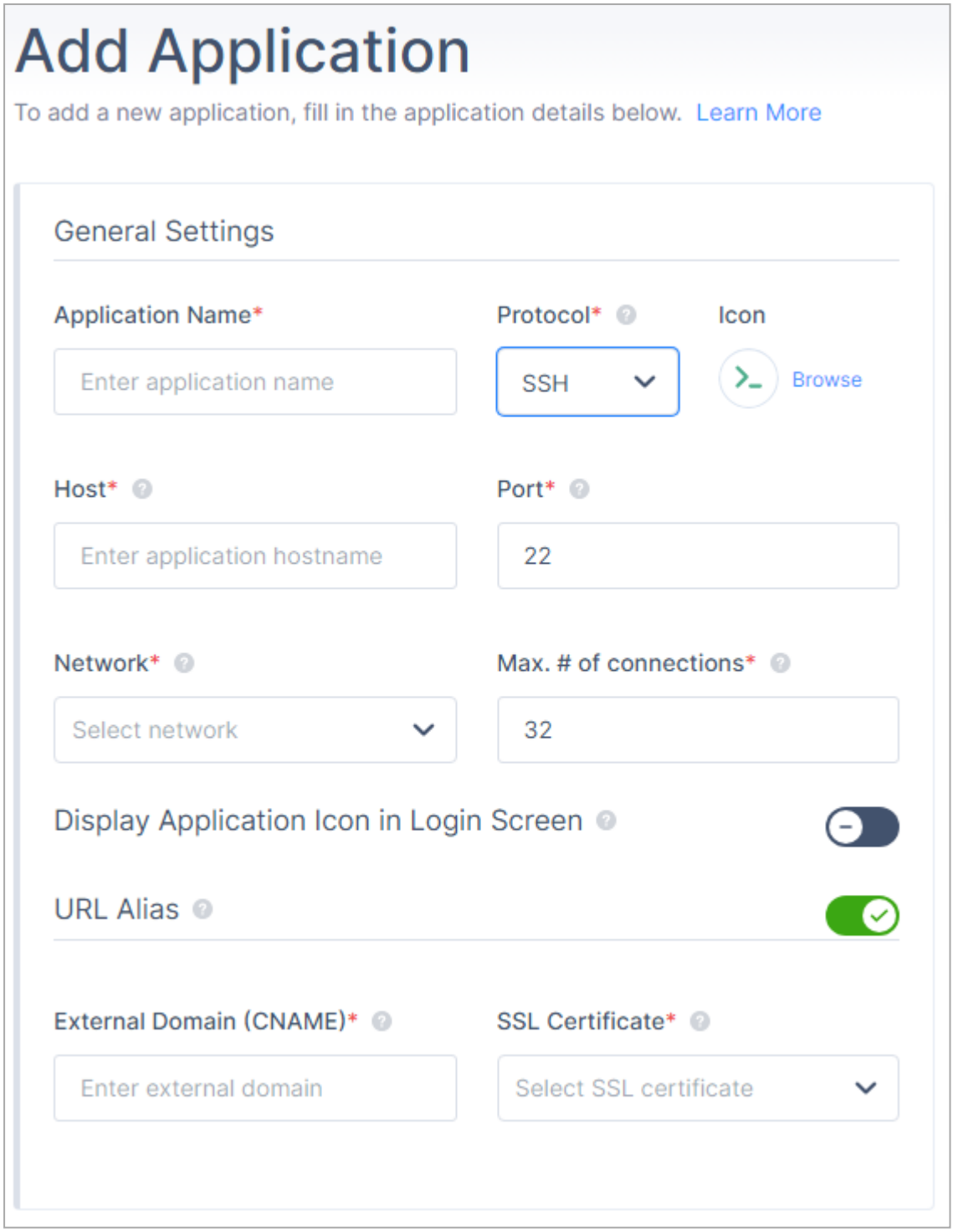
Make sure you have the credentials to access the application over SSH.

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.

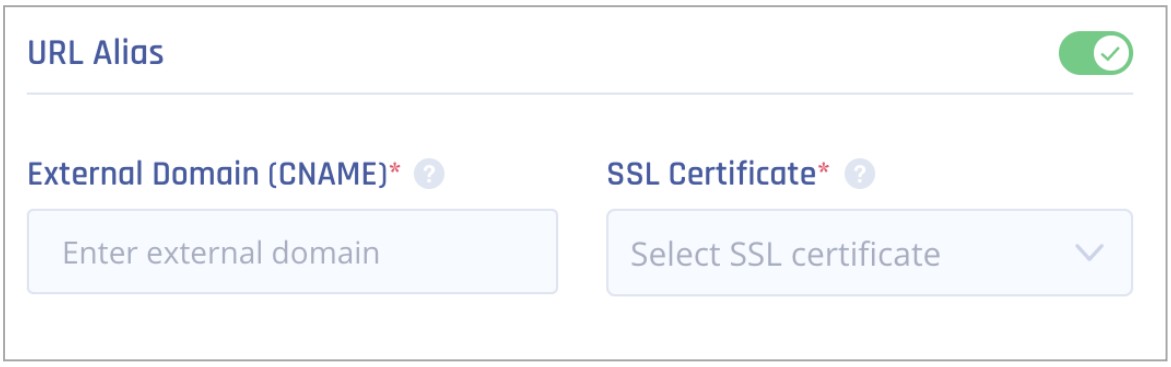
e. **Port** - 22

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.

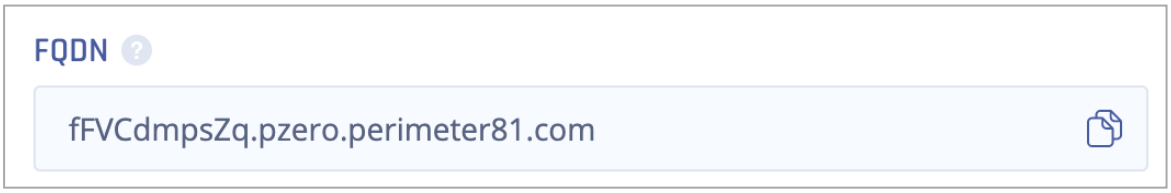


i. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

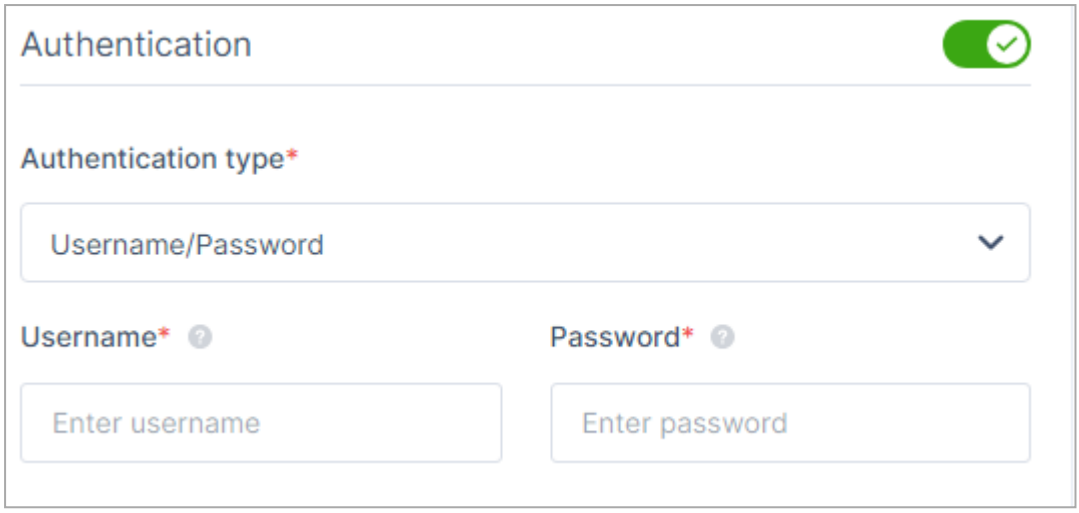
j. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

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

Under your domain, use the CNAME 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**:



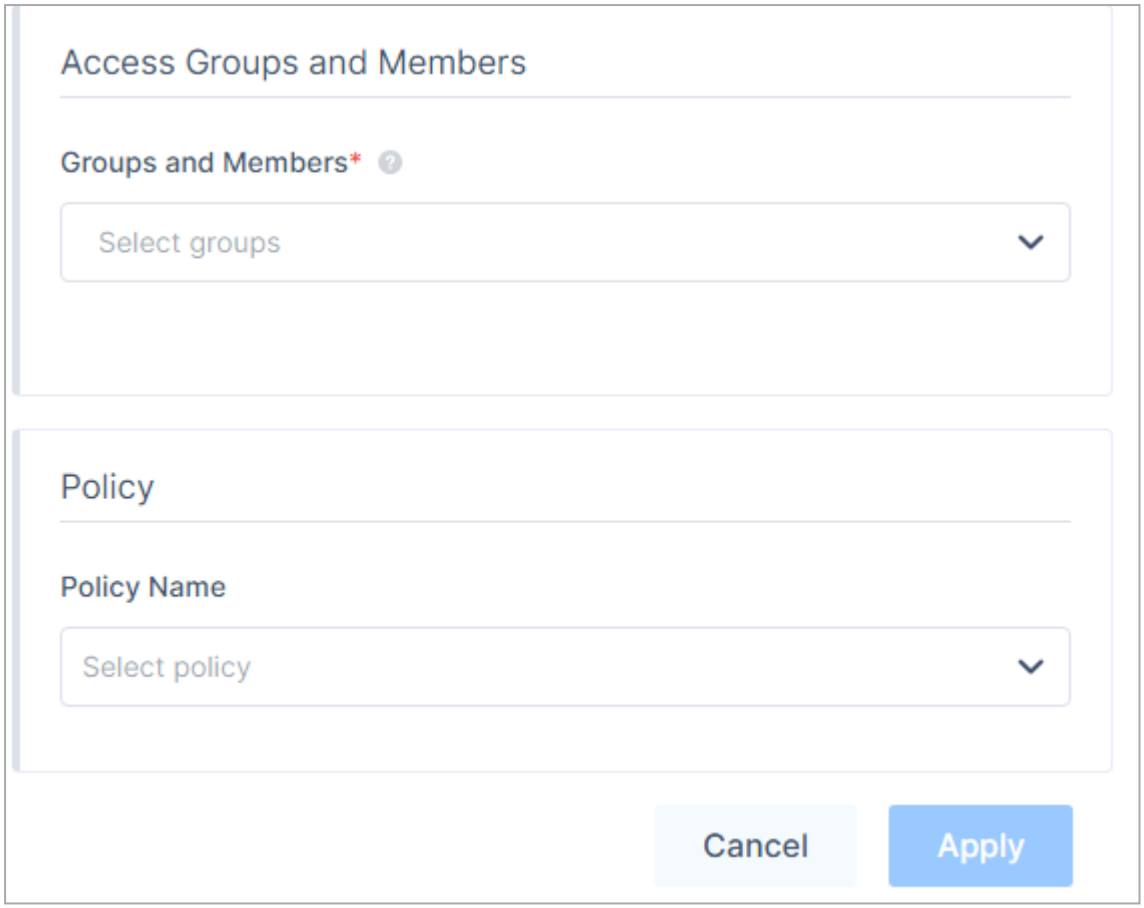
- For **Username/Password**, enter the username and password as predefined on the server.
- For **Private Key/Username/Passphrase**, enter these:
  a. **Username**: Username predefined on the server.
  b. **Private Key**: Your RSA-SSH key. Note that a certificate typically starts with a prefix and a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

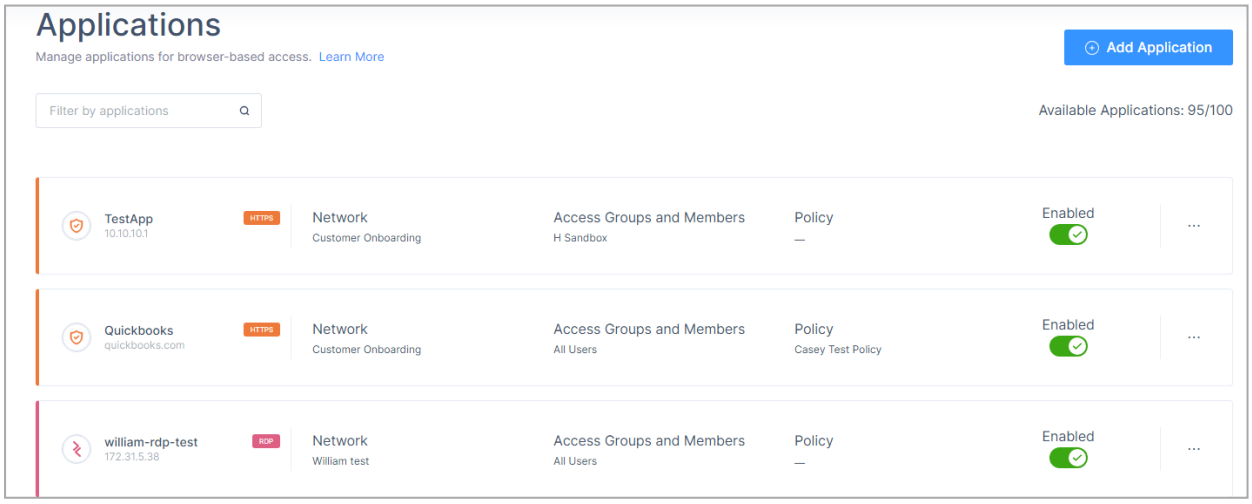
Note - If you disable **Authentication**, then the member must enter the credentials when accessing the machine.

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 *"Providing Application Access to Members" on page 636*.

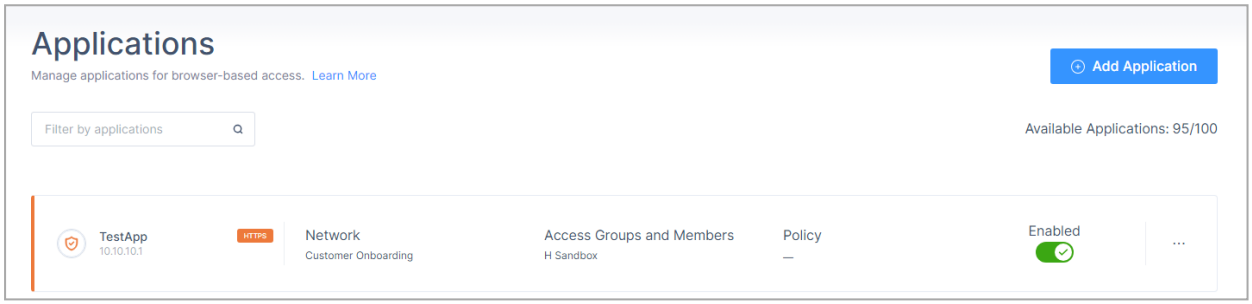
Adding a VNC Zero Trust Application

Prerequisite

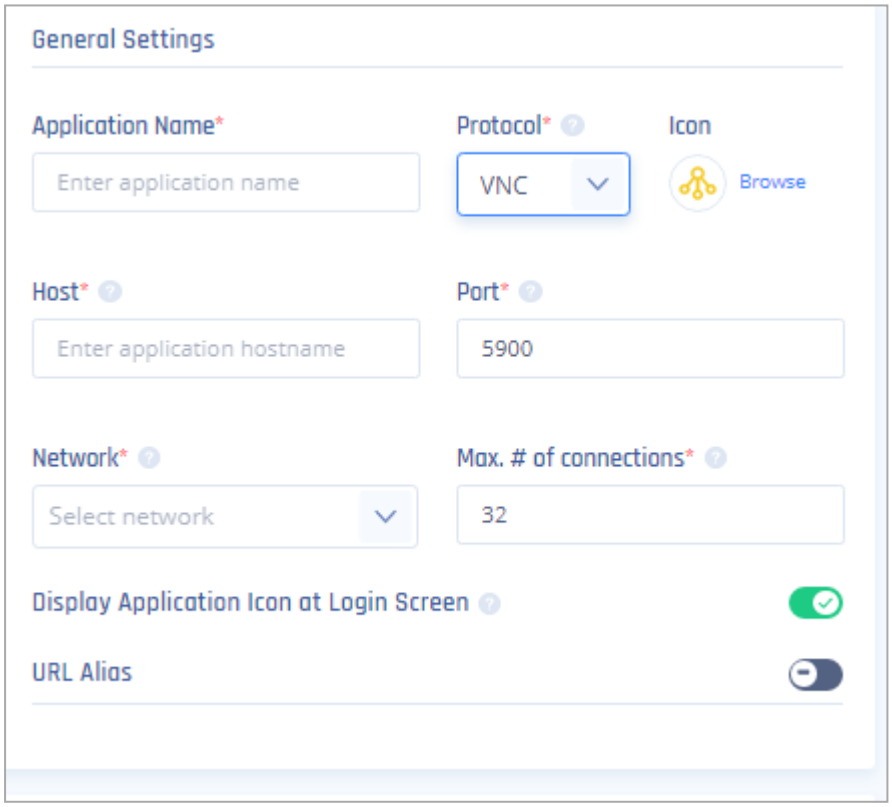
Make sure you have the credentials to access the application over VNC.

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.

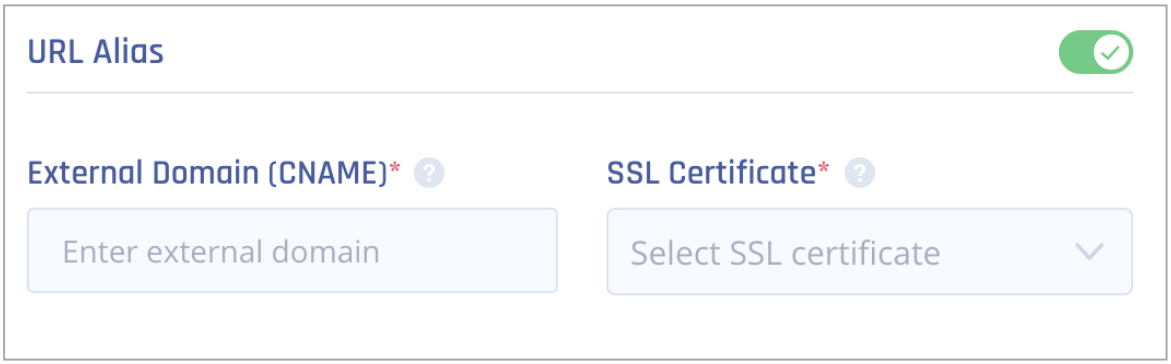
g. **Max number of connections**: 1

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.

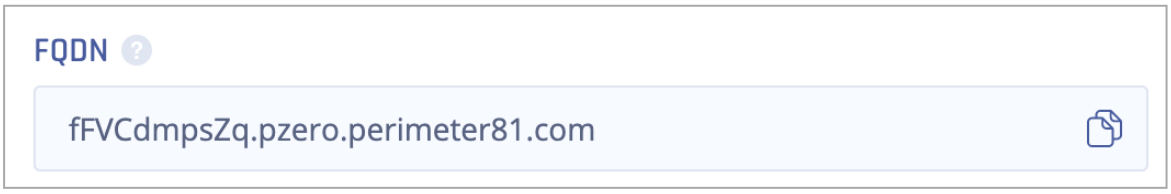


k. In the **External Domain (CNAME)** field, enter a CNAME associated with your domain.

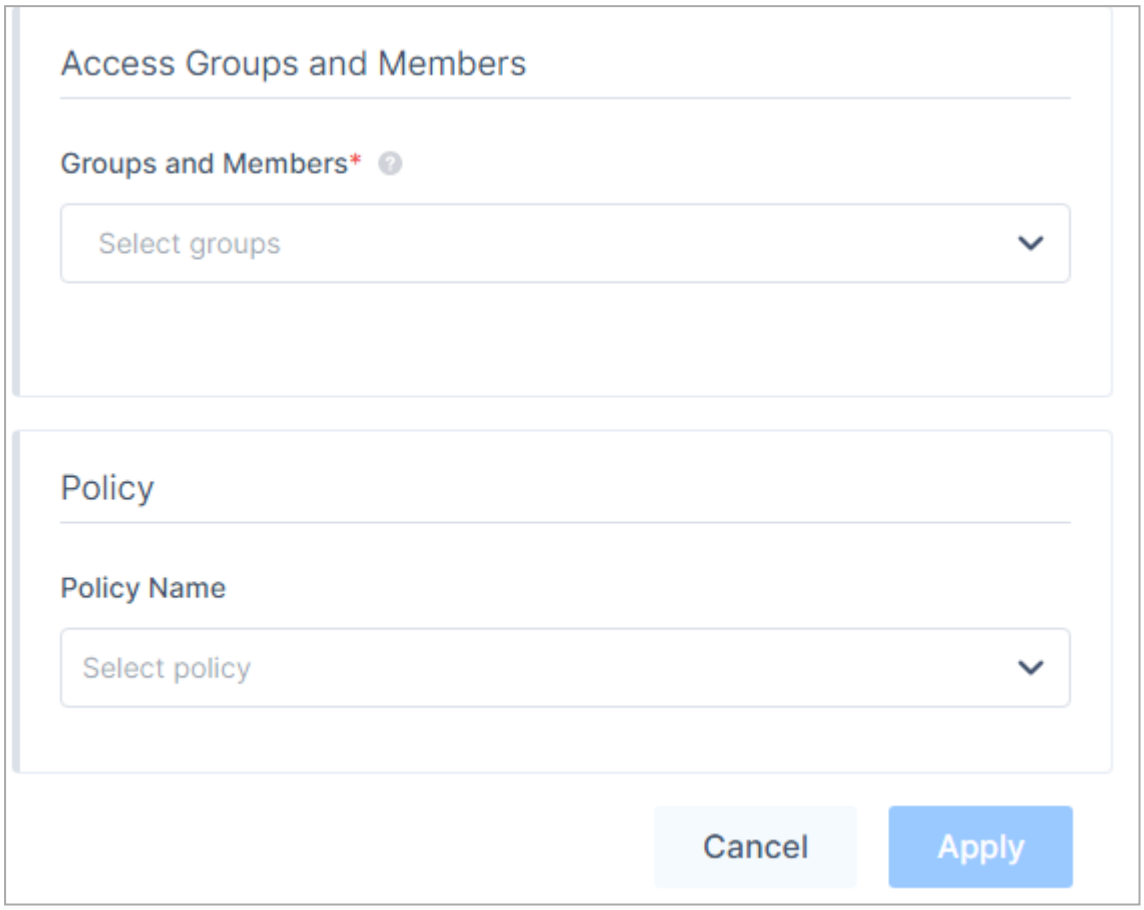
l. From the **SSL Certificate** list, select the application domain SSL certificate uploaded in Certificate Manager.

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

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

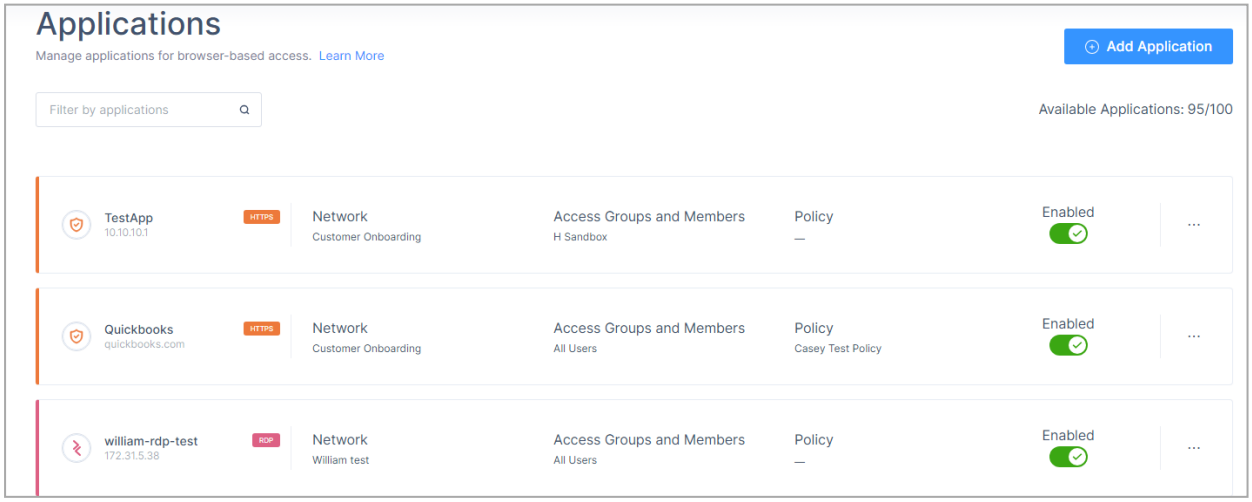


4. In the **Authentication** section, in the **Password** field, enter the password predefined in your VNC.
5. In the **Access Groups and Members** section, in the **Groups and Members** list, select the member groups that can access the application.



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

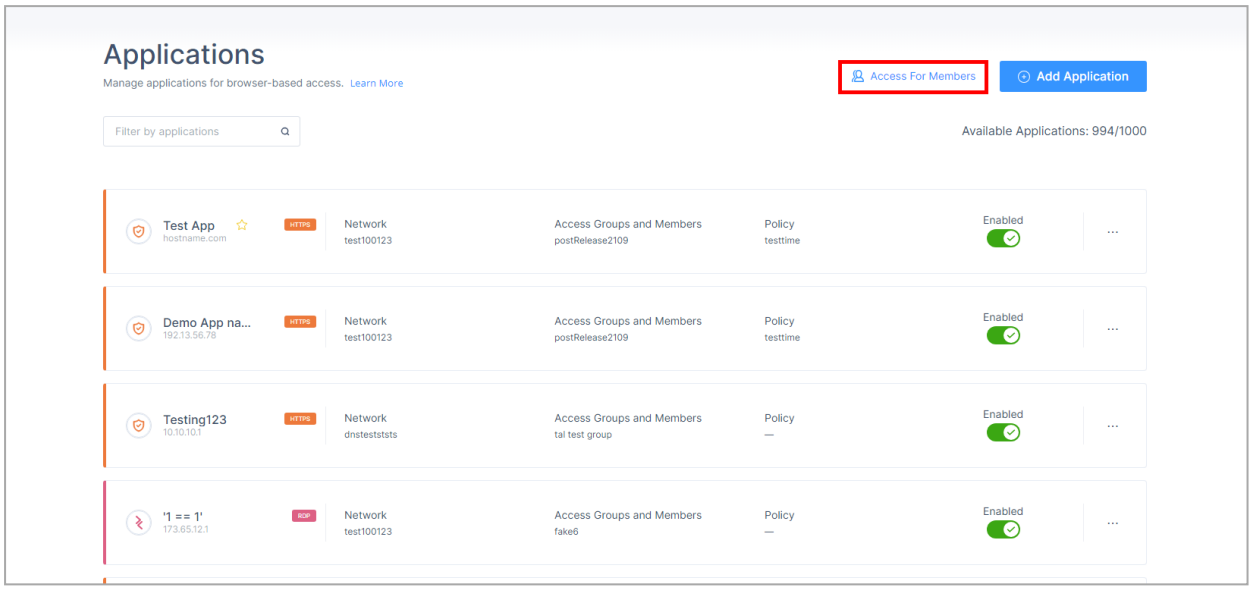
   The system lists the application in the **Applications** page and enables it by default.



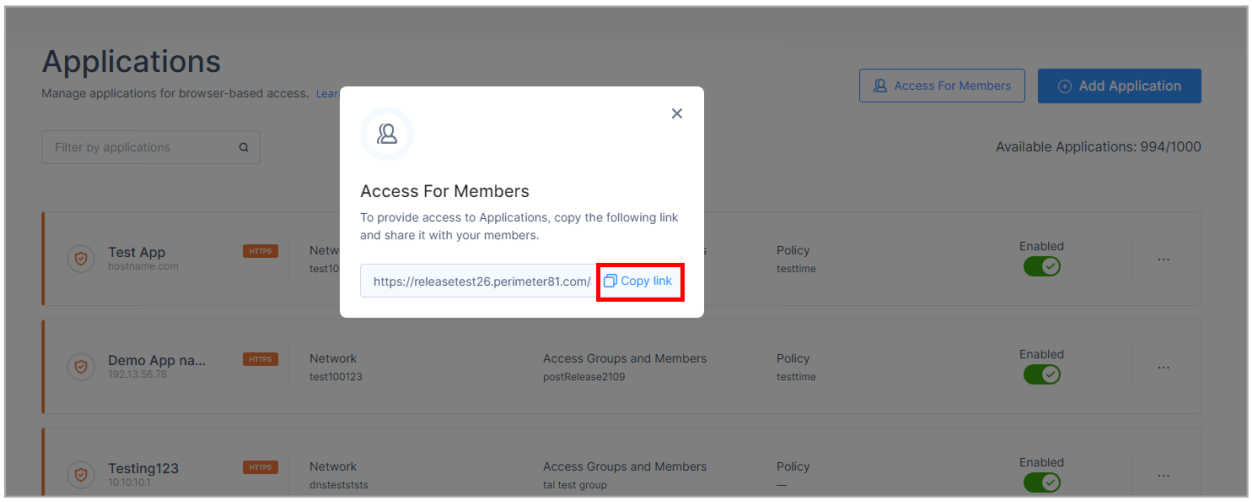
8. For members to access the application, see *"Providing Application Access to Members" on page 636*.

Providing Application Access to Members

1. On the **Applications** page, click **Access For Members**.

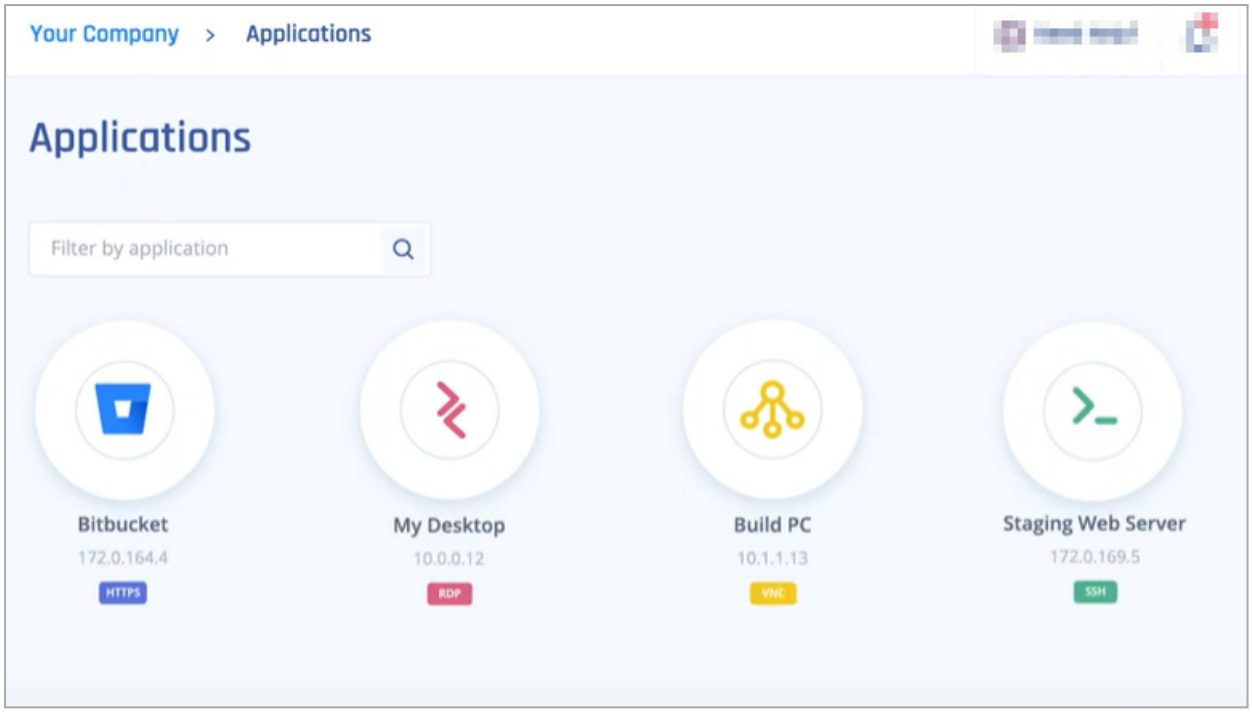


2. Click **Copy link**. Share this link with your members.



3. Member needs to log in to the Harmony SASE portal using the above link.

   After logging in to the portal, the member can view the list of authorized applications.

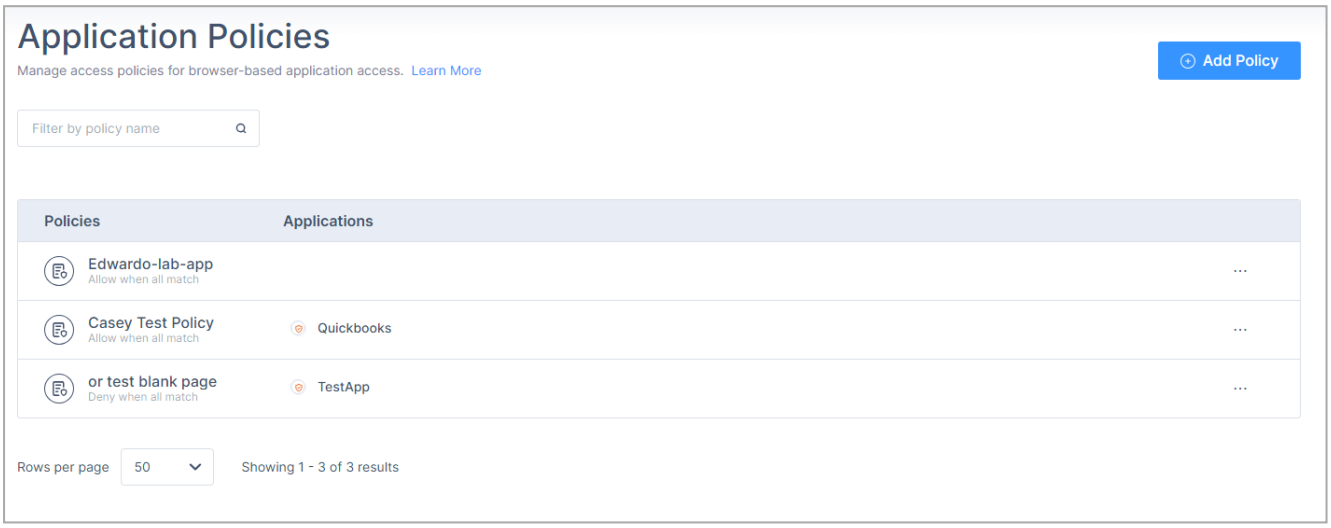


4. Click the application to access it.

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**.



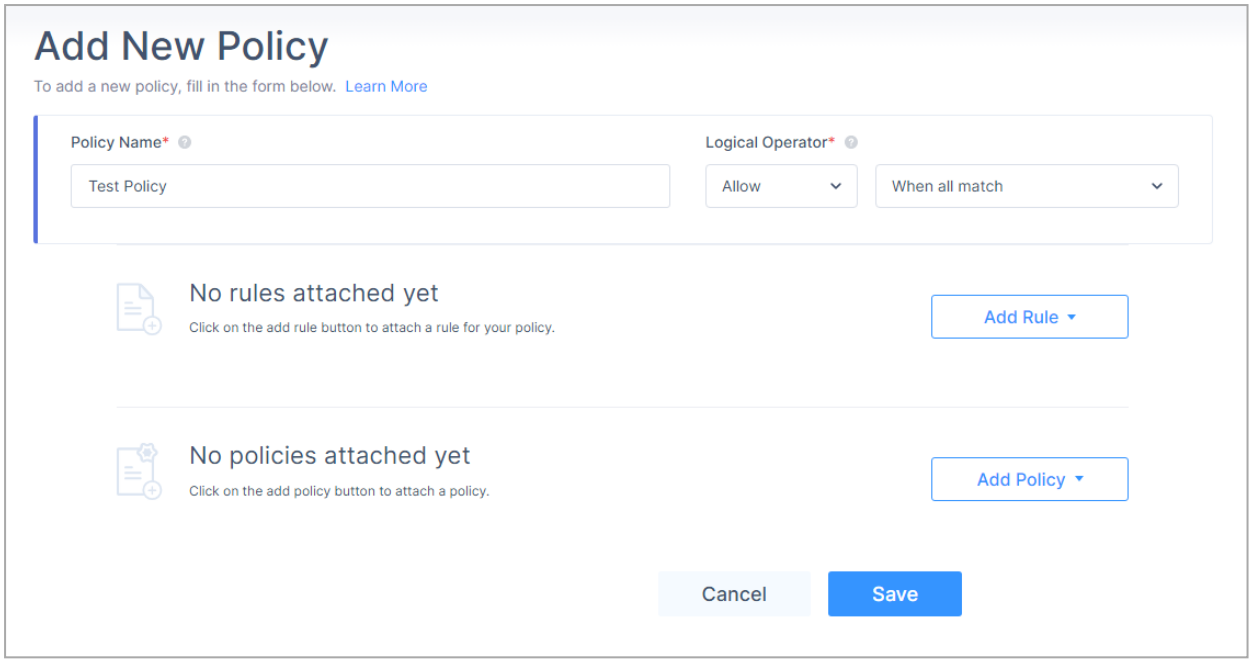
Best Practices -

- 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

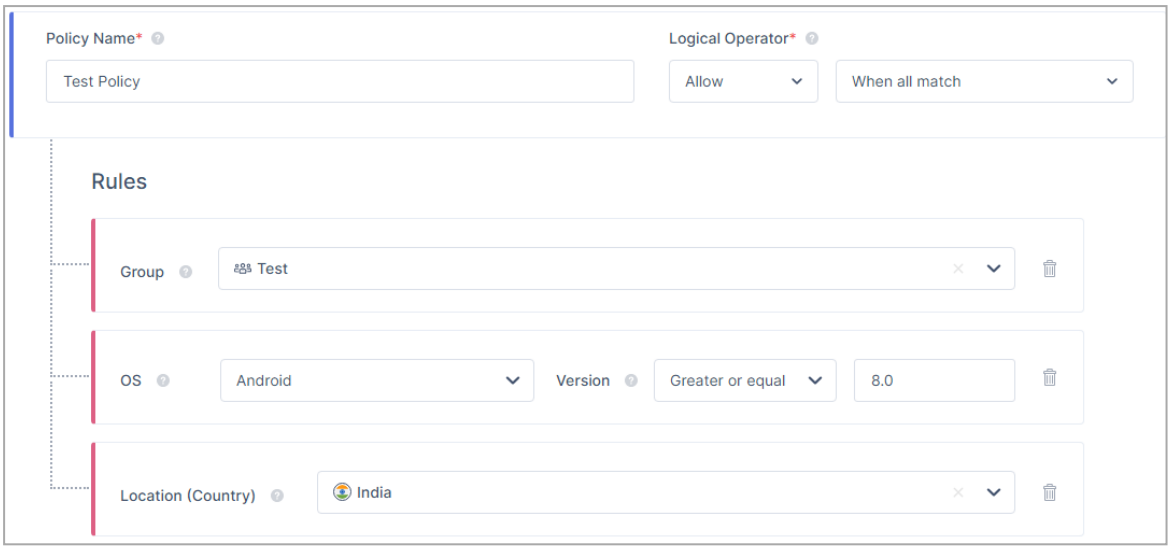
1. Access the Harmony SASE Administrator Portal and click **Private Access** > **Application Policies**.
2. Click **Add Policy**.

   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

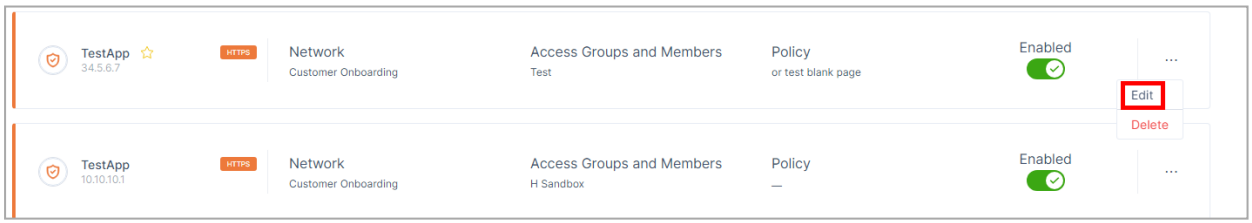


5. To attach an existing policy with the new policy, click **Add Policy** and select a policy.
6. Click **Save**.

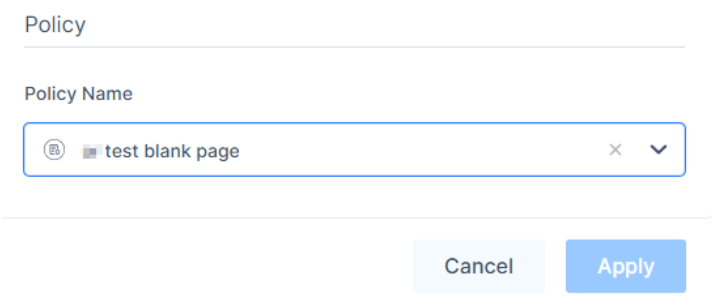
The new policy is listed in your **Policy** page.

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:

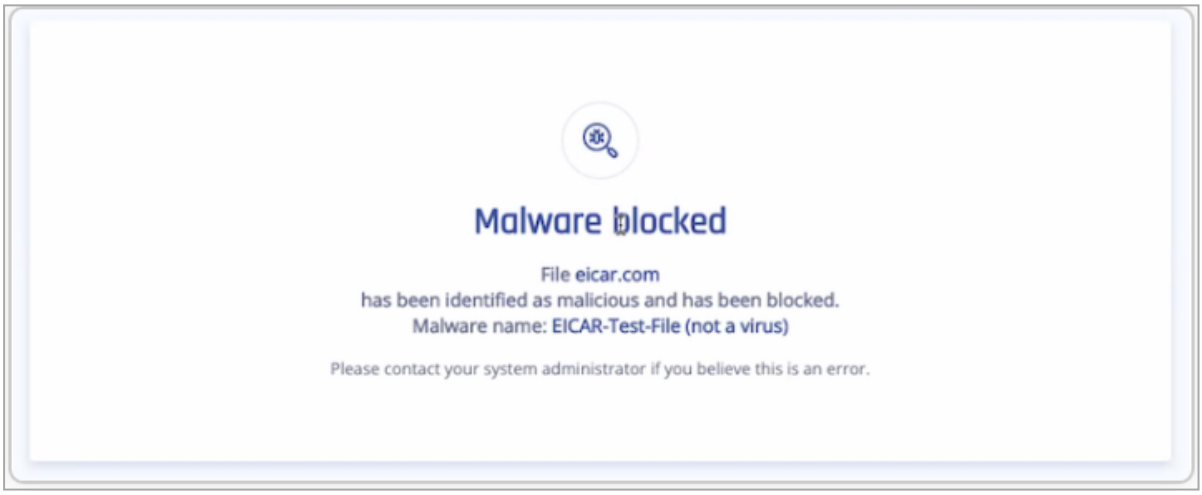
- *"Web Filter Rules" on page 642*
- *Bypass Rules*

The *"Web Filter Rules" on page 642* 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 642*.
2. (Optional) Configure bypass rules. See *"Bypass Rules" on page 649*.
   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 658*.

Web Filter Rules

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

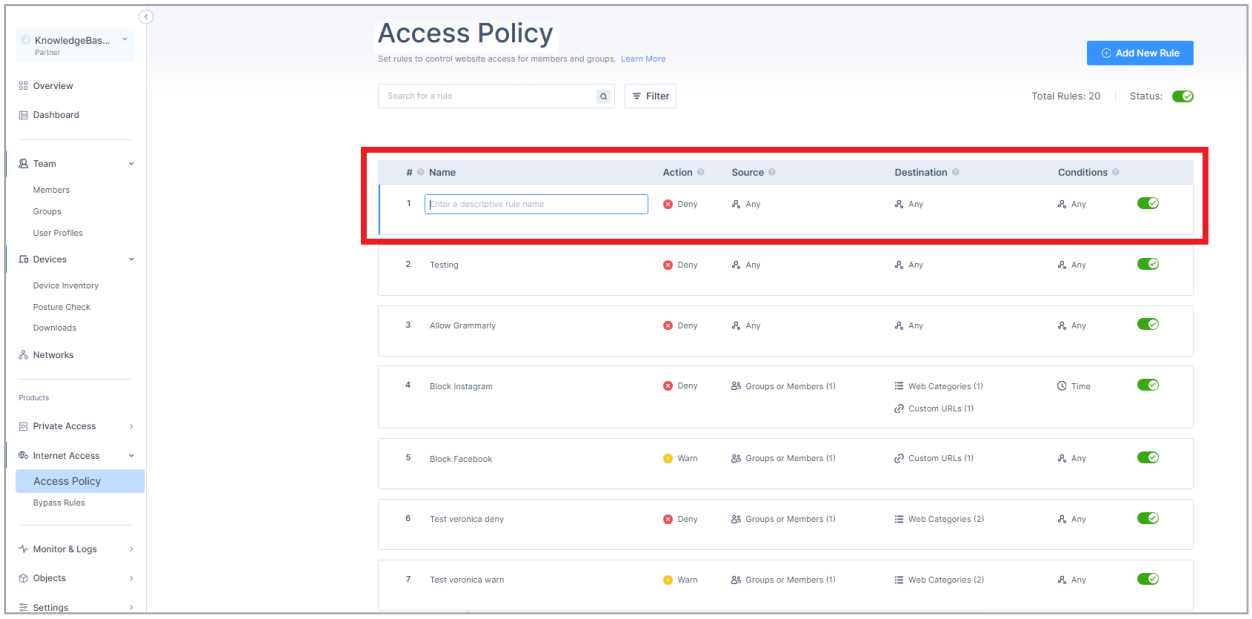
To view the **Web Filter Rules** page, access the Harmony SASE Administrator Portal and click **Internet Access** > **Web Filter Rules**.

Column	Description
Name	Name of the Rule.
Action	Action for web traffic: ▪ **Deny** - Blocks web traffic. ▪ **Allow** - Permits web traffic. ▪ **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 Rules

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

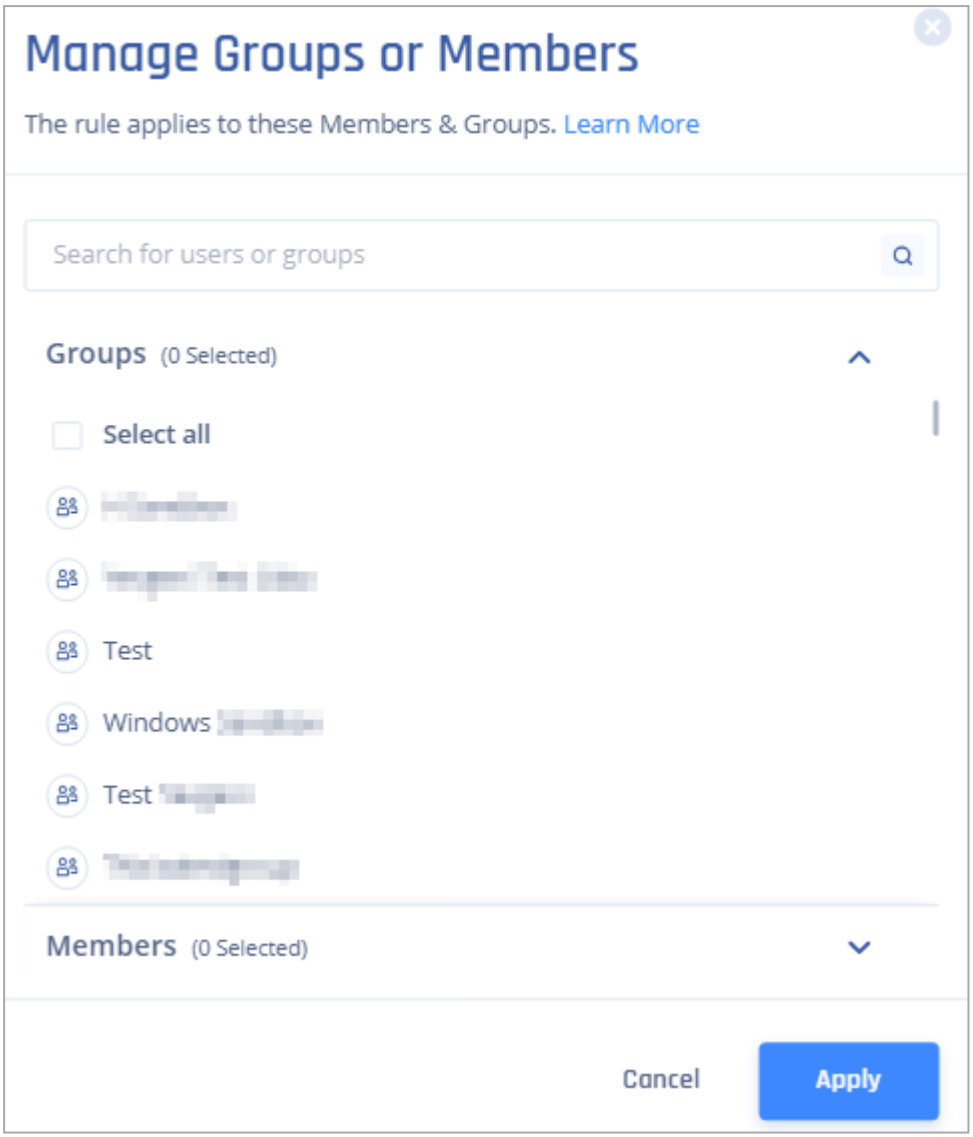
   A new rule appears in the table.



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.

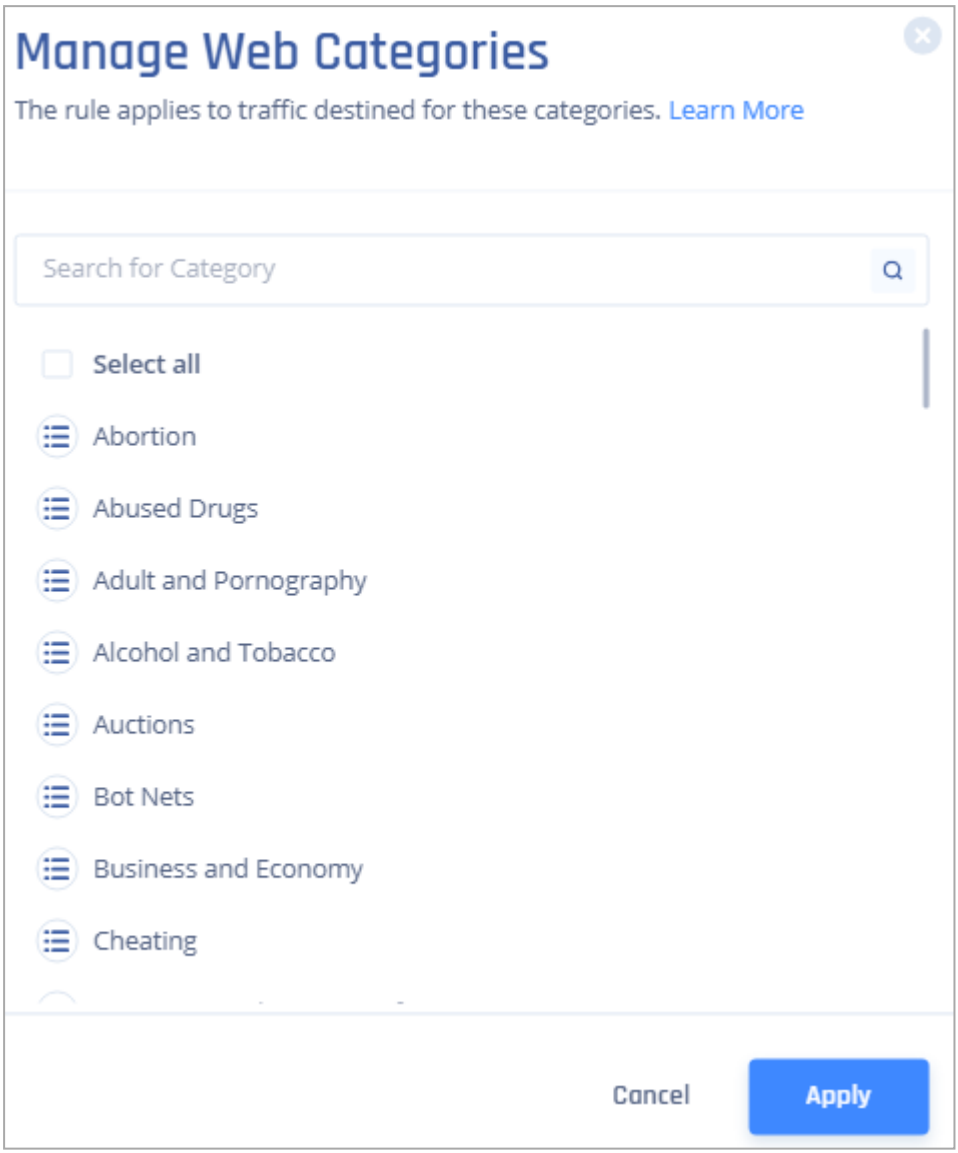
c. Click **Apply**.

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.

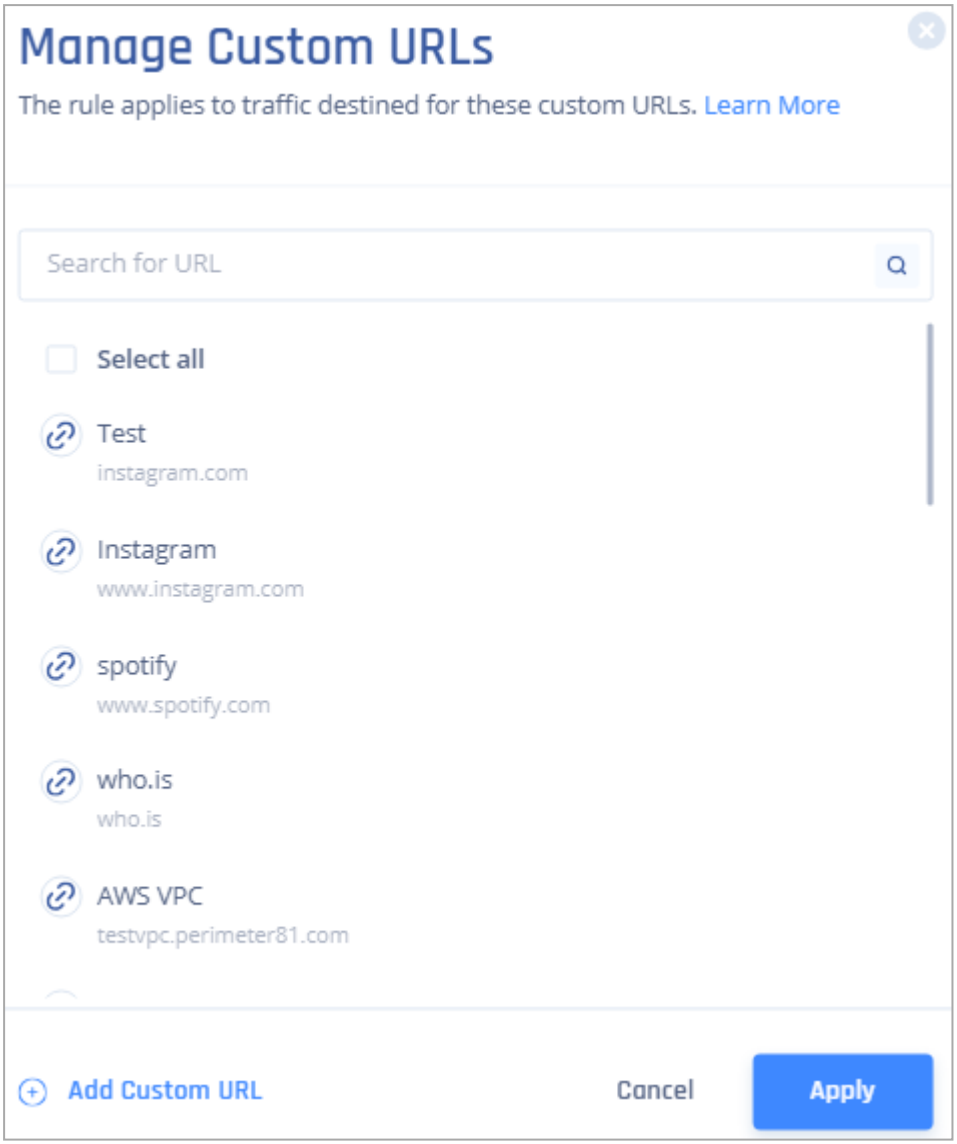


c. Select the categories from the list.

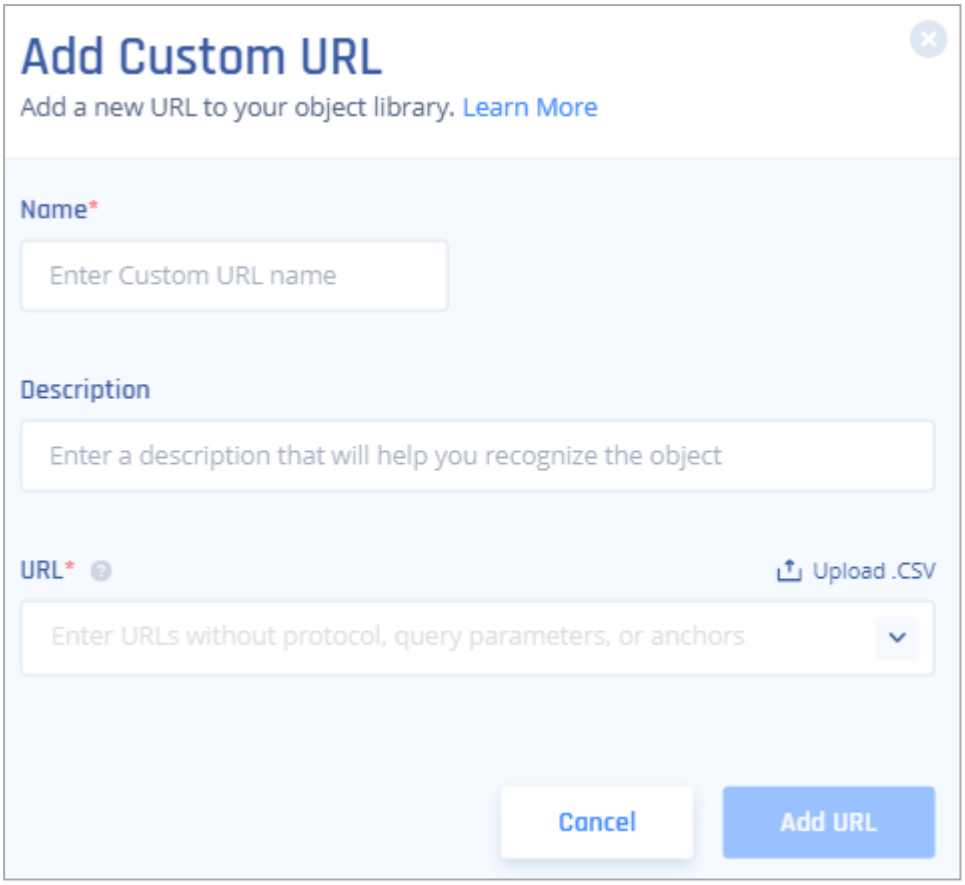
d. Click **Apply**.

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**

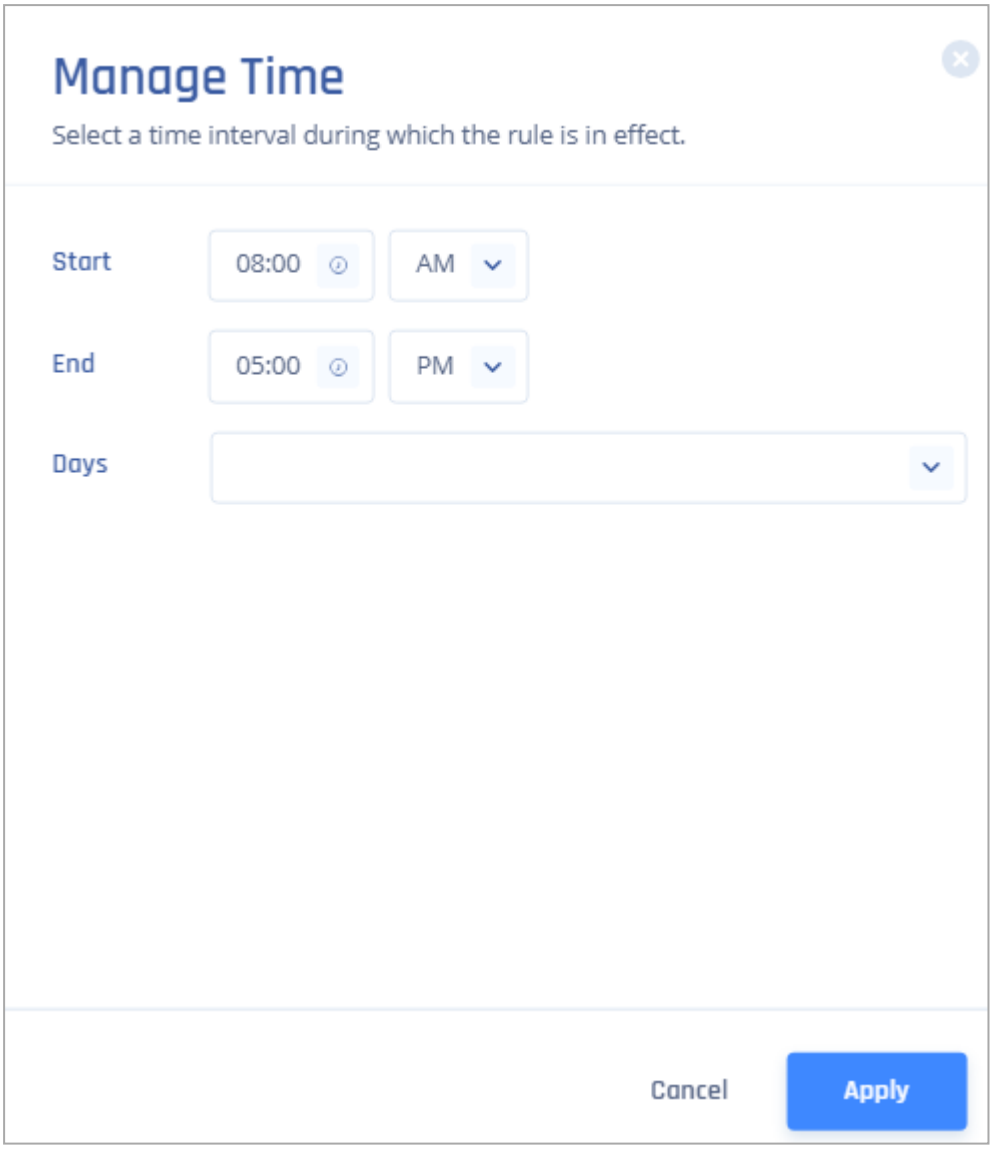
Optionally, click **Upload .CSV** to upload a .csv file with list of URLs.

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.

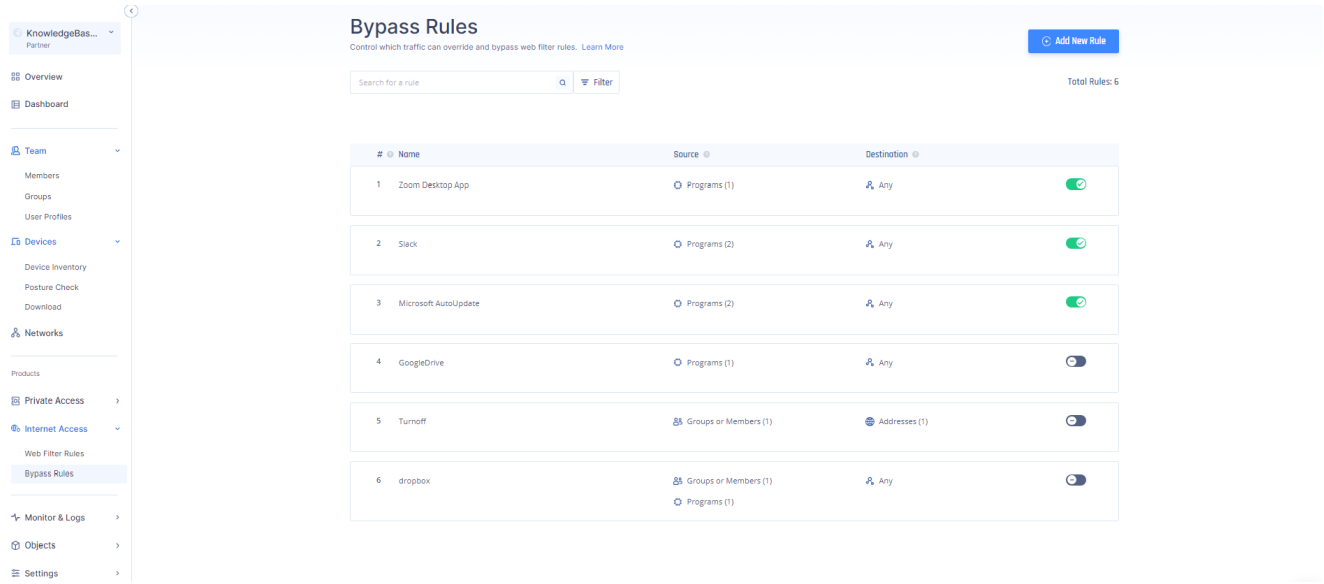
9. Click **Apply** in the bottom of the page.

10. Click **Apply**.

Bypass Rules

The **Bypass Rules** page allows you to specify traffic that must be ignored by the *"Web Filter Rules" on page 642*.

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

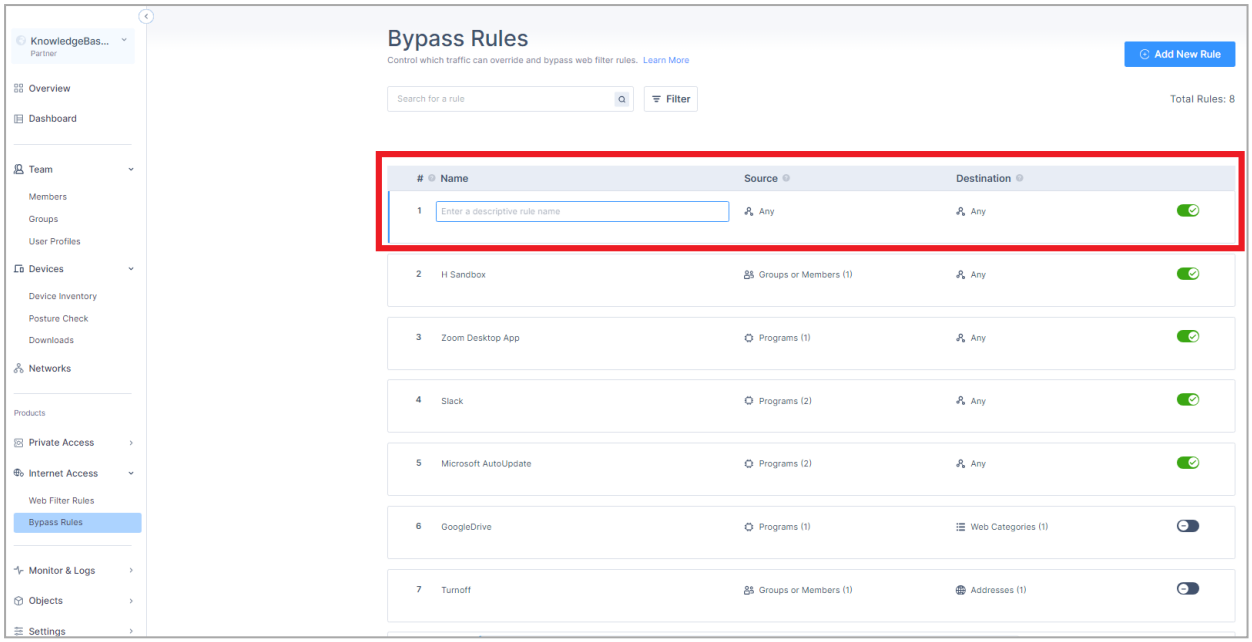


Column	Description
Name	Name of the rule.
Source	Programs, groups or members to which the bypass rule is applied.
Destination	Destination of the web traffic.

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.

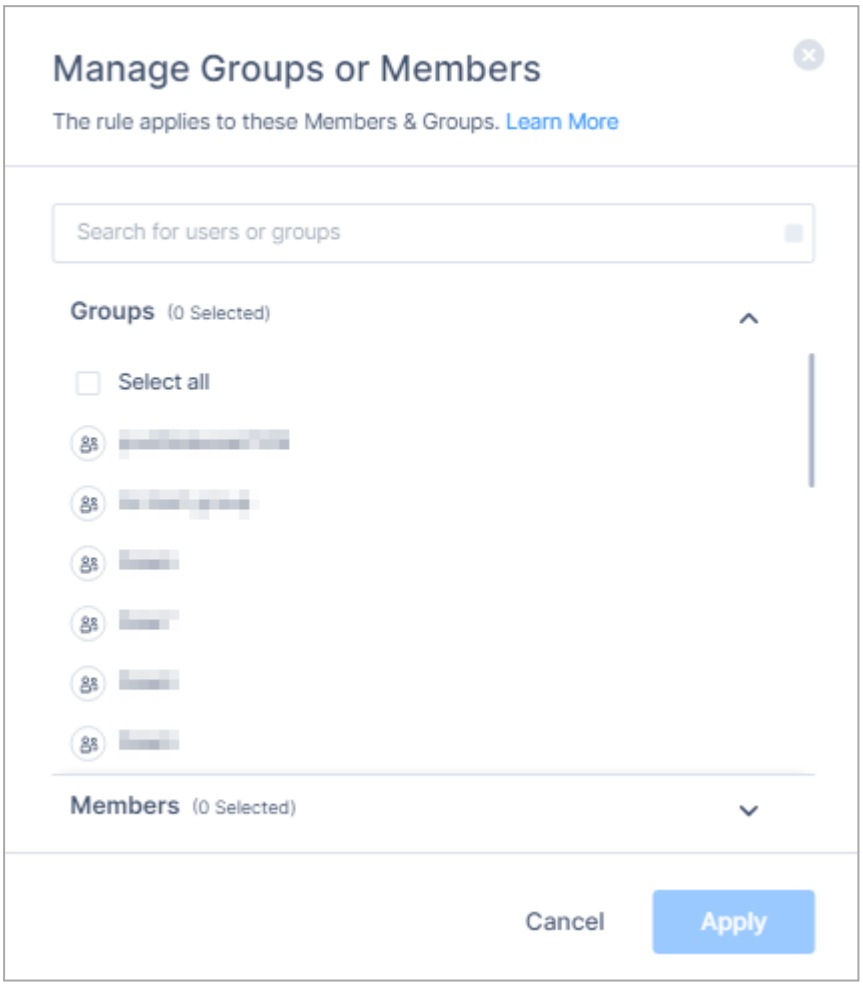


3. In the **Name** field, enter a name for the rule.
4. In the **Source** field, add user or group list to which you want to apply the rule. Default is **Any**.

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

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

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

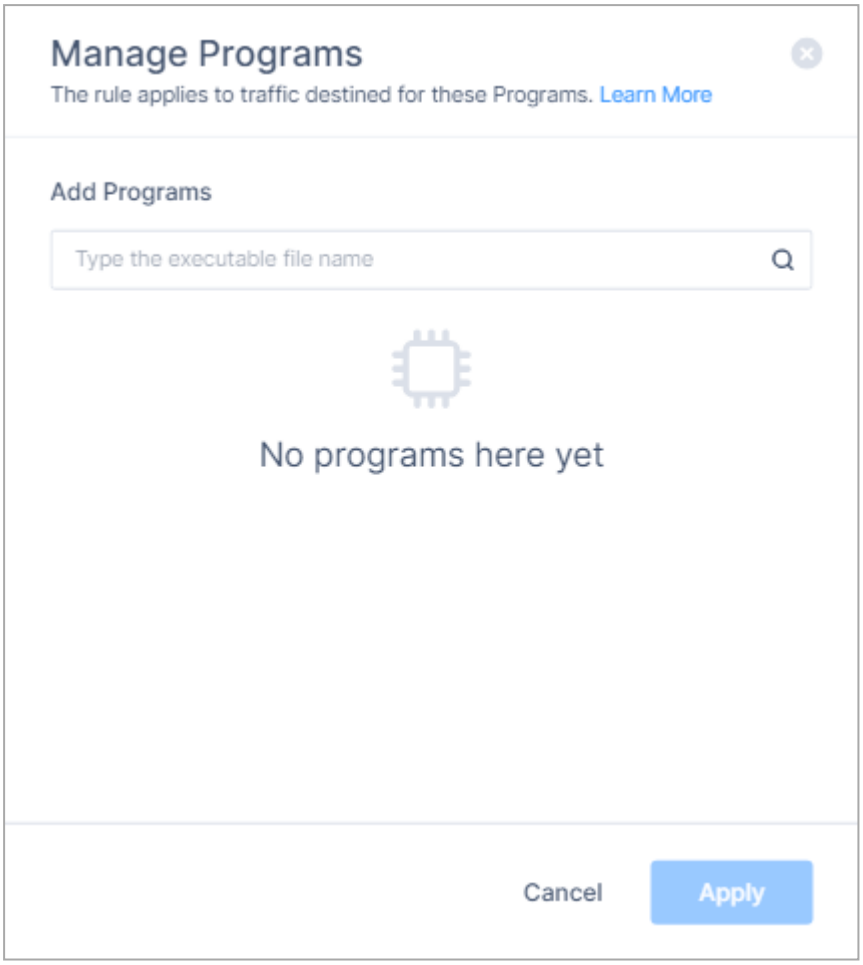


c. Select group(s) or member(s) from the list.

d. Click **Apply**.

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

The **Manage Programs** window appears.



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

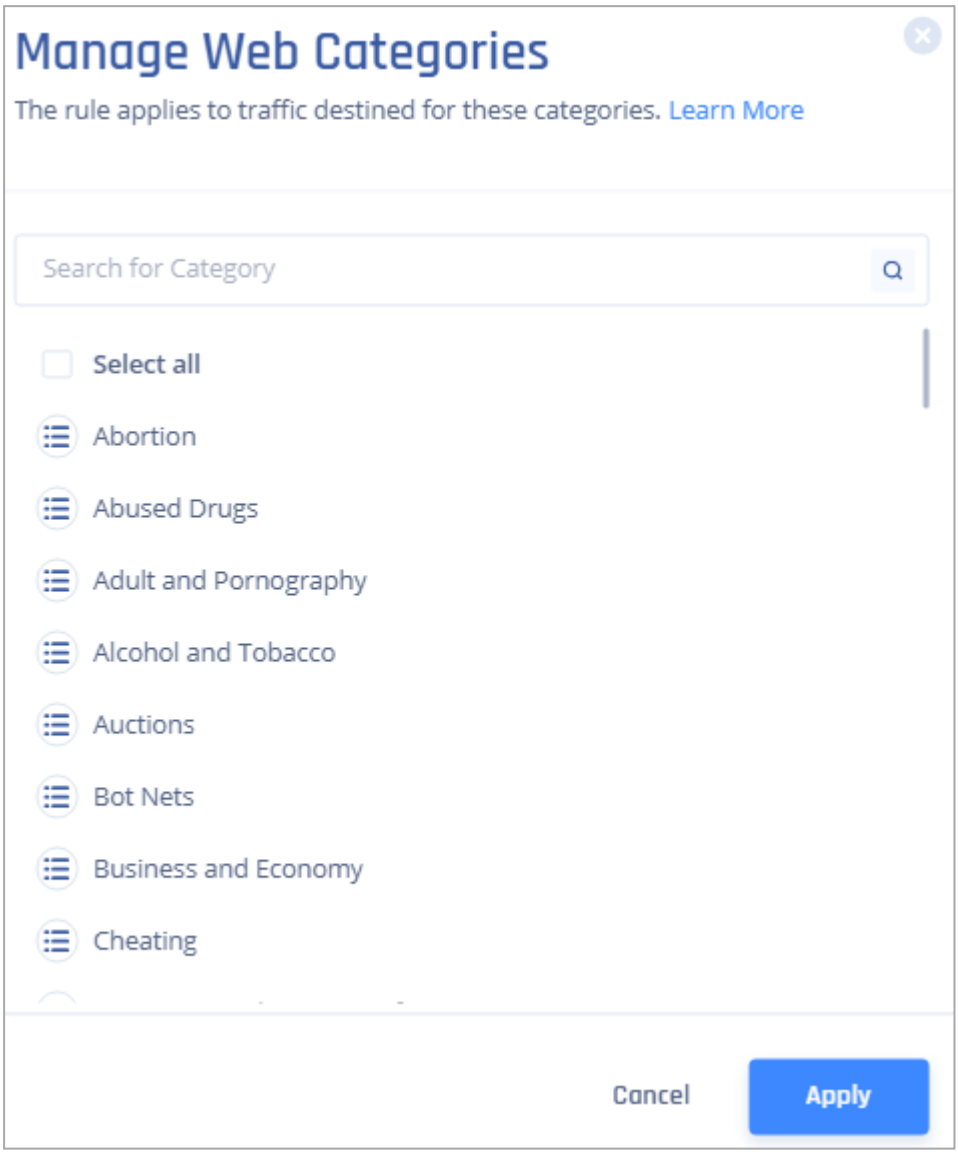
g. Click **Apply**.

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.

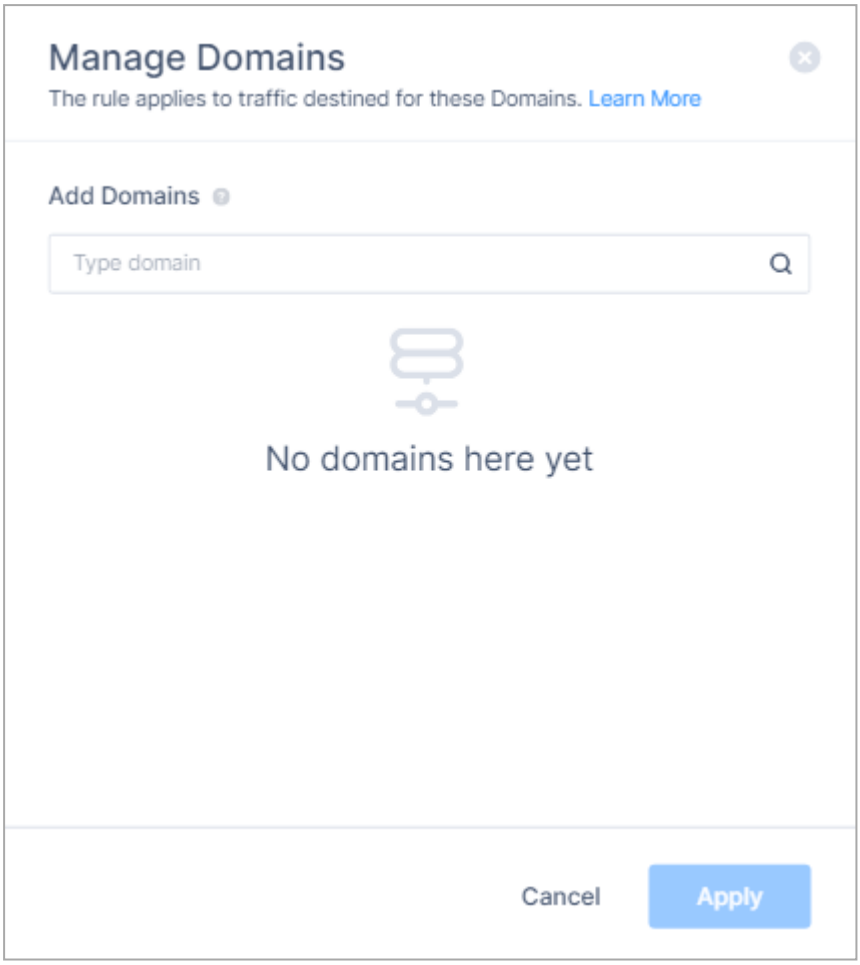


c. Select the categories from the list.

d. Click **Apply**.

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

The **Manage Domains** window appears.

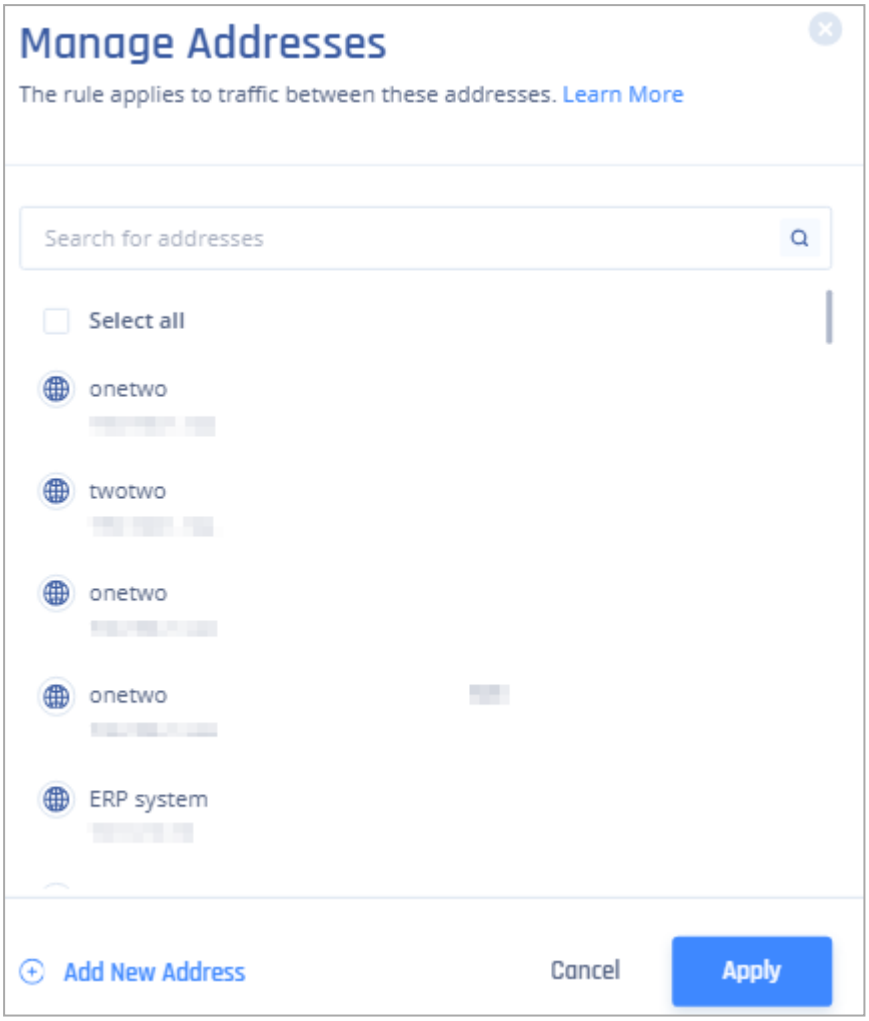


f. Enter the domain name and press **Enter**. For example, `google.com`.

g. Click **Apply**.

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

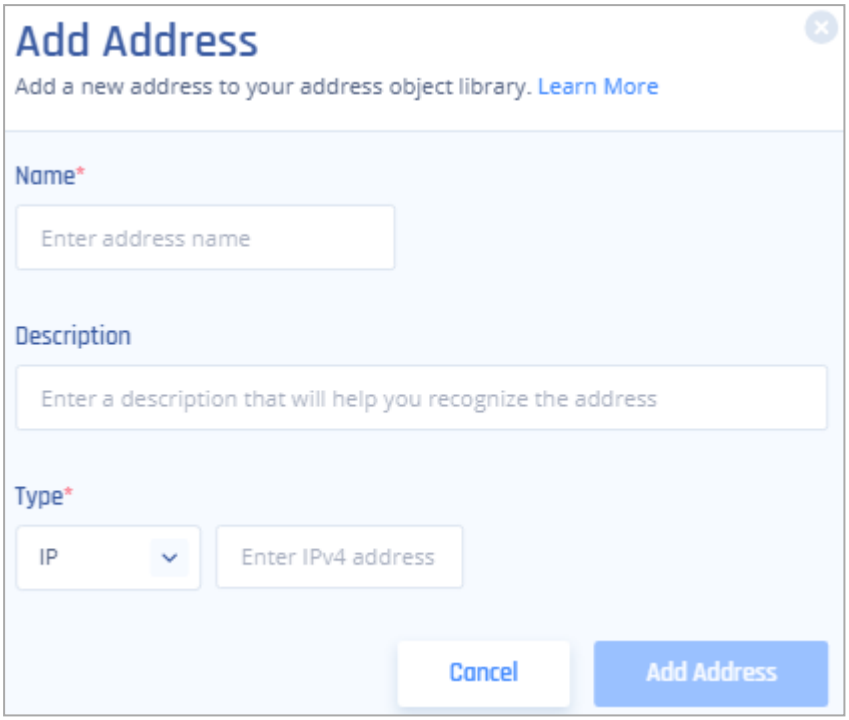
The **Manage Addresses** window appears.



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.

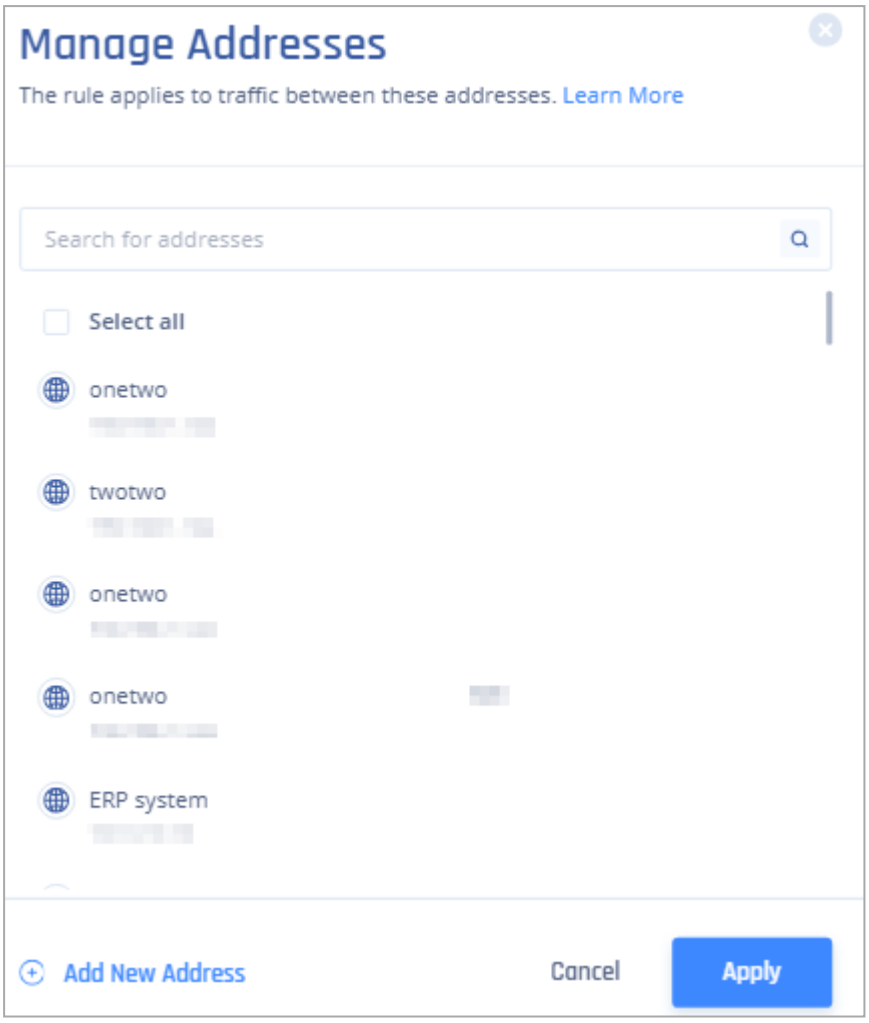
l. In the **Description** field, enter a description.

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: ▪ List 1 ▪ List 2
Apple's iMessages, iTunes, App Store, Mail	N/A	▪ p24-keyvalueservice.icloud.com ▪ apps.apple.com ▪ itunes.apple.com ▪ mzstatic.com ▪ gs-loc.apple.com ▪ gsa.apple.com ▪ securemetrics.apple.com ▪ swscan.apple.com ▪ xp.apple.com ▪ icloud.com ▪ ppq.apple.com ▪ akadns.net

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

Application	Program	Domain
Google Services	N/A	▪ accounts.google.com ▪ alt2-mtalk.google.com ▪ android.clients.google.com ▪ www.google.com ▪ android.googleapis.com ▪ cryptauthenrollment.googleapis.com ▪ device-provisioning.googleapis.com ▪ digitalassetlinks.googleapis.com ▪ fcmconnection.googleapis.com ▪ fcmtoken.googleapis.com ▪ firebaseperusertopics-pa.googleapis.com ▪ play.googleapis.com ▪ semanticlocation-pa.googleapis.com ▪ lh3.googleusercontent.com ▪ play-lh.googleusercontent.com ▪ gstatic.com ▪ gvt1.com
Java Updates	N/A	▪ sjremetrics.java.com ▪ 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 ▪ az801095.vo.msecnd.net ▪ i.s-microsoft.com
Microsoft Office365	Configure within Office365: Go to **Policy** > **URL & Cloud App Control** > **Advanced Settings**.	For outlook, add these domains: ▪ office365.com ▪ office.com

Application	Program	Domain
Microsoft OneDrive	N/A	▪ cdn.funcaptcha.com ▪ fpt.live.com ▪ login.live.com ▪ odc.officeapps.live.com ▪ skyapi.policies.live.net ▪ signup.live.com ▪ skyapi.live.net ▪ pipe.aria.microsoft.com ▪ data.microsoft.com ▪ svc.ms ▪ msauth.net ▪ onedrive.com ▪ cdn.onenote.net
Microsoft Windows Store	N/A	▪ eus-streaming-video-msn-com ▪ wns.windows.com ▪ live.com ▪ clientconfig.passport.net ▪ wustat.windows.com ▪ windowsupdate.com ▪ msftncsi.com ▪ microsoft.com
Microsoft Updates	N/A	▪ login.live.com ▪ settings-win.data.microsoft.com ▪ vortex-win.data.microsoft.com ▪ delivery.mp.microsoft.com ▪ tsfe.trafficshaping.dsp.mp.microsoft.com ▪ update.microsoft.com ▪ sls.update.microsoft.com login.microsoft.com
Slack	▪ **Windows** - slack.exe ▪ **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 **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 ▪ settings-win.data.microsoft.com ▪ vortex-win.data.microsoft.com ▪ delivery.mp.microsoft.com ▪ tsfe.trafficshaping.dsp.mp.microsoft.com ▪ update.microsoft.com ▪ sls.update.microsoft.com ▪ login.microsoft.com	N/A
Bypass Adobe updates - Pre-configured	Enabled	▪ adobe.com ▪ adobetag.com	N/A

Rule Name	Default Status	Domains	Categories
Bypass Java updates - Pre-configured	Enabled	▪ sjremetrics.java.com ▪ 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 ▪ docs.aws.amazon.com ▪ signin.aws.amazon.com ▪ signin.aws.amazon.com ▪ fls-na.amazon.com ▪ cdn.assets.as2.amazonaws.com ▪ aws-signin-website-assets.s3.amazonaws.com ▪ opfcaptcha-prod.s3.amazonaws.com ▪ d1dgtfo2wk29o4.cloudfront.net ▪ Images-na.ssl-images-amazon.com	N/A
Bypass Dropbox - Pre-configured	Enabled	▪ dropbox.com ▪ dropboxapi.com ▪ previews.dropboxusercontent.com ▪ mmp.getdropbox.com	N/A

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

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

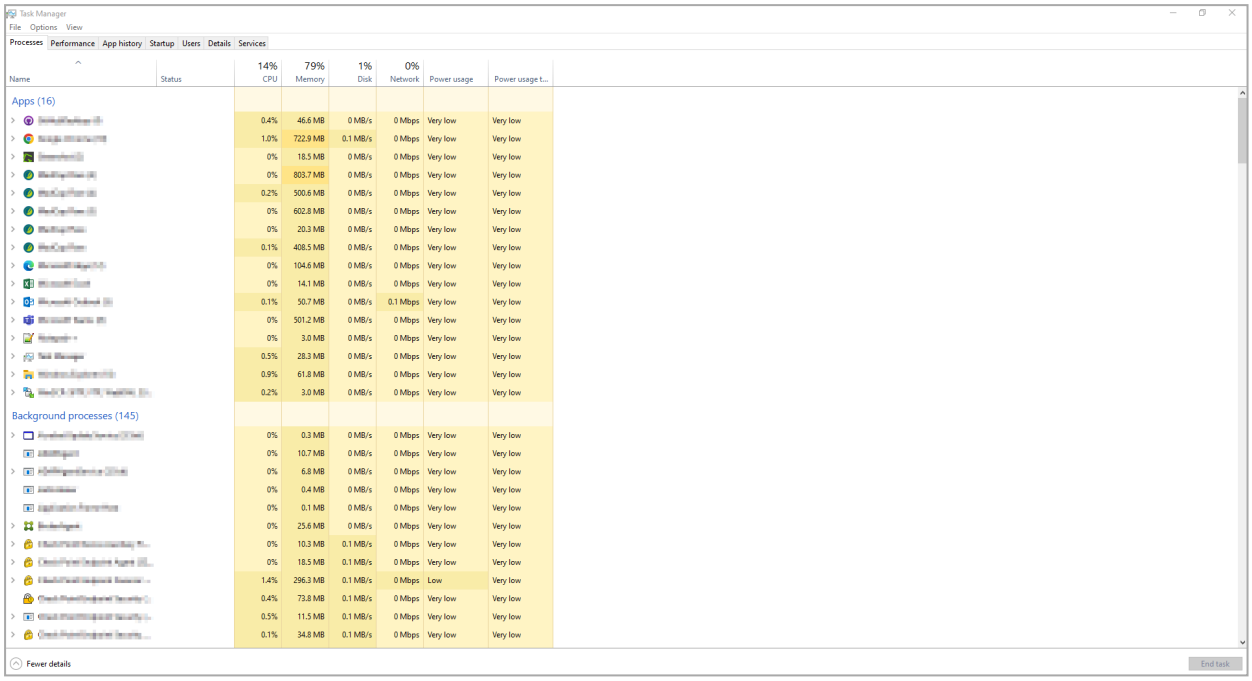
Rule Name	Default Status	Domains	Categories
Bypass Apple services - Pre-configured	Enabled	▪ p24-keyvalueservice.icloud.com ▪ apps.apple.com ▪ itunes.apple.com ▪ mzstatic.com ▪ gs-loc.apple.com ▪ gsa.apple.com ▪ securemetrics.apple.com ▪ swscan.apple.com ▪ xp.apple.com ▪ icloud.com ▪ ppq.apple.com ▪ akadns.net ▪ mail.me.com ▪ music.apple.com	N/A
Bypass Bitdefender services - Pre-configured	Enabled	▪ cdn.bitdefender.net ▪ download.bitdefender.com ▪ login.bitdefender.net ▪ login.bitdefender.com ▪ nimbus.bitdefender.net ▪ push.bitdefender.net ▪ 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.

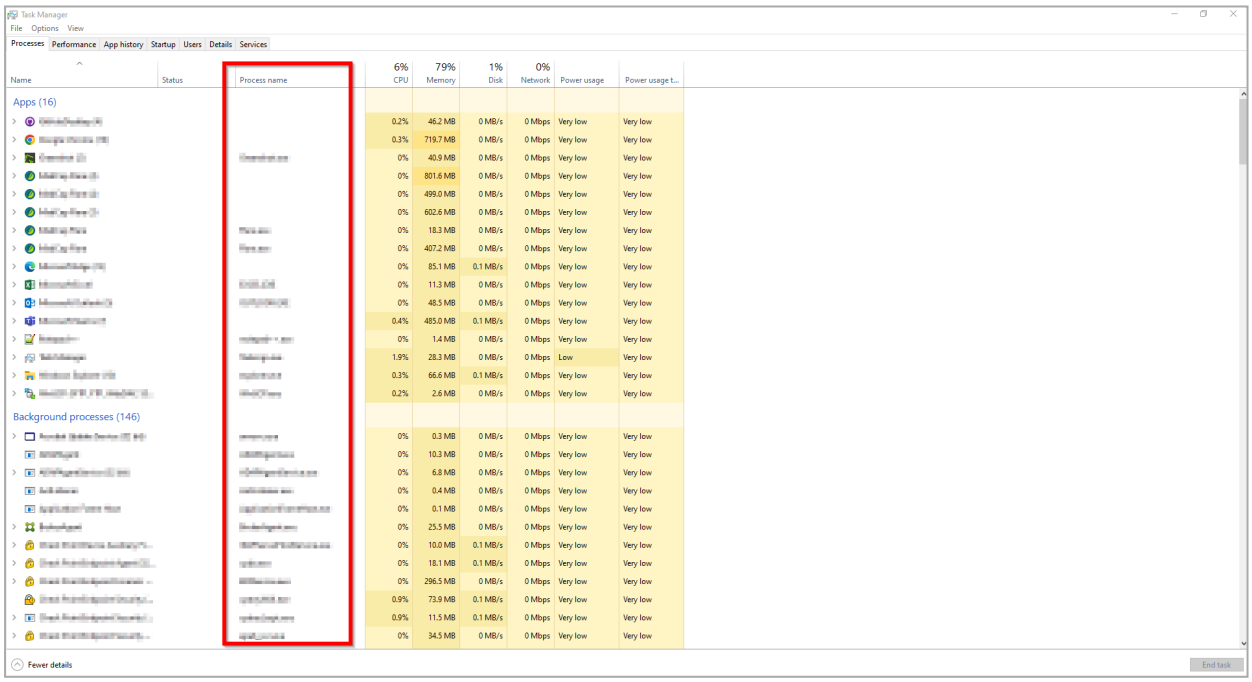
To find the process name in Windows:

