

Distribuire Cisco ThousandEyes Module tramite Microsoft Intune

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione Cisco](#)

[Configurazione di Microsoft Intune](#)

[Verifica](#)

Introduzione

In questo documento viene descritto passo a passo come distribuire il modulo Cisco ThousandEyes tramite Microsoft Intune.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza tramite MS Intune.
- Conoscenza di Cisco Secure Access.

Requisiti

Prima di procedere, è necessario soddisfare i seguenti requisiti:

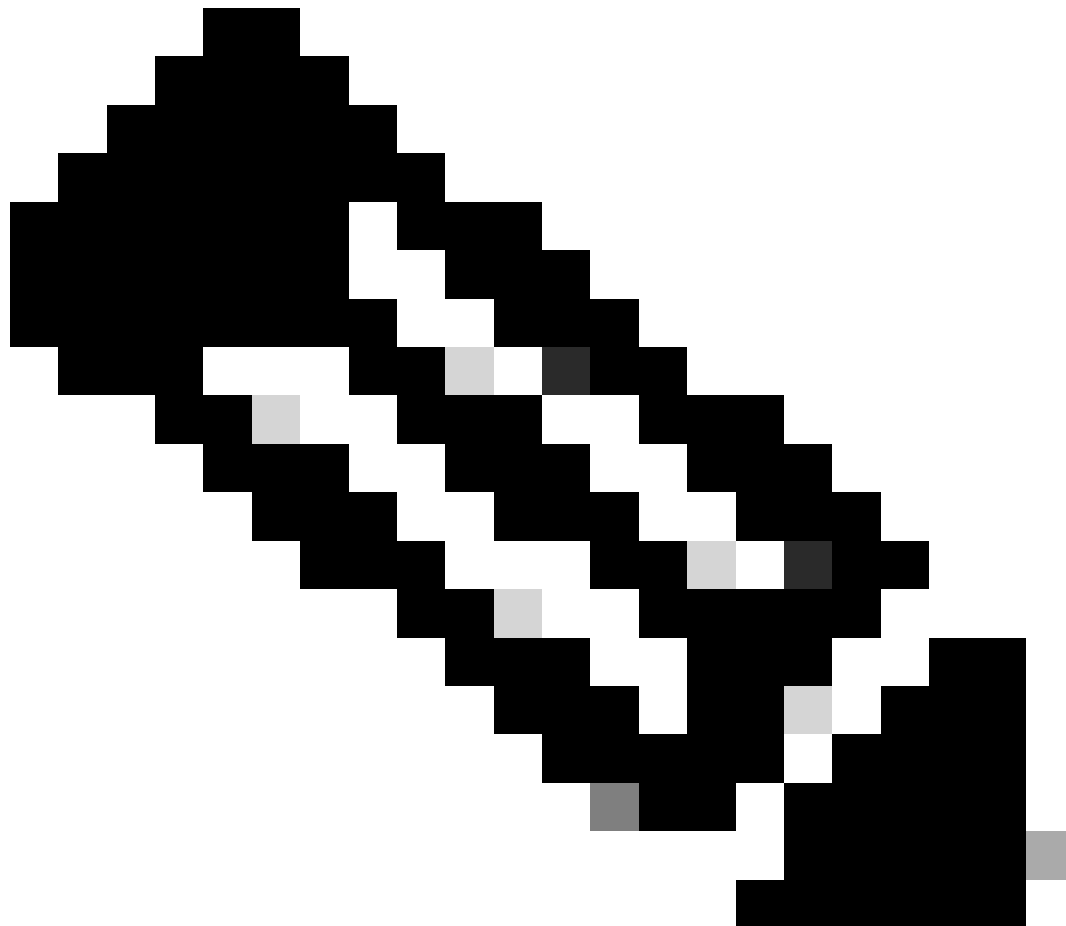
- Accedere a Cisco Secure Access [Dashboard](#) come amministratore completo.
- Cisco ThousandEyes è già integrato con Cisco Secure Access.
- Gli endpoint sono stati registrati in MS Intune.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Access Dashboard.
- Portale di Microsoft Intune.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.



