

信頼ネットワーク検出を使用したゼロトラストネットワークアクセスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ1: 信頼できるネットワークプロファイルの作成 – DNSサーバとドメイン](#)

[ステップ2: プライベートアクセスまたはインターネットアクセスに対してTNDを有効にする](#)

[ステップ3: クライアント側の設定](#)

[確認](#)

[Secure Clientから](#)

[DART/バンドルから – ZTAログ](#)

[関連情報](#)

はじめに

このドキュメントでは、ZTNA Trusted Network Detection(TND)を設定するために必要な手順について説明します。

前提条件

- Secure Clientバージョン5.1.10以上
- サポートされるプラットフォーム：WindowsおよびMacOS
- Windows用トラステッドプラットフォームモジュール(TPM)
- Appleデバイス向けSecure Enclaveコプロセッサ
- 信頼されたネットワークプロファイルで設定された「信頼されたサーバ」は、ZTA代行受信から暗黙的に除外されます。これらのサーバは、ZTAプライベートリソースとしてアクセスすることもできません。
- TNDの設定は、組織に登録されているすべてのクライアントに影響します
- 管理者は次の手順を使用して、信頼できるサーバーの'証明書の公開キーハッシュ'を生成できます
 - 信頼済みサーバーの公開証明書をダウンロードします
 - 次のシェルコマンドを実行して、ハッシュを生成します。

```
openssl x509 -in
```

```
-pubkey -noout | openssl pkey -pubin -outform DER | openssl dgst -sha256
```

要件

次の項目に関する知識があることが推奨されます。

- シスコセキュアアクセス
- SAMLまたは証明書ベースの認証を使用して、ゼロトラストアクセスでデバイスを登録します。

使用するコンポーネント

- Secure Clientバージョン5.1.13
- TPM
- セキュアアクセステナント
- Windowsデバイス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

- TNDを使用すると、管理者は、信頼できるネットワークでZTAトラフィックのステアリングと適用を一時的に一時停止するようにセキュアクライアントを設定できます。
- セキュアクライアントは、エンドポイントが信頼ネットワークから離れるときにZTAの適用を再開します。
- この機能では、エンドユーザの操作は必要ありません。
- ZTA TND設定は、プライベートおよびインターネットのZTA宛先に対して個別に管理できます。



主な利点

- ネットワークパフォーマンスの向上と遅延の低減により、よりスムーズなユーザエクスペリエンスが実現します。
- 信頼できるネットワークでローカルのセキュリティを適用することにより、柔軟で最適化されたリソースの使用が可能になります。
- エンドユーザは、プロンプトや操作を行わずに利点を活用できます。
- プライベートアクセスとインターネットアクセスのTNDを独立して制御することで、運用上およびセキュリティ上のさまざまな問題に対処できる柔軟性が管理者に提供されます。

設定

ステップ1：信頼できるネットワークプロファイルの作成 – DNSサーバとドメイン

[Secure Access Dashboard](#)に移動します。

- Connect > End User Connectivity > Manage Trusted Networks > +Addの順にクリックします。

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](#)

Zero Trust Access Virtual Private Network Internet Security

Enrollment methods [Manage](#)

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 Trusted Networks](#) [+ ZTA Profile](#)

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

- 信頼されたネットワークプロファイルの名前を指定し、次の条件のうち少なくとも1つを設定します。
 - DNS Servers：クライアントが信頼ネットワーク内に存在する場合にネットワークインターフェイスに割り当てる必要があるすべてのDNSサーバアドレスのカンマ区切り値。入力した任意のサーバをこのプロファイルの照合に使用できます。TNDが一致するためには、DNSサーバアドレスのいずれかがローカルインターフェイスと一致している必要があります。
 - DNSドメイン：クライアントが信頼ネットワーク内にあるときにネットワークインターフェイスに必要なDNSサフィックスのコンマ区切り値。
 - 信頼できるサーバ

：指定したハッシュと一致するハッシュを持つTLS証明書を提示する1つ以上のサーバをネットワークに追加します。443以外のポートを指定するには、標準の表記を使用してポートを追加します。最大10台の信頼されたサーバを追加できますが、そのうち1台のみが検証に合格する必要があります。

- Certificate Public Key Hash：証明書ハッシュの生成方法については、「[前提条件とシステム制限](#)」のステップを確認してください。

