Understand Automated Deployment with Bundled Umbrella Profile (Windows)

Contents

Introduction

This document describes the automated deployment tutorial with bundled Umbrella profile in the Cisco Secure Client (Windows).

Overview

Deployment of the Cisco Secure Client (CSC) (formerly AnyConnect) with Umbrella module involves these components:

- Installation of the **CSC Core VPN Module**
- Installation of the **Umbrella Roaming Security Module**
- Installation of the **Umbrella Profile (OrgInfo.json)**
- Installation of the **Diagnostic and Reporting Tool (DART) Module (Optional)**

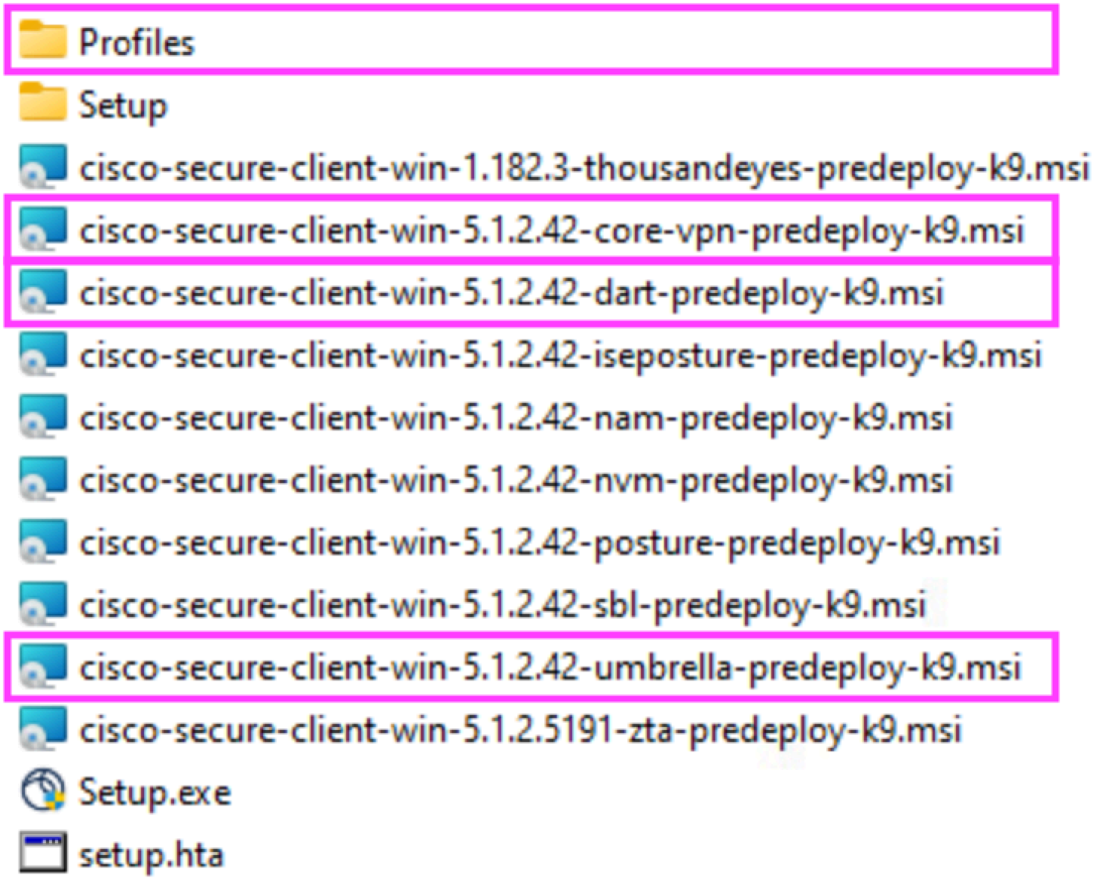
This article provides a tutorial on how to install these components programmatically (on Windows). The Umbrella Profile is embedded within the installation package suitable for installation from shared folders.

Create the pre-deployment package

These steps deploy the Umbrella module. Note that Cisco VPN functionality is completely disabled. However, the core VPN module still must be installed as it is used for underlying interception of DNS traffic.

