

Universal Zero Trust Network Access Solution 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 **Overview of Universal Zero Trust Network Access** 1

Universal Zero Trust Network Access 1

Components of Universal ZTNA Solution 1

Benefits of Universal ZTNA 2

Prerequisites for Universal ZTNA 3

CHAPTER 2 **Overview of Universal ZTNA Configuration** 5

Configuring Universal ZTNA Solutions 5

CHAPTER 3 **Deployment of Universal ZTNA solution** 9

Outcome 1: Optimal path for user traffic 9

Data flow for an on-premises user 10

Data flow for a remote user 11

Data flow for a branch user 12

Outcome 2: Private inspection for sensitive applications 13

Data flow to a sensitive application from a remote user 13

Configuration workflow 15

Monitoring events 27

CHAPTER 4 **Troubleshooting Universal ZTNA** 29

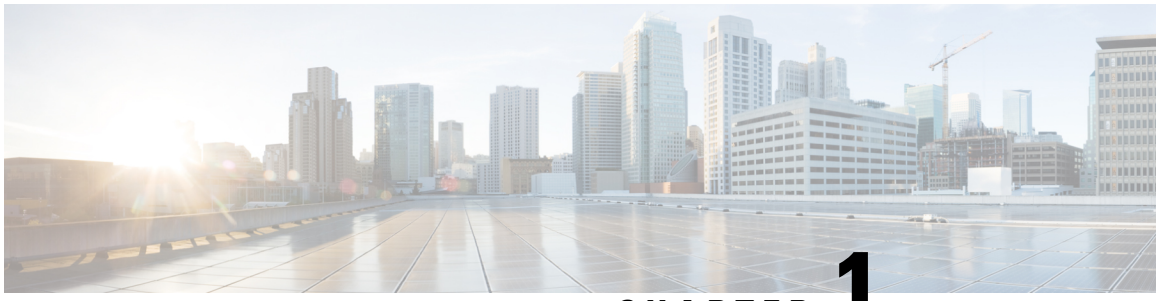
Issue: Private resource not reachable 29

Issue: universal ZTNA-enabled Threat Defense device not visible in Secure Access 30

Issue: Configuration deployment to device fails 31

CHAPTER 5 **Related Documentation** 33

Related Documentation 33



CHAPTER 1

Overview of Universal Zero Trust Network Access

This section provides an overview of Universal Zero Trust Network Access (universal ZTNA) including its components, benefits, and prerequisites.

- Universal Zero Trust Network Access, on page 1

Universal Zero Trust Network Access

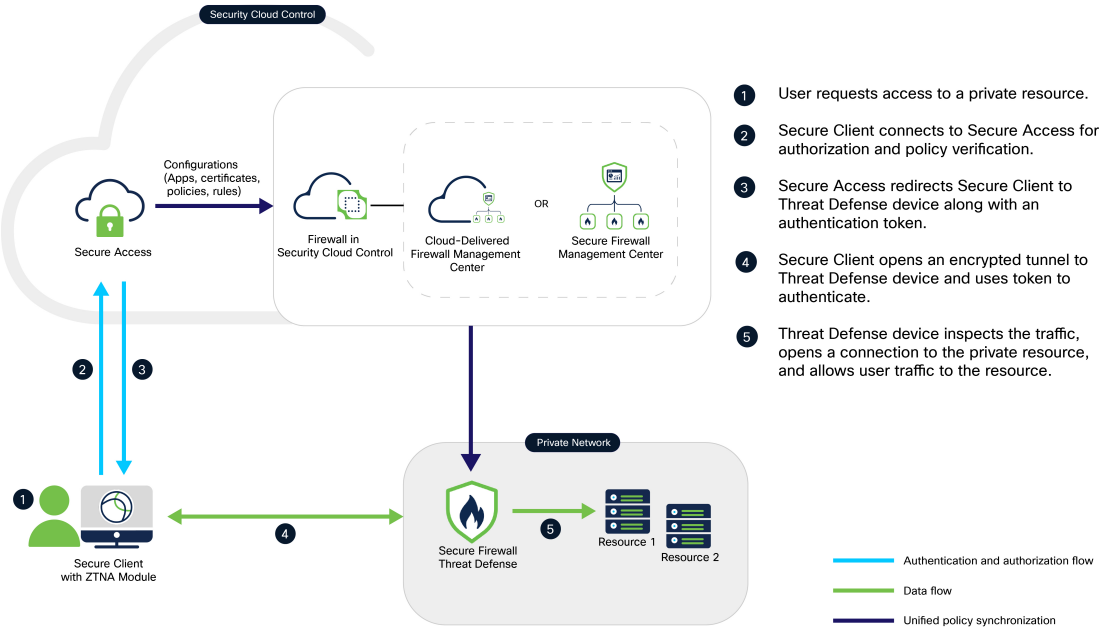
Universal Zero Trust Network Access (universal ZTNA) is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. Unlike traditional remote access VPNs, universal ZTNA ensures that access to one application does not implicitly grant access to others, thereby reducing the network attack surface.

Components of Universal ZTNA Solution

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

Universal ZTNA supports both on-premises Firewall Management Center, and Cloud-Delivered Firewall Management Center.

Figure 1: Components of Universal ZTNA Solution



- **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. A Threat Defense device inspects traffic and enforces intrusion prevention system (IPS), file, and malware policies.
- **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**: Provides a unified secure management plane for both Secure Access and Secure 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.

Benefits of Universal ZTNA

Universal ZTNA addresses the evolving network security challenges and operational complexities. Here is how deploying a universal ZTNA solution helps the administrators:

- Granular Access Control: Access is granted based on user identity and posture, ensuring secure access for both remote and on-premises users.
- Reduced Attack Surface: Access to one application does not imply access to others, minimizing potential vulnerabilities.
- Consistent Policy Enforcement: Policies are evaluated and managed in the Secure Access Cloud, while traffic proxying and enforcement (such IPS, malware) occur on Firewall Threat Defense devices.
- Dynamic Traffic Steering: Traffic is routed to the nearest enforcement point, optimizing connectivity and reducing latency for on-premises users.

- Simplified Policy Management: Policy enforcement is centralized across cloud and on-premises environments, allowing unified and granular control over application access based on identity and device compliance.
- Reduced Network Complexity: By intercepting and managing application access at the endpoint with the Secure Client, universal ZTNA eliminates the need for traditional VPNs and complex network segmentation, simplifying network design and management.

Prerequisites for Universal ZTNA

Secure Firewall Management Center and Threat Defense Devices

Ensure that Secure Firewall Management Center and Threat Defense devices meet the following configuration requirements:

- The devices must run version 7.7.10 or later.
- If the devices operate 7.7.10 or 10.0.x, they must have a minimum of 16 cores.
- The devices must be configured for routed mode.
- Configure Secure Firewall with a DNS server to resolve private resource FQDNs.

Security Cloud Control

Verify that your Security Cloud Control environment meets these account and subscription criteria:

- Requires an enterprise account.
- Requires a Subscription (claim code) for Secure Access and Secure Firewall.

Secure Client

Configure the Secure Client to support the ZTNA module with the following specifications:

- The client must run version 5.1.10 or later.
- The ZTNA module must be enabled on the Secure Client.
- The client must run on a platform that supports Trusted Platform Module (TPM), such as Windows 11.

Licenses

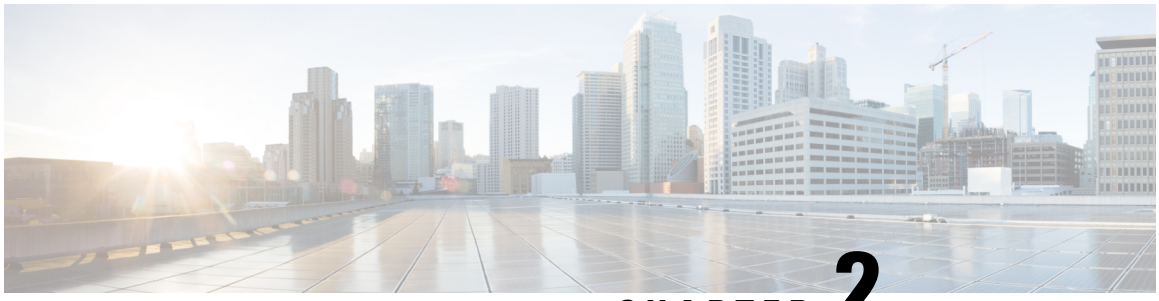
Maintain valid licensing for all components involved in the universal ZTNA solution.

- 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.

Certificates

Provision the required certificates to enable secure mTLS connections for the universal ZTNA solution.

