

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 1
- Set Up Firewall Threat Defense Devices, on page 1
- Integrate Firewall Management Center with Security Cloud Control, on page 3
- Configure Security Devices, on page 7

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.

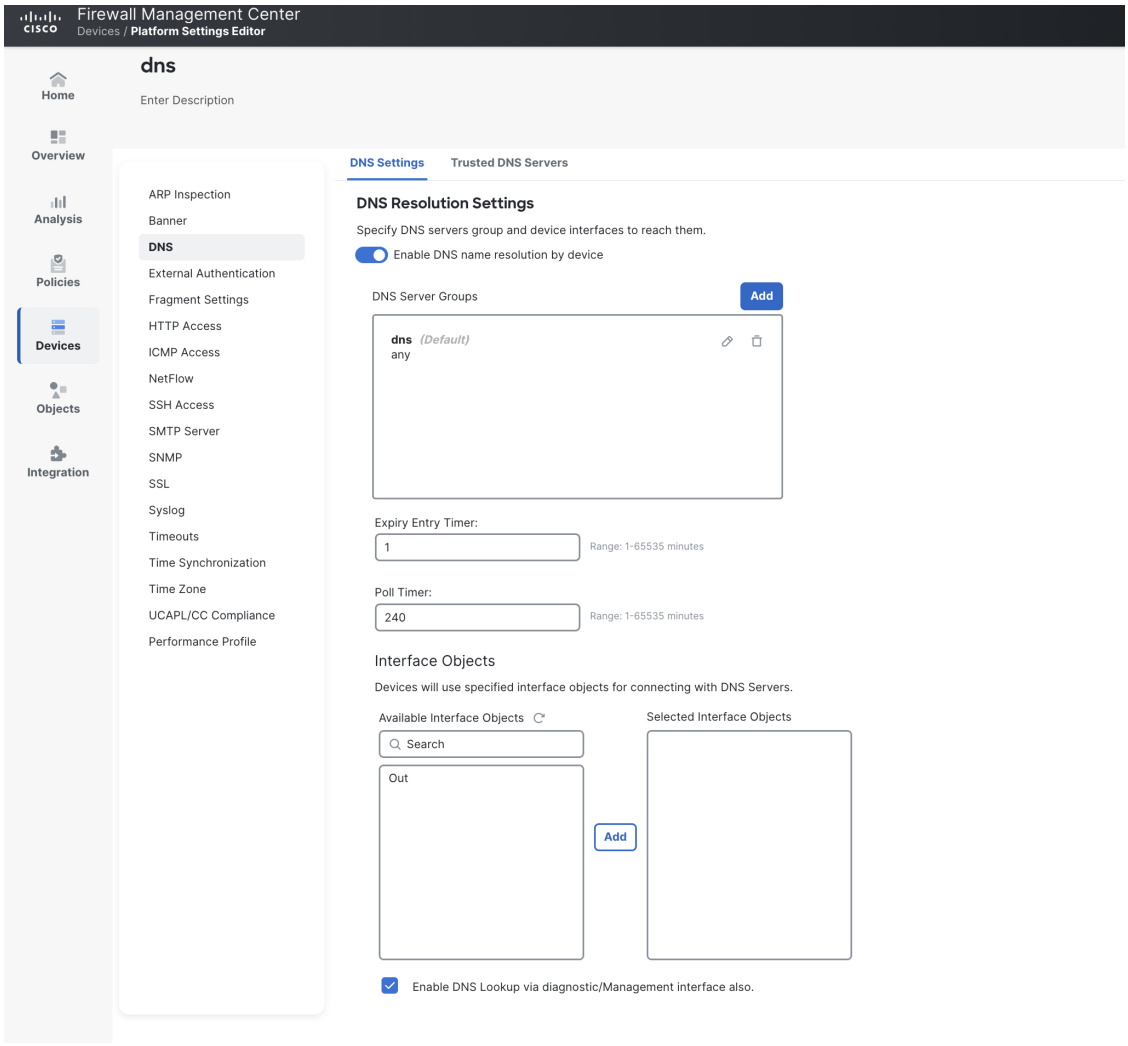
1. If you have purchased a subscription for the products, claim the subscription in Security Cloud Control and activate both the products. For information on claiming a subscription and activating products in Security Cloud Control, see the Security Cloud Control Administration Guide.
2. Configure user 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.

