

How to Protect Applications Using Zero Trust Access in Cisco Secure Firewall

First Published: 2024-01-29

Overview of Zero Trust Network Access

Zero Trust Secure Access Using Cisco Secure Firewall

Zero trust access is based on a security model that establishes trust through continuous authentication and monitoring of each network access attempt. You can use the Secure Firewall Management Center web interface to create a Zero Trust Application Policy that allows you to define private applications and assign threat policies to them. The policy is application-specific where the administrator decides the inspection levels based on the threat perception for that application.

This document outlines a scenario demonstrating the complete process of securing an application and implementing threat and malware protection. The document also includes the validation steps to access the application, protect it from threat and malware, and monitor the zero trust sessions.

Features of Zero Trust Access in Secure Firewall Management Center

The features are:

- Supports multiple SAML based identity providers such as Duo, Azure AD, Okta, and other identity providers.
- Client applications such as Cisco AnyConnect are not required on the endpoint (client devices) for secure access.
- Access and authentication are through the browser.
- Supports only web applications (HTTPS).
- Client device posture is supported through agents such as Duo Health, using which the posture of the device can be evaluated against a policy in Duo, and access can be provided based on the same. The same functionality can be performed in conjunction with third-party identity providers that support posture evaluation with their agents such as Okta or PingID.
- Supports HTTP-Redirect SAML binding.
- Supports Application Groups that make it easier to enable zero trust protection on a set of applications.
- Leverages threat defense intrusion and malware protection on zero trust application traffic.

Prerequisites

This document assumes that you have a basic understanding of zero trust concepts and have gone through the "Zero Trust Access" chapter in the [Cisco Secure Firewall Management Center Device Configuration Guide](#), version 7.4 or later.

Is This Use Case For You?

This use case outlines the process for accessing private applications and resources using the clientless Zero Trust Network Access model. We recommend using Cisco Secure Client for the client-based secure network and application access. For more information, see [Cisco Secure Client](#).

This use case assists network administrators who plan to use the zero trust feature in the Secure Firewall Management Center to enable their hybrid workforce to access protected resources and web applications. They also aim to safeguard the protected resources and applications against malware.

Scenario for Implementing Zero Trust Access

A large enterprise has a distributed workforce, with employees and contractors working from various locations and accessing private applications and resources hosted behind the company's firewall. The administrator wants to prevent the workforce from performing malicious activity when accessing the protected application.

What is at risk?

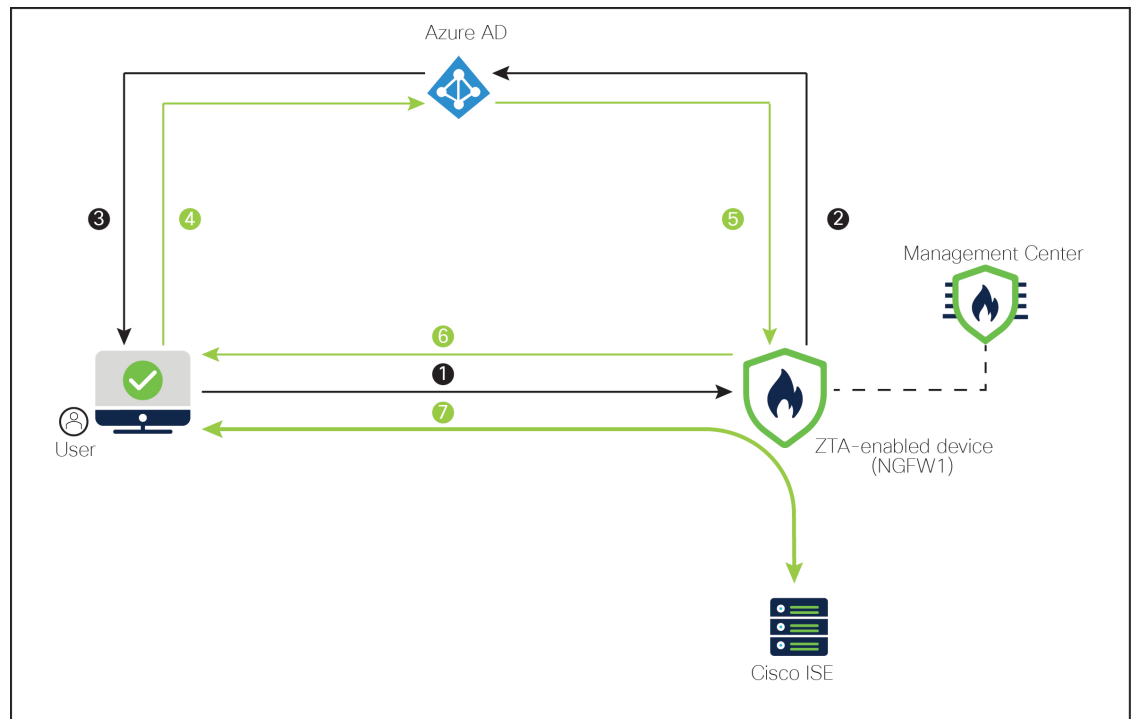
The workforce gains full network access, which can increase the attack surface and make the network more vulnerable to attacks. They also can upload files, including those that may potentially contain malicious content.

