

How to Install Secure Client Umbrella via Script Using a Windows Shared Folder

Contents

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration Steps](#)

[Verification](#)

[Troubleshoot](#)

Introduction

This document describes how to deploy the Secure Client Umbrella Module if you do not have an automation tool to push the software, for example, SCCM, In tune, GPO, and so on.

Background Information

This document simplifies the deployment using a Windows Shared Folder and running just one script from the PCs that need SC Umbrella installed.

Additionally, the DART module that is useful when you need to t-shoot a particular issue will also be installed.

As part of this configuration, you are going to hide the VPN UI; therefore, only the Umbrella module is visible to the user and for simplicity of the deployment. You will also import the **OrgInfo.json** file used by the Umbrella module, and import the Umbrella Root CA Certificate onto the machine, all this by running a **.bat** script.



Note: In order to have SC Umbrella Module installed, the SC VPN Core must also be installed since every module is Core/VPN-dependent.

The configuration example here assumes you do not need the VPN UI for the VPN capabilities nor any other **.xml** profile like the VPN Client Profile.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to the [Umbrella Dashboard](#)
- Admin rights on the PC you will install this on
- Access to the Windows Shared Folder from the PC you are installing the SC Umbrella on
- If possible, restrict admin access to the user to the C:\ProgramData\Cisco\Cisco Secure Client path, so they cannot remove/edit the profiles
- Also you can think about restricting access to start/stop/restart services on the PC

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

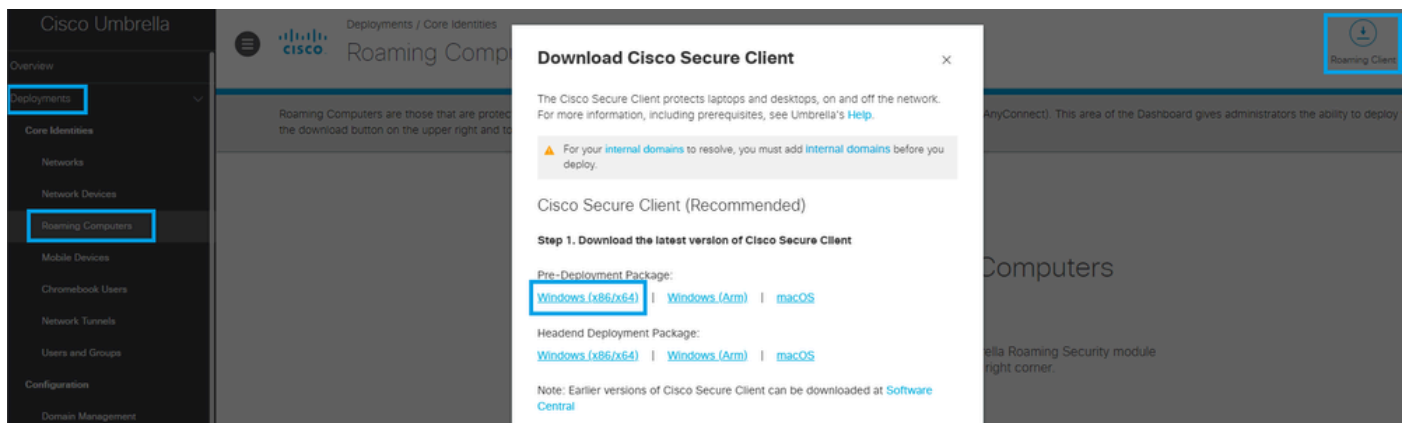
Configuration Steps

Step 1. Start by downloading the Secure Client software from the dashboard.

This file is found once logged in to the dashboard under: **Deployments > Roaming Computers > Roaming Client > Download Cisco Secure Client**.

Once downloaded, unzip the file and copy the files (used under Step 4.):