- User Identity Certificate: Secure Client 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. The client certificate is enrolled and managed as part of the Zero Trust Network Access module (ZTNA) on the Secure Client.
- Firewall Threat Defense Device Certificate: Threat Defense devices that are enabled for universal ZTNA use the device certificates to establish secure mTLS connections with the Secure Client and Secure Access. Ensure that the device identity certificate is of type PKCS12.
- (Optional) Decryption Certificate: To decrypt traffic sent to private resources, enable decryption for those resources in Secure Access and provide the server certificate and key. We recommend using a certificate signed by a publicly recognized certificate authority (CA).



CHAPTER 2

Overview of Universal ZTNA Configuration

This section describes the universal ZTNA configuration workflow.

- Configuring Universal ZTNA Solutions, on page 5

Configuring Universal ZTNA Solutions

As an administrator, set up the infrastructure, configure policies, deploy those policies at the enforcement point, and monitor the solution to ensure it works as expected. This section provides a high-level overview of the universal ZTNA configuration process.

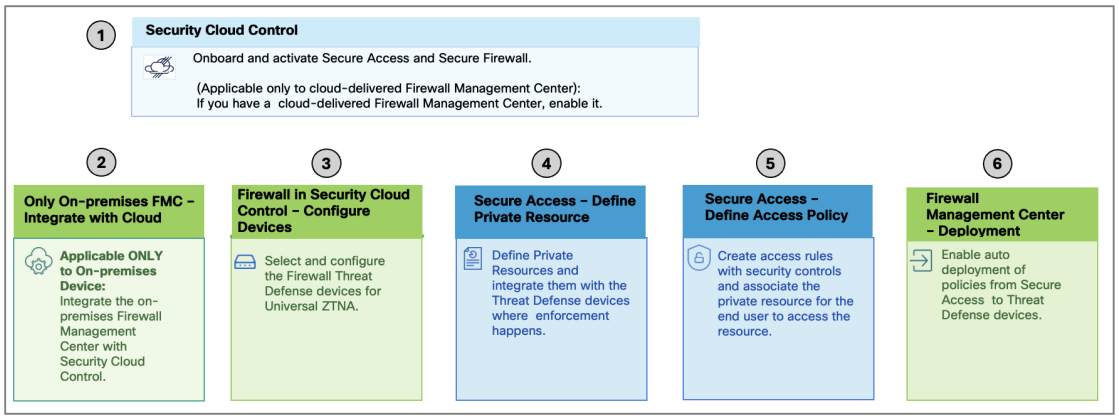
Summary

The configuration process involves the following key components and platforms:

- Security Cloud Control: Used for platform management, subscription claiming, and Firewall Management Center integration.
- Secure Access: Used for user management, trusted network configuration, and private resource definition.
- Firewall Management Center and Firewall Threat Defense, version 7.7.10 or later: Used for configuration deployment and policy enforcement.
- Secure Client: Used on remote user devices to enable zero trust access.

Workflow

Figure 2: Workflow to Set Up Universal ZTNA



These stages describe the configuration workflow for the universal ZTNA solution.

1. Onboard Security Cloud Control Firewall Management and Secure Access to the Security Cloud Control platform.
   - Claim a subscription and provision Secure Access and Security Cloud Control Firewall Management.
   - Configure user management in Secure Access manually or via an identity provider.
   - Configure trusted networks through Secure Access.
   - Update Secure Access with the CA certificate for the ZTNA user.
2. Prepare and set up Firewall Management Center and Firewall Threat Defense devices.
   - Enable cloud-delivered Firewall Management Center or onboard an on-premises Firewall Management Center to Security Cloud Control.
   - Register smart licenses and specify routed interfaces, platform settings, and DNS for Firewall Threat Defense devices.
3. Configure the Threat Defense devices for universal ZTNA in Security Cloud Control.
   - Specify device FQDN, interfaces, and PKCS12 certificate.
   - Deploy changes.

     If your Firewall Management Center and Firewall Threat Defense devices run versions 7.7 and 10.0: After the changes are deployed, the devices reboot to reallocate system resources. Rebooting takes several minutes. If you deploy a High Availability (HA) pair of devices, both devices reboot simultaneously, interrupting traffic flow.

     If your Firewall Management Center and Firewall Threat Defense devices run versions10.1 and later: After the changes are deployed, the devices do *not* reboot.
4. Configure private resources in Secure Access.

   Private resources include applications, networks, or subnets your organization controls. They are not publicly accessible from outside your network.

Define private resources and specify connection information for the resources.

5. Create access policy rules and associate them with the private resources.

   Configure access rules to determine which users and devices can access the resource using the enabled connection methods.

6. Associate the private resources with the Threat Defense device.

   Verify that all configurations from Secure Access are synchronized with the Threat Defense devices.

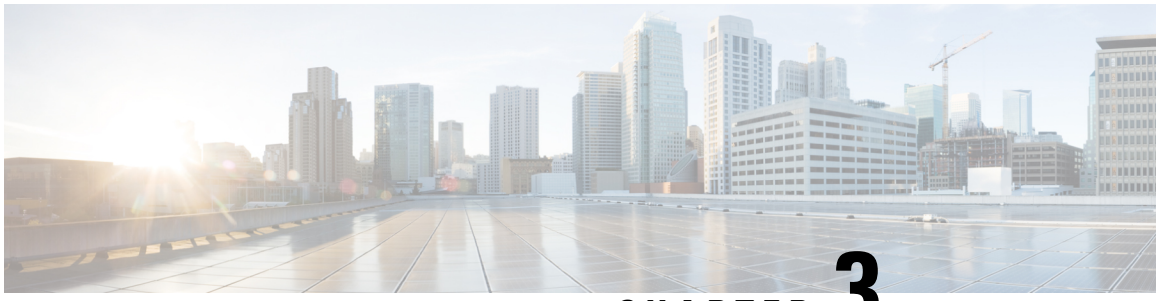
7. Configure Secure Client for universal ZTNA.

   - Install Secure Client version 5.1.10 or later on remote user devices.
   - Enroll the user with Secure Access and enable zero trust access.

Result

After deployment, monitor logs and events on both the Secure Access and Firewall Management Center dashboards to analyze and troubleshoot issues.

For configuration details, refer to the Universal Zero Trust Access Configuration Guide and the Secure Client Administration Guide.



CHAPTER 3

Deployment of Universal ZTNA solution

Universal ZTNA provides a secure and controlled way to access applications based on zero trust principles. An administrator workflow includes setting up the infrastructure (onboarding Secure Access and Firewall to Security Cloud Control), configuring policies on Secure Access, deploying those policies to the enforcement point (Threat Defense devices), and monitoring the solution to ensure it is working as expected.

An administrator can deploy the universal ZTNA solution to achieve the following outcomes:

- Optimal path for traffic based on the user location
- Private inspection for sensitive applications

- Outcome 1: Optimal path for user traffic , on page 9
- Outcome 2: Private inspection for sensitive applications, on page 13
- Configuration workflow, on page 15
- Monitoring events, on page 27

Outcome 1: Optimal path for user traffic

Universal ZTNA uses the trusted network detection (TND) mechanism to detect whether a user is inside a trusted network (on-premises) or in an untrusted network (remote). Based on this location, universal ZTNA dynamically steers user traffic through the nearest enforcement point, ensuring security and optimal performance.

On-premises users: When a user logs in through the office network, user traffic is routed through the local Firewall (Threat Defense device), which acts as the enforcement point. This routing prevents unnecessary traffic through the cloud, avoiding latency and optimizing network performance.

Remote users: When a user is located outside a trusted network, user traffic is proxied through the cloud-based Secure Access service, which evaluates policies and proxies traffic securely in the cloud.

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.

Secure Access enables you to define a trusted network based on specific criteria, such as DNS server addresses, DNS domains, and trusted servers. These trusted networks are included in TND profiles, which are then updated on the Secure Client.

When a user requests access to network resources, the Secure Client installed on the user's device detects the network context of the user. It includes this network information in the access request to Secure Access. Secure Access evaluates the TND data and determines how to route the user's access request:

- If the user is on a trusted network and the TND criteria match, the access request is routed through the on-premises firewall.
- If the TND criteria do not match, Secure Access identifies the user as being on an untrusted network and fulfills the access request through the cloud.

This hybrid approach ensures secure and optimized access to private network resources.