How does the Secure Firewall Management Center Zero Trust Access Policy protect your applications?

The network administrator incorporates zero trust access to the firewall, enabling secure remote access to important resources and applications without needing software installed on every endpoint device. This functionality boosts performance but also limits authorization to a single application, thereby minimizing potential attack points. Access to sensitive information or applications is granted only after verifying the user's identity, checking the request's context, and performing a risk analysis. Furthermore, a malware and file policy is in place to safeguard zero-trust application traffic.

Network Topology

The following network topology includes a threat defense device, which is set up at the data center. A security zone is established on the device's outbound interface.



In the above figure, the network administrator is using the management center to configure and deploy the zero trust policy to the threat defense labeled **NGFW1**. The **Cisco ISE** application is hosted in a data center behind the firewall, which the user accesses through the Zero Trust Application. Note: ISE is not being used for AAA (Authentication, Authorization, and Accounting). Microsoft Azure Active Directory is the SAML IdP server that is used for authentication and authorization. A network object is created to translate a public network source IP address of an incoming request to a routable IP address inside the corporate network.

1. The user types the application URL in the browser.
2. The ZTA-enabled managed device directs the user to the configured IdP.
3. The IdP prompts the user to enter their credentials.
4. The user enters the username and password.
5. The IdP sends a SAML response to the firewall. The user ID and other necessary parameters are retrieved from the SAML response through the browser.
6. The user is redirected to the application after validation is successful.
7. The user is allowed access to the application. Optionally, threat and malware protection is applied while accessing the application.

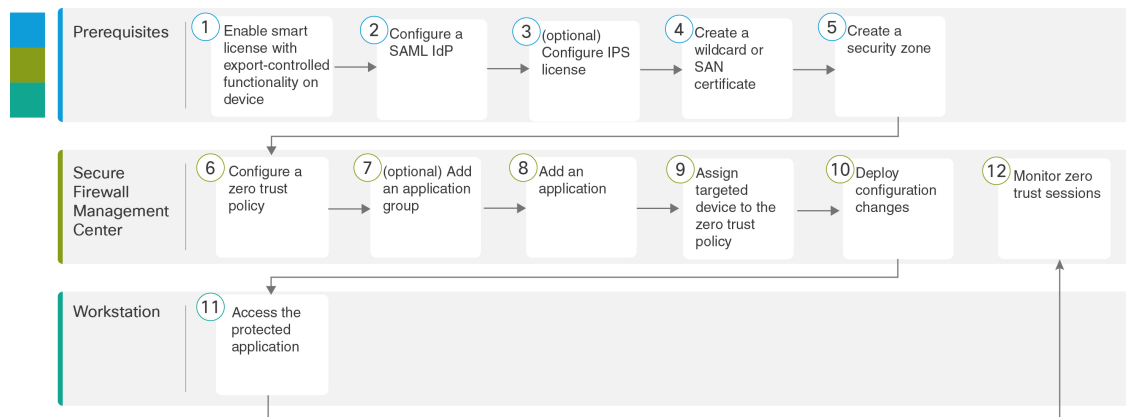
Limitations for Zero Trust Access

- 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.

End-to-End Procedure for Configuring Zero Trust Application

The following flowchart illustrates the workflow for configuring zero trust access in the Secure Firewall Management Center.



Step	Description
1	(Prerequisite) Enable smart license with export-controlled functionality on threat defense.
2	(Prerequisite) Configure a SAML IdP.
3	(Prerequisite) (optional) Configure IPS license.
4	(Prerequisite) Create a wildcard or Subject Alternative Name (SAN) certificate.
5	(Prerequisite) Create a security zone.

Step	Description
6	Create a Zero Trust Application Policy
7	Create an Application Group.
8	Create an Application.
9	Set Targeted Devices for Zero Trust Access Policy.
10	Deploy Configuration to Devices.
11	Access the Protected Application.
12	Monitor Zero Trust Sessions.