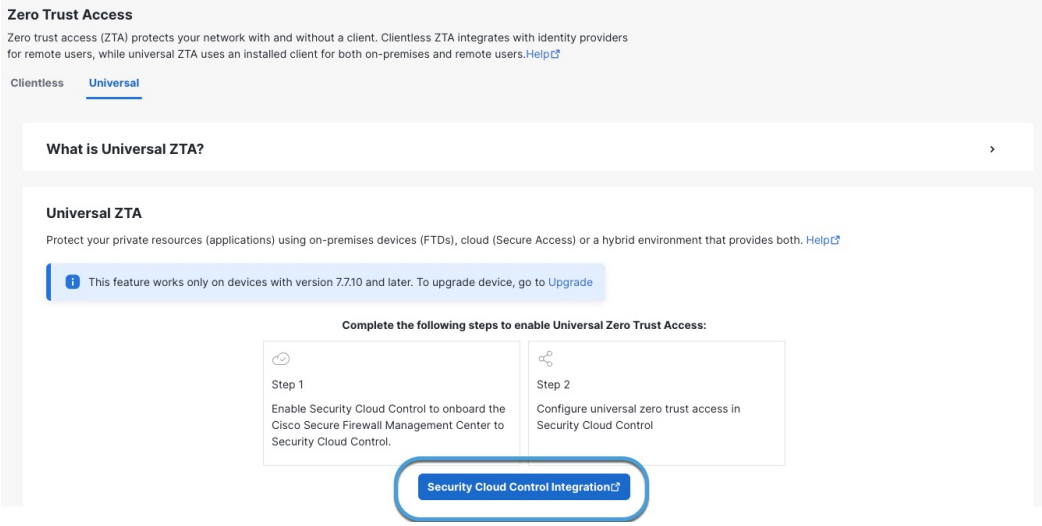
Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Click the **Universal** tab.

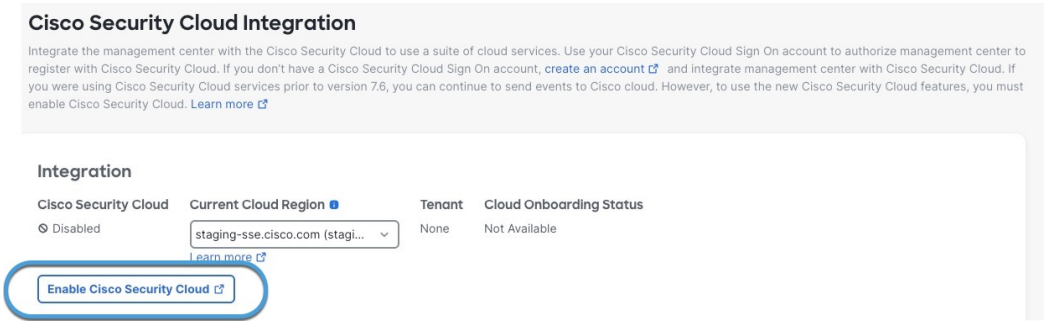
The Zero Trust Access page appears.



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**.

