

GUIDE

# CLOUD SECURITY WITH CISCO+ SECURE CONNECT

Portal User Guide

# Table of contents

- Getting started** .....4
- About Cloud Security with Cisco+ Secure Connect Portal..... 4
- Quick links** .....4
- Secure Connect Knowledge Base..... 4
- Resources for Administrators ..... 4
- Logging in**.....4
- Monitor**..... 5
- Overview (Secure Connect Dashboard)..... 5
- Security ..... 6
- Policy Count ..... 6
- Sites ..... 7
- Network Tunnels..... 7
- Remote Access ..... 8
- Private Applications..... 9
- Public Applications ..... 9
- Security Activity ..... 10
- Remote Access Log..... 11
- Audit Log ..... 11
- Identities and Connections** ..... 12
- Users..... 13
- Viewing Users and User Activity ..... 13
- Viewing User Groups..... 13
- Managing Users and User Groups ..... 16
- Applications** ..... 17
- Private Applications..... 18
- Public Applications ..... 22
- Application Groups and Categories ..... 23
- Sites** ..... 24
- Network Tunnels**..... 25
- Remote Access ..... 26
- Policies**..... 27
- Policies Overview ..... 27
- Browser Access..... 27

# Table of contents

Endpoint Posture .....	28
DNS .....	29
Web .....	31
Firewall .....	32
Data Loss Prevention .....	33

## Getting started

### About Cloud Security with Cisco+ Secure Connect

The Secure Connect Admin Portal allows administrators to view and configure most aspects of their Cloud Security with Cisco+ Secure Access service, including:

- Dashboard view of user activity and security threats.
- View and manage client based access to SaaS, internet and private applications.
- View and manage clientless access to private applications.

## Quick links

### Secure Connect Knowledge Base

[Secure Connect Self Help - Portal Documentation](#)

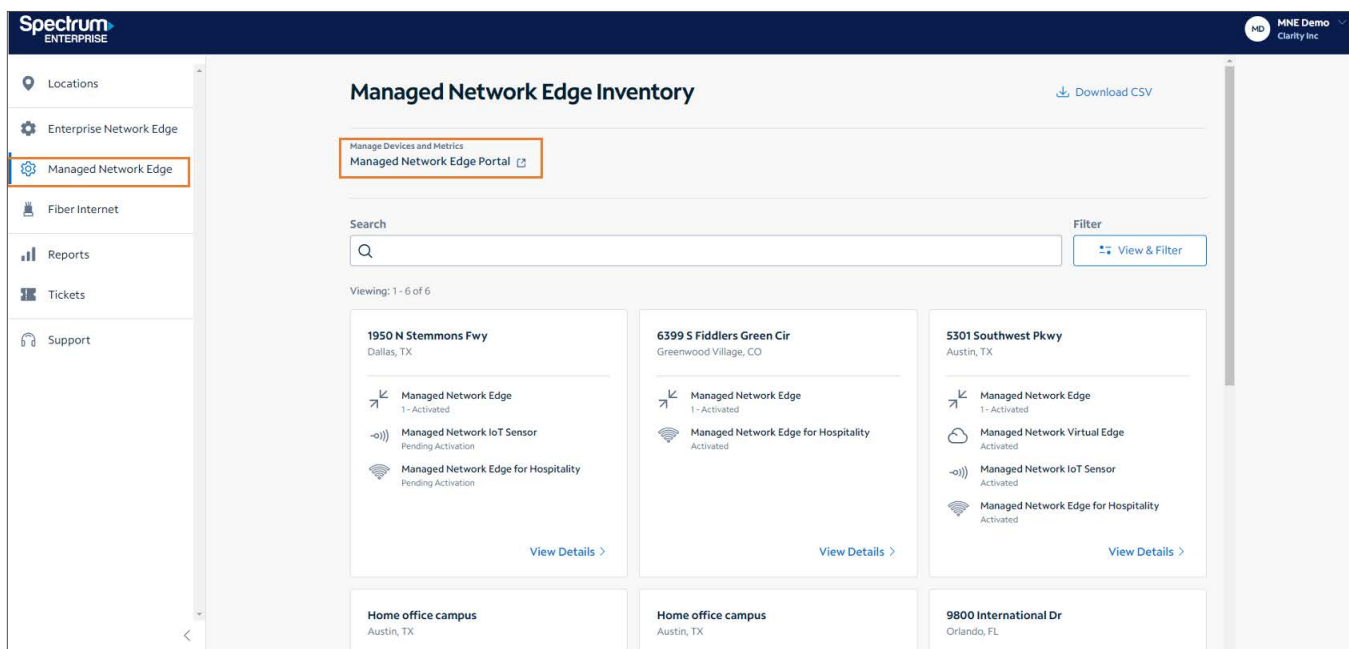
### Resources for Administrators

Spectrum Enterprise Managed Service support for Configuration and technical Support: 1-888-812-2591.

## Logging in

Log into your [Login | Spectrum Enterprise](#) account then navigate to the **Managed Network Edge** option from the menu on the right side of the portal.

Click on **Managed Network Edge Portal** to be connected directly to the Meraki dashboard via SSO.



It is also possible to login directly to the Meraki dashboard and the [Secure Connect Admin Portal](#) with the credentials provided during the service activation process.

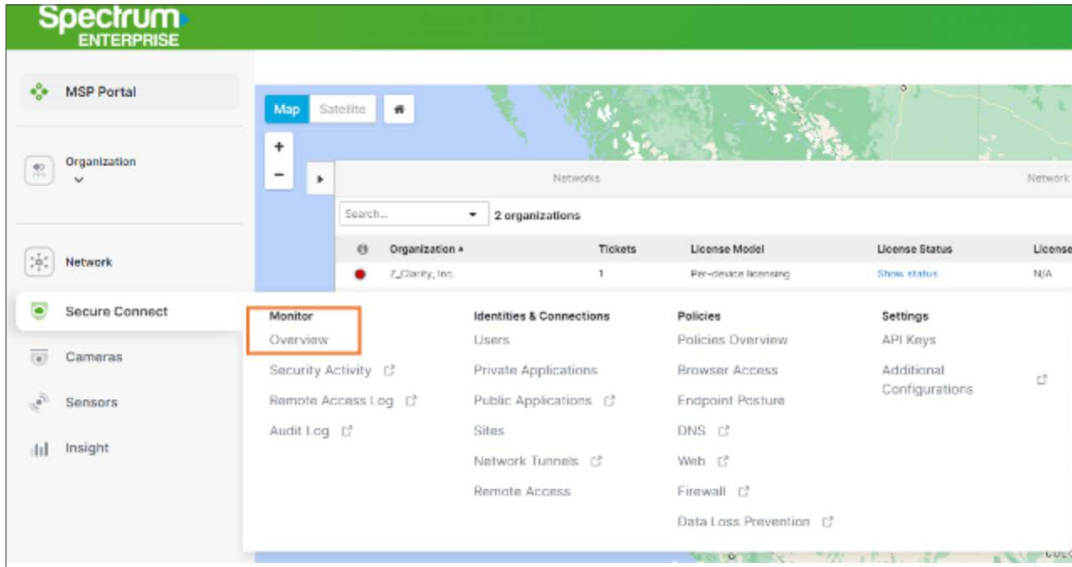
The Secure Connect portal menu will include direct links to the Cisco Umbrella portal [ [🔗](#) ] where security policies for web traffic, application, and users can be viewed and managed. From the Cisco Umbrella portal, you can always return to the Secure Connect portal by clicking the **Return to Secure Connect** box at the top of the page.

## Monitor

The Monitor section of the Secure Connect portal provides visibility to user and security events on the network.

### Overview (Secure Connect Dashboard)

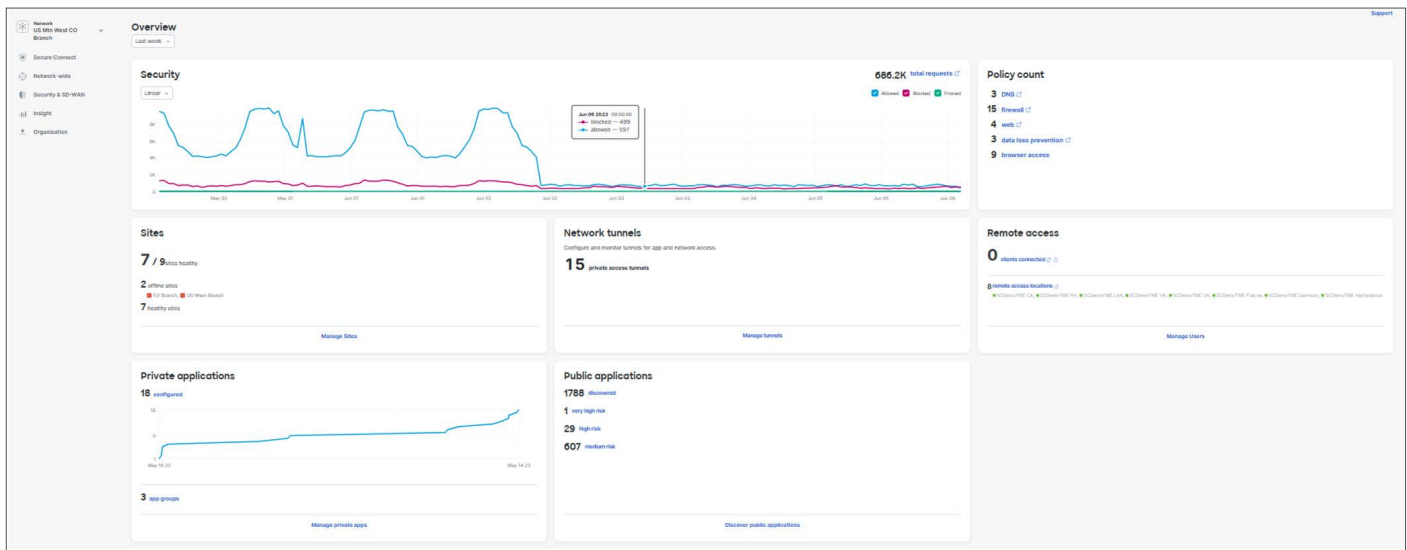
- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Monitor** then **Overview** to see a high-level dashboard view of your organization’s connectivity and security posture.



The Overview Tab provides a dashboard with visibility to:

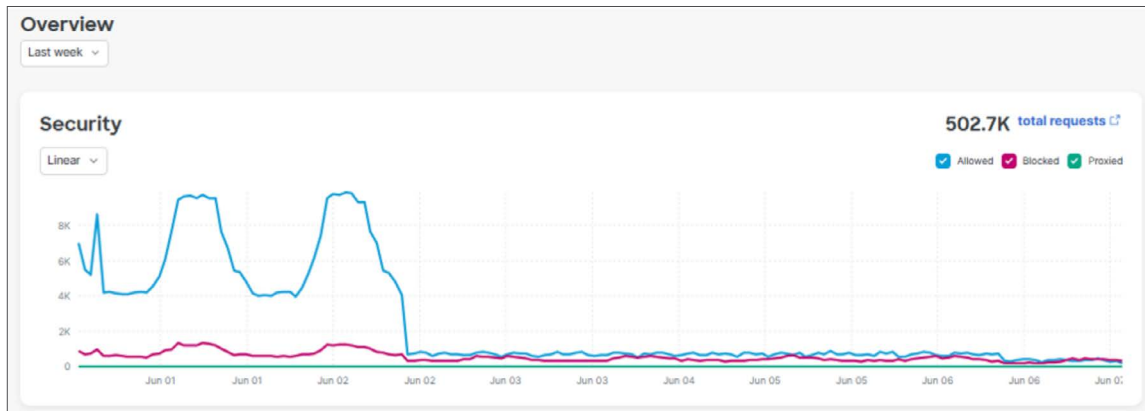
- Remote User activity including access attempts, count and location of users.
- Security policy summary.
- Health of Connections from Cisco Secure Connect to Meraki devices.
- Public and Private application connections and security threats.

- From the dashboard, click on the drop down under Overview to select the period of time you want to view.



### Security

1. The Security box in the top left side of the dashboard provides Administrators a view of historical information about user authentication including authentication attempts allowed, blocked, and proxied.



2. Click **total requests** to see activity log on the Cisco Umbrella platform.

Reporting / Core Reports  
Activity Search

RETURN TO SECURE CONNECT Schedule Export CSV LAST 24 HOURS

FILTERS Search by domain, identity, or URL. Advanced

Search filters

24,925 Total Viewing activity from Jun 6, 2023 5:33 PM to Jun 7, 2023 5:33 PM Results per page: 50 1 - 50

Request	Identity	Policy or Ruleset Identity	Destination	Destination IP	Internal IP	Ext
FW	Branch Access orgid:7478818	Branch Access orgid:7478818		192.168.128.3	10.1.200.115	...
FW	Branch Access orgid:7478818	Branch Access orgid:7478818		192.168.128.3	10.1.200.115	...
FW	Branch Access orgid:7478818	Branch Access orgid:7478818		192.168.128.3	10.1.200.115	...
FW	Branch Access orgid:7478818	Branch Access orgid:7478818		192.168.128.3	10.1.200.115	...
FW	Branch Access orgid:7478818	Branch Access orgid:7478818		192.168.128.3	10.1.200.115	...
FW	Branch Access orgid:7478818	Branch Access orgid:7478818		192.168.128.3	10.1.200.115	...

Response: Allowed, Blocked, Selectively Proxied  
Warn Page Behavior: Warned, Accessed After Warn

3. The Activity Search page is a log of activity requests. Users can search field and/or apply filters in the column on the right to see specific activities.
4. Use the options on the upper left side of the screen to **schedule** reports, **export** logs and select date range of logs.
5. Click the **Return to Secure Connect** box to return to the dashboard.

