Configure Zero Trust Network Access with Trusted Network Detection

Contents

Introduction

This document describes the required steps to configure the ZTNA Trusted Network Detecttion.

Prerequisites

- Secure Client minimum version 5.1.10
- Supported Platform - Windows and MacOS
- Trusted Platform Module (TPM) for Windows
- Secure Enclave coprocessor for Apple Devices
- 'Trusted Servers' configured in any Trusted Network profile are implicitly excluded from ZTA interception. Those servers cannot also be accesses as ZTA private resources.
- TND configuration affect all enrolled clients in the org
- Admins can use the next steps to generate a 'Certificate Public Key Hash' for Trusted Servers
  - Download the trusted servers public cert
  - Run this shell command to generate the hash:

```
openssl x509 -in <public_cert.pem> -pubkey -noout | openssl pkey -pubin -outform DER | openssl dgst -sh
```

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Access
- Enroll Devices in Zero Trust Access using SAML or Cert Based Authentication.

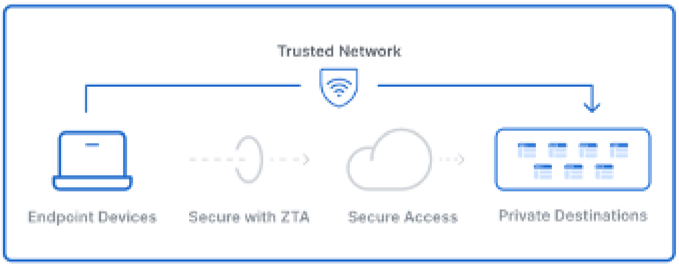
Components Used

- Secure Client Version 5.1.13
- TPM
- Secure Access Tenant
- Windows Device

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

- TND enables administrators to configure Secure Client to temporarily pause ZTA traffic steering and enforcement on Trusted Networks.
- Secure Client resume ZTA enforcement when the endpoint leaves the trusted network.
- This feature does not require any end-user interaction.
- ZTA TND configurations can be independently managed for private and internet ZTA destinations.



Key Benefits

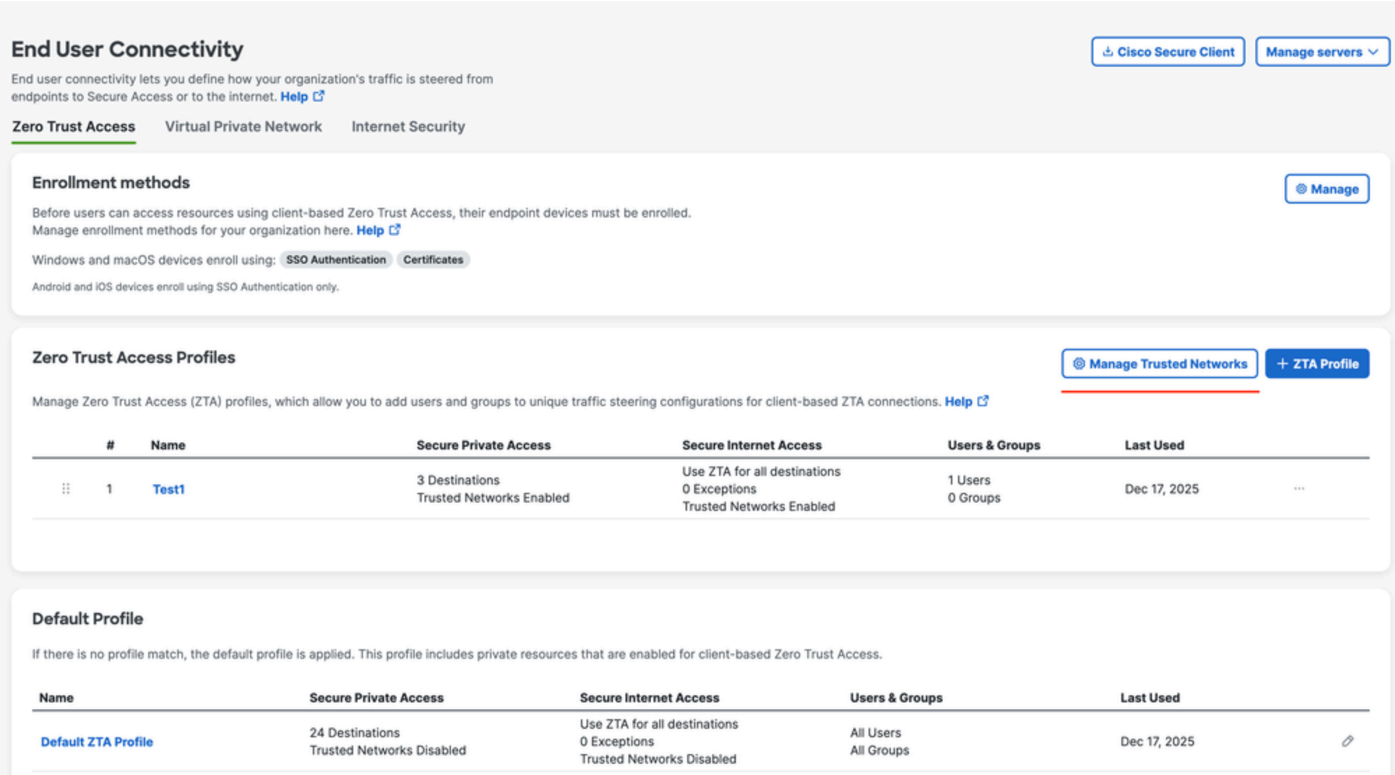
- Improved network performance and reduced latency provide a smoother user experience.
- Local security enforcement in the trusted network offers flexible and optimized resource utilization.
- End users can leverage the benefits without any prompts or actions.
- Independent control of TND for Private access and Internet access provide admin flexibility to handle different operational and security concerns

Configure

Step 1: Create Trusted Network Profile - DNS Server and Domain

Navigate to Secure Access Dashboard:

- Click on Connect > End User Connectivity > Manage Trusted Networks > +Add



End User Connectivity

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. Help

Enrollment methods

Before users can access resources using client-based Zero Trust Access, their endpoint devices must be enrolled. Manage enrollment methods for your organization here. Help

Windows and macOS devices enroll using: SSO Authentication Certificates

Android and iOS devices enroll using SSO Authentication only.

