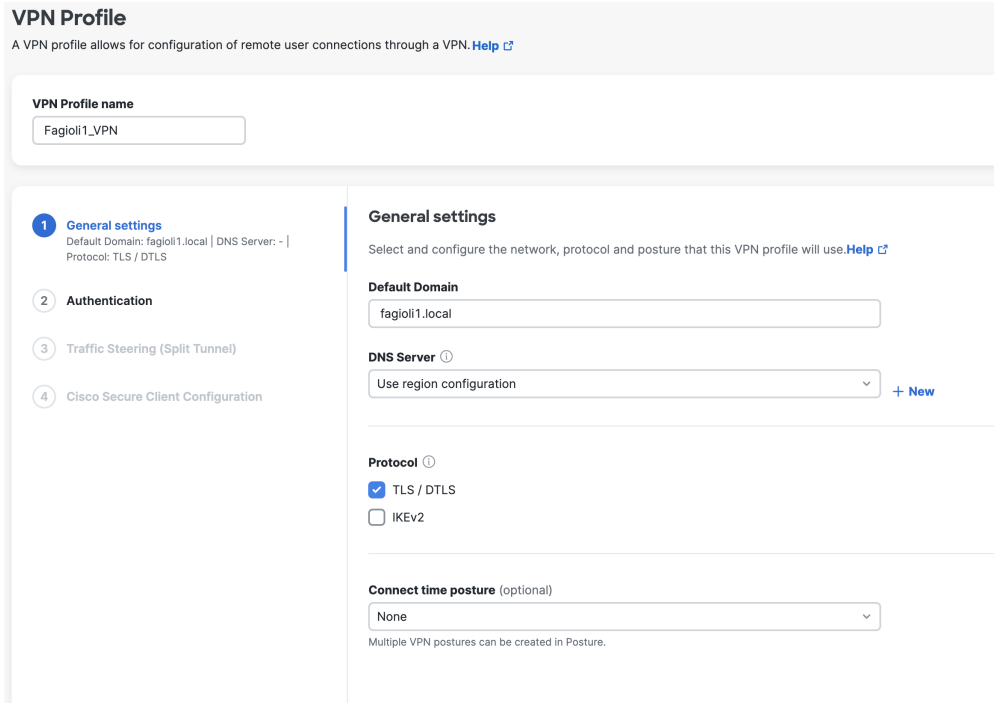
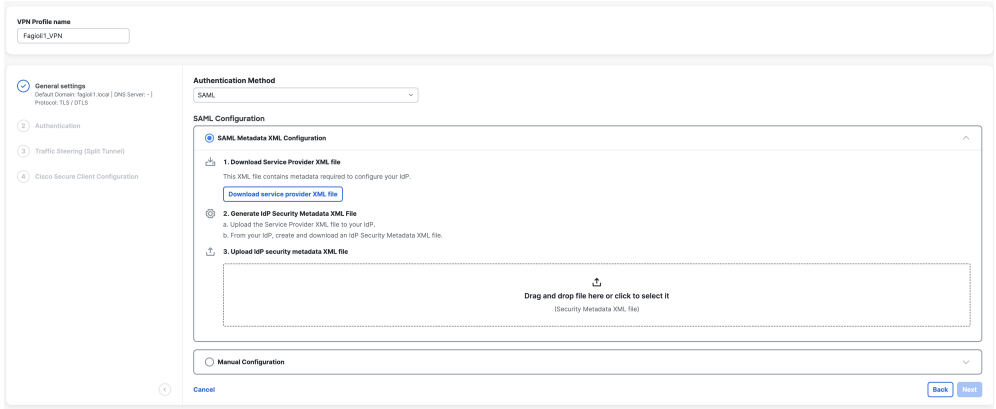
(Cisco Secure Access) Tectorial from Zero to Hero

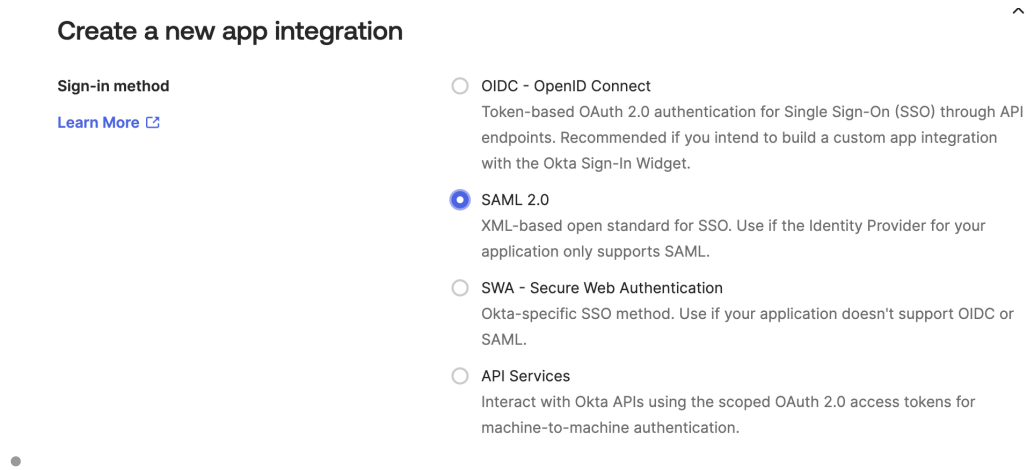
Index

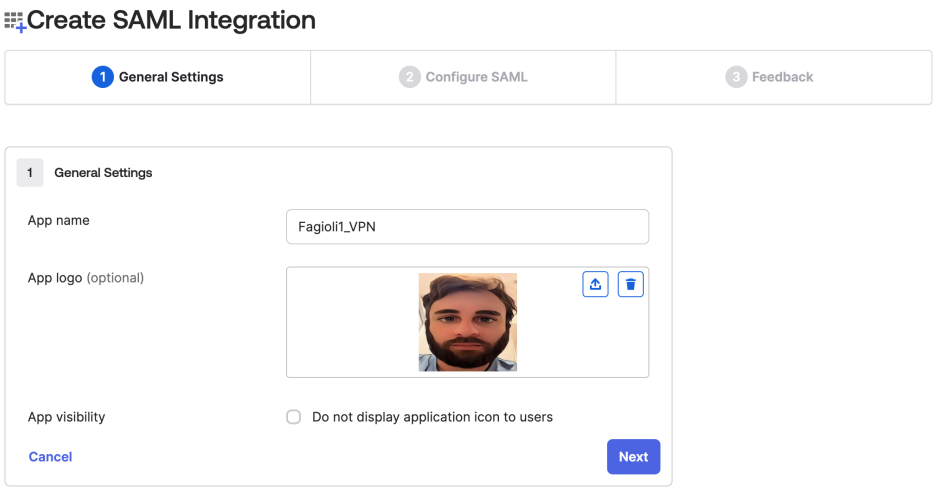
Secure Access

1. **Connect**
    1. End User Connectivity
        - Virtual Private Network: VPN Pools: **172.31.33.0/24** and **172.31.34.0/24**
        - Create new VPN

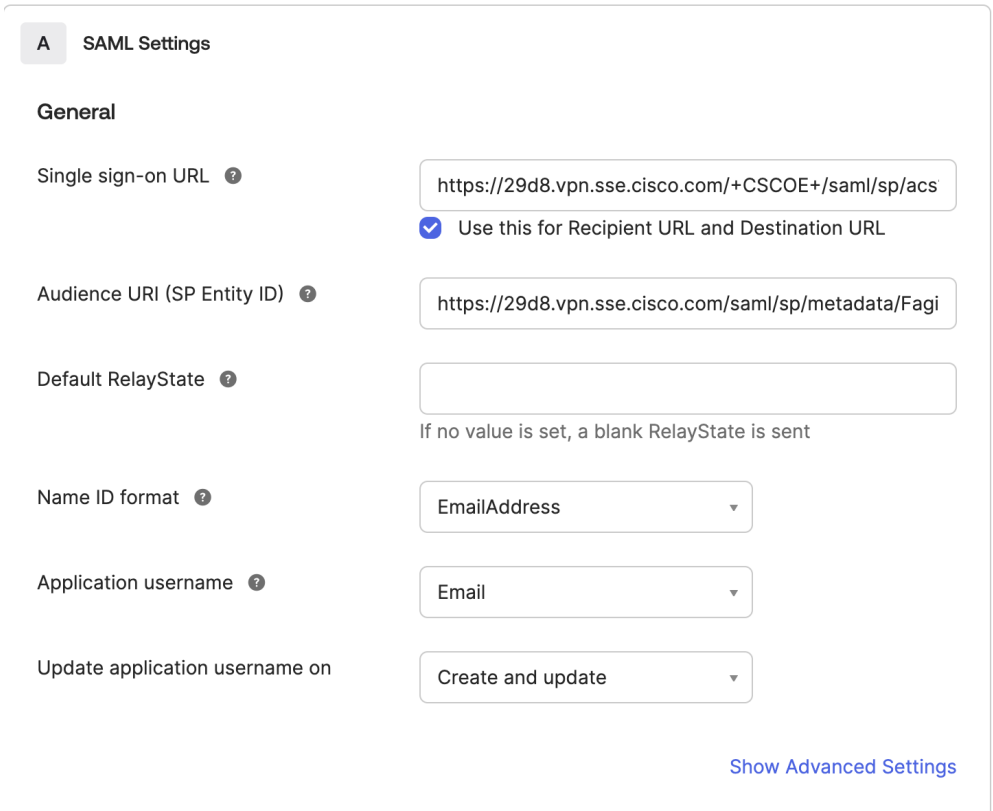

VPN Profile
A VPN profile allows for configuration of remote user connections through a VPN. Help
VPN Profile name
Fagioli1_VPN
1 General settings
Default Domain: fagioli1.local | DNS Server: - |
Protocol: TLS / DTLS
2 Authentication
3 Traffic Steering (Split Tunnel)
4 Cisco Secure Client Configuration
General settings
Select and configure the network, protocol and posture that this VPN profile will use. Help
Default Domain
fagioli1.local
DNS Server
Use region configuration
+ New
Protocol
TLS / DTLS
IKEv2
Connect time posture (optional)
None
Multiple VPN postures can be created in Posture.


VPN Profile name
Fagioli1_VPN
General settings
Default Domain: fagioli1.local | DNS Server: - |
Protocol: TLS / DTLS
Authentication
Traffic Steering (Split Tunnel)
Cisco Secure Client Configuration
Authentication Method
SAML
SAML Configuration
SAML Metadata XML Configuration
1. Download Service Provider XML file
This XML file contains metadata required to configure your IdP.
Download service provider XML file
2. Generate IdP Security Metadata XML File
a. Upload the Service Provider XML file to your IdP.
b. From your IdP, create and download an IdP Security Metadata XML file.
3. Upload IdP security metadata XML file
Drag and drop file here or click to select it
(Security Metadata XML file)
Manual Configuration
Cancel
Back
Next


Create a new app integration
Sign-in method
Learn More
OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