### Policy count

1. From the dashboard, Administrators can see the number of policies established for user traffic.



2. Click on any of the words in **blue** to be redirected to the Cisco Umbrella platform to view security policy details.

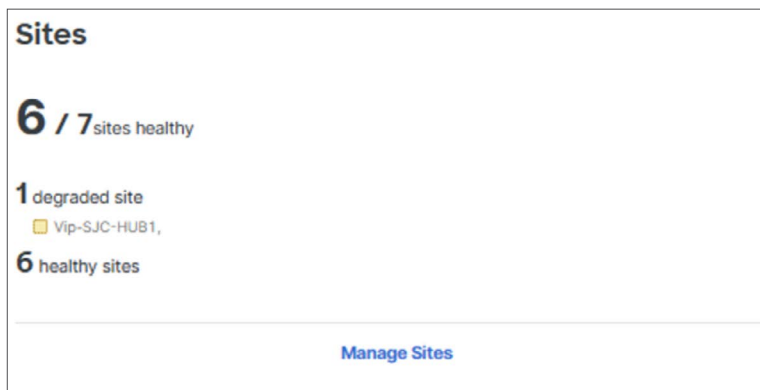
**NOTE: Browser Access** policies are contained within the Secure connect portal, not Cisco Umbrella.

Go to the **Policies** section of the Secure Connect Menu for more information on each of these policies:

- [DNS](#)
- [Firewall](#)
- [Web](#)
- [Data Loss Prevention](#)
- [Browser Access](#)

### Sites

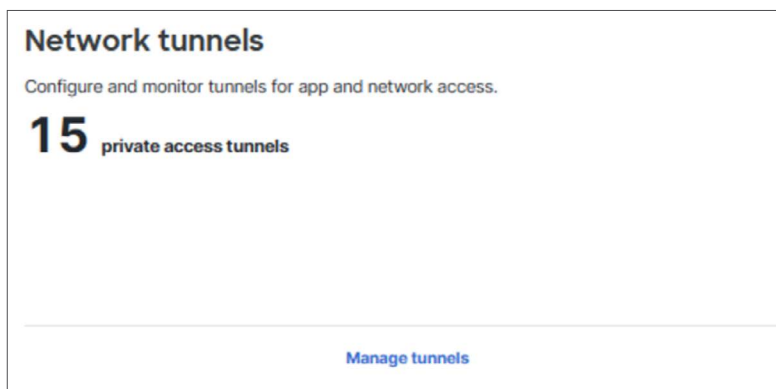
1. From the dashboard, Administrators can see the number of Meraki sites connected to the Secure Connect platform as well as the health of the connection to the site.



2. Click on **Manage Sites** to see/manage each site.
3. Go to the [Sites](#) section of the Secure Connect Menu for more information on the sites connected to the Secure Connect platform.

### Network Tunnels

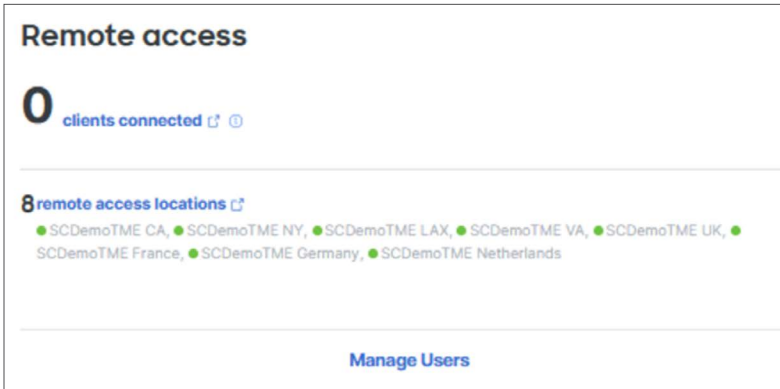
1. From the dashboard, Administrators can see the number tunnels connecting sites to the Secure Connect platform.



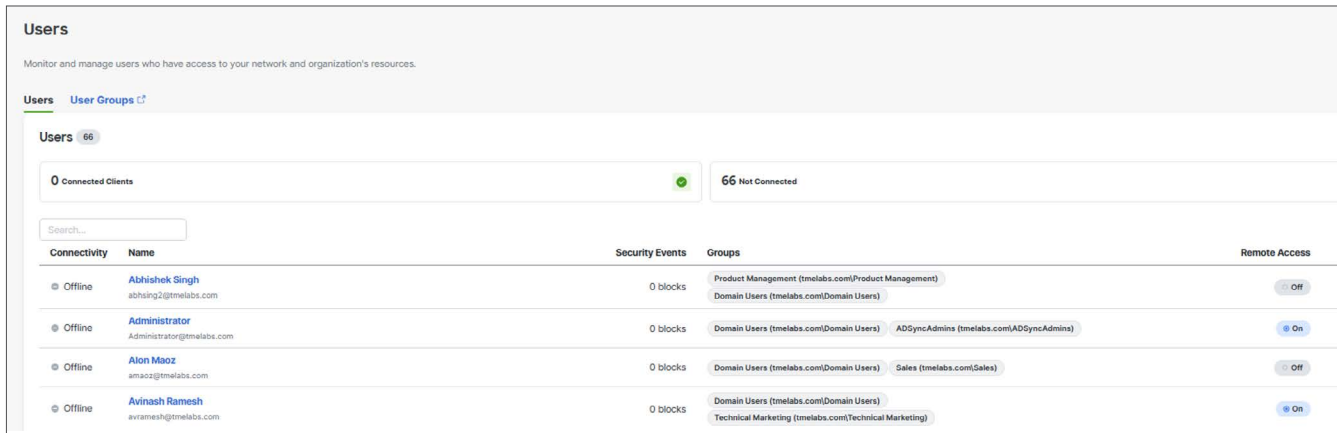
2. Click on **Manage Tunnels** to see/manage each site.
3. Go to the [Network Tunnels](#) section of the Secure Connect Menu for more information on the tunnels connected to the Secure Connect platform.

**Remote Access**

1. From the dashboard, Administrators can see the number of users (clients) connected via remote access as well as the Cisco Secure Connect locations.



2. Click on **Manage Users** to monitor/manage users and user groups who have access to your network and organization’s resources.

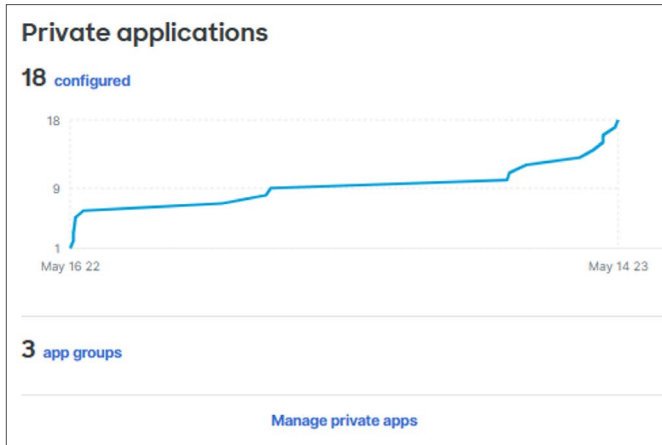


3. The User section provides the following information:
  - Count of users connected/not connected.
  - Connectivity Status.
  - User Name.
  - Security Events.
  - User Groups.
  - Remote Access (On/Off).
4. Use the search field to find a specific user.
5. Go to the [Users](#) section of the Secure Connect Menu for more information on managing users.



### Private applications

- From the dashboard, Administrators can see the number of Private Applications configured for access by remote users.



- Click on **Manage Private Apps** to monitor/manage the Private applications that have been configured to allow access from remote users as well as the user groups that have permissions to access the applications. Toggle the drop down next to **Applications** to see a historical view of applications.

**Applications** Last 2 hours

Private Apps Public Apps App Groups & Categories

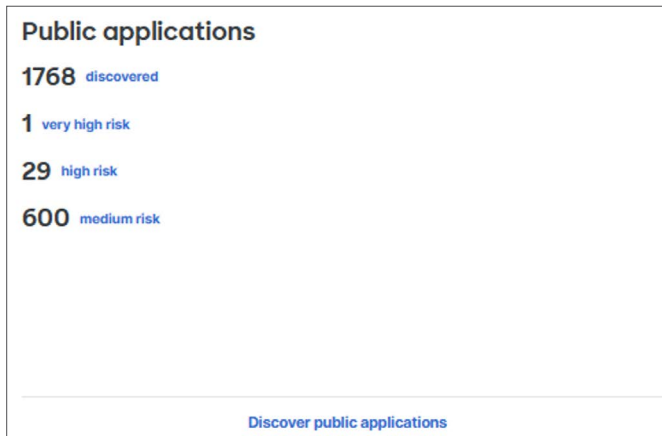
Total Apps 18 + Add App

Private application	Associated groups	Last Modified
a-super-app		Apr 27, 2023 4:38 PM
AS400-Retail-POS-App		May 4, 2023 11:12 AM
Console-Access		May 4, 2023 11:39 AM
Data Center		May 19, 2022 7:20 PM

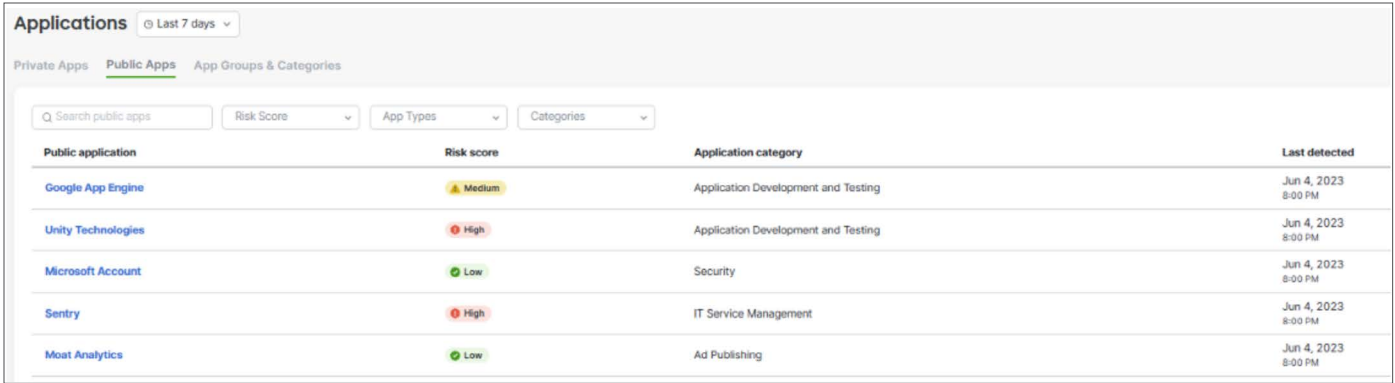
- Go to the [Private Applications](#) section of the Secure Connect Menu for more information on managing Private Applications.

### Public applications

- From the dashboard, Administrators can see the number of Public Applications accessed by remote users as well as the associated risk of these applications.



- Click on **discovered** or **Discover Public applications** to see a full list of applications, associated risk score, application category, and date last detected. Use the search bar and filter options to find specific applications.
  - Users can also click on the **blue** word next to the number for a short cut to a list of specific applications for each category.

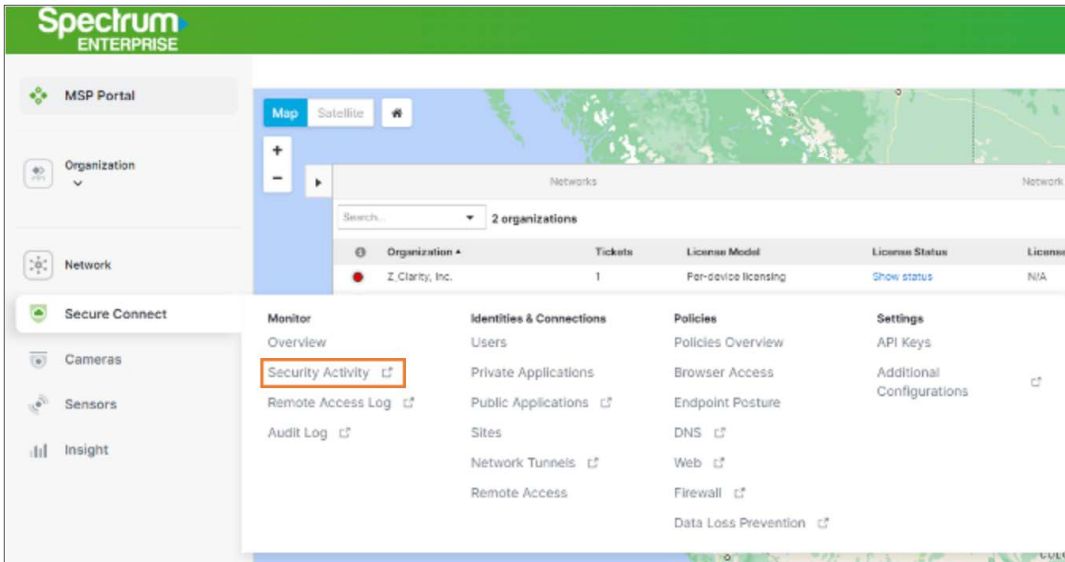


Public application	Risk score	Application category	Last detected
<a href="#">Google App Engine</a>	Medium	Application Development and Testing	Jun 4, 2023 8:00 PM
<a href="#">Unity Technologies</a>	High	Application Development and Testing	Jun 4, 2023 8:00 PM
<a href="#">Microsoft Account</a>	Low	Security	Jun 4, 2023 8:00 PM
<a href="#">Sentry</a>	High	IT Service Management	Jun 4, 2023 8:00 PM
<a href="#">Most Analytics</a>	Low	Ad Publishing	Jun 4, 2023 8:00 PM

