Dépanner les indicateurs d'accès sécurisé manquants dans Experience Insights sous la section Performances des terminaux

Table des matières

Introduction

Problème

Solution

Informations connexes

Introduction

Ce document décrit comment corriger les mesures manquantes dans Experience Insights sous la section Performances des points de terminaison.

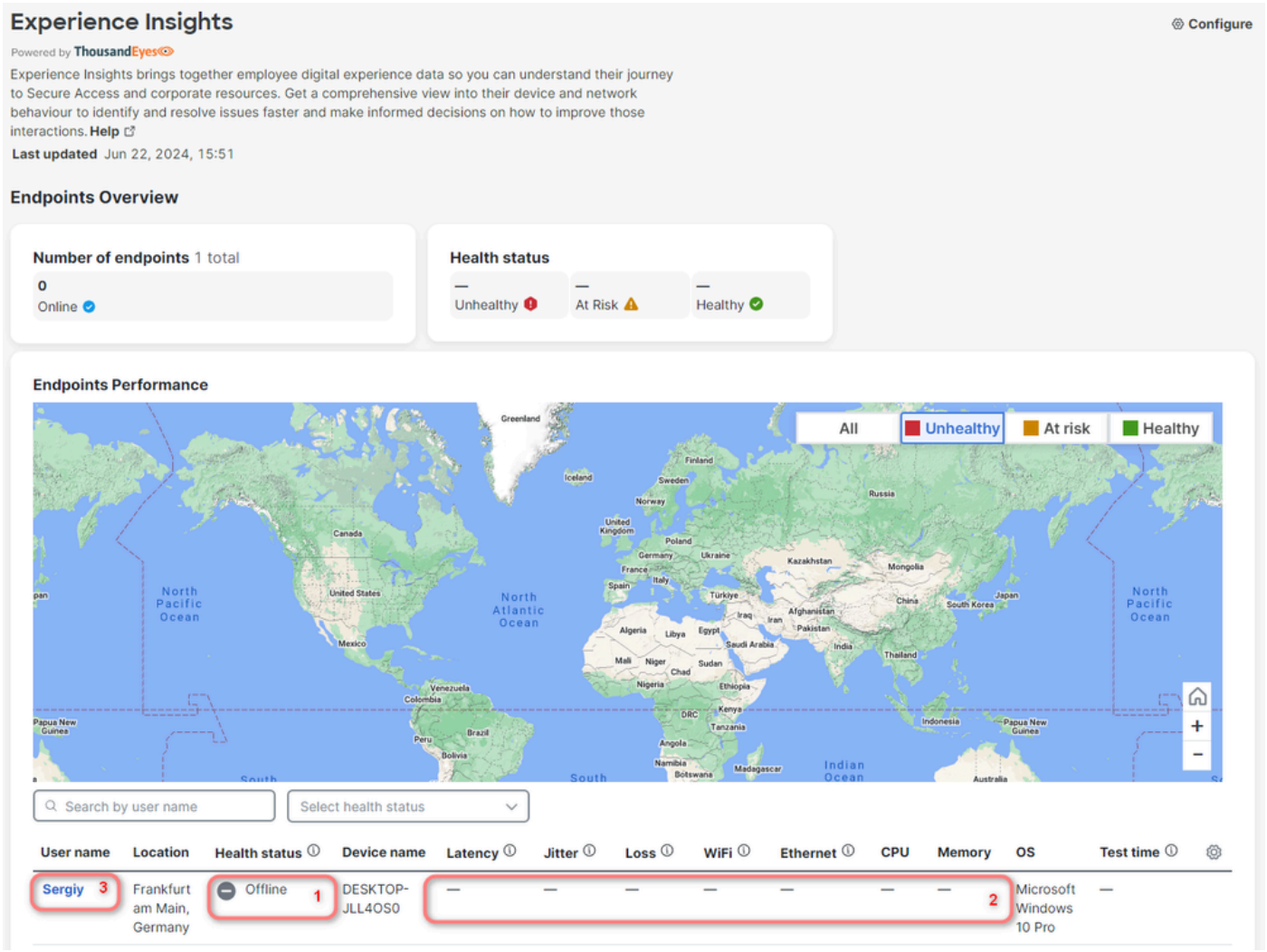
Problème

Pour vérifier si vous rencontrez le problème, procédez comme suit :

