DNS Logging and Device Registration Behavior with Cisco Secure Client on iOS for Remote Access VPN

Contents

Issue

When using Cisco Secure Client on iOS (iPad) to establish remote access VPN with Cisco Secure Access using SAML authentication via Microsoft Entra ID, DNS logs are not displayed in Secure Access after successful VPN connection, even though firewall and web logs are generated correctly. Additionally, the iPad does not appear under **Roaming Devices > Mobile Devices** in the Secure Access dashboard after establishing the VPN connection.

The specific symptoms observed include:

- Remote access logs show successful "connect" events in Secure Access
- Firewall and Web logs are generated and display the SAML authenticated user identity
- DNS logs are completely absent from Secure Access logging
- The iPad device information does not populate under Secure Access roaming devices section
- All traffic flows through the VPN tunnel (no split tunneling configured)

Environment

- iPad running iOS 26.2
- Cisco Secure Client
- Identity Provider: Microsoft Entra ID
- Security Connector: Not installed
- Cisco Secure Access with SSO Authentication configured
- SAML authentication implementation

- VPN profile configured with DNS Mode set to default
- No split tunneling configured (all traffic routed through VPN)
- Mobile Device Management (MDM) used for profile distribution

Resolution

The observed behavior is expected for the documented configuration. Cisco Secure Client on iOS functions as a VPN client (AnyConnect equivalent) and does not include RSM-equivalent functionality by default. Security Connector is the RSM-equivalent component on iOS that is required for endpoint identity population and Umbrella-style DNS control.

Understanding the Architecture

The absence of DNS logs and device registration occurs because:

- Cisco Secure Client alone provides VPN connectivity but lacks the endpoint agent functionality needed for DNS visibility
- Security Connector (equivalent to RSM on Windows) is required for DNS control and device registration in Secure Access
- Without Security Connector, DNS queries are handled by the VPN-obtained DNS servers without visibility to Umbrella/Secure Access

DNS Logging Solution via Traffic Steering

To enable DNS logging without installing Security Connector, configure traffic steering to direct DNS queries to Umbrella DNS servers:

Step 1: Configure Traffic Steering in Secure Access

Navigate to **Traffic Steering > Add > Add a source** and specify the DNS server IP as a source.

Step 2: Direct DNS Traffic to Umbrella Servers

Configure the VPN profile to use Umbrella DNS servers (208.67.222.222 and 208.67.220.220) to ensure

DNS queries are visible to Secure Access.

Step 3: Validate DNS Logging

After implementing traffic steering configuration, DNS logs should become visible in the Secure Access dashboard for VPN sessions.

VPN Profile DNS Mode Setting

The "DNS Mode" setting in the VPN profile is unrelated to the absence of DNS logs in this configuration. RAVPN (Remote Access VPN) sessions use the VPN-obtained DNS servers regardless of this setting, and the logging visibility depends on whether the DNS traffic is directed to monitored DNS infrastructure.

Security Connector Installation Option

Installing Security Connector on iOS will enable:

- DNS logging visibility in Secure Access
- Enhanced endpoint identity and device registration capabilities
- Umbrella-style DNS control and protection

Security Connector can be used in conjunction with Secure Client, but proper traffic exclusion and design considerations are required to prevent conflicts between the two components.

Cause

The root cause is architectural: Cisco Secure Client on iOS provides VPN connectivity but does not include the endpoint agent functionality required for DNS visibility and device registration in Secure Access. This functionality requires either Security Connector installation or traffic steering configuration to direct DNS queries through monitored infrastructure. Without these components, DNS queries bypass Secure Access monitoring, and device identity information is not populated in the roaming devices section.

Related Content

- Cisco Technical Support & Downloads