

Universal Zero Trust Network Access Configuration Guide

First Published: 2025-08-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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)

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Universal Zero Trust Network Access** 1

Overview of Universal Zero Trust Network Access 1

Prerequisites for Universal Zero Trust Network Access 2

Limitations of Universal Zero Trust Network Access 4

Configuration Workflow for Universal ZTNA 4

CHAPTER 2 **Configure Security Cloud Control Firewall Management** 7

Onboard Applications in Security Cloud Control 7

Set Up Firewall Threat Defense Devices 7

Integrate Firewall Management Center with Security Cloud Control 9

Security Cloud Control Settings 12

Configure Security Devices 13

CHAPTER 3 **Configure Secure Access** 19

Configure Private Resources 19

Configure Universal ZTNA Access Policies 20

Trusted Network Detection 22

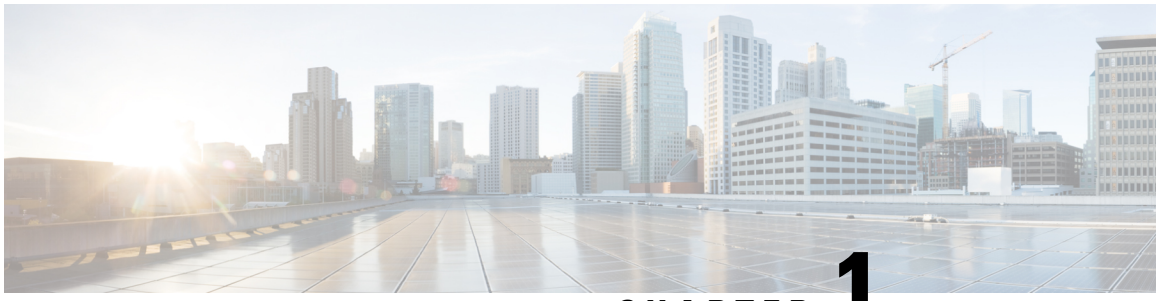
Add a Trusted Network 22

Map a Trusted Network to a Threat Defense Device 25

Associate Private Resources with Firewall Threat Defense 26

CHAPTER 4 **Related Documentation** 33

Related Documentation 33



CHAPTER 1

Universal Zero Trust Network Access

The following topics provide an overview of Universal Zero Trust Network Access (universal ZTNA), including the prerequisites, limitations, and workflow involved in configuring the universal ZTNA solution.

- Overview of Universal Zero Trust Network Access, on page 1
- Prerequisites for Universal Zero Trust Network Access, on page 2
- Limitations of Universal Zero Trust Network Access, on page 4
- Configuration Workflow for Universal ZTNA, on page 4

Overview of 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.

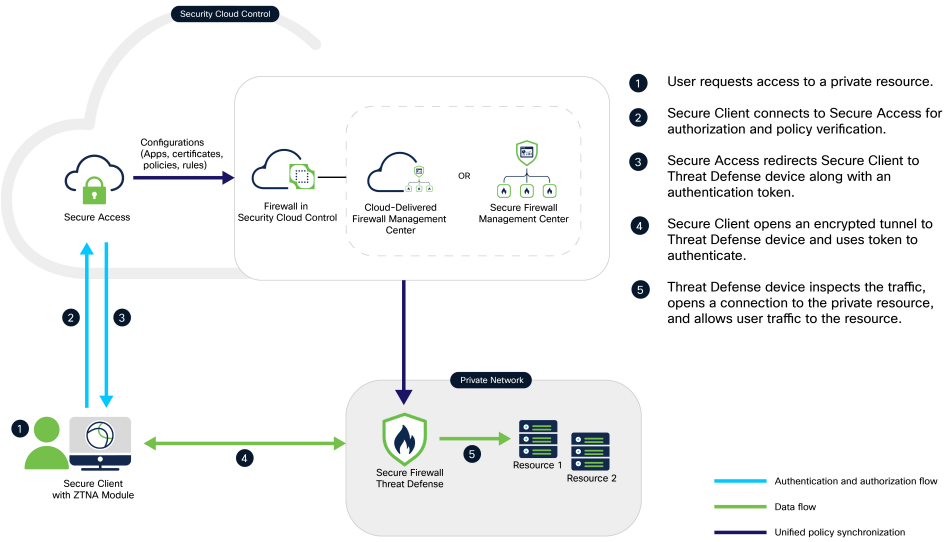
Because universal ZTNA does not assume that access granted to one application implicitly authorizes access to other applications, the network attack surface is reduced.

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 1: Components of Universal ZTNA



- **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.

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 Device 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

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.
- Currently, universal ZTNA supports only the United States and Europe regions.
- 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.

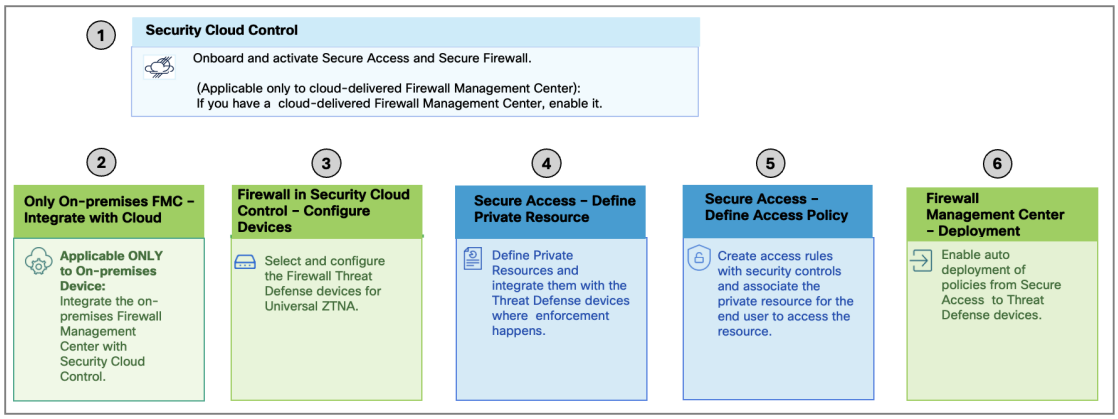
Configuration Workflow for Universal ZTNA

As an administrator, you set up the infrastructure, configure policies, deploy policies at the enforcement point, and monitor the solution to ensure it works as expected. These tasks can be classified by the product used:

- Configure Security Cloud Control Firewall Management, which includes setting up the Threat Defense devices with their Management Center.
- Configure Secure Access, which includes private resources, access policies, and network connections.

The steps described in the figure provide a high-level overview of the universal ZTNA configuration process. For detailed instructions, see the specific tasks.

Figure 2: Configuration Workflow for Universal ZTNA



Workflow

1. Onboard Secure Access and Security Cloud Control Firewall Management to the Security Cloud Control platform.

   See Onboard Applications in Security Cloud Control.

2. Prepare and set up Firewall Management Center and Firewall Threat Defense devices to enable universal ZTNA.

   See Set Up Firewall Threat Defense Devices.

3. Configure the Firewall Threat Defense devices.

   Enable **universal zero trust network access settings** for the Firewall Threat Defense device and ensure that the Threat Defense device is visible in Secure Access.

   See Configure Security Devices.

4. Configure private resources.

   Private resources include applications, networks, or subnets that your organization controls.

   In Secure Access, configure private resources to specify the connection information for the resources.

   See Configure Private Resources.

5. Define the access policies for user traffic.

   In Secure Access, add private access rules to control access and enforce security for private resources in the organization. The access rules determine which users and devices can access the resource using the connection methods you have enabled.

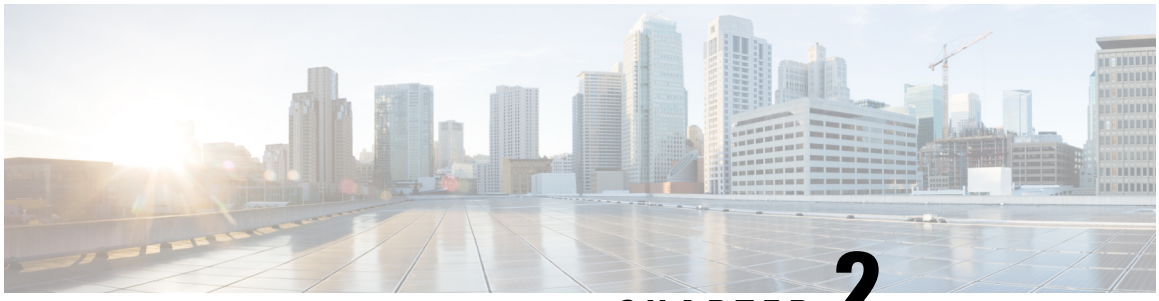
   See Configure Universal ZTNA Access Policies.

6. Deploy the configurations to the Firewall Threat Defense Device.

   In Secure Access, associate the private resources to the Threat Defense device and ensure that all configurations are synchronized with the Threat Defense device.

   See Associate Private Resources to Threat Defense Device.

Note that after you provision the applications in Security Cloud Control (Step 1 and Step 2), you can use the **Secure Access** > **Workflows** > **Set up hybrid private access** workflow to continue with the universal ZTNA configuration process.



CHAPTER 2

Configure Security Cloud Control Firewall Management

Firewall Threat Defense serves as the local enforcement point for on-premises user traffic. The Security Cloud Control Firewall Management manages the configuration and deployment of universal ZTNA policies to Threat Defense devices through the Firewall Management Center.

- Onboard Applications in Security Cloud Control, on page 7
- Set Up Firewall Threat Defense Devices, on page 7
- Integrate Firewall Management Center with Security Cloud Control, on page 9
- Configure Security Devices, on page 13

Onboard Applications in Security Cloud Control

The core elements of universal ZTNA are the Security Cloud Control Firewall Management and Secure Access applications. The first step to configuring universal ZTNA is to onboard both these applications to the Security Cloud Control platform.