この手順を繰り返して、追加の信頼できるネットワークプロファイルを追加します。



注：同じ条件内の複数のオプションはOR演算子です。定義されている別の基準は、AND演算子です。

Home

Experience Insights

Connect

Resources

Secure

Monitor

Investigate

Admin

Workflows

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

amitlab.com

Remove Criterion

AND

Criterion

DNS Servers

192.168.52.2

Remove Criterion

Add Criterion

ステップ2：プライベートアクセスまたはインターネットアクセスに対してTNDを有効にする

- Connect > End User Connectivityの順に選択します。
- ZTAプロファイルの編集
- セキュアなプライベート接続先またはセキュアなインターネットアクセス用

セキュアプライベートアクセス

1 Secure Private Access

1 Destination

2 Secure Internet Access

3 Users and Groups

Secure Private Access

Add the private destinations and private resources to

Traffic Steering Options

セキュアなインターネットアクセス



Secure Private Access

1 Destination

2

Secure Internet Access

3

Users and Groups


Secure Internet Access

Add the Internet and SaaS destinations to

Traffic Steering Options

- Optionsをクリックします。
 - Use trusted networks to secure private destinationsまたはUse trusted networks to secure internet destinationsをクリックします。
 - + Trusted Networkをクリックします。

Name	Inspector Adapters	DNS Domains	DNS Servers	Trusted Servers
------	--------------------	-------------	-------------	-----------------



