Secure Client VPN Connectivity Issues with Posture Detection Failures

Contents

Issue

Users are unable to establish Cisco Secure Client VPN connectivity within a Windows 365 VDI environment or Local PCs. The VPN connection consistently fails with posture-related errors, specifically displaying "hostscan csd prelogin verification failed" error messages.

The issue has been identified as being associated with posture detection failing when usernames contain non-ASCII (2-byte) characters, preventing affected VDI users from successfully connecting to the VPN.

When users press the connect button in the Cisco Secure Client interface, the VPN connection fails. The error manifests during the posture assessment phase of the connection process, preventing users from establishing secure remote access to corporate resources through the VPN tunnel.

Environment

- Windows 365 VDI environment or Local PC
- Cisco Secure Client installed
- Secure Access implementation: RAVPN

Resolution

This issue is currently under investigation by Cisco Engineering and is tracked under Cisco bug ID CSCwt59834. The problem stems from posture detection failures when usernames contain non-ASCII (2-byte) characters in the Windows 365 VDI environment.

```
Date : 03/03/2026|Time : 02:19:09|Type : Information|Source : csc_vpnapishim|Description : [TID=10348 P
```

```
Date : 03/03/2026|Time : 02:19:09|Type : Information|Source : csc_vpnapishim|Description : [TID=10348 P
Date : 03/03/2026|Time : 02:19:10|Type : Information|Source : csc_vpnapishim|Description : [TID=10348 P
Date : 03/03/2026|Time : 02:19:10|Type : Error|Source : csc_libcsd|Description : Function: open_logfile
Date : 03/03/2026|Time : 02:19:10|Type : Error|Source : csc_libcsd|Description : [Tue Mar 03 02:19:10.3
Date : 03/03/2026|Time : 02:19:10|Type : Error|Source : csc_libcsd|Description : Function: csd_prelogin
```

Initial Troubleshooting Steps Performed

These troubleshooting steps were attempted:

- Reinstalling the Cisco Secure Client module on the VDI
- Restarting the VDI environment

Current Status and Ongoing Resolution

The case is currently being worked on with Cisco Engineering to determine an estimated time of arrival (ETA) for a fix or enhancement related to Cisco bug ID CSCwt59834. Updates are provided as new information becomes available from the engineering team.

Diagnostic Information Collection

For proper diagnosis of this issue, collect this diagnostic information:

- Cisco Secure Client error screenshots showing the specific error messages
- DART (Diagnostic and Reporting Tool) files from the affected VDI environment or System.
- Verification of username character encoding, particularly for users with non-ASCII characters

Observe these errors in the SFP logs under DART bundle:

Cause

The root cause of this issue is related to posture detection failures in the Cisco Secure Client when operating within Windows 365 VDI environments or Local PCs , specifically when usernames contain non-ASCII (2-byte) characters. The posture assessment component fails to properly process these character encodings during the "hostscan csd prelogin verification" phase, resulting in connection failures.

This issue is documented and tracked under Cisco bug ID CSCwt59834.

Related Content

- Cisco Bug Search - Cisco bug ID CSCwt59834
- Cisco Technical Support & Downloads