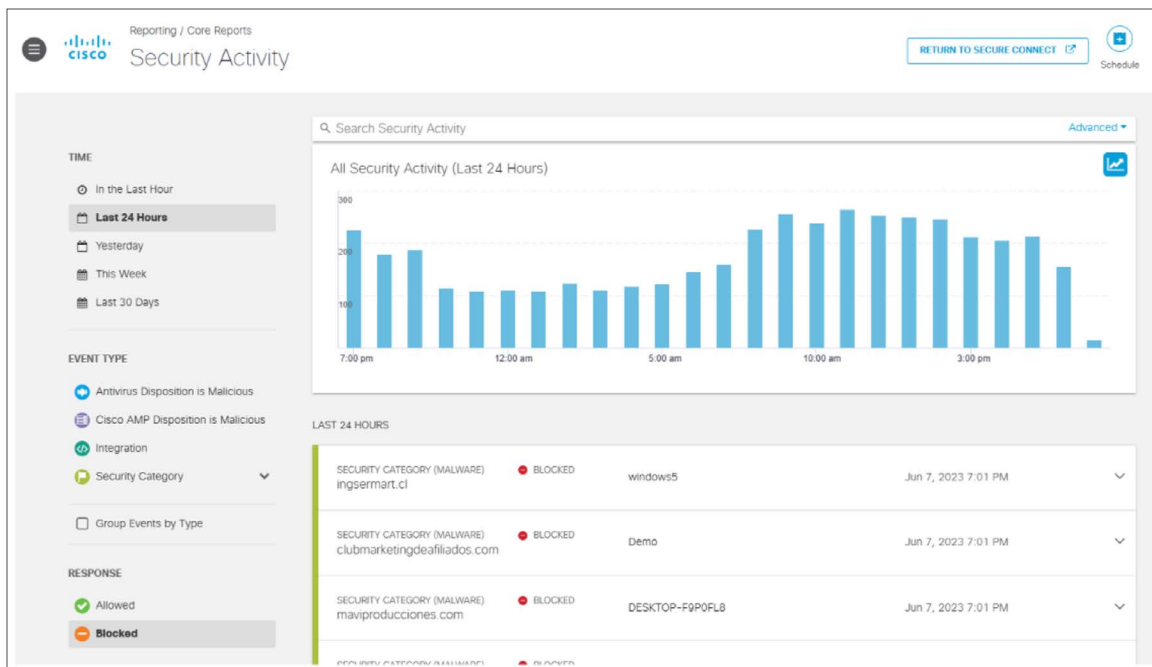
- Go to the **Public Applications** section of the Secure Connect Menu for more information on managing Public Applications.

### Security Activity

- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Monitor** then **Security Activity** to see a graph of all security activity within a specific time period.



- The Security Activity page in the Cisco Umbrella portal shows a graph of security events for a specific time period as well as log data for each security event.

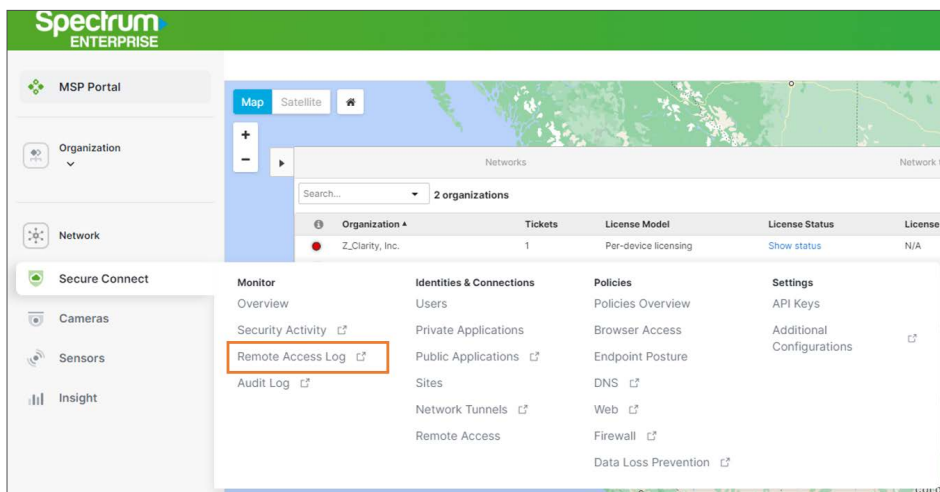


- Click on Advanced to search for a specific security event.
- Click on options in the menu on the left side of the page to apply a filter for a specific time period, event type, or security response.
- Click the Schedule button in the upper left hand corner to schedule a report.
- Click the **Return to Secure Connect** box to return to the Secure Connect portal.

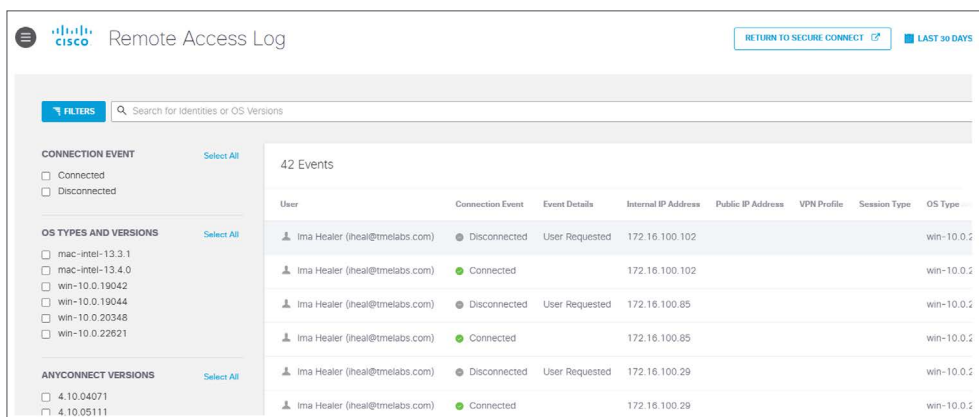
### Remote Access Log

The Remote Access Log page in the Cisco Umbrella portal shows events for users in a specific time period such as when users connect, disconnect, and what applications they use. This information can be helpful for troubleshooting problems, identifying security threats, and auditing user behavior.

- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Monitor** then **Remote Access Log** to see log data for remote users.



- The remote access log page in the Cisco Umbrella portal contains the following information:
  - Date and time of the event.
  - User name.
  - IP address of the user’s device.
  - Application used to connect to the VPN.
  - Duration of the connection.
  - Status of the connection (successful, failed, etc.).

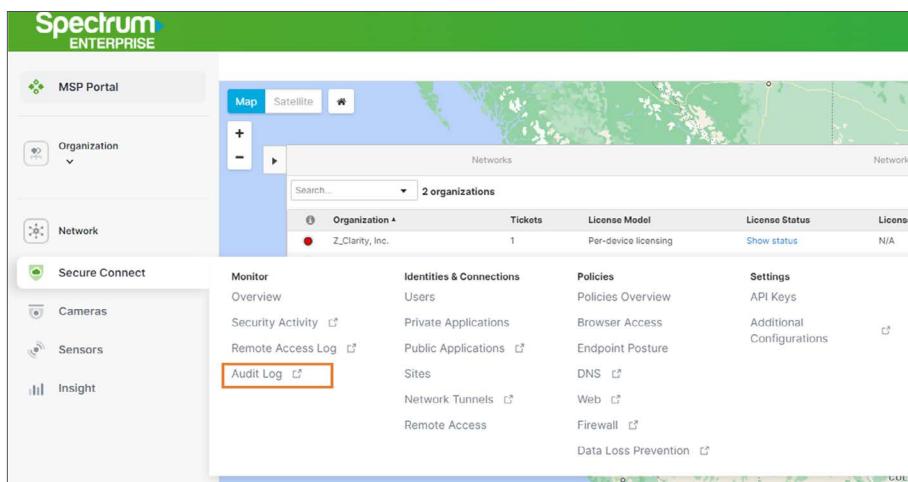


- Toggle the calendar in the upper right hand corner to select a specific time period.
- Use the search bar to apply a filter to search for a specific data point.
- Select the options in the menu on the left side of the page to apply a filter for a event, OS type or AnyConnect version.
- Click the **Return to Secure Connect** box to return to the Secure Connect portal.

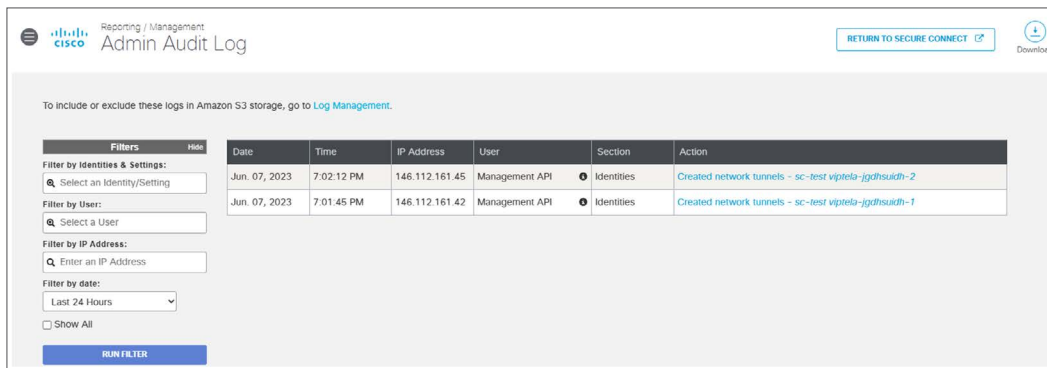
**Audit Log**

The **Admin Audit Log** is a file that records all administrative activity, such as when users create, modify, or delete accounts, change passwords, or access sensitive data. This information can be helpful for troubleshooting problems, identifying security threats, and auditing user behavior.

- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Monitor** then **Audit Log** to see a log of changes to the Secure Connect service.



2. The Audit Log page in the Cisco Umbrella portal shows events for a specific time period including:
  - Date and time of the event.
  - User name.
  - IP address of the user’s device.
  - Action taken (e.g., create account, change password, etc.).
  - Object affected (e.g., account, group, etc.).



3. Click on the action in **blue** to see details about the change that was made.
4. Click the **download** button in the upper left corner to download the audit log.
5. Use the filters on the right side of the page to search for a specific log.
6. Click the **Return to Secure Connect** box to return to the Secure Connect portal.

## Identities and Connections

The Identities and Connections section of the Secure Connect portal provides visibility to users on the network, sites connected to the Secure Connect platform, and applications that users are connecting to.

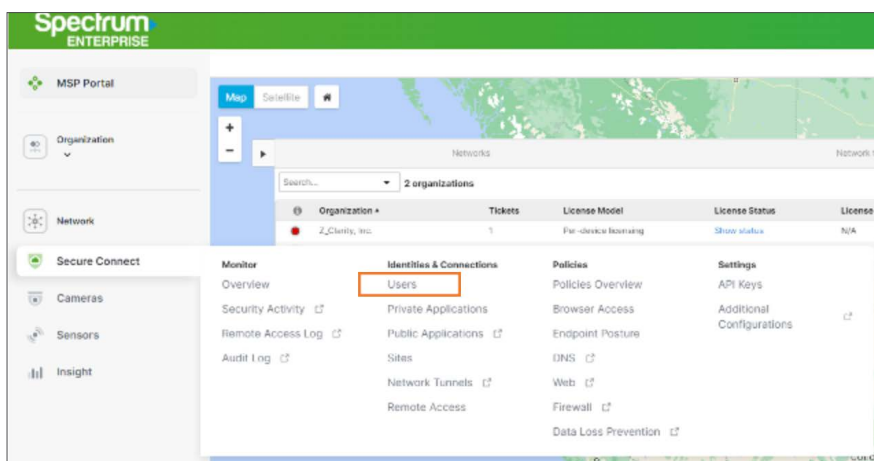
### Users

The **Users** section of the Secure Connections portal can be used to monitor and manage users who have access to your network and organization’s resources.

### Viewing users and user activities

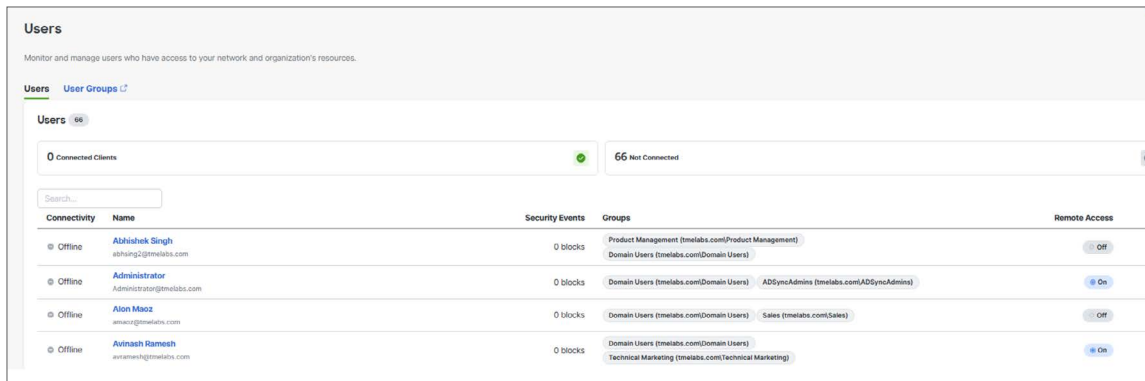
1. From the **Secure Connect** option in the menu on the right hand side of the page, go to **Identities and Connections** then **Users** to see and manage users who have access to your network and organization’s resources.

This page can also be accessed from the [Remote Access](#) section of the Secure Connect dashboard.



