# Deploy Cisco ThousandEyes Module via Microsoft Intune

## Contents

## Introduction

This document describes step by step how to deploy the Cisco ThousandEyes Module via Microsoft Intune.

## Prerequisites

Cisco recommends that you have knowledge of these topics:

- Knowledge using MS Intune.
- Knowledge with Cisco Secure Access.

## Requirements

These requirements must be fulfilled before proceeding further:

- Access to your Cisco Secure Access Dashboard as Full Admin.
- Cisco ThousandEyes already integrated with Cisco Secure Access.
- You endpoints registered in MS Intune.

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Access Dashboard.
- Microsoft Intune Portal.

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.

**Note**: For Cisco Secure Access the recommended modules to deploy are: AnyConnect VPN, Umbrella Roaming Security, Zero Trust, ThousandEyes and DART. The procedure of deploying any of the modules using Intune is the exact same as explained below, just use the correct .xml/.json file for each.

# Configure

## Cisco Configuration

1. Log in to you Cisco Secure Access Dashboard, download the "ThousandEyes Endpoint Agent Configuration.json" and save it in your computer.

Go to Connect > End User Connectivity > Virtual Private Network > Click on Download Cisco Secure Client > Download the ThousandEyes Profile (ThousandEyes Endpoint Agent Configuration.json).

# Download Cisco Secure Client ✕

The Cisco Secure Client protects computers, on and off the network. View detailed deployment instructions in **Help** ↗

### ⊞ **Windows (x86/x64)** ⓘ
Version 5.1.8.105                                                              ⬇

### ⊞ **Windows (Arm)** ⓘ
Version 5.1.8.105                                                              ⬇

###  **macOS** ⓘ
Version 5.1.8.105                                                              ⬇

**Download Profiles**

For Internet Security module: orgInfo.json  ⬇

For VPN module:  | None                                             ⌄ |

For ThousandEyes module:  ThousandEyes Endpoint Agent Configuration.json  ⬇

All Cisco Secure Client versions are available in **Cisco Software** ↗

For cloud-based management of clients, use **Secure Client Management** ↗

**Close**

*Download of the ThousandEyes profile*

2. If you have not downloaded the ThosandEyes module yet, you can download it from the same location as in step #1.

Note: if you already have the Cisco Secure Client  pre-deploy package, you can skip this step.

# Download Cisco Secure Client ✕

The Cisco Secure Client protects computers, on and off the network. View detailed deployment instructions in **Help** ⌐

**▦ Windows (x86/x64)** ⓘ       ⤓

Version 5.1.8.105

**▦ Windows (Arm)** ⓘ       ⤓

Version 5.1.8.105

**🍎 macOS** ⓘ       ⤓

Version 5.1.8.105

**Download Profiles**

For Internet Security module: orgInfo.json ⤓

For VPN module: [ None ⌄ ]

