Zero Trust Network Access

The following topics provide more information about Clientless Zero Trust Network Access, Universal Zero Trust Network Access, and how to configure and deploy them.

About Clientless and Universal Zero Trust Network Access

Zero Trust Access or Zero Trust Network Access (ZTNA) refers to processes that protect internal resources using identity-based access, including user trust and posture. It can provide intrusion protection, file, and malware protection.

Zero Trust Network Access can be of these types:

- *Clientless Zero Trust Network Access* (Clientless ZTNA) enables you to authenticate and authorize access to protected web based resources and applications from inside (on-premises) or outside (remote) the network using an external Security Assertion Markup Language (SAML) identity provider (IdP) policy. Use clientless ZTNA for remote users.
- *Universal Zero Trust Network Access* (Universal ZTNA) provides identity-based network protection and can be used with both remote and on-premises users. On-premises users access a trusted network using a Secure Firewall Threat Defense while remote users install an application such as Cisco Secure Client.

Zero Trust Access

Clientless Zero Trust Network Access is based on Zero Trust Access principles. Zero Trust Access 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.

Clientless Zero Trust Network Access enables you to authenticate and authorize access to protected web-based resources and applications from inside (on-premises) or outside (remote) the network using an external Security Assertion Markup Language (SAML) identity provider (IdP) policy.

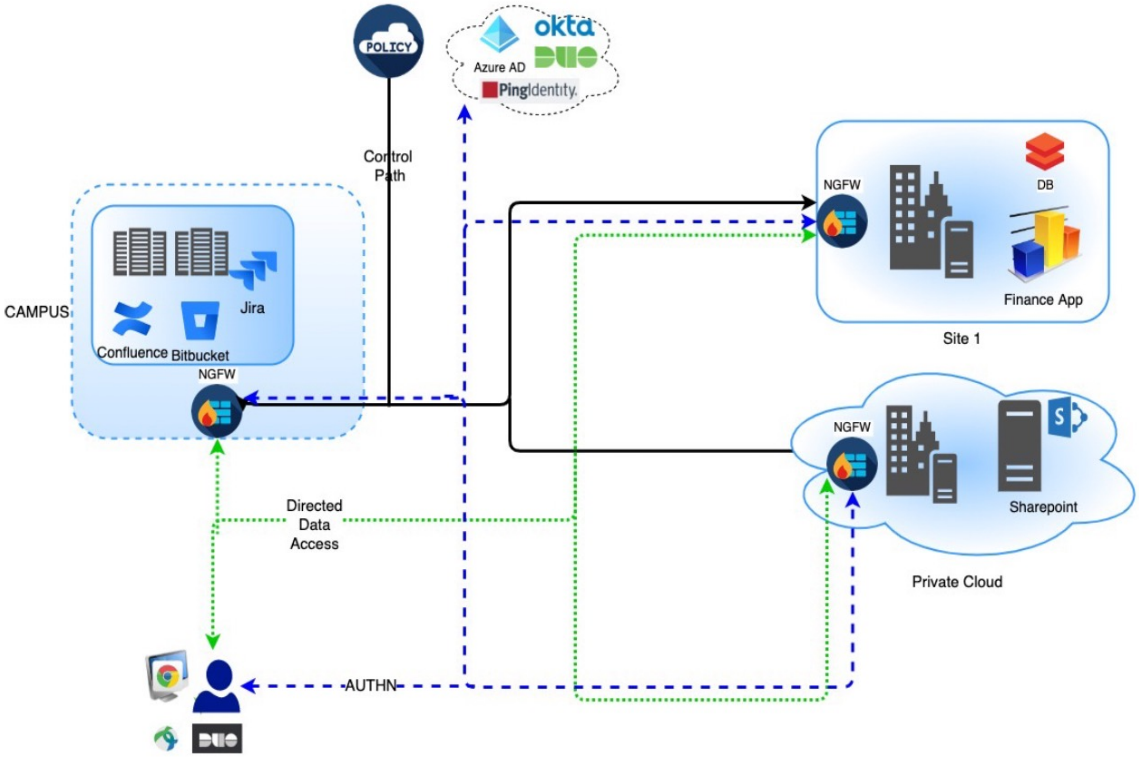
The features are:

- Supports multiple SAML-based identity providers such as Duo, Azure Active Directory (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.
- Access and authentication is through the browser.
- Supports only TLS web applications.
- 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 protection on a set of applications.
- Leverages threat defense intrusion and malware protection on zero trust application traffic.

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.

How Threat Defense Works with Zero Trust Access

Figure 1: Threat Defense Deployment



1. Using a browser, a remote or on-prem user sends a HTTPS request to connect to an application from an endpoint.
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-premises 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 Clientless Zero Trust Network 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 Firewall Threat Defense to masquerade as the applications.Firewall 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 Firewall Threat Defense.

- **IdP Certificate**—The IdP provides a certificate for each defined Application or Application Group. This certificate must be configured so that Firewall 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.