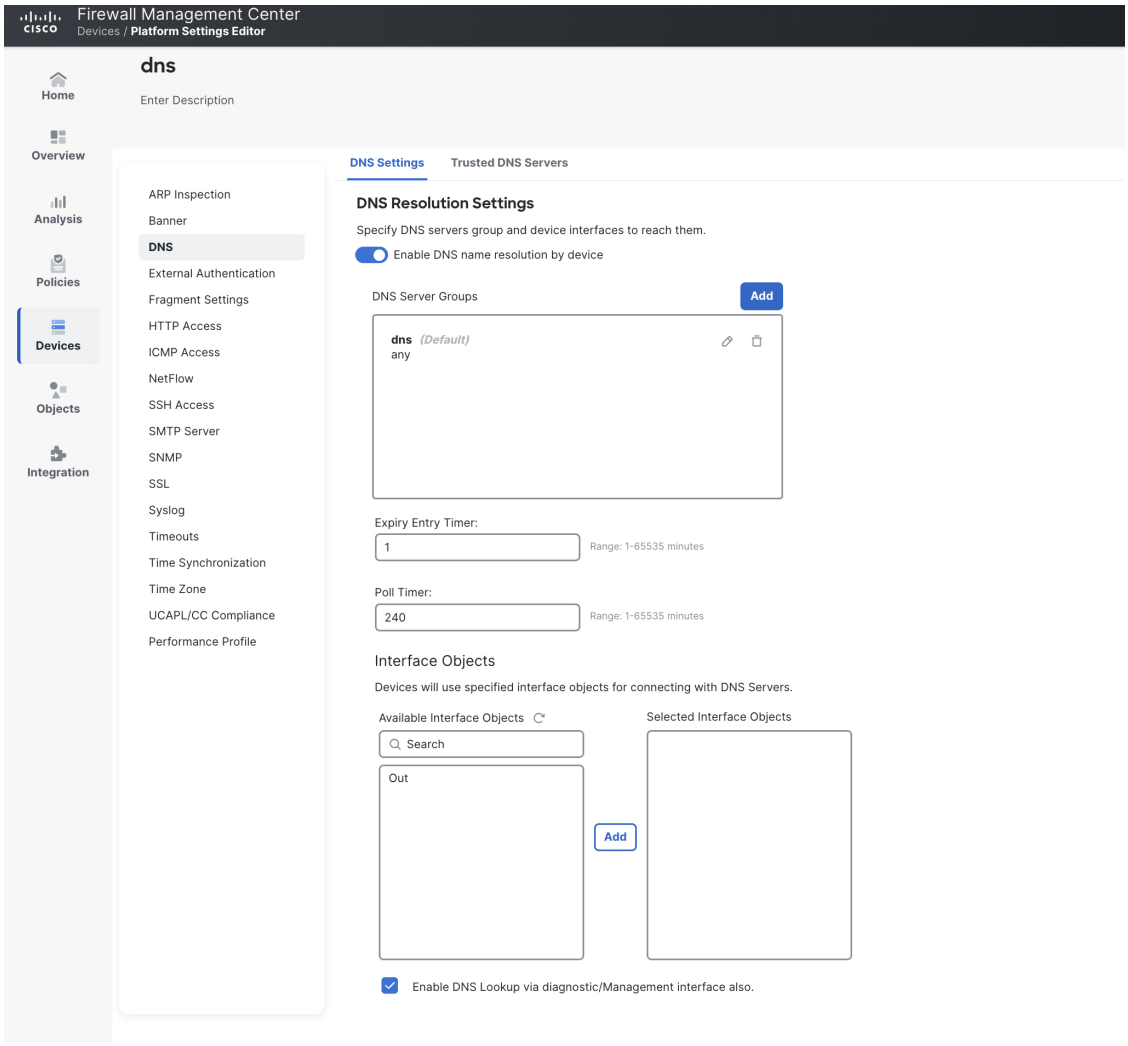
1. If you have purchased a subscription for the products, claim the subscription in Security Cloud Control and activate both the products. For information on claiming a subscription and activating products in Security Cloud Control, see the Security Cloud Control Administration Guide.
2. Configure user management in Secure Access—configure users and groups, either manually or integrate an identity provider.
3. Configure one or more trusted networks through Secure Access. We recommend having one default trusted network. A default trusted network is automatically assigned to a universal ZTNA-enabled Firewall Threat Defense device. Refer to Trusted Network Detection.
4. Update Secure Access with the CA certificate for the universal ZTNA user.

Set Up Firewall Threat Defense Devices

Prepare the Firewall Management Center and Firewall Threat Defense devices for universal ZTNA configuration.

1. Ensure that the Firewall Management Center is registered with a smart license.

2. Specify these configurations for the Threat Defense devices:
   - Routed interfaces to route the traffic.
   - Along with the required platform settings, configure a Domain Name Server (DNS) to resolve the IP address of the internal resources.



3. If you have an on-premises Firewall Management Center, onboard it to Security Cloud Control. See Integrate Firewall Management Center with Security Cloud Control.
4. If you have a cloud-delivered Firewall Management Center, enable it in Security Cloud Control.

Integrate Firewall Management Center with Security Cloud Control

Note This task is applicable only to on-premises Firewall Management Center.

Integrating the on-premises Secure Firewall Management Center with Cisco Security Cloud Control enables you to configure your Secure Firewall Management Center and its associated Secure Firewall Threat Defense devices. These devices can then use the networks, private resources, and policies necessary to configure and manage universal ZTNA.

Note Universal ZTNA uses *only* the access policies that are defined by Secure Access. Any other access control policies and rules deployed to the Threat Defense devices from the Secure Firewall Management Center are ignored for universal ZTNA.

Before you begin

Your Cisco contact must onboard your Cisco Security Cloud Control and Secure Access systems, and create users and tenants.

Also see Prerequisites for Universal Zero Trust Network Access, on page 2.

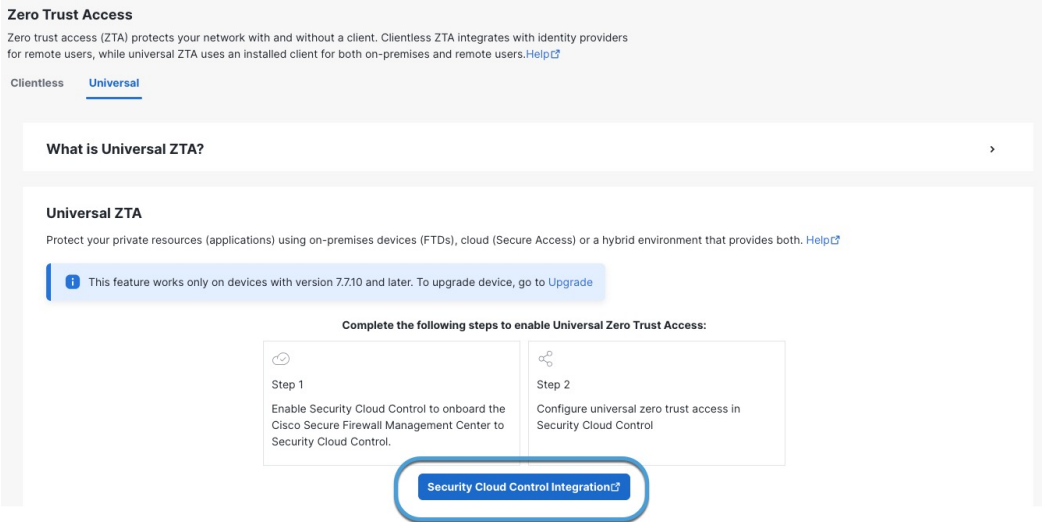
Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Policies** > **Zero Trust Application**.

Step 3 Click the **Universal** tab.

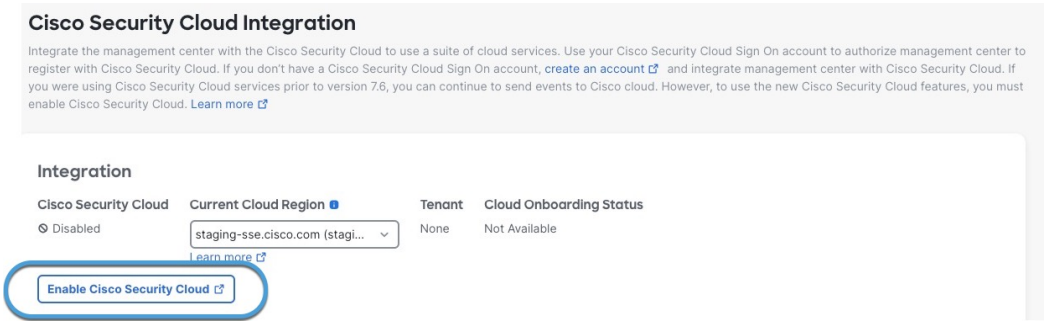
The Zero Trust Access page appears.



Step 4 Click **Security Cloud Control Integration**.

Step 5 From the **Current Cloud Region** list, click the name of your Cisco Security Cloud Control region.

Step 6 Click **Enable Cisco Security Cloud**.