Sample Scenario

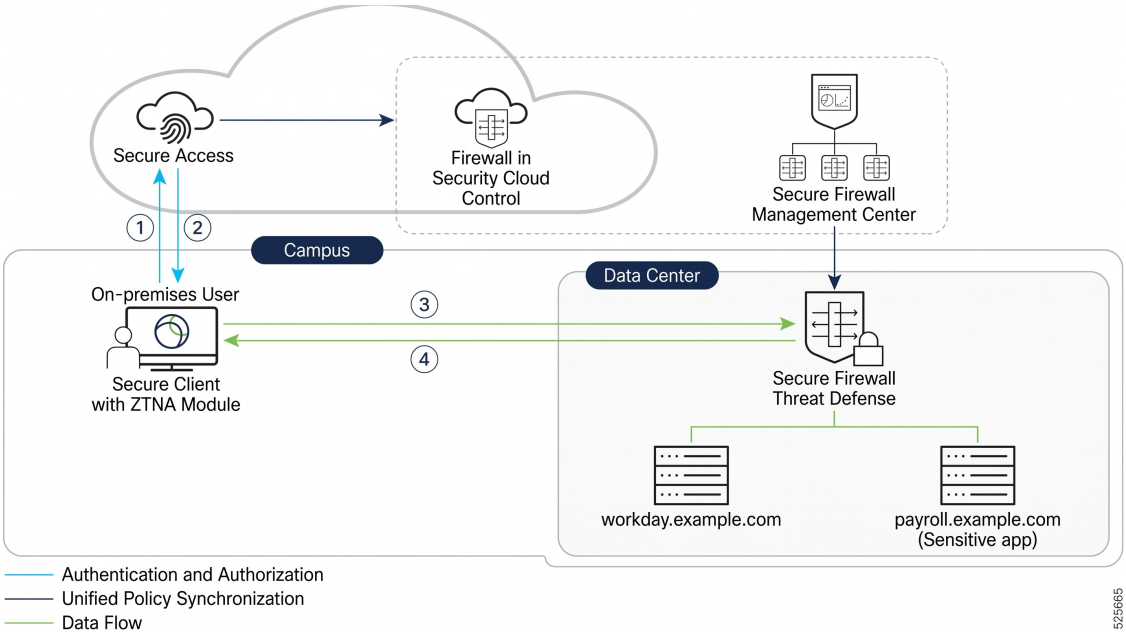
For example, Lee works from the office campus, and John works from home. When accessing HR resources such as https://workday.example.com, traffic is routed based on the user's location. For users who connect from office campus (example Lee), traffic is routed through the local Firewall (Threat Defense device)—avoiding unnecessary cloud traffic. For users who connect from outside the corporate network (example John), traffic is proxied through cloud-based Secure Access, which evaluates policies and ensures secure connectivity.

Data flow for an on-premises user

For a user operating within the private network, traffic to an internal resource is directed to the on-premises Threat Defense device, rather than being routed through the cloud.

In the sample scenario, Lee is working from the office campus and tries to access the internal resource workday.example.com through a browser.

Figure 3: Universal ZTNA Data Flow for On-Premises User



This sequence of events occurs when a user tries to access the internal resource, https://workday.example.com, from the office campus (trusted network):

- Secure Client Request: The secure client installed on Lee's laptop intercepts the connection and sends a connect request to Secure Access.
- Secure Access Policy Evaluation and Response: Secure Access evaluates the request based on the configured policies. These policies consider factors such as Lee's identity, device posture, and the application being requested. Since Lee is entitled to access this application, Secure Access authenticates Lee's credentials and authorizes the access request. It then sends a redirect message with a token as the response. Since Lee is within a trusted network, Secure Access redirects the Secure Client to the Threat Defense device.
- Secure Client Sends Access Request to Threat Defense: Secure Client sends a connect request to the Firewall Threat Defense device, providing the token and requesting access to workday.example.com.
- Firewall Threat Defense Validates and Enforces Security Profiles: Threat Defense device uses its configured DNS server to resolve the internal resource's FQDN to an IP address on the internal network. Threat Defense validates the token sent by Secure Client and responds with OK as the response. This establishes a connection between the Secure Client and the Threat Defense device. Threat Defense allows user access to https://workday.example.com and enforces security policies, such as IPS, file, and malware protection on the user traffic.

Data flow for a remote user

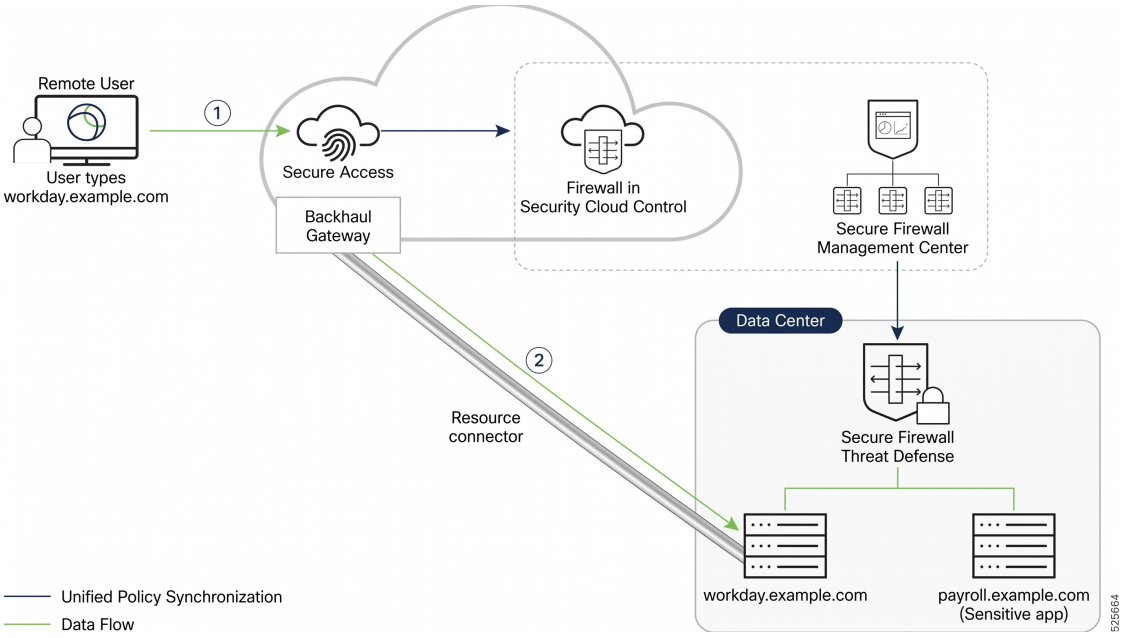
For a user operating from outside the private network, traffic to an internal private resource is directed through the cloud.

Summary

In the sample scenario, John is working from home and tries to access the internal resource workday.example.com through the browser.

Workflow

Figure 4: Universal ZTNA Data Flow for Remote User



This sequence of events occurs when John tries to access the internal resource (workday.example.com) from outside the office campus (untrusted network):

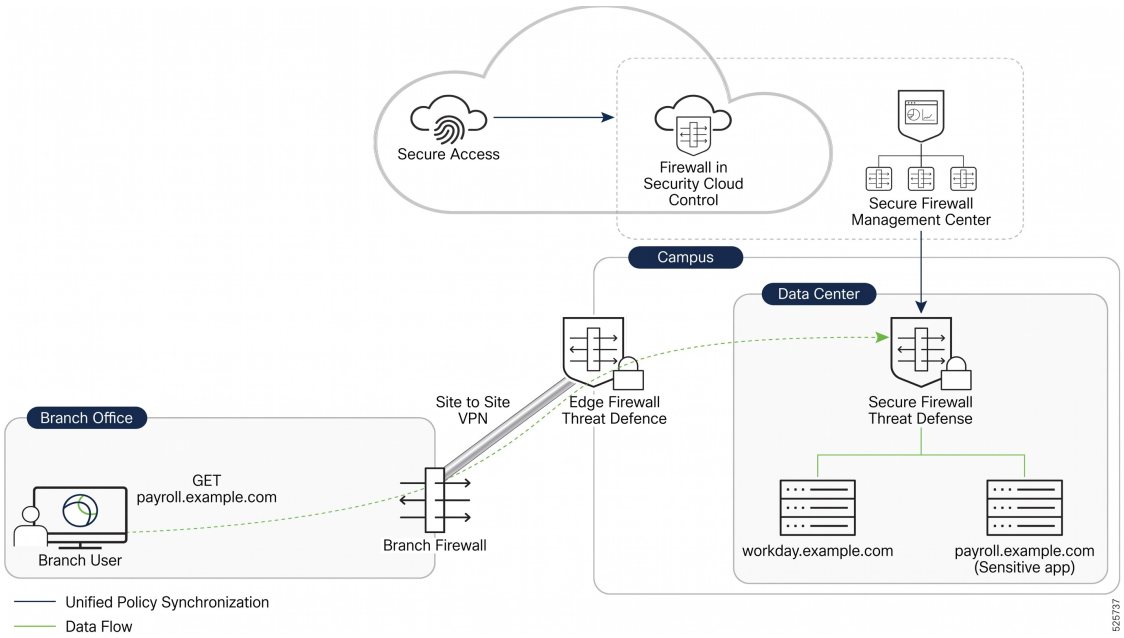
1. Secure Client intercepts the request: The Secure Client on John's system checks and finds that https://workday.example.com is a ZTNA-enabled application. It sends a connect request to Secure Access.
2. Secure Access Policy Evaluation and Response: Secure Access evaluates the policies and the user identity. Trusted Network Detection mechanism recognizes that the request has originated from an untrusted network. Secure Access Gateway establishes a connection to the Resource Connector, which then connects to workday.example.com residing on the private network.