Nota: Per Cisco Secure Access, i moduli consigliati da distribuire sono: AnyConnect VPN, sicurezza del roaming per gli ombrelli, Zero Trust, ThousandEyes e DART. La procedura di distribuzione di uno dei moduli con Intune è esattamente la stessa descritta di seguito. È sufficiente utilizzare il file .xml/.json corretto per ciascuno di essi.

Configurazione

Configurazione Cisco

1. Accedere a Cisco Secure Access Dashboard, scaricare il file "ThousandEyes Endpoint Agent Configuration.json" e salvarlo nel computer.

Selezionare Connect (Connetti) > End User Connectivity (Connettività utente finale) > Virtual Private Network (Rete privata virtuale) > Click on Download Cisco Secure Client (Scarica 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

Scarica il profilo ThousandEyes

2. Se il modulo ThousandEyes non è stato ancora scaricato, è possibile scaricarlo dalla stessa posizione della fase #1.

Nota: se si dispone già del pacchetto di predistribuzione di Cisco Secure Client, è possibile ignorare questo passaggio.

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:

For ThousandEyes module: ThousandEyes Endpoint Agent Configuration.json 

All Cisco Secure Client versions are available in [Cisco Software](#)

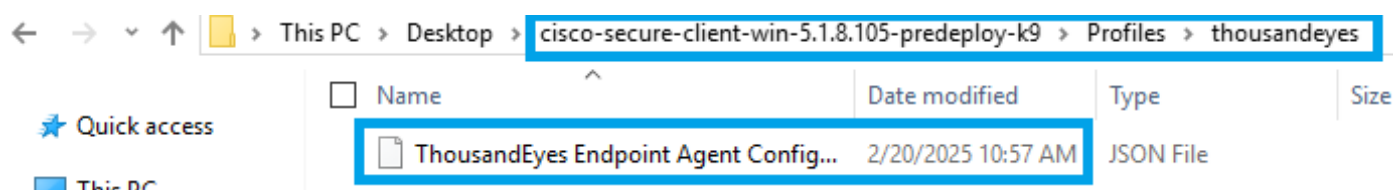
For cloud-based management of clients, use [Secure Client Management](#)

Close

Download del software Secure Client

3. Decomprimere cisco-secure-client-win-5.1.8.105-predeploy-k9 e rilasciare ThousandEyes

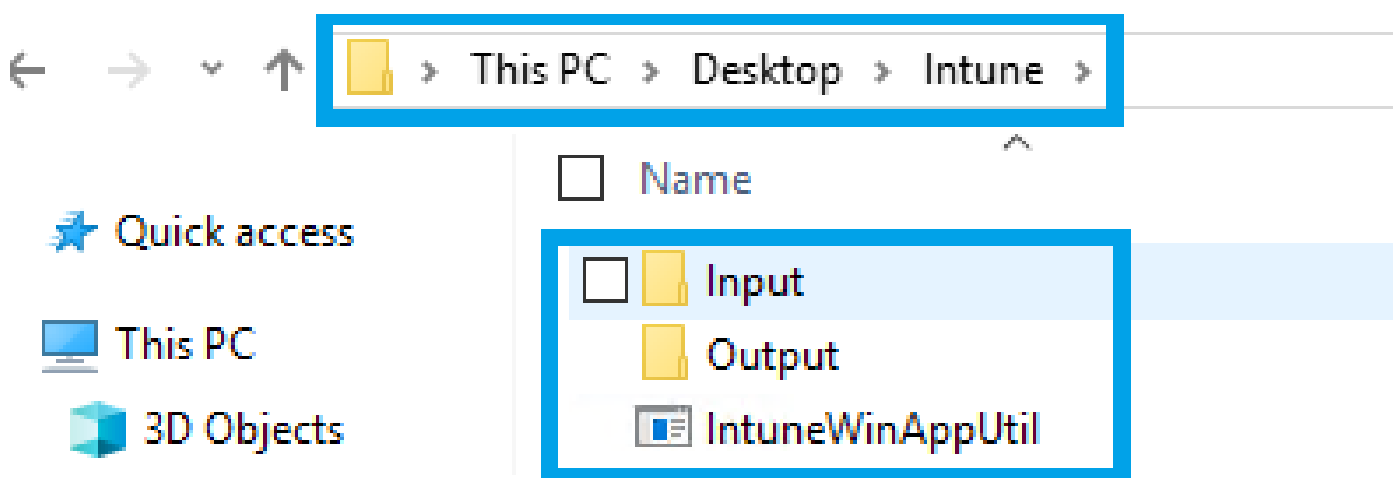
Endpoint Agent Configuration.json in cisco-secure-client-win-5.1.8.105-predeploy-k9\Profiles\thousandeyes path.