Prerequisites for Zero Trust Application Policy

Ensure that you have:

- Smart license account with export-controlled features.
- Configured a SAML Identity Provider (IdP) for authentication and authorization to access the private application.
- Configured IPS and Threat licenses for enabling security controls.
- Created a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of private applications. For more information, see the "Adding Certificate Enrollment Objects" section in the "Object Management" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)
- Created a security zone in the management center through which access to private applications is regulated. For more information, see the "Create Security Zone and Interface Group Object" section in the "Interface Overview" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)
- Public DNS updates are required.

Certificates

Ensure you create the following certificates:

- **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.

For more information, see the "Adding Certificate Enrollment Objects" section in the "Object Management" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)

For this example, we created an identity certificate **ZTAA-ID-Certificate**.

- **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.

For more information, see the "Add Certificate Enrollment" section in the "Object Management" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)

For this example, we create an IdP certificate, **Azure-AD-SAML-Certificate**.

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

For more information, see the "Adding Internal Certificate Objects" section in the "Object Management" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)

For this example, we created an internal certificate for the application, **ZTAA-ISE-GUI-Certificate**.



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.

Create a Zero Trust Application Policy

This task configures a Zero Trust Application Policy.

Before you begin

Ensure that you have:

- Domain name to resolve to the threat defense gateway interface from where the application is accessed.
- Security zones to regulate access to the private applications. For more information, see the "Create Security Zone and Interface Group Objects" section in the "Interface Overview" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)

Procedure

-
- Step 1** In the management center, choose **Policies > Access Control > Zero Trust Application**.
- Step 2** Click **Add Policy**.
- Step 3** Configure the zero trust policy settings as described below:
- **Name:** Enter a policy name. In this example, the zero trust policy name is **ZTAA-Policy**.
 - **Domain Name:** Enter a domain name. The domain name is used to generate the Assertion Consumer Service (ACS) URL for all private applications in an Application Group. In this example, the domain name is **ztaa.local**.

General	<p>Name *</p> <input type="text" value="ZTAA-Policy"/>
	<p>Description</p> <input type="text"/>
Domain Name	<p>The domain name must resolve to the interfaces that are part of the security zones from which private applications are accessed.</p> <p>Domain Name *</p> <input type="text" value="ztaa.local"/>
	<p>• 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.</p>

- **IdP Certificate:** Choose an existing certificate from the Identity Certificate drop-down list. In this example, we select the created identity certificate **ZTAA-ID-Certificate**.
- **Security Zones:** Choose a security zone from the drop-down list. In this example, we created a security zone, **OutZone**.
- **Port Range:** A unique port from this pool is assigned to each private application. This port range should avoid any conflicts with the existing NAT range. In this example, we use the default value, **20000-22000**.

Identity Certificate	<p>A common certificate that represents all the private applications at the pre-authentication stage.</p> <p>Certificate *</p> <input type="text" value="ZTAA-ID-Certificate"/> x v +
	<p>• This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications.</p>
Security Zones	<p>The access to private applications is regulated through security zones. Choose outside or/and inside zones through which the private applications are regulated.</p> <p>Security Zones *</p> <input type="text" value="OutZone"/> x v +
	<p>• This is the default setting for all private applications. It can be overridden at an Application or Application Group level.</p>
Global Port Pool	<p>Unique port from this pool is assigned to each private application.</p> <p>Port Range *</p> <input type="text" value="20000-22000"/> Range: (1024-65535)
	<p>• Ensure a sufficient range is provided to accommodate all private applications. Do not share these ports in NAT or other configurations.</p>

Step 4 In the **Security Controls** section, add an Intrusion or Malware and File policy. This configuration provides intrusion and malware protection on the zero trust application traffic.

- **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](#). For this example, we created an intrusion policy, **Balanced Intrusion**.

- **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, the "Creating Variable Sets" section in the "Object Management" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y](#). In this example, we used the default value, **Default-Set**.

- **Malware and File Policy:**

Choose an existing policy from the drop-down list or click the Add (+) icon to create a new custom malware policy.

Choose an existing policy from the drop-down list. For more information, see the "Managing File Policies" section in the "Network Malware Protection and File Policies" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y](#). For this example, we created a malware policy, **Block Malware**.

Security Controls <i>(Optional)</i>	Private applications can be subject to inspection using a selected Intrusion or Malware and File policy.
Intrusion Policy	Balanced Intrusion x v +
Variable Set	Default-Set x v +
Malware and File Policy	Block Malware x v +
<p>• These are default settings for all private applications. It can be overridden at an Application or Application Group level.</p>	

Step 5 Click **Save**.

Create an Application Group

Procedure

- Step 1** In the management center, choose **Policies > Access Control > Zero Trust Application**.
- Step 2** Click edit policy.
- Step 3** Click **Add Application Group**.
- Step 4** In the **Application Group** section, type the name in the **Name** field and click **Next**. In this example, the application group name is **ZTAA-Group**.

