



Zero Trust Access

The following topics provide an overview of Zero Trust Application Policies and how to configure and deploy them.

- [About Zero Trust Access, on page 1](#)
- [How Threat Defense Works with Zero Trust Access, on page 2](#)
- [Why Use Zero Trust Access?, on page 3](#)
- [Components of a Zero Trust Access Configuration, on page 3](#)
- [Zero Trust Access Workflow, on page 4](#)
- [Limitations for Zero Trust Access, on page 5](#)
- [Prerequisites for Zero Trust Application Policy, on page 6](#)
- [Manage Zero Trust Application Policies, on page 6](#)
- [Create a Zero Trust Application Policy, on page 7](#)
- [Create an Application Group, on page 8](#)
- [Create an Application, on page 9](#)
- [Set Targeted Devices for Zero Trust Access Policy, on page 11](#)
- [Edit a Zero Trust Application Policy, on page 12](#)
- [Monitor Zero Trust Sessions, on page 13](#)
- [History for Zero Trust Access, on page 15](#)

About Zero Trust Access

The Zero Trust Access feature is based on Zero Trust Network Access (ZTNA) principles. ZTNA is a zero trust security model that eliminates implicit trust. The model grants the least privilege access after verifying the user, the context of the request, and after analyzing the risk if access is granted.

Zero Trust Access allows you to authenticate and authorize access to protected web based resources and applications from inside (on-premise) or outside (remote) the network using an external SAML Identity Provider (IdP) policy.

The features are:

- Supports multiple SAML based identity providers such as Duo, Azure AD, Okta, and other identity providers.
- Client applications such as Cisco Secure Client are not required on the endpoint (client devices) for secure access.

2. The HTTPS request is intercepted by the firewall that protects the application.
3. The firewall redirects the user to application's configured IdP for authentication.



Note In the figure, each firewall protects a set of web applications. The user can directly access the applications behind the firewall after authentication and authorization.

4. After the authentication and authorization process is complete, the firewall allows the user to access the application.

Why Use Zero Trust Access?

Zero Trust Access leverages the existing deployment of threat defense as an enforcement point to application access. It allows for segmented access to a private application with per application authorization and per application tunnel for remote and on-premise users.

The feature hides the network from users and allows users to only access applications they are authorized for. Authorization for one application in the network does not give an implicit authorization for other applications on the network, thereby reducing the attack surface significantly. In other words, every access to an application must be explicitly authorized.

Adding the zero trust access functionality to threat defense enables migration to a more secure access model without having to install or manage yet another device in the network.

The feature is easy to manage as it does not require a client and is per application access.

Components of a Zero Trust Access Configuration

A new configuration consists of a Zero Trust Application Policy, Application Group, and Applications.

- **Zero Trust Application Policy**— Consists of application groups, and grouped or ungrouped applications. Security Zones and Security Controls settings are associated at a global level for all the ungrouped applications and group of applications.

A global port pool is assigned to the policy, by default. A unique port is automatically assigned from this pool to each private application that is configured.

Zero Trust Application policy consists of application groups, and grouped or ungrouped applications.

- **Application Groups**—Consists of a logical group of applications that share SAML authentication settings and can optionally share Security Zones and Security Controls settings.

Application Groups inherit the Security Zones and Security Controls settings from the global policy and can override the values.

When an Application Group is created, the same SAML IdP configuration can be used for authenticating multiple applications. Applications that are part of an Application Group inherit the Application Group's SAML configuration. This eliminates the need to configure the SAML settings for each application. After the Application Group is created, new applications can be added to it without configuring the IdP for it.

When an end user tries to access an Application that is part of group, the user is authenticated to the Application Group for the first time. When the user tries to access other applications that are part of the same Application Group, the user is provided access without being redirected again to the IdP for authentication. This prevents overloading the IdP with requests for application access and optimizes the usage of the IdP if a limit is enabled.