Zero Trust Access Profiles

Manage Zero Trust Access (ZTA) profiles, which allow you to add users and groups to unique traffic steering configurations for client-based ZTA connections. Help

#	Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
1	Test1	3 Destinations Trusted Networks Enabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Enabled	1 Users 0 Groups	Dec 17, 2025

Default Profile

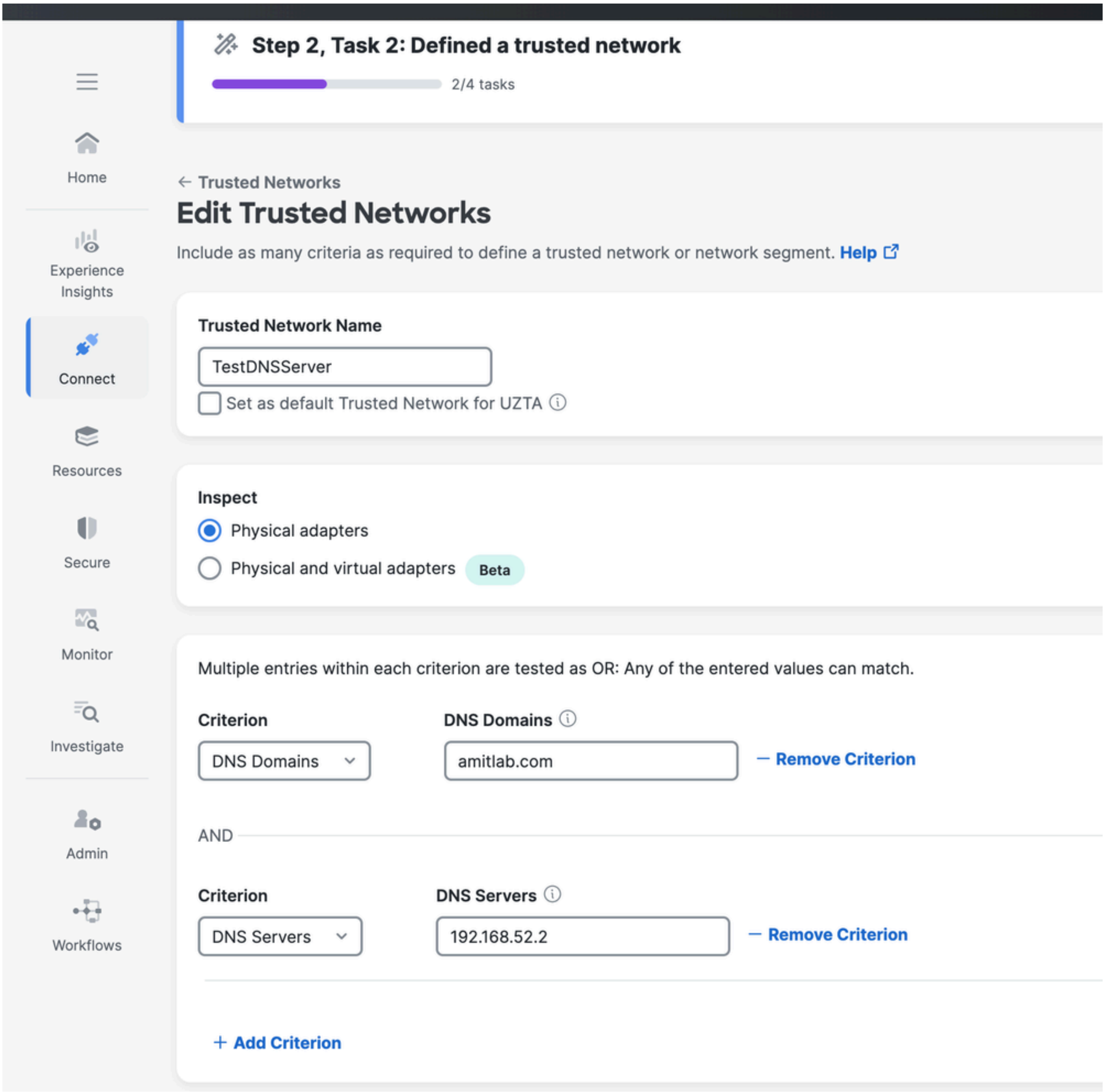
If there is no profile match, the default profile is applied. This profile includes private resources that are enabled for client-based Zero Trust Access.

Name	Secure Private Access	Secure Internet Access	Users & Groups	Last Used
Default ZTA Profile	24 Destinations Trusted Networks Disabled	Use ZTA for all destinations 0 Exceptions Trusted Networks Disabled	All Users All Groups	Dec 17, 2025

- Provide a name for the Trusted Network profile and configure at least one of the next criteria:
  - DNS Servers – Comma separated values of all DNS server addresses that a network interface must have when the client is in trusted network. Any entered server can be used to match this profile. For TND to match, any one of the DNS server address must match the local interface.
  - DNS Domains – Comma separated values of DNS suffixes that a network interface must have when the client is in trusted network.
  - Trusted Server- Add one or more servers on the network that present a TLS certificate with a hash that matches the hash you provide. To specify a port other than 443 append the port using standard notation. You can add up to 10 trusted servers, only one of which needs to pass validation.
    - Certificate Public Key Hash: Check step Prerequisites and System Limits to know how to generate the certificate hash.

Repeat the steps to add additional Trusted Network profiles.

Note: Multiple Options within the same Criteria is an OR operator. Different Criteria Defined is an AND operator.