Step 5 In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated from configuration elements you provided in the previous steps:

- Application Group: ZTAA-Group
- Domain name: ztaa.local

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.

For this example, the data is downloaded in the XML format and uploaded to the Azure Active Directory IdP.

Click **Next**.

Step 6 In the **SAML Identity Provider (IdP) Metadata** section, add the metadata.

In this example, the meta data is entered manually.

Select **Manual Configuration** to enter the meta data.

- **Entity ID:** Enter the URL that is defined in the SAML IdP to identify a service provider uniquely. In this example, we use **https://sts.windows.net/ b26f4c82-cf2b-40a2-9db0-33c93d3bb072/**.
- **Single Sign-On URL:** Enter the URL for signing into the SAML identity provider server. In this example, we use **https://login.microsoftonline.com/b26f4c82-cf2b-40a2-9db0-33c93d3bb072/saml2**.
- **IdP Certificate:** Choose the certificate of the IdP enrolled in threat defense.
In this example, we select the created IdP certificate, **Azure-AD-SAML-Certificate**.

3 SAML Identity Provider (IdP) Metadata

Import or enter the IdP metadata. If IdP metadata is not currently available, you can skip this step and configure it later.

Import IdP Metadata
 Manual Configuration
 Configure Later

Entity ID*

https://sts.windows.net/b26f4c82-cf2b-40a2-9db0-33c93d3bb072/

Single Sign-On URL*

https://login.microsoftonline.com/b26f4c82-cf2b-40a2-9db0-33c93d3bb072

IdP Certificate*

Azure-AD-SAML-Certificate x v +

Next

In this example, the manual configuration is selected.

Click **Next**.

Step 7 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. In this example, we use the default value, **1440**.

Step 8 In the **Security Zones and Security Controls**, the security zones and threat settings are inherited from the parent. In this example, the default values are retained. Click **Next**.

Step 9 Review the configuration summary. Click **Finish**.

Add Application Group

An Application Group allows you to group multiple Applications and share authentication, security zone, and threat configurations.

1 Application Group	Name	ZTAA-Group	Edit
2 SAML Service Provider (SP) Metadata	Entity ID	https://ztaa.local/ZTAA-Group/saml/sp/metadata	Edit
	Assertion Consumer Service (ACS) URL	https://ztaa.local/ZTAA-Group/+CSCOE+/saml/sp/acs?tname=DefaultZer...	
3 SAML Identity Provider (IdP) Metadata	Entity ID	https://sts.windows.net/b26f4c82-cf2b-40a2-9db0-33c93d3bb072/	Edit
	Single Sign-On URL	https://login.microsoftonline.com/b26f4c82-cf2b-40a2-9db0-33c93d3bb072	
	IdP Certificate	Azure-AD-SAML-Certificate	
4 Re-Authentication Interval	Timeout Interval	1440 minutes	Edit
5 Security Zones and Security Controls	Security Zones	Inherited: (OutZone)	Edit
	Intrusion Policy	Inherited: (Balanced Intrusion)	
	Variable Set	Inherited: (Default-Set)	
	Malware and File Policy	Inherited: (Block Malware)	

Step 10 Click **Save**.

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

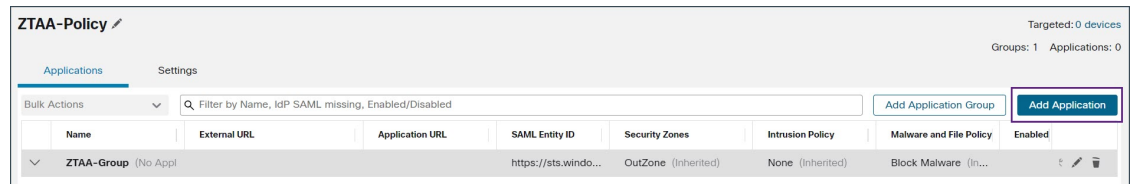
Create an Application

Procedure

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

Step 2 Choose the policy. In this example, we select **ZTAA-Policy**.

Step 3 Click **Add Application**.



Step 4 In the **Application Settings**, configure the following fields:

- **Application Name:** Enter the application name. In this example, the application name is **ZTAA-ISE-GUI-Access**.
- **External URL:** Enter the URL that is used by the user to access the application. In this example, we use **https://ise-external.local**.
- **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. In this example, we use **https://ise.local**.
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.
In this example, we select the created internal certificate, **ZTAA-ISE-GUI-Certificate**.
- **IPv4 Source Translation:** The 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. For more information, see the "Create Network Objects" section in the "Object Management" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y.](#)
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](#).
Note This field is not applicable for an ungrouped application.

In this example, we use **ZTAA-Group** application group.

