Zero Trust Access Module

- Zero Trust Access, on page 1
- Getting Zero Trust Access Up and Running on Desktop, on page 2
- Zero Trust Access on Android Devices, on page 3
- Zero Trust Access on iOS Devices, on page 4
- Starting Resource Access, on page 4
- How Do I Unenroll on Desktop, on page 4
- How Do I Uninstall on Desktop, on page 4
- Configuring Zero Trust Access on Desktop, on page 4
- Use Certificate Enrollment Without User Action, on page 5
- Operation Details for Desktop Zero Trust Access Module, on page 6
- Troubleshooting Zero Trust Access Module on Desktop, on page 6
- Troubleshooting Zero Trust Access App for Android, on page 7
- Troubleshooting Zero Trust Access App for iOS, on page 7

Zero Trust Access

Zero Trust Access Module is enabled and running when you see "Enrolled in Zero Trust Access" in the Cisco Secure Client Tile. This access is about knowing, understanding, and controlling who and what is on your network. By definitively knowing who a user is, the appropriate level of access is granted based on the person's role or function, and what network rights those roles are entitled to. Beyond AnyConnect VPN, it offers more granular control and a secure user experience for a complete network. While VPN trusts anyone or anything that passes network control, the Zero Trust Access approach is to not trust any user or device with access until proven. No one is automatically trusted; and once verified, only limited access is given and re-verified. It extends the zero-trust model beyond the network and reduces the attack surface by hiding applications from the internet.

Currently, the Zero Trust Access Module only supports the Cisco Secure Access service. Refer to Secure Access documentation for additional details. It covers configuring private resources to allow zero-trust connections, setting up access rules to determine who can access the resource using those connections, traffic steering, and so on.

Getting Zero Trust Access Up and Running on Desktop

To install using predeploy, download **cisco-secure-client-win-*version*-zta-k9.msi** for Windows. For macOS predeploy, download **cisco-secure-client-macos-*version*-predeploy-k9.dmg**, and the Zero Trust Module will be part of its optional components.

To install using webdeploy, download **cisco-secure-client-win-*version*-webdeploy-k9.pkg** for Windows. The module name for ASA configuration is zta.

Duo Desktop will also be packaged and installed automatically in the Zero Trust Access module installer (for Windows and macOS), even though it is a standalone application that is separate from Cisco Secure Client. However, on macOS, Duo Desktop requires additional setup requirements when deploying Zero Trust Access through MDM on macOS 11 (and later). Refer to the Guide to Duo Device Health App certificate deployment for macOS 11+ users for these additional Duo setup requirements. Refer to Duo Desktop documentation for any other Duo details.

Once the software is installed, enrollment is the user being prompted to sign into the service using the Zero Trust Access Module to obtain client certificates and necessary service URLs. Cisco Secure Access enrollment involves the user authentication portion, and these enrollments persist across reboots. The enrollments are stored in a global/machine context but are tied to a local user and applied on a per-local user basis.

Before you begin

- Due to a new macOS requirement, one-time administrator privileges are necessary when performing a fresh install of 5.1.x (or later), or upgrade from 5.0.x (or earlier). Further updates do not need them. You can circumvent this limitation by managing macOS devices via MDM and pre-approving the application. Refer to Managed Login Items for additional information. The ZTA module requires user approval before it can function.
- The Zero Trust Access Module is supported on Windows 10 and 11 (TPM-enabled devices) and macOS 11, 12, 13, and 14 (TPM-enabled devices).
- Windows devices must be running on systems that include Trusted Platform Module version 2.0. macOS devices must be running on systems that include a Secure Enclave such as MacBook Pro computers with Touch Bar (016 and 2017) that contain the Apple T1 chip, Intel-based Mac computers that contain the Apple T2 Security chip, or Mac computers with Apple silicon.
- You must have Windows WebView2 installed if you are going to use the Zero Trust Access Module, and you must deploy it out of band.
- If you are predeploying Zero Trust Access on macOS 11 or greater, refer to Additional Duo Desktop Requirements on macOS 11 (and later) for additional requirements.
- You must have versions of AnyConnect VPN and Zero Trust Access that align for proper functioning: AnyConnect VPN requires 5.1.1.38 and Zero Trust Access requires 5.1.1.4867.
- For best performance, you should use dynamic split exclude tunneling to exclude traffic targeting zpc.sse.cisco.com from the tunnel. Refer to Configure Dynamic Split Exclude Tunneling for configuration steps. If resolution of that domain over the tunnel does not produce an IP address with optimal geographic location, you should also configure split DNS for split exclude so that its name resolution is only attempted outside the tunnel. Refer to Split DNS for split exclude tunneling configurations.