Step 2, Task 2: Defined a trusted network

2/4 tasks

← Trusted Networks

Edit Trusted Networks

Include as many criteria as required to define a trusted network or network segment. Help

Trusted Network Name: TestDNSServer

□ Set as default Trusted Network for UZTA

Inspect

● Physical adapters

○ Physical and virtual adapters Beta

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

Criterion: DNS Domains — DNS Domains: amitlab.com — Remove Criterion

AND

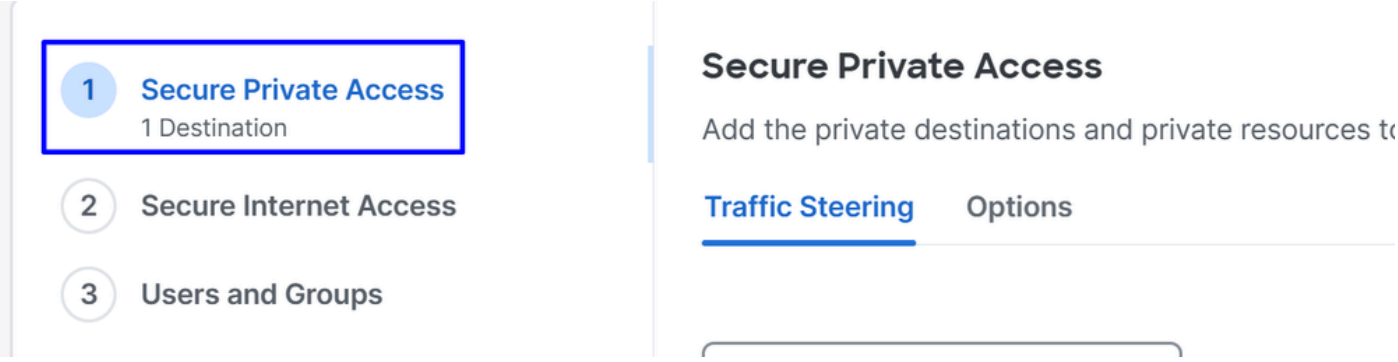
Criterion: DNS Servers — DNS Servers: 192.168.52.2 — Remove Criterion

+ Add Criterion

Step 2: Enable TND for Private or Internet access

- Navigate to Connect > End User Connectivity
- Edit ZTA Profile
- For eitherSecure Private Destinations or Secure Internet Access

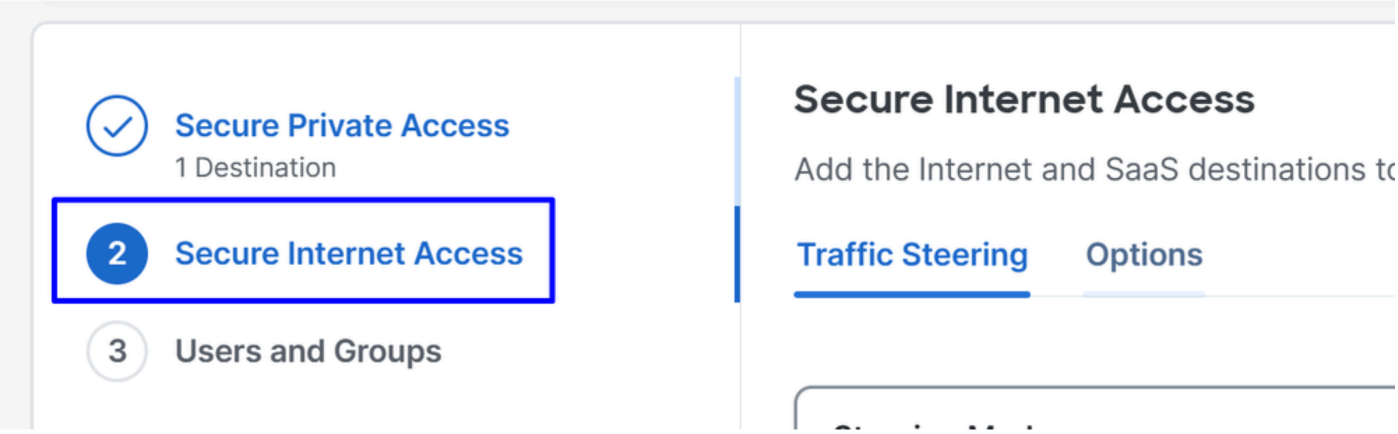
Secure Private Access



Secure Private Access

Add the private destinations and private resources t

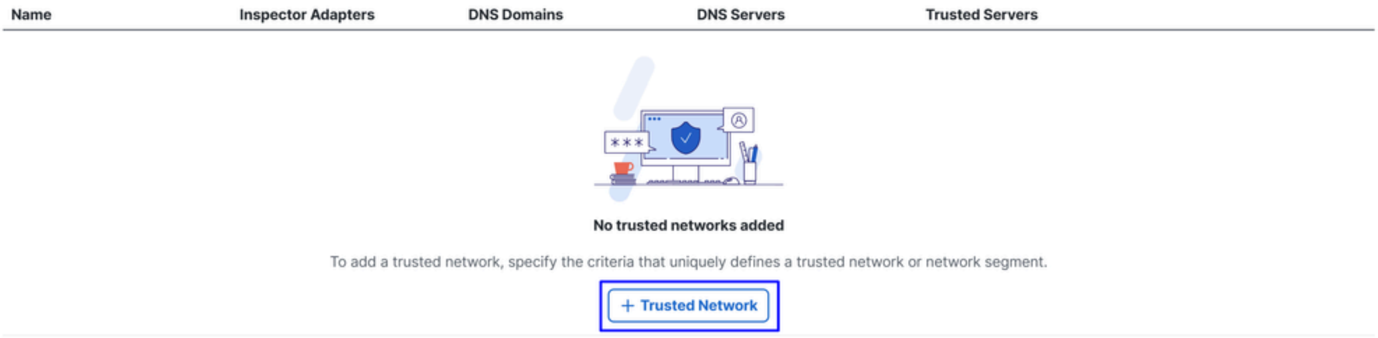
Secure Internet Access



Secure Internet Access

Add the Internet and SaaS destinations t

- Click on Options
  - Click on Use trusted networks to secure private destinations or Use trusted networks to secure internet destinationsdepends of the option choosen before
  - Click on + Trusted Network