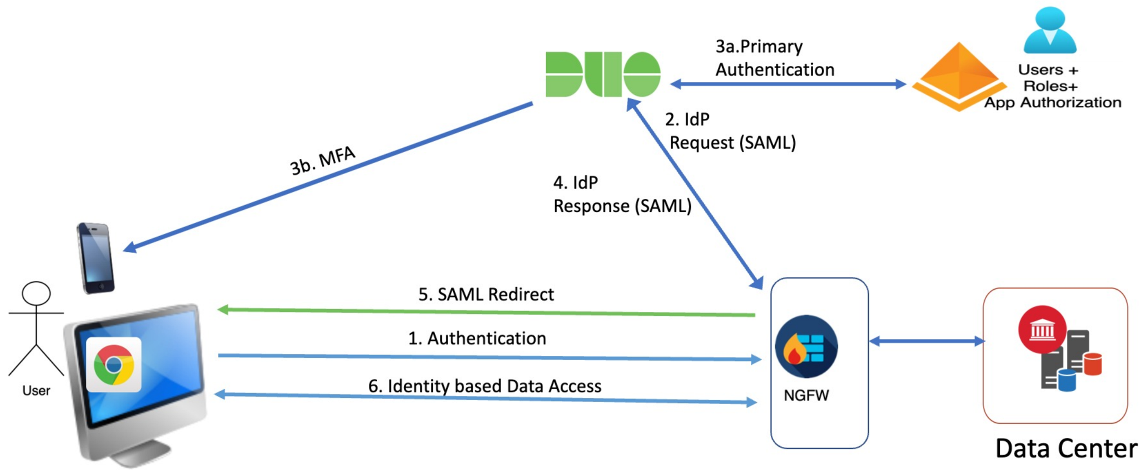
- **Application Certificate**—The encrypted traffic from user to the application is decrypted by Firewall Threat Defense using this certificate for the purpose of inspection.

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.

Clientless Zero Trust Network Access Workflow

This figure depicts the Zero Trust Access workflow.

Figure 2: Clientless Zero Trust Network 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 Clientless Zero Trust Network Access

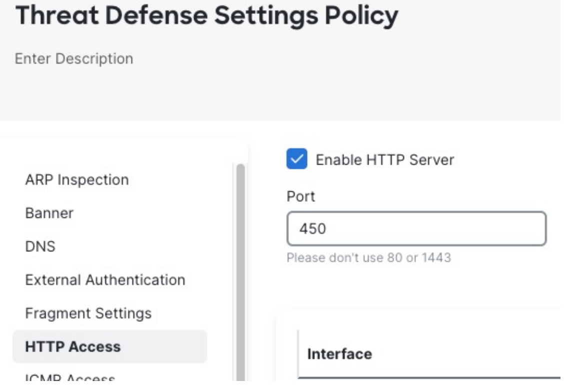
- Supports only TLS-enabled web applications. All traffic must be decrypted.
- Supports only SAML identity providers.
- IPv6 is not supported.

  NAT66, NAT64, and NAT46 scenarios are not supported.
- Supports IPv6; however, you can use only homogeneous network address translations (NAT) scenarios such as NAT66 and NAT44.

  NAT64, and NAT46 scenarios are not supported.
- Clientless zero trust network access is available on Firewall Threat Defense only if Snort 3 is enabled.
- By default, the Firewall Threat Defense device uses port 443 for secure communications. Because this is the same port used by TLS-enabled applications likely to be configured for zero trust network access, you must change the device's HTTP server port.

  Go to **Devices** > **Platform Settings**, then edit the Threat Defense Settings policy for the device, click **HTTP Access**, select the **Enable HTTP Server** check box, and enter a port other than 443 in the field. When you're finished, click **Save** in the upper right corner of the page.

  The following figure shows an example.



Threat Defense Settings Policy

Enter Description

☑ Enable HTTP Server

Port

450

Please don't use 80 or 1443

- 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 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	• 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** > **Zero Trust Application**

Step 2 Manage the zero trust access policies:

- Create—Click **New Policy**. See Create a Zero Trust Application Policy, on page 8
- Edit—Click **Edit** (✎). See Edit a Zero Trust Application Policy, on page 13
- 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 tasks 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 7.

Procedure

Step 1 Choose **Policies** > **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 Firewall 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.

If you select an ACME certificate as the policy's identity certificate in the next step, the domain name must match the common name (CN) of the ACME certificate.

Note
When you change the domain name, the SAML Service Provider (SP) metadata gets updated. You must reconfigure the following settings:

- IdP with the new SAML SP metadata
- DNS server with new domain name

When a deployment takes place after the domain name change, all the applications will be removed and readded, interrupting application access.

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.

You can choose an ACME certificate for authenticating the Firewall Threat Defense device as a SAML SP for a Zero Trust Application policy. ACME certificates automate the lifecycle management of SSL and TLS certificates, including their auto-renewal.