Traffic from John's system to the private resource is routed through the Secure Access cloud.

Data flow for a branch user

In a typical enterprise network, multiple firewalls are deployed to enhance security and network segmentation. For example, a firewall at the Data Center protects private resources in a large enterprise. Branch offices are protected by branch firewalls and connect to the main campus through a site-to-site virtual private network (VPN).

Figure 5: Universal ZTNA Data Flow for a Branch User



Authentication and authorization for any universal ZTNA user occur in Secure Access. The Secure Client on the branch user's device obtains the authentication token from Secure Access and redirects the user to the Data Center firewall for access to private resources.

Data traffic from a branch user terminates at the edge firewall, which then establishes a connection with the Data Center firewall to forward the traffic.

Outcome 2: Private inspection for sensitive applications

Universal ZTNA enables private inspection of sensitive applications such as source code, and internal applications. It allows traffic destined for these applications to be inspected locally by the firewall instead of routing it through the cloud. This ensures that sensitive data remains within the trusted network perimeter and is subject to inspection policies, including Intrusion Prevention System (IPS) policies, file policies, and malware policies.

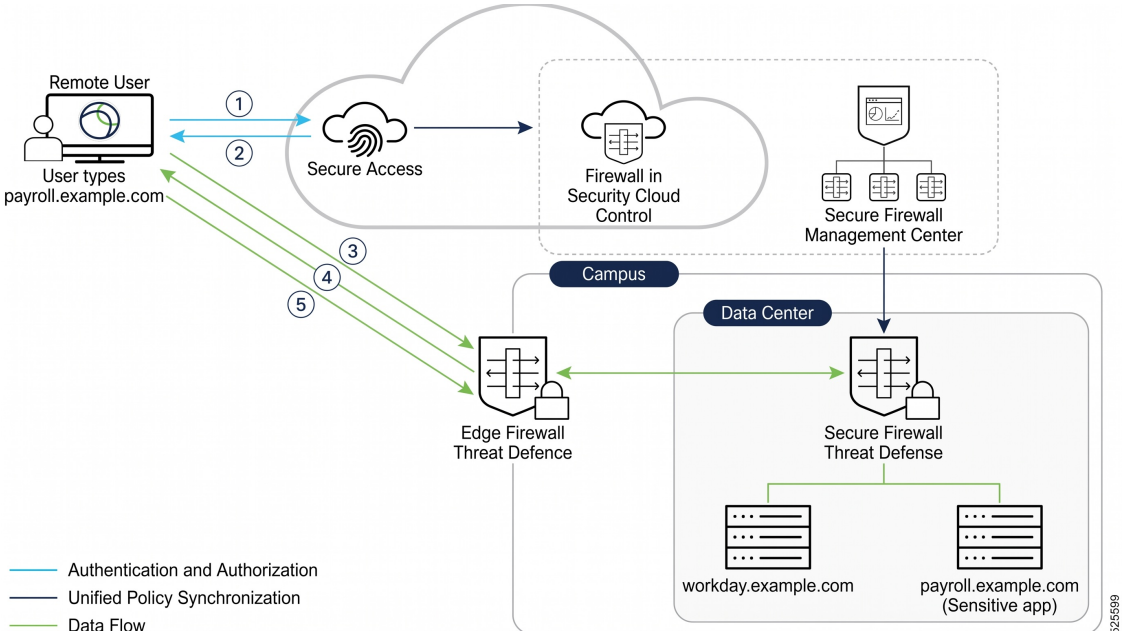
On-premises users and remote users: Traffic is routed through the local firewall (Threat Defense device), which acts as the enforcement point.

Data flow to a sensitive application from a remote user

This topic outlines the sequence of events that occur when a remote user attempts to access an internal resource from an untrusted network.

When a user operates from outside the private network, the local firewall directs user traffic to a sensitive resource. In this scenario, John works from home and tries to access the internal resource, payroll.example.com, through a browser.

Figure 6: Universal ZTNA Traffic Flow for Remote User



This is the sequence of events that happen when John tries to access the internal resource (payroll.example.com) from an untrusted network.

1. Secure Client request:

   The secure client installed on John's system intercepts the connection and sends a connect request to Secure Access.

2. Secure Access policy evaluation and response:

   Secure Access evaluates the request based on the configured policies. These policies consider factors like John's identity, device posture, and application being requested. Because John is an employee who is entitled to access payroll information, Secure Access authenticates John's credentials and authorizes the access request. It then sends a response with a token, redirecting Secure Client to the Threat Defense device.

3. Secure Client sends access request to Threat Defense device:

   Secure Client sends a connect request to the Firewall Threat Defense device, providing the token and requesting access to payroll.example.com.

4. Threat Defense device validates the request:

   The Threat Defense device uses its configured DNS server to resolve the internal resource’s FQDN to an IP address on the internal network. It validates the token sent by Secure Client and responds with "OK".

5. Threat Defense device enforces security policies:

   Threat Defense enforces the security policies, including IPS, file, and malware policies on the user traffic to payroll.example.com.

Configuration workflow

This reference provides the key steps to enable optimal path and private inspection for applications using Universal Zero Trust Access.

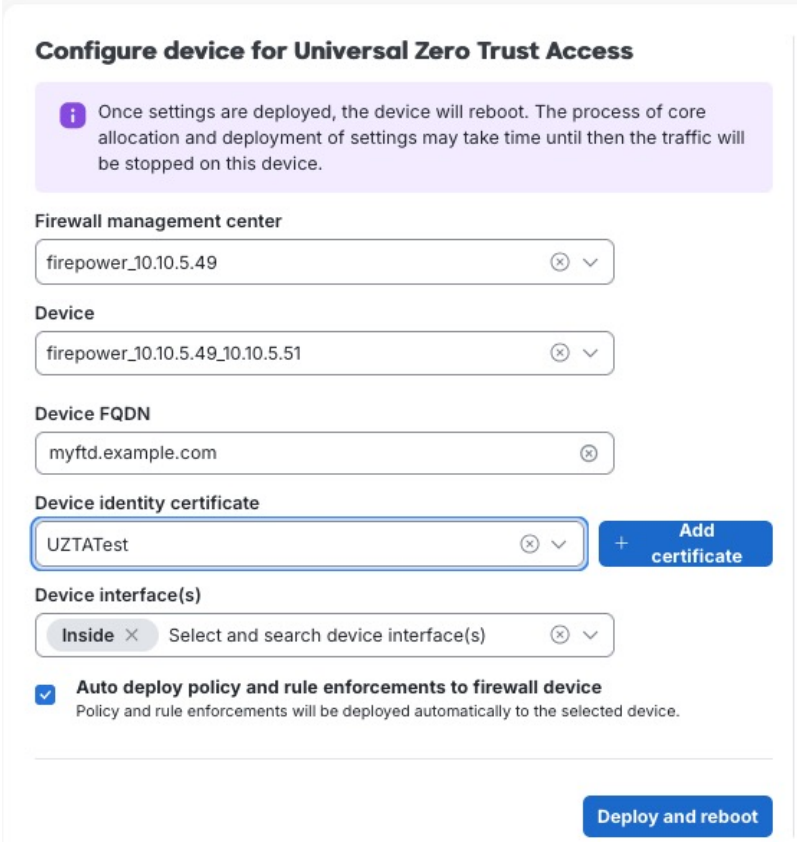
For detailed instructions, refer to the *Universal Zero Trust Network Access Configuration Guide*.

Note Unless specified otherwise, the term Firewall Management Center refers to both cloud-delivered and on-premises Firewall Management Center.