Goccia di ThousandEyes.json nella corretta posizione di Intune

4. Scaricare "[Microsoft Win32 Content Prep Tool](#)".

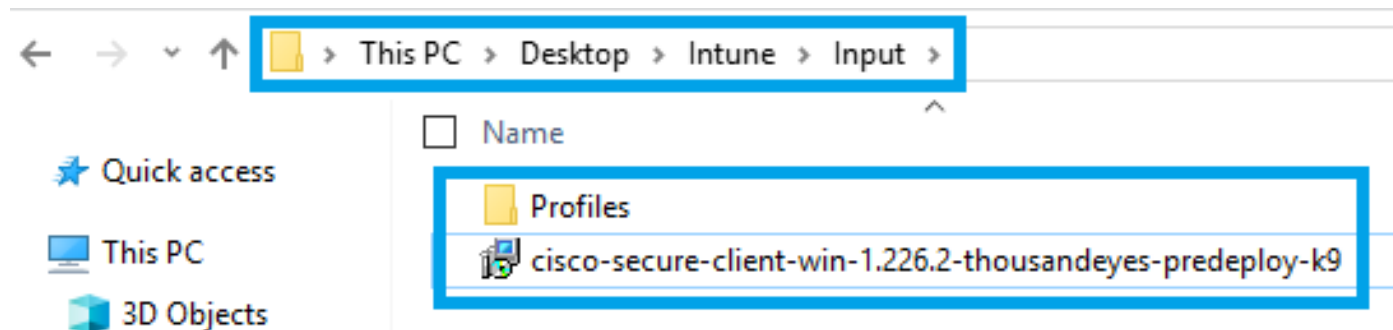
5. Creare una cartella ed eliminare l'applicazione "IntuneWinAppUtil", nonché creare una cartella di input e output nel computer



Creazione di cartelle utilizzate da Intune

6. Nella "cartella di input", eliminare il file cisco-secure-client-win-1.226.2-thousandeyes-predeploy-k9.

Inoltre, copiare/incollare la cartella "Profiles" e le sottocartelle (le sottocartelle Profiles sono le sottocartelle in cui è stato eliminato ThousandEyes Endpoint Agent Configuration.json nel Passaggio 3).



Elimina i file richiesti nella cartella di Input Intune

7. Eseguire "IntuneWinAppUtil.exe": specificare la cartella "Input" come cartella di origine, cisco-secure-client-win-1.226.2-thousandeyes-predeploy-k9.msi come file di configurazione di origine e la cartella "Output" come cartella di output (in questa posizione l'applicazione genera il file

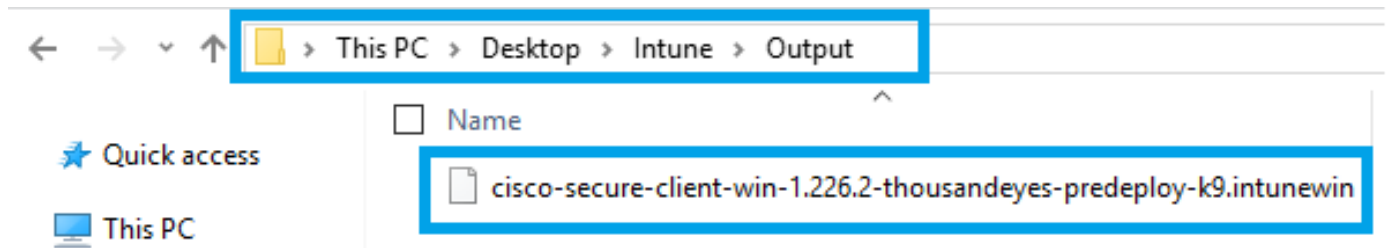
ThousandEyes.intunewin):

