

Secure Access Device Posture Intermittent "Out of Date" Error

Contents

Issue

Device Posture in Cisco Secure Access intermittently displays "out of date" status for enrolled devices, preventing Zero Trust Access posture validation.

Users encounter these error messages during specific time windows:

- "Your device posture is out of date"
- "A security check for your device could not be run automatically"

The issue occurs despite Duo Desktop indicating full compliance with all security requirements including Windows updates, system password configuration, BitLocker encryption, and firewall enablement. During the problematic periods, attempts to unenroll and re-enroll affected devices fail with internal errors. The only temporary workaround that restores normal operation is performing a complete system reboot, which disrupts user access and productivity.

Additional symptoms include AnyConnect VPN maintaining connectivity throughout the issue period, while Zero Trust Access enrollment and posture validation processes fail intermittently during predictable time windows.

Environment

- Cisco Secure Access with Device Posture functionality enabled
- Duo Desktop client for device compliance verification
- Windows endpoints with BitLocker encryption, system passwords, and Windows Firewall enabled
- Zero Trust Access deployment requiring posture validation
- Configured Posture Profiles in Cisco Secure Access matching device compliance status

Resolution

The issue was resolved by upgrading the Cisco Secure Access client to latest version 5.1.15.287. This version addresses the underlying defect that caused intermittent device posture validation failures.

Client Upgrade Process

Step 1: Identify the current client version on affected endpoints.

Verify the existing Cisco Secure Access client version through the application interface or system installation records.

Step 2: Download and deploy client version 5.1.15.287.

Obtain the updated client software from the appropriate Cisco distribution channel and deploy to all affected endpoints experiencing the device posture validation issues.

Step 3: Verify resolution.

After client upgrade completion, monitor device posture status during previously problematic time windows to confirm stable operation without requiring system reboots.



Note: Recommendation is to install latest version of Secure client.

Validation Steps

After the client upgrade, verify that:

- Device posture validation completes successfully during previously problematic time periods.
- Zero Trust Access enrollment functions without internal errors.
- Unenroll and re-enroll operations complete successfully when needed.
- No system reboots are required to maintain device posture compliance.
- Duo Desktop and Cisco Secure Access posture status remain synchronized.

Cause

The intermittent device posture validation failures were caused by Cisco bug ID CSCws68569. This defect affected the communication between the Cisco Secure Access client and the posture validation services, resulting in temporary synchronization issues that prevented accurate device compliance status reporting during specific operational windows.

Related Content

- [Cisco Technical Support & Downloads](#)