

# Risoluzione dei problemi relativi alle metriche mancanti per l'accesso sicuro in Experience Insights nella sezione Prestazioni degli endpoint

## Sommario

---

[Introduzione](#)

[Problema](#)

[Soluzione](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come correggere le metriche mancanti in Experience Insights nella sezione Prestazioni degli endpoint.

## Problema

Per verificare se il problema si ripresenta, procedere come segue:

- Fare clic su **Experience Insights > Management**

È necessario specificare le metriche **Experience Insights** nella sezione **Endpoints Performance**.

- Se lo stato del dispositivo è Non in linea
- Quindi, sono previste le metriche che mostrano i trattini
- Fare clic sul nome utente per visualizzare i dettagli del PC monitorato nel dashboard Secure Access

# Experience Insights

Configure

Powered by **ThousandEyes**

Experience Insights brings together employee digital experience data so you can understand their journey to Secure Access and corporate resources. Get a comprehensive view into their device and network behaviour to identify and resolve issues faster and make informed decisions on how to improve those interactions. [Help](#)

Last updated Jun 22, 2024, 15:51

## Endpoints Overview

Number of endpoints 1 total

0

Online

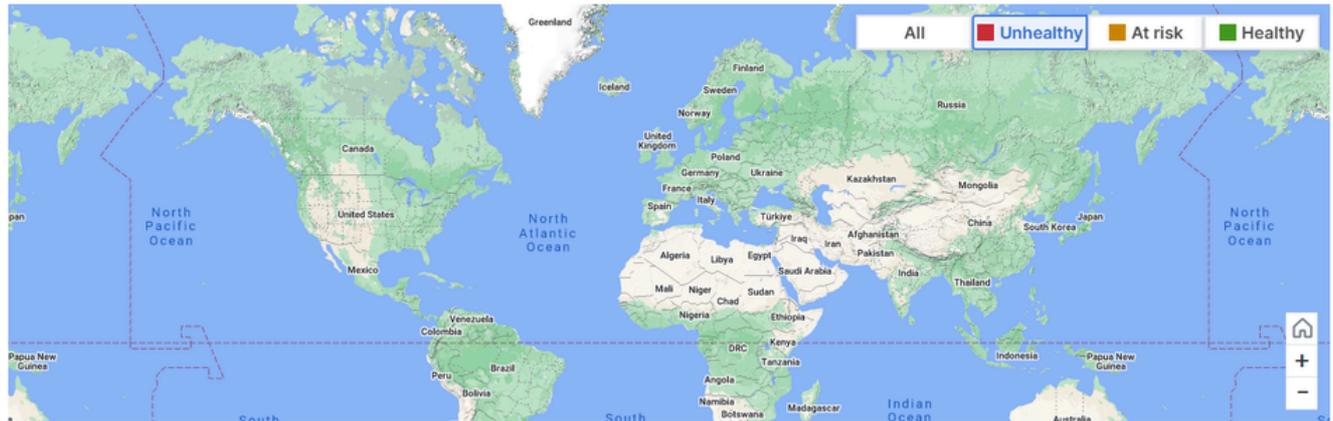
Health status

Unhealthy

At Risk

Healthy

## Endpoints Performance



Search by user name

Select health status

User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Sergiy 3	Frankfurt am Main, Germany	Offline 1	DESKTOP-JLL4OS0	—	—	—	—	—	—	—	Microsoft Windows 10 Pro	—

È possibile verificare la data dell'ultima connessione e non sono disponibili dati sulle prestazioni, come previsto perché il dispositivo è **Offline**.

# Sergiy

Explore device performance metrics, connection quality to application cloud and collaboration tools. Monitor real-time CPU, memory, Wi-Fi strength, and view summarized security and application events for user safety. [Help](#)

Last updated Jun 22, 2024, 15:53

← Experience Insights

## Summary

### User Details

Email —  
Identity Provider —  
Hostname DESKTOP-JLL4OS0  
Groups —  
Devices ✔ 1 connected ✖ 0 disconnected

### Device Details

Operating System t3.micro Microsoft Windows 10 Pro  
Client-based Zero Trust Access ✖ Unenrolled  
Public IP address 3.71.48.151 1  
Last Connected Jun 21, 2024 15:45:30  
Last Location Frankfurt am Main, Germany

### Performance <sup>ⓘ</sup>

No data available 2

### Collaboration Application Summary <sup>ⓘ</sup>

No data available for the last 12 hours

Accendere il PC monitorato con l'agente Thousand Eyes installato. Poi, torna a Experience Insights > Management.