2. The User section provides the following information:

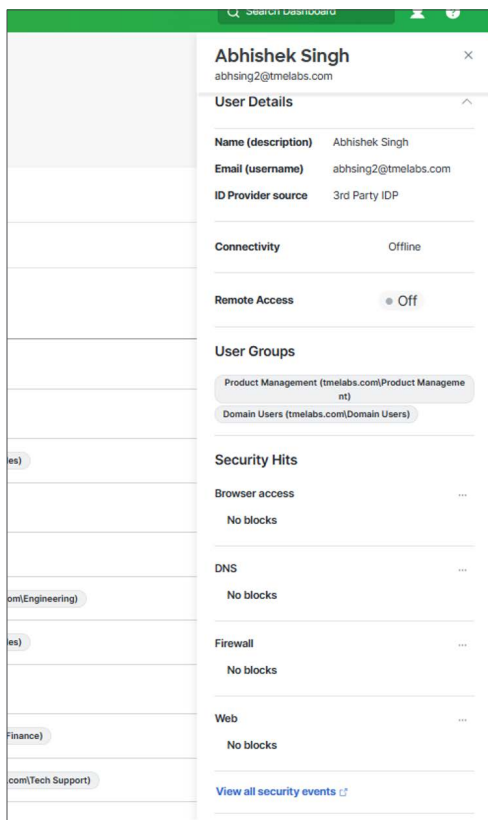
- Count of users connected/not connected.
- Connectivity Status.
- Name of each user.
- Security Events.
- User Groups.
- Remote Access (On/Off).



3. Use the search field to find a specific user.

4. Click on the **Name** in blue to see specific details about a user. User details will be displayed in a box on the right side of the screen.

5. Click on **View All Security Events** at the bottom of this pop up box to see log details of all security events related to this user.



6. In the Cisco Umbrella portal, Administrators can see all user activity, security rules applied and security threats.

Reporting / Core Reports  
Activity Search

RETURN TO SECURE CONNECT | Schedule | Export CSV | LAST 24 HOURS

Search by domain, identity, or URL | Advanced

38,185 Total | Viewing activity from Jun 8, 2023 6:07 PM to Jun 9, 2023 6:07 PM | Results per page: 50 | 1 - 50

Request	Identity	Policy or Ruleset Identity	Destination
IPS	Branch Access orgid:7478818		190.109.228.178:52871
IPS	Branch Access orgid:7478818		190.109.228.178:52871
IPS	Branch Access orgid:7478818		190.109.228.178:52871
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
WEB	Branch Access orgid:7478818	Branch Access orgid:7478818	http://nrp52-appboot.netflix.com/
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	

7. Click on a specific row to see log details.

38,185 Total | Viewing activity from Jun 8, 2023 6:07 PM to Jun 9, 2023 6:07 PM | Results per page: 50 | 1 - 50

Request	Identity	Policy or Ruleset Identity	Destination
IPS	Branch Access orgid:7478818		190.109.228.178:52871
IPS	Branch Access orgid:7478818		190.109.228.178:52871
IPS	Branch Access orgid:7478818		190.109.228.178:52871
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
WEB	Branch Access orgid:7478818	Branch Access orgid:7478818	http://nrp52-appboot
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	
FW	Branch Access orgid:7478818	Branch Access orgid:7478818	

**Event Details**

Action: Allowed

Time: Jun 9, 2023 6:07 PM

Rule Name: Default Internet (435067)

Identity: Branch Access orgid:7478818

Source IP: 192.168.20.4

Destination IP: 157.240.3.54

Source Port: 39696

Destination Port: 80

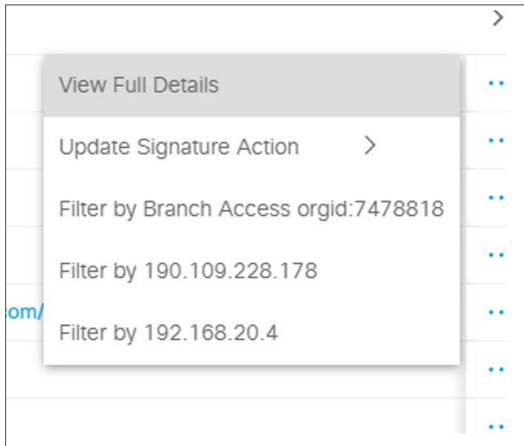
Public Application: Whatsapp

Application Category: Collaboration

8. Use the options at the top of the page to schedule a report or export User Activity log data. Toggle the calendar button to see log data for a specific time period.

9. Use the filters in the menu on the left to search for specific security event or action.

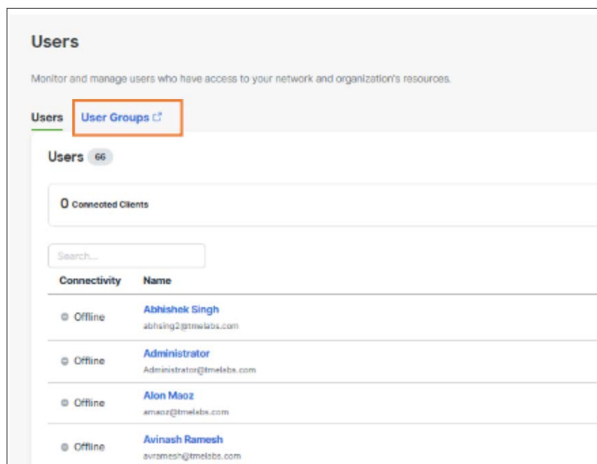
10. Click on the 3 dots at the end of a log row to apply additional filters to the log data.



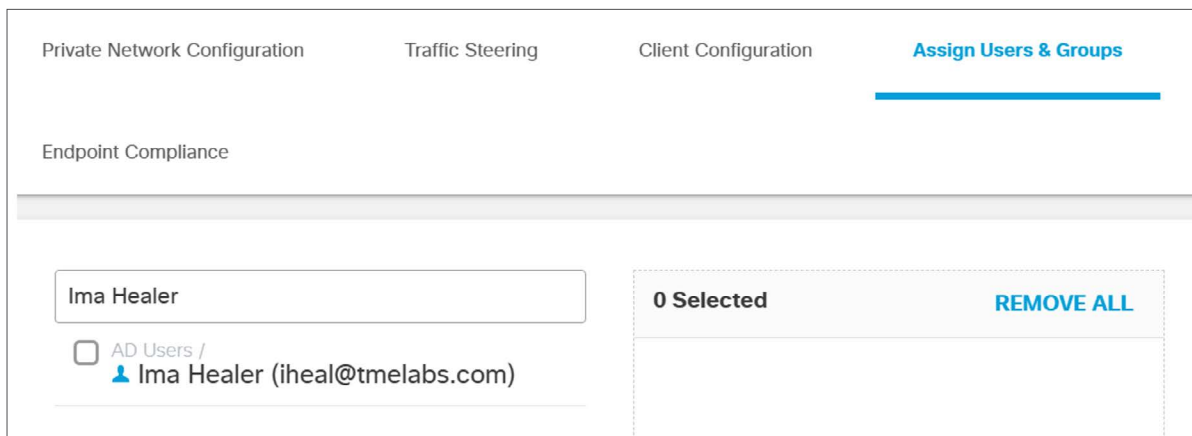
11. Click the **Return to Secure Connect** box to return to the Secure Connect portal.

**Viewing user groups**

1. From the Users page, Click on **User Group** to go to the Remote Access section of the Cisco Umbrella portal for visibility and management of user groups.



2. Once redirected to the Remote Access section of the Cisco Umbrella portal. Type the user or user group name in the search bar to view a specific user or group. The user or user group will display in the box on the left. The email for the user or user group will be displayed next to the user or group name.



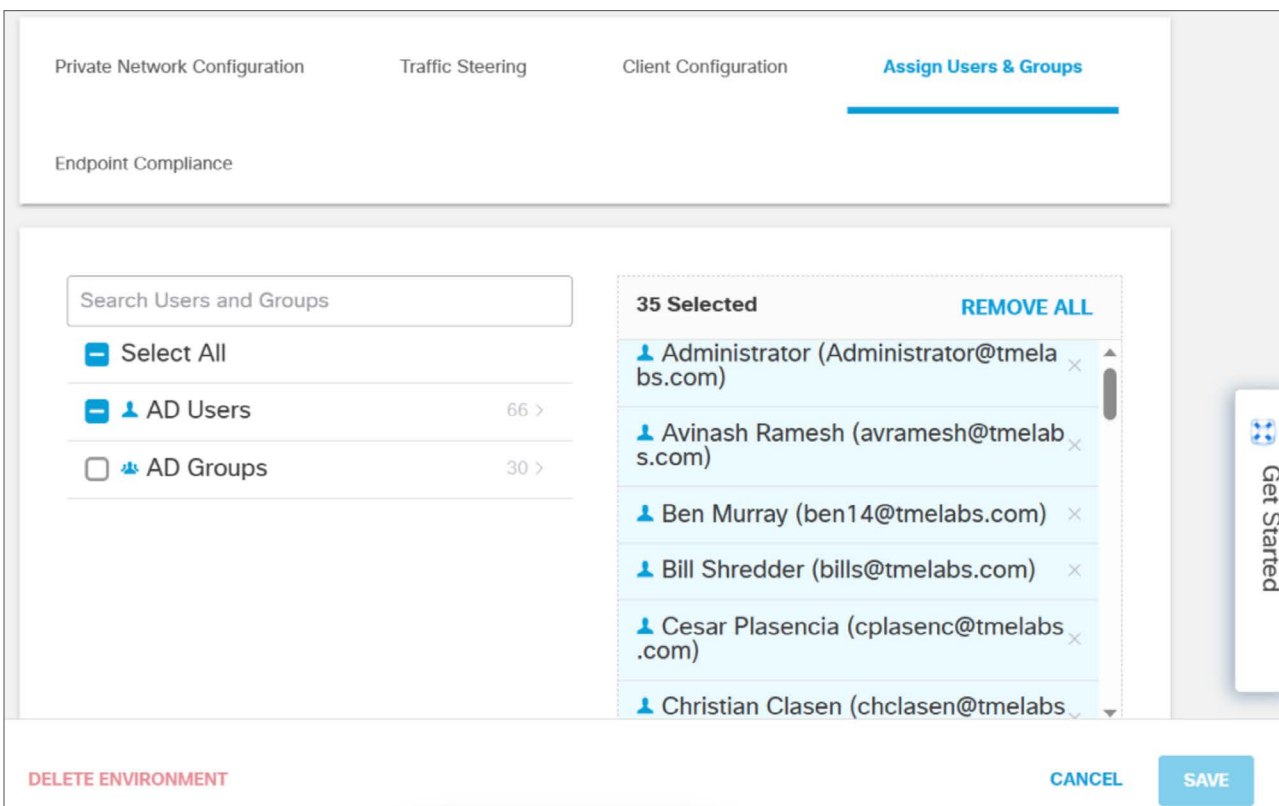


- To see all users or user groups, toggle the box next to AD users or AD groups then click the number at the end of the row to see the users associated with that row.



### Managing Users and User Groups

- Search for the user or user group from the search box. Once you find the user/user group in the box on the left, toggle the box next to the Username or Group to be removed. Once selected the user or group will appear in the selected box on the right.



- Click the (x) in the row of the User/Group name to remove. Or click **Remove All** to remove all users/groups.
- Click **Save** at the bottom of the page.

## Applications

The Applications section of the Secure Connect portal provides visibility to:

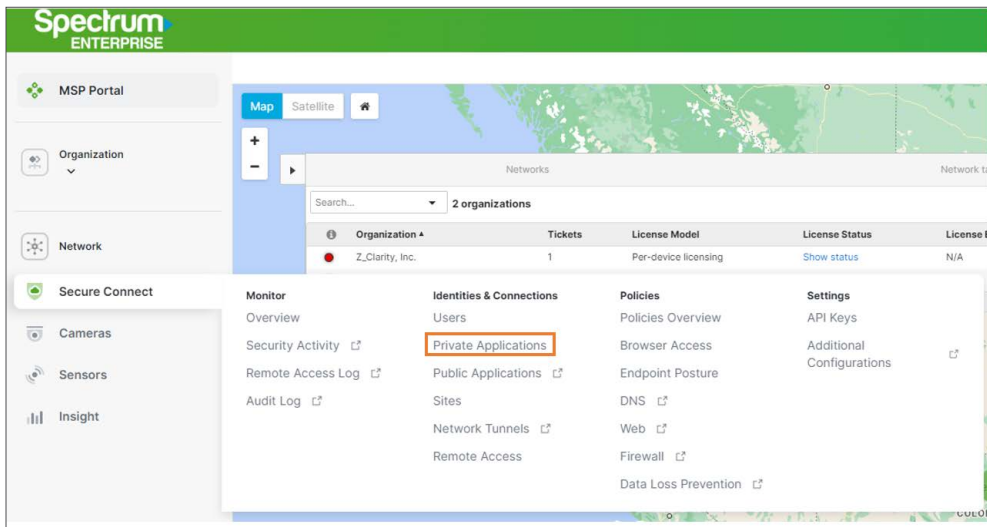
- Private applications that have been integrated with the Secure Connect platform.
- Public internet sites that have been accessed by the users in the organization.
- Application groups/categories.