Building the deployment package

1. Download the Umbrella roaming security module profile from your Umbrella Dashboard. **Deployments > Roaming Computers > Roaming Clients**.
    - The downloaded file name of the module profile is **Orginfo.json**
2. Download the Umbrella Roaming Security Module "pre-deployment" package for Windows from one of these locations:
    - :software.cisco.com
    - Umbrella Release Notes
3. Extract the downloaded AnyConnect Client and find the version number. Take note of the file names and version numbers in the extracted package



```
Profiles
Setup
cisco-secure-client-win-1.182.3-thousandeyes-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-core-vpn-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-dart-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-iseposture-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-nam-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-nvm-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-posture-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-sbl-predeploy-k9.msi
cisco-secure-client-win-5.1.2.42-umbrella-predeploy-k9.msi
cisco-secure-client-win-5.1.2.5191-zta-predeploy-k9.msi
Setup.exe
setup.hta
```

27073502800788

4. Add your **OrgInfo.json** file inside of the "Profiles\Umbrella"* folder in the same directory as the installer. **This step is crucial for the Cisco Umbrella module to register automatically after installation.** The folder structure must look like this:
   <#root>

```
cisco-secure-client-win-X.X.XXXXX-core-vpn-predeploy-k9.msicisco-secure-client-win-win-X.X.X

\Profiles\umbrella\OrgInfo.json
```

Create the **\Profiles\Umbrella** sub-folder next to your MSI files if it does not already exist.

Hosting the package

The package must be distributed to end users with the 'Profiles\Umbrella' sub-folder. This could be achieved in these ways:

- A shared network folder
- Endpoint management software that supports composition of multi-file install packages

Deploy the Package

The MSI files can now simply be deployed using endpoint management software or with 'msiexec'.

MSI commands

<#root>

```
msiexec /package cisco-secure-client-win-

X.X.XXXXX

-core-vpn-predeploy-k9.msi

PRE_DEPLOY_DISABLE_VPN=1

/norestart /passive /lvx* vpninstall.log
msiexec /package cisco-secure-client-win-

X.X.XXXXX

-umbrella-predeploy-k9.msi

PRE_DEPLOY_DISABLE_VPN=1

/norestart /passive /lvx* umbrellainstall.log
msiexec /package cisco-secure-client-win-

X.X.XXXXX

-dart-predeploy-k9.msi /norestart /passive /lvx* dartinstall.log
```

IMPORTANT: Replace X.X.XXXXX with the correct version numbers matching your MSI file names.

Ensure that the PRE_DEPLOY_DISABLE_VPN=1 option is added to the installation arguments to disable the VPN functionality., Alternatively, omit this argument to enable VPN functionality.

Additional MSI properties during installation

Cisco installation packages support several MSI properties which can be changed during installation. The commonly used properties for Cisco Umbrella are:

- **LOCKDOWN** = As described, prevents service from manually being disabled
- **ARPSYSTEMCOMPONENT** = Hides the program from Windows "Programs and Features" list

To set these during installation use the same installation steps but pass the additional properties to the msiexec command:

Enable Lockdown

```
<#root>

msiexec /package <MSI> /passive

LOCKDOWN=1

 /lvx*
```