- Quindi, viene visualizzato il numero aggiornato di endpoint online
- Lo stato di integrità indica che un endpoint è **At Risk**
- Nella tabella sono presenti trattini
- Tuttavia, questi trattini sono previsti se non è stata configurata la versione di NPCAP consentita

## Experience Insights

Powered by **ThousandEyes**

Configure

Experience Insights brings together employee digital experience data so you can understand their journey to Secure Access and corporate resources. Get a comprehensive view into their device and network behaviour to identify and resolve issues faster and make informed decisions on how to improve those interactions. [Help](#)

Last updated Jun 22, 2024, 15:59

### Endpoints Overview

Number of endpoints 1 total

1

Online

1

Health status

0

Unhealthy

1

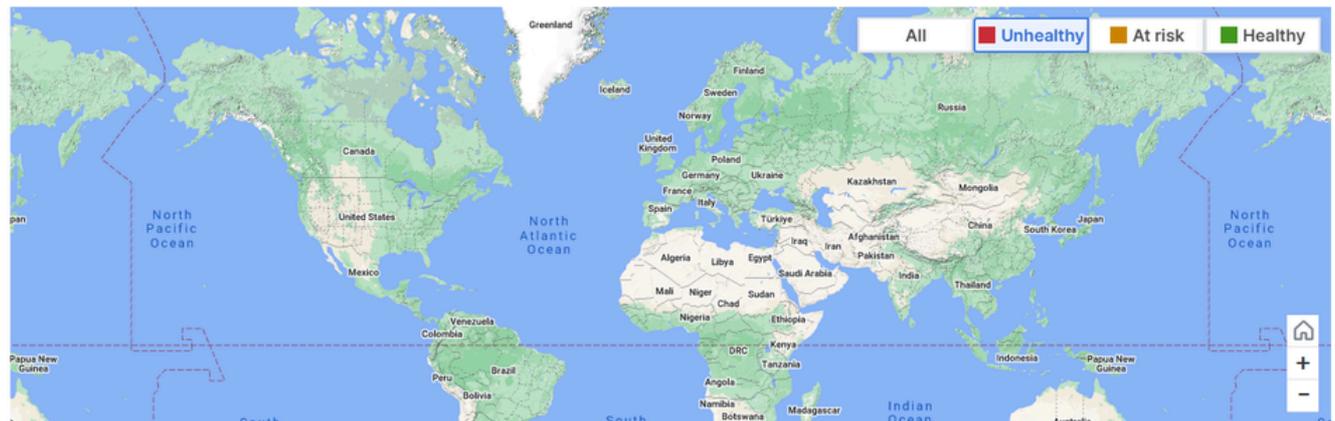
At Risk

0

Healthy

2

### Endpoints Performance



Search by user name

Select location

Select health status

User name	Location	Health status	Device name	Latency	Jitter	Loss	WiFi	Ethernet	CPU	Memory	OS	Test time
Sergiy	Frankfurt am Main, Germany	Unhealthy	DESKTOP-JLL40S0	—	—	—	—	—	—	—	Microsoft Windows 10 Pro	—