For ThousandEyes module: ThousandEyes Endpoint Agent Configuration.json ⤓

All Cisco Secure Client versions are available in **Cisco Software** ⌐

For cloud-based management of clients, use **Secure Client Management** ⌐

**Close**

*Download of the Secure Client software*

3. Unzip the cisco-secure-client-win-5.1.8.105-predeploy-k9, and drop the ThousandEyes Endpoint Agent
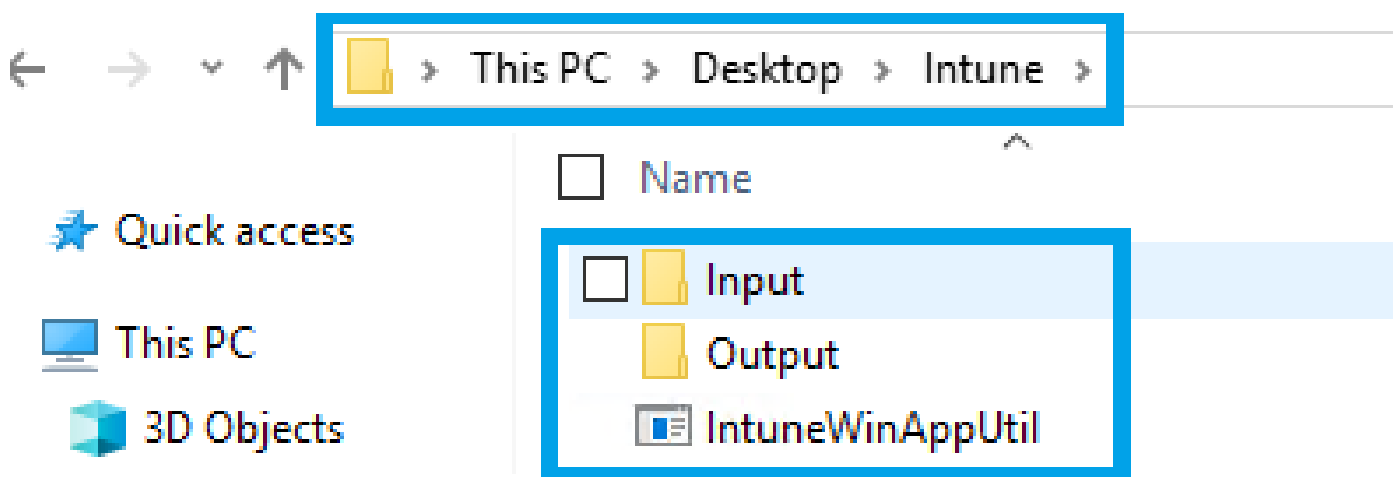
Configuration.json under cisco-secure-client-win-5.1.8.105-predeploy-k9\Profiles\thousandeyes path.
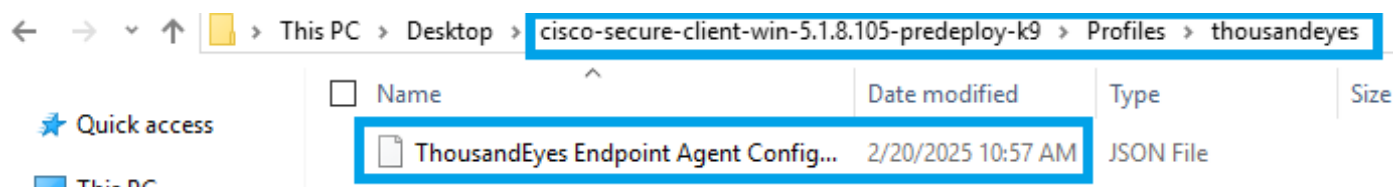


*Drop of ThousandEyes.json in proper Intune location*

4. Download "Microsoft Win32 Content Prep Tool".

5. Create a folder and drop the "IntuneWinAppUtil" application, also create an input and output folder in your machine



*Create folders used by Intune*

6. In the "Input folder", drop the cisco-secure-client-win-1.226.2-thousandeyes-predeploy-k9 file. Also, copy/paste the "Profiles" folder and subfolders (the Profiles subfolders is where you dropped the ThousandEyes Endpoint Agent Configuration.json in Step 3).
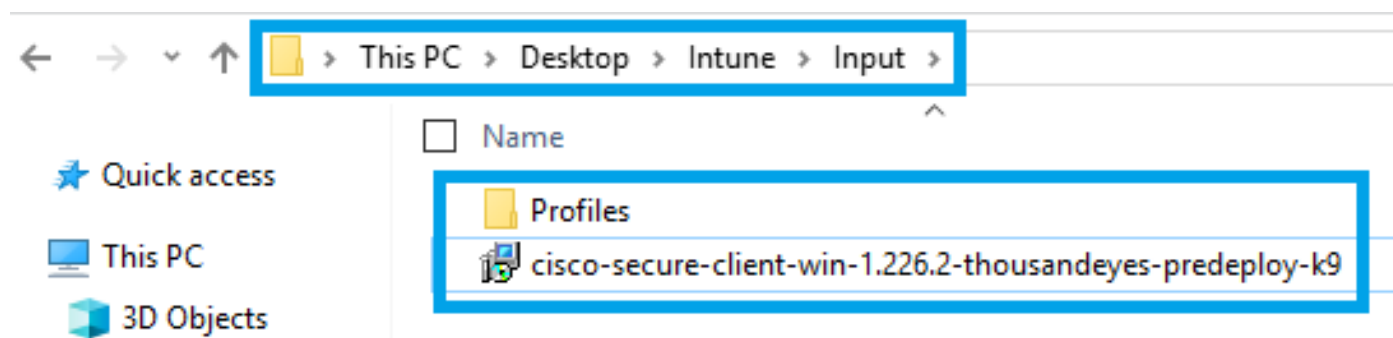