- **Applications**—There are two types:
 - **Ungrouped Applications**— Are standalone applications. SAML settings must be configured for every application. The applications inherit the Security Zones and Security Controls settings from the global policy and can be overridden by the application.
 - **Grouped Applications**— Are multiple applications that are grouped under an Application Group. The SAML settings are inherited from the Application Group and cannot be overridden. However, the Security Zones and Security Controls settings can be overridden for each application.

The following certificates are required for the configuration:

- **Identity Certificate**—This certificate is used by threat defense to masquerade as the applications. Threat Defense behaves as a SAML Service Provider (SP). This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications. It is a common certificate for all applications protected by threat defense.
- **IdP Certificate**—The IdP provides a certificate for each defined Application or Application Group. This certificate must be configured so that threat defense can verify the IDP's signature on incoming SAML assertions.



Note IdP certificates are commonly included within the metadata file; otherwise, users are required to have the IdP certificate readily available during the configuration of applications.

- **Application Certificate**—The encrypted traffic from user to the application is decrypted by threat defense using this certificate for the purpose of inspection.

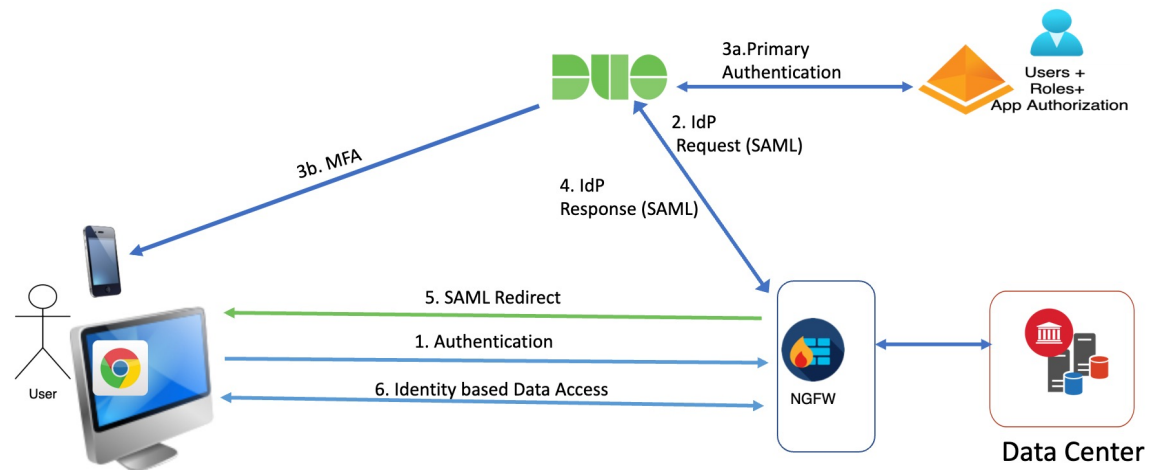


Note This certificate is required to verify the cookies in the header to authorize connections, even if we are not conducting an IPS/Malware inspection.

Zero Trust Access Workflow

This figure depicts the Zero Trust Access workflow.

Figure 2: Zero Trust Access Workflow



The workflow is as follows:

1. User types the application URL in the browser.
 - If the HTTPS request is valid, the user is redirected to the mapped port (Step 6).
 - If the HTTPS request is invalid, the user is sent for authentication per application (Step 2).
2. The user is redirected to the configured identity provider (IdP).
3.
 - a. The user is redirected to the configured primary authentication source.
 - b. The user is challenged with the configured secondary multi-factor authentication, if any.
4. The IdP sends a SAML response to threat defense. The user ID and other necessary parameters are retrieved from the SAML response through the browser.
5. The user is redirected to the application.
6. The user is allowed access to the application after validation is successful.

Limitations for Zero Trust Access

- Only web applications (HTTPS) are supported. Scenarios requiring decryption exemption are not supported.
- Supports only SAML IdPs.
- IPv6 is not supported. NAT66, NAT64, and NAT46 scenarios are not supported.
- The feature is available on threat defense only if Snort 3 is enabled.
- All hyperlinks in protected web applications must have a relative path and are not supported on individual mode clusters.