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_
```

Conversione in file intunewin

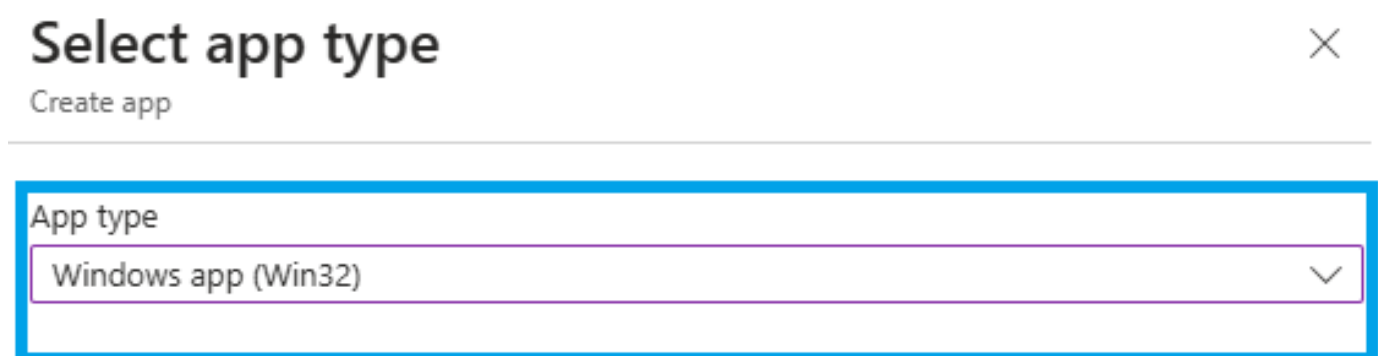
Al termine, confermare la creazione del file .intunewin ThousandEyes nella cartella Intune_output:



file intunewin nella cartella di output di MS Intune

Configurazione di Microsoft Intune

1. Nel portale di MS Intune, andare su "Home > App > Windows > + Aggiungi" e per Seleziona tipo di app scegliere "Applicazione Windows (Win32)", quindi fare clic su "Seleziona":



Windows app (Win32)

Creazione dell'app in Azure

2. Fare clic su "Select app package file" e caricare il file ThousandEyes.intunewin, quindi fare clic su "OK":

App package file



App package file * ⓘ

"cisco-secure-client-win-1.226.2-thousandeyes-predeploy-k9.intunewin"

Name: Cisco Secure Client - ThousandEyes Endpoint Agent
Platform: windows
App version: 1.226.2
Size: 13.24 MiB
MAM Enabled: No

OK

Selezionare il file del pacchetto

3. In questo passo specificare le informazioni minime come "Publisher" e "Category" e fare clic su "Next":

Microsoft Intune admin center

Home > Apps | Windows > Windows | Windows apps >

Add App ...
Windows app (Win32)

Name * ⓘ
Cisco Secure Client - ThousandEyes Endpoint Agent

Description *
[Get help with markdown supported for descriptions.](#)
Cisco Secure Client - ThousandEyes Endpoint Agent

Preview
Cisco Secure Client - ThousandEyes Endpoint Agent

Publisher * ⓘ
Cisco

App Version ⓘ
1.226.2

Category ⓘ
Other apps

Definire le informazioni minime

4. (Facoltativo) Specificare i parametri del comando di installazione.