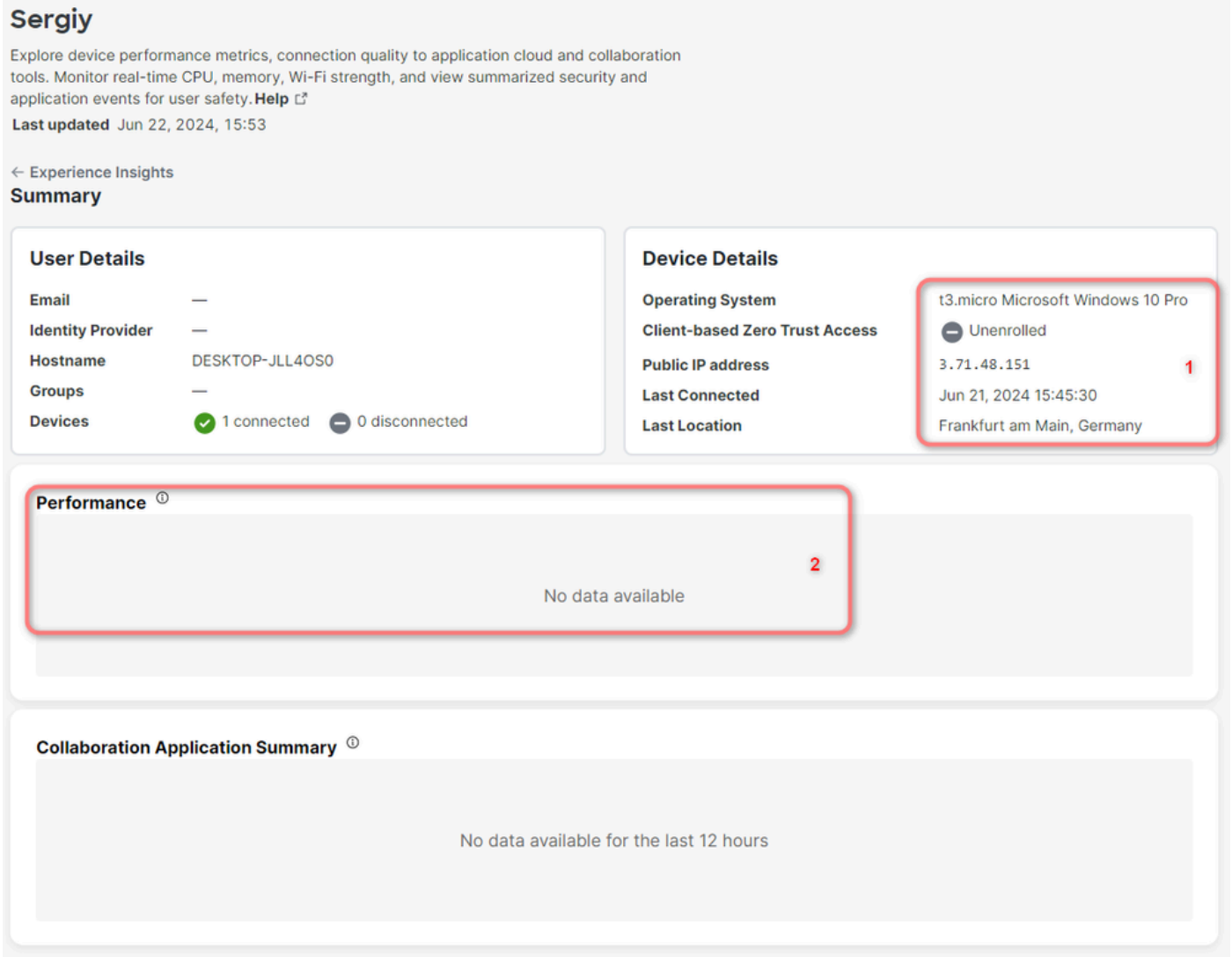
- Cliquer **Experience Insights > Management**