Hide from Programs and Features

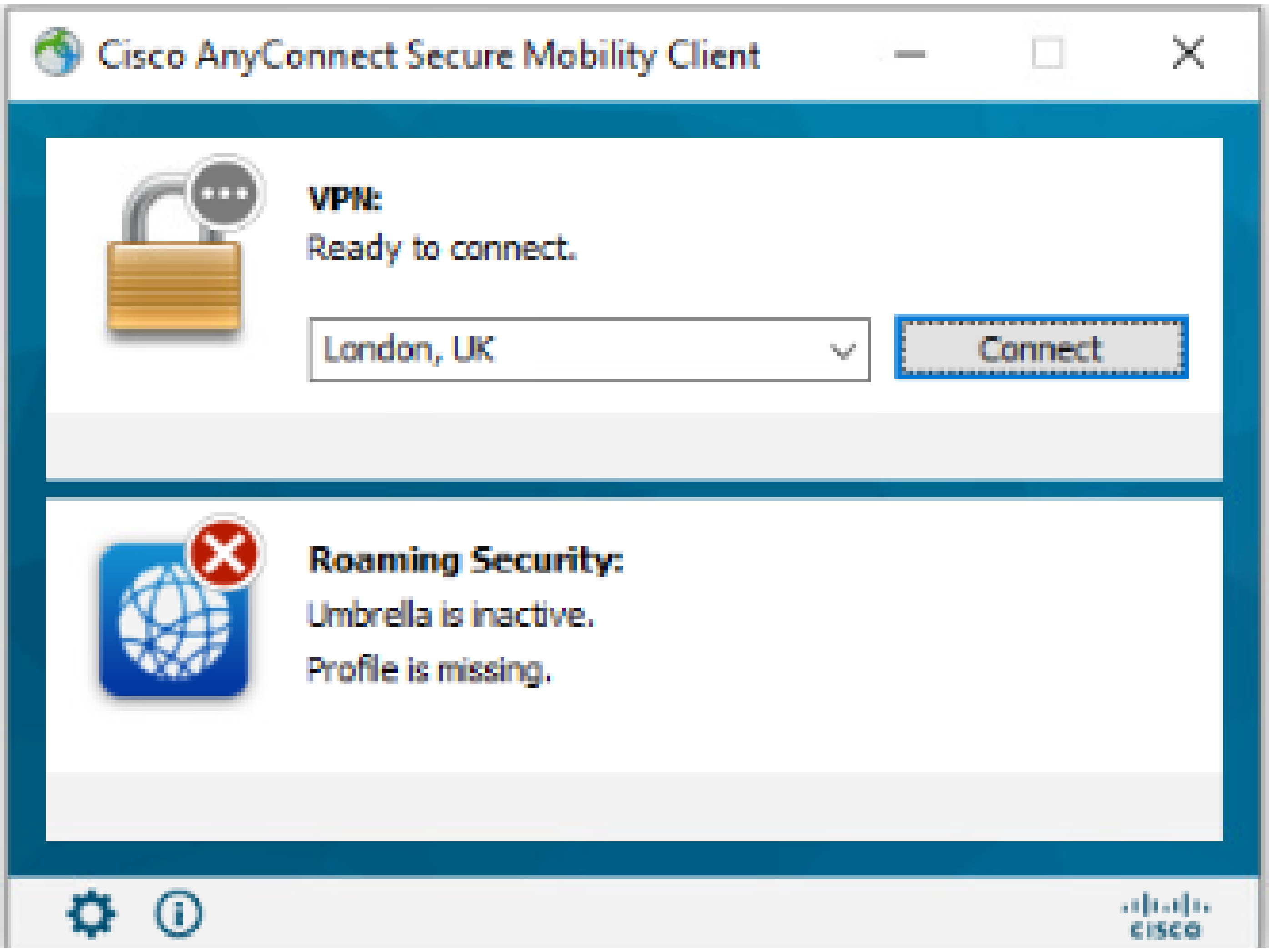
```
<#root>

msiexec /package <MSI> /passive

ARPSYSTEMCOMPONENT=1

 /lvx*
```

Alternatively, these MSI settings could be configured by supplying customized installer transform files (.mst files). For more information, see Configure AnyConnect Lockdown.

Deploying the Umbrella Profile (Post-Installation)

The common error "Profile is missing" indicates that the Cisco Umbrella module is installed but the profile (**OrgInfo.json**) is not. This means that the Cisco Umbrella module cannot register with Cisco Umbrella or enable protection.

Note that this problem does not happen if the profile was correctly embedded in the installation package.



VPN:
Ready to connect.

London, UK

Roaming Security:
Umbrella is inactive.
Profile is missing.

4435402655892

If it is not possible to embed the profile in the installation package it can be copied separately to the endpoint using an installation task or script. The profile must be deployed to this location:

```
%PROGRAMDATA%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json
```

The PowerShell script shows an example of how to create the OrgInfo.json programmatically as a post install task. Replace the ORG_ID, FINGERPRINT, and USER_ID placeholders with the relevant values from your profile.

```
$org_file = "%PROGRAMDATA%\Cisco\Cisco Secure Client\Umbrella\OrgInfo.json"
$data=@"
{
    "organizationId" : "ORG_ID",
    "fingerprint" : "FINGERPRINT",
    "userId" : "USER_ID"
}
"@

if(-not(Test-Path -Path $org_file))
{
```

```
$data > $org_file
}
```

Disabling VPN functionality (Post-Installation)

If the VPN functionality was not disabled during deployment, it is possible to disable it at a later time by deploying a special VPN profile to the device. See https://support.umbrella.com/hc/en-us/articles/18211951038740-How-to-hide-the-VPN-module-in-Cisco-Secure-Client-Windows

Deploy the Cisco Root CA

For error-less block pages and HTTPS browsing it is a requirement to trust the Cisco Umbrella Root CA to every endpoint. Refer to your endpoint management software for details on how to centrally deploy a Certificate Authority.