### Private applications

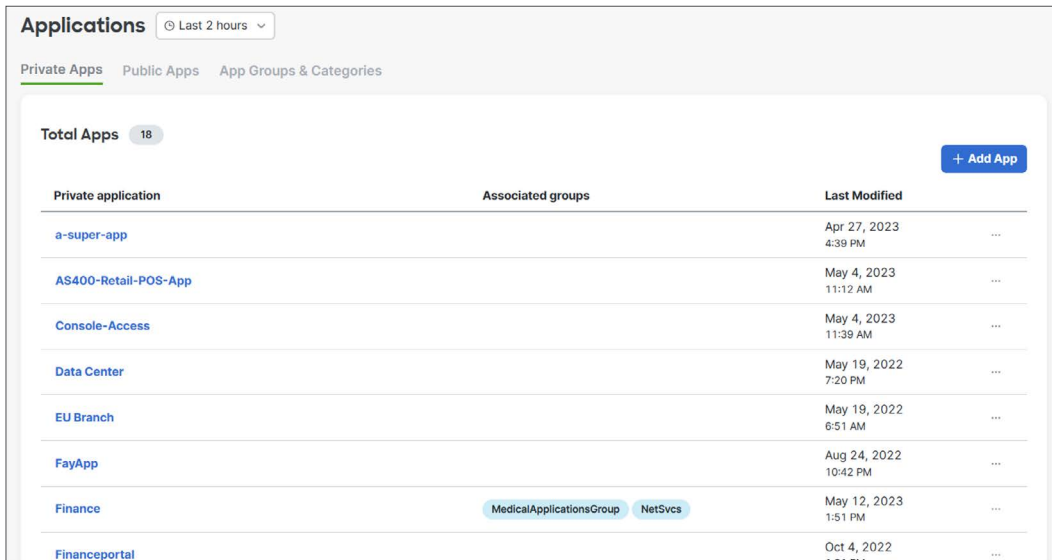
Private applications are applications that are hosted within an enterprise network and accessible only to users on the network. The **Private Applications** section of the Secure Connect portal provides Administrators with the ability to manage access to private applications for users outside of the network.

1. From the **Secure Connect** option in the menu on the right hand side of the page, go to **Identities and Connections** then **Applications** to see and manage private applications.

This page can also be accessed from the [Private Applications](#) section of the Secure Connect dashboard.



2. On the Private Apps page, you can see a list of applications that are available to remote users, as well as the group the application is associated to and the date the application was last modified.



3. Click on the application name in blue to see details about a specific application.

### Adding Private Applications – Network Based Access (Client)

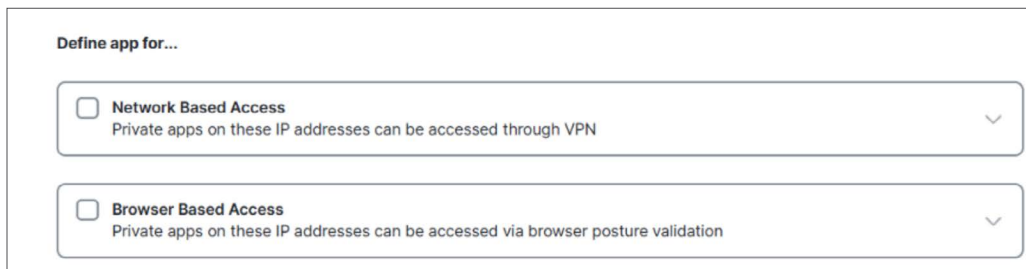
The Network Based Access option allows a user to access an application only by authenticating through the client. Upon authentication, users will be connected to the application through the Secure Connect platform to the application via a VPN. User access to application data is granted based on identity and end point posture (Zero Trust Network Access - ZTNA).

1. Click on the **Add App** button in the right hand corner of the list of private applications.
2. Populate the Application **Name** and Application **Description** fields for the application being added.



The screenshot shows a form titled "Define App". It has two input fields: "Name" and "Description".

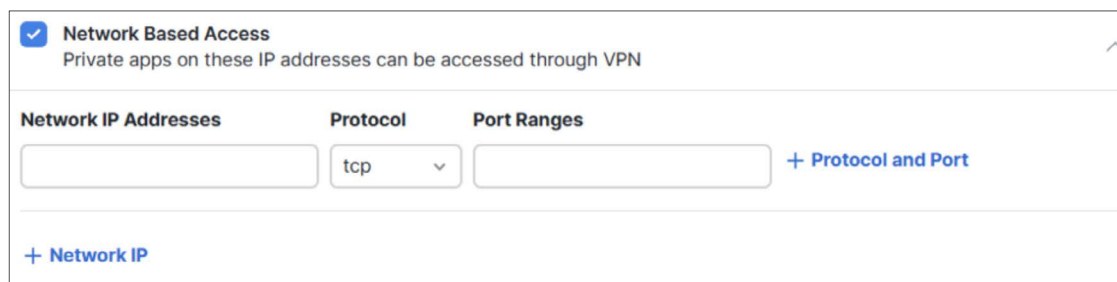
3. Toggle the box to select **Network Based Access**.



The screenshot shows a section titled "Define app for...". It contains two options, each with a checkbox and a dropdown arrow:

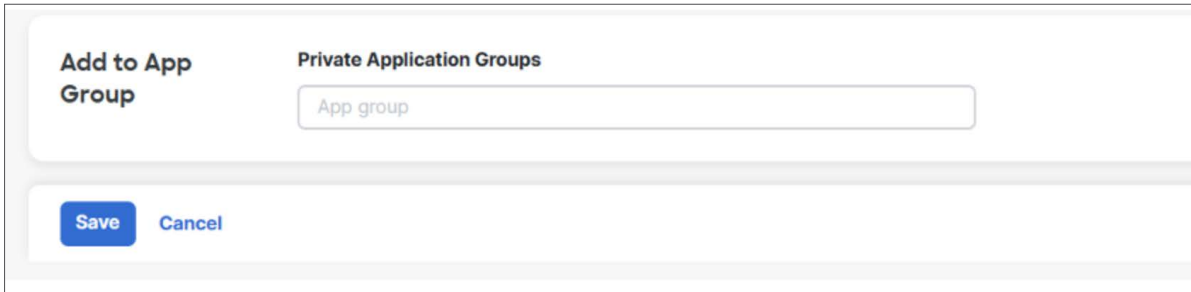
- Network Based Access**  
Private apps on these IP addresses can be accessed through VPN
- Browser Based Access**  
Private apps on these IP addresses can be accessed via browser posture validation

4. When the Network Based Access option is selected, the field will expand and require additional information inputs such as:
  - Network IP Address.
  - Protocol.
  - Port Ranges.

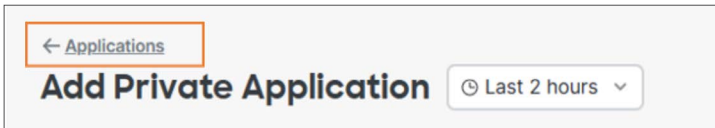


The screenshot shows the expanded "Network Based Access" form. It includes a checked checkbox and a description. Below are three input fields: "Network IP Addresses", "Protocol" (with a dropdown menu showing "tcp"), and "Port Ranges". There is a "+ Protocol and Port" button and a "+ Network IP" button at the bottom.

5. Click on **+ Protocol and Port** to add additional Protocol and Port Ranges.
6. Click on **+ Network IP** to add additional Network IPs.
7. Add the name of the group of the private application (optional).



8. Click Save.
9. Scroll to the top of the page and click **<- Applications** to return to the list of Private Applications to see the Application that was added.



### Adding Private Applications - Browser Based Access (Clientless)

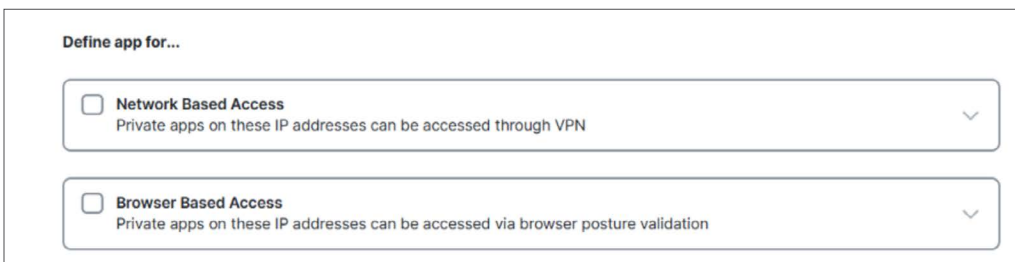
The Browser Based Access option allows a user to access an application through a custom URL (generated by the Secure Connect platform) without authenticating through the client. User access to application data is granted based on identity and end point posture (Zero Trust Network Access - ZTNA). User traffic is not routed through the Secure Connect platform. The Browser Based Access option is most often used for:

- Users unable to install AnyConnect client because the OS of their device is not supported by AnyConnect.
- Users accessing an application from a device that is not owned or managed by your company (ex: partner/contractors).

1. Click on the **Add App** button in the right hand corner of the list of private applications.
2. Populate the Application Name and Application Description fields for the application being added.



3. Toggle the box to select **Browser Based Access**.



- When the Browser Based Access option is selected, the field will expand and require additional information inputs such as:
  - Network IP Address.
  - Application protocol.
  - Port.
  - Server name Indication and protocol.

Toggle the Validate Application Certificate field to the right to enable a certificate to be generated.

The screenshot shows a configuration form for 'Browser Based Access'. At the top, there is a checked checkbox and the text 'Private apps on these IP addresses can be accessed via browser posture validation'. Below this, there are three input fields: 'Network IP Addresses' (empty), 'App Protocol' (containing 'tcp'), and 'Port' (containing '443'). Underneath, there are two more fields: 'Protocol' (a dropdown menu showing 'https') and 'Server Name Indication' (empty). A toggle switch for 'Validate Application Certificate' is currently turned off, labeled 'Not Enabled'. At the bottom, there is an 'External URL' section with explanatory text and a 'Certificate' section with the text 'Will be generated on Save'.

- Add the name of the group of the private application (optional).

The screenshot shows a dialog box titled 'Add to App Group'. It has a sub-header 'Private Application Groups' and a single text input field containing 'App group'. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'.

- Click Save.
- The custom URL will be generated and can be distributed to users accessing the application without authenticating first with the client.
- Scroll to the top of the page and click **<- Applications** to return to the list of Private Applications to see the Application that was added.

The screenshot shows a button labeled '<- Applications' with a red border. Below it is a larger button labeled 'Add Private Application' followed by a dropdown menu showing 'Last 2 hours'.

### Public applications

Public applications are applications that are hosted on the internet, such as Microsoft 365, Salesforce, and Google Workspace. The Public Applications section of the Application page provides Administrators with visibility to public applications accessed by users, the security risk associated with each application, as well as the ability to respond in real time.

1. Click on the Public Apps section to see the following information specific to the public applications accessed by users on the network:
  - Application Name.
  - Risk Score.
  - Application category.
  - Last Detected.

Public application	Risk score	Application category	Last detected
<a href="#">Google App Engine</a>	Medium	Application Development and Testing	Jun 4, 2023 8:00 PM
<a href="#">Unity Technologies</a>	High	Application Development and Testing	Jun 4, 2023 8:00 PM
<a href="#">Microsoft Account</a>	Low	Security	Jun 4, 2023 8:00 PM
<a href="#">Sentry</a>	High	IT Service Management	Jun 4, 2023 8:00 PM
<a href="#">Moat Analytics</a>	Low	Ad Publishing	Jun 4, 2023 8:00 PM
<a href="#">Microsoft Outlook Live</a>	Low	Office Productivity	Jun 4, 2023 8:00 PM

2. Click on the application name in **blue** to see details about the application.

### Application groups and categories

The Application Group and Categories section provides visibility to the Groups and Categories of all public and private applications.

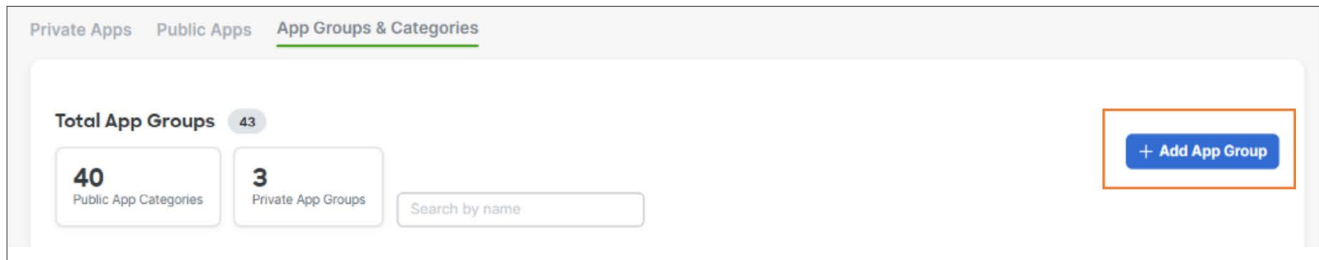
1. Click on the App Groups and Categories section to see a list of the groups/categories of the public and private applications. Use the search bar to search for a specific application.

Groups / Categories	Apps	Last Modified
MedicalApplicationsGroup Private	3 Apps	Mar 3, 2023 12:26 PM
NetSvcs Private	3 Apps	Sep 10, 2022 7:03 AM
PatientApplicationsGroup Private	2 Apps	May 12, 2023 2:26 PM
Ad Publishing Public	<a href="#">View Apps</a>	-
Anonymizer Public	<a href="#">View Apps</a>	-

- 2. Private applications groups are defined by the group associated with the Private application when it was added (access was enabled) via the Secure Connect portal. See [Private Applications](#).
- 3. Public applications categories are defined by the application. Click on **View Apps** to see specific applications within a specific category.