Il doit y avoir des indicateurs dans **Experience Insights** la section **Endpoints Performance.**

1. Si le périphérique a l'état Hors connexion
2. Ensuite, les mesures indiquant les tirets sont attendues
3. Cliquez sur le nom d'utilisateur pour afficher les détails du PC surveillé dans le tableau de bord d'accès sécurisé

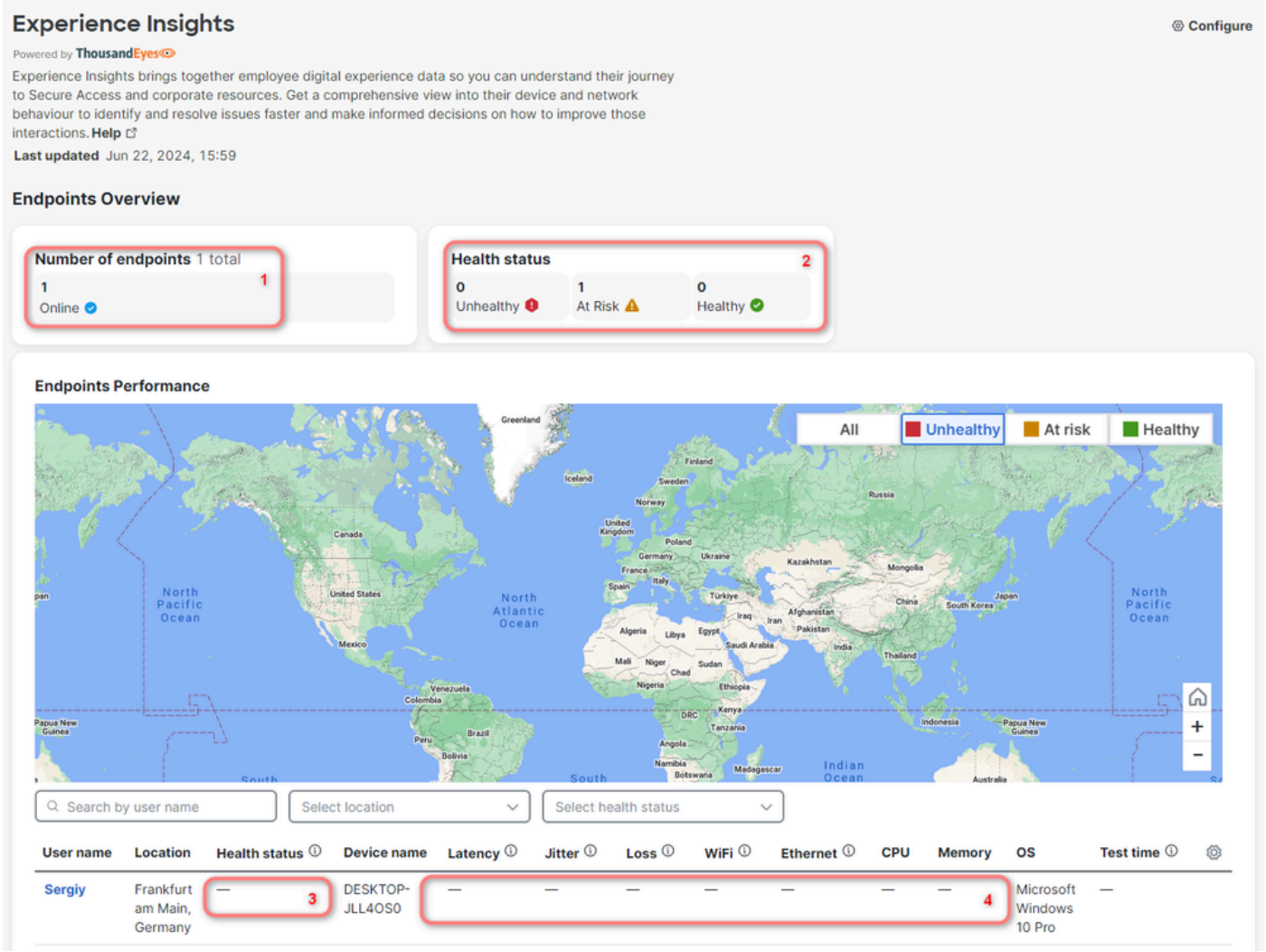


Vous pouvez voir quand il a été connecté pour la dernière fois et aucune donnée de performance n'est disponible, ce qui est attendu car le périphérique est **Offline**.