5. Come parte dei Requisiti, è necessario specificare l'architettura del sistema operativo e il numero minimo di sistemi operativi in esecuzione sui dispositivi su cui si desidera eseguire il push del modulo Cisco ThousandEyes (è possibile specificare anche altri requisiti, se necessario).

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

Operating system architecture *	64-bit	▼
Minimum operating system *	Windows 10 1607	▼

Definire le informazioni sul sistema operativo

6. Se si desidera, è possibile configurare le regole di rilevamento per rilevare se sul dispositivo è già presente un'altra versione. Con questa opzione è inoltre possibile rilevare se viene trovata la stessa immagine ThousandEyes o un'immagine ThousandEyes diversa.

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

Definisci regola di rilevamento

7. Per l'opzione Dipendenze stiamo configurando qualsiasi per il modulo ThousandEyes, quindi basta fare clic su "Avanti" qui.

8. Facoltativamente, è possibile configurare Supersedense per aggiornare o sostituire un'applicazione esistente sul dispositivo. Si applica solo alle app Win32. Per ulteriori informazioni su Supersedense, consultare la [documentazione di MS Intune](#). Nell'esempio non viene specificata alcuna applicazione da sostituire, quindi fare clic su "Avanti".

9. Specificare le assegnazioni per specificare il gruppo o i dispositivi in cui installare Secure Client VPN Core. Una volta assegnato, fare clic su "Next" (Avanti):

i 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 device.

Required ⓘ

Group mode	Group	Filter mode	Filter	End user notification
+ Included	Intune Group	None	None	Show all toast notifications

Assegnarlo agli utenti per la distribuzione