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>
   ```

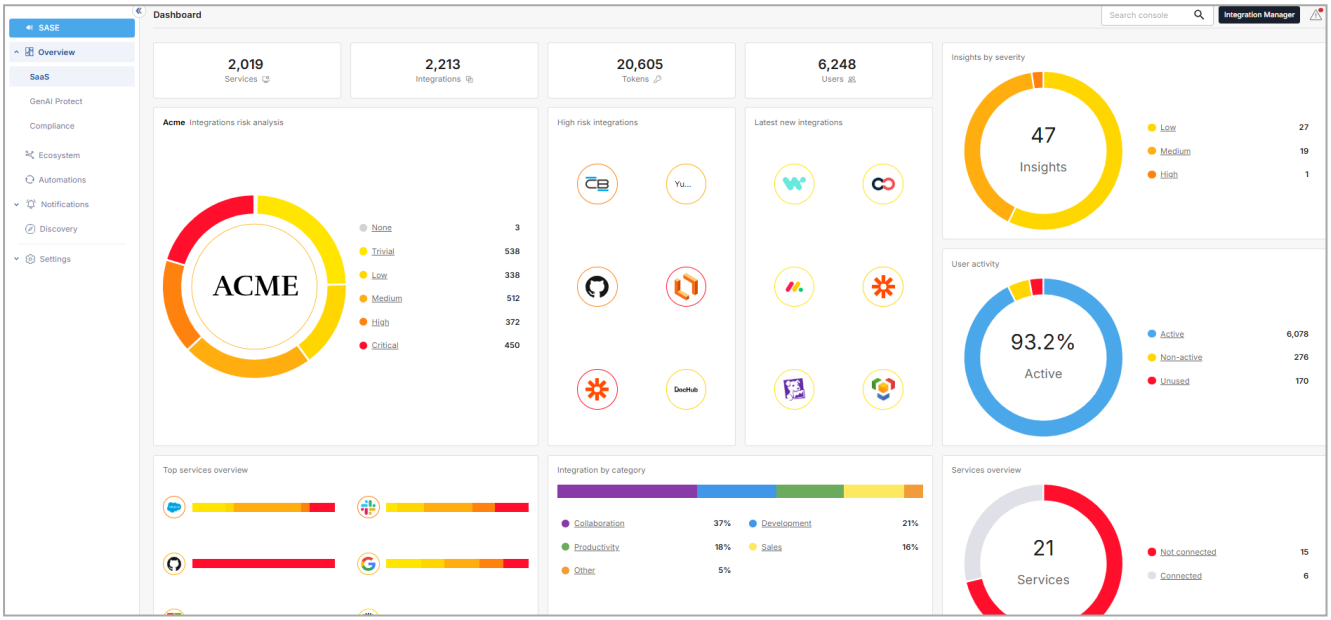
   The process name is displayed in the second-to-last column of the output.

SaaS API

Harmony SaaS provides automated monitoring and threat prevention for your organization's SaaS ecosystem, protecting against data theft, cyber espionage, unauthorized access, risky connections, and poor security configurations like missing MFA or SSO.

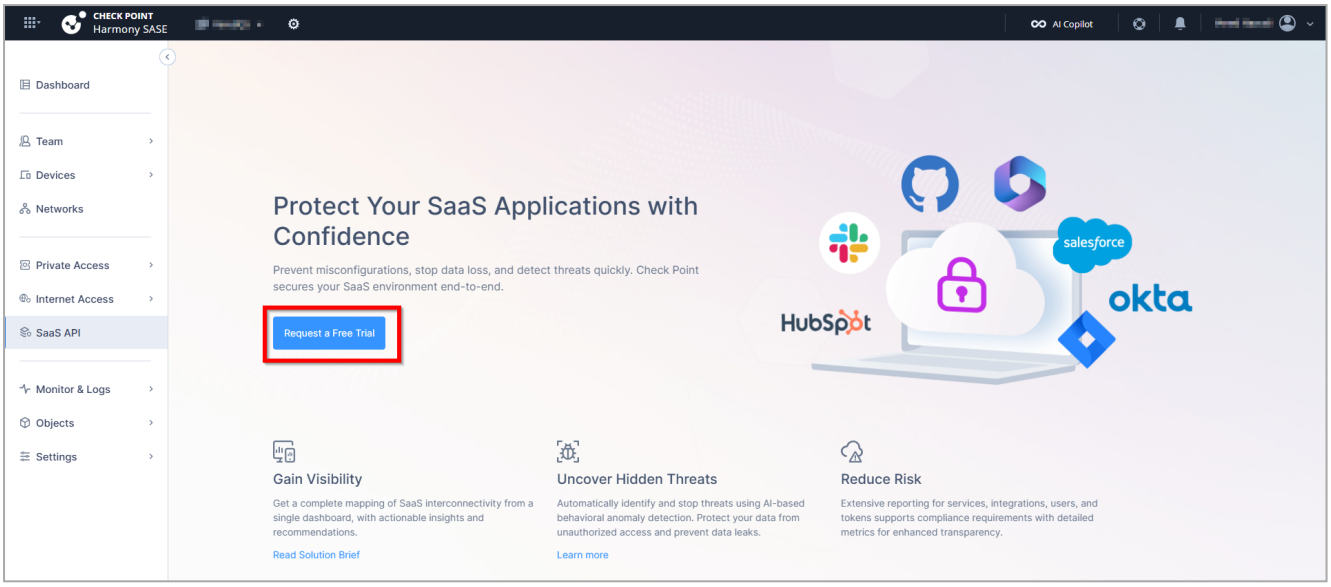
To access the **SaaS API** page, access the Harmony SASE Administrator Portal and click **SaaS API**.

The Harmony SaaS application page appears.



Note - To return to the Harmony SASE Administrator Portal, click **SASE** in the left navigation pane.

If you are accessing SaaS API for the first time, the Harmony SaaS introduction page appears. Click **Request a Free Trial** to explore Harmony SaaS.



For information on integrating your SaaS applications, refer to the [Harmony SaaS Administration Guide].

Monitor & Logs

Monitor & Logs allows you to view:

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: ▪ **app** - Member is connected to an application. ▪ **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. 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.

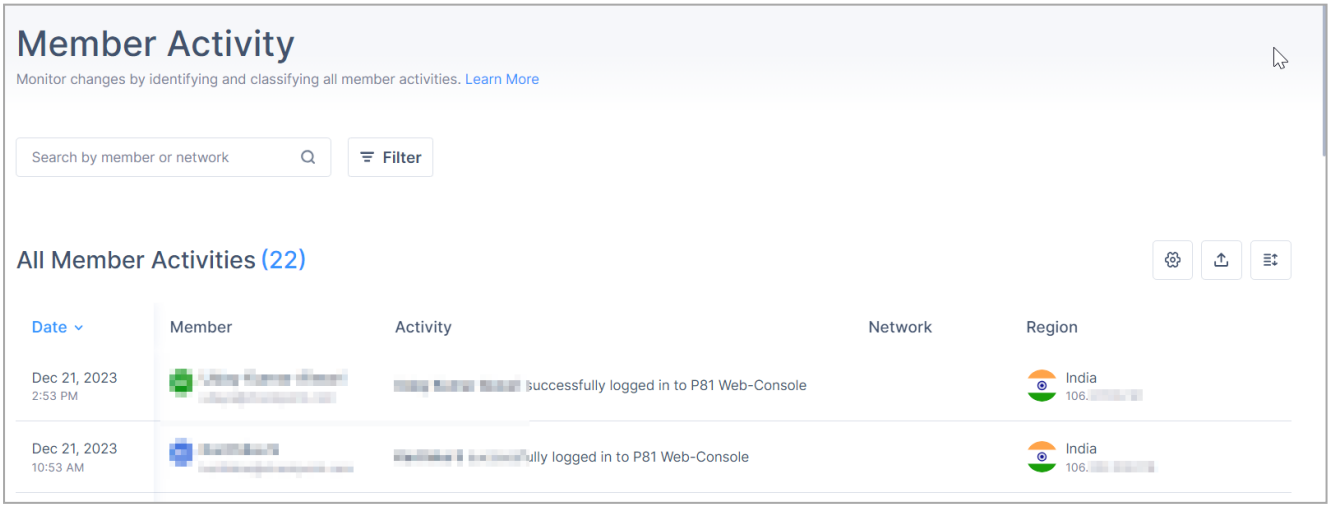
Note - You can export only the latest 1000 active sessions at a time.

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:

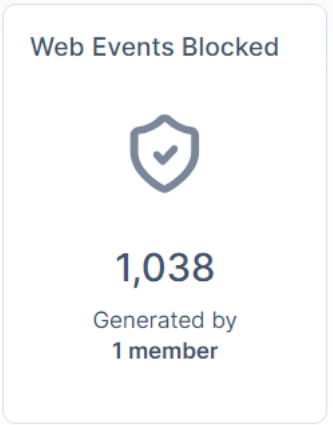
- *"Web Events Blocked" below*
- *"Top Web Categories" on the next page*
- *"Events Per User" on the next page*
- *"All Web Activities" on the next page*

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

Insights

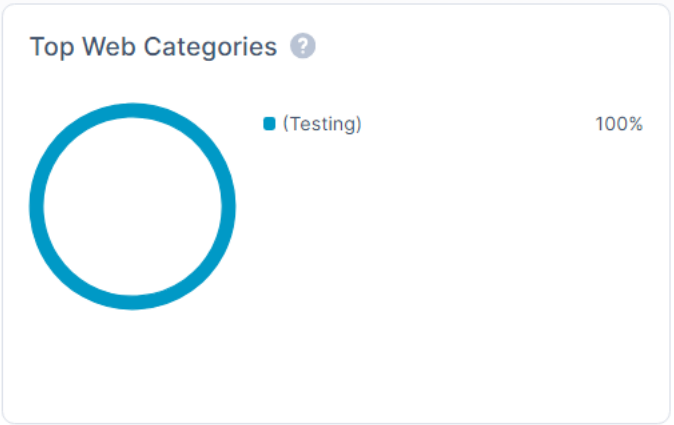
Insights shows the number of blocked web events, top web categories blocked, and top number of events blocked in the last 1 day, 7 days, and 30 days.

Web Events Blocked



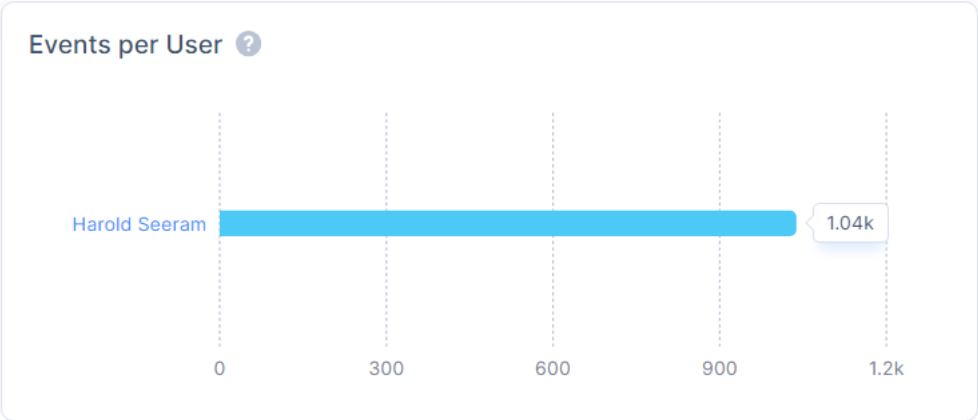
The **Web Events Blocked** widget shows the total number of URLs blocked in the selected time frame.

Top Web Categories



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

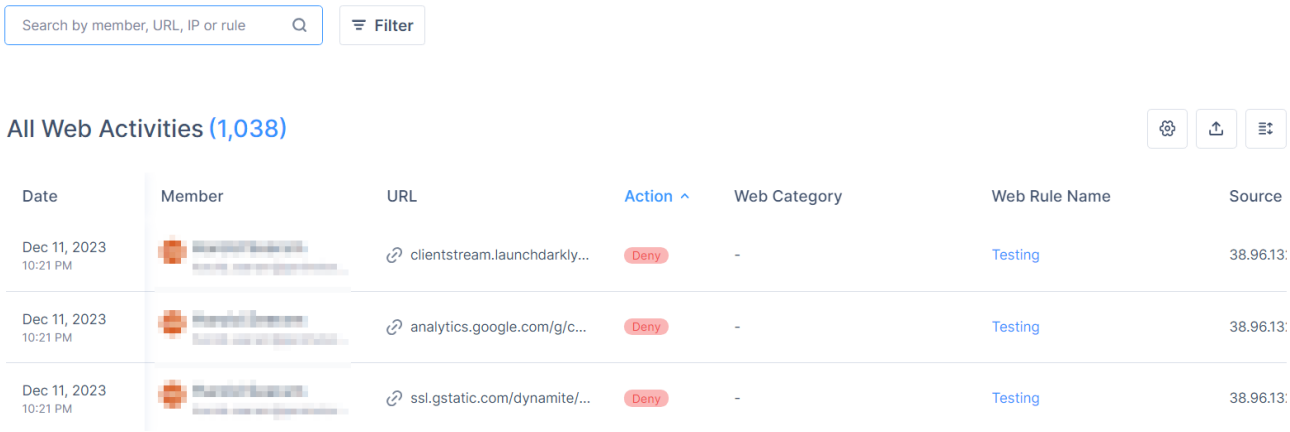
Events Per User



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 table shows a log of all the URLs (web traffic) where the user is either warned or denied actions.



Column	Description
Date	Date and time of the activity.
Member	Member name.
URL	Accessed URL.
Action	Action taken by Harmony SASE: ▪ Deny - Member is denied access to the URL. ▪ Warn - Member is warned before accessing URL.
Web category	Category name configured in the *"Web Filter Rules" on page 642*.
Web Rule Name	Web Rule name configured in the *"Web Filter Rules" on page 642*.
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:

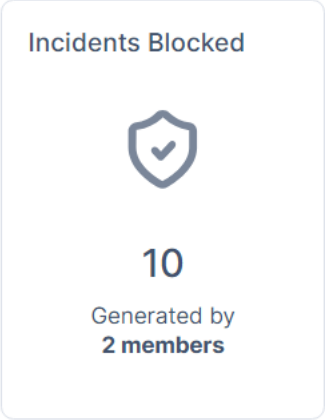
- *"Incidents Blocked" below*
- *"Malware Types" on the next page*
- *"Blocked Malware Per User" on the next page*
- *"All Malware Activities" on the next page*

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

Insights

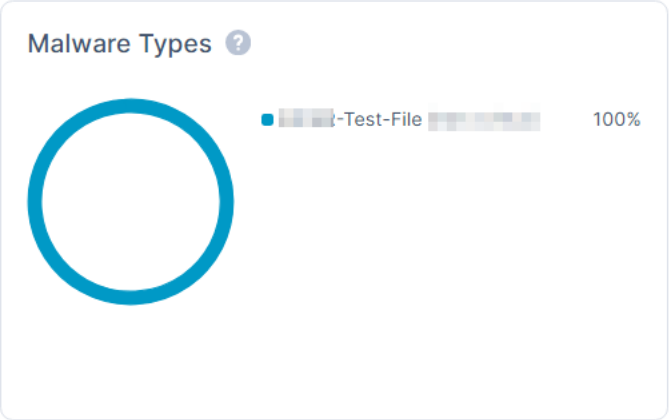
Insights shows the number of blocked malicious events, top malware types blocked, and top number of blocked events per user in the last 1 day, 7 days, and 30 days.

Incidents Blocked



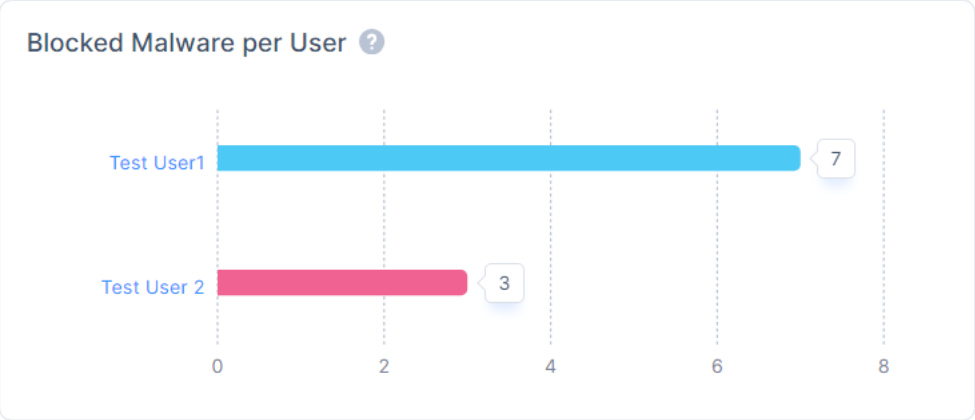
The **Incidents Blocked** widget shows the total number of blocked malicious files and URLs in the selected time frame.

Malware Types



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

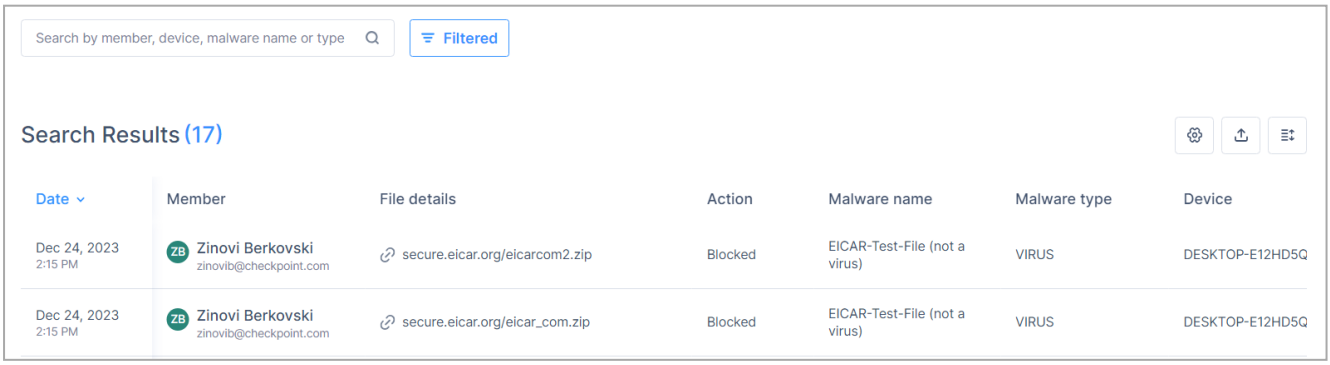
Blocked Malware Per User



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: ▪ Blocked ▪ 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

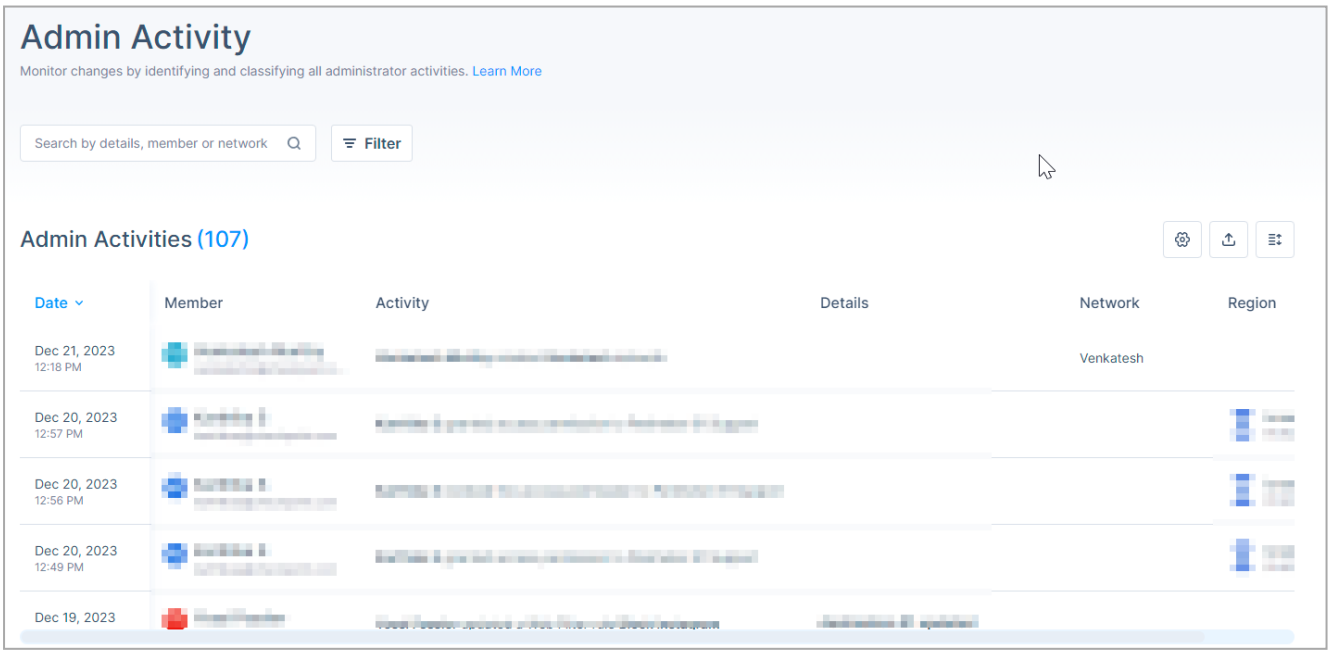
The **Admin Activity** page allows to you to view these administrator activities:

- 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.

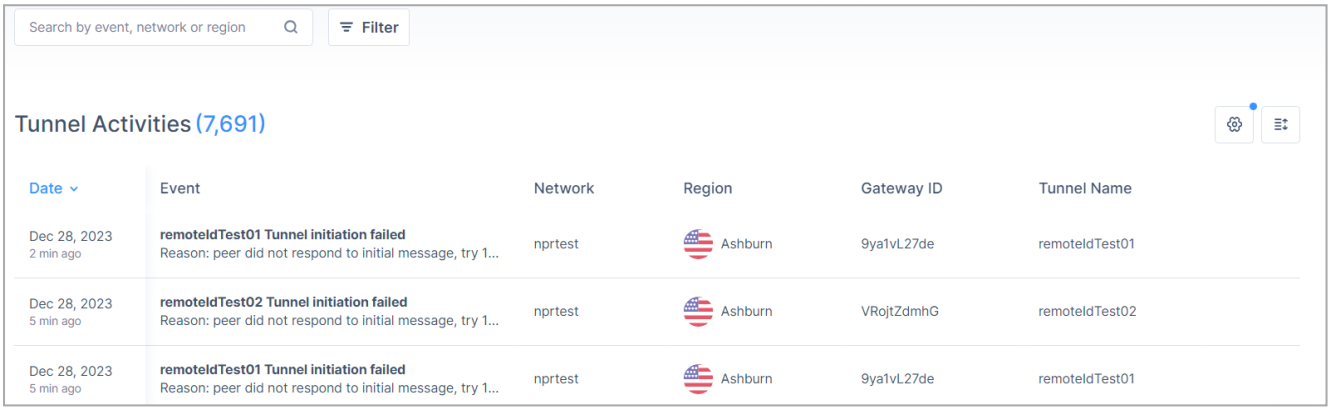
Note - You can export data of only 1000 activities at a time.

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**.



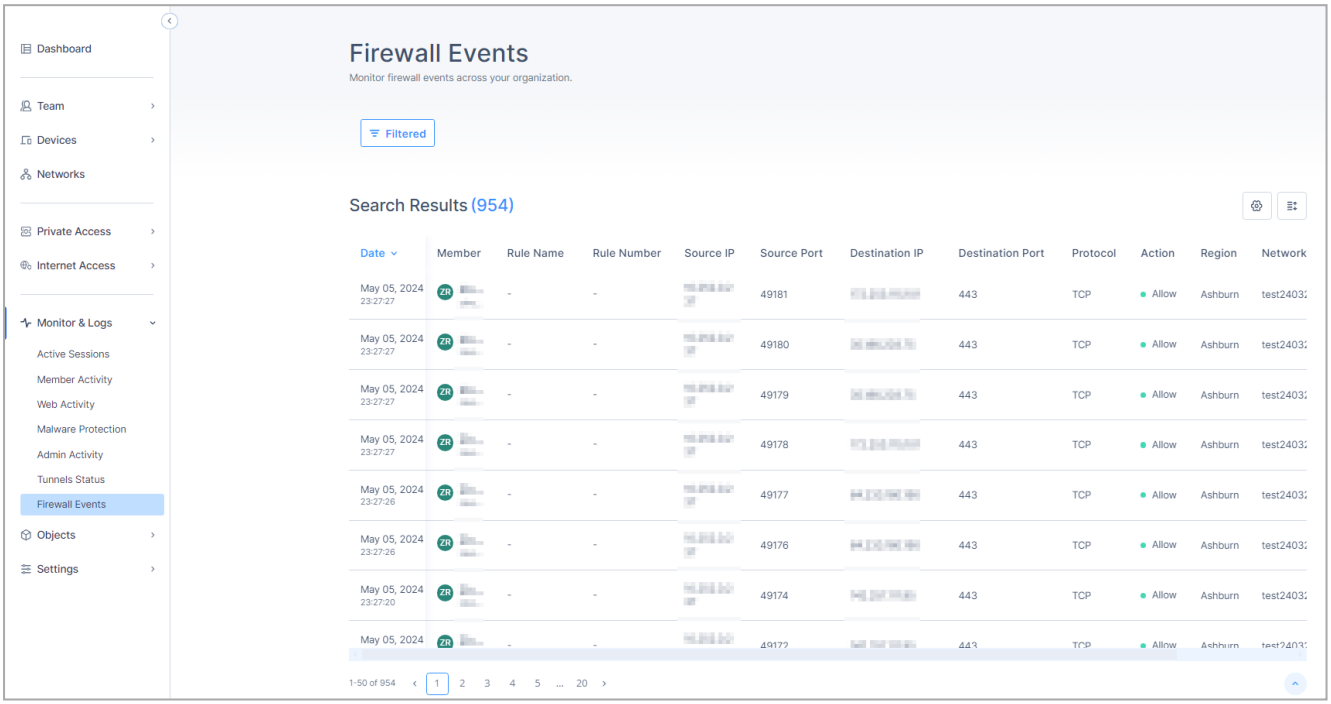
Column	Description
Date	Date and time of the activity.
Event	Event type and the reason.
Network	Associated network.
Region	Region of the network.
Gateway ID	Harmony SASE gateway ID.
Tunnel Name	Tunnel name.
Tunnel Peer IP	Tunnel peer IP address.
Tunnel Source IP	Tunnel source IP address.
Tunnel Type	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 605*.
Rule Number	Rule number configured in the *"Firewall" on page 605*.
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: ▪ Allow ▪ 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

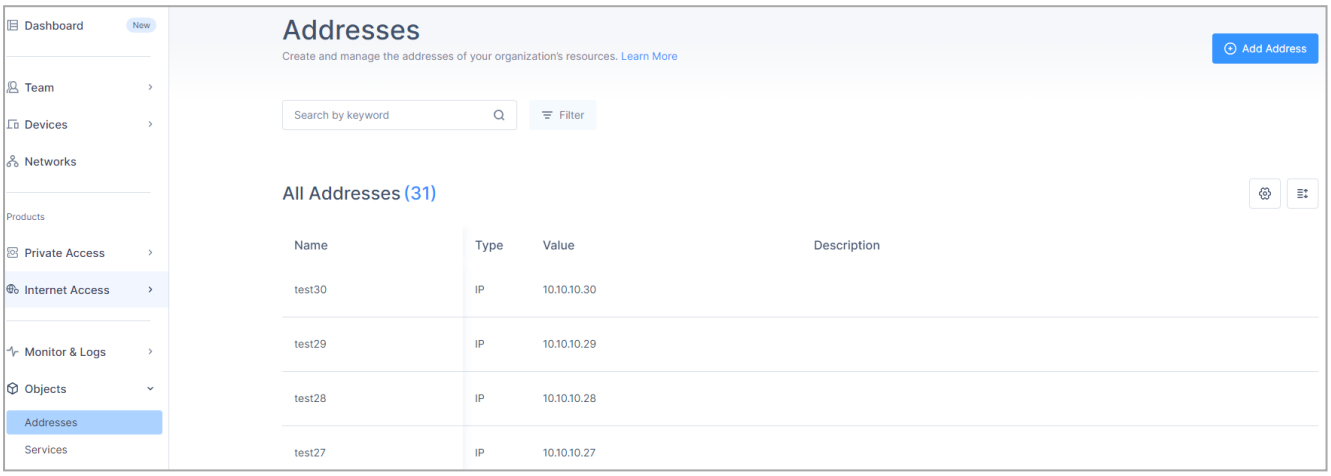
Objects allow you create:

- *"Addresses" on page 689*
- *"Services" on page 694*
- *"Custom URLs" on page 698*

Addresses

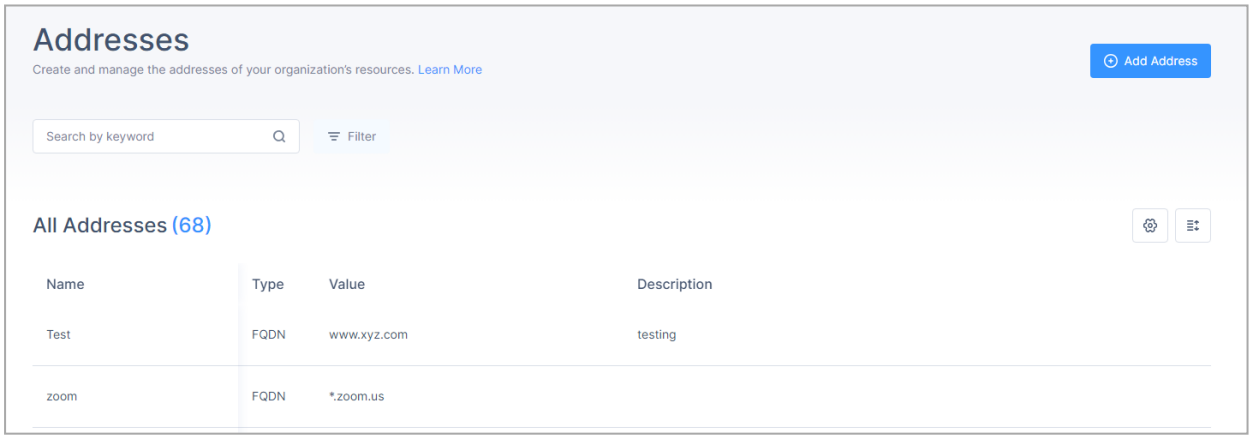
The **Address** object allows you manage the IP addresses and subnets that you use to define your network, firewall rules, application access rules and access policies.

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



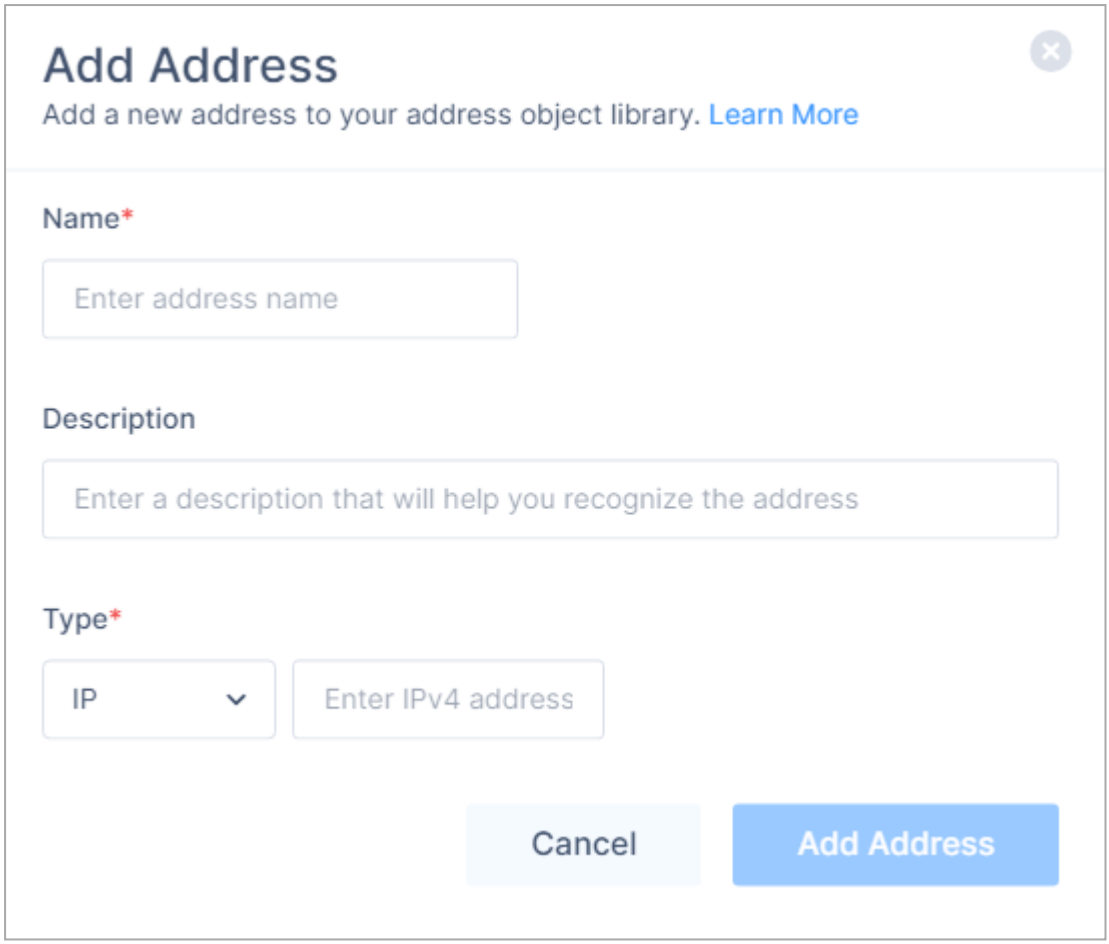
Creating an Address Object

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:

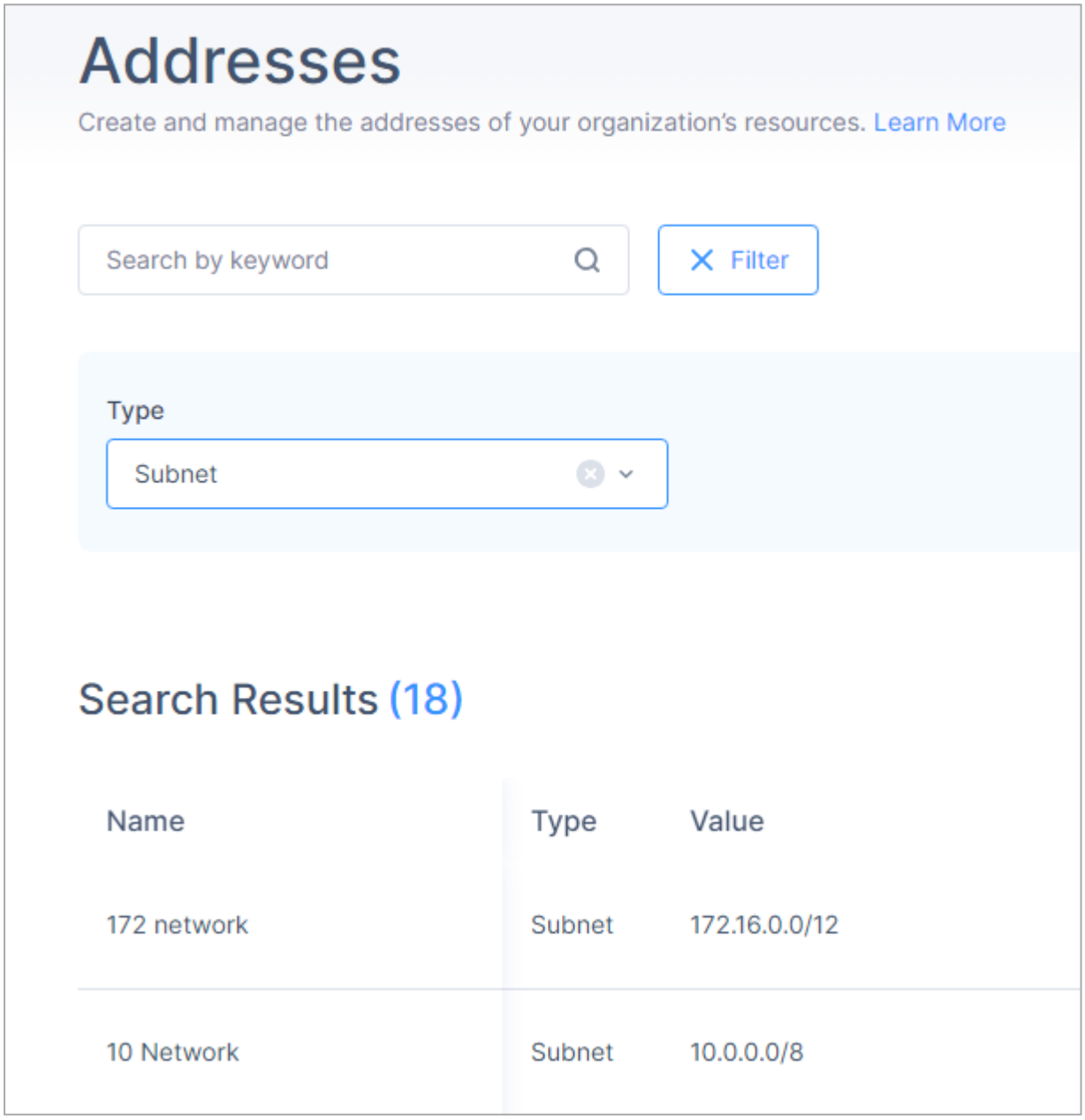
- To edit, click .

  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

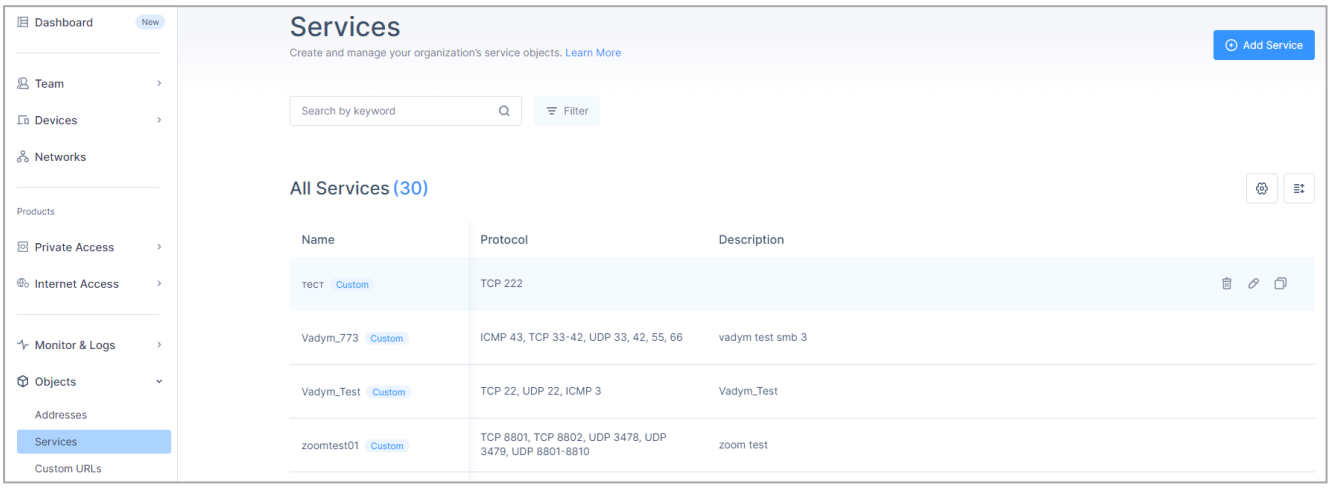
- FQDN firewall rules may be bypassed by using an IP.
- CDN is not permitted, only FQDN.
- If you have two or more FQDNs sharing the same IP, both are affected by the Firewall rule. For example, if you block one FQDN, another resource sharing the same IP is also be blocked.
- Limited compatibility with 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

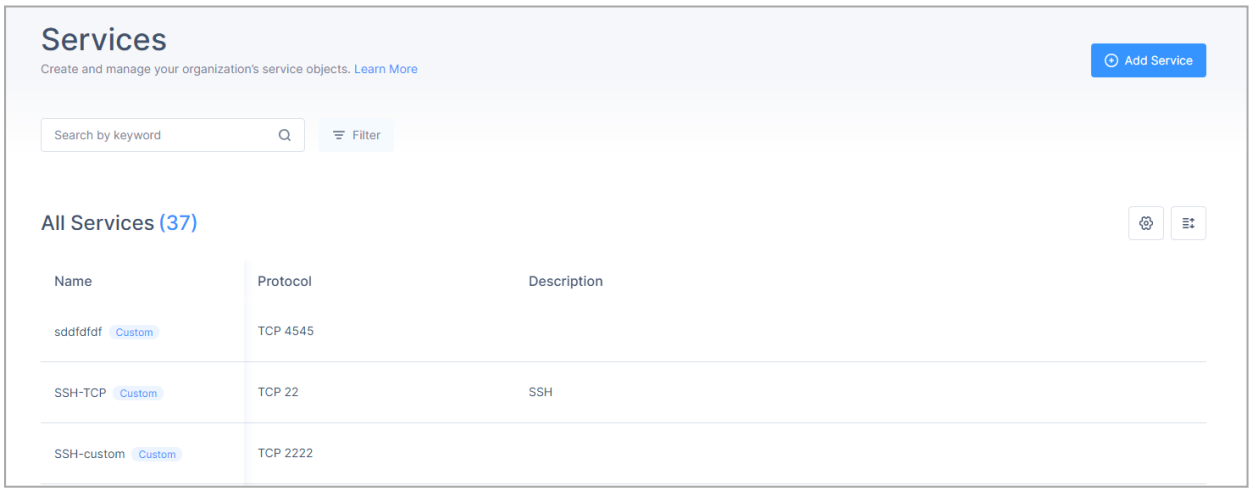
The **Services** object allows you to define the applications that you want to allow access to. These services belong to the Layer 4 of the OSI model with protocol and port combinations. For example, protocol TCP port 80 or protocol UDP port 53.

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



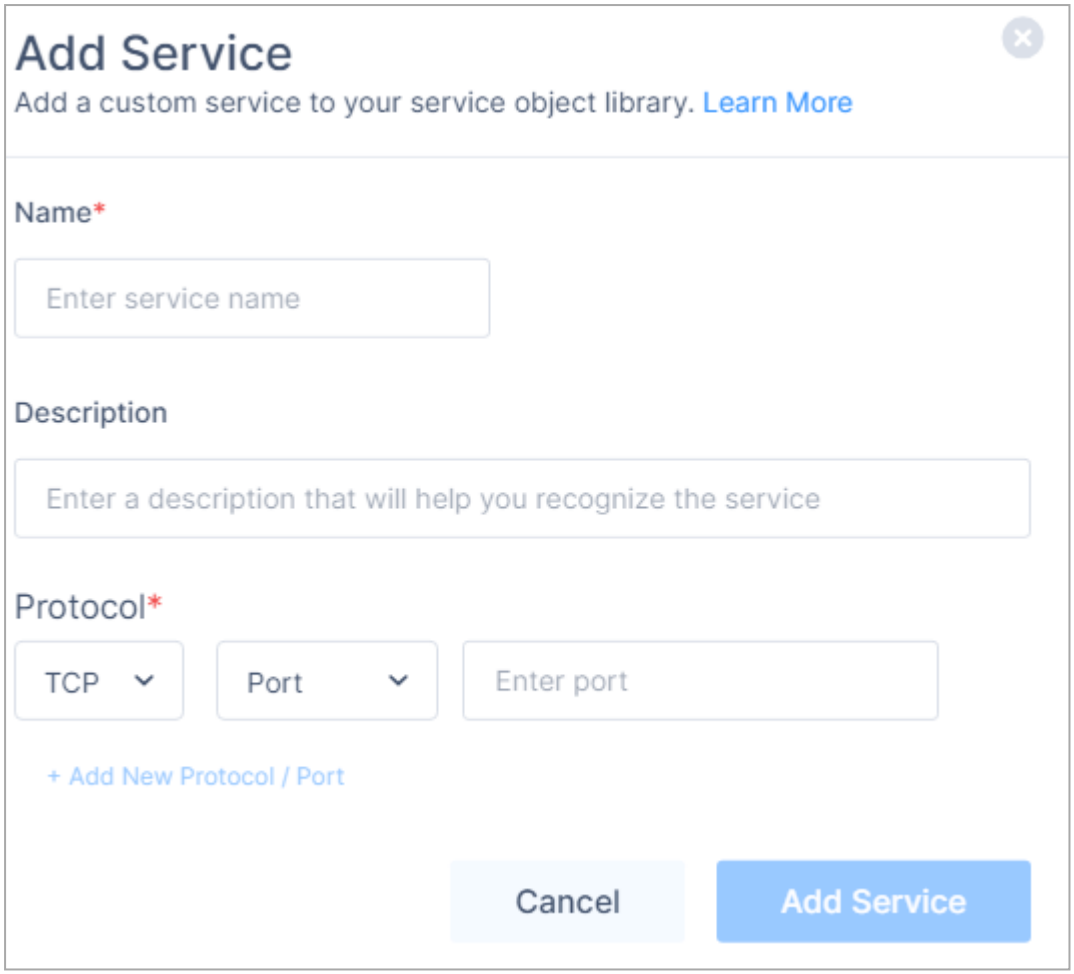
Creating a Service Object

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



2. Click **Add Service**.

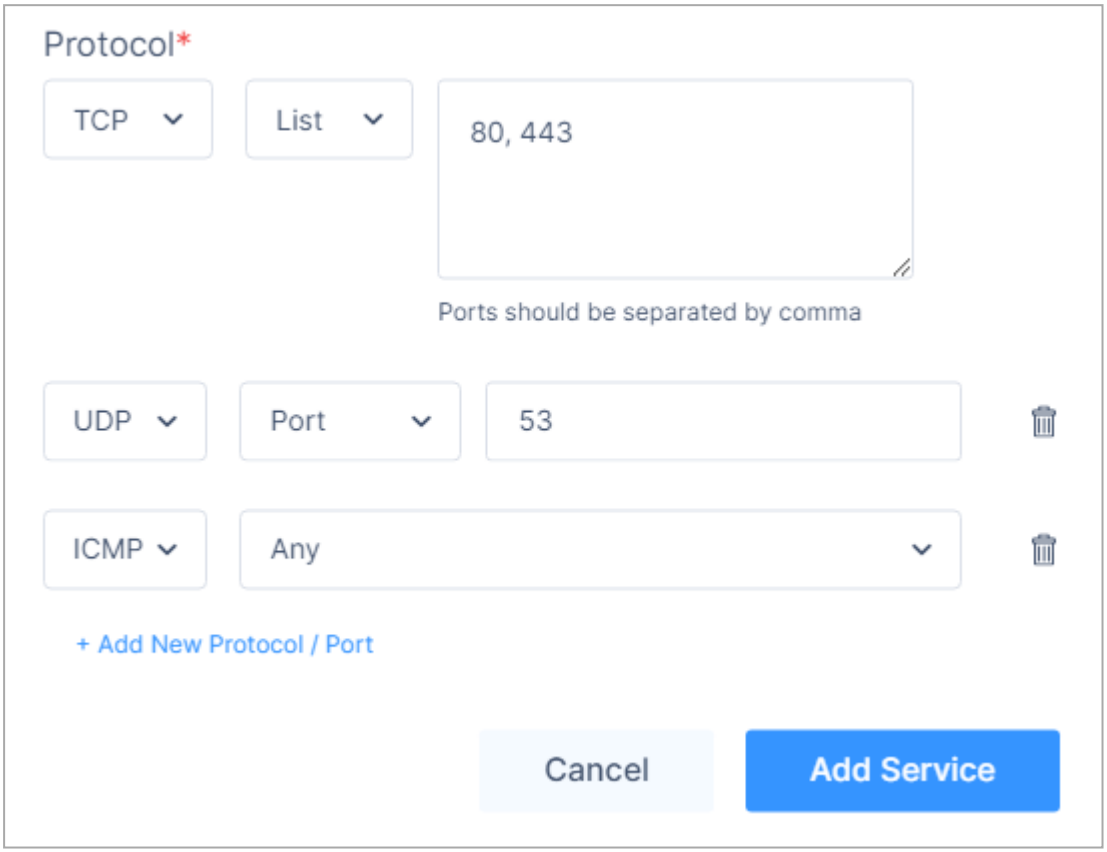
   The **Add Service** window appears.



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

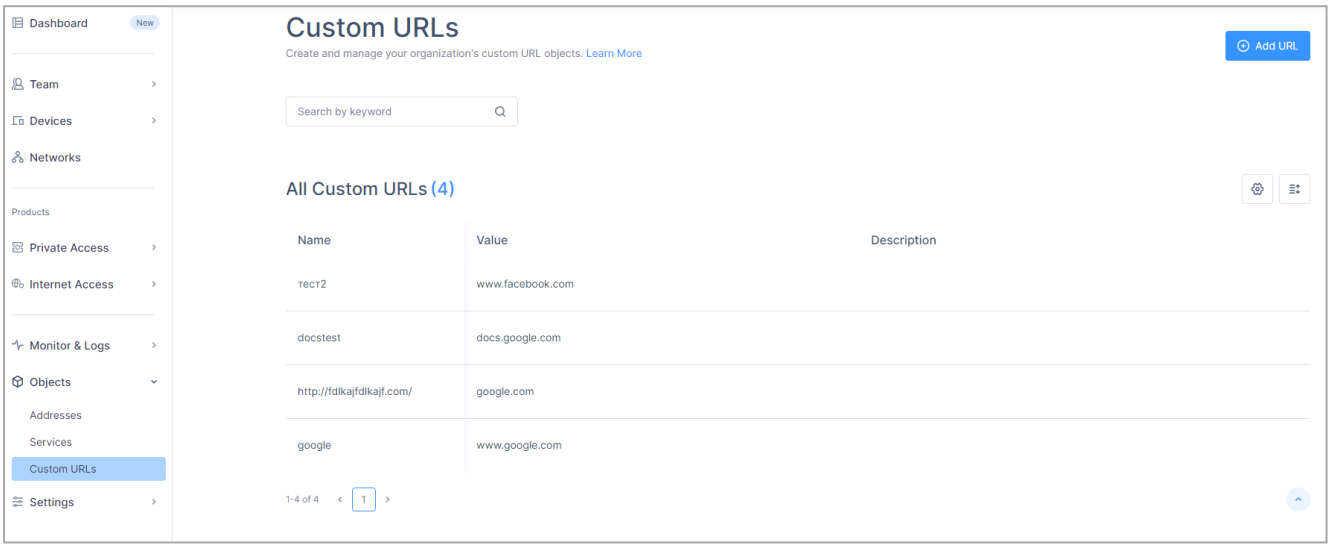
1. Access the Harmony SASE Administrator Portal and click **Objects** > **Services**.
2. Hover over the service and do one of these:
   - To edit, click .

     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" on page 642*.

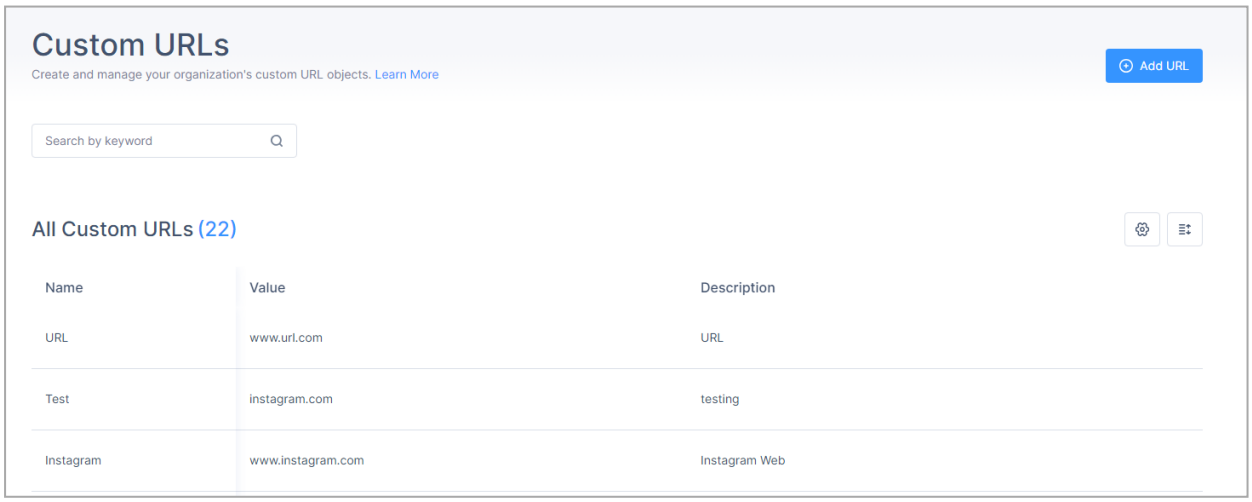
To view the **Custom URL** object, access the Harmony SASE Administrator Portal and click **Objects**.



Creating a Custom URL Object

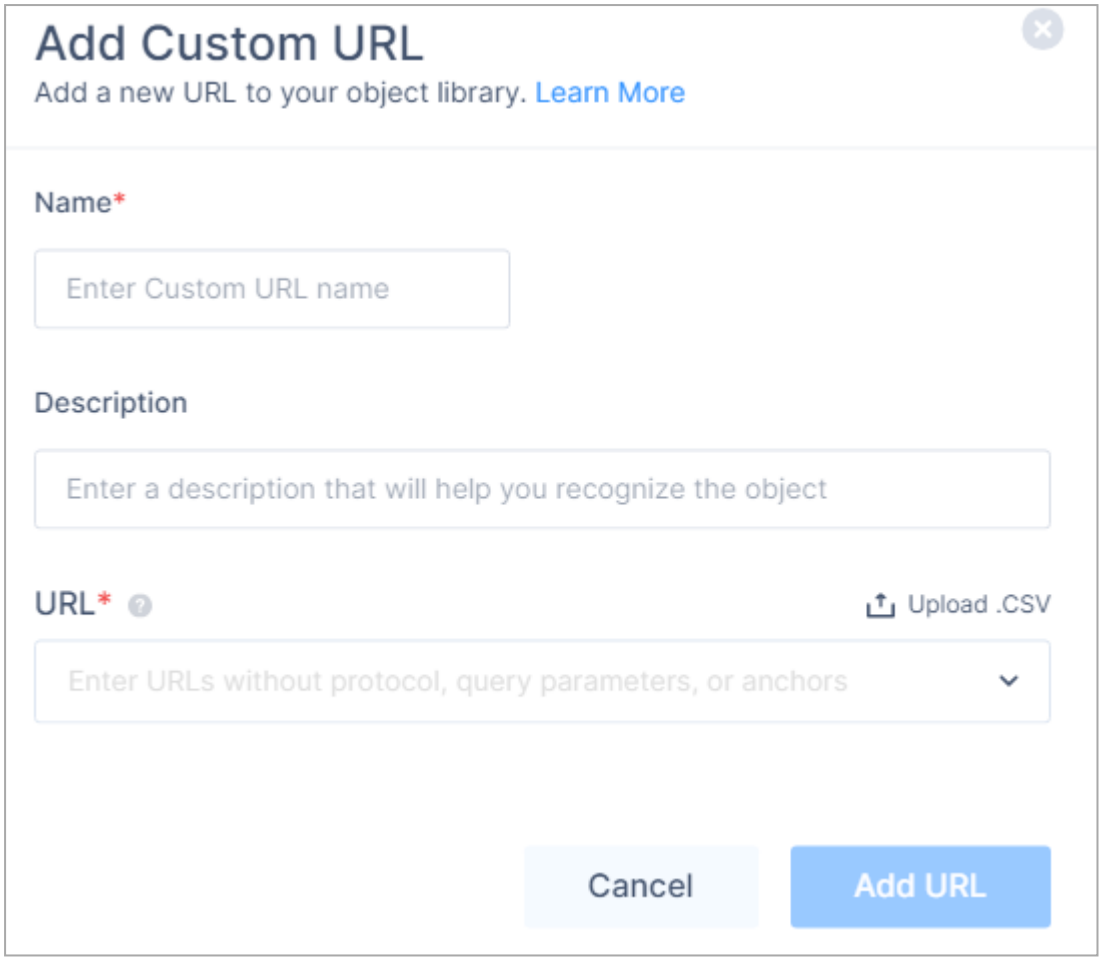
1. Access the Harmony SASE Administrator Portal and click **Objects** > **Custom URLs**.

   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 an access policy.
  Before you delete the URL, remove its references from the *"Web Filter Rules" on page 642* .

- 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 702*
- *"Identity Providers" on page 727*
- *"Two-Factor Authentication" on page 896*
- *"Certificate Manager" on page 900*
- *"Support Access" on page 905*

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 707*
- *"Amazon S3" on page 711*

Professional Services Automation (PSA) Integrations

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

- *"ConnectWise PSA" on page 720*

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.

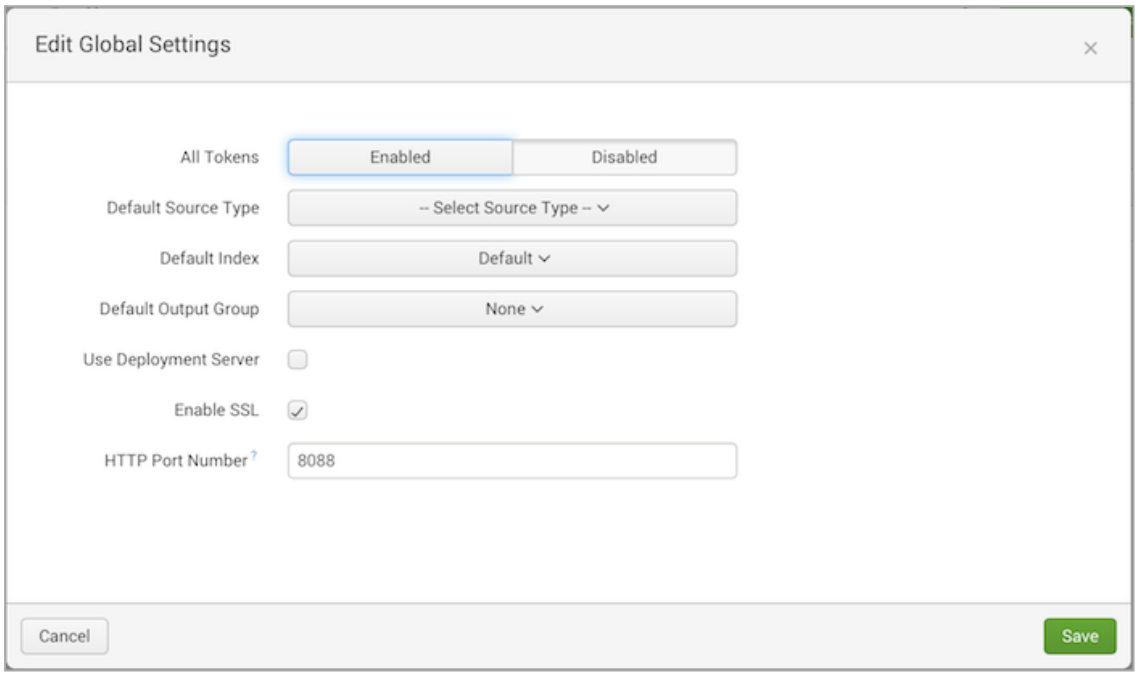
Step 2 - Enabling an HTTP Event Collector

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**.

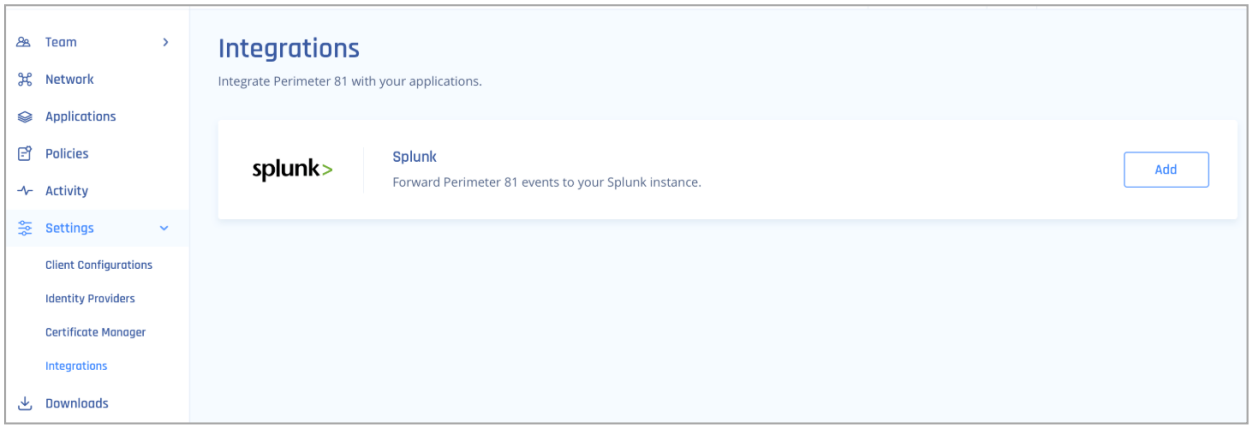
Step 3 - Creating an Event Collector Token

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**.

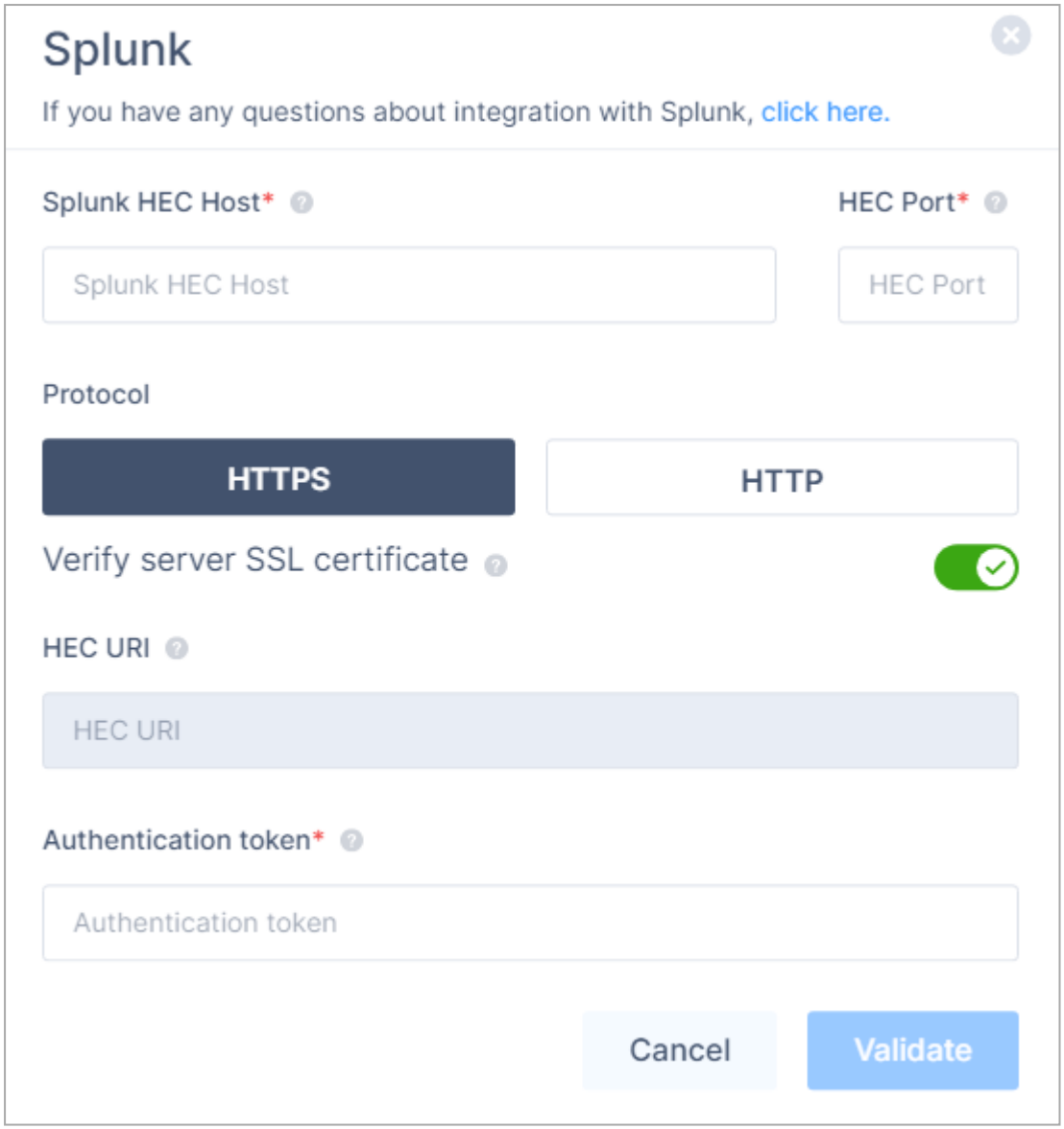
8. Click **Review**.
9. Verify the settings.
10. Click **Submit**.

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. Replace {hostname} with your Splunk server hostname. ▪ Splunk Cloud (paid): inputs-<host> ▪ Splunk Cloud (free-trial): <host> ORinputs.<host>
HEC Port	▪ Splunk Cloud free trial: 8088 ▪ Splunk Cloud paid: 443
Protocol	▪ Splunk Cloud free trial: HTTP ▪ Splunk Cloud paid: HTTPS

Item	Description
(For HTTPS only) **Verify server SSL certificate**:	▪ If you are using a self-signed certificate disable SSL verification. ▪ 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

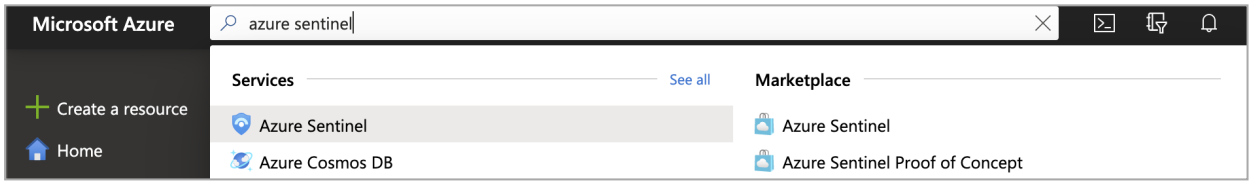
Microsoft Sentinel (formerly Azure Sentinel) is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. It delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Configuring the Integration in the Microsoft Azure Portal

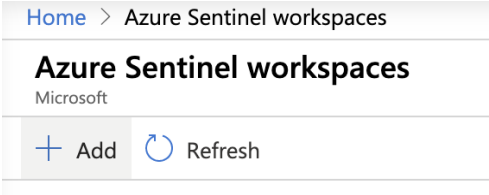
Step 1 - Setting up a Log Analytics Workspace

Note - If you are using an existing log analytics workspace, skip this section.

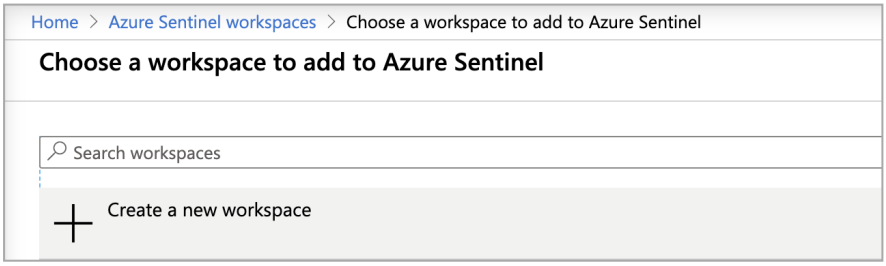
1. Log in to the Microsoft Azure portal.
2. Search for **Azure Sentinel** and select it.



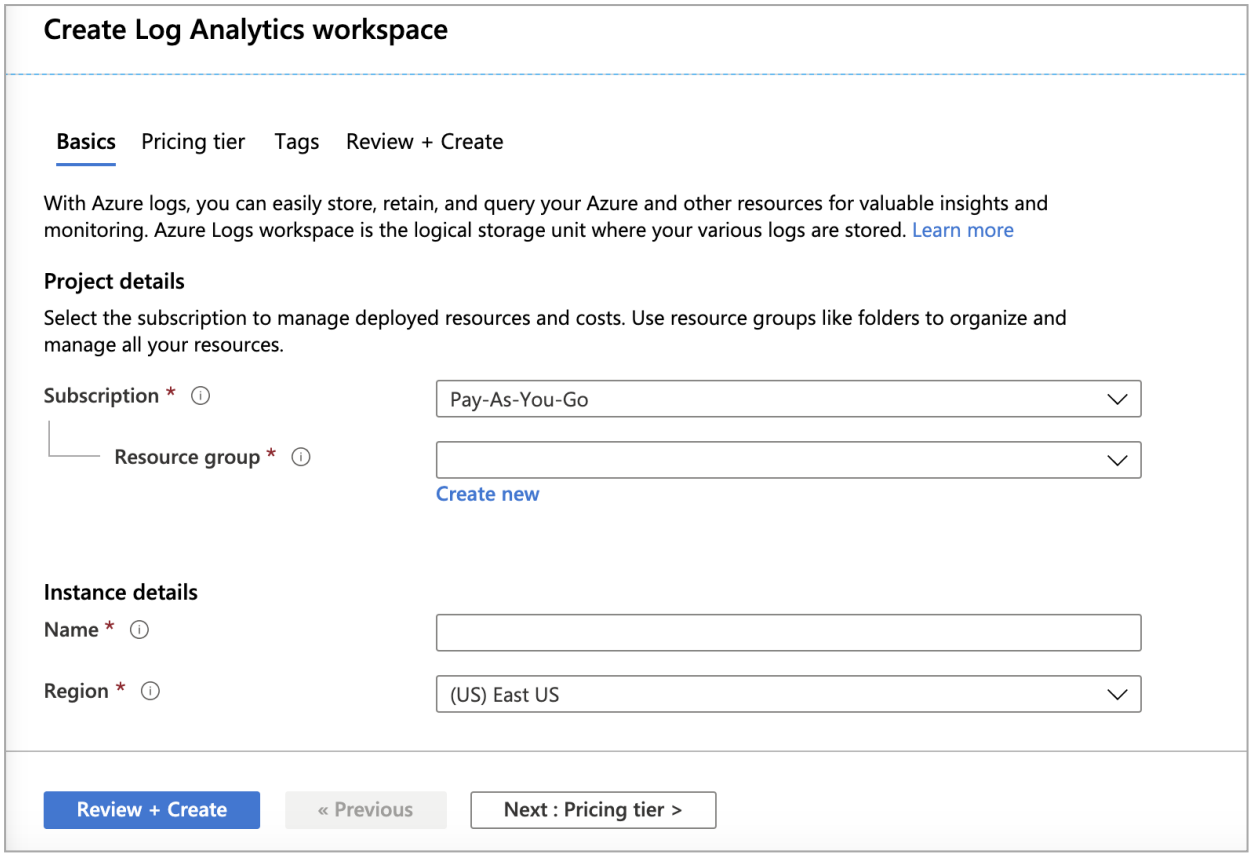
3. Click **Add**.



4. Click **Create a new workspace**.



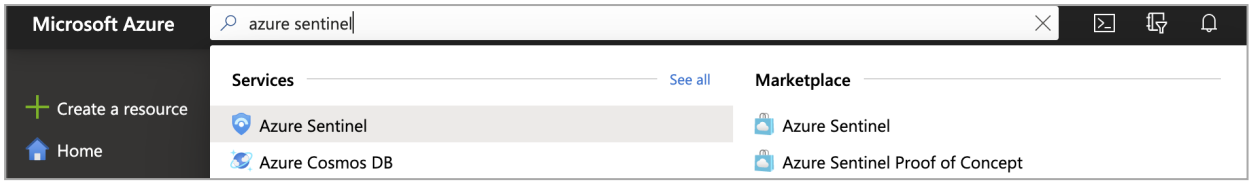
The **Create Log Analytics workspace** window appears.



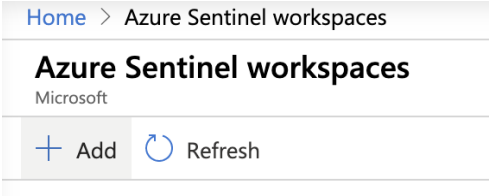
5. Enter these:
   a. **Subscription** - A subscription according to your business needs.
      - **Resource group** - Associate the log analytics workspace with the appropriate business unit.
   b. **Name** - Name of the workspace. It must contain minimum four characters (alphabets, numerals and hyphen) 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.



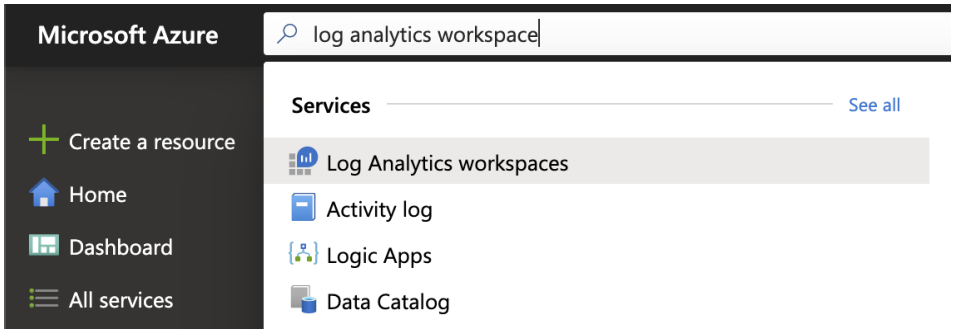
3. Click **Add**.



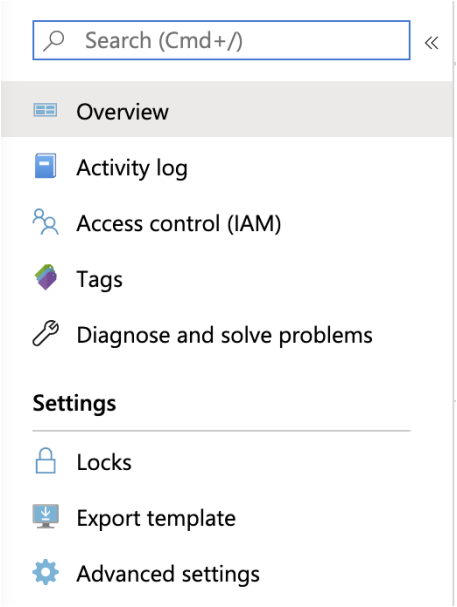
4. Select the Log Analytics Workspace that you have created or an existing one that you want to utilize.

Step 3 - Finding your Log Analytics Workspace ID and Primary Key

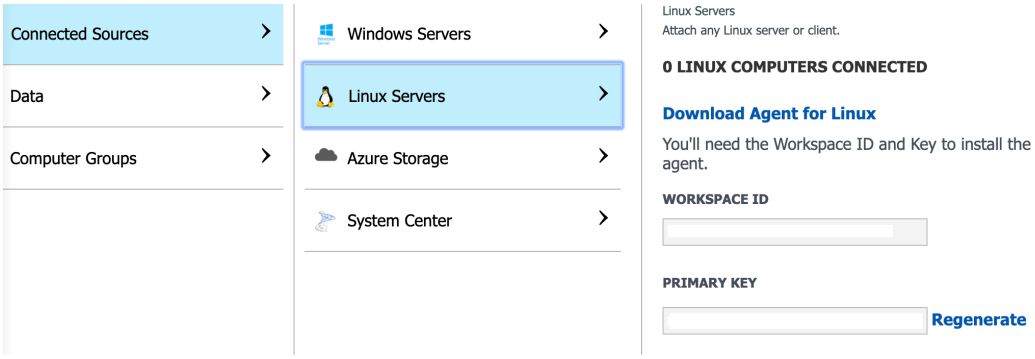
1. Log in to the Microsoft Azure portal.
2. Search for **Log Analytics Workspace** and select it.



3. Select the workspace you connected to Microsoft Sentinel.
4. In the **Settings** section, click **Advanced settings**.

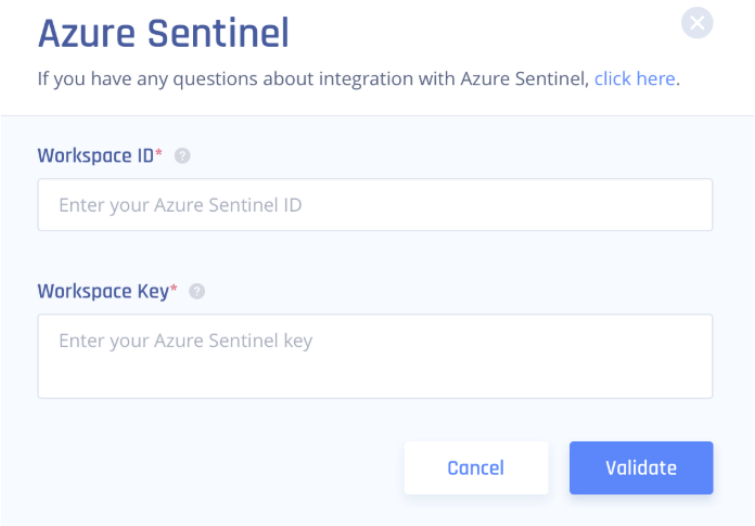


5. Click **Connected Sources** > **Linux Servers** and then copy the **Workspace ID** and the **Primary Key**.



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

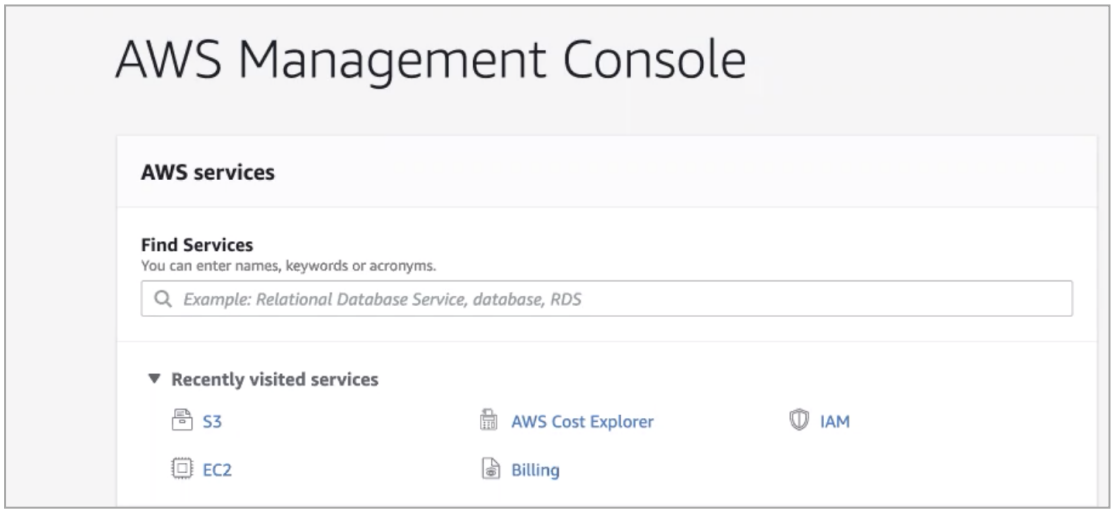
- Ensure that the IAM user has the necessary permissions to access the S3 bucket.
- Harmony SASE uses these IP addresses to deliver SIEM logs:

- US tenant:
  - 44.199.0.186
  - 44.198.227.127
  - 50.19.134.176
  - 23.20.83.77
  - 54.85.165.134
- EU tenant
  - 52.50.186.78
  - 79.125.50.175
  - 34.246.127.40

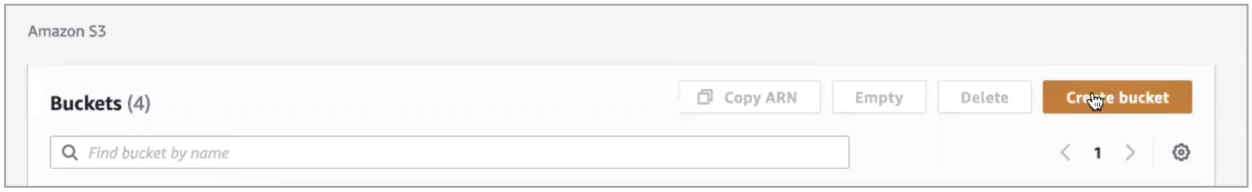
Configuring the Integration in the AWS Management Console

Step 1 - Creating a New Bucket

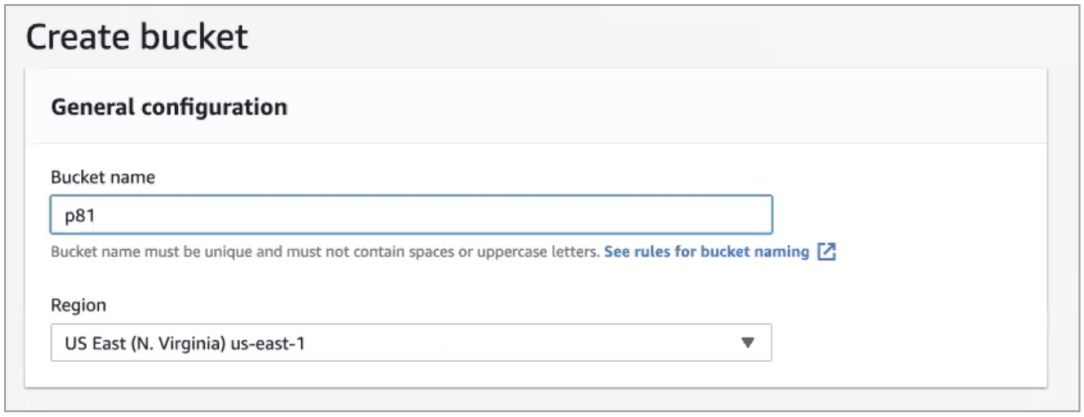
1. Log in to the AWS Management Console.
2. Go to **AWS Services** and select **S3**.



3. Click **Create Bucket**.



The **Create bucket** window appears.

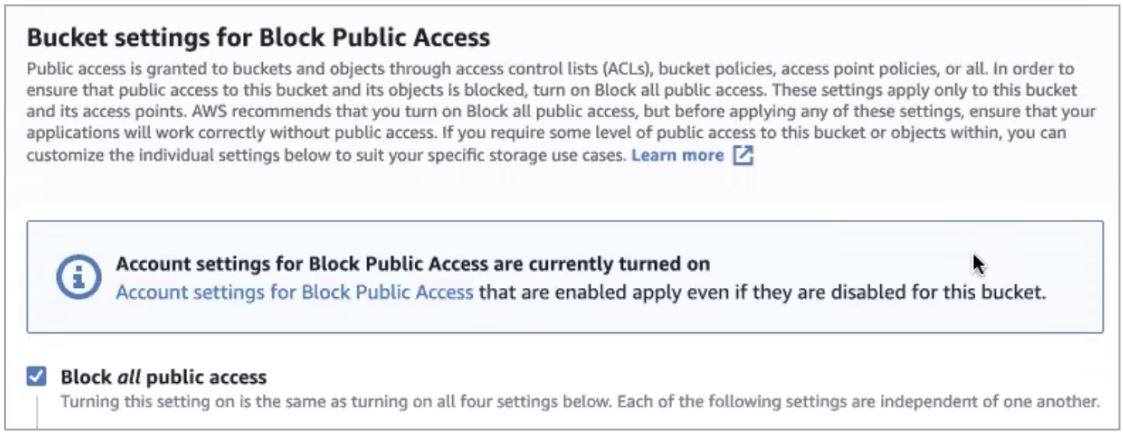


4. In the **Bucket name** field, enter the name of the bucket.

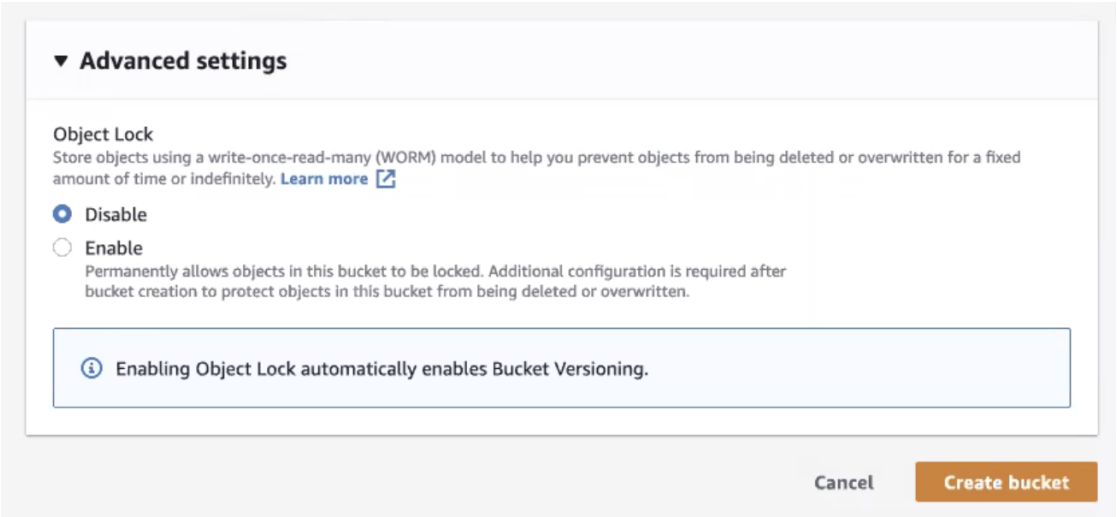
   The name must contain alphabets only. Hypen (-) and period (.) are not supported.

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.

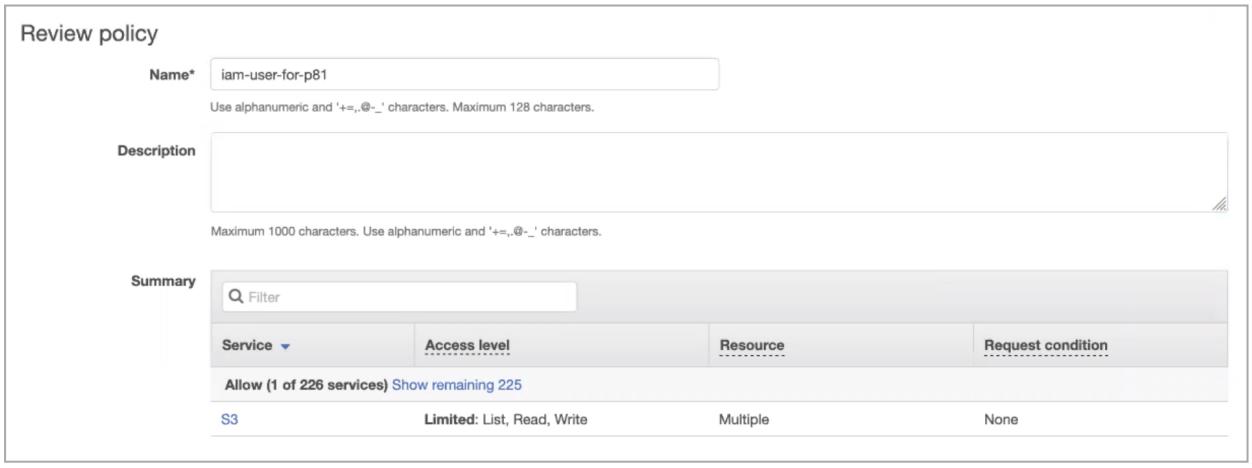
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test"
        },
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::test/*"
        }
    ]
}
```

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.

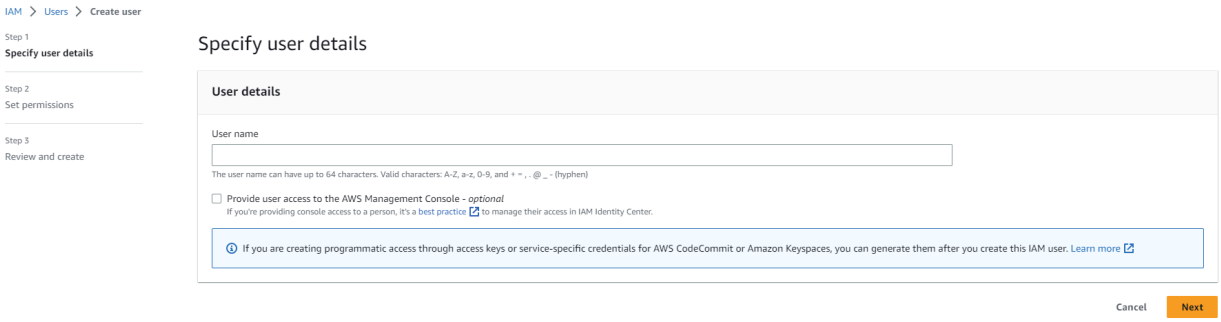
   b. (Optional) **Description**

7. Click **Create policy**.

Step 3 - Creating an AWS User

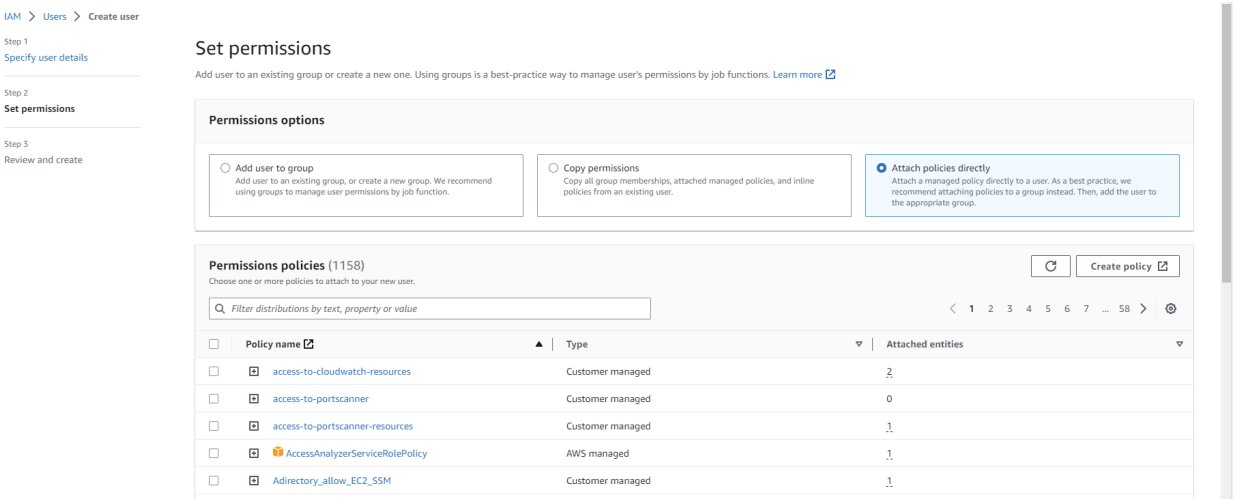
1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Users** tab and click **Create user**.
4. In the **Username** field, enter a name.

   Click **Next**.



5. Click **Attach policies directly** and select the policy you created earlier.

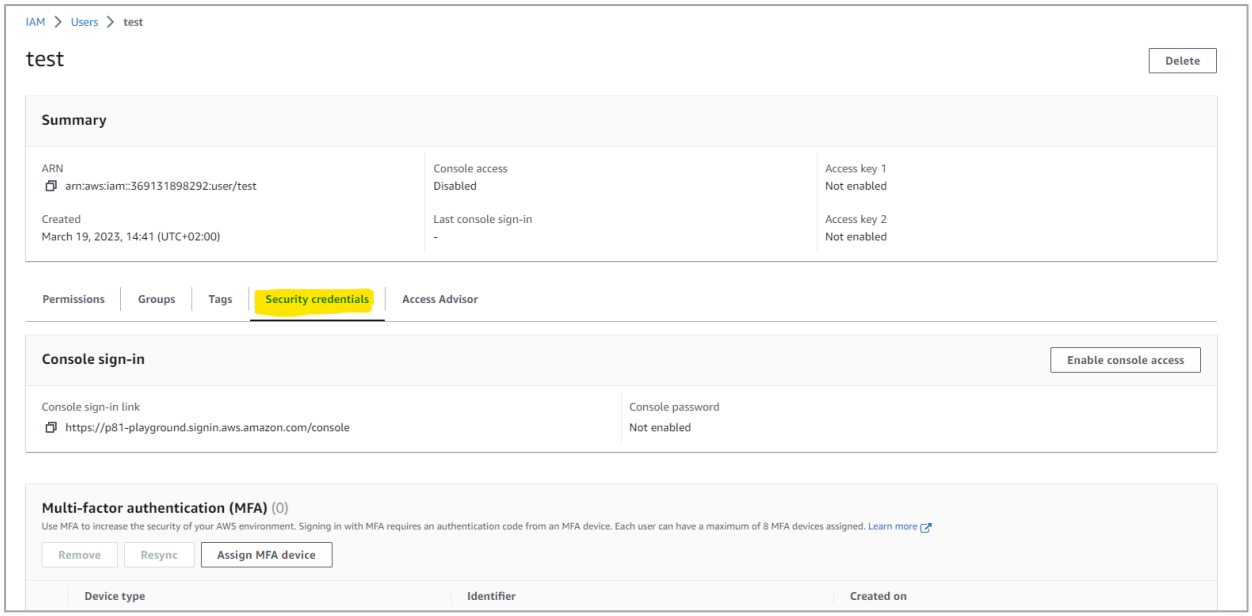
   If you have granted full access, then select the S3 full access AWS managed policy.



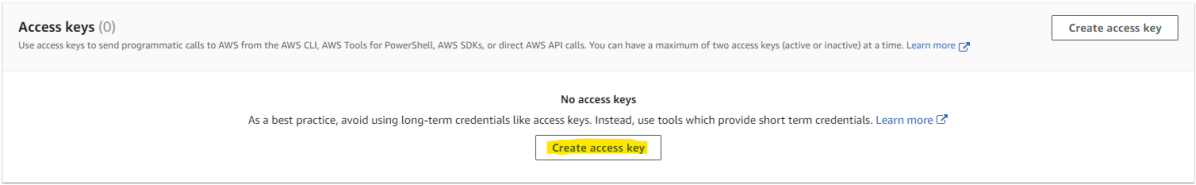
6. Click **Next**.

Step 4 - Creating an AWS Access Key

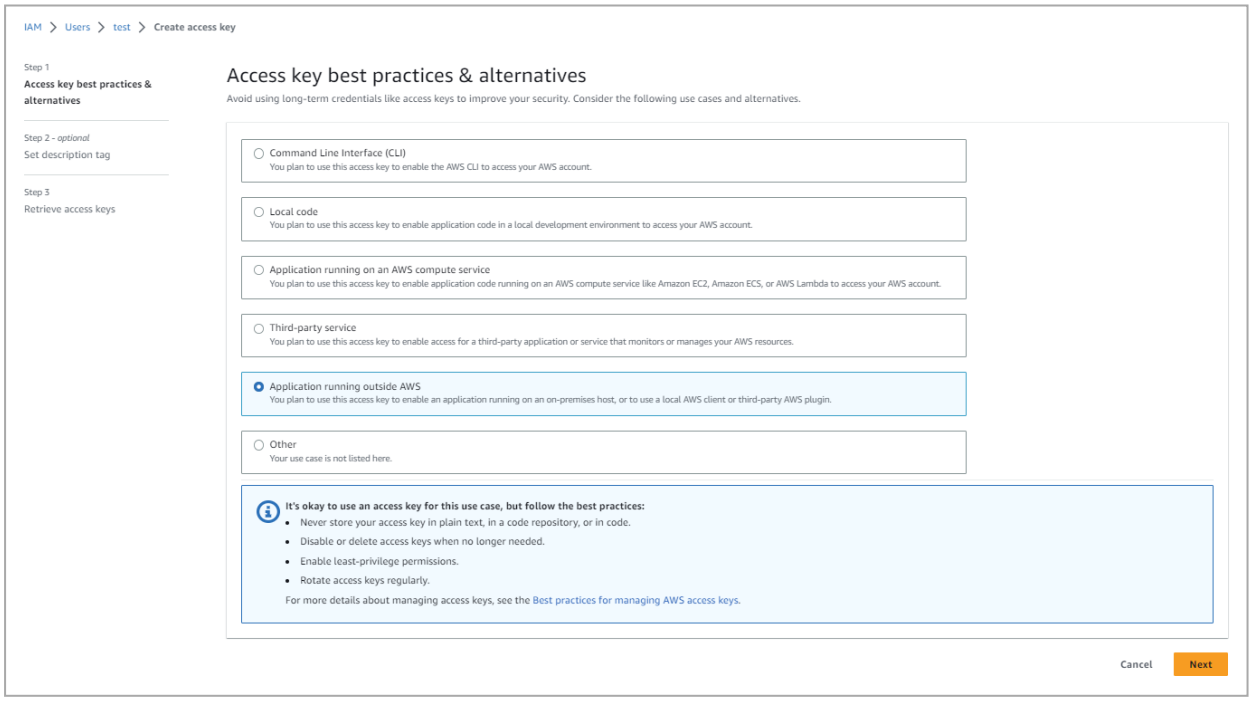
1. Log in to the AWS Management Console.
2. Open the AWS Identity and Access Management (IAM) dashboard.
3. Go to the **Users** tab and select the user you have created.
4. Click the **Security credentials** tab.



5. Scroll down to **Access keys** and click **Create access key**.

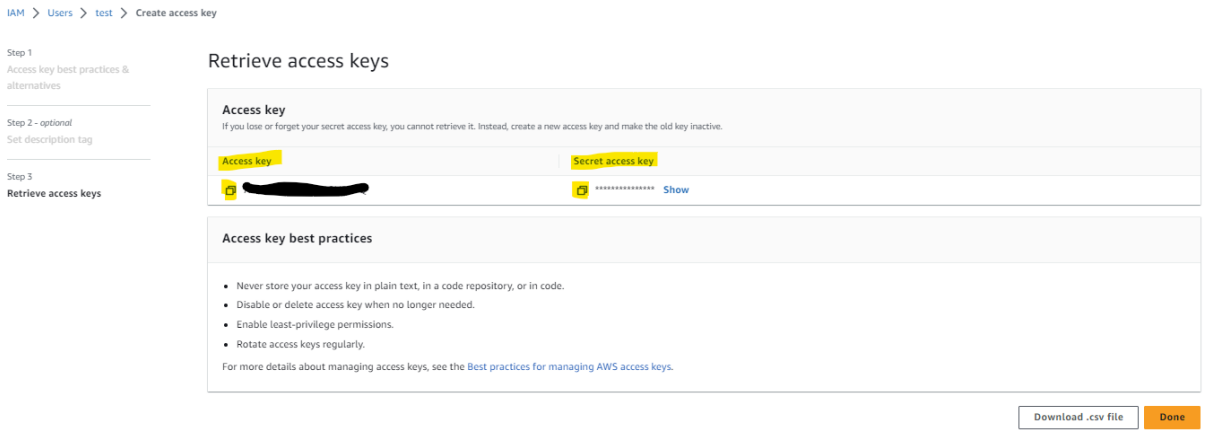


6. Select **Application running outside AWS** and click **Next**.



7. Select **Create access key**.
8. Description tag is optional.

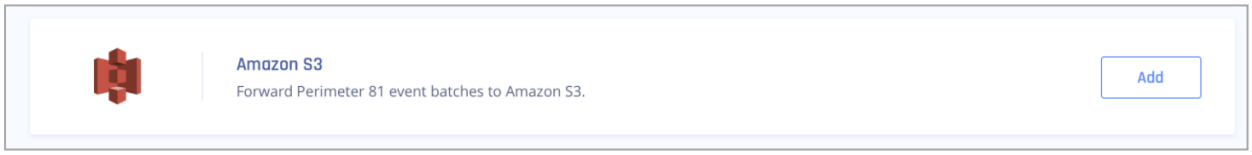
9. Copy the **Secret access key** and the **Access key**.



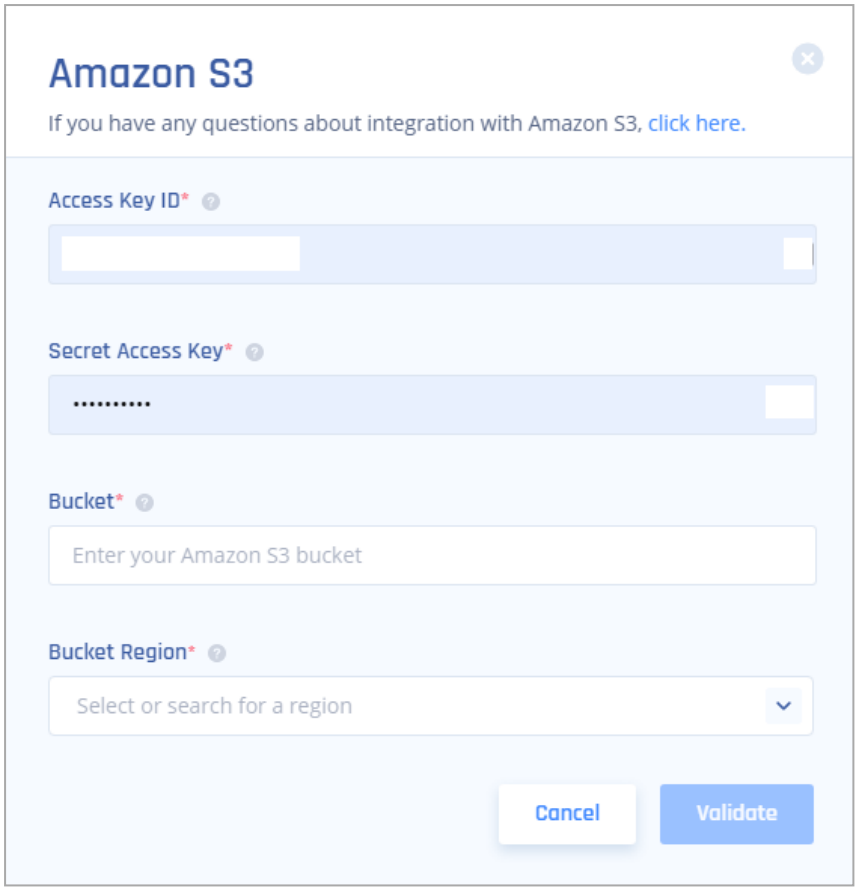
10. Click **Done**.

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.

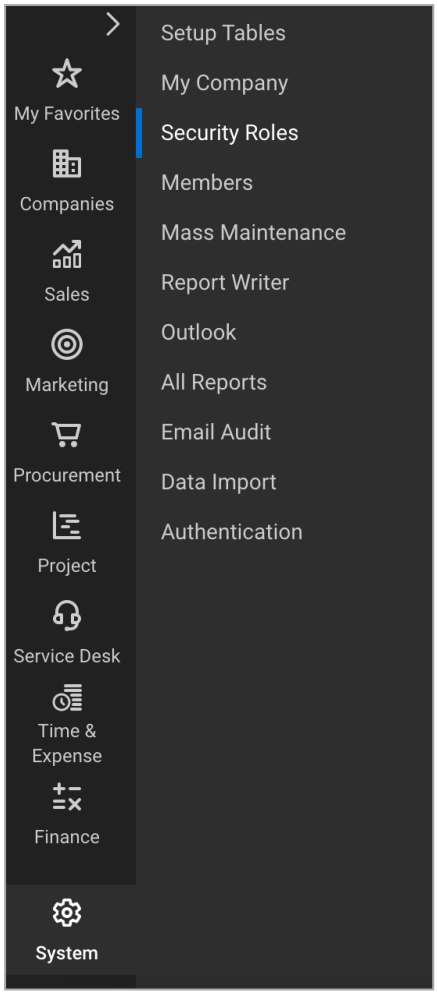
Note - This is available only for the accounts in the Perimeter 81 workspace.

Generating API Key in ConnectWise PSA

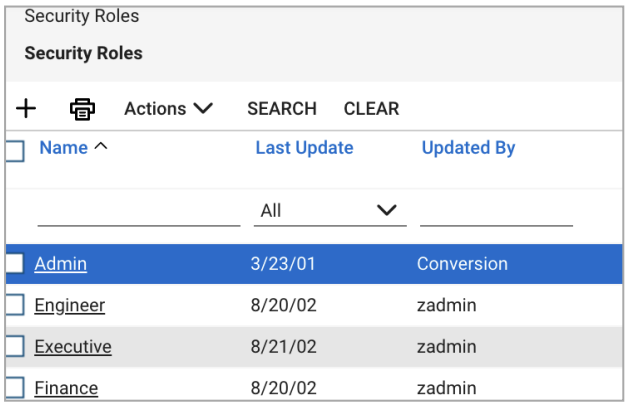
Harmony SASE uses an API key to authenticate the ConnectWise PSA integration.

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**

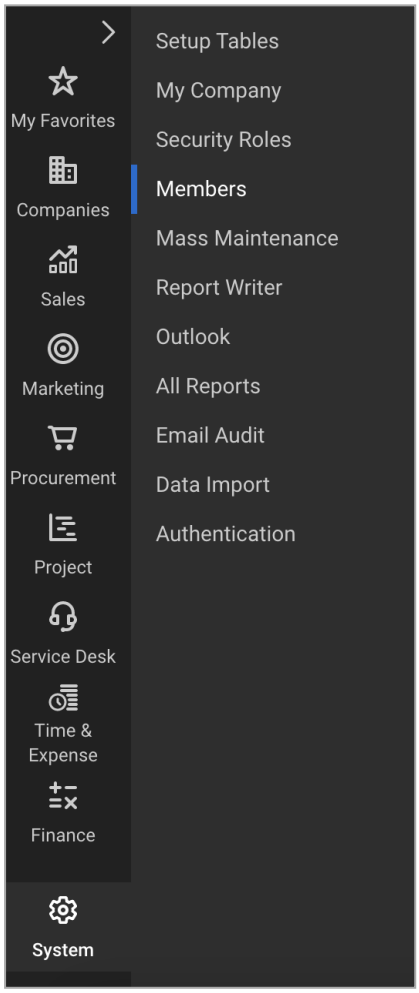
d. **Procurement** > **Product Catalog** > **Inquire Level= All**

e. **Procurement** > **Product Catalog** > **Add Level= All**

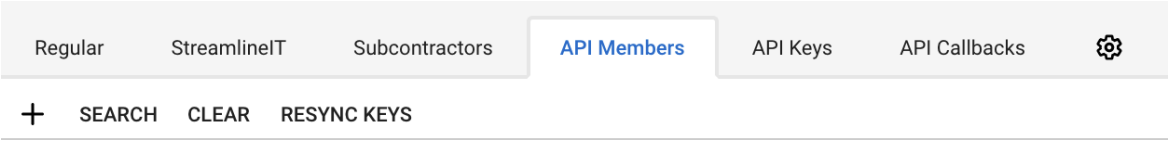
f. **System** > **Table setup** > **Inquire Level= All**

5. Click **Save**.

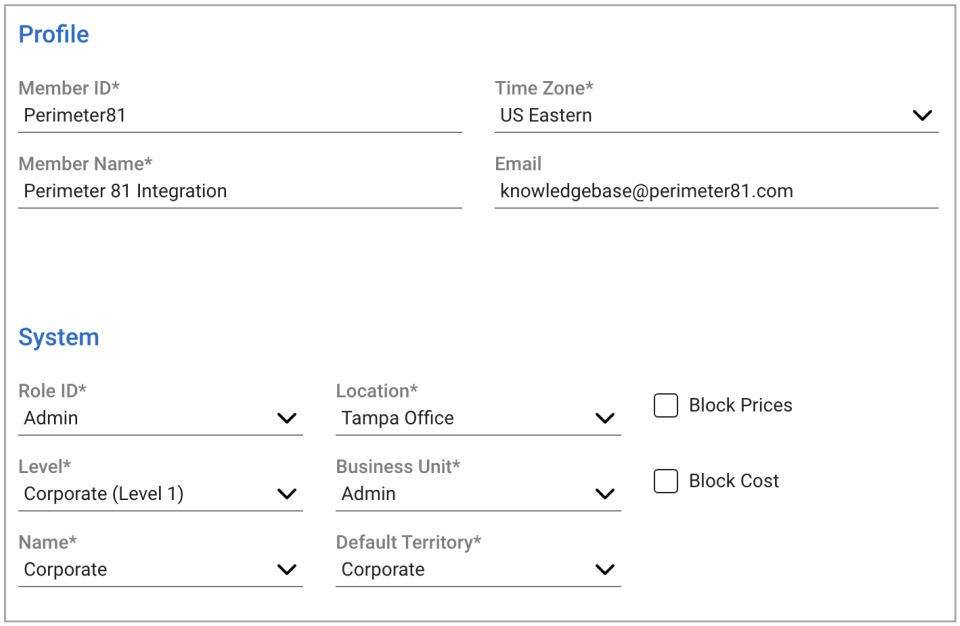
6. To generate the API key, from the **System** menu, click **Members**.



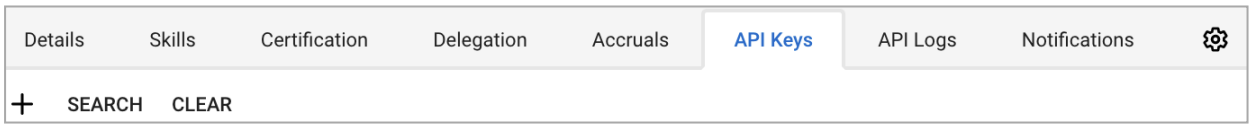
7. To add an API membership for Perimeter 81, click **API Members** tab and then click **+**.



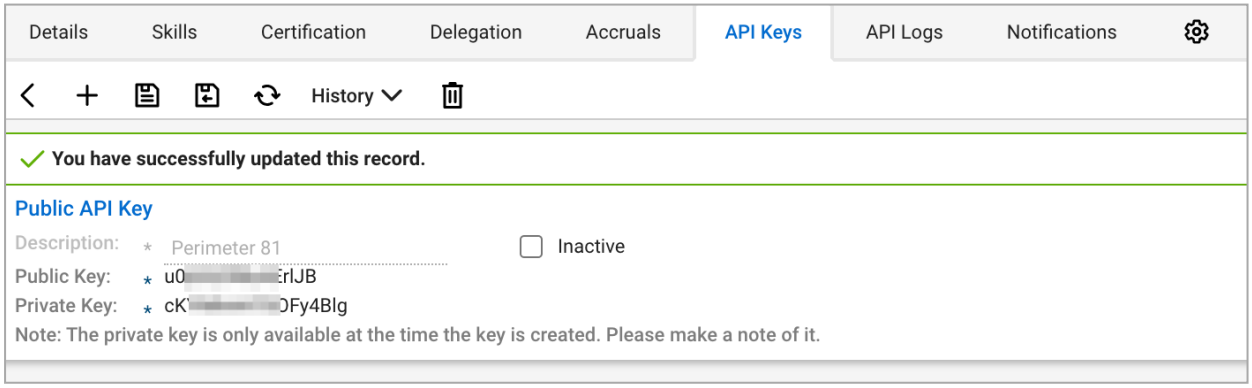
8. Enter the member details and click **Save**.



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.

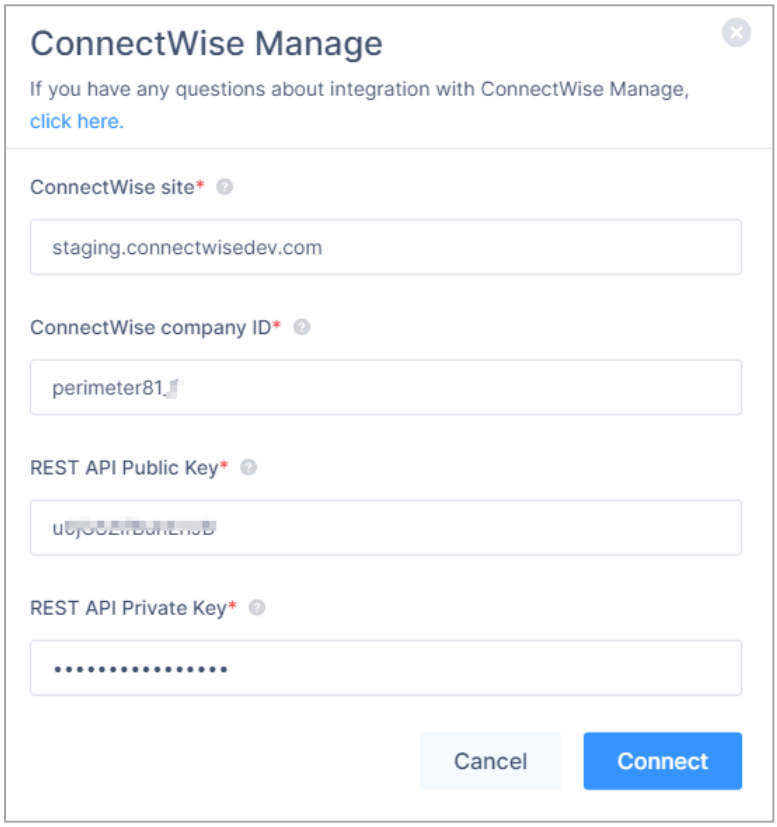


11. Copy the public and private keys.

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**.

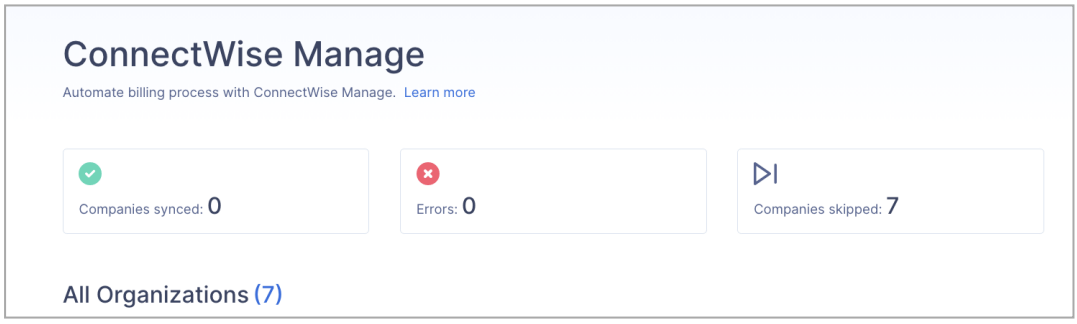
   The *ConnectWise integration has been configured successfully* message appears.

   After a successful integration, the Harmony SASE product catalog is synchronized with ConnectWise PSA.

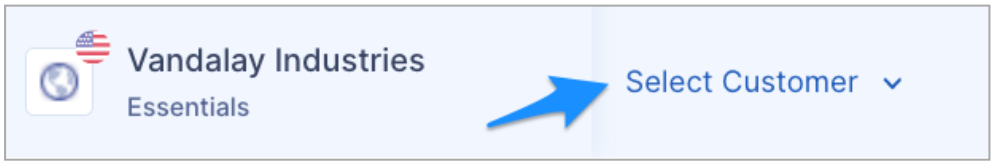
Mapping Customers and Agreements

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Integrations**.
2. In the **PSA integrations** section, in the **ConnectWise Manage** row, click **Manage**.

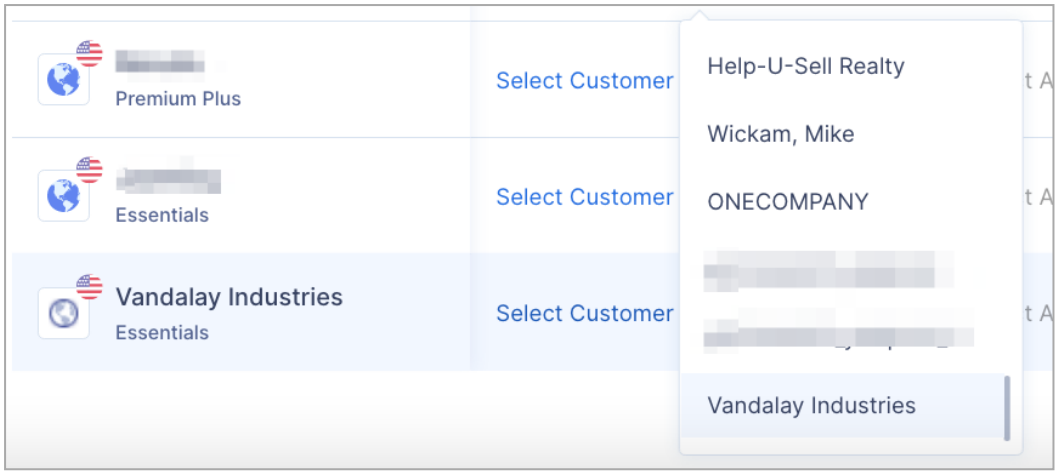
   The **ConnectWise Manage** page appears that displays all the organizations you manage in Perimeter 81.



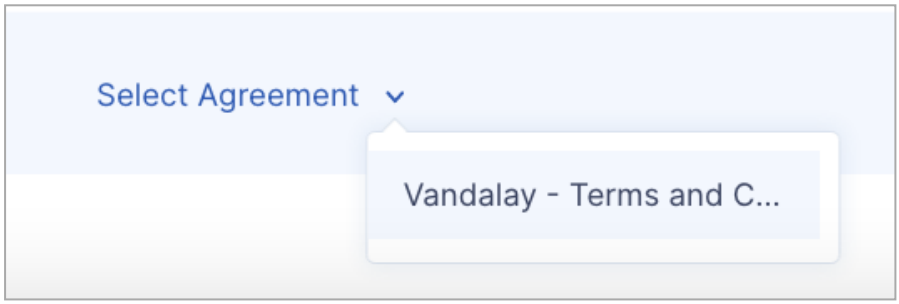
3. For the organization you want to sync with ConnectWise Manage, click **Select Customer**.



4. Select the corresponding account on ConnectWise Manage.

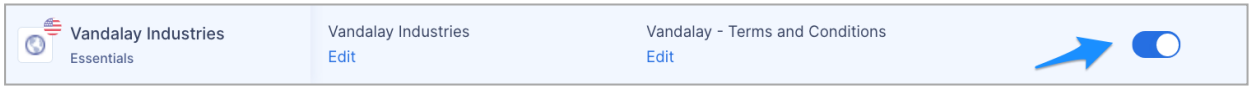


5. Select the ConnectWise Manage agreement that you have with your customer.



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 SASEAgent.

SAML 2.0

Harmony SASE allows users to authenticate using the third-party Identity Providers (IdP) that support Security Assertion Markup Language (SAML) 2.0 protocol.

SAML-based authentication involves two parties:

- Identity Provider (IdP): Authenticates the user and if successful, it provides a *SAML Assertion* to the Service Provider (SP).
- Service Provider (SP): Checks the *SAML Assertion* and if successful, it allows the user to access the service.

Harmony SASE serves as the Service Provider (SP) to authenticate the users and integrates with these Identity Providers that support SAML 2.0 protocol:

Generic SAML

Prerequisites

- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

Step 1 - Configure the SAML Identity Provider

To integrate Harmony SASE with a Generic SAML IdP, create a dedicated Harmony SASE Application in your SAML Identity Provider using these values:

- **Single Sign-On URL**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
- **Audience URI (SP Entity ID)**: `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
- Map these user attributes to Harmony SASE:

User Attributes		Harmony SASE Mapping
IdP Attribute	IdP Object	
Email Address	-	email
First Name	-	given_name
Last Name	-	family_name
-	Groups	groups

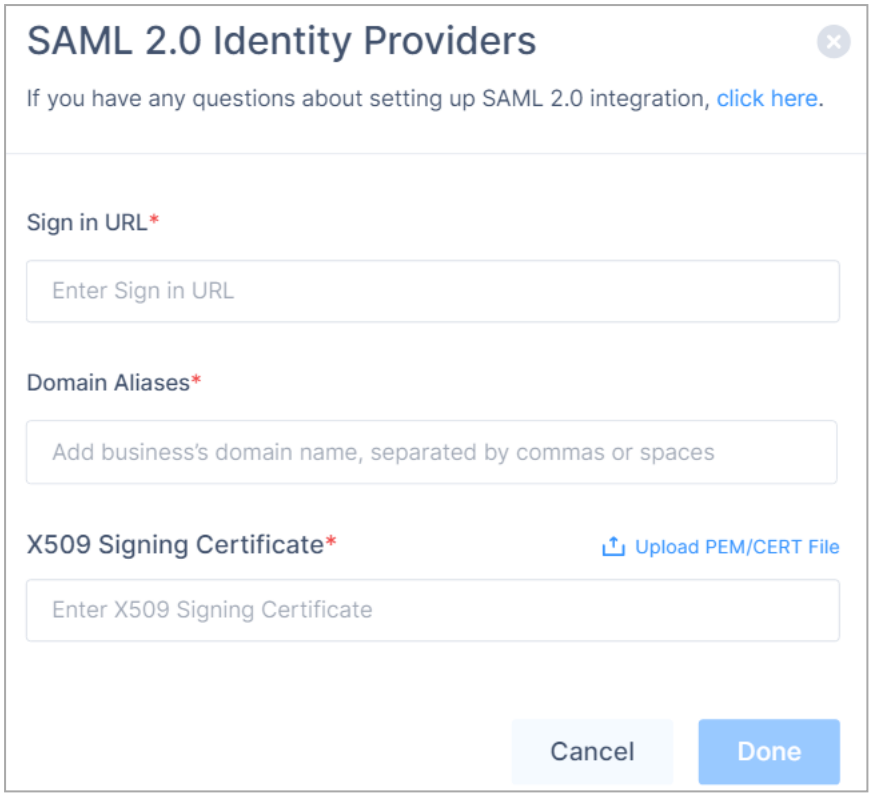
After creating the application, copy these values:

- Identity Provider Sign-in URL
- X.509 Certificate

Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Active Directory Federation Services (AD FS)

Prerequisites

- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

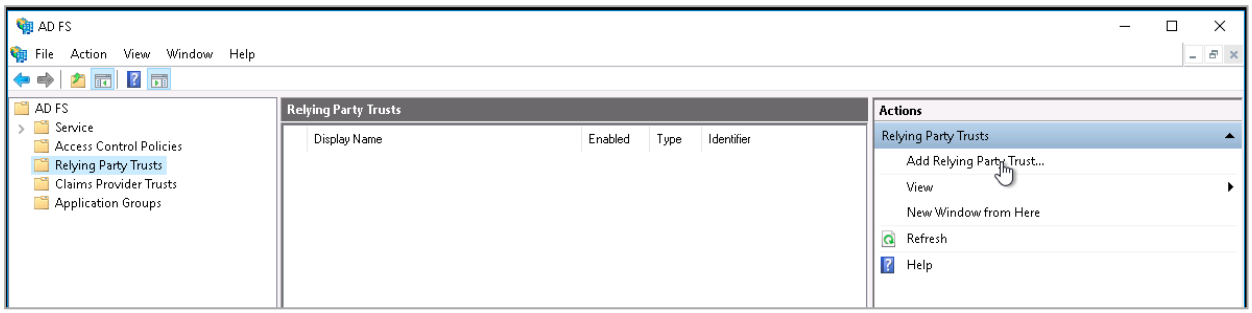
High-Level Procedure

- *"Step 1 - Configure the AD FS Management Portal" on the next page*
  1. *"Create a Relying Party Trust" on the next page*
  2. *"Edit Claim Issuance Policy" on page 736*
  3. *"Export the Signing Certificate" on page 737*
- *"Step 2 - Configure the Harmony SASE Administrator Portal" on page 739*

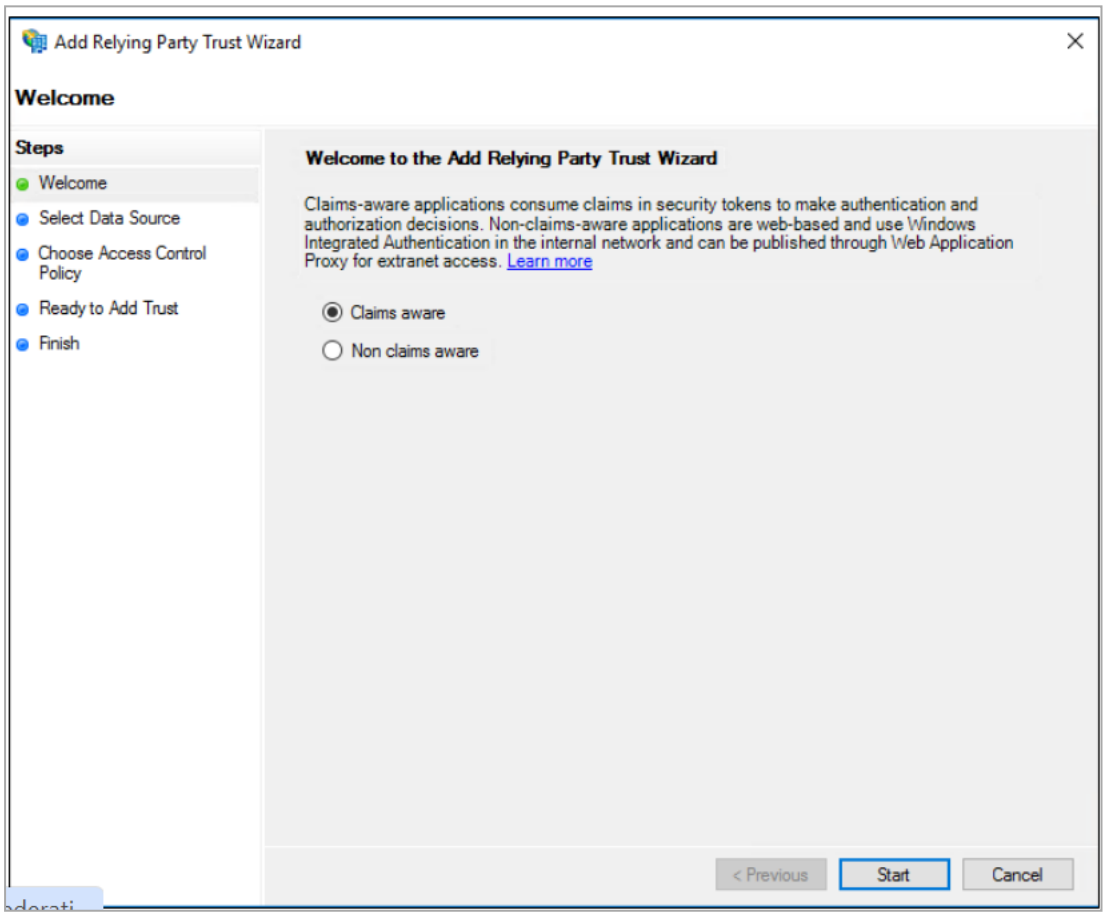
Step 1 - Configure the AD FS Management Portal

Create a Relying Party Trust

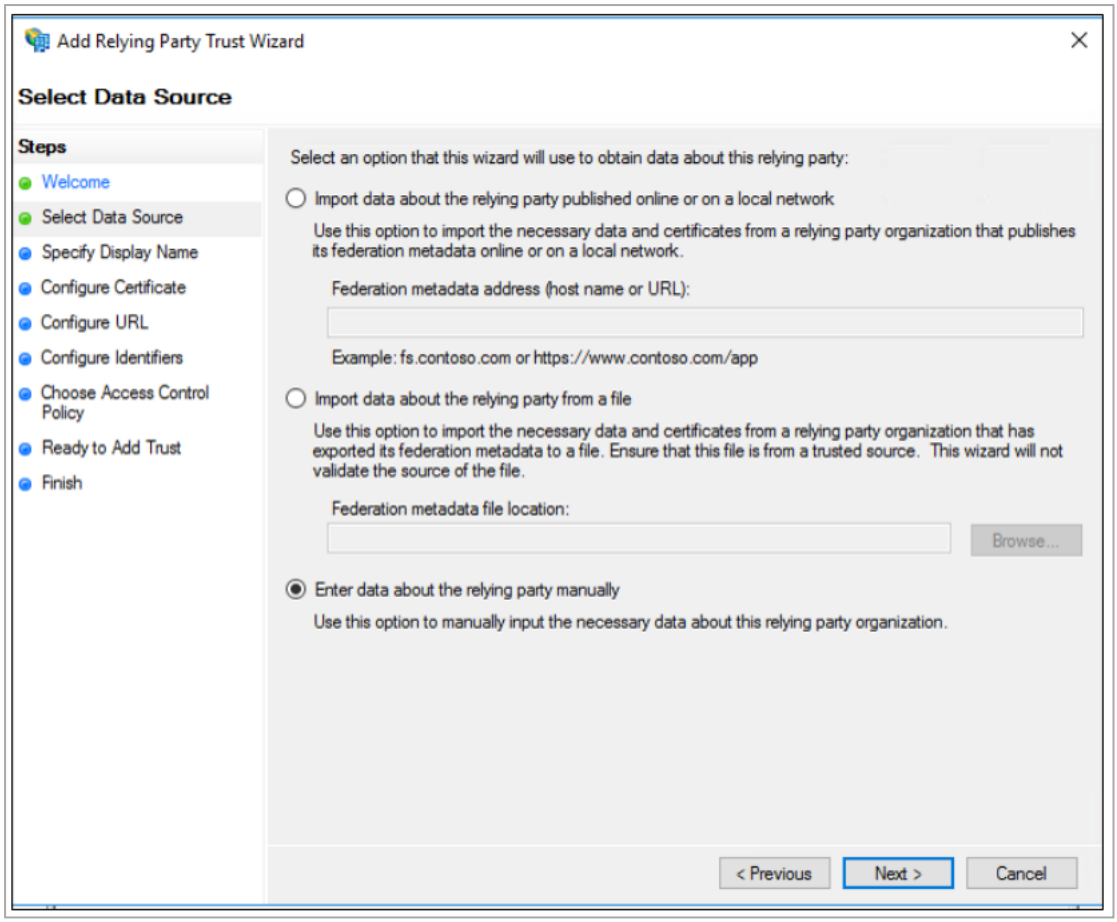
1. In the **Server Manager**, click **Tools**, and then select **AD FS Management**.
2. Under **Actions**, click **Add Relying Party Trust**.



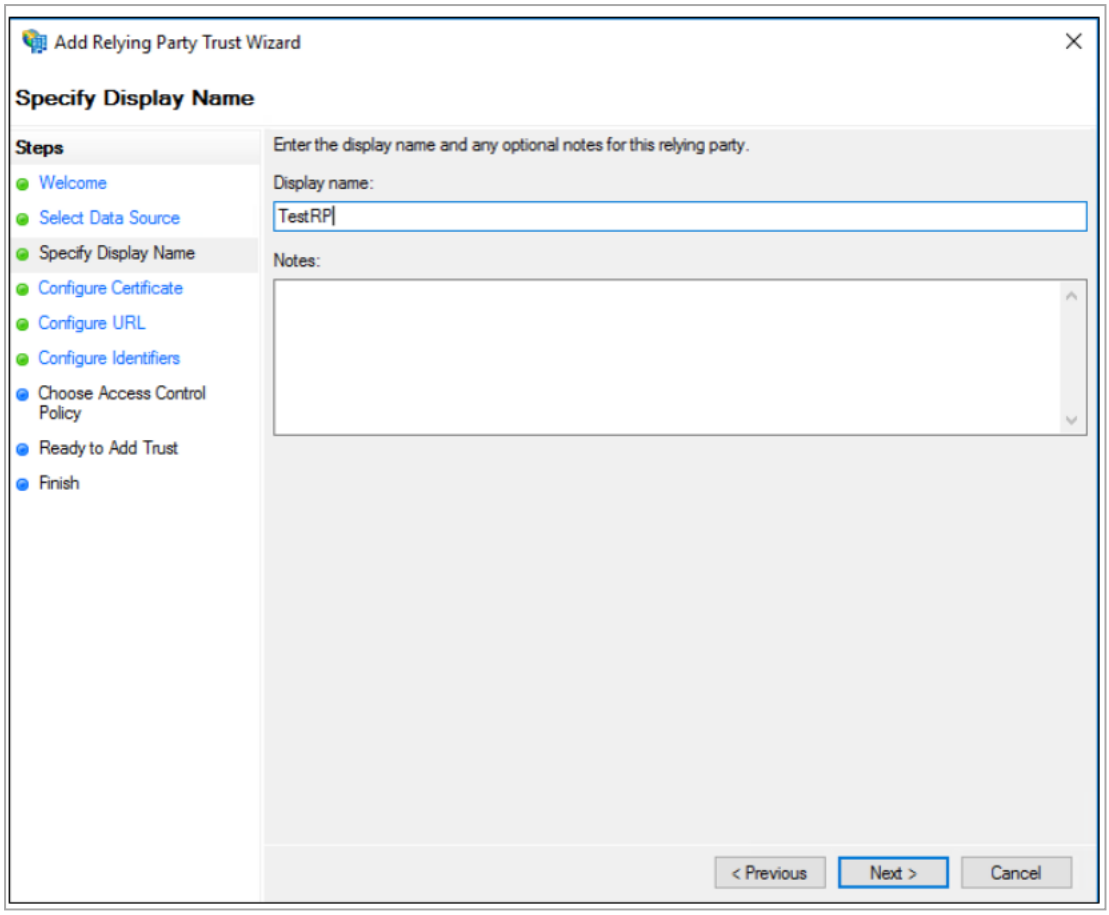
3. On the **Welcome** page, choose **Claims aware** and click **Start**.



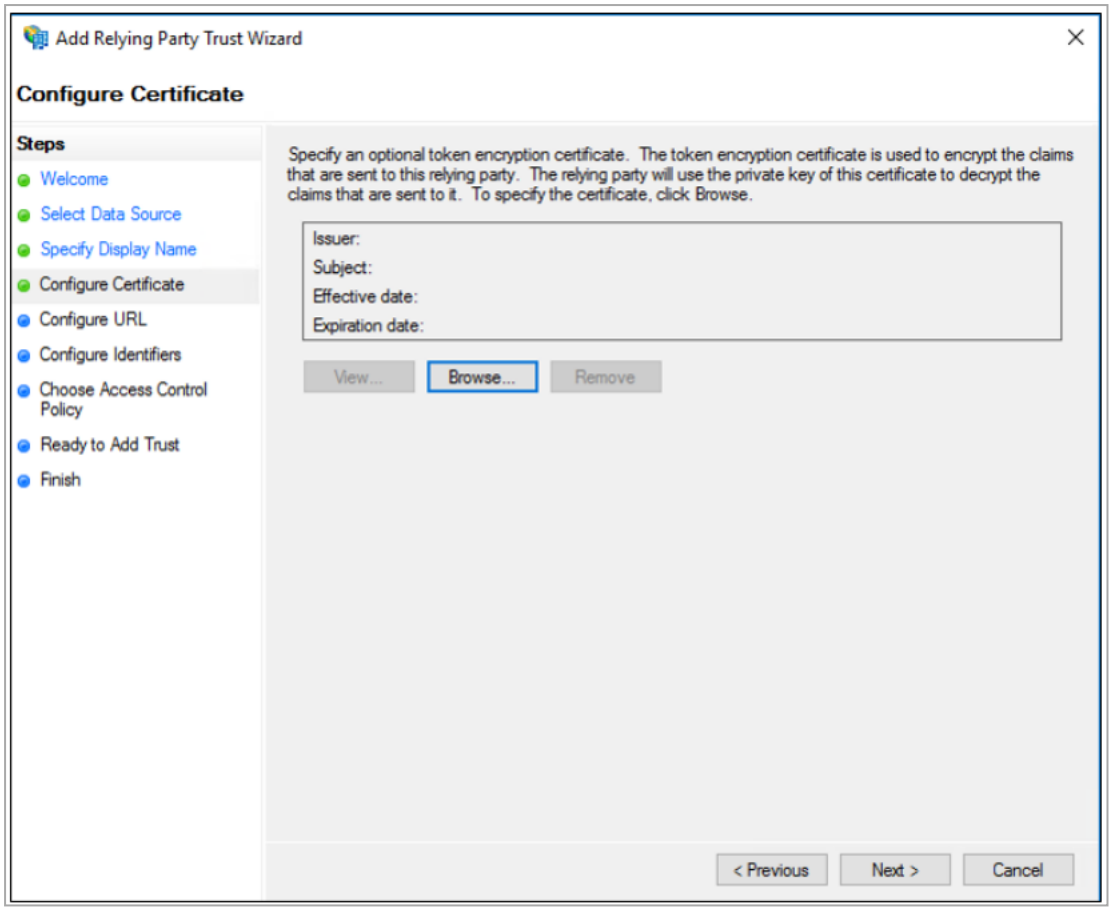
4. On the **Select Data Source** page, click **Enter data about the relying party manually**, and then click **Next**.



5. On the **Specify Display Name** page, type a name in **Display name**, under **Notes** type a description for this relying party trust, and then click **Next**.



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



7. On the **Configure URL** page:
   a. Select the **Enable support for the SAML 2.0 WebSSO protocol** checkbox.
   b. Under **Relying party SAML 2.0 SSO service URL**, enter `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   c. Click **Next**.
8. On the **Configure Identifiers** page:
   a. Enter the Relying party trust identifier as `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   b. Click **Add** to add it to the list, and then click **Next**.
9. On the **Choose Access Control Policy** page, select **Permit everyone** and then click **Next**.
10. On the **Ready to Add Trust** page, review the settings, and then click **Next** to save your relying party trust information.

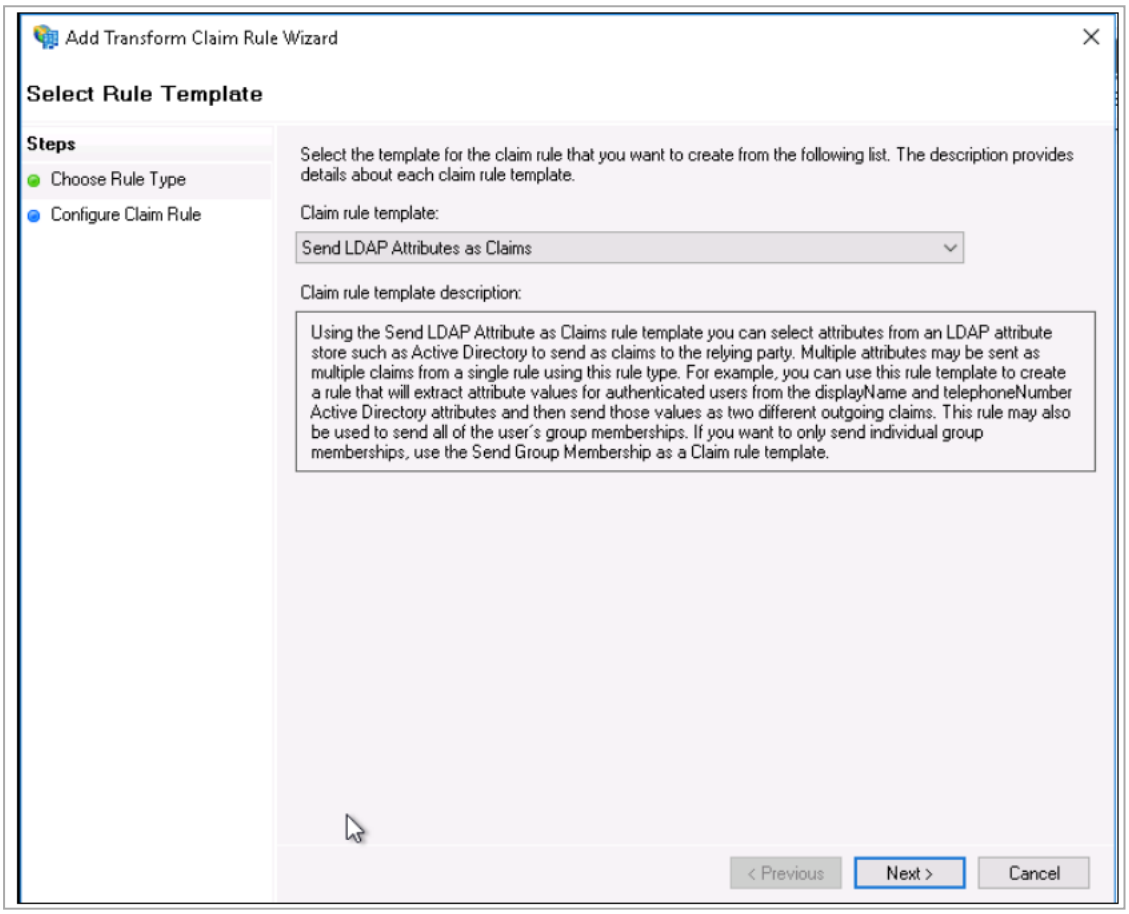
11. On the **Finish** page, make sure that the **Configure claims issuance policy for this application** checkbox is selected, and then click **Close**.

