

Understand Command Line Installation and RMM Reference for Umbrella Module

Contents

[Introduction](#)

[Purpose](#)

[Upgrades and migration](#)

[Components and approach](#)

[Profile Installation](#)

[Command line examples - Windows](#)

[Optional Arguments](#)

[macOS installations](#)

[Directory Structure](#)

[Cisco Secure Client Directories](#)

Introduction

This document describes the command line installation and RMM reference in the Cisco Secure Client Umbrella module.

Purpose

This article serves as a guide for anyone who wants to automate installation of the Umbrella module for Cisco Secure Client. It provides the context and commands that can be used to build your own scripts for automating the deployment of Cisco Secure Client.

Upgrades and migration

For customers migrating from older Cisco AnyConnect or Umbrella Roaming Client, it is not mandatory to remove the old software prior to upgrade. The old Umbrella software is detected and automatically removed during installation.

It is imperative to ensure that any automated installation tasks for AnyConnect or Umbrella Roaming Client are disabled to prevent re-installation of the older software.

Components and approach

Whether you are installing from the GUI or any other method, a successful installation requires:

- Installation of Cisco Secure Client
- Installation of the Umbrella Module
- Umbrella Profile (OrgInfo.plist on Mac and OrgInfo.json on Windows)
- Installation of DART Diagnostic Tool (Recommended)

Cisco provides precise documentation on how to build the commands to install this. For full documentation

on this, see the pre-deployment guide below:

[Predeploying Cisco Secure Client Modules as Standalone Applications](#)

Profile Installation

A key consideration when deploying Umbrella is installation of your unique organization profile (OrgInfo.json). This profile uniquely identifies your Umbrella organization and allows the client to register with the Umbrella cloud. You can download this from your dashboard by browsing to *Deployments > Core Identities > Roaming Computers > Roaming Client* then clicking on *Download* on top right corner and selecting *Download Module Profile*.

This step is **mandatory** for the Umbrella module to operate.

- **Bundle Profile** - The profile (*OrgInfo.json*) is bundled within the installation package prior to installation. See Pre-Deployment tutorial (Windows) and [pre-deployment tutorial \(OSX\)](#) for examples.
- **Copy Profile** - The profile (*OrgInfo.json*) is copied to a location on the endpoint after installation

If you choose to copy the profile to the endpoint it must be deployed to these locations programmatically:

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json (Windows) /opt/cisco/secureclient/umb
```

Command line examples - Windows

These commands demonstrate how to deploy the Secure Client, Umbrella, and DART modules on Windows via command-line or automation software.

- Replace <version> with the version number of the downloaded MSI file
- Replace <log_file_name> with the path and file name for the log file.

```
msiexec /package cisco-secure-client-win-<version>-core-vpn-predeploy-k9.msi /norestart /passive PRE_DE
```

```
msiexec /package cisco-secure-client-win-<version>-umbrella-predeploy-k9.msi /norestart /passive /lvx*
```

```
msiexec /package cisco-secure-client-win-<version>-dart-predeploy-k9.msi /norestart /passive /lvx* <log
```

These commands disable the Secure Client VPN functionality entirely using the PRE_DEPLOY_DISABLE_VPN=1 switch - which is a common configuration. Please note that the core VPN module must still be installed but the VPN itself is entirely disabled.



Note: For the Umbrella module to operate you **must** have deployed the OrgInfo.json file before or after installation as described in 'Profile Installation'.

Optional Arguments

There are several optional switches that can be used when installing the Cisco Secure Client and Umbrella Module. Here are some of the most useful:

Installer	Optional Argument	Purpose
cisco-secure-client-win-<version>-core-vpn-predeploy-k9.msi	PRE_DEPLOY_DISABLE_VPN=1	The core module includes the VPN capability, even if it is not used. This tells the system to hide the inactive VPN module. This can also be done after installation by using the steps listed here .
cisco-secure-client-win-<version>-	LOCKDOWN=1	This prevents the Umbrella service

umbrella-predeploy-k9.msi		from being disabled manually. More information can be found here .
Any module	ARPSYSTEMCOMPONENT=1	This prevents the module from being displayed in the Add/Remove Programs Dialog.

macOS installations

For more information on installation and customization on macOS, see this page:

[Command line and customization](#)

Directory Structure

The directory locations have changed with Cisco Secure Client.

Cisco Secure Client Directories

Windows

Executable

C:\Program Files (x86)\Cisco\Cisco Secure Client

Umbrella Directory

C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\

macOS

Executable

/Applications/Cisco/Cisco Secure Client.app

Umbrella Directory

/opt/cisco/secureclient/Umbrella/

For deployment references for some popular RMM product, please review

[https://docs.umbrella.com/deployment-umbrella/docs/additional-references.](https://docs.umbrella.com/deployment-umbrella/docs/additional-references)