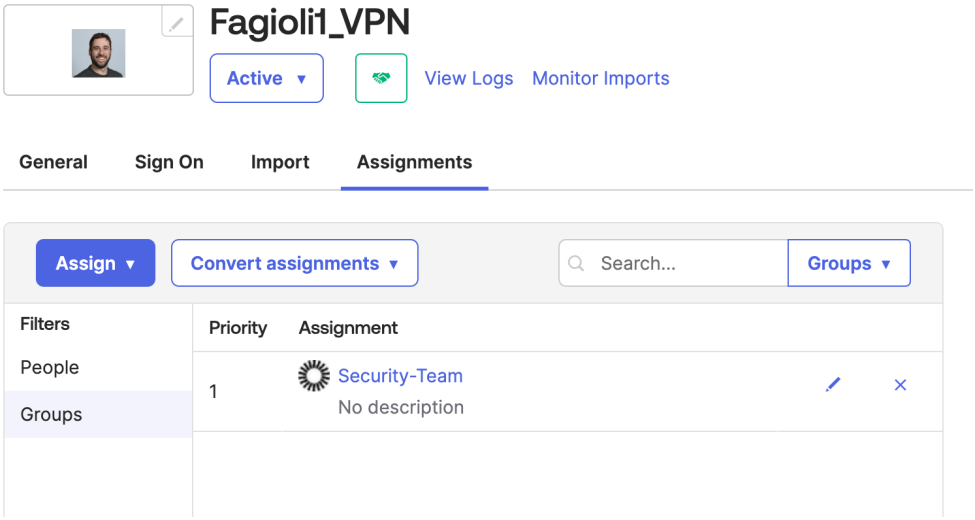


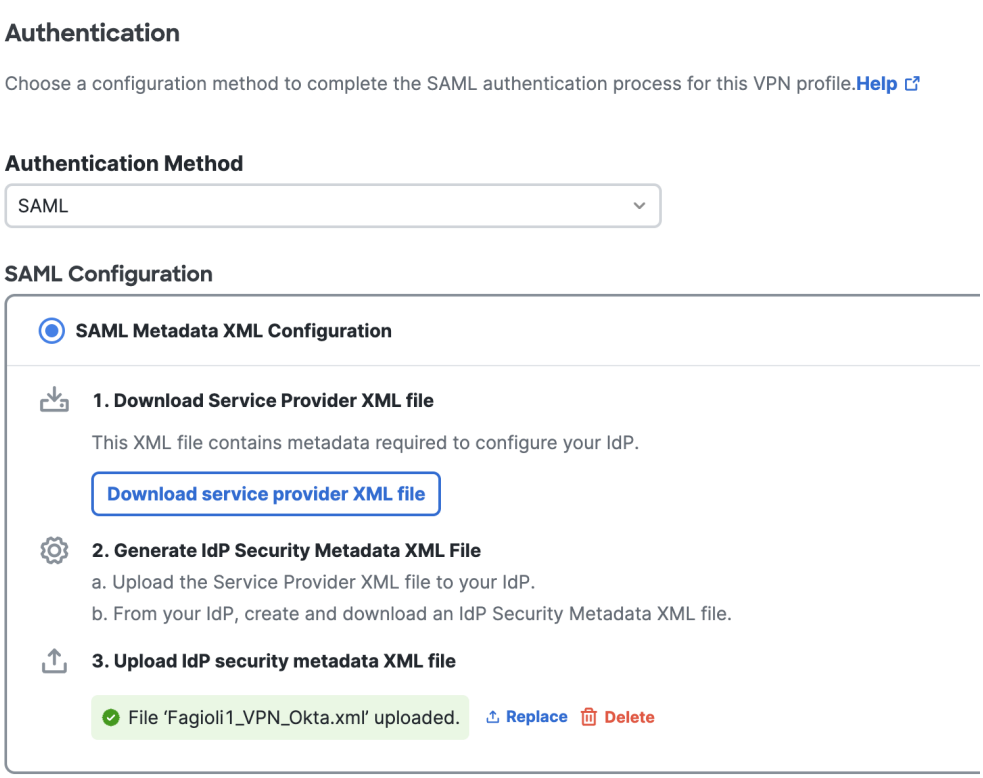
- Picture name: **IMG_7160.jpg**
- Single sign-on URL: **<< AssertionConsumeService >>**
- Audience URI (SP Entity ID): **<< EntityDescriptor >>**



- XML > save to a file Fagioli1_VPN_Okta.xml

- Select which groups





General settings
Default Domain: fagioli1.local | DNS Server: - | Protocol: TLS / DTLS

Authentication
SAML

3 Traffic Steering (Split Tunnel)
Bypass Secure Access | 1 Exceptions

4 Cisco Secure Client Configuration

Traffic Steering (Split Tunnel)

Configure how VPN traffic traverses your network. Help

Tunnel Mode

Bypass Secure Access

All traffic is steered outside the tunnel.

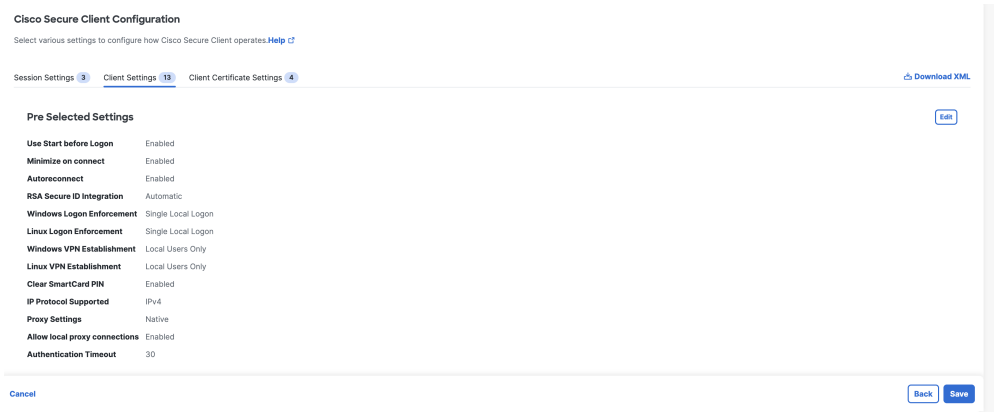
Add Exceptions

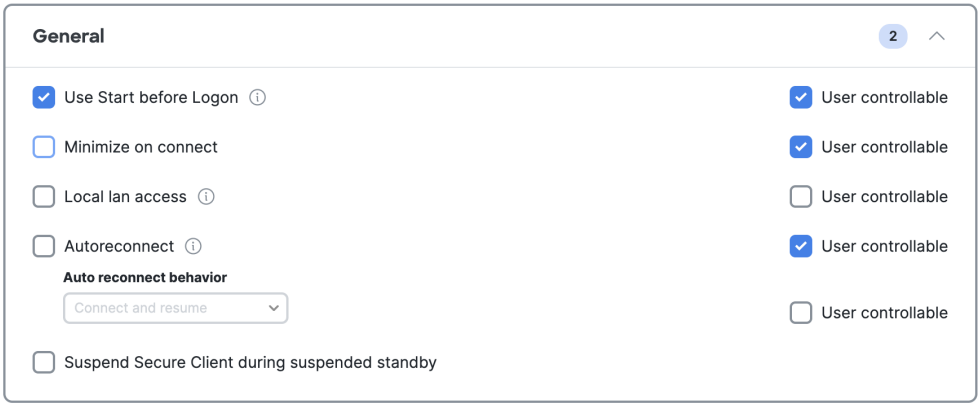
Destinations specified here will be steered INSIDE the tunnel.