Table 1: Configuration Workflow Steps

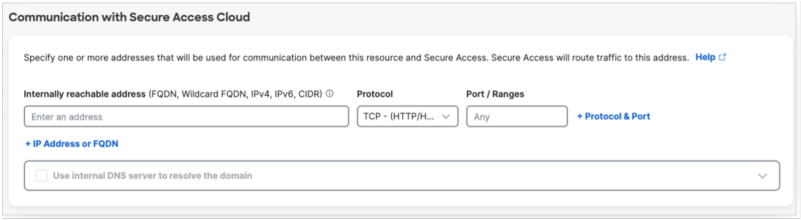
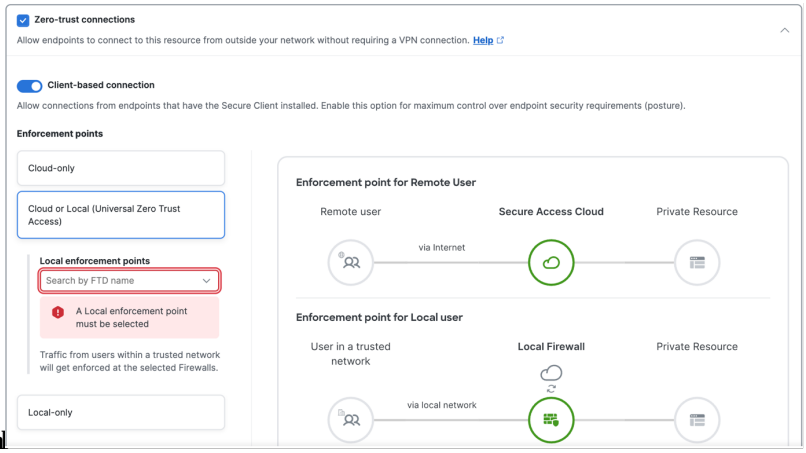
Configuration Task	Description
1. Onboard Secure Access and Firewall in Security Cloud Control	**1.** In a Security Cloud Control organization, claim a subscription to activate Secure Access and Security Cloud Control Firewall Management. **2.** Configure user management in Secure Access by setting up users and groups, either manually or by integrating with an identity provider. Enable the cloud-delivered Firewall Management Center if you have one. **3.** (This step applies only to Outcome 1: Optimal path for user traffic.) Configure one or more trusted networks through Secure Access. We recommend configuring a default trusted network. Secure Access automatically assigns a default trusted network to a universal ZTNA-enabled Firewall Threat Defense device. **4.** Update Secure Access with the CA certificate for the ZTNA user.
2. Prepare and set up Firewall Management Center and Firewall Threat Defense devices	**1.** Install the universal ZTNA build on the devices. Ensure that the Firewall Management Center has a smart license registered. **2.** Specify these configurations on the Management Center for the Firewall Threat Defense device: **a.** Routed interfaces to route the traffic **b.** Platform settings **c.** Domain Name Server (DNS) to resolve the IP address of the internal resources **3.** Onboard the on-premises Firewall Management Center to Security Cloud Control.

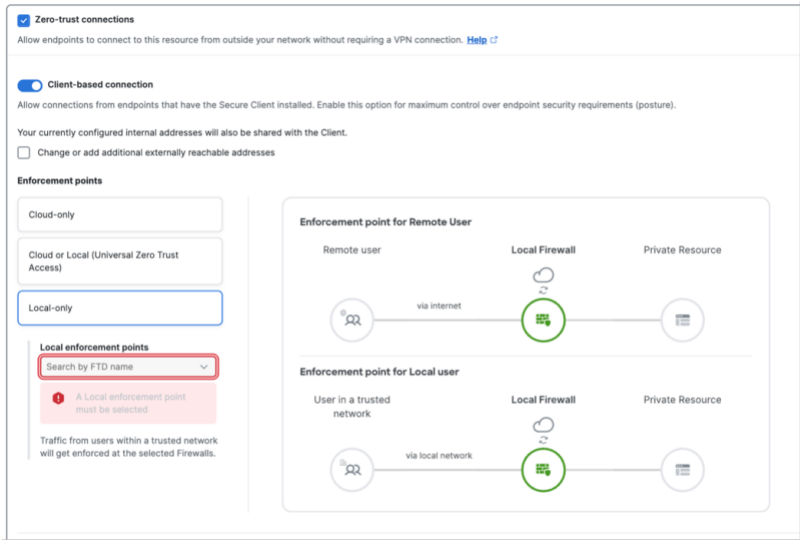
Configuration Task	Description
3. Configure the Threat Defense devices	

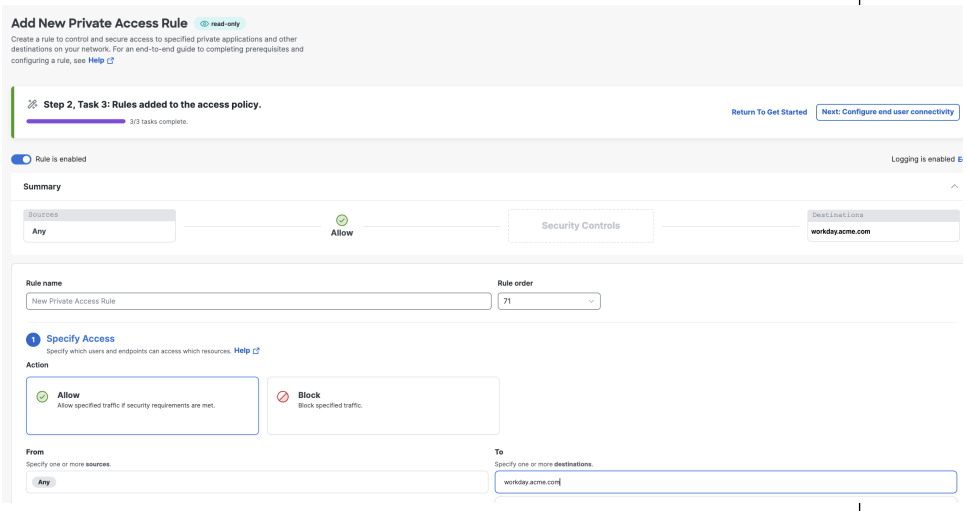
Configuration Task	Description
	1. Enable **universal zero trust network access settings** for the Firewall Threat Defense device (**Security Cloud Control** > **Security Devices** > **Firewall Threat Defense device**): **a.** Configure the device FQDN, inside interface, outside interface, and PKCS #12 certificate to enable universal ZTNA .  **b.** Deploy the changes. **Note** If your device operates version 7.7.10 or 10.0, it reboots so the system can reallocate resources for universal ZTNA components. During the reboot, traffic through this device is disrupted. If you deploy a High Availability pair of devices, both devices reboot simultaneously and traffic is disrupted. **c.** To see the events during the deployment process, click **Device Actions** > **Workflows** on the Security Devices page. After the changes are deployed, the device is connected to Secure Access. **2.** Check the availability of the Threat Defense device under Secure Access. **a.** Choose **Secure Access** > **Connect** > **Network Connections** . **b.** Click the **FTD** tab.

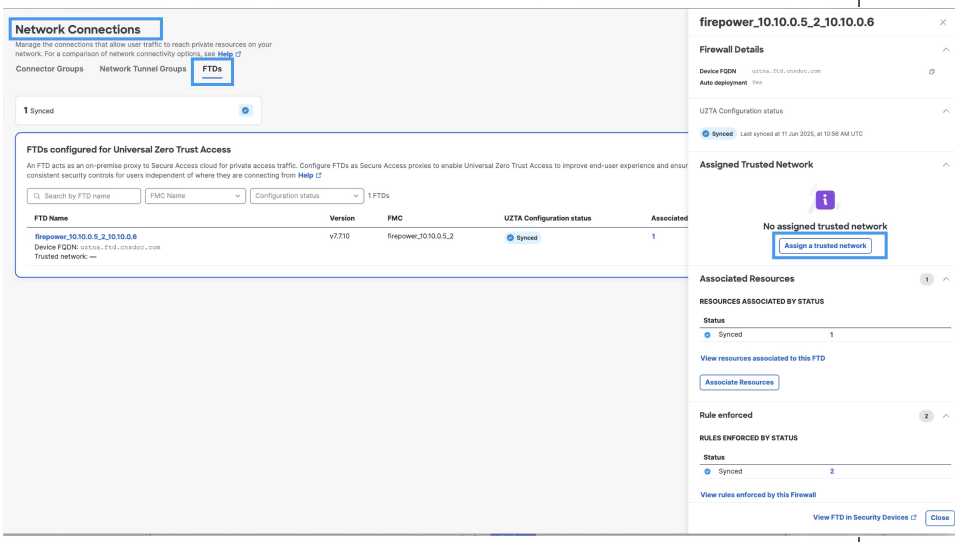
Configuration Task	Description
	Universal ZTNA -enabled devices are displayed. For more information, see "Configure Security Devices" in the *Universal Zero Trust Network Access Configuration Guide* .