    This action automatically shows the **Edit Claim Issuance Policy** dialog box.

Edit Claim Issuance Policy

After you have created the Relying Party Trust, the **Edit Claim Issuance Policy** dialog box appears.

1. Click **Add Rule** to launch the wizard.
2. In the **Claim rule template** drop-down, select **Send LDAP Attributes as Claims** and click **Next**.



3. Enter a value for the **Claim rule** name, such as **LDAP Attributes**.
4. Choose **Active Directory** as your **Attribute Store**.
5. Map the **LDAP attributes** to these outgoing claim types:

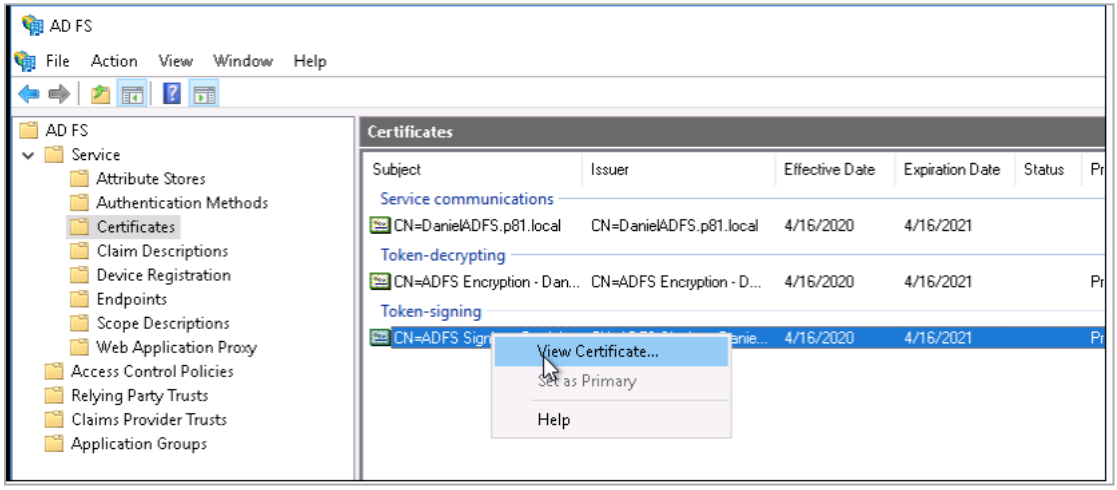
LDAP Attribute	Claim Type
E-mail Addresses	email

LDAP Attribute	Claim Type
Given-Name	given_name
Surname	family_name
Token-Groups Unqualified-Names	groups
User-Principal-Name	user_id

6. Click **Finish**.
7. In the **Edit Claim Issuance Policy** window, click **Apply**.

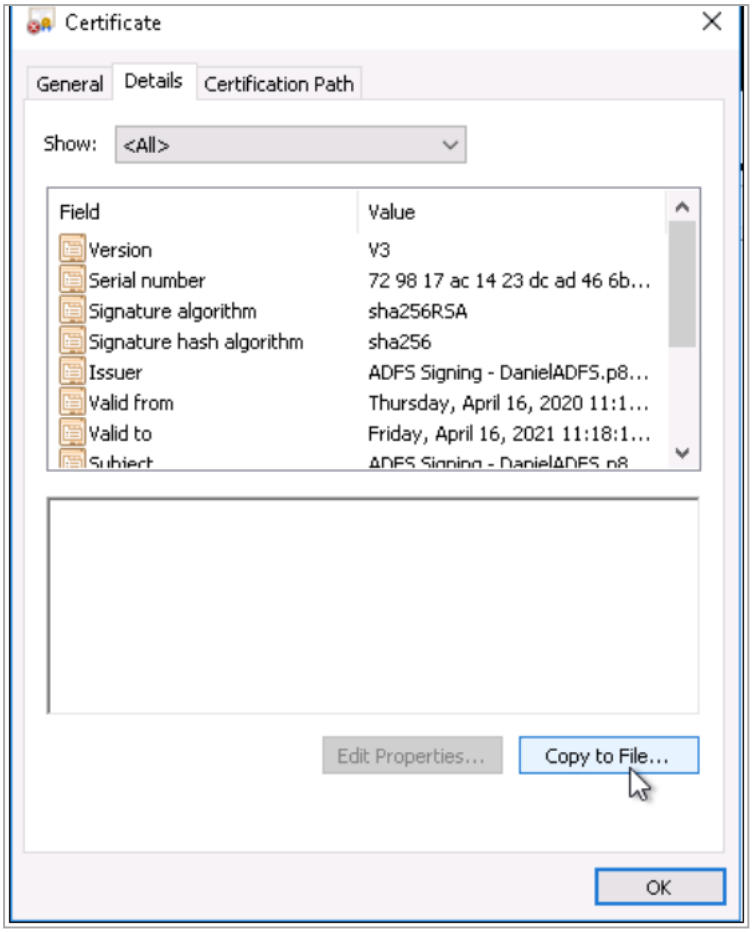
Export the Signing Certificate

1. From the left navigation pane, click **AD FS** > **Service** > **Certificates**.
2. Right-click **Token-signing** and then select **View Certificate**.

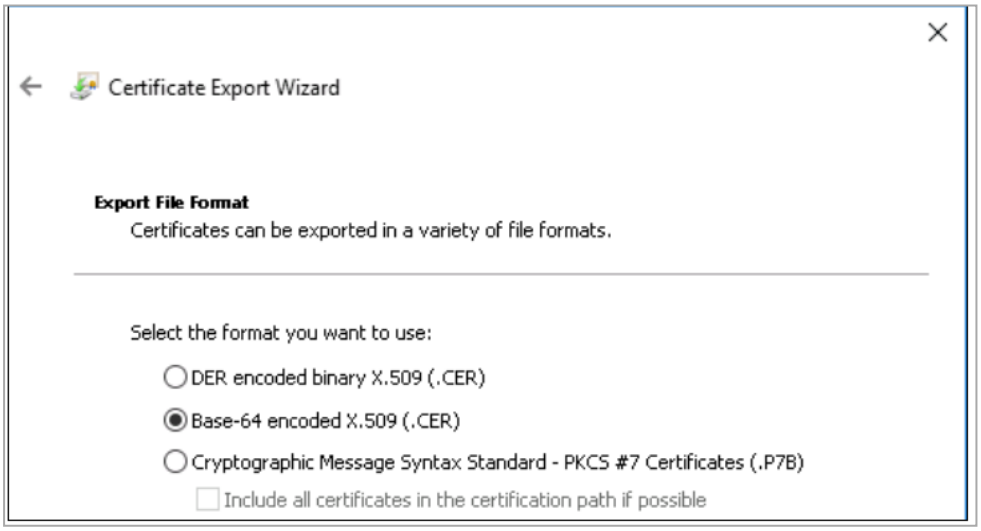


The **Certificate** pop-up appears.

3. Go to the **Details** tab, and click **Copy to File**.



4. In the **Certificate Export Wizard**, click **Next**.
5. Select the file format as **Base-64 encoded X.509 (.CER)** and then click **Next**.

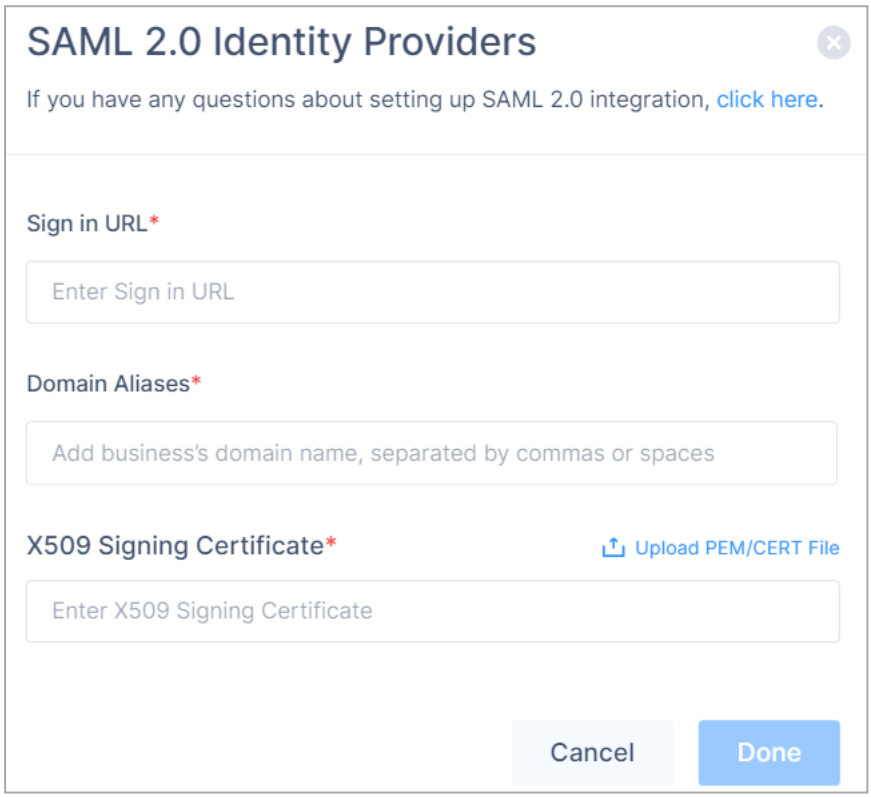


6. Select the location where you want to export the certificate and click **Next**.
7. Click **Finish**.

Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`

Identity Provider	Sign in URL
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Auth0

Prerequisites

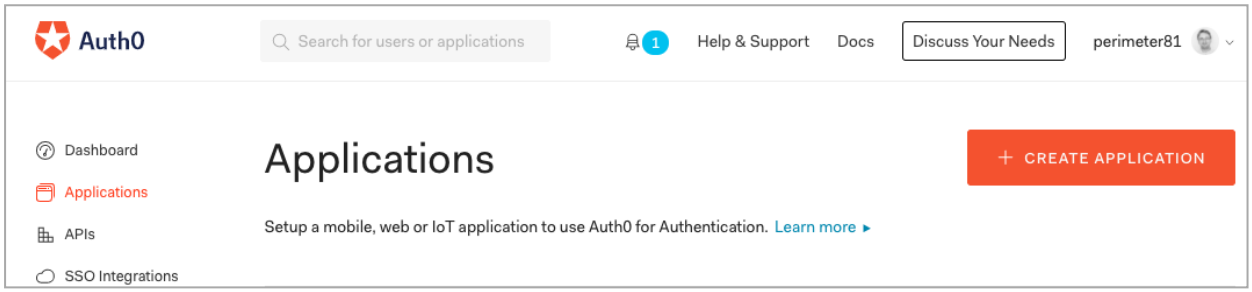
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

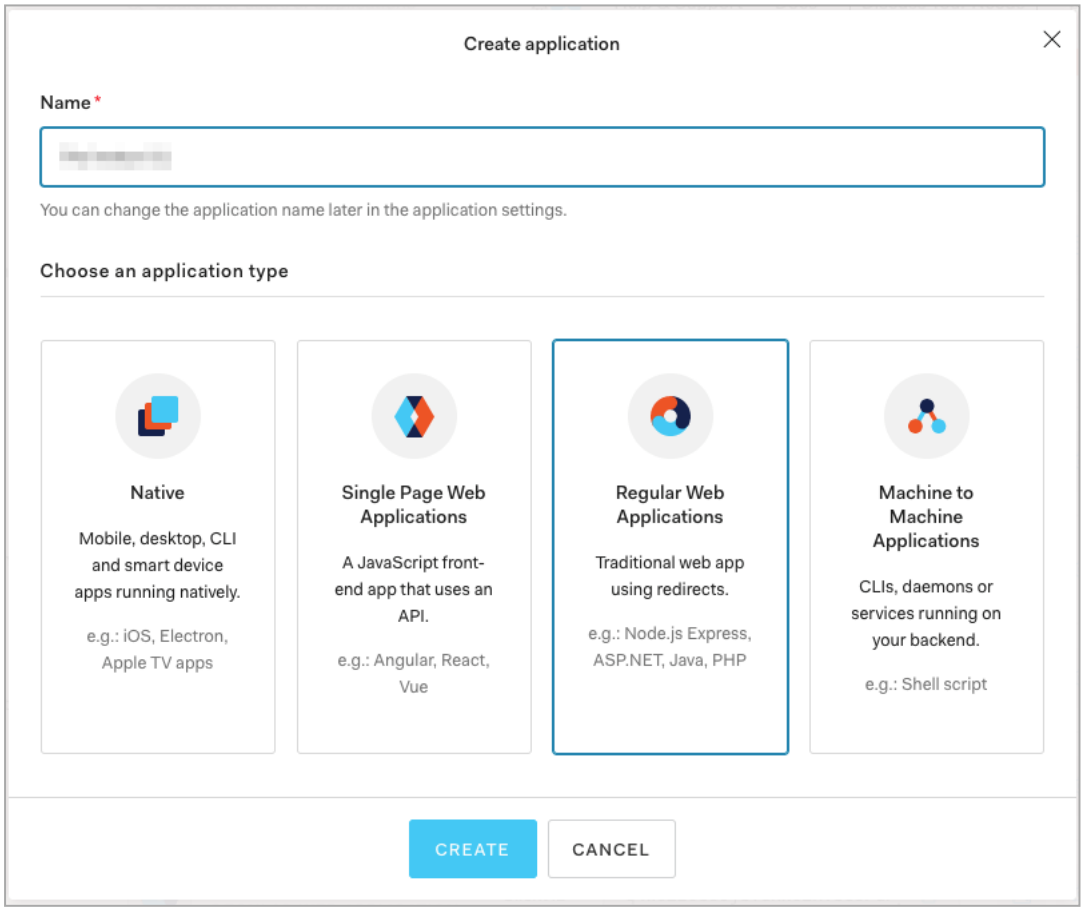
- *"Step 1 - Configure the Auth0 Management Portal" below*
- *"Step 2 - Configure the Harmony SASE Administrator Portal" on page 744*

Step 1 - Configure the Auth0 Management Portal

1. Log in to Auth0 Management Portal.
2. From the left navigation pane, click **Applications**.
3. Click **Create Application**.

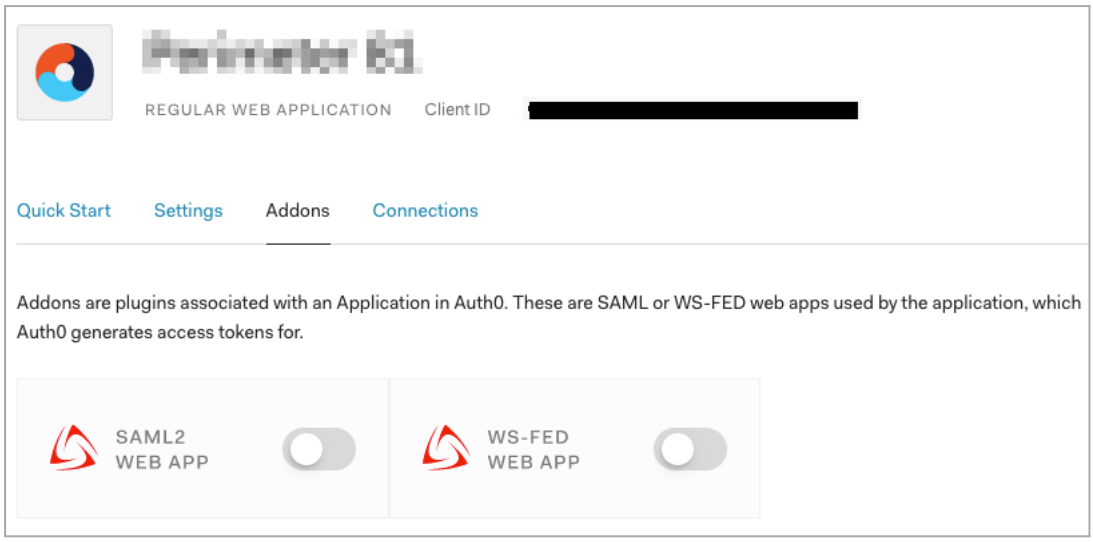


4. In the **Name** field, enter a name for the application.



5. Select **Regular Web Application** and click **Create**.

6. Go to **Addons** tab and toggle **SAML2 Web App** to **ON**.



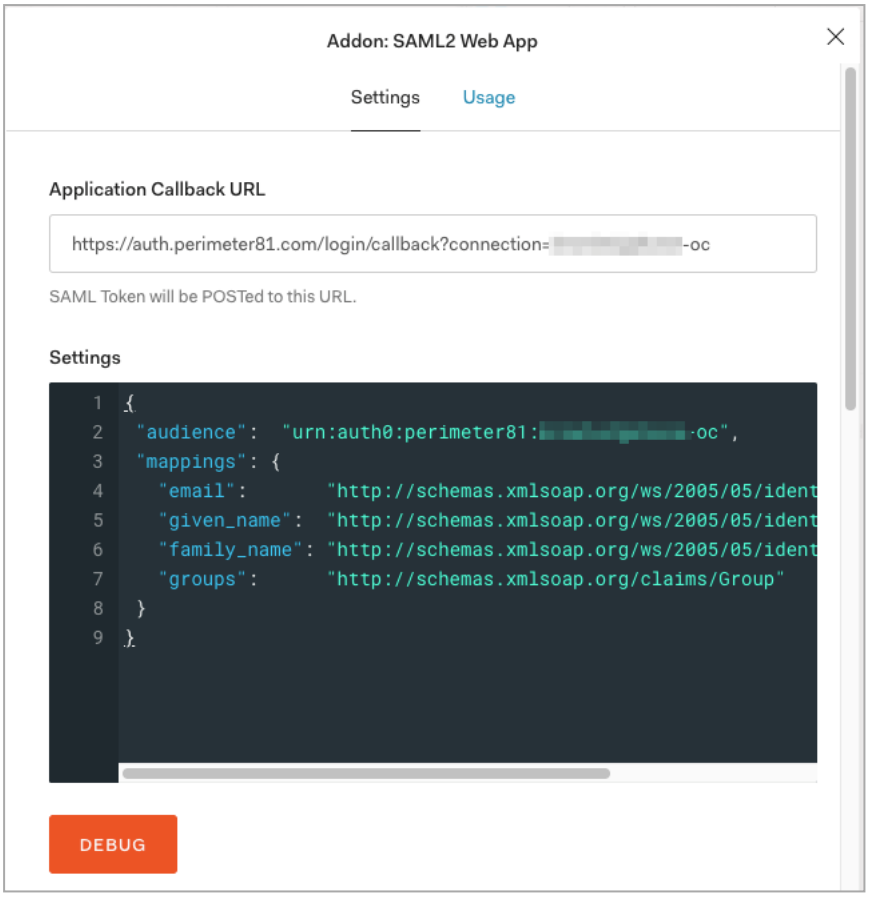
The **SAML2 Web App** window appears.

7. In the **Settings** tab, enter these values:

   - **Application Callback URL**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.

- **Settings**: Copy the code, replace `{{WORKSPACE}}` with your Harmony SASE workspace name and paste it in **Settings**.

```
{

"audience": "urn:auth0:perimeter81:{{WORKSPACE}}-oc",

"mappings": {

"email":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emaila
ddress",

"given_name":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn
ame",

"family_name":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surnam
e",

"groups": "http://schemas.xmlsoap.org/claims/Group"

}

}
```

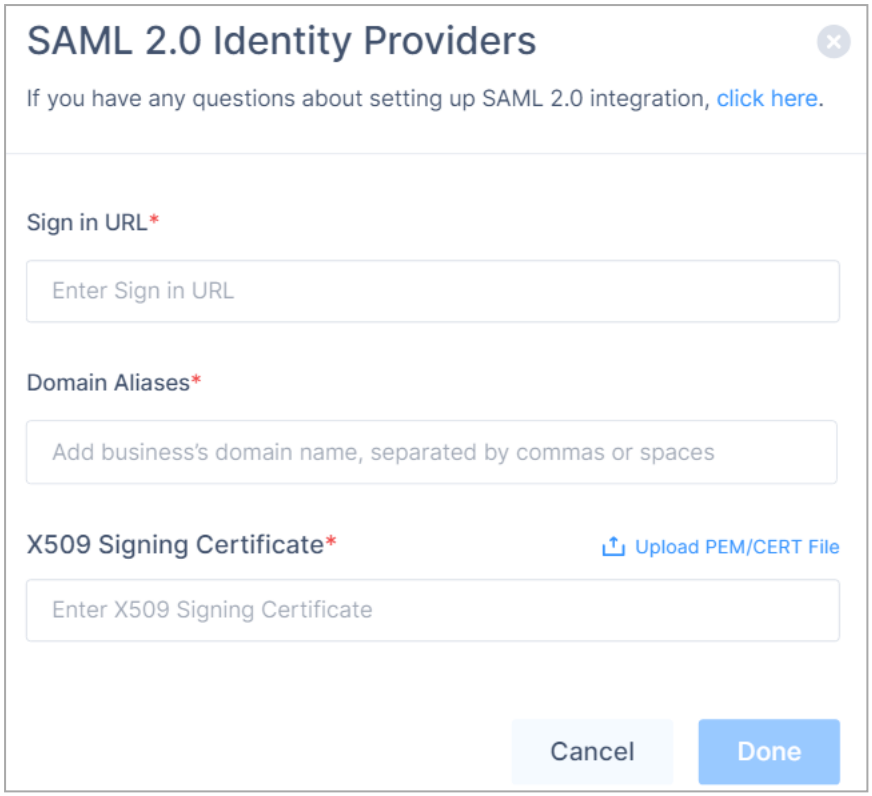


8. Click **Enable** to save and activate the application.
9. Click **Debug** and verify your configuration.
10. Go to the **Usage** tab.
11. Click **Download Auth0 certificate**.
12. Copy the **Identity Provider Login URL**.

Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Keycloak

Harmony SASE can authenticate users through Keycloak, ensuring a secure and efficient login process by utilizing the Security Assertion Markup Language (SAML) protocol.

Prerequisites

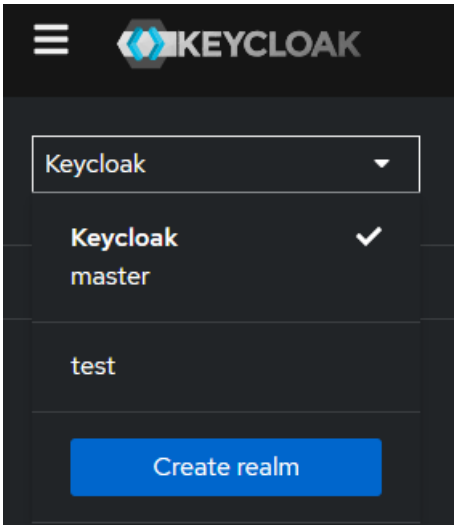
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

Integration Procedure

To configure Keycloak as an Identity Provider:

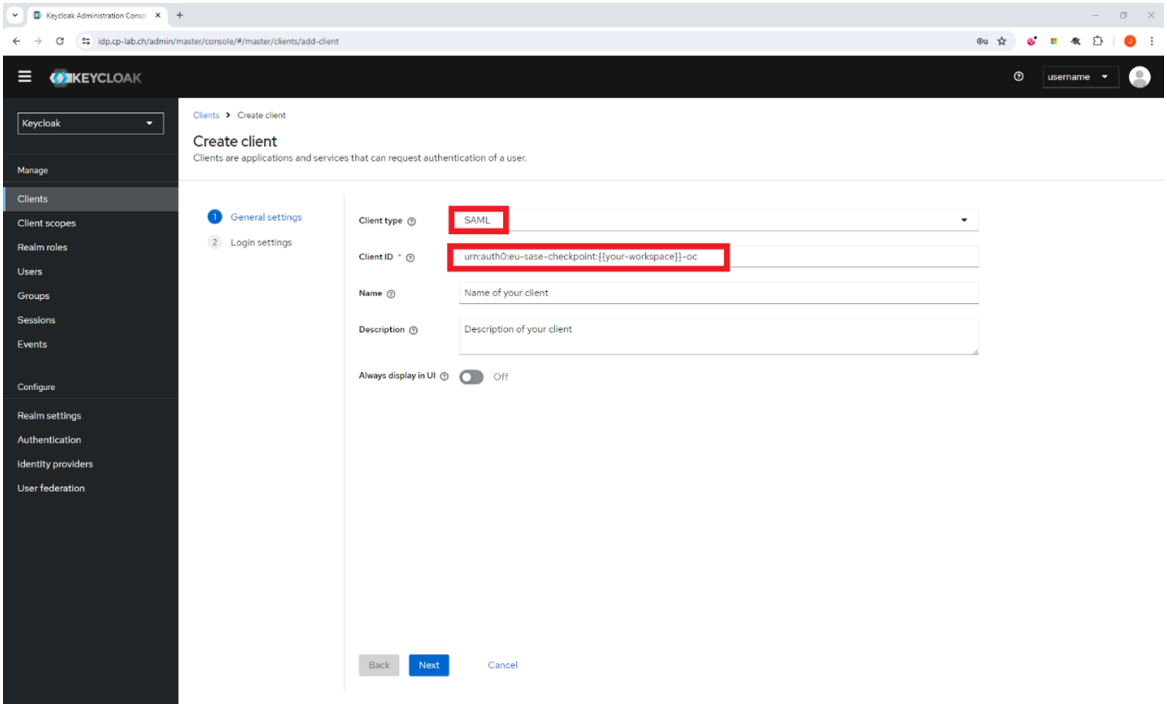
1. Log in to your Keycloak Administrator Console:

   a. Select the realm you want to configure.



   b. Go to **Clients** and click **Create client**.

   The **Create client** page appears.



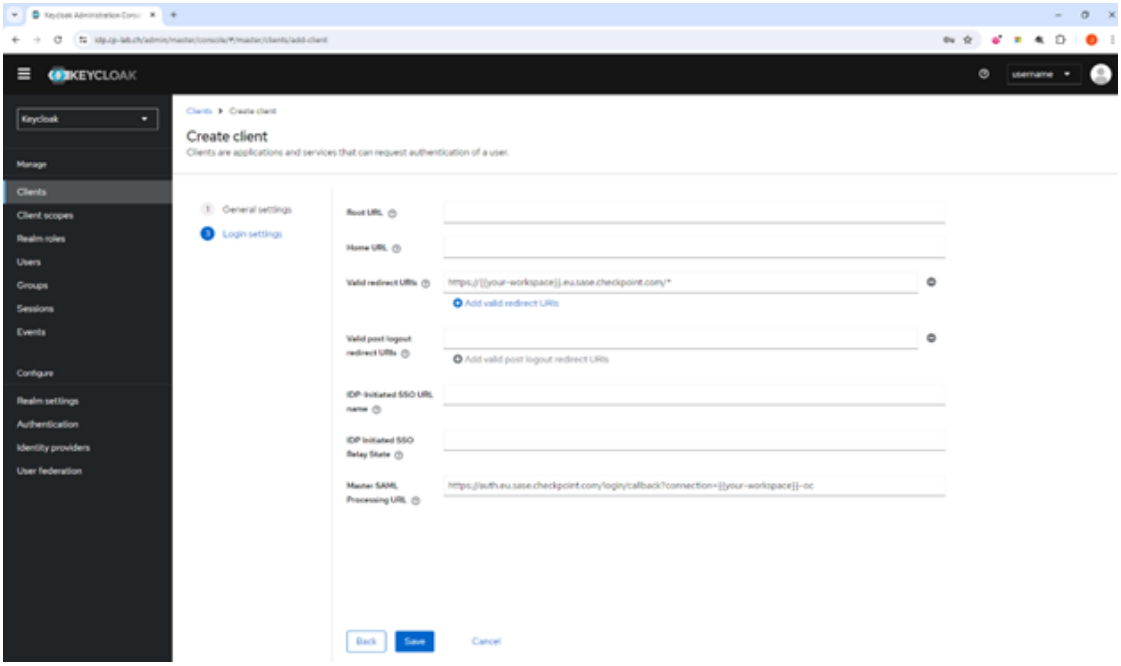
   c. From the **Client type** list, select SAML.

d. In the **Client ID** field, enter the audience URI (SP Entity ID) of your Harmony SASE workspace:

   - For US based platform - `urn:auth0:perimeter81:{{WORKSPACE}}-oc`
   - For EU based platform - `urn:auth0:eu-sase-checkpoint:{{WORKSPACE}}-oc`

     For example - acme.perimeter81.com workspace should translate to `urn:auth0:perimeter81:acme-oc`

e. Click **Next**.



f. In the **Valid redirect URIs** field, enter your workspace URL:

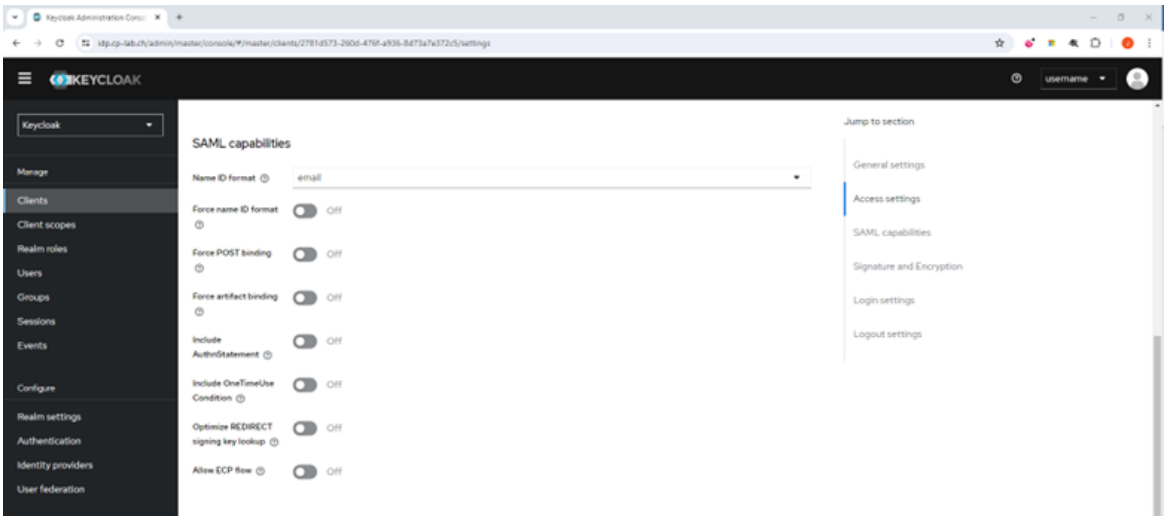
   - For US based platform - `https://{{your-workspace}}.perimeter81.com/*`
   - For EU based platform - `https://{{your-workspace}}.eu.sase.checkpoint.com/*`

g. In the **Master SAML Processing URL** field, enter your Single sign-on URL:

   - For US based platform - `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
   - For EU based platform - `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

h. Click **Save**.

i. Go to **Access capabilities** and do these in the **SAML capabilities** section.

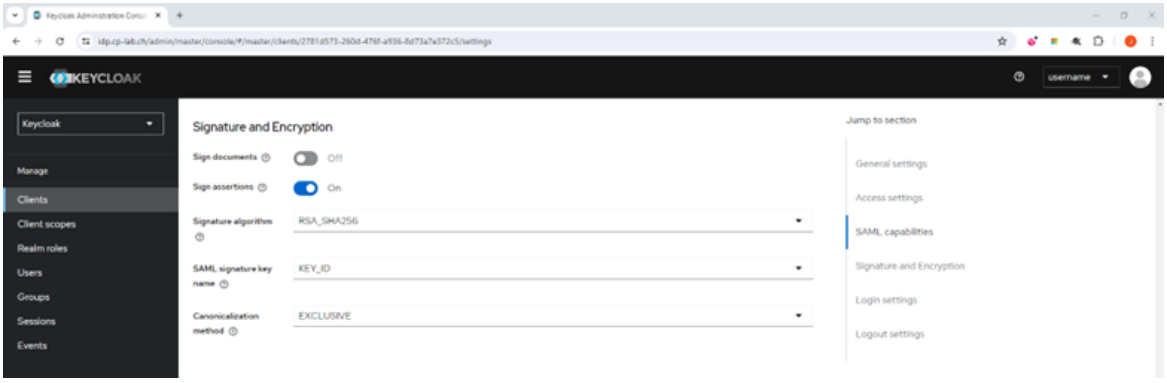


j. From the **Name ID format** list, select your email address.

k. Turn off the **Force POST billing** toggle button.

l. Turn off the **Include AuthnStatement** toggle button.

m. Go to the **Signature and Encryption** section.



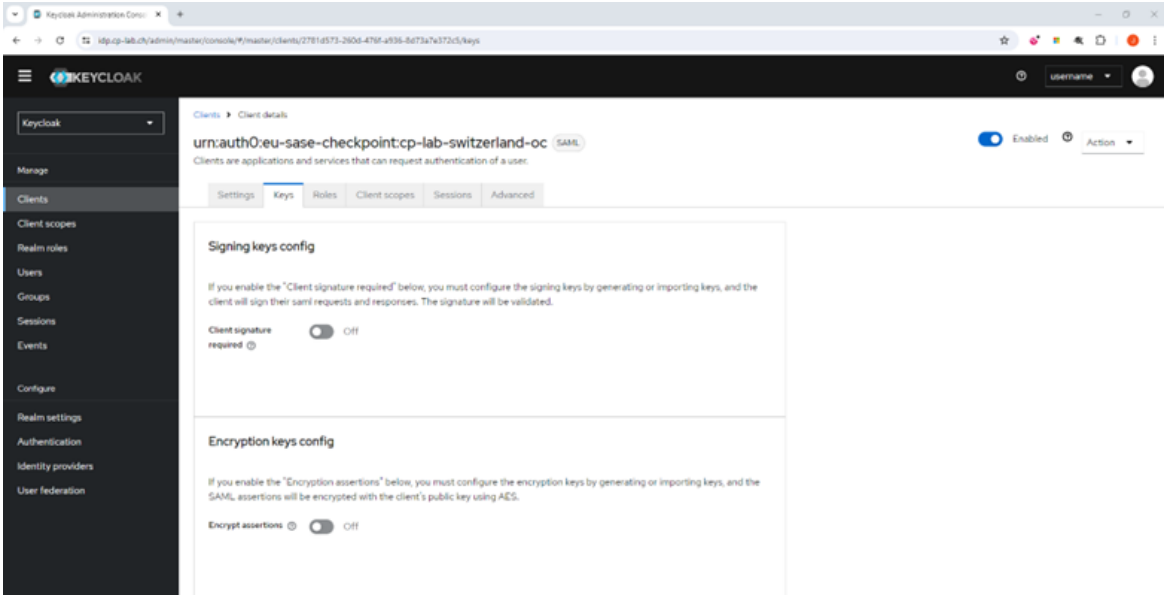
n. Turn off the **Sign documents** toggle button.

o. Turn off the **Sign assertion** toggle button.

p. From the **Signature algorithm** list, select **RSA_SHA256**.

q. From the **SAML signature key name** list, select **KEY_ID**.

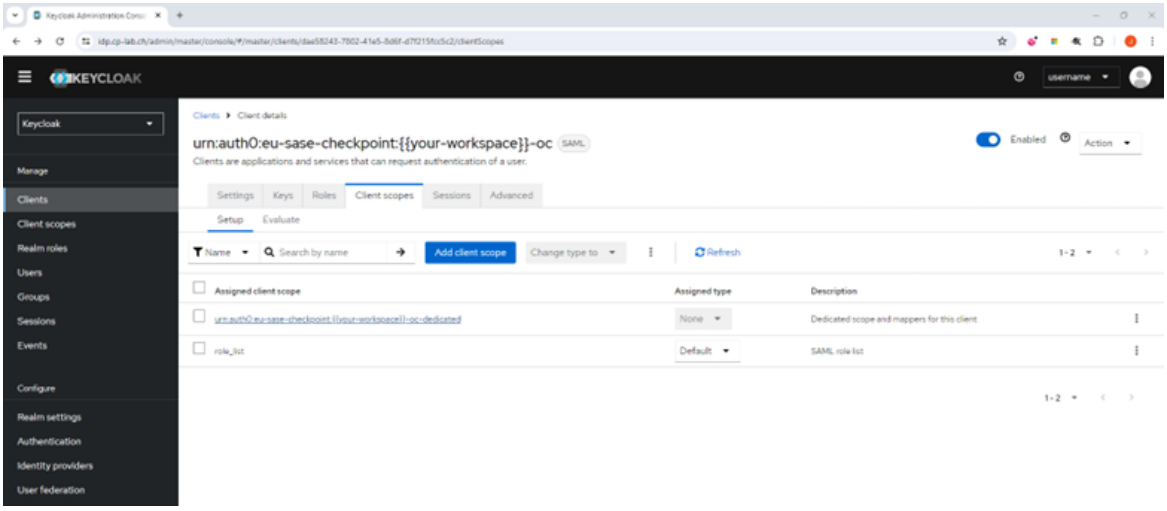
r. Click the **Keys** tab.



s. Turn off the **Client signature required** toggle button.

t. Turn off the **Encrypt assertions** toggle button.

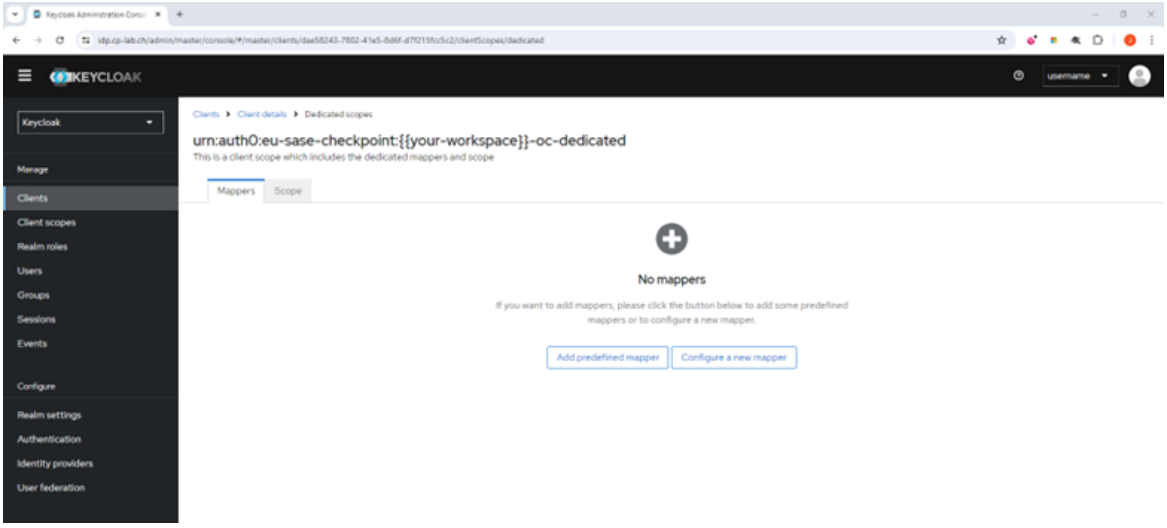
u. Click the **Client scopes** tab.



v. Select the assigned client scope named as your audience URI (SP Entity ID), for example, the name starts with `urn:auth0`.

w. Click the **Mappers** tab.

x. Click **Add predefined mapper**.



y. Select these checkboxes:

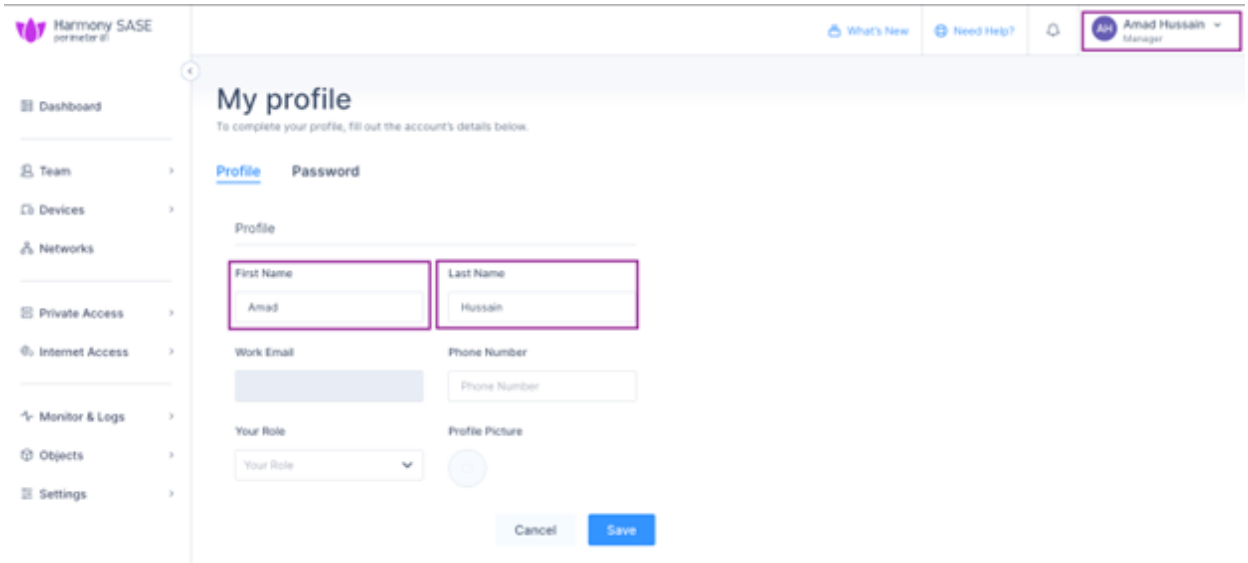
   i. **X500 email**

   ii. **X500 givenName**

   iii. **X500 surname**

   This configuration permits to pass through the SAML response the Users given name and surname.

2. To map the user profile, log in to the Harmony SASE Administrator Portal, click your profile icon at the top right corner and enter these:

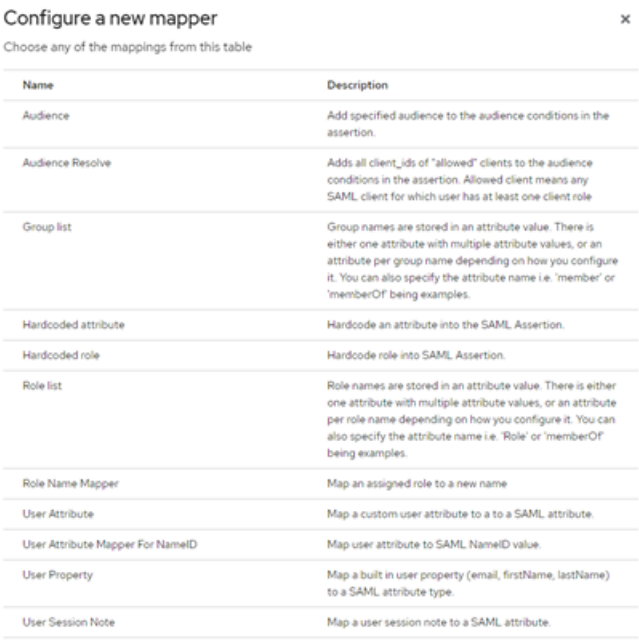


- **First Name**
- **Last Name**

Note - The groups in Keycloak must match the groups in Harmony SASE to be able to add the users into the corresponding groups in Harmony SASE.

3. Log in to your Keycloak Administration Console:

   a. (Optional) Select **Add mapper**, then **By configuration** and select **Group list** to pass Group membership to Harmony SASE.

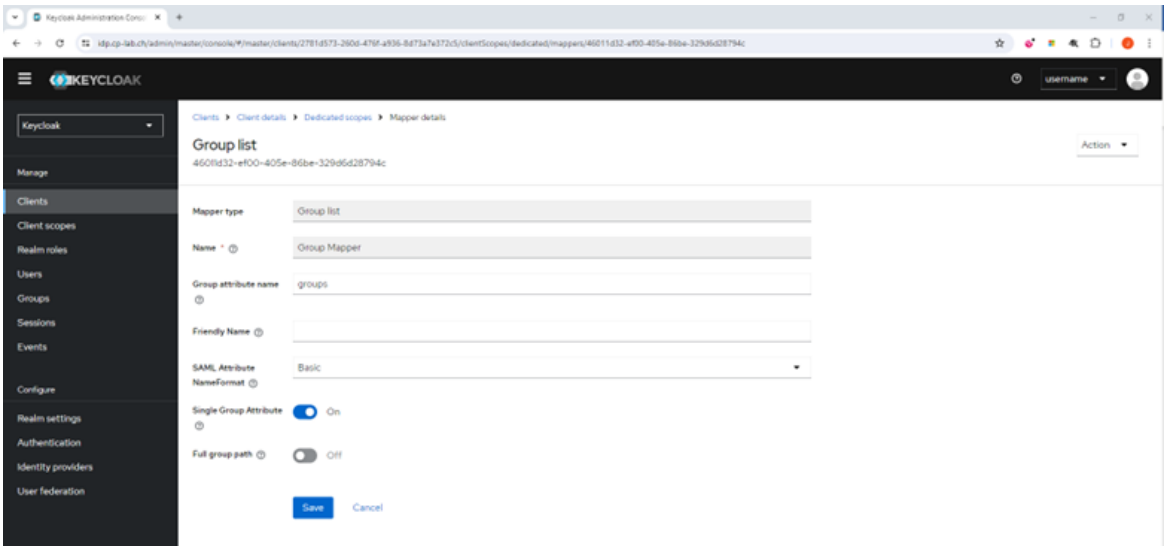


Configure a new mapper

Choose any of the mappings from this table

Name	Description
Audience	Add specified audience to the audience conditions in the assertion.
Audience Resolve	Adds all client_ids of "allowed" clients to the audience conditions in the assertion. Allowed client means any SAML client for which user has at least one client role
Group list	Group names are stored in an attribute value. There is either one attribute with multiple attribute values, or an attribute per group name depending on how you configure it. You can also specify the attribute name i.e. 'member' or 'memberOf' being examples.
Hardcoded attribute	Hardcode an attribute into the SAML Assertion.
Hardcoded role	Hardcode role into SAML Assertion.
Role list	Role names are stored in an attribute value. There is either one attribute with multiple attribute values, or an attribute per role name depending on how you configure it. You can also specify the attribute name i.e. 'Role' or 'memberOf' being examples.
Role Name Mapper	Map an assigned role to a new name
User Attribute	Map a custom user attribute to a to a SAML attribute.
User Attribute Mapper For NameID	Map user attribute to SAML NameID value.
User Property	Map a built in user property (email, firstName, lastName) to a SAML attribute type.
User Session Note	Map a user session note to a SAML attribute.

   b. In the **Name** field, enter **Group Mapper**.



   c. In the **Group attribute name** field, enter **groups**.

   d. From the **SAML Attribute NameFormat** list, select **Basic**.

   e. Turn on the **Single Group Attribute** toggle button.

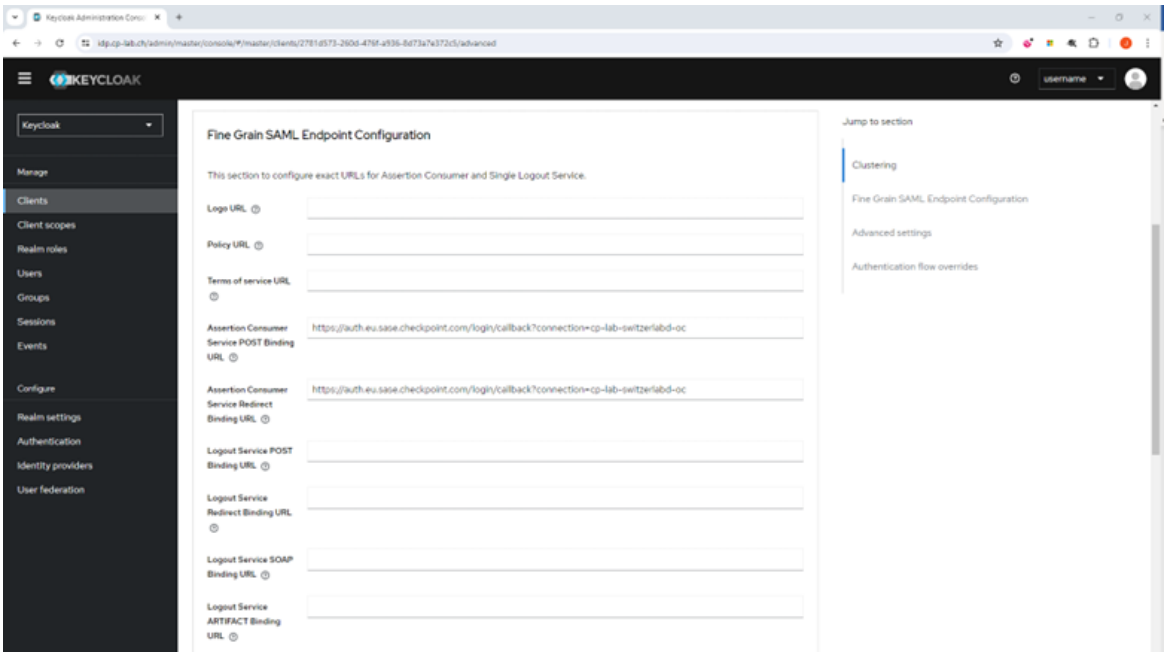
f. Turn off the **Full group path** toggle button.

g. Click **Save**.

h. Go to **Clients** and then click **Create client**.

i. Click the **Advanced** tab.

j. Click **Fine Grain SAML Endpoint Configuration**.



k. In the **Assertion Consumer Service POST Binding URL** field, enter your Single sign-on URL:

- For US based platform - `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc`
- For EU based platform - `https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc`

l. In the **Assertion Consumer Service Redirect Binding URL** field, enter your Single sign-on URL:

- For US based platform - **https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc**
- For EU based platform - **https://auth.eu.sase.checkpoint.com/login/callback?connection={{WORKSPACE}}-oc**

m. Click **Save**.

n. To collect Sign-in URL and X509 Signing Certificate of your realm to configure the Identity Providers configuration in Harmony SASE:

o. Go to **Realm settings**.

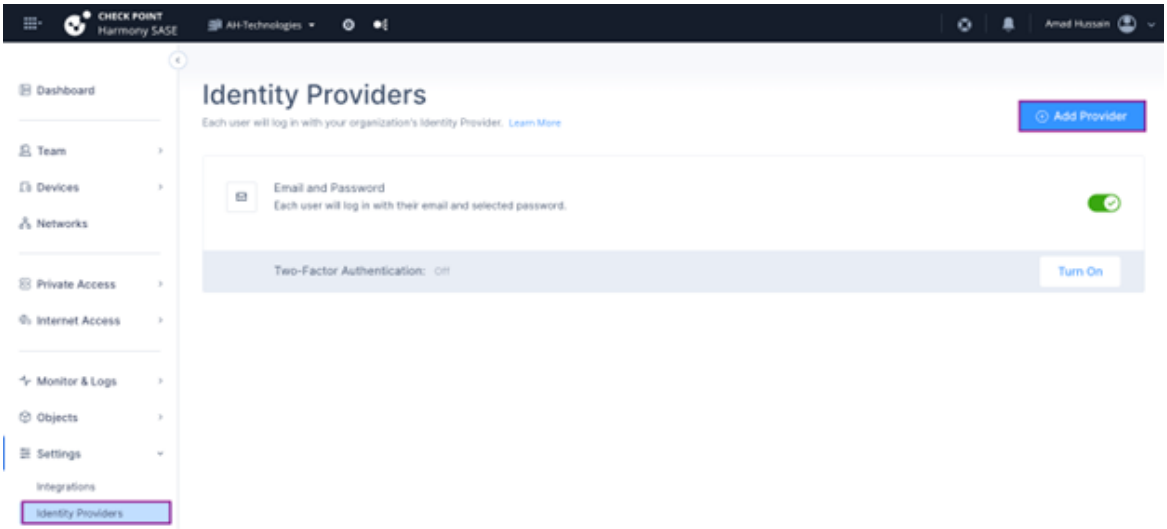
p. Click the **General** tab and click **SAML 2.0 Identity Provider Metadata** under Endpoints.

q. Copy the Sign-in URL and the X509 Signing Certificate.

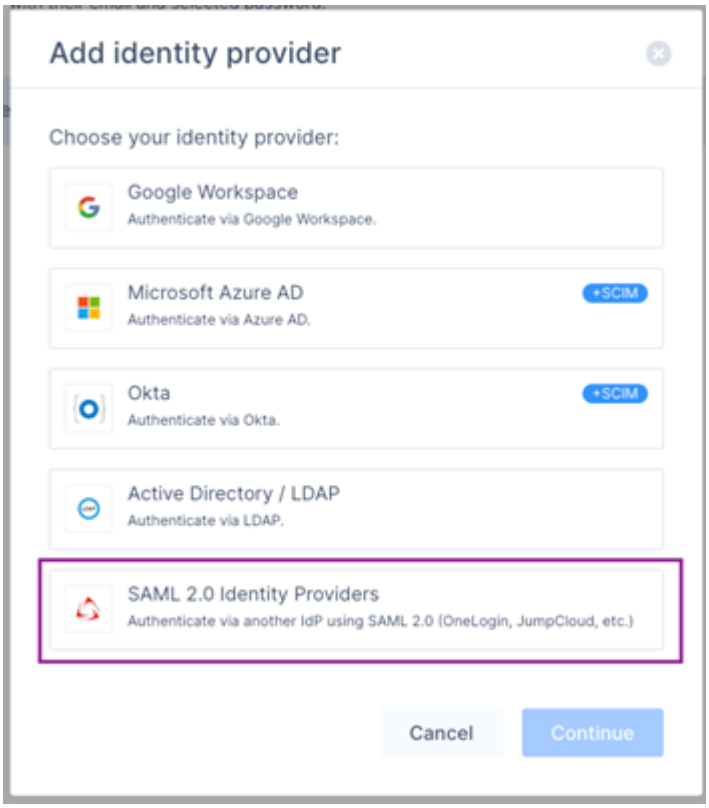
4. To configure Harmony SASE, log in to the Harmony SASE Administrator Portal:

   a. Go to **Settings** > **Identity Providers**.

   b. Click **Add Provider**.

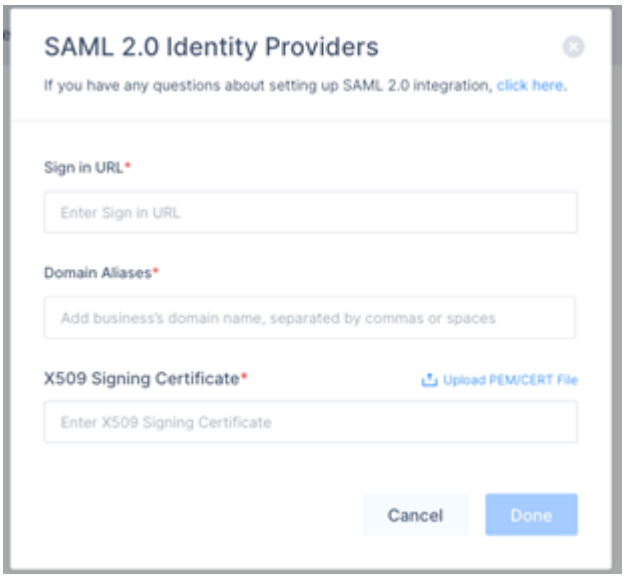


c. Select **SAML 2.0 Identity Providers**.



d. Click **Continue**.

The **SAML 2.0 Identity Providers** window appears.



e. In the **Sign in URL** field, enter the sign-in url copied in step **3.i.i**.

f. In the **Domain Aliases** field, enter your organization domain.

g. In the **X509 Signing Certificate** field, enter the certificate copied in step **3.i.i**.

h. Click **Done**.

OneLogin

Prerequisites

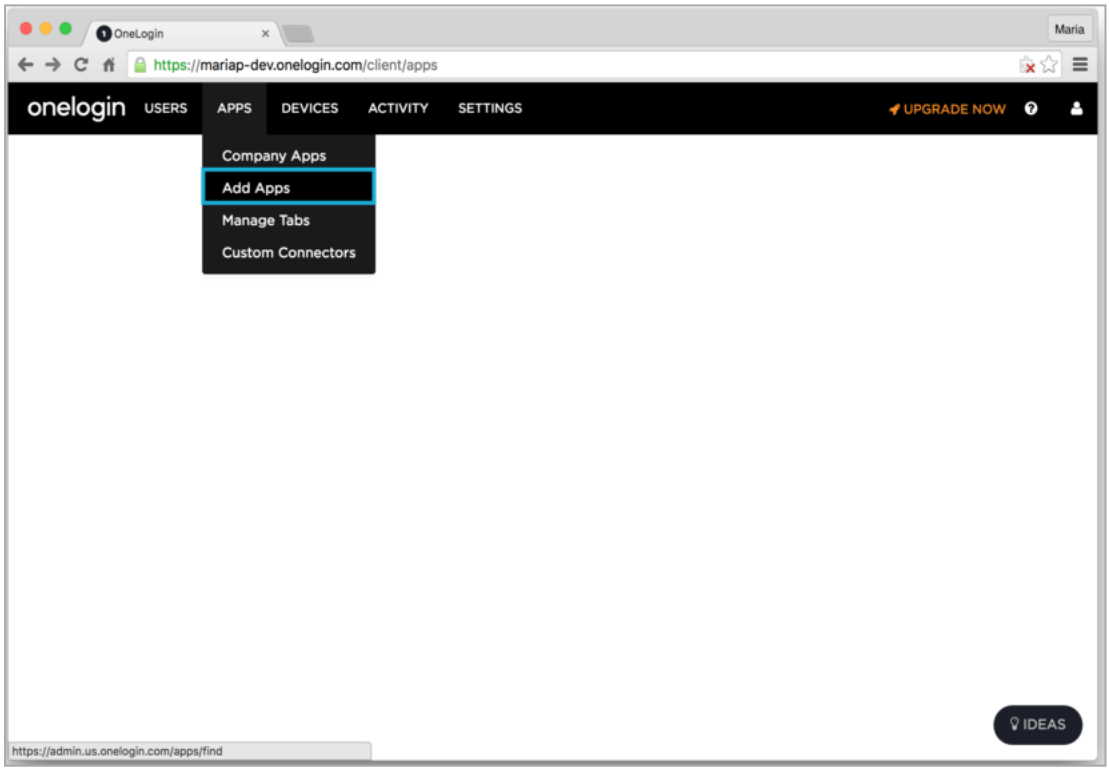
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Configure the OneLogin Management Portal" below*
- *"Step 2 - Configure the Harmony SASE Administrator Portal" on page 758*

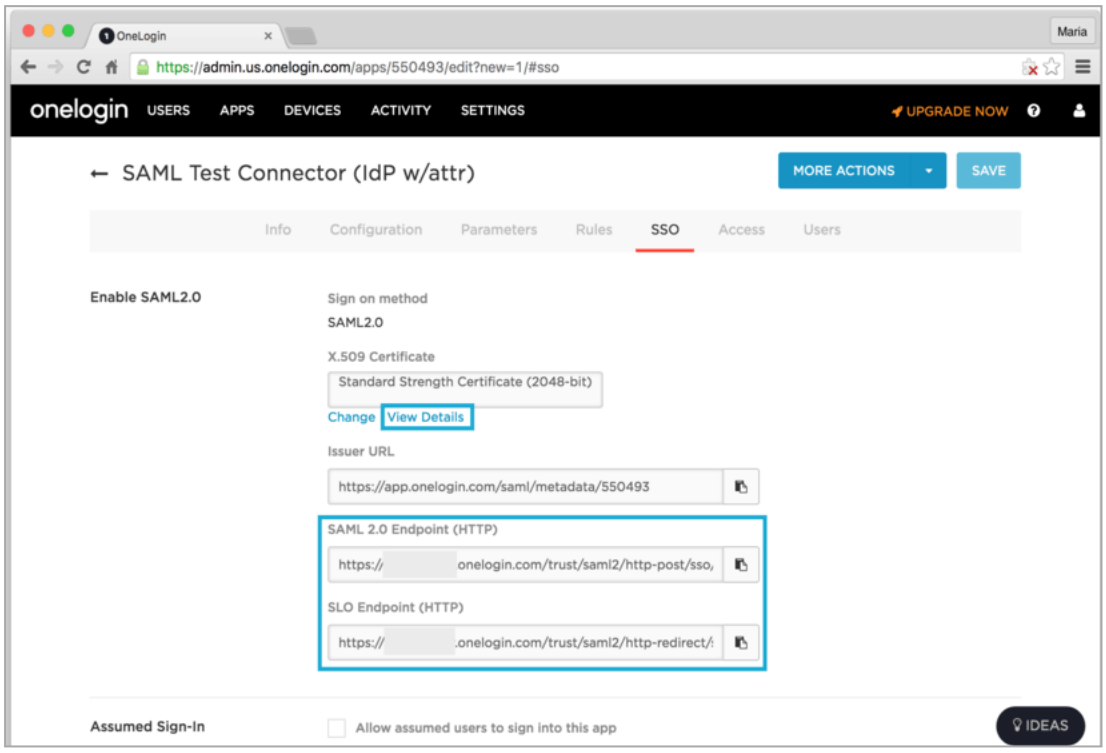
Step 1 - Configure the OneLogin Management Portal

1. Log in to OneLogin Management Portal.
2. Go to **Select Apps** > **Add Apps**.
3. From the **Applications**, click **SAML Test Connector (IdP w/attr)**.



4. Change the **Display Name** to Harmony SASE and click **Save**.
5. Go to the **SSO** tab, and copy these values:

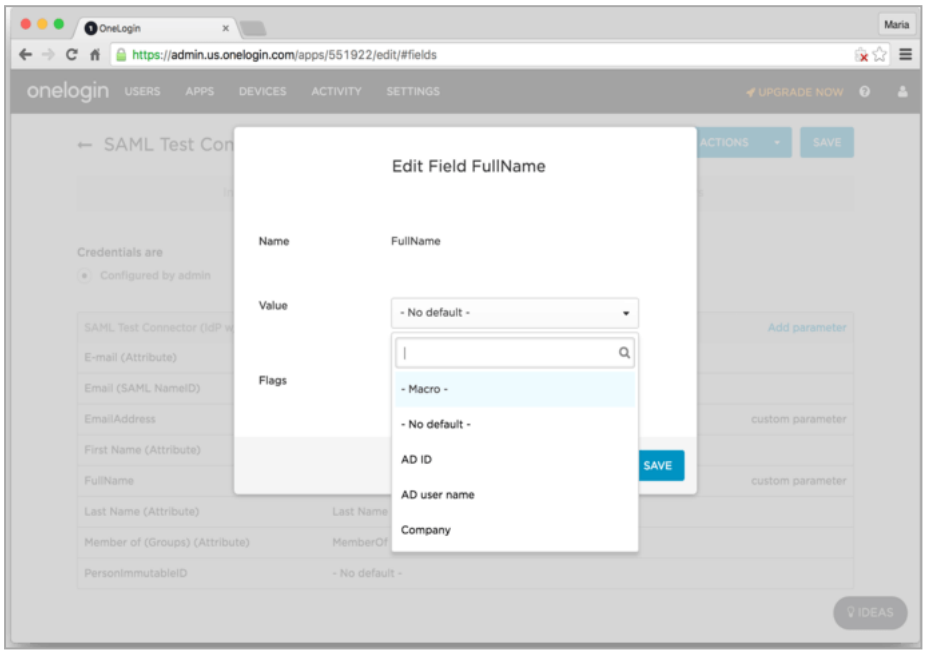
- SAML 2.0 Endpoint (HTTP) - You need to use this value in the **Sign In URL** field while configuring Harmony SASE Administrator Portal.
- SLO Endpoint (HTTP).



6. To download the X.509 certificate, click **View Details** and then click **Download**.
7. Go to the **Configuration** tab and enter these values:
   - **Audience**: `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **Recipient**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **ACS (Consumer) URL**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **ACS (Consumer) URL Validator**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
8. Go the **Parameters** tab and click **Add Parameter**.

9. In the pop-up that appears, using the **Field name** field, enter a name for the custom attribute.
10. Select the **Include in the SAML assertion** checkbox and click **Save**.

    The system shows the new attribute you created with the **Value**: **No default**.
11. Change the **No default** value to **Macro**.



12. Add these properties to the Macro:

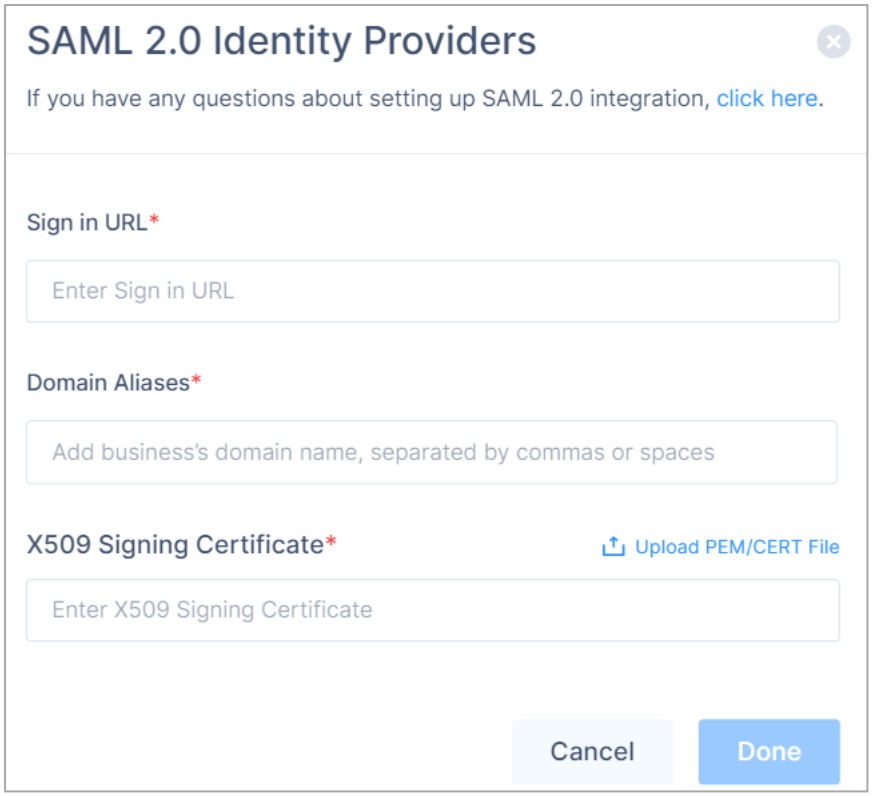
Field Name	Macro Text Box Value	SAML Assertion Flag
email	{email}	Checked
given_name	{firstname}	Checked
family_name	{lastname}	Checked

13. Click **Save**.

Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

PingOne for Enterprise

Prerequisites

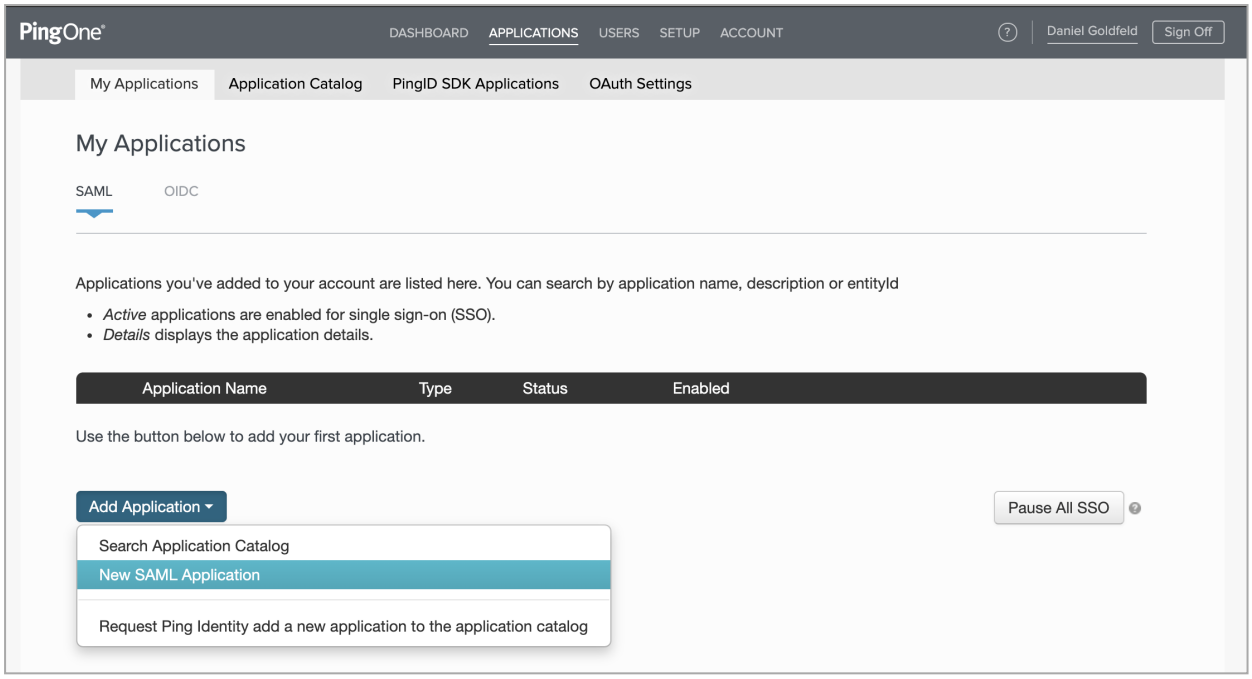
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Configure the PingOne Management Portal" below*
- *"Step 2 - Configure the Harmony SASE Administrator Portal" on page 764*

Step 1 - Configure the PingOne Management Portal

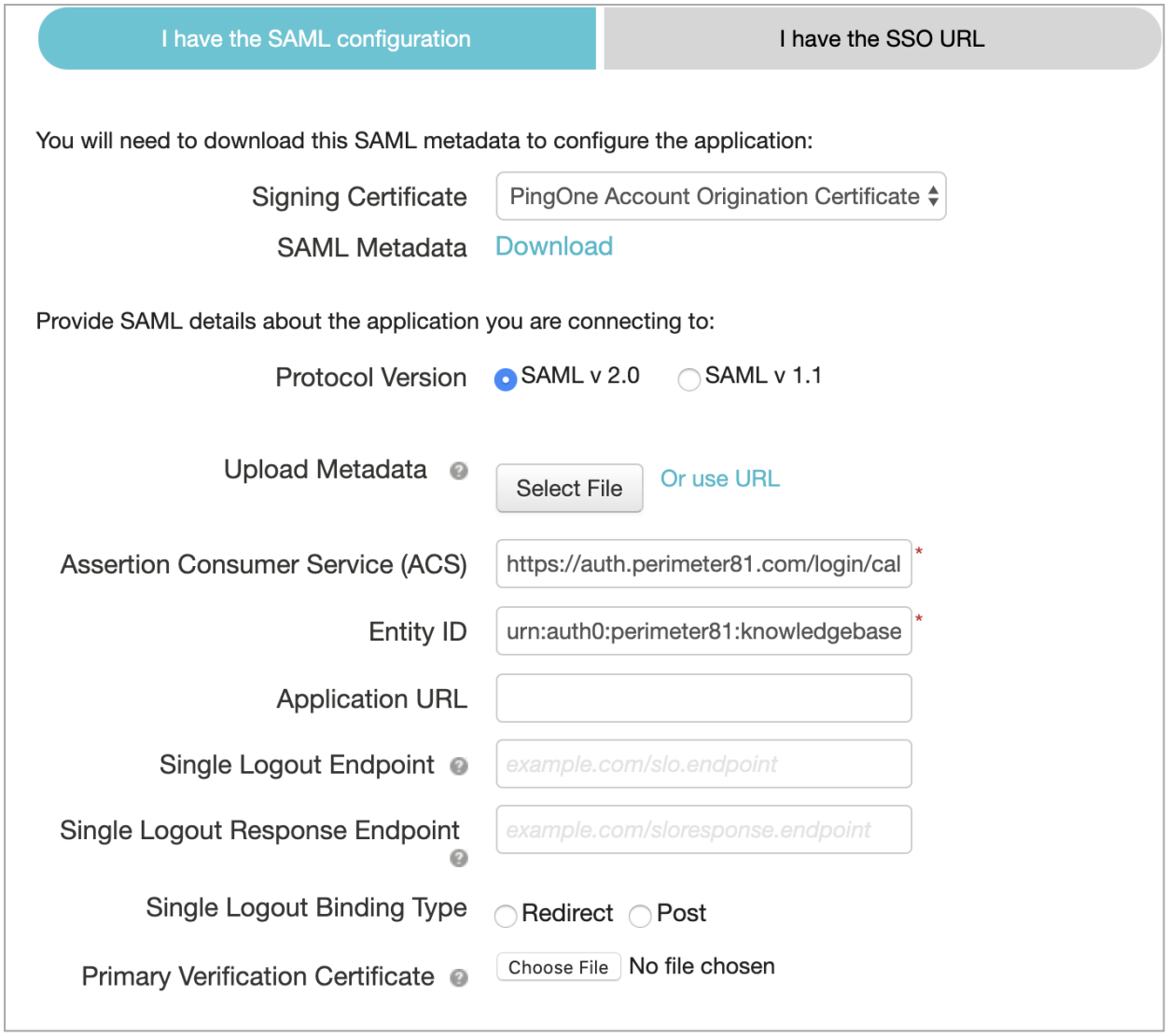
1. Log in to PingOne Management Portal.
2. From the top navigation bar, click **Applications**.
3. In the **SAML** tab, click **Add Application** and then select **New SAML Application**.



The **New Application** window appears.

4. Enter these details:
   - **Application Name**: Harmony SASE
   - **Application Description**: Harmony SASE SAML Connection
   - **Category**: Information Technology
   - **Graphics**: (Optional) Add the Harmony SASE logo
5. Click **Continue to Next Step**.

   The **Application Configuration** window appears.
6. Click **I have the SAML configuration** and then enter these details:
   - **Signing Certificate**: PingOne Account Origination Certificate
   - **Protocol Version**: SAML v 2.0
   - **Assertion Consumer Service (ACS)**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **Entity ID**: `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.

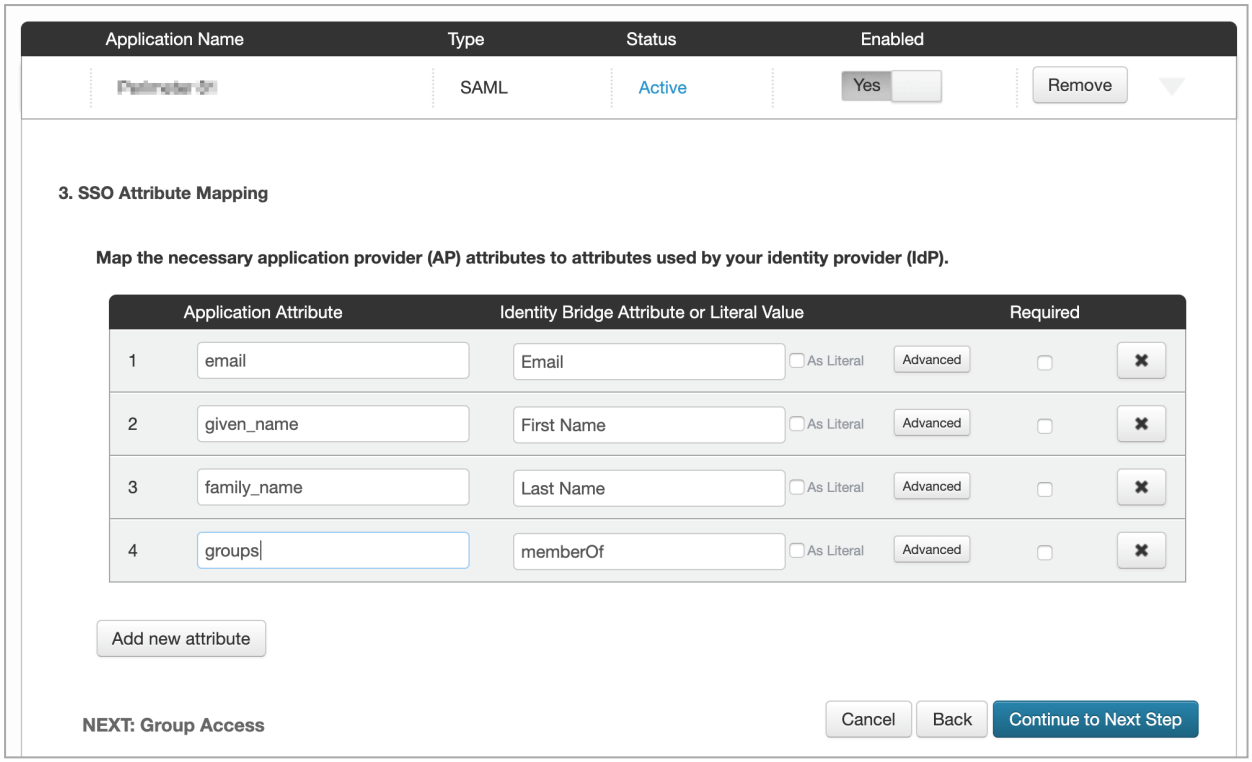


7. Click **Continue to Next Step**.

   The **SSO Attribute Mapping** window appears.

8. Map these attributes:

Application Attribute	Identity Bridge Attribute or Literal Value
email	Email
given_name	First Name
family_name	Last Name
groups	memberOf



9. Click **Continue to Next Step**.

   The **Group Access** window appears.

10. Select the user groups that need access to the PingOne for Enterprise login page.

    Note - To allow access to all users, add **Users@Directory**.

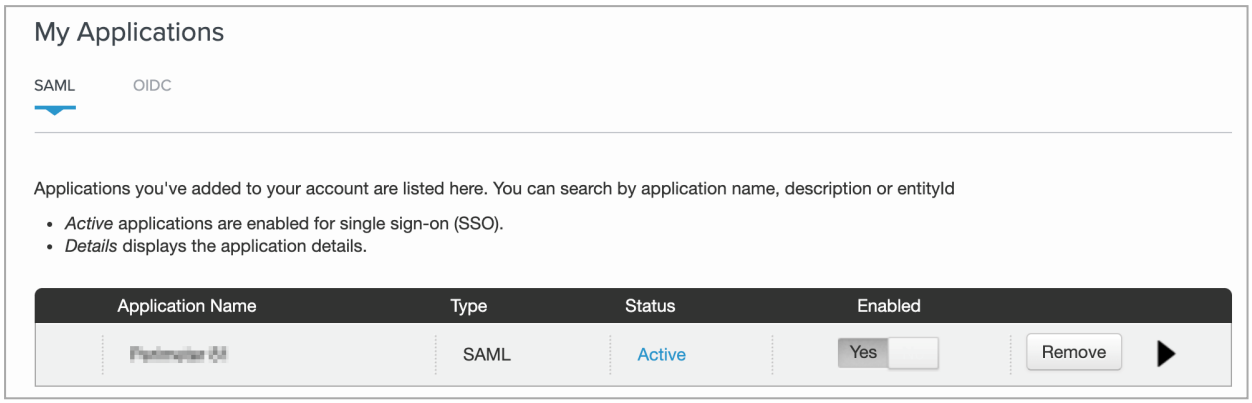
11. Click **Continue to Next Step**.

    The **Review Setup** window appears.

12. Copy the **idpid**.

13. Click **Download** to download the **Signing Certificate**.

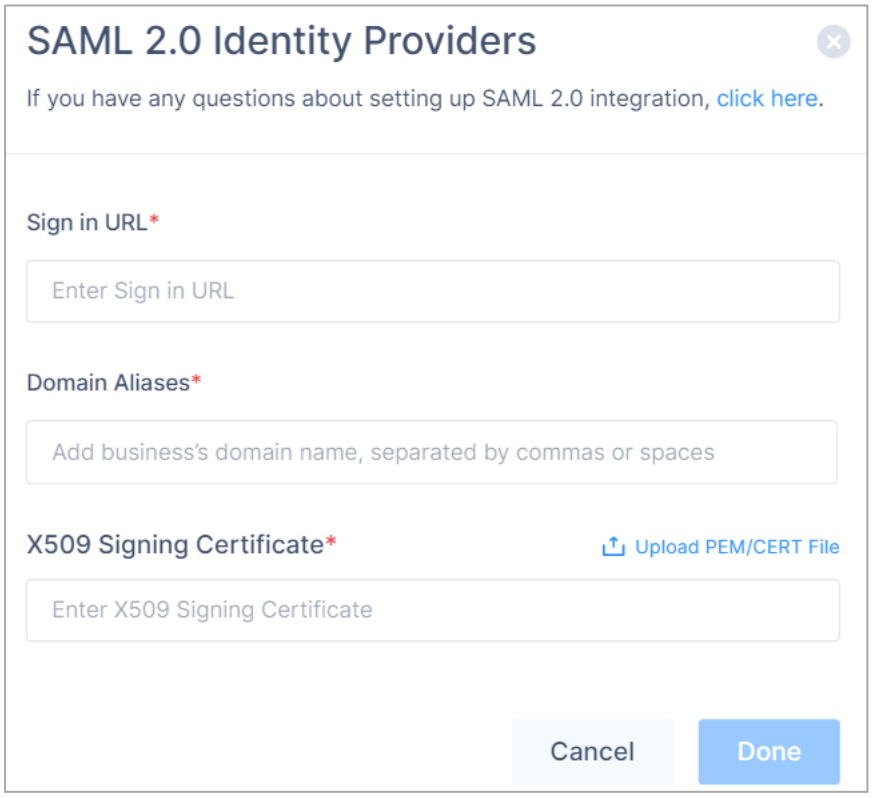
14. Click **Save and Close**.
15. Go to **My Applications** and ensure that the Harmony SASE application is set to **Enabled - Yes**.



Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

PingFederate

Prerequisites

- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Configure the PingFederate Management Portal" below*
- *"Step 2 - Configure the Harmony SASE Administrator Portal" on the next page*

Step 1 - Configure the PingFederate Management Portal

1. Log in to PingFederate Management Portal.
2. Go to **SP Connections** and click **Create New**.
3. Select **Browser SSO Profiles** as **Connection Type**.
4. Select **Browser SSO** as **Connection Options**.
5. Configure the parameters and map the attributes.
   - **Entity ID**: `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **Assertion Consumer Service URL**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **SAML Request**: HTTP-Redirect Binding

- **SAML Response**: HTTP-POST Binding
- Attributes:

Harmony SASE Attribute	PingFederate Attribute
email	Mail
given_name	Given Name
family_name	Surname

6. Configure **Browser SSO**.
   a. In the SAML Profiles, select **SP-Initiated SSO** and **SP-Initiated SLO**.
   b. Go to **Assertion Creation** section and select **Configure Assertion**.
   c. Accept all defaults for the next two screens.
7. Go to **IdP Adapter Mapping** section and select the existing authentication or add a new one.

   Note - Auth0 only requires the NameIdentifier claim. All other attributes will be passed further to the end application.
8. Configure **Protocol Settings**.

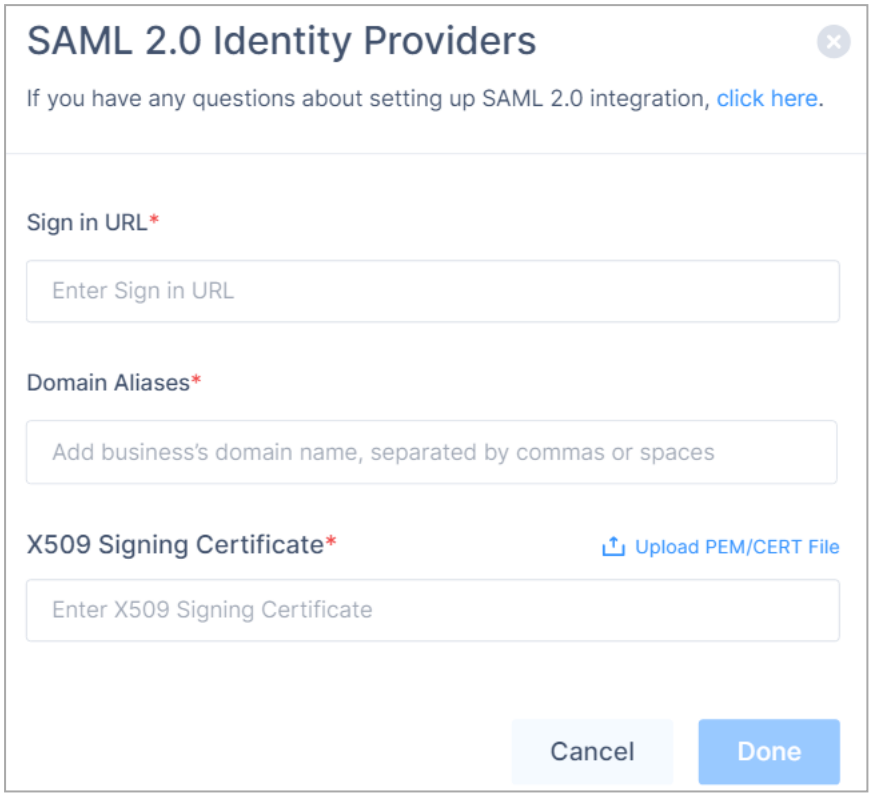
   Values for **Protocol Settings** are imported from the metadata file. Next, you will see the Assertion Consumer Service URL and the Sign-Out URLs. Click Next to the Allowable SAML Bindings section.
9. Leave POST and Redirect enabled. Make sure SAML Assertion is always signed.
10. Configure Credentials. On Digital Signature Settings, select your signing certificate and make sure you check the option to include it in the element.
11. Configure the certificate used to sign incoming requests.
12. Review your settings and set as Active or Inactive.
13. Click Save at the bottom of the screen. You should see the new SP Connection on the Main screen.

Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

The **Add identity provider** pop-up appears.

4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`

Identity Provider	Sign in URL
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Rippling

Prerequisites

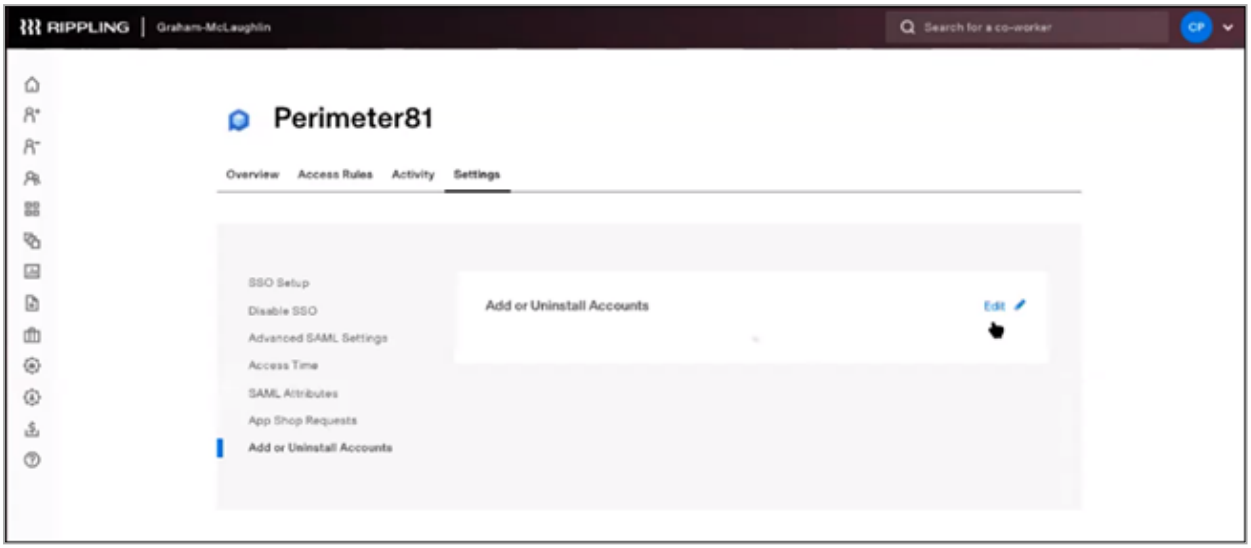
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

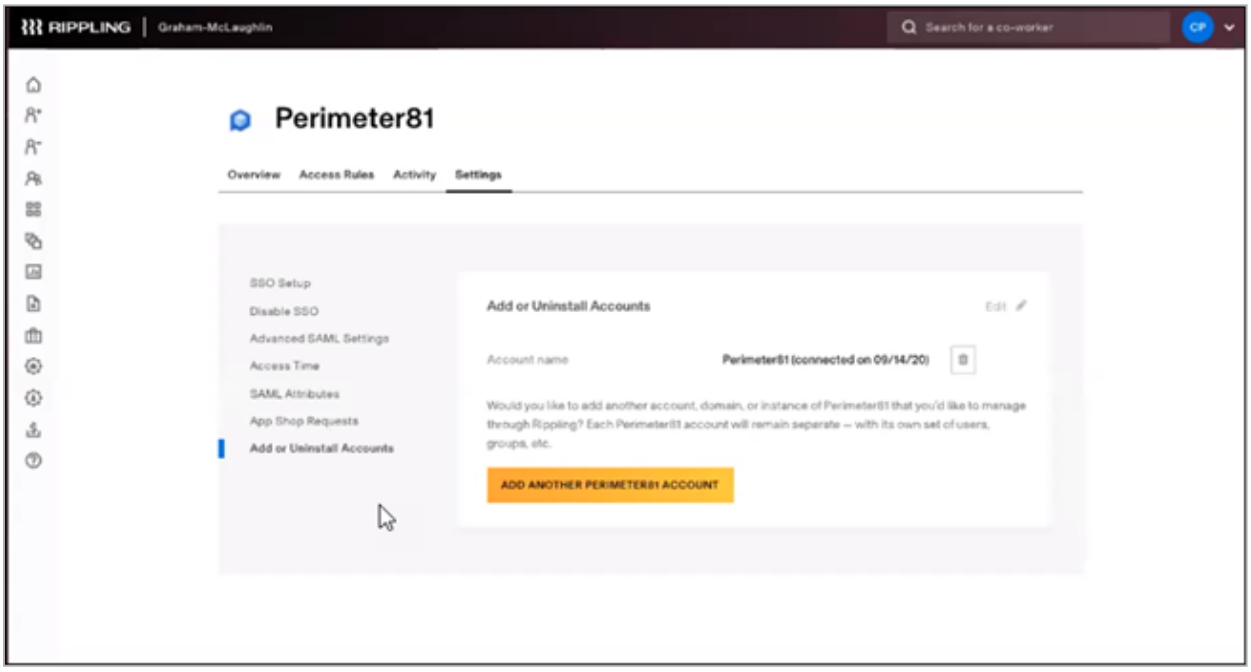
- *"Step 1 - Configure the Rippling Management Portal" on the next page*
- *"Step 2 - Configure the Harmony SASE Administrator Portal" on page 776*

Step 1 - Configure the Rippling Management Portal

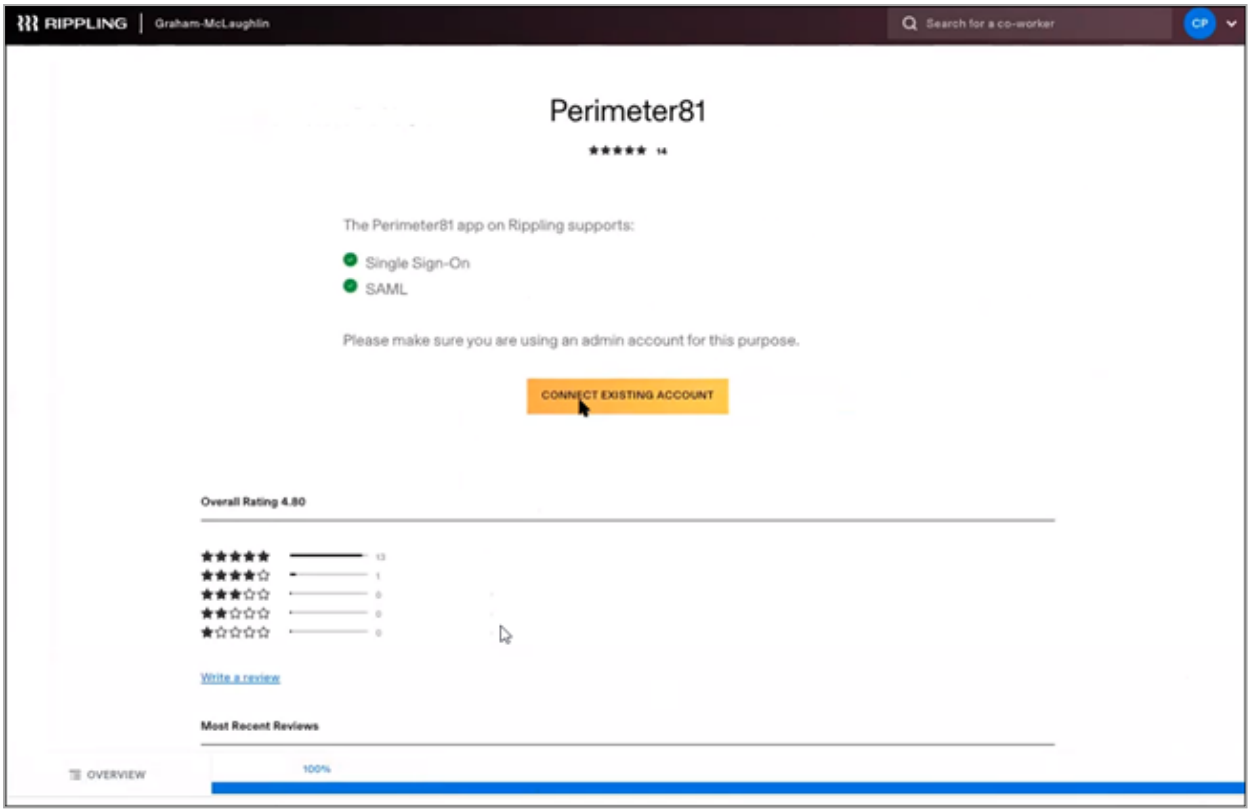
1. Log in to Rippling Management Portal.
2. Go to **Settings** tab and click **Add or Uninstall Accounts**.



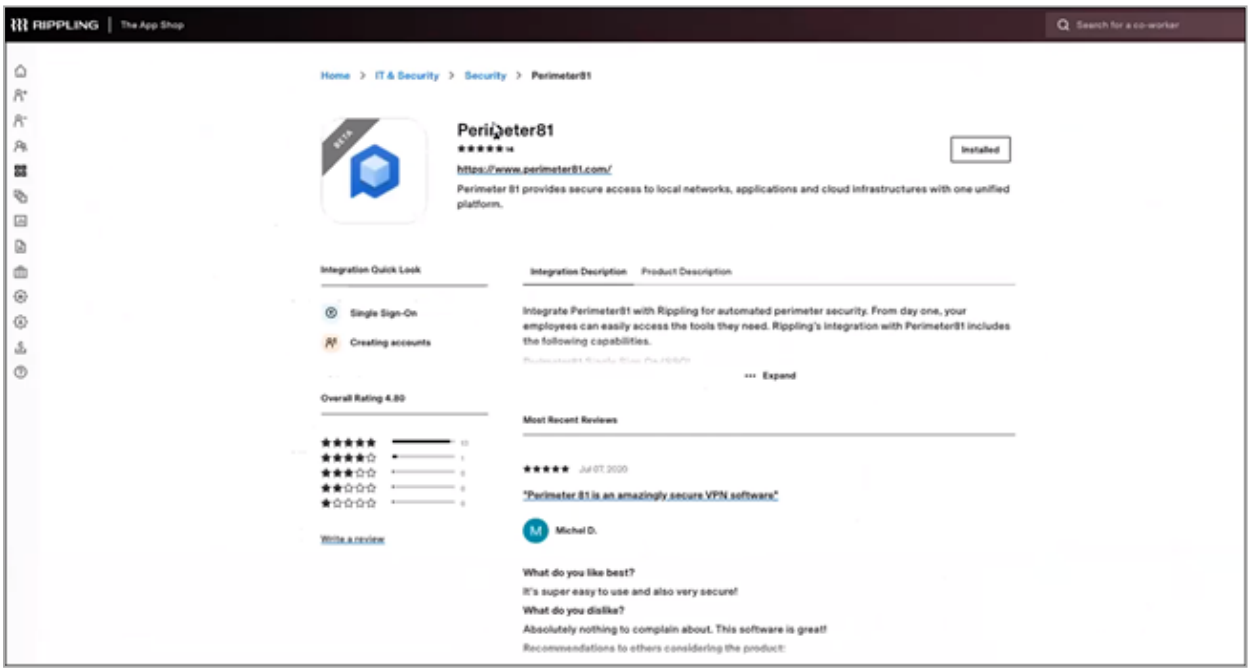
3. Click **Add Another Harmony SASE Account**.



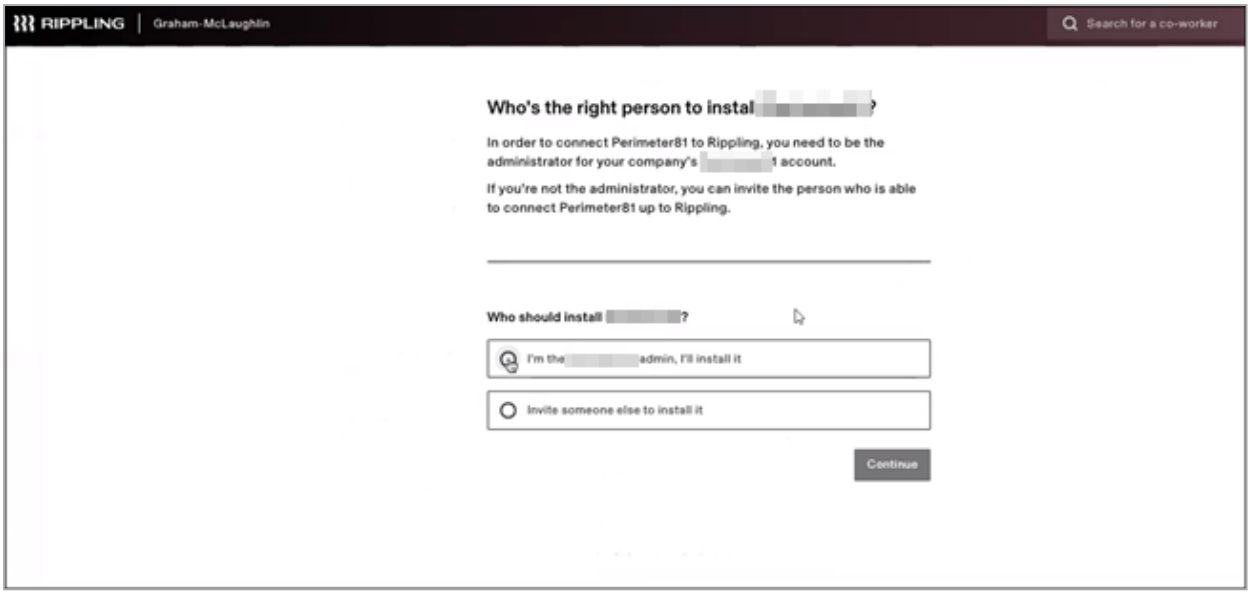
4. Click **Connect Existing Account**.



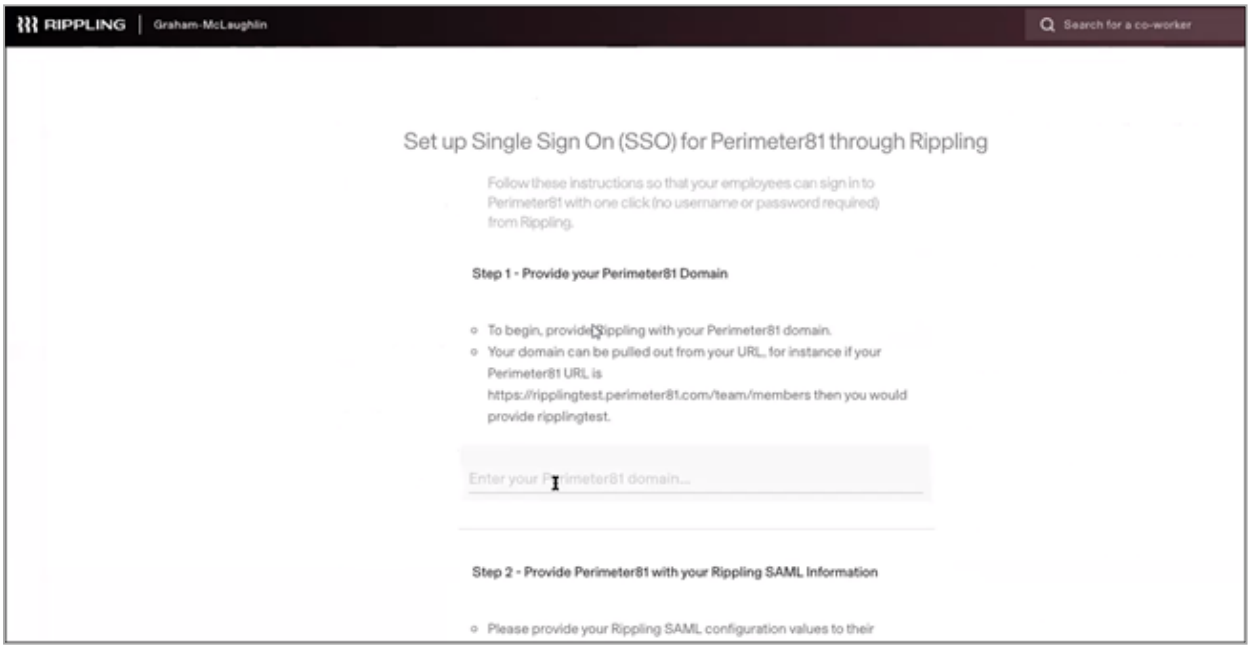
5. Click **Install**.



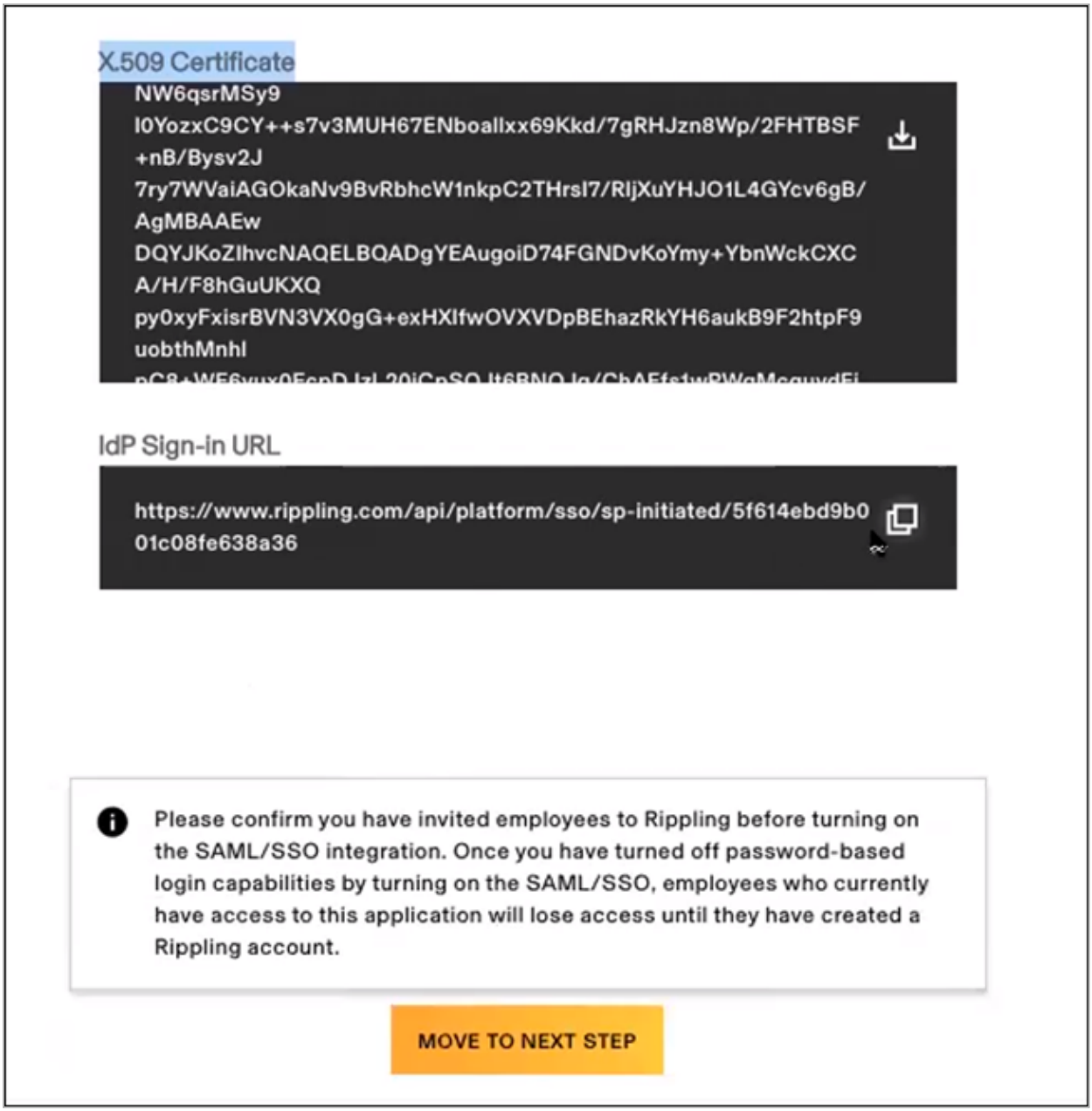
6. Select who should install Harmony SASE and click **Continue**.



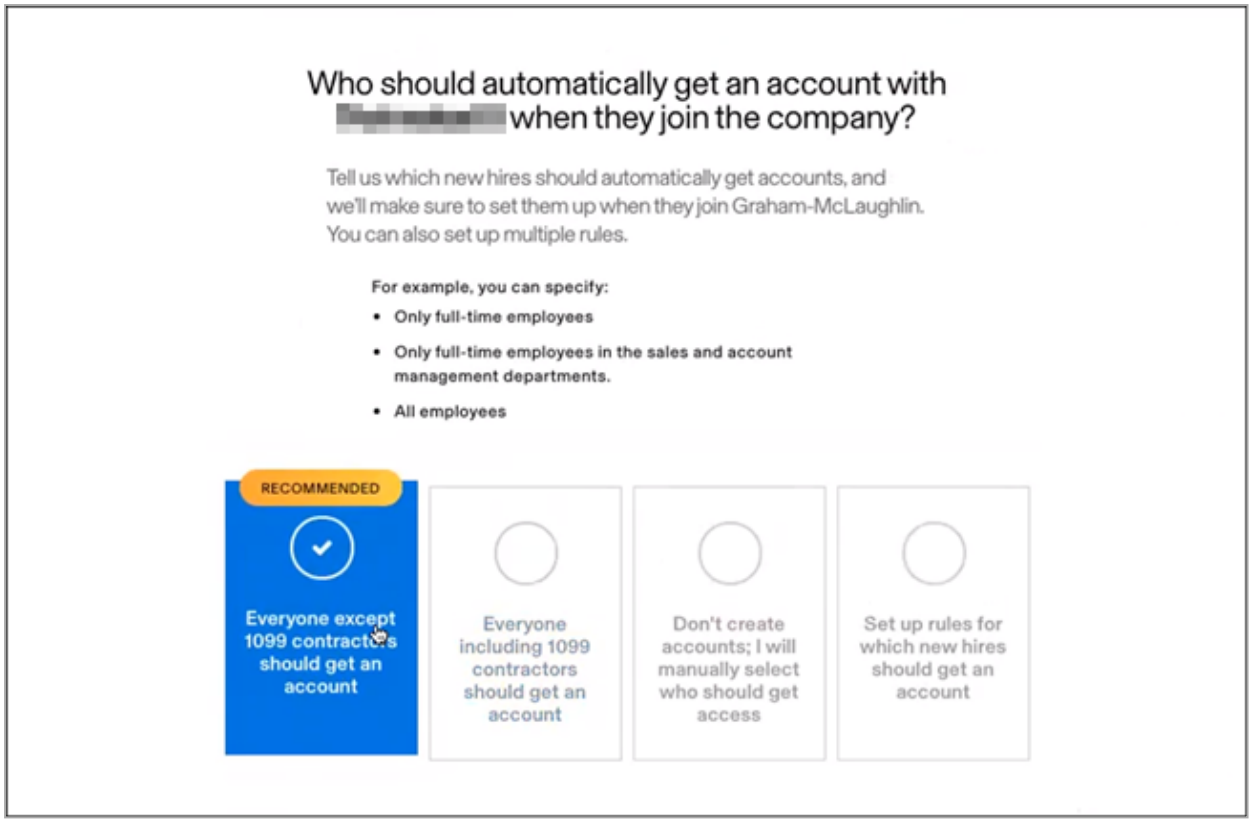
7. In **Step 1 - Provide your Harmony SASE Domain**, enter your Harmony SASE domain name.



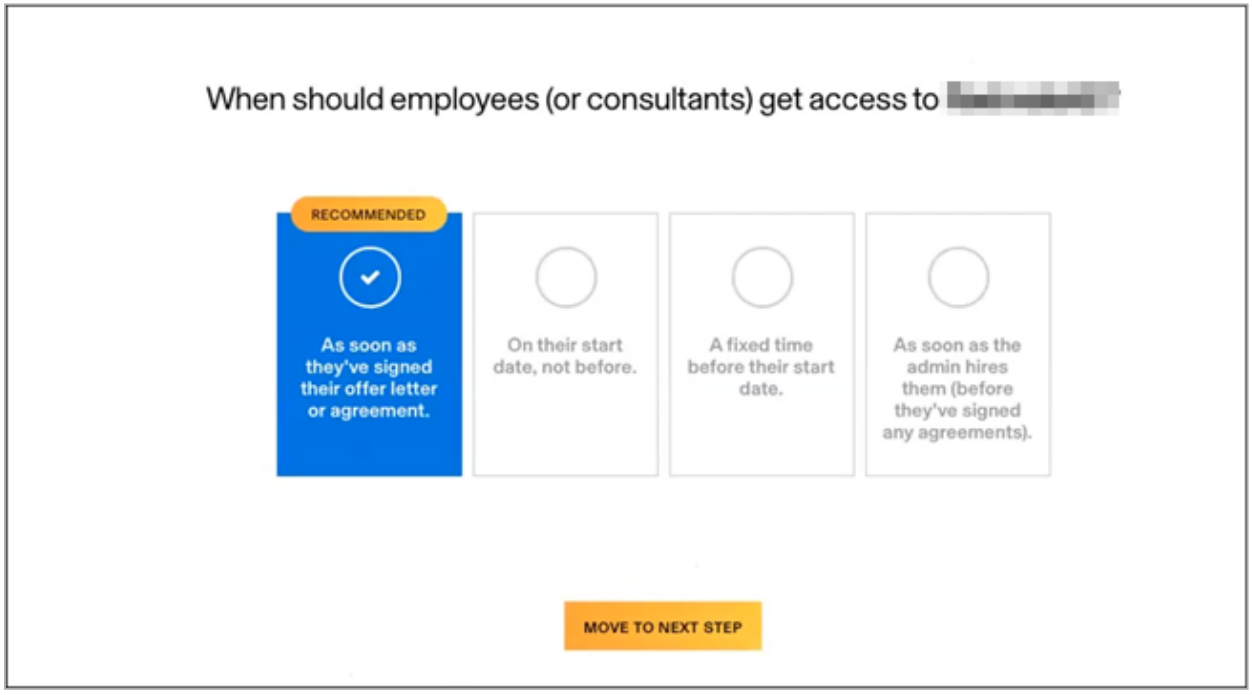
8. Copy or download the **X.509 Certificate**.



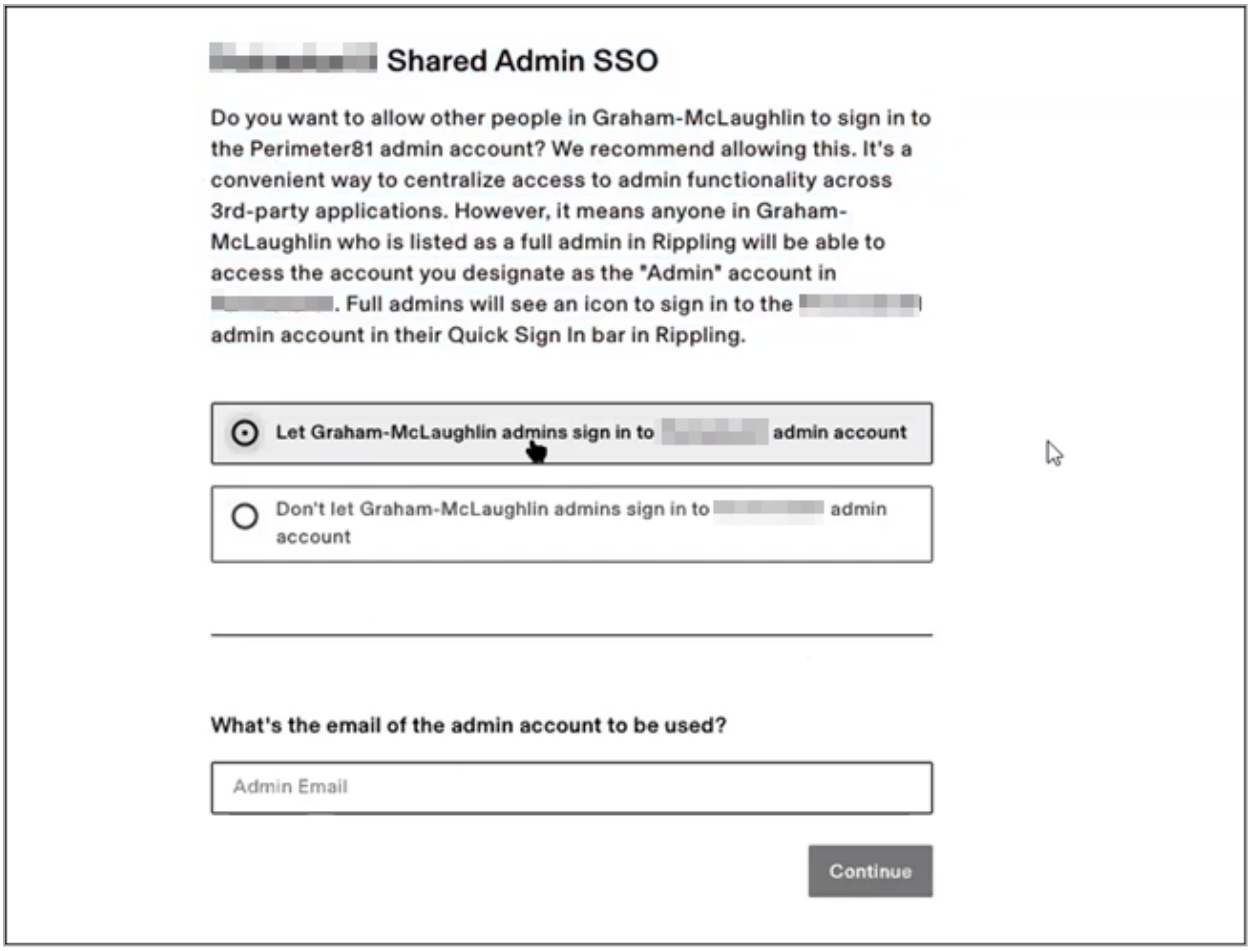
9. Copy the **IdP Sign-in URL** and click **Move to Next Step**.
10. Select who will get a Harmony SASE account when they join the company and click **Move to Next Step**.



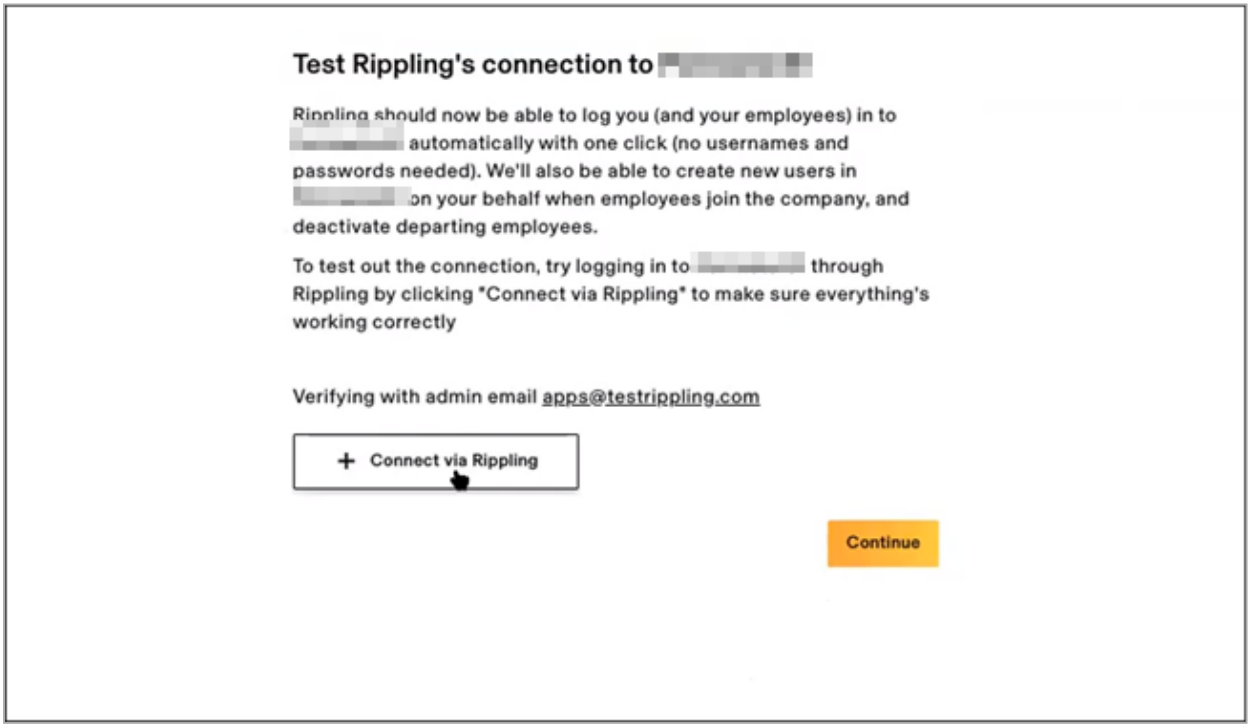
11. Select when employees or consultants should get access to Harmony SASE and click **Move to Next Step**.