Mettez sous tension l'ordinateur surveillé avec l'agent Thousand Eyes installé. Ensuite, revenez à la page Experience Insights > Management.

1. Ensuite, vous voyez le nombre mis à jour de terminaux en ligne
2. L'état de santé indique qu'un terminal **At Risk**
3. Dans le tableau, vous pouvez voir des tirets
4. Cependant, ces tirets sont attendus si vous n'avez pas configuré la version NPCAP autorisée



Solution

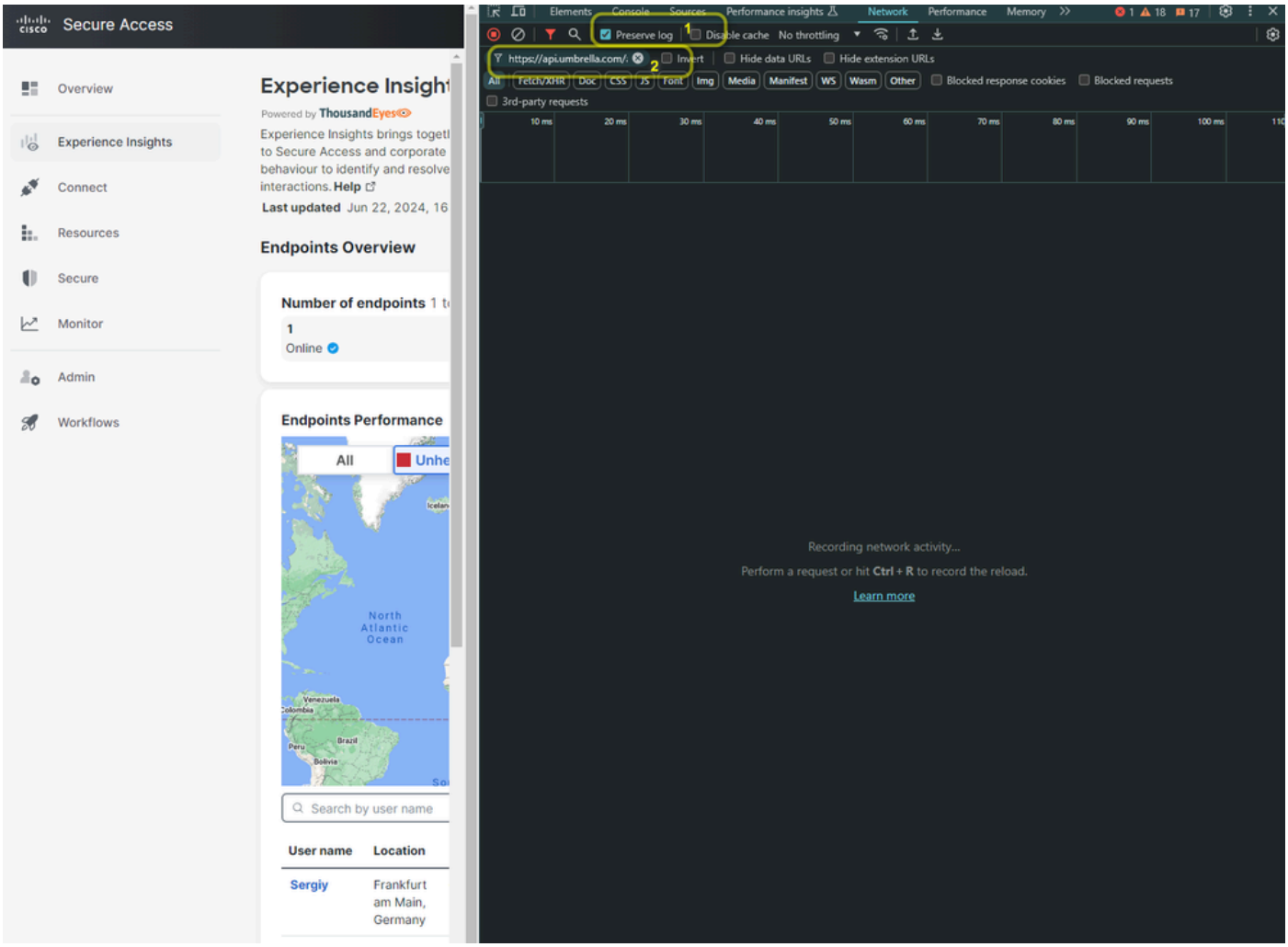
Pour résoudre le problème, vérifiez les étapes suivantes :