Current Limitations or Restrictions:

- No DART collection of Duo Desktop logs on macOS.
- No support for tunneling applications where server sends traffic first (ex:: MySQL).
- Zero Trust Access functionality is disabled when multiple users are logged in concurrently to an endpoint.
- ZTA webdeploy is not supported on macOS.
- Any client TCP or UDP applications that do not rely on ICMP or DNS SRV discovery are supported, with the following restrictions:
  - All TCP connection or UDP flows must be initiated by the client application.
  - Any protocol requiring a unique client IP address at the server, like SMBv1, is not supported. (SMBv3 works as expected.)

Procedure

Step 1 To begin using Zero Trust Access, registration is required. Click **Enroll** in the Zero Trust Access tile of the Cisco Secure Client.

Step 2 Enter your work email address.

Step 3 If the desired organization is auto selected in the SSO/SAML login, enter the email address and password for authentication. If you belong to more than one organization, choose the appropriate one from the drop-down menu.
The Zero Trust Access tile displays when the authentication process is complete or if it is continuing enrollment. The Zero Trust Access module installs to a common Cisco Secure Client folder:

- Windows: C:\Program Files (x86)\Cisco\Cisco Secure Client\ZTA
- macOS: /opt/cisco/secureclient/zta

Note
For the highest security during enrollment, we strongly advise that you take advantage of your established MFA-based authentication and the use of biometric identity for user authentication.

What to do next

Refer to Troubleshooting Zero Trust Access Module on Desktop, on page 6 for DART log file locations.

Refer to How Do I Unenroll on Desktop, on page 4 or How Do I Uninstall on Desktop, on page 4 for those procedures.

Refer to Operation Details for Desktop Zero Trust Access Module, on page 6 for interoperability requirements and expected flow.

Zero Trust Access on Android Devices

Zero Trust Access is available as a new application, downloaded separately from Cisco Secure Client, on the Google Play Store. You must have a device running Android 14 with Samsung Knox 3.10 (or later). The Samsung Knox Service Plugin (KSP) is also available on the Google Play Store and is required when

configuring an MDM vendor (such as Ivanti MobileIron) for device enrollment with Zero Trust Access. Refer to Set up the Zero Trust Access App for Android on Samsung Devices for the first time use, enrollment, and troubleshooting procedures.

Zero Trust Access on iOS Devices

Zero Trust Access is available as a new application, downloaded separately from Cisco Secure Client, on the Apple Play Store. You must have a device running iOS/iPadOS 17.2 (or later). Refer to Set up the Zero Trust Access App for iOS Devices for the first time use, enrollment, and troubleshooting procedures.

Starting Resource Access

When enrollment is complete, the Zero Trust Access tile shows that it is active. You can then begin accessing the internal applications that the administrator defined as available based on access rules. Any issues with resource access appears in the Zero Trust Access Module tile. You can click **Details** for additional information about what is affecting the secure resource access.

How Do I Unenroll on Desktop

If you want to unregister from Zero Trust Access service, click the **Advanced** tab in the Zero Trust Access Module and then click **Unenroll**. It unregisters your account, deletes client certificates, and removes any associated configuration from your service.

How Do I Uninstall on Desktop

In macOS, use the UI installer or command line to uninstall AnyConnect VPN or just the Zero Trust Access Module. In Windows, use the Add/Remote Program to uninstall AnyConnect VPN or just the Zero Trust Access Module. Uninstalling Zero Trust Access will not uninstall Duo Desktop.

Configuring Zero Trust Access on Desktop

After enrollment, Zero Trust Access Module does a configuration sync to get the initial json configuration in the appropriate folder. After that, it periodically checks to ensure that the latest json file is in the folder. What is returned from the check determines if Zero Trust Access requires no configuration change or if it needs to download a new configuration. On demand, you can also choose the **Configuration** tab in the Zero Trust Access Module and click **Sync Now** to pull the most recent json file from the SSE dashboard. The date of the last configuration sync is displayed.

All additional configuration is done with Cisco Secure Access in the cloud.

Use Certificate Enrollment Without User Action

Enrollment with user certificates involves enrolling Windows and macOS devices in Zero Trust Access without requiring any action or awareness from the users. User endpoint devices present an identity certificate when enrolling and renewing enrollment. On macOS, the certificate used for zero touch must be accessible by our app. When the certificate is pushed by MDM, click **Allow all app access** on the MDM config portal to enable accessing the private key without being prompted during auto enrollment. If the certificate is manually imported, the following command line steps are required to avoid the OS prompts when accessing the private key:

Before you begin

Each individual user is expected to have a client certificate capable of enrolling. We don't currently offer different choice files for different users on the same device.