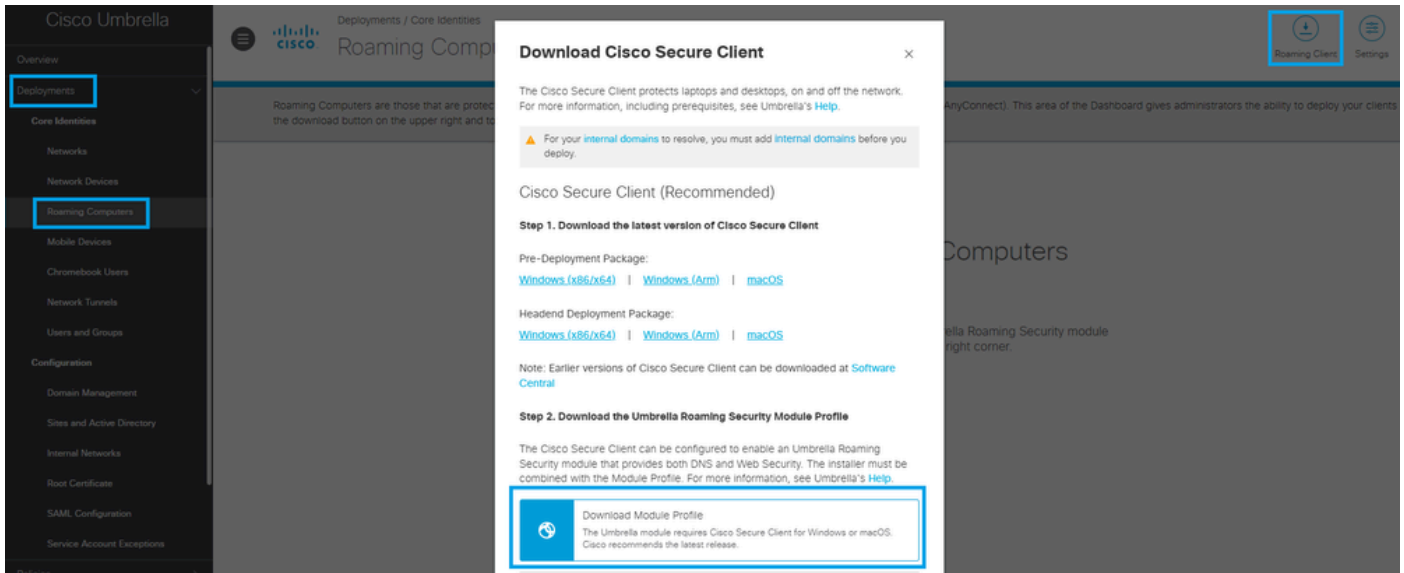
- cisco-secure-client-win-5.0.05040-core-vpn-predeploy-k9.msi
- cisco-secure-client-win-5.0.05040-dart-predeploy-k9.msi
- cisco-secure-client-win-5.0.05040-umbrella-predeploy-k9.msi



20144836311828

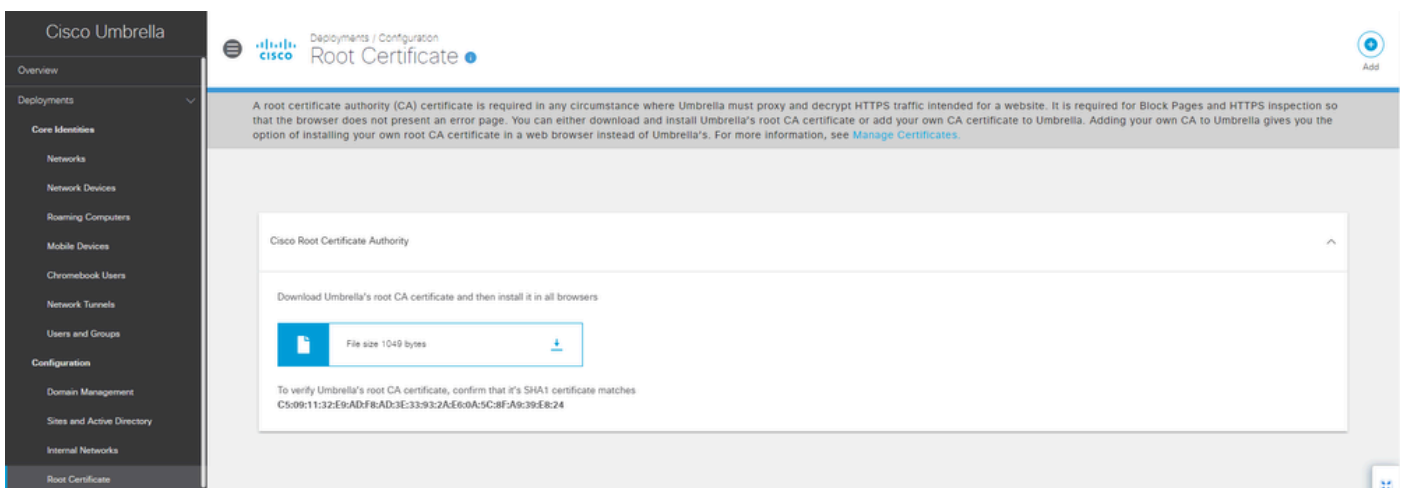
Step 2. Download the **OrgInfo.json** file from the dashboard.