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 9.
2. Create an Application. See Create an Application, on page 10.
3. Associate a Zero Trust Application Policy with a device. See Set Targeted Devices for Zero Trust Access Policy, on page 13
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 8

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 10.
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 8.
2. Create an Application Group, on page 9 (required only for Grouped Applications).

Procedure

Step 1 Choose **Policies** > **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 Threat Defense uses an internal DNS, the Application URL must match an entry within that DNS to ensure it resolves to the application. In addition, if you enter a fully qualified domain name (FQDN) that could have either an IPv4 or IPv6 address, the FQDN must resolve to both IPv4 and IPv6. Threat Defense does not translate between these types of addresses.
- **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.
- **Source Network Address Translation**—Source Network Address Translation (source NAT) translates the source IP address in a packet to an address from a specified range.

  Enable **Source Network Address Translation** to specify an IP address range. The source IP address of an incoming request is translated to an IP address from the specified range. Source NAT works for both IPv4 and IPv6 addresses.

  - **IPv4**—Choose the source network for NAT from the list. Click **Add** (+) to create a network object. For more information, see Network.
  - **IPv6**—Choose the source network for NAT from the list. Click **Add** (+) to create a network object. For more information, see Network.

  Source NAT translates the source IP address of an incoming request to a routable IP address specified in the network object or the object group.

  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 9.

  Note
  This field is not applicable for an ungrouped application.

Step 5 Click **Next**.

Step 6 Depending on the type of application:

- 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**, **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**—If 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 enabled by default.

What to do next

1. Set Targeted Devices for Zero Trust Access Policy, on page 13.
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 8.
2. Create an Application Group, on page 9.
3. Create an Application, on page 10.

Procedure

Step 1 Choose **Policies** > **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** > **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. Click 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 are displayed, click the **x** icon in any column name to display a field selector.
4. Select the following fields:
   - **Authentication Source**
   - **Zero Trust Application**
   - **Zero Trust Application Group**
   - **Zero Trust Application Host**
   - **Zero Trust Application Policy**
   - **Zero Trust Origin User**
   - **Zero Trust Proxy**
   - **Zero Trust Rule**
   - **Zero Trust Status**
   - **Zero Trust Tunnel ID**
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 heading** > **Dashboard**, and click the **Zero Trust** tab 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 running-config zero-trust-hybrid	To view the running configuration for a universal 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.

Universal Zero Trust Network Access

Universal Zero Trust Network Access (universal ZTNA) enables administrators to specifically allow access to internal network resources according to user identity including user trust and posture, without granting access to the entire network as with Remote Access VPN. Universal ZTNA is a client-based ZTNA solution that enables users to securely access internal resources and applications regardless of their location, whether remote or on-premises.

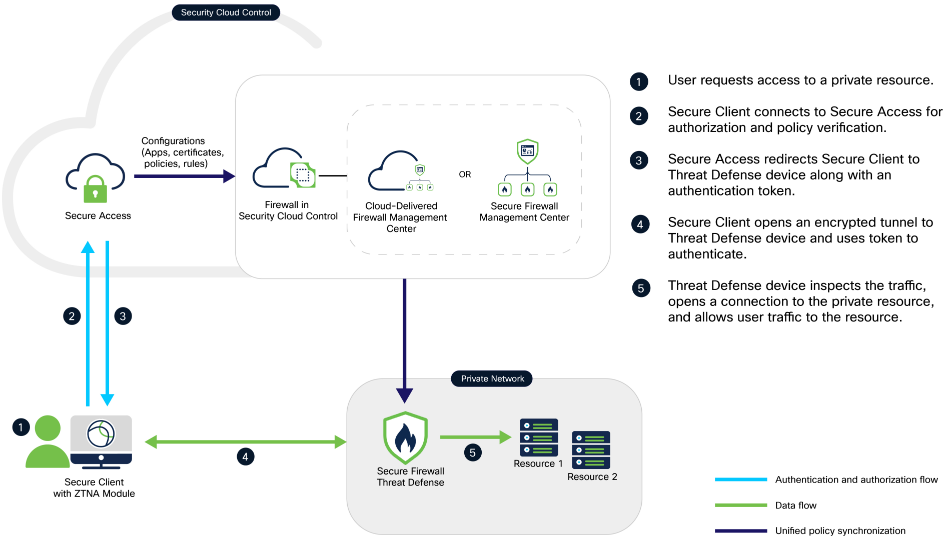
Because universal ZTNA does not assume that access granted to one application implicitly authorizes access to other applications, the network attack surface is reduced.

Universal ZTNA ensures least-privileged, per-application, per-user access with strong authentication, posture validation, and comprehensive traffic inspection. It secures applications effectively across hybrid environments.

Components of Universal ZTNA

A new configuration of universal ZTNA consists of Security Cloud Control Firewall Management (formerly called Cisco Defense Orchestrator), and Secure Access, both provisioned on the Security Cloud Control platform. Security Cloud Control Firewall Management manages the Firewall Threat Defense devices through the Secure Firewall Management Center.