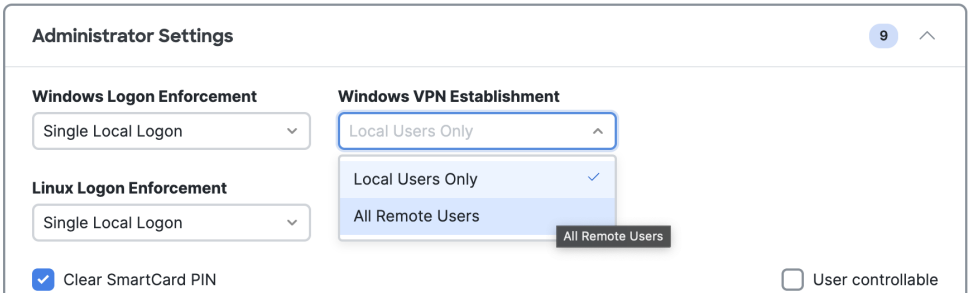
Destinations
10.1.1.0/24

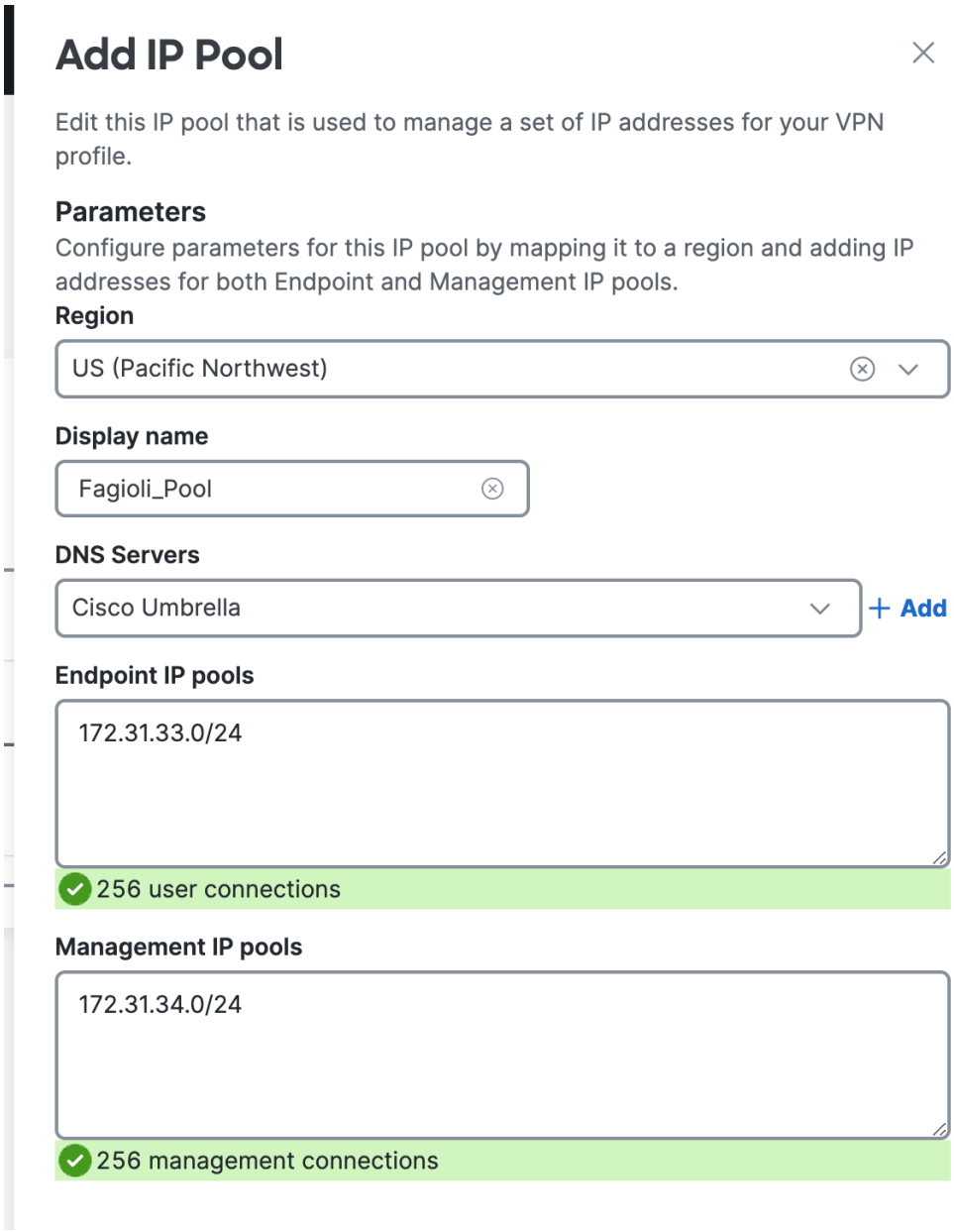
DNS Mode

Default DNS

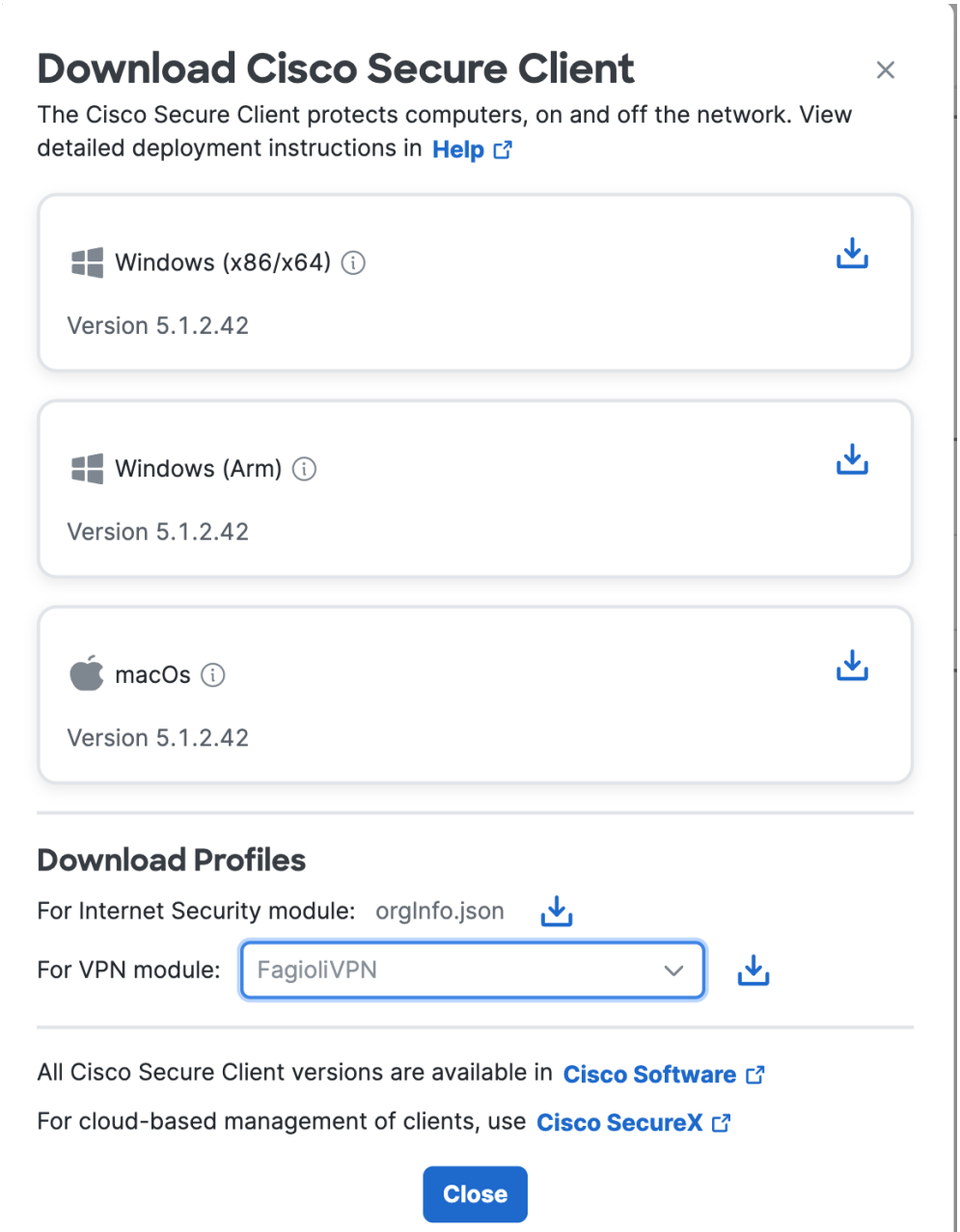




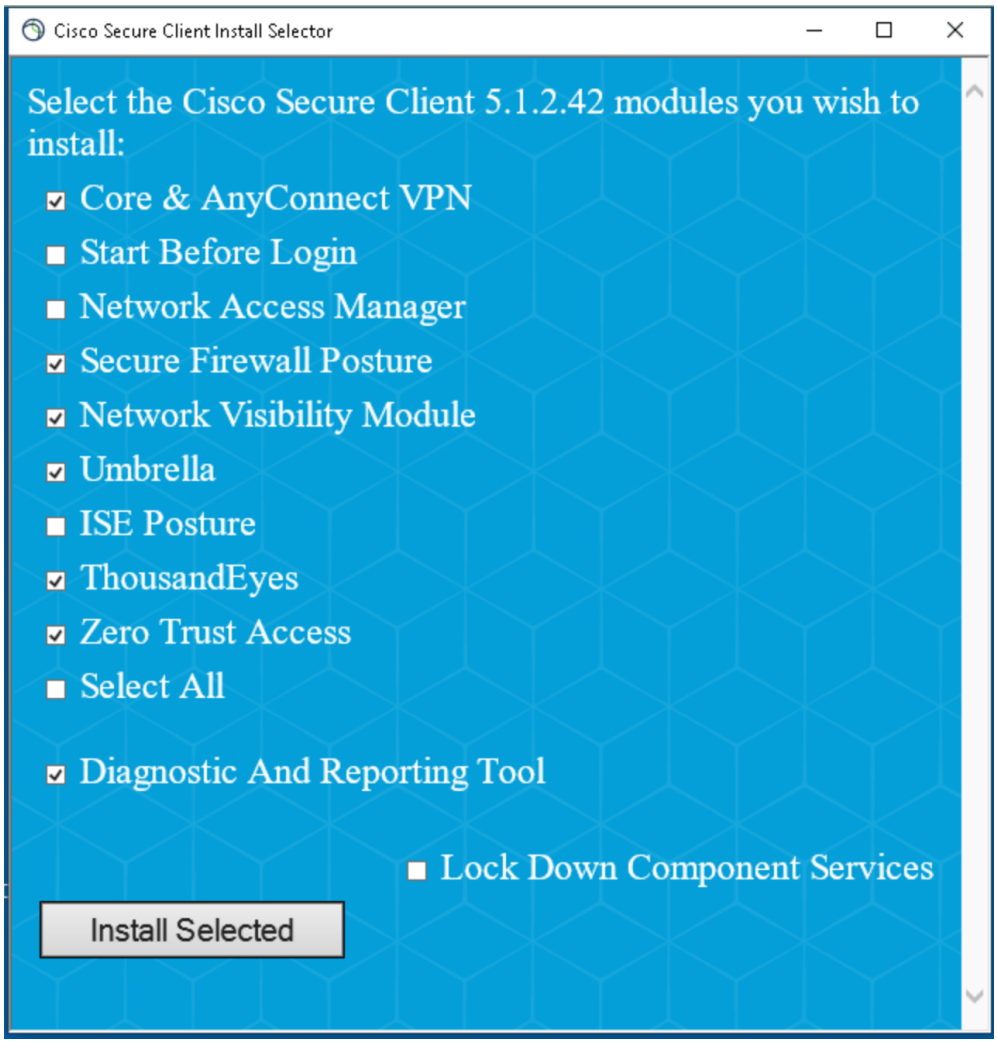




- Download Cisco Secure Client and Profiles
  - Open Secure Access console inside Win10-TPM

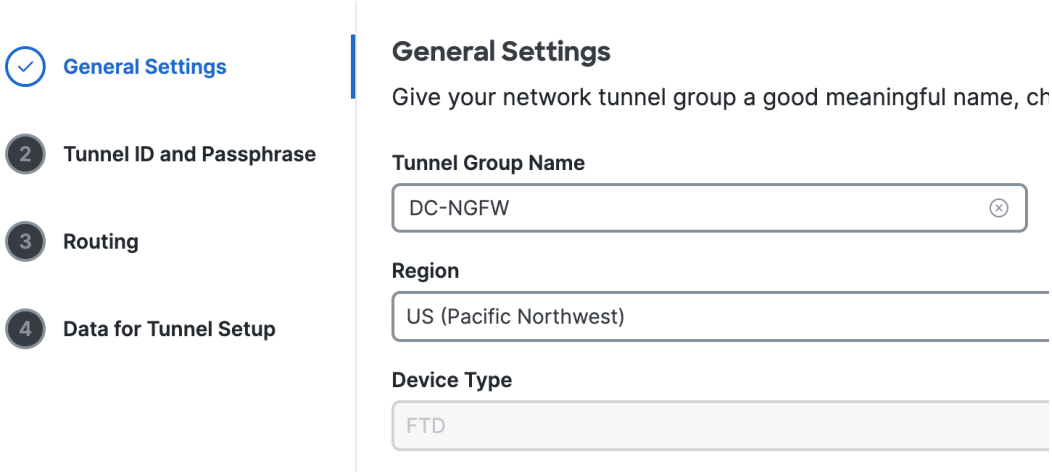


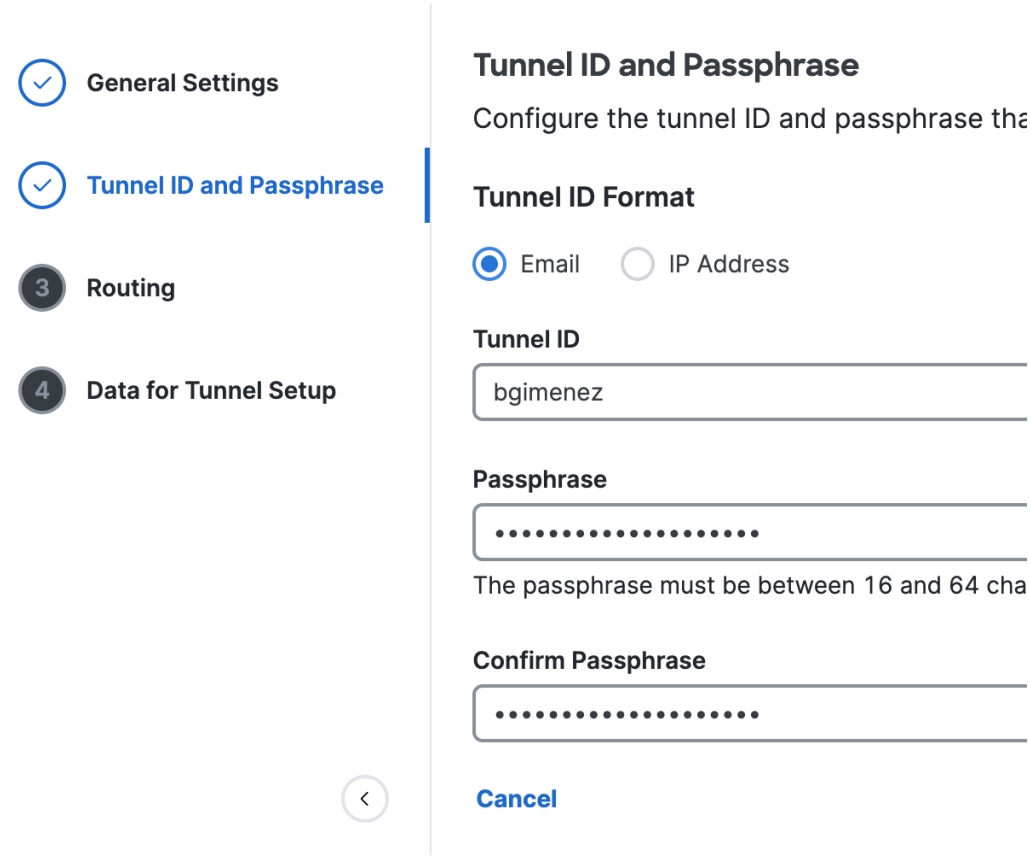
-
- Add the profiles inside the folders
- Install Secure Client