## Soluzione

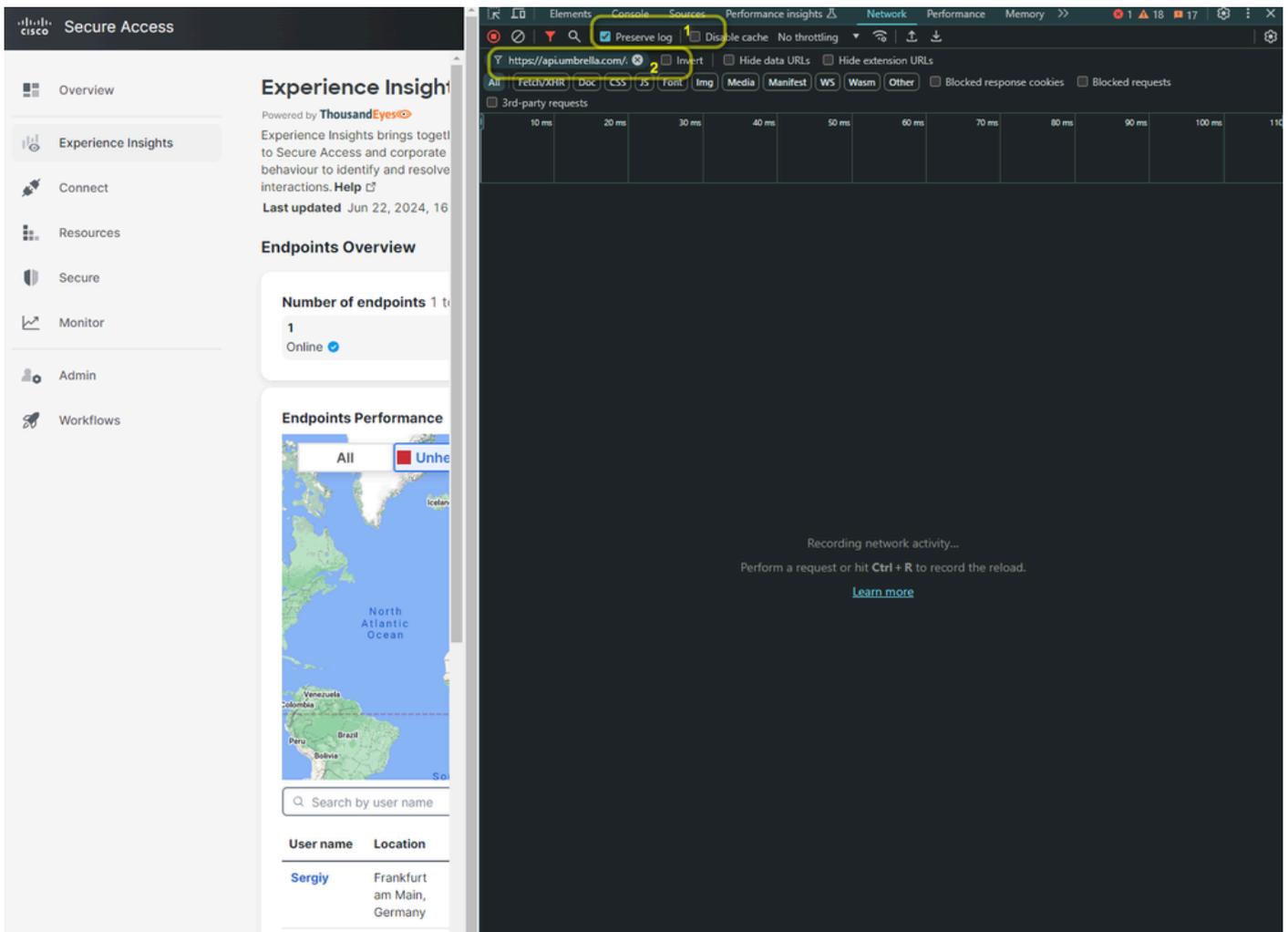
Per risolvere il problema, verificare i passaggi successivi:

Nel browser (in questo esempio, è necessario utilizzare Chrome)