- Protected web applications running on a virtual host or behind internal load balancers must use the same external and internal URL.
- Not supported on individual mode clusters.
- Not supported on applications with strict HTTP Host Header validation enabled.
- If the application server hosts multiple applications and serves content based on the Server Name Indication (SNI) header in the TLS Client Hello, the external URL of the zero trust application configuration must match the SNI of that specific application.

Prerequisites for Zero Trust Application Policy

Prerequisite Type	Description
Licensing	<ul style="list-style-type: none"> • Smart license account with export-controlled features • (Optional) IPS and Threat licenses—It is required if security controls are used.
Configurations	Create a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of private applications. For more information, see Adding Certificate Enrollment Objects .
	Create a security zone through which access to private applications are regulated. For more information, see Create Security Zone and Interface Group Objects .

Manage Zero Trust Application Policies

You can create, edit, and delete zero trust application policies.

Procedure

Step 1 Choose **Policies > Access Control > Zero Trust Application**

Step 2 Manage the zero trust access policies:

- Create—Click **New Policy**. See [Create a Zero Trust Application Policy, on page 7](#)
- Edit—Click **Edit** (✎). See [Edit a Zero Trust Application Policy, on page 12](#)
- Report—Click **Report** (📄).
- Delete—Click **Delete** (🗑).

Step 3 Click **Save**.

What to do next

Ensure that there are no warnings before you deploy the configuration to threat defense. To deploy configuration changes, see Deploy Configuration Changes in the [Cisco Secure Firewall Management Center Administration Guide](#).

Create a Zero Trust Application Policy

This task configures a Zero Trust Application Policy.

Before you begin

Ensure that you complete all the prerequisites listed in [Prerequisites for Zero Trust Application Policy](#), on page 6.

Procedure

- Step 1** Choose **Policies > Access Control > Zero Trust Application**.
- Step 2** Click **Add Policy**.
- Step 3** In the **General** section, enter the policy name in the **Name** field. The description field is optional.
- Step 4** Enter a domain name in the **Domain Name** field.
- Ensure that the domain name is added to the DNS. The domain name resolves to the threat defense gateway interface from where the application is accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.
- Step 5** Choose an existing certificate from the **Identity Certificate** drop-down list.
- Click the **Add (+)** icon to configure a certificate enrollment object. For more information, see [Adding Certificate Enrollment Objects](#).
- Step 6** Choose a security zone from the **Security Zones** drop-down list.
- Click the **Add (+)** icon to add a new security zone.
- To add security zones, see [Create Security Zone and Interface Group Objects](#).
- Step 7** In the **Global Port Pool** section, a default port range is displayed. Modify, if required. Port values range from 1024 to 65535. A unique port from this pool is assigned to each private application.
- Note** This port range should avoid any conflicts with the existing NAT range.
- Step 8** (Optional) In the **Security Controls** section, you can add an Intrusion or Malware and File policy:
- **Intrusion Policy**—Choose a default policy from the drop-down list or click the **Add (+)** icon to create a new custom intrusion policy. For more information, see [Creating a Custom Snort 3 Intrusion Policy](#) topic in the latest version of the [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#).

- **Variable Set**—Choose a default variable set from the drop-down list or click the **Add (+)** icon to create a new variable set. For more information, see [Creating Variable Sets](#).

Note To use variable sets, you must have the Secure Firewall Threat Defense IPS license for your managed devices.

- **Malware and File Policy**—Choose an existing policy from the drop-down list. Click the **Add (+)** icon to create a new malware and file policy. For more information, see [Managing File Policies](#).

Step 9 Click **Save** to save the policy.