### Adding application group

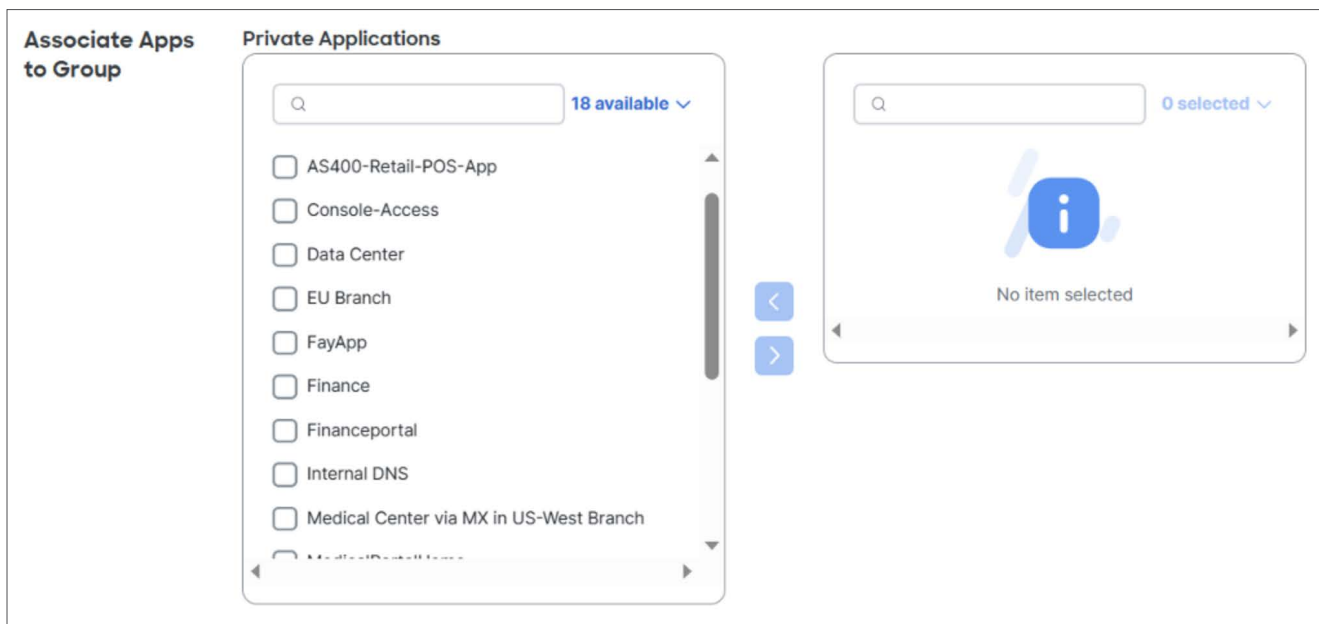
- 1. From the Application Group and Category page, click on the **+ Add App Group** button on the upper right hand side of the page. Application groups are used to group Private Applications.



- 2. Enter the Application Group name (required) and Description (optional).



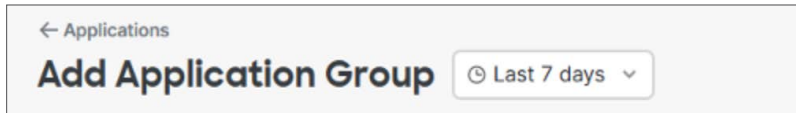
- 3. Select the application(s) to associate to the new group by first toggling the box next to the application name then move the application to the box on the right hand side by clicking the > button. Move as many applications as necessary to the box on the right. To select all applications, click on the drop down next to the number of applications available (next to the search bar).



- Once all applications are moved to the box on the right, click Save.



- Scroll to the top of the page and click **<- Applications** to return to the Application Group and Category page and see the new Application Group.

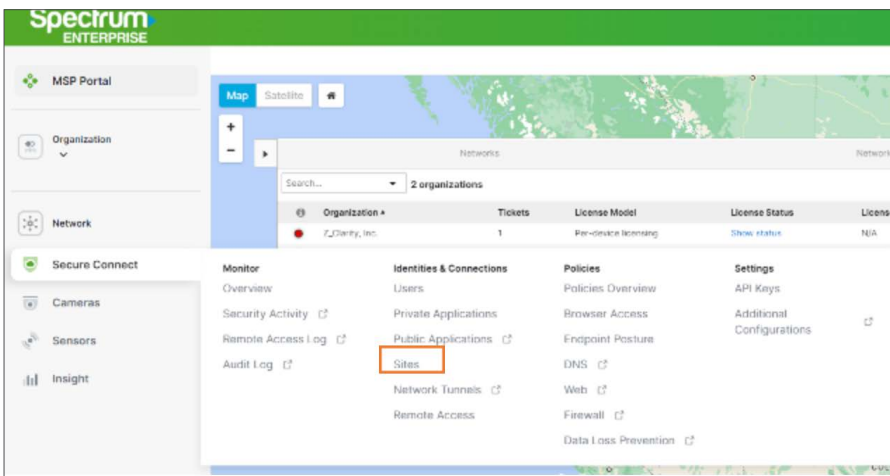


## Sites

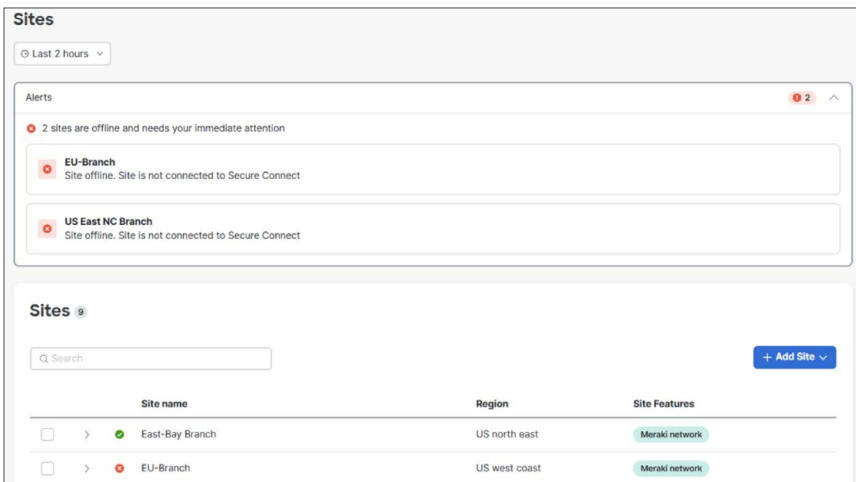
The Sites Section of the Secure Connect Portal provides visibility to your network sites connected to the Secure Connect platform. Spectrum Enterprise Managed Services will connect your locations when your service is activated.

- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Identities and Connections** then **Sites** to see a list of sites connected to the Secure Connect platform.

**NOTE:** As part of the onboarding process, Spectrum Enterprise Managed Services will connect sites (network locations) to the Secure Connect platform.



- On the Sites page, you will see a list of network locations connected to the Secure Connect platform as well as any security alerts which may need your attention.





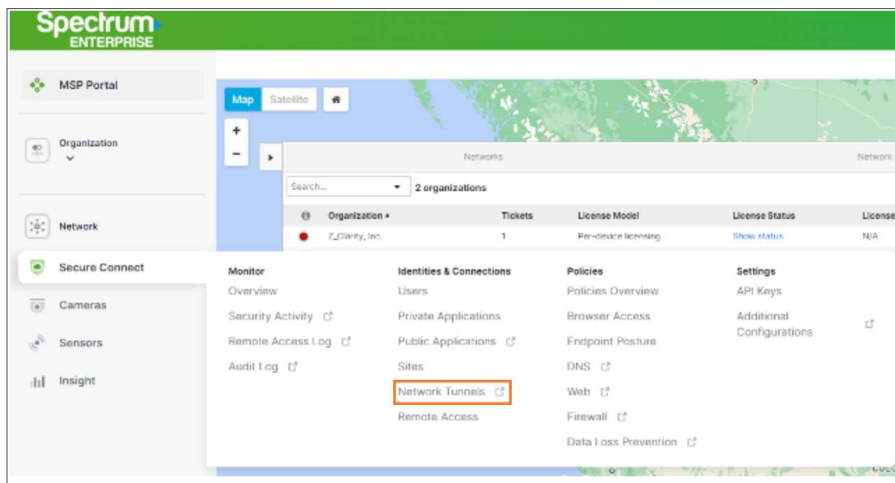
- The button next to the Site Name will indicate if the site is connected or offline.
- Spectrum Enterprise Managed Services can be engaged to troubleshoot an offline site and/or to add a new site. See the [Resources for Administrators](#) section for Spectrum Enterprise Contact Information.

### Network Tunnels

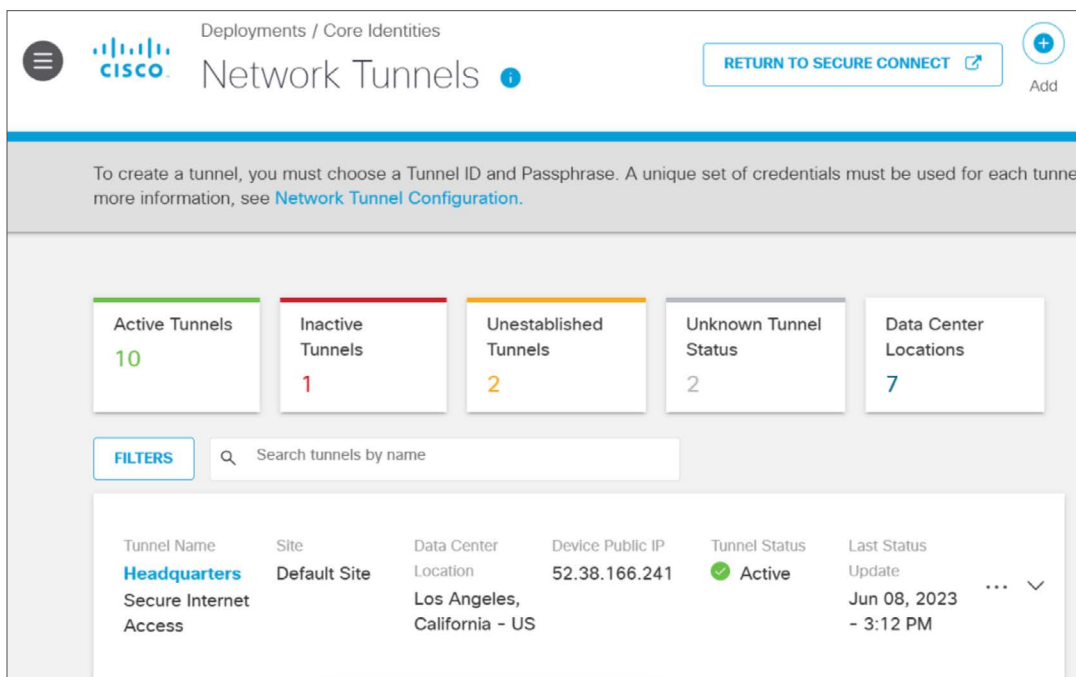
The Network Tunnels section of the Secure Connect portal provides visibility to the health of the tunnels connecting the network locations (sites) to the Secure Connect platform.

- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Identities and Connections** then **Network Tunnels** to see a list of tunnels connecting to the Secure Connect platform.

**NOTE:** As part of the onboarding process, Spectrum Enterprise Managed Services will build tunnels from each site (network location) to the Secure Connect platform.



- On the Network Tunnels page of the Cisco Umbrella portal, you will see a dashboard view displaying the health of the network tunnels.



- Use the search field to apply a filter and find a specific tunnel by name. Click on the 3 dots and/or down arrow to see configuration details for a specific tunnel.
- Spectrum Enterprise Managed Services can be engaged to add a new tunnel or troubleshoot an inactive or unestablished tunnel. See the [Resources for Administrators](#) section for Spectrum Enterprise Contact Information.

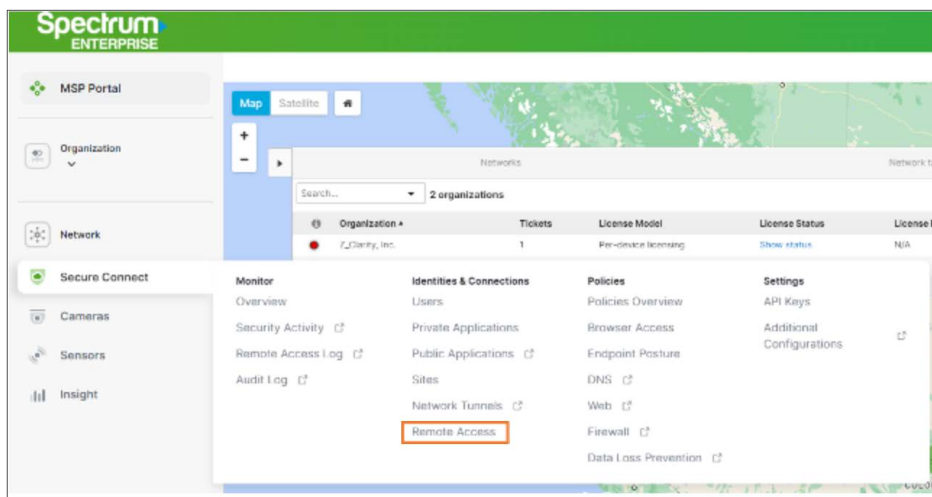
### Remote Access

Remote Access enables remote users to access public and private applications from anywhere through the Cisco+ Secure Connect fabric using a Cisco Secure Client. Secure Connect provides Administrators with Identity-based access control and Endpoint Posture, enabling granular access control to private resources.

The Remote Access section of the Secure Connect portal guides the Administrator through setting up Remote Access for users within their network.

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Remote Access for their users upon Service Activation.

- From the **Secure Connect** option in the menu on the right hand side of the page, go to **Identities and Connections** then **Remote Access**.



- From the Remote Access page, Administrators can follow the step by step guide to setting up remote access as well as links to Cisco process documentation.