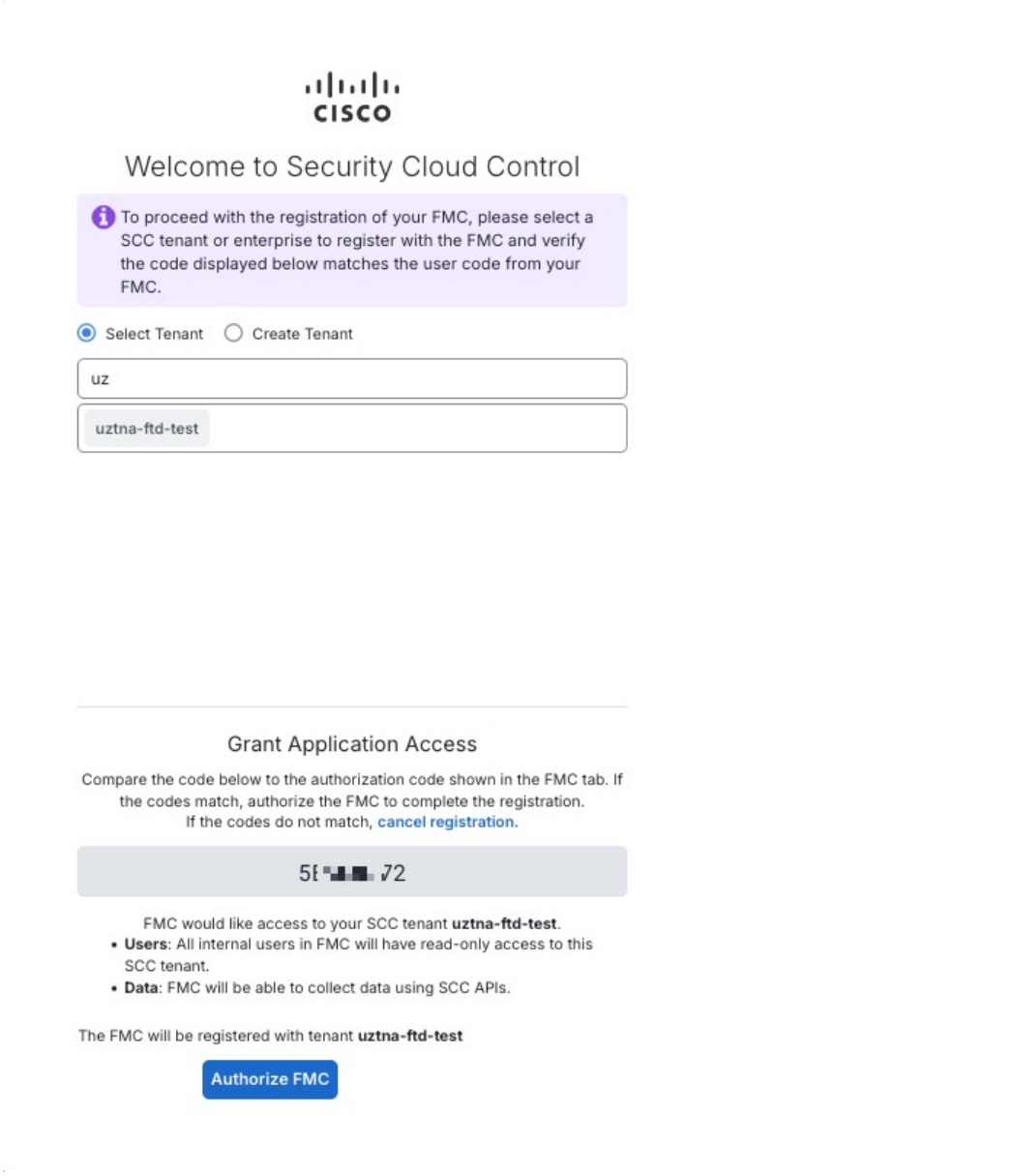


Step 7 When prompted, click **Continue to Cisco SSO**.

Step 8 Log in to Cisco Security Cloud Control.

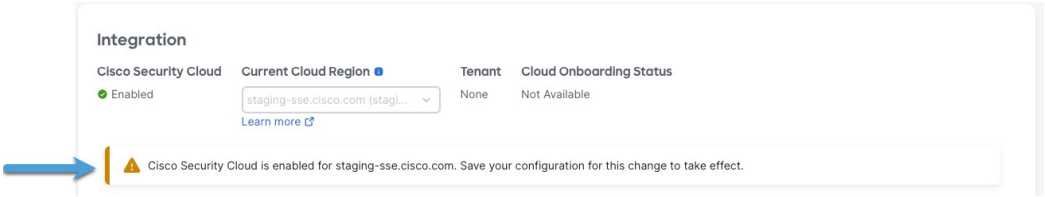
Step 9 From the **Select Tenant** list, click the name of your tenant.

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



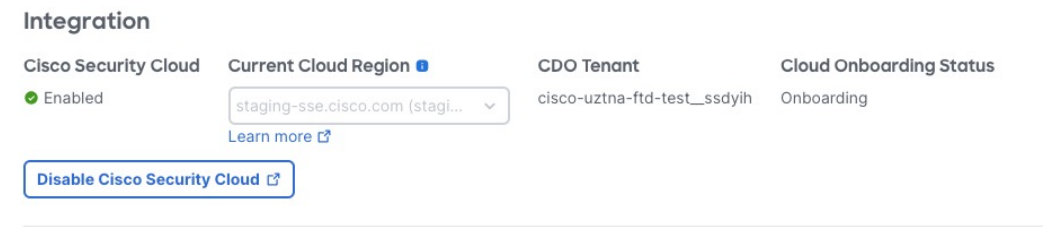
Step 11 When prompted, close the tab page.

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 6.

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.