12. Select if you want to allow other individuals to sign into the account and then click **Continue**.

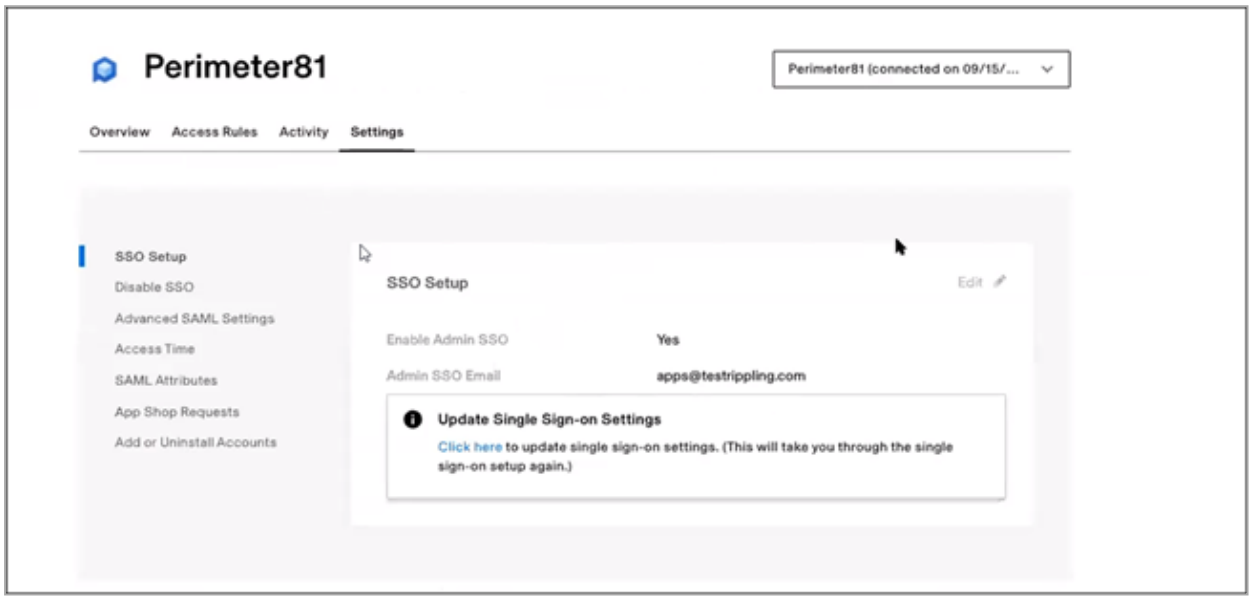


13. Click **Connect via Rippling** to test the connection and then click **Continue**.



14. Wait for the application to complete installation and then open the application.

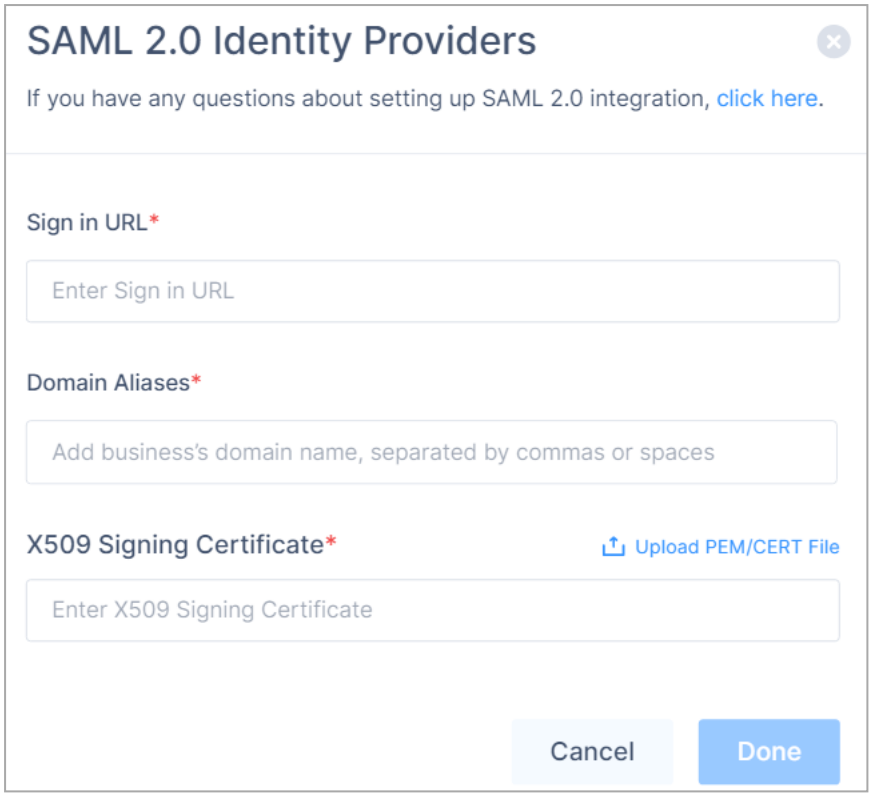
15. Go to the **Settings** tab and then enter the Harmony SASE information.



Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

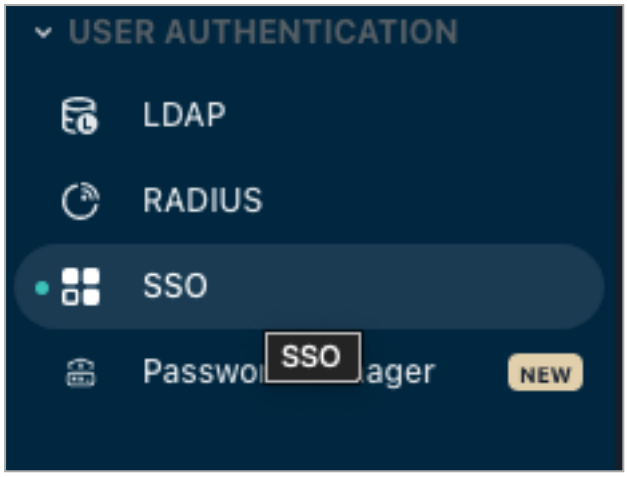
Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

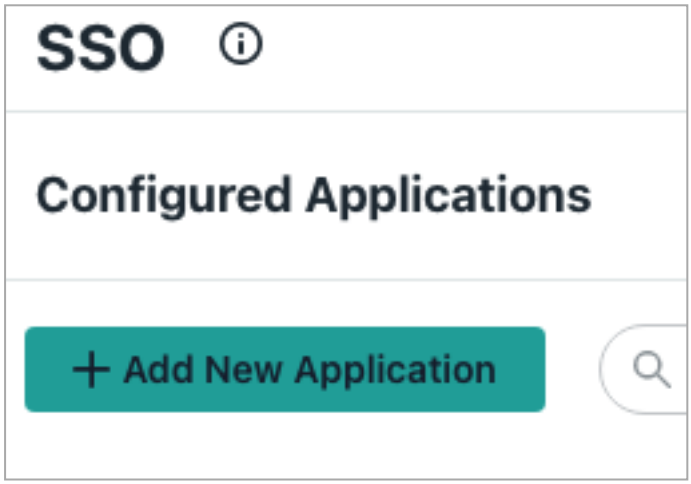
JumpCloud

Step 1 - Configure your JumpCloud Management Portal

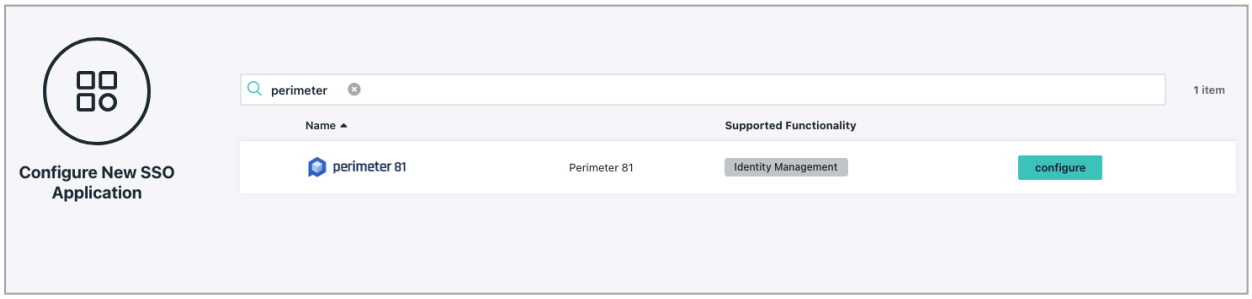
1. Log in to JumpCloud Management Portal.
2. From the main navigation panel, click **User Authentication** and select **SSO**.



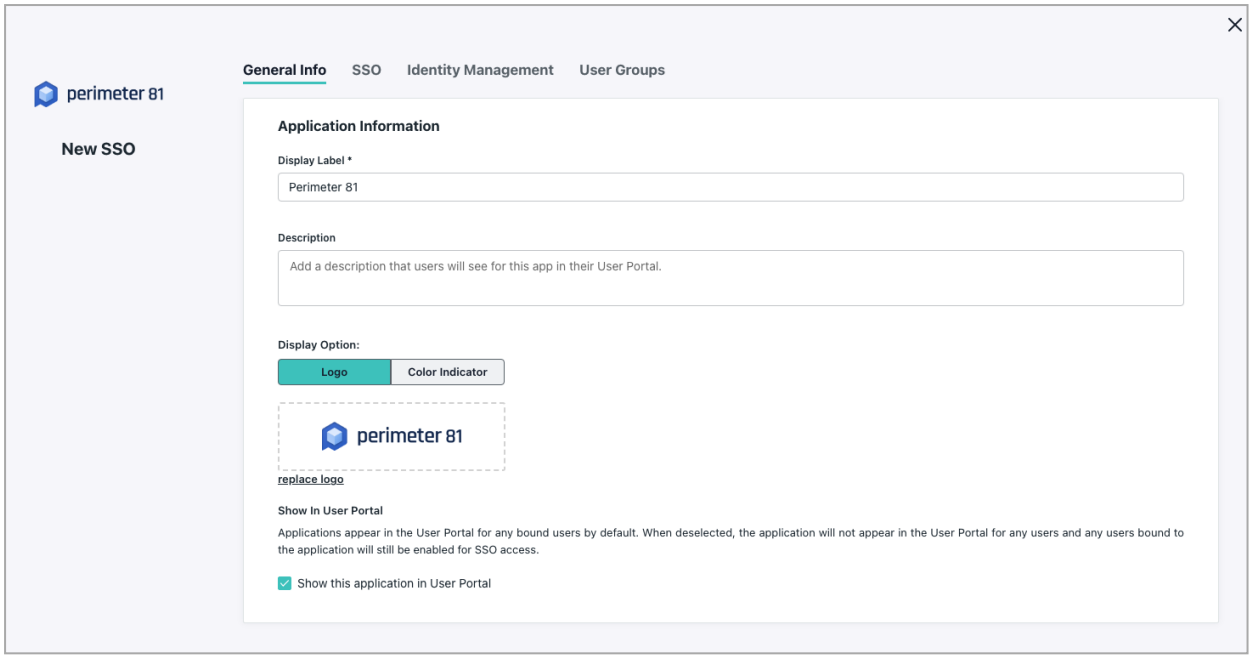
3. Click **Add New Application**.



4. Search for Harmony SASE application and click **Configure**.

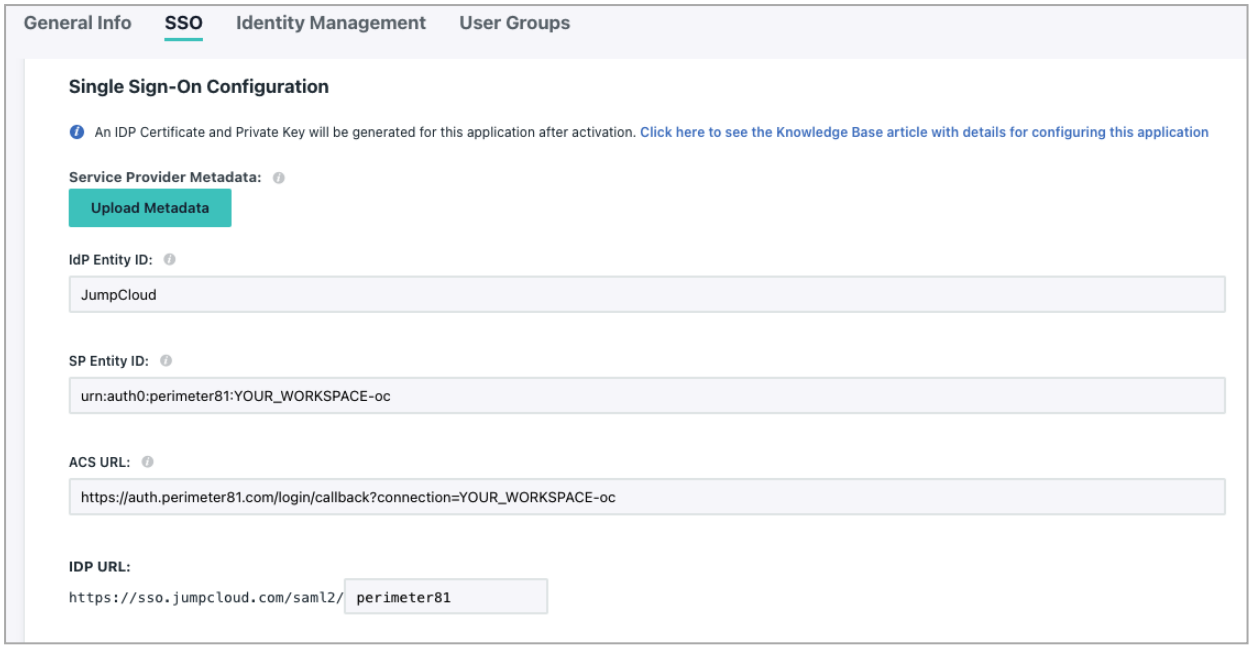


5. In the **General Info** tab, enter a name for the application in the **Display Label** field.

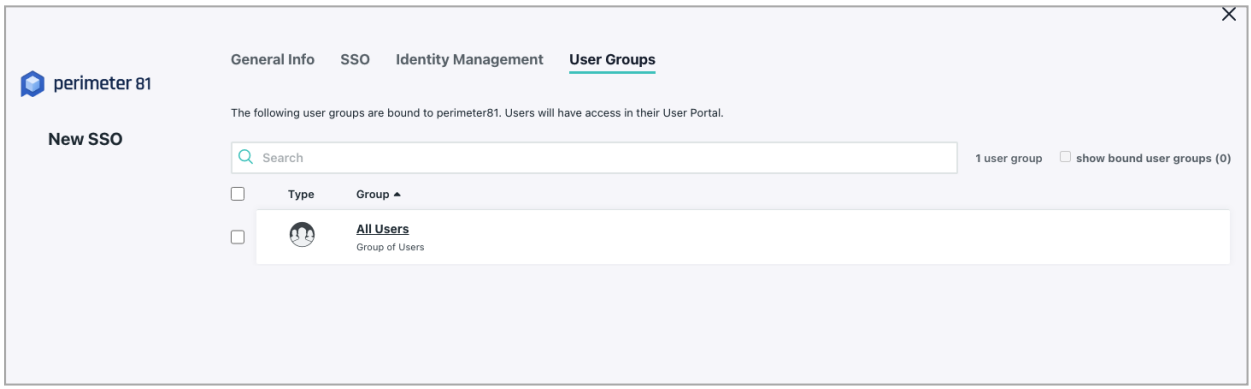


6. Go to the **SSO** tab and enter these values in the **Single Sign-On configuration** section:
   - **IDP Entity ID**: `https://{{WORKSPACE}}.perimeter81.com/`
   - **SP Entity ID**: `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **ACS URL**: `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
   - **IDP URL**: `https://sso.jumpcloud.com/saml2/{{required text}}`

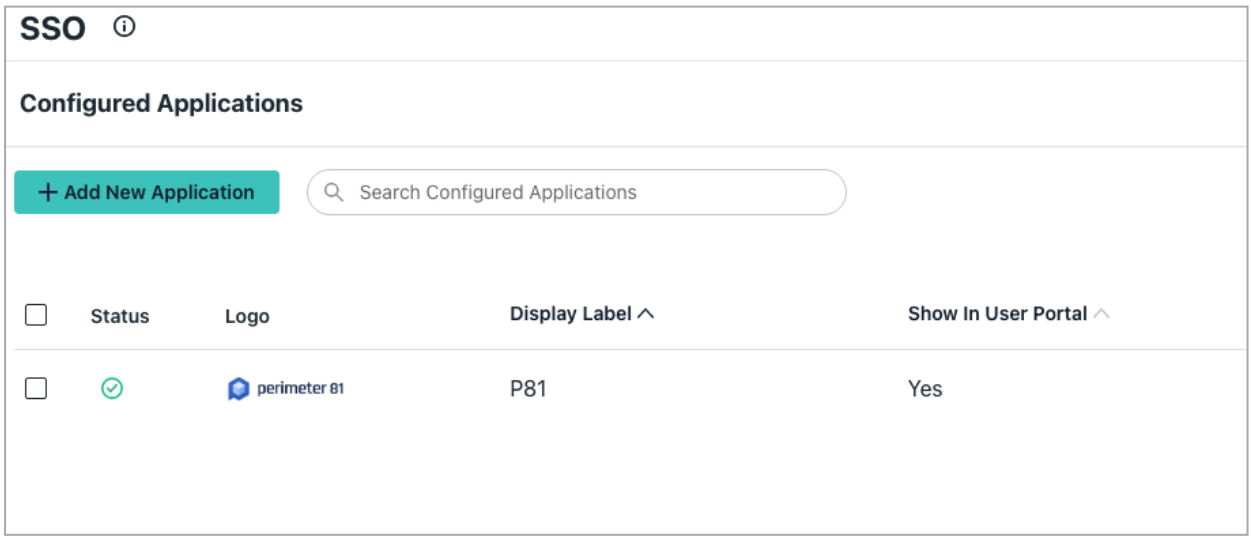
     For example, `https://sso.jumpcloud.com/saml2/perimeter81`.
   - Do not change the default values in the other fields.



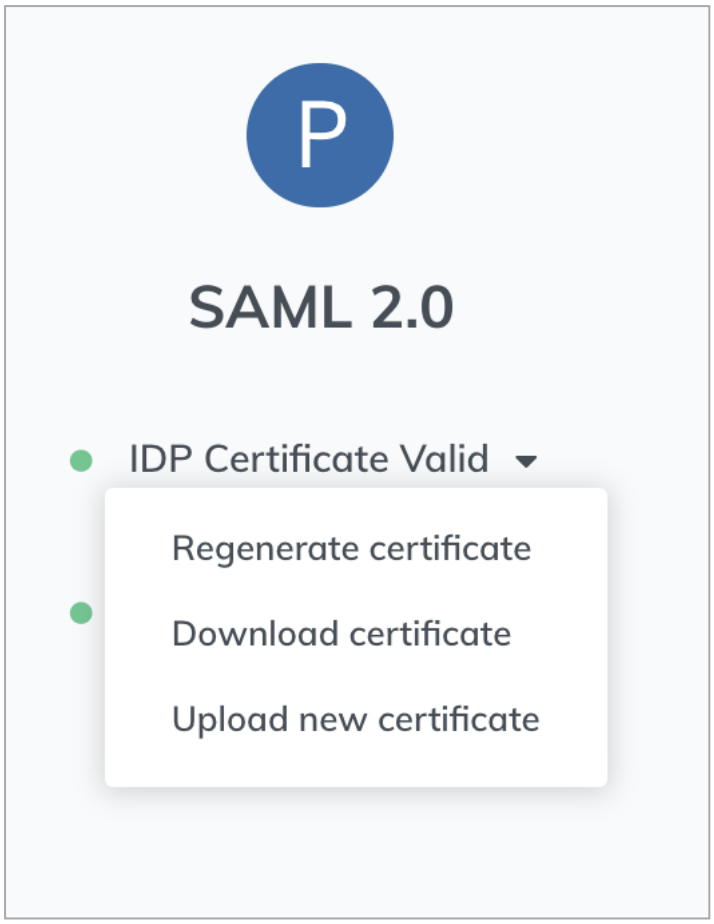
7. Go to the **User Groups** tab and verify that the required groups have the permissions.



8. Click **Activate**.
9. Click the newly created application.



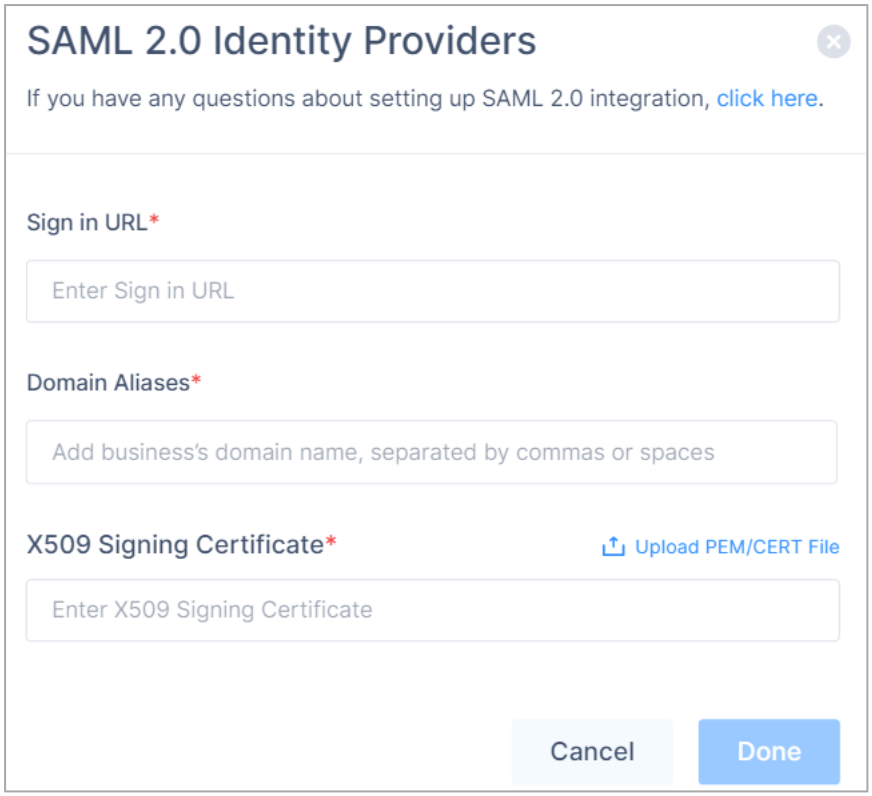
10. Click the **IDP Certificate Valid** drop-down and select **Download certificate**.



Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Okta with SAML

Supported Features

Integrating Okta with Harmony SASE using SAML protocol supports these features:

- SP-initiated SSO (only supported for the Web Client login)
- IdP-initiated SSO (only supported for the Web Client and Agent login)
- JIT (Just In Time) Provisioning

Prerequisites

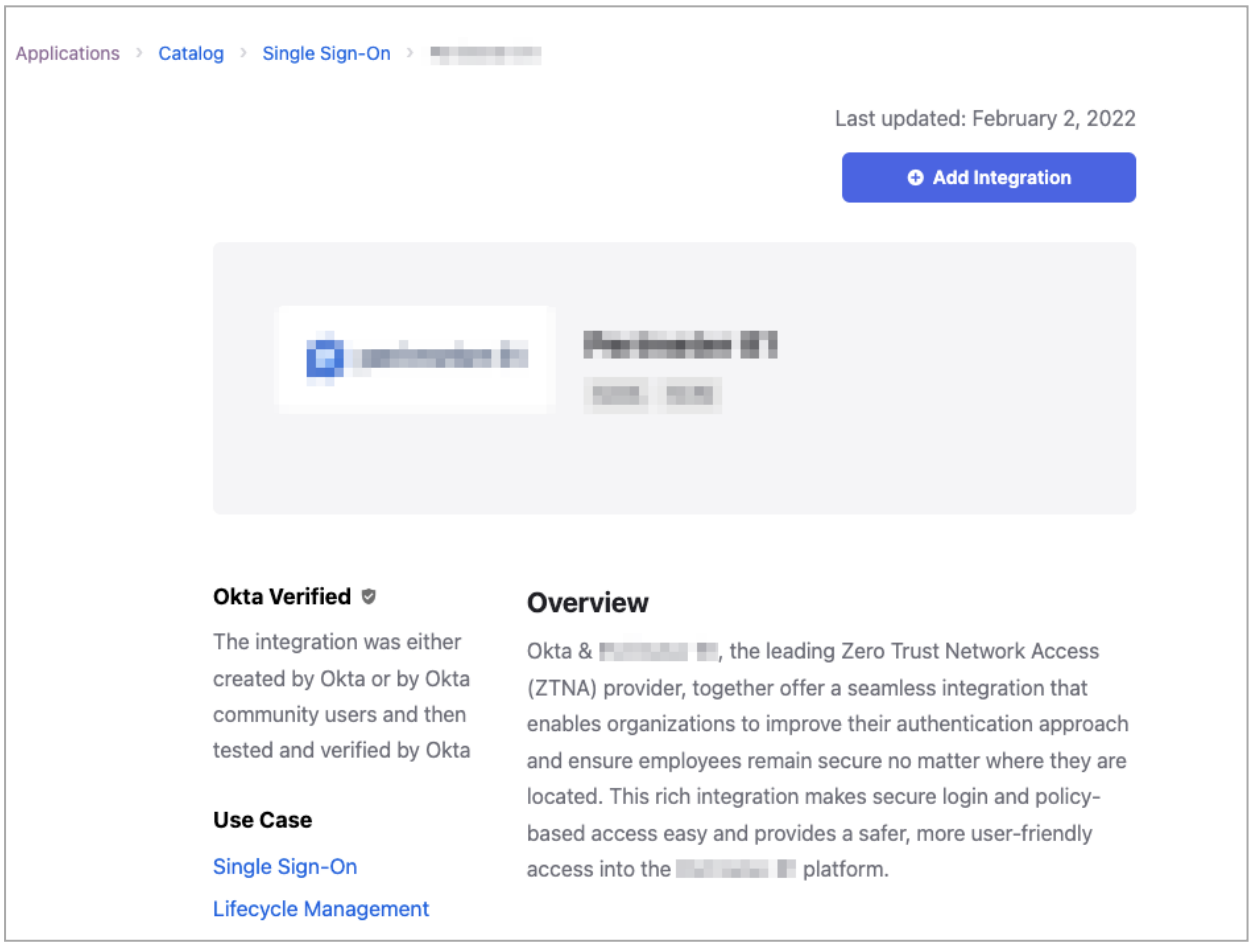
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

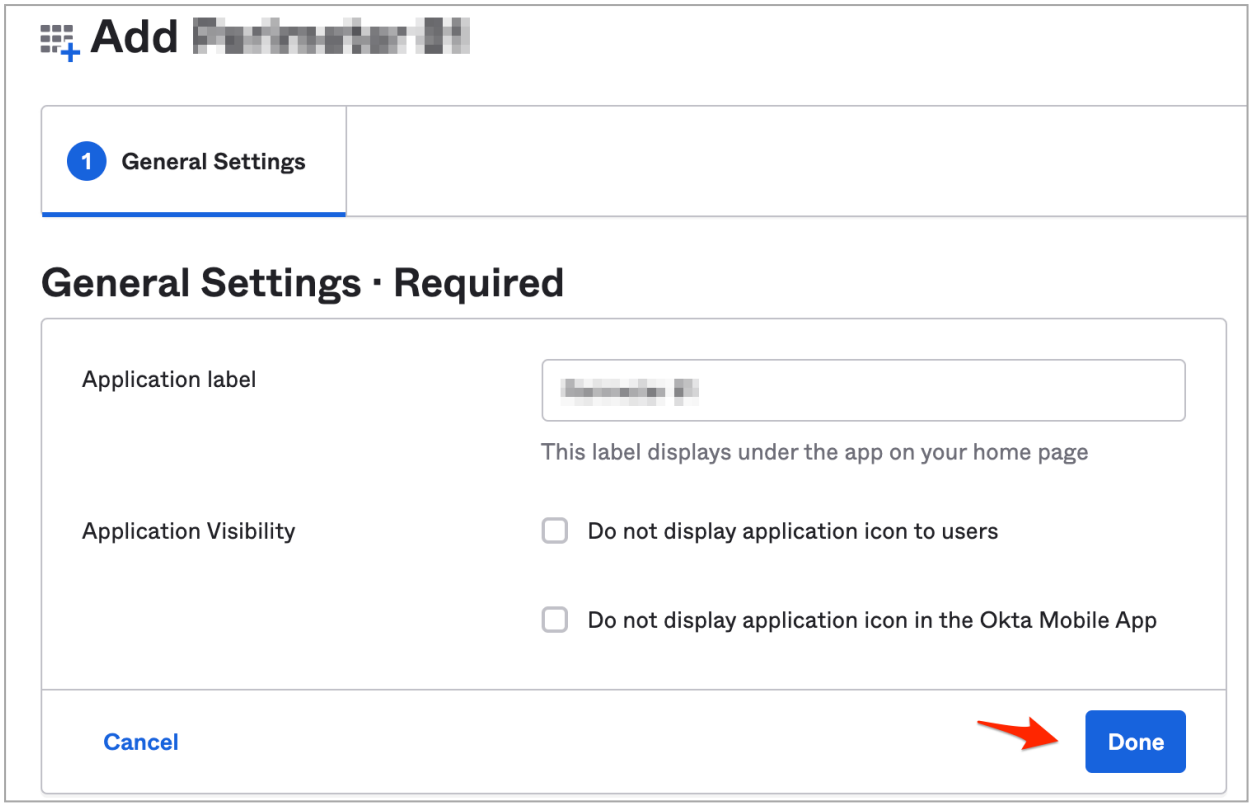
- Step 1 - Configure the Okta Management Portal
- Step 2 - Configure the Harmony SASE Administrator Portal
- Step 3 - Assign the App
- Step 4 - Verify SP-initiated SSO

Step 1 - Configure the Okta Management Portal

1. Log in to Okta Management Portal.
2. Go to **Applications**.
3. Click **Browse App Catalog** and search for Perimeter 81.
4. Click **Add Integration**.

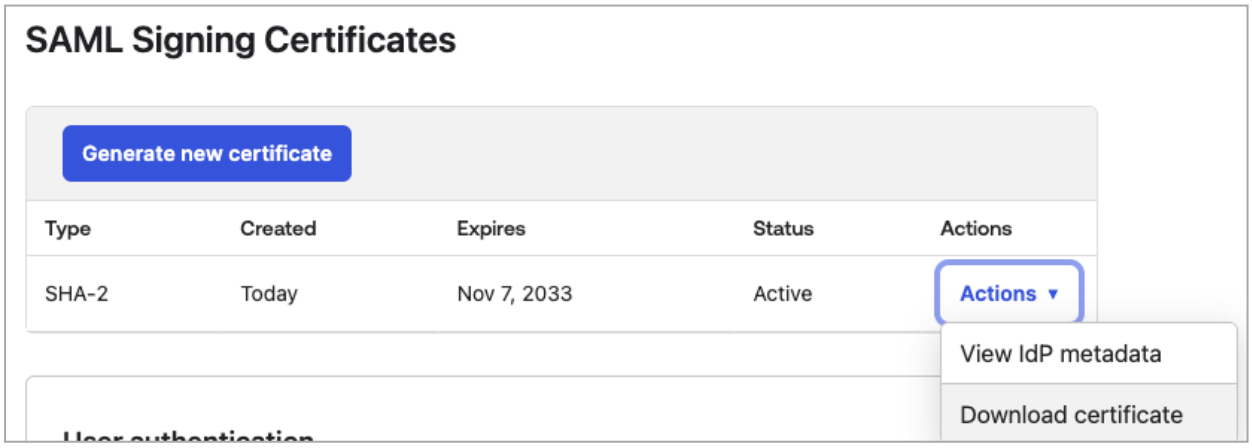


5. Click **Done**.

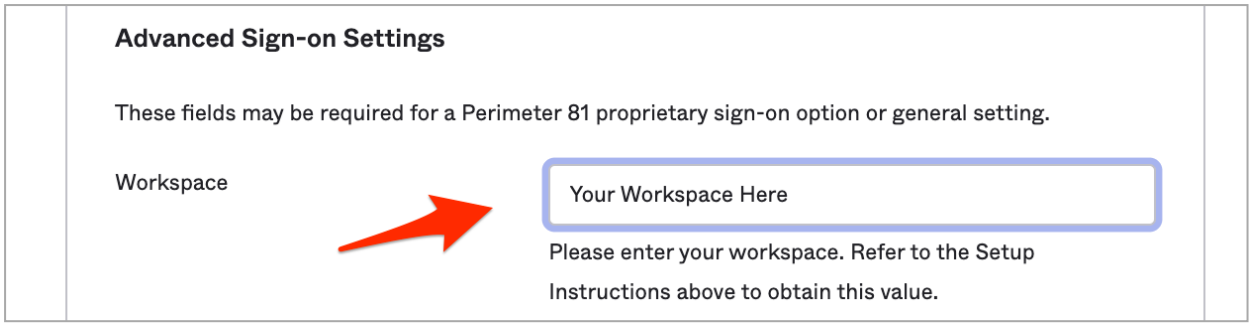


A Harmony SASE application is generated.

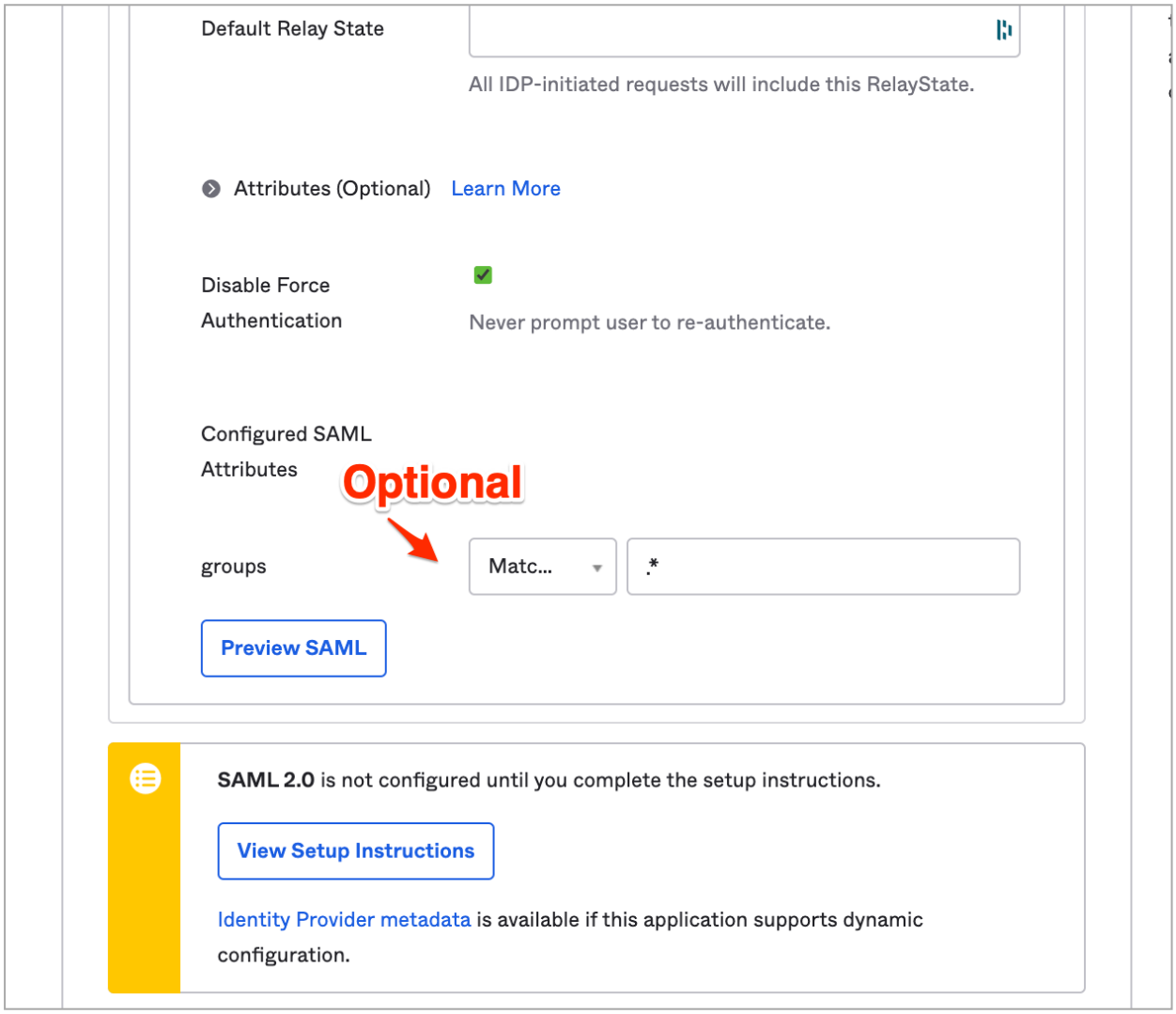
6. Go to the **Sign On** tab.
7. In the **SAML 2.0** section, click **More details** and then copy the **Sign on URL**.
8. In the **SAML Signing Certificates** section, click **Actions** and then select **Download certificate**.



9. On the **Sign On** page, go to **Settings** and click **Edit**.
10. In the **Workspace** field, enter your Harmony SASE workspace name.



11. (Optional) If you want the group membership of your Okta account to sync with Harmony SASE, make sure that the Groups has the **"Matches Regex" .*** syntax.



Note - You must create the group on Harmony SASE manually for this option to work.

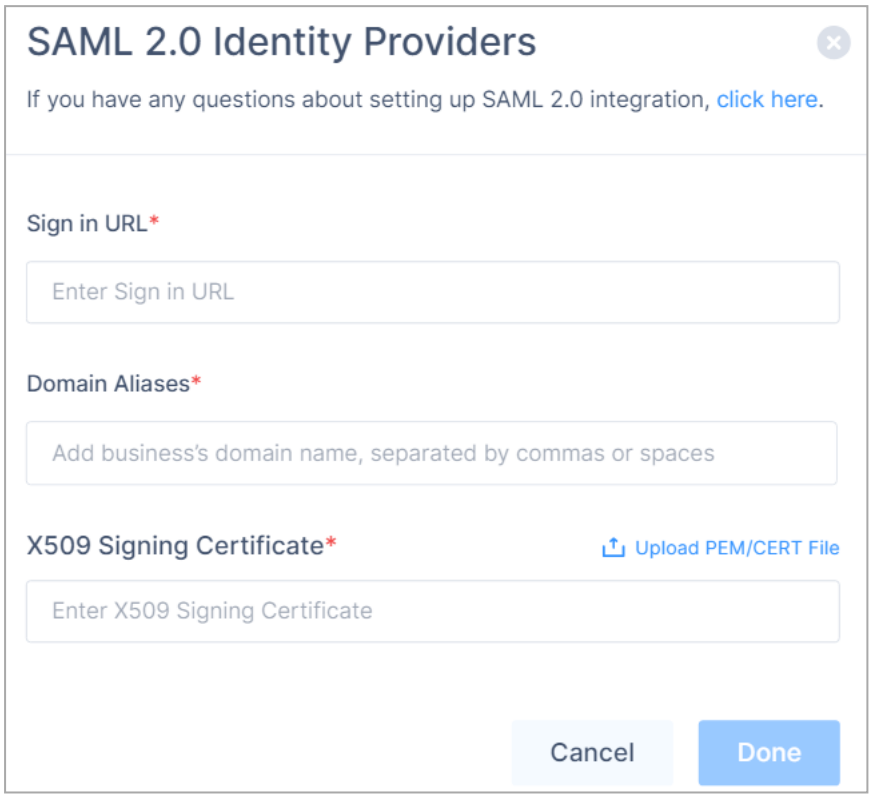
Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.

3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.

4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`

Identity Provider	Sign in URL
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

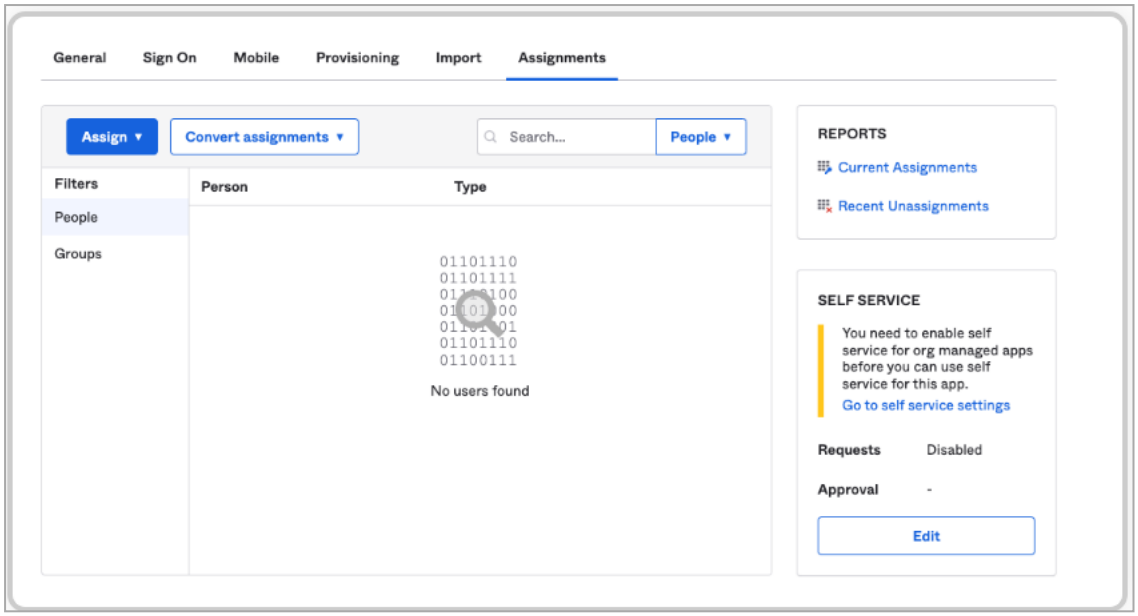
   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Step 3 - Assign the App

1. Log in to Okta Management Portal.
2. Go to **Applications** and select your SAML 2.0 Application.
3. Go to **Assignments** tab.



4. Assign the **People** or **Groups** you want to get synchronized with Harmony SASE.
5. Click **Save and Go Back** and then click **Done**.

Step 4 - Verify SP-initiated SSO

1. Log in to Harmony SASE workspace URL.
2. Click **Sign in with Okta**.
3. Verify you can successfully connect using your Okta credentials.

Supported SAML Attributes

Attribute Name	Value
given_name	user.firstName
family_name	user.lastName
email	user.email
groups	As configured in the app. **Note** - Local users not defined through Okta will not be automatically added or removed from any Okta-associated group to which they are assigned. You must manually add or remove them from the required groups.

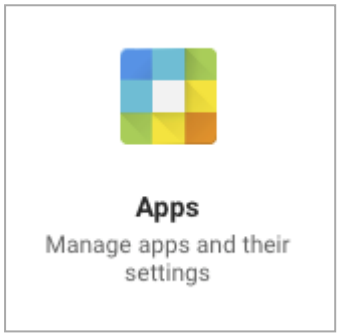
Google Applications with SAML 2.0

Prerequisites

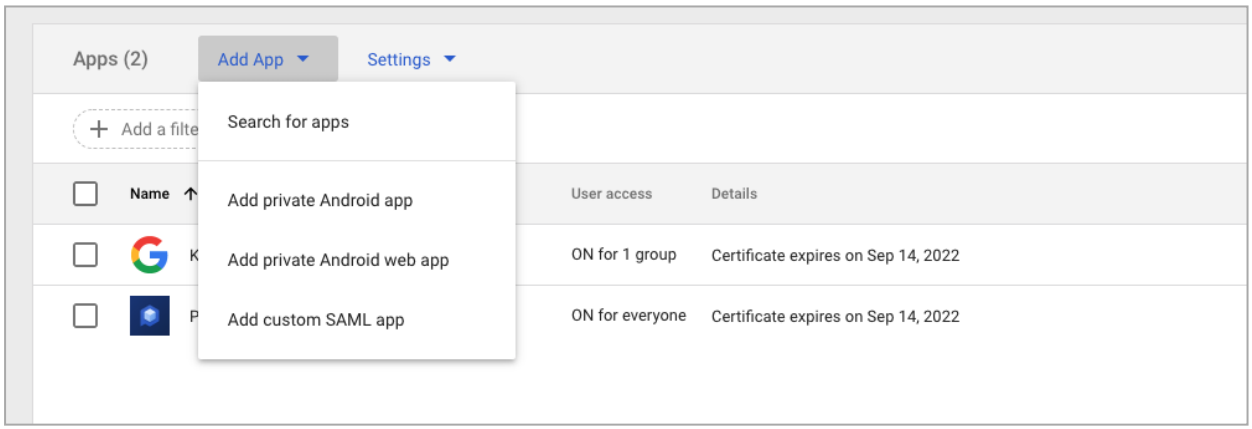
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

Step 1 - Configuring the Application in the Google Admin Console

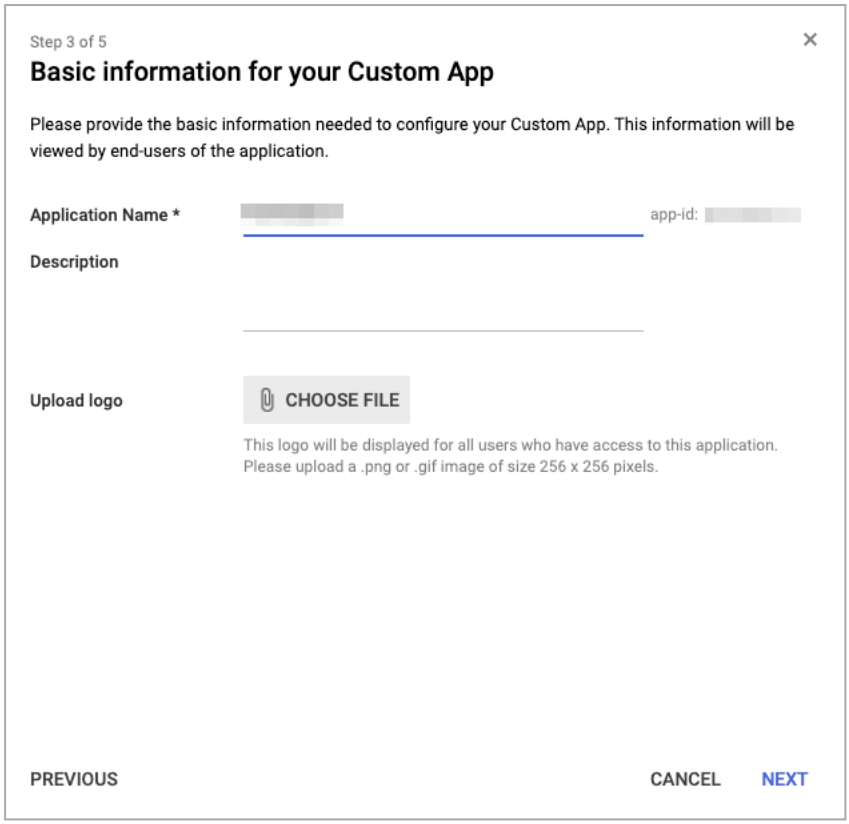
1. Log in to the Google Admin Console with a administrator account.
2. Go to **Apps**.



3. Click **Add App** and select **Add custom SAML app**.

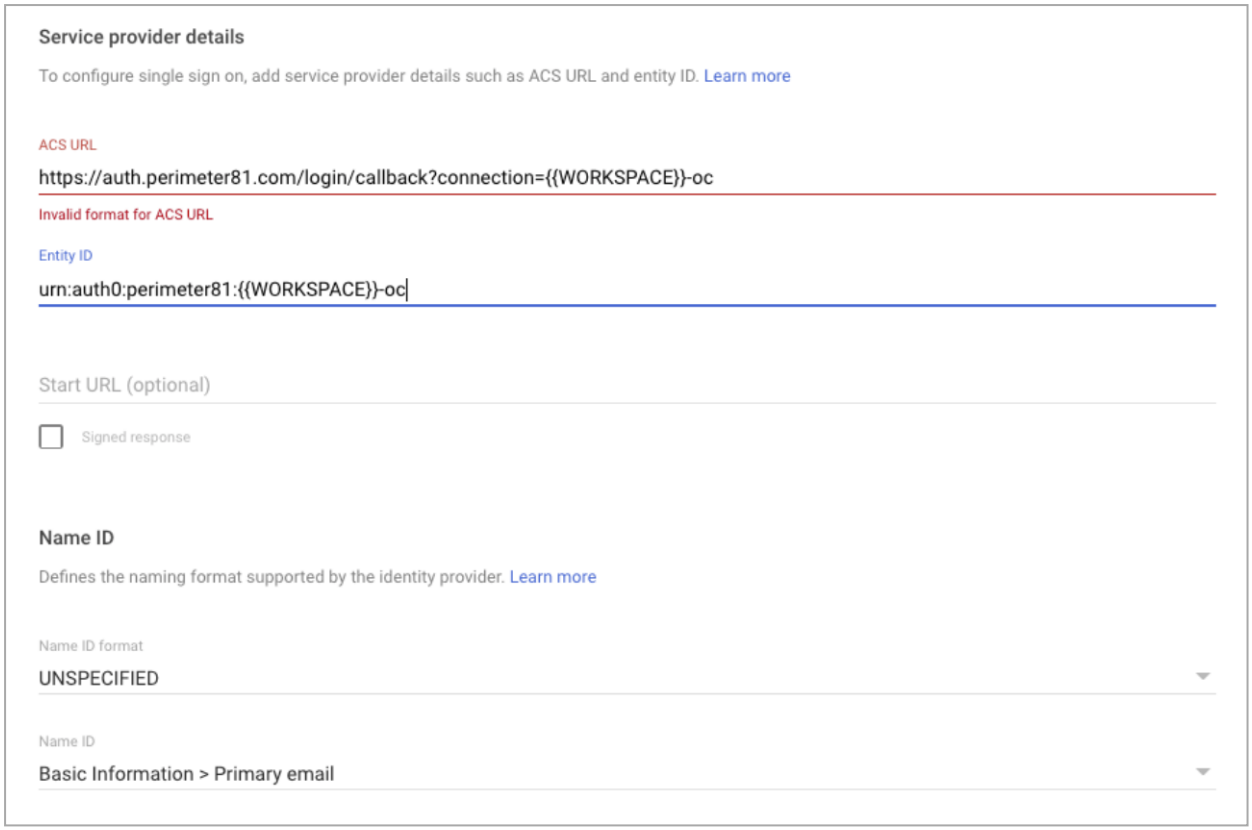


4. In the **Application Name** field, enter a name for the application.



5. (Optional) In the **Description** field, enter a description about the application.
6. (Optional) To add a logo to the application, click **Upload Logo** and select the file.
7. Click **Next**.
8. Copy the **SSO URL**.

9. Copy the certificate or click the download icon to download it.
10. Click **Next**.
11. In the **Service provider details** section:



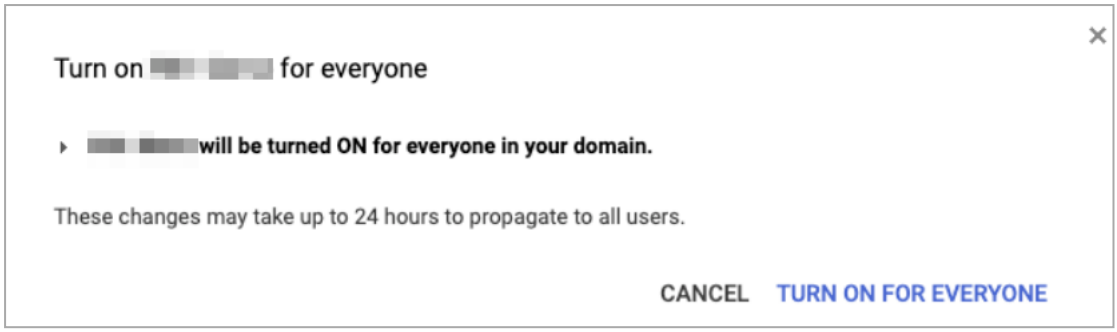
- **ACS URL** : Enter `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
- **Entity ID** : Enter `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.
- **Name ID**: Select *Basic Information > Primary Email*
- **Name ID Format**: Select *UNSPECIFIED*

12. Click **Add mapping** and enter these attribute / value pairs in separate rows:

Attribute	value
Basic Information > Primary email	email
Basic Information > Last Name	family_name
Basic Information > First Name	given_name
Employee Details > Department	groups

The system creates the application.

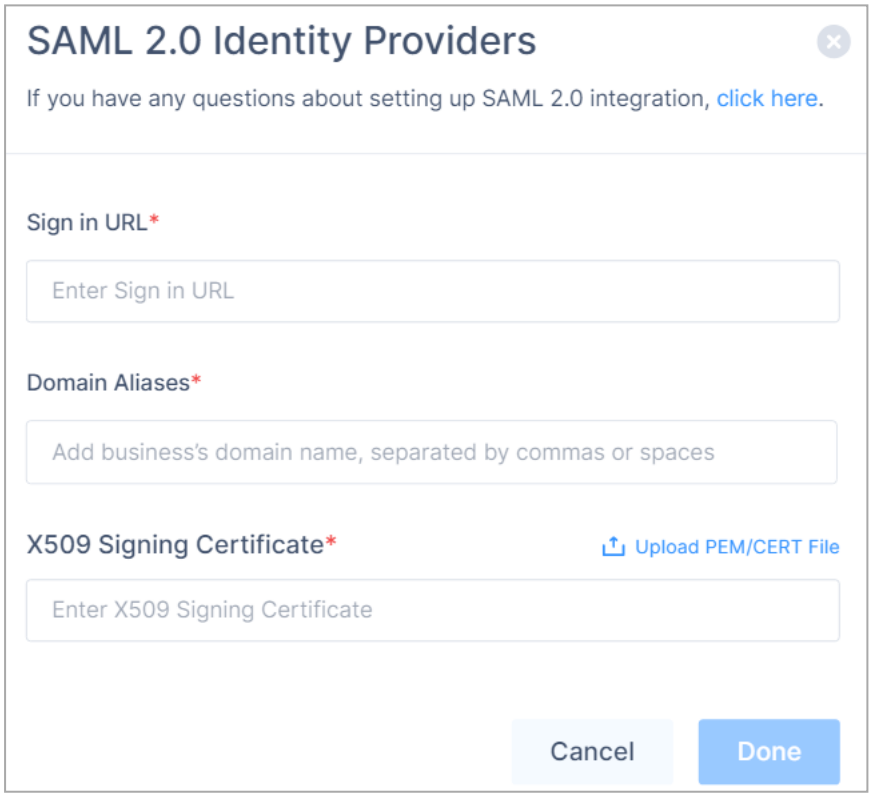
13. Click **Status** and select **Turn on for everyone**.



Step 2 - Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Google Services

Before opting for Google Services instead of the Google SAML application to log in with your Google Workspace account, evaluate the potential cost implications for using Google Services.

Prerequisites

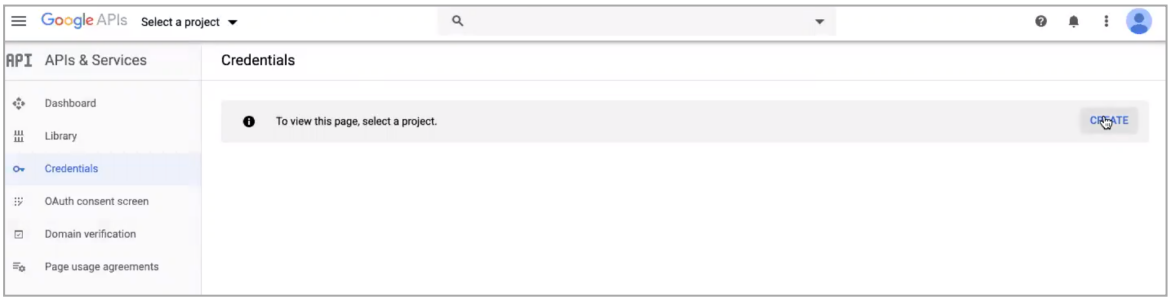
- Administrator access to the Harmony SASE Administrator Portal.
- Administrator account with the Identity Provider Management Portal.

High-Level Procedure

- *"Step 1 - Generate the Google Client ID and Client Secret" below*
- *"Step 2 - Enable the Admin SDK Service" on page 804*
- *"Step 3 - Configure the Harmony SASE Administrator Portal" on page 804*

Step 1 - Generate the Google Client ID and Client Secret

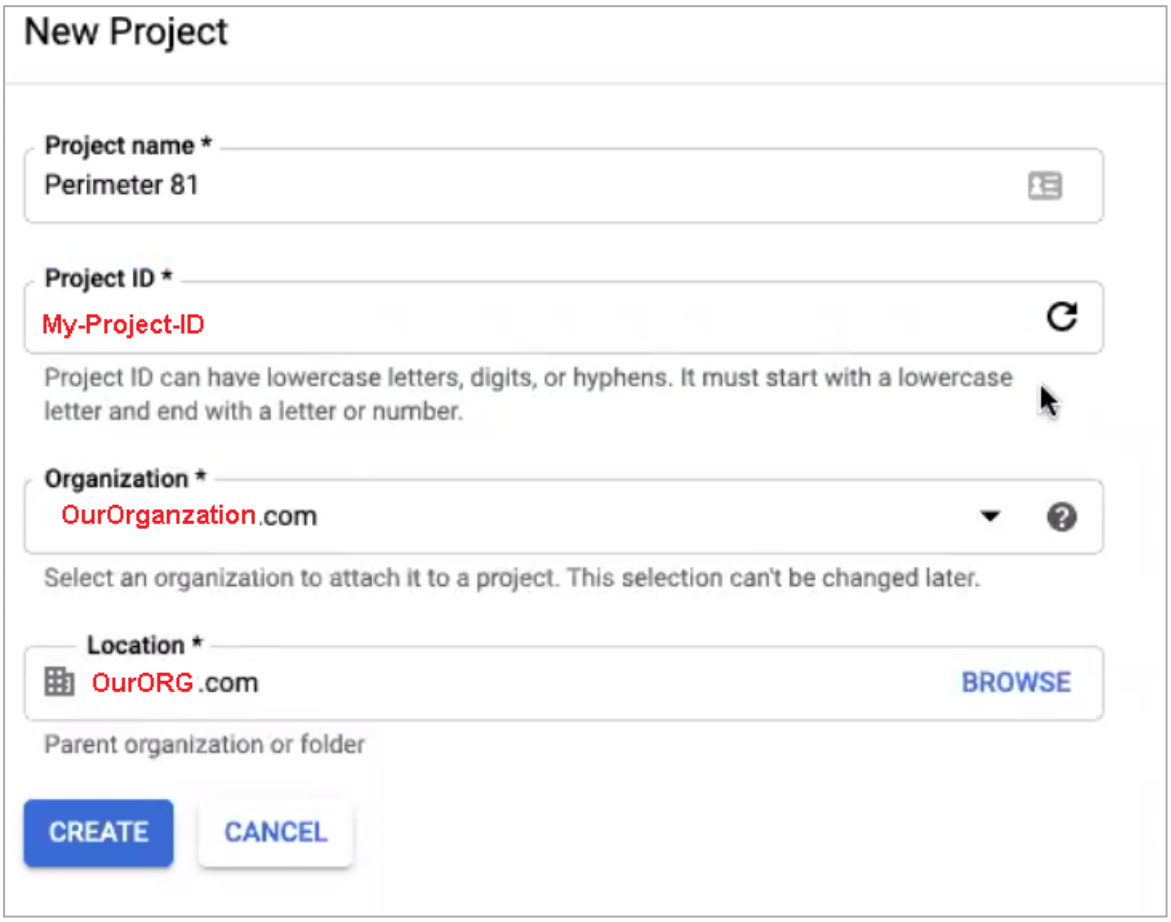
1. Log in to the Google Admin Console.
2. Open the console left side menu and select **APIs & services**, and then select **Credentials**.
3. Select a project.
4. If you do not have a project defined on Google Cloud Platform:
   a. Click **Create**.



The **New Project** pop-up appears.

b. Enter these details:

- **Project Name**
- **Project ID**
- **Organization** - The organization to which the project should attach to.
- **Location** - Parent organization or folder where the project should be saved.



c. Click **Create**.

5. Go to **OAuth consent screen**, select **User Type** as **External** and then click **Create**.

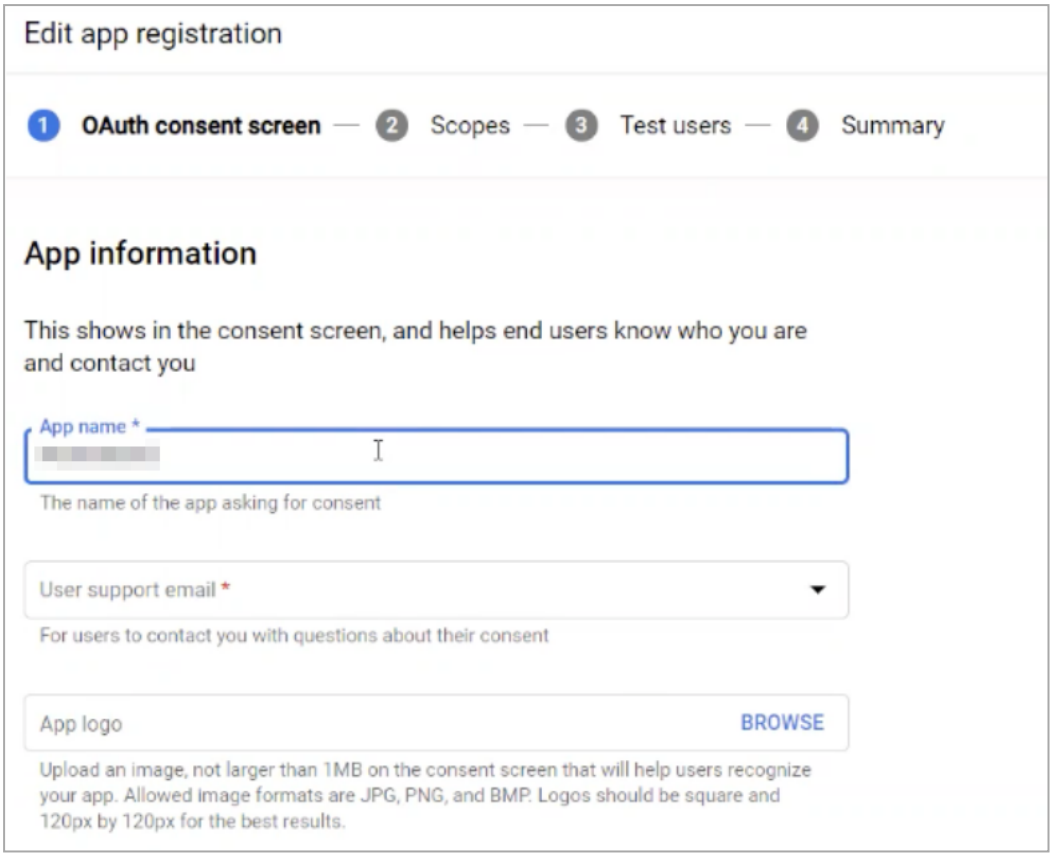
   The **Edit app registration** page appears. The information entered here will be used by the users to know who you are and contact you.

6. In the **OAuth consent screen** section, enter these values:

   a. Select the **Application Type** as **Public**.

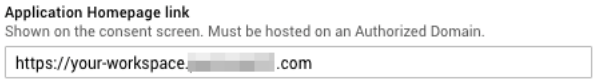
   b. In the **Application Name** field, enter a name for the application.

c. In the **User support email** field, enter an email address. The users use this email address to contact for questions about the consent.



d. (Optional) To add a logo, in the **Add logo** field, click **Browse** and select the logo.

e. In the **Application Homepage link** field, enter your Harmony SASE workspace URL.

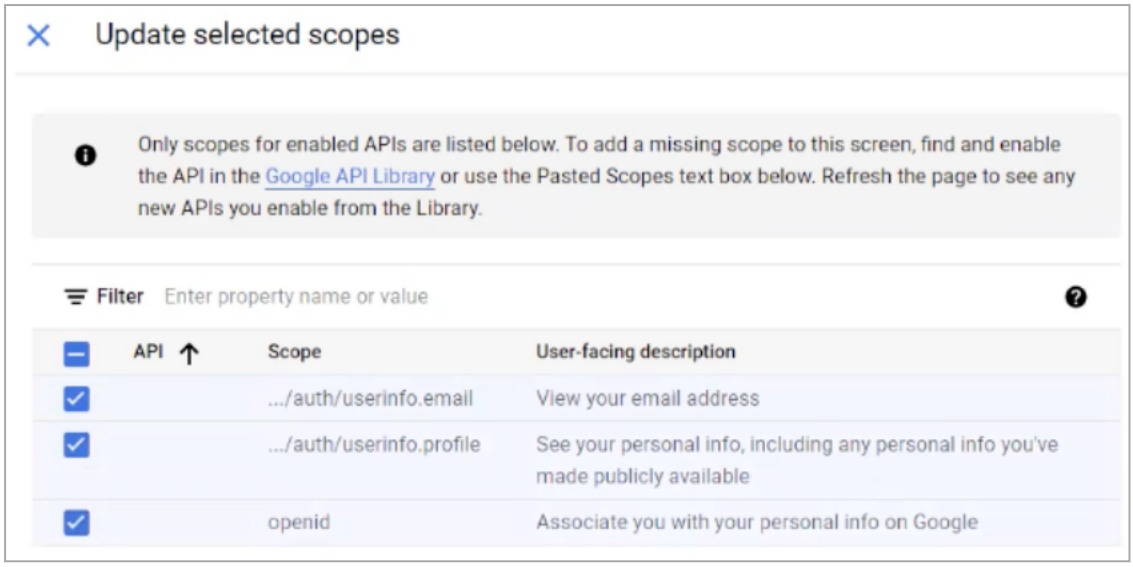


f. In the **Authorized domains** section, enter your domain name and click **Add Domain**.

g. In the **Developer contact information** field, enter your support email address.

h. Click **Save and Continue**.

7. In the **Scopes** section, select these options:



a. Click **Add or Remove Scopes**.

b. Select these scopes:

   i. userinfo.email

   ii. userinfo.profile

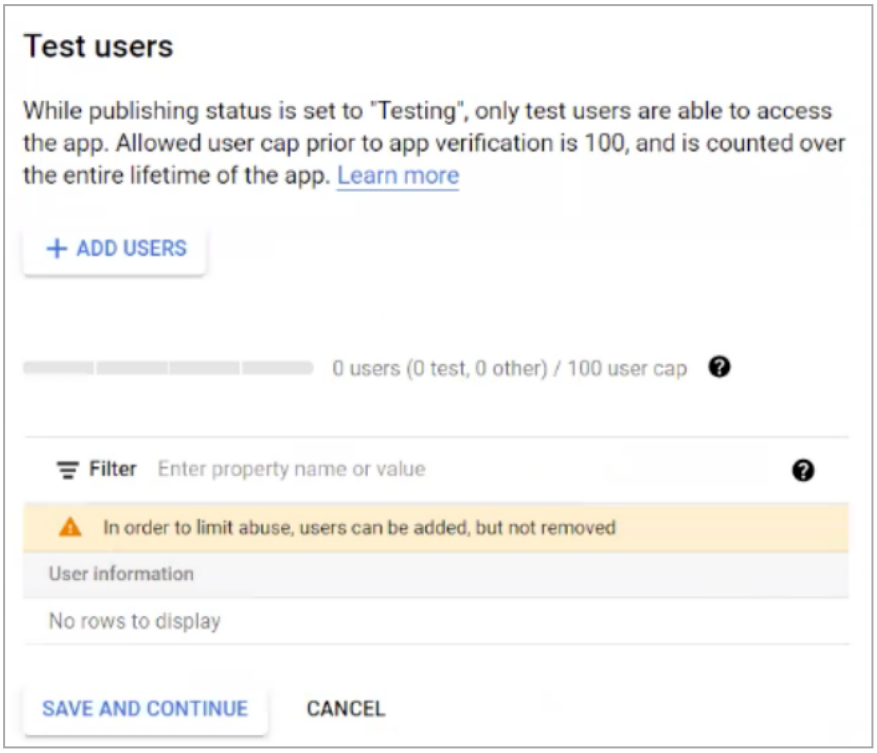
   iii. openid

c. Click **Update** and then click **Save and Continue**.

8. (Optional) To test the users if they are able to access the application:

a. Click **Add Users**.

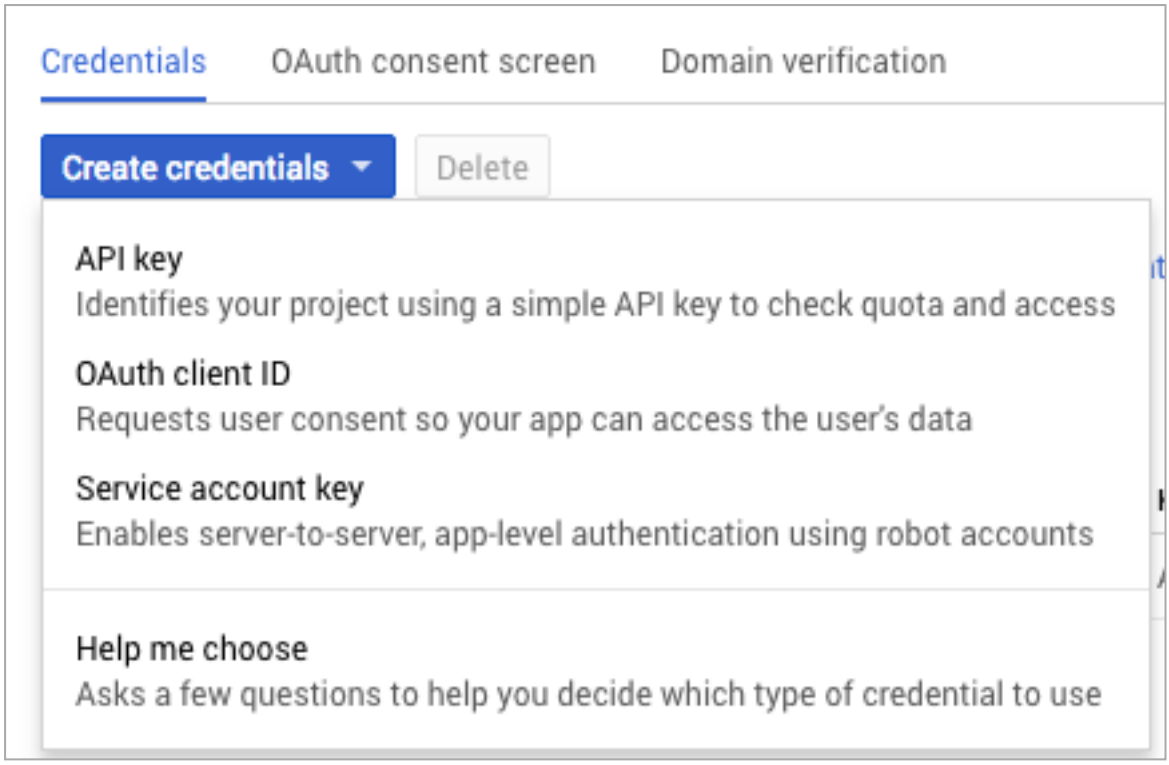
b. Enter the user email addresses.



9. To skip testing the users and continue, click **Save and Continue**.

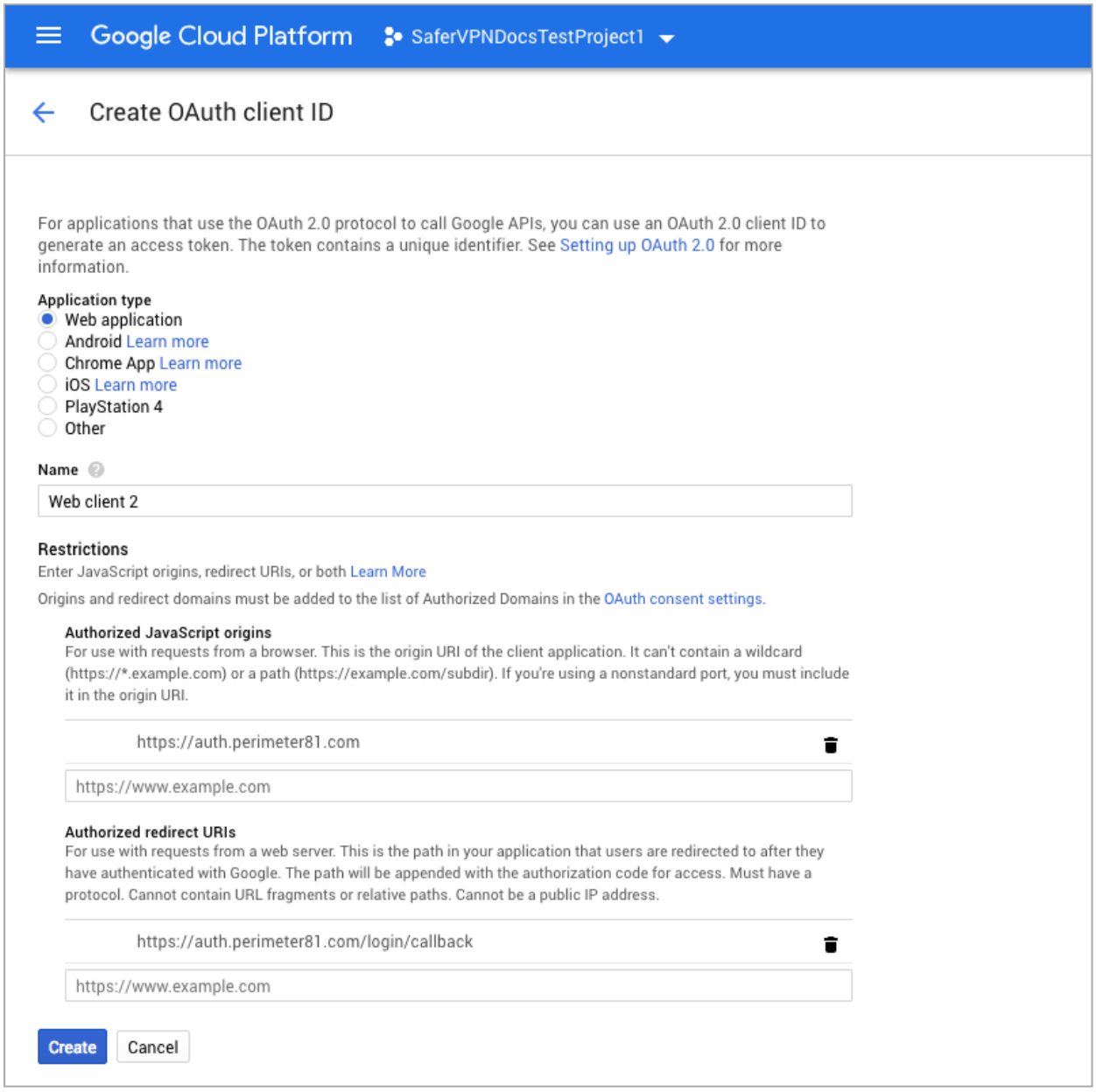
   Google creates your project and when the process completes, it prompts you to create credentials.

10. Click **Create credentials** and then select **OAuth client ID**.



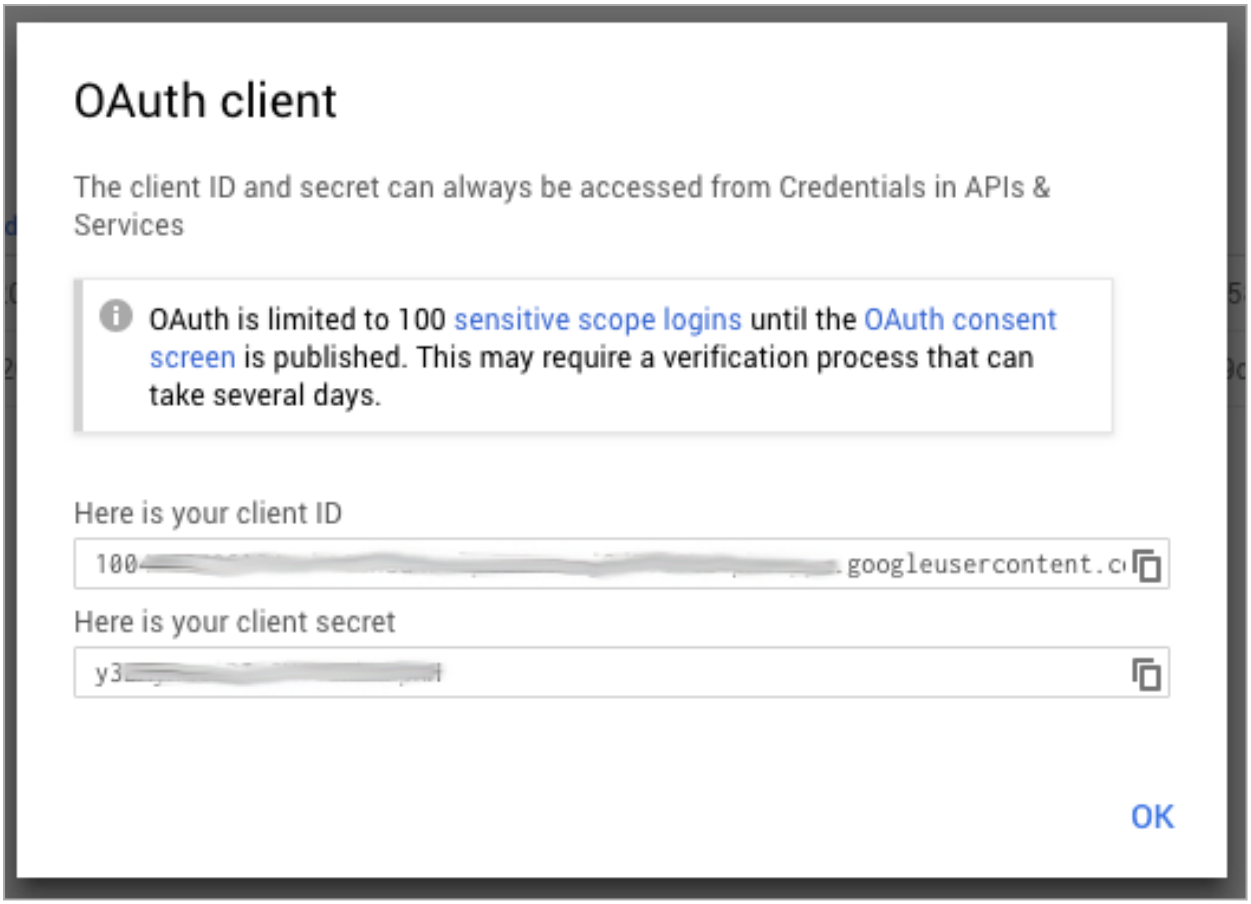
Google shows a **To create an OAuth client ID, you must first set a product name on the consent screen** warning.

11. Click **Configure consent** and enter a product name to appear for the users when they log in through Google.
12. Google prompts you to provide additional information about the newly-created app. Enter these details:



- In the **Application type**, select **Web application**.
- In the **Name** field, enter a name for the application.
- In the Restrictions section, enter these details:
  - **Authorized JavaScript origins**: https://auth.perimeter81.com
  - **Authorized redirect URI**: https://auth.perimeter81.com/login/callback
- Click **Create**.

13. If Google shows "unverified app" screen before showing the consent for your app, complete the OAuth Developer Verification.
14. Copy the **Client ID** and **Client Secret**.



Step 2 - Enable the Admin SDK Service

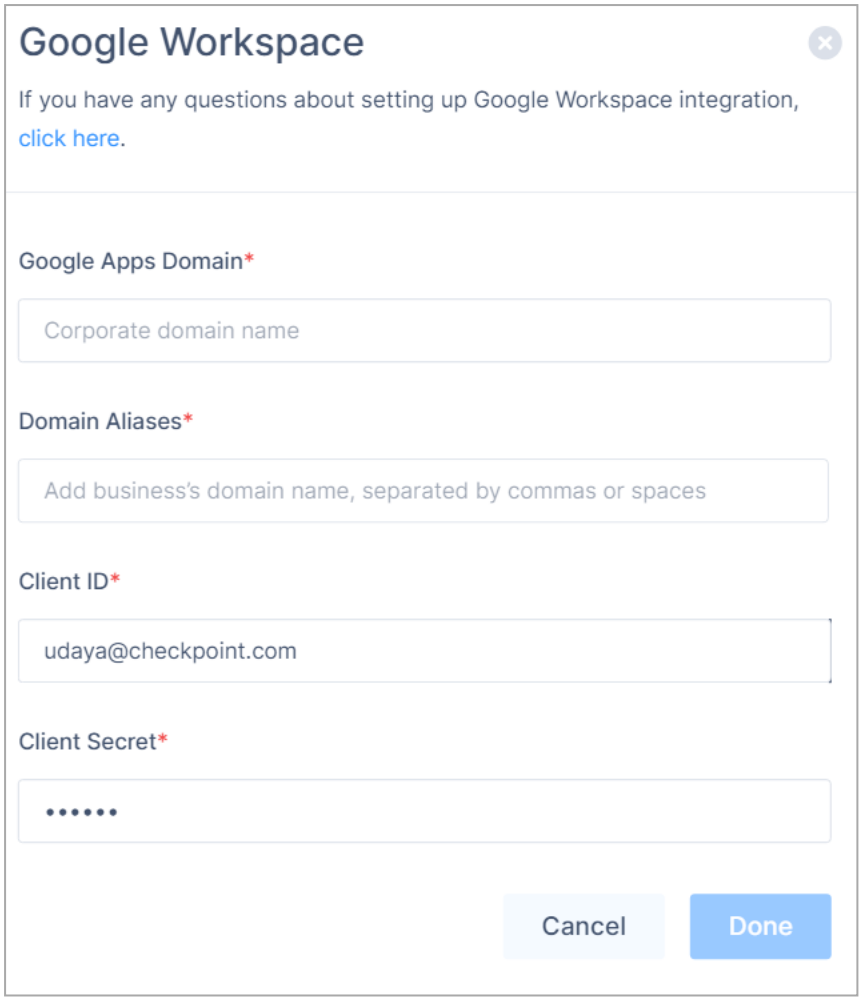
To connect to Google Suite enterprise domains, you need to enable the **Admin SDK** service. To do that:

1. Log in to the Google Admin Console with a administrator account.
2. From the console left side menu, select **APIs & services**, and then select **Library**.
3. Select **Admin SDK**.
4. On the **Admin SDK** page, select **Enable**.

Step 3 - Configure the Harmony SASE Administrator Portal

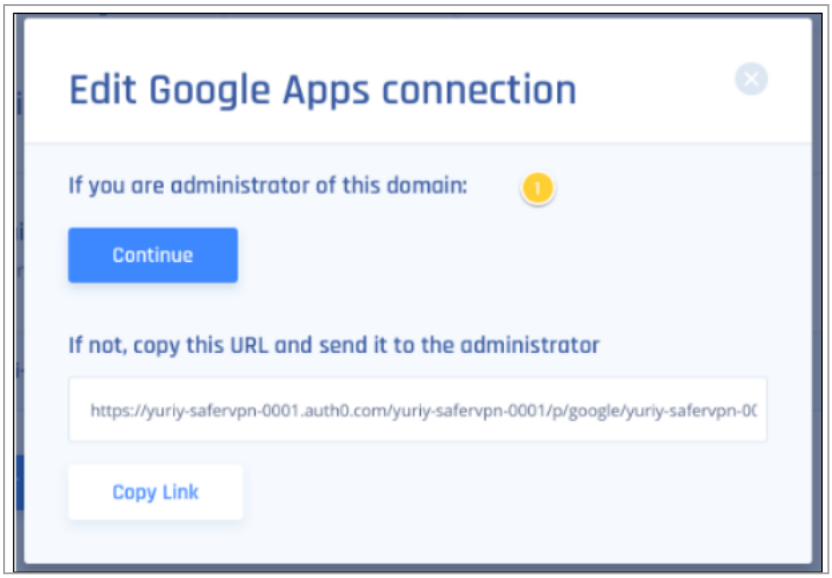
1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **Google Workspace** and click **Continue**.
5. In the **Google Apps Domain** field, enter your corporate domain name.



6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **Client ID** field, enter the client ID.
8. In the **Client Secret** field, enter the client secret.
9. Click **Done**.

   The **Edit Google Apps connection** pop-up appears.



You must configure the application to use Google's Admin APIs. To do that, you must authenticate the application.

10. If you are an administrator in Google Workspace or you have the credentials of such a user, click **Continue** and authenticate the application.

    Best Practice - To authenticate, use a service user account with the sufficient permissions. If you authenticate with an administrator account and if that administrator leaves the organization, you must create a new **Client ID** and **Client Secret** and then re-authenticate with the new user.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

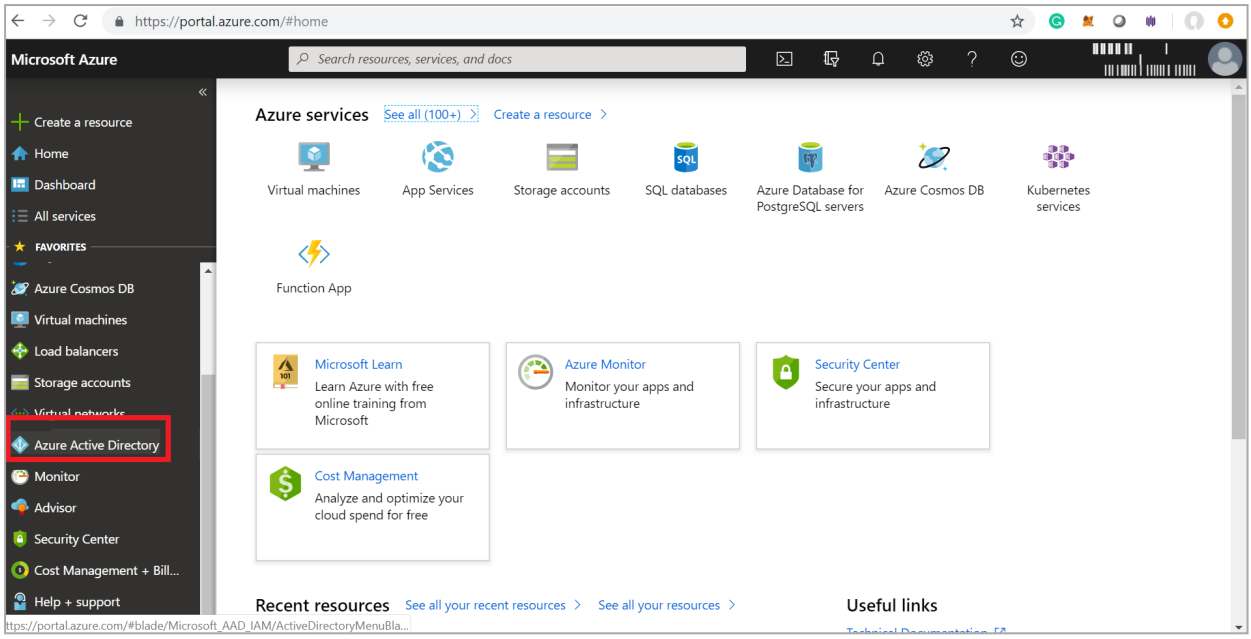
- Associates the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Microsoft Entra ID (formerly Azure AD) (SAML 2.0)

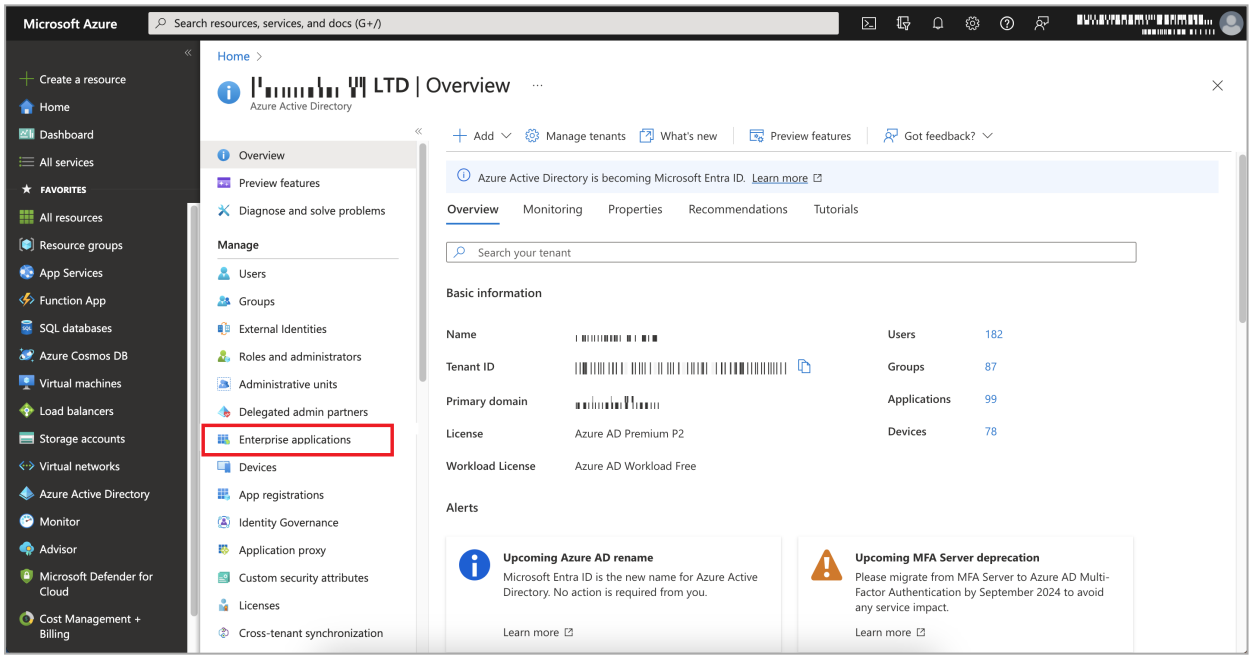
Harmony SASE allows you to authenticate securely by integrating Microsoft Entra ID (formerly Azure AD) with SAML 2.0.

Configure Microsoft Azure Portal

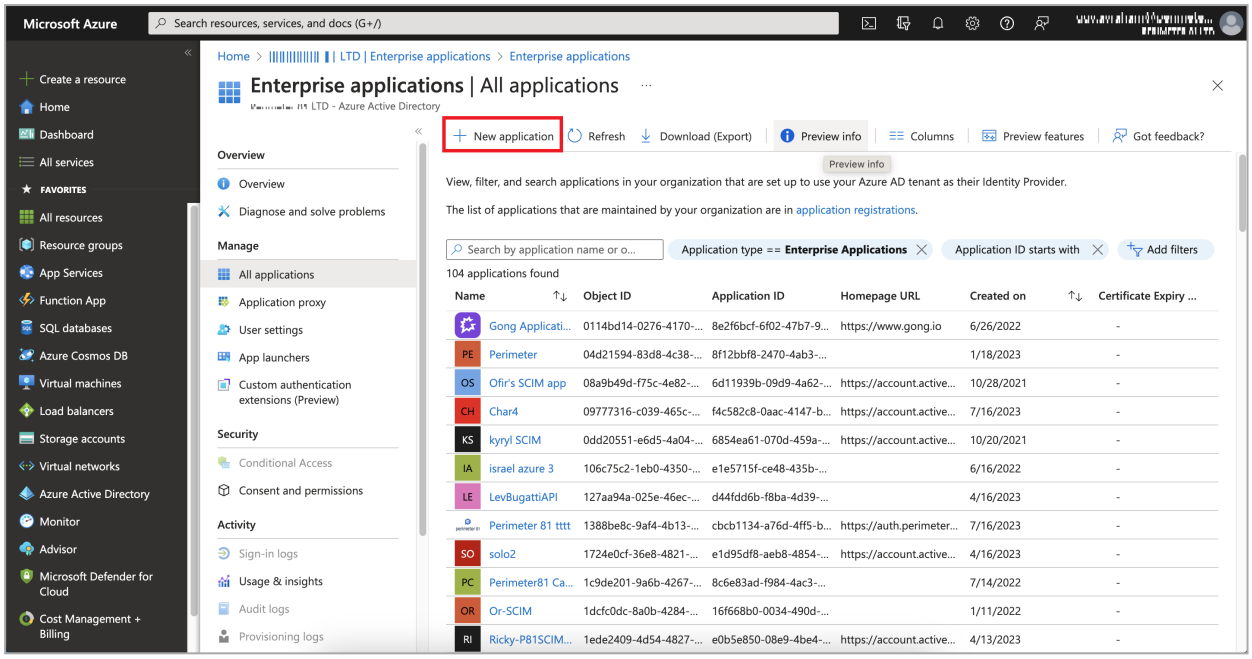
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.



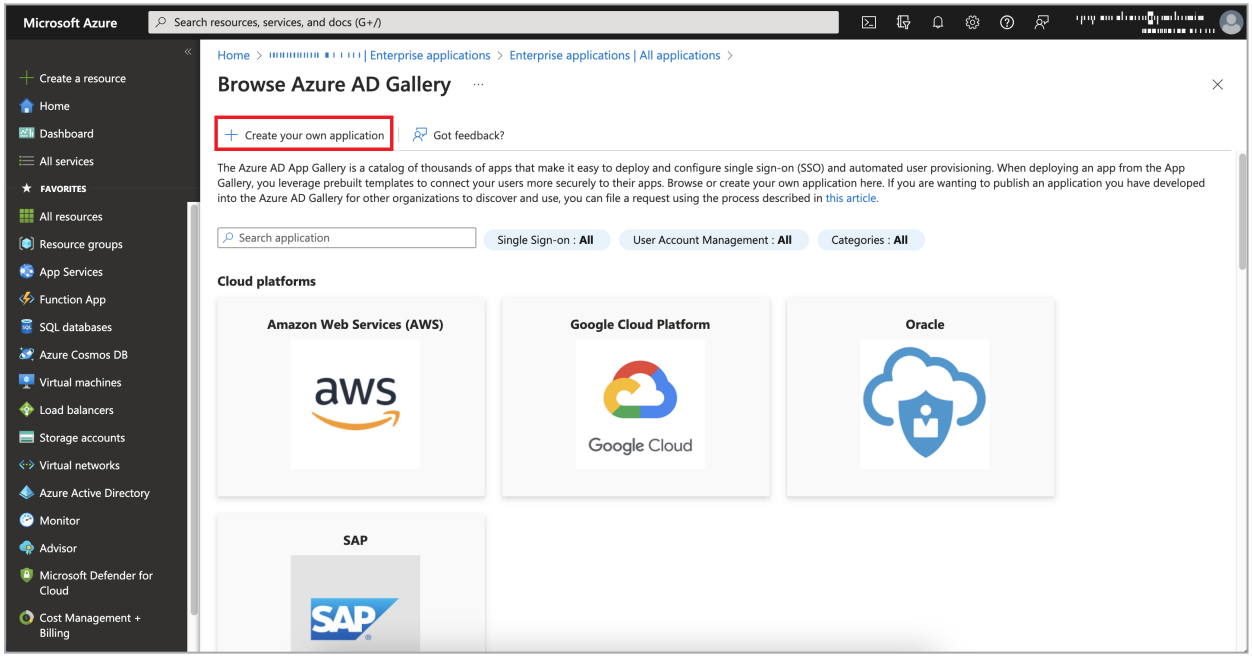
3. Go to **Manage** > **Enterprise applications**.



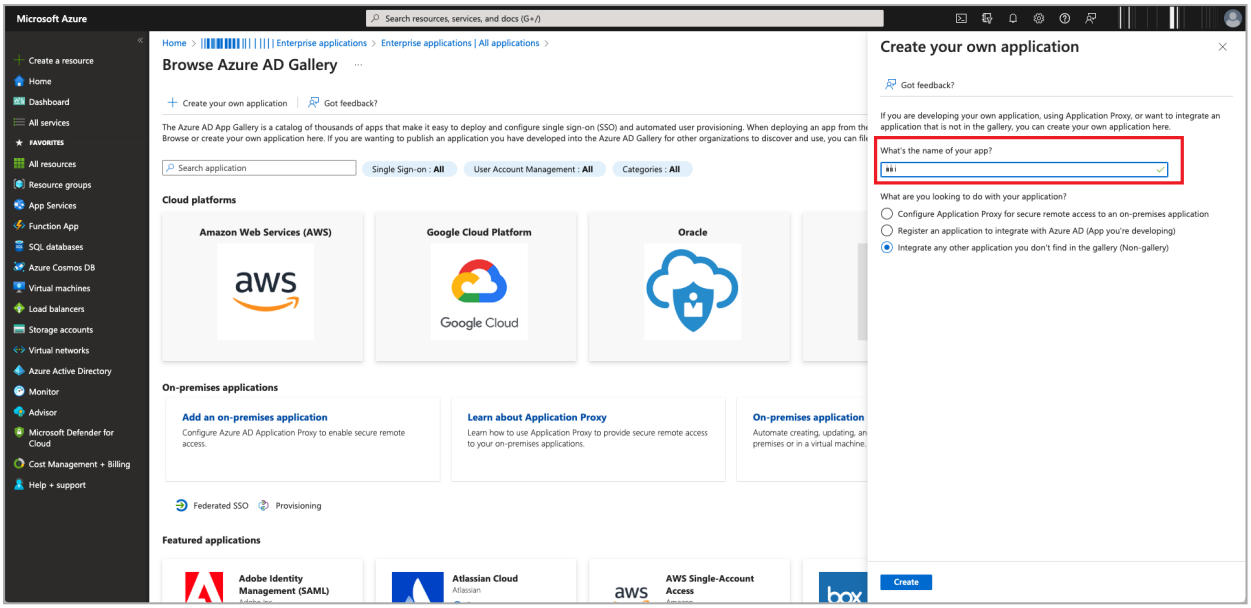
4. Click **New application**.



5. Click **Create your own application**.



6. In the **What's the name of your app** filed, enter a name for your application.

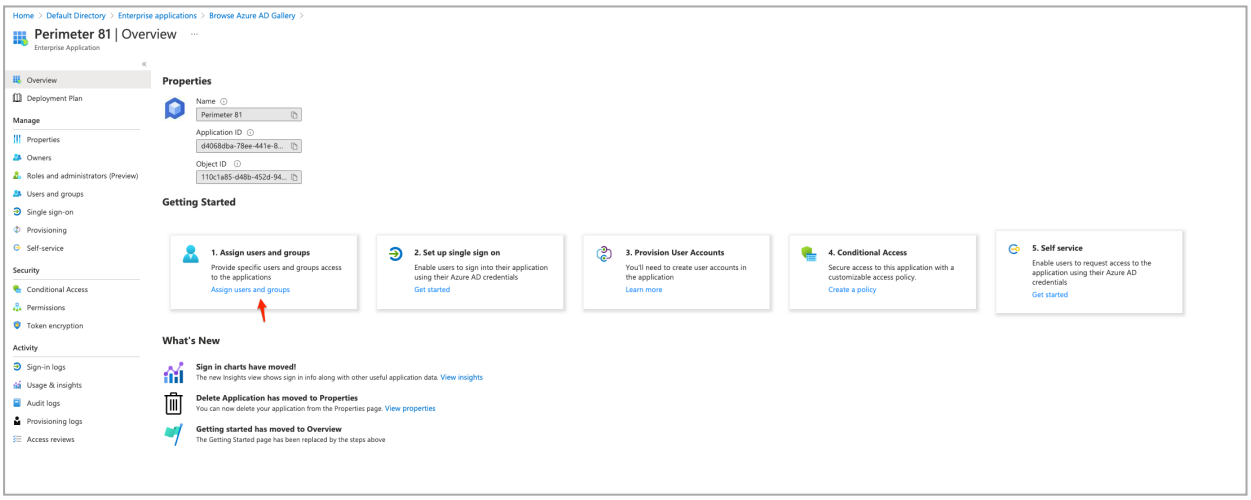


Note - Do not change the default setting.

7. Click **Create**.

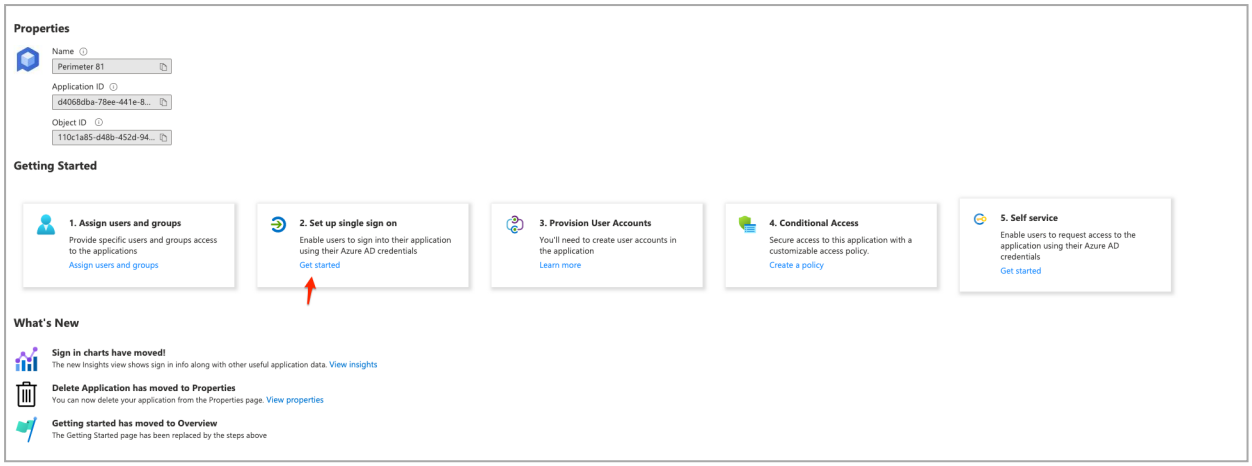
   The Microsoft Azure application is created.

1. Click **Assign users and groups** tile in the **Getting Started** section.

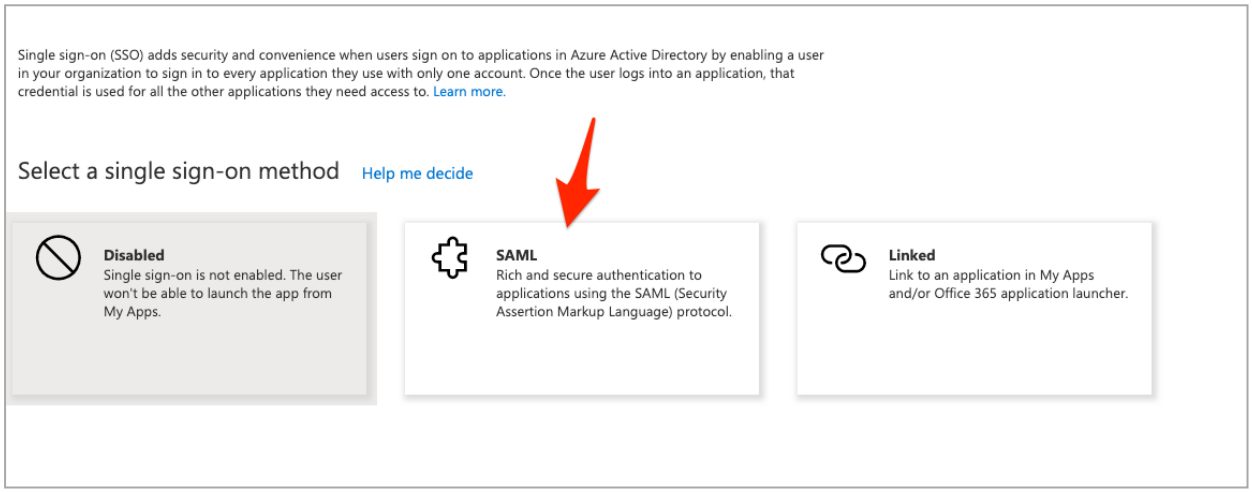


2. Search for and select the user and group that you want to assign to the application. If you are using Azure AD Free edition, you cannot add groups, add individual users instead.

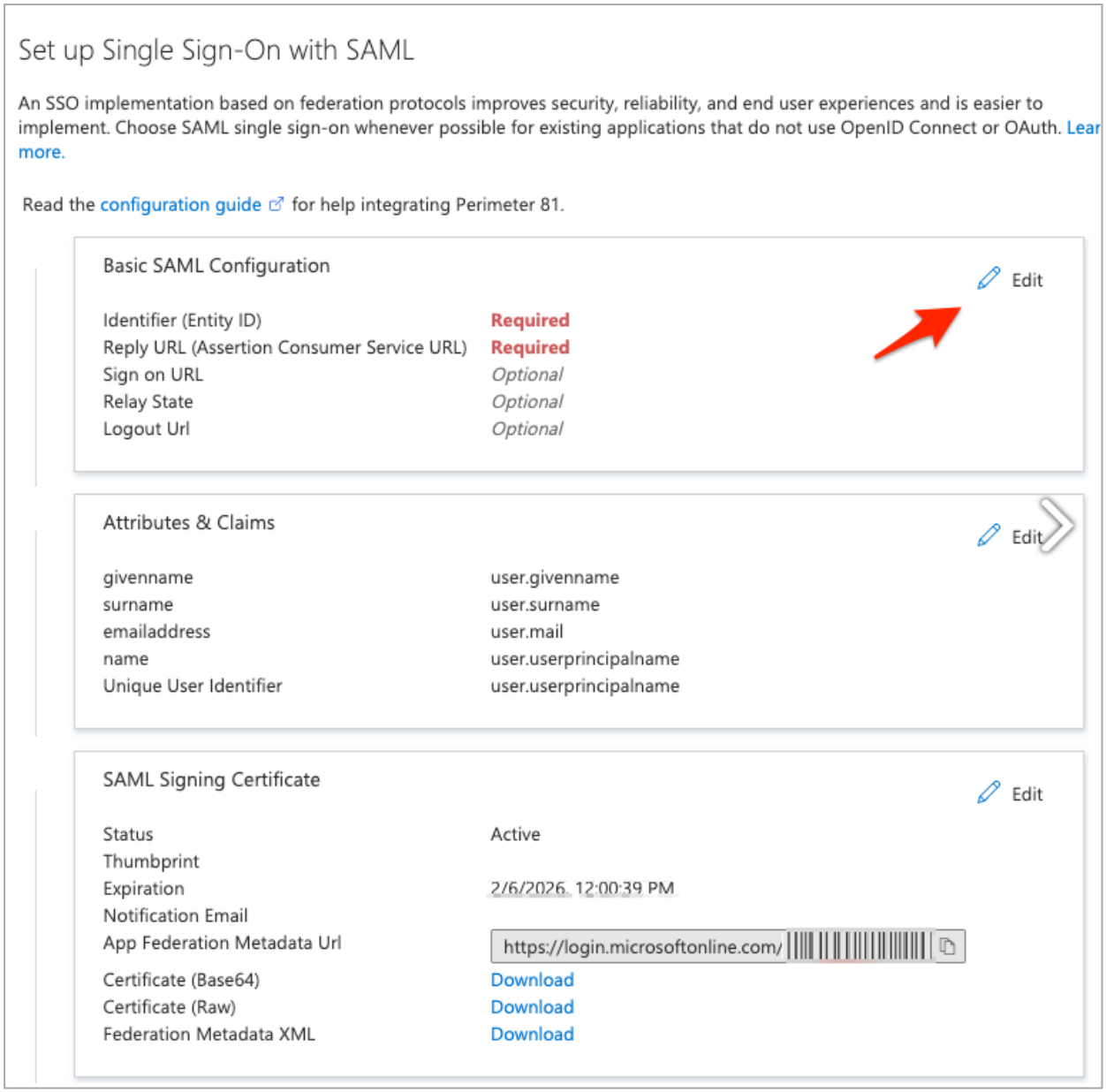
3. Click **Set up single sign on** to enable and configure single sign-on for your application.



The **Select a single sign-on method** window appears.



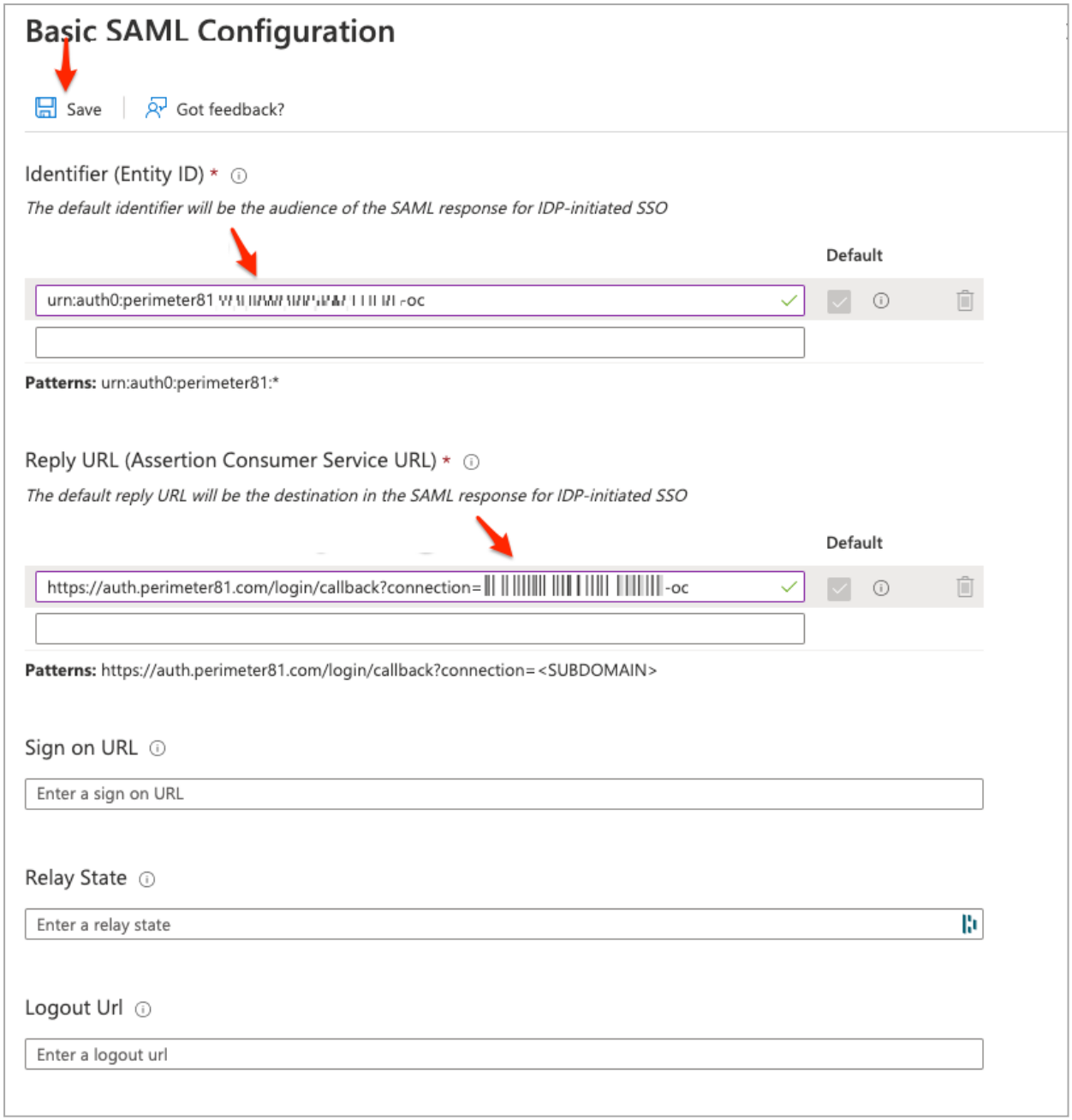
4. Click **SAML**.
5. Click **Edit** in the **Basic SAML Configuration** tile.



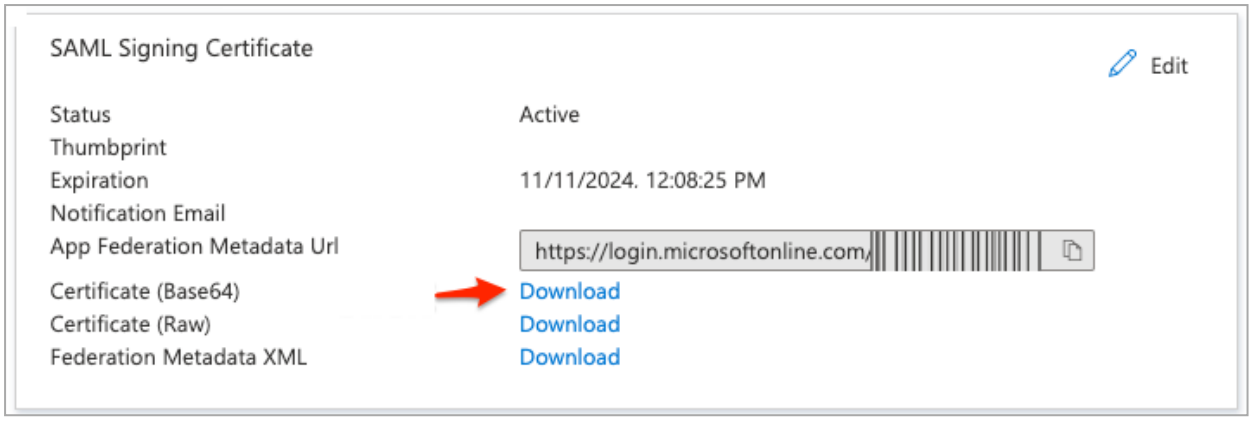
6. Enter these:

   a. **Identifier** - `urn:auth0:perimeter81:{{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.

   b. **Reply URL (Assertion Consumer Service URL)** - `https://auth.perimeter81.com/login/callback?connection={{WORKSPACE}}-oc` where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.

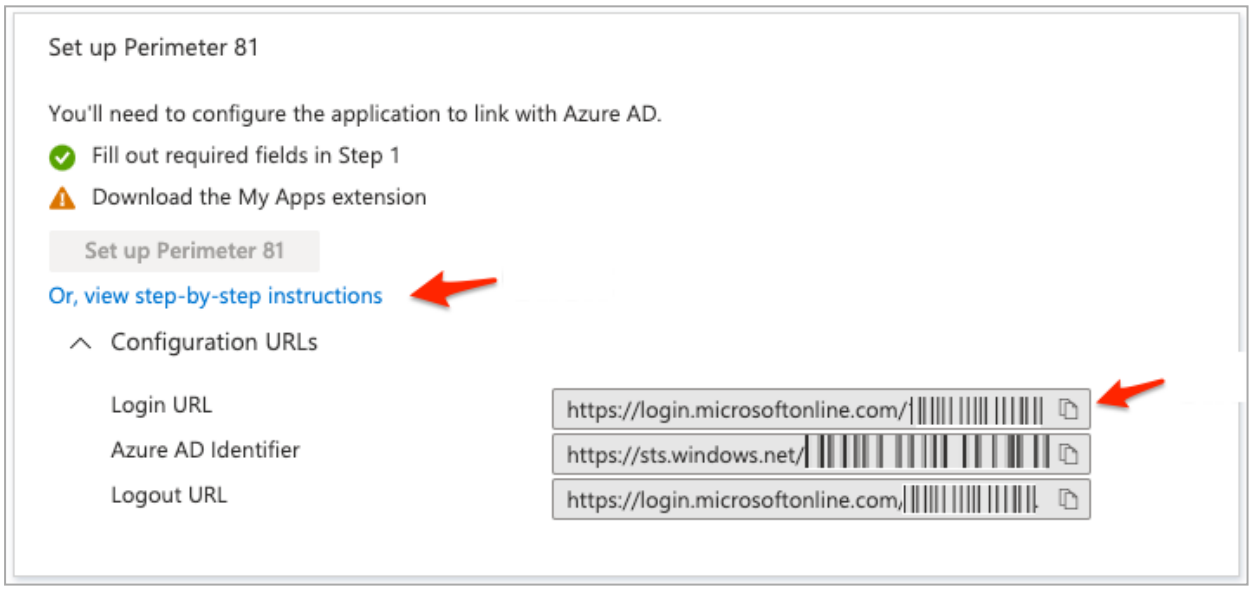


7. Click **Save**.
8. Back on the **SAML Signing Certificate** tile, go to the **Certificate (Base64)** file and click **Download**.



The Certificate (Base64) is downloaded. This certificate will be used for configuring the SAML settings for the application.

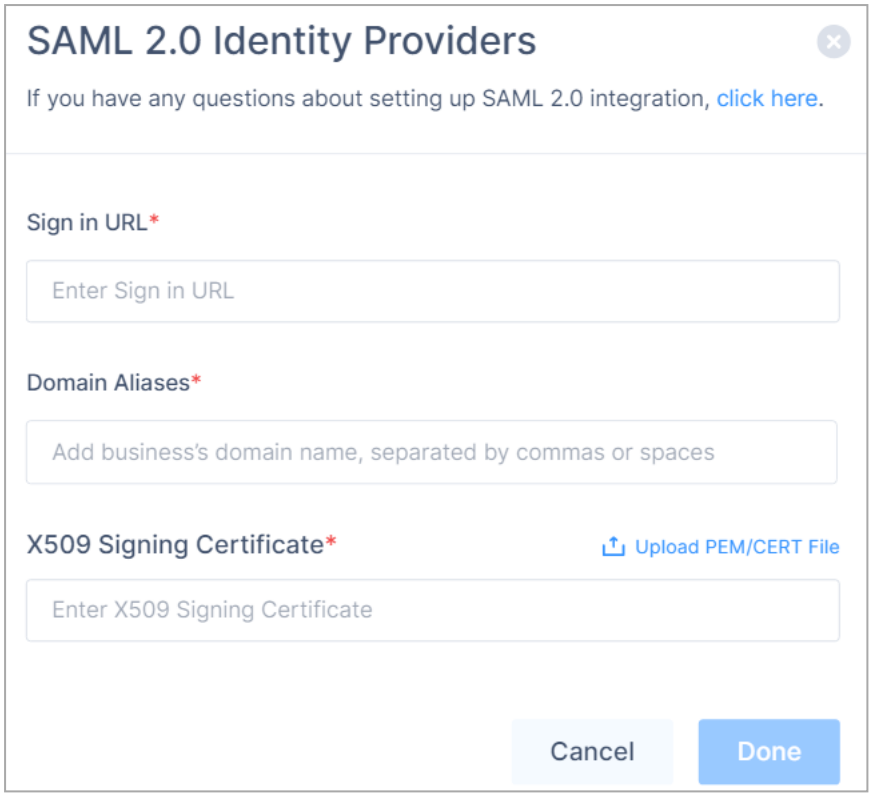
9. To copy your Login URL, go to the **Set up Harmony SASE** tile, expand **Or, view step-by-step instructions** and click ⧉.



Configure the Harmony SASE Administrator Portal

1. Log in to the Harmony SASE Administrator Portal with a administrator account.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.

   The **Add identity provider** pop-up appears.
4. Select **SAML 2.0 Identity Providers** and click **Continue**.



5. In the **Sign in URL** field, enter the Identity Provider Sign-in URL from your SAML Identity Provider.

Identity Provider	Sign in URL
Generic SAML	Identity Provider **Sign in URL**
Active Directory Federation Services (AD FS)	`https://{{Your ADFS Domain}}/adfs/ls`
Auth0	Auth0 login URL
OneLogin	SAML 2.0 Endpoint (HTTP) value
PingOne	`https://sso.connect.pingidentity.com/sso/idp/SSO.saml2?idpid={{idpid}}`
PingFederate	`https://sso.{{Your PingFederate Domain}}.com/idp/SSO.saml2`

Identity Provider	Sign in URL
Rippling	Rippling **IdP Sign-in URL**.
JumpCloud	JumpCloud **IDP URL**
Okta	Okta **Sign on URL**
Google Applications	**SSO URL**

6. In the **Domain Aliases** field, enter the business domain names separated by commas or space.
7. In the **X509 Signing Certificate** field, enter the X.509 signing certificate for the application from the SAML Identity Provider.