Dans le navigateur (dans cet exemple, vous devez utiliser Chrome)

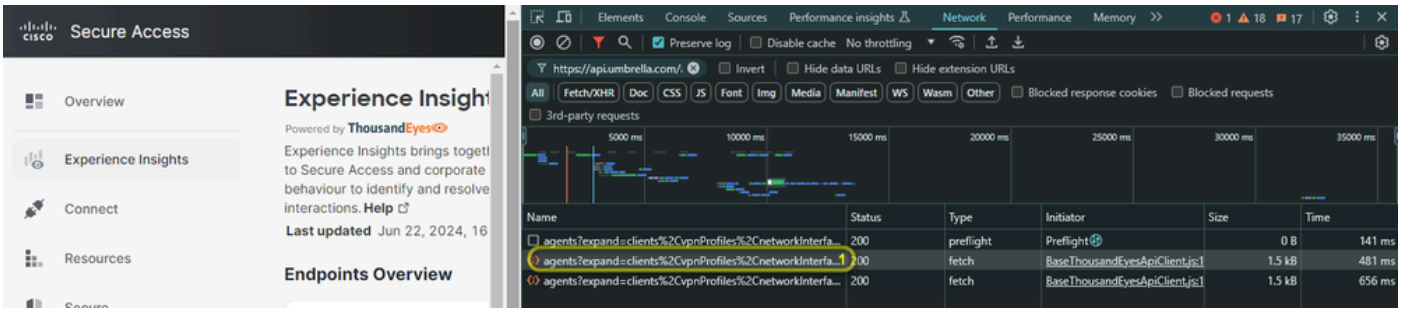
- Clic Settings > More Tools > Developer Tools
- Cochez la case **Preserve log**

Dans l'option filter, saisissez la chaîne suivante :