What to do next

1. Create an Application Group. See [Create an Application Group, on page 8](#).
2. Create an Application. See [Create an Application, on page 9](#).
3. Associate a Zero Trust Application Policy with a device. See [Set Targeted Devices for Zero Trust Access Policy, on page 11](#)
4. Deploy configuration changes. See Deploy Configuration Changes in the [Cisco Secure Firewall Management Center Administration Guide](#).

Create an Application Group

Before you begin

[Create a Zero Trust Application Policy, on page 7](#)

Procedure

- Step 1** Click **Add Application Group**.
- Step 2** In the **Application Group** section, type the name in the **Name** field and click **Next**.
- Step 3** In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated. Copy the values of the **Entity ID** and **Assertion Consumer Service (ACS) URL** fields or click **Download SP Metadata** to download this data in XML format for adding it to the IdP. Click **Next**.
- Step 4** In the **SAML Identity Provider (IdP) Metadata** section, add the metadata using any one of the methods:
- **XML File Upload**—Choose a file or drag and drop the XML file.
The details of the **Entity ID**, **Single Sign-On URL**, and **IdP Certificate** are displayed.
 - **Manual Configuration**—Perform these steps:
 - **Entity ID**—Enter the URL that is defined in the SAML IdP to identify a service provider uniquely.
 - **Single Sign-On URL**—Enter the URL for signing into the SAML identity provider server.

- **IdP Certificate**—Choose the certificate of the IdP enrolled in threat defense to verify the messages signed by the IdP.

Click the **Add** (+) icon to configure a new certificate enrollment object. For more information, see [Add Certificate Enrollment](#).

- **Configure Later**—In the event you do not have the IdP metadata, you can configure it later.

Click **Next**.

- Step 5** In the **Re-authentication Interval** section, enter the value in the **Timeout Interval** field and click **Next**. The re-authentication interval allows you to provide a value that determines when a user must authenticate again.
- Step 6** In the **Security Zones and Security Controls** section, the security zones and threat settings are inherited from the parent policy. You can override these settings. Click **Next**.
- Step 7** Review the configuration summary. Click **Edit** to modify the details in any of the sections. Click **Finish**.
- Step 8** Click **Save**.

The Application Group is created and is displayed on the Zero Trust Application page.

What to do next

1. [Create an Application, on page 9](#).
2. Deploy configuration changes. See Deploy Configuration Changes in the [Cisco Secure Firewall Management Center Administration Guide](#).

Create an Application

Use this task to create a Grouped or Ungrouped Application.

Before you begin

1. [Create a Zero Trust Application Policy, on page 7](#).
2. [Create an Application Group, on page 8](#) (required only for Grouped Applications).

Procedure

- Step 1** Choose **Policies > Access Control > Zero Trust Application**
- Step 2** Choose the policy.
- Step 3** Click **Add Application**.
- Step 4** In the **Application Settings** section, complete the following fields.
- **Application Name**—Enter the application name.

- **External URL**—Enter the URL that is used by the user to access the application.
- **Application URL**—By default, the external URL is used as the Application URL. Uncheck the **Use External URL as Application URL** check box to specify a different URL.

If the threat defense uses an internal DNS, then the Application URL must align with an entry within that DNS, to ensure resolution to the application.

- **Application Certificate**—Choose the certificate for the private application. Click the **Add (+)** icon to configure an internal certificate object. For more information, see [Adding Internal Certificate Objects](#).
- **IPv4 Source Translation**—Choose the source network for NAT from the drop-down list. Click the **Add (+)** icon to create a network object. For more information, see [Network](#).

This Network Object or Object Group is used to translate a public network source IP address of an incoming request to a routable IP address inside the corporate network.

Note Only object or object groups of type Host or Range are supported.

- **Application Group**—Choose the Application Group from the drop-down list. See [Create an Application Group, on page 8](#).

Note This field is not applicable for an ungrouped application.

Step 5 Click **Next**.