   If you have the signing certificate as PEM/CERT file, click **Upload PEM/CERT File** and select the file.
8. Click **Done**.

Note - After the first successful authentication of a member with SAML, Harmony SASE does this:

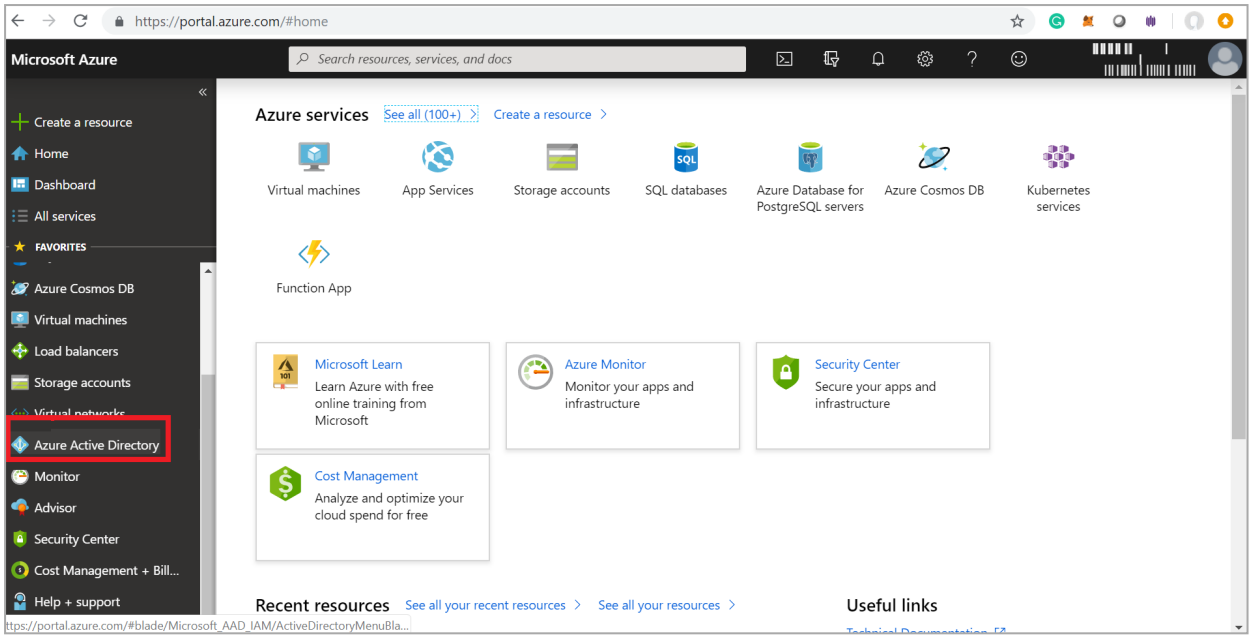
- Assigns the member with the appropriate role.
- Adds the member to the groups related to Identity Provider.
- Applies the relevant configuration profiles to the member.

Microsoft Entra ID (formerly Azure AD) (Enterprise Application)

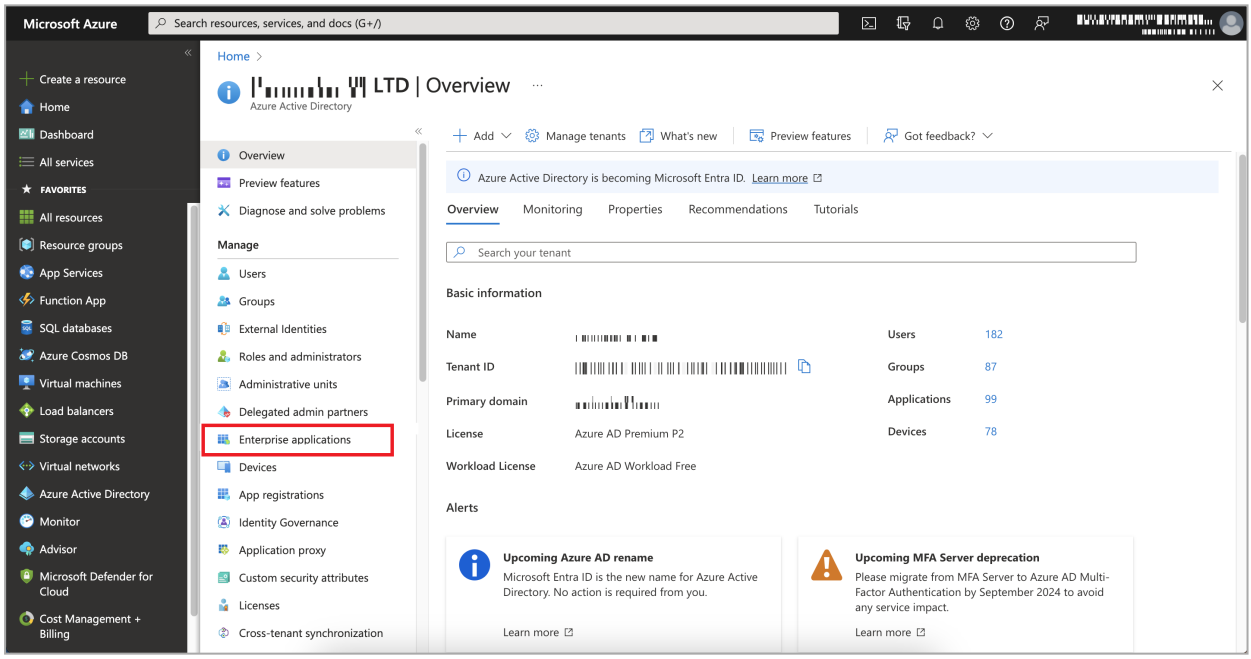
You can enable users to log in using a Microsoft Entra ID (formerly Azure AD) account, either from your computer or from the external directory.

Registering Application through the Microsoft Azure Portal

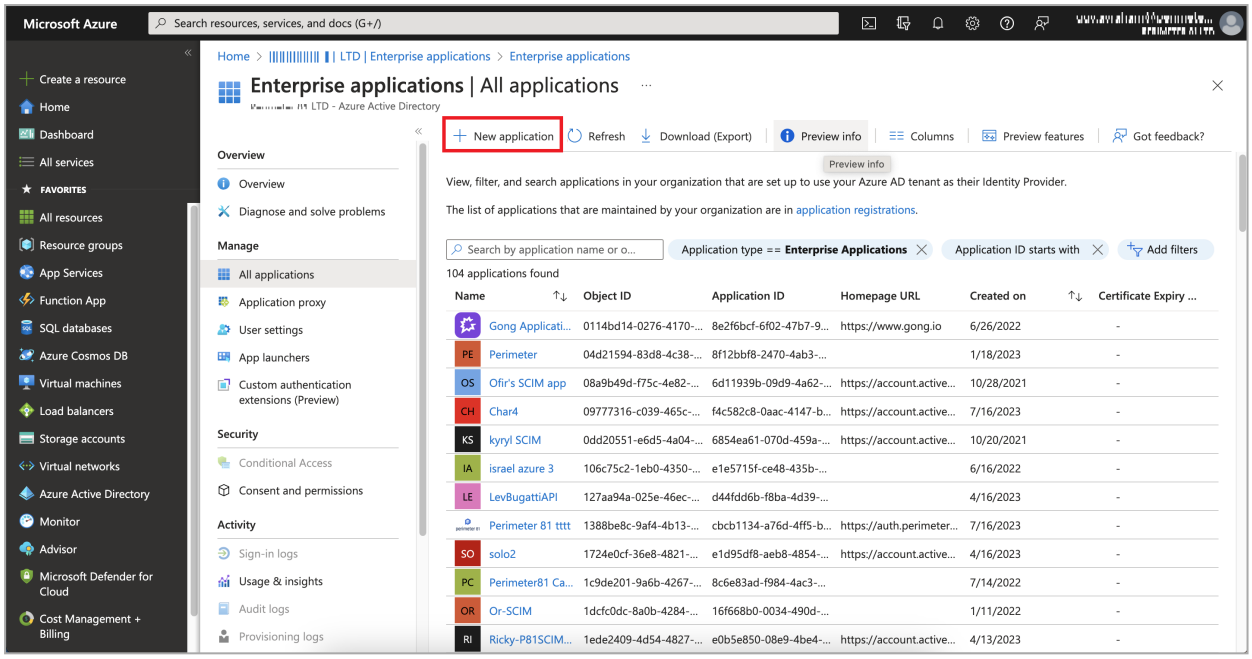
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.



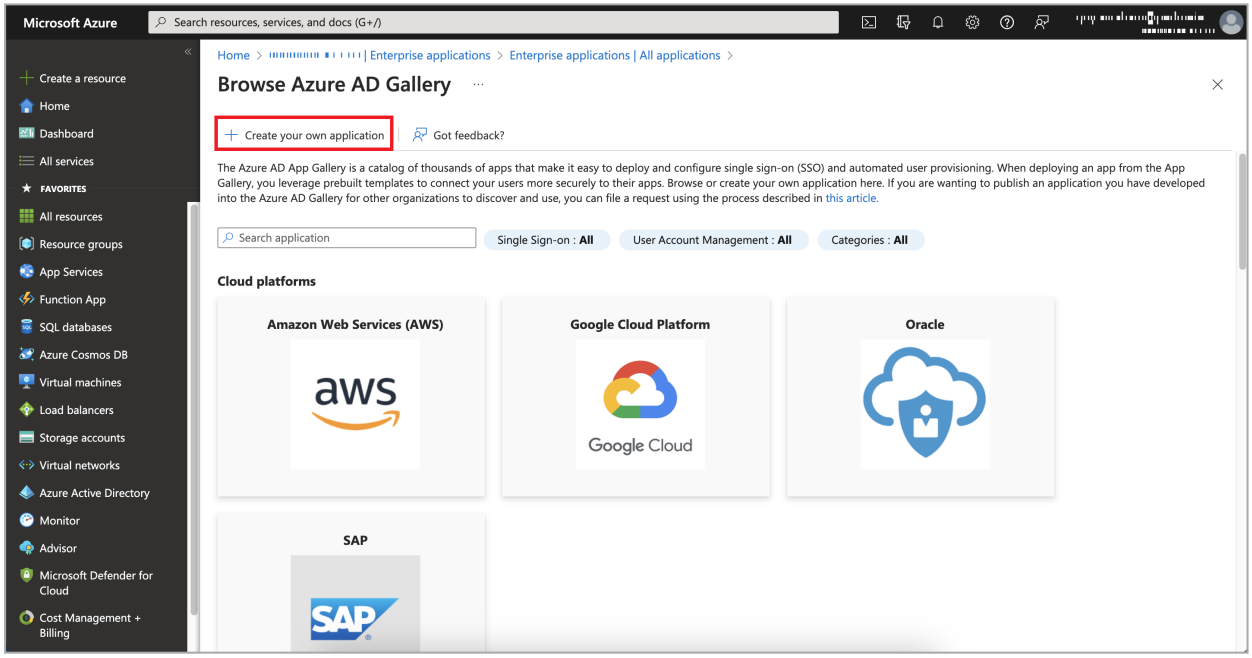
3. Go to **Manage** > **Enterprise applications**.



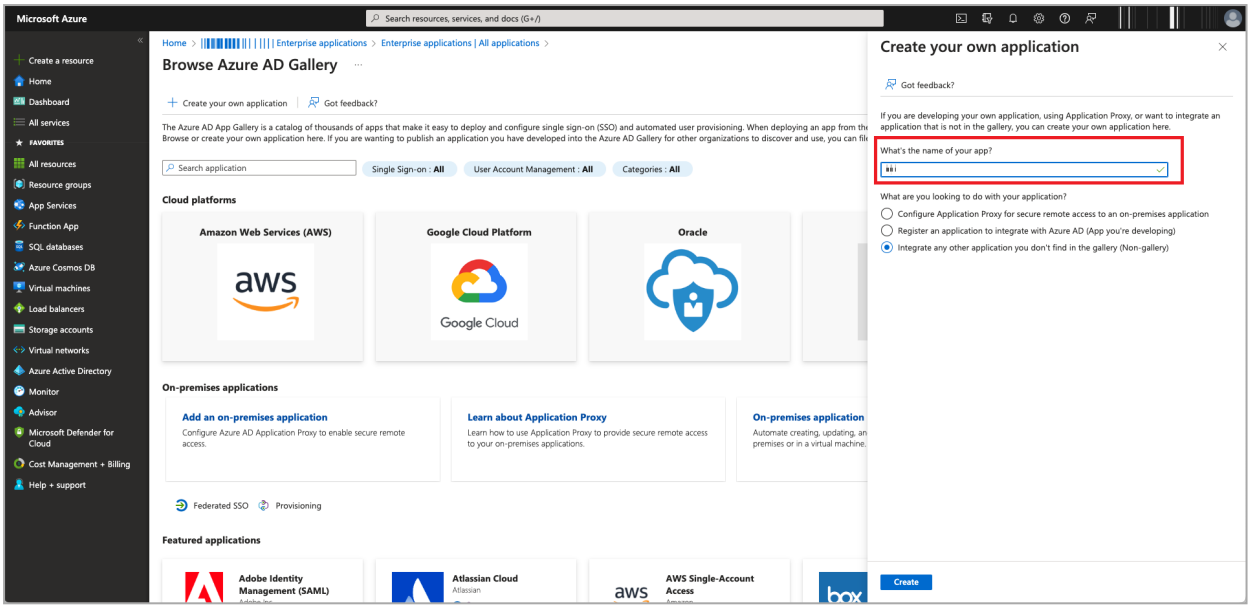
4. Click **New application**.



5. Click **Create your own application**.



6. In the **What's the name of your app** filed, enter a name for your application.



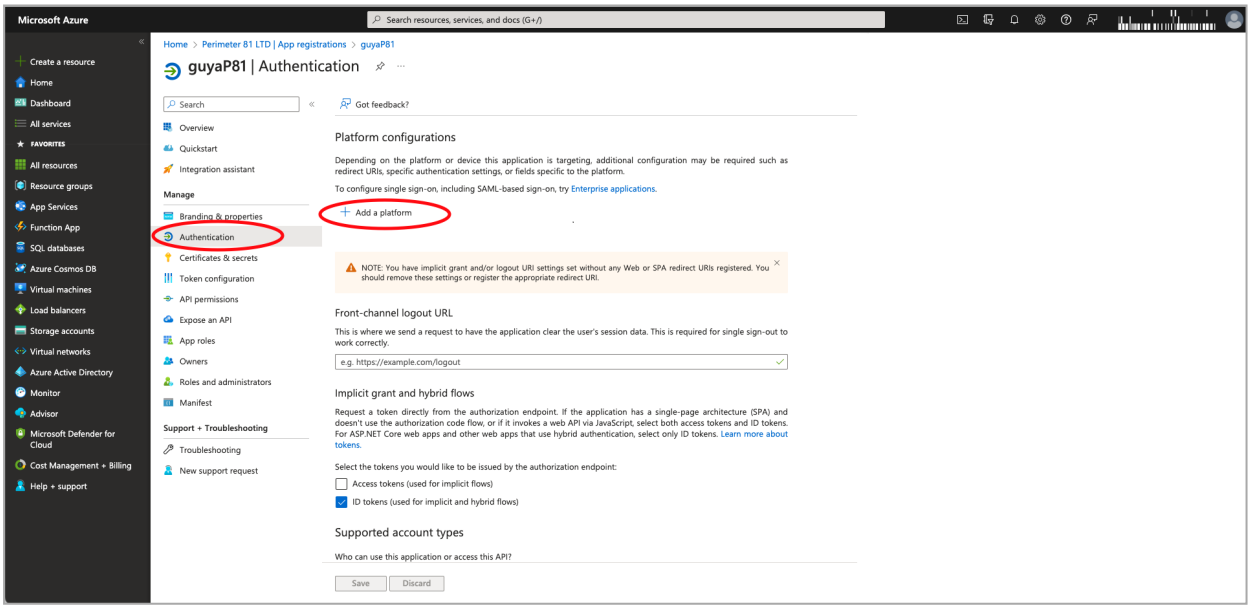
Note - Do not change the default setting.

7. Click **Create**.

   The Microsoft Azure application is created.

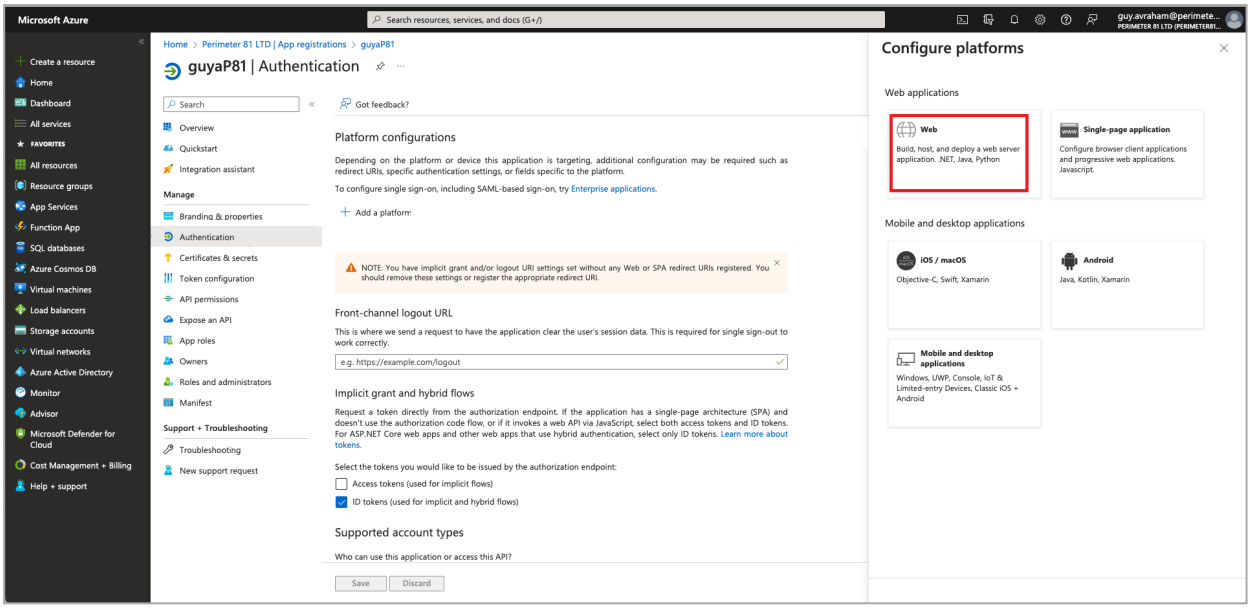
8. Browse to **App registrations**, locate and select your application.

9. Click **Manage** > **Authentication** > **Add a platform**.



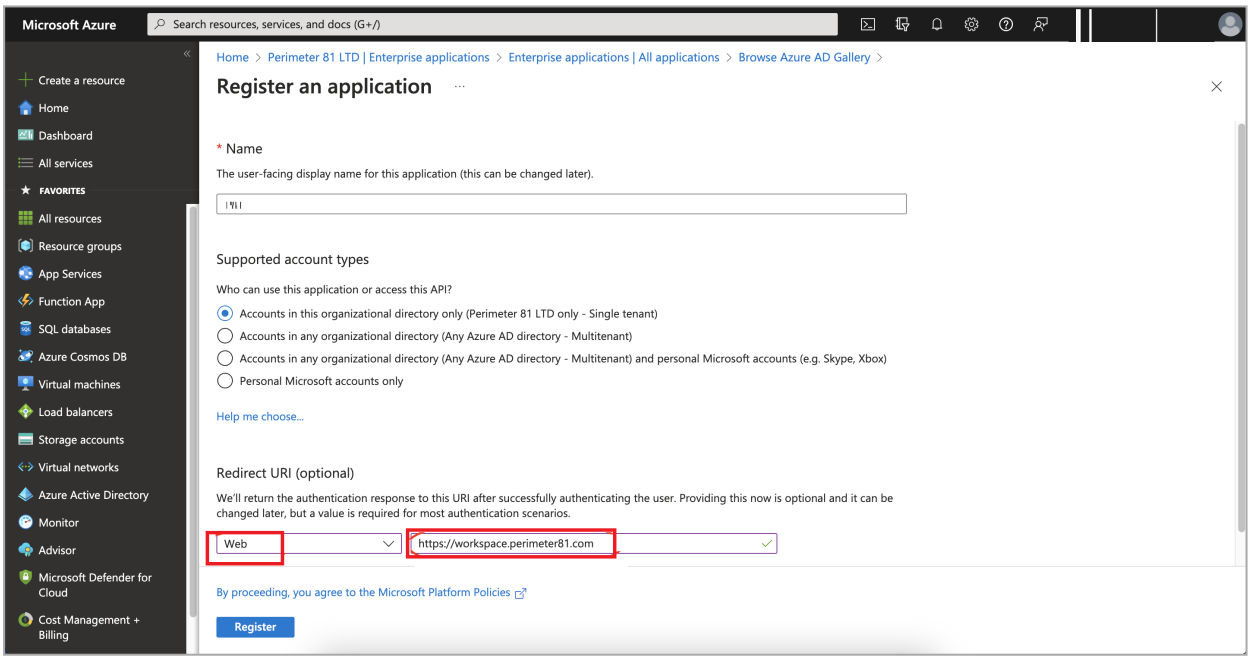
   The **Configure platforms** window appears.

10. Select **Web**.



11. In the **Redirect URI (Optional)** field, select **Web** from the type of application list and enter the relevant URI where the access token is sent to:

    - For US data residency - `https://<workspace>.perimeter81.com`
    - For EU data residency - `https://<workspace>.eu.sase.checkpoint.com`

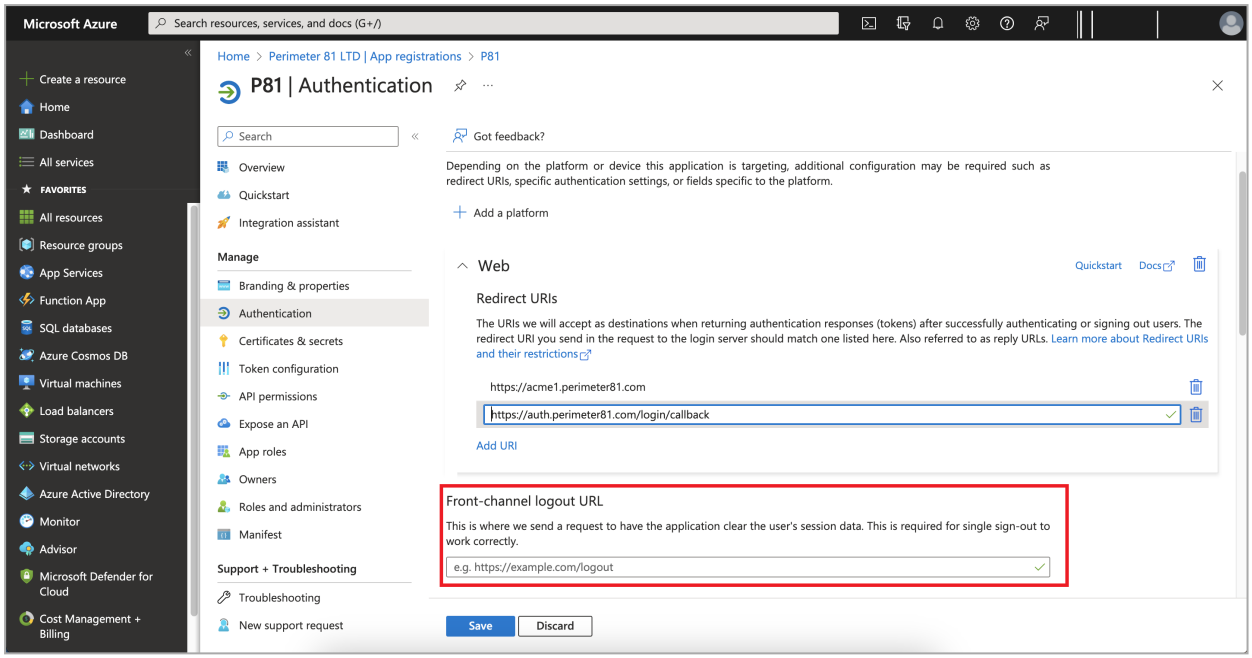


12. Click **Configure**.

13. In the **Redirect URIs** section, enter:

    - For US data residency - `https://auth.perimeter81.com/login/callback`

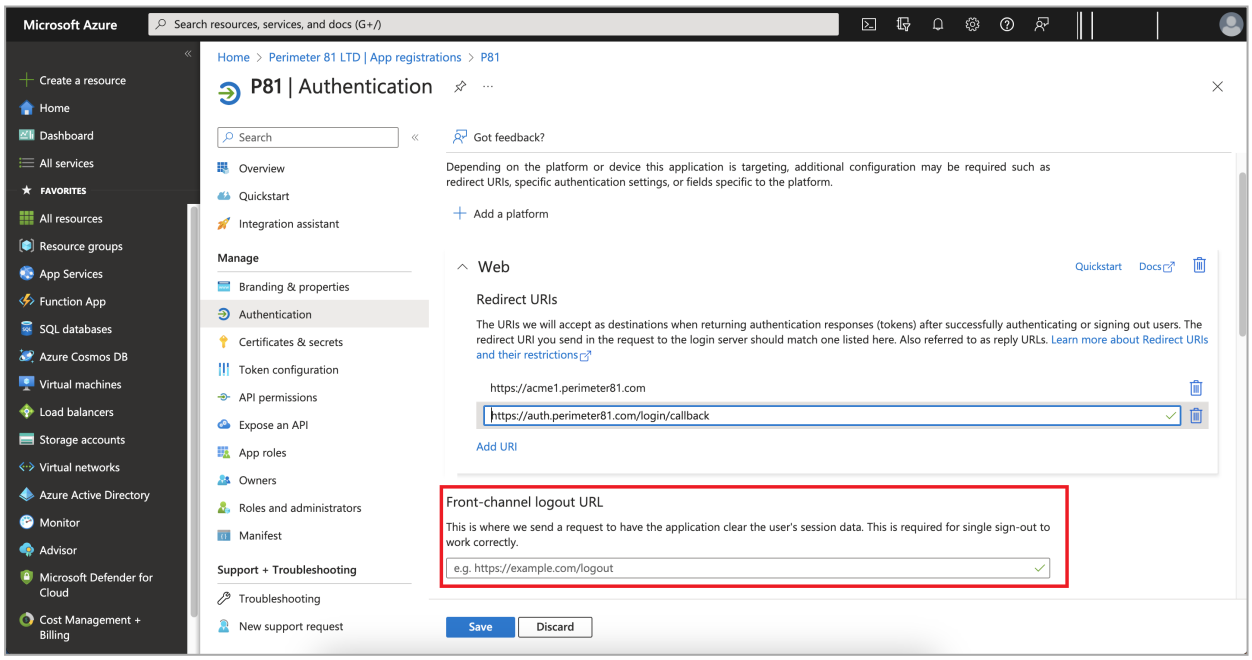
- For EU data residency - `https://auth.eu.sase.checkpoint.com/login/callback`



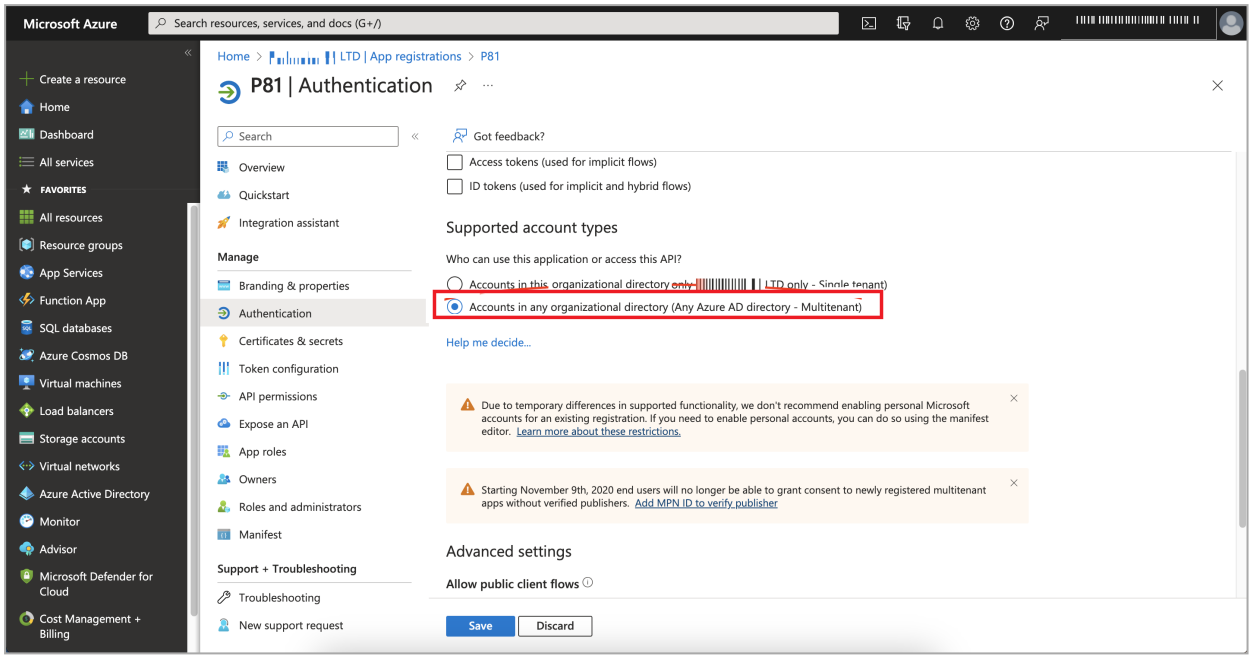
14. In the **Front-channel logout URL** section, enter your workspace name:

    - For US data residency - `https://{{WORKSPACE}}.perimeter81.com`
    - For EU data residency - `https://{{WORKSPACE}}.eu.sase.checkpoint.com`

    where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.



15. To allow access from external organizations, in the **Supported account types** section, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.

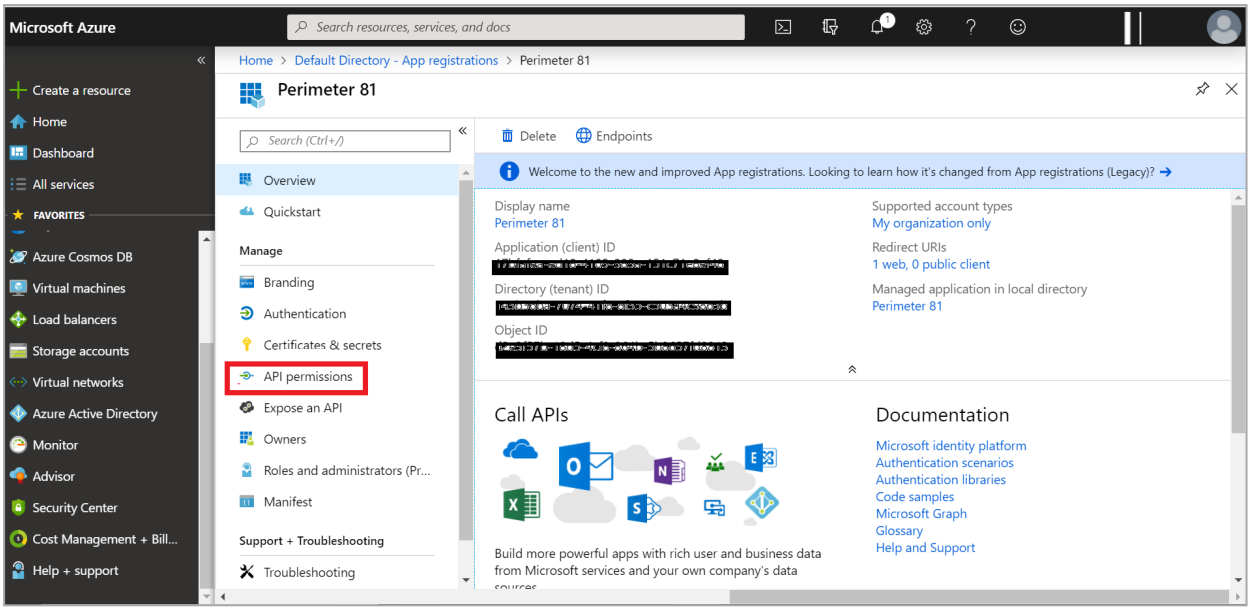


16. Click **Save**.

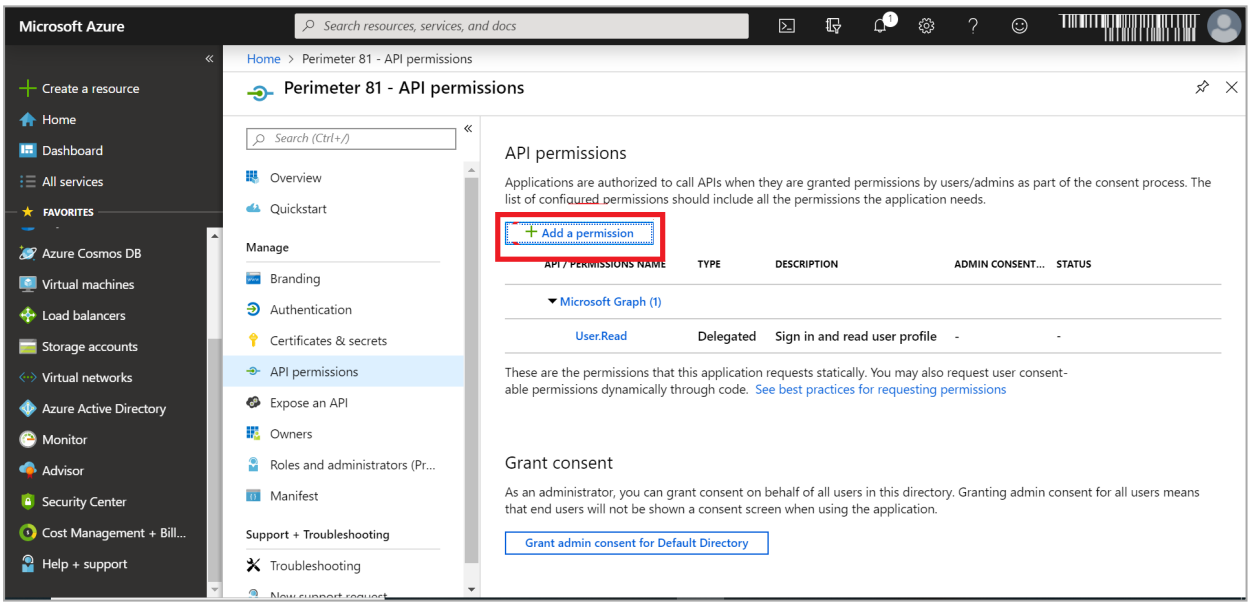
Configuring the Permissions for the Application

To configure the permissions for the application:

1. Log in to your Microsoft Azure Portal.
2. Click **Identity** > **Applications** > **App registrations** > **All applications**.
3. Select your application.
4. Click **Overview** > **Manage** > **API Permissions**.

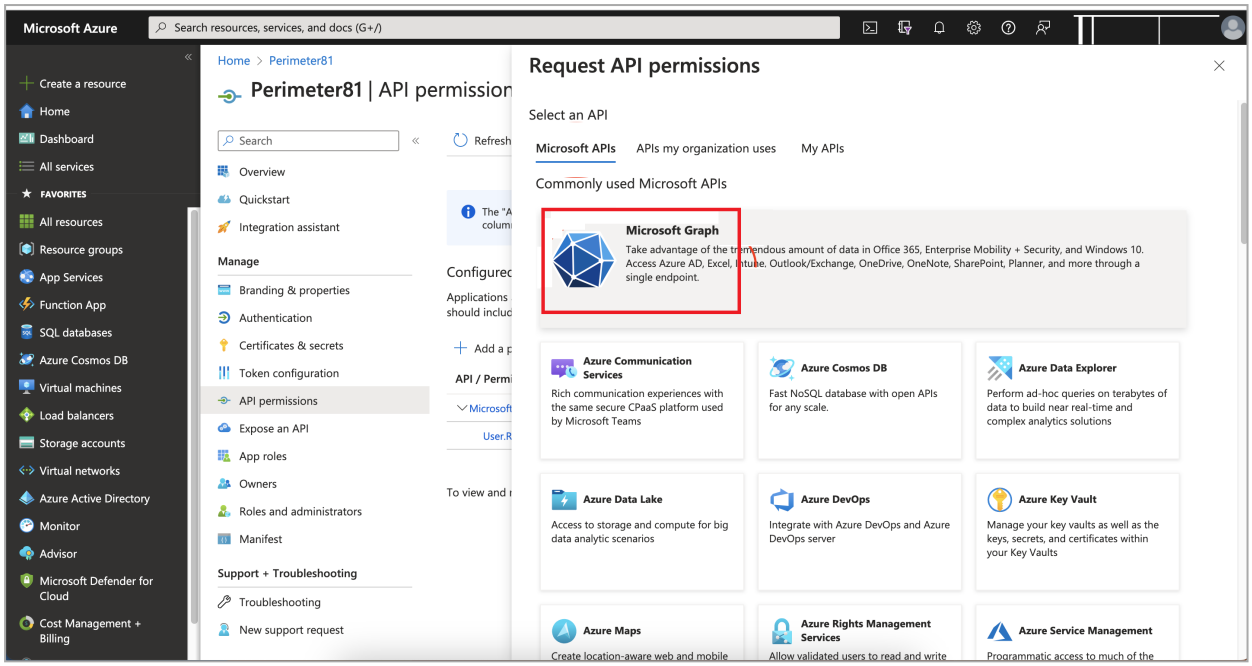


5. Click **Add a permission**.



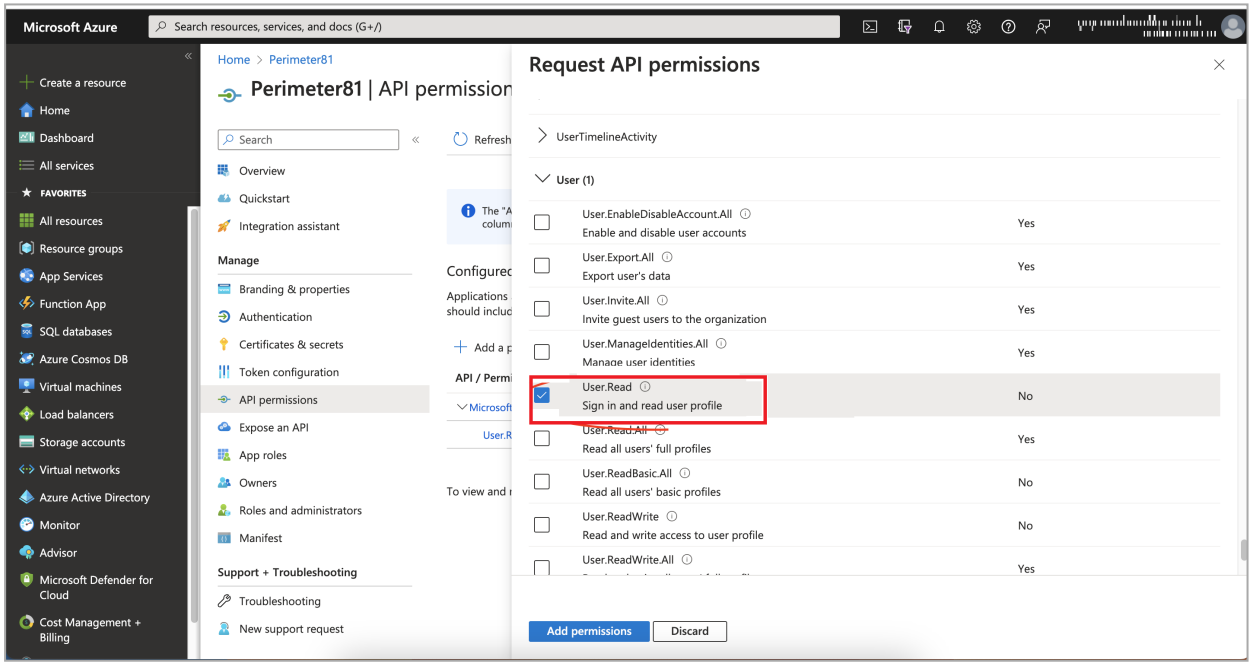
The **Request API permissions** page appears.

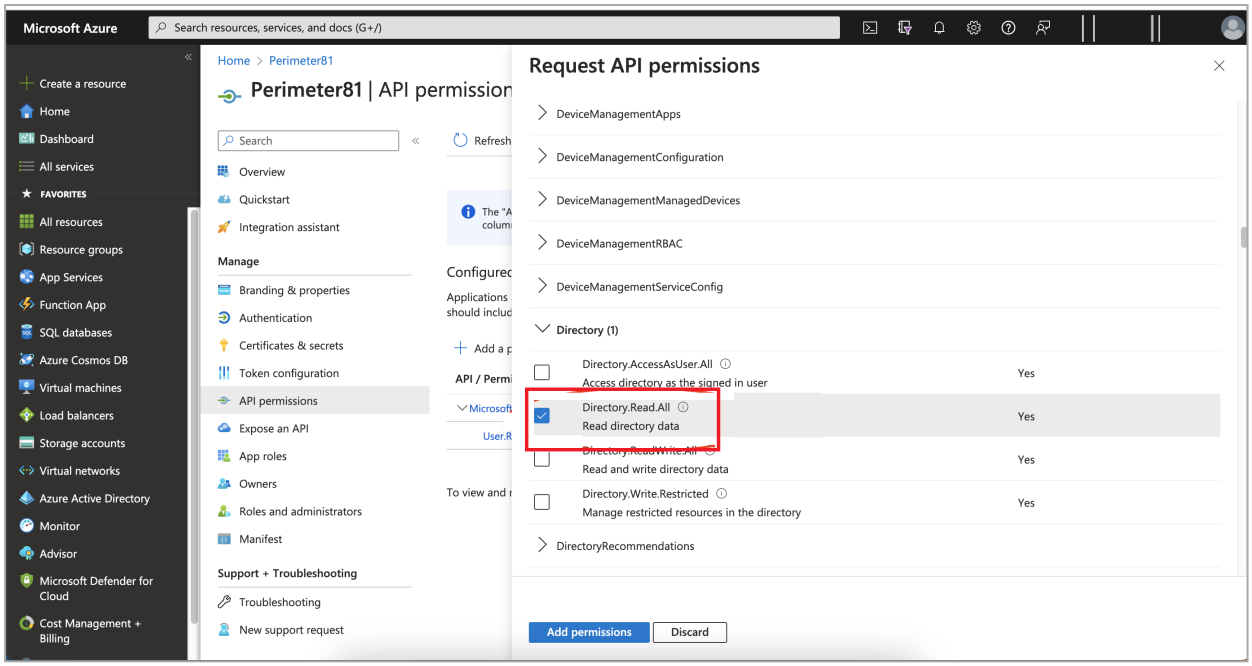
6. Click **Microsoft APIs** and select **Microsoft Graph** from the list of available APIs to change the access level.



7. Click **Delegated permissions**.

8. Select the **User.Read** and **Directory.Read.All** checkbox to modify the permissions so your application can read the directory..



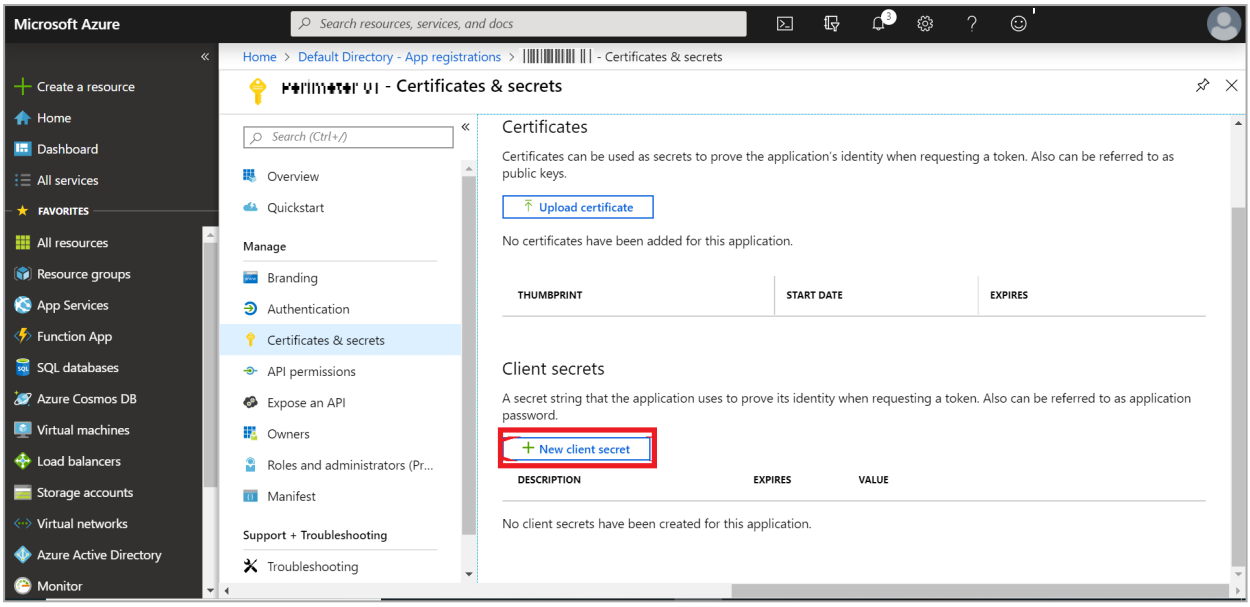


9. Click **Add permissions** > **Configured permissions** > **Grant admin consent** for approval of your app API permissions.
10. Click **Yes**.

    Your application gets the granted permissions.
11. To enable user group support, enable:
    a. **Application Permissions**: Read directory data.
    b. **Delegated permissions**: Access the directory as the signed in user.
12. Click **Save** to save the changes.
13. To remove the Windows Azure Active Directory API permission, see *"Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions" on page 896*.

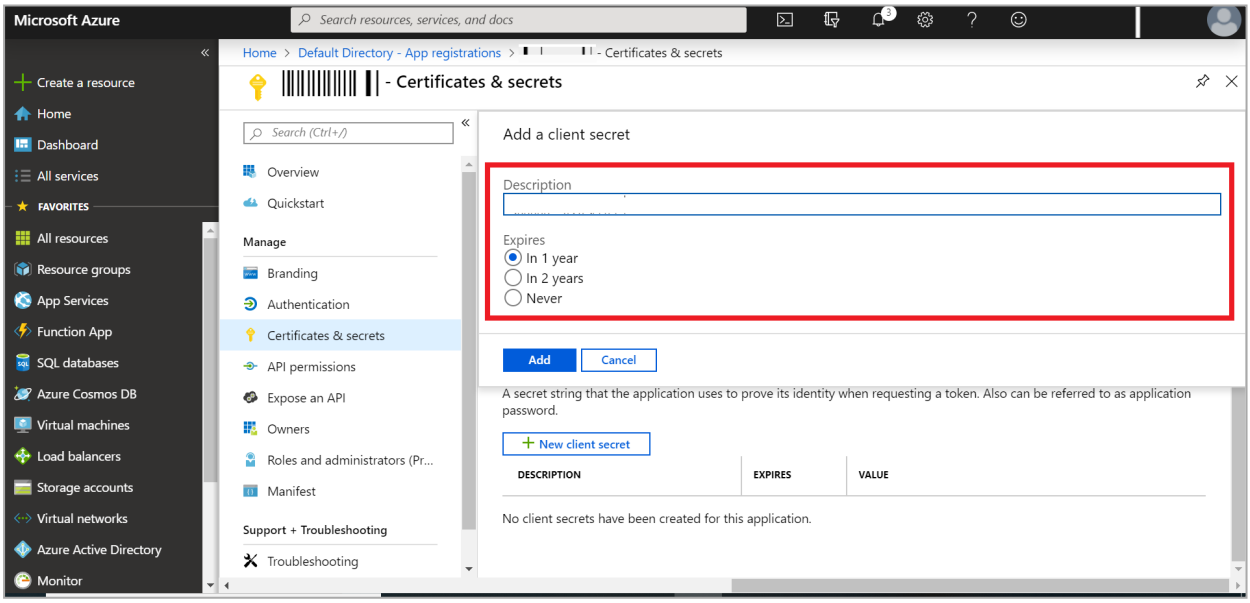
Configuring the Key

1. Log in to your Microsoft Azure Portal.
2. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
3. Browse to **App registrations**, locate and select your application.
4. Go to **Manage** > **Certificates & secrets**.
5. Click **New client secret**.



The **Add a Client secret** window appears.

6. In the **Description** filed, enter a name for the key.
7. In the **Expires** field, select the expiry:
   - **In 1 year**
   - **In 2 years**
   - **Never**



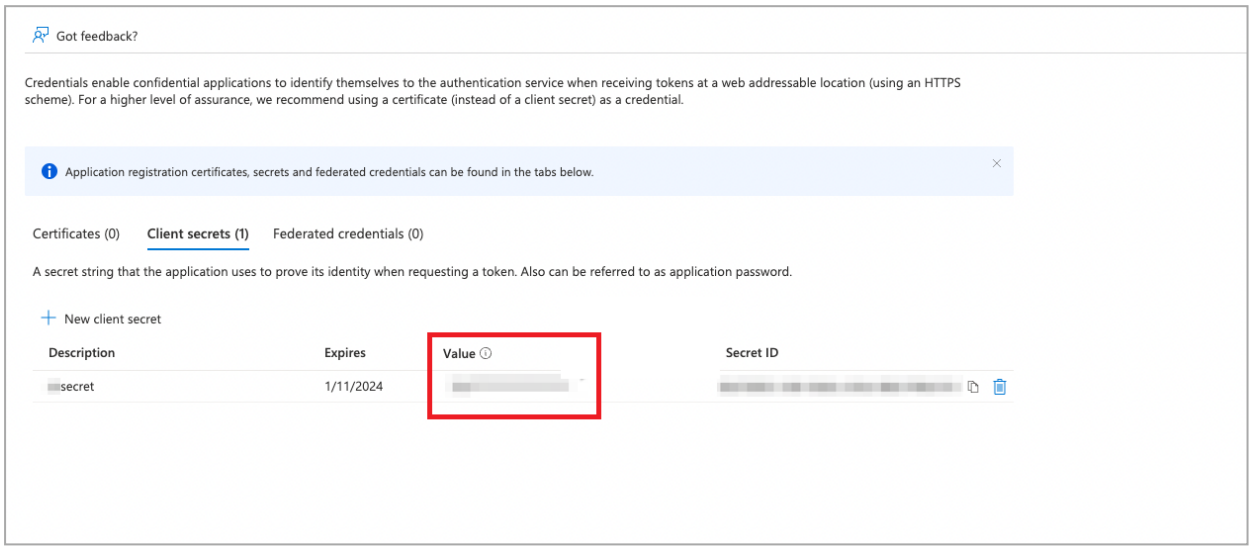
8. Click **Add**.

   The new key is added.

9. To get the secret value of the key, go to the **Client secrets** tab and copy the secret **Value**.

   This value is the **Client Secret** in Harmony SASE Admin console. .

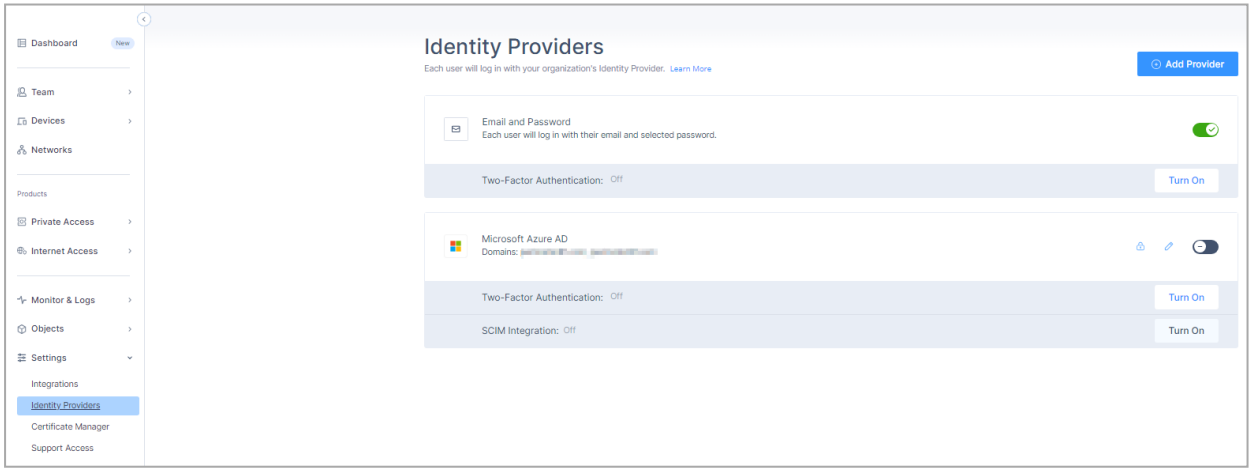
   Note - The Secret value of the key need to be copied before you close the screen. If not, you need to create a new key.



Configuring IDP Connection in Harmony SASE

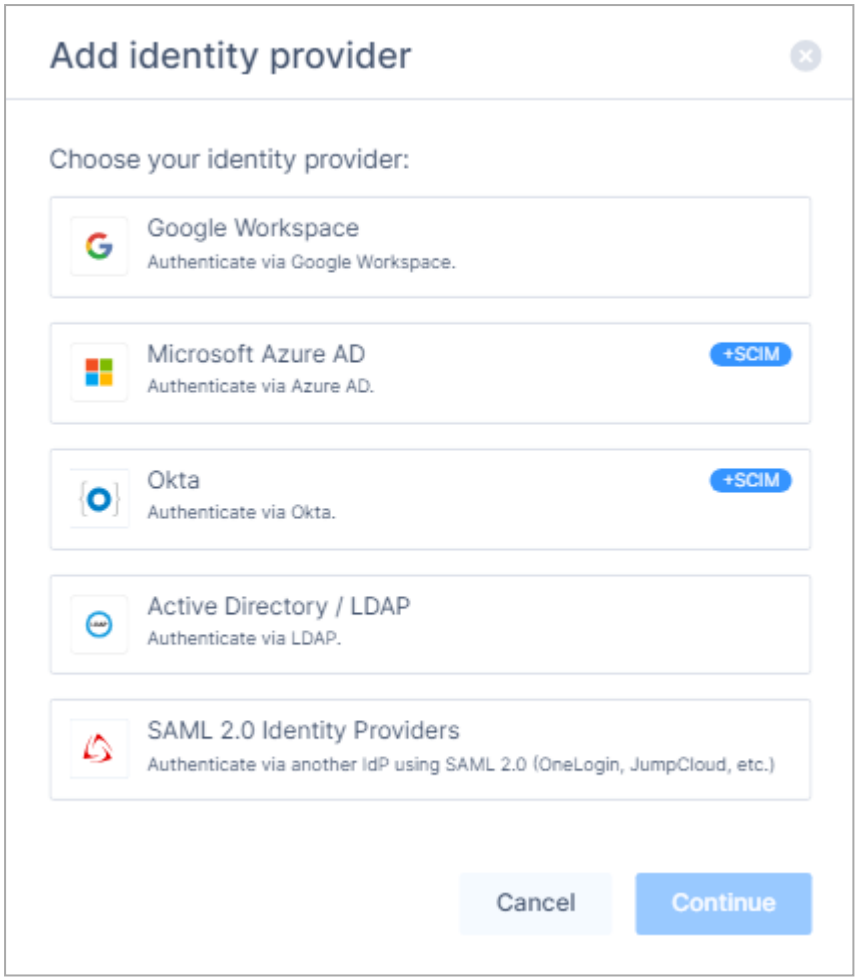
1. Access the Harmony SASE Administrator Portal and click **Settings** > **Identity Providers**.

   The **Identity Providers** page appears.



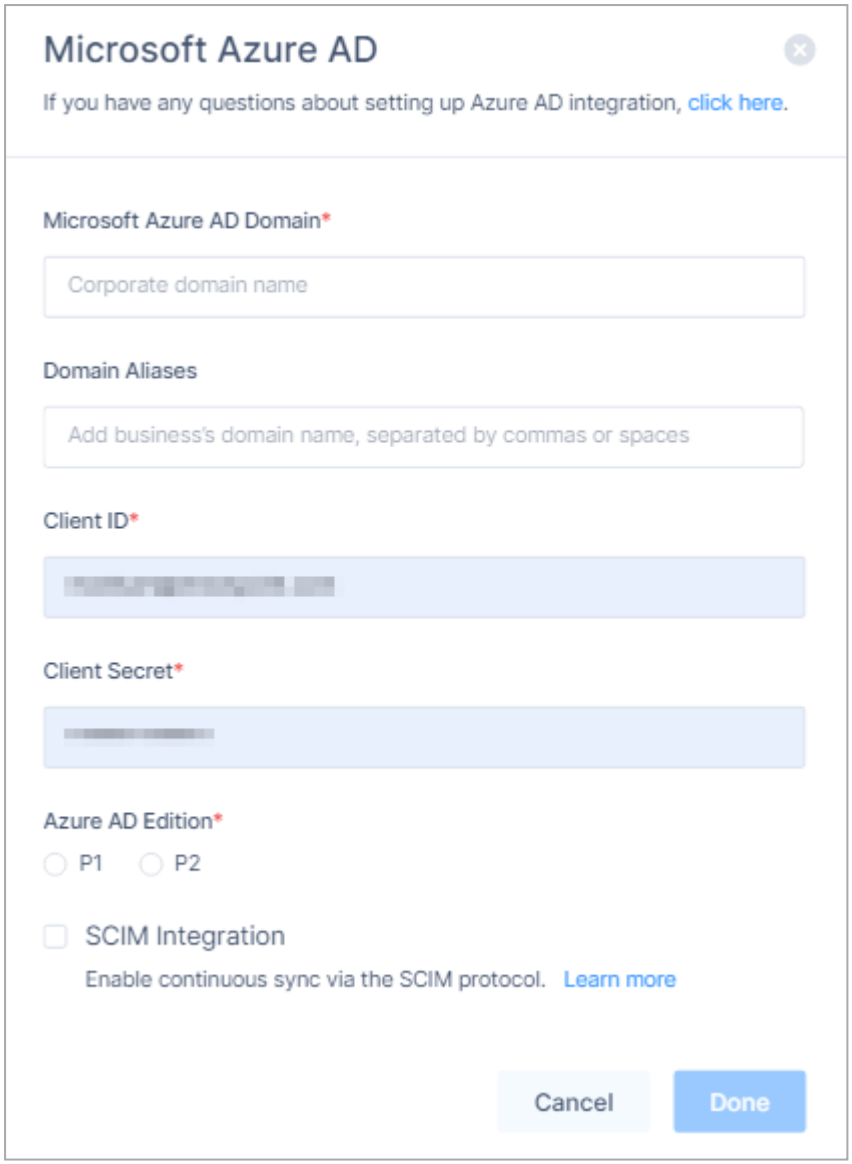
2. Click **Add Provider**.

   The **Add identity provider** window appears.



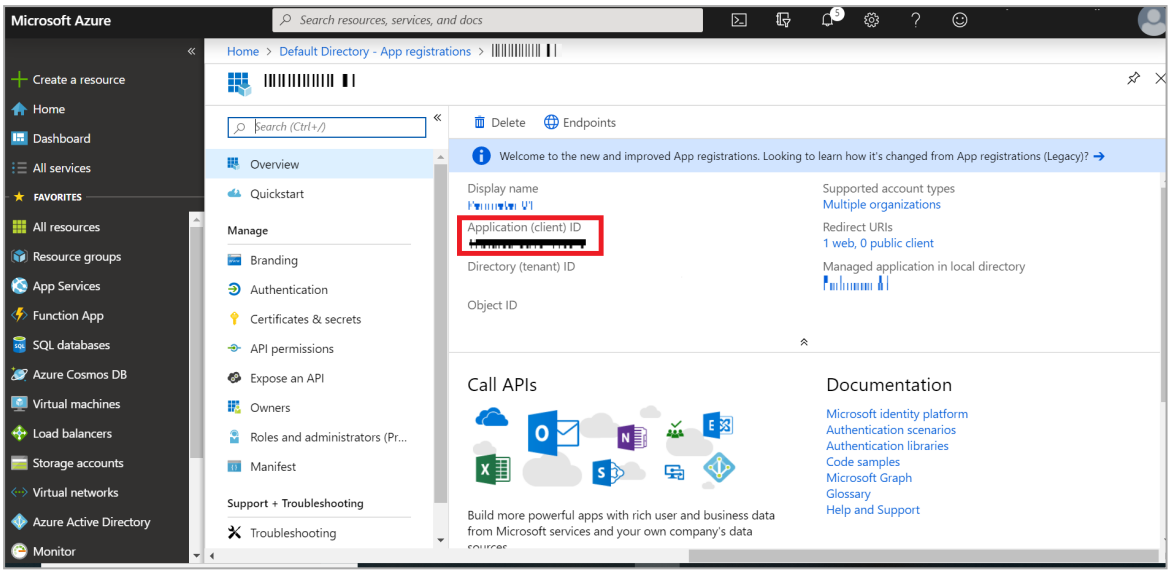
3. Select **Microsoft Azure AD**.
4. Click **Continue**.

   The **Microsoft Azure AD** page appears.



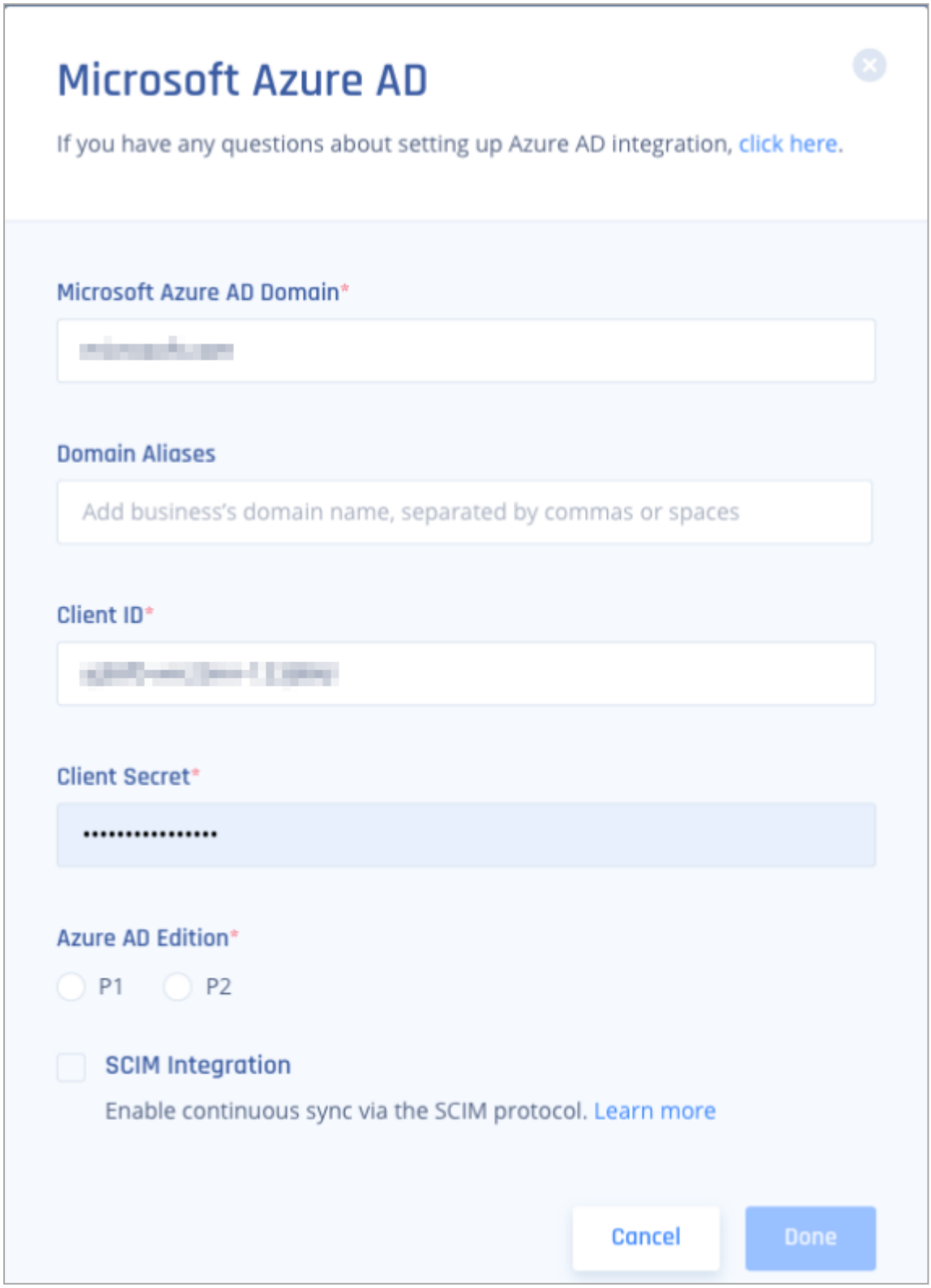
5. In the **Microsoft Azure AD Domain** field, enter the domain name.
6. In the **Domain Aliases** field, enter the email ID(s) separated by commas or spaces.
7. In the **Client ID** field, enter the **Application (client) ID** in Microsoft Azure AD:
   a. Log in to your Microsoft Azure Portal.
   b. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
   c. Browse to **App registrations**, locate and select your application.

d. Go to **Overview** > **Application (client) ID**.



e. Copy the **Application (cient) ID** value.

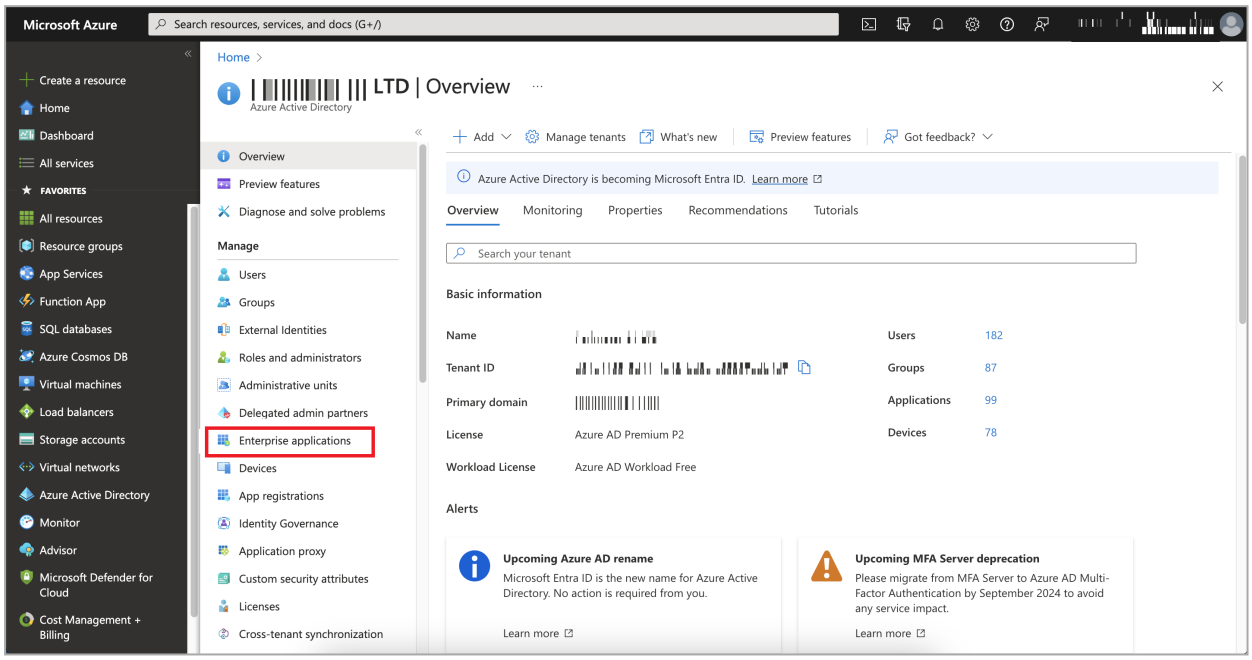
8. In the **Client Secret** field, enter the secret value. See step 9 in Configuring the Key.



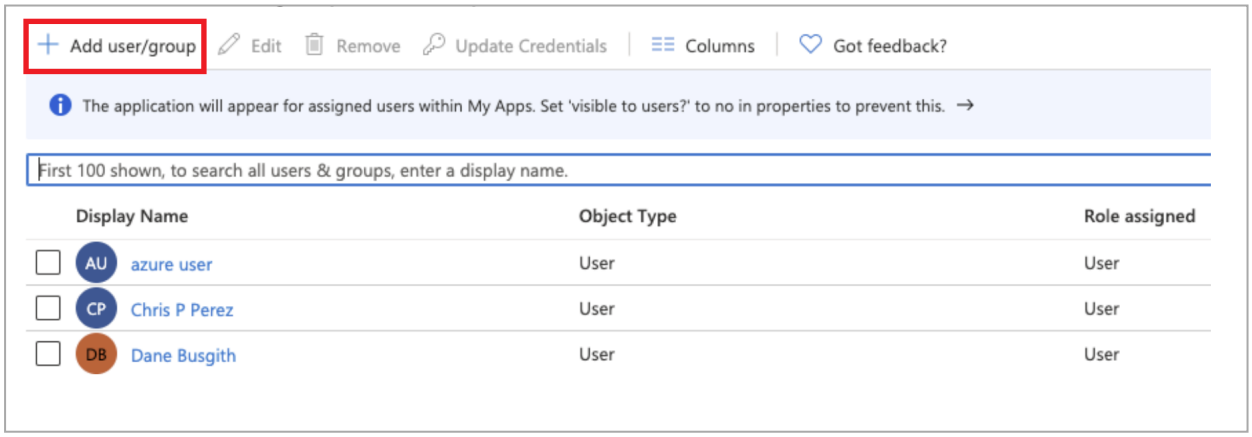
9. In the **Azure AD Edition**, select either:
   a. **PI**
   b. **P2**
10. Click **Done**.

Assigning Users and Groups in Microsoft Azure

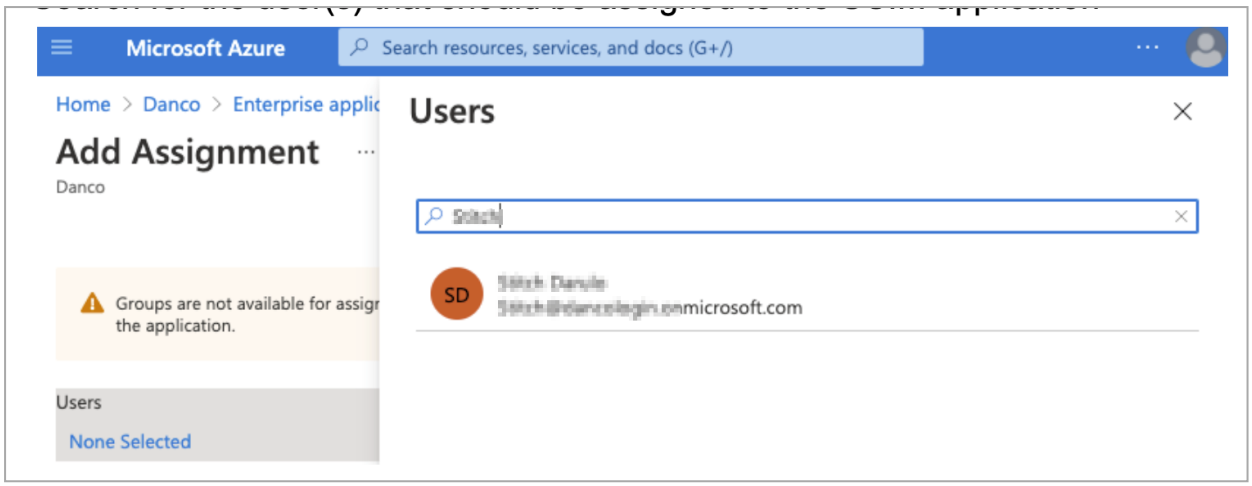
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.
3. Go to **Manage** > **Enterprise applications**.



4. Search and select your application.
5. Go to **Users and groups** and click **Add user/group**.



6. Click **None Selected** in **Users**.



7. Search and select the user(s) or group(s) you want to add to the application.

   Note - Special characters are not supported in groups.

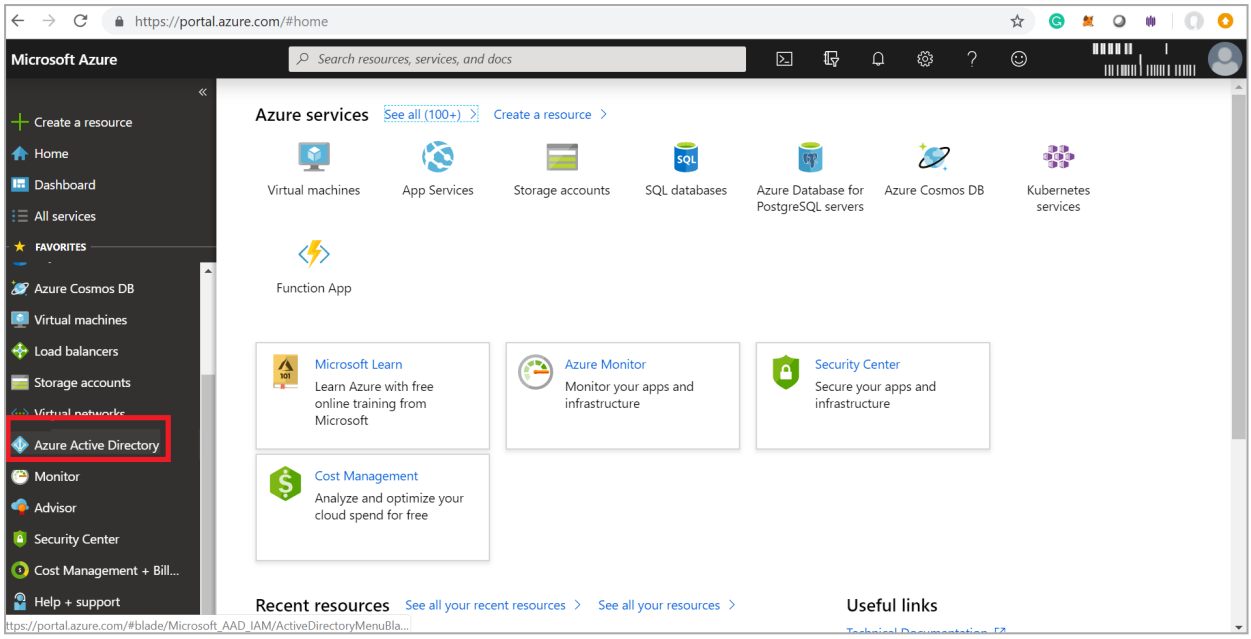
8. Click **Select**.
9. Click **Assign**.

Microsoft Entra ID (formerly Azure AD) (App Registration)

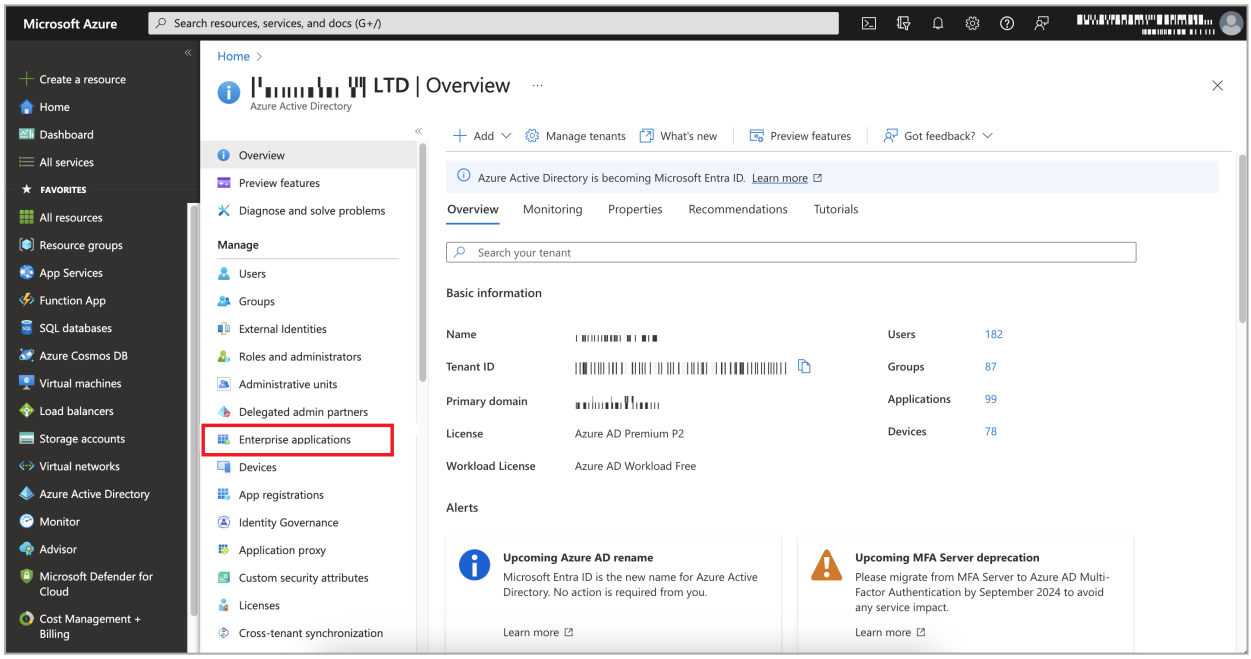
You can enable users to log in using a Microsoft Entra ID (formerly Azure AD) account, either from your computer or from the external directory.

Registering Application through the Microsoft Azure Portal

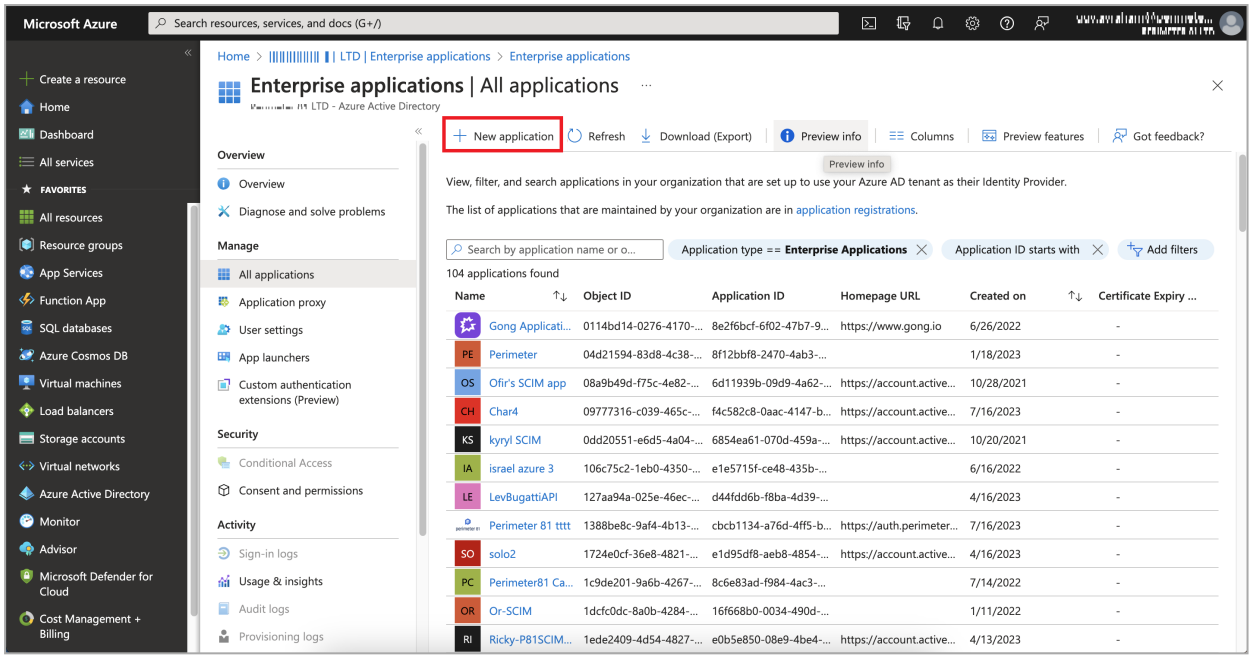
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.



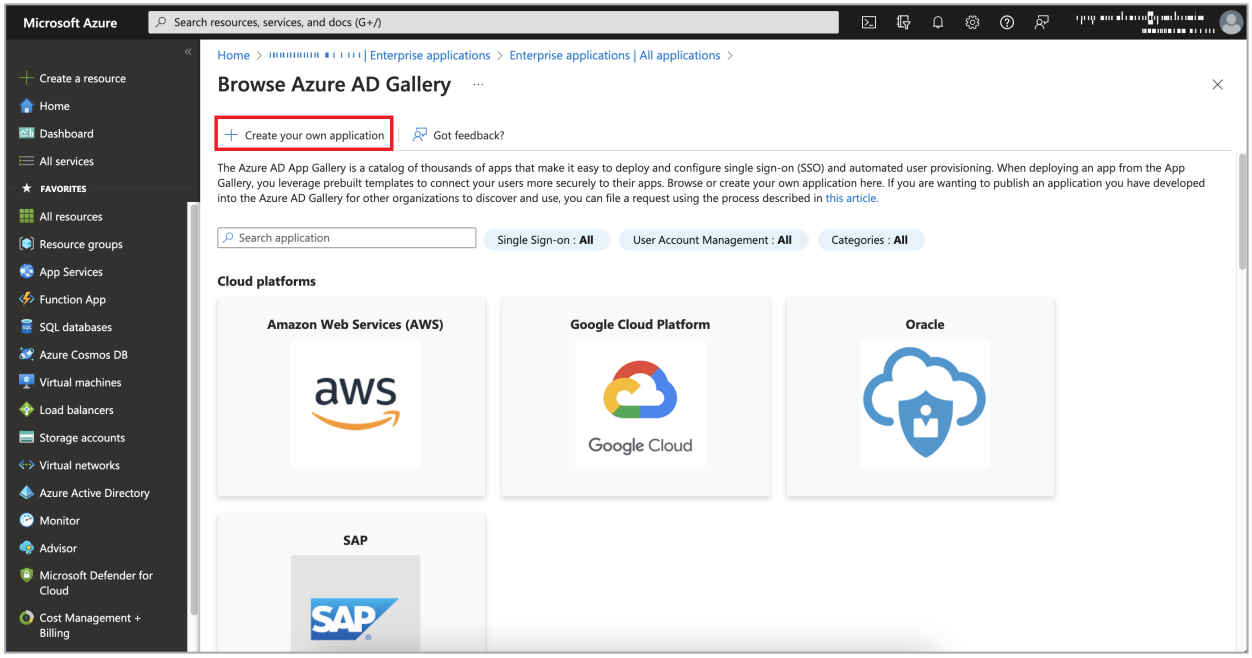
3. Go to **Manage** > **Enterprise applications**.



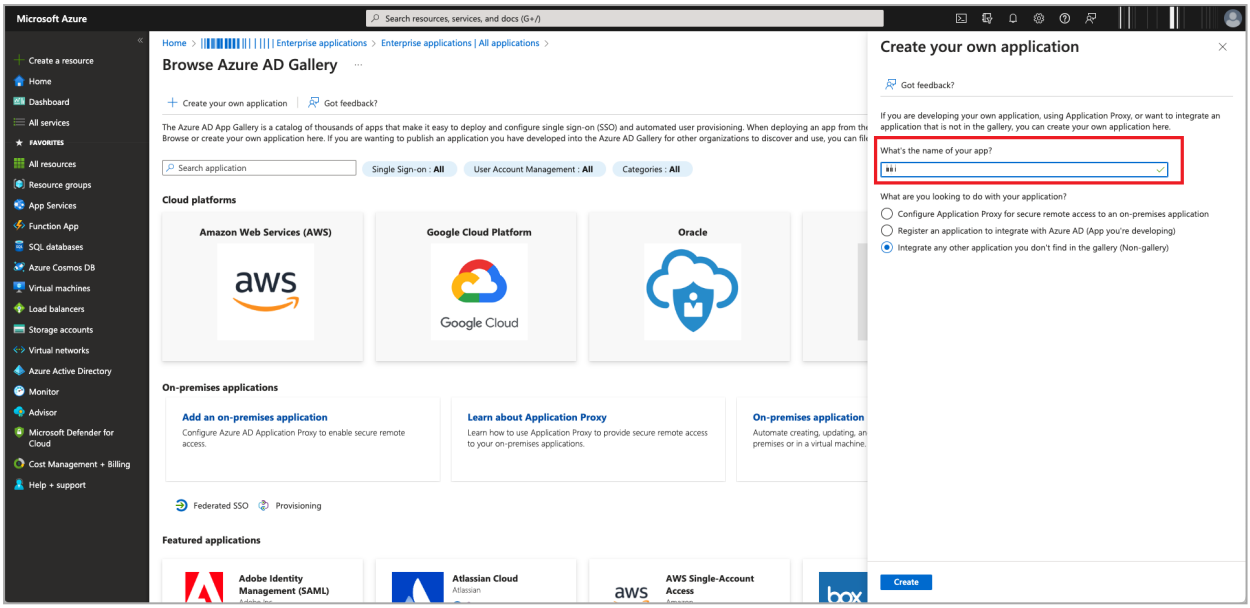
4. Click **New application**.



5. Click **Create your own application**.



6. In the **What's the name of your app** filed, enter a name for your application.



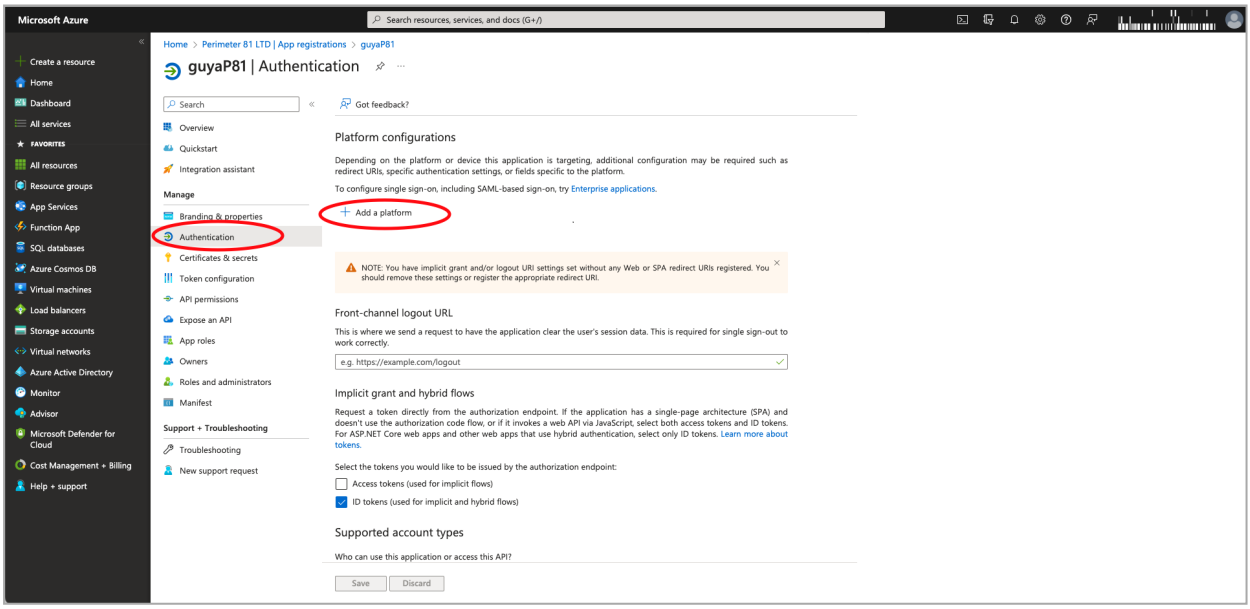
Note - Do not change the default setting.

7. Click **Create**.

   The Microsoft Azure application is created.

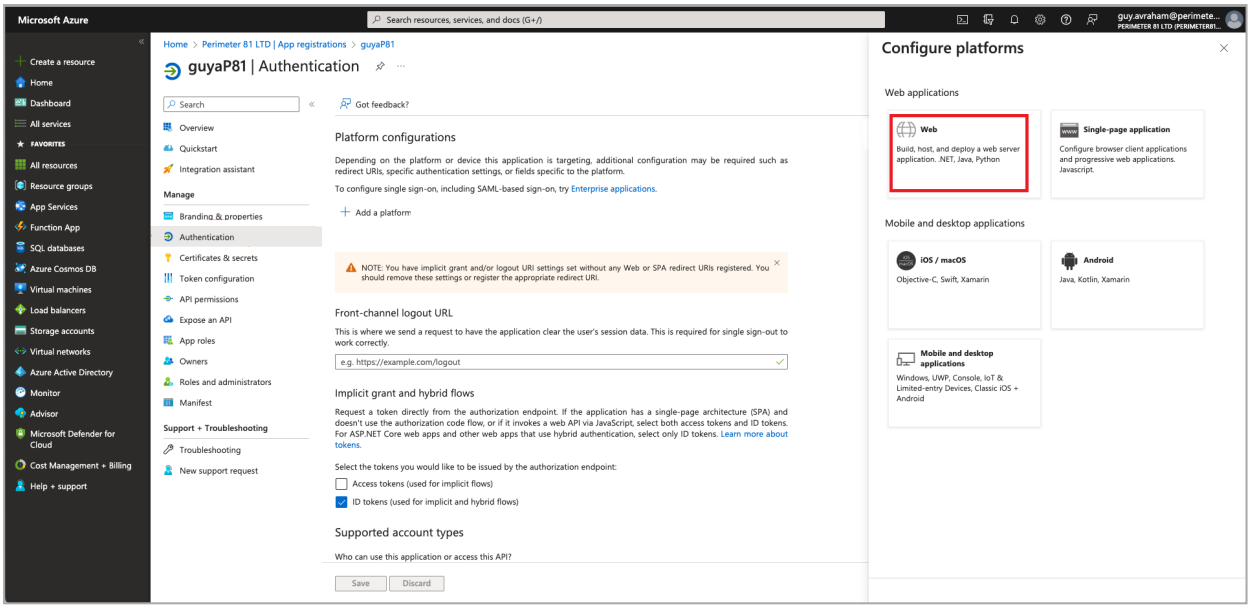
8. Browse to **App registrations**, locate and select your application.

9. Click **Manage** > **Authentication** > **Add a platform**.



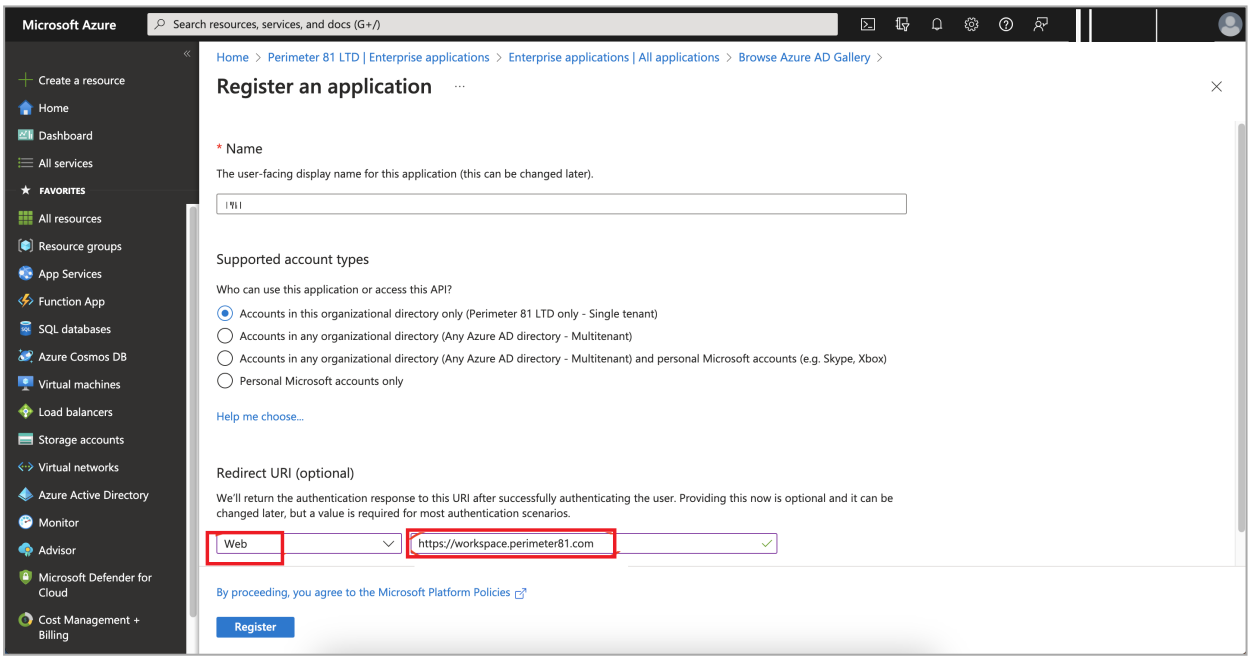
   The **Configure platforms** window appears.

10. Select **Web**.



11. In the **Redirect URI (Optional)** field, select **Web** from the type of application list and enter the relevant URI where the access token is sent to:

    - For US data residency - `https://<workspace>.perimeter81.com`
    - For EU data residency - `https://<workspace>.eu.sase.checkpoint.com`

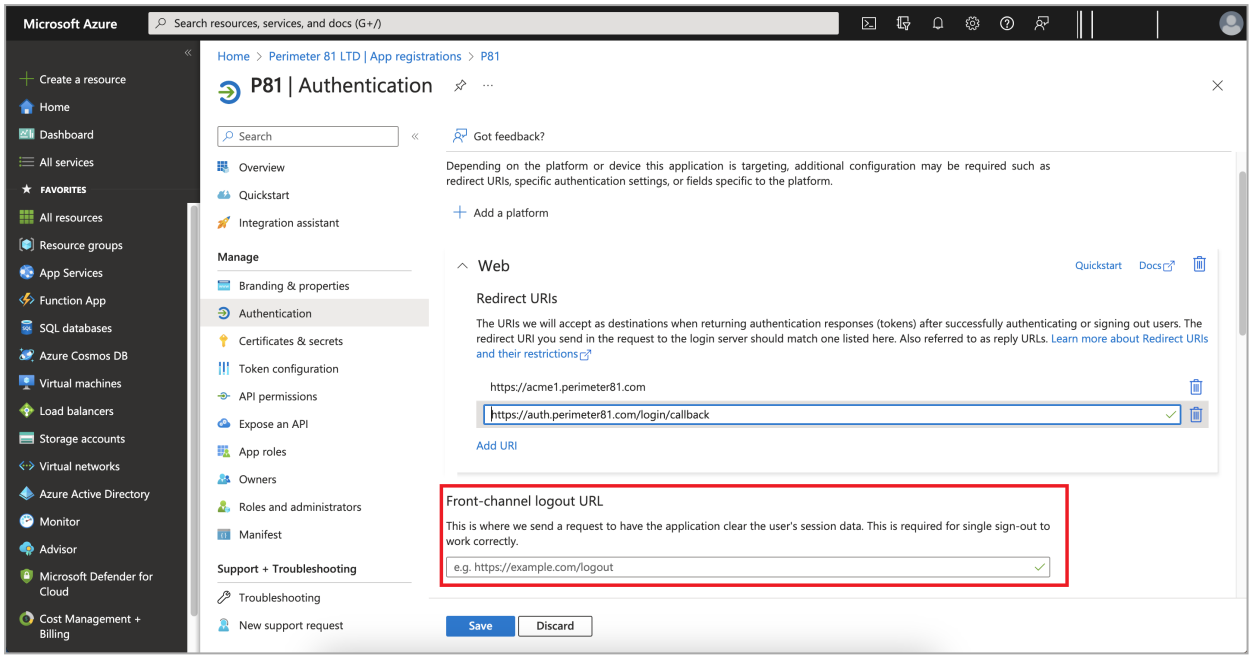


12. Click **Configure**.

13. In the **Redirect URIs** section, enter:

    - For US data residency - `https://auth.perimeter81.com/login/callback`

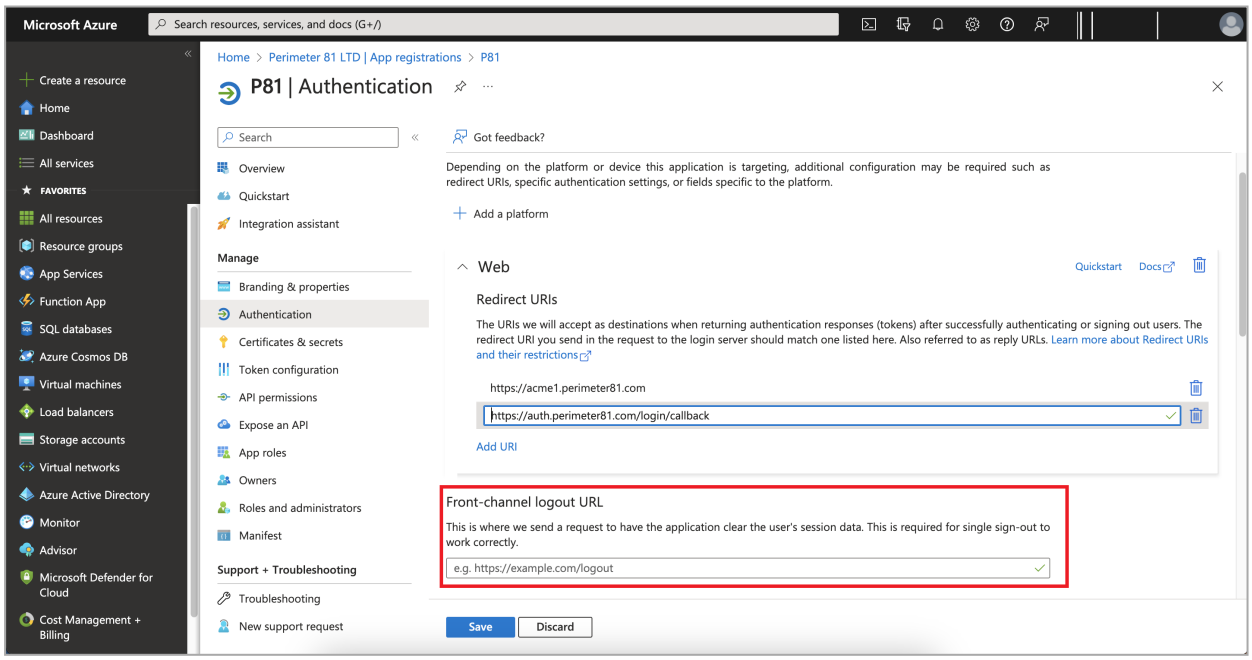
- For EU data residency - `https://auth.eu.sase.checkpoint.com/login/callback`



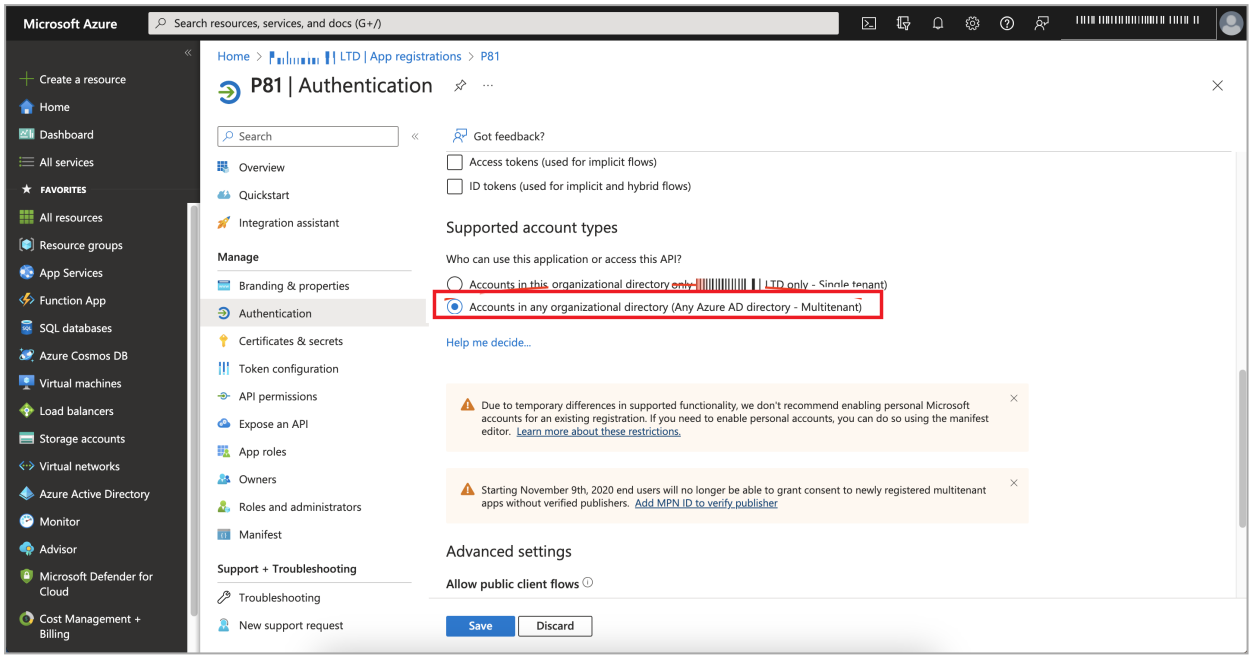
14. In the **Front-channel logout URL** section, enter your workspace name:

    - For US data residency - `https://{{WORKSPACE}}.perimeter81.com`
    - For EU data residency - `https://{{WORKSPACE}}.eu.sase.checkpoint.com`

    where `{{WORKSPACE}}` refers to your Harmony SASE workspace name.



15. To allow access from external organizations, in the **Supported account types** section, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.

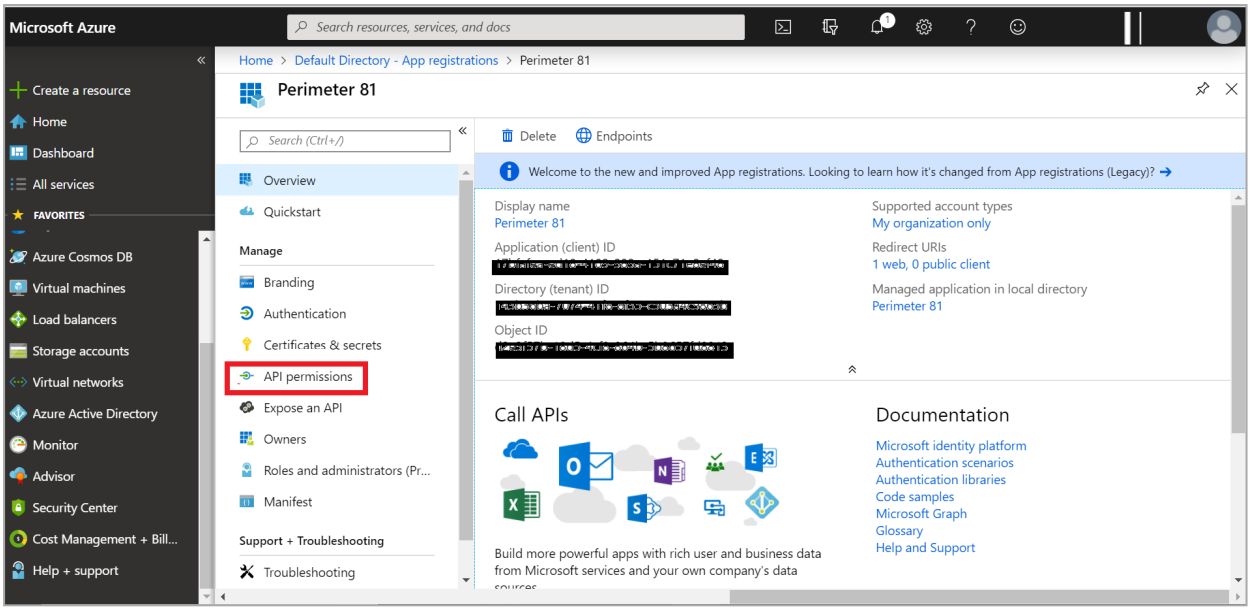


16. Click **Save**.

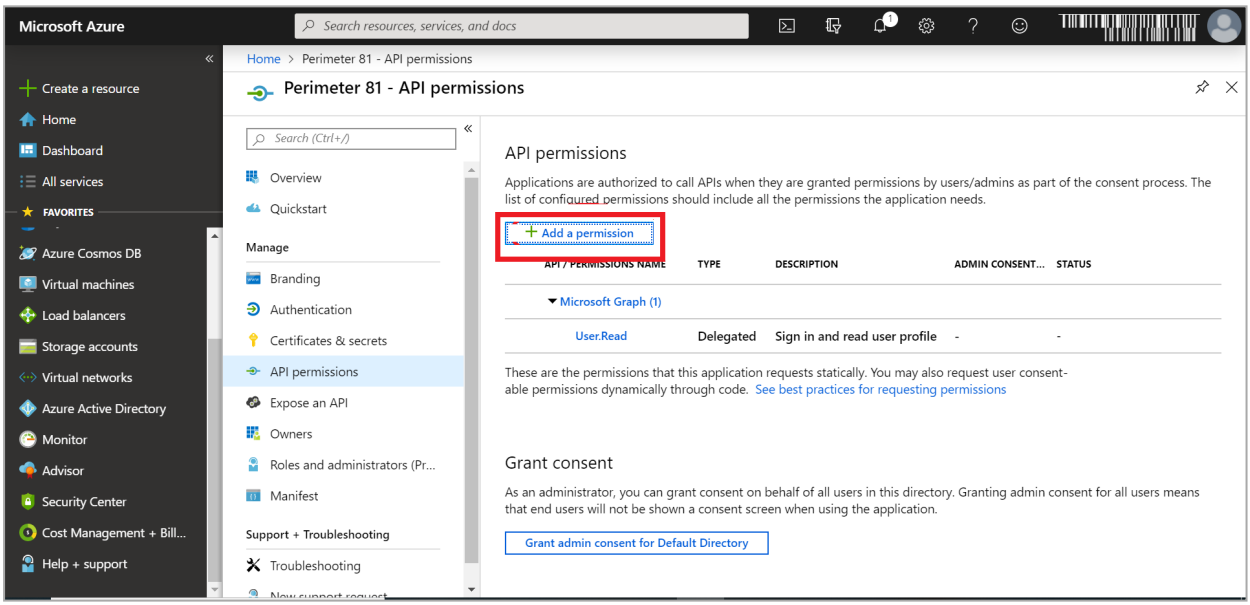
Configuring the Permissions for the Application

To configure the permissions for the application:

1. Log in to your Microsoft Azure Portal.
2. Click **Identity** > **Applications** > **App registrations** > **All applications**.
3. Select your application.
4. Click **Overview** > **Manage** > **API Permissions**.

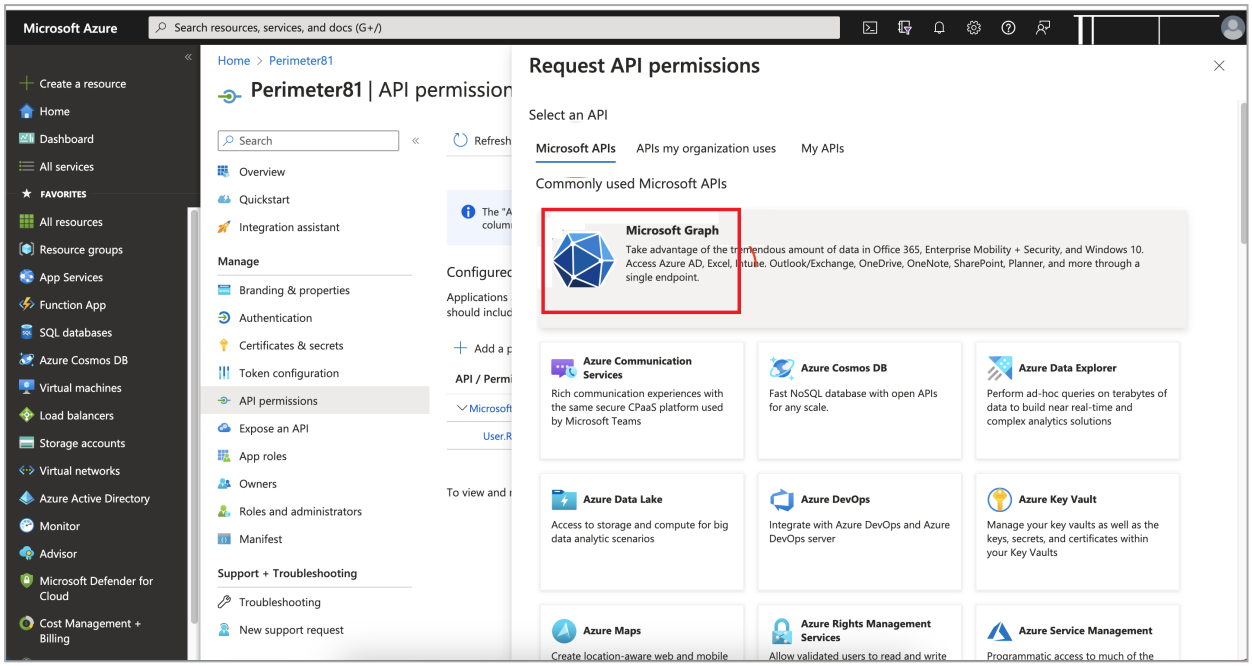


5. Click **Add a permission**.



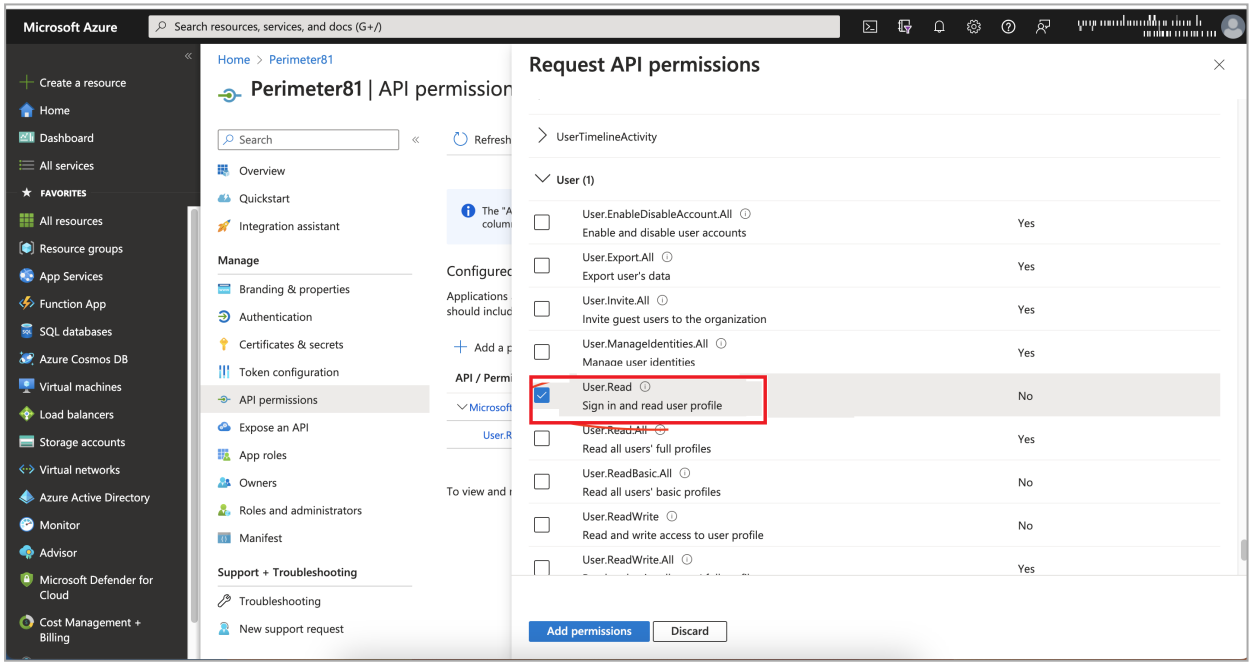
The **Request API permissions** page appears.

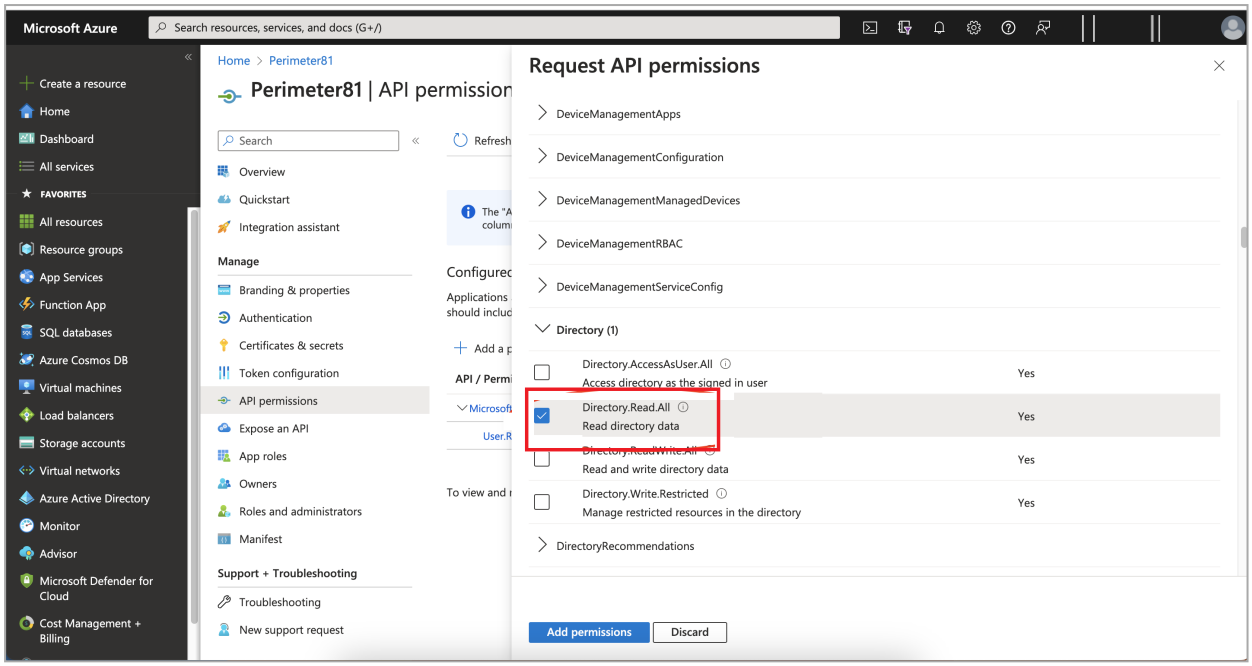
6. Click **Microsoft APIs** and select **Microsoft Graph** from the list of available APIs to change the access level.



7. Click **Delegated permissions**.

8. Select the **User.Read** and **Directory.Read.All** checkbox to modify the permissions so your application can read the directory..



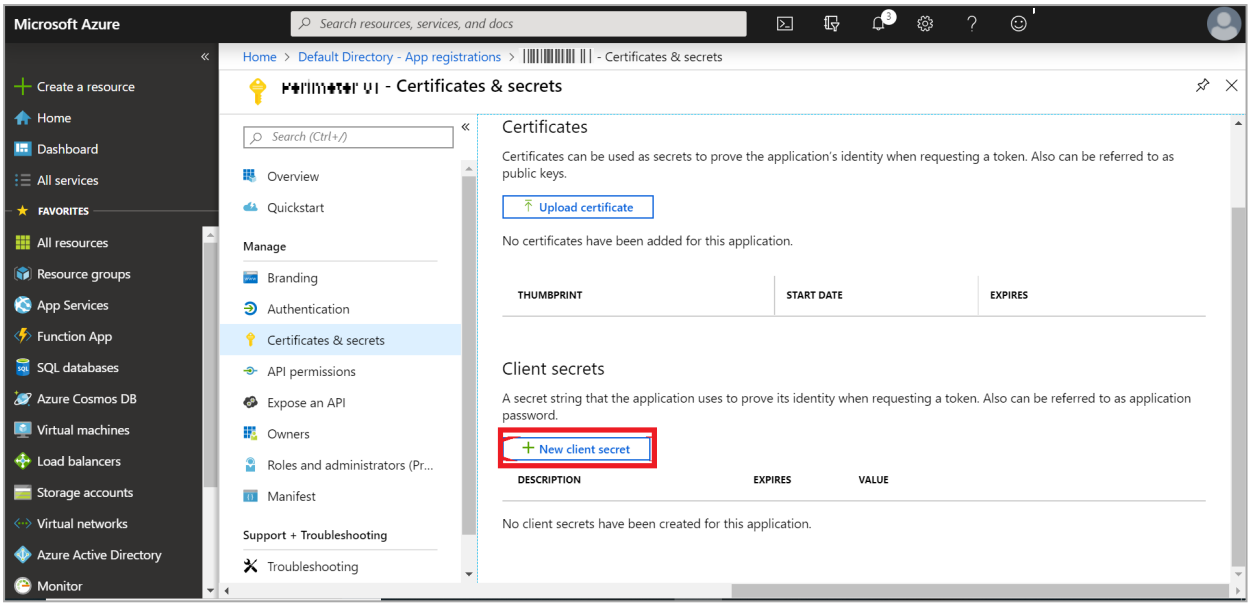


9. Click **Add permissions** > **Configured permissions** > **Grant admin consent** for approval of your app API permissions.
10. Click **Yes**.

    Your application gets the granted permissions.
11. To enable user group support, enable:
    a. **Application Permissions**: Read directory data.
    b. **Delegated permissions**: Access the directory as the signed in user.
12. Click **Save** to save the changes.
13. To remove the Windows Azure Active Directory API permission, see *"Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions" on page 896*.