*Drop the required files in the Input Intune Folder*

7. Run the "IntuneWinAppUtil.exe" application: specify the "Input" folder as your source folder, cisco-secure-client-win-1.226.2-thousandeyes-predeploy-k9.msi as your source setup file, and the "Output" folder as your output folder (here is where the application generates the ThousandEyes.intunewin file):

```
C:\Users\Administrator\Desktop\Intune\IntuneWinAppUtil.exe
Please specify the source folder: Input
Please specify the setup file: cisco-secure-client-win-1.226.2-thousandeyes-predeploy-k9.msi
Please specify the output folder: Output
Do you want to specify catalog folder (Y/N)?N_
```
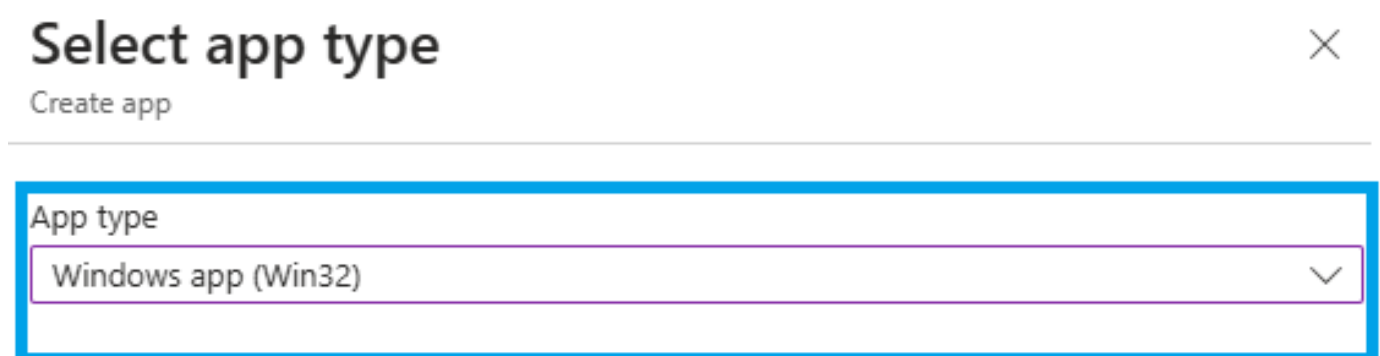
*Conversion to intunewin file*

After this step is done, confirm the creation of the ThousandEyes .intunewin file under the Intune_output folder:
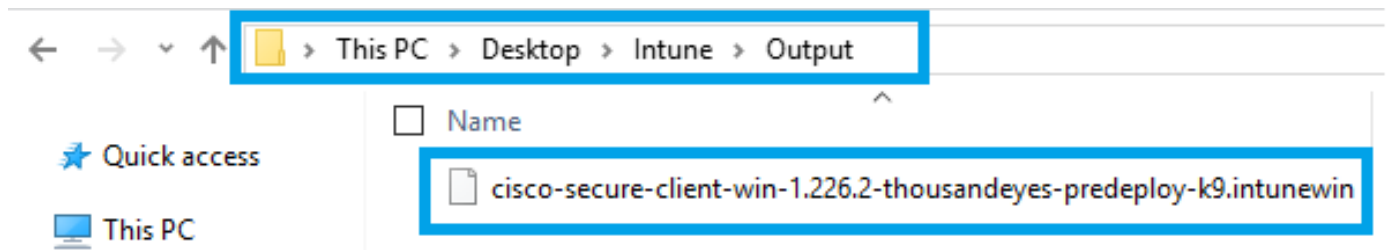


*intunewin file in MS Intune Output Folder*

## Microsoft Intune Configuration

1. In the MS Intune Portal, go to "Home > Apps > Windows > + Add" and for Select app Type choose "Windows app (Win32)" then click "Select":



*Creation of App in Azure*

2. Click on "Select app package file" and upload the ThousandEyes.intunewin file, then click "OK":

*Select the package file*

3. On this step specify the minimum information like "Publisher" and "Category" and click "Next":



*Define minimum information*

4. (Optional) Specify the installation command parameters.

5. As part of the Requirements, you need to specify the OS architecture and Minimum OS running on the devices you want to push the Cisco ThousandEyes Module (you can also specify other requirements if needed).