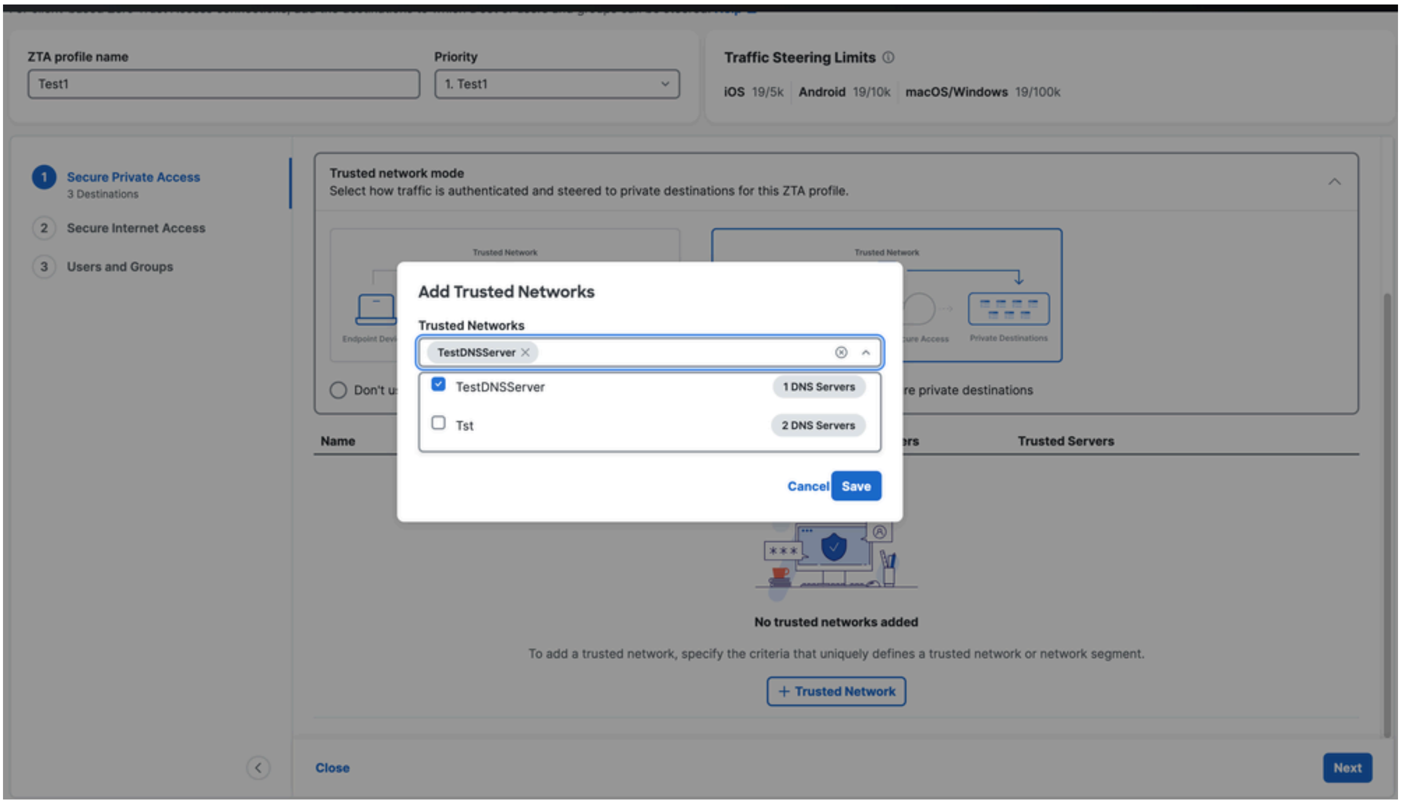
Name	Inspector Adapters	DNS Domains	DNS Servers	Trusted Servers

No trusted networks added

To add a trusted network, specify the criteria that uniquely defines a trusted network or network segment.

- Choose the Trusted Network profile(s) you have configured in the previous page and click Save

Secure Private Access



ZTA profile name: Test1

Priority: 1. Test1

Traffic Steering Limits

iOS 19/5k | Android 19/10k | macOS/Windows 19/100k

1 Secure Private Access
3 Destinations

2 Secure Internet Access

3 Users and Groups

Trusted network mode
Select how traffic is authenticated and steered to private destinations for this ZTA profile.