Configuration Task	Description
4. Configure a private resource (payroll.example.com) on Secure Access	

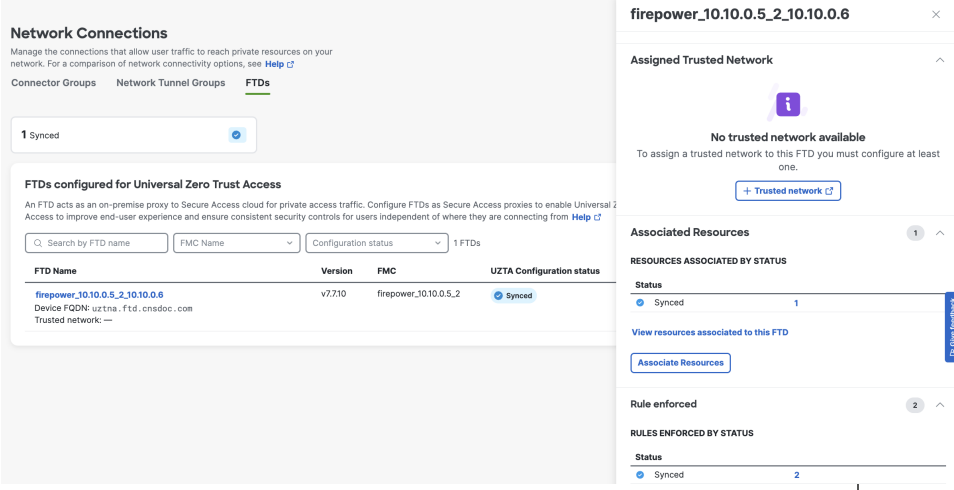
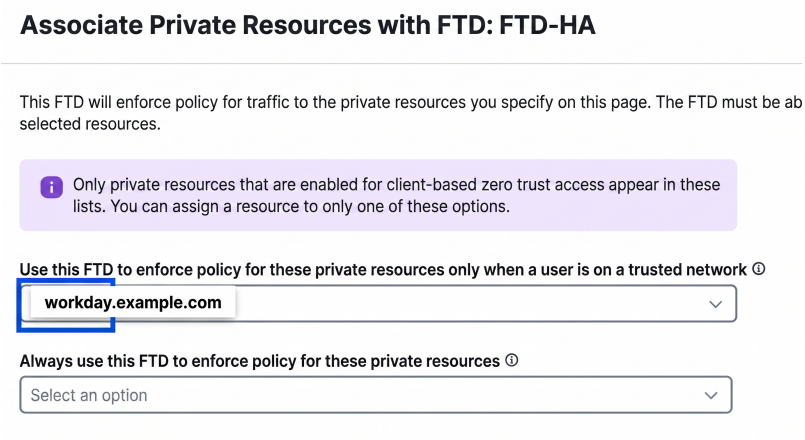
Configuration Task	Description
	In Security Cloud Control: **1.** Choose **Secure Access** > **Resources** > **Destinations** > **Private Resources** and click **+Add** . Specify the method Secure Access uses to communicate with the resource.  **2.** Specify how users can access this private resource: Under **Endpoint Connection Methods** , choose **Zero-trust connections** > **Client-based connection** . **3.** Specify the enforcement points. For Outcome 1: Optimal path for user traffic, select **Cloud or Local**  For Outcome 2: Private inspection for sensitive applications, select **Local only**.

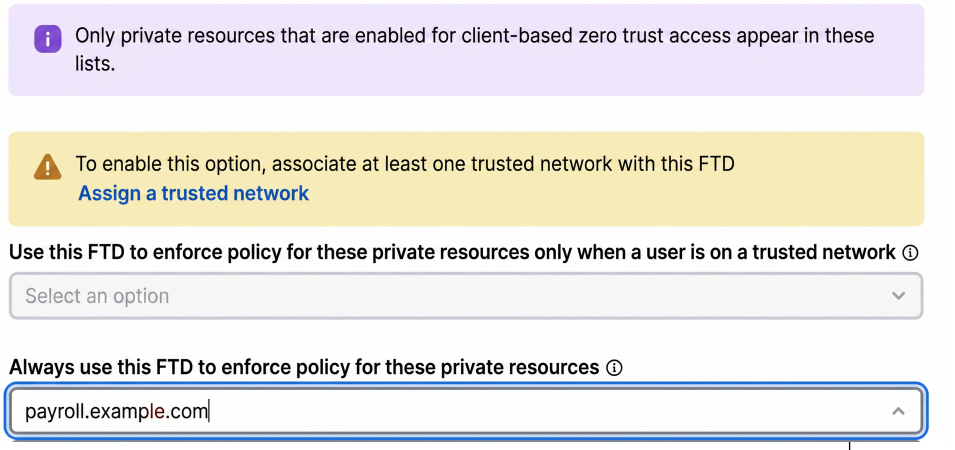
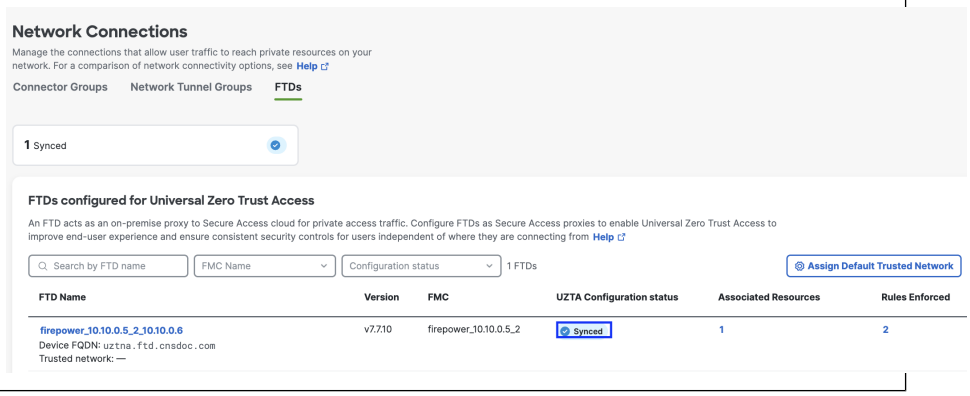
Configuration Task	Description
	 From the **Local enforcement points** drop-down list, select a device to enforce the policies. **4.** Save your configuration.

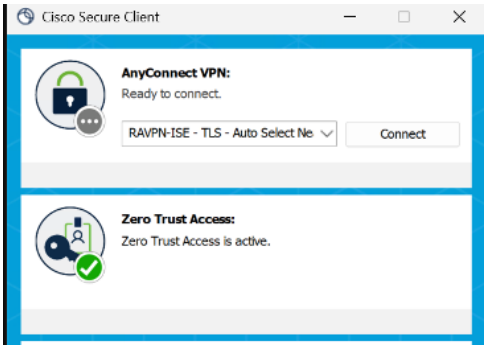
Configuration Task	Description
5. Create an Access Policy to allow users access to the private resource	In Security Cloud Control: **1.** Choose **Secure Access** > **Secure** > **Policy** > **Access Policy** > **Add Rule** > **Private Access** .  **2.** Specify the resources that an endpoint can access.  Next, follow the on-screen prompts to configure security such as Intrusion Prevention (IPS).

Configuration Task	Description
(Only for Outcome 1: Optimal path for user traffic) Verify that the Threat defense device is associated with a trusted network.	Assigning a trusted network to the device allows universal ZTNA to route user traffic to the correct Threat Defense device. Also, the device inspects and enforces security policies on traffic originating from or destined to that trusted network. This ensures that even trusted networks are continuously monitored for threats and policy compliance. Assign a trusted network to the Threat Defense device by completing these steps: 1. Click **Assign a Trusted Network**.  2. From the **Trusted Networks** drop-down list, select a trusted network to map to the device. 3. Click **Save**.

Configuration Task	Description
6. Associate the private resource to the Firewall Threat Defense Device	

Configuration Task	Description
	In Security Cloud Control: 1. Choose **Secure Access** > **Connect** > **Network Connections** > **FTDs** . 2. Click a device in the **FTD Name** column.  A slide-in pane displays details of the selected Firewall Threat Defense device. 3. Under **Associated Resources**, click **Associate Resource**. 4. In the **Associate Private Resources with FTD** window: (For Outcome 1: Optimal path for user traffic) Select the private resource from the **Use this FTD to enforce policy for private resources only when a user is in a trusted network** drop-down list.  (For Outcome 2: Private inspection of sensitive applications) Select the private resource from the **Always use this FTD to enforce policy for these private resources** drop-down list.

Configuration Task	Description
	This FTD will enforce policy for traffic to the private resources you specify on this page. The FTD must be able to reach all selected resources.  5. Click **Save**.
7. Wait for the UZTNA Configuration Status to display “Synced”	Secure Access policy and access configurations are automatically deployed to the Firewall Threat Defense device. Successful configuration synchronization displays a "Synced" status. 