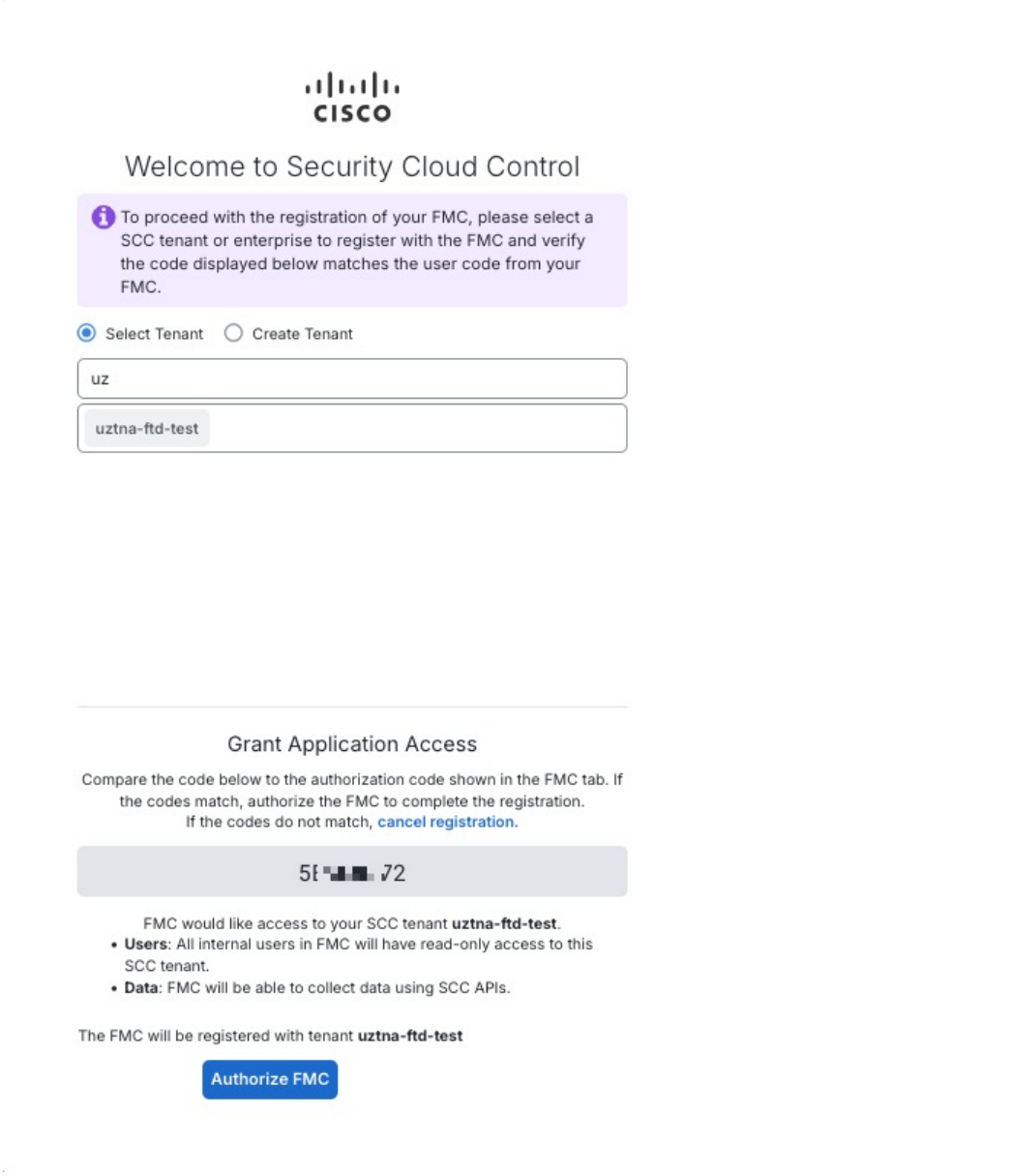


Step 7 When prompted, click **Continue to Cisco SSO**.

Step 8 Log in to Cisco Security Cloud Control.

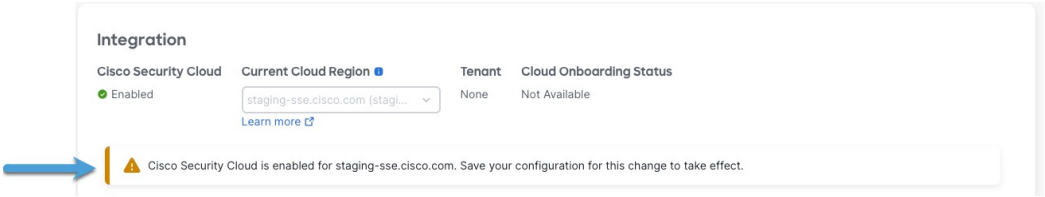
Step 9 From the **Select Tenant** list, click the name of your tenant.

Step 10 At the following page, click **Authorize FMC**.



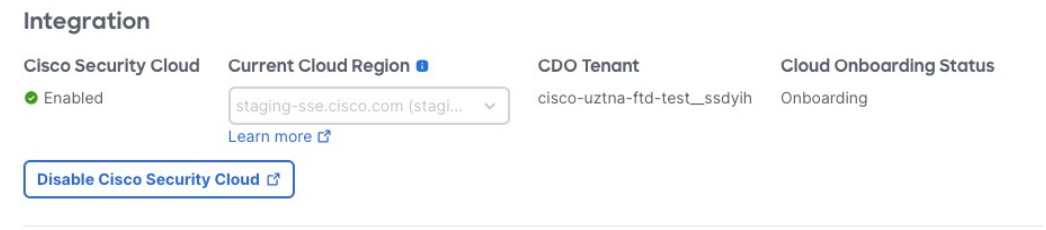
Step 11 When prompted, close the tab page.

Step 12 A confirmation message appears to indicate that the onboarding was successful.



Step 13 Click **Save** at the bottom of the page.

It can take several minutes to save the configuration. After the configuration is saved, the page displays the onboarding status and the tenant name.



Step 14 For more information about other options on this page, see Security Cloud Control Settings, on page 12.

Security Cloud Control Settings

The following topics discuss settings on the Cisco Security Cloud Integration page, which can be reached by choosing **Integration** > **SecureX** on Secure Firewall Management Center.

Event Configuration

Monitor the selected events in Cisco Security Cloud Control:

- **Send events to the cloud**: Select this check box to monitor events in Cisco Security Cloud Control; clear the check box to not monitor any events.

  You can view events in Cisco Security Cloud Control at **Firewall** > **Events & Logs**.
- **Intrusion events**: If you are using IPS policies, select this check box to monitor those policies.
- **File and malware events**: If you are using file or malware policies, select this check box to monitor those policies.
- **Connection events**: Select the check box next to the events to monitor, either **Security** (for file and IPS events) or **All**.

For more information about events, see Event Types in Security Cloud Control.

Cisco Security Cloud Support (Optional)

Optionally, select the check box to enable the following:

- **Enable Cisco Success Network**: Select the check box to enable collection of statistics discussed in *Cisco Success Network Telemetry Data Collected from Cisco Secure Firewall Management Center, Version 7.7*.
- **Enable Cisco Support Diagnostics**: Select the check box to enable collection of statistics discussed in the Cisco Secure Firewall Management Center Administration Guide.

Cisco AI Assistant for Security

Select the check box to enable the AI assistant as discussed in Use Cisco AI Assistant for Security to Manage Your Threat Defense Devices Effectively.

Cisco XDR Automation

Select the check box to enable XDR workflow automation as discussed in the Cisco XDR Help Center.

Policy Analyzer and Optimizer

Select the check box to enable the policy analyzer; click **Learn more** for details.

Zero-Touch Provisioning (ZTP)

Select the check box to enable zero-touch provisioning as discussed in the Cisco Secure Firewall Management Center Administration Guide.

Configure Security Devices

All Firewall Threat Defense devices associated with the Secure Firewall Management Center that you onboarded to Cisco 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.

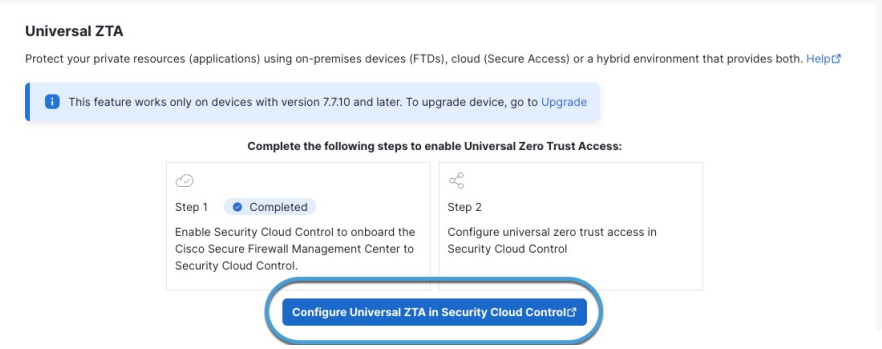
You can choose internal, external, or both types of interfaces for each security device.

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.

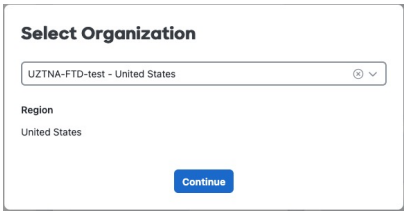


Step 3 When prompted, log in to Cisco Security Cloud Control.

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

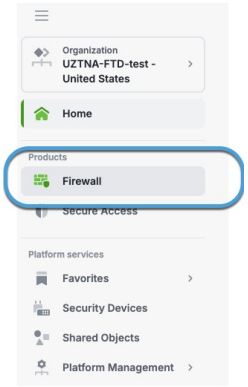
Select an organization that has both Secure Access and Secure Firewall micro applications configured.

This figure shows an example.



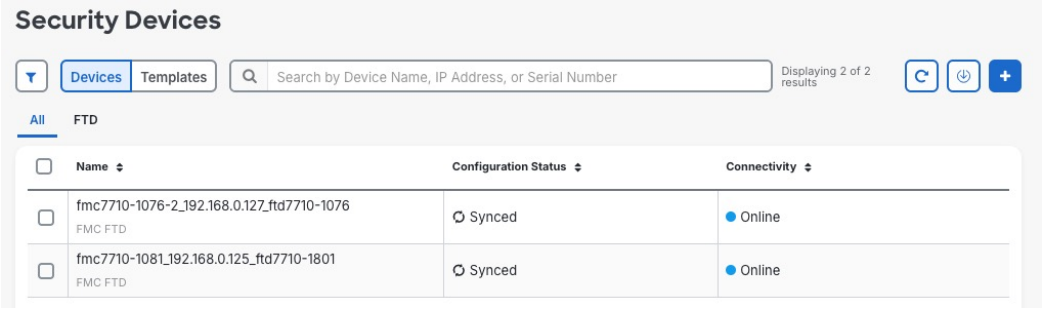
Step 5 In Cisco Security Cloud Control, in the Products section, click **Firewall**.

This figure shows an example.