Add Trusted Networks

Trusted Networks: TestDNSServer ×

☑ TestDNSServer — 1 DNS Servers

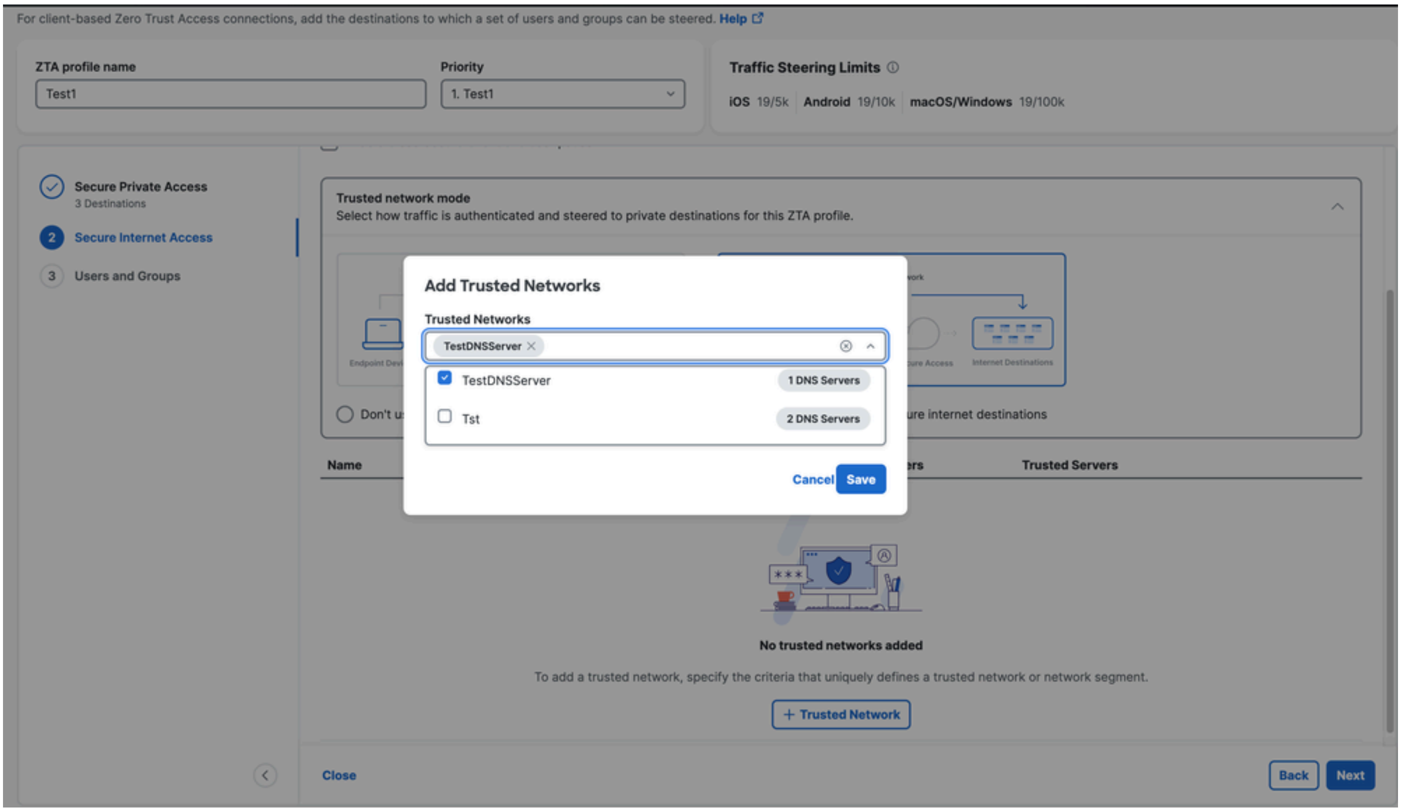
□ Tst — 2 DNS Servers

Cancel | Save

No trusted networks added

To add a trusted network, specify the criteria that uniquely defines a trusted network or network segment.

Secure Internet Access



For client-based Zero Trust Access connections, add the destinations to which a set of users and groups can be steered. Help

ZTA profile name: Test1

Priority: 1. Test1

Traffic Steering Limits

iOS 19/5k | Android 19/10k | macOS/Windows 19/100k

Secure Private Access
3 Destinations

2 Secure Internet Access

3 Users and Groups

Trusted network mode
Select how traffic is authenticated and steered to private destinations for this ZTA profile.