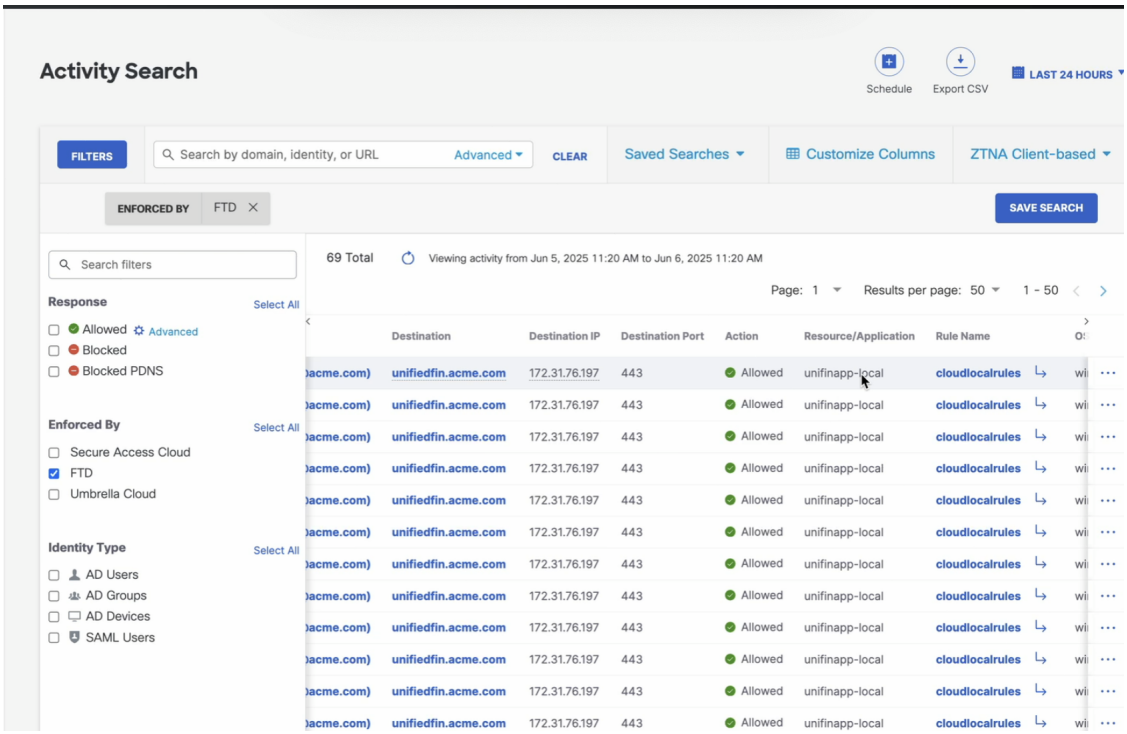
Configuration Task	Description
8. End User Device Configuration	**1.** Install Secure Client version 5.1.10 or later on the user devices. **2.** Enroll the user with Secure Access using the device enrollment certificate **3.** Enable Zero Trust Access in Secure Client.  For information on setting up Secure Client, refer to Secure Client Administration Guide .

Monitoring events

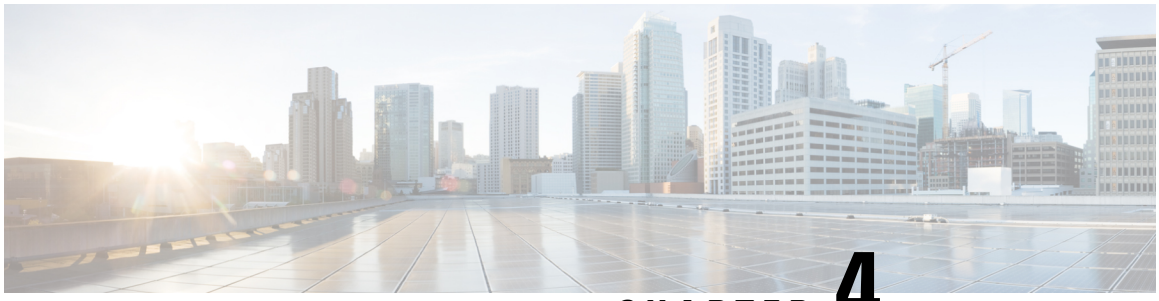
After you deploy universal ZTNA, you can monitor the access events in real time. Traffic to and from the private resources that traverses the Firewall Threat Defense is sent to Secure Access. Secure Access aggregates event logs from all access points and provides a centralized monitoring dashboard.

To see a log of the universal ZTNA activities, do these steps:

1. In Security Cloud Control, choose **Secure Access** > **Monitor** > **Activity Search**.
2. Click **All** under the **Filters** menu and select **ZTNA Client-based**.



3. Choose **FTD** to monitor the events and policies enforced by the Threat Defense device.



CHAPTER 4

Troubleshooting Universal ZTNA

This section provides a troubleshooting guide for universal ZTNA configuration. It outlines common issues, their symptoms, and the Workaround or Solution required to diagnose and resolve them across various components including Firepower Threat Defense (FTD), Secure Access, Firewall Management Center (FMC), and Security Cloud Control (SCC Firewall).

- Issue: Private resource not reachable, on page 29
- Issue: universal ZTNA-enabled Threat Defense device not visible in Secure Access, on page 30
- Issue: Configuration deployment to device fails, on page 31

Issue: Private resource not reachable

A user is unable to connect to the private resource by using either its IP address or its fully qualified domain name (FQDN).

To troubleshoot this issue, perform these steps:

In Secure Access:

- Confirm that the private resource is correctly defined under **Resources** > **Destinations** > **Private Resources**.
- Confirm that an access policy rule allows the user access to the private resource.
- Confirm that the private resource is associated with the correct Firewall Threat Defense device under **Connect** > **Network Connections** > **FTDs**.
- Use the Activity Search report to view all zero trust events on Secure Access. Apply the **ZTNA Client-based** filter, and filter by **FTD** as the enforcement point.

In Firewall:

- Confirm that the DNS servers on Firewall Management Center are correctly configured so that the Threat Defense device can resolve private resource names.
- Confirm that the internal DNS server has entries for the private resources.
- Confirm that the DNS policy is correctly deployed to the Firewall Threat Defense device.

Issue: universal ZTNA-enabled Threat Defense device not visible in Secure Access

Configuration changes made in Secure Access are not reflected on the Firewall Threat Defense device after a commit.

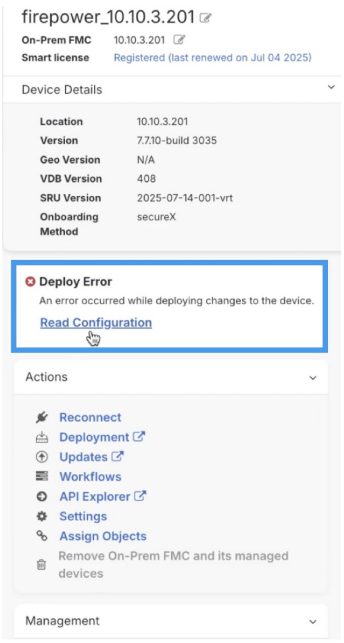
After you have completed the universal ZTNA settings on a Threat Defense device and rebooted it, Secure Access must display this device on the **FTDs configured for Universal Zero Trust Access** page. In rare instances, however, the Threat Defense device may not be available on Secure Access.

To troubleshoot this issue, check if the configurations from Secure Access are deployed on the Threat Defense device.

1. Choose **Firewall** > **Administration** > **Integrations** > **Firewall Management Center**.
2. Under the **FMC** tab, click the Management Center that manages the device.

   A slide-in pane on the right displays the details and status of the selected Management Center.
3. Depending on the required corrective action, such as Read Configuration or Check for Status, click the appropriate action button.

   This example describes an error that occurs when deploying the configurations to the device.



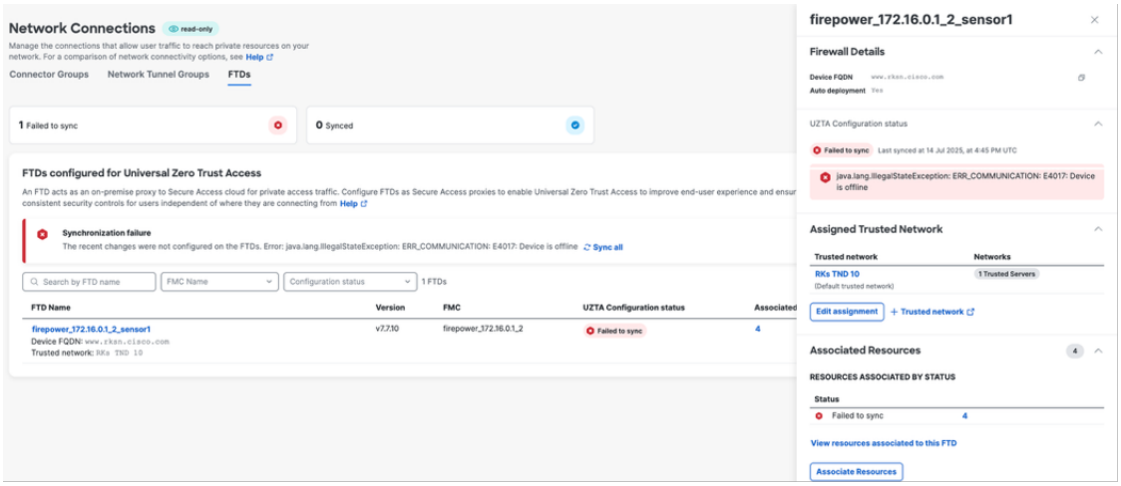
4. Click **Read Configuration**.