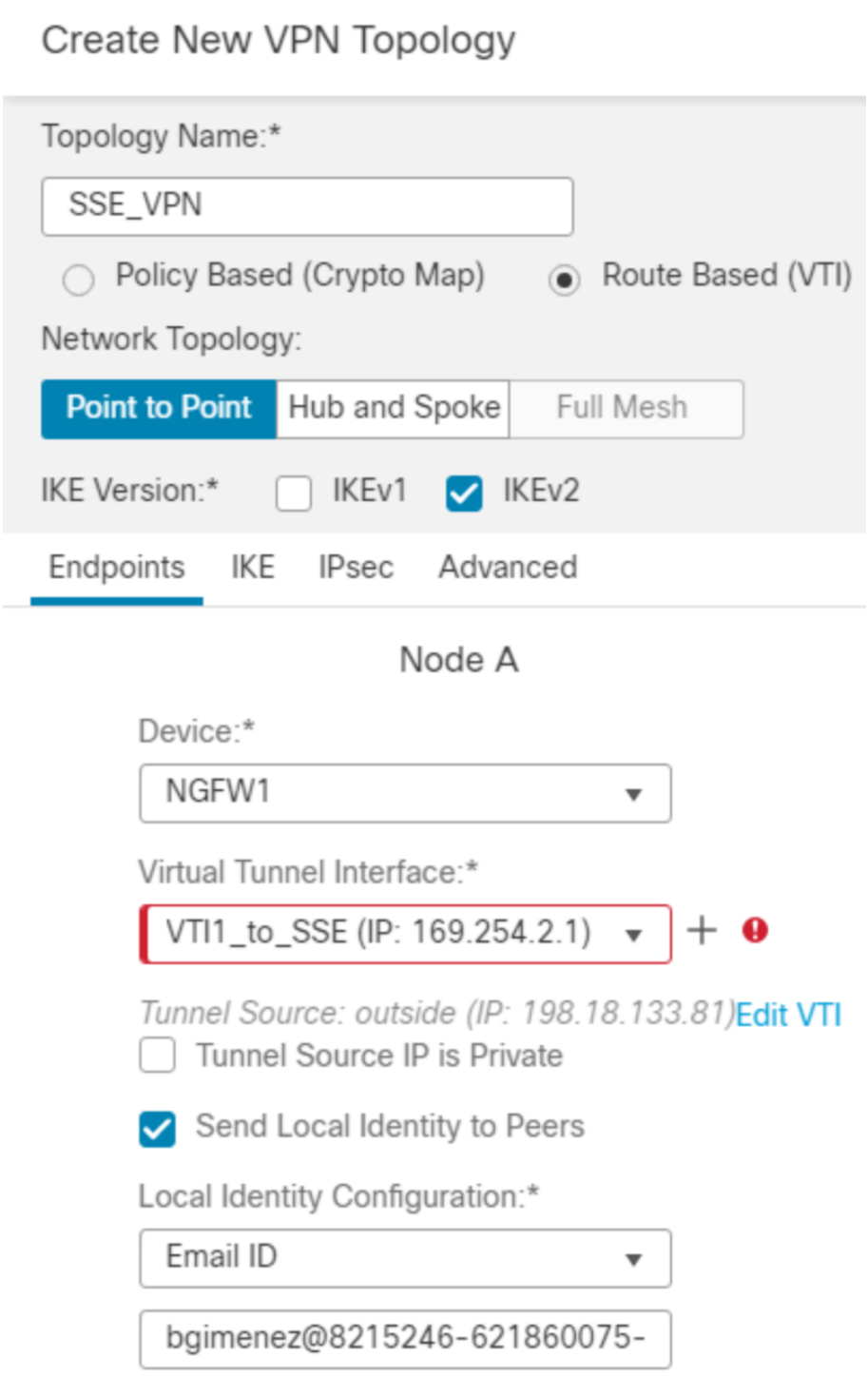
- Reboot
- Test VPN Login

2. Network Connections
    - Network Tunnel Groups



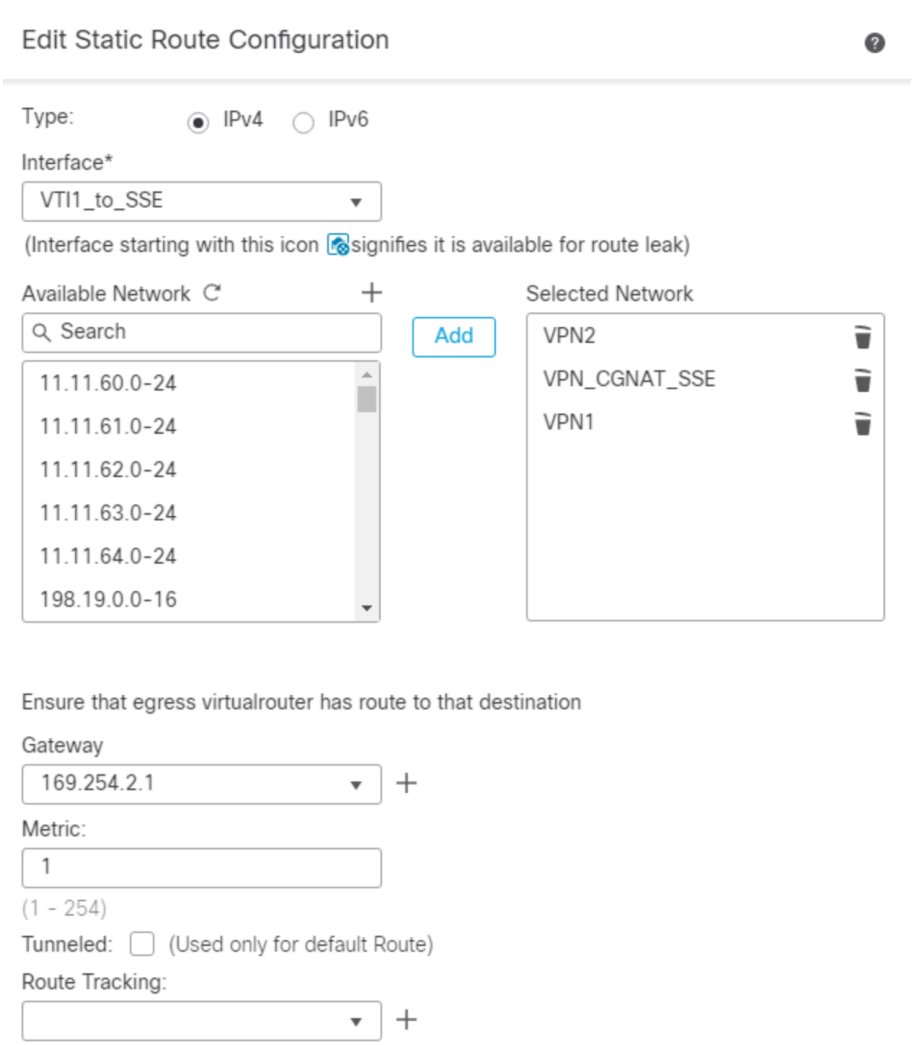


- Passphrase: C1sco12345C1sco12345
- Static Routing: 10.1.1.0/24
- FMC configuration
    1. VPN S2S

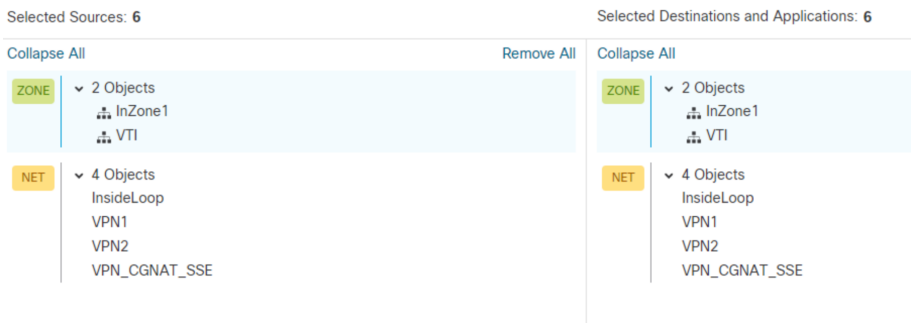


2. Routing
   - Secure Access is always .1 IP address for VTI VPN-Based
   - VPN1: 172.31.33.0/24
   - VPN2: 172.31.34.0/24
   - VPN_CGNAT: 100.64.0.0/10

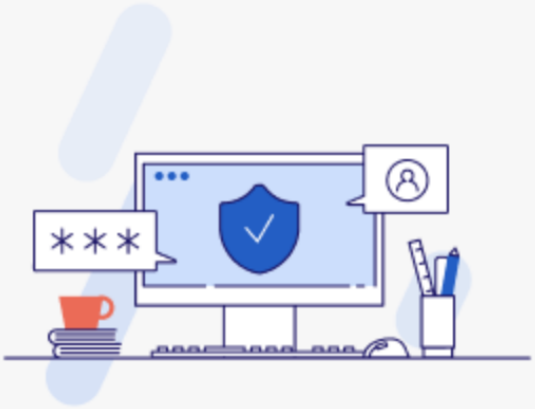
Name	Value
VPN1	172.31.33.0/24
VPN2	172.31.34.0/24
VPN_CGNAT_SSE	100.64.0.0/10



3. ACP
    - Create a rule at the top



3. Users and Groups
    - Configuration Management



Connect to any SAML and supported ID Providers.

Configure

Configure SSO Authentication

Manage how users are authenticated to Secure Access and log in. Help

- Authentication Method
  SAML
- Identity Provider
  Okta , Re-Authenticate Users Daily
- 3 Configuration

SAML Provider Authentication

Configure how your IdP authenticates to Secure Access.

Select Identity Provider

You must complete the IdP's prerequisites before configuring it.

Okta

Entity ID

Use Secure Access's entity ID to authentiate Secure Access to your IdP.

Organization-specific Entity ID

Enable to configure SAML for multiple organizations that use the same IdP.

Disabled

Entity ID URL

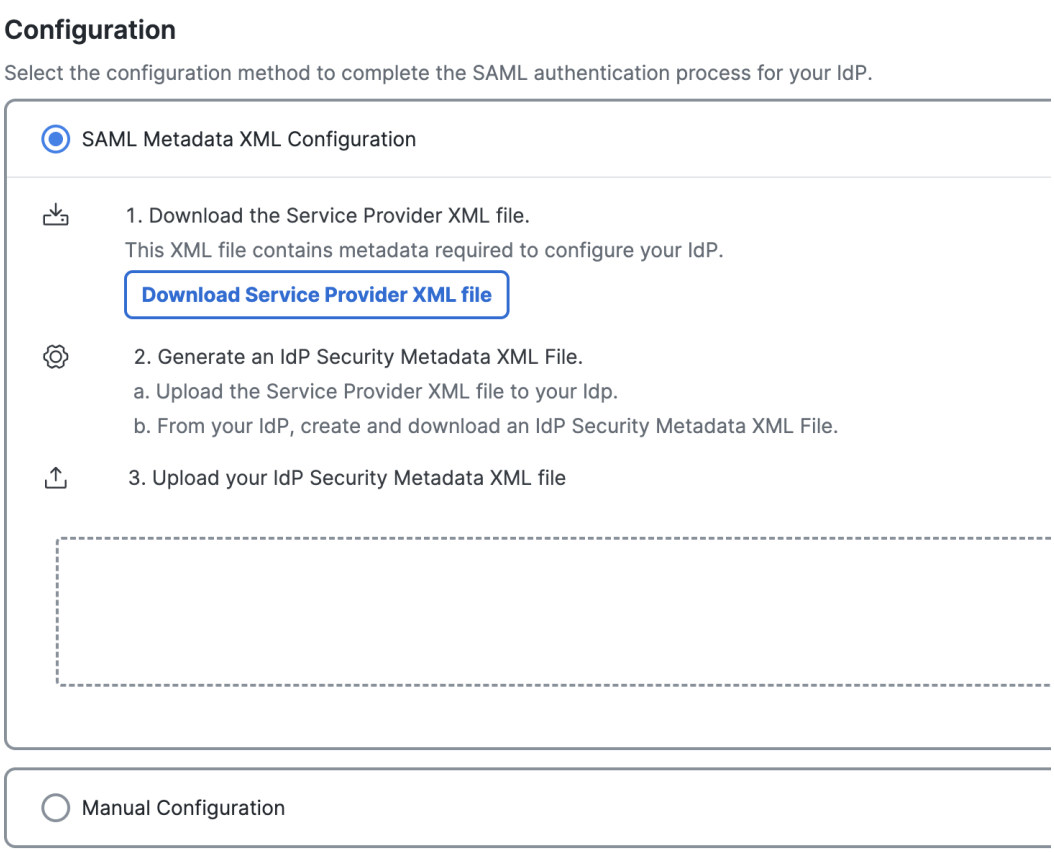
Copy and save this Entity URL. It is required when configuring your IdP.