Step 6 Based on the application type:

- For a Grouped Application, the **SAML Service Provider (SP) Metadata**, **SAML Identity Provider (IdP) Metadata**, and **Re-authentication Interval** are inherited from the Application Group and do not need to be configured by the user.
- For an Ungrouped Application, perform these steps:
 - a. In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated. Copy the **Entity ID** or **Assertion Consumer Service (ACS) URL** of the IdP or click **Download SP Metadata** to download this data in XML format for adding it to the IdP. Click **Next**.
 - b. In the **SAML Identity Provider (IdP) Metadata** section, add the metadata using any one of the methods:
 - **XML File Upload**—Choose a file or drag and drop the XML file.
The details of the **Entity ID**, **Single Sign-On URL**, and **IdP Certificate** are displayed.
 - **Manual Configuration**—Perform these steps:
 - **Entity ID**—Enter the URL that is defined in the SAML IdP to identify a service provider uniquely.
 - **Single Sign-On URL**—Enter the URL for signing into the SAML identity provider server.
 - **IdP Certificate**—Choose the certificate of the IdP enrolled in threat defense to verify the messages signed by the IdP.

Click the **Add (+)** icon to configure a new certificate enrollment object. For more information, see [Add Certificate Enrollment](#).

- **Configure Later**—In the event you do not have the IdP metadata, you can configure it later.

Click **Next**.

- c. In the **Re-authentication Interval** section, enter the value in the **Timeout Interval** field and click **Next**. The reauthentication interval allows you to provide a value that determines when a user must authenticate again.

Step 7 In the **Security Zones and Security Controls** section, the security zones and threat settings are inherited from the parent policy or application group. You can override these settings. Click **Next**.

Step 8 Review the configuration summary. Click **Edit** to modify the details in any of the sections. Click **Finish**.

Step 9 Click **Save**.

The Application is listed on the Zero Trust Application page and is enabled by default.

What to do next

1. [Set Targeted Devices for Zero Trust Access Policy, on page 11.](#)
2. Deploy configuration changes. See Deploy Configuration Changes in the [Cisco Secure Firewall Management Center Administration Guide](#).

Set Targeted Devices for Zero Trust Access Policy

Each Zero Trust Application policy can target multiple devices; each device can have one deployed policy at a time.

Before you begin

1. [Create a Zero Trust Application Policy, on page 7.](#)
2. [Create an Application Group, on page 8.](#)
3. [Create an Application, on page 9.](#)

Procedure

Step 1 Choose **Policies > Access Control > Zero Trust Application**

Step 2 Choose the policy.

Step 3 Click **Targeted Devices**.

Step 4 Choose the devices where you want to deploy the policy using any one of the methods:

- Choose a device in the **Available Devices** list and click >> or the **Add (+)** icon.
- To remove a device from the **Selected Devices** list, choose a device and click << or the **Delete (🗑)** icon.

Step 5 Click **Apply** to save policy assignments.

Step 6 Click **Save** to save the policy.

What to do next

Deploy configuration changes. See Deploy Configuration Changes in the [Cisco Secure Firewall Management Center Administration Guide](#).

Edit a Zero Trust Application Policy

You can edit the settings of a Zero Trust Application Policy, Application Group, or Application.

Procedure

Step 1 Choose **Policies > Access Control > Zero Trust Application**

Step 2 Click **Edit** (✎) next to the Zero Trust Application Policy you want to edit.

Step 3 Edit your Zero Trust Application Policy.

You can change the following settings or perform these actions:

- Name and Description—Click **Edit** (✎) next to the policy name, make your changes, and click **Apply**.
- To modify the policy settings:
 - Click **Settings**
 - Modify the settings as required.
 - Important** Editing the domain name for the SAML ACS URL interrupts application access.
 - Click **Save**.
- To modify the Application Group settings:
 - Click **Applications**.
 - Click **Edit** (✎) next to the Application Group you want to edit.
 - In each section, click **Edit** to modify the settings, as required
 - Important** Editing the Application Group name interrupts application access.
 - Click **Apply** after you modify the settings in a section.
 - Click **Finish**.
 - Click **Save**.
- To modify the Application settings:
 - Click **Applications**.