### Remote Access

#### Get started with Secure Connect Remote Access

Secure Connect enables remote users to access resources securely from anywhere through the Secure Client. Learn more in the [Secure Connect Remote Access Documentation](#)

3/4

- ✔ **Configure remote access service**  
 Configure details for the Remote Access service, and select what data center regions to deploy Remote Access.  
[Edit configuration](#)
- ✔ **Enable application connectivity**  

**Meraki network**  
Add your Meraki network as a Secure Connect site to connect Remote Access users to internal applications.  
[Manage sites](#)

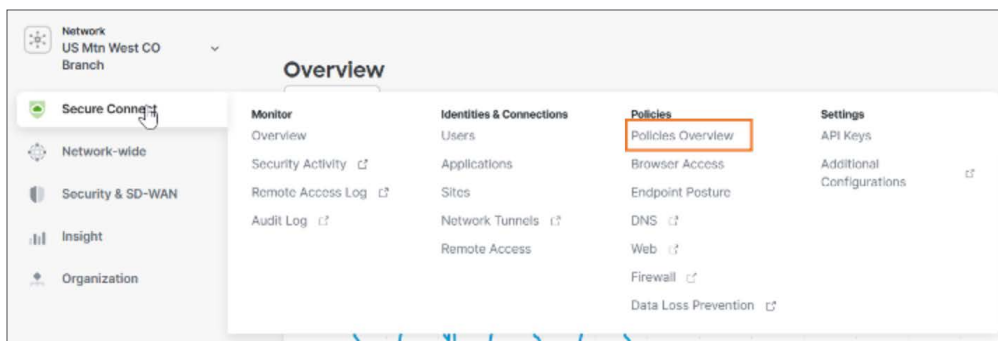
**Non-Meraki network**  
Connect network devices through IPsec tunnels to connect Remote Access users to internal applications.  
[Edit tunnels](#)
- ✔ **Configure and provision users**  
 Enable Secure Connect to authenticate and authorize users.  
[Edit configuration](#)

## Policies

The policy section of the Secure Connect portal allows for visibility and management of security policies for end users and applications.

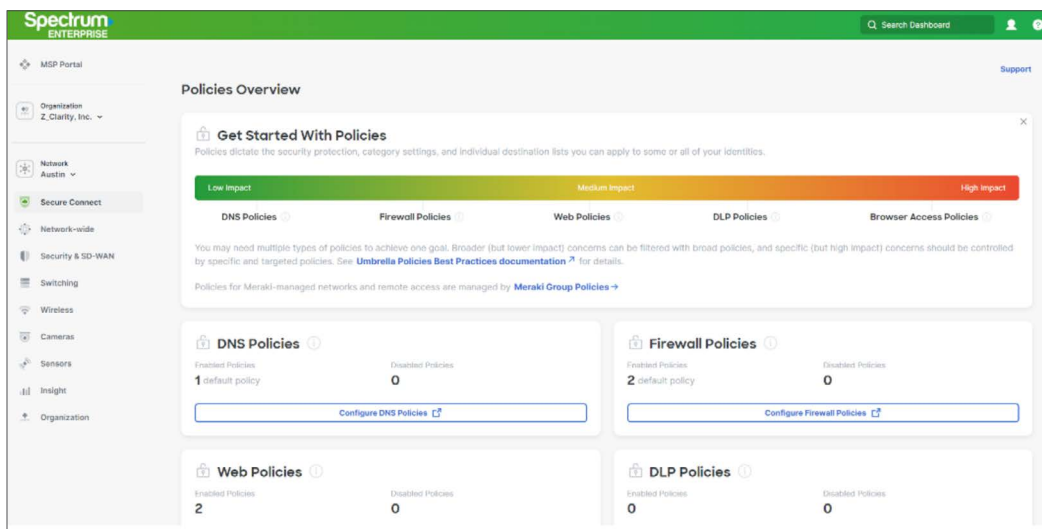
### Policies Overview

- From the **Secure Connect** menu, go to **Policies** then **Overview** for a dashboard view of all security policies and tips to help Admins get started defining security policies.



- The bar at the top of the page in the **Getting Started with Policies** box displays a color coded scale to show the impact each policy can have on your network. Click the links in **blue** to see [Cisco Umbrella Best Practices Documentation](#).

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Security Policies upon Service Activation as well as assist with ongoing tuning and management of security policies.

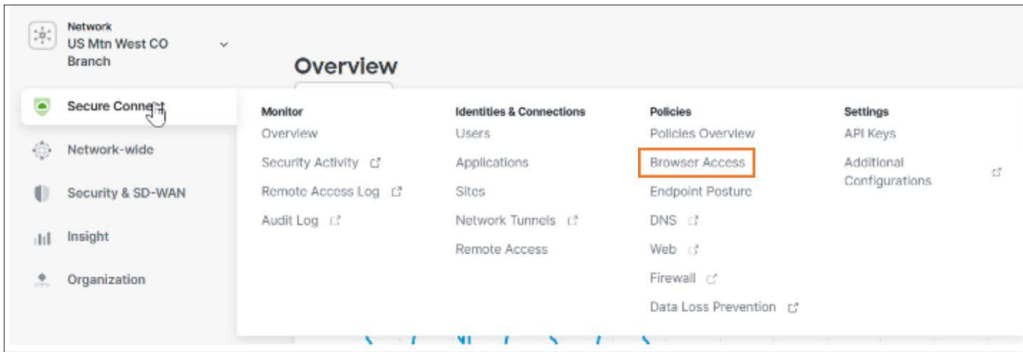


- The boxes below the Getting Started bar show the count of security policies that are enabled as well as links to the Cisco Umbrella portal where granular policy control and specific security events can be viewed and managed.

### Browser Access

The Browser Access section of the Secure Connect portal allows Administrators to view and manage security policies related to application access.

- From the **Secure Connect** menu, go to **Policies** then **Browser Access** to see a list of all browser access rules that determine who and how an application can be accessed.



2. The Browser Access page lists the rules in the order they are applied and provides the following information:

- Browser Rule Name.
- Rule Action (allow or deny).
- User/user group the rule applies to.
- Application/application group the rule applies to.
- Endpoint posture profile (system requirements for the user endpoint).
- Number of “hits” or attempts the rule has applied to and the time period in which the rule was applied.

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Browser Access Policies upon Service Activation as well as assist with ongoing tuning and management of security policies.

**Browser Access**

Q Search Rules 9 Rules + Add Rule

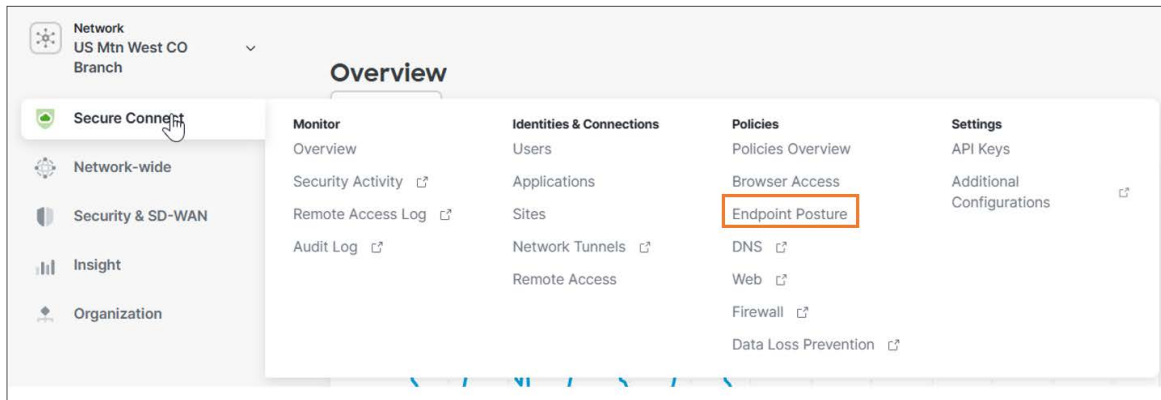
#	Name	Action	Users & Groups	Apps & Groups	Endpoint Posture Profile	Hits
1	PatientPortal <span>Enabled</span>	Allow	Bill Shredder (bills@tmelabs.com) Mai Besick (mbesick@tmelabs.com)	PatientPortal	PostureProfile1	No Data
2	New Rule <span>Enabled</span>	Allow	Contractors (tmelabs.com/Contractors) (1)	PatientApplicationsGroup (2)	None	No Data
3	New Rule <span>Enabled</span>	Allow	Contractors (tmelabs.com/Contractors) (1)	MedicalApplicationsGroup (3)	PostureProfile1	No Data
4	app-viptela-tme-sase-pod <span>Enabled</span>	Allow	All	viptela-demo-app-sase-pod2	ChromeLive	No Data

3. Click on the 3 dots at the end on the right side of each row to edit, duplicate, reorder or disable the browser access rule.
4. Click on the **+ Add Rule** button to add a new rule.

### Endpoint Posture

The Endpoint Posture section of the Secure Connect portal allows IT Administrators to provide granular controls on device posture, ensuring security threats are not introduced by an unsecured device accessing the network and applications.

1. From the **Secure Connect** menu, go to **Policies** then **Endpoint Posture** to see a list of all endpoint posture profiles.



2. The Endpoint Posture page lists all Endpoint profiles that have been created including:

- Profile Name.
- Supported Operating system.
- Supported browsers.
- Supported location.
- Application or Application group that the policy applies to.

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Endpoint Posture Profiles upon Service Activation as well as assist with ongoing tuning and management of security policies.

Profile Name	Operating System	Browser	Location	Applied To
PostureProfile1	Windows: current Linux: all Mac OS X: all	Firefox: current Firefox: 111.0 Chrome: current Edge Chromium: current	AF BD BT IN <a href="#">View 155 more</a>	PatientPortal New Rule MediportalAccess FinancePortalAccess
ChromeLive	Windows: current Android: current Mac OS X: all iOS: current	Chrome: current Chrome: 112.0	AI AG AR AW <a href="#">View 53 more</a>	app-viptela-tme-sase-pod
Apple or Windows	Windows: all Mac OS X: all	Chrome: current Chrome: 112.0	BM CA GL PM <a href="#">View 1 more</a>	MedicalHomebehindMX NextCloudPortal

3. Click on the 3 dots at the end on the right side of each row to edit, endpoint posture profile.
4. Click on the **+ Add Rule** button to add a new rule.

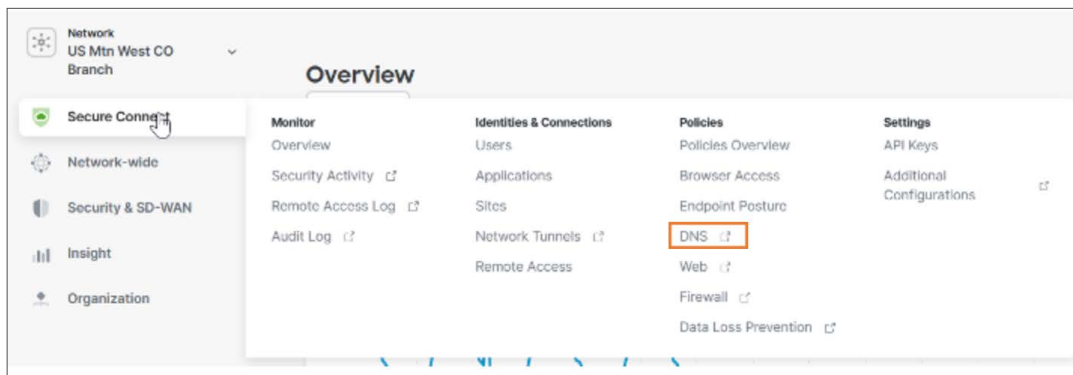
**DNS**

DNS policies provide DNS-layer visibility, security, and enforcement with the ability to selectively proxy risky domains for added security. The DNS page of the Secure Connect portal provides visibility to DNS activity and DNS related security events on the network.

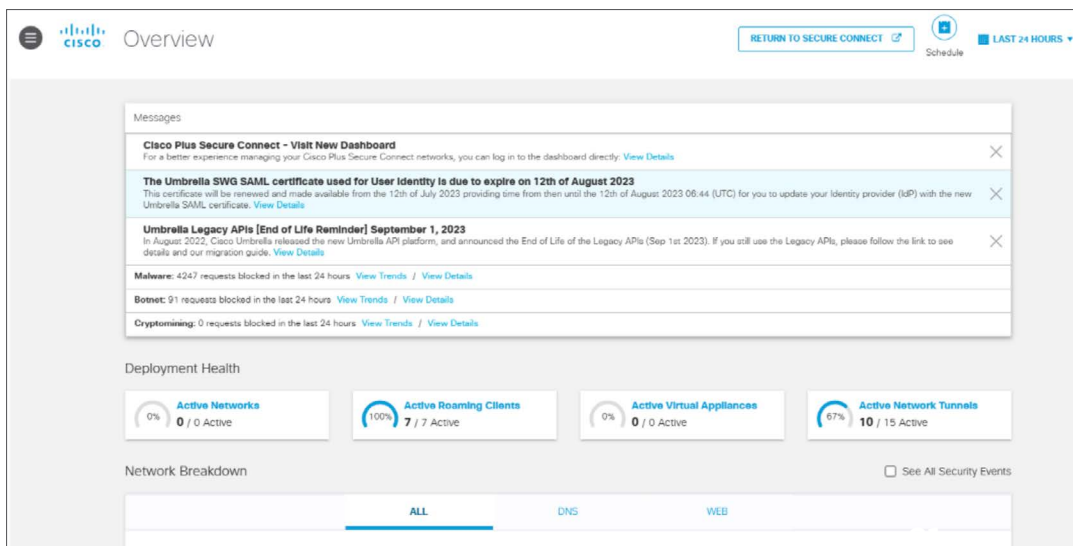
See the Cisco resources to get more information on DNS policy management and best practices:

- [Manage DNS Policies \(umbrella.com\)](https://umbrella.com/learn/manage-dns-policies)
- [Best Practices for DNS Policies \(umbrella.com\)](https://umbrella.com/learn/best-practices-for-dns-policies)

1. From the **Secure Connect** menu, go to **Policies** then **DNS** to be redirected to the DNS page in the Cisco Umbrella portal.



