

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 1
- Issue: universal ZTNA-enabled Threat Defense device not visible in Secure Access, on page 2
- Issue: Configuration deployment to device fails, on page 3

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.

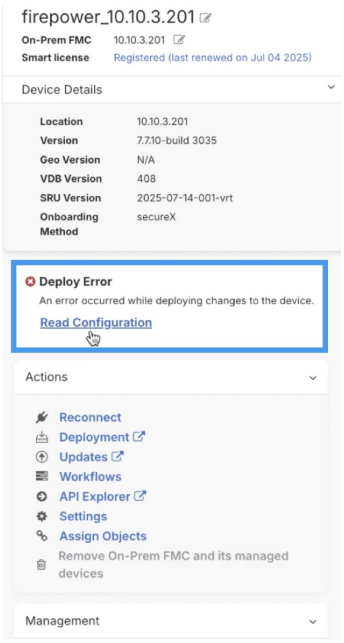
After you have completed the universal ZTNA settings on a Threat Defense device and rebooted it, Secure Access must display this device on the **FTDs configured for Universal Zero Trust Access** page. In rare instances, however, the Threat Defense device may not be available on Secure Access.

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.



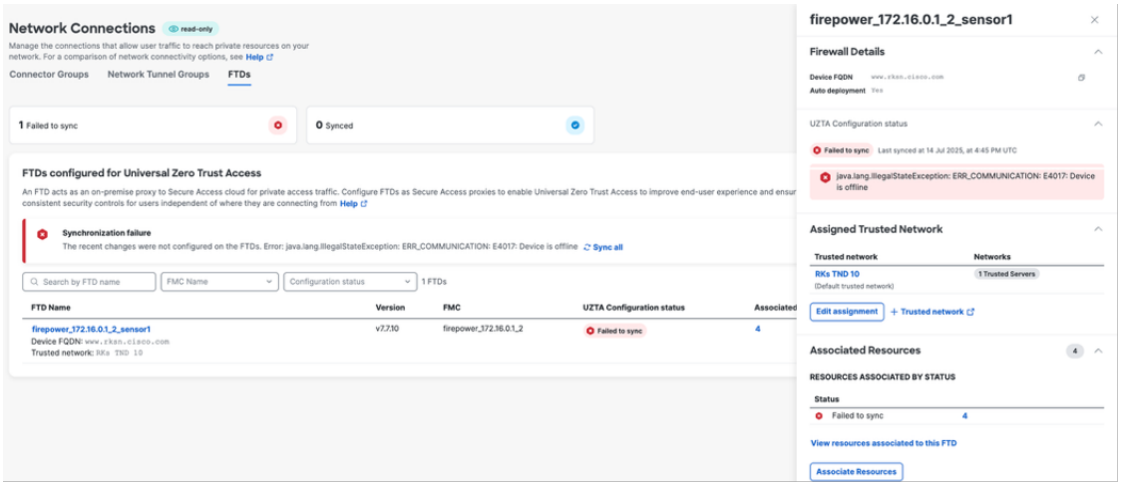
4. Click **Read Configuration**.