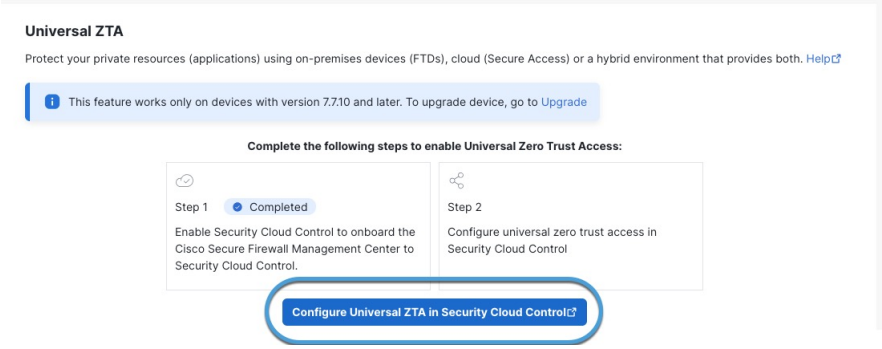
You can choose internal, external, or both types of interfaces for each security device.

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.

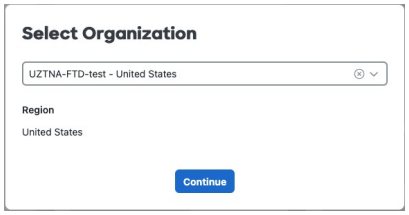


Step 3 When prompted, log in to Cisco Security Cloud Control.

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

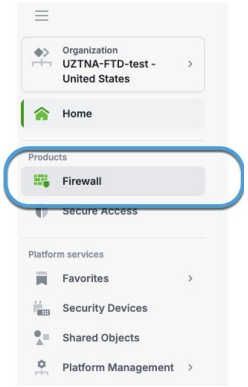
Select an organization that has both Secure Access and Secure Firewall micro applications configured.

This figure shows an example.



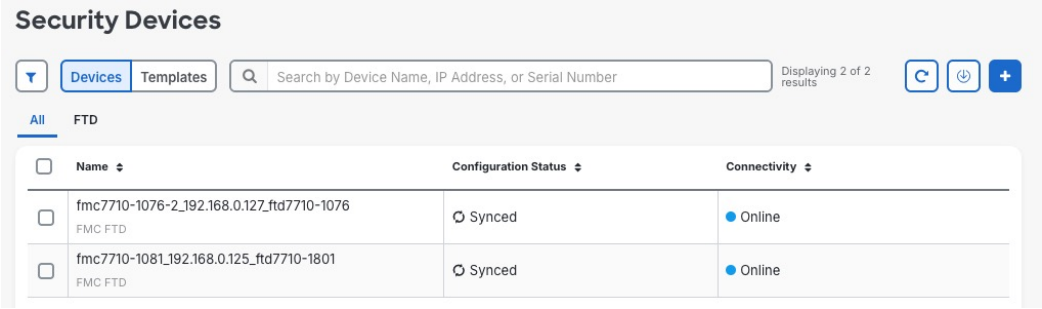
Step 5 In Cisco Security Cloud Control, in the Products section, click **Firewall**.

This figure shows an example.



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

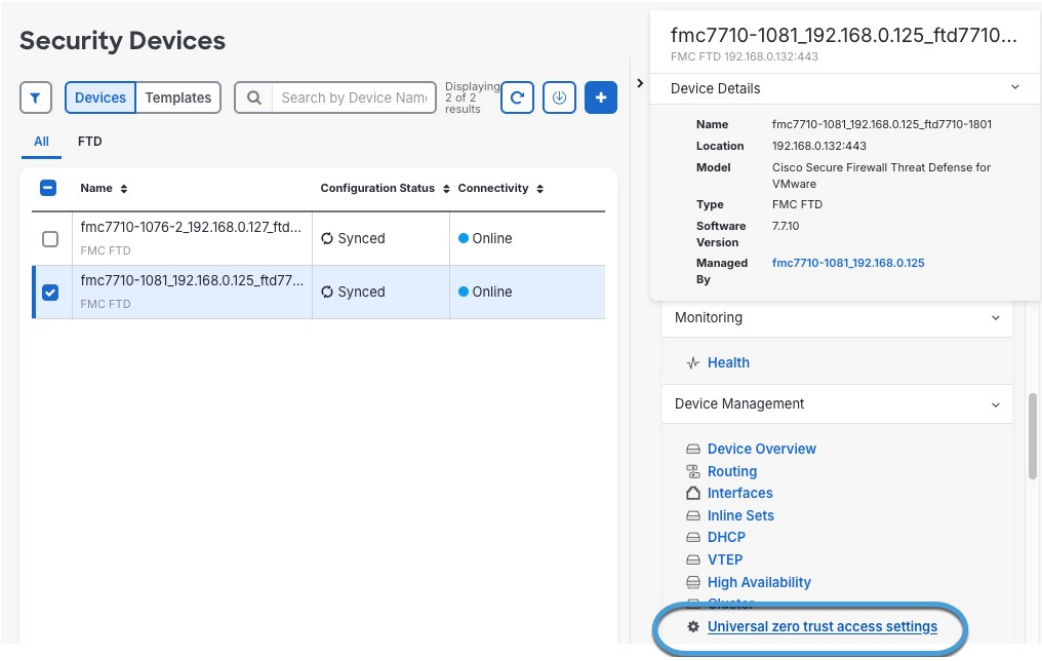
The **Security Devices** page displays the available security devices.