Figure 3: Components of Universal ZTNA


Security Cloud Control
Configurations (Apps, certificates, policies, rules)
Secure Access
Firewall in Security Cloud Control
Cloud-Delivered Firewall Management Center
OR
Secure Firewall Management Center
2
3
1
Secure Client with ZTNA Module
4
Private Network
Secure Firewall Threat Defense
5
Resource 1
Resource 2
Authentication and authorization flow
Data flow
Unified policy synchronization

1 User requests access to a private resource.

2 Secure Client connects to Secure Access for authorization and policy verification.

3 Secure Access redirects Secure Client to Threat Defense device along with an authentication token.

4 Secure Client opens an encrypted tunnel to Threat Defense device and uses token to authenticate.

5 Threat Defense device inspects the traffic, opens a connection to the private resource, and allows user traffic to the resource.

- **Security Cloud Control Firewall Management**: Manages the configuration and deployment of universal ZTNA policies to the Firewall Threat Defense devices. The Threat Defense devices protect on-premises resources by enforcing universal ZTNA policies. Threat Defense inspects traffic and enforces intrusion prevention system (IPS), file, and malware policies on the traffic.
- **Secure Access**: Secure Access defines the access policies, posture, and security profiles for the user. It enforces the policies for user traffic through the cloud.
- **Security Cloud Control platform**: Security Cloud Control provides a unified secure management plane for both Secure Access and Firewall, simplifying the administration of universal ZTNA policies across them.
- **Secure Client**: The Secure Client is installed on the end user's device. It acts as the enforcement point that intercepts connection requests to protected internal resources, enabling secure, identity-based access.

The following sections describe how to enable universal ZTNA on a Threat Defense device. For the complete configuration of universal ZTNA, refer to the *Universal Zero Trust Network Access Configuration Guide*.

How Threat Defense Works with Universal ZTNA

A universal ZTNA-enabled Firewall Threat Defense device is a critical enforcement point that protects private resources by integrating zero trust principles with firewall capabilities. Here’s how it operates to secure private resources:

- **Enforces access and Validates Policy**: A Threat Defense device intercepts all access requests to private resources. It enforces granular, context-aware access policies that verify user identity, device posture, and contextual factors before granting access. Only requests that meet the least-privilege criteria are allowed, blocking the unauthorized attempts to access resources.
- **Establishes a Secure Tunnel to the Resource**: After validating the access policy, the Threat Defense device establishes a secure, encrypted tunnel between the user’s device and the private resource. This tunnel ensures that private resources are isolated from direct network exposure.

- **Inspects Traffic**: Threat Defense device continuously inspects the traffic and blocks threats before they reach the resources. The device applies the intrusion prevention system, file, and malware detection capabilities to detect and block the threats.
- **Microsegments and Prevents Lateral Movement**: The device enforces microsegmentation by restricting traffic flows to only the authorized resources. This containment prevents lateral movement within the network, limiting the impact of any potential breach.

Prerequisites for Universal Zero Trust Network Access

This topic discusses requirements and guidelines for Universal Zero Trust Network Access (universal ZTNA).

Licensing Requirements

- Secure Firewall Management Center requires a smart license account with export-controlled features. It does not function in evaluation mode for universal ZTNA.

  Secure Firewall Threat Defense devices require an IPS license if Intrusion policy is configured. If Malware policies are configured, the devices require IPS and Malware Defense licenses. For more information, refer to the "Licenses" section in the *Cisco Secure Firewall Management Center Administration Guide*.
- Secure Access requires a subscription of Cisco Secure Private Access Essentials or Advantage.

Device Requirements

- All Secure Firewall Management Center and Secure Firewall Threat Defense devices must be running Version 7.7.10 or later.
- All Secure Firewall Threat Defense devices must be configured for routed mode; transparent mode is not supported.
- In Security Cloud Control, when you are configuring universal zero trust access for a device, ensure that the Enrollment Type for the device identity certificate is an object that is created using the PKCS12 file format. No other certificate type is supported. If necessary, you can also create a new certificate object from Security Cloud Control, which supports the PKCS12 format. See Configure Security Devices.
- Configure the Domain Name System (DNS) to resolve Fully Qualified Domain Name (FQDN) of private resources. Use the Platform Settings menu on the Secure Firewall to configure the DNS. See Interface and Device Settings.
- High Availability (HA) devices *are* supported; they are displayed as one entity.
- Secure Client (with ZTNA module enabled) Version 5.1.10 and later is supported.

  The client must be running in a platform that supports Trusted Platform Module (TPM), such as Windows 11.

Guidelines on Certificate Types

- **User Identity Certificate**: Secure Client, which is zero trust access enabled, presents the user identity certificate during the Mutual Transport Layer Security (mTLS) session with Secure Access and Firewall Threat Defense to request access to private resources.