   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

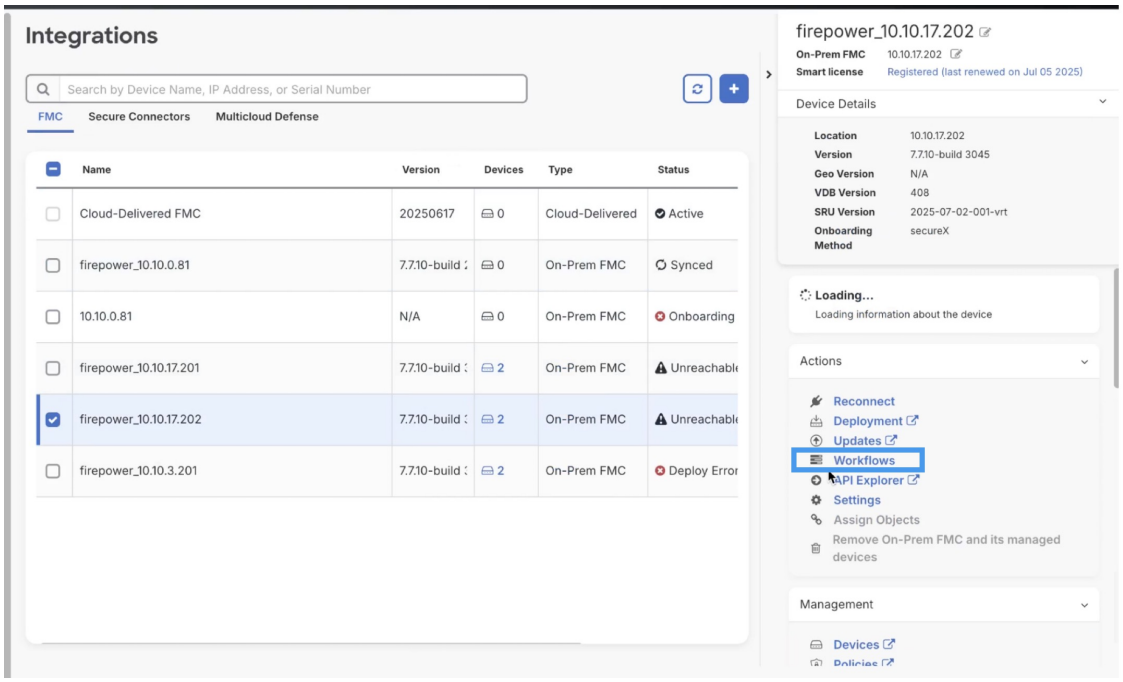
The Firewall Threat Defense device displays a "Failed to Sync" or "Syncing" status. Configuration changes are not deployed to the Threat Defense device.



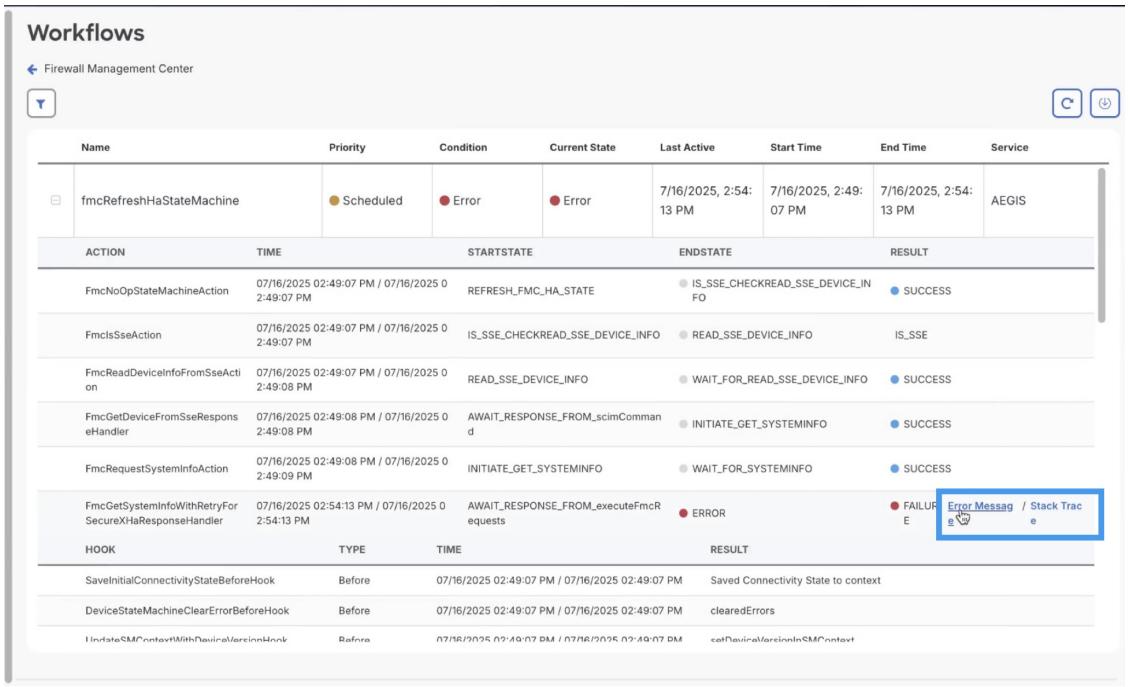
To troubleshoot this issue:

- 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.