Secure Access Roaming Device Information Collection and Update Behavior

Contents

Issue

A request for clarification regarding Cisco Secure Access (CSA) roaming device information behavior and specifications.

The inquiry focused on understanding how CSA collects and displays endpoint device information in the management portal under **Management Portal > Resources > Roaming Devices**, specifically:

- Which endpoint attributes CSA extracts from Windows, macOS, and Cisco iOS operating systems for roaming device information
- Whether device information updates automatically when hostname or OS version changes occur on endpoints
- The frequency and timing of roaming device information synchronization between endpoints and CSA cloud
- How CSA determines device identity when attributes change (same-device determination logic)

The observed device information displayed in the CSA management portal varies by operating system.

Windows and macOS

- Hostname
- Original Hostname
- Operating System
- Serial Number

Cisco iOS

- Device Name (Serial Number)
- Serial Number
- OS Version

Environment

- Cisco Secure Access (CSA) management portal
- Secure Access client (formerly AnyConnect/Secure Client)
- Endpoint operating systems: Windows, macOS, Cisco iOS
- CSA cloud infrastructure

Resolution

The clarifications described in the next sections were provided regarding CSA roaming device information behavior.

Device Attribute Collection by Operating System

Windows and macOS

The Secure Access client collects device attributes from standard OS-provided device properties:

- **Hostname:** Current device name set in the OS
- **Original Hostname:** Device name captured during initial registration or first client connection
- **Operating System:** OS type and version information
- **Serial Number:** Hardware identification information obtainable from the OS

Cisco iOS

Due to Apple platform restrictions, available information is limited to what Cisco iOS permits applications to access:

- **Device Name:** Name defined by i Cisco iOS (can be displayed with serial number)
- **Serial Number:** Device identification information permitted by Cisco iOS to applications (not direct hardware access, but Apple-authorized identification information)
- **OS Version:** Cisco iOS system version information (such as, Cisco iOS xx.x.x)

Host-level attributes available on desktop operating systems are not accessible on Cisco iOS due to platform constraints.

Device Information Update Behavior

When endpoint changes occur (hostname modifications or OS version updates), CSA automatically updates the existing roaming device entry rather than creating a new device record. Updates occur when the client next communicates with the CSA cloud, not immediately upon the endpoint change. The **Original Hostname** field is preserved as an identification reference from initial registration and remains unchanged even after hostname modifications.

Synchronization Timing and Triggers

Device information transmission and updates occur during these events:

- Secure Access client startup
- User sign-in
- CSA service connection or reconnection
- Periodic cloud synchronization

Periodic Synchronization Details

Automatic synchronization occurs approximately every 20-30 minutes when no restart or reconnection events occur. This is not a fixed interval but uses an internal synchronization window with slight per-client jitter to prevent cloud load concentration. The timing is neither completely fixed nor completely random.

For immediate device information updates, client restart or reconnection provides the most reliable trigger.

Same-Device Determination Logic

CSA does not rely on a single identifier to determine device identity. Same-device determination uses a combination of these operating systems.

Windows and macOS

- Multiple stable OS-provided device identifiers obtained by the Secure Access client
- CSA cloud-managed internal device identifier issued and maintained by CSA cloud during initial client registration

Cisco iOS

- Cisco iOS-permitted device identifiers available to the Secure Access client
- CSA cloud-managed internal device identifier

The serial number displayed in the management portal is one element of the identification process but is not used alone for device identity determination. This composite approach allows CSA to recognize the same device even when individual attributes like hostname or OS version change.

Important Notes

- Roaming device information is provided for management and visibility purposes, not for detailed endpoint control or enforcement like MDM solutions.
- Displayed attributes and granularity can change in future product releases due to OS-side restrictions or product updates.

- The behavior described represents expected product functionality, not a defect.

Cause

This was a product specification and behavior clarification request rather than a technical issue requiring root cause analysis. The inquiry arose from the need to understand the CSA device identification and information synchronization mechanisms for proper system administration and planning purposes.

Related Content

- Cisco Technical Support & Downloads