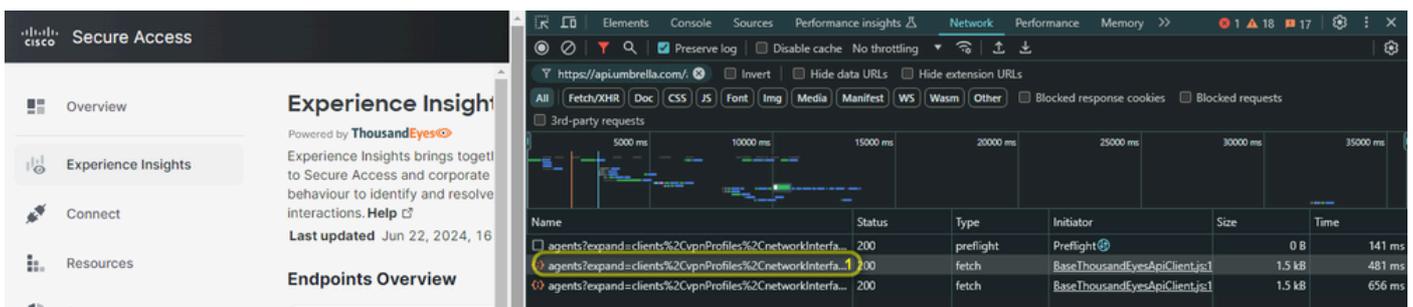
- Fare clic Settings > More Tools > Developer Tools
- Fare clic sulla casella di controllo **Preserve log**

Nell'opzione di filtro, inserire la stringa successiva:

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



Aggiornare quindi la pagina per visualizzare le richieste in **Developer Tools**.



- Fare clic su **Response**
- La risposta contiene il formato JSON strutturato con sezioni per ogni PC monitorato. È possibile scorrere verso il basso fino alla fine della sezione per un PC specifico e annotare la versione npcap. In questo esempio, si dispone di un PC di prova con versione npcap 1.78
- Se la tabella contiene altre informazioni, controllare **User name** la versione npcap di ciascun PC monitorato

**Secure Access**

- Overview
- Experience Insights
  - Powered by **ThousandEyes**
  - Experience Insights brings together Secure Access and corporate behaviour to identify and resolve interactions. [Help](#)
  - Last updated Jun 22, 2024, 16
- Endpoints Overview
  - Number of endpoints 1 total
  - 1 Online
- Endpoints Performance
  - All Unhealthy
  - Map showing North Pacific Ocean and Caspian Sea
  - Search by user name

User name	Location
Sergiy 3	Frankfurt am Main, Germany

Network tab of a browser developer tool showing a response from `https://api.umbrella.com/v7/endpoint/agents/037f0aa3-656e-4235`.

The response body is a JSON object with the following structure:

```

{
  "asNumber": 16509,
  "asName": "AMAZON-02",
  "licenseType": "advantage",
  "npcapVersion": "1.78",
  "totalAgents": 1,
  "_links": {
    "self": {
      "href": "https://api.umbrella.com/v7/endpoint/agents/037f0aa3-656e-4235"
    }
  }
}

```

Annotations in the image highlight:

- The `asName` field: "AMAZON-02"
- The `licenseType` field: "advantage"
- The `npcapVersion` field: "1.78"
- The `totalAgents` field: 1
- The `self` link href: "https://api.umbrella.com/v7/endpoint/agents/037f0aa3-656e-4235"



**Nota:** la tabella mostra un limite di 10 dispositivi monitorati. Se si dispone di più di 10 dispositivi, è necessario eseguire la stessa operazione in ogni pagina.