Add Trusted Networks

Trusted Networks: TestDNSServer ×

☑ TestDNSServer — 1 DNS Servers

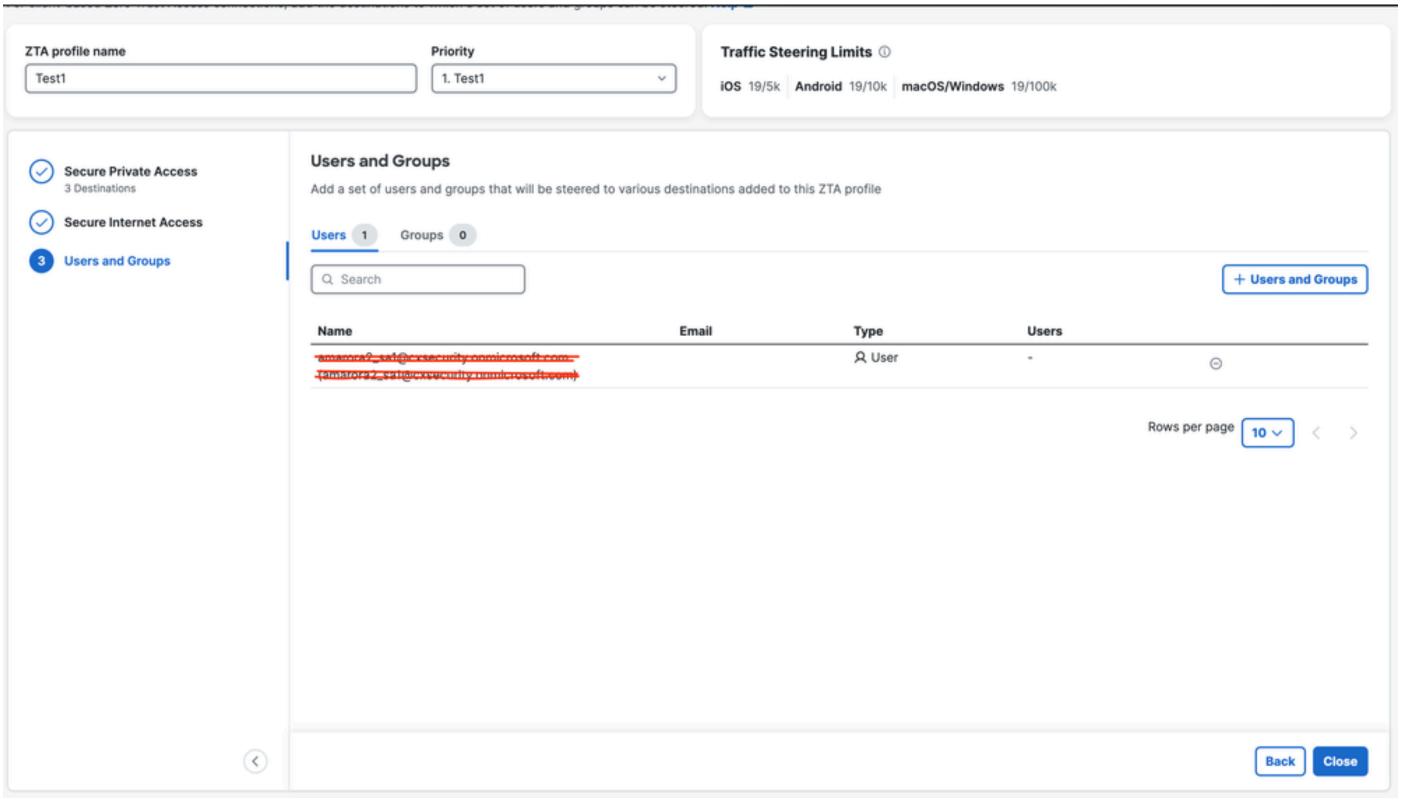
□ Tst — 2 DNS Servers

Cancel | Save

No trusted networks added

To add a trusted network, specify the criteria that uniquely defines a trusted network or network segment.

- Assign the Users/Groups to ZTA Profile and click Close.



ZTA profile name: Test1

Priority: 1. Test1

Traffic Steering Limits
iOS 19/5k | Android 19/10k | macOS/Windows 19/100k

Users and Groups

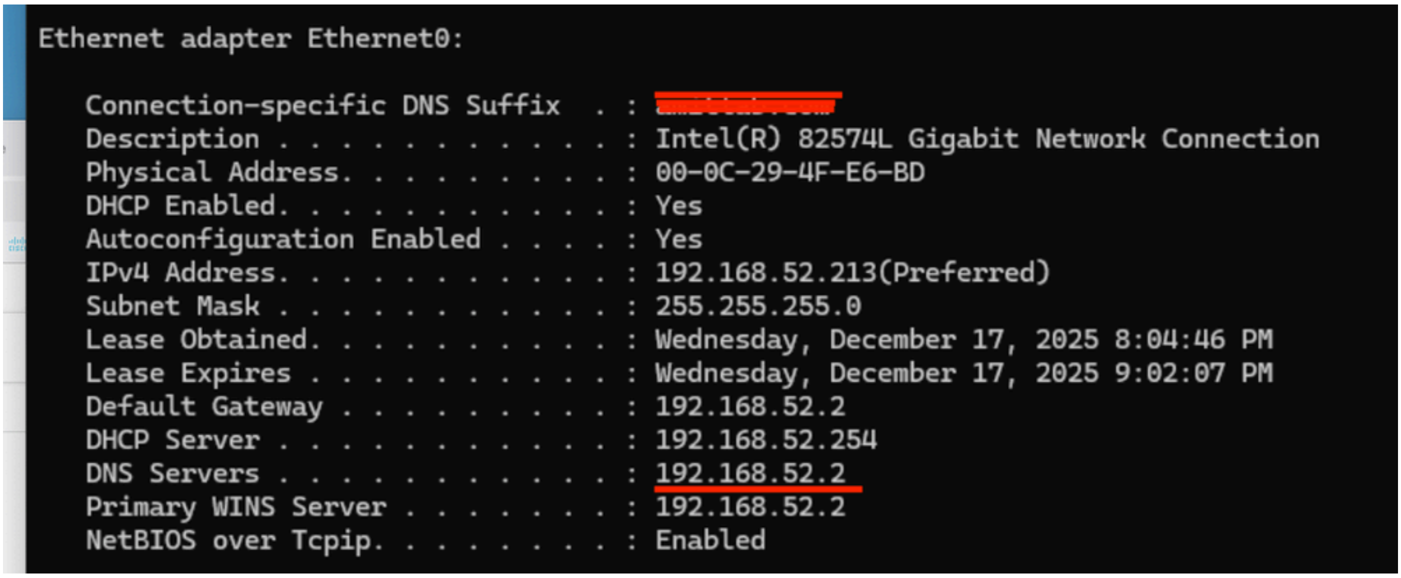
Add a set of users and groups that will be steered to various destinations added to this ZTA profile