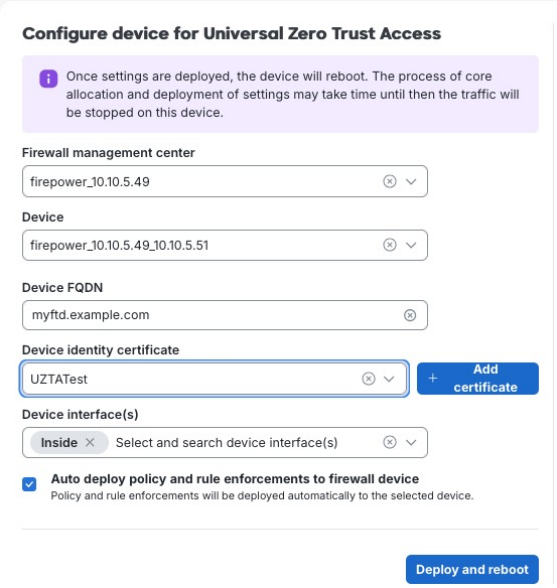
Step 7 Select the check box next to a device to add to the universal zero trust network access configuration.

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**.

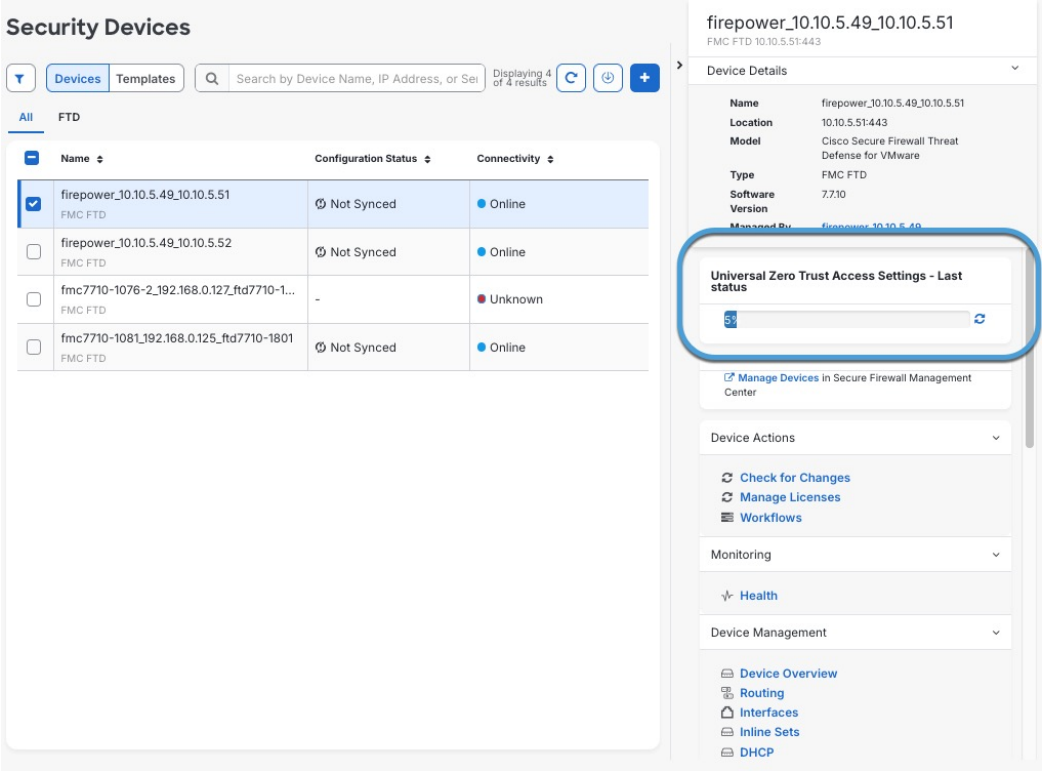
The device reboots to reallocate the system resources for universal ZTNA components.

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**.