- **Firewall Threat Defense Device Certificate**: Threat Defense devices that are universal ZTNA-enabled use device certificates to establish secure mTLS connections with the Secure Client and Secure Access. Ensure that the device identity certificate is of type PKCS12.

  If you have already enrolled a manual certificate for the device, first export it to the PKCS12 format using the **Devices** > **Certificates** > **Export Certificate** menu on Firewall Management Center. Use the exported PKCS12 file to create a new PKCS12 certificate enrollment object.

- **Decryption Certificate**: (Optional) To decrypt the traffic that is sent to private resources, enable **Decryption** for the resources in Secure Access and provide the server certificate and key. We recommend that you use a certificate that is signed by a publicly recognized certificate authority (CA).

Supported Devices

Both on-premises Firewall Management Center and cloud-delivered Firewall Management Center can be configured to manage the devices.

Only devices that have 16 cores or more are supported. Such models of Secure Firewall Threat Defense are:

- 1150
- 3105, 3110, 3120, 3130, 3140
- 4115, 4125, 4145, 4112
- 4215, 4225, 4245
- FTDv

Note You can configure universal ZTNA on a 16 core FTDv. No other deployment configuration of FTDv supports universal ZTNA.

Limitations of Universal Zero Trust Network Access

- Universal ZTNA does not support IPv6.
- Universal ZTNA-enabled devices do not enforce policies for traffic over a site-to-site tunnel.
- Universal ZTNA does not support clustered devices.
- Universal ZTNA does not support devices in multi-instance mode.
- Universal ZTNA sessions do not support jumbo frames.
- Universal ZTNA supports only global VRF.
- Universal ZTNA does not support protocols such as FTP or TFP, where the data or secondary connection originates from a server.

  For example, an active FTP connection uses a persistent control connection for commands and creates temporary data connections for file transfers. Universal ZTNA does not support such data connections that originate from the server.

Enable Cloud-Delivered Firewall Management Center in Security Cloud Control

To configure universal ZTNA, first enable the cloud-delivered Firewall Management Center in Cisco Security Cloud Control. After you enable it, configure the associated Secure Firewall Threat Defense devices. The devices can then use the networks, private resources, and policies needed to configure and manage universal ZTNA.

Procedure

Step 1 From the Security Cloud Control menu, click **Administration** > **Integrations** > **Firewall Management Center**.

Step 2 Click **Enable Cloud-Delivered FMC**.

Security Cloud Control starts provisioning the instance. This process takes a few minutes to complete. You can track the progress in the **Status** column of **Cloud-Delivered FMC**.

After the provisioning is complete, the status changes to **Active**.

What to do next

Onboard the Firewall Threat Defense devices to the cloud-delivered Firewall Management Center. To learn how to onboard a Threat Defense device, see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center

Configure Security Devices

All Firewall Threat Defense devices associated with the Secure Firewall Management Center that you onboarded to Security Cloud Control are *security devices* to which you can:

- Associate private resources, which are internal applications you want to protect with identity-based access control, IPS, malware, and other protections.
- Deploy Secure Access access rules. Security devices are responsible for enforcing access rules for on-premises users, remote users, or both.

Perform these steps to enable **universal zero trust network access settings** on the Threat Defense devices. These steps include configuring the device FQDN, inside interface, outside interface, and PKCS12 certificate to enable universal ZTNA on the devices.

Before you begin

You must know the name of each device's internal and external network interfaces:

- The internal interface (also referred to as the *DMZ* interface) is used to apply access rules to on-premises users.
- The external interface is used to apply access rules to remote users.

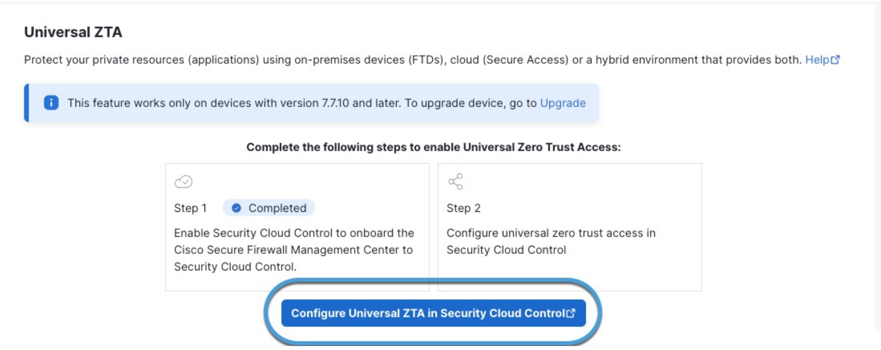
You can choose internal, external, or both types of interfaces for each security device.

Procedure

Step 1 In the Secure Firewall Management Center, click **Policies** > **Zero Trust Application**.

Step 2 Click **Configure Universal ZTA in Security Cloud Control**.

This figure shows an example.