10. Esaminare la configurazione e fare clic su "Crea"

11. Se si torna al portale di MS Intune in "Home>Apps>Windows", è possibile visualizzare l'app AnyConnect Core VPN Win32 creata:

[Home](#) > [Apps | Windows](#) >

Windows | Windows apps ...

✕ ⏪

[+](#) Add [↻](#) Refresh [🔍](#) Filter [↓](#) Export [☰](#) Columns

 Windows apps

Filters applied: Platform, App type

Name

↑↓

Type

Cisco Secure Client - ThousandEyes Endpoint Agent Windows app (Win32)

Verificare che l'app sia stata creata

Verifica

Verificare che l'applicazione sia stata installata correttamente in MS Intune.

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

[Home](#) > [Cisco Secure Client - ThousandEyes Endpoint Agent](#)

Cisco Secure Client - ThousandEyes Endpoint Agent | Device install status ...

Client Apps

⊞ ⏪

[↻](#) Refresh [☰](#) Columns [↓](#) Export

① Overview

> Manage

✓ Monitor

 Device install status

 User install status

 Dependency viewer

ⓘ

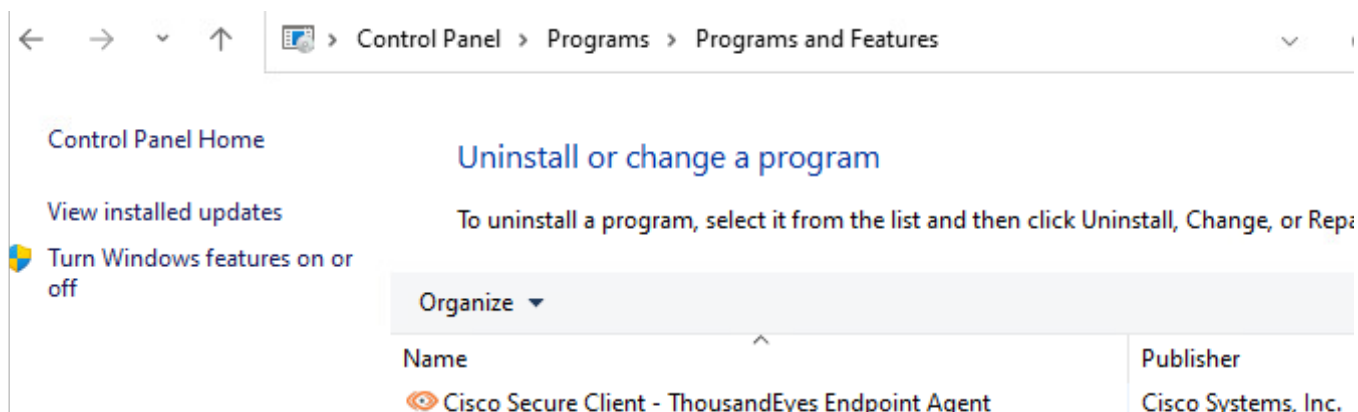
[+](#) Add filter

Showing 1 to 1 of 1 records

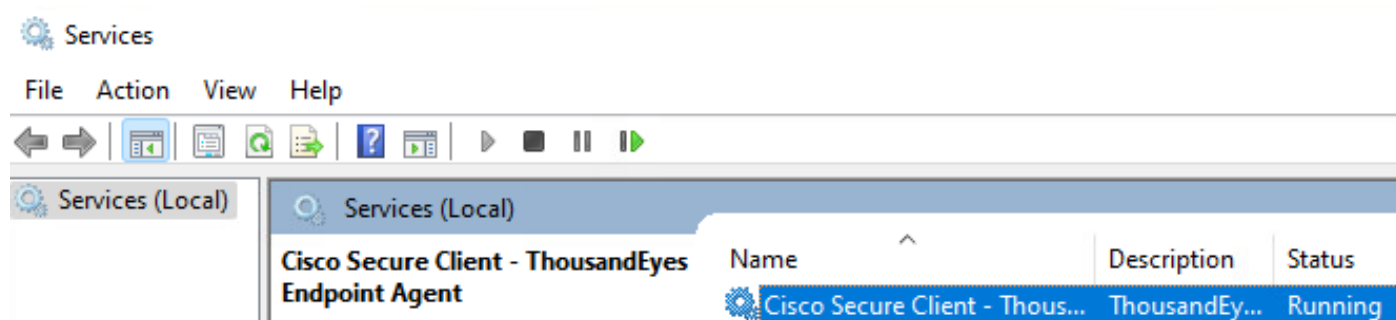
Device Name ↑↓	UPN ↑↓	Device Platform ↑↓	App Version ↑↓	Status ↑↓
J-WIN11	jbrenesm	Windows 10.0.22000.2538	1.226.2	Installed

Verifica in MS Intune

Verificare localmente sul PC che l'app ThousandEyes venga visualizzata come applicazione installata e/o che il servizio sia in esecuzione:



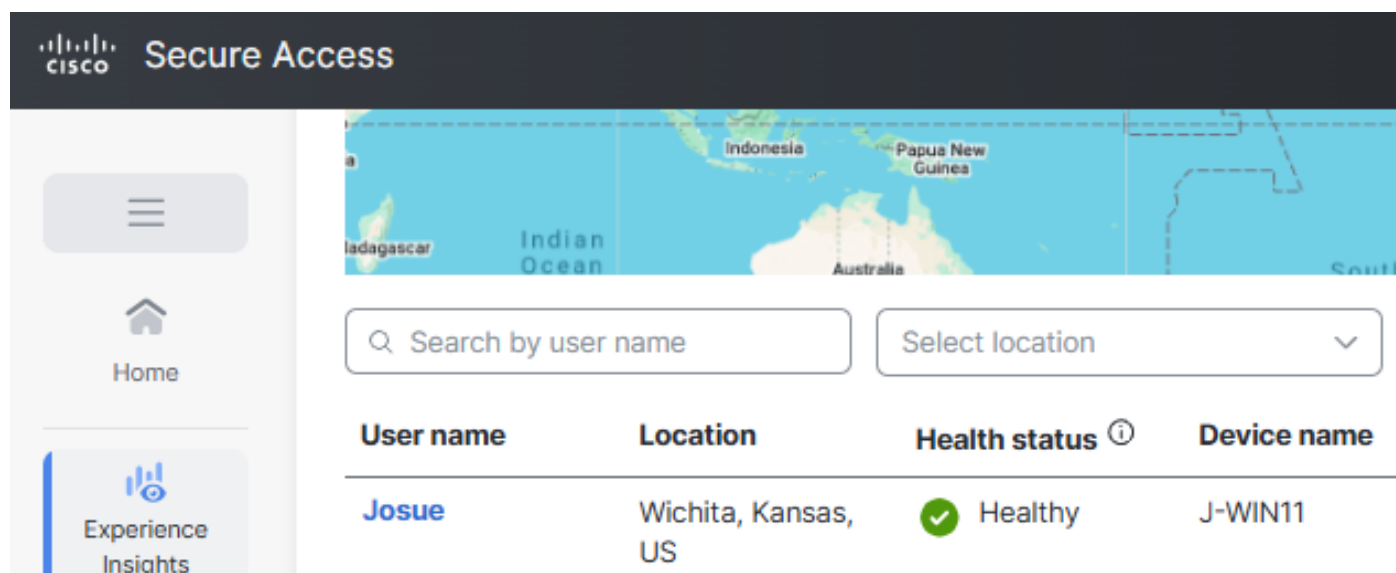
Verifica in locale nel PC



Verifica in locale nel PC

Verificare nel Dashboard di accesso sicuro Cisco che l'endpoint sia stato registrato.

Experience Insights > Gestione:



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).