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

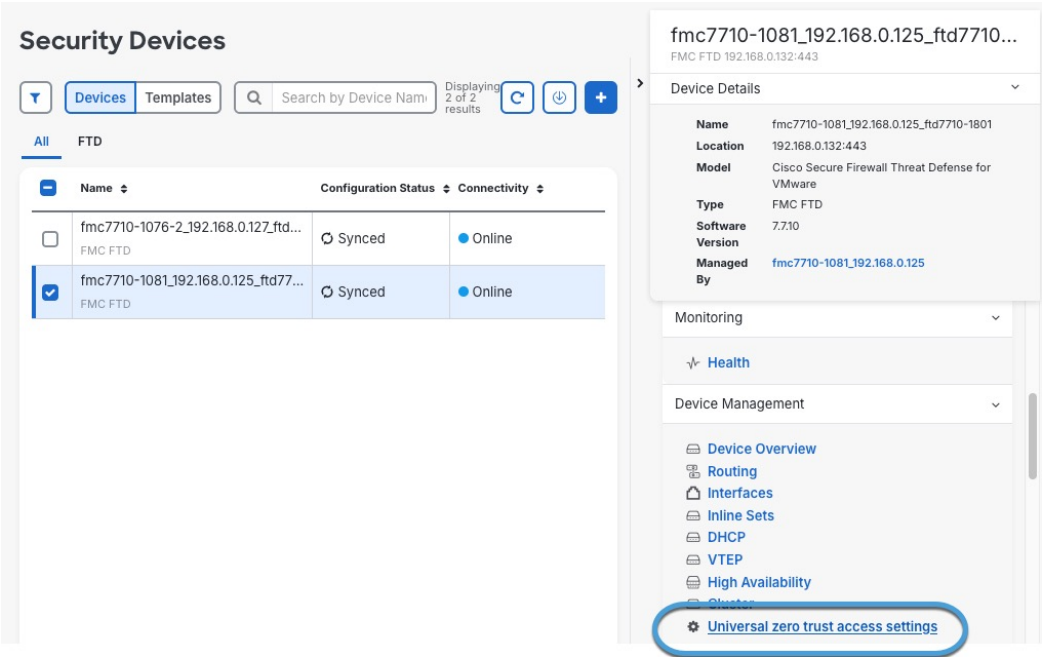
The **Security Devices** page displays the available security devices.



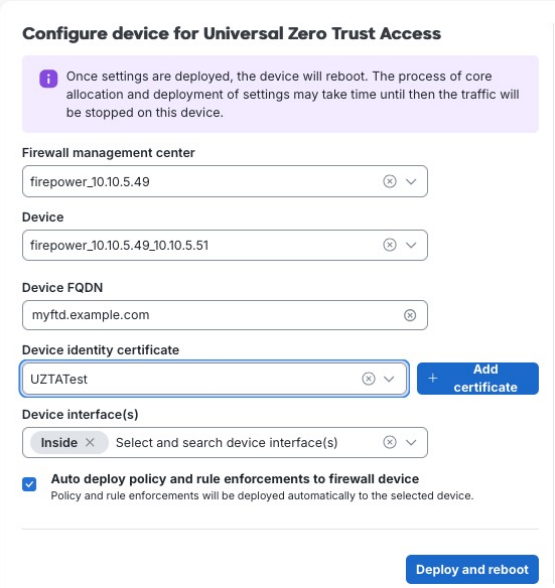
Step 7 Select the check box next to a device to add to the universal zero trust network access configuration.

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

This figure shows an example.



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



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. The **Device identity certificate** must have a Common Name that either: • *Exactly matches* the value you enter in this field. • Matches a Subject Alternative Name (SAN) in the certificate. For more information, consult a resource such as What is the Common Name? on ssl.com.
Device identity 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.

Item	Description
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**.

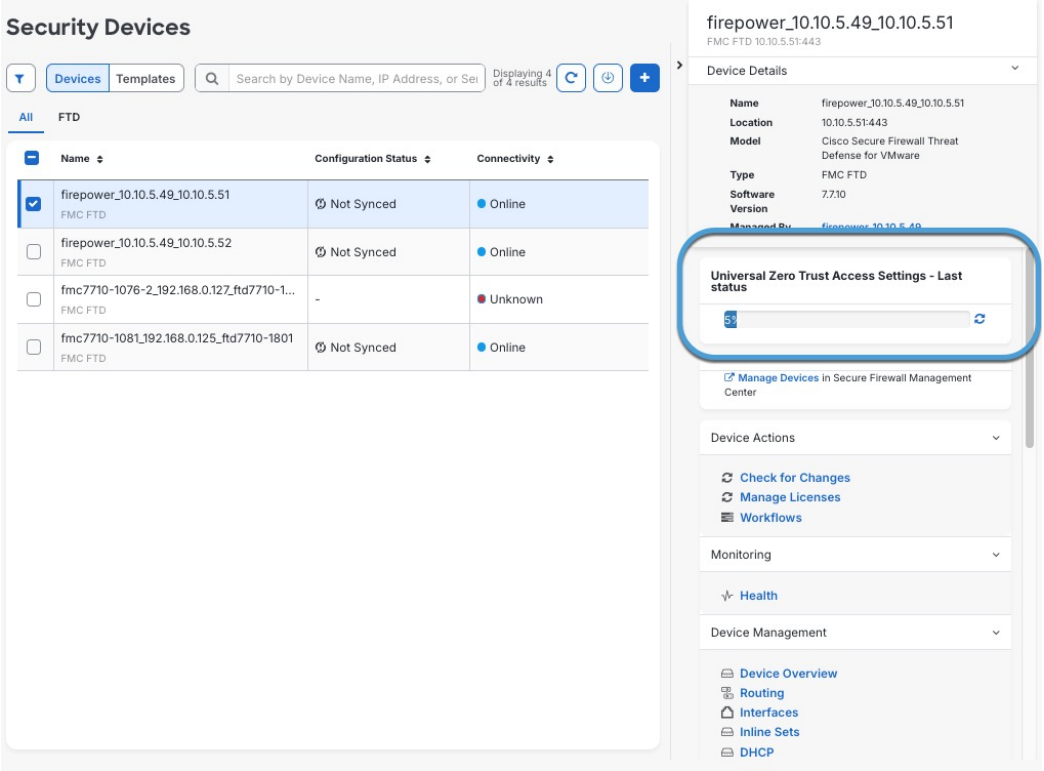
The device reboots to reallocate the system resources for universal ZTNA components.

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.



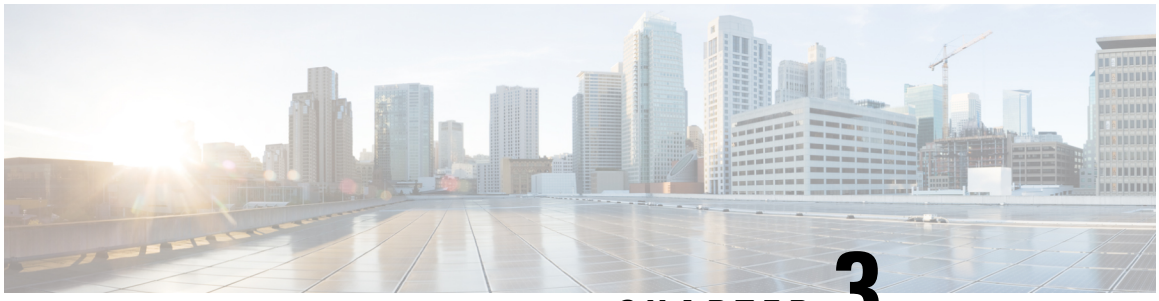
For additional information, click **Device Actions** > **Workflows** in the right pane.

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**.



CHAPTER 3

Configure Secure Access

The final step in configuring universal ZTNA is to configure access policies, private resources, and the devices that are responsible for protecting the resources.

- Configure Private Resources, on page 19
- Configure Universal ZTNA Access Policies, on page 20
- Trusted Network Detection, on page 22
- Associate Private Resources with Firewall Threat Defense, on page 26

Configure Private Resources

Perform these steps to create the private resources in your organization.

Procedure

Step 1 In Cisco Security Cloud Control, click **Products** > **Secure Access**.

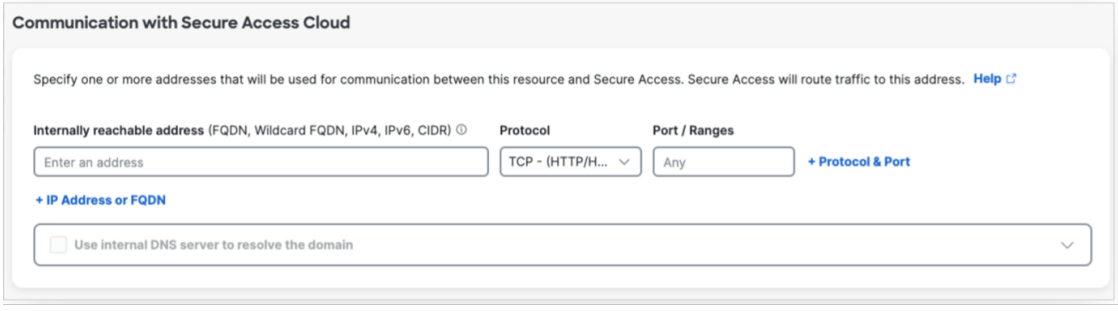
The Secure Access product menu appears in the left navigation bar.

Step 2 Click **Resources** > **Destinations** > **Private Resources**.

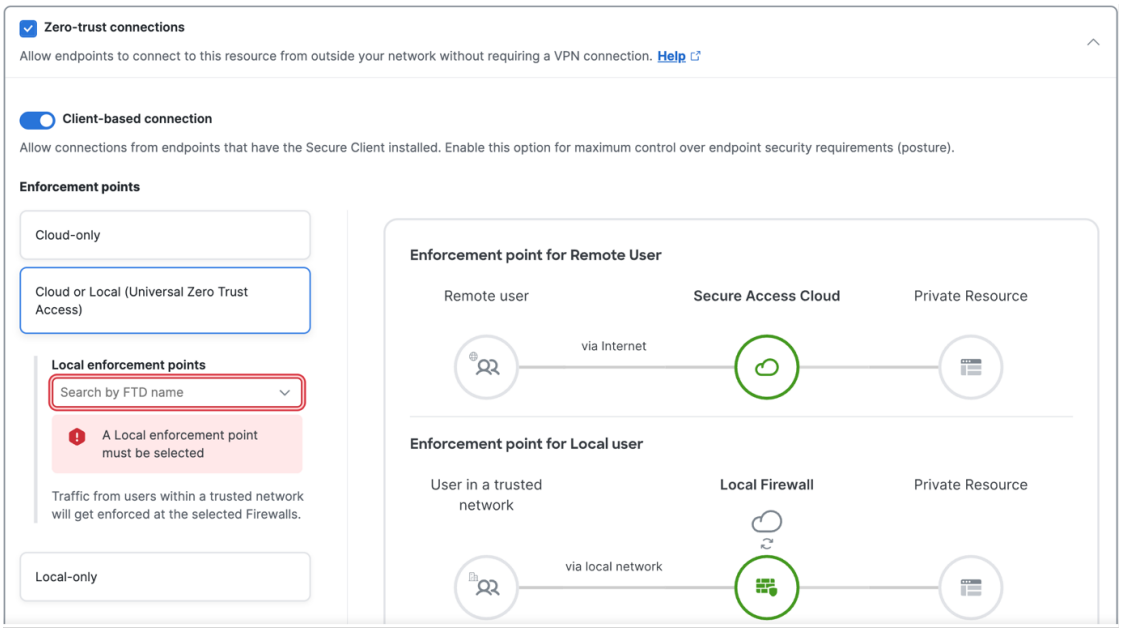
Step 3 Click **+Add**.