Universal ZTA

Protect your private resources (applications) using on-premises devices (FTDs), cloud (Secure Access) or a hybrid environment that provides both. Help

This feature works only on devices with version 7.7.10 and later. To upgrade device, go to Upgrade

Complete the following steps to enable Universal Zero Trust Access:

Step 1 Completed

Enable Security Cloud Control to onboard the Cisco Secure Firewall Management Center to Security Cloud Control.

Step 2

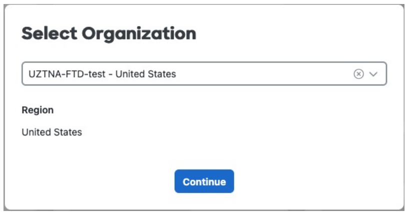
Configure universal zero trust access in Security Cloud Control

Step 3 When prompted, log in to Security Cloud Control.

Step 4 When prompted, select your organization from the drop-down list and click **Continue**.

Select an organization that has both Secure Access and Secure Firewall micro applications configured.

This figure shows an example.



Select Organization

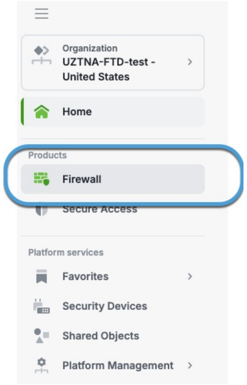
UZTNA-FTD-test - United States

Region

United States

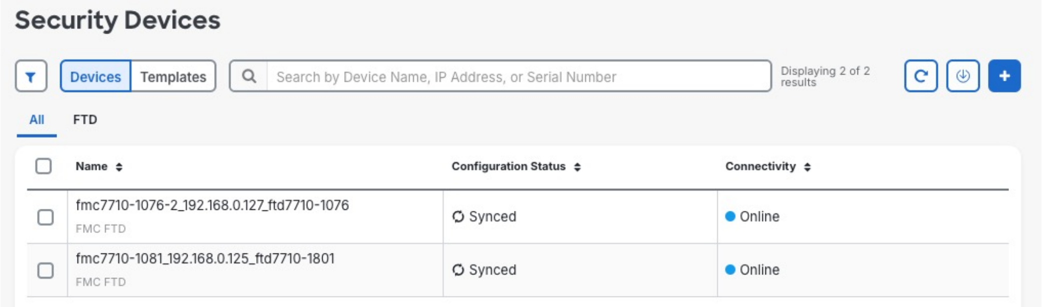
Step 5 In Security Cloud Control, in the Products section, click **Firewall**.

This figure shows an example.



Step 6 In the Manage section, click **Security Devices**.

The **Security Devices** page displays the available security devices.



Security Devices

Devices | Templates | Search by Device Name, IP Address, or Serial Number | Displaying 2 of 2 results

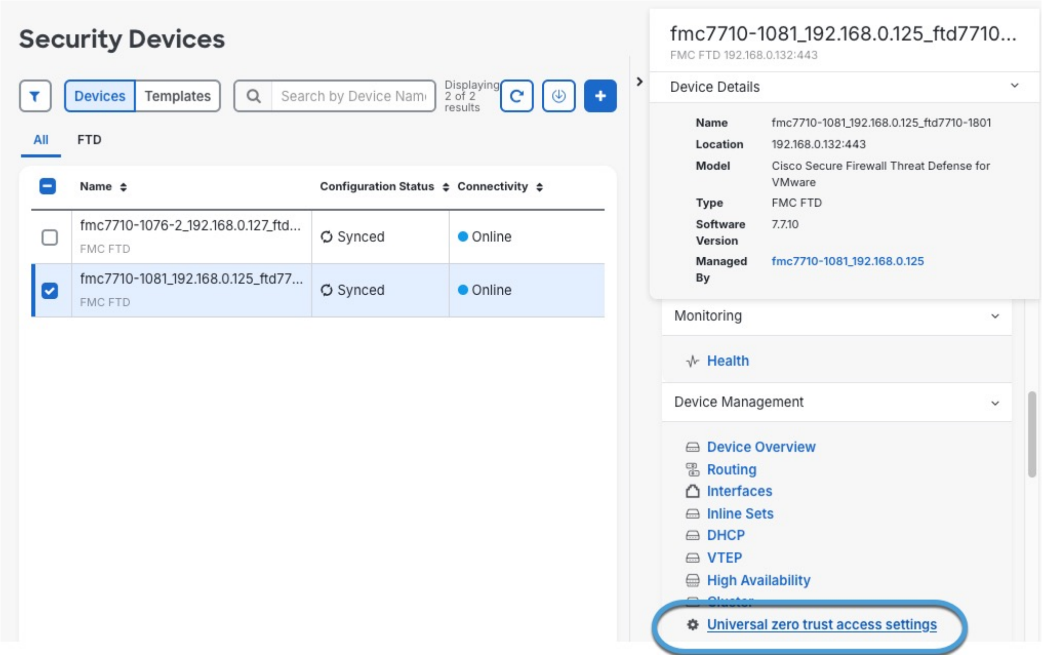
All | FTD

☐	Name	Configuration Status	Connectivity
☐	fmc7710-1076-2_192.168.0.127_ftd7710-1076 FMC FTD	Synced	● Online
☐	fmc7710-1081_192.168.0.125_ftd7710-1801 FMC FTD	Synced	● Online

Step 7 Select the check box next to a device to add to the universal zero trust network access configuration.