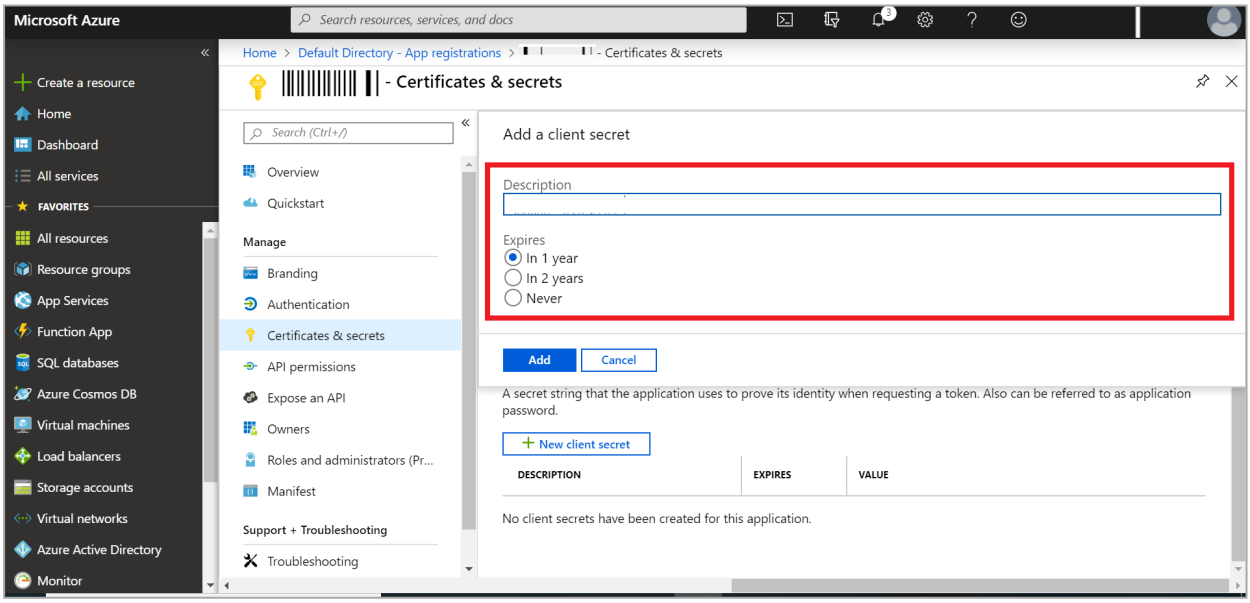
Configuring the Key

1. Log in to your Microsoft Azure Portal.
2. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
3. Browse to **App registrations**, locate and select your application.
4. Go to **Manage** > **Certificates & secrets**.
5. Click **New client secret**.



The **Add a Client secret** window appears.

6. In the **Description** filed, enter a name for the key.
7. In the **Expires** field, select the expiry:
   - **In 1 year**
   - **In 2 years**
   - **Never**



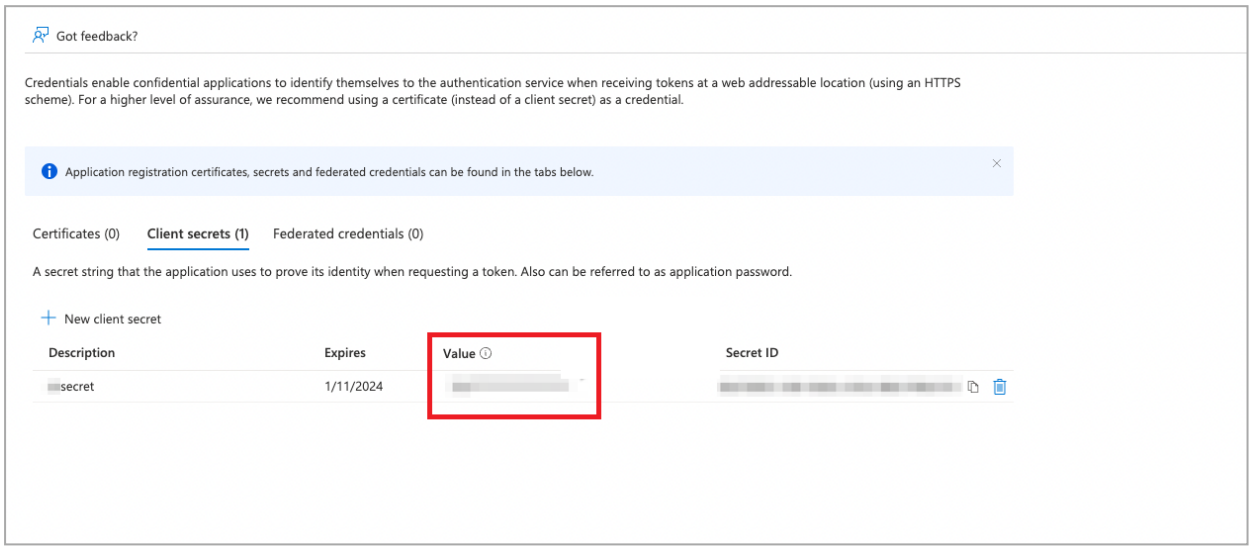
8. Click **Add**.

   The new key is added.

9. To get the secret value of the key, go to the **Client secrets** tab and copy the secret **Value**.

   This value is the **Client Secret** in Harmony SASE Admin console. .

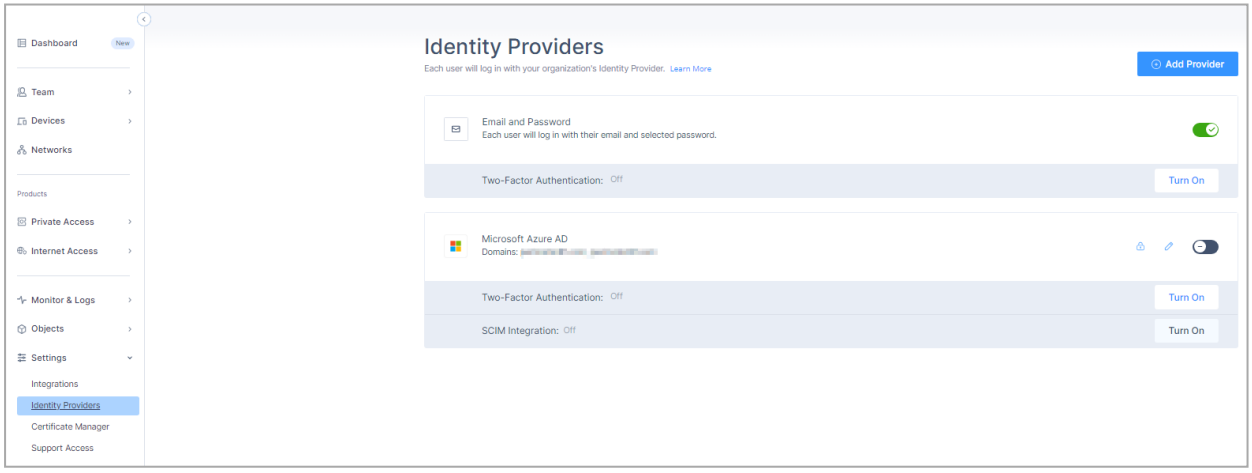
   Note - The Secret value of the key need to be copied before you close the screen. If not, you need to create a new key.



Configuring IDP Connection in Harmony SASE

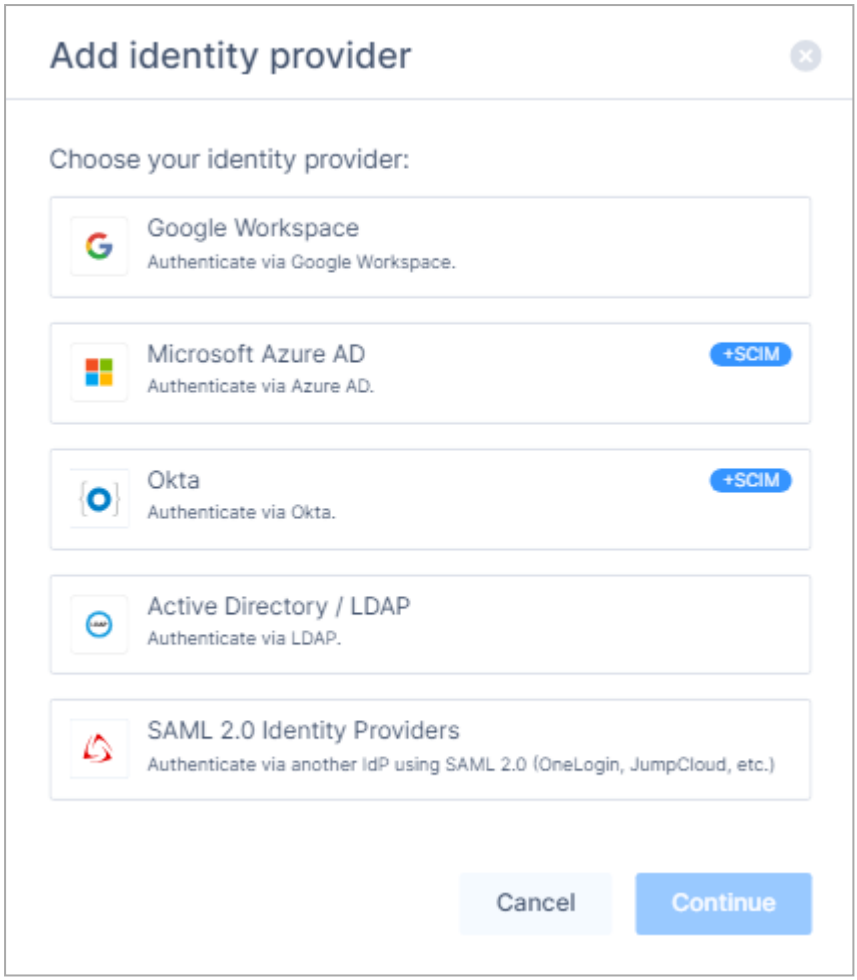
1. Access the Harmony SASE Administrator Portal and click **Settings** > **Identity Providers**.

   The **Identity Providers** page appears.



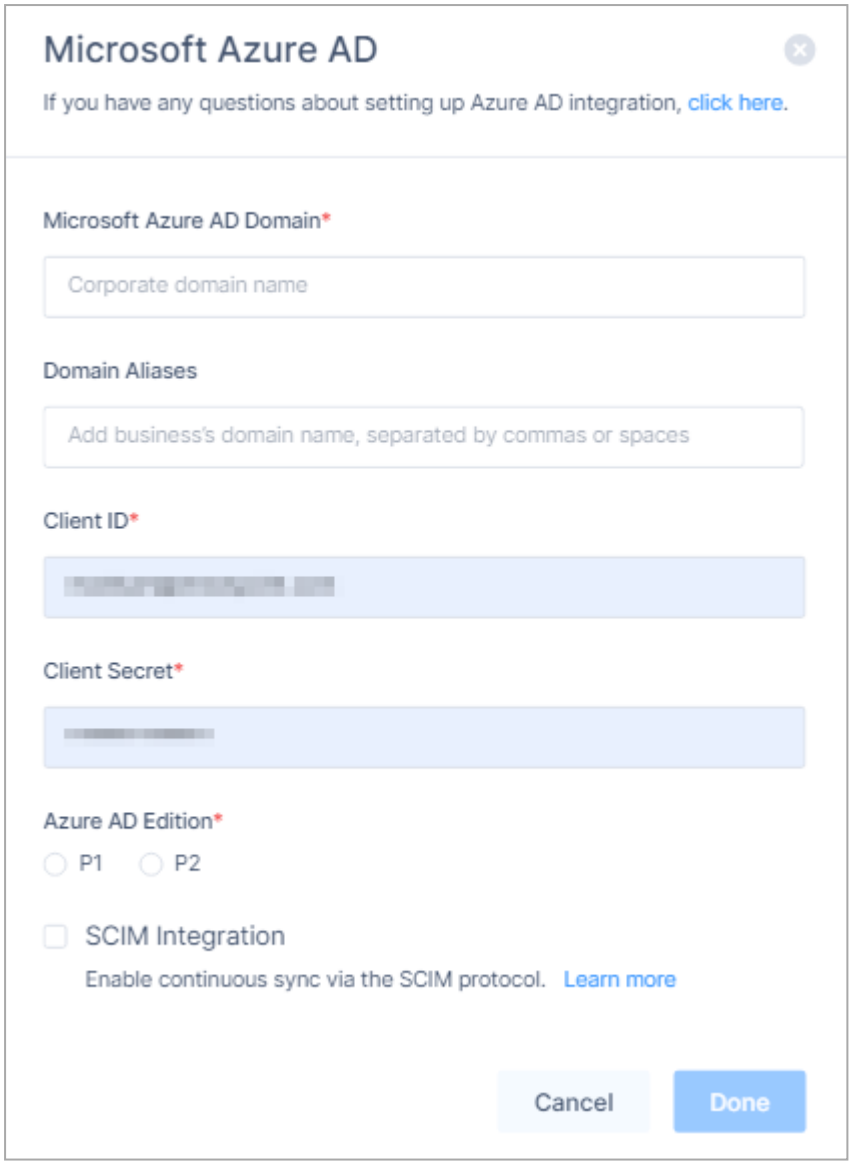
2. Click **Add Provider**.

   The **Add identity provider** window appears.



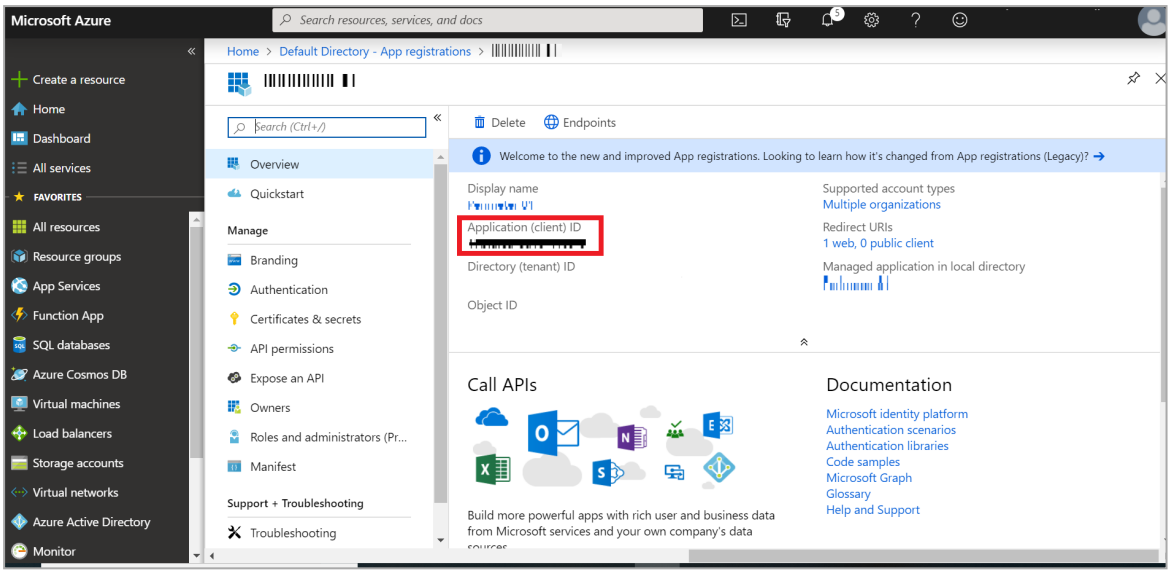
3. Select **Microsoft Azure AD**.
4. Click **Continue**.

   The **Microsoft Azure AD** page appears.



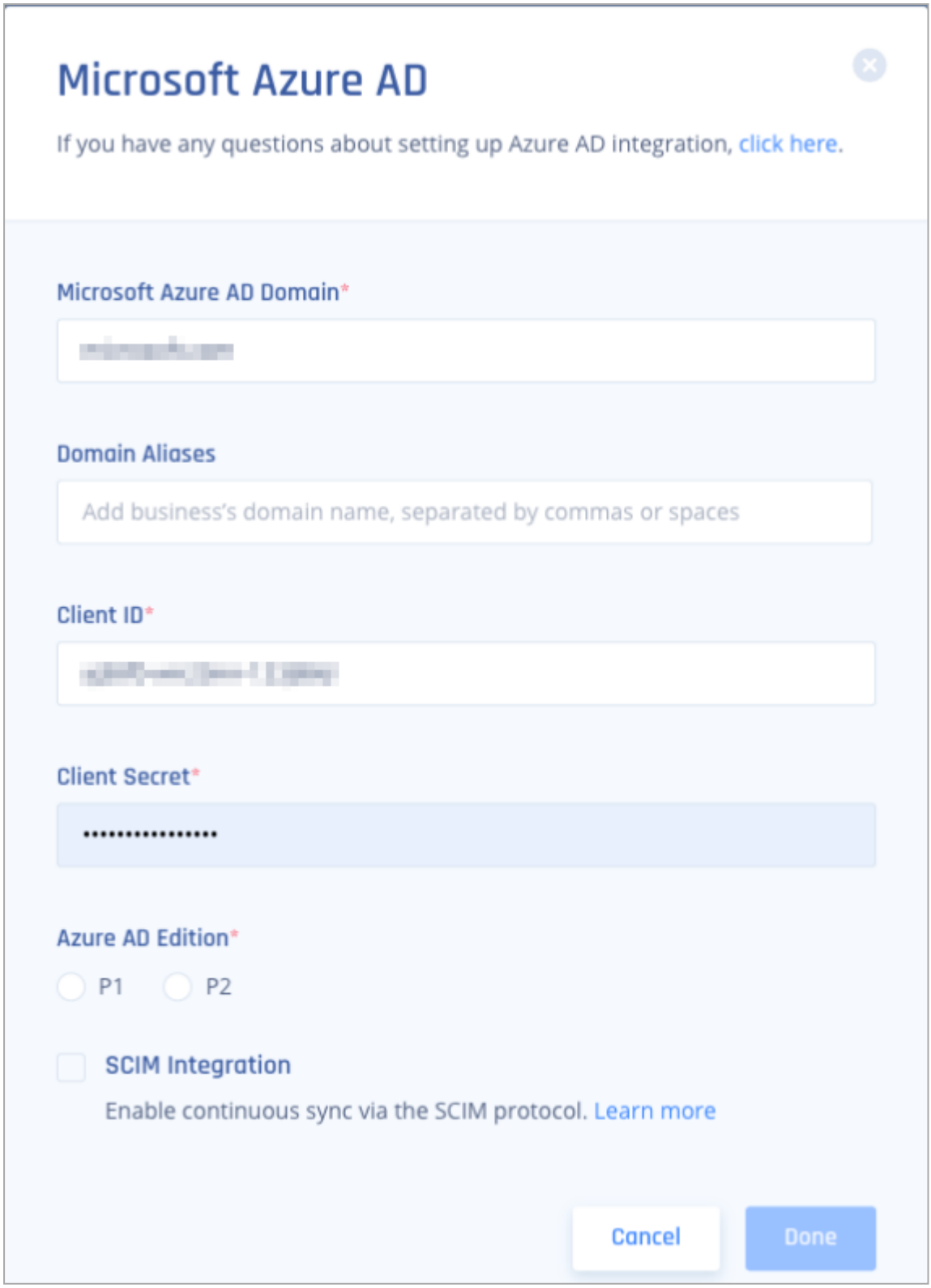
5. In the **Microsoft Azure AD Domain** field, enter the domain name.
6. In the **Domain Aliases** field, enter the email ID(s) separated by commas or spaces.
7. In the **Client ID** field, enter the **Application (client) ID** in Microsoft Azure AD:
   a. Log in to your Microsoft Azure Portal.
   b. Go to **Identity** > **Applications** > **App registrations** > **All applications**.
   c. Browse to **App registrations**, locate and select your application.

d. Go to **Overview** > **Application (client) ID**.



e. Copy the **Application (cient) ID** value.

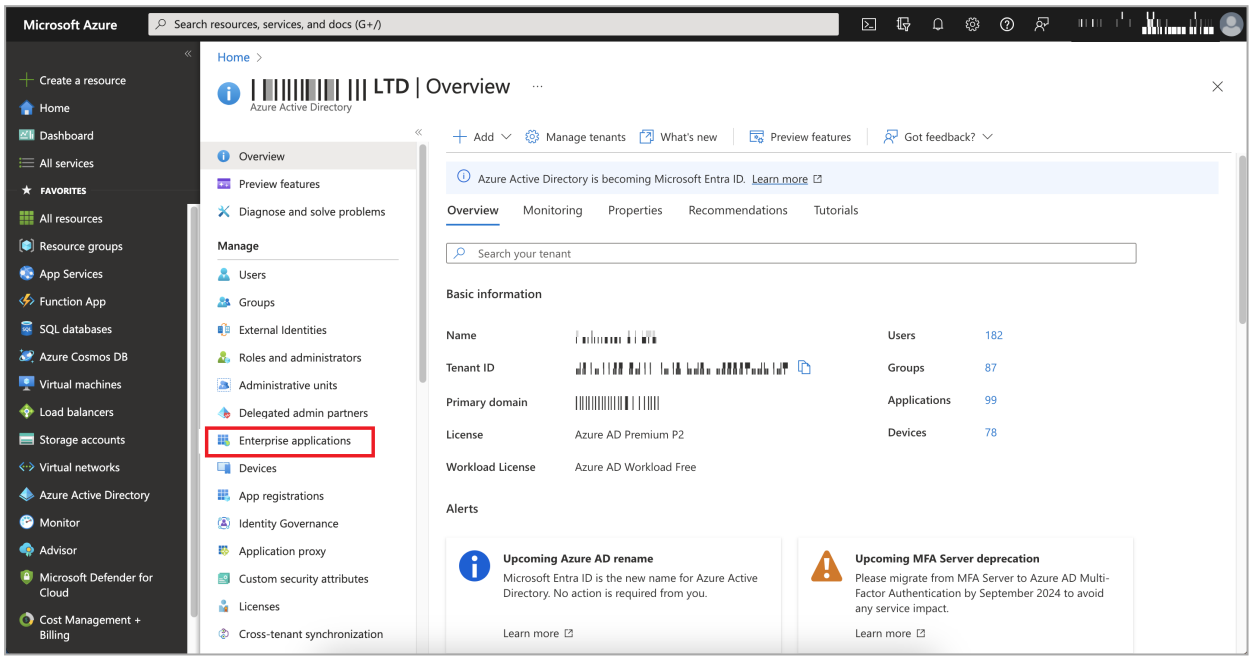
8. In the **Client Secret** field, enter the secret value. See step 9 in Configuring the Key.



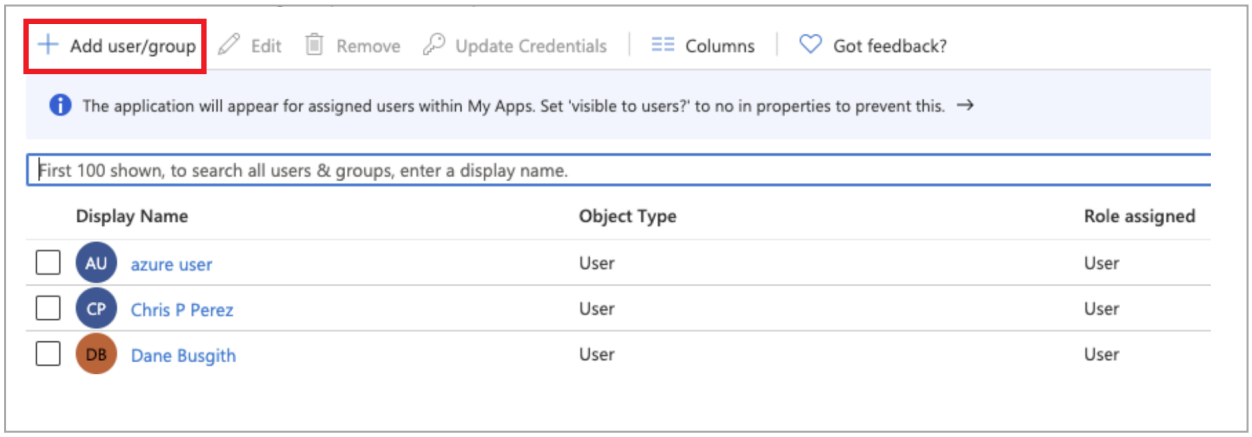
9. In the **Azure AD Edition**, select either:
   a. **PI**
   b. **P2**
10. Click **Done**.

Assigning Users and Groups in Microsoft Azure

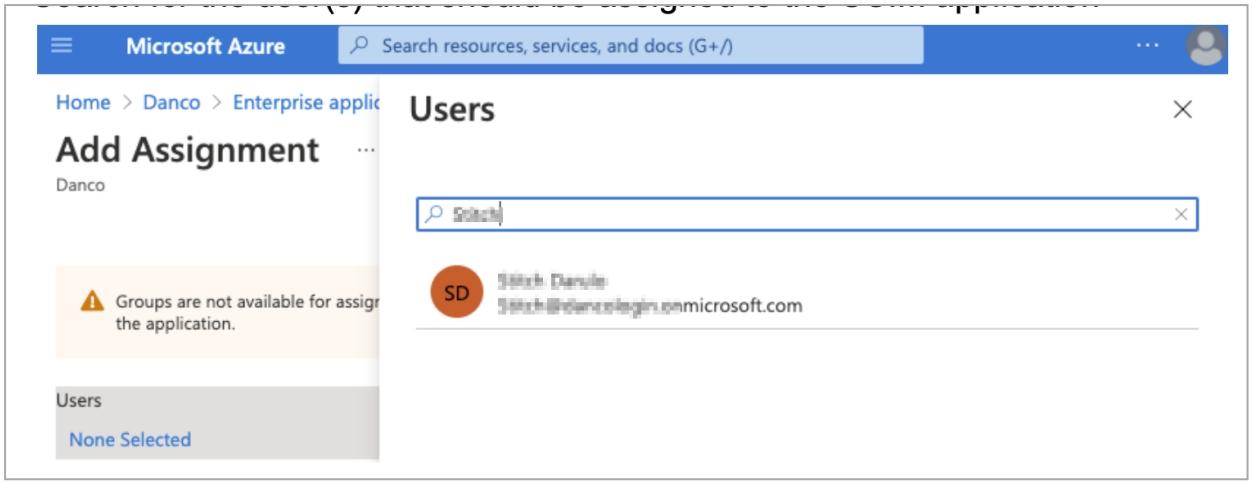
1. Log in to your Microsoft Azure Portal.
2. Navigate to **Azure Active Directory** in the left pane.
3. Go to **Manage** > **Enterprise applications**.



4. Search and select your application.
5. Go to **Users and groups** and click **Add user/group**.



6. Click **None Selected** in **Users**.



7. Search and select the user(s) or group(s) you want to add to the application.

   Note - Special characters are not supported in groups.

8. Click **Select**.
9. Click **Assign**.

System for Cross-domain Identity Management (SCIM)

SCIM is an open standard that manage user identity information, enhances the automation of user provisioning and management.

When using SCIM, changes you make to users on the identity provider side are automatically synced to Harmony SASE Agent.

Examples:

- Deleting a user within your IDP, removes the user from the Harmony SASE console, freeing up the user's license.
- When creating a new user within your IDP, and provisioning them through the SCIM integration, the user is automatically created in the Harmony SASE console.

Harmony SASE offers SCIM integration with these Identity Providers:

- *"Okta (SCIM)" below*
- *Azure Active Directory (SCIM)*

Okta (SCIM)

Harmony SASE integrates with Okta using SCIM, ensuring automatic user synchronization, profile updates, and streamlined deactivation when users are removed from the Okta SCIM Application.

Prerequisites

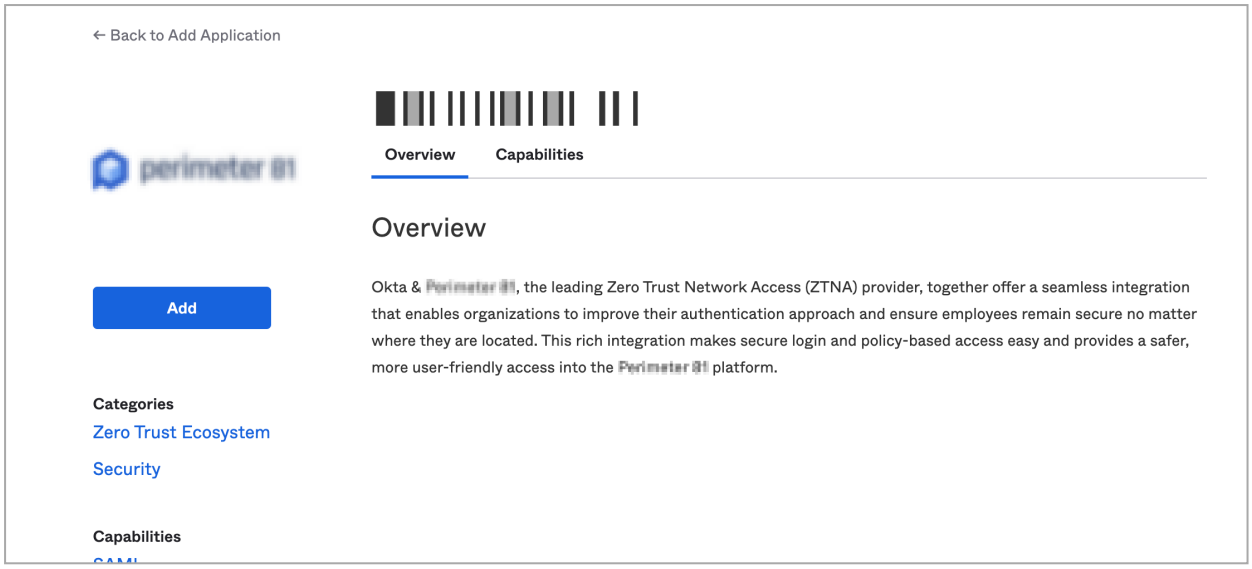
To integrate Okta and Harmony SASE, you must have:

- Administrator access to both Okta and Harmony SASE Administrator Portal.
- Active Harmony SASE Okta application configured for Single Sign-On.

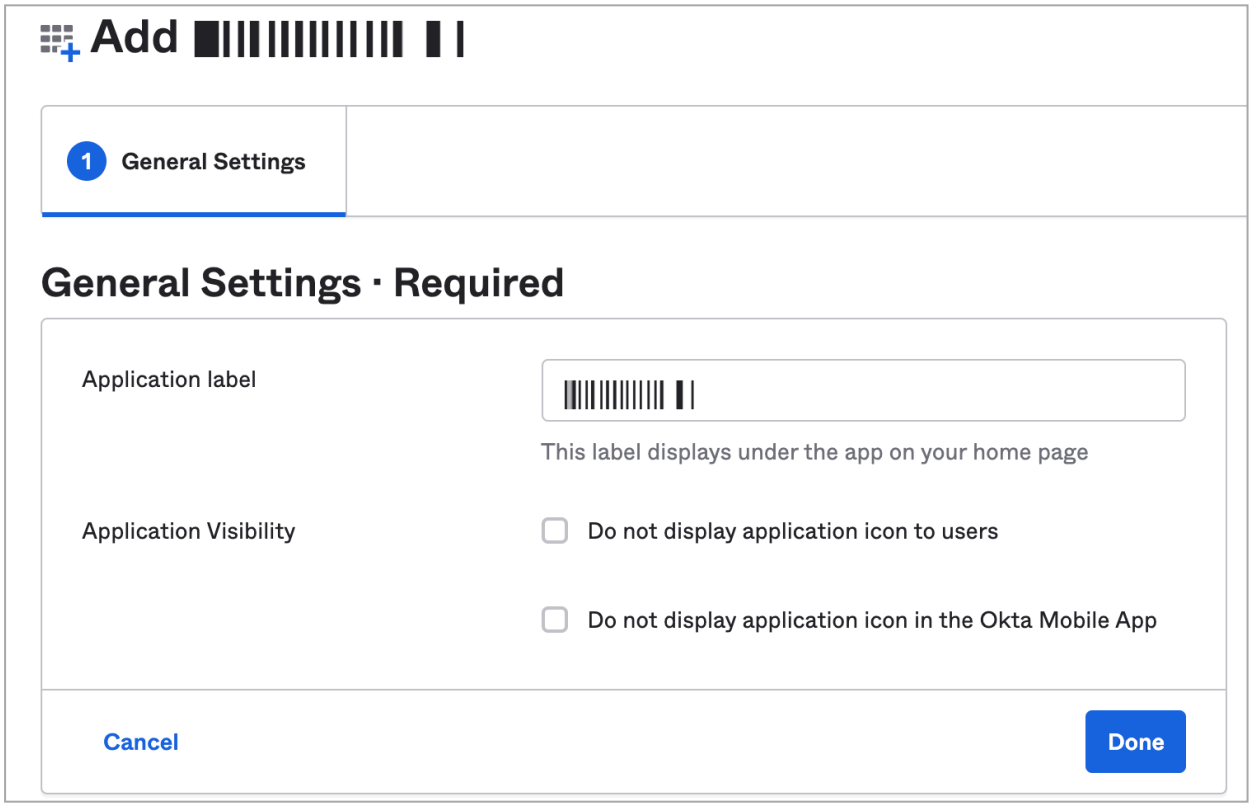
Note - SCIM based user provisioning is available to Harmony SASE Enterprise customers only.

Enabling SCIM on Okta Management Portal

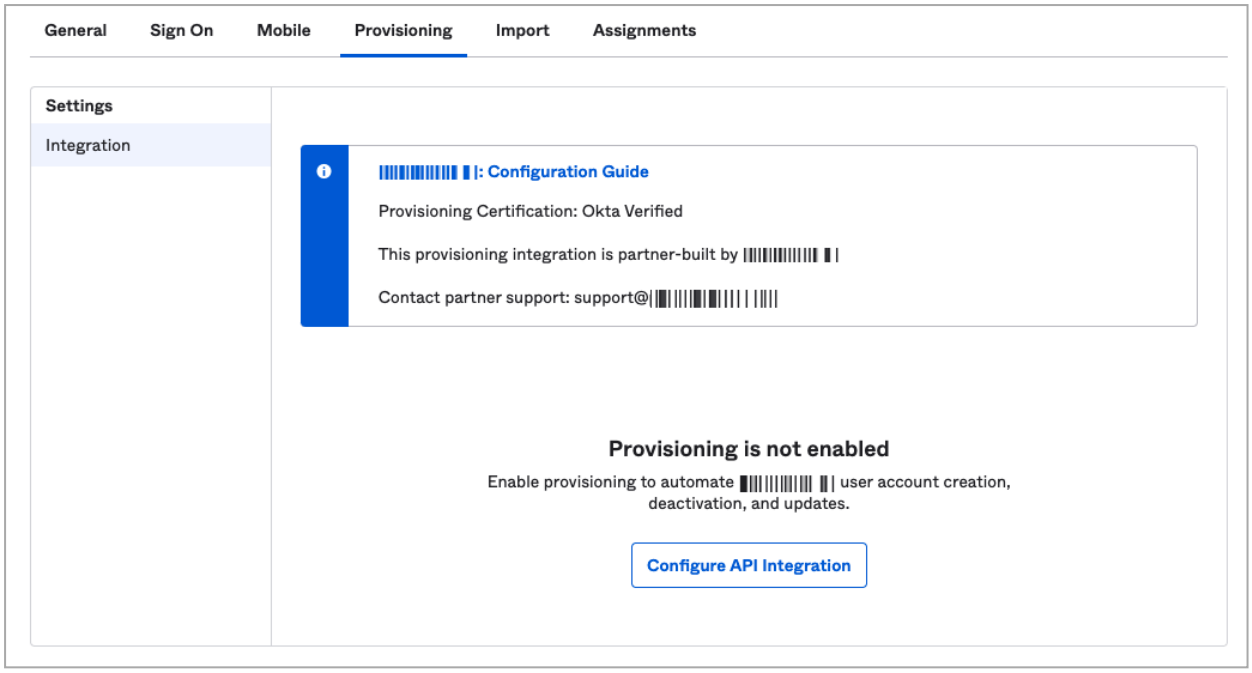
1. Log in to your Okta Management Portal.
2. Go to **Applications** > **Browse app Catalog**.
3. Search and select your application and click **Add**.



4. Click **Done**.

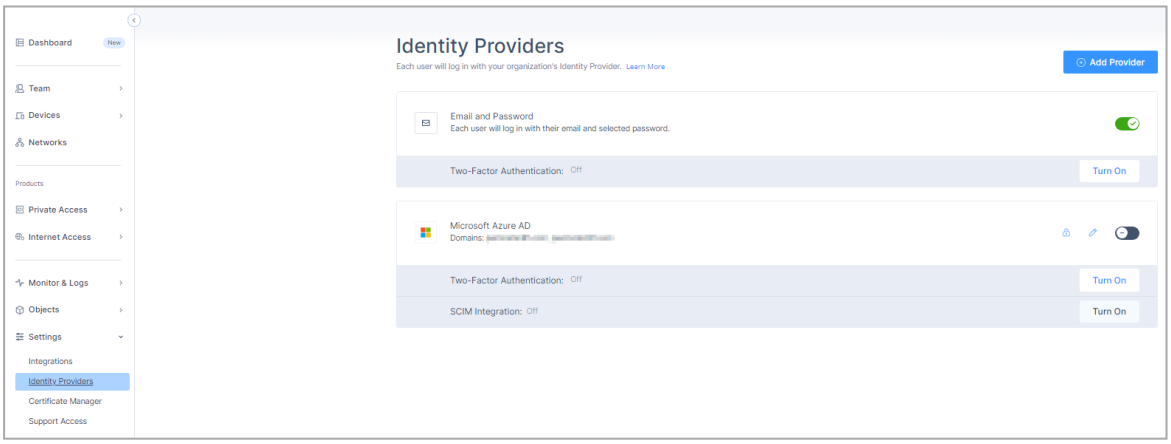


5. Go to the **Provisioning** tab and click **Configure API Integration**.

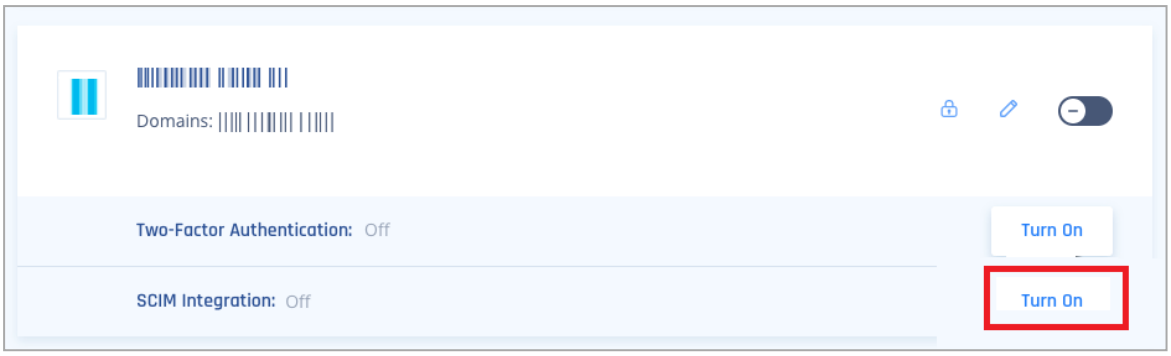


6. Select the **Enable API Integration** checkbox.
7. In the **API Token** field, enter the generated token. To get the generated token:
   a. Access the Harmony SASE Administrator Portal and click **Settings** > **Identity Providers**.

      The **Identity Providers** page appears.

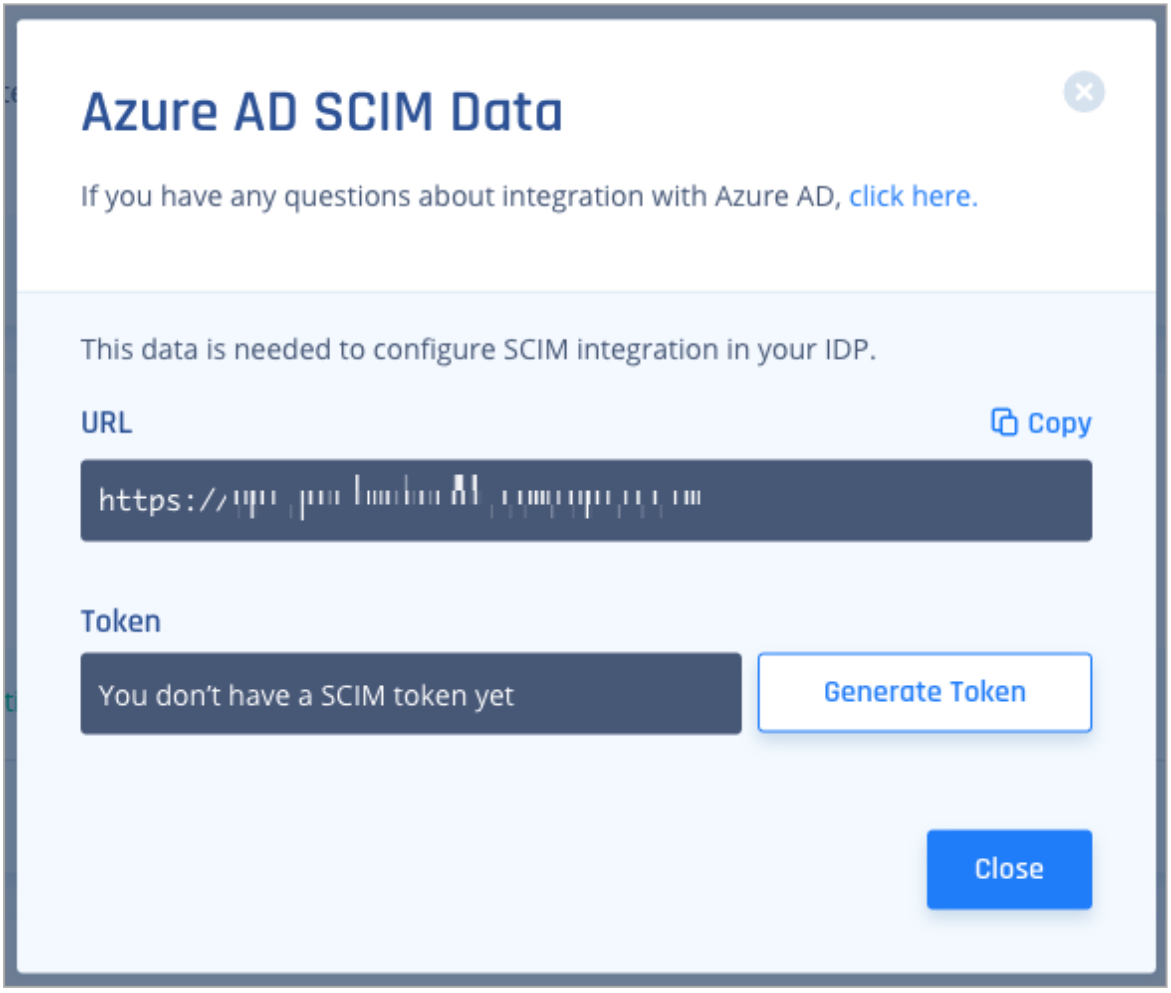


b. Click **Turn On** in the **SCIM Integration** section.



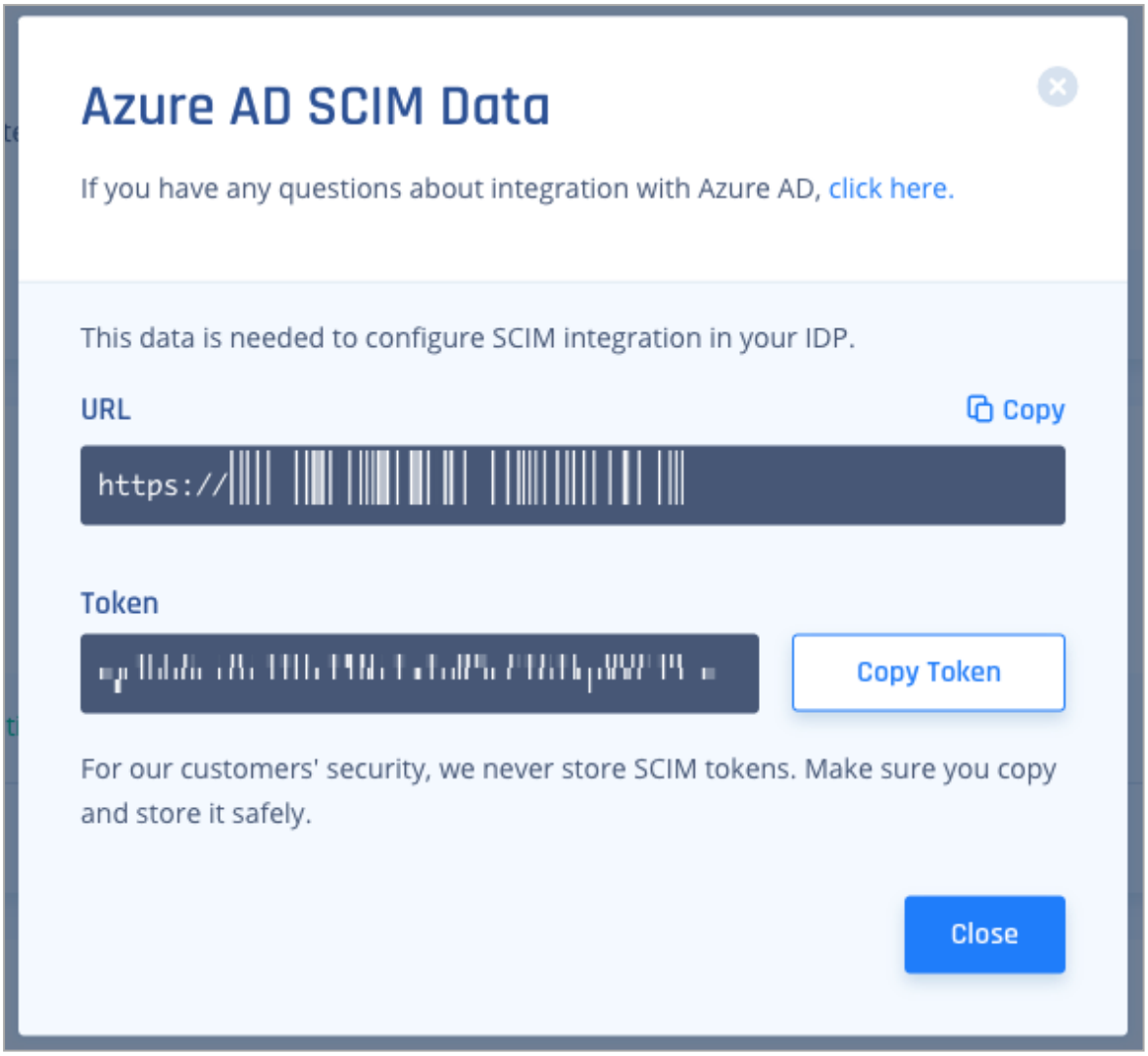
c. Click **Settings** in the **SCIM Integration** section.

d. Click **Generate Token**.



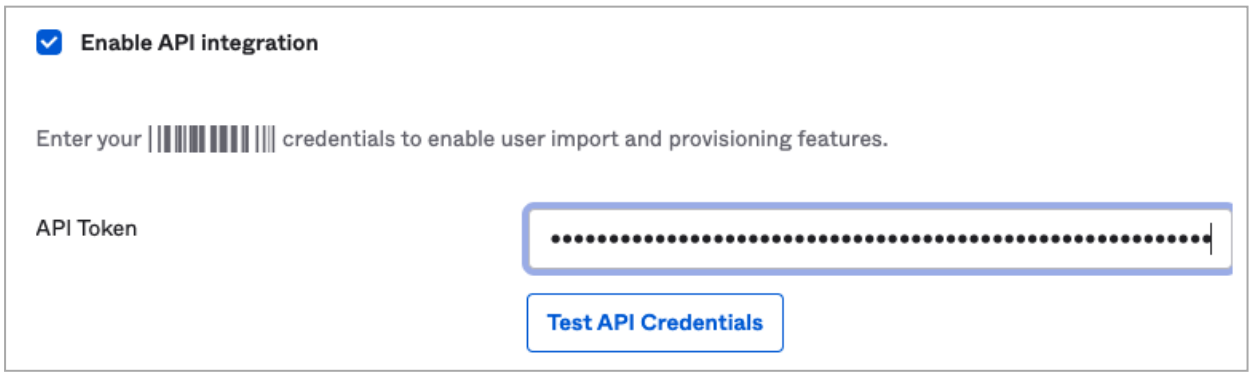
e. The secret token is generated.

f. Click **Copy Token**.



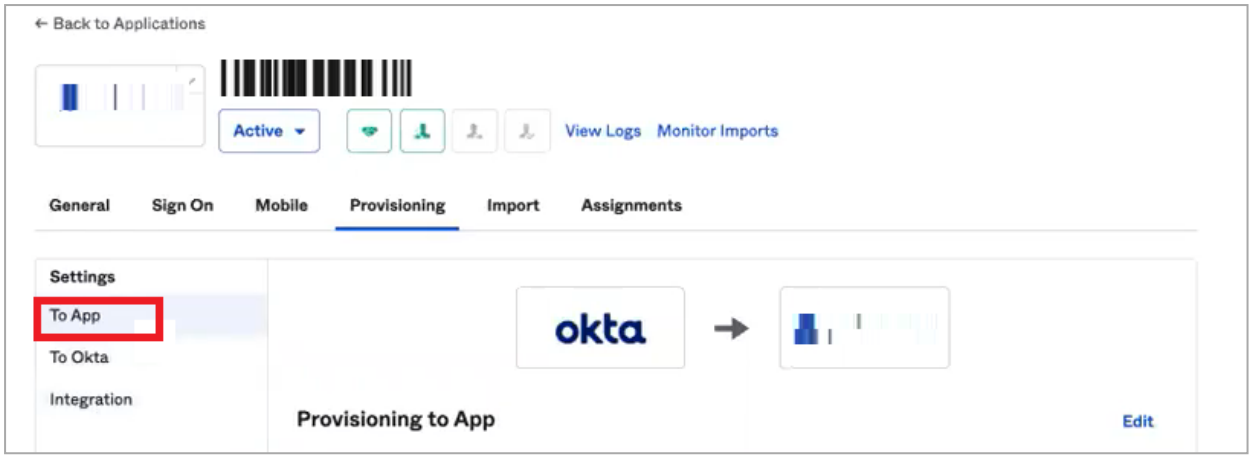
g. Click **Close**.

8. Click **Test API Credentials**.

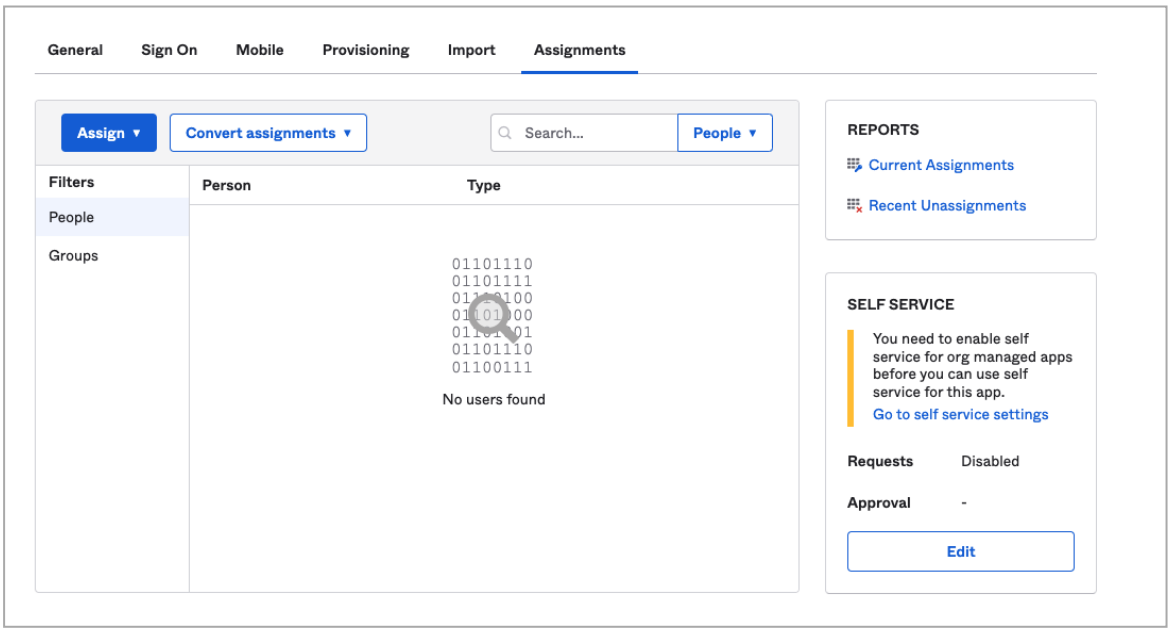


9. Click **Save**.

10. Go to **Settings** > **To App**.

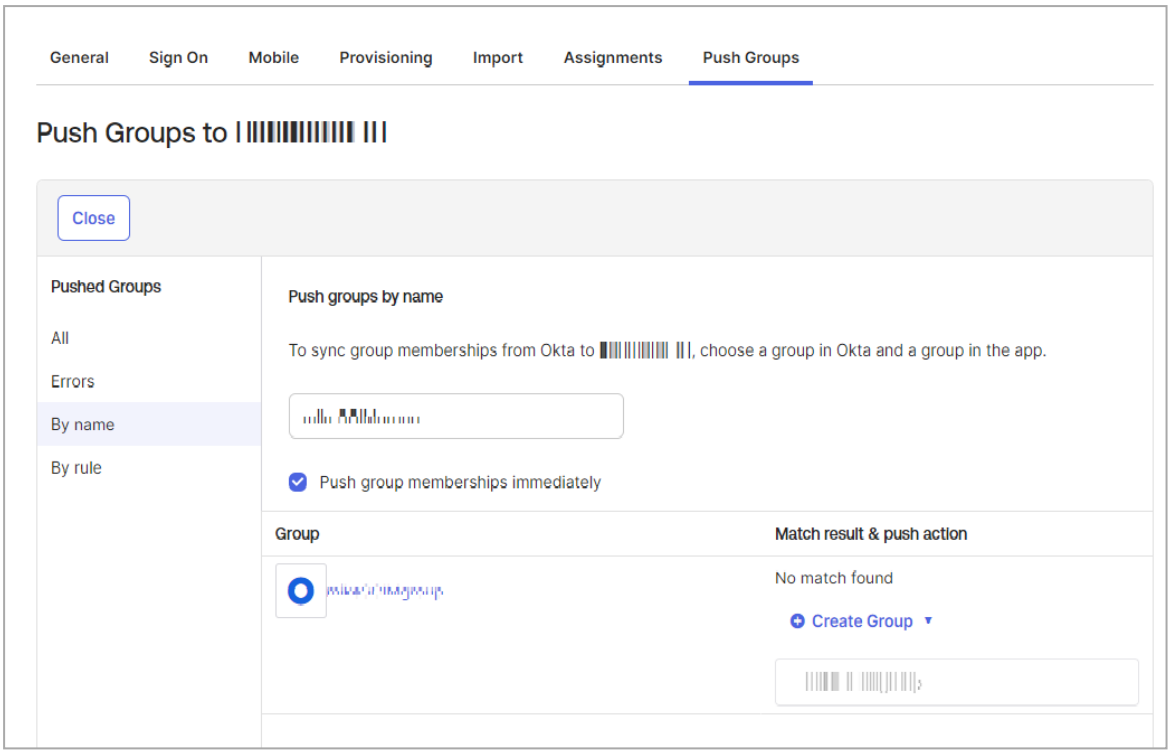


11. Click **Edit**.
12. Select the checkbox for:
    - **Create Users**
    - **Update User Attributes**
    - **Deactivate Users**
13. Click **Save**.
14. To provision users and groups:
    a. Go to **Applications** and select your SAML 2.0 application.
    b. Go to **Assignments** tab.



    c. Click **Assign**.
    d. Search and select the user name, email id, or group(s) name.

e. To push groups, click the **Push groups** tab and select **By name**.



f. In the **Push groups by name** field, enter the group name.

g. Select the **Push group memberships immediately** checkbox.

h. Click **Save and Go Back**.

i. Click **Done**.

These SAML attributes are supported:

Application Attribute	Identity Bridge Attribute or Literal Value
email	user.email
given_name	user.firstName
family_name	user.lastName
groups	Configured in the app UI. See Group Support section.

Microsoft Entra ID (formerly Azure Active Directory) (SCIM)

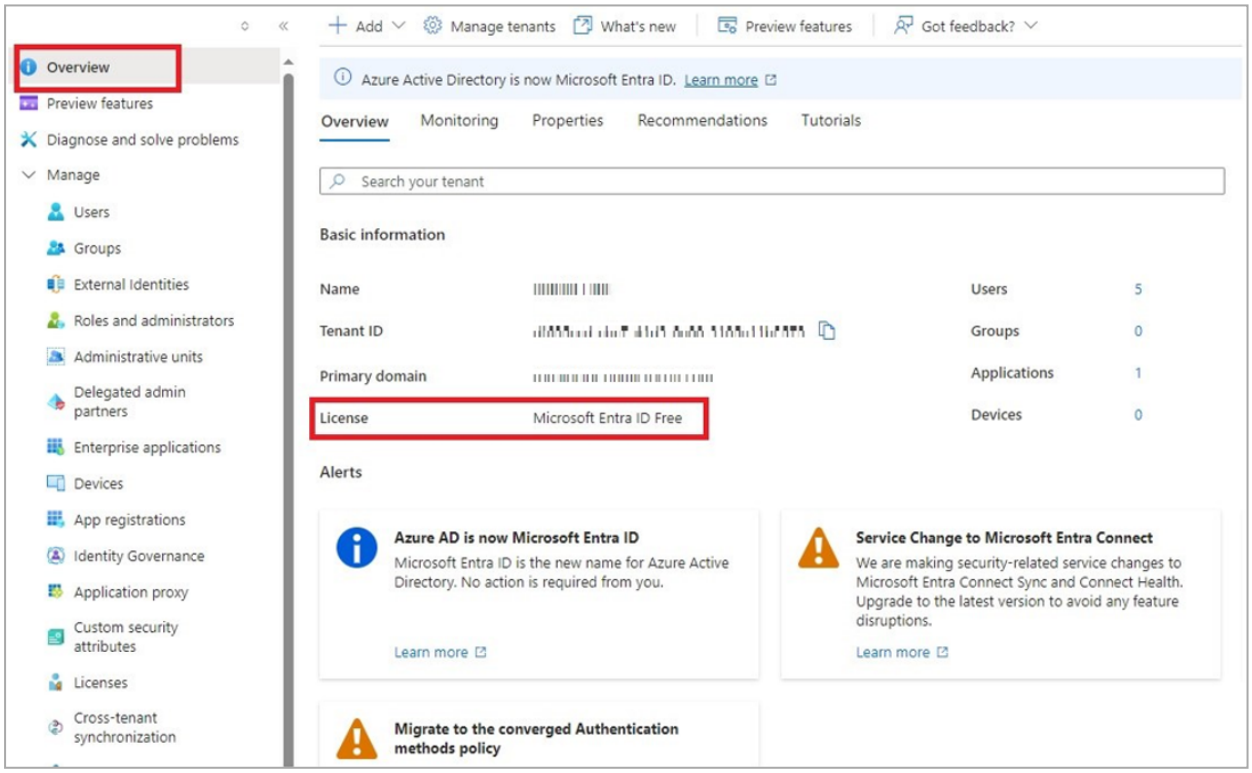
High-Level Procedure

- Part 1: Configure Entra ID
  - Step 1 - Creating an application in Entra ID
  - Step 2 - Configuring API Permissions
  - Step 3 - Configuring Secret Key for the Application
- Part 2: Configuring Harmony SASE IdP
- Part 3: Configuring SCIM

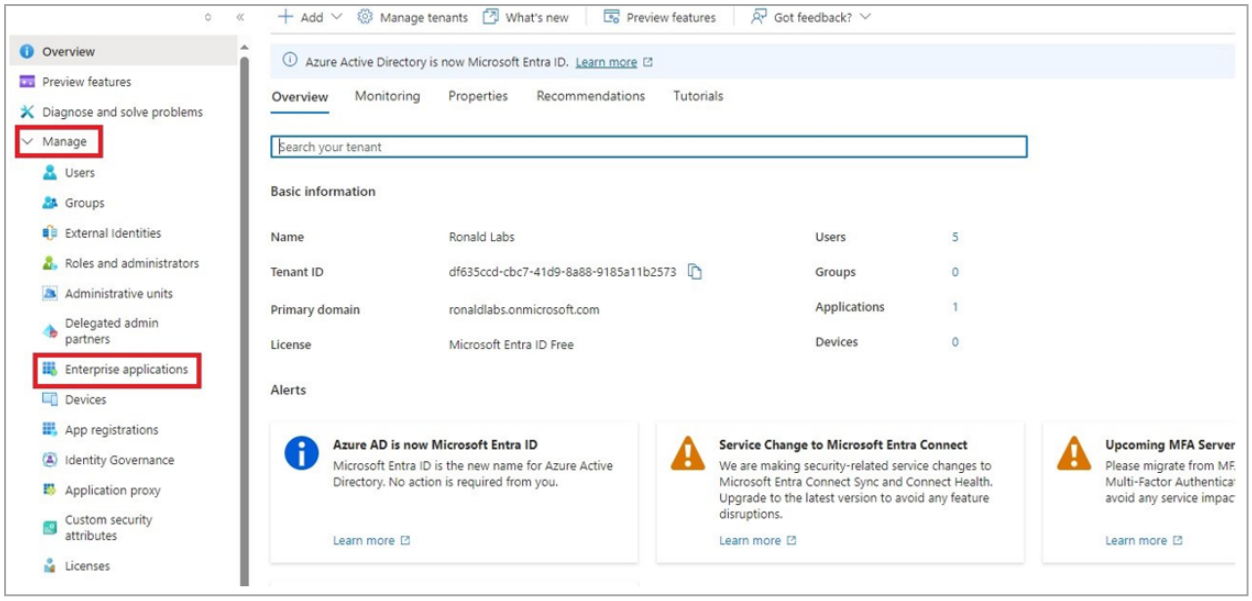
Part 1: Configure Entra ID

Step 1 - Creating an application in Entra ID

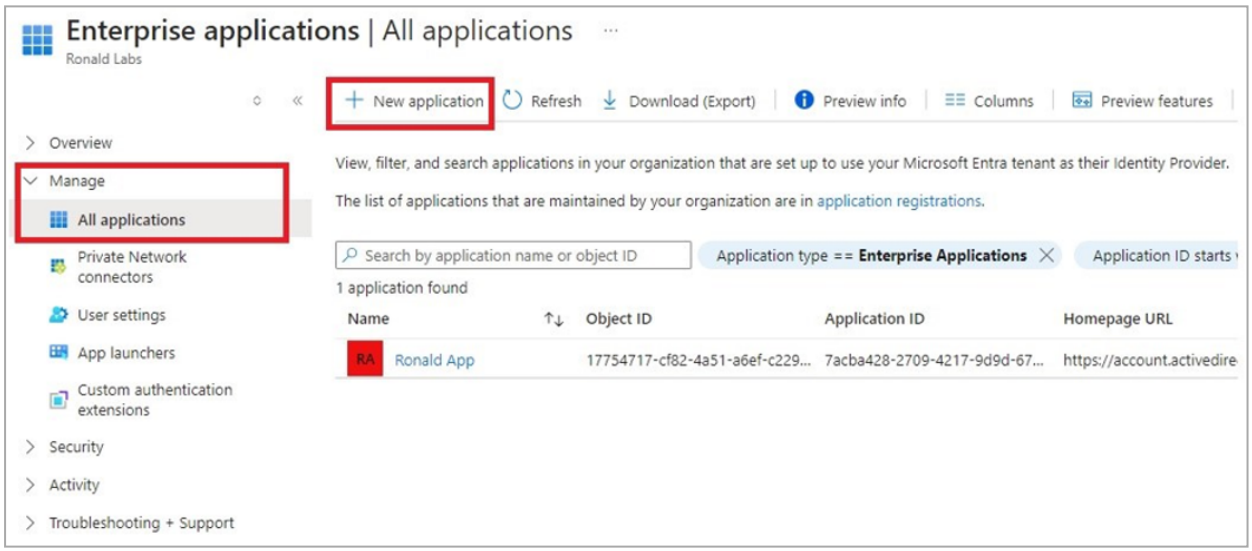
1. Access the Microsoft Azure Portal using administrator credentials.
2. From Azure services, click **Microsoft Entra ID**.
3. Click **Overview**.



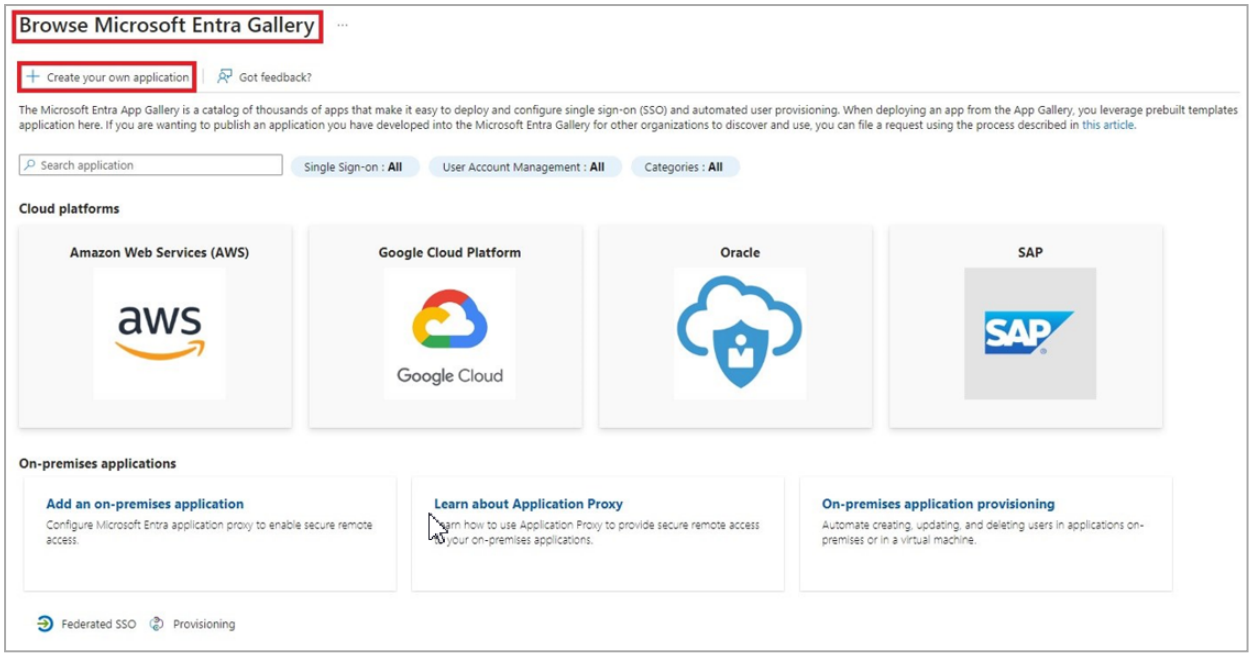
4. From the **Basic information** section, make a note of the **License**.
5. Go to **Manage** > **Enterprise applications**.



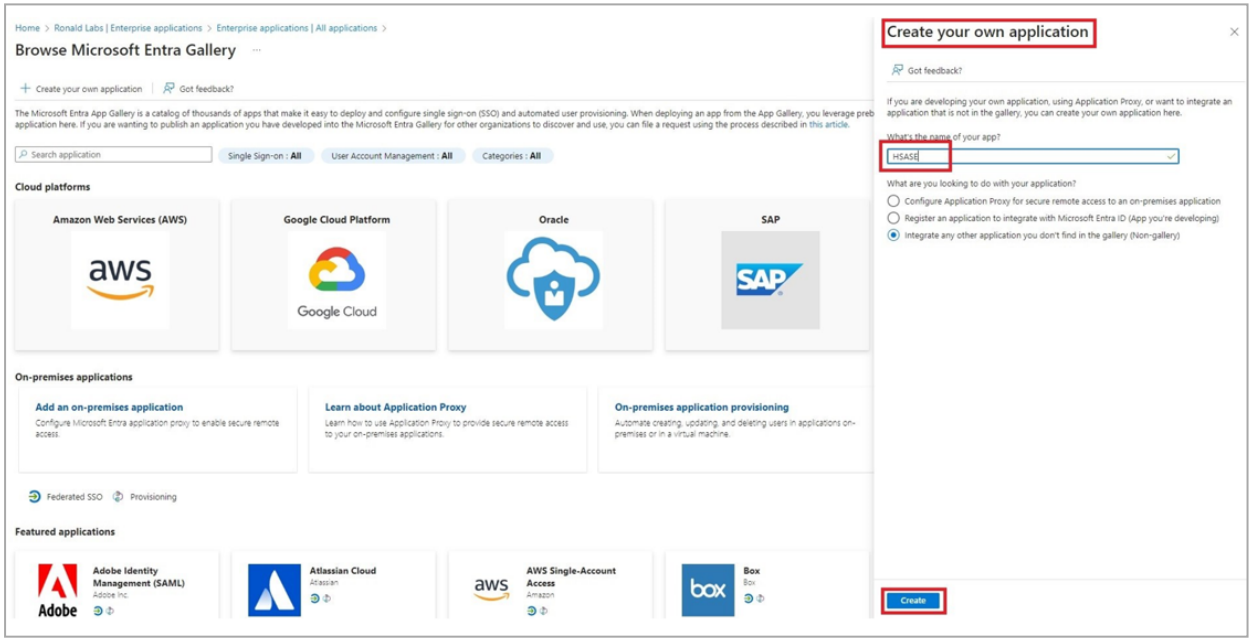
6. Go to **All applications**.
7. Click **New application**.



8. In the **Browse Microsoft Entra Gallery** page, click **Create your own application**.

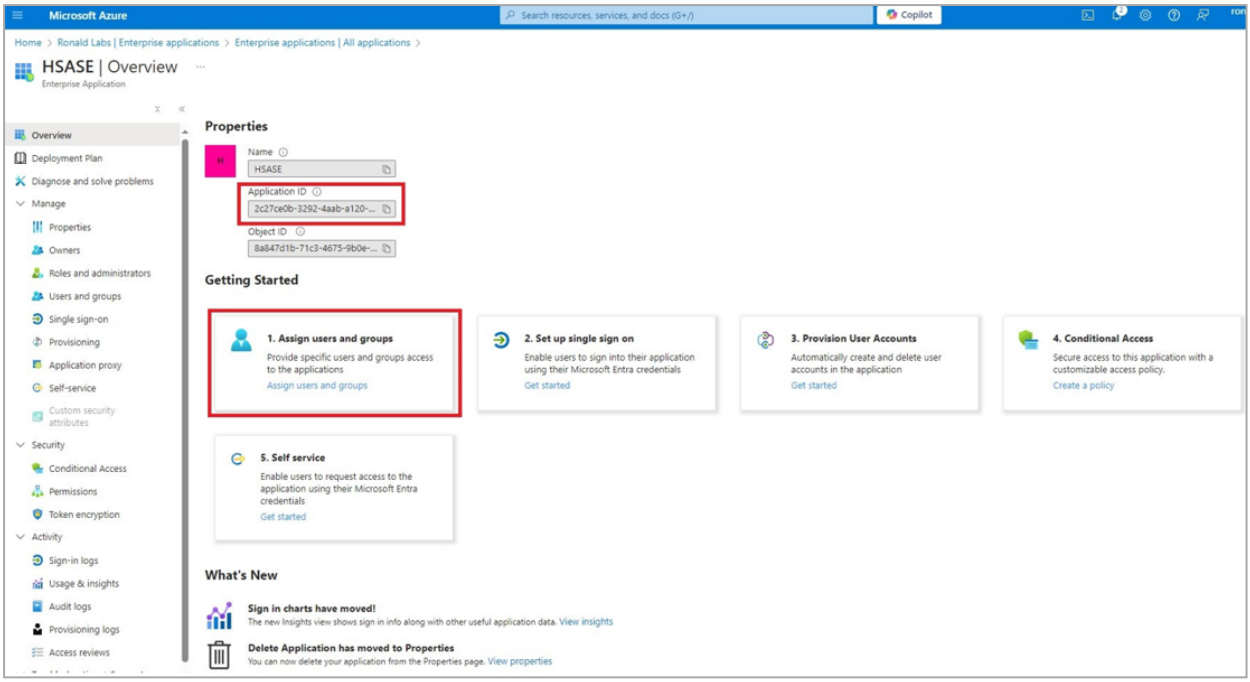


9. In the **Create your own application** panel that appears on the right, enter the application name (for example, Harmony SASE) and click **Create**.

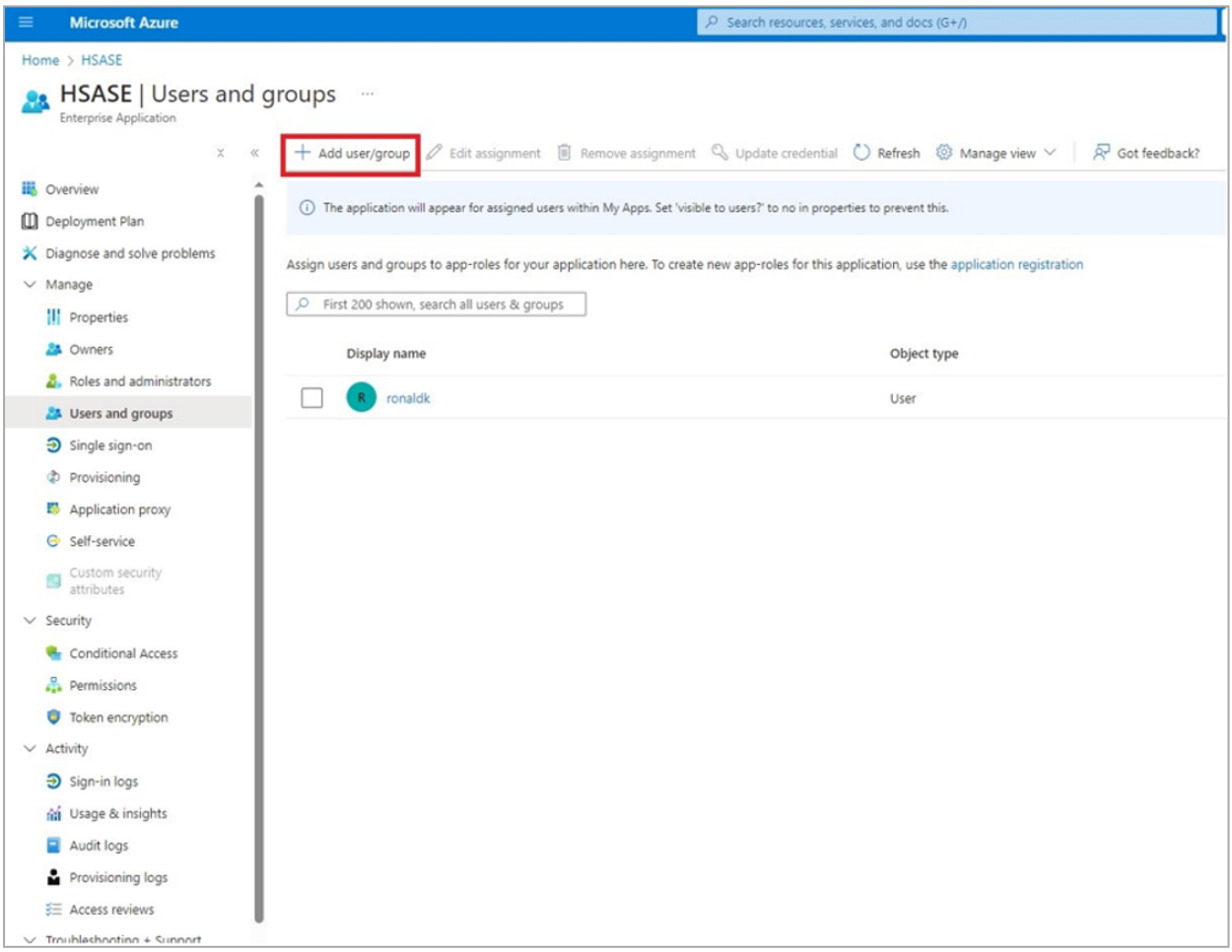


Once the application is created, the **Overview** page appears.

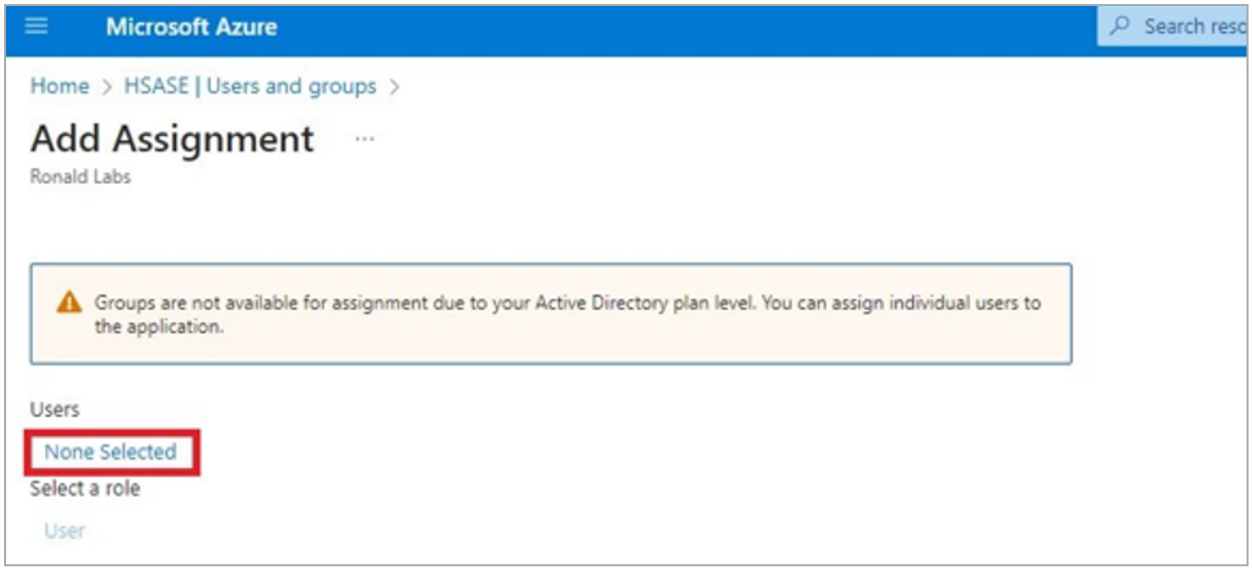
10. Click the icon next to **Application ID** to copy it.



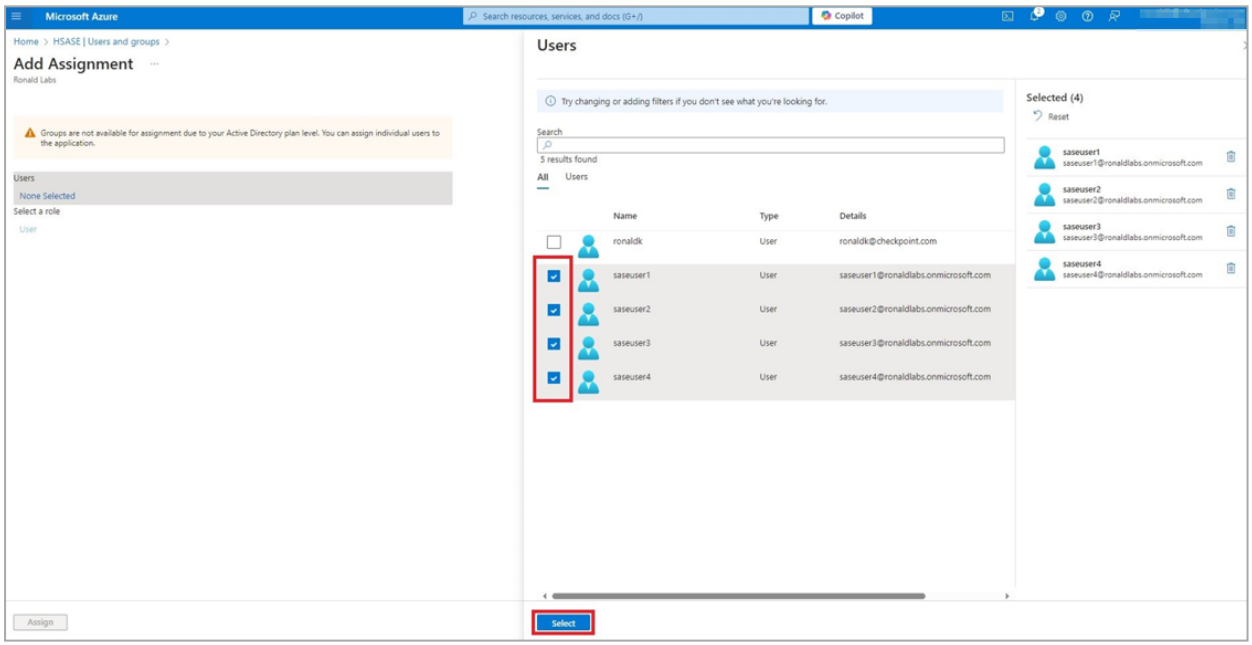
11. Click **Assign users and groups** and then click **Add user/group**.



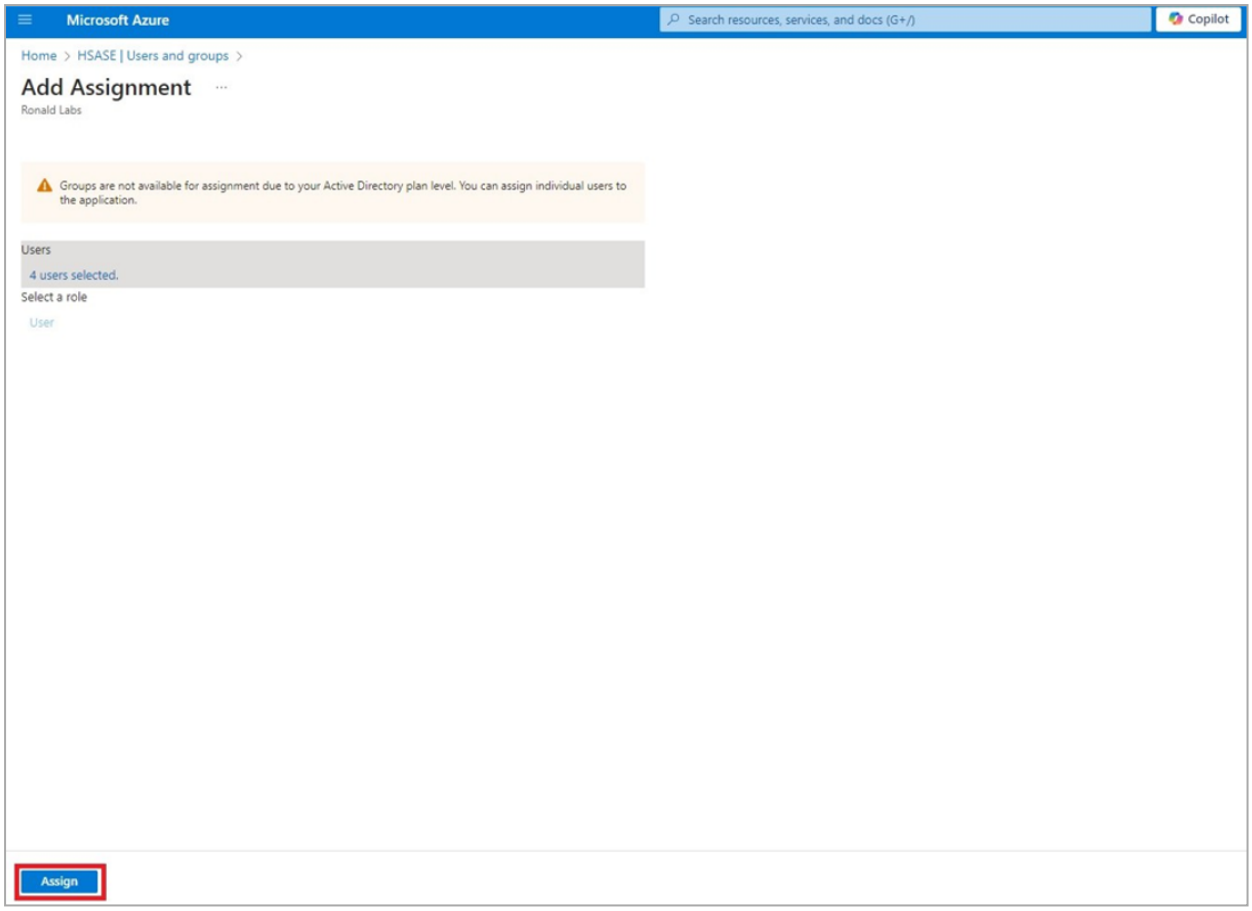
12. In the **Users** section, click **None Selected**.



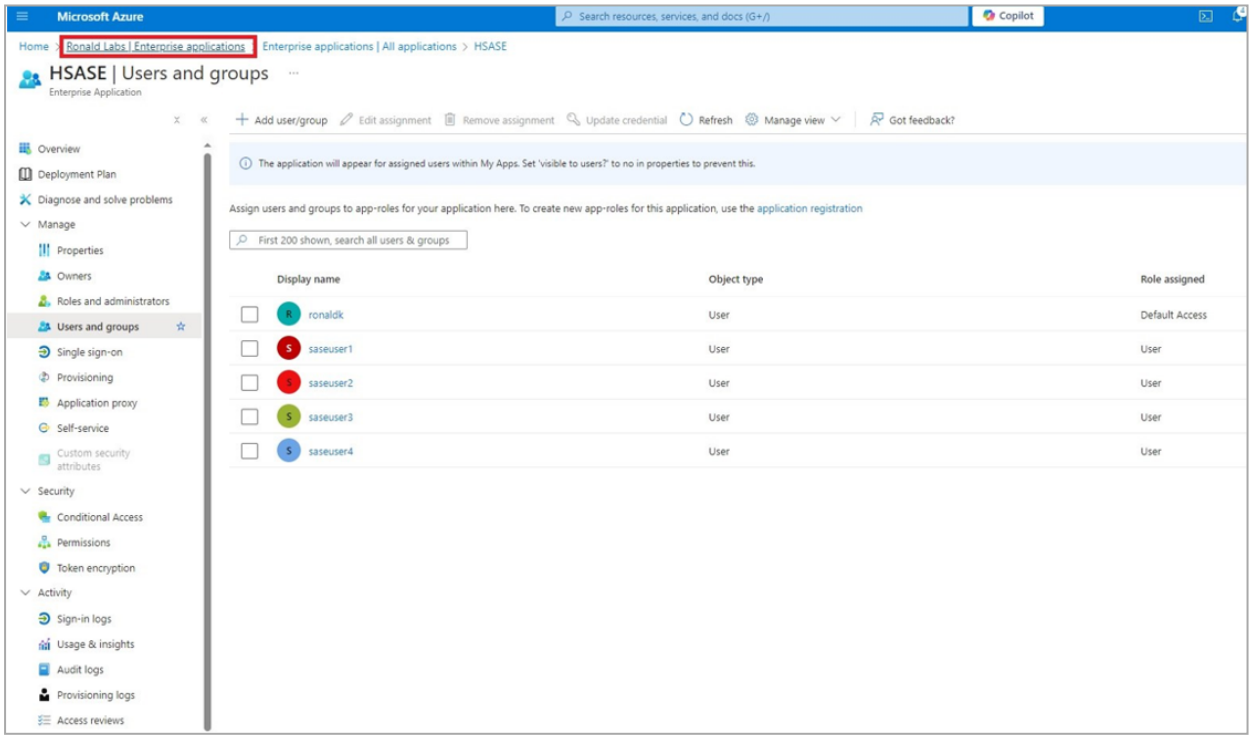
13. Select the users and groups you want to add to the application and click **Select**.



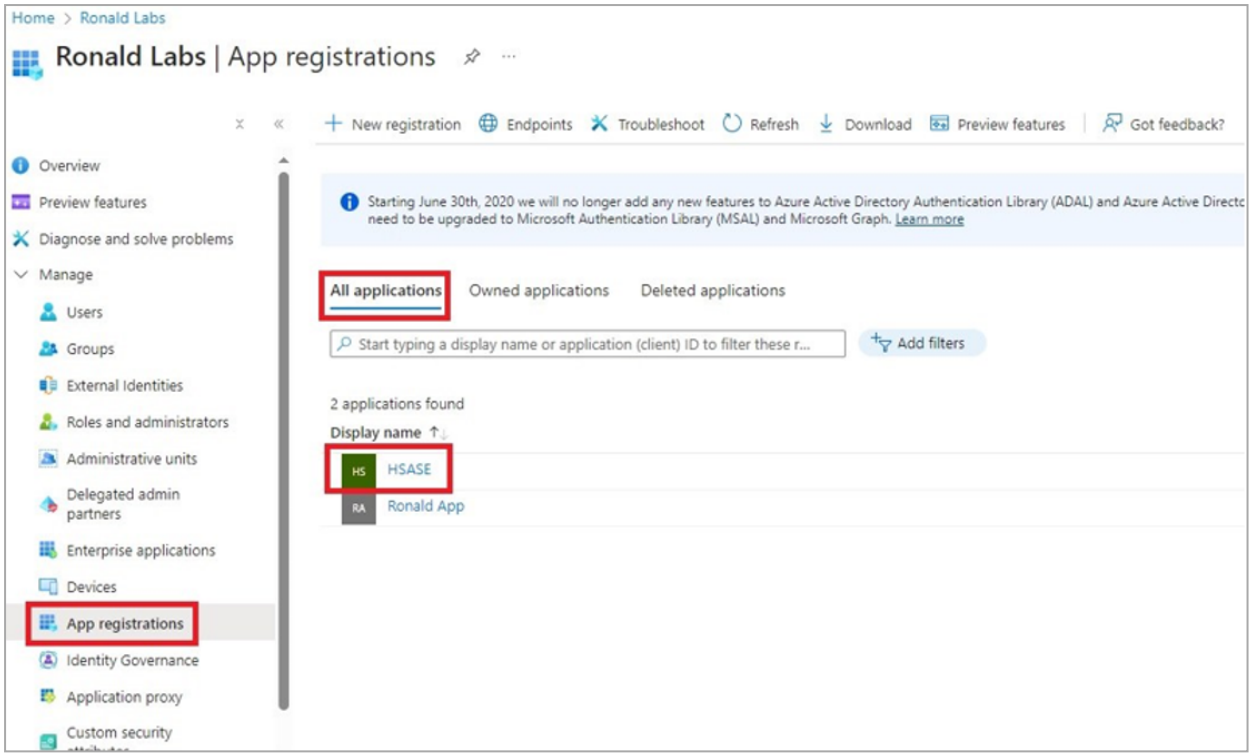
14. Click **Assign**.



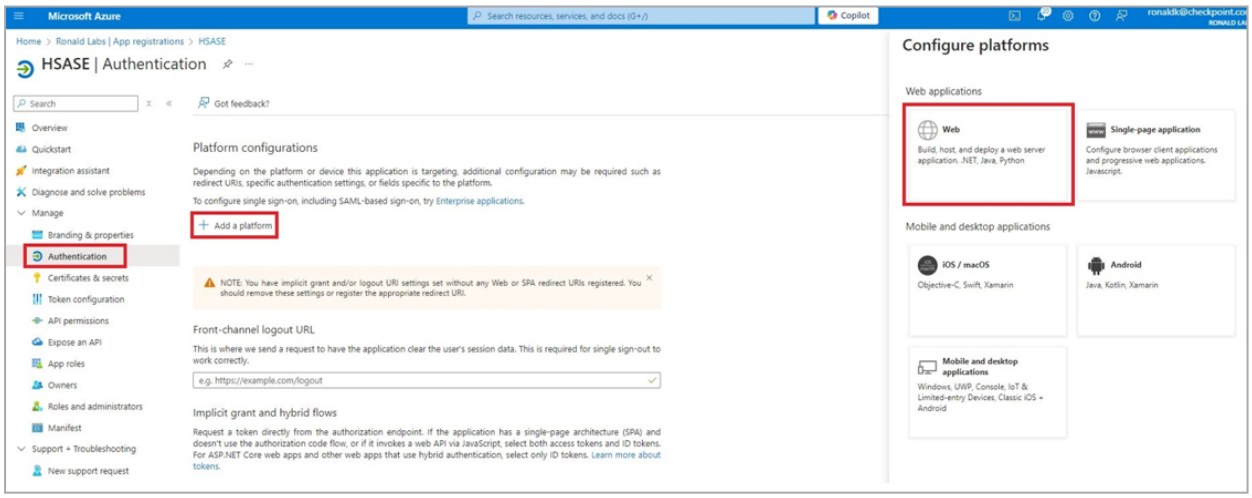
15. Click **Enterprise applications** in the top left corner.



16. From the left panel, click **App registrations**.

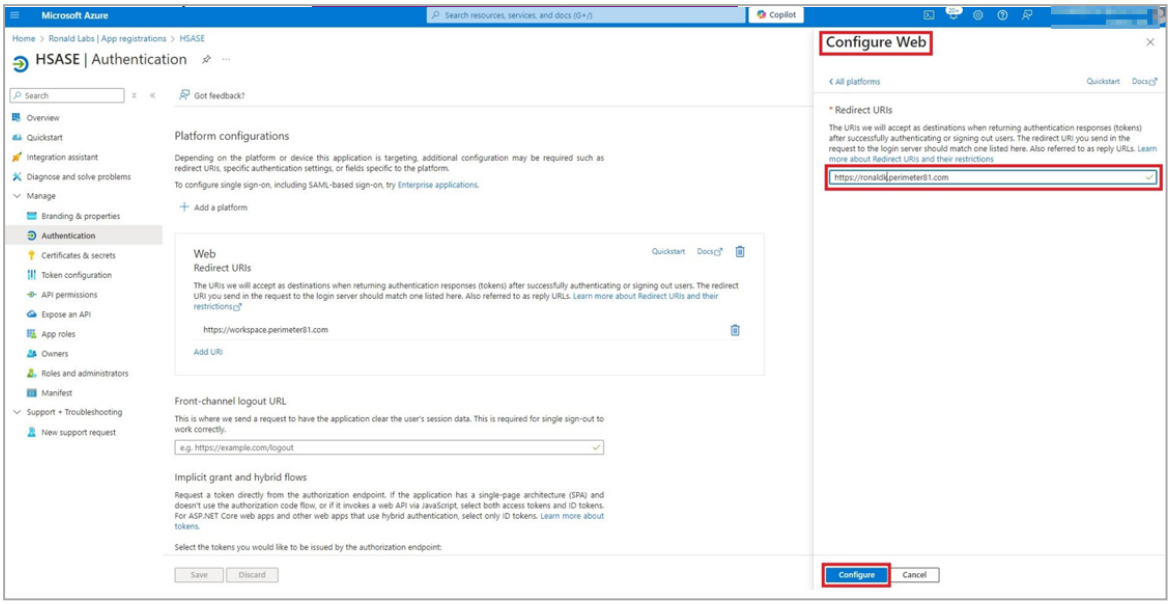


17. In the **All applications** tab, click the application you created.
18. Go to **Manage** > **Authentication** and click **Add a platform**.
19. In the **Configure platforms** panel that appears on the right, click **Web**.



20. In the **Redirect URIs** field, enter your workspace name and click **Configure**:

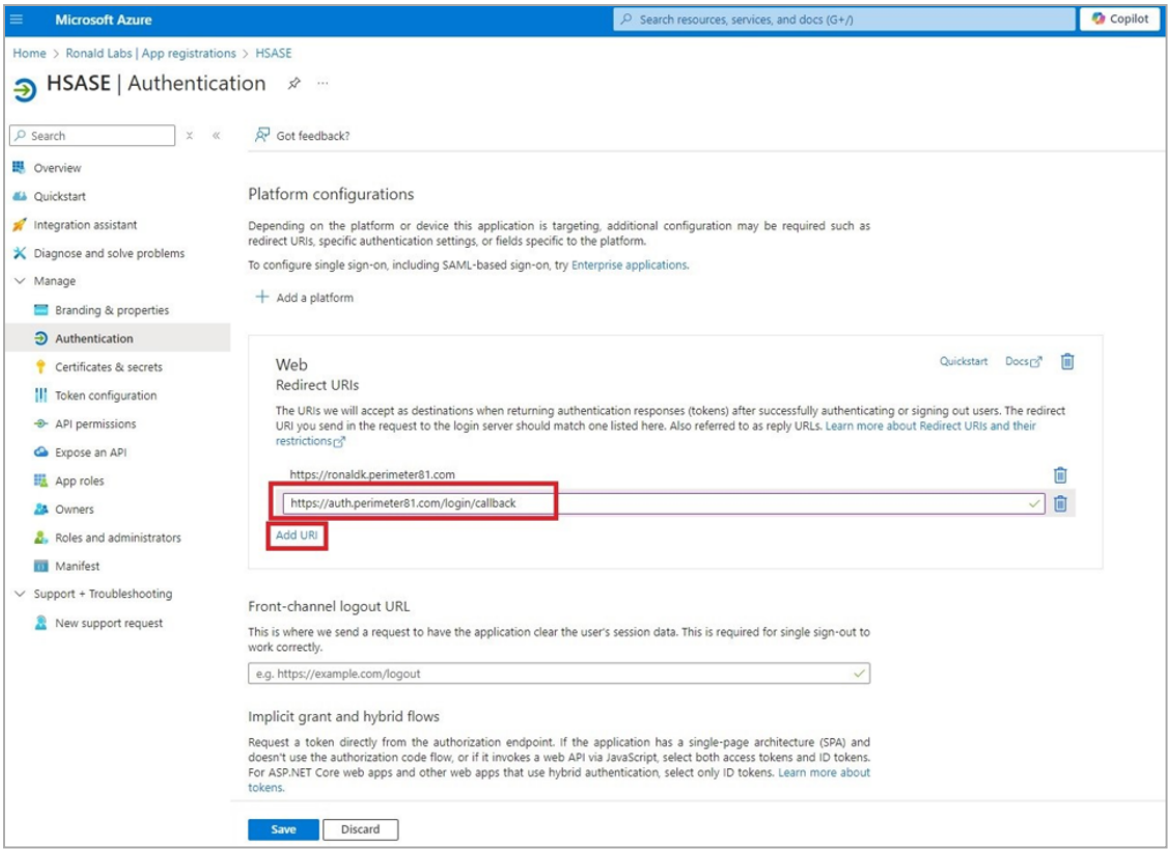
- For EU based platform - `https://workspace.eu.sase.checkpoint.com`
- For US based platform - `https://workspace.perimeter81.com`



21. In the **Redirect URIs** section, click **Add URI** and add these:

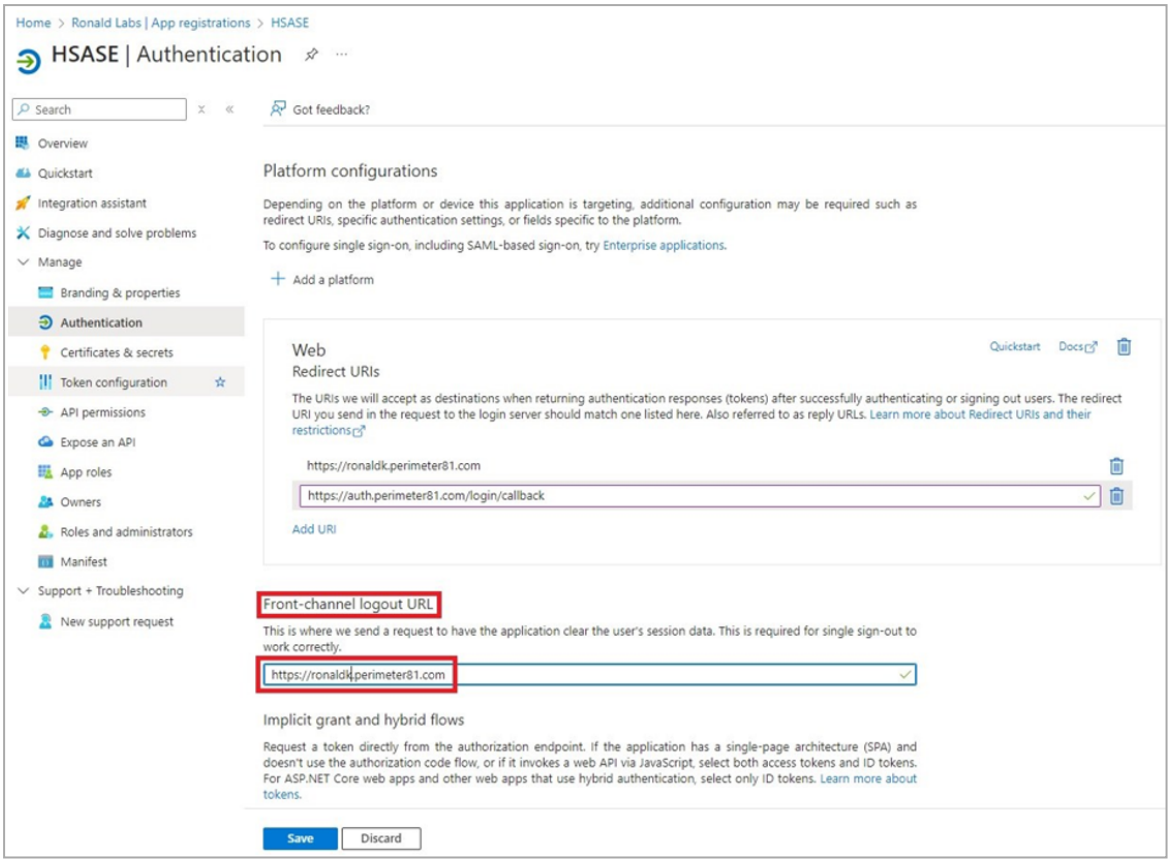
    - For EU based platform - `https://auth.eu.sase.checkpoint.com/login/callback`

- For US based platform - `https://auth.perimeter81.com/login/callback`

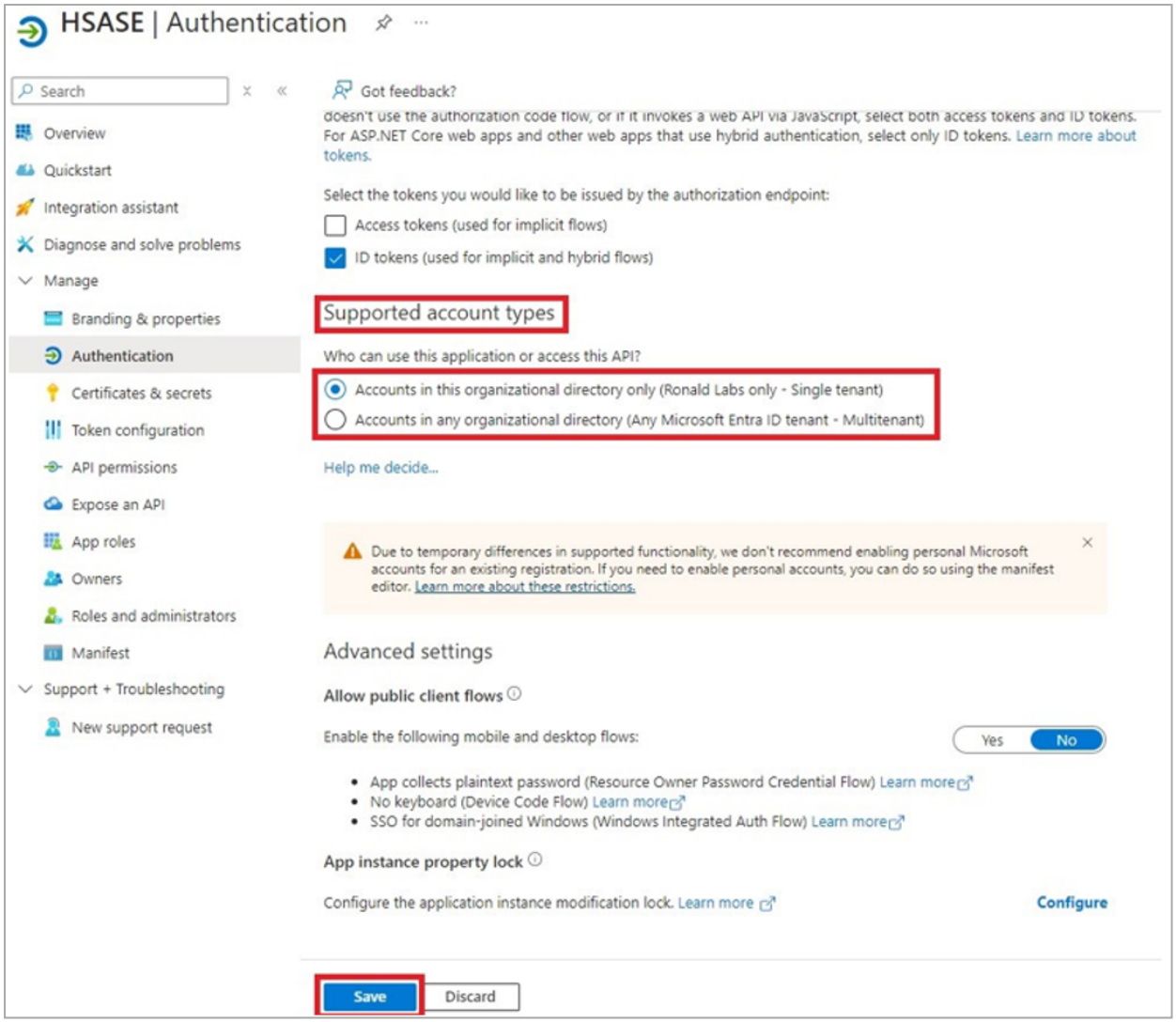


22. In the **Front-channel logout URL** section, enter your workspace name:

- For EU based platform - `https://workspace.eu.sase.checkpoint.com`
- For US based platform - `https://workspace.perimeter81.com`

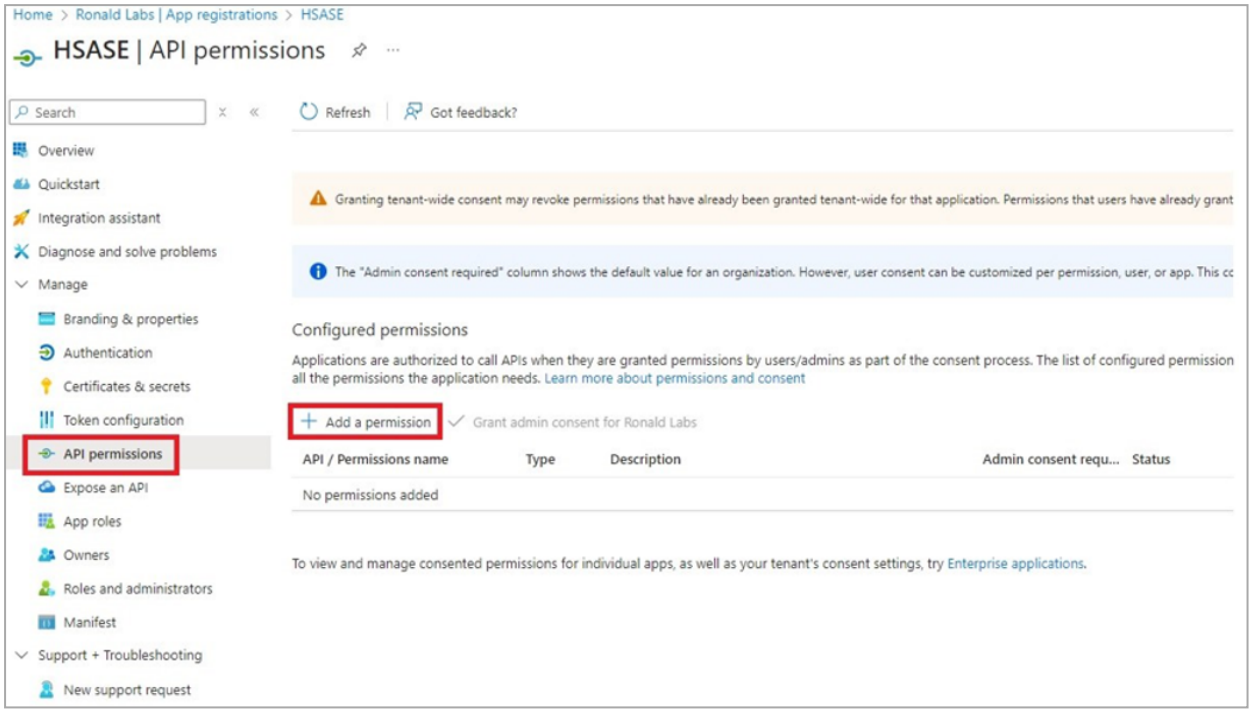


23. In the **Supported account types** section, select the applicable option for supported account types and click **Save**.


HSASE | Authentication
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest
Support + Troubleshooting
New support request
Got feedback?
doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. Learn more about tokens.
Select the tokens you would like to be issued by the authorization endpoint:
Access tokens (used for implicit flows)
ID tokens (used for implicit and hybrid flows)
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Ronald Labs only - Single tenant)
Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
Help me decide...
Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. Learn more about these restrictions.
Advanced settings
Allow public client flows
Enable the following mobile and desktop flows:
Yes
No
App collects plaintext password (Resource Owner Password Credential Flow) Learn more
No keyboard (Device Code Flow) Learn more
SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more
App instance property lock
Configure the application instance modification lock. Learn more
Configure
Save
Discard

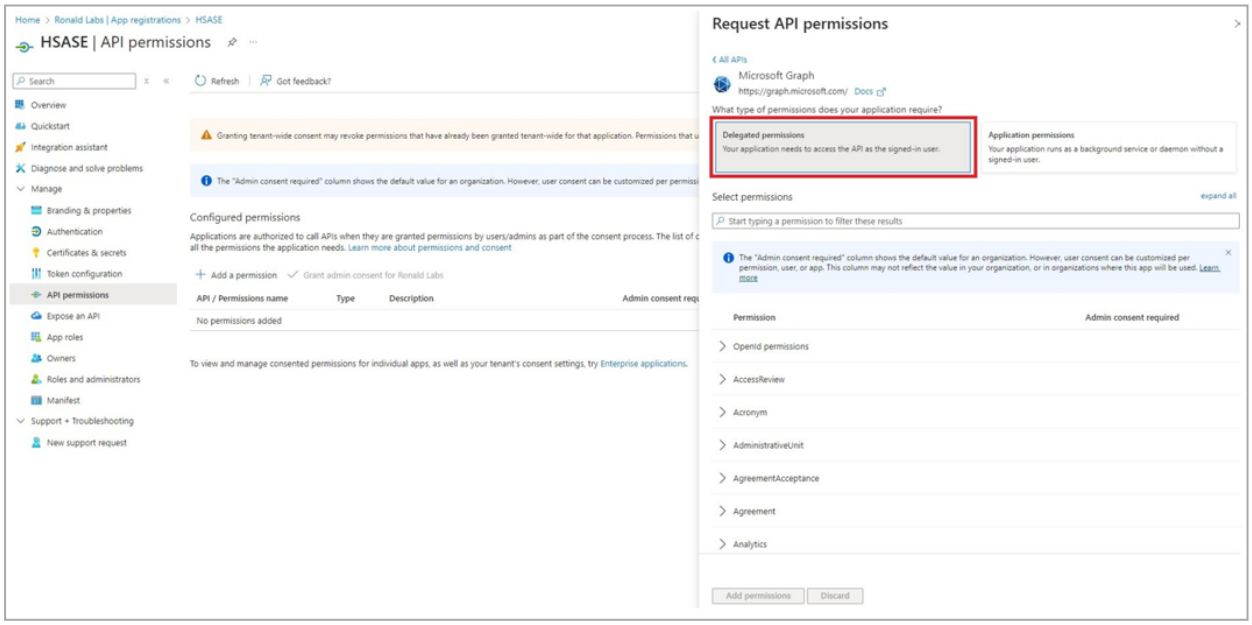
Step 2 - Configuring API Permissions

1. From the left panel, click **Manage** > **API permissions** and then click **Add a permission**.

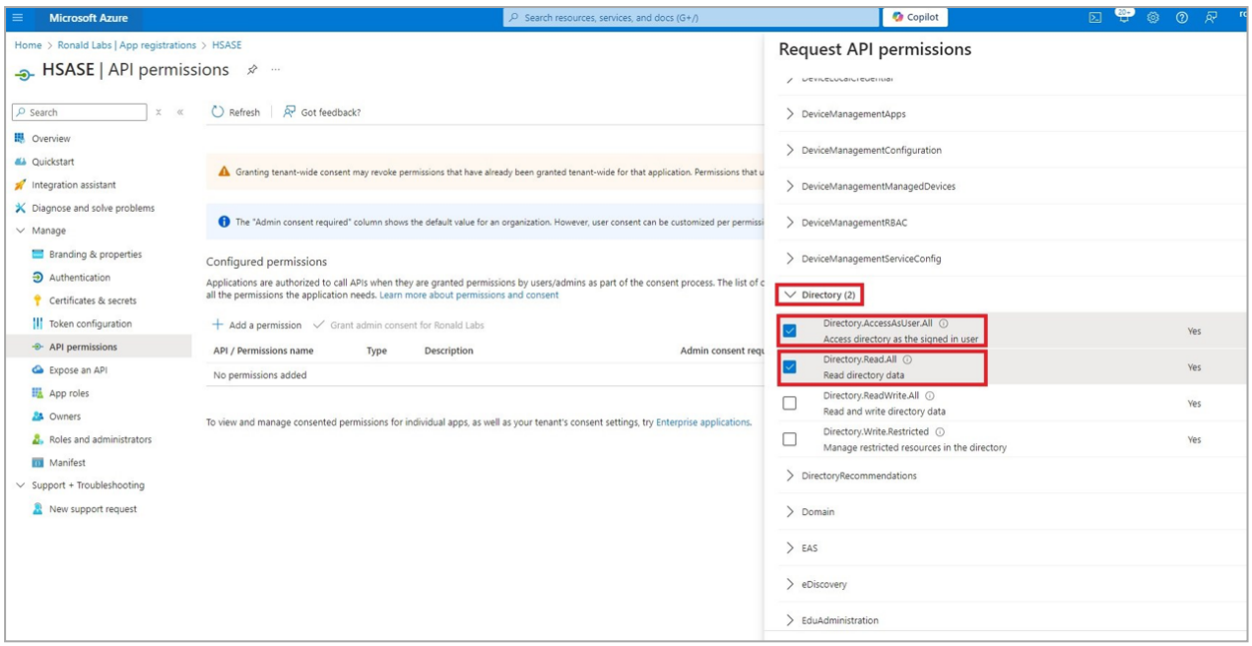


The **Request API permissions** panel appears to the right.

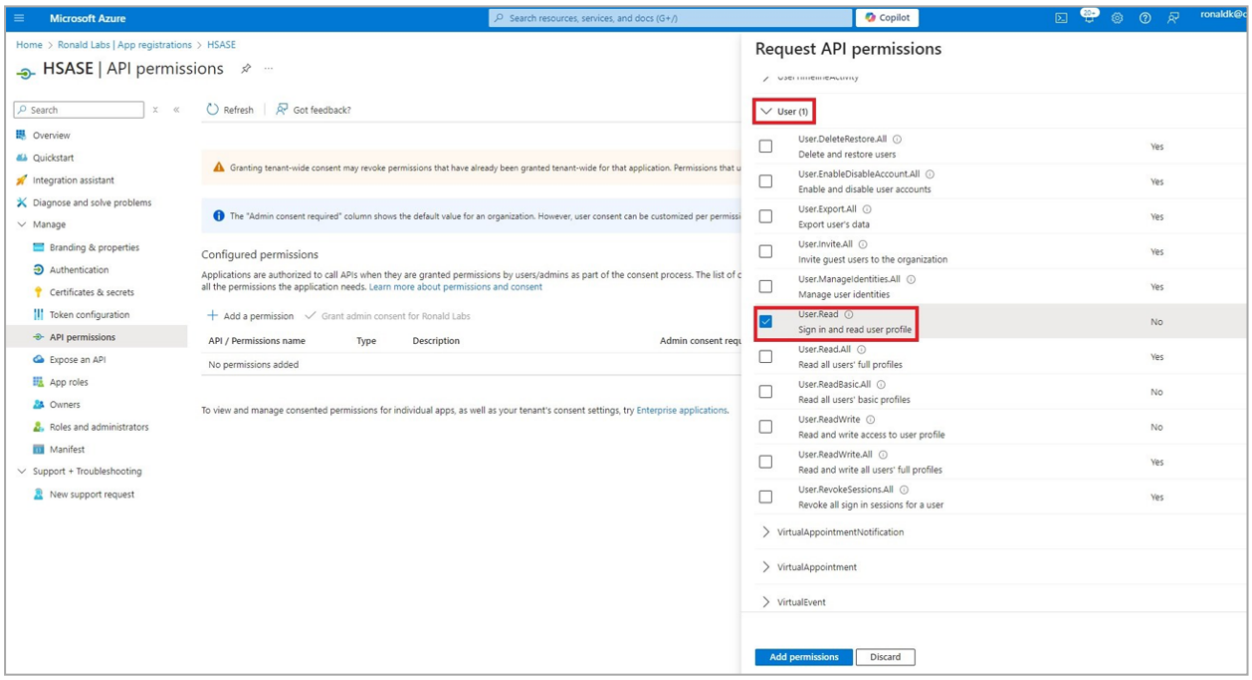
2. Select **Microsoft APIs** tab and then select **Microsoft Graph**.
3. Click **Delegated permissions**.



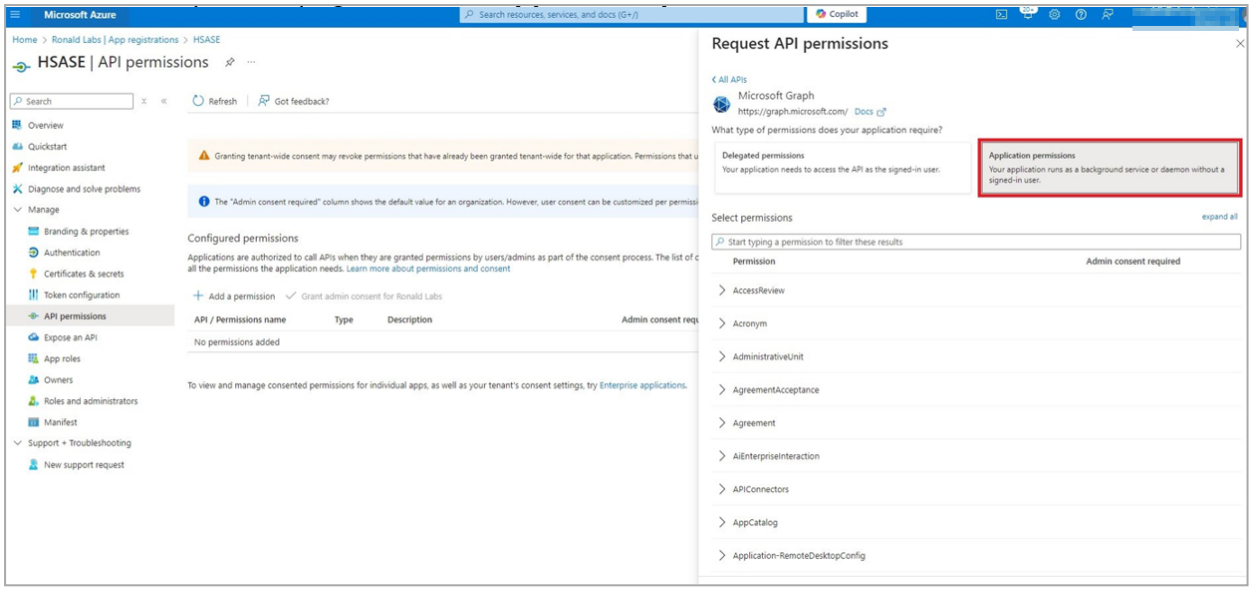
4. Click **Directory** to view the permissions and then select **Directory.Read.All**.