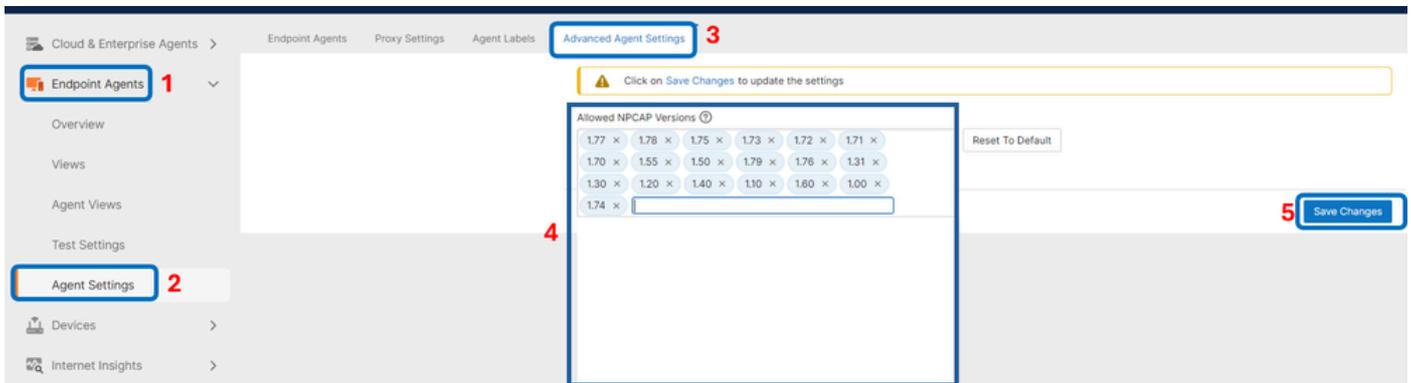
---

Dopo aver raccolto tutte le versioni npcap dell'agente, è necessario accedere a TE per aggiungere le versioni supportate.

Per continuare con la configurazione, verificare i passaggi successivi:

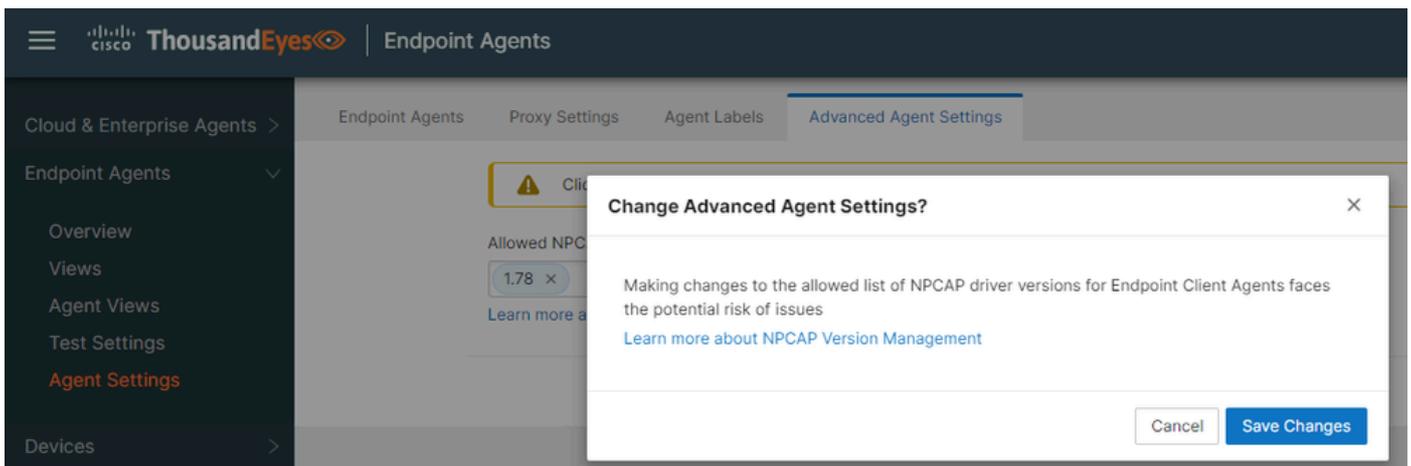
- Fare clic su **Endpoint Agents**
- Agent Settings
- Advanced Agent Settings

- Scegliere le versioni trovate negli strumenti per sviluppatori nel passaggio precedente
- Fare clic su **Save**



In seguito si dispone di una finestra popup in cui viene richiesto di applicare le modifiche.

- Fare clic su **Save**



---

**Nota:** il link rimanda alla documentazione successiva: [Thousand Eyes - Endpoint Agent - Advanced Settings](#)

---

Dopo qualche tempo, le metriche mancanti mostrano il valore corretto.

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	

Informazioni correlate

[Informazioni su Experience Insights](#)

[Visualizza riepilogo endpoint](#)

[Impostazioni avanzate agente](#)

[Gestione aggiornamento driver NPCAP](#)

## 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).