saml.fg.id.sse.cisco.com Copy URL

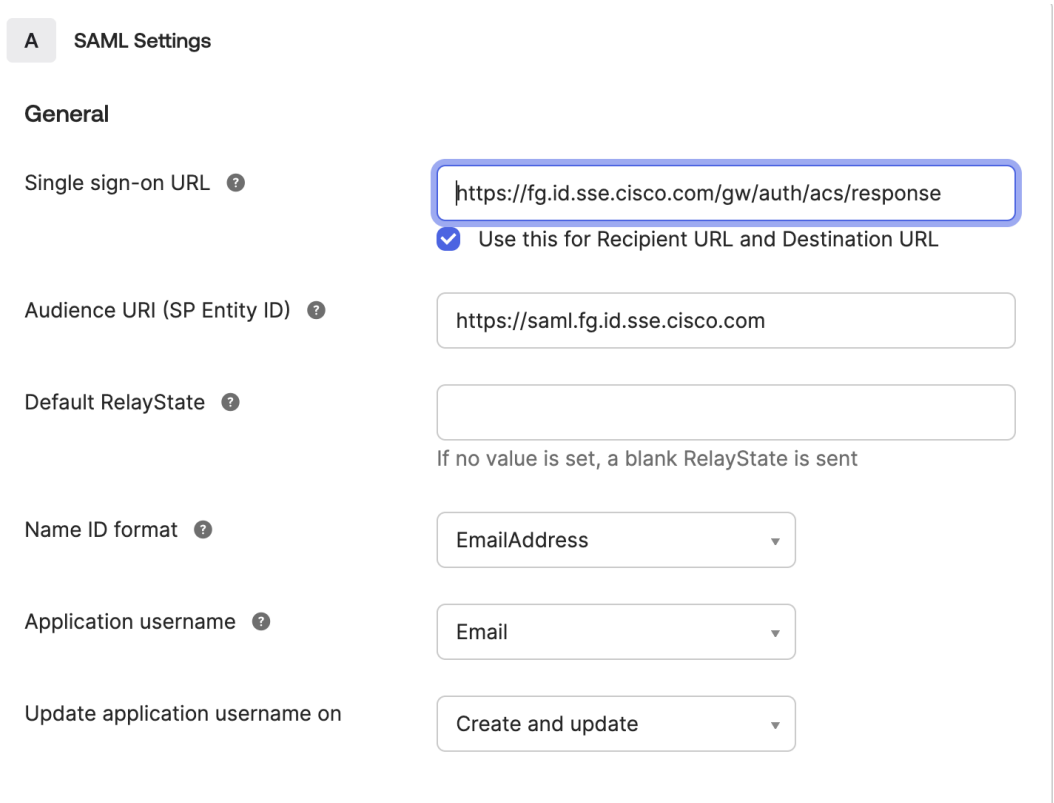
IdP authentication frequency

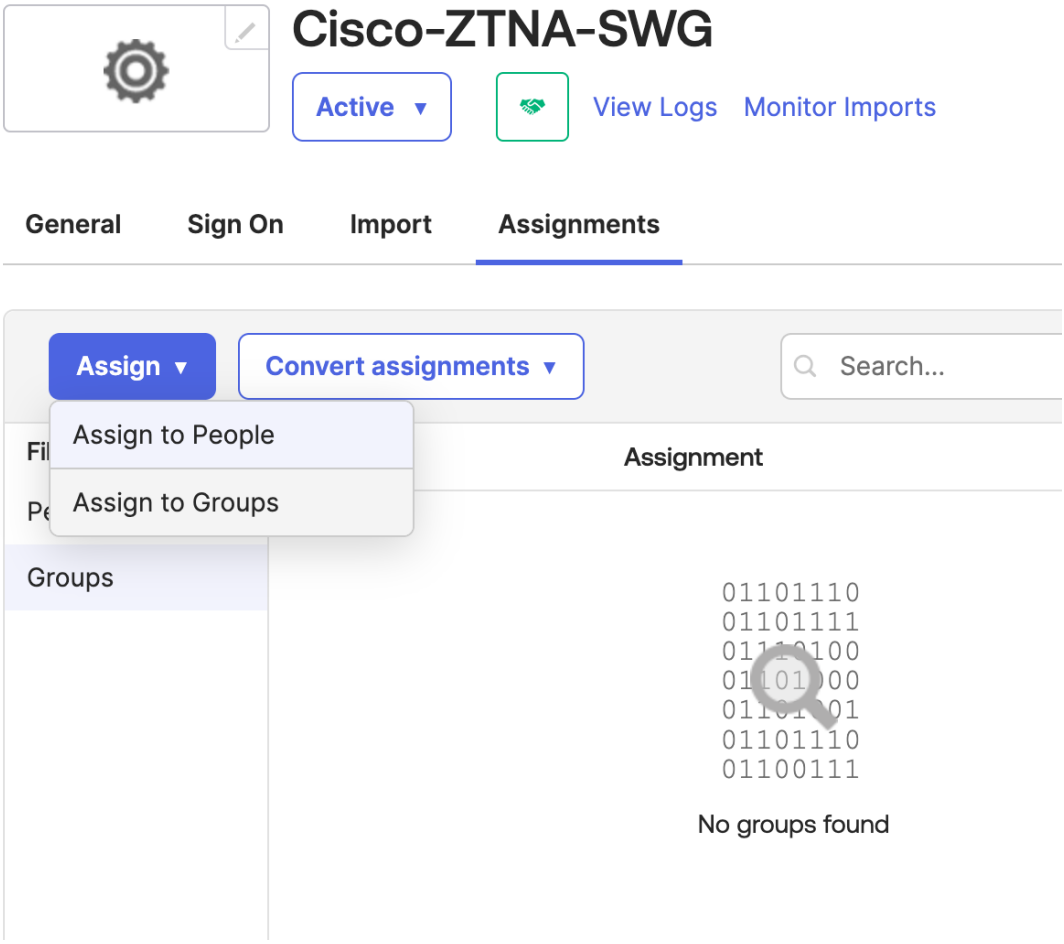
Chose how often Secure Access verifies web proxy users by re-authenticating them.

Daily



- Single sign-on URL: << AssertionConsumerService >>
- SP Entity ID: << EntityDescriptor : entityID : https:// >>





- Picture name: **IMG_7160.jpg**
- Enroll Win10 computer

2. **Resources**
    1. Private Resources

Private Resource Name

Net-10-1-1-0-25

Description (optional)

Entire 10.1.1.0/25

ommunication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secu

Internally reachable address (FQDN, Wildcard FQDN, IP Address, CIDR) ⓘ | **Protocol** | **Port / Rang**

10.1.1.0/25 | Any TCP | 22,80

+ IP Address or FQDN

Use internal DNS server to resolve the domain

ndpoint Connection Methods

Specify the ways user endpoints can reach this resource. Later, access rules will determine which users and devices

Branch Connections

Allow users and devices on the network, such as printers or kiosks, to connect to this resource if allowed by acces

Zero-trust connections

Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. **Help**

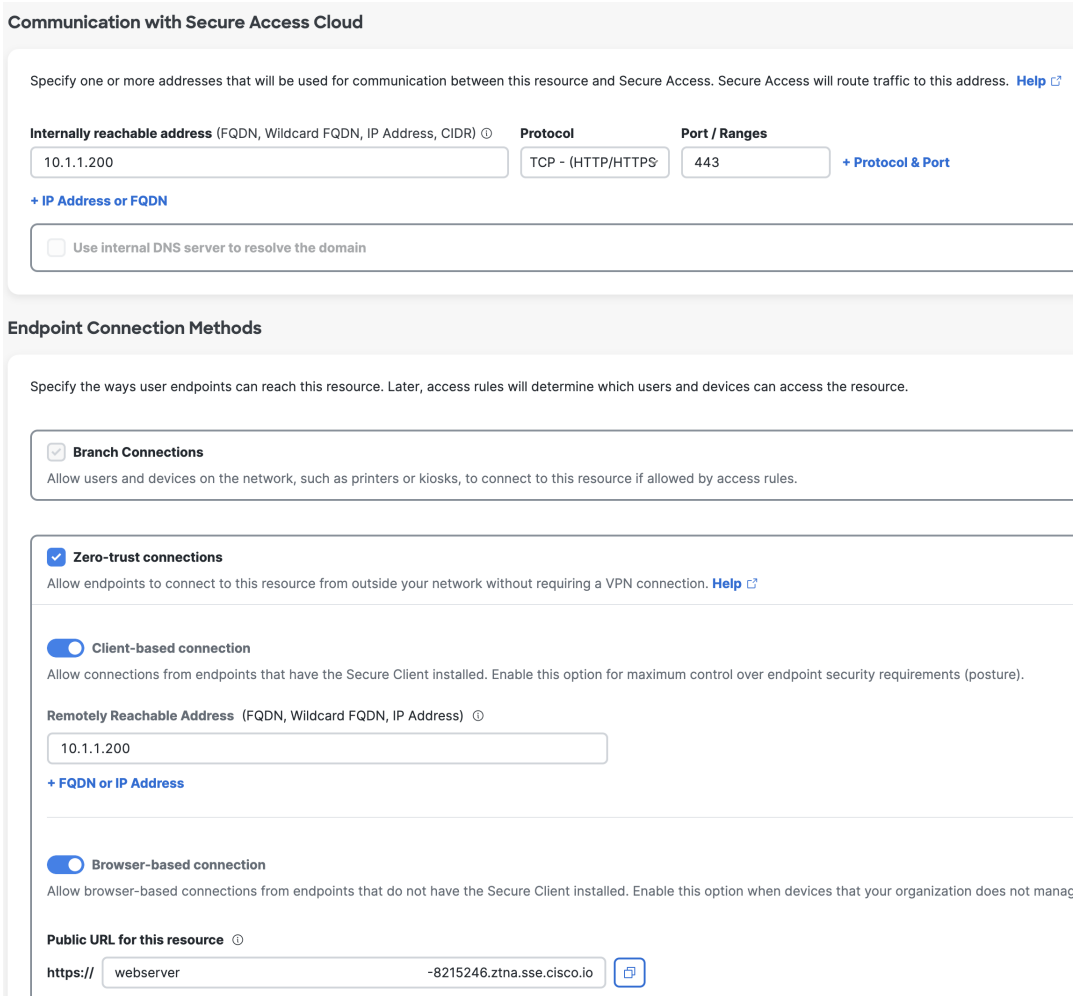
Client-based connection

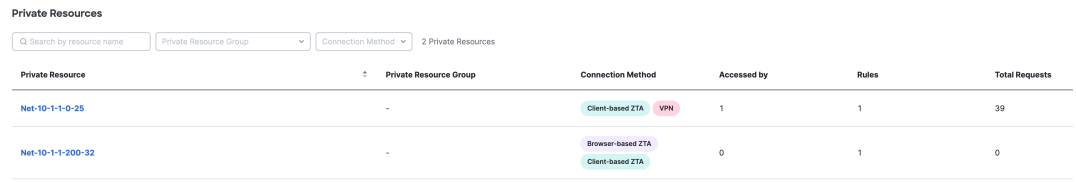
Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control ov