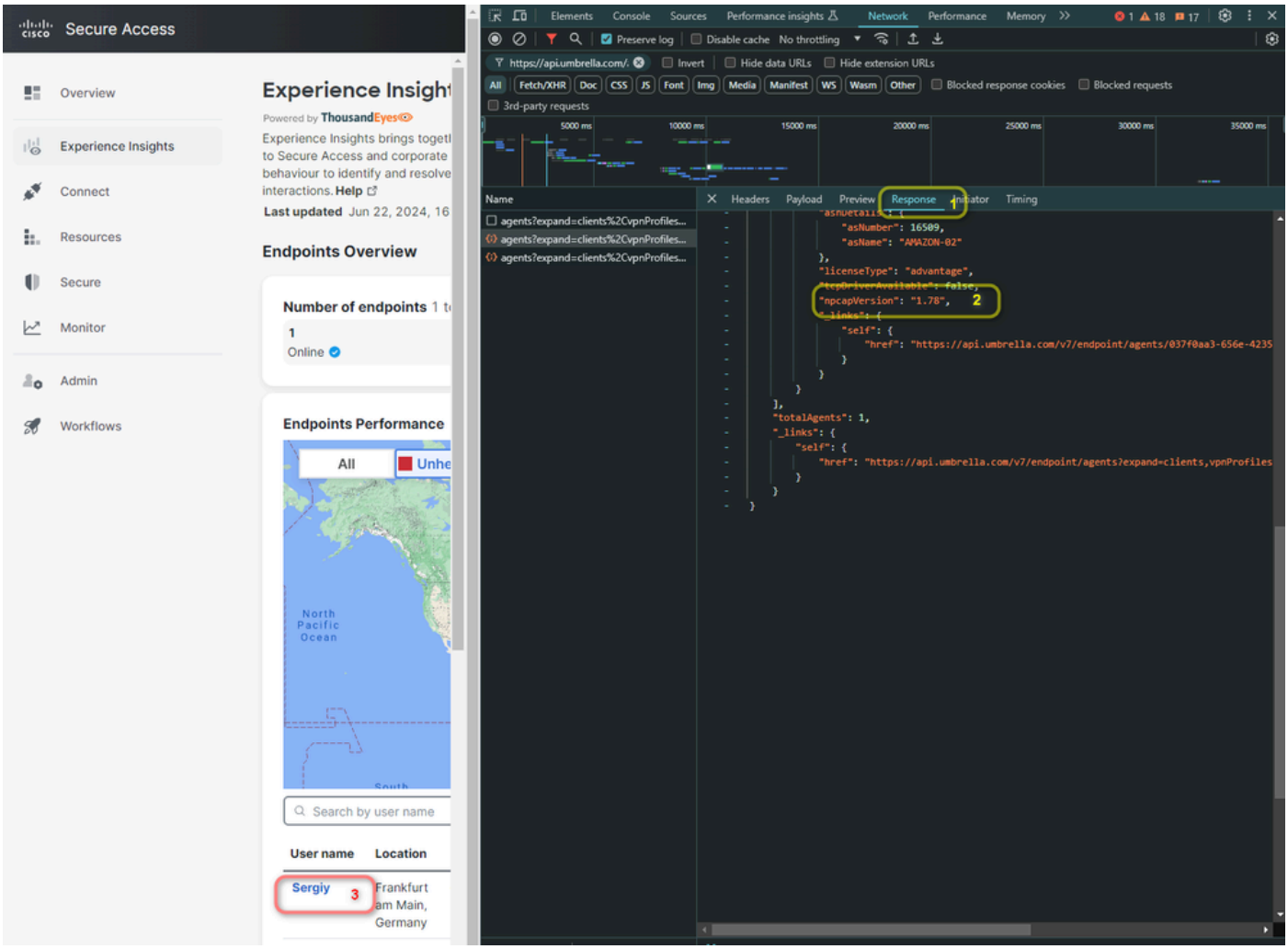
```
https://api.umbrella.com/auth/v2/internal/thousandeyes/v7/endpoint/agents?expand
```



Ensuite, actualisez la page pour afficher les demandes dans **Developer Tools**.



1. Cliquer **Response**
2. La réponse contient le format JSON structuré avec des sections pour chaque PC surveillé. Vous pouvez faire défiler jusqu'à la fin de la section pour un PC spécifique et noter la version npcap. Dans cet exemple, j'ai un PC test avec la version 1.78 de npcap
3. Si vous en avez d'autres **User name** dans le tableau, vérifiez la version de npcap pour chaque PC surveillé