2. On the DNS page in the Cisco Umbrella portal, Administrators can see:
  - Messages pertaining to the Secure Connect and Umbrella platform.
  - Summary of security events on the network with links to details and trends.
  - Health of the network.



3. The data on this page defaults to the last 24 hours. Toggle the down arrow next to the calendar to select a different time period.
4. Click on the **schedule** button in the upper right corner to schedule a report of all security blocks.
5. Click on any of the words in **blue** to be redirected to other pages in the Cisco umbrella portal to view, search, and export specific security activity detail.

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up security policies upon Service Activation as well as assist with ongoing tuning and management.

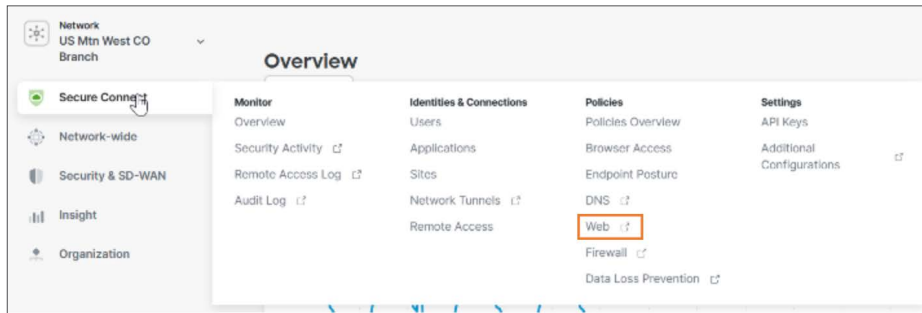
6. Click the **Return to Secure Connect** box to return to the dashboard.

**Web**

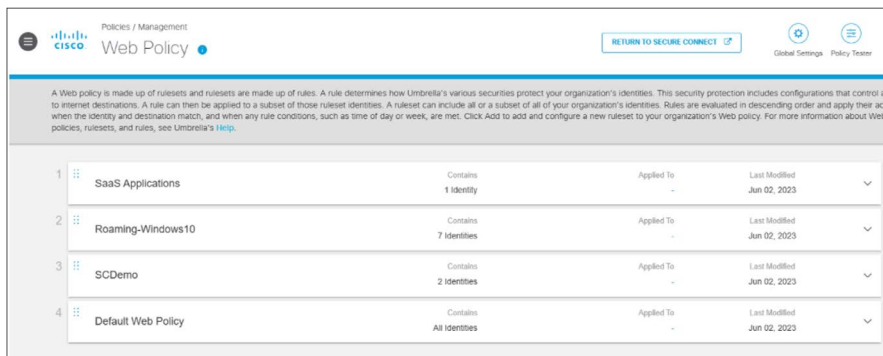
The secure web gateway (SWG) functionality can proxy all web traffic by leveraging a web policy to provide URL-layer visibility, security, and enforcement of your organization's web traffic. Enterprise networks will have one Web Policy, which is made up of rulesets and rules that set various security, permission, and access controls for your identities. The Web Policy page of the Secure Connect portal provides visibility to the rulesets that have been defined for the network. See the Cisco resource to get more information on managing the Web policy:

- [Manage the Web Policy \(umbrella.com\)](https://umbrella.com)

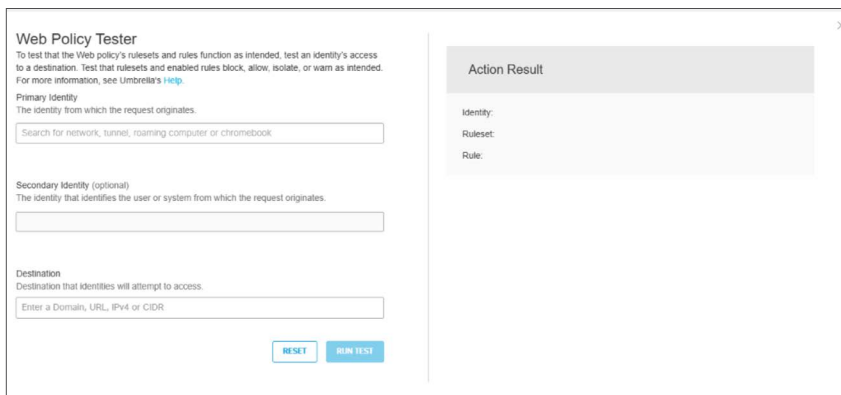
1. From the **Secure Connect** menu, go to **Policies** then **Web** to be redirected to the Web Policy page in the Cisco Umbrella portal.



2. From the Web page in the Cisco Umbrella portal, Administrators can see the rulesets that have been defined within the Web policy. Rules are applied to web traffic in descending order to the identities (use/user groups) defined by each ruleset. Click on the down arrow at the end of the row to see details about the rules and ruleset, to add a rule, or modify the ruleset settings.



3. Click on **Global Settings** at the top of the page to manage the rules applied to all identities.
4. Click on **Policy Tester** at the top of the page to test the web policy. The policy tester option allows Administrators to enter an identity and web destination and see the test result action.



**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Web policies upon Service Activation as well as assist with ongoing tuning and management.

5. Click the **Return to Secure Connect** box to return to the dashboard.

### Firewall

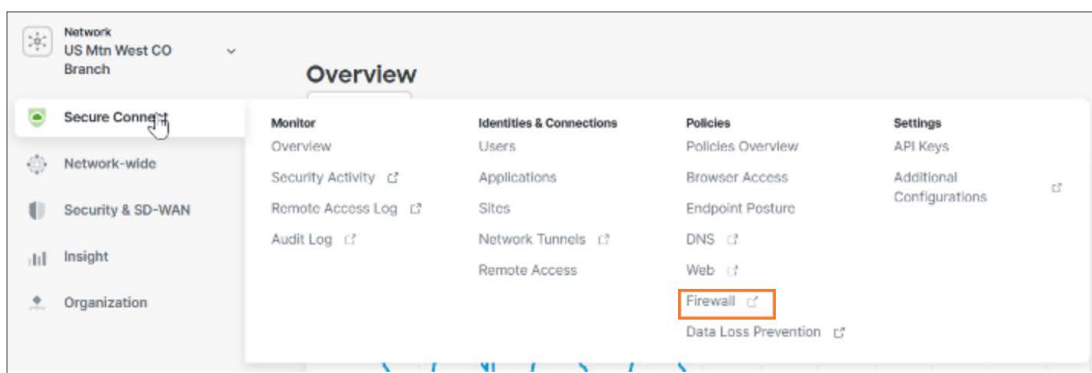
The Secure Connect firewall supports visibility and control of internet traffic across branch offices and logs all network activity and blocks unwanted traffic using IP, port, and protocol rule criteria.

The Firewall page of the Secure Connect portal provides visibility to the firewall policy that describes the active firewall configuration and Intrusion Prevention System (IPS).

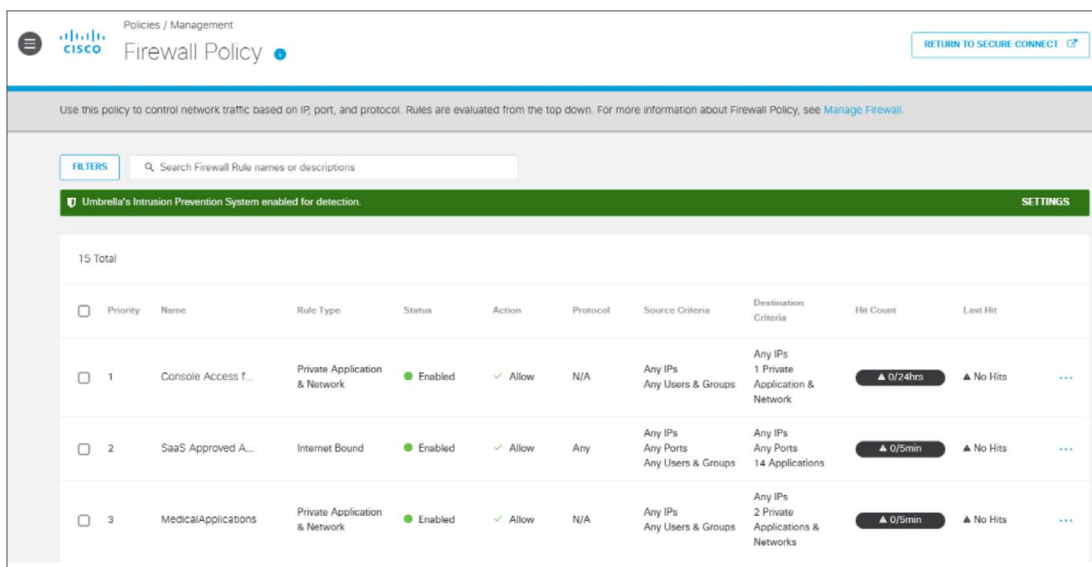
See the Cisco resource to get more information about managing Firewall rules and policies:

- [Manage the Firewall Policy \(umbrella.com\)](https://umbrella.com)

1. From the **Secure Connect** menu, go to **Policies** then **Firewall** to be redirected to the Firewall Policy page in the Cisco Umbrella portal.



2. From the Firewall Policy page in the Cisco Umbrella portal, Administrators can see the rulesets that have been defined. Rules are applied in descending order to the identities (use/user groups) defined by each ruleset.





3. Use the search bar to apply a filter to find a specific rule.
4. To manage a rule, toggle the box on the far left side of the rule or rules to manage. Once selected, the following actions can be taken:
  - Export rule(s).
  - Enable rule(s).
  - Disable rule(s).
  - Change rule action (allow or block).
  - Change logging preference (enable/disable).

**NOTE:** Enabling/Disabling rules take effect immediately upon making the change.

Priority	Name	Rule Type	Status	Action	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit
1	Console Access f...	Private Application & Network	Enabled	Allow	N/A	Any IPs Any Users & Groups	Any IPs 1 Private Application & Network	0/24hrs	No Hits

5. To change edit, or delete a rule, click on the 3 dots at the end of a row to manage a specific rule.

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Firewall policies upon Service Activation as well as assist with ongoing tuning and management.

6. Click the **Return to Secure Connect** box to return to the dashboard.

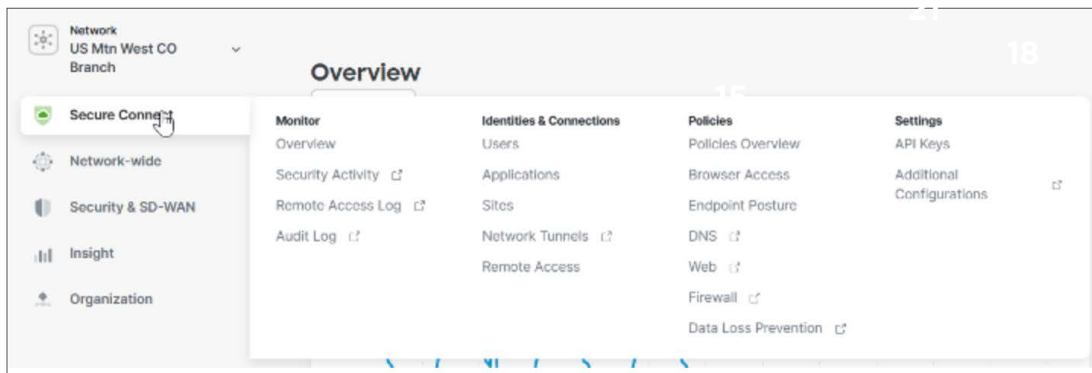
**Data Loss Prevention**

Data Loss Prevention (DLP) analyzes data being uploaded to the web (in-line) to provide control over sensitive data leaving your organization. DLP policies can monitor or block the data as well as inspect data in line with full SSL inspection. The Data Loss Prevention page of the Secure Connect portal, provides visibility to the DLP policies defined for the network.

See the Cisco resource to get more information about managing DLP policies:

- [Manage the Data Loss Prevention Policy \(umbrella.com\)](https://umbrella.com)

1. From the **Secure Connect** menu, go to **Policies** then **Data Loss Prevention** to be redirected to the Data Loss Prevention page in the Cisco Umbrella portal.



2. The Cisco Umbrella portal provides visibility to the DLP policies.

Rule Type	Name	Severity	Action	Identities or File Owners	Destinations	Data Classifications File Labels	Last Modified
Real Time	Employee Data	Medium	Block	1 Identity	Inclusion 2 Applications	Data Classifications Employee Data	May 30, 2023
Real Time	PCI	Medium	Monitor	1 Identity	Inclusion All Destinations	Data Classifications Built-in PCI Classification Credit Card	May 30, 2023
Real Time	PII Data	Critical	Block	4 Identities	Inclusion 2 Applications	Data Classifications Personal Data (US)	Apr 28, 2023

3. Click on the **Add Rule** button to add a new DLP rule.
4. Click on the 3 dots at the end of the row to Disable, Edit, or Delete a DLP rule.

**NOTE:** Spectrum Enterprise Managed Services will assist IT Administrators with setting up Firewall policies upon Service Activation as well as assist with ongoing tuning and management.

5. Click the **Return to Secure Connect** box to return to the dashboard.

**About Spectrum Enterprise**

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America’s largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes [networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions](#). The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit [enterprise.spectrum.com](https://enterprise.spectrum.com).

Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply. Subject to change without notice. ©2023 Charter Communications. All rights reserved.