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

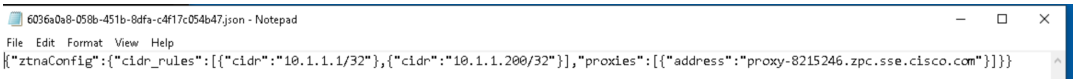
10.1.1.0/25

+ FQDN or IP Address

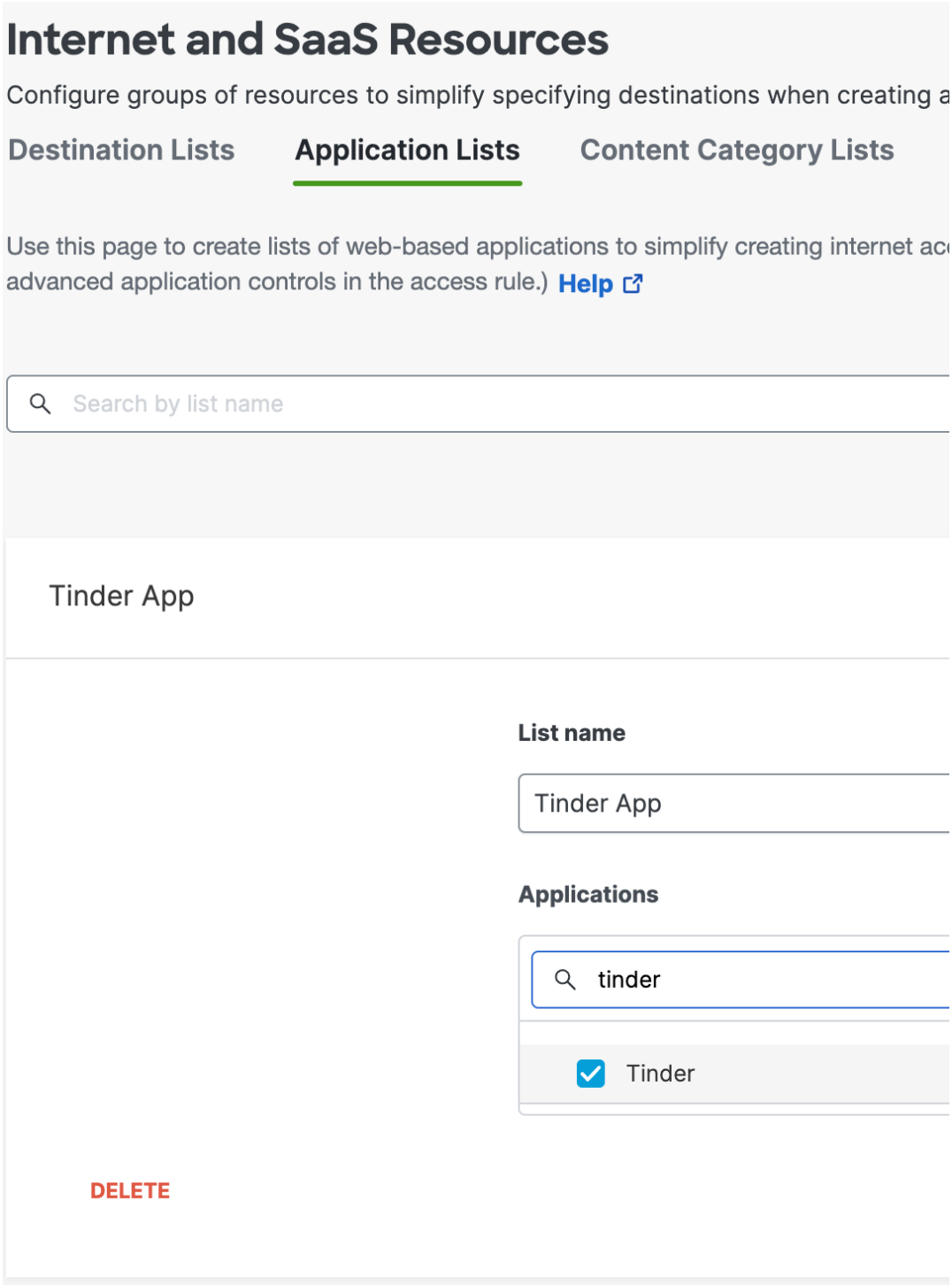




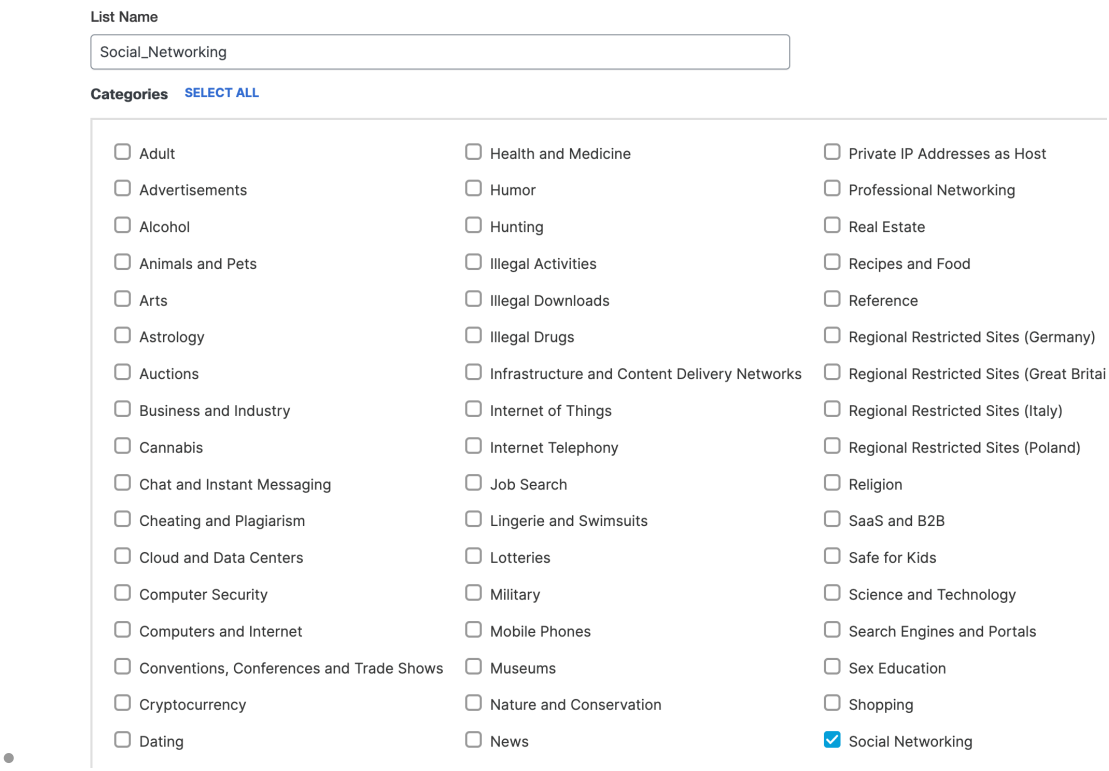
- Check ZTNA configuration on Win10
  - C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs



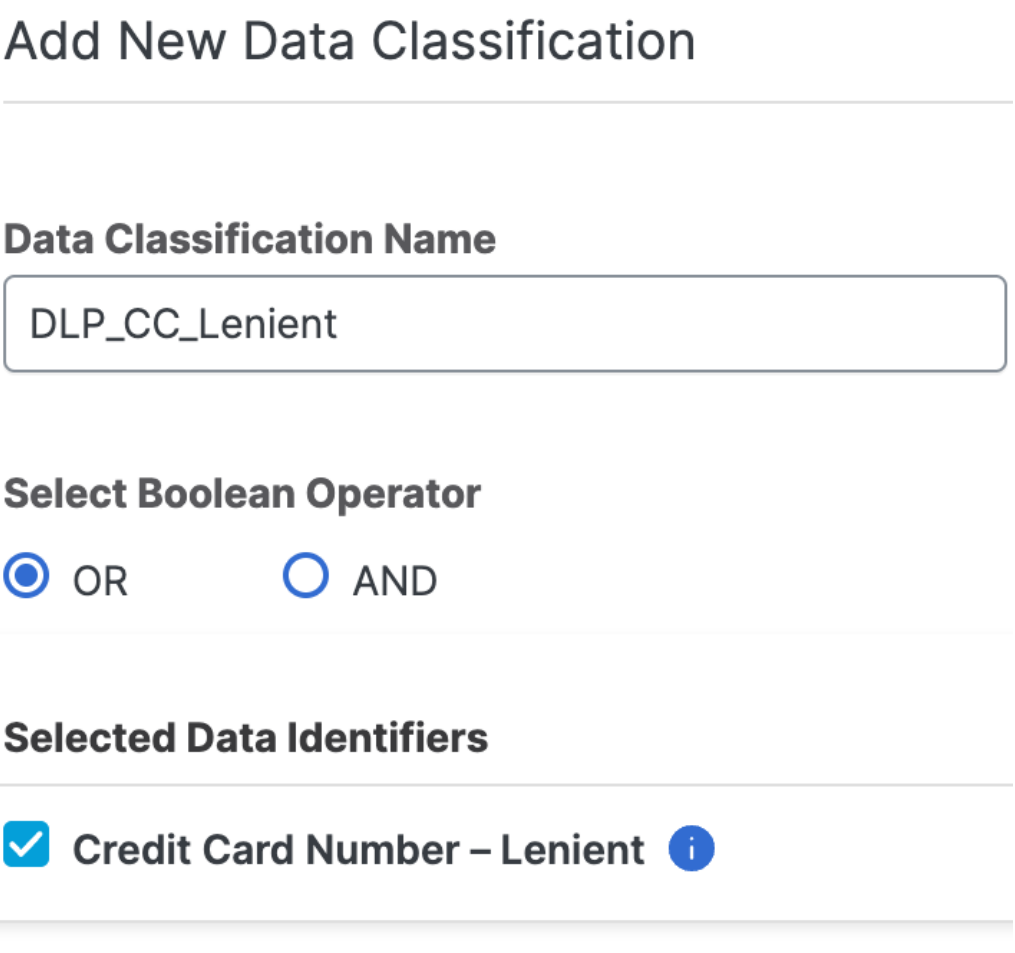
2. Internet and SaaS Resources


Internet and SaaS Resources
Configure groups of resources to simplify specifying destinations when creating a
Destination Lists
Application Lists
Content Category Lists
Use this page to create lists of web-based applications to simplify creating internet ac
advanced application controls in the access rule.) Help
Search by list name
Tinder App
List name
Tinder App
Applications
tinder
Tinder
DELETE

