Troubleshooting Universal ZTNA

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

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 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.

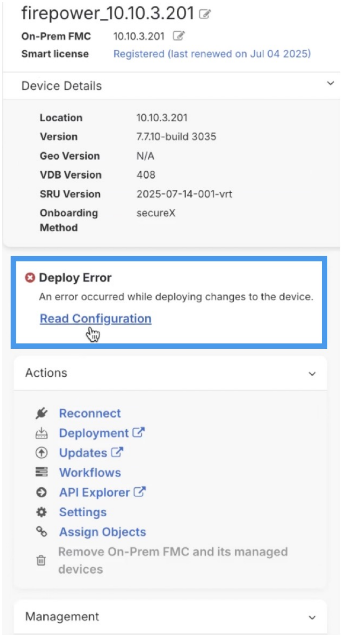
1. Choose **Firewall** > **Administration** > **Integrations** > **Firewall Management Center**.

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.



firepower_10.10.3.201

On-Prem FMC	10.10.3.201
Smart license	Registered (last renewed on Jul 04 2025)

Device Details

Location	10.10.3.201
Version	7.7.10-build 3035
Geo Version	N/A
VDB Version	408
SRU Version	2025-07-14-001-vrt
Onboarding Method	secureX

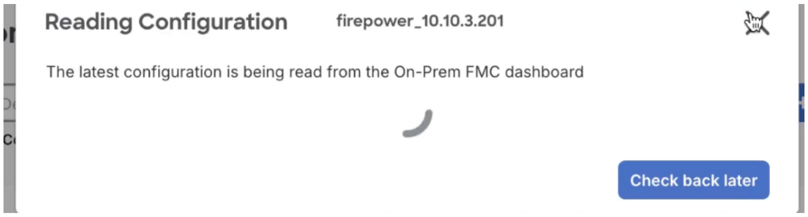
Deploy Error

An error occurred while deploying changes to the device.

Read Configuration

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.

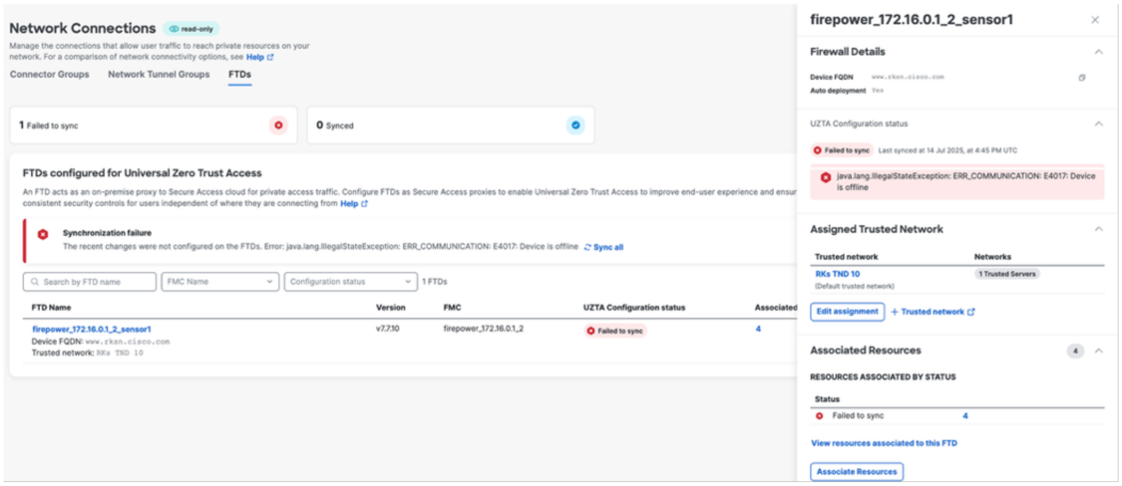


Reading Configuration firepower_10.10.3.201

The latest configuration is being read from the On-Prem FMC dashboard

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.



Network Connections read-only

Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help

1 Failed to sync

0 Synced

FTDs configured for Universal Zero Trust Access

An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve end-user experience and ensur consistent security controls for users independent of where they are connecting from Help

Synchronization failure

The recent changes were not configured on the FTDs. Error: java.lang.IllegalStateException: ERR_COMMUNICATION: E4017: Device is offline