Step 4 Provide a meaningful name for the resource in the **Define a Private Resource** section.

Step 5 To define how Secure Access can communicate with the resource, provide the network address or the fully qualified domain name (FQDN) of the resource.



Step 6 Under **Endpoint Connection Methods**, choose **Zero-trust connections** > **Client-based connections**. This selection allows endpoints with Secure Client to communicate with Secure Access.



Depending on how you want to enforce traffic flow, choose an appropriate enforcement point.

- Choose **Cloud or Local** to steer the traffic dynamically based on its origin.

  If the user is in a trusted network, a local Firewall performs the traffic inspection. If the user is outside the trusted network, Secure Access (cloud) performs the traffic inspection.

- The enforcement point must be set to **Local only** for sensitive applications. This choice ensures that traffic inspection occurs only at the on-premises Firewall, regardless of the location of the user.

Choose a Threat Defense device from the **Local enforcement points** drop-down list. All devices that share the same FQDN as the selected device act as the enforcement points.

Step 7 Click **Save** to save the configuration.

Private resources are now added to the network.

For more information on managing private resources, refer to Managing Private Resources in the Secure Access documentation.

Configure Universal ZTNA Access Policies

Create a rule to control and secure the access to specified private resources.

An access rule consists of sources, destinations, endpoint profiles, and security controls. Sources specify the origin of the network traffic. Destinations specify the endpoint of the network traffic.

Endpoint profiles describe the requirements for a rule to match the traffic. For universal ZTNA, use the Client-based Zero Trust profile.

Procedure

Step 1 In Cisco Security Cloud Control, click **Products** > **Secure Access**.

Secure Access product menu displays in the left navigation bar.

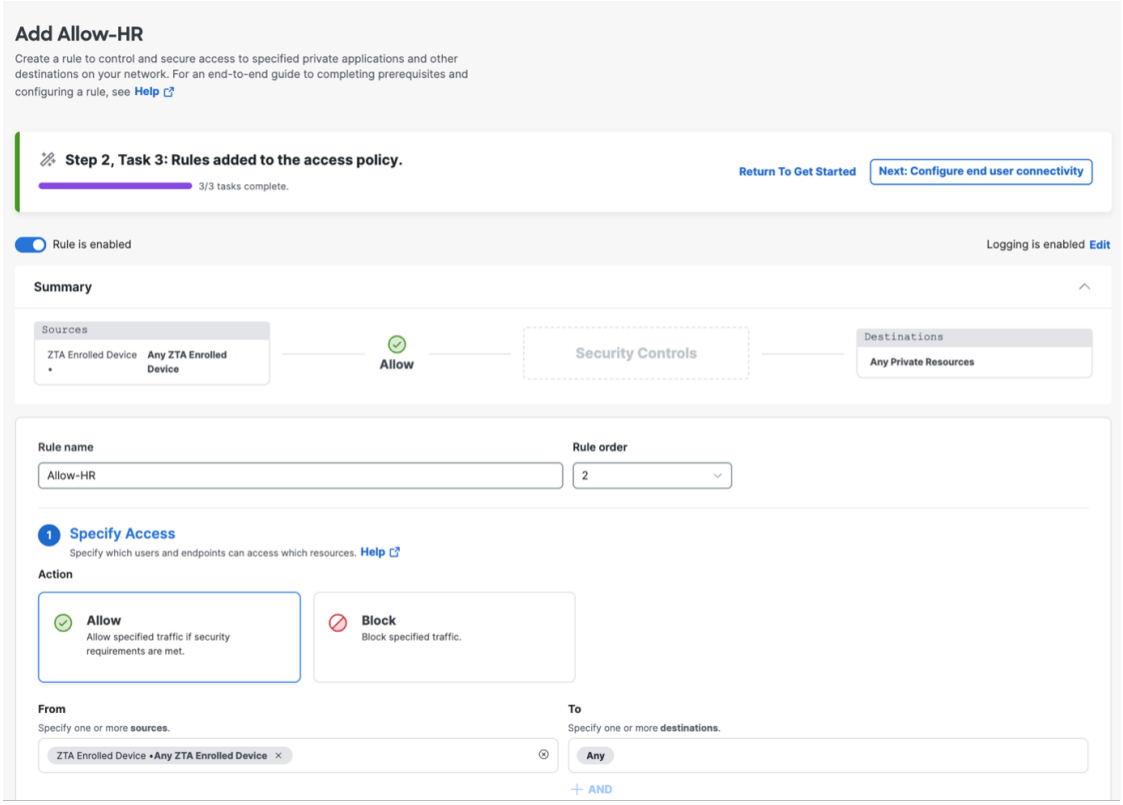
Step 2 Click **Secure** > **Access Policy** .

Step 3 Click **Add Rule** and choose **Private Access**.

Step 4 Add a rule name and specify the order in which the rule must be executed.

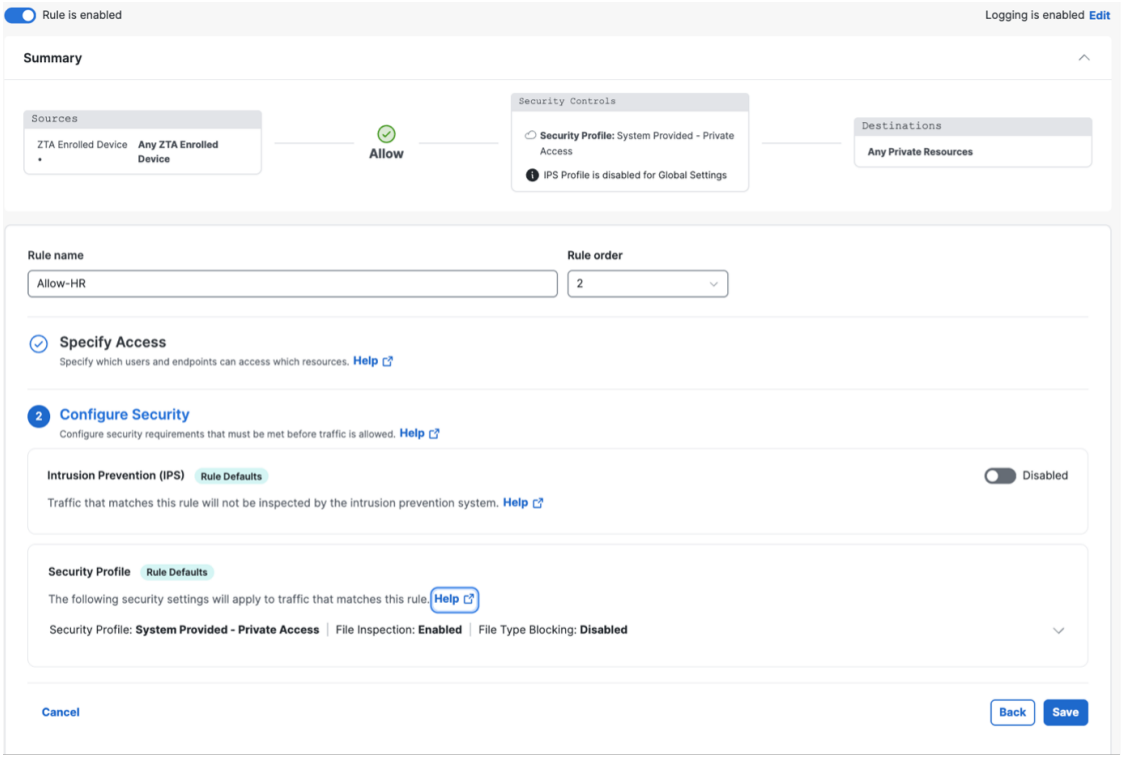
Step 5 Under **Specify Access**, specify one or more sources (users or devices) that can access a destination (private resource).

The **Summary** pane at the beginning of the page shows the rule that you have specified.



Step 6 (Optional) Under **Configure Security**:

- Define the Intrusion Prevention (IPS) method. Traffic is decrypted and inspected based on this IPS profile.
- Define the security profile to protect the resources from malicious files.



Step 7 Save the configurations.

To understand more about private access policies in Secure Access, refer to Get Started With Private Access Rules.

Trusted Network Detection

Trusted network detection (TND) identifies if a user or device is connected to a trusted internal network, such as a corporate LAN, or to an untrusted external network, such as public Wi-Fi. TND determines the network context of a user or device before granting access to applications or resources.

By defining trusted networks, enabling TND, and integrating it with access policies, universal ZTNA enforces granular security controls. It ensures that access privileges are granted based not only on user identity but also on the security posture of the network connection.

To configure TND, add a trusted network and map it to a Threat Defense device.

Add a Trusted Network

Define a trusted network by specifying a set of criteria such as DNS Servers, DNS Domains, and trusted servers. Secure Client uses these criteria to determine if an endpoint device is connected to the trusted network and routes the user's traffic accordingly.

Perform these steps to create a trusted network.

Before you begin

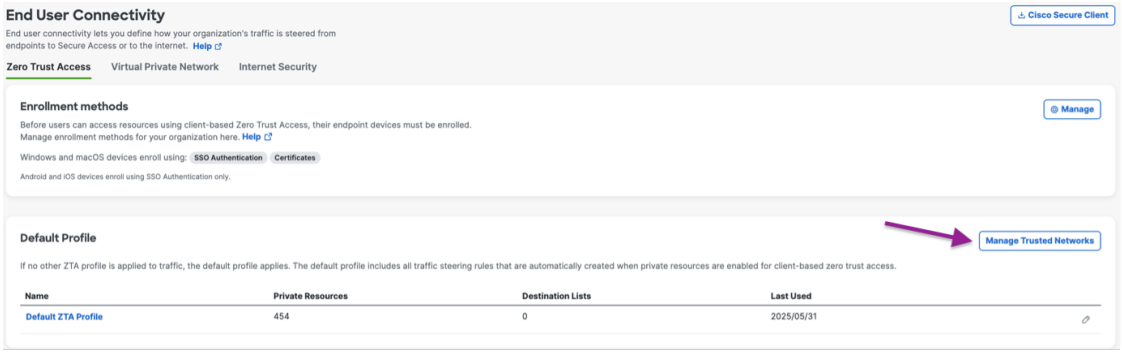
Procedure

Step 1 In Cisco Security Cloud Control, click **Products** > **Secure Access**.