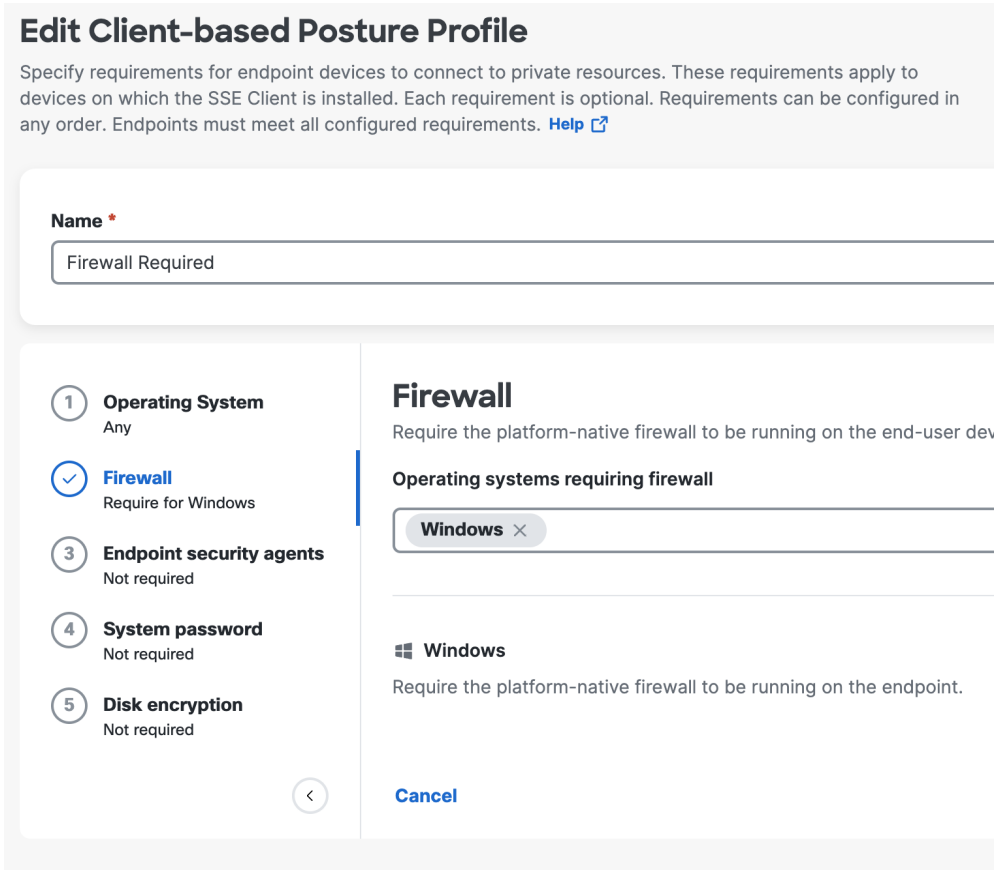
Social_Networking

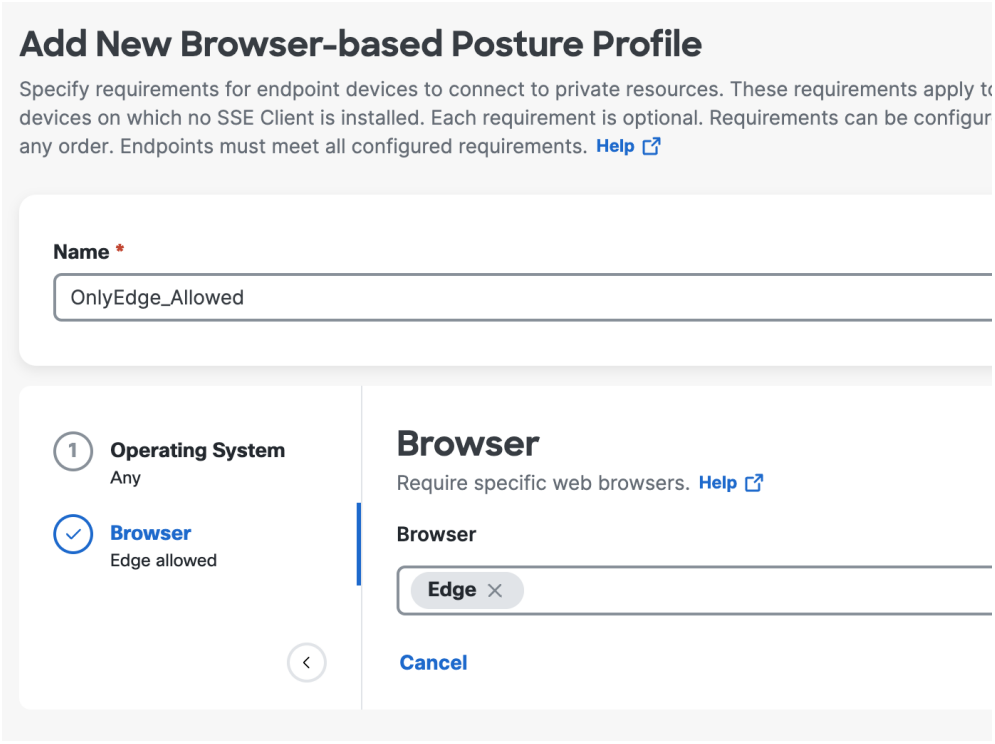


3. **Secure**
    1. Data Classification

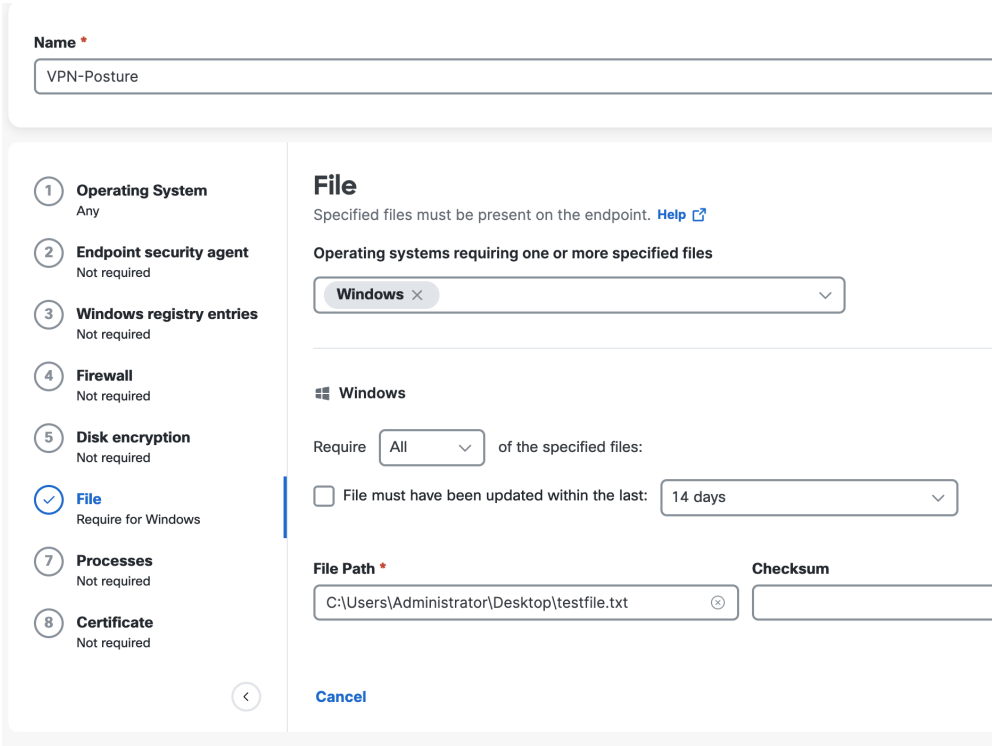


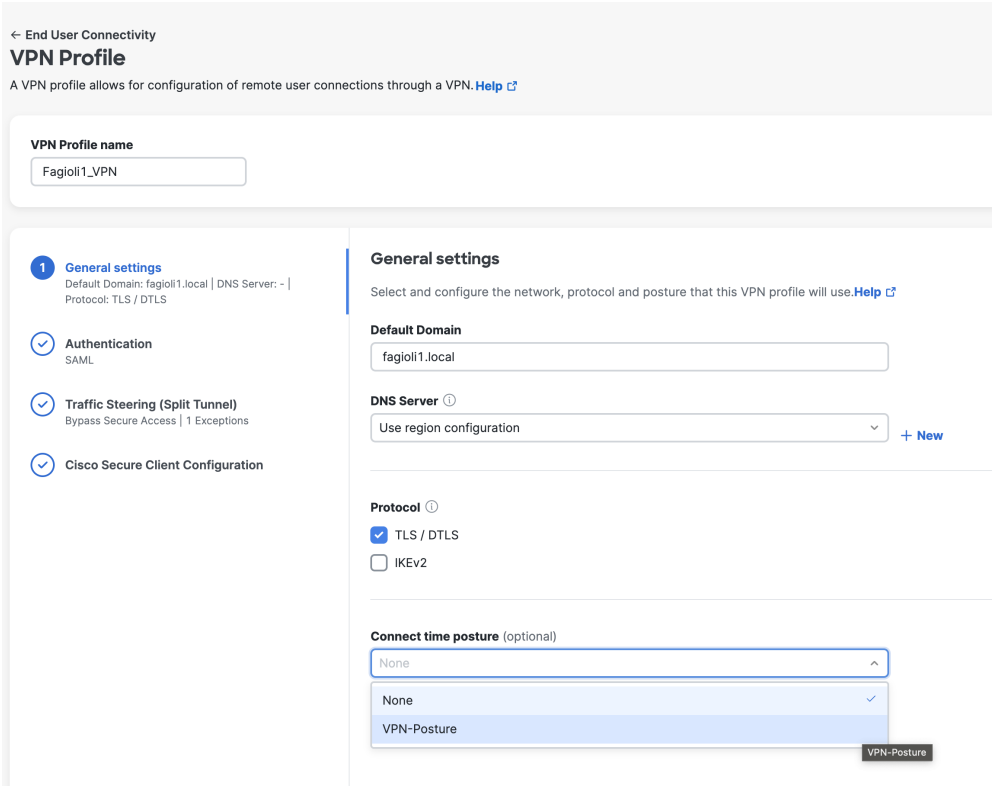
2. Endpoint Posture Profiles
    - Zero Trust Connection



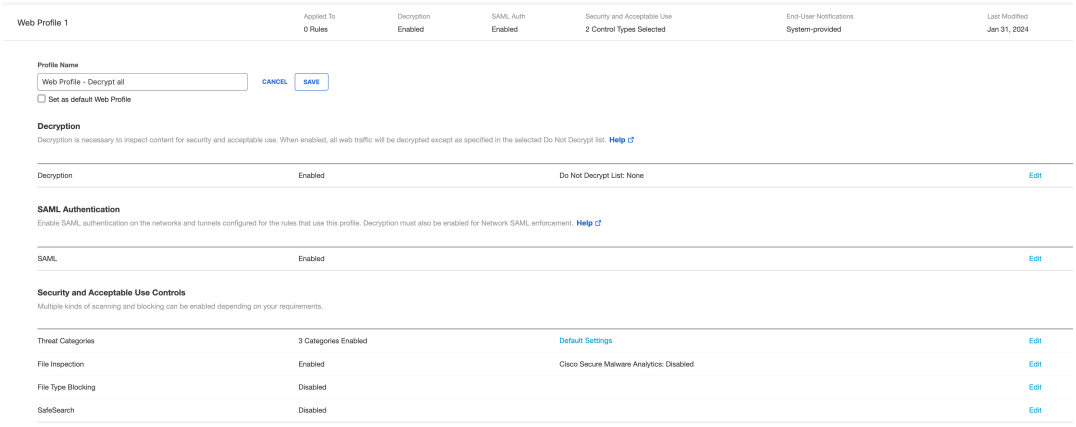


- VPN Connection





3. Web Profiles



4. Data Loss Prevention Policy

Add New Real Time Rule

Configure this rule to set the criteria as to what triggers its enforcement. The Realtime DLP inspects data violation is detected, this rule's Action setting is automatically enforced. Help

Rule Name

block-CreditCard

Severity

High

Data Classifications

Select where to search for the selected data classifications.

Content File Name Content and File Name

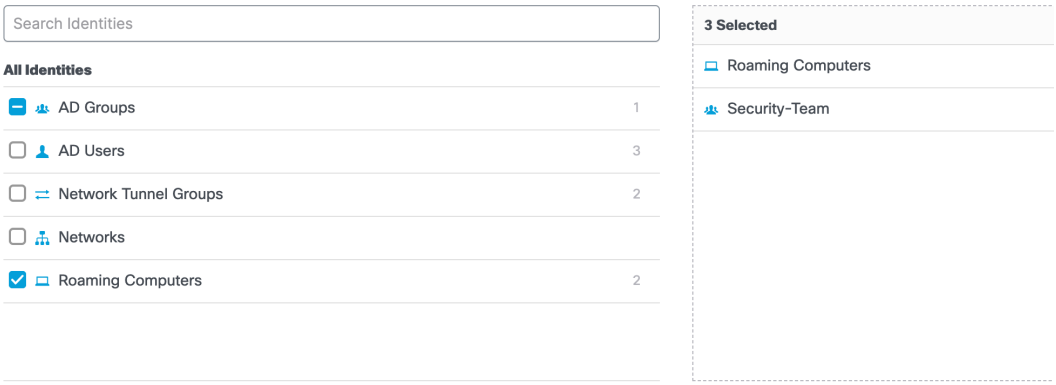
Select data classifications to add them to this rule.

Search Classifications

☐	Built-in GDPR Classification	PREVIEW
☐	Built-in HIPAA Classification	PREVIEW
☐	Built-in PCI Classification	PREVIEW
☐	Built-in PII Classification	PREVIEW
☑	DLP_CC_Lenient	PREVIEW

Identities

Select identities to add them to this rule.

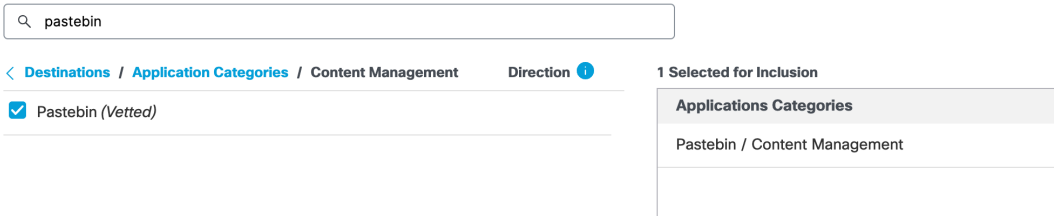


Destinations

Manage destination lists and vetted applications for this rule.

All Destinations
Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

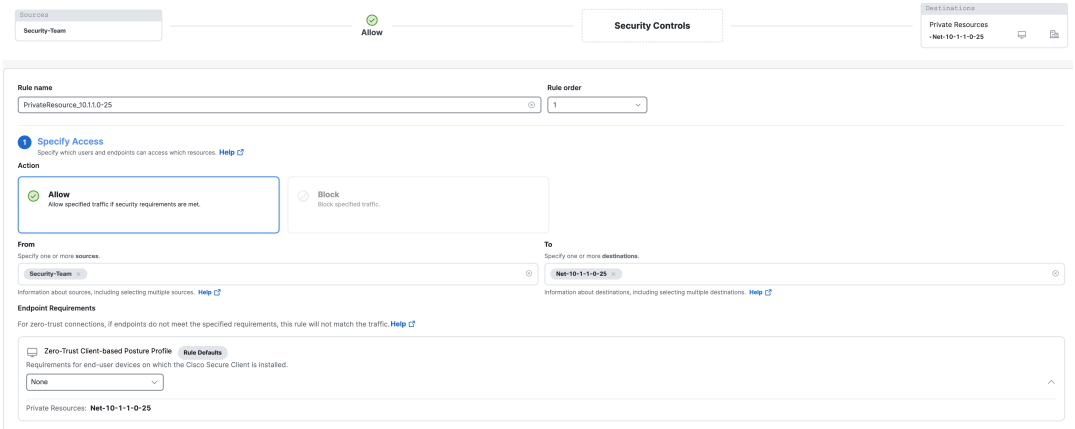
Select Destinations Lists and Applications for Inclusion
Scans selected destination lists and vetted applications.

