Resolve "Posture Check Failed or Posture Too Old" Error in Activity Search for ZTNA Flow

Contents

Issue

After Enforcing Zero Trust Network Access Posture check, the issue manifests in two ways depending on policy configuration:

- When fail-open rule exists: Traffic bypasses posture enforcement and matches the "No Posture Checks" rule.
- When strict enforcement is enabled: Users are denied access to private applications.

Environment

- Cisco Secure Access — Zero trust network access Flow
- Duo Desktop

Resolution

Collecting Duo Desktop Diagnostics: Enable Debug Logging and Run the Support Tool

Step 1 - Enable Debug Logging (macOS and Windows)

1. Open the **Duo Desktop** app.

2. Navigate to **Preferences**.

3. Check **Enable detailed diagnostic reports**.

Step 2 - Reproduce the Issue

Step 3 — Collect the Dart Bundle - Collect DART Bundle for Secure Client

Step 4 — Run the Support Tool

The Support Tool script ships with **Duo Desktop 6.0.0+** and **Duo Device Health 2.26.1+** for macOS and Windows.

It collects the necessary files, scrubs them of sensitive information, and creates a ready-to-send ZIP.

Script locations

Windows

- Duo Desktop: `C:\Program Files (x86)\Duo Desktop\DuoDesktop-Support.ps1`

- Duo Device Health: `C:\Program Files (x86)\Duo Device Health\DeviceHealth-Support.ps1`

macOS

- Duo Desktop: `/Applications/Duo Desktop.app/Contents/Resources/duo_desktop_support.sh`

- Duo Device Health: `/Applications/Duo Device Health.app/Contents/Resources/device_health_support.sh`

Note: Paths differ between the older *Duo Device Health* releases and the newer *Duo Desktop* releases — use the pair that matches your installation.

What the Support Tool collects

Windows

1. Creates a ZIP to hold the collected information.

2. Runs `Invoke-WebRequest` to test connectivity to Duo.

3. Captures: system proxy settings; OS version, build, and bit; BitLocker status; time zone; Duo-related Application event logs.

4. Copies `...\AppData\Local\DuoDesktop\Logs` (or `...\DuoDeviceHealth\Logs`) into the ZIP.

5. Exports Duo registry keys from `HKLM:\SOFTWARE\Duo` and `HKCU\SOFTWARE\Duo Device Health` to `system_info.txt`.

6. Copies certificates associated with the loopback adapter `127.0.0.1`).

7. *(Optional)* Exports System Event logs.

8. Saves the ZIP to the signed-in user's Desktop, for example, `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` **(or** `DHA_Support_...zip`**).**

MacOS

1. Creates a ZIP to hold the collected information.

2. Runs `curl` to test connectivity to Duo.

3. Captures: system proxy settings; `install.log`; `system.log`; Duo-related crash logs; OS and kernel version.

4. Copies `/Users/user_name/Library/Logs/Duo Desktop/*.log` (or `Duo Device Health`) into the ZIP.

5. Copies certificates associated with the loopback adapter `127.0.0.1`).

6. *(Optional)* Exports all User and Kernel logs.

7. Saves the ZIP to the signed-in user's Desktop, for example, `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (or `DHA_Support_...zip`).

Command-line options

Windows (PowerShell)

Option | Description

| `-eventlogs` | Exports System logs. Options: `system` |

| `-days` | Number of days of Security event logs to export |

| `-user` | Specifies which user to gather logs from (needed when running as admin under a different username) |

| `Get-Help` | Built-in cmdlet; call it **before** the script, for example, `Get-Help .\DuoDesktop-Support.ps1` |

macOS (Terminal)

`-a` | Exports all User and Kernel panic logs.

`-h` | Displays a help message.

End-to-End Procedure

Windows (example: export system event logs from the last 2 days)

1. Open an **administrative PowerShell** session on the endpoint where Duo Desktop is installed.

2. **Enable debug logging** (Part 1).

3. **Reproduce** the Duo issue.

4. Run the **script**:

- Duo Desktop:

```powershell

**& 'C:\Program Files (x86)\Duo Desktop\DuoDesktop-Support.ps1' -eventlogs system -days 2**

```

- Duo Device Health:

```powershell

& 'C:\Program Files (x86)\Duo Device Health\DeviceHealth-Support.ps1' -eventlogs system -days 2
```

```

> **If you see "Running scripts is disabled on this system":** adjust the PowerShell **execution policy** to allow the script to run, then re-run the command.

### **MacOS** (example: export all User and Kernel panic logs)

1. Open a **Terminal** session on the endpoint where Duo Desktop is installed.

2. **Enable debug logging** (Part 1).

3. **Reproduce** the Duo issue.

4. Run the **script**:

- Duo Desktop:

```bash

**/Applications/Duo\ Desktop.app/Contents/Resources/duo_desktop_support.sh -a**

```

- Duo Device Health:

```bash

/Applications/Duo\ Device\ Health.app/Contents/Resources/device_health_support.sh -a

```

Submit these to Cisco TAC -

1 Dart and `Duo_Desktop_Support Folder on your desktop to Cisco TAC.`

`2 Time frames for a failed attempt`

`3 Posture Checks enforced in Posture Profile.`
```

Cause

One or more posture checks (OS version, AV status, disk encryption, domain join, firewall state) did not meet the threshold defined in the Zero Trust Network access policy.

Related Content

- Duo Desktop Debug Logging Configuration
- Duo Desktop Support Tool
- Cisco Technical Support & Downloads