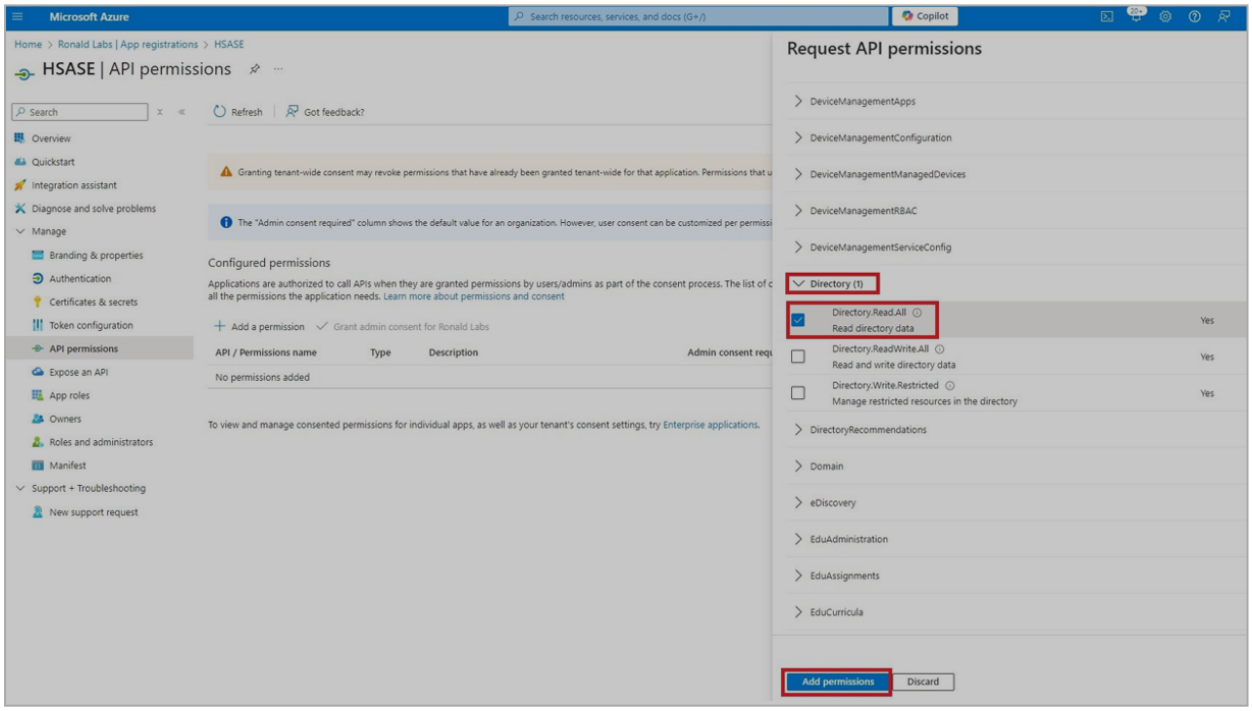
5. Click **User** to view the permissions and then select **User.Read.All**.



6. Scroll to the top of the page and click **Application permissions**.



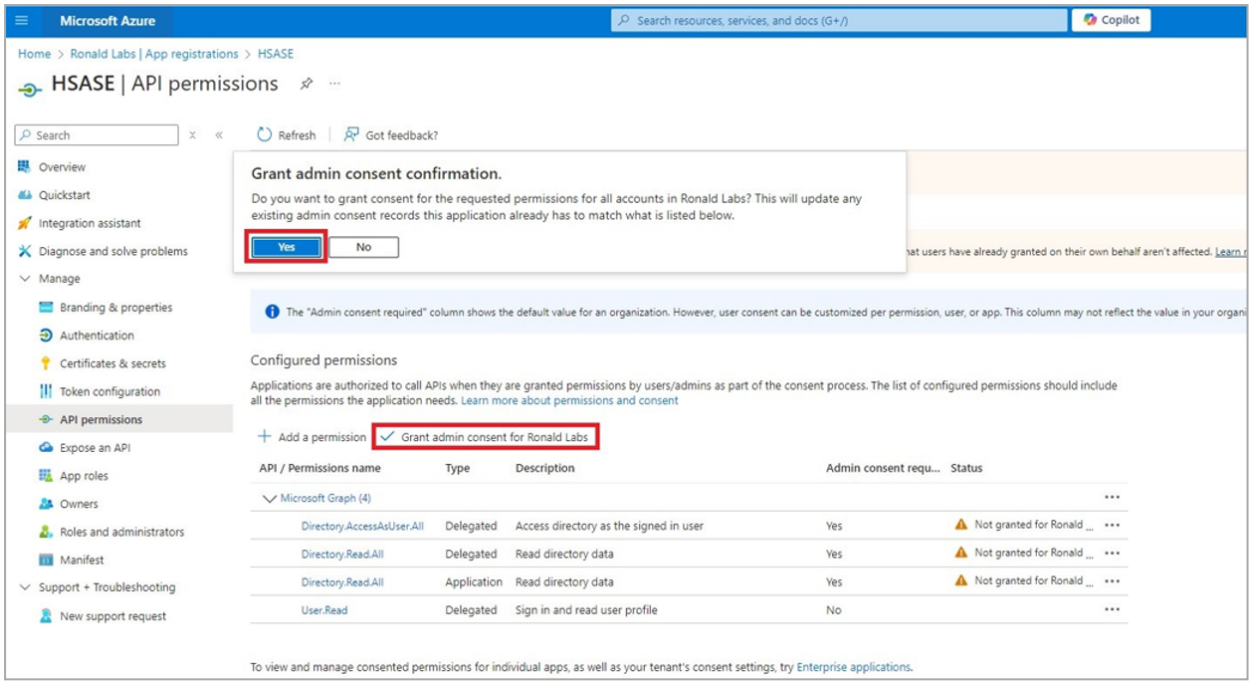
7. Click **Directory** to view the permissions and then select **Directory.Read.All**.
8. Scroll to the bottom of the page and click **Add permissions**.



9. Click **Grant admin**.

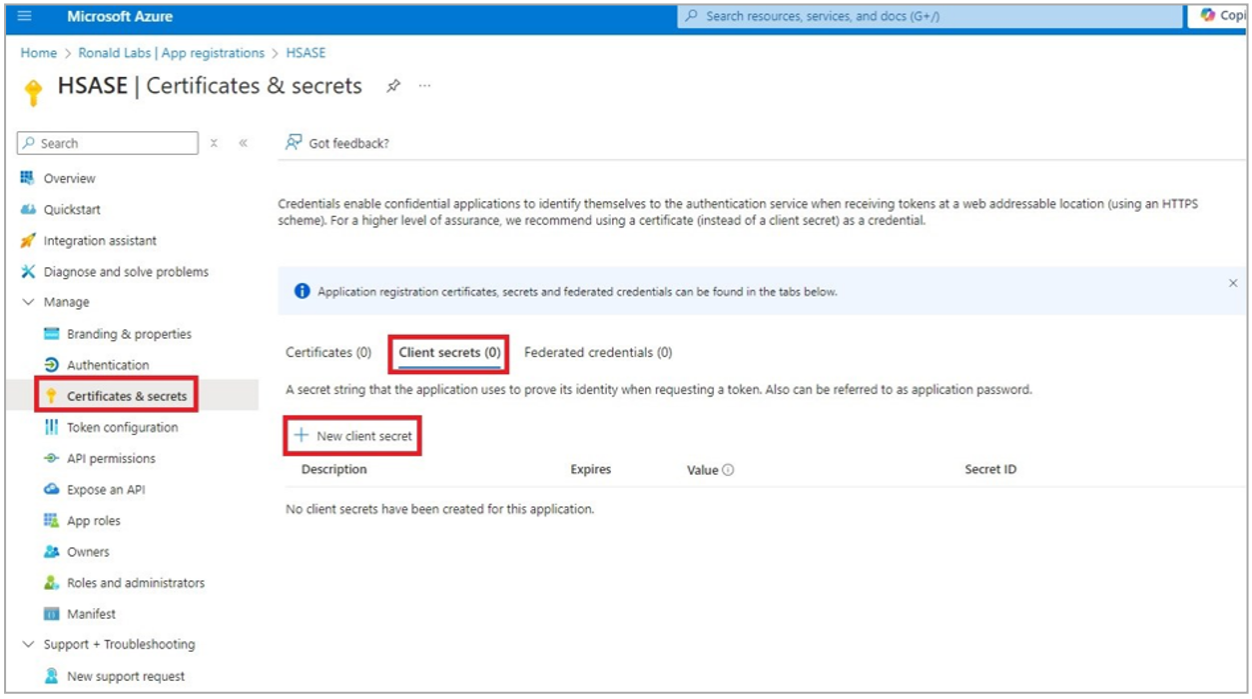
   The **Grant admin consent confirmation** window appears.

10. Click **Yes**.



Step 3 - Configuring Secret Key for the Application

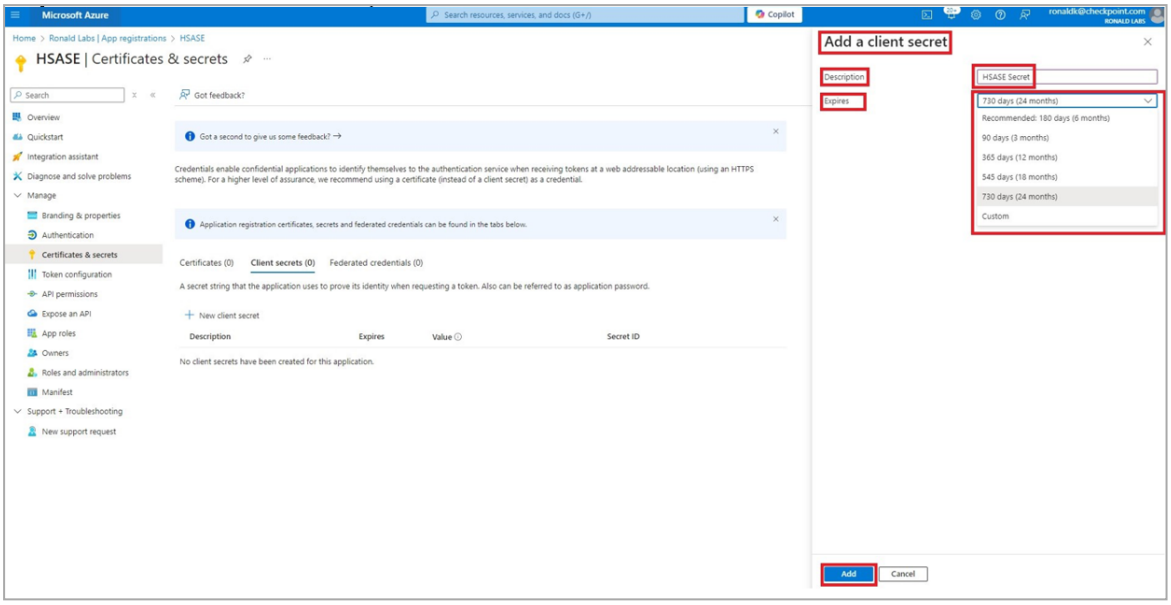
1. From the left panel, select **Certificates & secrets** and click the **Client secrets** tab.
2. Click **New client secret**.



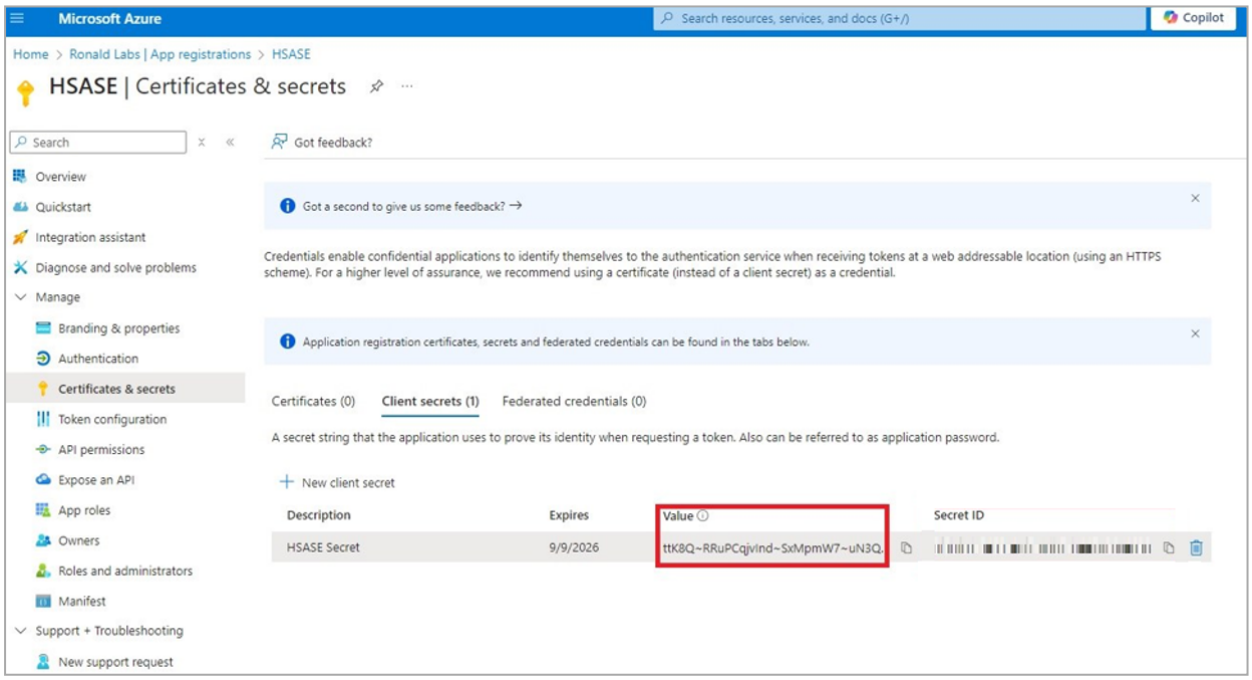
Note - You must use this client secret (password) as the Client Secret when connecting with the Harmony SASE IdP.

3. In the **Add a client secret** panel that appears on the right, specify these:

- **Description** - Enter a description.
- **Expires** - Select the secret expiration from the list.

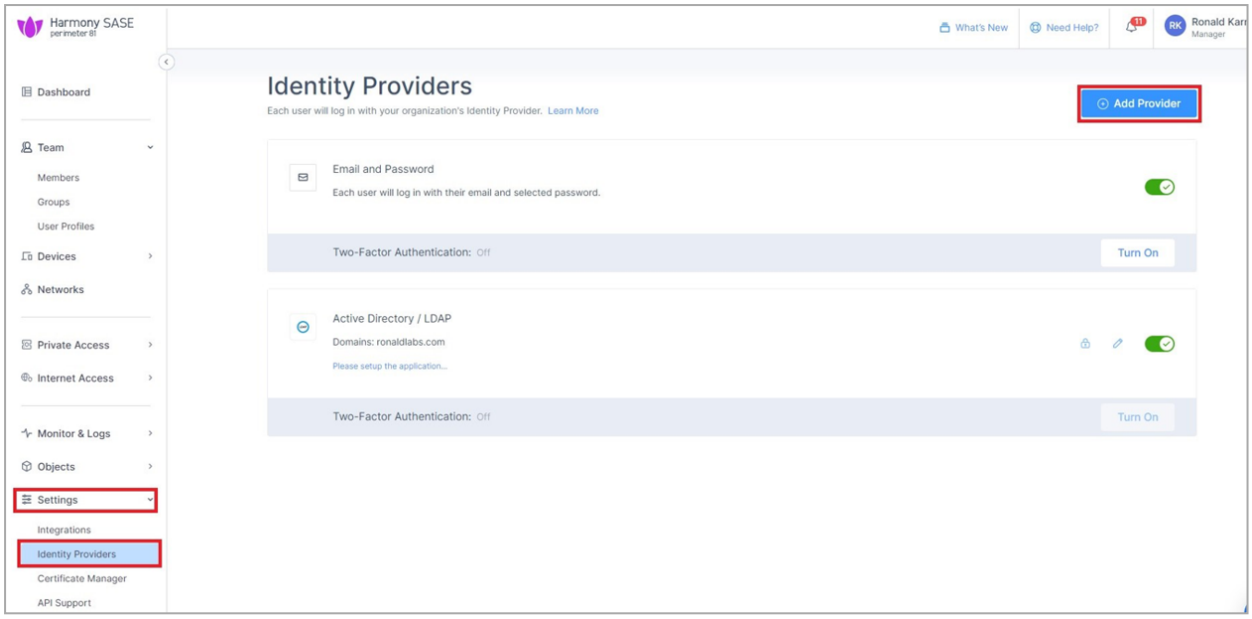


4. Click **Add**.
5. To copy the secret value, in the **Value** field, click ⧉.



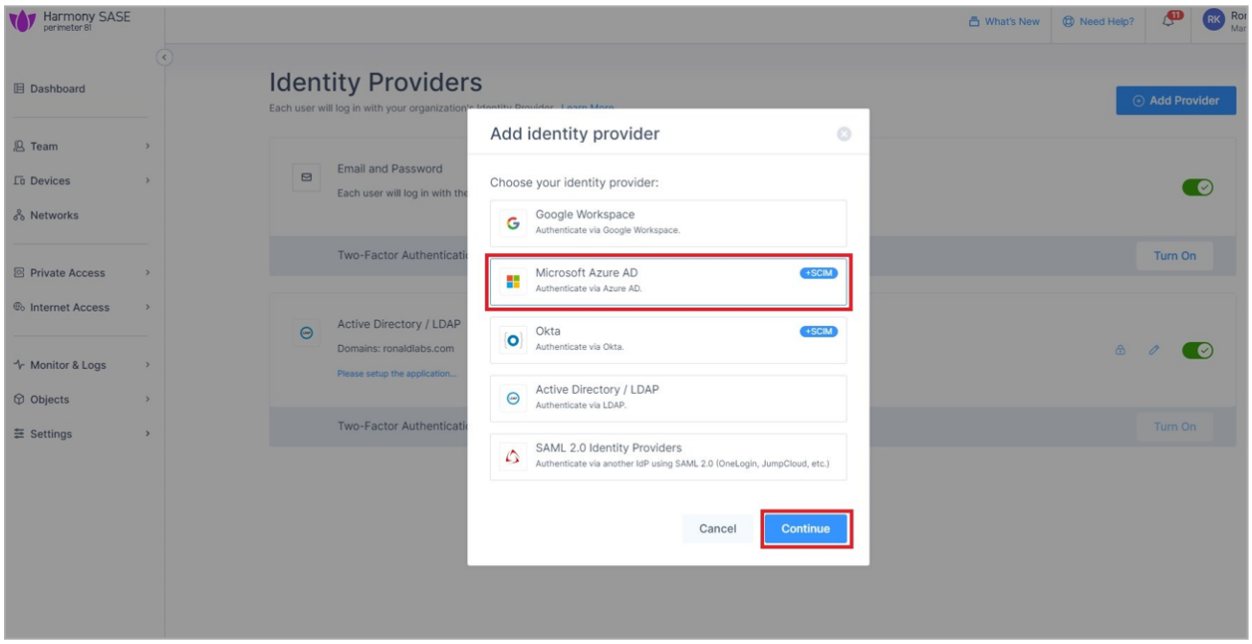
Part 2: Configuring Harmony SASE IDP

1. Access the Harmony SASE Administrator Portal.
2. Go to **Settings** > **Identity Providers**.
3. Click **Add Provider**.



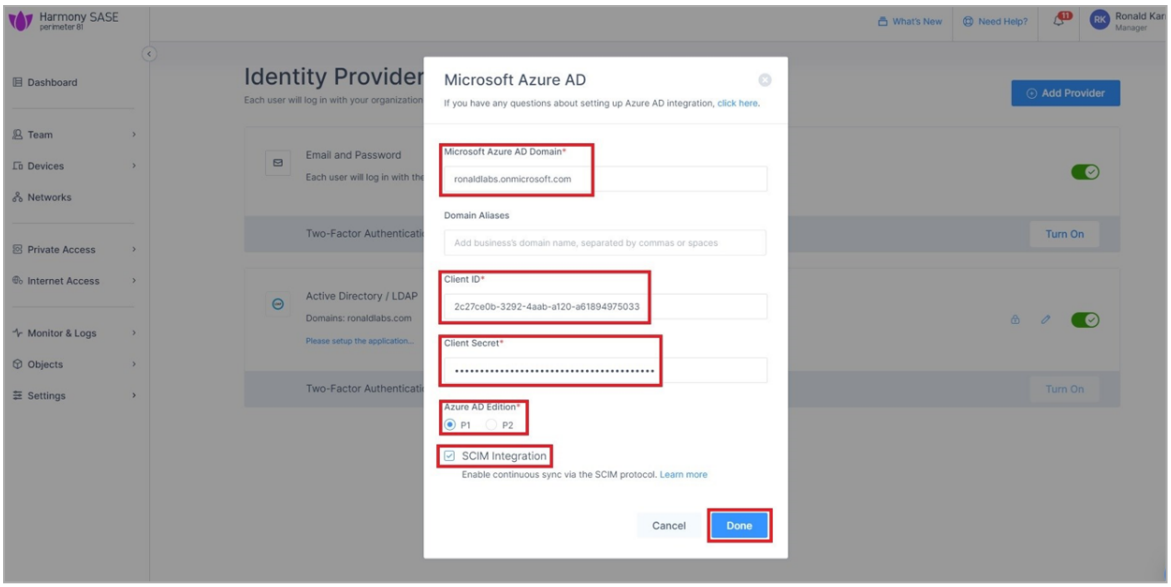
The **Add identity provider** window appears.

4. Select **Microsoft Azure AD** and click **Continue**.



5. Enter these details:
   - **Microsoft Azure AD Domain**
   - (Optional) **Domain Aliases**
   - **Client ID** (you copied while configuring the key)

- **Client Secret**



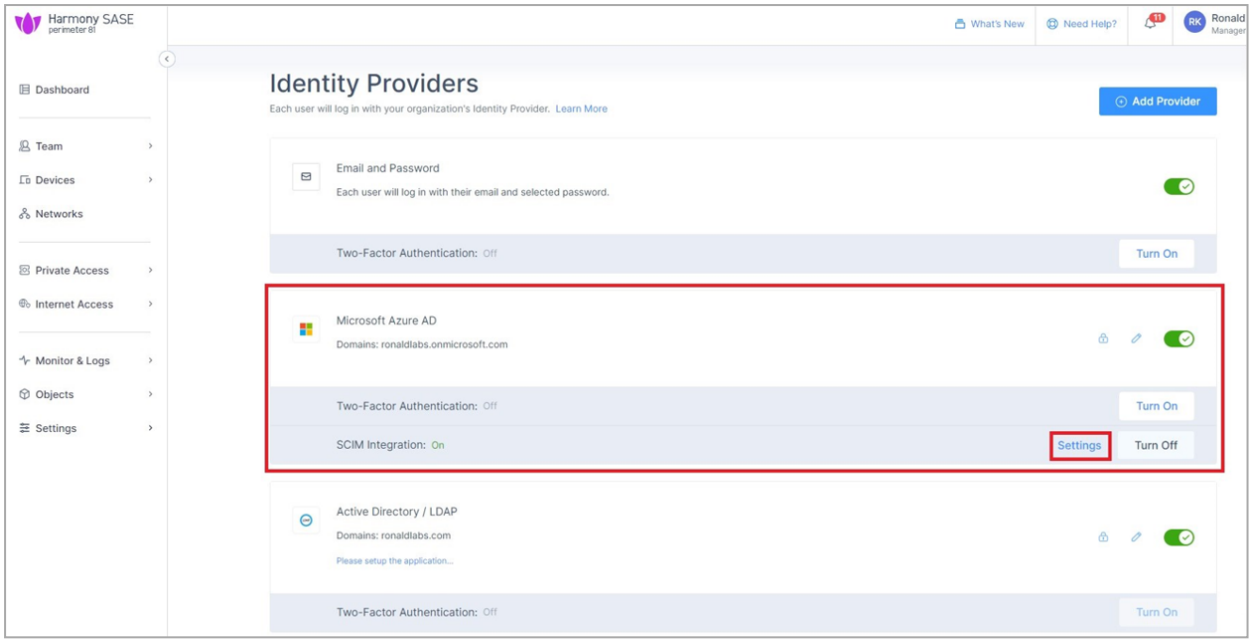
6. In the Azure AD Edition section, select your Azure premium type that you noted in step 4 of Step 1 - Creating an application in Entra ID:
   - **P1**
   - **P2**

   Note - If the license is **Entra Free**, select **P1** and the Part 3 - Configuring SCIM is not applicable as SCIM is not available.

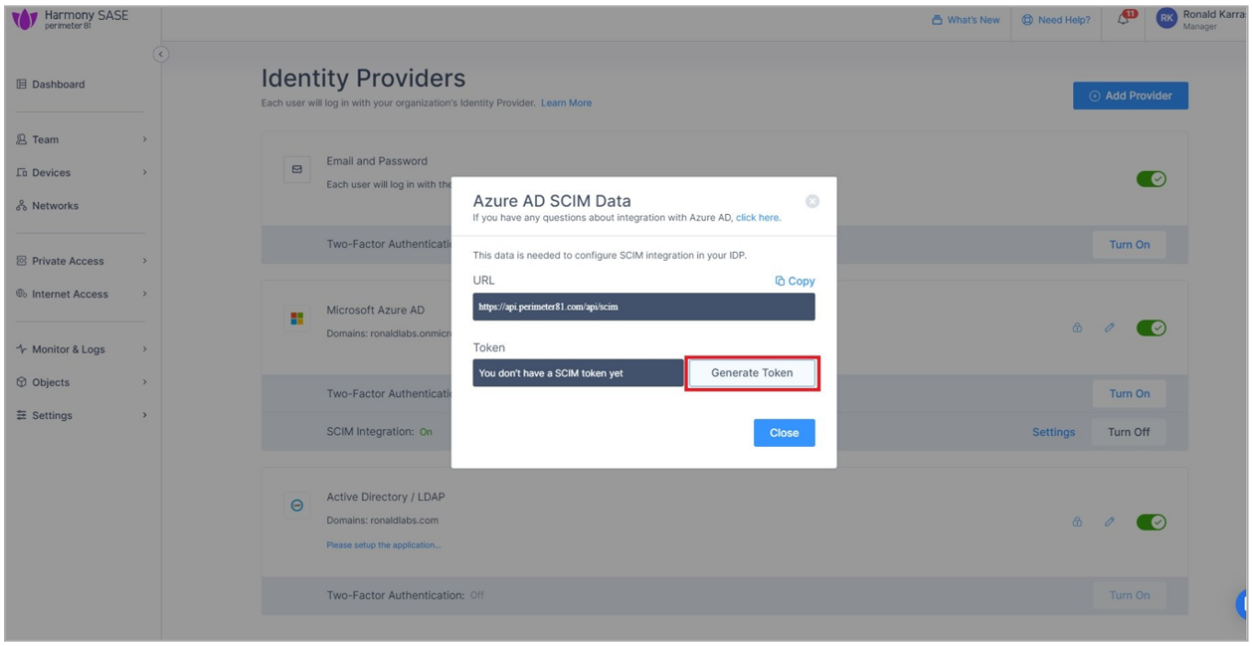
7. Select the **SCIM Integration** checkbox.
8. Click **Done**.

   The Azure AD gets created successfully.

9. In the **Microsoft Azure AD** section, click **Settings**.

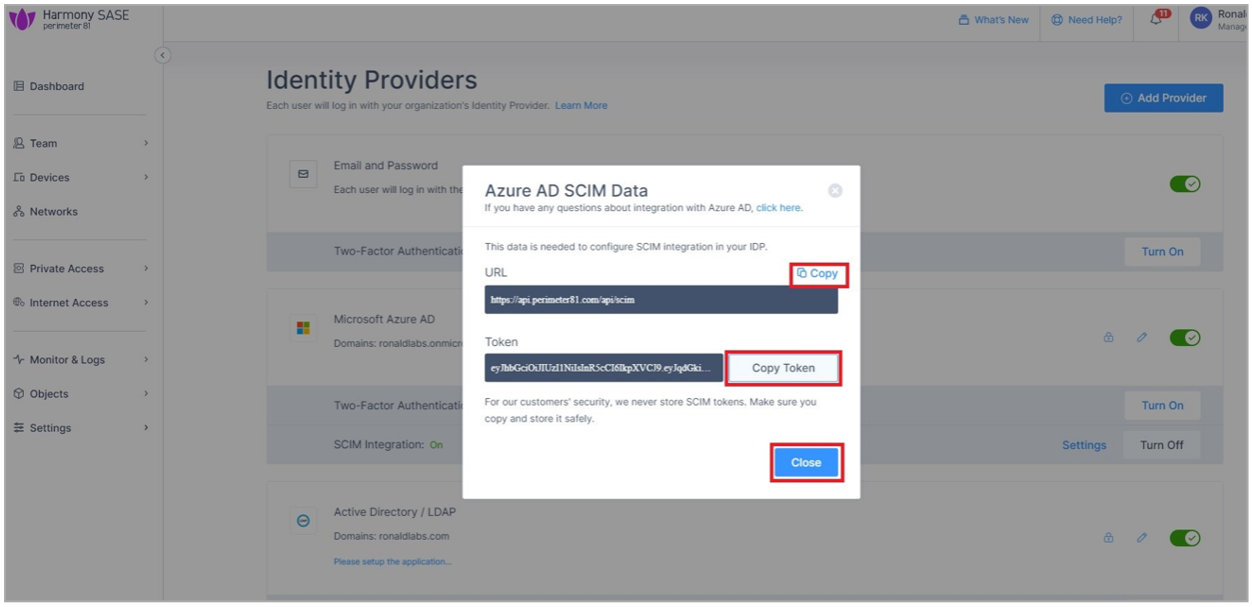


10. Click **Generate Token**.



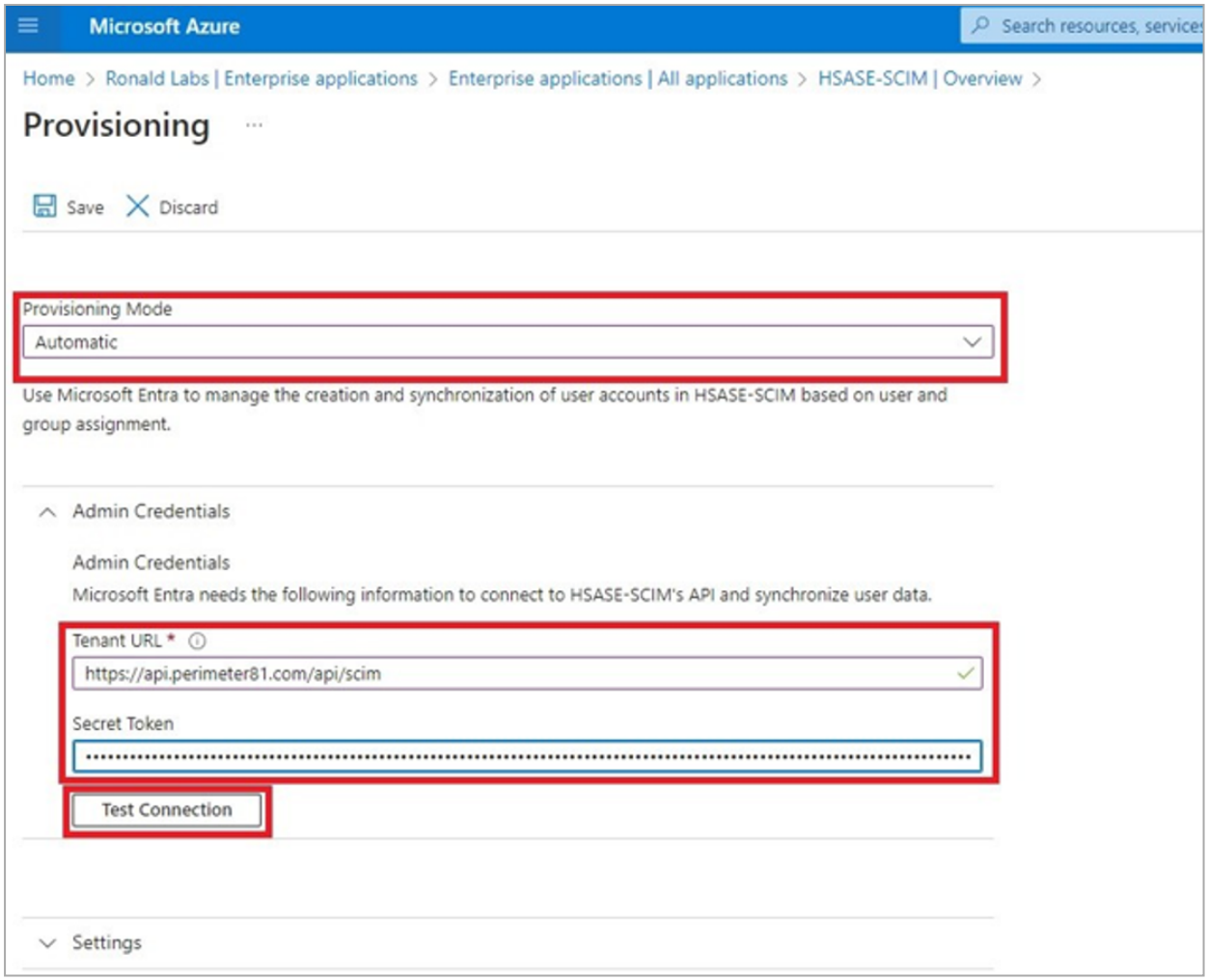
The **Azure AD SCIM Data** window appears.

11. Copy the URL and Token and then click **Close**.

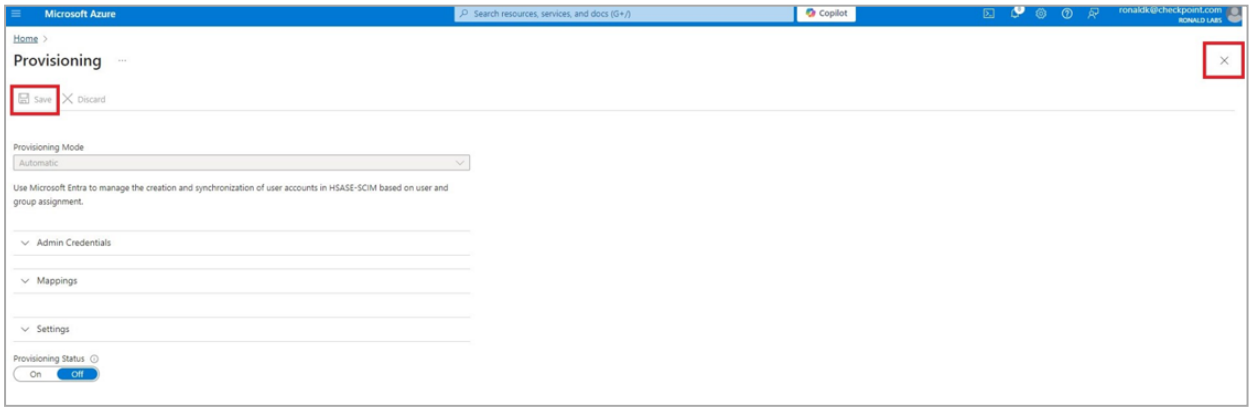


Part 3: Configuring SCIM

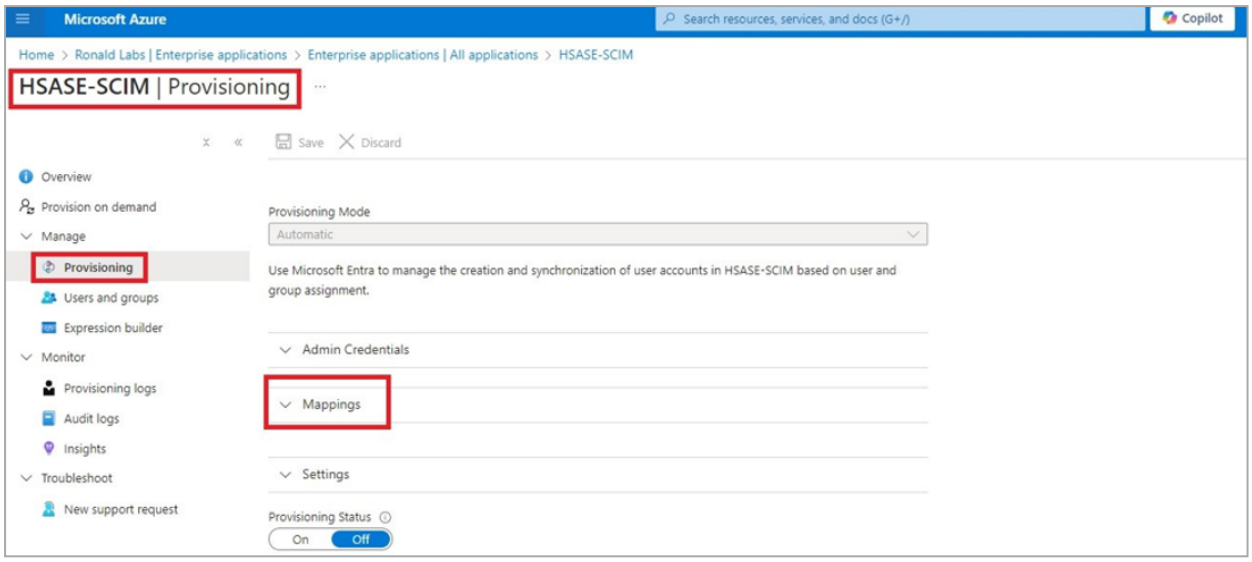
1. Access the Microsoft Azure Portal using administrator credentials.
2. Go to **Entra ID** > **Enterprise Applications** and locate the application previously created in [Step 1 - Creating an application in Entra ID](#).
3. Click the application name to open the configuration.
4. Click **Get Started** in the **Provision User Accounts** tile.
5. From the **Provisioning Mode** list, select **Automatic**.



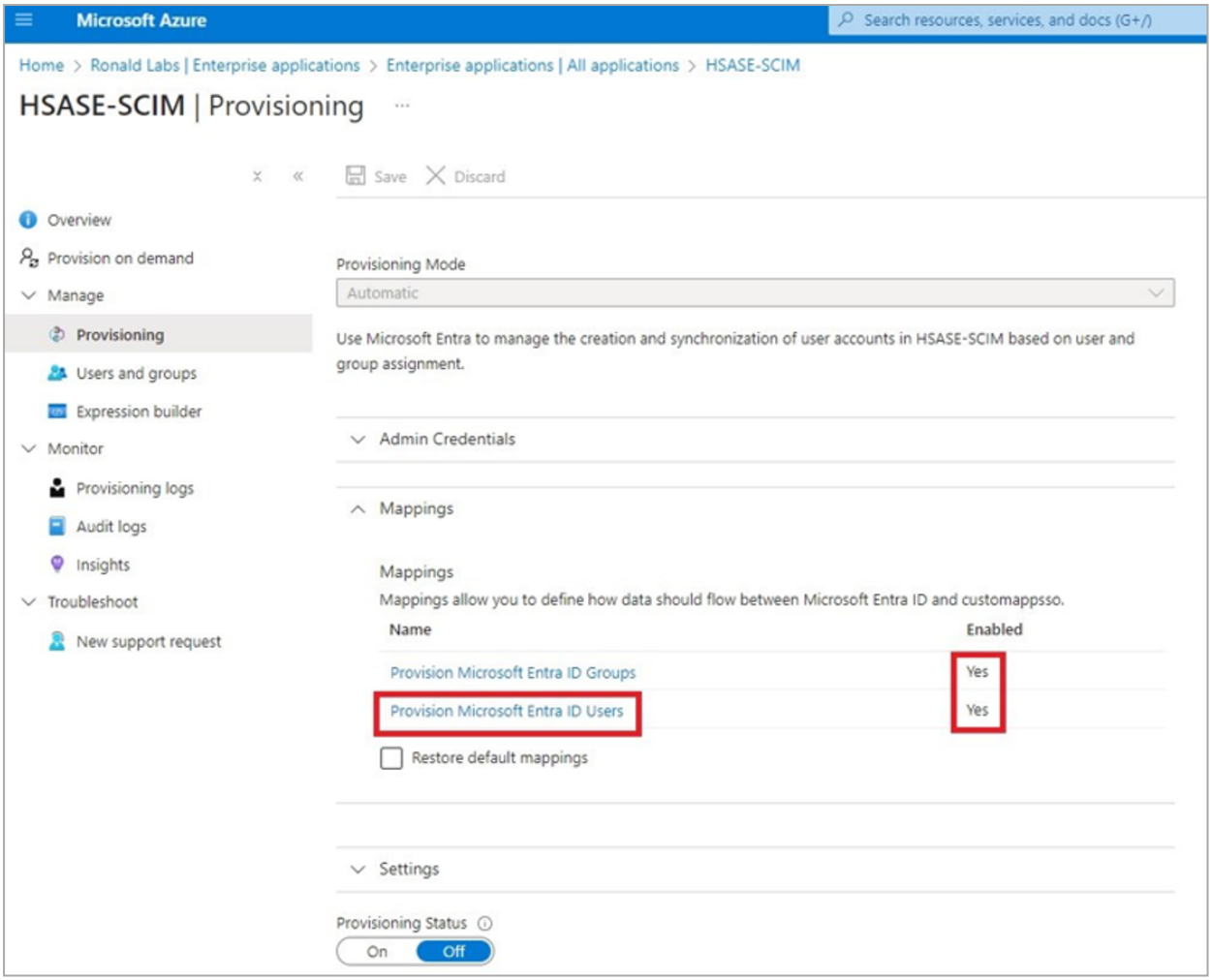
6. Expand **Admin Credentials**.
7. In the **Tenant URL** field, enter the SCIM URL.
8. In the **Secret Token** field, paste the token you copied in [Part 2: Configuring Harmony SASE IDP]() section **step 11**.
9. Click **Test Connection**.
10. Click **Save** at the top left corner.



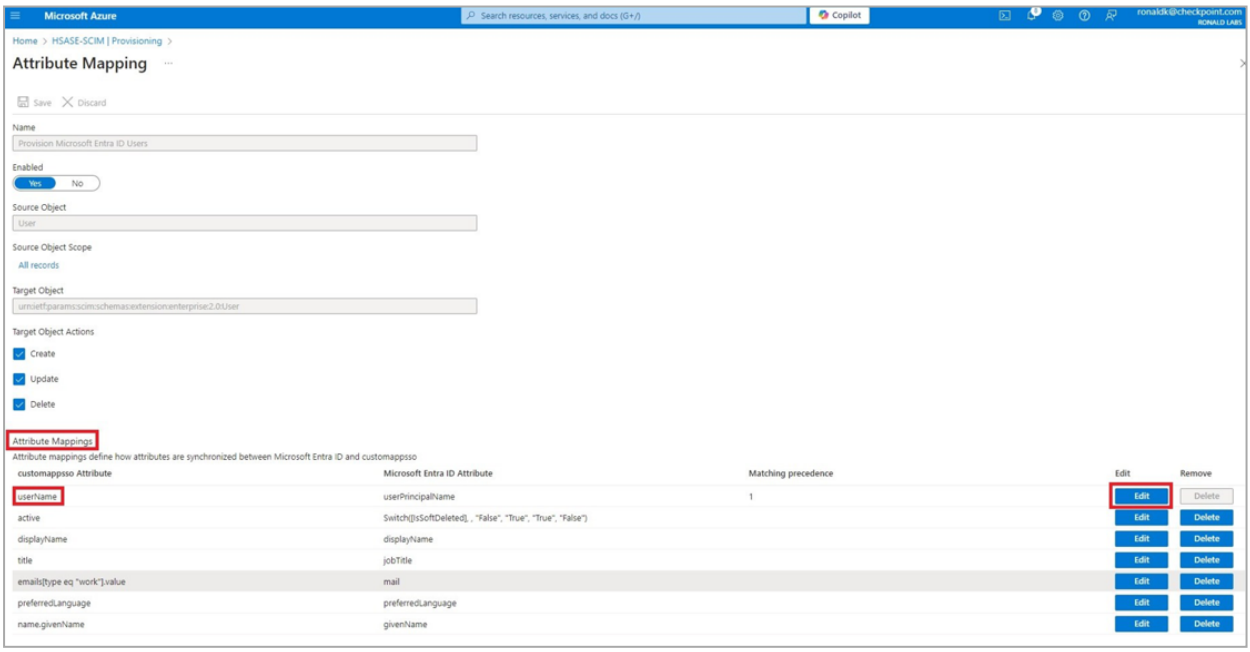
11. Expand **Mappings**.



12. Make sure that these options are enabled:
    a. **Provision Microsoft Entra ID Groups**
    b. **Provision Microsoft Entra ID Users**
13. Click **Provision Microsoft Entra ID Users**.

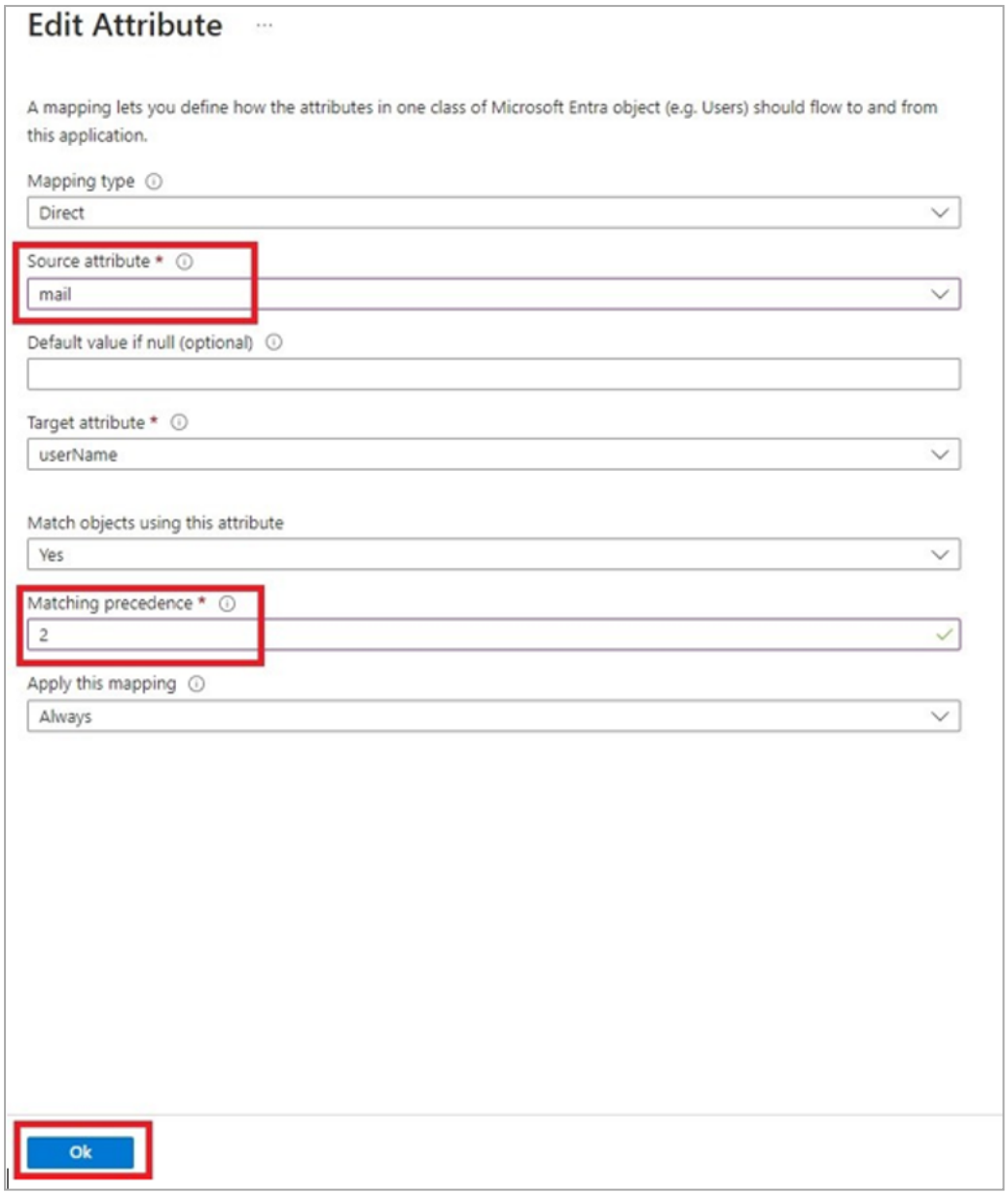


14. In the **Attribute Mappings** section, for **userName**, click **Edit**.

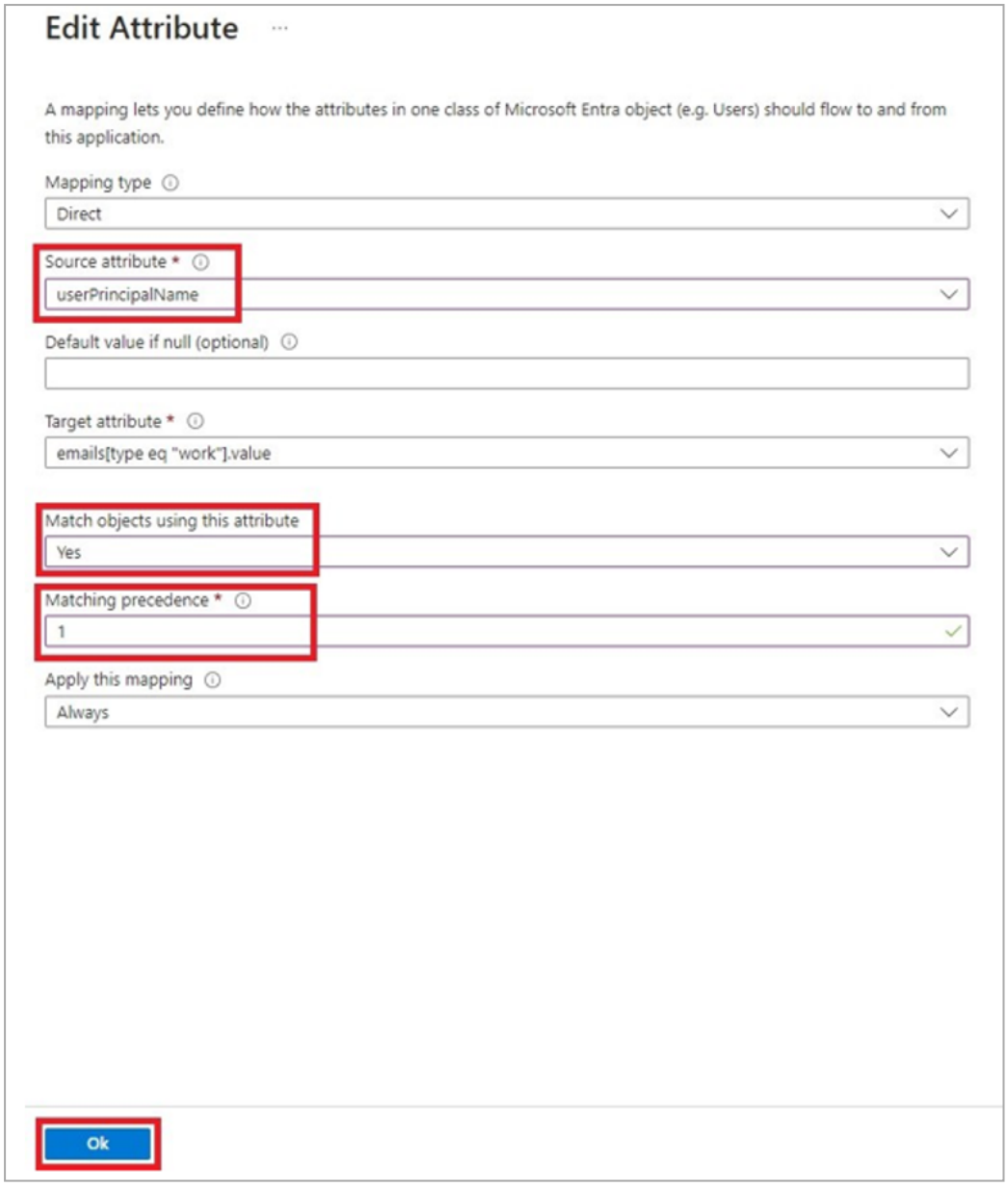


15. From the **Source attribute** list, select **mail**.

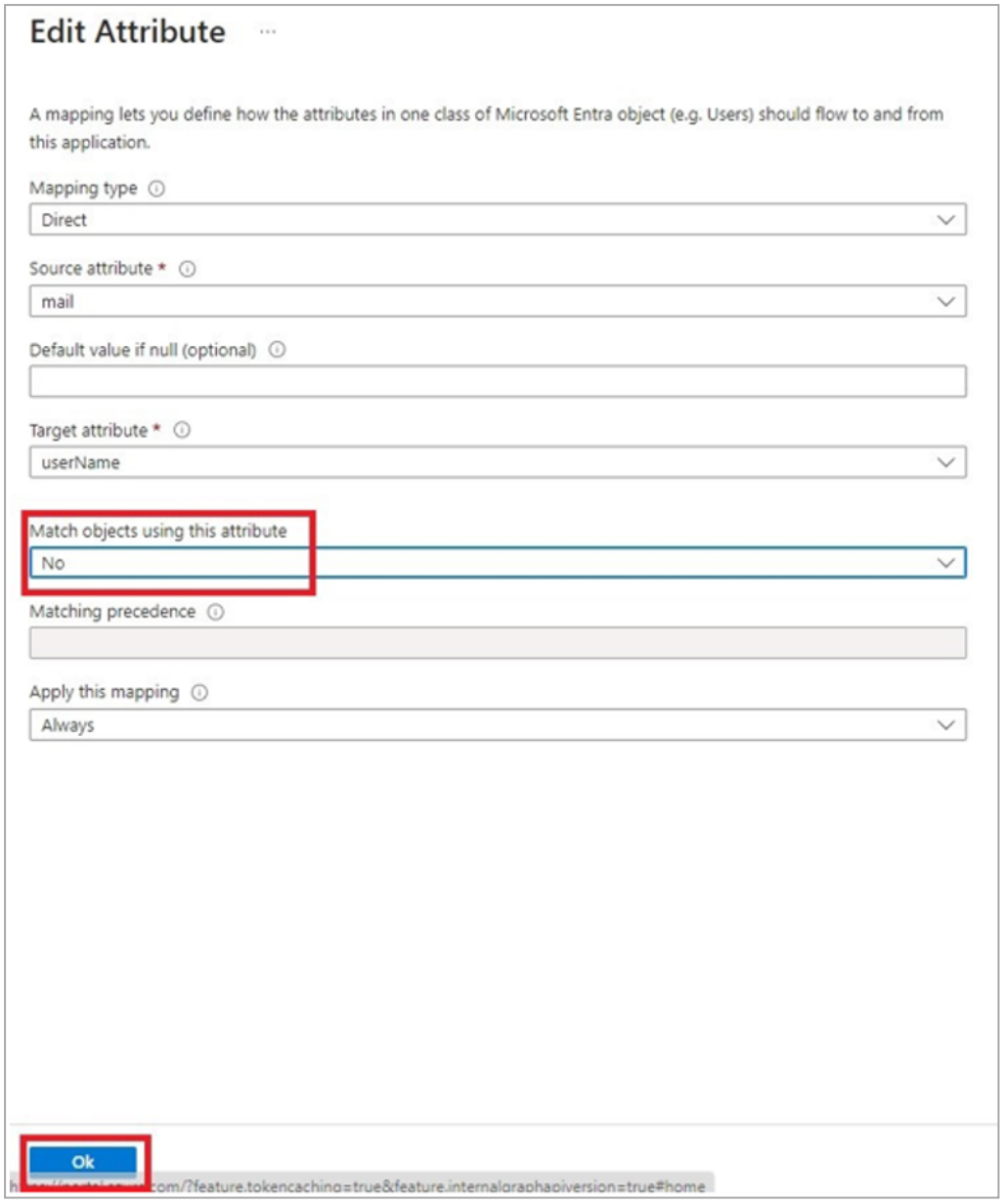
16. From the **Match precedence** list, select **2**.



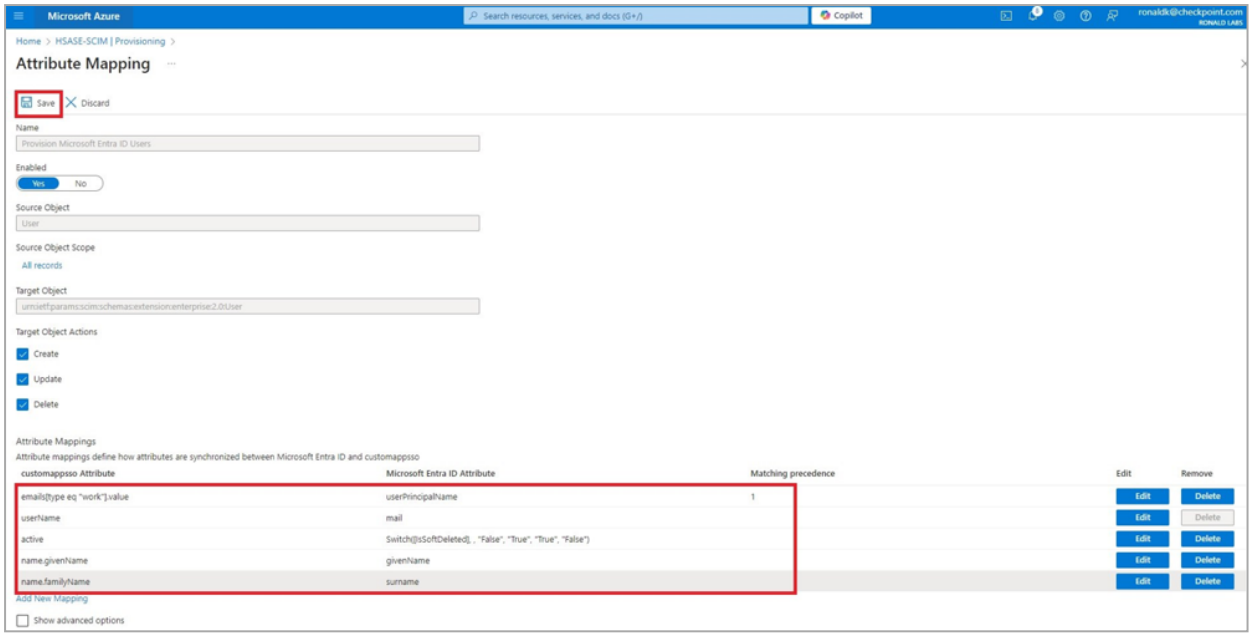
17. Click **OK**.
18. Locate the `emails[type eq "work"].value` attribute and click **Edit**.
19. From the **Source attribute** list, select **userPrincipalName**.
20. From the **Match objects using this attribute** list, select **Yes**.
21. From the **Matching precedence** list, select **1**.



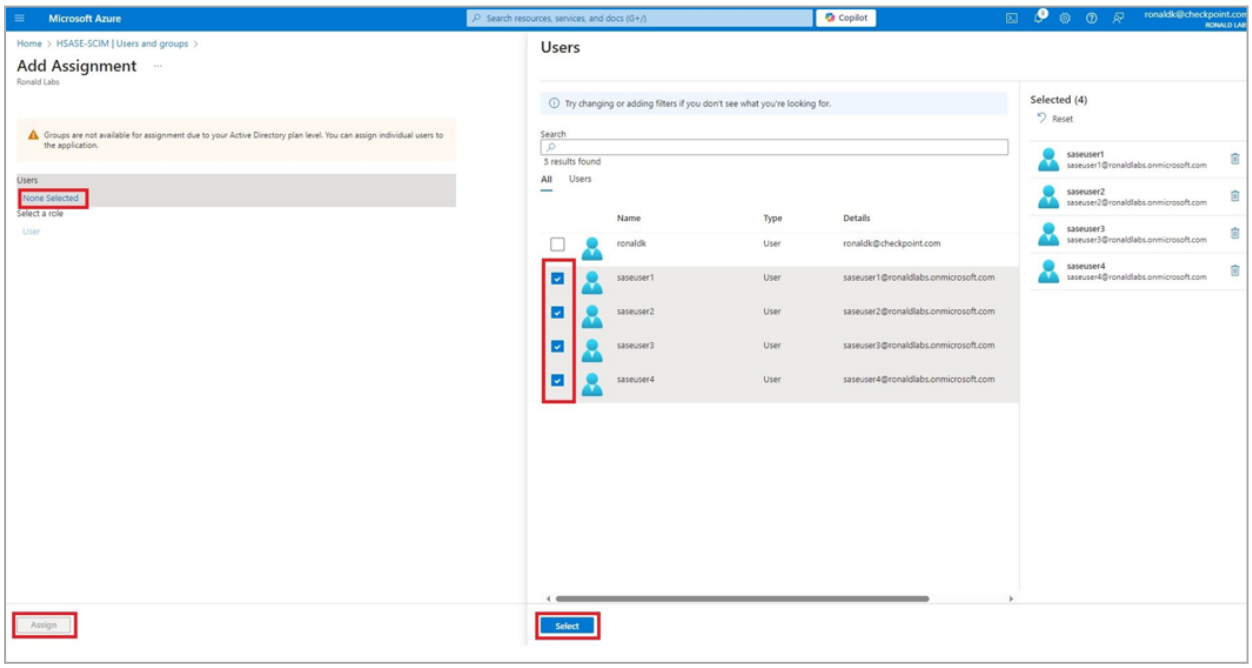
22. Click **OK**.
23. Go back to **Attribute Mappings** section and for **userName**, click **Edit**.
24. From the **Match objects using this attribute** list, select **No**.



25. Click **OK**.
26. Retain these attributes and delete other attributes:
    - `emails[type eq "work"].value`
    - `userNamemail`
    - `active`
    - `name.givenName`
    - `name.familyNamesurname`

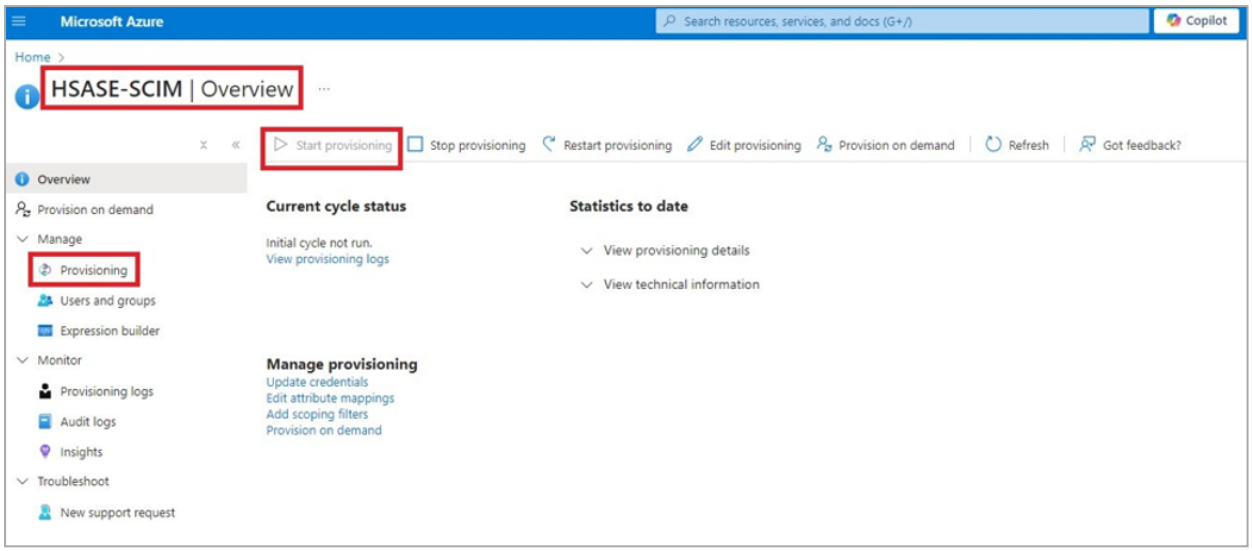


27. Click **Save**.
28. Go to SCIM Application and select **Users and groups**.
29. Click **Add users/group**.
30. In the **Users** section, click **None Selected**.
31. Select the user(s).
32. Click **Select** and then click **Assign**.



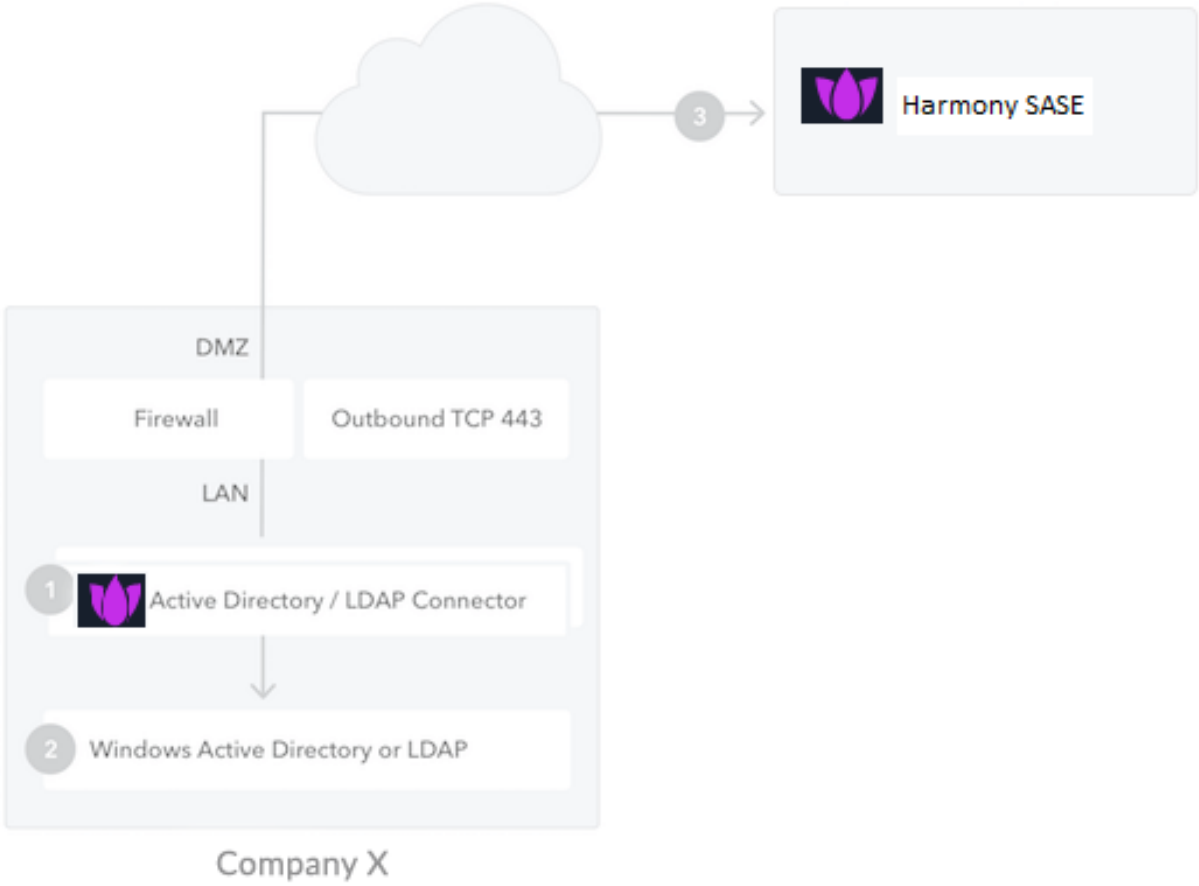
33. Go to the SCIM application.
34. Go to **Manage** > **Provisioning**.

35. Click **Start provisioning**.



On-Premises Active Directory

You can integrate Harmony SASE with Active Directory/LDAP through the Active Directory/LDAP connector installed on your network. The Active Directory/LDAP connector serves as a bridge between Active Directory and the Harmony SASE service.

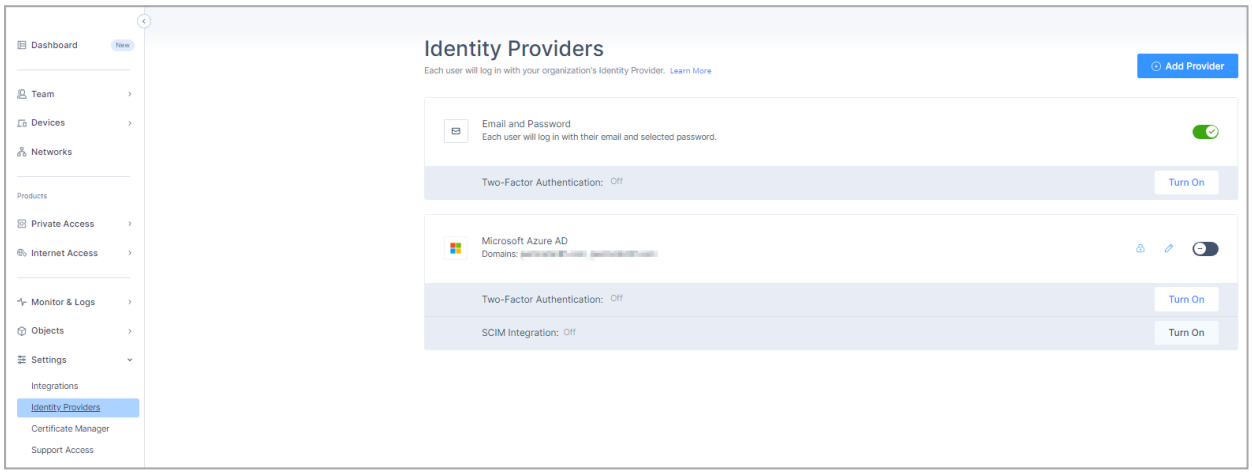


Note - For high availability and load balancing, you can install multiple instances of the connector. All connections are outbound from the connector to Harmony SASE Agent, so changes to your firewall are generally unnecessary.

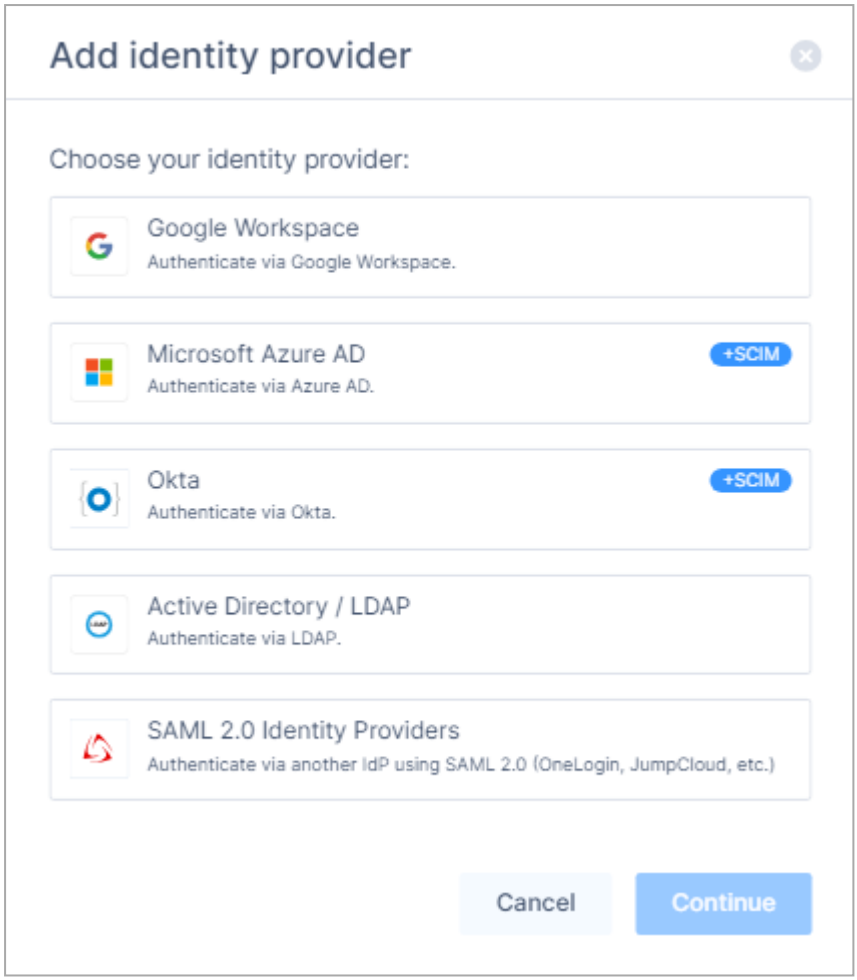
Enabling Active Directory/LDAP Connection

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Identity Providers**.

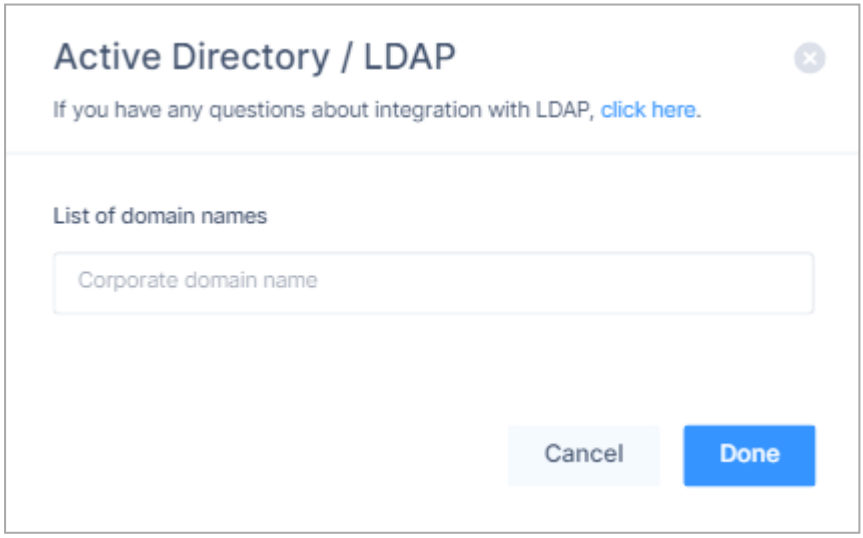
   The **Identity Providers** page opens.



2. Click **Add Provider**.



3. Select **Active Directory / LDAP**.
4. Click **Continue**.



5. In the **List of domains names** field, enter the domain name to allow log in to the Active Directory/LDAP connection. For example, `quantumsase.com`.
6. To find your domain name:

a. Open **Control Panel** on your computer.

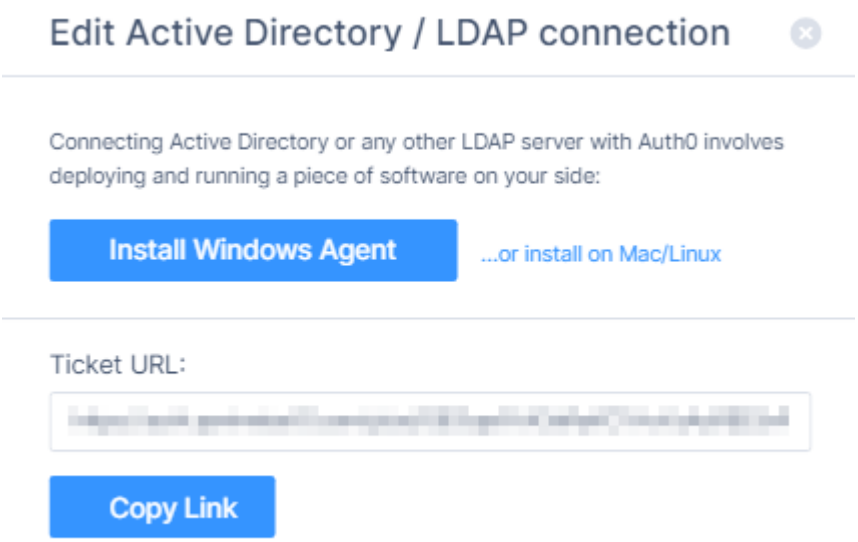
b. Go to **System and Security** > **System** > **Advanced system settings**.

   The **System Properties** window appears.

c. Go to the **Computer Name** tab to find your domain name.

7. Click **Done**.

   The **Edit Active Directory / LDAP connection** window appears.



8. To copy the **Ticket URL**, click **Copy Link**.

   This Ticket URL is required when you are linking to Harmony SASE.

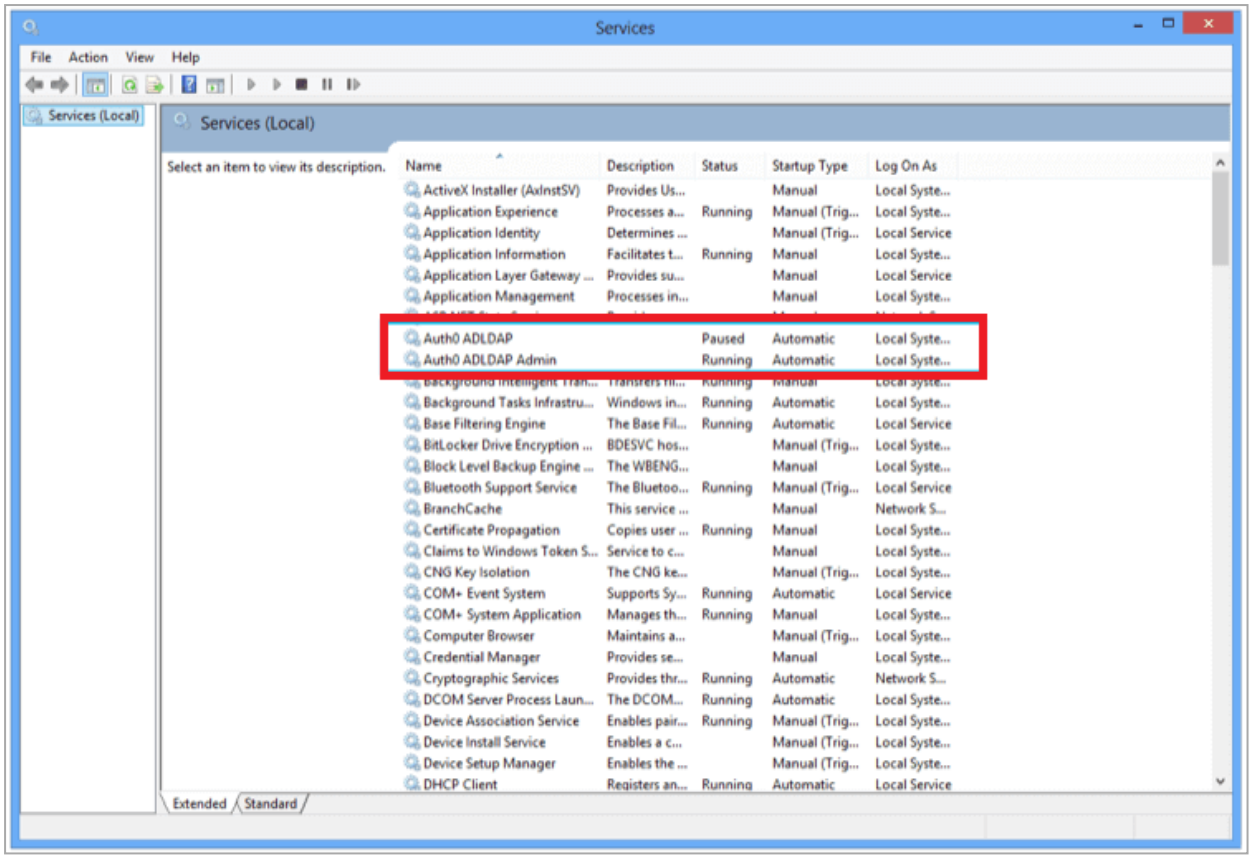
9. Click **Install Windows Agent** and follow the instruction to download the **Auth0 Active Directory/LDAP Connector for Windows** file, see Download the Installer.

   The MSI file gets downloaded.

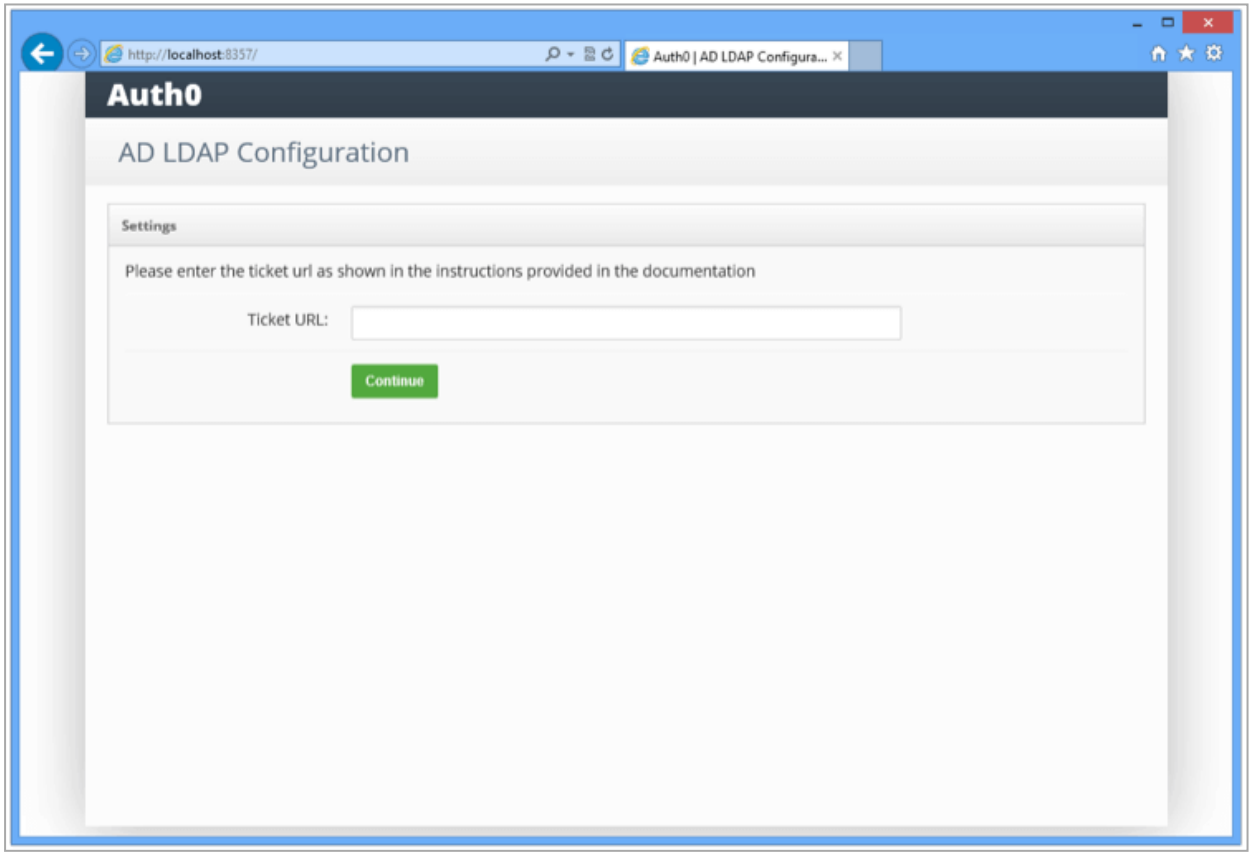
10. Locate the downloaded MSI file, run the installer, and follow the instructions.

Note - The Connector can be installed on an existing server, even a Domain Controller. However, more often it is installed on virtual machines provisioned just for the Connector.

The AD/LDAP connector is installed as a Windows Service.



The **Auth0** window appears, once the installation is complete.

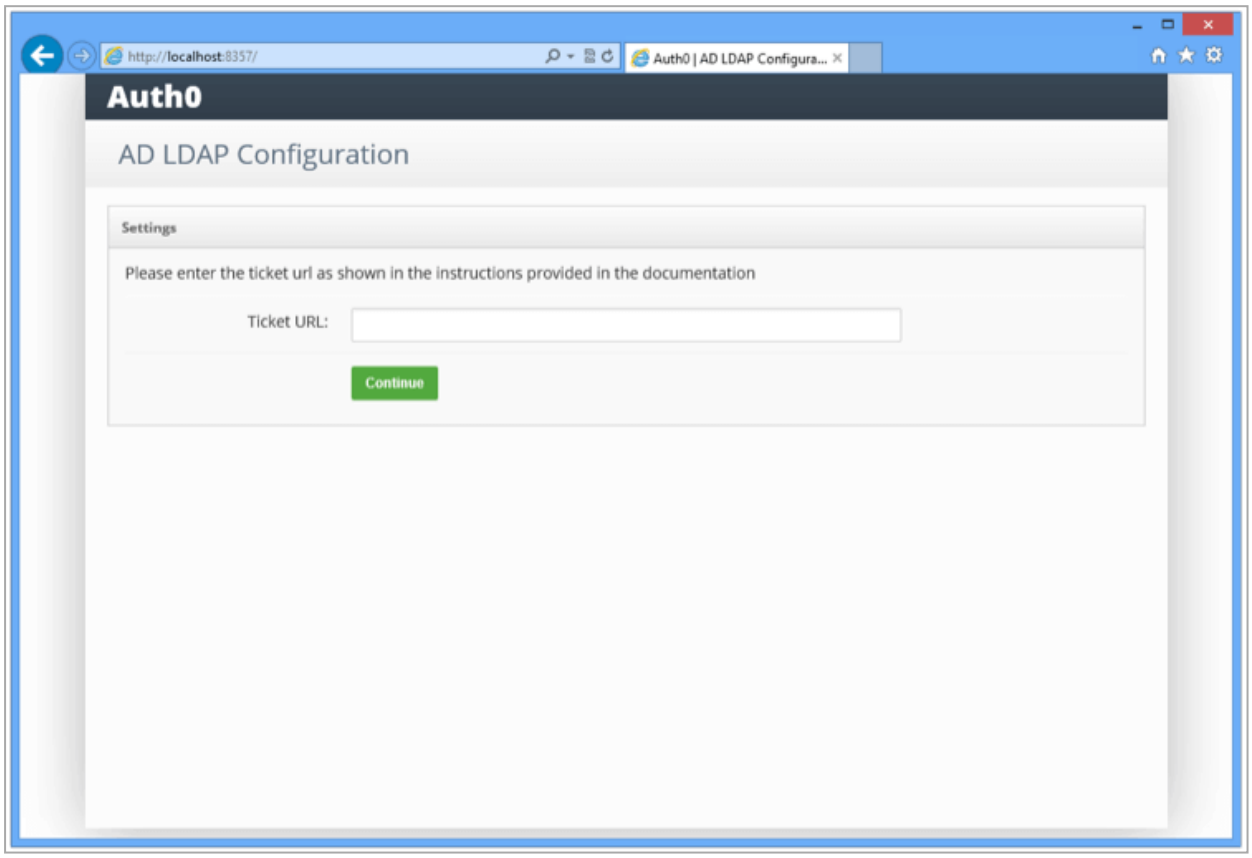


Link to Harmony SASE and LDAP

1. To link Harmony SASE:

   a. In the **Ticket URL** field, enter the URL. See step 8 in Enabling Active Directory/LDAP Connection.

   b. Click **Continue**.



   Note - If you receive an **Unable to get local issuer certificate** error message, set an environment variable `NODE_TLS_REJECT_UNAUTHORIZED` with value `0` in your windows system, and then restart the two Auth0 services. For more information, see Creating and Modifying Environment Variable in Windows.

2. To link LDAP, enter these:

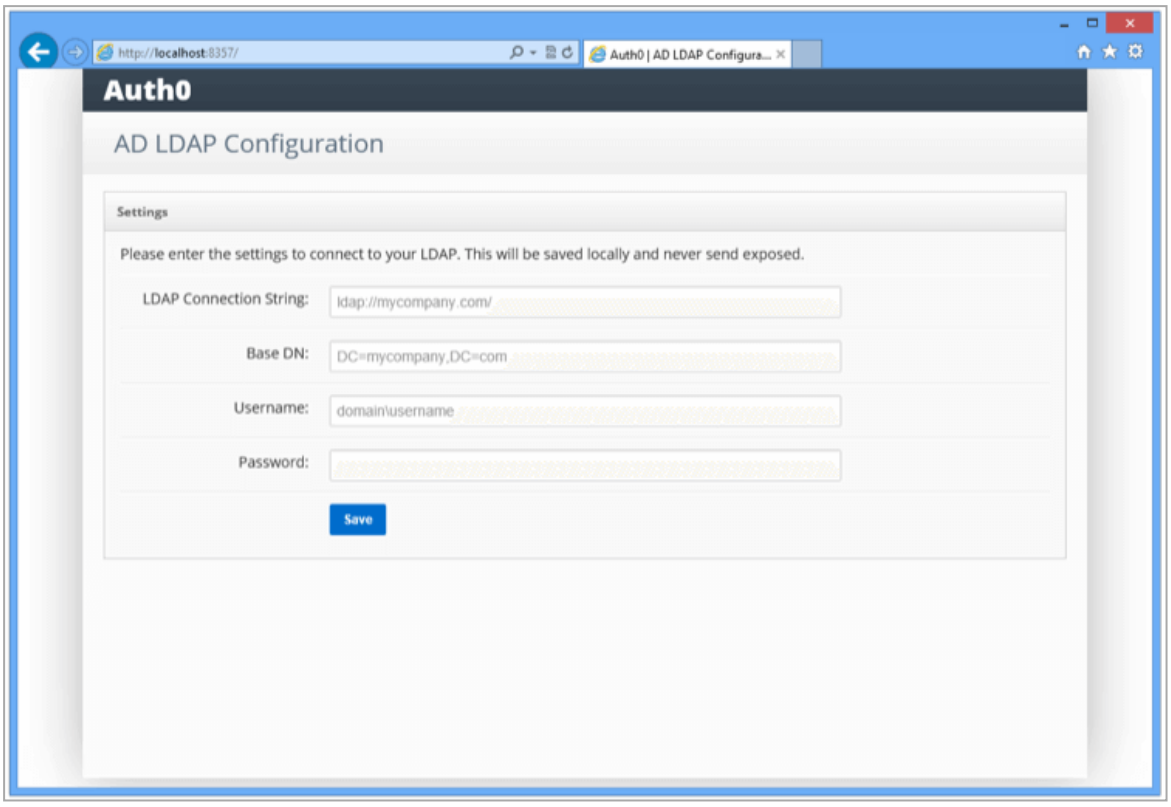
   a. **LDAP Connection String** - Domain name or IP address of your LDAP server. For example, `ldap://<my company>.com/`

      Note - Your LDAP server is the local domain controller where Active Directory is installed. The protocol can be either LDAP or LDAPS. To use LDAPS, make sure that the certificate is valid in the current server.

   b. **Base DN** - Base container for all the queries performed by the connector. For example, `dc=<my company>,dc=com`

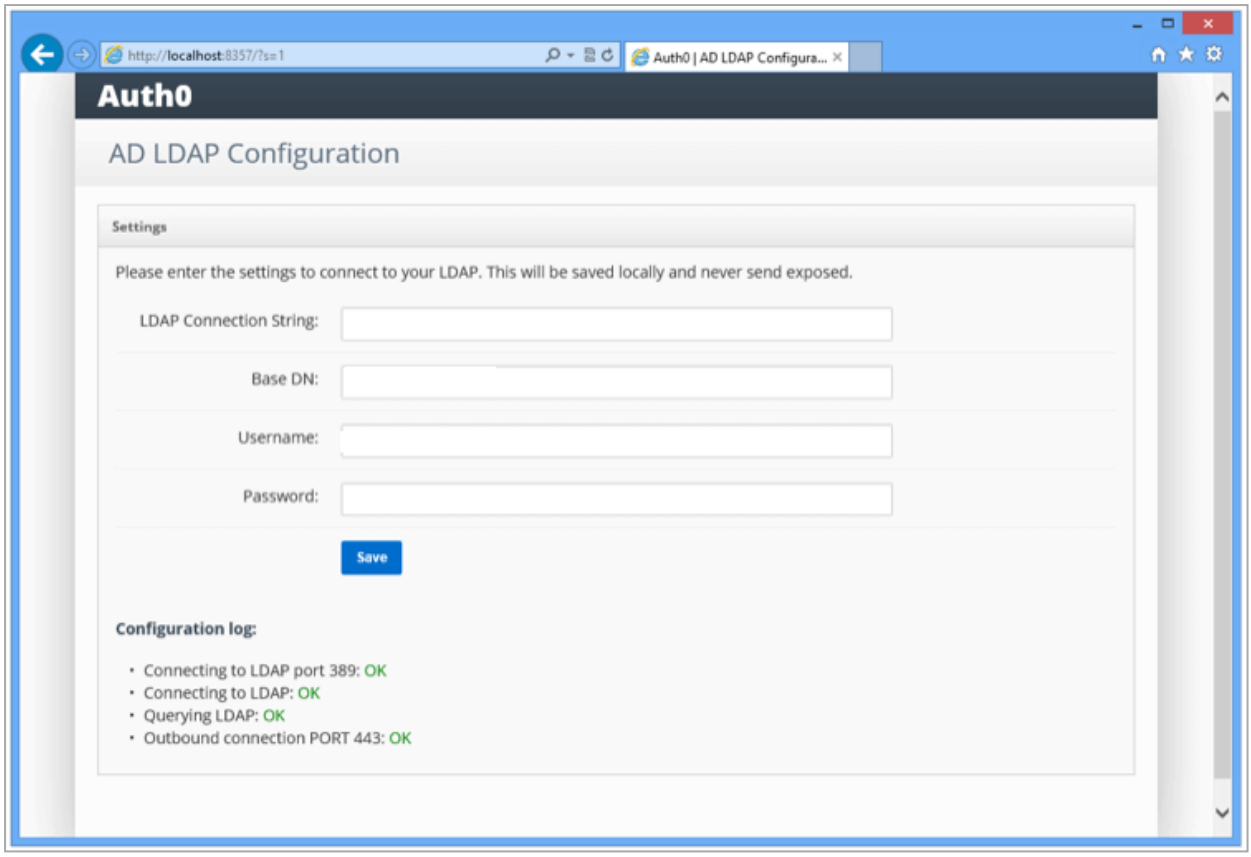
c. **Username** - Full name of the user with administrator rights to perform queries. For example, `cn=<domain name>,dc=<my company>,dc=com`

d. **Password** - Password of the user.



3. Click **Save**.

   The connector performs a series of tests. Make sure all tests result appear **OK**.



4. Find the AD/LDAP connector's config.json file in this location:

   C:\Program Files (x86)\Auth0\AD LDAP Connector

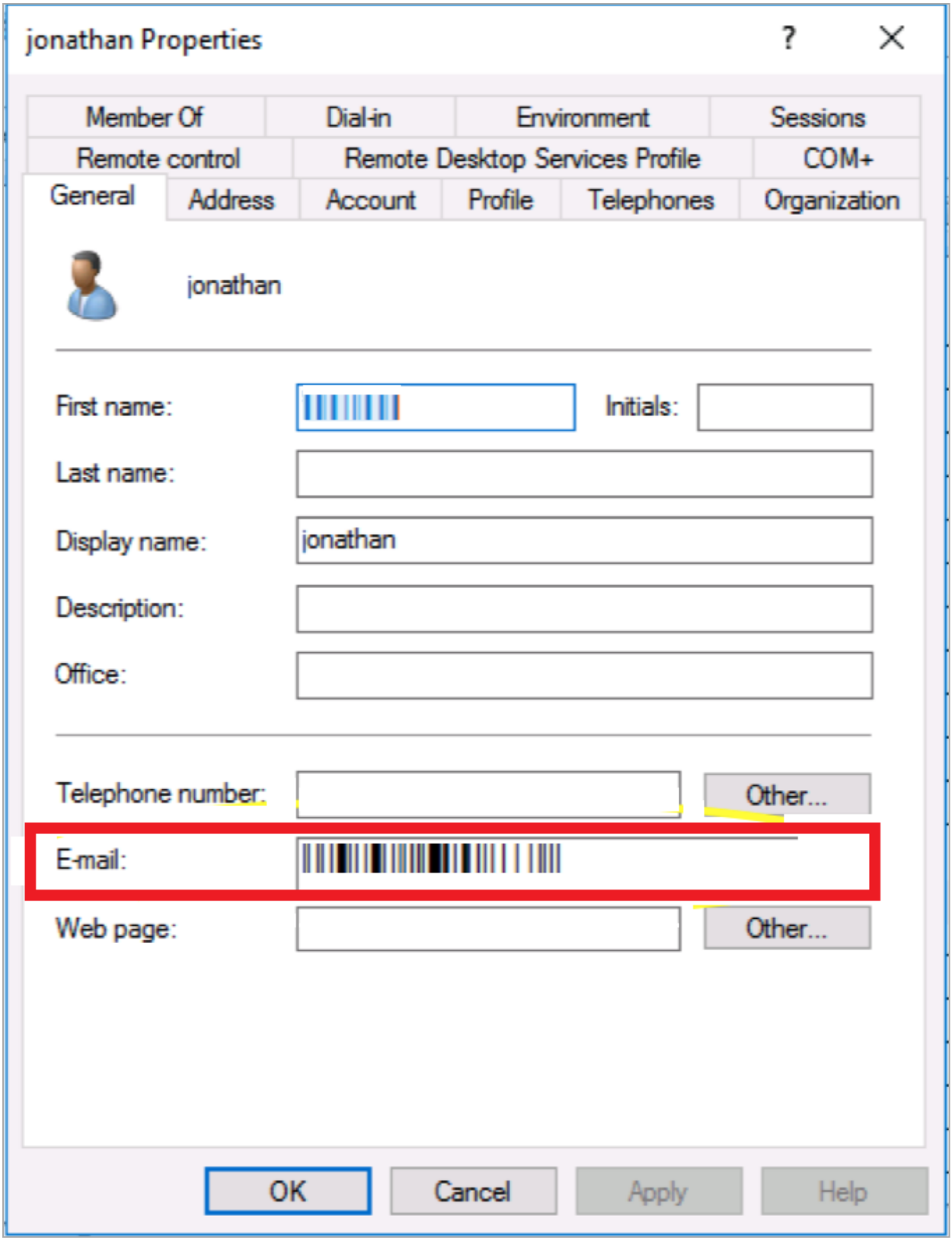
5. Open the config.json file in a text editor and add this after the second line:

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

File Edit Format View Help


```
{
  "PROVISIONING_TICKET": "https://auth.perimeter81.com/p/ad/EiFzIADC",
  "AD_HUB": "https://perimeter81.auth0.com/lo/hub",
  "LDAP_USER_BY_NAME": "(mail={0})",
  "LDAP_URL": "ldap://WIN-R26JB5G7KGS.test-p81.com",
  "LDAP_BASE": "DC=test-p81,DC=com",
  "LDAP_BIND_USER": "test-p81\\Administrator",
  "ENABLE_WRITE_BACK": false,
  "ENABLE_ACTIVE_DIRECTORY_UNICODE_PASSWORD": false,
  "PORT": 51241,
  "ANONYMOUS_SEARCH_ENABLED": false,
  "WSFED_ISSUER": "urn:perimeter81",
  "CONNECTION": "knowledgebase-ldap-nqzCRHHYx4",
  "REALM": "urn:auth0:perimeter81",
  "SITE_NAME": "knowledgebase-ldap-nqzCRHHYx4",
  "urn:auth0:perimeter81": "https://auth.perimeter81.com/login/callback",
  "LDAP_BIND_CREDENTIALS": "cf7c0a890804133c6df87d2288d193e4",
  "SERVER_URL": "http://WIN-R26JB5G7KGS:51241",
  "LAST_SENT_THUMBPRINT": "d52a7872a66d51d6487559d0833591a206f8b738",
  "TENANT_SIGNING_KEY": "-----BEGIN CERTIFICATE-----\r\nMIIDBTCCAe2gAwIBAgIJMU6R3v5TbHzVMA0GCSqG
7S4dIaEX/57ZWxBYPhHVkHuBRTUDRE4cz/qhOxb7plK776L0\r\npMcrdp0sjExezhkImauO38fMlQdnjfPCwJD3Z2kI9IMW
}
```


6. Go to **File** and then click **Save** to save the config.json file.
7. Go to **Properties** > **General**.

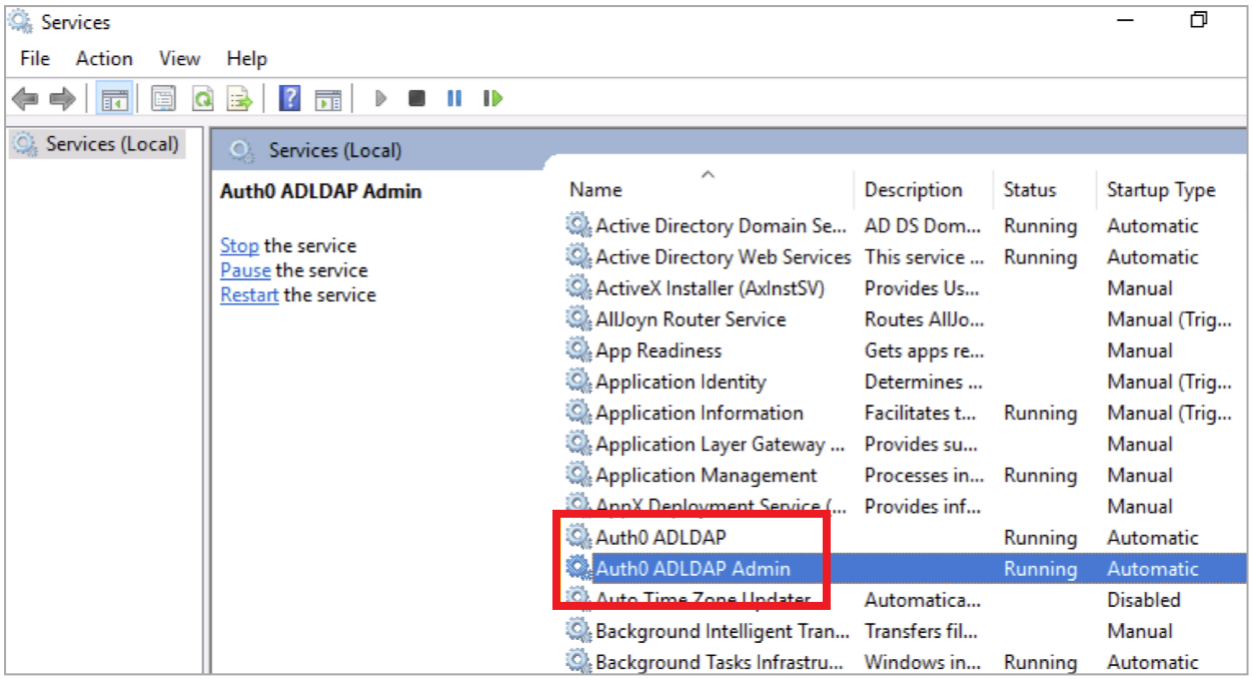


8. In the **First name** field, enter the user name.

   In the **E-mail** field, enter email id of the user.

9. Click **OK**.

10. Restart the AD/LDAP Connector service.



11. To prevent unauthenticated LDAP bind requests (unauthorized access to directory information and protecting sensitive data from potential exploitation):

    a. Open **ADSI Edit** (press `Win + R`, type `adsiedit.msc`, and press **Enter**).

    b. In **ADSI Edit**, right-click on **ADSI Edit** at the top of the left navigation pane and select **Connect to**.

    c. Connect to the **Configuration Naming Context**.

    d. In the left navigation pane, expand **Configuration** > **Services** > **Windows NT**.

    e. Right-click **Directory Service** and select **Properties**.

    f. In the **Attributes** list, find **msDS-Other-Settings**.

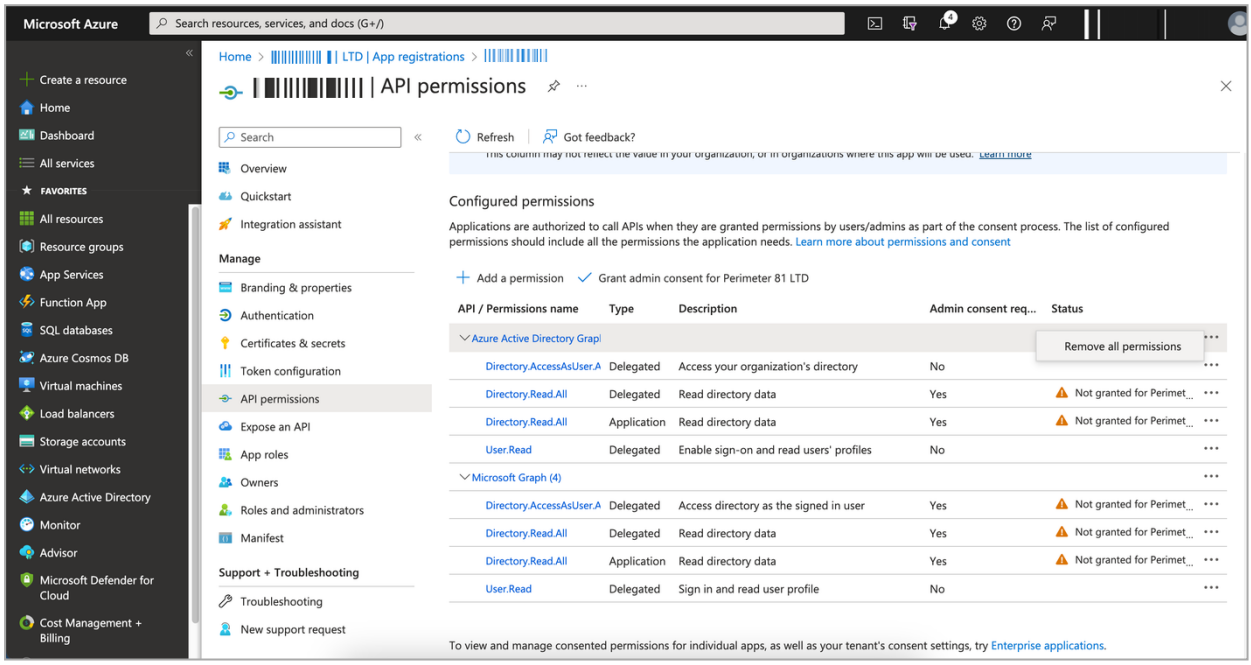
    g. Select **msDS-Other-Settings** and click **Edit**.

    h. In the **Value to** add field, enter **DenyUnauthenticatedBind=True** and click **Add**.

    i. Click **OK** to save your changes.

Appendix A - Removing Microsoft Entra ID (formerly Azure AD) API Permissions

1. Configure the permissions for the application.
2. In the **Configured permissions** section, for **Azure Active Directory Graph**, scroll to the end of the row and click ⋮.
3. Click **Remove all permissions**.

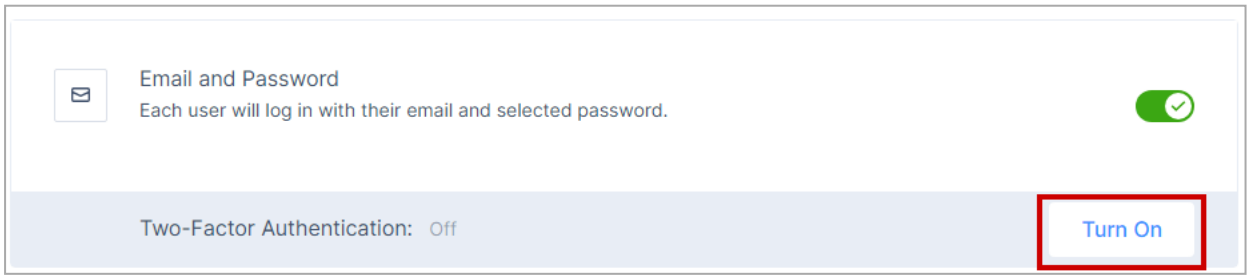


4. Click **Confirm**.

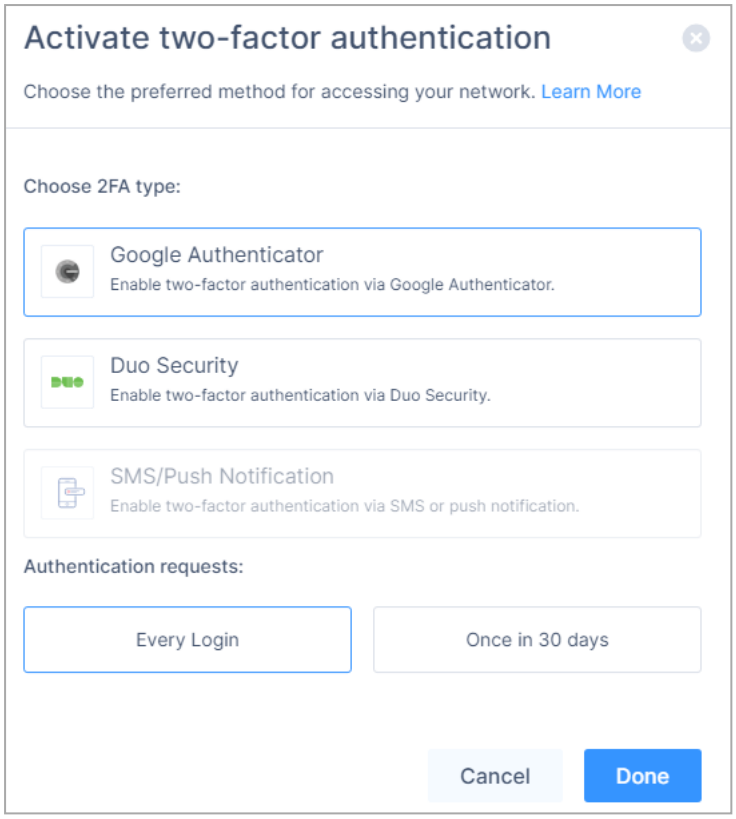
Two-Factor Authentication

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:



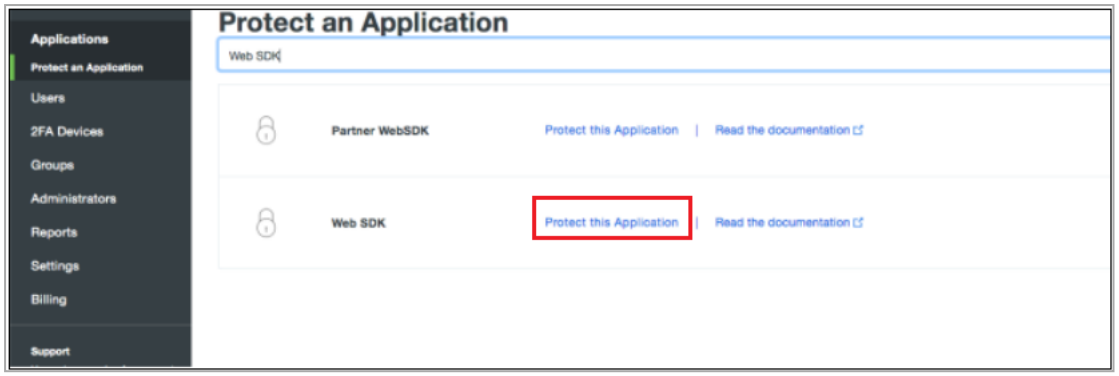
- Google Authenticator
- Duo Security
  - Enter the details in the **Integration key**, **API hostname**, and **Secret key** fields. See *"Configuring Duo Security for Two-Factor Authentication" below*.
- SMS/Push Notification

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

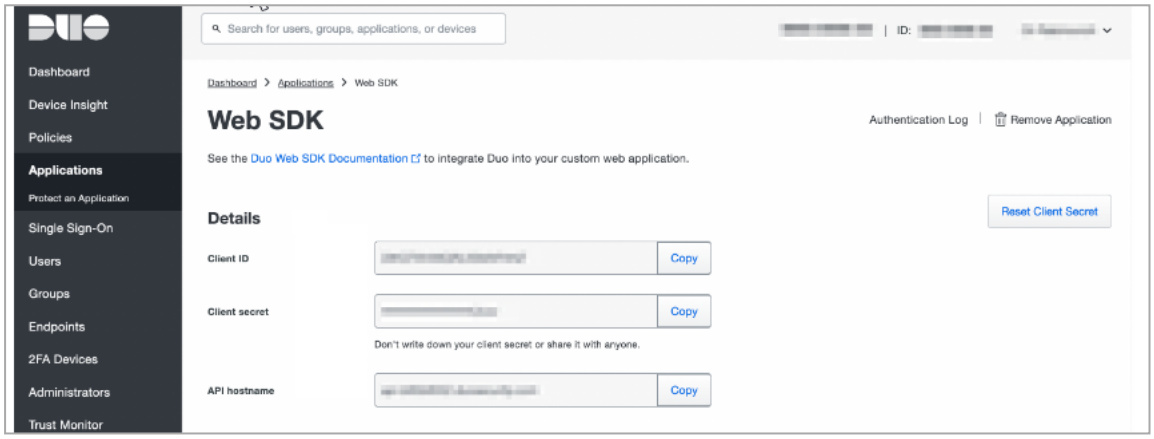
1. Log in to the Duo Security Management Portal.
2. Go to **Applications** and click **Protect an Application**.

3. Search for **Web SDK** and click **Protect this Application** for **Web SDK**.

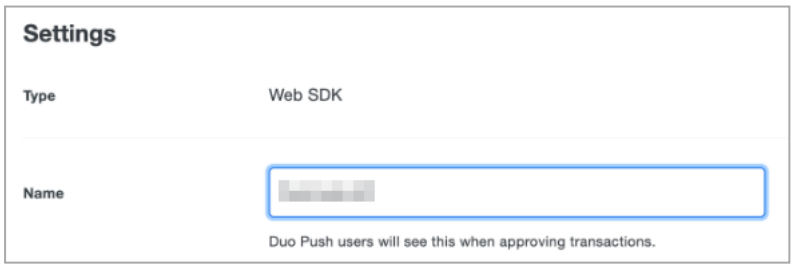


The system creates the application.

4. In the **Details** section, copy the **Client ID**, **Client secret**, and **API hostname**.

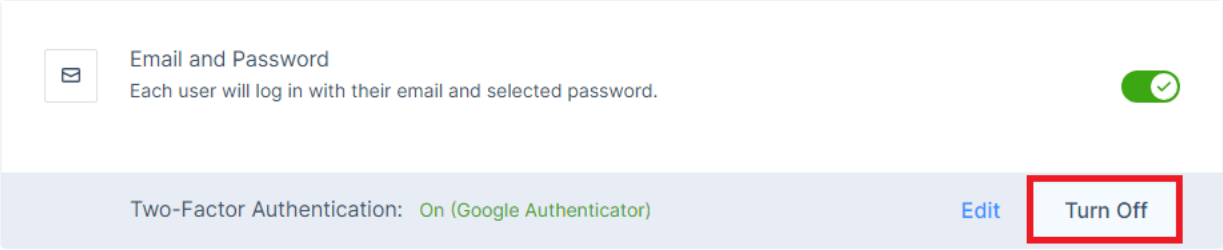


5. (Optional) Scroll down to **Settings** and in the **Name** field, change the name of the application.

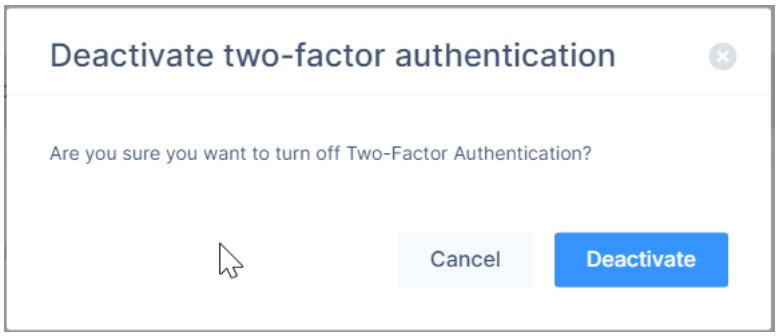


Deactivating Two-Factor Authentication

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.



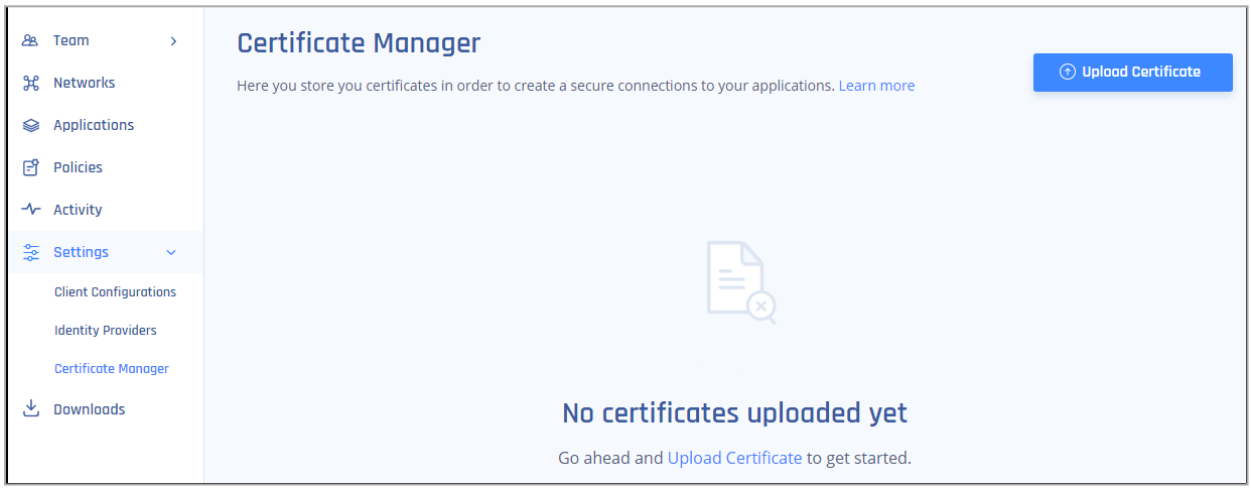
Certificate Manager

Certificate Manager allows to upload the application domain SSL certificate. This certificate is required to configure URL Alias for members to access the applications.