The screenshot shows the 'Add Application' configuration window. At the top right, there is an 'Enabled' toggle switch. The main configuration area is titled 'Application Settings' and includes the following fields:

- Application Name ***: ZTAA-ISE-GUI-Access
- External URL ***: https://ise-external.local
- Application URL (FQDN or Network IP) ***: https://ise.local
- Use External URL as Application URL
- Application Certificate ***: ZTAA-ISE-GUI-Certificate
- IPv4 Source Translation ***: any
- Application Group**: ZTAA-Group

A 'Next' button is located at the bottom right of the configuration area.

Click **Next**.

Step 5 Review the configuration summary and click **Finish**.

Step 6 Click **Save**.

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

Note The management center provides the diagnostics tool for each application to facilitate troubleshooting by detecting possible issues with zero trust configurations. For more information, see the "Monitor Zero Trust Sessions" section in the "Zero Trust Access" chapter of [Cisco Secure Firewall Management Center Device Configuration Guide, X.Y](#).

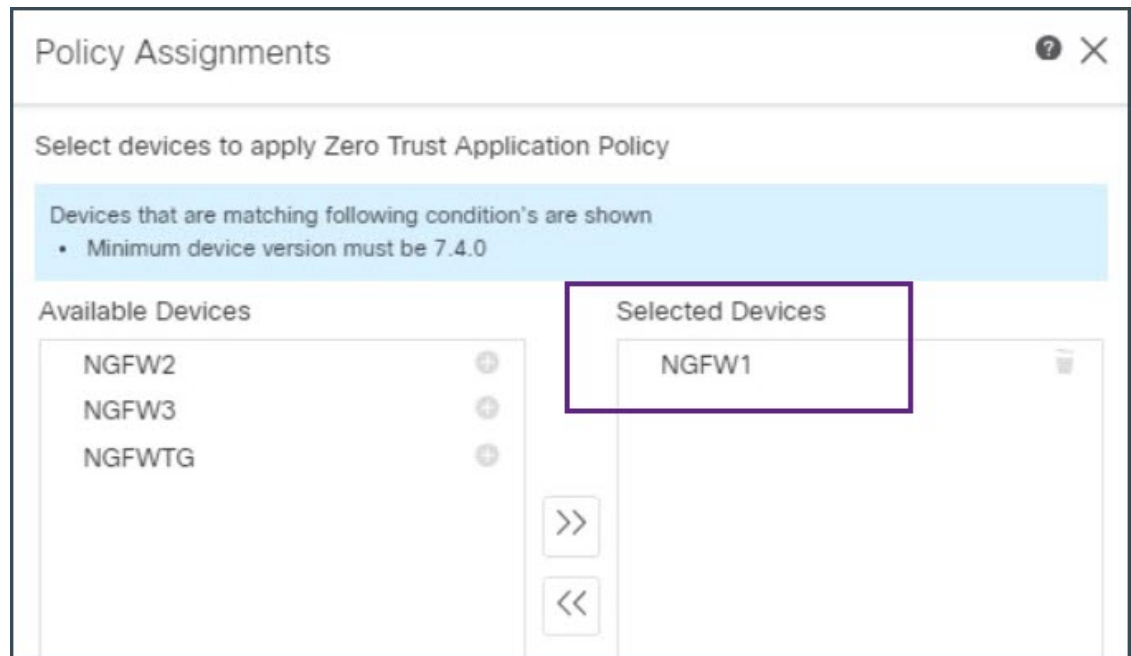
Set Targeted Devices for Zero Trust Access Policy

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

Procedure

- Step 1** Choose **Policies > Access Control > Zero Trust Application**.
- Step 2** Choose the policy. In this example, we select **ZTAA-Policy**.
- Step 3** Click **Targeted Devices**.
- Step 4** Choose the device you want to deploy.

In this example, we select **NGFW1**.



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

Step 6 Click **Save**.

What to do next

[Deploy Configuration to Devices](#)

Deploy Configuration to Devices

After you complete all the configurations, deploy them to the managed device.

Procedure

- Step 1** On the management center menu bar, click **Deploy**. This displays the list of devices that are Ready for Deployment.
- Step 2** Check the checkboxes adjacent to the device on which you want to deploy configuration changes. In this example, the device is **NGFW1**.
- Step 3** Click **Deploy**. Wait till the deployment is marked Completed on the Deploy dialog box.
- Step 4** If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Errors** or **Validation Warnings** window. To view complete details, click the **Validation Errors** or **Validation Warnings** link.

You have the following choices:

- **Proceed with Deploy:** Continue deploying without resolving warning conditions. You cannot proceed if the system identifies errors.
- **Close:** Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.