The Secure Access product menu appears in the left navigation bar.

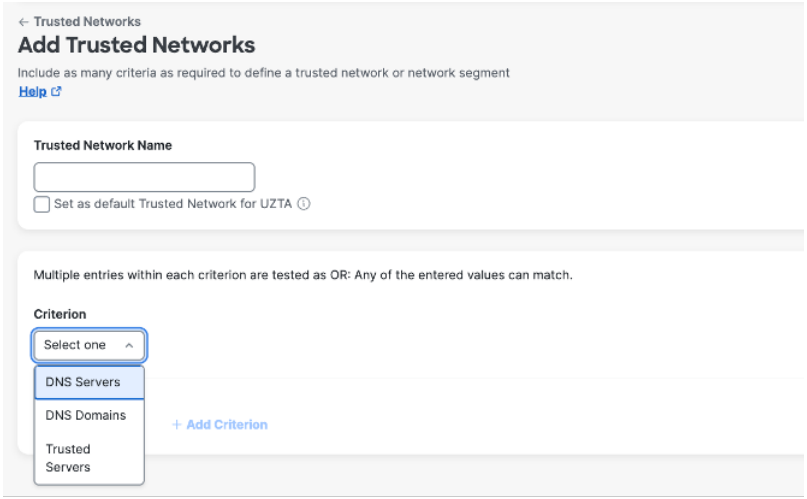
Step 2 Click **Connect** > **End User Connectivity** .

Step 3 Under the **Zero Trust Access** tab, click **Manage Trusted Networks**.



Step 4 Click **+Add**.

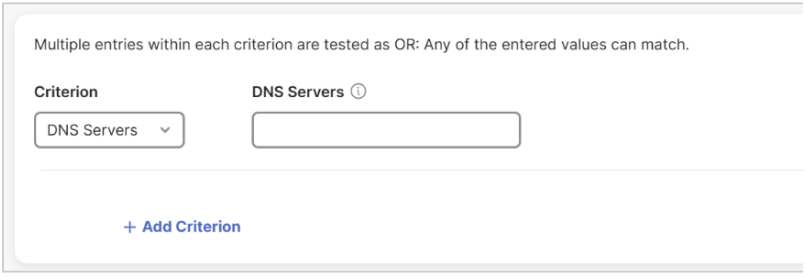
Step 5 On the **Add Trusted Networks** page, enter a name for the network. Then, define the criteria for the trusted network.



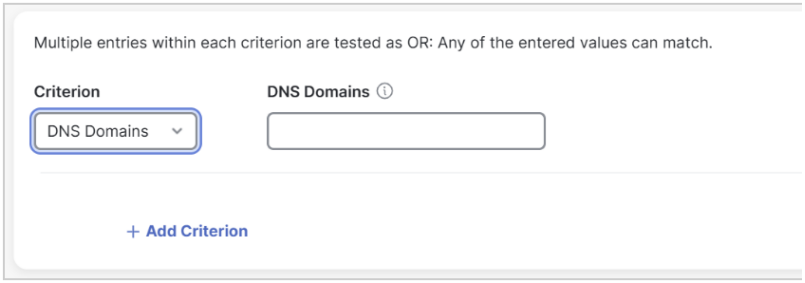
(Optional) To set this network as the default trusted network, check the **Set as default Trusted Network for UZTA** check box.

You can choose one or more criteria for a trusted network.

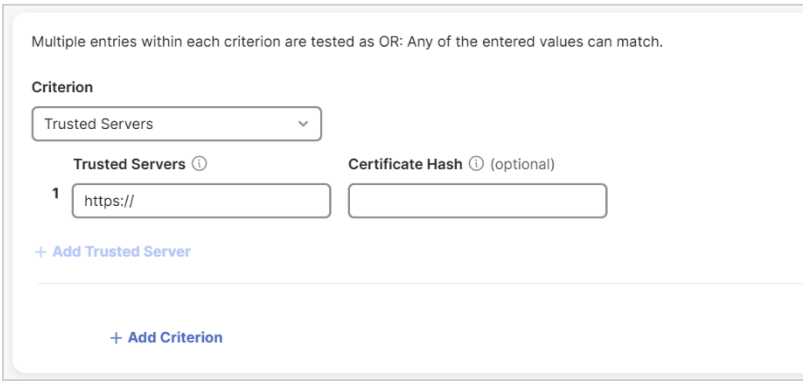
- **DNS Servers**: Enter all DNS server addresses for the trusted network in the **DNS Servers** field, separated by commas. Secure Client treats a network as trusted if it matches any of these addresses.



- **DNS Domain**: Enter all DNS domain suffixes for the trusted network in the **DNS Domains** field, separated by commas. Secure Client treats a network as trusted if it matches any of these DNS domain suffixes.



- **Trusted Servers**: Enter a trusted server address in the **Trusted Servers** field. A DNS server that you specify in this profile must translate the domain name of the server to its IP address and provide a TLS certificate.



(Optional) In the **Certificate Hash** field, enter the hash of the public key of this certificate.

(Optional) Click **+Add Trusted Server** to add up to 10 trusted servers.

Step 6 Click **Save**.

A trusted network is created.

What to do next

Assign this trusted network to a Threat Defense device.

Map a Trusted Network to a Threat Defense Device

If a default trusted network exists when a Threat Defense is added to the network, this default network is automatically mapped to the Threat Defense device.

If a default trusted network does not exist, map a trusted network to a device by performing the following steps.

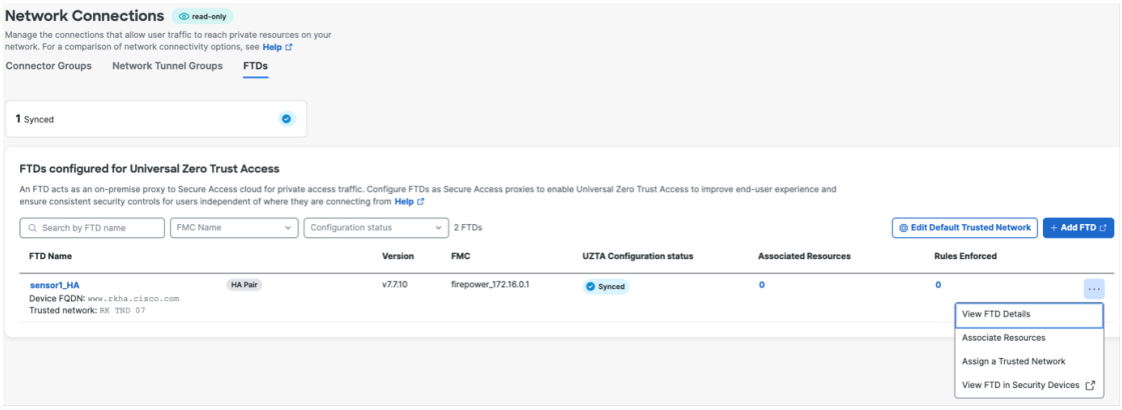
Procedure

Step 1 In Cisco Security Cloud Control, click **Products** > **Secure Access**.

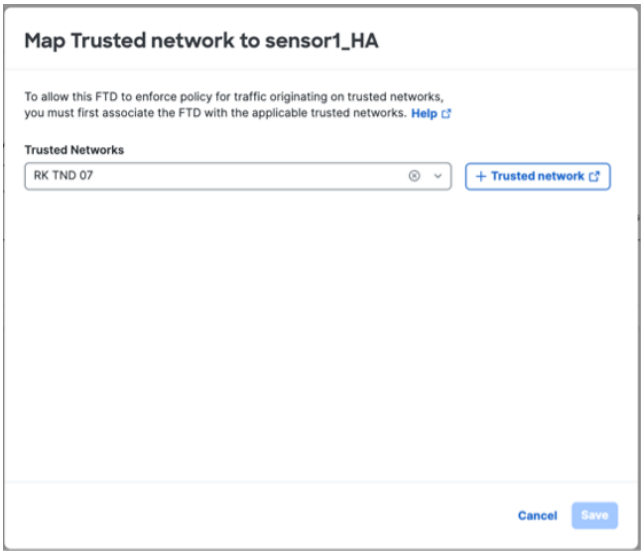
The Secure Access product menu appears in the left navigation bar.

Step 2 Click **Connect** > **Network Connections** > **FTD**.

Step 3 Click the three dots (…) next to a Threat Defense device and select **Assign a Trusted Network** from the drop-down menu.



Step 4 From the **Trusted Networks** drop-down list, select a trusted network to map to the device and click **Save**.



The trusted network is now associated with the Threat Defense device.

Note

- If this Threat Defense device shares its fully qualified domain name (FQDN) with other devices, the trusted network is also mapped to those devices.
- A Threat Defense device can be associated with only one trusted network.

Associate Private Resources with Firewall Threat Defense

Before you begin

You must have created the private resources on Secure Access.