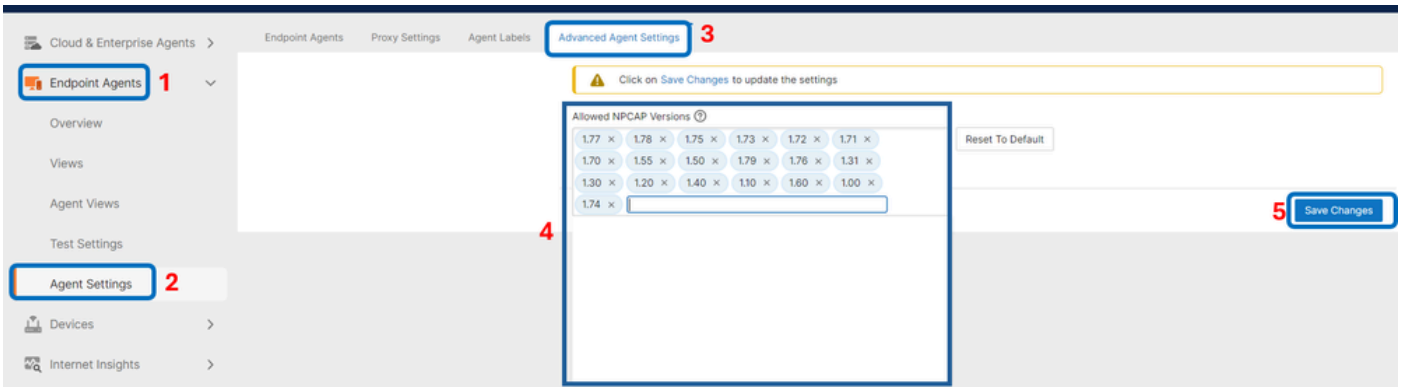


Remarque : Le tableau indique une limite de 10 périphériques surveillés. Si vous disposez de plus de 10 périphériques, vous devez faire de même sur chaque page.

Après avoir collecté toutes les versions d'agent npcap, vous devez accéder à TE pour ajouter les versions prises en charge.

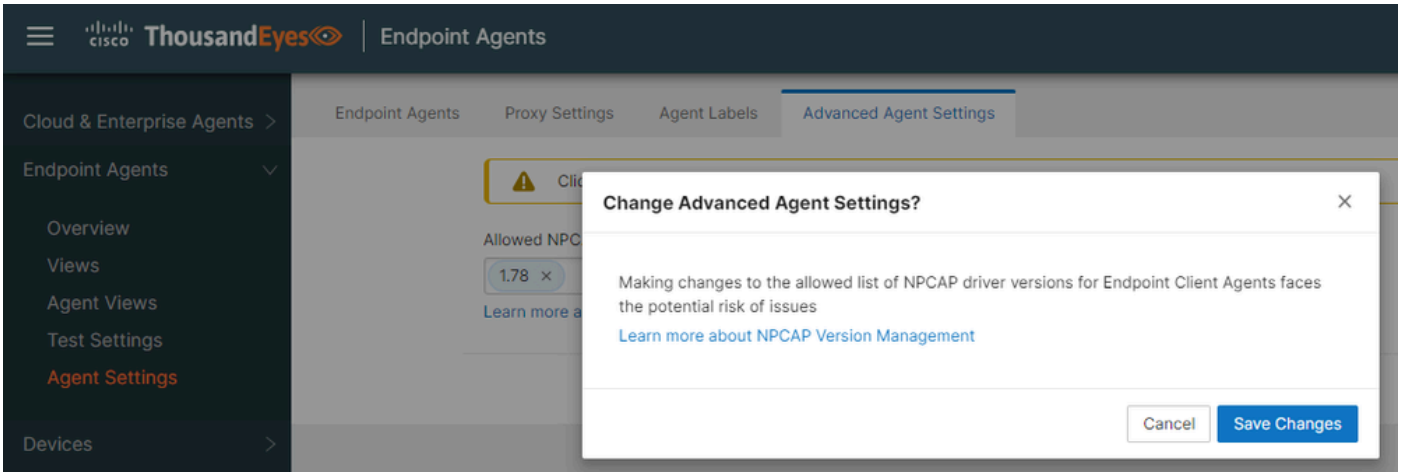
Pour poursuivre la configuration, vérifiez les étapes suivantes :

1. Cliquez sur **Endpoint Agents**
2. Agent Settings
3. Advanced Agent Settings
4. Choisissez les versions que vous avez trouvées sous les outils de développeurs à l'étape précédente
5. Cliquer **Save**



Vous disposez ensuite d'une fenêtre contextuelle vous demandant d'appliquer les modifications.

- Cliquer **Save**



Remarque : Le lien redirige vers la documentation suivante - [Thousand Eyes - Endpoint Agent - Advanced Settings]

Au bout d'un certain temps, les mesures manquantes indiquent la valeur correcte.

User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Sergiy	Frankfurt am Main, Germany	Healthy	DESKTOP-JLL4OS0	1 ms	1 ms	0.00%	—	25000 Mbps	3.67%	79.31%	Microsoft Windows 10 Pro	Jun 22, 2024 5:25PM

Informations connexes

[À propos de Experience Insights]

[Afficher le résumé des terminaux]

[Paramètres avancés de l'agent]

[Gestion des mises à niveau du pilote NPCAP]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.