This file is found once logged in to the dashboard under: **Deployments > Roaming Computers > Roaming Client > Download Module Profile**.



20145027908116

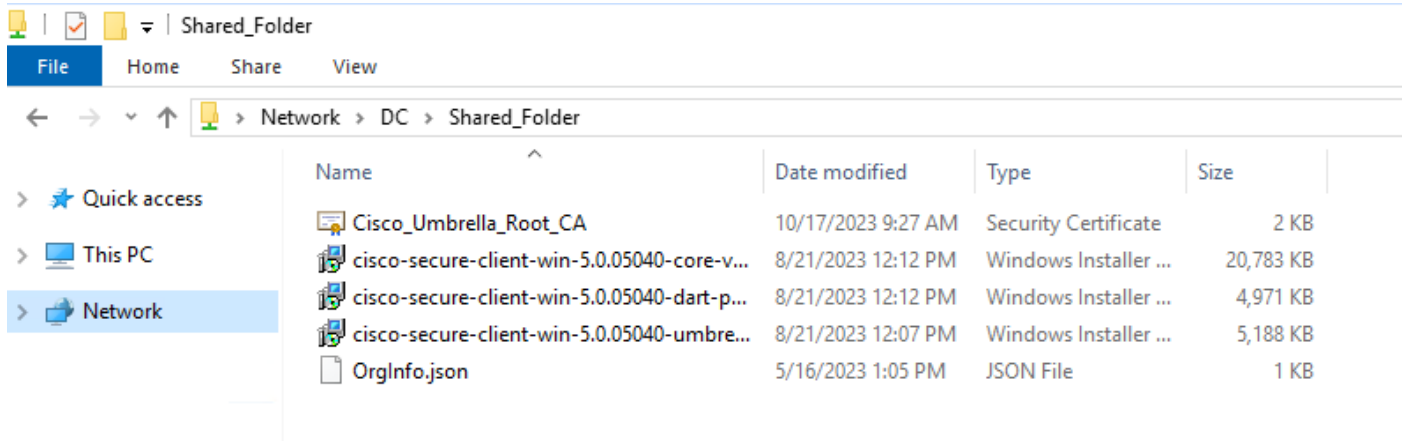
Step 3. (Optional) In order to install the Umbrella Root CA Certificate as part of the installation script, download the Root CA from the Umbrella Dashboard under: **Deployments > Root Certificate > Cisco Root Certificate Authority** and click the **download** icon.



20144836332692

Step 4. Place all the files on the Shared Folder where all the PCs have access to. The files needed in this case are:

- Cisco_Umbrella_Root_CA.cer
- OrgInfo.json
- cisco-secure-client-win-5.0.05040-core-vpn-predeploy-k9.msi
- cisco-secure-client-win-5.0.05040-dart-predeploy-k9.msi
- cisco-secure-client-win-5.0.05040-umbrella-predeploy-k9.msi



20144820279700

Step 5. Create your custom **.bat** script using any of the options described in [this](#) documentation. For the purpose of lab, you can make use of the 'PRE_DEPLOY_DISABLE_VPN=1' option.

You can also use 'ARPSYSTEMCOMPONENT=1' in order to hide the Secure Client software from the Add/Remove Programs List, and/or the LOCKDOWN=1 to lock down the service.

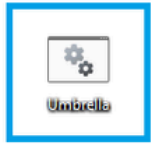
If you do not want to hide the VPN UI, ignore the 'PRE_DEPLOY_DISABLE_VPN=1' at the end of the first line of the next script.

```
msiexec /package "\\DC\Shared_Folder\cisco-secure-client-win-5.0.05040-core-vpn-predeploy-k9.msi" /norestart
msiexec /package "\\DC\Shared_Folder\cisco-secure-client-win-5.0.05040-umbrella-predeploy-k9.msi" /norestart
msiexec /package "\\DC\Shared_Folder\cisco-secure-client-win-5.0.05040-dart-predeploy-k9.msi" /norestart
copy "\\DC\Shared_Folder\OrgInfo.json" "C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json"
certutil -enterprise -f -v -AddStore "Root" "\\DC\Shared_Folder\Cisco_Umbrella_Root_CA.cer"
```

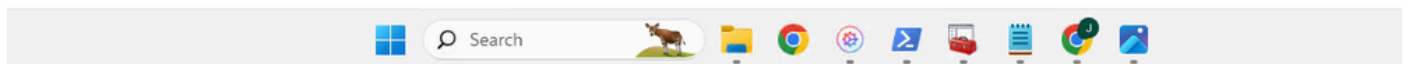


Note: Replace the '\\DC\Shared_Folder\' with your local shared folder path.