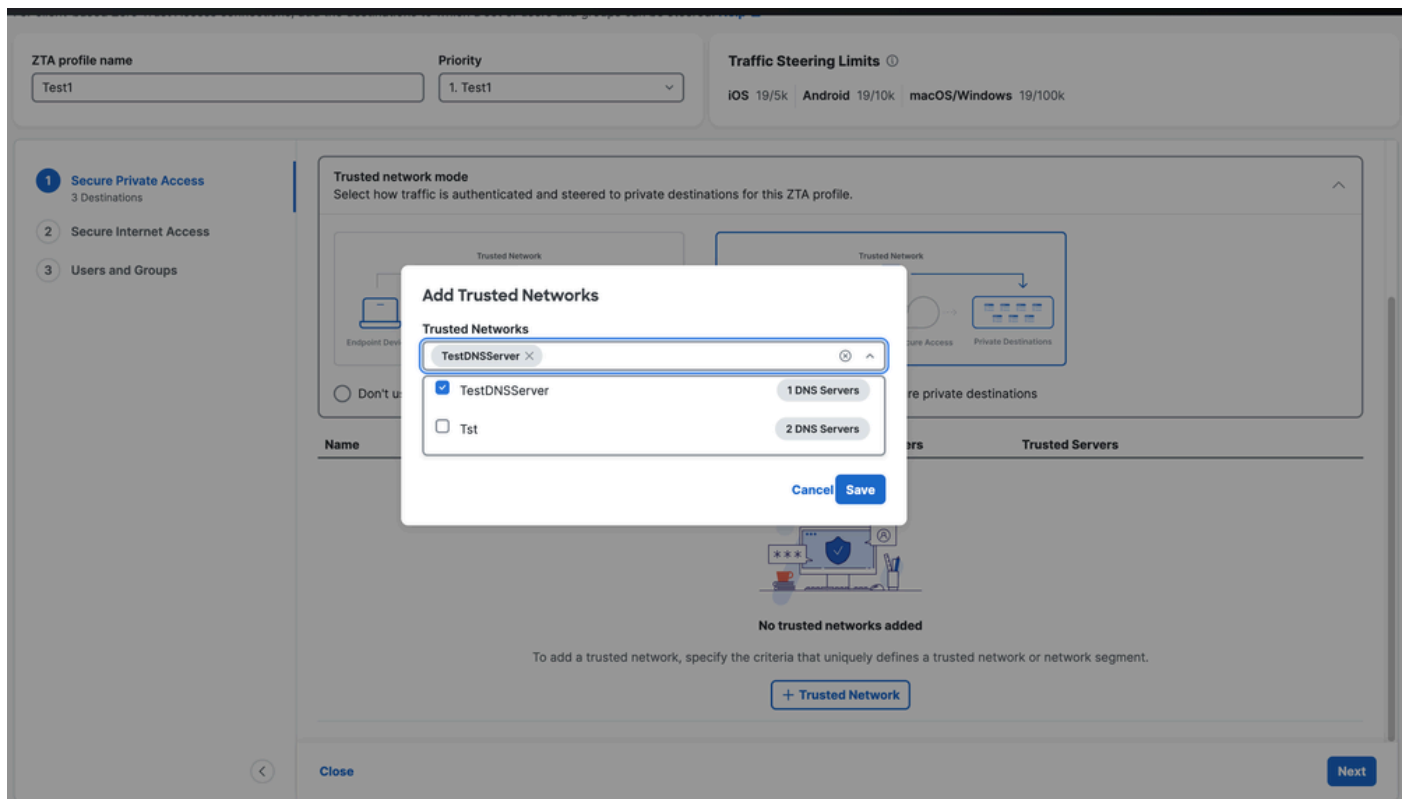
No trusted networks added

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

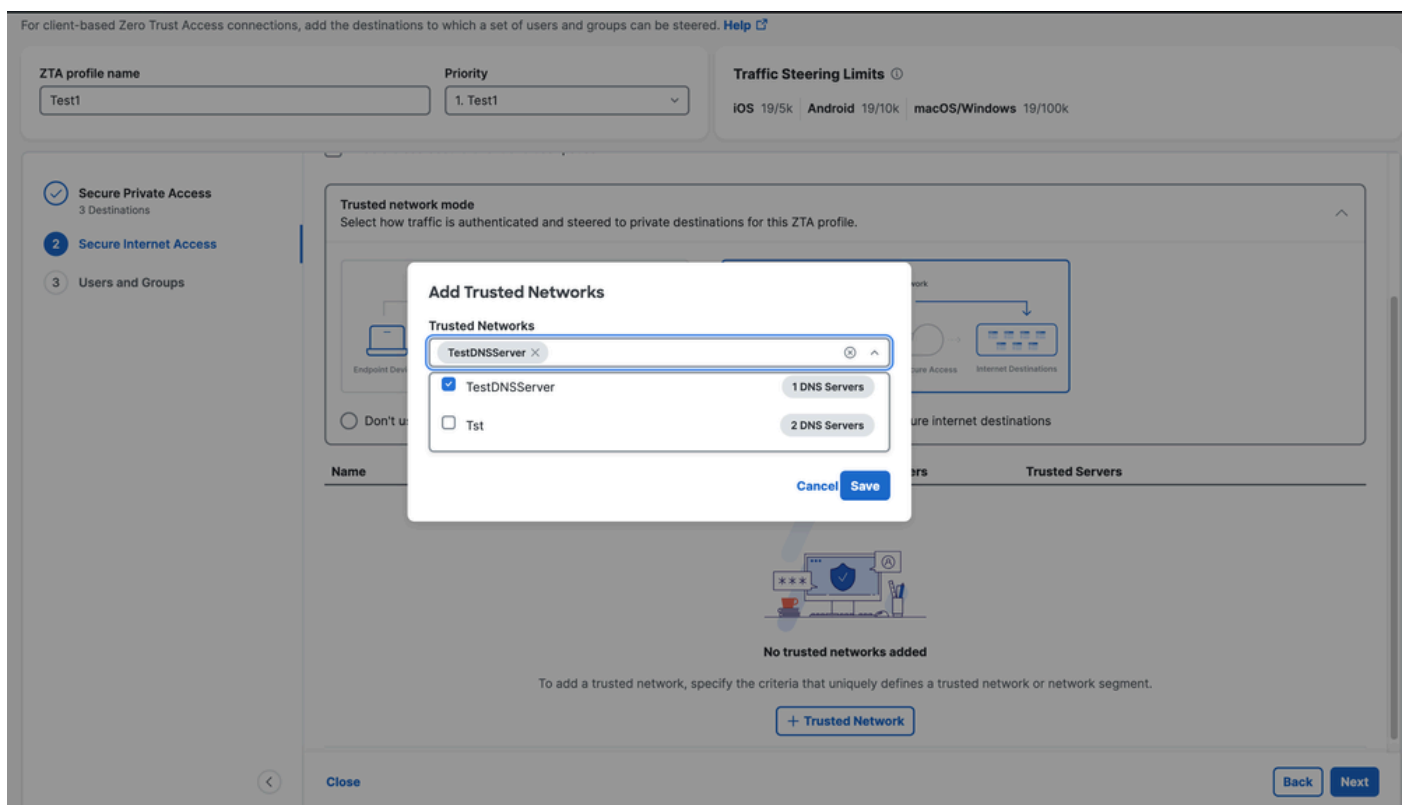
[+ Trusted Network](#)

- 前のページで設定したTrusted Networkプロファイルを選択し、Saveをクリックします。

セキュアプライベートアクセス



セキュアなインターネットアクセス



- ZTAプロファイルにユーザ/グループを割り当て、Closeをクリックします。

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
Secure Internet Access
Users and Groups

Users and Groups

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

Users 1
Groups 0

+ Users and Groups

Name	Email	Type	Users
amara2_sat@cssecurity.comicosoft.com		User	-
amara2_sat@cssecurity.comicosoft.com			