1 FTDs

FTD Name	Version	FMC	UZTA Configuration status	Associated
firepower_172.16.0.1_2_sensor1 Device FQDN: www.rksn.cisco.com Trusted network: RKs TND 10	v7.7.10	firepower_172.16.0.1_2	Failed to sync	4

firepower_172.16.0.1_2_sensor1

Firewall Details

Device FQDN www.rksn.cisco.com

Auto deployment Yes

UZTA Configuration status

Failed to sync Last synced at 14 Jul 2025, at 4:45 PM UTC

java.lang.IllegalStateException: ERR_COMMUNICATION: E4017: Device is offline

Assigned Trusted Network

Trusted network	Networks
RKs TND 10 (Default trusted network)	1 Trusted Servers

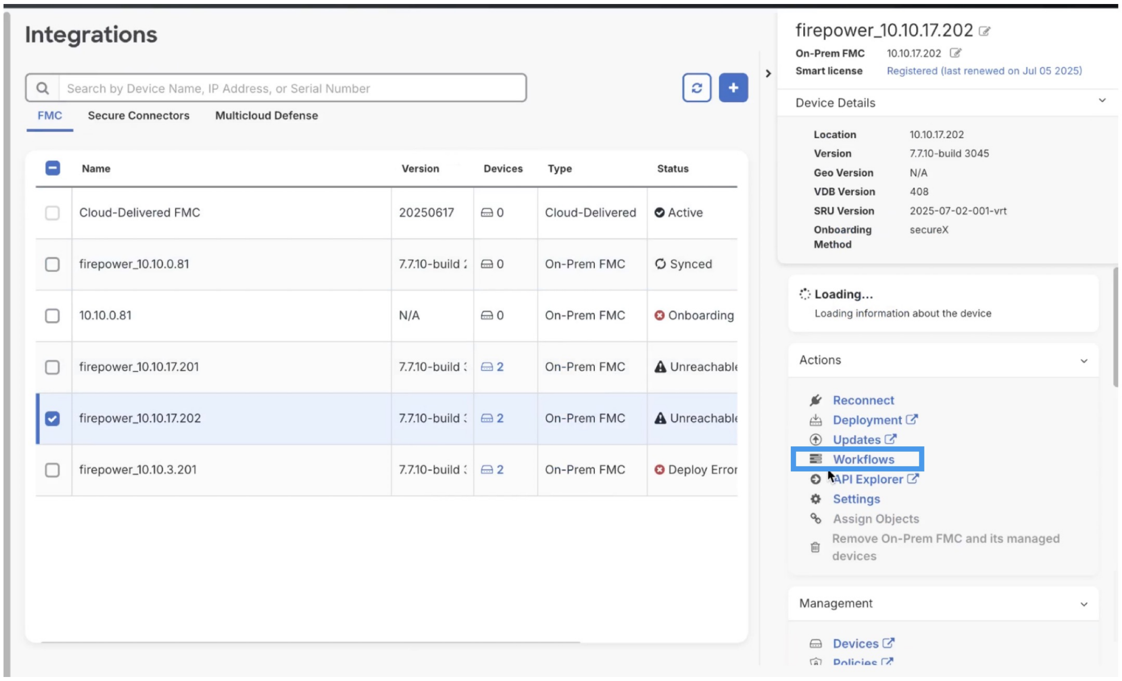
Associated Resources 4

RESOURCES ASSOCIATED BY STATUS

Status	
Failed to sync	4

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.



Integrations

Search by Device Name, IP Address, or Serial Number

FMC | Secure Connectors | Multicloud Defense

	Name	Version	Devices	Type	Status
□	Cloud-Delivered FMC	20250617	0	Cloud-Delivered	Active
□	firepower_10.10.0.81	7.7.10-build :	0	On-Prem FMC	Synced
□	10.10.0.81	N/A	0	On-Prem FMC	Onboarding
□	firepower_10.10.17.201	7.7.10-build :	2	On-Prem FMC	Unreachabl
☑	firepower_10.10.17.202	7.7.10-build :	2	On-Prem FMC	Unreachabl
□	firepower_10.10.3.201	7.7.10-build :	2	On-Prem FMC	Deploy Error

firepower_10.10.17.202

On-Prem FMC 10.10.17.202

Smart license Registered (last renewed on Jul 05 2025)

Device Details

Location	10.10.17.202
Version	7.7.10-build 3045
Geo Version	N/A
VDB Version	408
SRU Version	2025-07-02-001-vrt
Onboarding Method	secureX

Loading...