Step 8 In the right pane, click **Device Management** > **Universal zero trust access settings**.

This figure shows an example.



Security Devices

Devices | Templates | Search by Device Name | Displaying 2 of 2 results

All | FTD

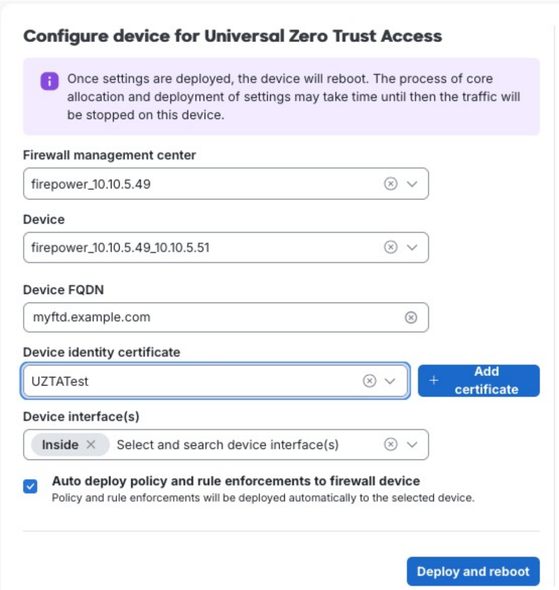
☐	Name	Configuration Status	Connectivity
☐	fmc7710-1076-2_192.168.0.127_ftd... FMC FTD	Synced	● Online
☑	fmc7710-1081_192.168.0.125_ftd77... FMC FTD	Synced	● Online

fmc7710-1081_192.168.0.125_ftd7710...
FMC FTD 192.168.0.132:443

Device Details

Name	fmc7710-1081_192.168.0.125_ftd7710-1801
Location	192.168.0.132:443
Model	Cisco Secure Firewall Threat Defense for VMware
Type	FMC FTD
Software Version	7.7.10
Managed By	fmc7710-1081_192.168.0.125

Step 9 Enter or edit the following information on the **Configure device for Universal Zero Trust Access** page.



Configure device for Universal Zero Trust Access

Once settings are deployed, the device will reboot. The process of core allocation and deployment of settings may take time until then the traffic will be stopped on this device.

Firewall management center: firepower_10.10.5.49

Device: firepower_10.10.5.49_10.10.5.51

Device FQDN: myftd.example.com

Device identity certificate: UZTATest

Device interface(s): Inside × Select and search device interface(s)

☑ Auto deploy policy and rule enforcements to firewall device
Policy and rule enforcements will be deployed automatically to the selected device.

This table describes the configurations to enable universal ZTNA on the device.

Item	Description
Firewall management center	From the drop-down list, click the name of a Secure Firewall Management Center to use for policy deployment, monitoring, and other tasks.
Device	From the drop-down list, click the name of a device to use for rule deployment and enforcement.
Device FQDN	Enter the security device's fully qualified domain name (FQDN). The FQDN is also referred to as the TLS/SSL certificate's Common Name. Secure Access redirects the clients to the resource that is represented by this FQDN. Ensure that the device FQDN *exactly matches* the Common Name (CN) of the device identity certificate and must also match a Subject Alternative Name (SAN) in the certificate.

Item	Description
Device identity certificate	The **Device identity certificate** must have a Common Name that: - *Exactly matches* the value you enter in the **Device FQDN** field. - Matches a Subject Alternative Name (SAN) in the certificate. From the drop-down list, click the name of an existing identity certificate from the list. Click **Add certificate** and add an identity certificate in **.p12** format (also referred to as PKCS#12; see this article on ssl.com). **Note** Universal ZTNA supports only the PKCS#12 format of certificate enrollment. In the provided fields, enter a **Name** to identify the certificate. Then copy/paste, drag/drop, or upload the certificate and private key. If the certificate is encrypted, enter its password in the provided field. You can optionally use a wildcard certificate as discussed in What is a Wildcard Certificate? on ssl.com.
Device Interface(s)	From the drop-down list, select the check box next to any of the following types of interfaces. - Internal network interface (or DMZ): deploys access rules for on-premises users only. - External network interface: deploys access rules for remote users only. - Both types of interfaces: deploys access rules for either on-premises or remote users.
Auto deploy policy and rule enforcements to firewall device	Select the check box to automatically deploy access rules to the device after they are updated on Secure Access. On the device, the Auto deploy feature selectively deploys only the Universal ZTNA access policy. It does not impact other changes or configurations on the Firewall Management Center. **Note** If there are other interdependent policies on the device (which are interlinked with the Universal ZTNA access policy), the Firewall configuration status displays an error message. The deployment then stops. In such cases, you should manually deploy the Universal ZTNA access policy from the Firewall Management Center.