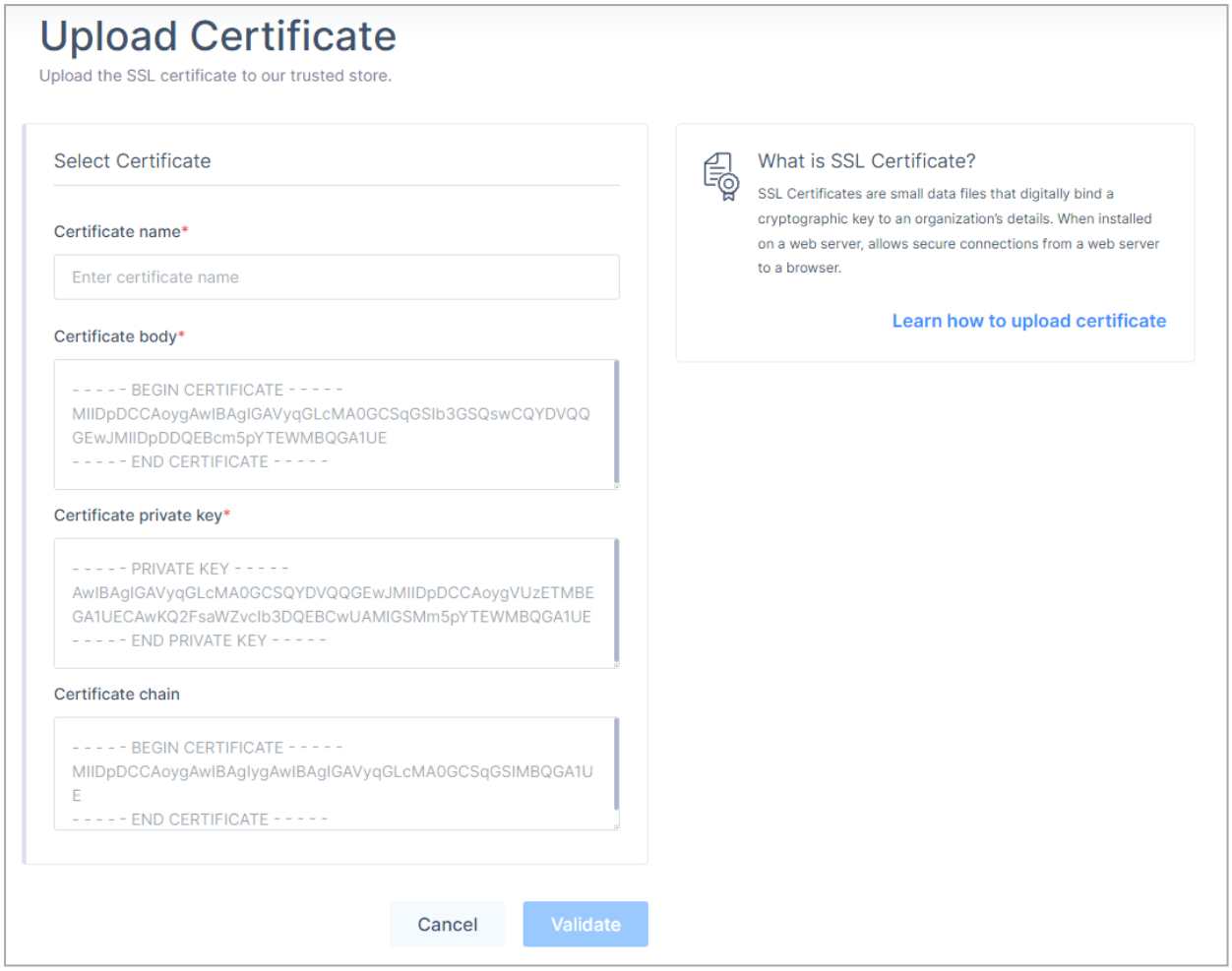
Uploading Domain SSL Certificates

Note - 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.

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

URL Aliasing for Zero-Trust Applications on Harmony SASE

URL aliasing enables Zero-Trust Applications on the Harmony SASE platform to utilize a custom URL instead of the default FQDN assigned upon creation. This feature is essential for applications that establish connections from a trusted customer domain rather than the default Harmony Zero-Trust Application domain (pzero.perimeter81.com). It is used to authenticate the accessed resource through the company's domain and help troubleshoot security blocks, such as CORS issues when web servers require connections from a trusted Domain-Validated SSL certificate.

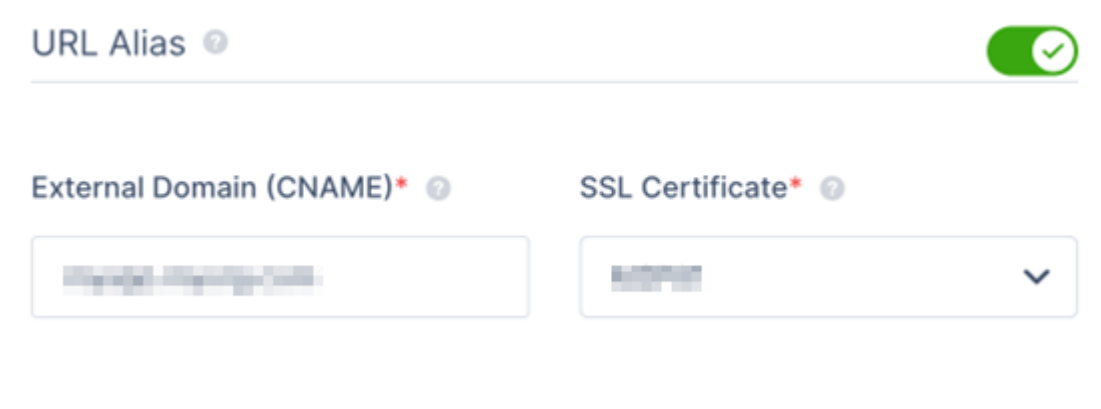
To define a URL Alias, do these:

1. Access the Harmony SASE Administrator Portal.
2. Go to **Private Access** > **Applications**.
3. Find or set up the application you wish to alias.

   Note - The Zero Trust Application's FQDN is allocated in the Harmony SASE Administrator Portal only after you save your application's settings.

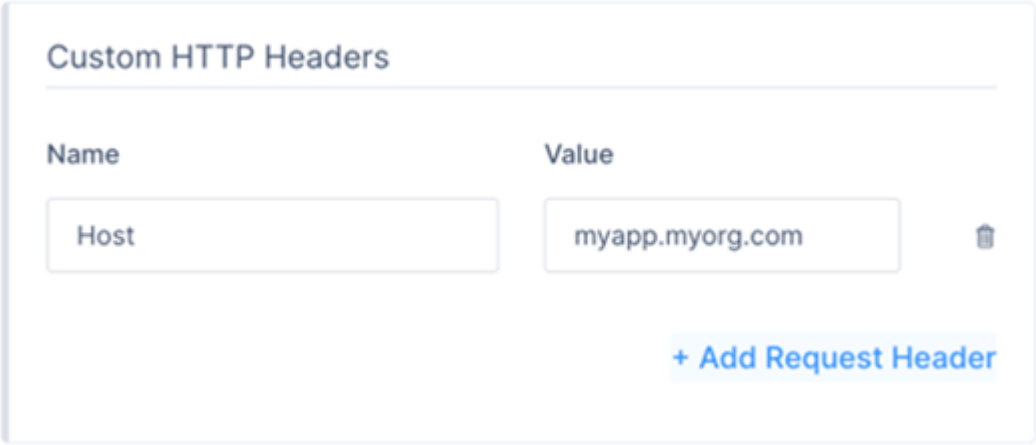
4. Once the application setting is saved, in the FQDN field, click to copy the FQDN.

5. Go to your public DNS server (example: GoDaddy or Route53), define a **CNAME** record for a validated domain to point to the copied FQDN.
6. Go back to the Harmony SASE Administrator Portal, go to the **URL Alias** section, and turn on the **URL Alias** toggle button.
7. In the **External Domain (CNAME)** field, enter the CNAME associated with your domain.



8. From the **SSL Certificate** list, select the certificate.

9. If your security mechanisms require the connection to originate from a specific host for successful webpage:
10. Go to the **Custom HTTP Headers** section.



11. In the **Name** field, enter Host.
12. In the **Value** field, enter the configured CNAME.

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.

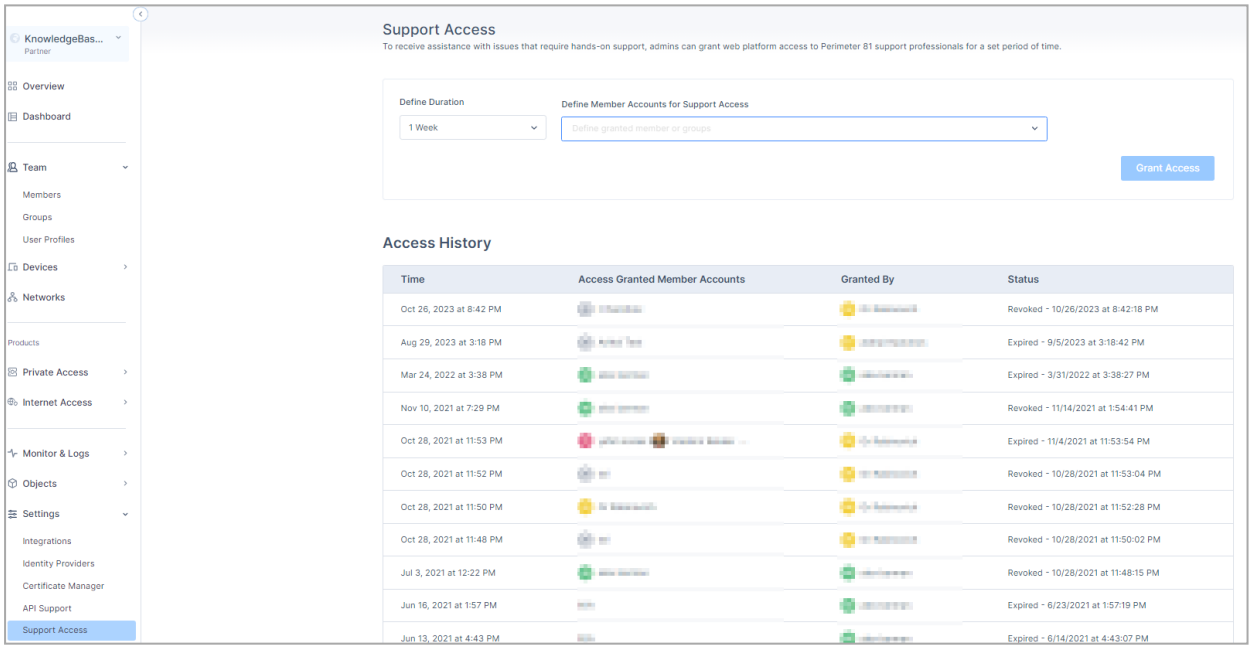
Notes -

- You do not require an additional user license to enable the Support Access role.
- When a Harmony SASE support engineer access your tenant, the system logs it in *"Member Activity" on page 673*.

Granting the Support Access Role

1. Access the Harmony SASE Administrator Portal and click **Settings** > **Support Access**.

   The **Support Access** page appears.

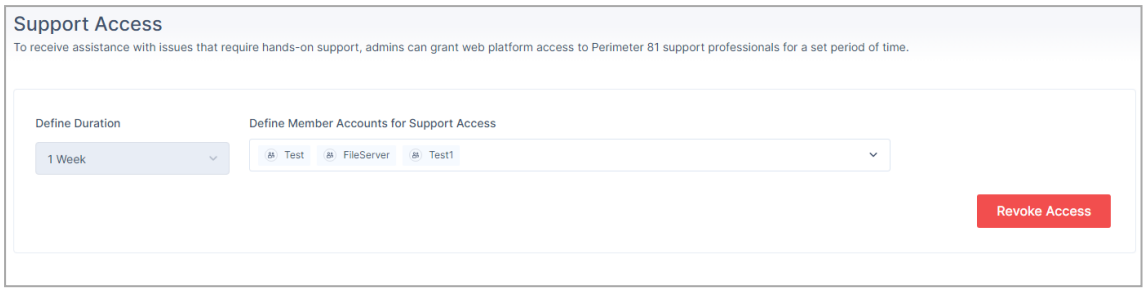


2. From the **Define Duration** list, select the time duration for which Support Access role is valid.

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. ▪ Active ▪ Revoked ▪ Expired

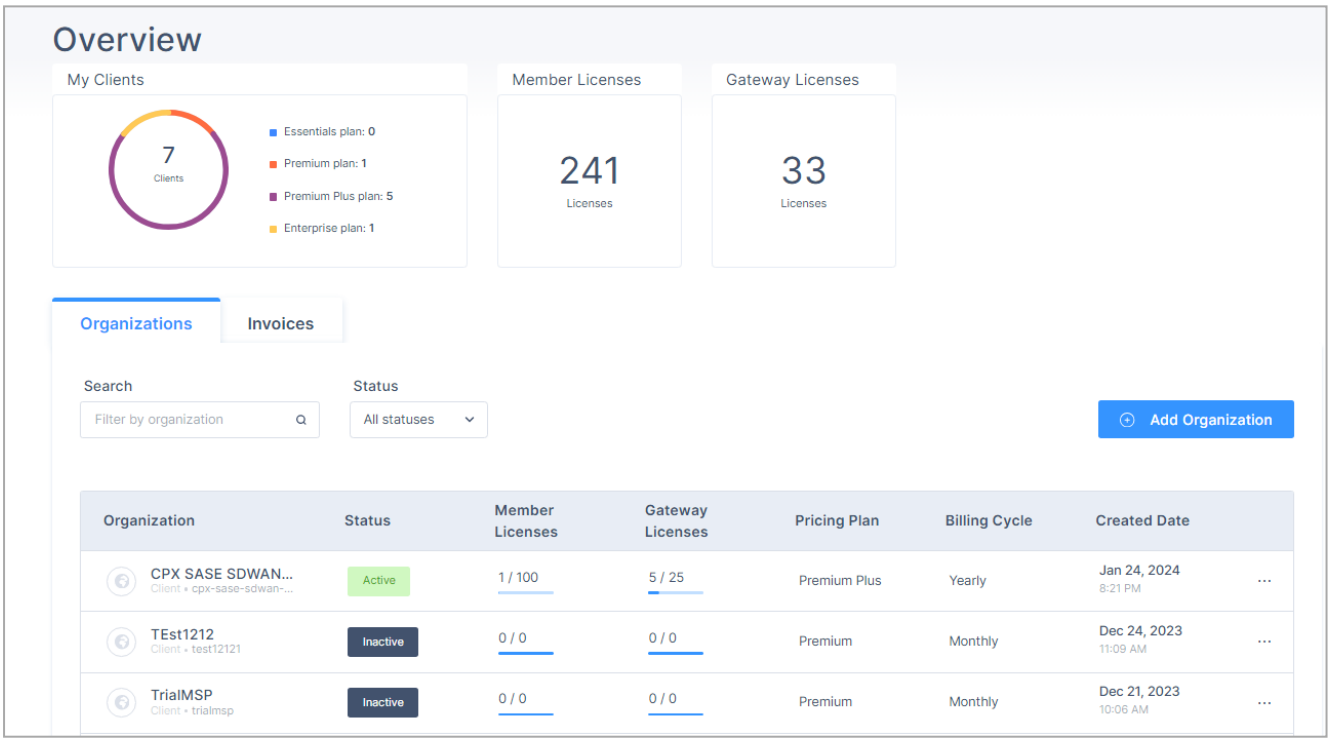
Overview

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

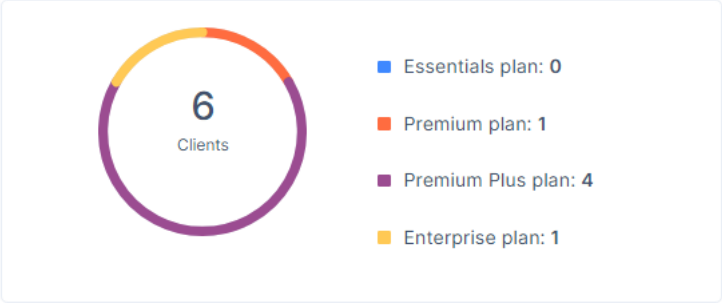
The **Overview** page allows you to view:

- *"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 912*

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

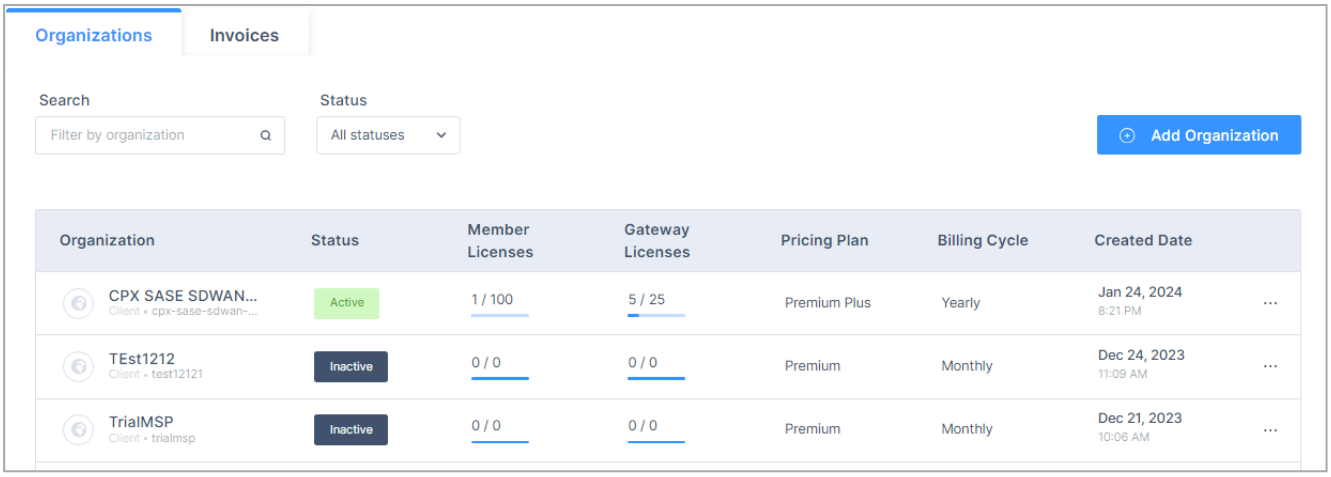
The **Member Licenses** widget shows the total number of purchased member licenses.

Gateway Licenses

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

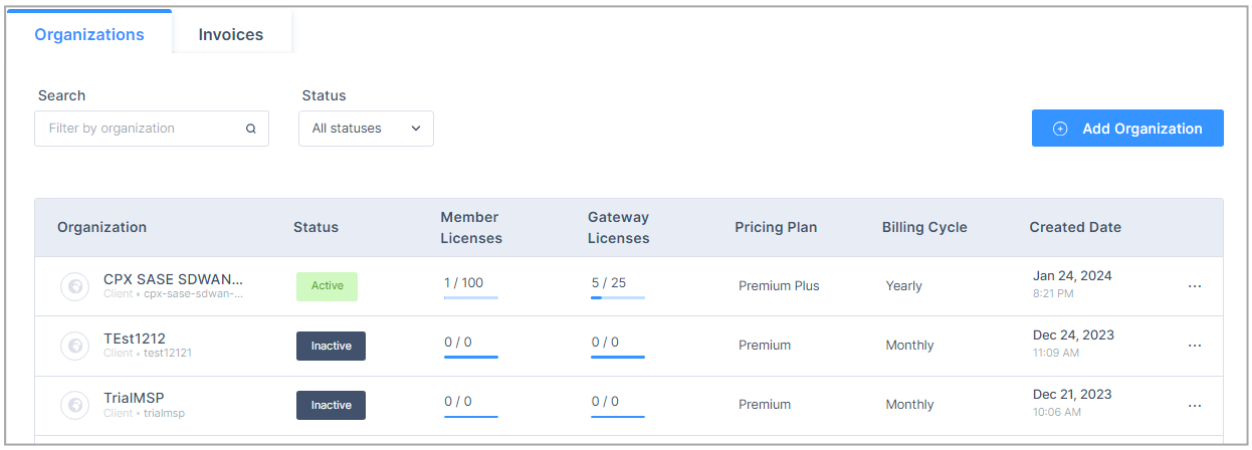
Organizations

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

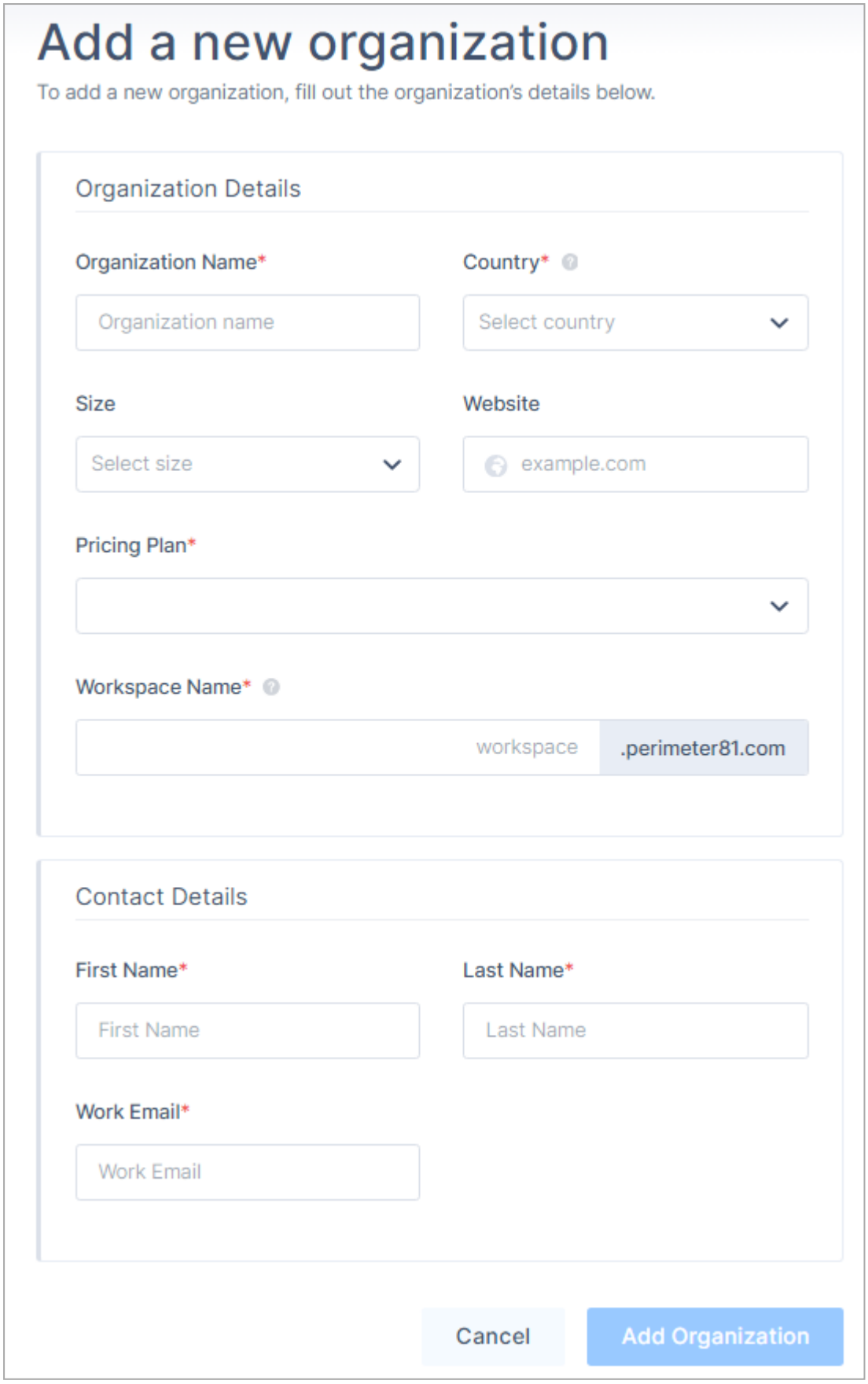


Adding an Organization

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.



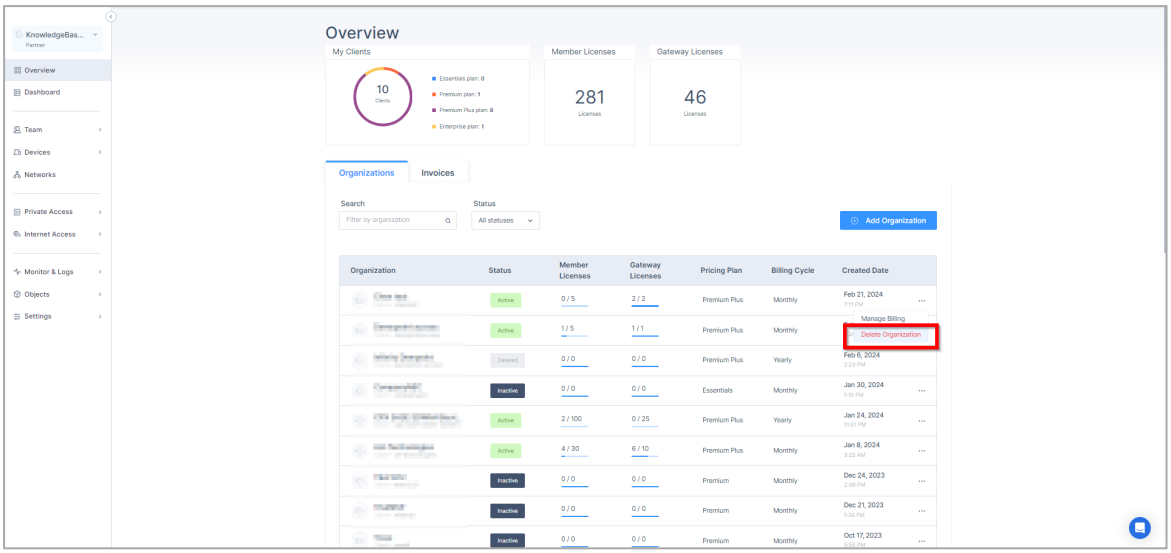
3. In the **Organization Details** section, specify these:

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

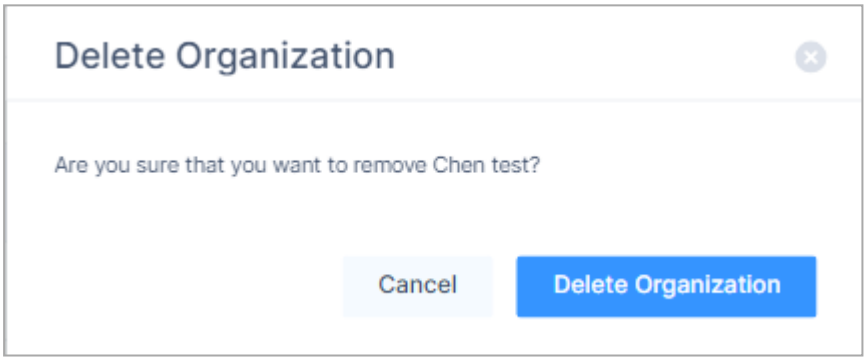
Note - You cannot change the workspace name after you create it.

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**.



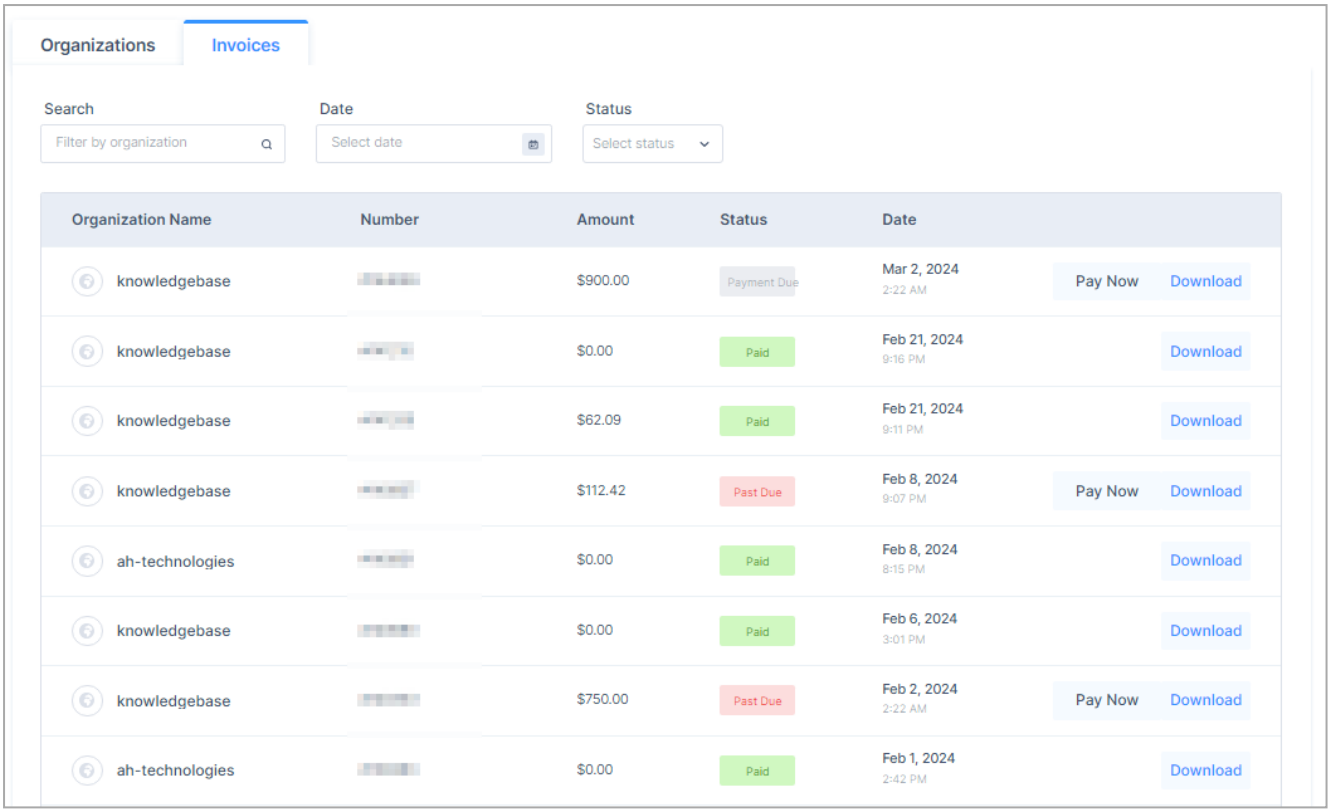
The **Delete Organization** window appears.



b. Click **Delete Organization**.

Invoices

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

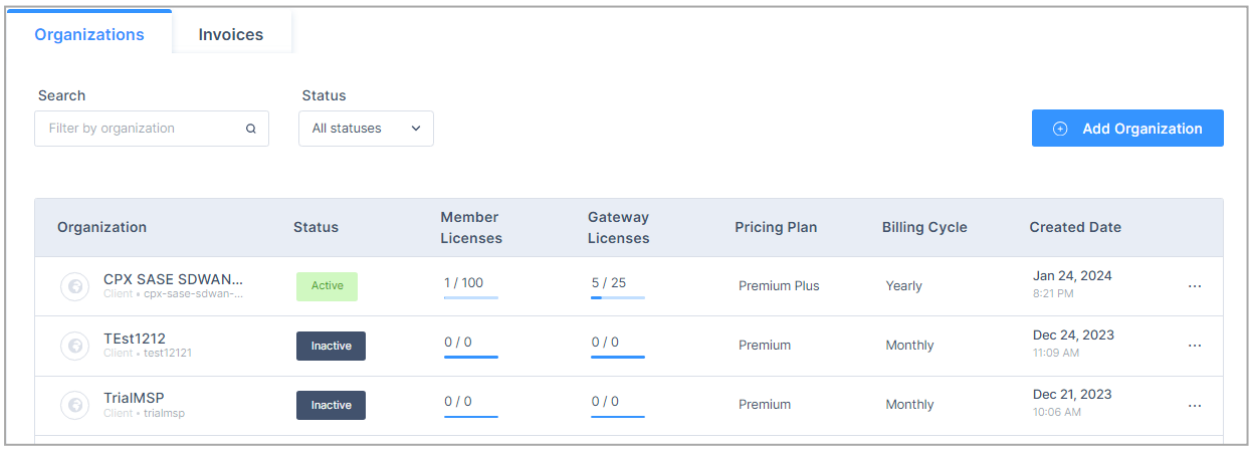


To pay an invoice, click **Pay Now**.

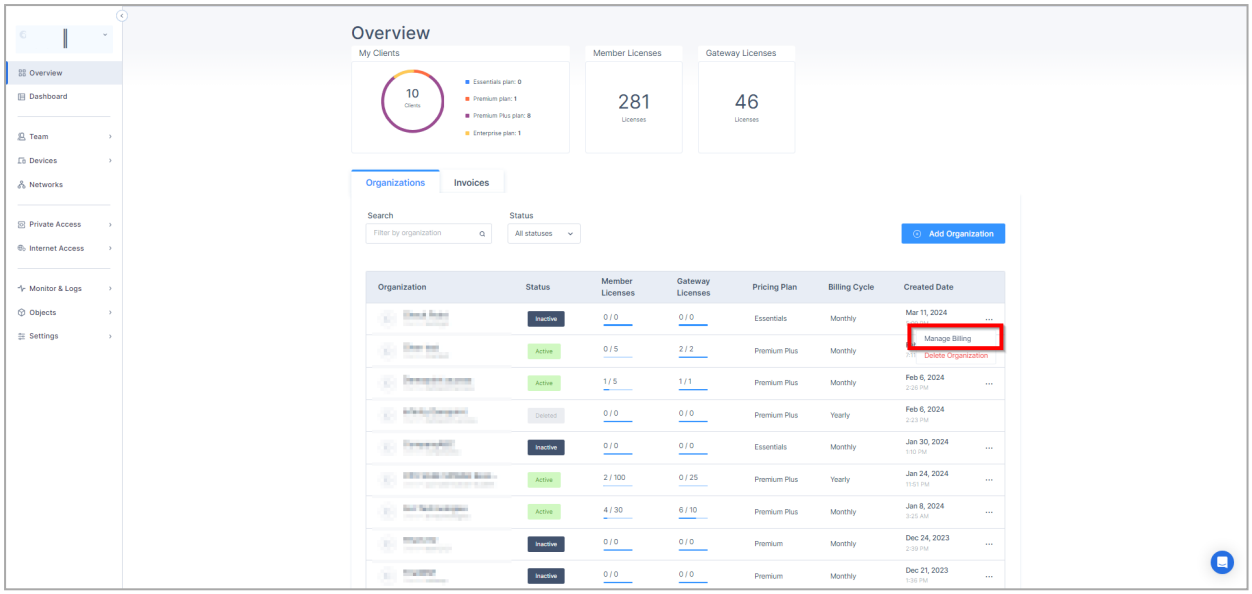
To download an invoice, click **Download**.

Managing Billing

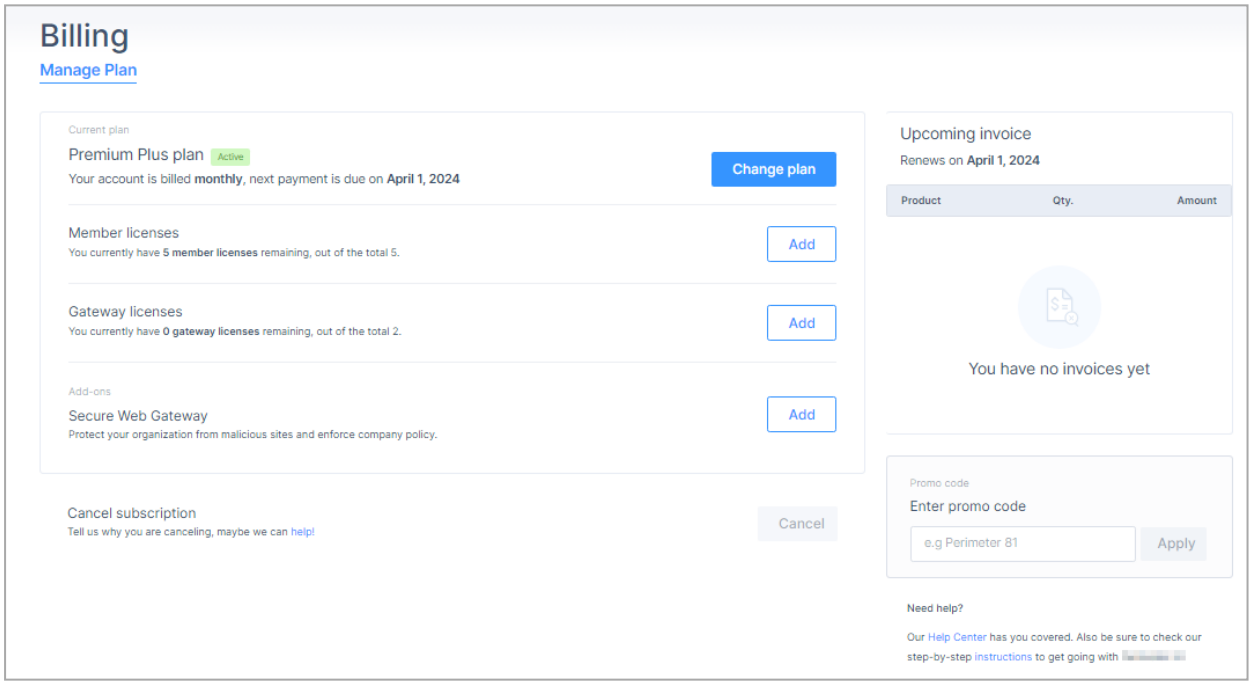
1. Access the **Harmony SASE** (Perimeter 81) Administrator Portal and go to **Overview** and click the **Organizations** tab.



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.

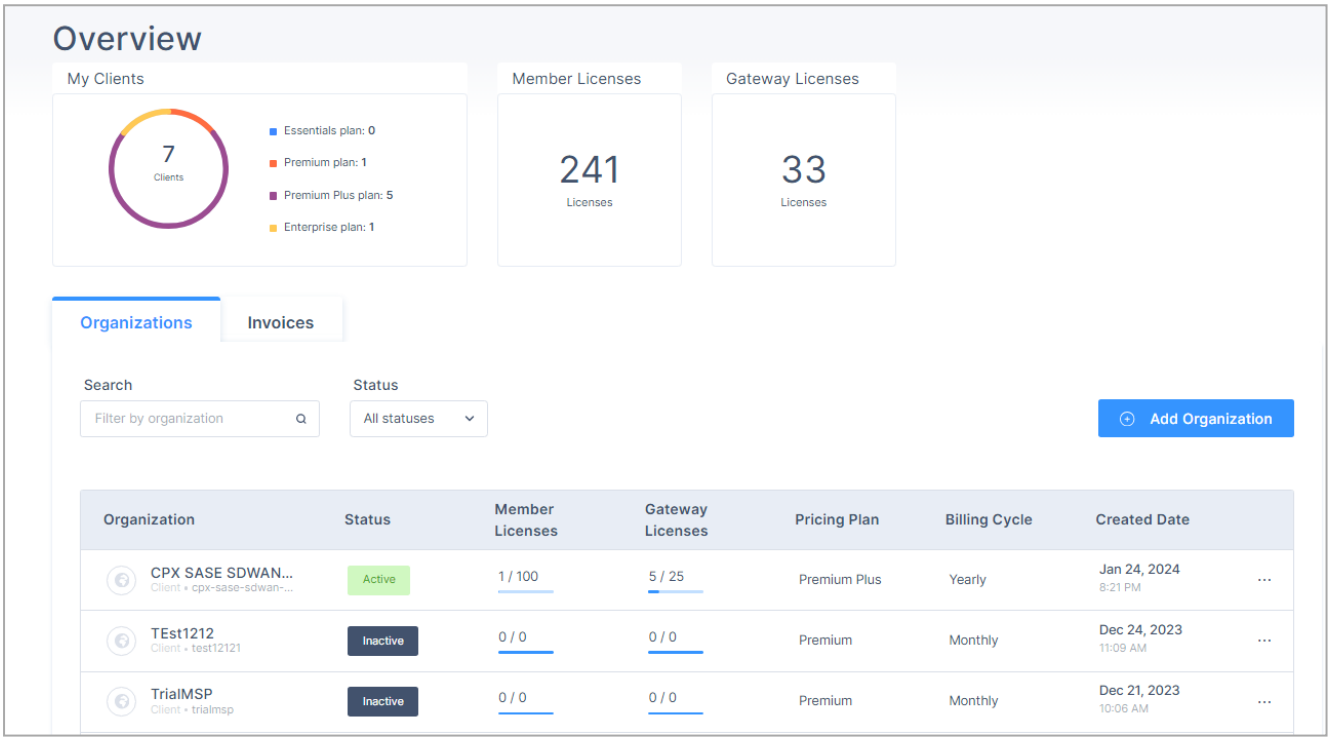
Overview

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

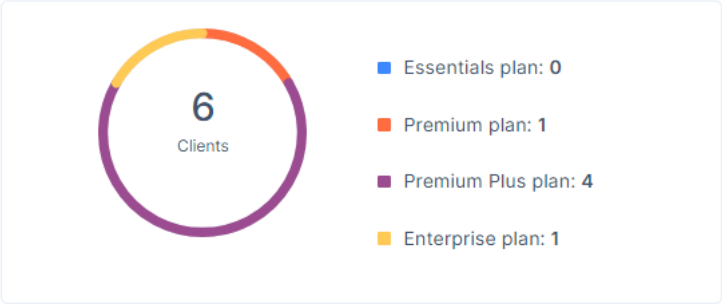
The **Overview** page allows you to view:

- *"My Clients" below*
- *"Member Licenses" below*
- *"Gateway Licenses" on the next page*
- *"Organizations" on the next page*
- *"Invoices" on page 920*

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

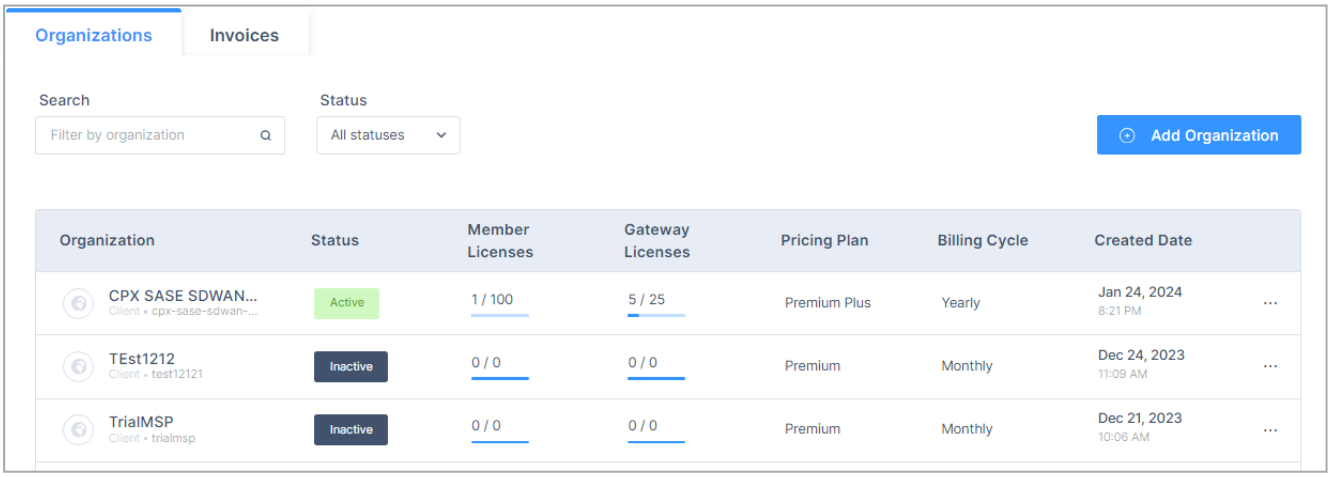
The **Member Licenses** widget shows the total number of purchased member licenses.

Gateway Licenses

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

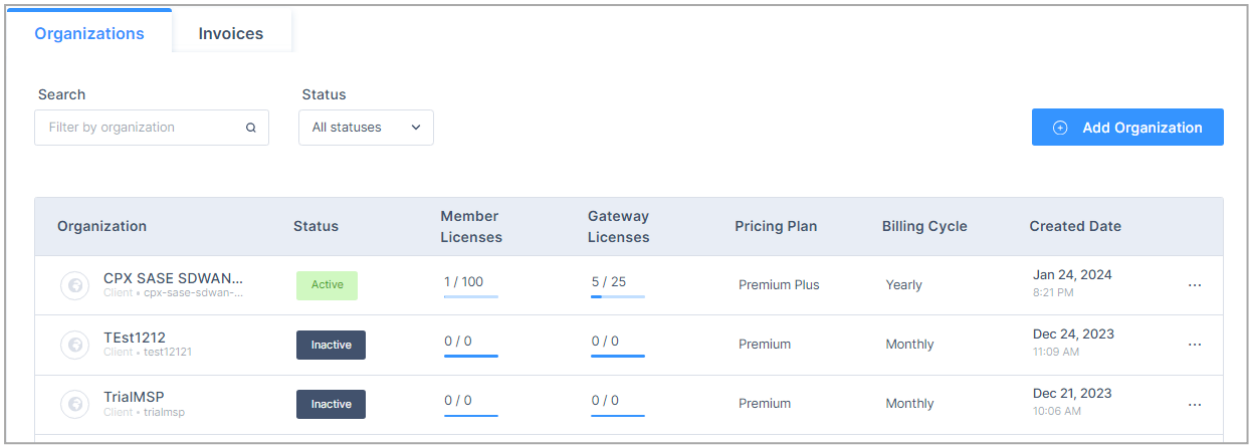
Organizations

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

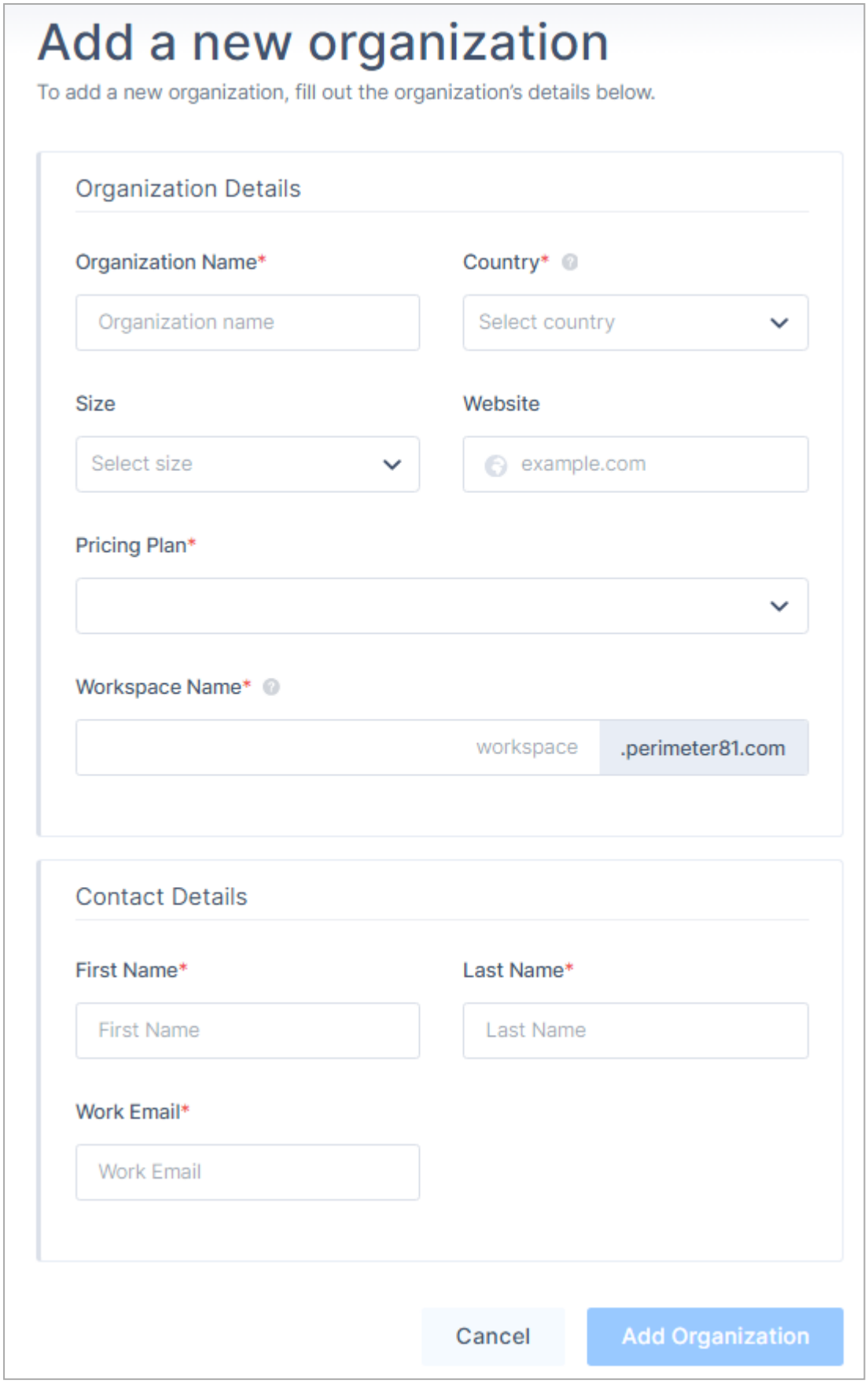


Adding an Organization

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.



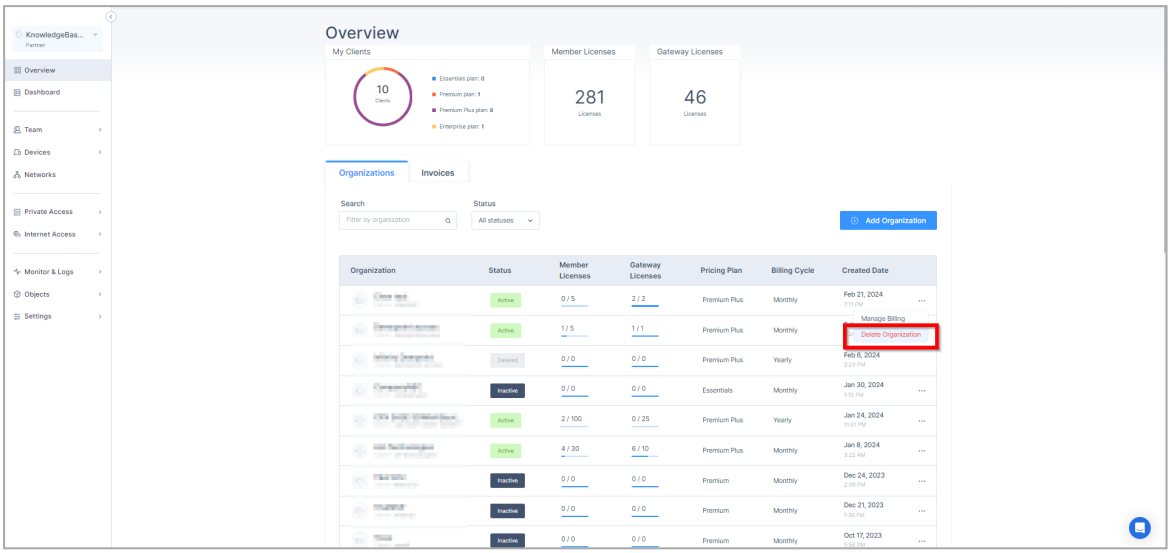
3. In the **Organization Details** section, specify these:

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

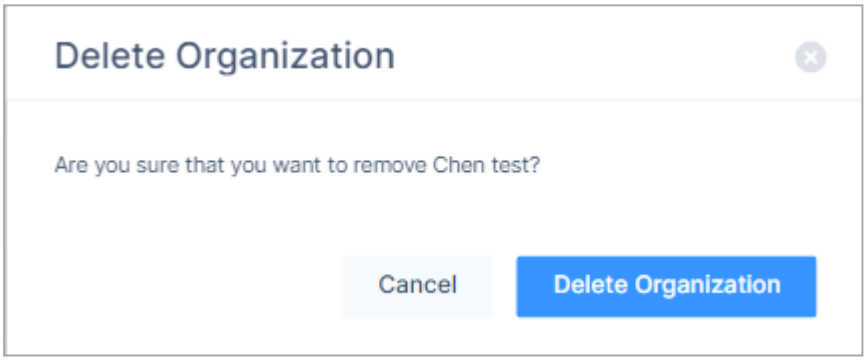
Note - You cannot change the workspace name after you create it.

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**.



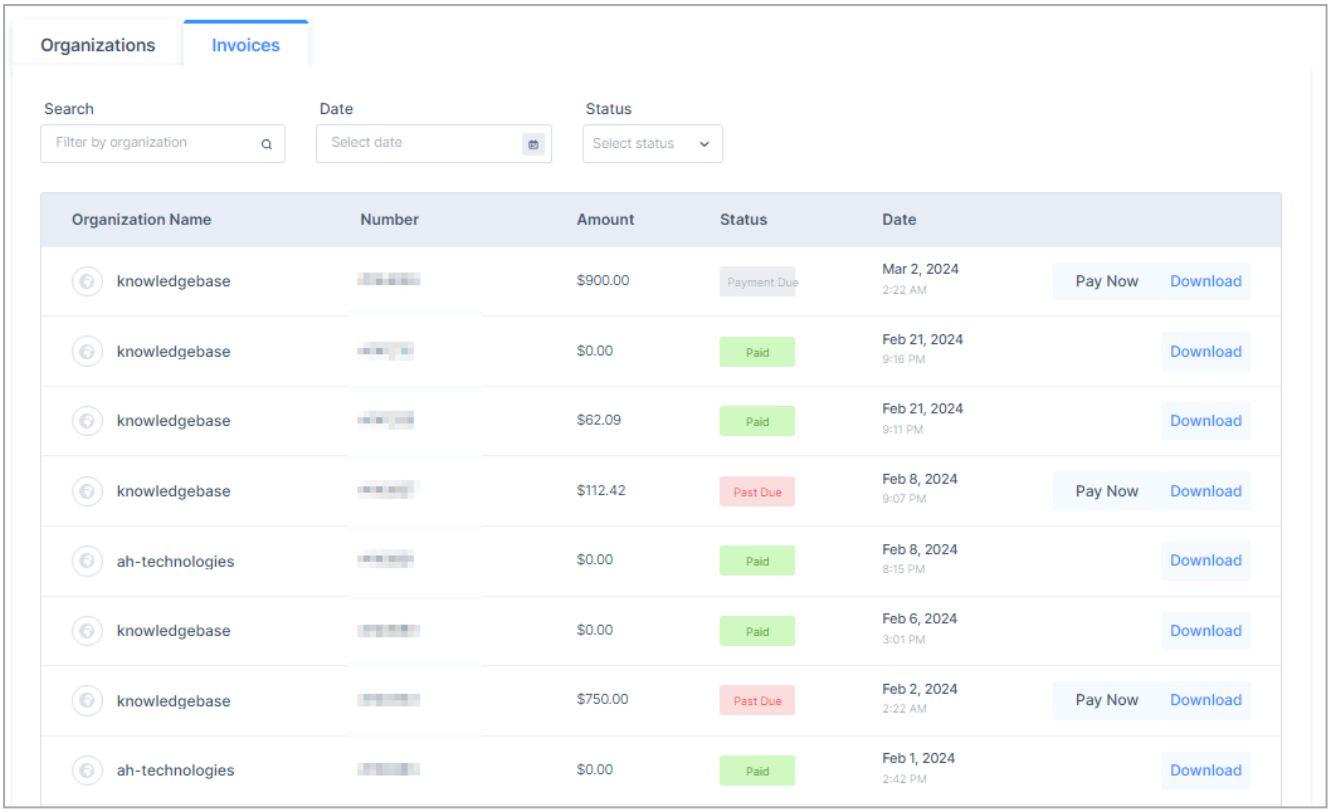
The **Delete Organization** window appears.



b. Click **Delete Organization**.

Invoices

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

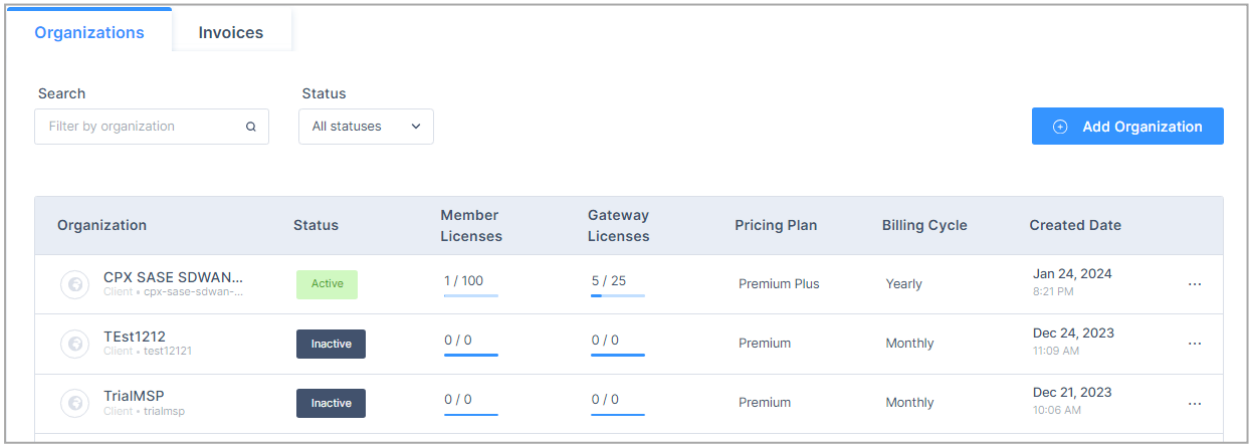


To pay an invoice, click **Pay Now**.

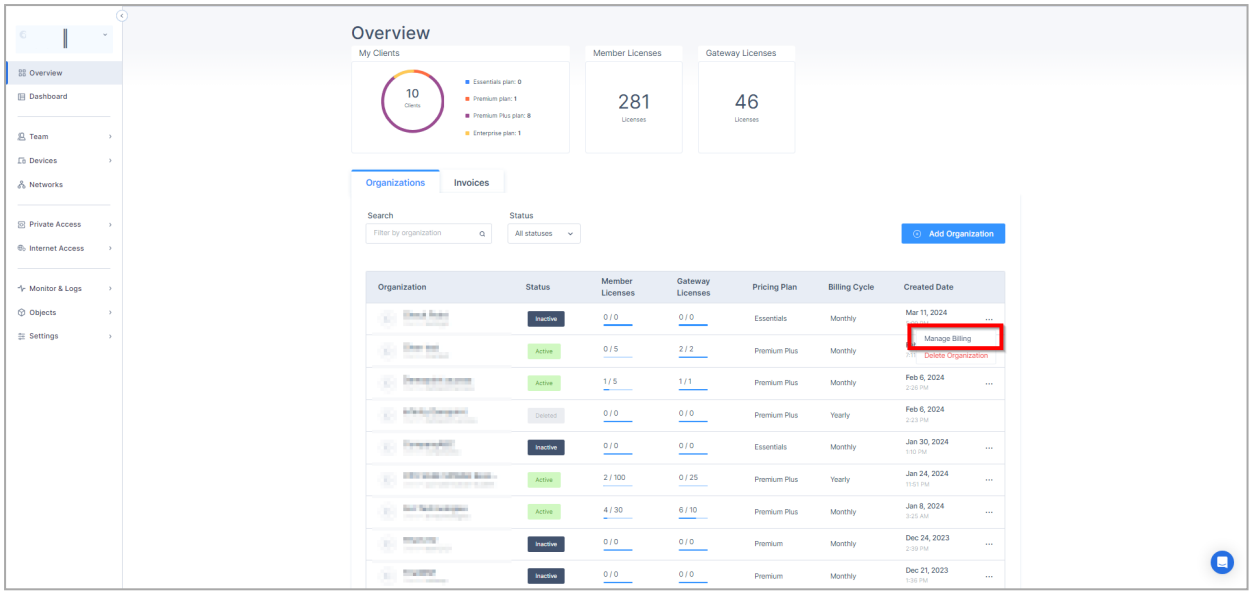
To download an invoice, click **Download**.

Managing Billing

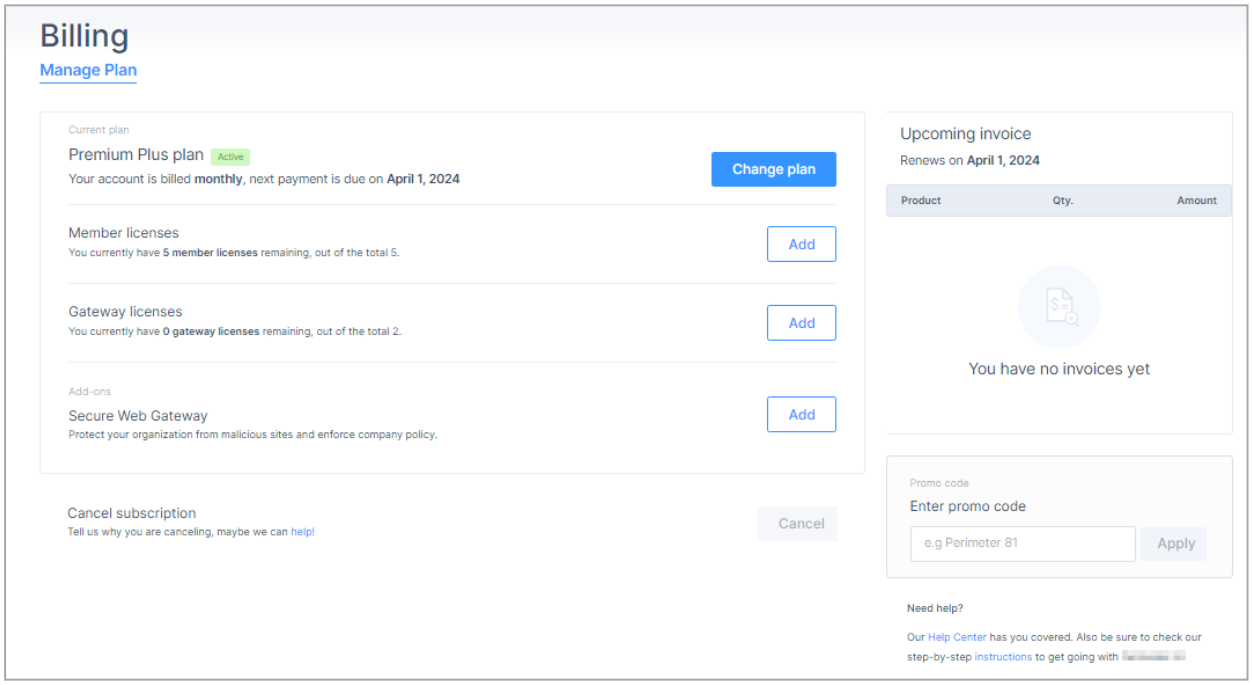
1. Access the **Harmony SASE** (Perimeter 81) Administrator Portal and go to **Overview** and click the **Organizations** tab.



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.

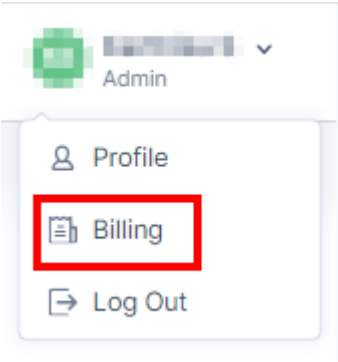
Billing

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

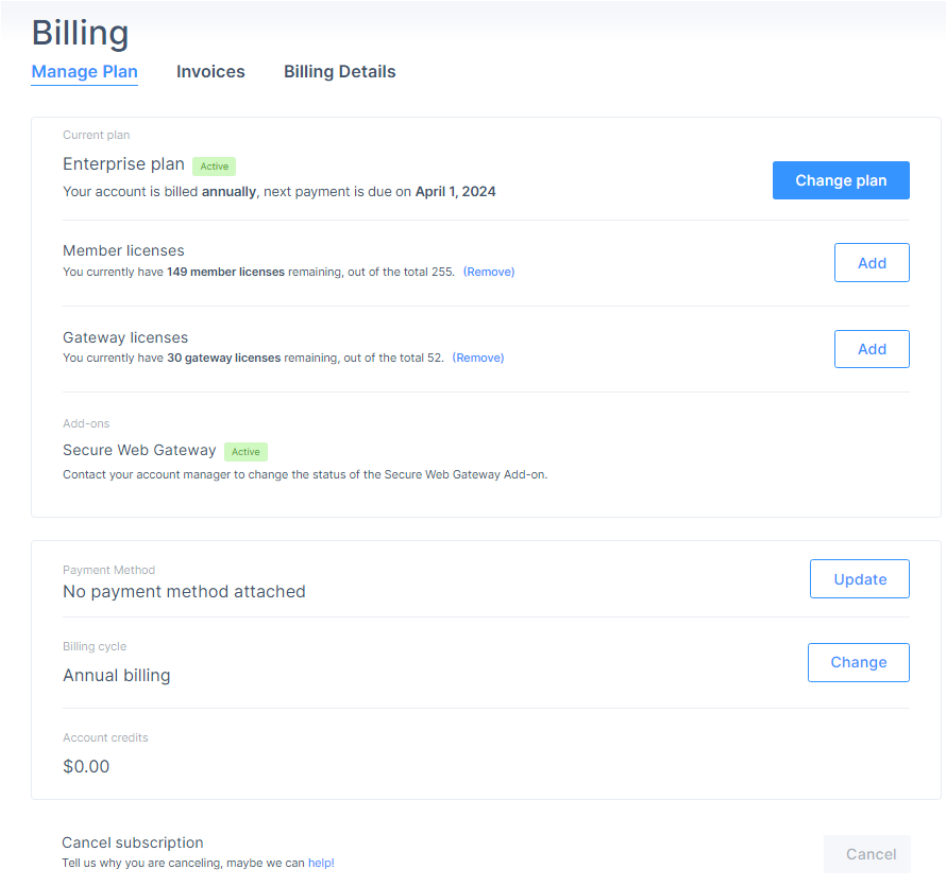
Billing allows you to manage your billing plan, pay invoices and update billing details.

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.

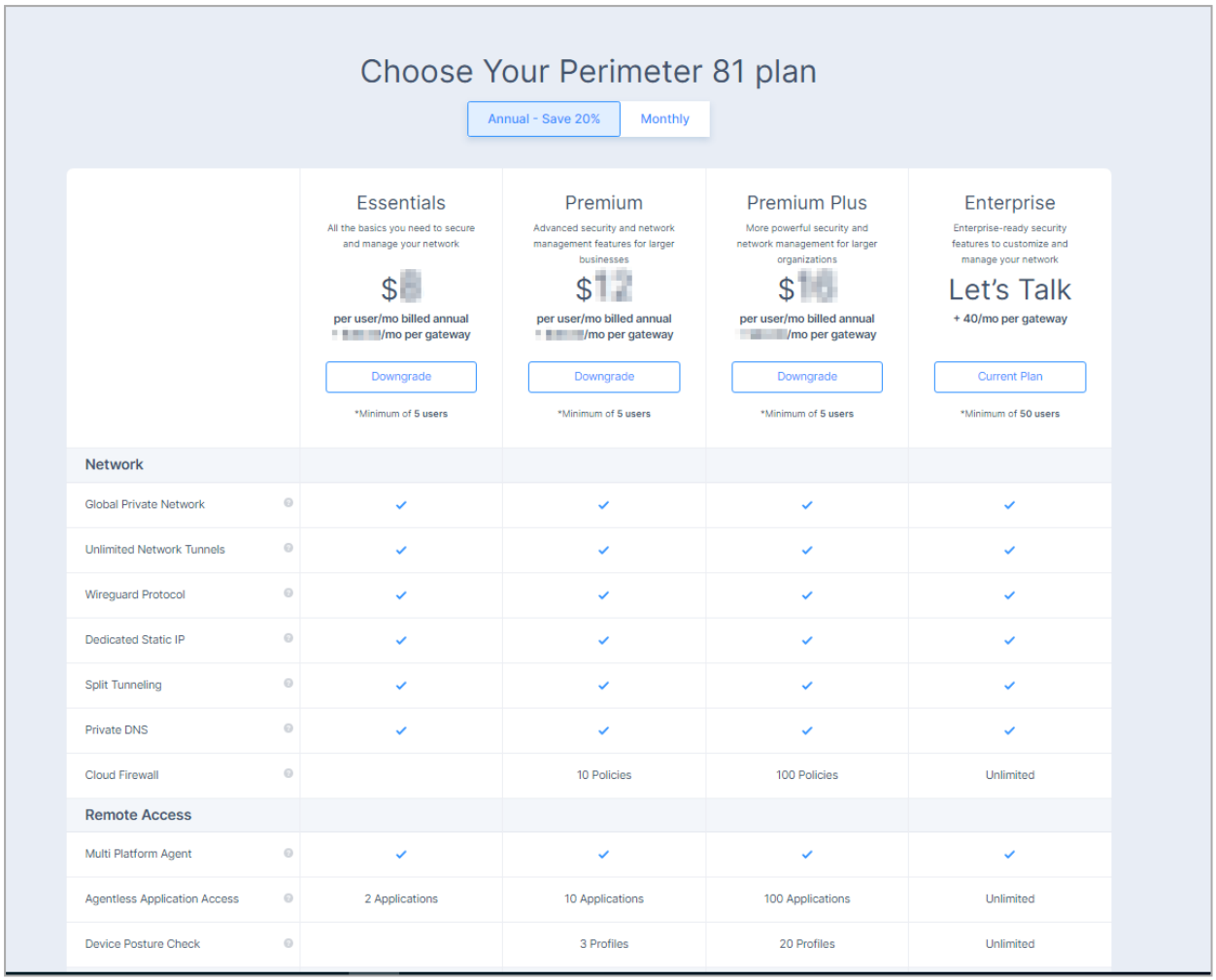
- Update your Subscription Plan
- Modify Member Licenses
- Modify Gateway / Application Licenses
- Add a payment method
- Cancel subscription

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.



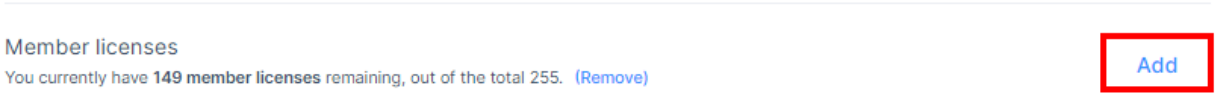
2. Select your billing cycle:
   - Annual
   - Monthly

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.

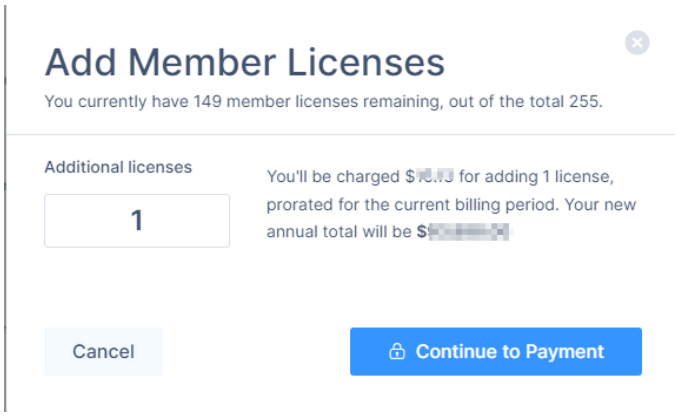
3. Select the plan you want to upgrade to.

Modifying Member Licenses

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

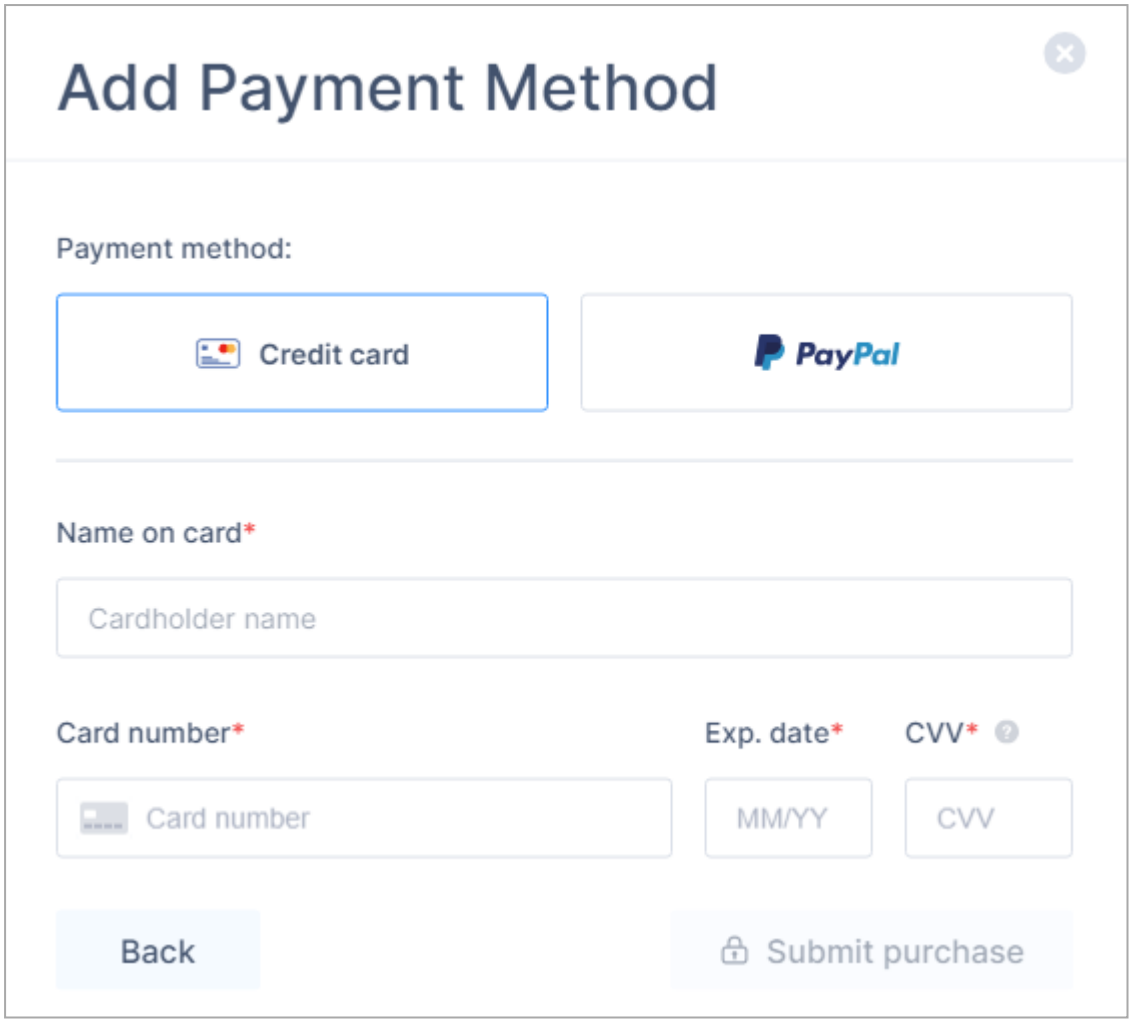


   The **Add Member Licenses** window appears.



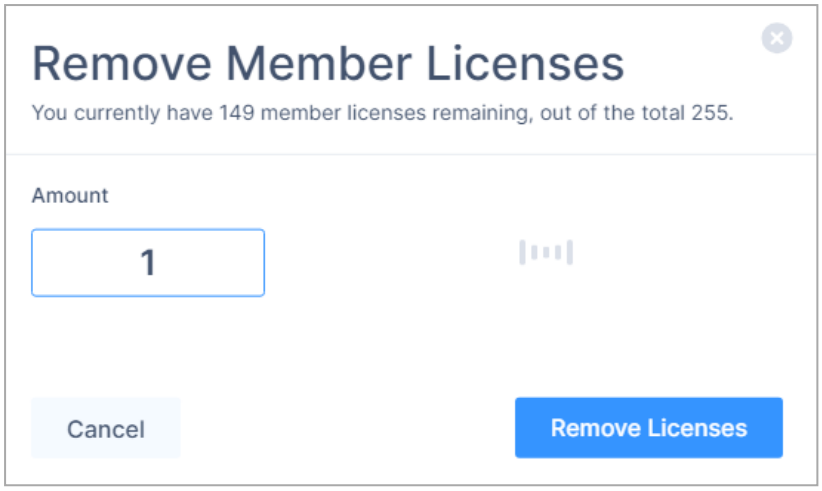
2. In the **Additional licenses** field, enter the number of member licenses.
3. Click **Continue to Payment**.

   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**.

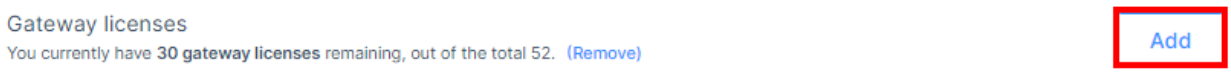
The **Remove Member Licenses** window appears.



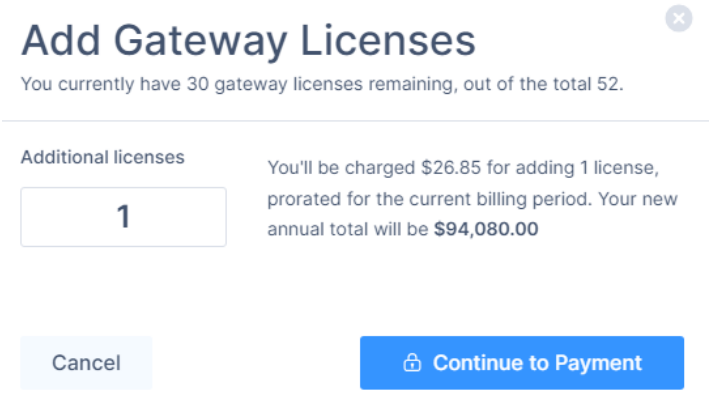
7. Enter the number of licenses to remove and click **Remove Licenses**.

Modifying Gateway / Application Licenses

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

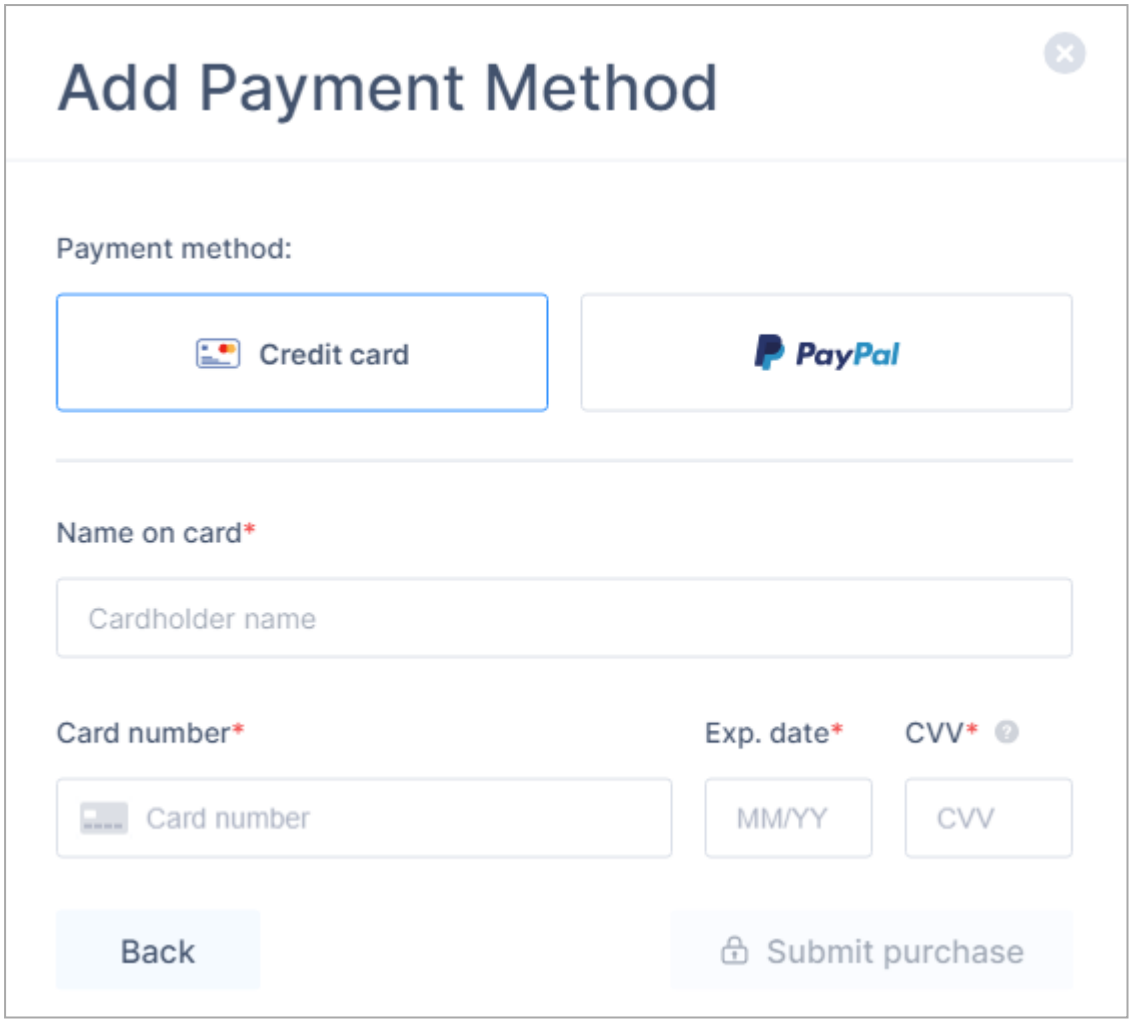


The **Add Gateway Licenses** window appears.



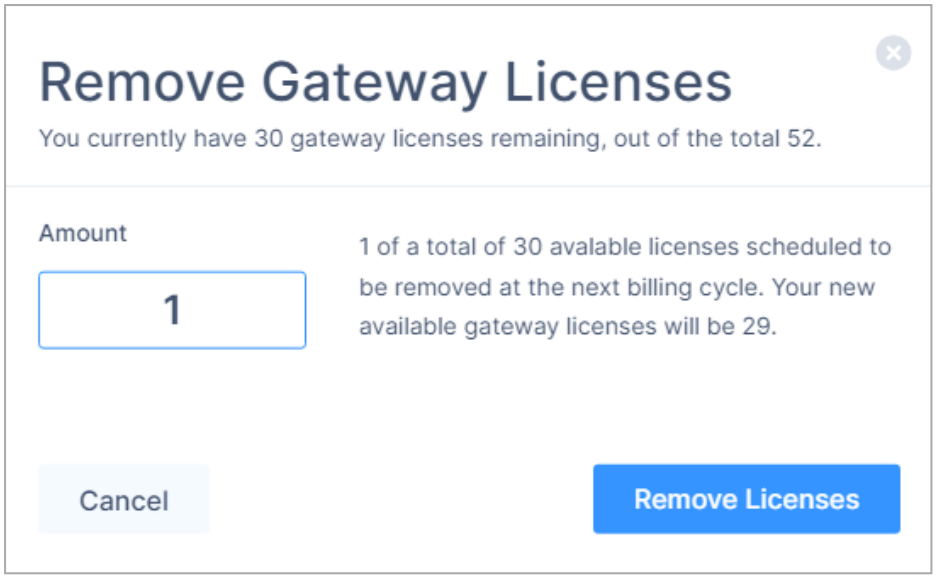
2. In the **Additional licenses** field, enter the number of gateway licenses.
3. Click **Continue to Payment**.

   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.

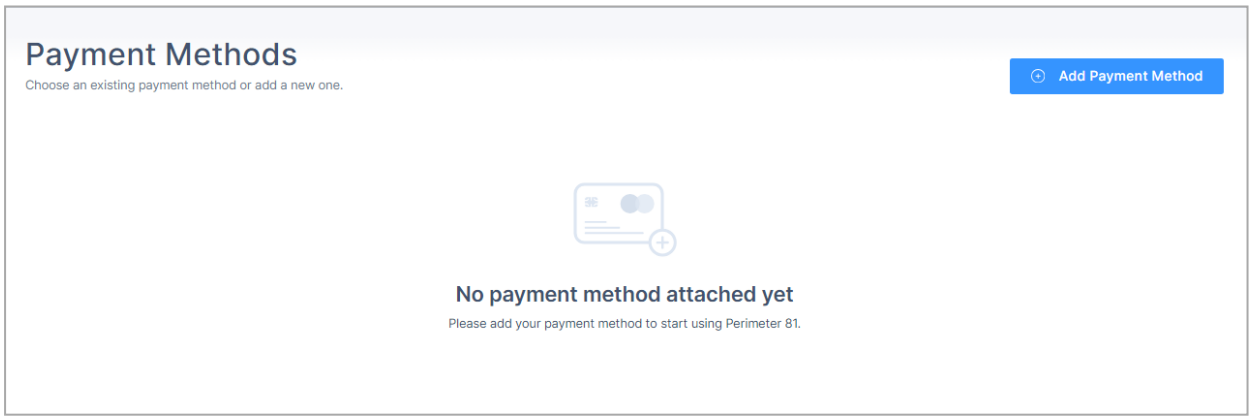


7. Enter the number of licenses to remove and click **Remove Licenses**.

Adding a Payment Method

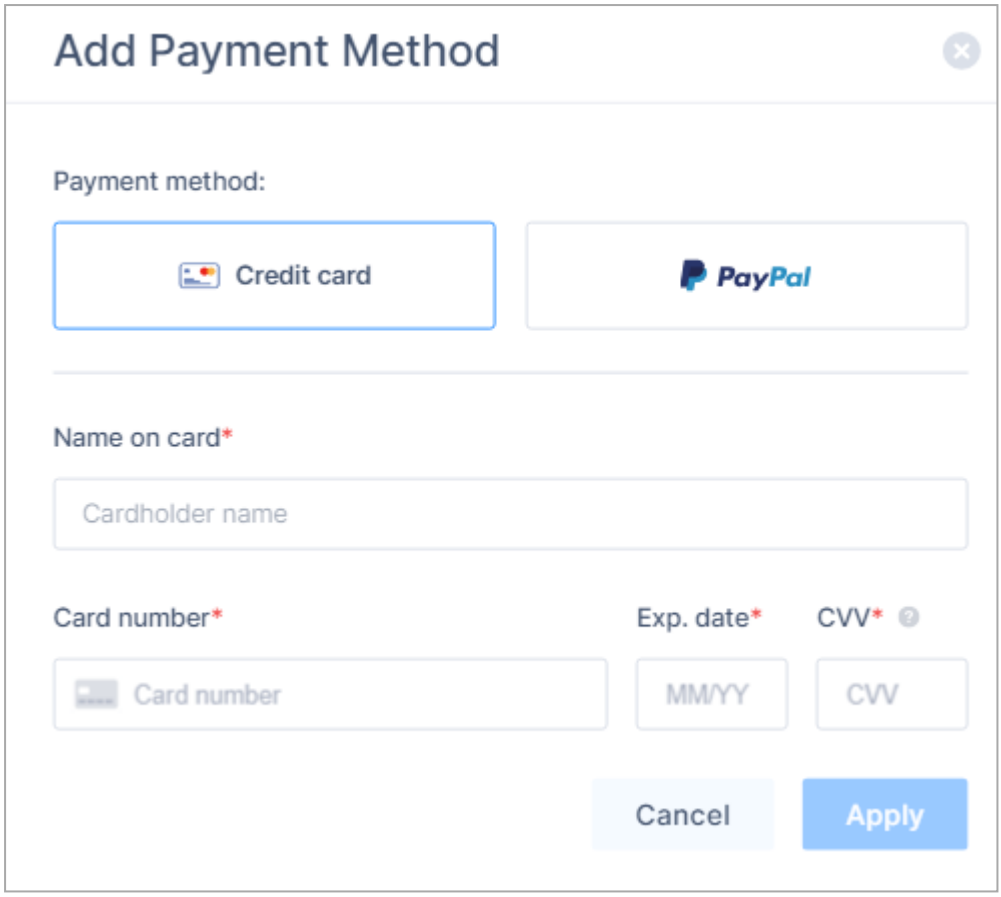
1. In the **Payment Method** section, click **Update**.

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.

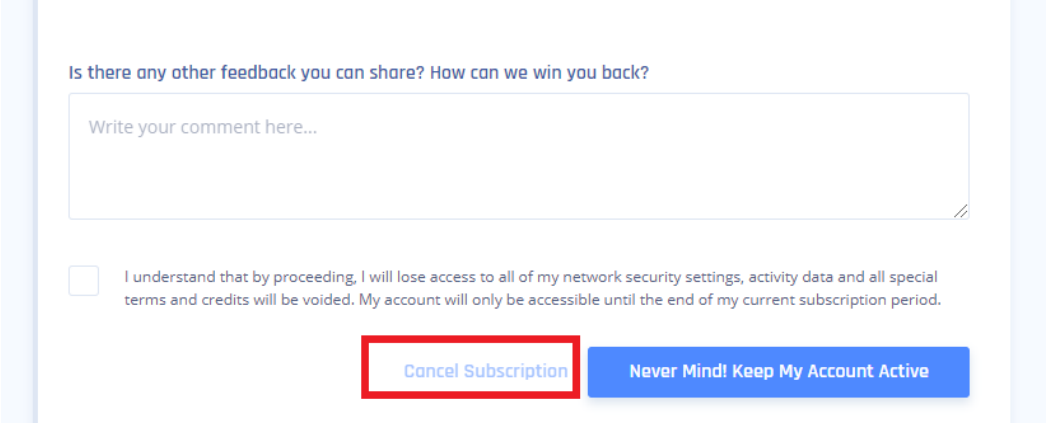
Cancelling Subscription

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**.

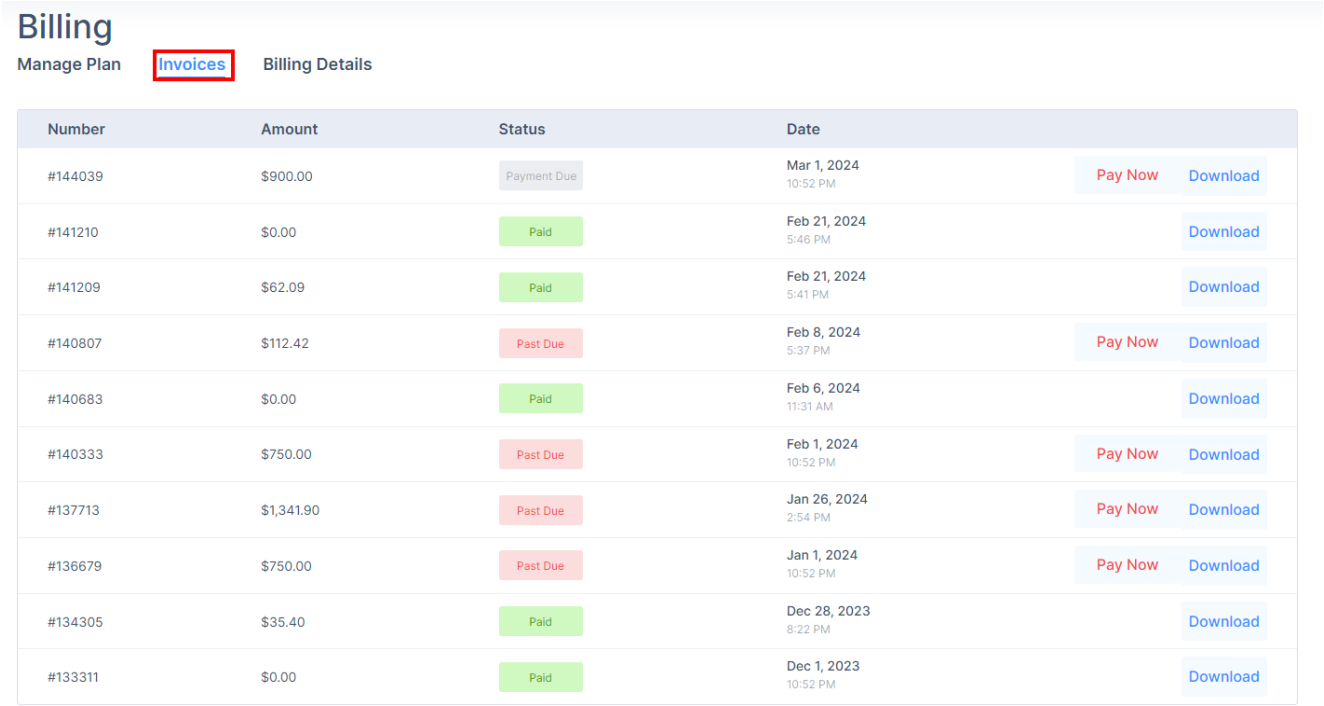
2. Enter a feedback (optional), select the checkbox and then click **Cancel Subscription**.



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**.

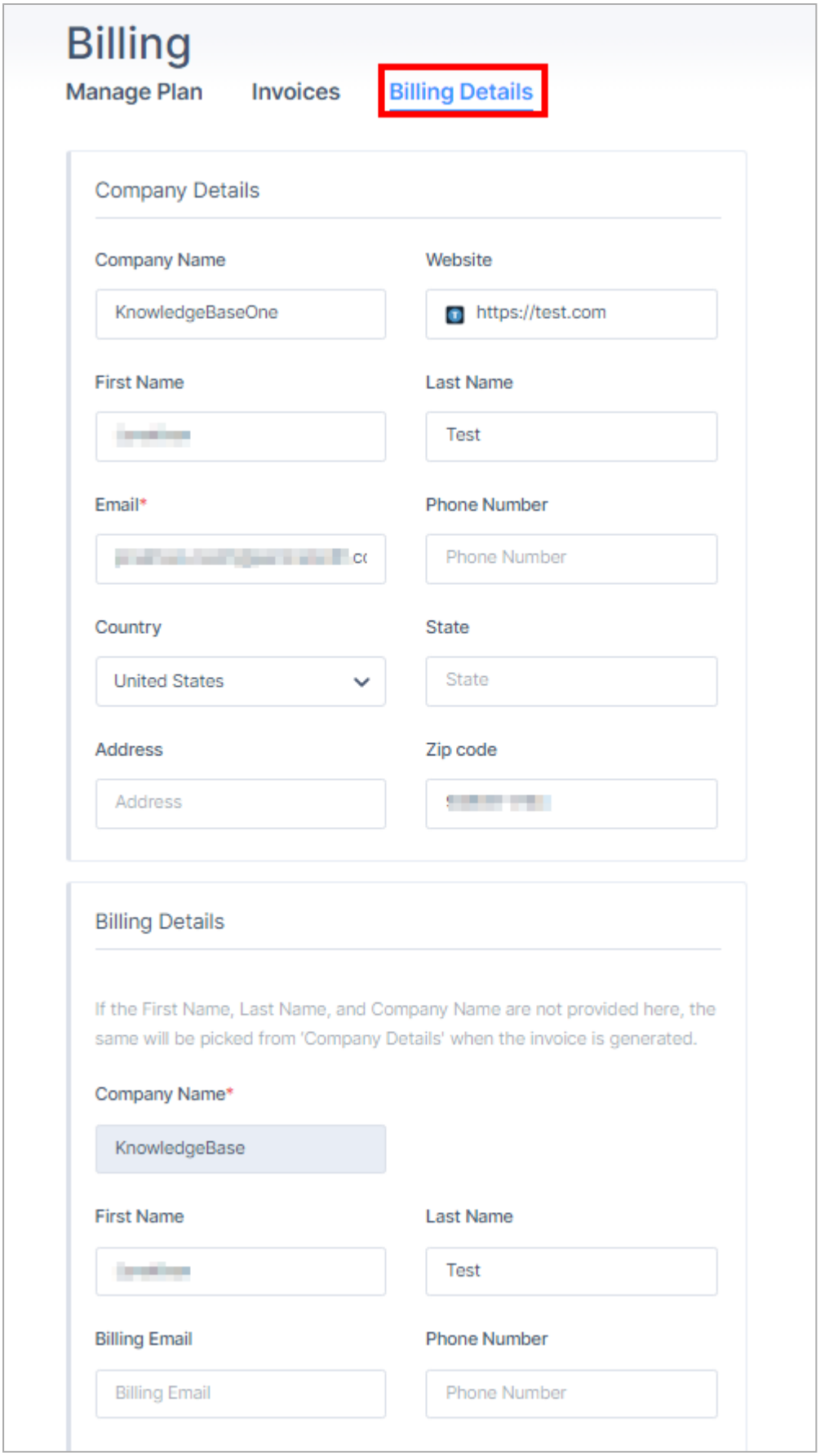
To download an invoice, click **Download**.

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**.

How-To and Troubleshooting References

How-To References

- For Harmony SASE Frequently Asked Questions (FAQ), see sk182225.
- For information on how to segment networks, see *"Segmenting Networks" on page 163*.
- For information on how to upload tunnel configuration files, see *"Using the Configuration File for Tunnel Configuration" on page 407*.
- For information on how to securely connect sites and cloud resources using Harmony SASE, see *"Interconnectivity (Cloud-Agnostic)" on page 165*.
- For information on how to create Route 53 Inbound Endpoints, see sk182274.
- For information on how to manage member devices, see *"Managing Members" on page 56*.
- For information on certificate manager and how to upload application domain certificate, see *"Certificate Manager" on page 900*.
- For information on how to whitelist resources, see sk182260.
- For integrating Google Cloud's Private Zone/Private DNS feature with Harmony SASE gateway, see *"Google Cloud DNS" on page 587*.
- For information on Google Cloud VPC Peering, *"Google Cloud VPC Peering" on page 586*.
- For information on how to change region and language for accurate Google search results, see sk182250.
- For information on how to change DNS settings in Windows and Mac, see sk182255.
- For information on how to remove the Wireguard Connector, see *"Removing the WireGuard Connector" on page 137*.
- For information on how to deactivate a gateway, see *"Deactivating a Gateway" on page 123*.

Troubleshooting References

- For troubleshooting common errors in IPsec Site-to-Site connection setup, see sk182243.

- For information on how to collect logs manually, see *"Collecting Logs Manually" on page 106*.
- For assigning Support Access role to Harmony SASE support engineer to temporarily access your tenant without credentials, see *"Support Access" on page 905*
- For troubleshooting web application issues, generate the HTTP Archive (HAR) file. For more information, see sk182245.
- For troubleshooting connectivity issue with Harmony SASE Agent, see sk182251.

Release Notes

- Harmony SASE Administrator Portal
  - *"2025" on page 937*
  - *"2024" on page 939*
- Harmony SASE Agent
  - *"Android / Chromebook" on page 953*
  - *"iOS" on page 952*
  - *"Linux" on page 950*
  - *"MacOS" on page 948*
  - *"Windows" on page 944*

Harmony SASE Administrator Portal

2025

February

New Features	▪ New PoP in Brussels - Launched a new Point of Presence (PoP) in Brussels, Belgium, expanding coverage and enhancing performance.
Feature Enhancements	▪ Hybrid-Split Tunneling Enhancement - Administrators are now guided to configure automatic split tunneling for optimal traffic routing. Existing configurations are migrated automatically with no impact on current networks. ▪ Microsoft Outlook is now excluded by default from Internet Access bypass rules. ▪ Administrators can now manage the multi-monitor settings for ZTA RDP applications. ▪ Improved security warning when disabling 2FA for local users. Administrators can now see a clear notification highlighting the security risks before confirming the action.
Resolved Issues	▪ P81-55537 - Bypassed URLs are now case-insensitive, ensuring consistent enforcement regardless of letter casing.

January

New Features	▪ The new **Hybrid Split Tunneling** functionality automates tunneling of private traffic only, ensuring an optimized end-user experience along with full connectivity (Currently available in Early Availability) ▪ Added two new predefined member roles, **Network Manager** and **User Manager**, for simplified management. These roles simplify permissions setup, enhance security, and improve access control. For more information, see Member Roles and Permissions. ▪ Added the new **Explore Harmony SASE** page that helps customers discover and understand Harmony SASE features. It guides them to enhance their security posture, manage SASE effectively, and follow best practices with video guides and tips. ▪ Harmony SaaS is now accessible through Harmony SASE, offering enhanced security for your SaaS applications. Make sure you have the appropriate license to fully utilize Harmony SaaS. For more information, refer to the Harmony SaaS solution brief (Currently available in Early Availability) ▪ Wildcard support is now available for URL Filtering rules, offering greater flexibility and efficiency. Use the * wildcard to match multiple URLs with similar patterns (for example, **.example.com* covers all subdomains and paths under example.com). For more information, see the blog post.
Feature Enhancements	N/A
Resolved Issues	N/A

2024

December

New Features	▪ Enhanced admin experience for managing groups – While assigning new members to a group, the **Assign new members** pane now supports improved search and scrolling, enabling easier navigation and management of groups with a large number of members. ▪ The Internet Access policy is now distributed to end users more efficiently and at a larger scale, ensuring quicker updates and improved performance. ▪ Introduced an enhanced **Get Started** wizard for Private Access Onboarding. ▪ Admins can now view the workspace name from the main dashboard. For example, a workspace name is required for agent installation.
Feature Enhancements	N/A
Resolved Issues	▪ P81-55727 - Retrieving custom properties for ZTA Dynamic RDP can end up with a timeout.

November

New Features	▪ **IDP Okta integration supports EU region** - IDP Okta now supports tenants and workspaces configured in the EU region. For more information, see here. ▪ **Customer Admin Role** - MSP admins can now create and manage granular access policies for child accounts.
Feature Enhancements	N/A
Resolved Issues	▪ P81-50352 - Deleted user groups are now visually distinguished on the User Groups page. ▪ P81-54824 - Positioning of addresses combo box and drop-down list is fixed, ensuring the appropriate controls' layout. ▪ P81-55740 - Resolved an issue that caused a "Cross origin login not allowed" error, blocking platform access after sign-up.

October

New Features	▪ **MSP Child Tenant Allocation** - Managed Service Providers (MSPs) can now manage access permissions for specific child tenants within their partner organization. This allows MSPs to control and allocate access for team members, ensuring that only authorized personnel can manage designated child tenants, enhancing security and streamlining tenant administration. ▪ You can now avail a 30-day free trial of the complete Harmony SASE platform.
Feature Enhancements	N/A
Deprecations	▪ Configuring members' image is now deprecated.
Resolved Issues	▪ P81-51616 - Clicking on Device Name leads to the proper page, based on the tenants' licensing. ▪ P81-52473 - Logging out when using Google SSO, logs out Google account entirely. ▪ P81-52796 - Auto logout at 3am, doesn't work when session duration is set to 24 hours. ▪ P81-54660 - Firewall logs not generated for rules created by API ▪ P81-54685 - Disable Sign-out option not available ▪ P81-51935 - ZTA application fails to load after gateway upgrade

September

New Features	▪ **Native RDP support** - This feature enables users to connect to agentless applications through their native RDP client. It now offers improved performance, multi-monitor support, and clipboard and printing controls for a more seamless experience. ▪ **Personal RDP for agentless application access** – Generates personalized RDP access based on the user's IDP attributes. It is available for beta customers. ▪ **Copilot available for Harmony SASE** - Administrators can now consult the **Infinity AI Copilot** within the Infinity Portal for topics related to Harmony SASE. We have trained our LLM model on our SASE documentation and it currently supports queries on an array of Harmony SASE topics, including setup, configuration, features, best practices, and more. ▪ Allow usage of single IP Address in Redundant IPSec tunnel.
Feature Enhancements	N/A

Resolved Issues	▪ P81-51169 - Improved policy editing for a smoother user experience. ▪ P81-51040 - Allow the admin to unblock a user when the user is signed in to multiple tenants. ▪ P81-51187 - Active sessions now accurately display detailed user information for VPN-connected sessions, while addressing previous discrepancies.

August

New Features	▪ Bundle of Harmony SASE with Harmony Browse is now GA. The service is available with a new SKU. ▪ Enhanced session synchronization with the Infinity Portal.
Feature Enhancements	N/A
Resolved Issues	N/A

July

New Features	▪ **MSPs Support**: • Support for PAYG plan for sub-tenants. • Support for MSPs with a large number of sub-tenants. ▪ **Added new regions**: • New York 3, USA • London 3, UK • Sao Paulo 3, Brazil ▪ Improved network operations infrastructure in APAC. ▪ **Sign In** page now shows the data residency region in the Workspace drop-down list. ▪ Updated the Wireguard connector script to support Ubuntu 24.04 LTS and future versions.
Feature Enhancements	N/A
Resolved Issues	▪ P81-47263 - iPad agent is signed out the next day, in case it remained connected overnight ▪ P81-48176 - SAML 2.0 IDP URL configuration now supports all valid domain extensions, allowing for broader customization

June

New Features	■ Added a new **Remove Device** action on the **Device Inventory** page, allowing Administrators to optimize device inventory by removing unused devices. ■ Partners can now create trial tenants for their customers with a 30-day free trial to evaluate Harmony SASE. When a partner creates a new trial workspace for a customer, select the **Premium+30 Day** trial plan. ■ Improved Gateway geographic location announcements (RFC 9092)
Feature Enhancements	N/A
Resolved Issues	■ P81-46499 - Active user sessions, accessible from the dashboard, now display the correct country under Session Origin. ■ P91-46780 - Device posture check (DPC) for Mac agents is compatible with Check Point's End Point process names.

May

New Features	A new **Browser Security** menu is now available (in Beta). It supports the new *Internet Security Essentials+* offering which includes the Harmony Browse browser extension.
Feature Enhancements	N/A
Resolved Issues	■ P81-42112 - Can't create a group where the name contains ":" ■ P81-46478 - Can't create a network with /22 subnet ■ P81-39418 - Can't update Configuration profile

April

New Features	Harmony SASE now supports EU data residency, using a separate new instance of the platform.
Feature Enhancements	■ Aligned Web Filtering category names to Check Point standard categories. ■ Added support for **Specific Service Roles** in the Check Point Infinity Portal, so users with a Read-Only role in the portal can be given an Admin role specifically for Harmony SASE. ■ Implemented minor UI fixes.
Resolved Issues	N/A

March

New Features	N/A
Feature Enhancements	▪ Zero trust applications - Added an **Access for Members** button for admins to display the URL to be sent to users to allow access. ▪ Further platform scalability improvements.
Resolved Issues	▪ P81-38343 - Networks tab - 'undefined' error

February

New Features	▪ SWG certificates for macOS can now be installed using MDM tools. This allows administrators to configure SWG (Internet Access) seamlessly for macOS devices using MDM tools without user intervention. The certificate can be generated and downloaded from the tenant **Downloads** page. **Harmony SASE** Agent for macOS version 10.4 and above supports this functionality.
Feature Enhancements	▪ Two-Factor authentication improvements: • Added support for Duo Security Universal Prompt. • Changed verbiage to better reflect the support for different TOTPs such as Microsoft Authenticator and Google Authenticator. ▪ IDP/SCIM Integration - Added support for syncing user names which include commas. ▪ Web Activity page: • Log data in the table is now updated when changing selection in the widgets. • Improved display for deleted users. ▪ Scalability improvements in the web platform to support large customers.
Resolved Issues	N/A

January

New Features	▪ Rebranded to **Harmony SASE** and changed to the **Harmony** pillar in Check Point Infinity Portal.
Feature Enhancements	▪ SCIM Group Sync for Okta is now available to all customers.
Resolved Issues	N/A

Harmony SASE Agent

Windows

11.2.1.2378

Release Date	22 January 2025
New Features	N/A
Enhancements	▪ New URL Reputation security engine detects and prevents access to malicious URLs. (Available in Early Availability (EA) mode) ▪ New Threat Emulation engine uses connected sandboxes to prevent multi-stage attacks at the earliest available stage. (Available in Early Availability (EA) mode)
Resolved Issues	▪ P81-53008 - Long VPN connection time post device reboot ▪ P81-53330 - DNS connectivity loss post network connection ▪ P81-54570 - Some deny logs does not appear in management platform ▪ P81-55316 - Trusted environment users are presented in platform as VPN connected users
Status	Under gradual rollout to all customers.
Download Agent	Download

11.1.0.2248

Release Date	12 November 2024
New Features	N/A
Enhancements	▪ Enhanced Trusted Network capability, now supporting the use of an HTTPS server and a TLS certificate ▪ Implemented a comprehensive update to our Malware protection engine

Resolved Issues	▪ P81-47954 - Users experience BSOD ▪ P81-51792 - Device status does not updates after sleep when connected to trusted router

11.0.11.2205

Release Date	16 October 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-54903 - User gets stuck in obtaining an IP address mode

11.0.10.2177

Release Date	30 September 2024
New Features	N/A
Enhancements	▪ Added support for wildcards in URL filtering rules
Resolved Issues	▪ Updated vulnerable library (CVE-2024-21907) ▪ P81-48205 - Unable to remove configured default DNS

11.0.1.2083

Release Date	28 August 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ Mitigation for OpenVPN vulnerability (CVE-2024-1305) ▪ P81-50980 - Custom URL SWG allow rule mismatch

11.0.0.2050

Release Date	30 July 2024
New Features	N/A

Enhancements	▪ Implemented a comprehensive update to our Web filtering security engine. ▪ Rebranded the task bar icons. ▪ Rebranded **Block**, **Warn**, and **Malware Protection** pages. ▪ Renamed installation file from *Perimeter81_10.x.x.xxxx.msi/exe* to *HarmonySASE11.x.x.xxxx.msi/exe* ▪ Bug fixes and stability improvements.
Resolved Issues	▪ P81-36415 - Agent not opening channel ▪ P81-38160 - Unexpected Timeout On Agent ▪ P81-38285 - Stuck in Connecting State when on Trusted Routers ▪ P81-42138 - Windows 10.5 Web activity doesn't log events when signed out ▪ P81-42248 - Windows agent installer deploys with older .net8 version ▪ P81-46702 - Windows agent connected to EU platform is not showing the GW IP but the native IP address ▪ P81-47192 - SWG not blocking site

10.5.2.1979

Release Date	28 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-47112, P81-47119, P81-47205 - Latency issue with Citrix and RDP

10.5.1.1790

Release Date	20 May 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-37892 - Compatibility with N-Able Web protection ▪ P81-38465 - Windows 11 machines BSOD with specific netio.sys with DRIVER_IRQL_NOT_LESS_OR_EQUAL ▪ P81-39767 - SWG events initially not sent correctly after switching to a workspace in a different region

10.5.0.1760

Release Date	29 March 2024

New Features	Secure Web Gateway (which includes Web Filtering and Malware Protection) now stays active even when the user is signed out of the agent, using the most recently cached web filtering policy. The user interface has been updated to show that the SWG is enabled in this situation. If allowed by the admin, the SWG can be turned off by quitting the agent.
Enhancements	▪ The agent supports the new European Data Residency instance of Harmony SASE, which will be launched in April. The data residency region can be configured when installing the agent using a new 'region' parameter, or by switching to it from the platform sign-in page when signing in to the agent. ▪ Improved, simplified connection logic and refactoring for speed. ▪ Agent logging events have been moved to a new, robust and more scalable infrastructure. ▪ Improvements to the Web Filtering category resolving mechanism. ▪ .Net version updated to 8.0. ▪ The agent is now signed with a Check Point certificate instead of a Perimeter 81 certificate.
Resolved Issues	▪ P81-27360 - DNS resolution issue when using split tunneling + Custom DNS ▪ P81-35882 - Latency in video calls (Zoom, Google Meet) ▪ P81-36299 - Web Filtering rule with all categories is applied partially ▪ P81-38526 - Memory used by agent grows over time

10.4.3.1672

Release Date	27 February 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	P81-37301 - Compatibility issue with external DNS filtering tool

10.4.2.1645

Release Date	29 January 2024
New Features	N/A
Enhancements	The Perimeter 81 agent is now rebranded to Check Point - Harmony SASE.
Resolved Issues	N/A

MacOS

11.2.1.3411

Release Date	22 January 2025
New Features	N/A
Enhancements	▪ Enhanced Trusted Network capability, now supporting the use of an HTTPS server and a TLS certificate. ▪ Implemented a comprehensive update to the Malware protection engine. ▪ New URL Reputation security engine detects and prevents access to malicious URLs (Available in Early Availability (EA) mode) ▪ New Threat Emulation engine uses connected sandboxes to prevent multi-stage attacks at the earliest available stage. (Available in Early Availability (EA) mode)
Resolved Issues	▪ P81 - 51175 – SWG not active after reboot ▪ P81 - 54570 – Some deny logs do not appear in management platform
Status	Under gradual rollout to all customers.
Download Agent	Download

11.0.10.2696

Release Date	21 October 2024
New Features	N/A
Enhancements	▪ Added support for wildcards in URL filtering rules ▪ Renamed installation file from **Perimeter81_10.x.x.xxxx.pkg** to **Harmony_SASE_11.x.x.xxxx.pkg**
Resolved Issues	▪ P81-51175 - Agent failed to start URL filtering after reboot ▪ P81-50195 - Agent blocked downloads from IBM aspera ▪ P81-37249 - User can't run FaceTime calls when URL filtering feature is enabled

11.0.1.2339

Release Date	28 August 2024
New Features	N/A

Enhancements	N/A
Resolved Issues	▪ Mitigation for OpenVPN vulnerability (CVE-2024-1305) ▪ P81-50980 - Custom URL SWG allow rule mismatch

11.0.0.2227

Release Date	7 August 2024
New Features	N/A
Enhancements	▪ Implemented a comprehensive update to our Web filtering security engine. ▪ Rebranded the taskbar icons. ▪ Rebranded **Block**, **Warn**, and **Malware Protection** pages.
Resolved Issues	▪ P81-37479 - Quick access UI disappear ▪ P81-37717 - Failed to connect to private access network ▪ P81-38526 - Agent memory usage ▪ P81-39300 - Agent frequent disconnects ▪ P81-40851 - Can't remove Trusted Wi-Fi from Trusted network list ▪ P81-46855 - Changing network requires device admin's permission ▪ P81-46907 - Agent unexpected crashes

10.5.0.1476

Release Date	29 March 2024
New Features	Secure Web Gateway (which includes Web Filtering and Malware Protection) now stays active even when the user is signed out of the agent, using the most recently cached web filtering policy. The user interface has been updated to show that the SWG is enabled in this situation. If allowed by the admin, the SWG can be turned off by quitting the agent.
Enhancements	▪ The agent supports the new European Data Residency instance of Harmony SASE, which will be launched in April. The data residency region can be configured when installing the agent using a new 'region' parameter, or by switching to it from the platform sign-in page when signing in to the agent. ▪ Agent logging events have been moved to a new, robust and more scalable infrastructure.

Resolved Issues	▪ P81-37479 - UI is hidden on mouse cursor move when an application is running full-screen in the background ▪ P81-37735 - Unable to connect to the agent when Mac has Homebrew installed

10.4.2.1198

Release Date	29 January 2024
New Features	N/A
Enhancements	The Perimeter 81 agent is now rebranded to Check Point - Harmony SASE.
Resolved Issues	N/A

Linux

10.0.1.885

Release Date	30 December 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-58390 - Login fail in ubuntu 20.04.6 ▪ P81-59734 - Split tunnel include mode bug on private DNS
Download Agent	Download

10.0.0.879

Release Date	04 December 2024
New Features	▪ Support for split tunneling configuration by domains (FQDN)
Enhancements	N/A
Resolved Issues	N/A

9.0.1.843

Release Date	03 June 2024
New Features	N/A

Enhancements	N/A
Resolved Issues	▪ P81-46506 - apt remove perimeter81 could delete /home/user folder when specific chars are used ▪ P81-46999 - Errors when uninstalling from terminal

9.0.0.832

Release Date	24 April 2024
New Features	▪ The Perimeter 81 agent is now rebranded to Check Point - Harmony SASE. This includes new logos and a new color scheme. ▪ Secure Web Gateway (SWG) now includes Malware Protection. SWG users now have an additional layer of protection against malicious software, on top of the existing web filtering functionality. Malware Protection actively scans content before it reaches the user's browser, blocks multiple types of threats, and notifies the user. Admins can view logs of blocked malware in a new page under the **Monitor & Logs** section.
Enhancements	▪ The agent supports the new European Data Residency instance of Harmony SASE, launched earlier in April. The data residency region can be configured when installing the agent using a new 'region' parameter, or by switching to it from the platform sign-in page when signing in to the agent. ▪ The agent now reports the exact Linux distribution (Ubuntu 23.04) in the **Device Inventory** page. Also, the agent version number now has a lin_ prefix to align the versioning with the other operating systems.
Resolved Issues	▪ P81-37246 - Agent not displaying DPC failure notifications ▪ P81-34266 - SWG bypass rule not being respected ▪ P81-40066 - Issue connecting to shared networks with openVPN protocol ▪ P81-41876 - RHEL & Fedora - issue connecting with split tunneling enabled

8.1.0.778

Release Date	23 November 2023
New Features	N/A
Enhancements	Deprecated IKEv2 protocol as a method of agent connection and removed it from the agent UI

Resolved Issues	▪ P81-24634, P81-26185 - Agent is stuck while connecting ▪ P81-26613 - Connection takes too long ▪ P81-27881 - Agent disconnects and connects constantly ▪ P81-27963 - Agent crashes after 8 hours ▪ P81-28239 - Unable to connect to network until restarting helper service + crashes ▪ P81-29403 - Agent is failing to launch on Fedora 38 ▪ P81-28797 - When returning from sleep, agent does not reconnect to VPN ▪ P81-34181 - Issue when updating UI to latest version on RHEL

iOS

8.3.0.2600

Release Date	25 September 2024
New Features	N/A
Enhancements	▪ New application icon
Resolved Issues	▪ P81-48119 - App stuck in loading page
Download Agent	Download

8.2.0.1934

Release Date	13 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-47262 - App stuck on splash screen

8.1.0.1831

Release Date	03 June 2024
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-30654 - Agent keeps disconnecting and reconnecting ▪ P81-46602 - OS version is displayed incorrectly in the Device Inventory page

8.0.0.1730

Release Date	12 May 2024
New Features	N/A
Enhancements	▪ The agent is now rebranded to Check Point - Harmony SASE. ▪ The agent supports the new European Data Residency instance of Harmony SASE. ▪ The agent now blocks usage on jailbroken devices.
Resolved Issues	▪ P81-30654 - Agent keeps disconnecting and reconnecting ▪ P81-42234 - When typing the sign-out code, digits are not visible in dark mode ▪ P81-42091 - Private DNS icon is not displayed in the agent

7.0.6.1

Release Date	01 August 2023
New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-14047 - Agent does not open on iPad ▪ P81-12409 - AppStore crash reports ▪ P81-7559 - Occasional disconnections during long sessions ▪ P81-7245 - Wrong app version shown in Monitoring Dashboard ▪ P81-5900 - Issue logging out users by the workspace admin ▪ P81-3133 - 'Login error. Failed to establish SDP socket connection' when no Internet connection is available ▪ P81-2676 - Automatic Wi-Fi Security doesn't work on unsecured networks ▪ P81-2396 - Device Posture Check - the user isn't signed out when DPC failed (but still cannot connect) ▪ P81-2359 - No autoconnect to the next network if existing network was deleted, while AlwaysOn is enabled ▪ P81-1956 - VPN does not connect automatically when signing in ▪ P81-1542 - Auto Reconnect value is set to OFF on every disconnect when changing networks

Android / Chromebook

8.1.2.3355

Release Date	29 November 2024

New Features	N/A
Enhancements	N/A
Resolved Issues	▪ P81-47928 - Nonresponsive connect button during agent installation on Chromebook
Download Agent	Download

8.1.0.3337

Release Date	25 September 2024
New Features	N/A
Enhancements	▪ Android 14 support ▪ New application icon
Resolved Issues	N/A

8.0.0.3276

Release Date	9 April 2024
New Features	N/A
Enhancements	▪ The agent is now rebranded to Check Point - Harmony SASE. ▪ The agent supports the new European Data Residency instance of Harmony SASE. ▪ IKEv2 protocol deprecated as a method of agent connection - removed from agent UI.
Resolved Issues	▪ P81-33813 - Users can't connect Agent using Android - Job Cancellation Exception ▪ P81-34474 - Obfuscation of data

7.1.9.2577

Release Date	13 February 2024
New Features	N/A
Enhancements	▪ Updated reconnection logic. ▪ Improved logging. ▪ When the user session expires (according to the session length set by the administrator), the agent automatically logs out during local night time, to avoid disconnections during the workday. This applies to session lengths of two days and higher. ▪ Prevent usage on rooted devices.

Resolved Issues	▪ P81-19677 - StackOverflowError in Sets.kt ▪ P81-18833 - Failed to login with 'Too Many Open Sessions' error ▪ P81-18608 - Agent does not present 'All the time' option in Location Permissions, causing disconnects when idle

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.