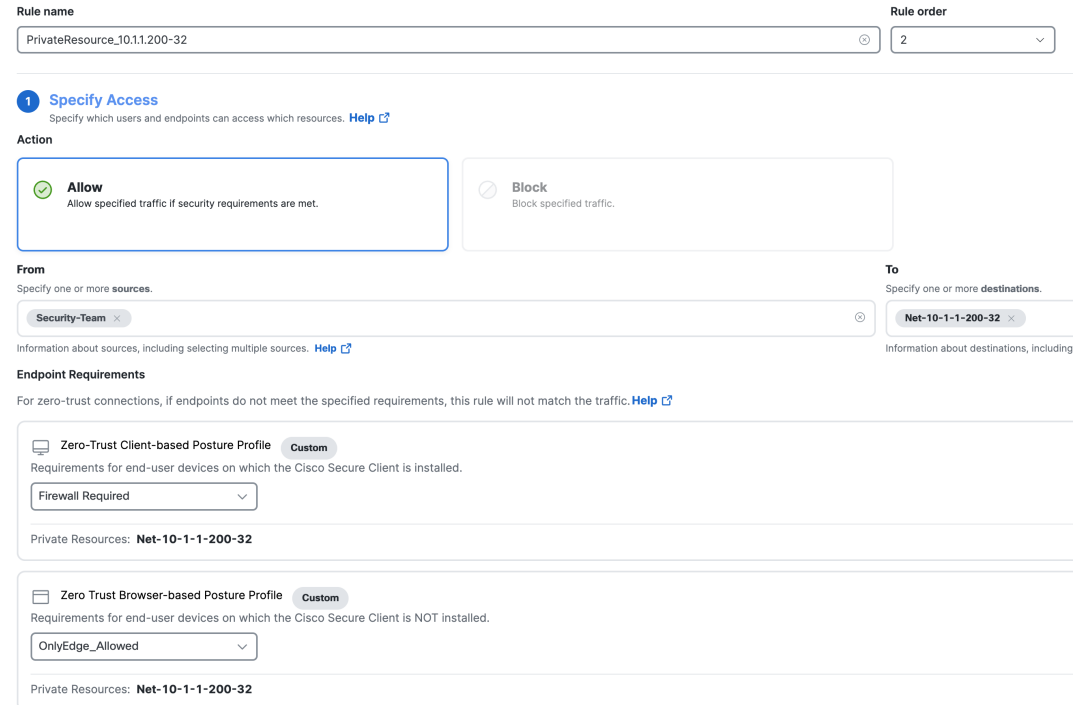


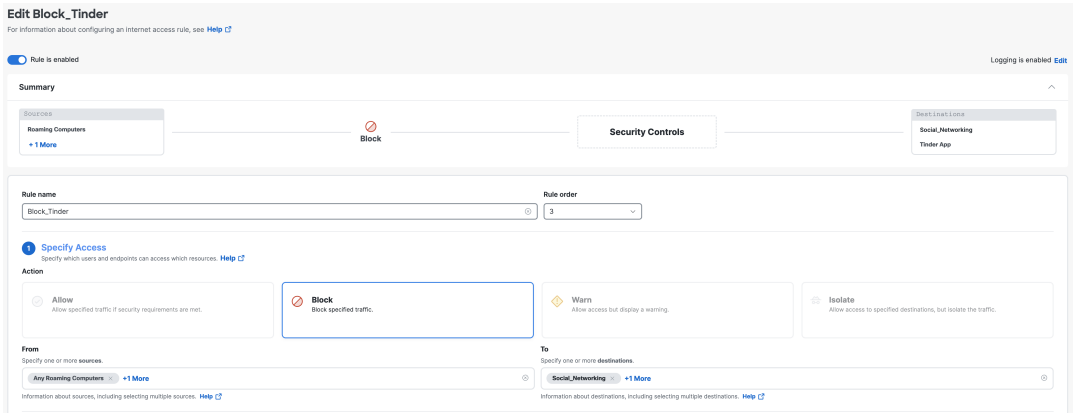
1 DLP Rule

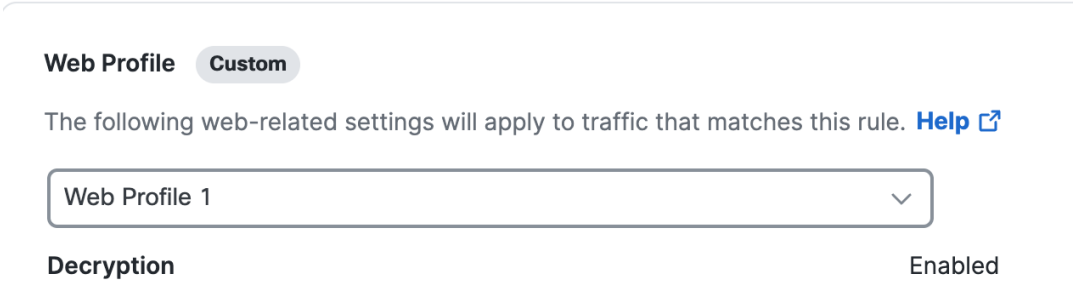
Rule Type	Name	Severity	Action	Identities or File Owners	Destinations	Data Classifications File Labels	Last Modified
Real Time	block-CreditCard	High	Block	2 Identities	Inclusion 1 Application	Data Classifications DLP_CC_Lenient	Feb 18, 2024

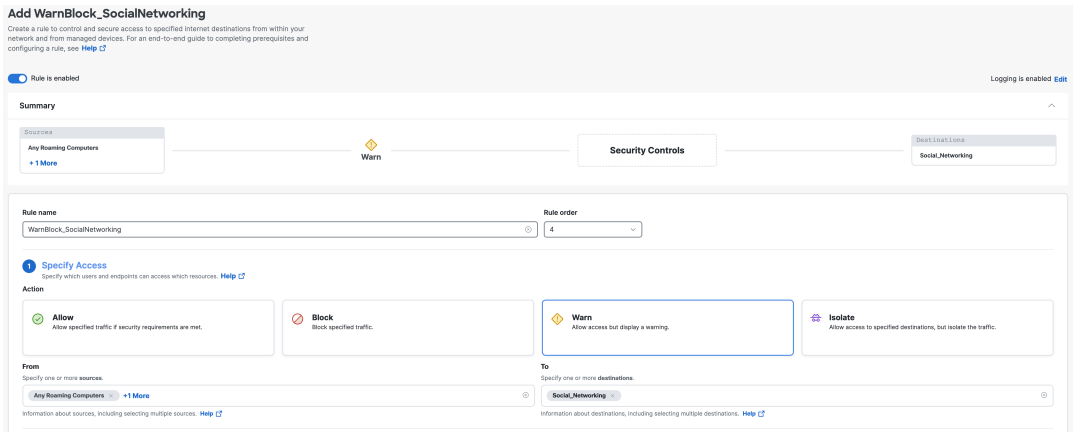
5. Access Policy

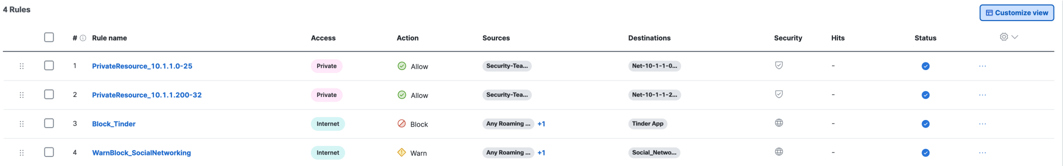



Rule name
PrivateResource_10.1.1.200-32
Rule order
2
1 Specify Access
Specify which users and endpoints can access which resources. Help
Action
Allow
Allow specified traffic if security requirements are met.
Block
Block specified traffic.
From
Specify one or more sources.
Security-Team
To
Specify one or more destinations.
Net-10-1-1-200-32
Information about sources, including selecting multiple sources. Help
Information about destinations, including
Endpoint Requirements
For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. Help
Zero-Trust Client-based Posture Profile
Custom
Requirements for end-user devices on which the Cisco Secure Client is installed.
Firewall Required
Private Resources: Net-10-1-1-200-32
Zero Trust Browser-based Posture Profile
Custom
Requirements for end-user devices on which the Cisco Secure Client is NOT installed.
OnlyEdge_Allowed
Private Resources: Net-10-1-1-200-32


Edit Block_Tinder
For information about configuring an internet access rule, see Help
Rule is enabled
Logging is enabled Edit
Summary
Sources
Roaming Computers
+ 1 More
Block
Security Controls
Destinations
Social_Networking
Tinder App
Rule name
Block_Tinder
Rule order
3
1 Specify Access
Specify which users and endpoints can access which resources. Help
Action
Allow
Allow specified traffic if security requirements are met.
Block
Block specified traffic.
Warn
Allow access but display a warning.
Isolate
Allow access to specified destinations, but isolate the traffic.
From
Specify one or more sources.
Any Roaming Computers
+1 More
To
Specify one or more destinations.
Social_Networking
+1 More
Information about sources, including selecting multiple sources. Help
Information about destinations, including selecting multiple destinations. Help


Web Profile
Custom
The following web-related settings will apply to traffic that matches this rule. Help
Web Profile 1
Decryption
Enabled

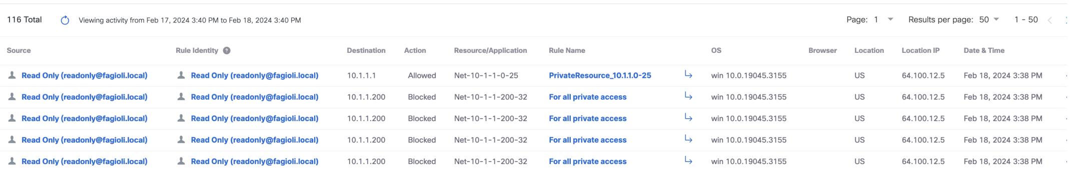

Add WarnBlock_SocialNetworking
Create a rule to control and secure access to specified internet destinations from within your network and from managed devices. For an end-to-end guide to completing prerequisites and configuring a rule, see Help
Rule is enabled
Logging is enabled Edit
Summary
Sources
Any Roaming Computers
+ 1 More
Warn
Security Controls
Destinations
Social_Networking
Rule name
WarnBlock_SocialNetworking
Rule order
4
1 Specify Access
Specify which users and endpoints can access which resources. Help
Action
Allow
Allow specified traffic if security requirements are met.
Block
Block specified traffic.
Warn
Allow access but display a warning.
Isolate
Allow access to specified destinations, but isolate the traffic.
From
Specify one or more sources.
Any Roaming Computers
+1 More
To
Specify one or more destinations.
Social_Networking
Information about sources, including selecting multiple sources. Help
Information about destinations, including selecting multiple destinations. Help

- 
4 Rules

Customize view

	#	Rule name	Access	Action	Sources	Destinations	Security	Hits	Status
	1	PrivateResource_10.1.1.0-25	Private	Allow	Security-Tea...	Net-10-1-1-0...		-	
	2	PrivateResource_10.1.1.200-32	Private	Allow	Security-Tea...	Net-10-1-1-2...		-	
	3	Block_Tinder	Internet	Block	Any Roaming ... +1	Tinder App		-	
	4	WarnBlock_SocialNetworking	Internet	Warn	Any Roaming ... +1	Social_Netwo...		-	

4. **Tests**
    1. Posture for VPN and ZTNA
        - VPN
            - Check file testfile.txt exists in Desktop. It fails if it doesn't
        - ZTNA Client-based
            - SSH to 10.1.1.1 - it doesn't require firewall, it should work
            - HTTPS to 10.1.1.200 - Requires Firewall, it should fail otherwise
        - ZTNA Browser
            - Access clientless from other computer to https://webserver-8215246.ztna.sse.cisco.io/ - only Edge allowed, it should fail otherwise
    2. VPN on
        - Ping 10.1.1.1-126 - it should work
        - Ping 10.1.1.200 - it should fail, it is not published via VPN access
    3. Web Access
        - DLP - pastebin using creditcard - it should fail
        - Tinder - Application block - it should fail (on/off VPN) - since it is NOT full tunnel, always comes using Roaming client
        - Facebook - Content category block - since it is NOT full tunnel, always comes using Roaming client
5. **Monitor**
    1. ZTNA Client-Based

- 
116 Total   Viewing activity from Feb 17, 2024 3:40 PM to Feb 18, 2024 3:40 PM   Page: 1   Results per page: 50   1 - 50

Source	Rule Identity	Destination	Action	Resource/Application	Rule Name	OS	Browser	Location	Location IP	Date & Time
Read Only (readonly@fagioli.local)	Read Only (readonly@fagioli.local)	10.1.1.1	Allowed	Net-10-1-1-0-25	PrivateResource_10.1.1.0-25	win 10.0.19045.3155		US	64.100.12.5	Feb 18, 2024 3:38 PM
Read Only (readonly@fagioli.local)	Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	win 10.0.19045.3155		US	64.100.12.5	Feb 18, 2024 3:38 PM
Read Only (readonly@fagioli.local)	Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	win 10.0.19045.3155		US	64.100.12.5	Feb 18, 2024 3:38 PM
Read Only (readonly@fagioli.local)	Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	win 10.0.19045.3155		US	64.100.12.5	Feb 18, 2024 3:38 PM
Read Only (readonly@fagioli.local)	Read Only (readonly@fagioli.local)	10.1.1.200	Blocked	Net-10-1-1-200-32	For all private access	win 10.0.19045.3155		US	64.100.12.5	Feb 18, 2024 3:38 PM

Event Details

Action

Allowed

Time

Feb 18, 2024 3:37 PM

Rule Name

PrivateResource_10.1.1.200-32

Identity

Read Only (readonly@fagioli.local)

Security-Team

Policy or Ruleset Identity

Read Only (readonly@fagioli.local)

Resource/Application

Net-10-1-1-200-32

OS

win 10.0.19045.3155

Location

US

Location IP

64.100.12.5

Enpoint Security Agent

windows-defender[]

Firewall

System

System Password

enabled[]

Disk Encryption

None

2. ZTNA Browser-based

Action

Blocked

Time

Feb 18, 2024 3:32 PM

Rule Name

For all private access

Source

Bruno Fagioli (bgimenez@cisco.com)

Rule Identity

Bruno Fagioli (bgimenez@cisco.com)

Resource/Application

Net-10-1-1-200-32

OS

Mac OS X 10.15

Browser

Chrome 121.0

Results per page: 50 1 - 1 of 1

3. Web access

Event Details

Action

Blocked — Public Application

Time

Feb 18, 2024 4:49 PM

Rule Name

Block Tinder

Source

ciscosse

Rule Identity

ciscosse

Internal IP Address

198.18.133.252

External IP Address

64.100.12.5

Destination

https://www.tinder.com/

Hostname

www.tinder.com

Categories

Application Block, Dating

Dispute Categorization

Resource/Application

Tinder

Application Category

- Social Networking

Event Details

Action

Allowed — Warn Page Displayed

Time

Feb 18, 2024 4:49 PM

Rule Name

Warn - Social Networking

Source

ciscosse

Rule Identity

ciscosse

Internal IP Address

198.18.133.252

External IP Address

64.100.12.5

Destination

https://facebook.com/

Hostname

facebook.com

Categories

Social Networking

Dispute Categorization

Resource/Application

Facebook

Application Category

Application Category

Social Networking

Content Type

text/html

File Action (Remote Browser Isolation)

Event Details

Action

Blocked — Public Application

Time

Feb 18, 2024 4:56 PM

Rule Name

Block Tinder

Source

Read Only (readonly@fagioli.local)

Security-Team

Rule Identity

Security-Team

Internal IP Address

-

External IP Address

172.31.33.1

Destination

http://tinder.com/

Hostname

tinder.com

Categories

Application Block, Dating

Dispute Categorization

Resource/Application

Tinder

Application Category

Social Networking