Hostscan CSD Prelogin Verification Failed Error in Secure Client

Contents

Issue

A user encounters the error message "Hostscan CSD prelogin verification failed" when attempting to connect to a VPN using Cisco Secure Client on a Windows 11 device. The error occurs before the login prompt is displayed, preventing the user from accessing the VPN connection. The same user can successfully connect to the VPN from another device using identical credentials and VPN profile, indicating the issue is device-specific rather than credential-related.

Additional error log entries observed include:

- CONNECTIFC_ERROR_FILE_OPEN_FAILED (Return Code: -30015466 / 0xFE360016)
- HostScan Processing Failed
- Connection attempt has failed due to network or PC issue

The user was able to connect to other VPN profiles where posturing was not enabled, but could not connect to profiles where posturing was enabled. The setup had been working previously with no known changes made to the configuration.

Environment

- Cisco Secure Client version 5.1.7.80
- Operating System: Windows 11
- VPN profile with posturing enabled
- Issue is device-specific, affecting only one user on one particular device
- Related to Cisco Bug ID: CSCwk54713

Resolution

The resolution involves performing a complete clean uninstallation of Cisco Secure Client and reinstalling the software. Standard uninstallation and reinstallation methods does not always resolve the issue due to corrupted registry entries or residual files.

Step 1: Disable Third-Party Services

Disable all third-party services in Msconfig, including proxy services if available, and keep only Cisco Secure Client modules active.

Step 2: Clean Uninstallation Using Microsoft Tool

Use the Microsoft Program Install and Uninstall Troubleshooter tool to remove all Cisco modules from the affected device. This tool provides more thorough uninstallation than standard Windows uninstall methods.

Fix problems that block programs from being installed or removed.

Step 3: Manual File Cleanup

After uninstalling, manually check and delete any remaining Cisco folders, files, executables, and DLL files from these directories:

```
C:\Program Files (x86)\Cisco
C:\ProgramData\Cisco\
C:\Users\<current user>\AppData\Local\Cisco
```

Remove any residual files and folders found in these locations, as they do not always remain even after the uninstallation process.

Step 4: Registry Cleanup

Check this registry paths for any old Cisco Secure Client entries and remove them if present:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco
```

Step 5: Enable Debug Logging (Optional)

If further troubleshooting is needed, enable Curl logging by copying the debuglogconfig.json file:

```
{
"web_helper" : 3,
"vpn_ipsec_ikev2" : 3,
"vpn_curl" : 3,
"vpn_state" : 3
}
```

into this directory:

```
C:\ProgramData\Cisco\Cisco Secure Client
```

Step 6: System Reboot

Reboot the endpoint to ensure all changes take effect and clear any remaining processes or registry locks.

Step 7: Reinstall Cisco Secure Client

Install the pre-deploy package of Cisco Secure Client or allow automatic installation via management tools such as Intune. Verify successful installation before proceeding.

Step 8: Test VPN Connection

Attempt to connect to the VPN profile that was previously failing. If the issue persists, generate a new DART bundle for further analysis.

⚠ **Caution**: Possible. The details mentioned here appears to contain procedures or commands that could cause significant impact if executed. Please ensure these procedures or commands have been evaluated by an SME or Business Unit before executing or recommending.

Cause

The issue is caused by corrupted registry entries or interference from third-party software that prevents Hostscan libraries and executions from launching or updating properly. This corruption affects the CSD (Cisco Security Desktop) pre-login verification process, which is required for VPN profiles with posturing enabled. The corruption typically occurs at the device level, explaining why the same user can connect successfully from other devices. Standard uninstallation methods do not always remove all corrupted components, requiring manual cleanup of files and registry entries.

Related Content

- Cisco Technical Support & Downloads