- Click **Edit** (✎) next to the Application you want to edit.
 - In each section, click **Edit** to modify the settings, as required.
Important Editing the Application name interrupts application access.
 - Click **Apply** after you modify the settings in a section.
 - Click **Finish**.
 - Click **Save**.
- To enable, disable, or delete multiple Applications, choose the Applications, click the required bulk action, and click **Save**.
Note These actions are also available in the right-click menu.
 - To enable all Applications, click **Bulk Actions > Enable**.
 - To disable all Applications, click **Bulk Actions > Disable**.
 - To delete all Applications, click **Bulk Actions > Delete**.
 - Click **Return to Zero Trust Application** to return to the policy page.
-

What to do next

Deploy configuration changes. See Deploy Configuration Changes in the [Cisco Secure Firewall Management Center Administration Guide](#).

Monitor Zero Trust Sessions

Connection Events

After a Zero Trust Application Policy is deployed, new fields are available. To add the fields to the table view:

1. Choose **Analysis > Connections > Events**.
2. Go to the **Table View of Connection Events** tab.
3. In the table view of events, multiple fields are hidden by default. To change the fields that appear, click the **x** icon in any column name to display a field selector.
4. Choose the following fields:
 - Authentication Source
 - Zero Trust Application
 - Zero Trust Application Group
 - Zero Trust Application Policy

5. Click **Apply**.

See Connection and Security-Related Connection Events in the [Secure Firewall Management Center Administration Guide](#) for more information on the connection events.

Zero Trust Dashboard

The Zero Trust dashboard allows you to monitor real-time data from active zero trust sessions on the devices.

The Zero Trust dashboard provides a summary of the top zero trust applications and zero trust users that are managed by the management center. Choose **Overview > Dashboards > Zero Trust** to access the dashboard.

The dashboard has the following widgets:

- Top Zero Trust Applications
- Top Zero Trust Users

CLI Commands

Log in to the device CLI and use the following commands:

CLI Command	Description
show running-config zero-trust	To view the running configuration for a zero trust configuration
show zero-trust	To display the run-time zero trust statistics and session information
show cluster zero-trust	To display the summary of zero trust statistics across nodes in a cluster
clear zero-trust	To clear zero trust sessions and statistics
show counters protocol zero_trust	To view the counters that are hit for zero trust flow


Diagnostics Tool

The diagnostics tool facilitates the troubleshooting process by detecting possible issues with zero trust configurations. The diagnostics can be classified into two types:

- **Application-specific diagnostics** are used to detect issues such as:
 - DNS-related issues
 - Misconfigurations such as socket not open, and issues with classification and NAT rules.
 - Issues with deployment of zero trust policy or SSL rules
 - Issues with source NAT issues and exhaustion of PAT pool
- **General diagnostics** are used to detect issues such as:
 - Strong cipher license not enabled
 - Invalid application certificate

- SAML-related issues
- Home agent and cluster bulk sync issues

To run the diagnostic tool:

1. Click Diagnostics () next to the zero trust application that you want to troubleshoot. The **Diagnostics** dialog box appears.
2. Choose the device from the **Select Device** drop-down list and click **Run**. A report is generated in the **Reports** tab after the diagnostic process is complete.
3. To view, copy, or download the logs, click the **Logs** tab.

History for Zero Trust Access

Feature	Minimum Management Center	Minimum Threat Defense	Details
Enhancements to Zero Trust Access	7.4.1	7.4.1	<ul style="list-style-type: none"> • You can now configure the source network for NAT for an application. The configured Network Object or Object Group is used to translate a public network source IP address of an incoming request to a routable IP address inside the application network. • A diagnostics tool is now available to facilitate the troubleshooting process. The tool detects possible issues with zero trust configurations.
Zero Trust Access	7.4.0	7.4.0	You can allow users to access private applications without requiring additional software on their personal devices. This functionality leverages SAML-based authentication and supports Duo, as well as all other major identity providers.