Procedure

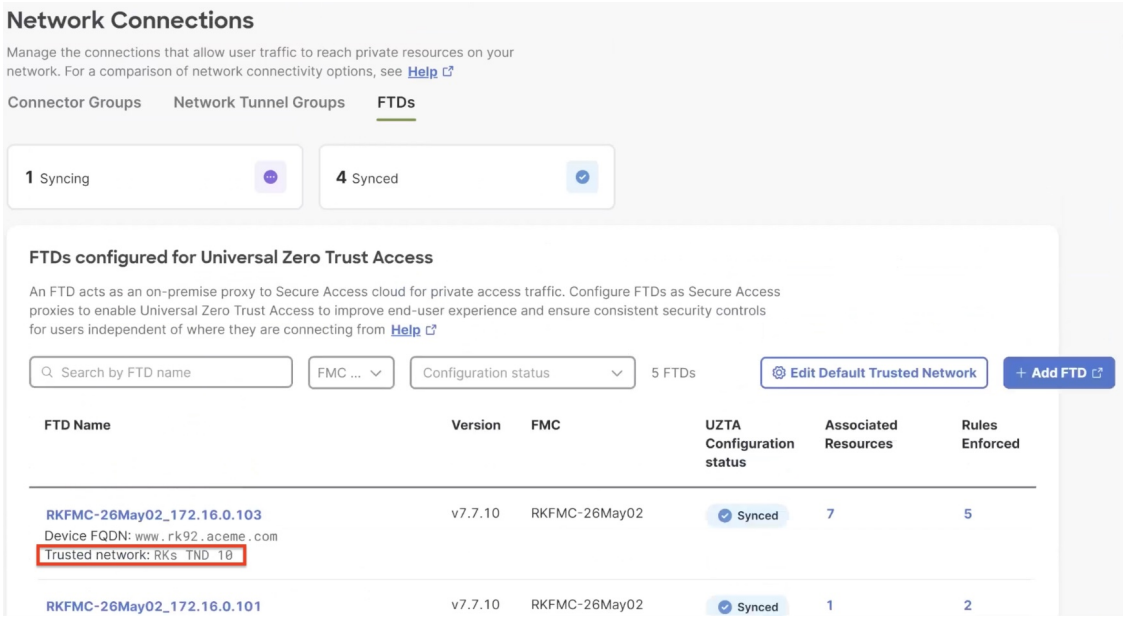
Step 1 In Cisco Security Cloud Control, click **Products** > **Secure Access**.

Secure Access product menu displays in the left navigation bar.

Step 2 Click **Connect** > **Network Connections**.

Step 3 Click the **FTDs** tab.

The available Secure Firewall Threat Defense devices that are configured for universal zero trust network access are displayed.



Ensure that the device is associated with a trusted network to enforce policies on traffic originating from the trusted network before proceeding to the next step.

After a Threat Defense device is onboarded, it is automatically associated with a default trusted network if one exists. Otherwise, you must create a trusted network and associate it with the Threat Defense device.

Step 4 Click the name of a Threat Defense device to configure.

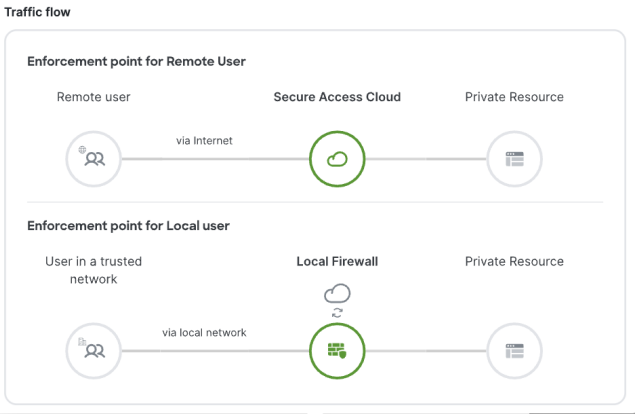
Step 5 In the right pane, click **Associate Resources**.

Note

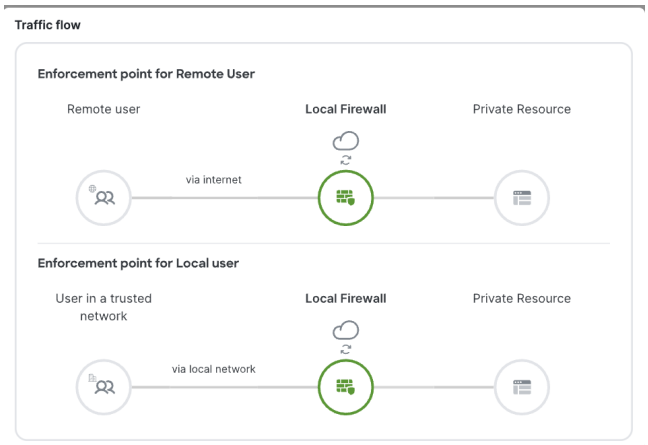
- Only those resources that are enabled for zero trust access may associate with a Threat Defense device.
- A Threat Defense device must reach the associated private resources.
- Resources associated with a Threat Defense device are shared with other devices with the same FQDN.

Step 6 In the **Associate Private Resources** dialog box, make the following selections to specify the access policy enforcement and traffic flow for a user:

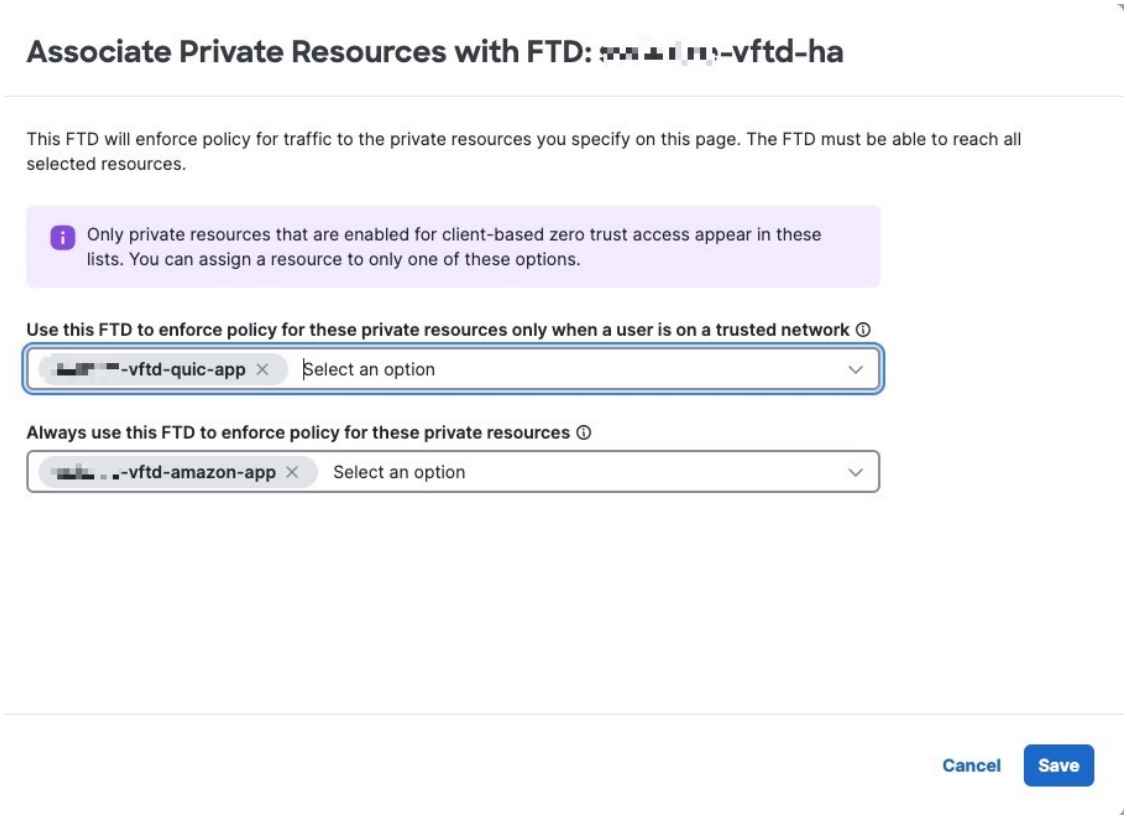
- **Use Threat Defense device to enforce policy only for on-premises users**: From the **Use this FTD to enforce policy** drop-down list, select the private resources, which a user should be able to access only from an on-premises location.



- **Use Threat Defense device to enforce policy for both on-premises and remote users**: From the **Always use this FTD to enforce policy** drop-down list, select the private resources for which the selected Threat Defense device always enforces policy, regardless of whether the user is located on-premises or is remote.



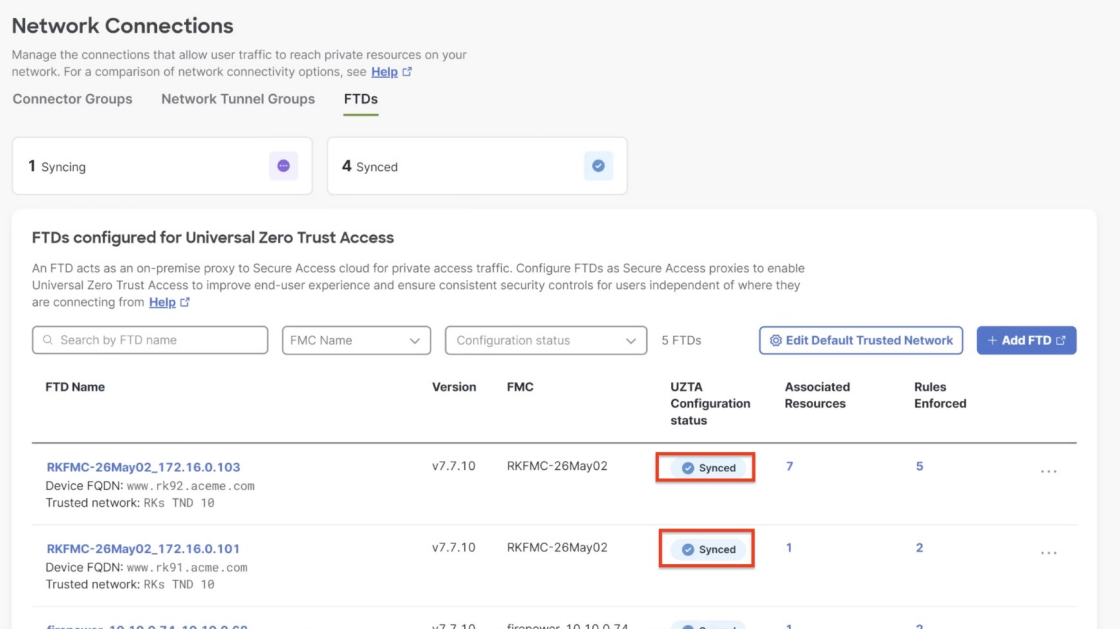
The following figure shows an example of using a Threat Defense device to enforce access rules for the **vftd-quic-app** for on-premises users and **vftd-amazon-app** for all users, whether on-premises or remote.



Step 7 Click **Save**.

The configurations are applied to the device, and the **UZTA Configuration status** column for the device displays **Synced**.

The following figure shows an example.