   The Firewall reads the device configuration and communicates to Secure Access that a universal ZTNA-enabled Threat Defense device is present.



Issue: Configuration deployment to device fails

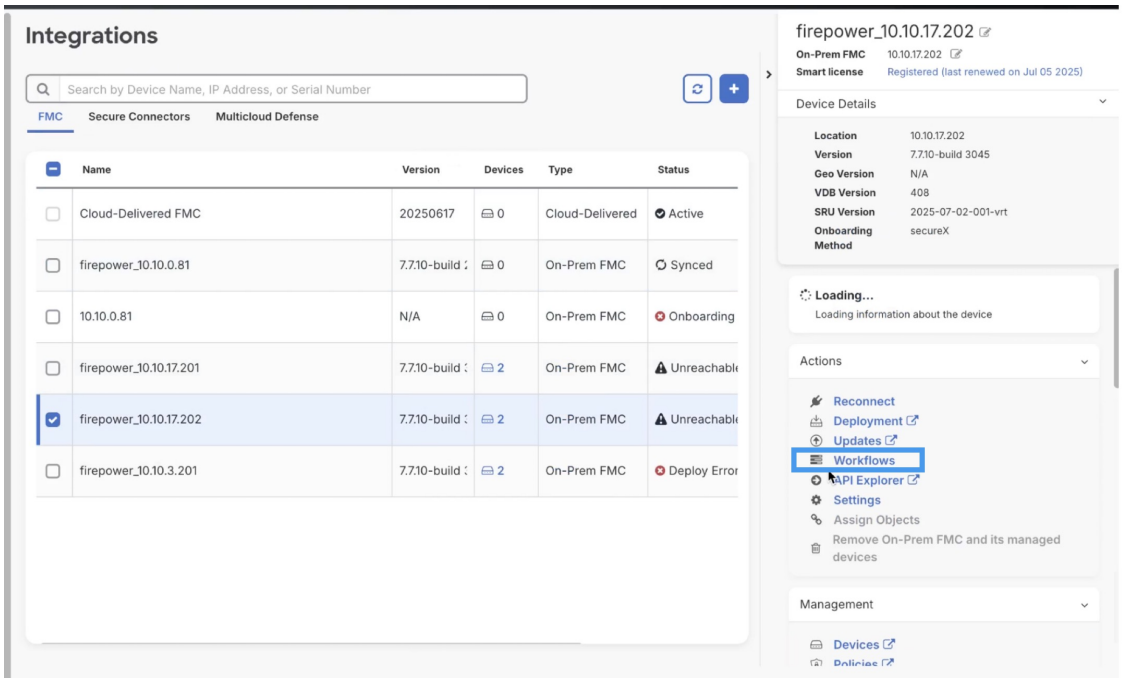
The Firewall Threat Defense device displays a "Failed to Sync" or "Syncing" status. Configuration changes are not deployed to the Threat Defense device.



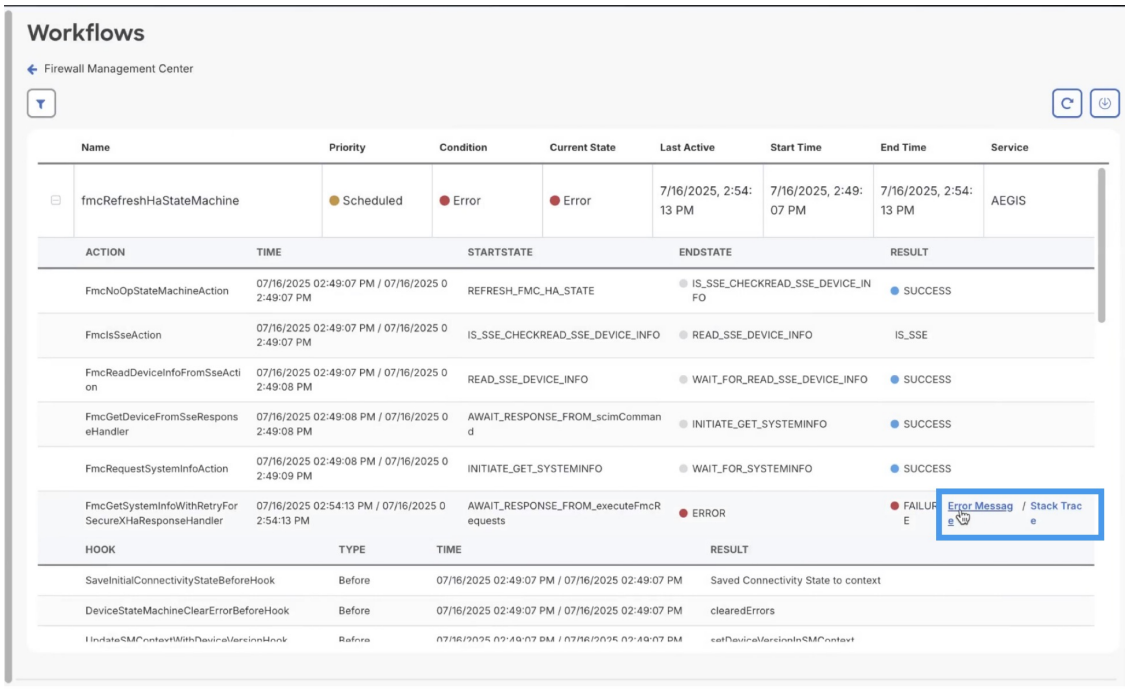
To troubleshoot this issue:

- Identify the reason for failure to deploy the configurations on the device:
  1. In Secure Access, choose **Connect** > **Network Connections** > **FTDs** to see the list of Firewall Threat Defense devices.
  2. Click the name of the device you want to troubleshoot.
  3. The slide-in pane displays the reason for the failure to synchronize the configurations with the Threat Defense device.

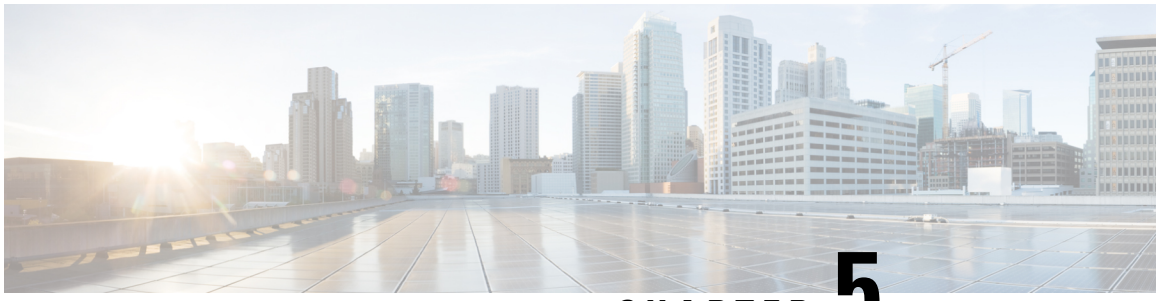
- Check the Workflows on Firewall Management Center to see the cause of the error:
  1. Choose **Firewall** > **Administration** > **Integrations** > **Firewall Management Center**.
  2. From the list of Firewall Management Centers, click the Management Center that manages the Threat Defense device with an issue.



3. In the slide-in pane, click **Workflows**.
4. In the **Workflows** page, expand the state machine entry that shows an **Error** state.



5. Click **Error Message** to view the error.
6. Click **Stack Trace** to obtain the call stack for further investigation.



CHAPTER 5

Related Documentation

Additional documents you can refer to.

- Related Documentation, on page 33

Related Documentation

For a visual walkthrough of the configuration process, watch the videos at this link.

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

To know more about...	Read this document...
Universal Zero Trust Network Access Configuration	Universal Zero Trust Network Access Configuration Guide
Secure Access	Secure Access Help Center
Firewall in Security Cloud Control	What's New for Firewall Management Center in Security Cloud Control
Security Cloud Control	Getting Started Guide for Security Cloud Control
Firewall Threat Defense	Secure Firewall Management Center Device Configuration Guide Secure Firewall Threat Defense Release Notes
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

Related Documentation