Step 10 Click **Deploy and Reboot**.

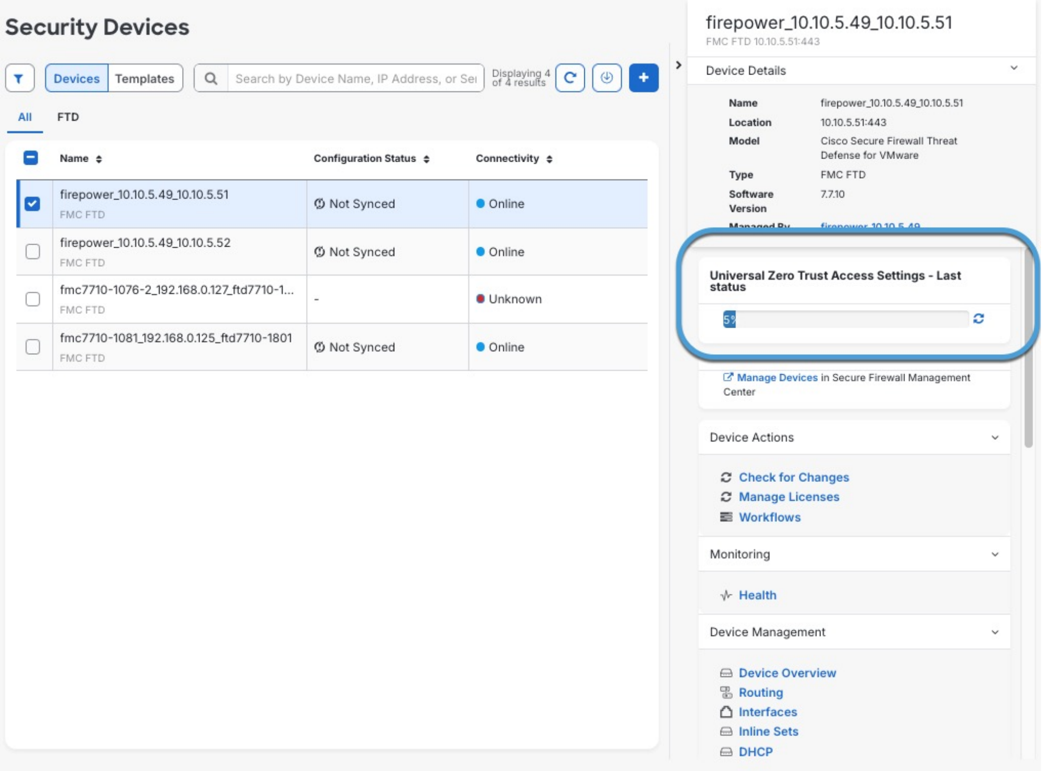
The device reboots to reallocate the system resources for universal ZTNA components.

Note
The device takes several minutes to reboot, during which time all traffic handled by the device is disrupted.

If you deploy a High Availability (HA) pair of devices, both devices reboot simultaneously.

Step 11 On the **Security Devices** page, select the check box next to the device to which you just deployed the Universal ZTNA configuration.

The right pane displays the deployment status, as shown in the figure.



Security Devices

Devices
Templates
Search by Device Name, IP Address, or Sei
Displaying 4 of 4 results
All
FTD

☐	Name	Configuration Status	Connectivity
☑	firepower_10.10.5.49_10.10.5.51 FMC FTD	Not Synced	● Online
☐	firepower_10.10.5.49_10.10.5.52 FMC FTD	Not Synced	● Online
☐	fmc7710-1076-2_192.168.0.127_ftd7710-1... FMC FTD	-	● Unknown
☐	fmc7710-1081_192.168.0.125_ftd7710-1801 FMC FTD	Not Synced	● Online

firepower_10.10.5.49_10.10.5.51
FMC FTD 10.10.5.51:443

Device Details

Name	firepower_10.10.5.49_10.10.5.51
Location	10.10.5.51:443
Model	Cisco Secure Firewall Threat Defense for VMware
Type	FMC FTD
Software Version	7.7.10
Managed By	firepower_10.10.5.49

Universal Zero Trust Access Settings - Last status

5%

Manage Devices in Secure Firewall Management Center

For additional information, click **Device Actions** > **Workflows** in the right pane.

After the deployment completes, you can view the completion status in the **Universal Zero trust Access Settings - Last status** tab for the device.

Universal ZTNA-enabled Firewall Threat Defense device is connected to Secure Access.

What to do next

Check the availability of the Threat Defense device under Secure Access by clicking **Security Cloud Control** > **Secure Access** > **Connect** > **Network Connections** > **FTD**.