Oplossen " Houdingscontrole mislukt of Houding te oud" Fout bij zoeken naar activiteit voor ZTNA-stroom

Inhoud

uitgifte

Na de controle van de netwerktoegangshouding met nulvertrouwen wordt het probleem op twee manieren gemanifesteerd, afhankelijk van de beleidsconfiguratie:

- Wanneer de regel voor het openen van een fout bestaat: het verkeer omzeilt de handhaving van de houding en komt overeen met de regel "Geen houdingscontroles".
- Wanneer strikte handhaving is ingeschakeld: gebruikers wordt de toegang tot privétoepassingen geweigerd.

milieu

- Cisco Secure Access — Nul vertrouwen netwerktoegangsstroom
- Duo-desktop

resolutie

Duo Desktop Diagnostics verzamelen: foutopsporingslogboekregistratie inschakelen en de ondersteuningstool uitvoeren

Stap 1 - Foutmelding inschakelen (macOS en Windows)

1. Open de app Duo Desktop.

2. Navigeer naar Voorkeuren.

3. Controleer Gedetailleerde diagnoserapporten inschakelen.

Stap 2 - Reproduceer het probleem

Stap 3 — Verzamel de Dart Bundel - Verzamel DART Bundel voor Secure Client

Stap 4 — Voer het hulpprogramma voor ondersteuning uit

Het script van de Support Tool wordt geleverd met Duo Desktop 6.0.0+ en Duo Device Health 2.26.1+ voor macOS en Windows.

Het verzamelt de benodigde bestanden, schrobt ze van gevoelige informatie en maakt een kant-en-klare ZIP.

Script-locaties

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`

Opmerking: Paden verschillen tussen de oudere Duo Device Health-releases en de

---

nieuwere Duo Desktop-releases - gebruik het paar dat overeenkomt met uw installatie.

Wat verzamelt de ondersteuningstool

Windows

1. Creëert een ZIP om de verzamelde informatie te bewaren.

2. Voert `Invoke-WebRequest uit` om de connectiviteit met Duo te testen.

3. Legt vast: systeemproxyinstellingen; OS-versie, build en bit; BitLocker-status; tijdzone; Duo-gerelateerde gebeurtenislogboeken van toepassingen.

4. Kopieert `...\AppData\Local\DuoDesktop\Logs` (of `...\DuoDeviceHealth\Logs`) in de postcode.

5. Exporteert Duo-registersleutels van `HKLM:\SOFTWARE\Duo` en `HKCU\SOFTWARE\Duo Device Health` naar `system_info.txt`.

6. Kopieert certificaten die zijn gekoppeld aan de loopback-adapter (`127.0.0.1`).

7. (Optioneel) Exporteert systeemgebeurtenislogboeken.

8. Slaat de ZIP op op het bureaublad van de ingelogde gebruiker, bijvoorbeeld `C:\Users\user_name\Desktop\Duo_Desktop_Support_2022-06-21-02-04-44.zip` (of `DHA_Support_...zip`).

MacOS

1. Creëert een ZIP om de verzamelde informatie te bewaren.

2. Loopt `krullen` om de connectiviteit met Duo te testen.

3. Legt vast: systeemproxyinstellingen; `install.log`; `system.log`; Duo-gerelateerde crashlogs; OS- en kernelversie.

4. Kopieert `/Gebruikers/user_name/Library/Logs/Duo Desktop/*.log` (of `Duo Device Health`) in de ZIP.

5. Kopieert certificaten die zijn gekoppeld aan de loopback-adapter (`127.0.0.1`).

6. (Optioneel) Exporteert alle gebruiker- en kernel-logs.

7. Slaat de ZIP op het bureaublad van de ingelogde gebruiker op, bijvoorbeeld `/Users/user_name/Desktop/duo_desktop_support_2022-06-21-16-27-59.zip` (of `DHA_Support_...zip`).

Opdrachtregelopties

Windows (PowerShell)

Optie | Beschrijving

| `-eventlogs` | Systeemlogs exporteren. Opties: `systeem` |

| `-days` | Aantal dagen waarop logboeken van beveiligingsgebeurtenissen moeten worden geëxporteerd |

| `-user` | Specificeert van welke gebruiker logs moeten worden verzameld (nodig bij het uitvoeren als admin onder een andere gebruikersnaam) |

| `Get-Help` | Ingebouwde cmdlet; noem het vóór het script, bijvoorbeeld `Get-Help .\DuoDesktop-Support.ps1` |

macOS (Terminal)

`-a` | Exporteert alle gebruikers- en kernel-panieklogboeken.

`-h` | Geeft een helpbericht weer.

End-to-end procedure

Windows (voorbeeld: systeemgebeurtenislogboeken exporteren van de laatste 2 dagen)

1. Open een beheersessie voor PowerShell op het eindpunt waarop Duo Desktop is geïnstalleerd.

2. Logboekregistratie voor foutopsporing inschakelen (deel 1).

3. Reproductie van de Duo-kwestie.

4. Voer het script uit:

- 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

"

> Als u ziet dat het uitvoeren van scripts is uitgeschakeld op dit systeem: pas het PowerShell-uitvoeringsbeleid aan zodat het script kan worden uitgevoerd. Voer de opdracht vervolgens opnieuw uit.

### MacOS (voorbeeld: exporteer alle gebruikers- en kernel-panieklogboeken)

1. Open een Terminal-sessie op het eindpunt waar Duo Desktop is geïnstalleerd.

2. Logboekregistratie voor foutopsporing inschakelen (deel 1).

3. Reproductie van de Duo-kwestie.

4. Voer het script uit:

- 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

"

---

## Stuur deze naar Cisco TAC -

1 Dart en `Duo_Desktop_Support-map op uw bureaublad naar Cisco TAC.`

`2 Tijdframes voor een mislukte poging`

`3 Houdingscontroles afgedwongen in Houdingsprofiel.`

# Oorzaak

Een of meer houdingscontroles (OS-versie, AV-status, schijfcodering, domeinverbinding, firewallstatus) voldeden niet aan de drempelwaarde die is gedefinieerd in het toegangsbeleid voor het Zero Trust Network.

# Gerelateerde inhoud

- Configuratie voor registratie van fouten bij Duo Desktop
- Duo Desktop Support Tool
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.