Procedure

Step 1 Import the client certificate:

security import "PATH_TO_CLIENT_CERT" -k ~/Library/Keychains/login.keychain-db -x -A

Step 2 Set the correct partition list:

security set-key-partition list -S teamid:DE8Y96K9QP -l "PRIVATE_KEY_LABEL" -t private

What to do next

When choosing the client certificate from the endpoint, consider these details:

- include either a UPN (Principal Name) or an RFC822 name. UPN takes precedence over RFC822 if both are present.
- the UPN or RFC822 value should map to a user identity that is imported into SSE.
- MDM-ID is an optional value that you can use for posture correlation. Below are examples of MDM ID syntax:
  - Intune: *URL=ID:Microsoft Endpoint Manager:GUID:{{DeviceID}}*
  - JAMF: *cert ID:JAMF:GUID:$MANAGEMENTID*
  - Ivanti/MobileIron: *ID:Mobileiron:GUID:${deviceGUID}*

Refer to Integrate MDM and UEM Servers with Cisco ISE - Integrate Microsoft Endpoint Manager Intune [Cisco Identity Services Engine] or Integrate MDM and UEM Servers with Cisco ISE - Integrate Ivanti (previously MobileIron) UEM [Cisco Identity Services Engine] for ISE documentation on MDM-IDs in certificates. The Secure Access Help has further details about auto enrollment and configuring.

Operation Details for Desktop Zero Trust Access Module

Domains to Exclude

For proper interoperability with VPN and Umbrella SWG, you should exclude the following domains (and underlying subdomains/hosts) from VPN tunneling and SWG proxying:

- ztna.sse.cisco.com (Registration)
- acme.sse.cisco.com (Certificates)
- devices.api.umbrella.com (Config Sync)
- zpc.sse.cisco.com (Proxying)
- sseposture-routing-commercial.k8s.5c10.org (Posture)
- sseposture-routing-commercial.posture.duosecurity.com (Posture)

Paths Where Config Files Are Saved

Configuration files are stored in a a global directory but are tracked on a per local user basis. The local enrollment files are saved in the following locations:

Windows— C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments

macOS— /opt/cisco/secureclient/zta/enrollments

The cached configuration files can be found here:

Windows—C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollments\cached_configs

macOS—/opt/cisco/secureclient/zta/enrollments/cached_configs

Interoperability With Other Secure Client Modules

Any traffic intercepted by Zero Trust Access won't be available for Umbrella proxying or VPN tunneling. The first traffic to get intercepted is Zero Trust Access, followed by Umbrella DNS/SWG, and then VPN. Likewise, Network Visibility Module reporting won't report individual network flows that have been intercepted by Zero Trust Access. It will only report on network traffic to the Zero Trust Access proxy, containing encrypted application flows intercepted by Zero Trust Access.

Certificate Details

Certificates are issued with five week lifetimes, and renewal attempts begin two weeks prior to expiration. Upon renewal, a new key is generated. If automatic renewal is not performed, the user will have to follow the re-enrollment process. The keys are generated in the platform's system certificate store, using TPM on Windows and system keychain on macOS. On unenrollment or uninstallation, the certificate/key is removed.

Troubleshooting Zero Trust Access Module on Desktop

Any errors encountered with Zero Trust Access appear on the Zero Trust Access tile or in the Message History tab of the Secure Client UI.

You may encounter any of the following:

- A requirement to verify your identity
- A firewall that needs to be enabled and turned on
- A permissions error which denies access
- An unreachable application because of an outage or a move to a new location

DART collects data for troubleshooting Cisco Secure Client installation and connection problems. You must have the Diagnostics and Reporting Tool (DART) installed and run it as an administrator. All necessary logs for the client are stored in the DARTBundle.zip by default and saved to the local desktop. You can also specify what files to include in the bundle and where to store it with a Custom bundle creation. By default, data collection is based on U.S. region format (MM/DD/YY).

Note DART was enhanced to collect Duo Desktop logs. On Windows, Duo uses a PowerShell script to collect logs. Because PowerShell script execution is blocked by default, DART can only collect Duo logs when it is launched with administrator privileges. In the initial 5.1 release, DART will not collect Duo Desktop logs on macOS. It will collect them for Windows.

DART launches when Cisco Secure Client is running on a Windows device. For macOS devices, choose **Applications > Cisco > Cisco DART**. Then click the gear icon and **Diagnostics**.

To enhance logging and get more visibility for troubleshooting purposes, you can enable trace logging for Zero Trust Access with a logconfig.json file.

Troubleshooting Zero Trust Access App for Android

On an Android device, logs are sent to ZTA > Settings. Click **Send Logs** to email Zero Trust Access activity logs to your IT help desk for troubleshooting. You can also enable Verbose Logging within the app and view Zero Trust Access certificate information and other statistics on the Enrollment Window. Refer to Set up the Zero Trust Access App for Android on Samsung Devices for additional information.

Troubleshooting Zero Trust Access App for iOS

When troubleshooting enrolled iOS devices, you should first confirm that Zero Trust Access relay configuration was added. You can view added relay configuration by going to Settings > VPN&Relays. Under Per-App Relays, look for the Zero Trust app and click the **info (i)** icon to view the Zero Trust relay configuration. You can also view and send logs. Refer to Set up the Zero Trust Access App for Android for iOS Devices for additional information.

Note If a user has deleted the relay in phone settings, the Zero Trust Access home view will show text requiring the relay to be added back. You cannot access enrollment settings to do a config synch or unenroll unless the relay is added back.