Loading information about the device

Actions

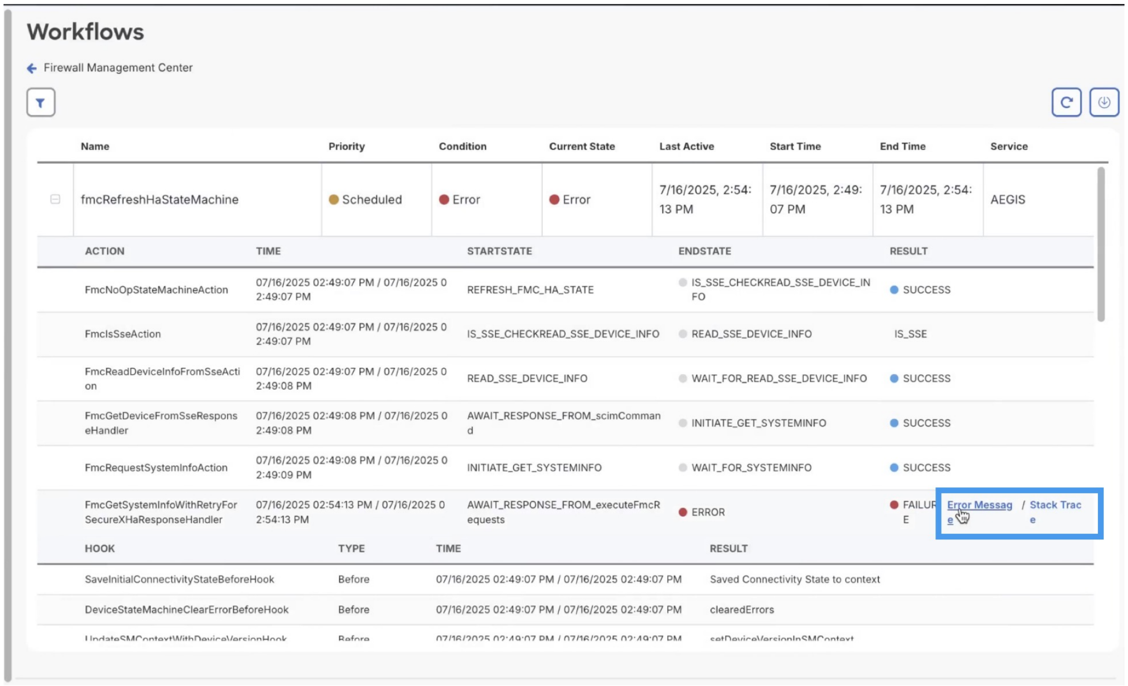
- Reconnect
- Deployment
- Updates
- Workflows
- API Explorer
- Settings
- Assign Objects
- Remove On-Prem FMC and its managed devices

Management

- Devices
- Policies

3. In the slide-in pane, click **Workflows**.

4. In the **Workflows** page, expand the state machine entry that shows an **Error** state.



Workflows

Firewall Management Center

Name	Priority	Condition	Current State	Last Active	Start Time	End Time	Service
fmcRefreshHaStateMachine	Scheduled	Error	Error	7/16/2025, 2:54:13 PM	7/16/2025, 2:49:07 PM	7/16/2025, 2:54:13 PM	AEGIS

ACTION	TIME	STARTSTATE	ENDSTATE	RESULT
FmcNoOpStateMachineAction	07/16/2025 02:49:07 PM / 07/16/2025 02:49:07 PM	REFRESH_FMC_HA_STATE	IS_SSE_CHECKREAD_SSE_DEVICE_INFO	SUCCESS
FmcIsSseAction	07/16/2025 02:49:07 PM / 07/16/2025 02:49:07 PM	IS_SSE_CHECKREAD_SSE_DEVICE_INFO	READ_SSE_DEVICE_INFO	IS_SSE
FmcReadDeviceInfoFromSseAction	07/16/2025 02:49:07 PM / 07/16/2025 02:49:08 PM	READ_SSE_DEVICE_INFO	WAIT_FOR_READ_SSE_DEVICE_INFO	SUCCESS
FmcGetDeviceFromSseResponseHandler	07/16/2025 02:49:08 PM / 07/16/2025 02:49:08 PM	AWAIT_RESPONSE_FROM_scimCommand	INITIATE_GET_SYSTEMINFO	SUCCESS
FmcRequestSystemInfoAction	07/16/2025 02:49:08 PM / 07/16/2025 02:49:09 PM	INITIATE_GET_SYSTEMINFO	WAIT_FOR_SYSTEMINFO	SUCCESS
FmcGetSystemInfoWithRetryForSecureXHaResponseHandler	07/16/2025 02:54:13 PM / 07/16/2025 02:54:13 PM	AWAIT_RESPONSE_FROM_executeFmcRequests	ERROR	FAILURE Error Message / Stack Trace

HOOK	TYPE	TIME	RESULT
SaveInitialConnectivityStateBeforeHook	Before	07/16/2025 02:49:07 PM / 07/16/2025 02:49:07 PM	Saved Connectivity State to context
DeviceStateMachineClearErrorBeforeHook	Before	07/16/2025 02:49:07 PM / 07/16/2025 02:49:07 PM	clearedErrors
UpdateSMContextWithDeviceVersionHook	Before	07/16/2025 02:49:07 PM / 07/16/2025 02:49:07 PM	setDeviceVersionInSMContext

5. Click **Error Message** to view the error.

6. Click **Stack Trace** to obtain the call stack for further investigation.