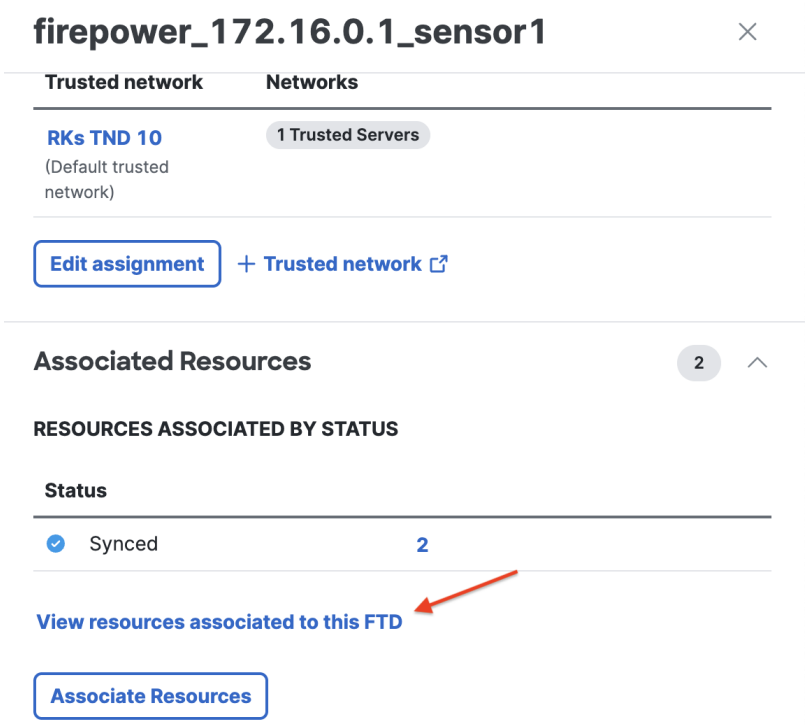
Configuration status can also be:

- Syncing—updates to the Threat Defense device are ongoing.
- Out of sync—modifications to Secure Access configurations are pending update to the Threat Defense device.
- Failed to sync—configurations were not updated on the Threat Defense device.

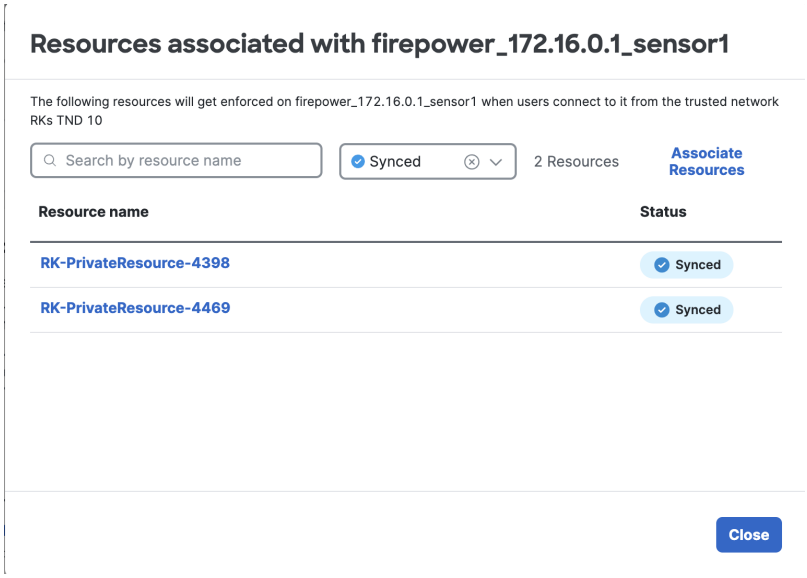
To view a detailed and granular status for each resource and rule associated with a Threat Defense device, perform the actions outlined:

a) Click the numeral in the **Associated Resources** column.

In the slide-in pane, under the **Associated Resources** section, click **View resources associated with this FTD**.

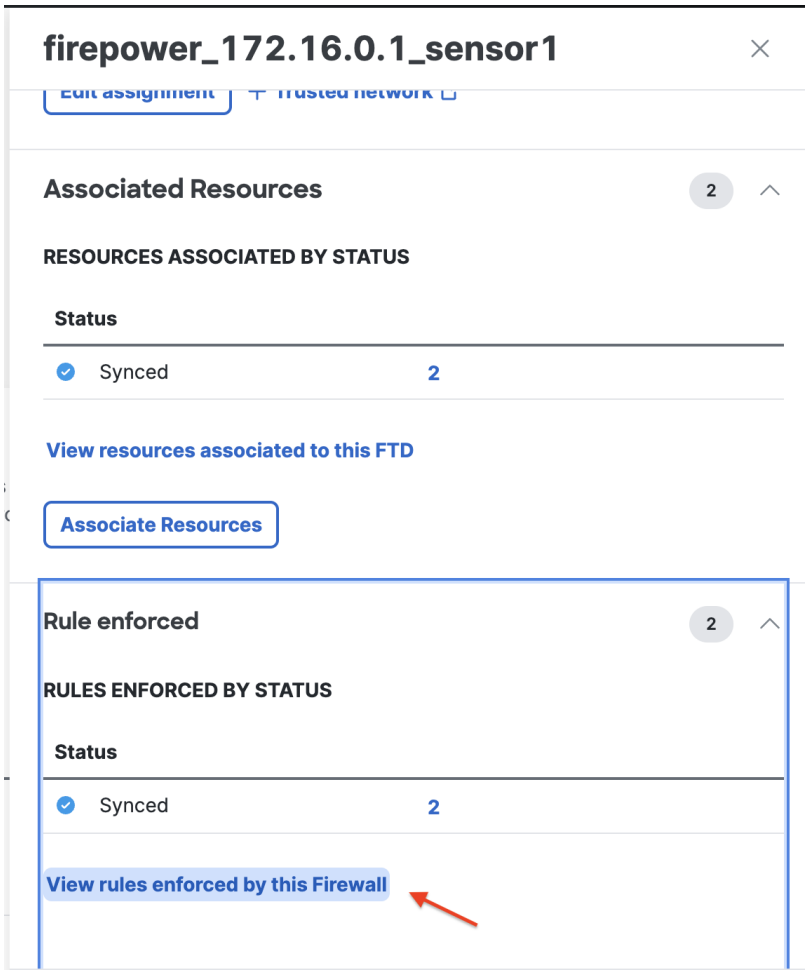


The configuration status of each resource is displayed.

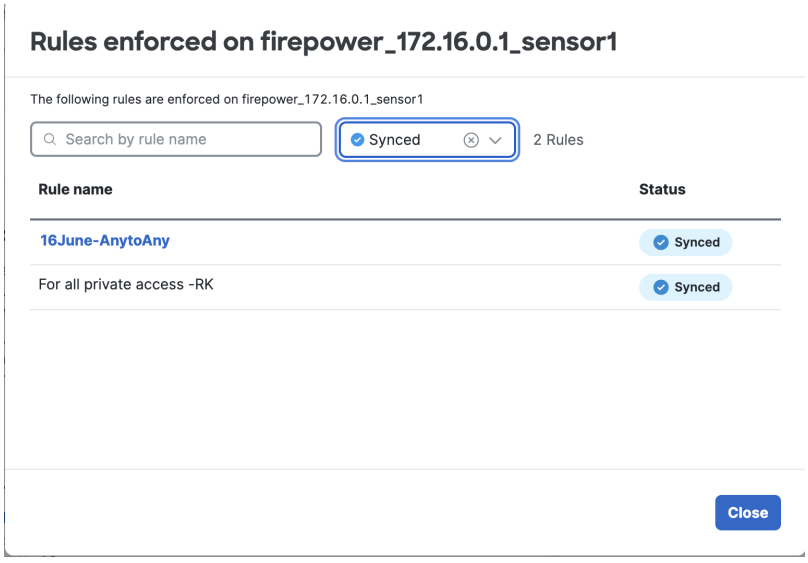


b) Similarly, to check the configuration status of each rule that is enforced by the Threat Defense device, click the numeral in the **Rules Enforced** column.

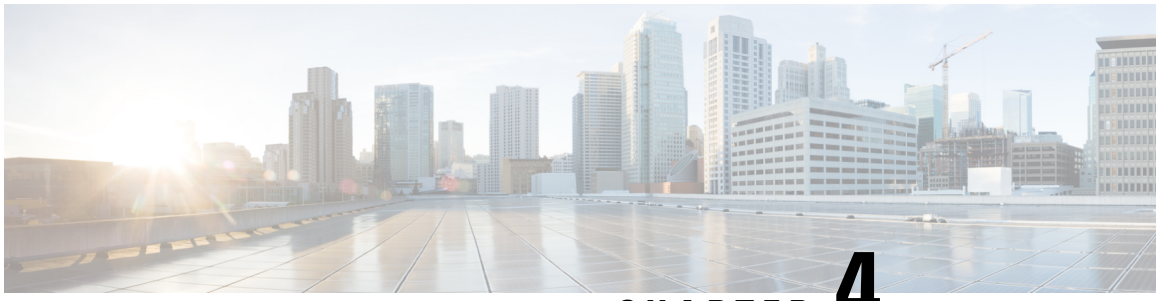
In the slide-in pane, under the **Rules Enforced** section, click **View rules enforced by this Firewall**.



The configuration status of each rule that is enforced is displayed.



Universal ZTNA is now set up for your clients to securely access the private resources in your network.



CHAPTER 4

Related Documentation

Additional documents that you can refer.

- Related Documentation, on page 33

Related Documentation

Read the following documents for additional information on the components of universal ZTNA.

To know more about...	Read this document...
Universal ZTNA Solution	Universal Zero Trust Network Access Solution Guide
Secure Access	Secure Access Help Center
Security Cloud Control	Security Cloud Control Getting Started Guide
Firewall Threat Defense	Secure Firewall Management Center Device Configuration Guide https://www.cisco.com/c/en/us/support/security/security-cloud-control/products-installation-and-configuration-guides-list.html
Firewall Threat Defense Health Metrics	Secure Firewall Threat Defense Health Metrics Collected by Firewall Management Center Health Monitor
Firewall Management Center	Secure Firewall Management Center Administration Guide
Cloud-Delivered Firewall Management Center	Managing Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control Release Notes for Cloud-Delivered Management Center
Secure Client	Secure Client Administrator Guide
Supported Device Release	Secure Firewall Threat Defense Release Notes

Related Documentation