

Secure Client AnyConnect VPN Access Denied Due to Endpoint Security Posture Compliance Issues

Contents

Issue

Multiple users are unable to connect to AnyConnect VPN and Zero Trust Access (ZTA) and receive the error message "Login denied. Your environment does not meet the access criteria defined by your administrator."

The issue is related to endpoint posture compliance, where the Endpoint Security Agent requirement is reported as not matching. Users experience VPN and ZTA access denial when attempting to connect through Cisco Secure Client.

The posture evaluation shows that the Trellix Endpoint Security posture is failing on affected endpoints, preventing successful authentication to the VPN service.

Environment

- Cisco Secure Client (AnyConnect and Zero Trust Access)
- Trellix Endpoint Security Agent version 5.8.4.505
- VPN Posture Profile: KFIN_SECURE_VPN with endpoint security agent enforcement
- Posture requirement: Endpoint security agent running with updates within last 14 days
- Windows endpoints with Trellix Agent Service running
- Umbrella Agent processes detected on endpoints

Resolution

The issue was resolved by addressing the Trellix Endpoint Security agent posture compliance problems. The troubleshooting and resolution steps described in the next sections were implemented.

Step 1: Validate Posture Profile Configuration

Review the VPN posture profile to confirm the endpoint security agent requirements. The KFIN_SECURE_VPN profile enforces that an endpoint security agent must be running and updated within the last 14 days.

Step 2: Verify Trellix Endpoint Security Status

Check the current status of the Trellix Endpoint Security agent on affected endpoints:

```
Trellix Agent Service: masvc.exe
Version: 5.8.4.505
Install Location: C:\Program Files\McAfee\Agent\
Display Name: Trellix Agent
Publisher: Trellix
```

Step 3: Reinstall Trellix Endpoint Security

Perform a complete reinstallation of Trellix Endpoint Security on affected endpoints:

1. Fully uninstall the existing Trellix Endpoint Security agent.
2. Reboot the system.
3. Install the latest approved Trellix agent version as per organizational standards.
4. Ensure the agent is running successfully after installation.
5. Confirm that signature/content updates complete successfully.

Step 4: Enable TRACE Logging for Cisco Secure Client (ZTA)

Enable detailed logging to capture posture evaluation details.

Create the logconfig.json file with this content:

```
{ "global": "DBG_TRACE" }
```

Place the file in the appropriate directory:

- **Windows:** C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- **macOS:** /opt/cisco/secureclient/zta

Restart the Cisco Secure Client/ZTA service after creating the file.

Step 5: Collect Updated DART Bundle

After implementing the changes, collect a new DART bundle to validate the resolution and confirm proper posture compliance detection.

Cause

The root cause was identified as Trellix Endpoint Security agent posture compliance issues. The VPN posture profile required an endpoint security agent to be running with updates within the last 14 days, but the Trellix Endpoint Security agent was not meeting these compliance criteria. The posture evaluation module was unable to properly detect or validate the endpoint security agent status, resulting in access denial for VPN and ZTA connections. The issue was specifically related to the Trellix agent configuration and required intervention from the Trellix support team to resolve the underlying agent compliance problems.

Related Content

- [Collect Detailed ZTNA Logs for Troubleshooting](#)
- [Cisco Technical Support & Downloads](#)