

Secure Client Distribution Methods for Secure Access RAVPN

Contents

Issue

When configuring external vendor access to Remote Access VPN (RAVPN) in Cisco Secure Access, administrators need a method for vendors to download the AnyConnect/Secure Client software. Unlike previous ASA deployments where the VPN URL provided direct client downloads, Cisco Secure Access VPN headend URLs do not provide a client download function. This limitation impacts the onboarding process for external vendors who require remote access capabilities.

Administrators expect the VPN setup URLs within Secure Access to grant vendors access to download the AnyConnect client, similar to the behavior previously available with ASA-based deployments where the VPN URL would allow client downloads prior to connecting.

Environment

- Cisco Secure Access with RAVPN configuration
- External vendor access requirements
- Migration from ASA-based VPN deployment
- AnyConnect/Secure Client distribution needs

Resolution

Cisco Secure Access does not host Secure Client packages on the VPN headend URLs. The solution uses hostscan technology instead of providing direct client downloads through the VPN URL. To distribute the Secure Client software to external vendors, use one of the these approved methods.

Method 1: Secure Access Dashboard Distribution

- 1.- Obtain installer packages directly from the Secure Access dashboard for manual distribution.
- 2.- Navigate to **End User Connectivity** and click the **Cisco Secure Client** button to download installer packages for distribution to vendors.

Method 2: Cisco Software Download Site

Vendors can download packages directly if they have the proper entitlements:

- Vendor must have a Cisco account with software entitlement
- Access packages through software.cisco.com
- Requires pre-deployment planning and vendor Cisco account setup

Method 3: Manual Distribution

Distribute the Secure Client software to external vendors manually or through alternative distribution channels outside of the VPN URL. This method provides the most control over the distribution process and does not require vendor Cisco accounts.

Cause

Cisco Secure Access VPN headend URLs are designed differently from ASA-based deployments. The Secure Access solution does not host client installer packages on the headends and instead uses hostscan technology. This architectural difference means that the VPN URLs cannot provide the same client download functionality that was available with ASA deployments.

Related Content

- [Cisco Technical Support & Downloads](#)