Cisco Secure Client: Deployment Instructions

admin
SOUTH CAROLINA
DEPARTMENT *of* ADMINISTRATION

OVERVIEW

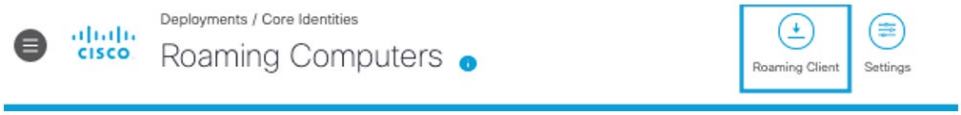
The following guide is designed to assist agencies in the deployment of the Cisco Secure Client. If you experience any issues during this process, please contact Admin's Service Desk (servicedesk@admin.sc.gov or 803.896.0001).

DEPLOYING CISCO UMBRELLA SECURE CLIENT

Migrating to Cisco Secure Client from an existing Umbrella Roaming Client deployment will automatically copy over the configuration of the standalone client and uninstall it.

SECURE CLIENT SOFTWARE DOWNLOAD

1. Navigate to **Deployments** > **Roaming Computers** and select **Roaming Client**.



2. Select and download the Cisco Secure Client pre-deployment packages.

   A. **Pre-Deployment Package** – Click the link to the Secure Client Pre-Deployment Package for the operating system of the user devices in your organization. **Note**: These packages cannot be installed on the headend of the ASA or FTD devices.

   Pre-Deployment Package:
   Windows (x86/x64) | Windows (Arm) | macOS

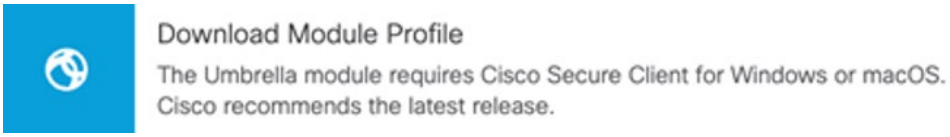
   B. **Headend Deployment Package** – Click the link to the Secure Client Headend Deployment Package for the operating system of the user devices in your organization. Then, upload the package to the ASA or FTD headend.

   Headend Deployment Package:
   Windows (x86/x64) | Windows (Arm) | macOS

UMBRELLA PROFILE (JSON FILE) DOWNLOAD

1. Navigate to **Deployments** > **Roaming Computers** and select **Roaming Client**.

2. In the Download Cisco Secure Client page, select **Download Module Profile**.



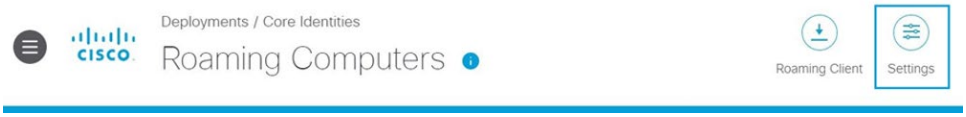
3. Select **Download Module Profile** to download the OrgInfo.json file (Umbrella Roaming Security Module profile) to your local system.