Name	Email	Type	Users
[redacted]		User	-

Step 3: Client Side Configuration

1. Make sure you have right DNS Server defined under Ethernet Adaptor as we have chosen Physical Adaptor as a Criteria

2. Make sure you have Connection Specific DNS Suffix defined.



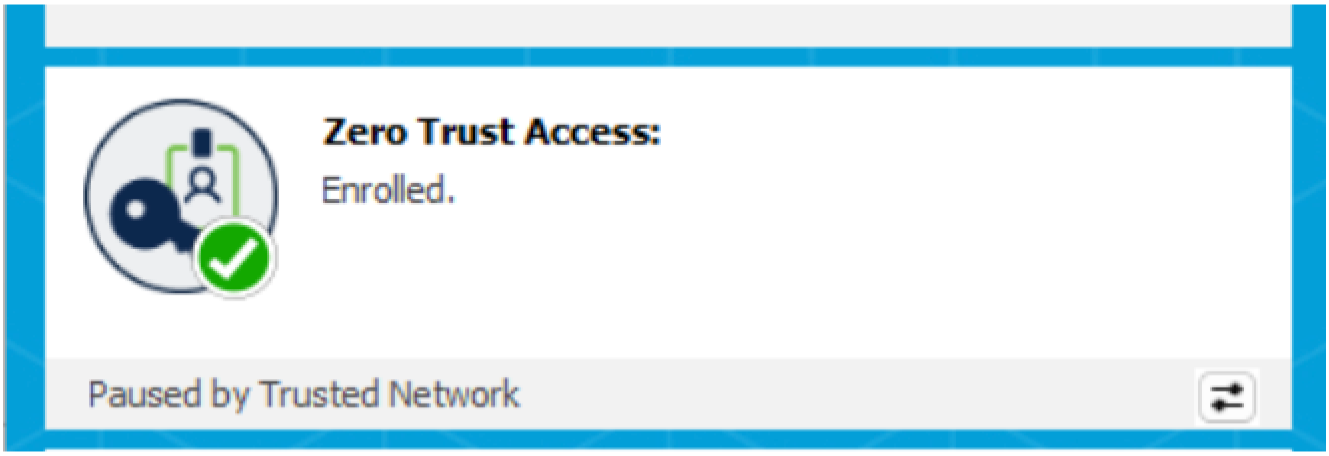
```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : [redacted]
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-4F-E6-BD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.52.213(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, December 17, 2025 8:04:46 PM
   Lease Expires . . . . . . . . . . : Wednesday, December 17, 2025 9:02:07 PM
   Default Gateway . . . . . . . . . : 192.168.52.2
   DHCP Server . . . . . . . . . . . : 192.168.52.254
   DNS Servers . . . . . . . . . . . : 192.168.52.2
   Primary WINS Server . . . . . . . : 192.168.52.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

With the next ZTA config sync to Secure Client in a few minutes, the ZTA module automatically pause when it detects it is on one of the configured Trusted Networks.

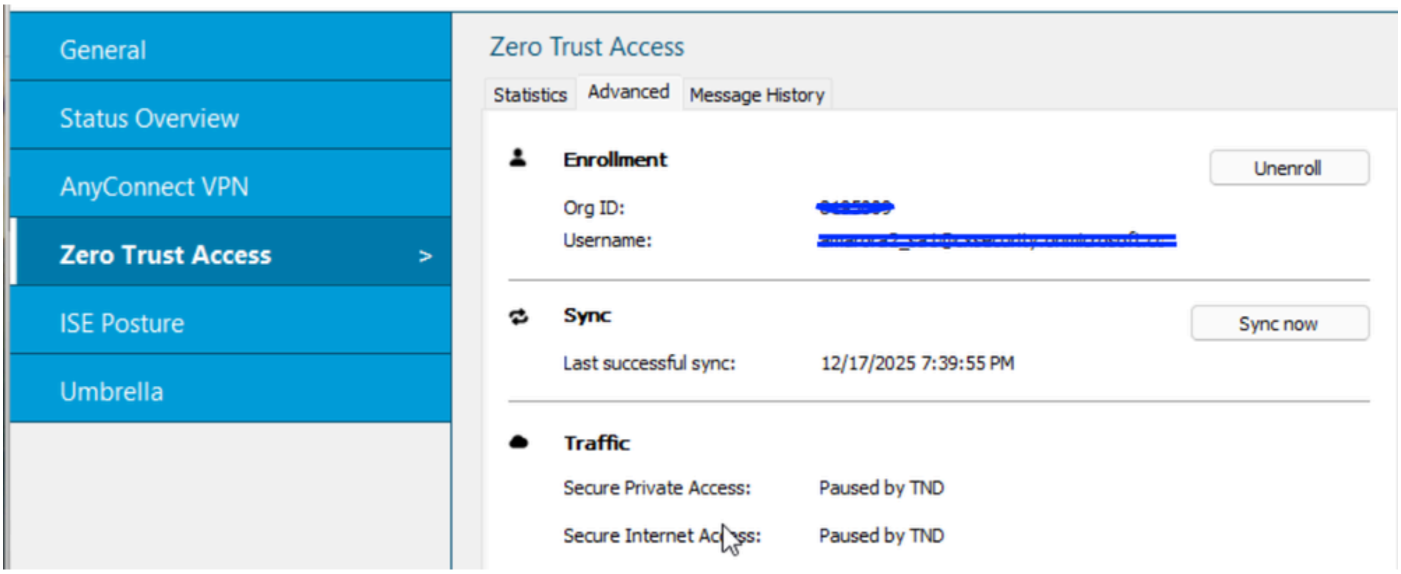
Verify

- **From Secure Client**


Zero Trust Access:

Enrolled.

Paused by Trusted Network



Zero Trust Access

Enrollment

Org ID: [redacted]

Username: [redacted]

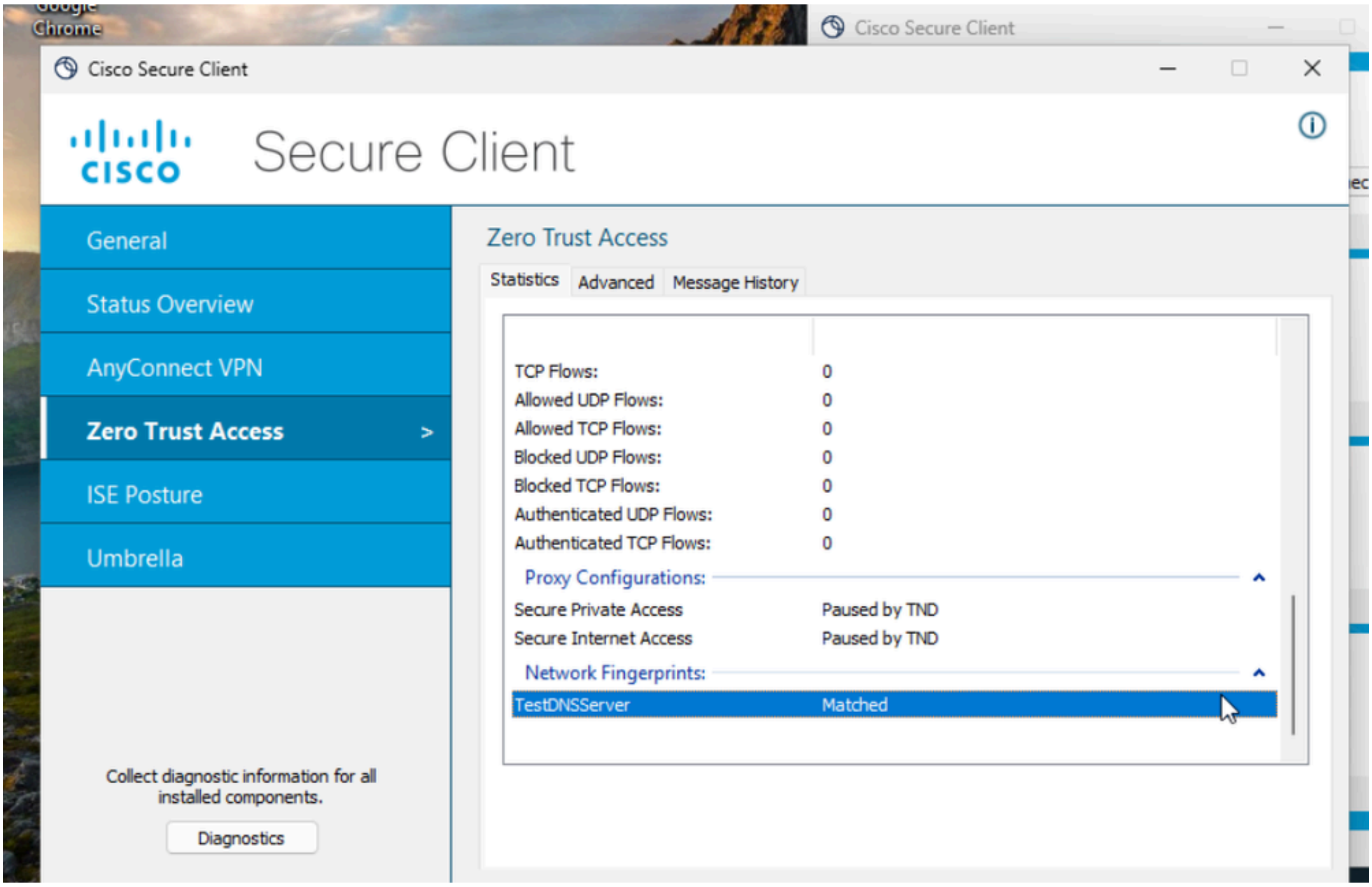
Sync

Last successful sync: 12/17/2025 7:39:55 PM

Traffic

Secure Private Access: Paused by TND

Secure Internet Access: Paused by TND