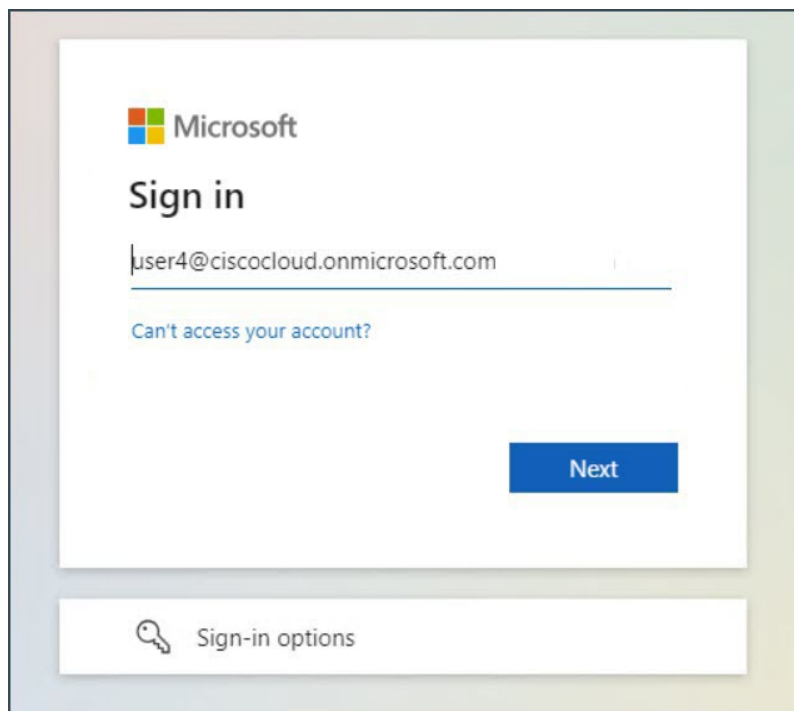
Access the Protected Application

After a successful configuration deployment, you can access the application by using the external URL of the application.

Procedure

Step 1 In the client machine, open a browser and access the protected application using the external URL. In this example, the external URL used is **https://ise-external.local**.

The user is redirected to the login page, and the SAML IdP prompts them to enter their credentials. In this example, the SAML IdP used is Microsoft Azure Active Directory.



Step 2 After submitting the credentials, the user is redirected to the application once IdP authenticates and authorizes the user and sends the SAML assertion in the response to the threat defense device.

Step 3 After a successful authentication, the user can access the application. In this example, the Cisco ISE home page is displayed.

Step 4 The user logs in to Cisco ISE using their credentials.

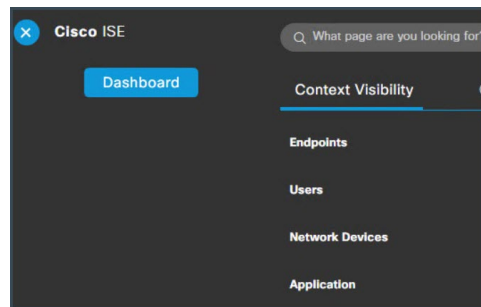
Test Malware Protection on Zero Trust Application Traffic

If the user attempts to upload a malware file to the protected application, ZTA policy blocks the malware file upload on their network.

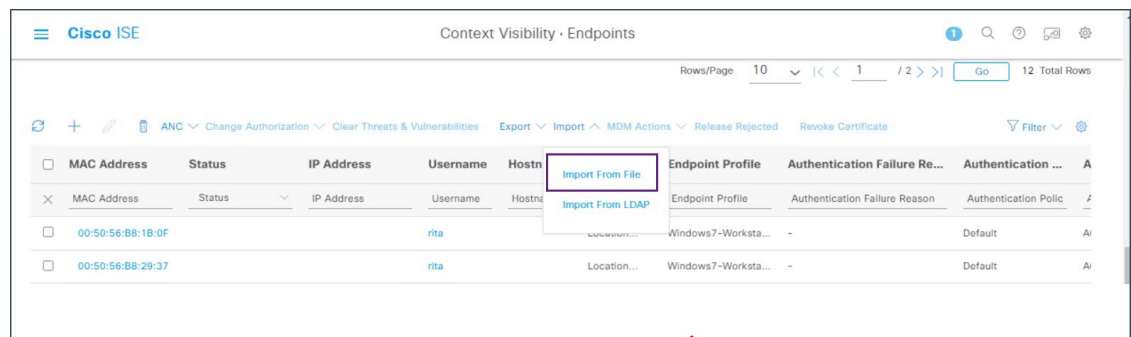
Procedure

Step 1 Log in to the Cisco ISE application.

Step 2 In the Cisco ISE GUI, click the Menu icon () and choose **Context Visibility > Endpoints**.