App information    Program    **Requirements**    Detection rules    Review + save

Specify the requirements that devices must meet before the app is installed:

| Operating system architecture * ⓘ | 64-bit | ⌄ |
| Minimum operating system * ⓘ | Windows 10 1607 | ⌄ |

*Define OS information*

6. You can optionally configure detection rules to detect if the if another version is already present on the device, with this option you can also detect if same or different ThousandEyes image is found.

# Detection rule      ✕

Create a rule that indicates the presence of the app.

| Rule type * ⓘ | MSI | ⌄ |

| MSI product code * ⓘ | {BB14E2E6-C433-44C8-BEB5-0FA310B14C2E} | ✓ |

MSI product version check ⓘ    ( Yes    **No** )

*Define Detection Rule*

7. On the Dependencies option we are configuring any for the ThousandEyes Module so just click "Next" here.

8. Optionally, you can configure Supersedense in order to update or replace an existing application on the device, it only applies to Win32 apps, for further information about Supersedense you can refer to the [MS Intune documentation](#). In our example we are not specifying any application to be replaced so just click "Next".

9. Specify the assignments to specify the group/devices we want to install the Secure Client VPN Core to. Once assigned, click "Next":



✅ App information   ✅ Program   ✅ Requirements   ✅ Detection rules   ✅ Dependencies   ✅ Supersedence   7️⃣ **Assignments**

ⓘ Any Win32 app deployed using Intune will not be automatically removed from the device when the device is retired. The app and the data it contains will remain on the de... the app.

**Required** ⓘ

| Group mode | Group | Filter mode | Filter | End user notifi... |
|---|---|---|---|---|
| ⊕ Included | Intune Group | None | None | Show all toast ... |

*Assign it to users for deployment*

10. Review the configuration, and click "Create"

11. If you go back to MS Intune Portal under "Home>Apps>Windows" you can see the created AnyConnect Core VPN Win32 app:



*Verify the app was created*

## Verify

Check in MS Intune that the application was successfully installed.

Home > Apps > All Apps > Cisco Secure Client - ThousandEyes Endpoint Agent:



*Verify in MS Intune*

Check locally on the PC that the ThousandEyes app shows as an installed application and/or that the service is running:
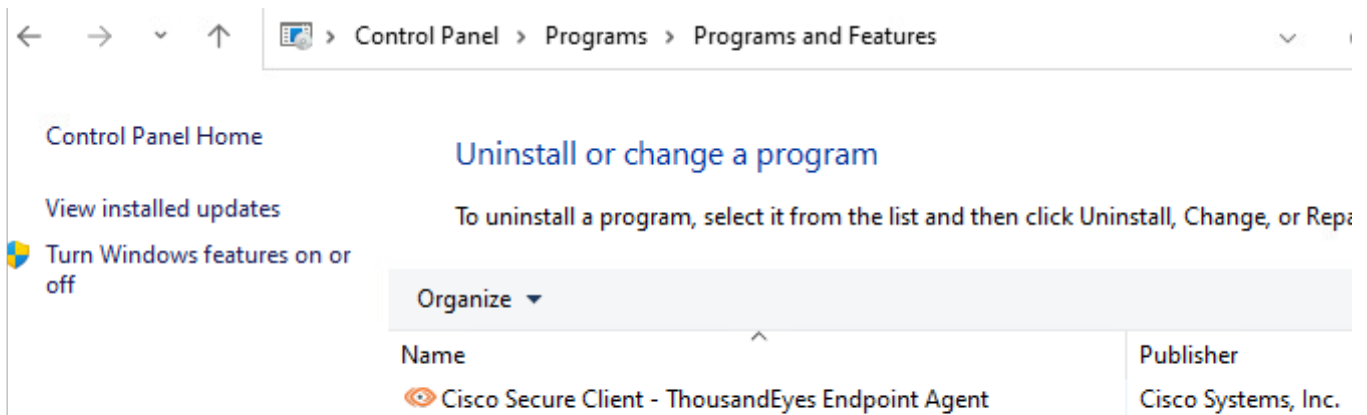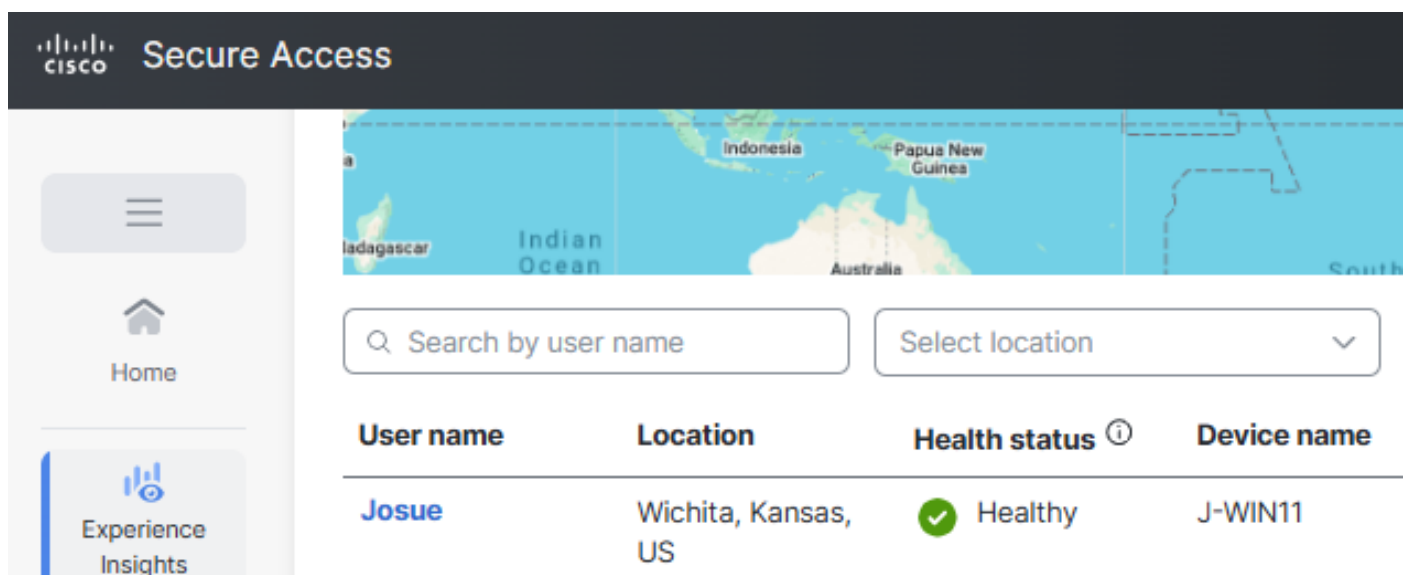
*Verify locally in the PC*
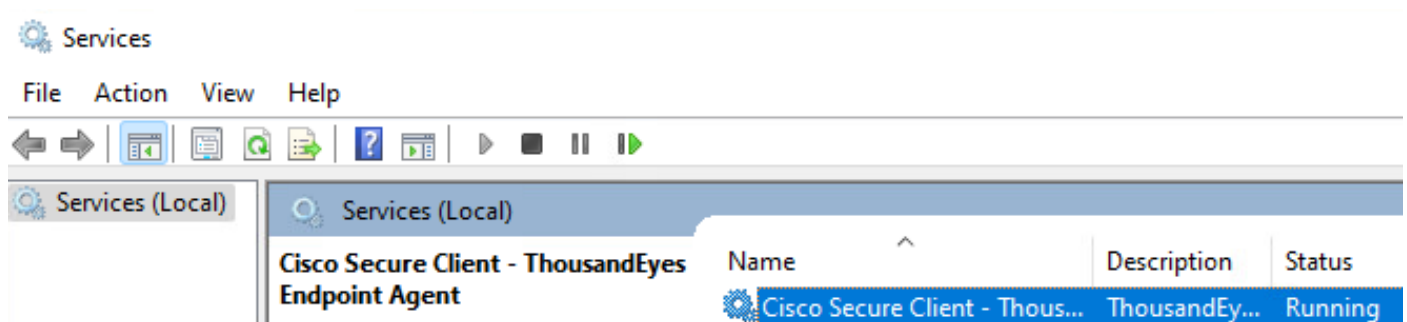


*Verify locally in the PC*

Check in the Cisco Secure Access Dashboard that the endpoint was registered.

Experience Insights > Management:



*Verify in Cisco Secure Access*