```
TCP Flows:                      0
Allowed UDP Flows:              0
Allowed TCP Flows:              0
Blocked UDP Flows:              0
Blocked TCP Flows:              0
Authenticated UDP Flows:        0
Authenticated TCP Flows:        0
Proxy Configurations:
Secure Private Access           Paused by TND
Secure Internet Access          Paused by TND
Network Fingerprints:
TestDNSServer                   Matched
```

- **From DART Bundle - ZTA Logs**

No TND rules configured.

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND will connect ProxyConfig 'default_spa_config' (no rules)

2025-12-17 17:53:40.711938 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:316 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND will connect ProxyConfig 'default_tia_config' (no rules)

Configured TND rule - DNS Server - Client Recieved Config

25-12-17 20:33:15.987956 csc_zta_agent[0x00000f80, 0x00000ed4] W/ CaptivePortalDetectionService.cpp:308 CaptivePortalDetectionService::getProbeUrl() no last network snapshot, using first probe url

2025-12-17 20:33:15.992042 csc_zta_agent[0x00000f80, 0x00000ed4] I/ NetworkChangeService.cpp:144 NetworkChangeService::**Start() Initial network snapshot:**
Ethernet0: subnets=192.168.52.213/24 dns_servers=192.168.52.2 dns_domain=amitlab.com dns_suffixes=amitlab.com isPhysical=true default_gateways=192.168.52.2
captivePortalState=Unknown

conditional_actions":[{"action":"disconnect" tells TND is configured in the ZTA Profile.

2025-12-17 17:55:36.430233 csc_zta_agent[0x00000c90/config_service, 0x0000343c] I/ ConfigSync.cpp:309 ConfigSync::HandleRequestComplete() **received new config:**

{"ztnaConfig":{"global_settings":{"exclude_local_lan":true},**"network_fingerprints":[{"id":"28f629ee-7618-44cd-852d-6ae1674e3cac","label":"TestDNSServer","match_dns_domains":["amitlab.com"],"match_dns_servers":**

["192.168.52.2"],"retry_interval":300}],"proxy_configs":[{**"conditional_actions":[{"action":"disconnect"**,"check_type":"on_network","match_network_fingerpr
7618-44cd-852d-6ae1674e3cac"]},{"action":"connect"}],"id":"default_spa_config","label":"Secure Private Access","match_resource_configs":["spa_steering_config"],"proxy_server":"spa_proxy_server"},{"conditional_actions":[{"action":"disconnect","check_type":"on_
44cd-852d-6ae1674e3cac"]},{"action":"connect"}],"id":

```
2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main, 0x0000343c] I/ NetworkFingerprintService.cpp:196
NetworkFingerprintService::handleStatusUpdate() broadcasting network fingerprint status: Fingerprint: 28f629ee-7618-44cd-852d-6ae1674e3cac
Interfaces: Ethernet0
```

TND Disconnect on a DNS Condition

```
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:378
ActiveSteeringPolicy::UpdateActiveProxyConfigs() updating active proxy configuration
```

```
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:287
ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND will disconnect ProxyConfig "Secure Internet Access" due to condition: on_network:
28f629ee-7618-44cd-852d-6ae1674e3cac action=Disconnect
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366
ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Private Access' is disconnecting due to: InactiveTnd
2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] I/ ActiveSteeringPolicy.cpp:366
ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Internet Access' is disconnecting due to: InactiveTnd
```

Match rule type DNS

```
2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main, 0x0000343c] I/ ZtnaTransportManager.cpp:1251
ZtnaTransportManager::closeObsoleteAppFlows() force closing app flow due to obsolete ProxyConfig enrollmentId=7b35249c-64e1-4f55-b12b-
58875a806969 proxyConfigId=default_tia_config TCP destination [safebrowsing.googleapis.com]:443 srcPort=61049
realDestIpAddr=172.253.122.95 process=<chrome.exe|PID 11904|user amit\amita> parentProcess=<chrome.exe|PID 5220|user amit\amita>
matchRuleType=DNS
```

Related Information

- Cisco Technical Support & Downloads
- Cisco Secure Access Help Center
- Cisco SASE Design Guide