Step 3 Scroll down this page to locate the list of endpoints and choose **Import > Import From File**.

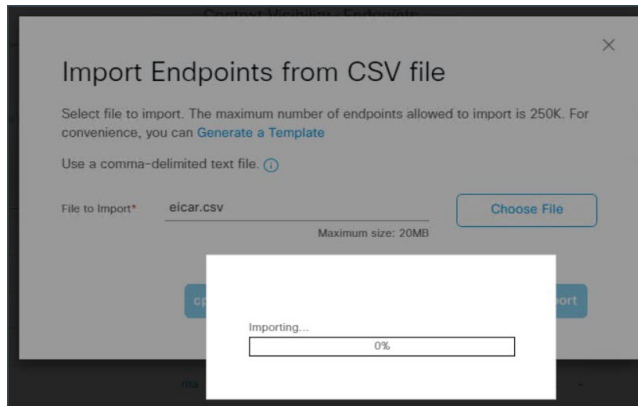


Step 4 Click **Choose File** and select the file you want to upload. The navigation steps to select a file may differ depending on your operating system.

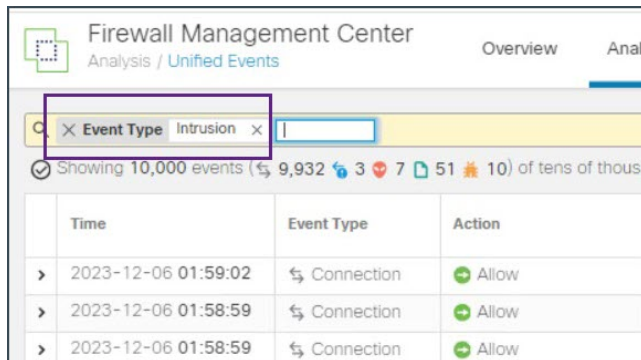
In this example, we are selecting a precreated sample malware file.

Step 5 Click **Import**.

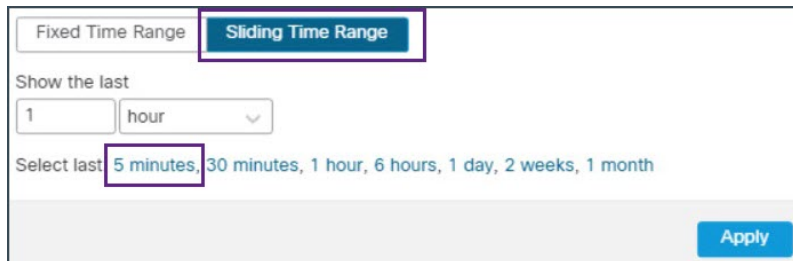
The upload action doesn't progress beyond 0%. This is a malware file and ZTA policy has blocked the file from being uploaded.



- Step 6** Log in to the management center, and choose **Analysis > Unified Events**.
- Step 7** In the search bar, set the filter **Event Type** to **Intrusion** and click **Apply**.



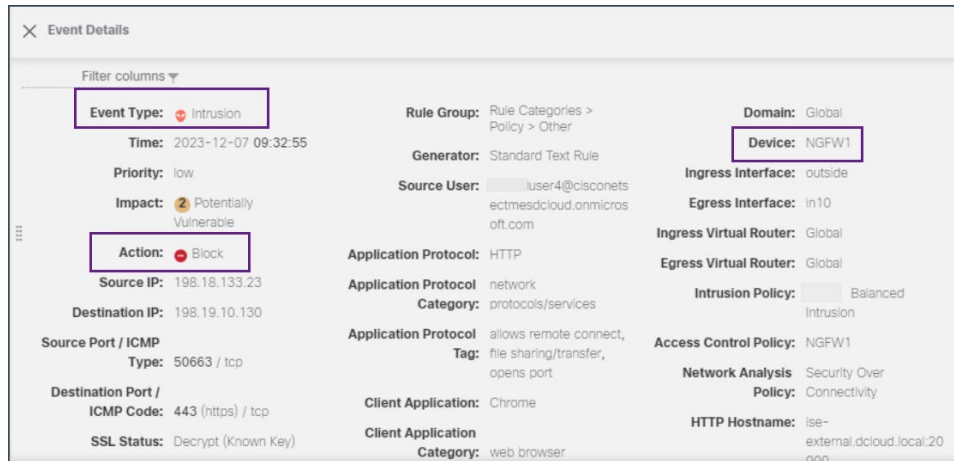
In this example, we are configuring a sliding default time window to **5 minutes**. Click **Sliding Time Range**.



The eventing page displays that a malicious file was detected and blocked.



Double-click the event to see more information in the **Event Details** page.