AUTOMATIC UPDATES

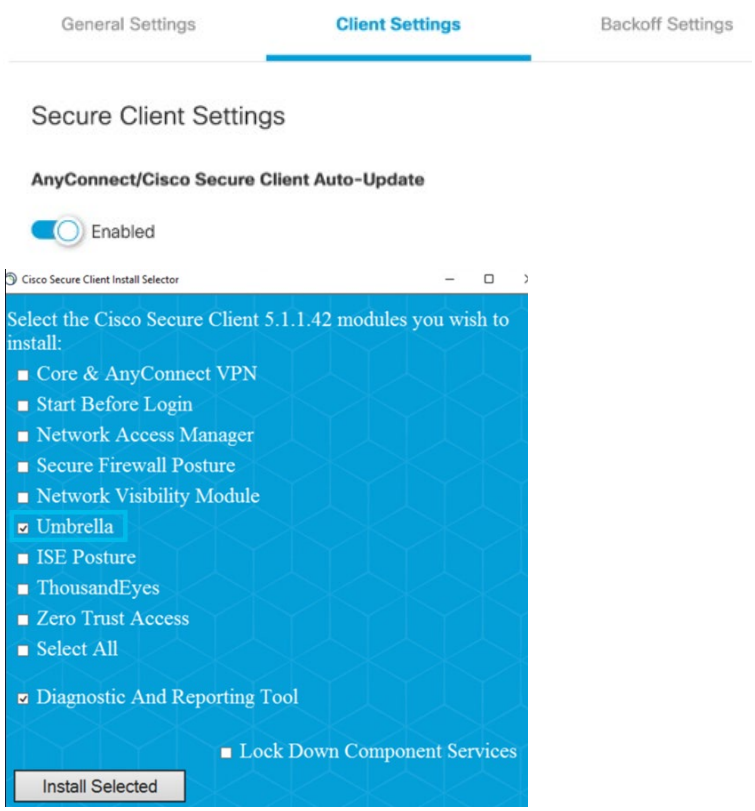
Cisco has provided Umbrella-managed auto-updates for the Cisco Secure client. When enabled, Secure Client and all its installed modules are automatically updated within 30 days of a release being posted to Cisco.com.

Note: Auto-update is not enabled by default. Each agency will need to enable auto-update for their organization in their own Umbrella dashboard by following the steps provided below.

1. Navigate to **Deployments** > **Roaming Computers** and select **Settings**.



2. Select **Client Settings**, then enable **AnyConnect/Cisco Secure Client Auto-Update**.



Note: The Diagnostic and Reporting Tool (DART) module is optional, but must be installed to generate the Secure Client's troubleshooting logs. DIS recommends that organizations install the DART module.

STANDARD INSTALLATION (MOST COMMON)

Standard deployments consist of manual or mass installing the client with the module's MSI installer or with the setup.exe installer contained in the client's download ZIP file. When installing the Secure Client, choose the software modules to install on the client.

A. For Umbrella only, select **Umbrella** and **DART**.
B. For Umbrella and VPN, select **Core/VPN**, **DART** and **Umbrella**.

Note: The DART module is optional, but must be installed to generate the Secure Client's troubleshooting logs. DIS recommends that organizations install the DART module.

To begin, download the prerequisite software:

1. Download the Cisco Secure Client deployment packages from software.cisco.com or from Umbrella. Cisco Secure Client is licensed for use with all Umbrella packages but may require linking your contract ID to your Cisco account.
2. Download a copy of the Secure Client's configuration profile, OrgInfo.json, from Umbrella.
3. Depending on your system, drop or push the Umbrella profile (OrgInfo.json) into the client's profile directory:

    A. Windows: %ProgramData%\Cisco\Cisco Secure Client\Umbrella
    B. macOS: /opt/cisco/secureclient/umbrella/

Note: To deploy the OrgInfo.json file before installing the Secure Client, create the directory for the Umbrella profile. After you deploy the Secure Client and copy the OrgInfo.json file in the Umbrella directory on the user device, the Secure Client activates the Umbrella module.

Important: When you deploy the OrgInfo.json file for the first time, it is copied to the data subdirectory (/umbrella/data), where several other registration files are also created. Therefore, if you need to deploy a replacement OrgInfo.json file, the data subdirectory must be deleted. Alternatively, you can uninstall the Umbrella Roaming Security module (which deletes the data subdirectory) and reinstall it with the new OrgInfo.json file.

The OrgInfo.json file has specific information about your Umbrella dashboard instance that lets the Roaming Security module know where to report to and which policies to enforce. If you use another OrgInfo.json file from a different dashboard to install the Roaming Security module, the client computer appears in that dashboard instead.

QUESTIONS OR CONCERNS

For questions or concerns regarding the deployment of Cisco Secure Client, please contact Admin's Service Desk (servicedesk@admin.sc.gov or 803.896.0001). For Admin's Division of Information Security, please contact (informationsecurity@admin.sc.gov).