Rows per page 10

Back Close

ステップ3：クライアント側の設定

- 条件として物理アダプタを選択したので、イーサネットアダプタで正しいDNSサーバが定義されていることを確認します
- 接続固有のDNSサフィックスが定義されていることを確認します。

```

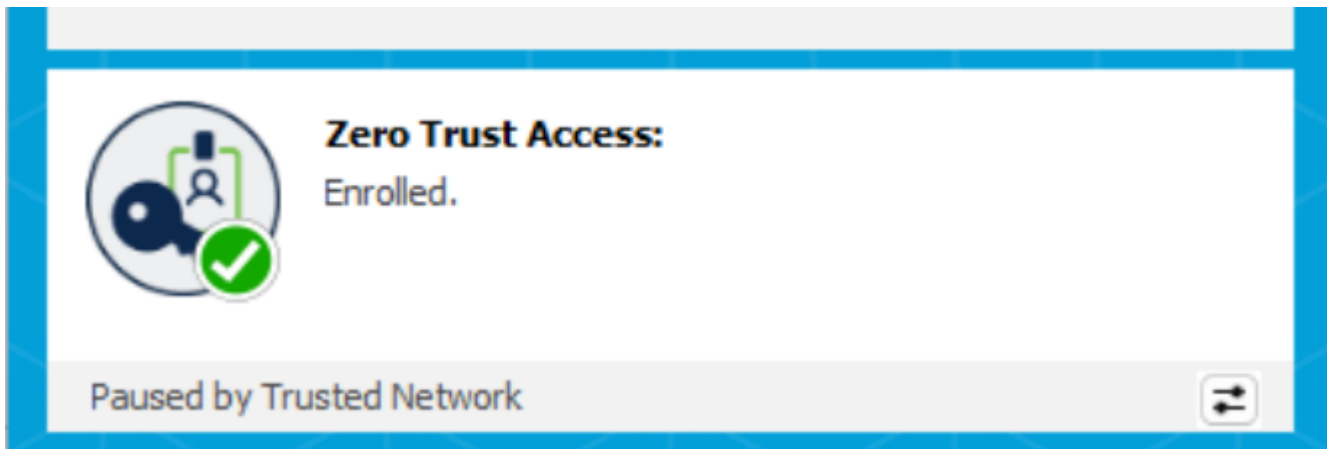
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix  . : 
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
  
```

次のZTA設定のセキュアクライアントへの同期が数分以内に完了すると、ZTAモジュールは、設定された信頼ネットワークの1つにあったことを検出すると、自動的に一時停止します。

確認

- Secure Clientから



General

Status Overview

AnyConnect VPN

Zero Trust Access

ISE Posture

Umbrella

Zero Trust Access

Statistics

Advanced

Message History

Enrollment

Unenroll

Org ID:

Username:

Sync

Sync now

Last successful sync:

12/17/2025 7:39:55 PM

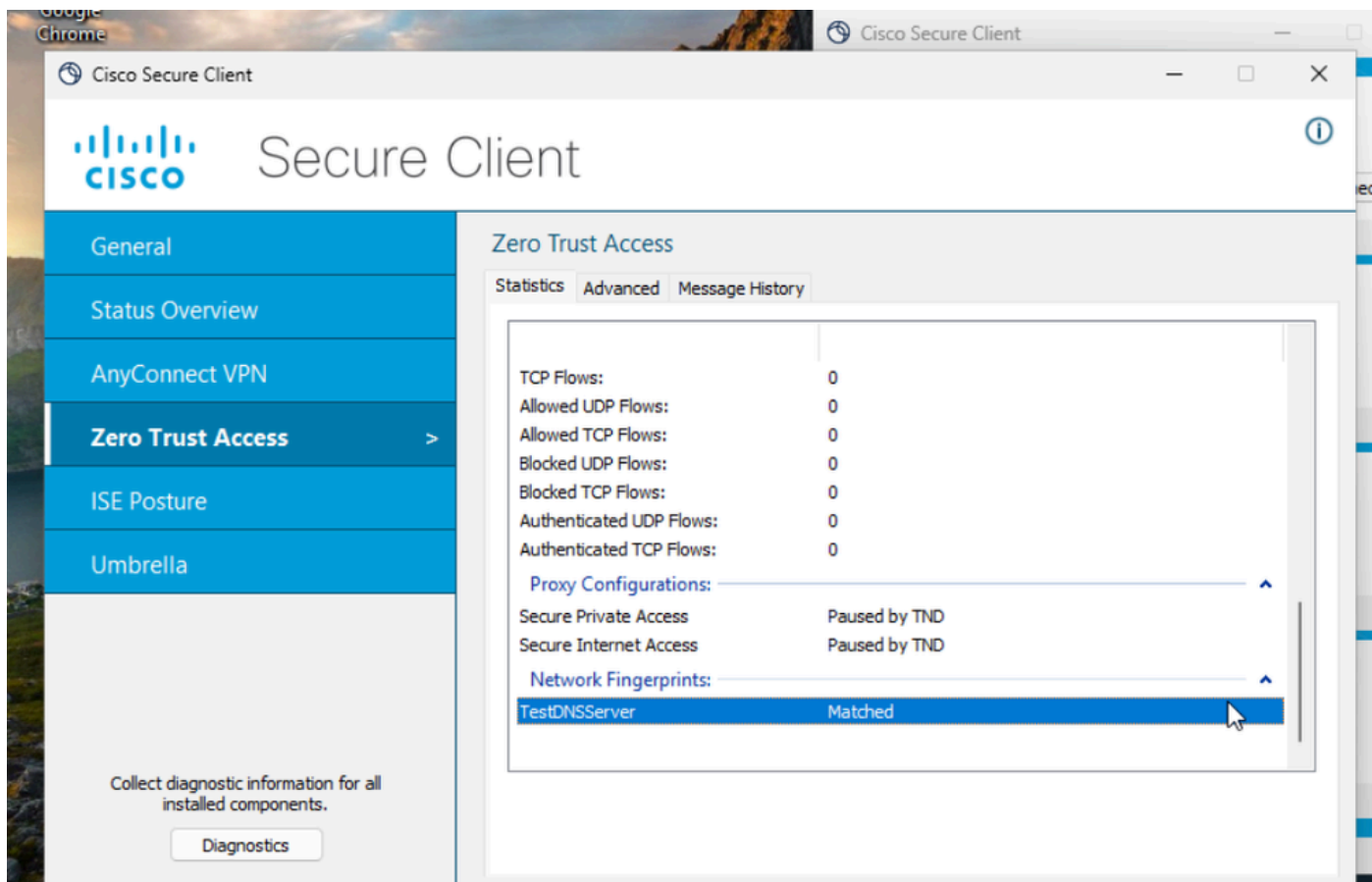
Traffic

Secure Private Access:

Secure Internet Access:

Paused by TND

Paused by TND



・ DARTバンドルから : ZTAログ

TNDルールが設定されていません。

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

設定済みTNDルール - DNSサーバークライアントが受信した設定

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] // NetworkChangeService.cpp:144 NetworkChangeService::Start()初期ネットワークスナップショット:

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=不明

conditional_actions":[{"action":"disconnect"}]は、TNDがZTAプロファイルで設定されていることを示します。

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

```
{"ztnaConfig":{"global_settings":{"exclude_local_ip":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_fingerprint":"28f629ee-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_network","match_network_fingerprints":["28f629ee-7618-44cd-852d-6ae1674e3cac"]],{"action":"connect"},"id":

2025-12-17 17:55:36.472435 csc_zta_agent[0x000039a8/main, 0x0000343c] // NetworkFingerprintService.cpp:196 NetworkFingerprintService::handleStatusUpdate()ブロードキャストネットワークのフィンガープリントの状態 : Fingerprint: 28f629ee-7618-44cd-852d-6ae1674e3cac インターフェイス : Ethernet0

DNS状態でのTND切断

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:378 ActiveSteeringPolicy::UpdateActiveProxyConfigs() アクティブプロキシ設定の更新

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // ActiveSteeringPolicy.cpp:287 ActiveSteeringPolicy::collectProxyConfigPauseReasons() TND will disconnect ProxyConfig "Secure Internet Access" due to condition: on_network: 28f629ee-7618-44cd-852d-6ae1674e3cac action=接続解除

2025-12-17 17:55:36.729130 csc_zta_agent[0x0000206c/config_enforcer, 0x0000343c] // 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] // ActiveSteeringPolicy.cpp:366 ActiveSteeringPolicy::updateProxyConfigStatus() ProxyConfig 'Secure Internet Access' is disconnecting due to: InactiveTnd
一致ルールタイプDNS

2025-12-17 17:55:36.731286 csc_zta_agent[0x000039a8/main, 0x0000343c] // ZtnaTransportManager.cpp:1251 ZtnaTransportManager::closeObsoleteAppFlows()により、古いProxyConfigEnrollmentId=7b35249c-64e1-4f55-b12b-5887512 806969 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

関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [Cisco Secure Accessヘルプセンター](#)
- [Cisco SASE設計ガイド](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。