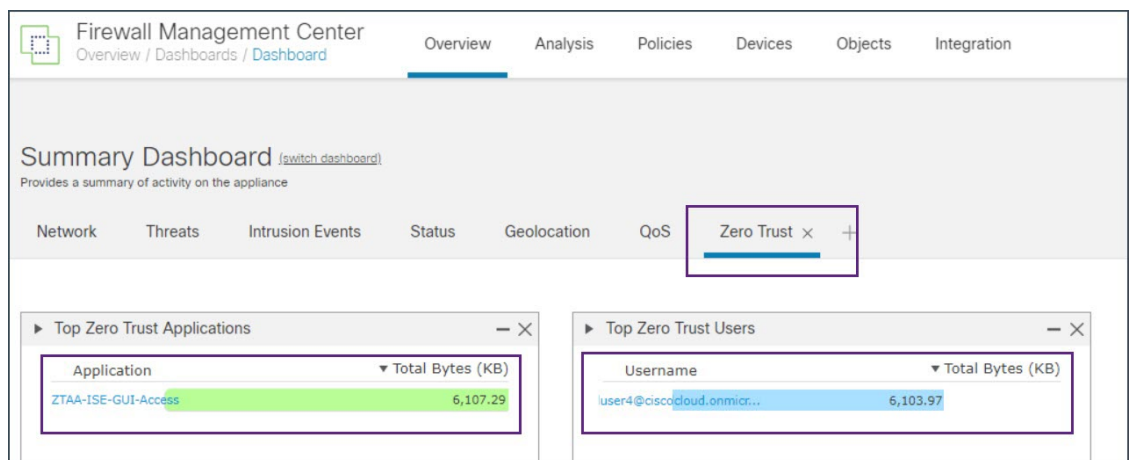
Monitor Zero Trust Sessions

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.

In this example, the **Top Zero Trust Applications** widget shows the zero trust application **ZTAA_ISE_GUI_Access** and the username of the user accessing the application.



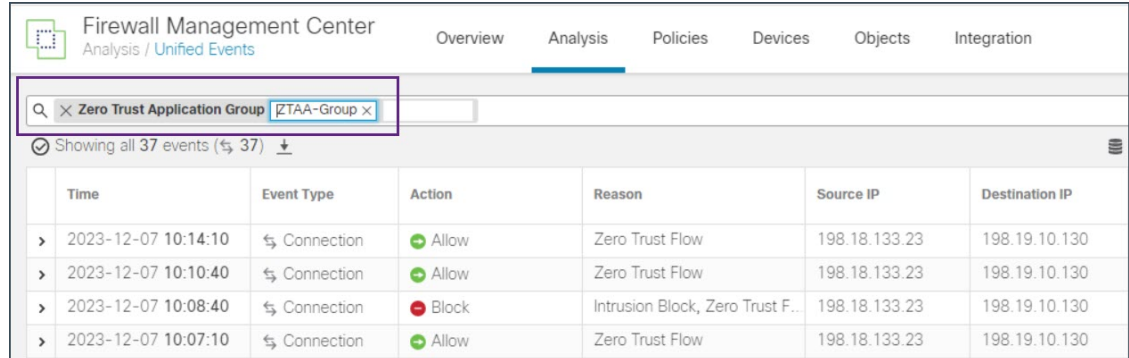
Connection Events

After establishing zero trust sessions, you can view the events that are associated with those sessions and monitor the activity of the users.

1. In the management center, choose **Analysis > Unified Events**.

- In the **Search** bar, search for **Zero Trust Application**, **Zero Trust Application Group**, or **Zero Trust Application Policy** and enter the corresponding name that you specified while creating it.

In this example, we use the **Zero Trust Application Group**, which is **ZTAA-Group**, to search for the events.



The screenshot shows the Firewall Management Center interface. The search bar contains the text "Zero Trust Application Group" and a tag "ZTAA-Group". Below the search bar, it indicates "Showing all 37 events (37)". The table below displays the search results:

	Time	Event Type	Action	Reason	Source IP	Destination IP
>	2023-12-07 10:14:10	↔ Connection	→ Allow	Zero Trust Flow	198.18.133.23	198.19.10.130
>	2023-12-07 10:10:40	↔ Connection	→ Allow	Zero Trust Flow	198.18.133.23	198.19.10.130
>	2023-12-07 10:08:40	↔ Connection	→ Block	Intrusion Block, Zero Trust F...	198.18.133.23	198.19.10.130
>	2023-12-07 10:07:10	↔ Connection	→ Allow	Zero Trust Flow	198.18.133.23	198.19.10.130

You can scroll the slider to the right to see the **Authentication Source**, **Zero Trust Application**, and **Zero Trust Application Policy**.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.