Step 6. Deploy/copy the **.bat** script to the PCs that you want to install the Secure Client Umbrella module on.



CISCO SECURE



20144820283796

Step 7. Proceed with running the script from the client machines, preferably using PowerShell as Admin.



CISCO

```
Administrator: Windows PowerShell
PS C:\Users\Josue\Desktop> .\Umbrella.bat

C:\Users\Josue\Desktop>msiexec /package "\\DC\Shared_Folder\cisco-secure-client-win-5.0.05040-core-vpn-predeploy-k9.msi" /norestart /quiet PRE_DEPLOY_DISABLE_VPN=1
C:\Users\Josue\Desktop>msiexec /package "\\DC\Shared_Folder\cisco-secure-client-win-5.0.05040-umbrella-predeploy-k9.msi" /norestart /quiet
C:\Users\Josue\Desktop>msiexec /package "\\DC\Shared_Folder\cisco-secure-client-win-5.0.05040-dart-predeploy-k9.msi" /norestart /quiet
C:\Users\Josue\Desktop>copy "\\DC\Shared_Folder\OrgInfo.json" "C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json"
1 file(s) copied.

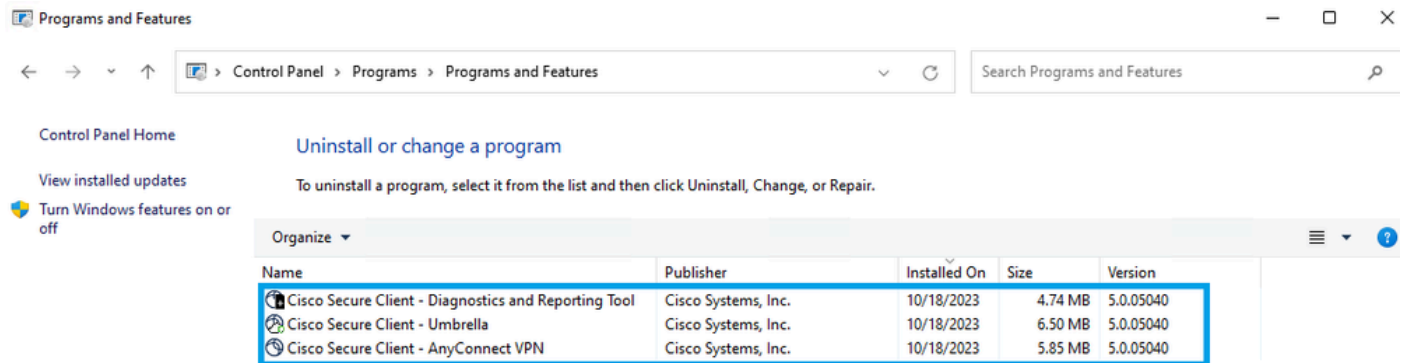
C:\Users\Josue\Desktop>certutil -enterprise -f -v -AddStore "Root" "\\DC\Shared_Folder\Cisco_Umbrella_Root_CA.cer"
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "Cisco Umbrella Root CA" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Users\Josue\Desktop>
```

20144836348948

Step 8. Repeat Steps 6 and 7 on the PCs you want to Install Umbrella.

Verification

Verify the software has been installed on the PC.



20144836357012

Verify that only the Umbrella module is visible to the user. In case you want the VPN module to also be visible (in order to use for VPN purposes, ignore the 'PRE_DEPLOY_DISABLE_VPN=1' at the end of the first line of the script in Step 5.).



20144820307220

Confirm the PC was properly registered to your dashboard.

Cisco Umbrella

Overview

Deployments

Core Identities

Networks

Network Devices

Roaming Computers

Mobile Devices

Chromebook Users

Network Tunnels

Users and Groups

Configuration

Deployments / Core Identities

Roaming Computers

Roaming Client

Settings

Roaming Computers are those that are protected by either the Umbrella Roaming Client, or Cisco Secure Client Umbrella module (formerly AnyConnect). This area of the Dashboard gives administrators the ability to deploy your c the download button on the upper right and to manage your Roaming Computers below.

Search

Advanced

6 Total

<input type="checkbox"/>	Identity Name	Status	Tags	SWG Override Setting	Last Sync
<input type="checkbox"/>	PC-1 (AD)	Protected & Encrypted at the DNS Layer DNS Layer Encryption: enabled		Enabled	9 minutes ago

20144921697684

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.