

# Secure Access VPN Administrator Reset Disconnections Due to VPN Profile Name Length Limitation

## Contents

---

---

## Issue

Remote access VPN users experienced intermittent disconnections on Cisco Secure Access during active sessions. The Cisco Secure Access (CSA) logs recorded these disconnection events as Administrator Reset despite no scheduled maintenance activity occurring at the time. The disconnections impacted remote access users during normal business operations, causing unexpected session terminations while users were actively connected to the VPN service.

The disconnection events appeared in the Remote Access logs as Administrator Reset entries, which typically indicate administrative intervention or system-initiated session termination. However, no administrative actions were being performed on the system during the reported timeframe.

## Environment

- Cisco Secure Access (CSA) - Remote Access VPN service
- VPN Profile configurations with names exceeding 46 characters in length

## Resolution

The resolution involves implementing a workaround to address the VPN Profile name length limitation that causes the Administrator Reset events:

## Immediate Workaround

## **Step 1: Identify VPN Profiles with Names Exceeding 46 Characters**

Review all existing VPN Profile configurations in the Cisco Secure Access dashboard and identify any profiles with names longer than 46 characters.

## **Step 2: Rename VPN Profiles to Comply with Character Limit**

Rename all VPN Profiles that exceed 46 characters to ensure they are 46 characters or fewer in length. This can be done through the Cisco Secure Access management interface.

## **Step 3: Monitor for Disconnection Events**

After implementing the VPN Profile name changes, monitor the Remote Access logs to verify that Administrator Reset events no longer occur during normal operations.

## **Long-term Solution**

A permanent fix is being developed to address the GUI limitation that allows VPN Profile names to exceed the backend processing limit. This fix enforces the 46-character limit at the user interface level, preventing the creation of VPN Profiles with names that cause backend processing issues.

The development team is working on implementing proper validation in the GUI to restrict VPN Profile name length during creation and modification, which prevents this issue from occurring in future configurations.

## **Additional Considerations**

In some cases, Wi-Fi adapter power management settings on client devices can contribute to connection issues. If disconnections persist after implementing the VPN Profile name length fix, verify that Wi-Fi adapter power saving features are disabled on affected client devices, as these settings can cause reconnection events that appear as Administrator Reset entries in the logs.

## **Cause**

The root cause of the Administrator Reset events is a backend processing limitation in Cisco Secure Access

where VPN Profile names exceeding 46 characters cause system errors during session management. When the backend system encounters VPN Profiles with names longer than this limit, it triggers an Administrator Reset to terminate the affected sessions as a protective measure.

This issue occurs because the GUI interface allows users to create VPN Profile names longer than 46 characters, but the backend processing system has a strict 46-character limit. When large string lengths are processed by the backend, it causes an Administrator Reset event to be logged and forces disconnection of the associated VPN sessions.

## **Related Content**