

Secure Client Auto-Update Causes Application Access Failures

Contents

Issue

Users are experiencing repeated service disruptions where they become unable to access applications after Cisco Secure Client automatically updates to newer versions. The automatic updates are triggered whenever Cisco releases a new version of the Secure Client software, resulting in application access failures that require intervention to resolve. This creates an ongoing operational challenge where each new client release potentially disrupts user connectivity.

Environment

- Cisco Secure Access with Secure Client Remote Access
- Cisco Secure Client installed manually from Secure Access dashboard
- No deployment tools used, such as MDM, SCCM, Intune, JAMF
- AnyConnect/Cisco Secure Client Auto-Update feature enabled in Umbrella

Resolution

The automatic client updates were being triggered by the AnyConnect/Cisco Secure Client Auto-Update setting in Cisco Umbrella. To resolve this issue and prevent future automatic updates that cause application access disruptions, disable the auto-update feature in the Umbrella dashboard.

Step 1: Access Cisco Umbrella Dashboard

Log into the Cisco Umbrella dashboard for your organization (ORG 4007750 in this case).

Step 2: Locate Auto-Update Settings

Navigate to the AnyConnect/Cisco Secure Client Auto-Update configuration section within the Umbrella dashboard.

Step 3: Disable Auto-Update Feature

Turn off the AnyConnect/Cisco Secure Client Auto-Update setting to prevent automatic client upgrades from occurring.

Step 4: Verify Resolution

After disabling the auto-update feature, confirm that users can access applications normally and that no further automatic client updates occur.

This workaround allows the IT Security team to investigate the root cause and work on a more permanent fix while maintaining stable user access to applications.

Cause

The automatic client updates were being initiated by the AnyConnect/Cisco Secure Client Auto-Update feature enabled in Cisco Umbrella. This setting was configured to automatically upgrade Secure Client installations whenever new versions became available, which was causing the application access failures. The Cisco Secure Access backend infrastructure itself was confirmed to have no auto-update flags that would force client upgrades from the cloud side.

Related Content

- [Cisco Technical Support & Downloads](#)