

# Troubleshoot Secure Access Missing Metrics in Experience Insights under the Section Endpoints Performance

## Contents

---

[Introduction](#)

[Problem](#)

[Solution](#)

[Related Information](#)

---

## Introduction

This document describes how to fix missing metrics in Experience Insights under the section Endpoints Performance.

## Problem

To verify if you face the issue, please verify the next steps:

- Click **Experience Insights > Management**

There needs to be metrics in **Experience Insights** under the section **Endpoints Performance**.

1. If the device has the status **Offline**
2. Then, the metrics showing the dashes are expected
3. Click on the Username to see the details of the monitored PC in the Secure Acces dashboard

# 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

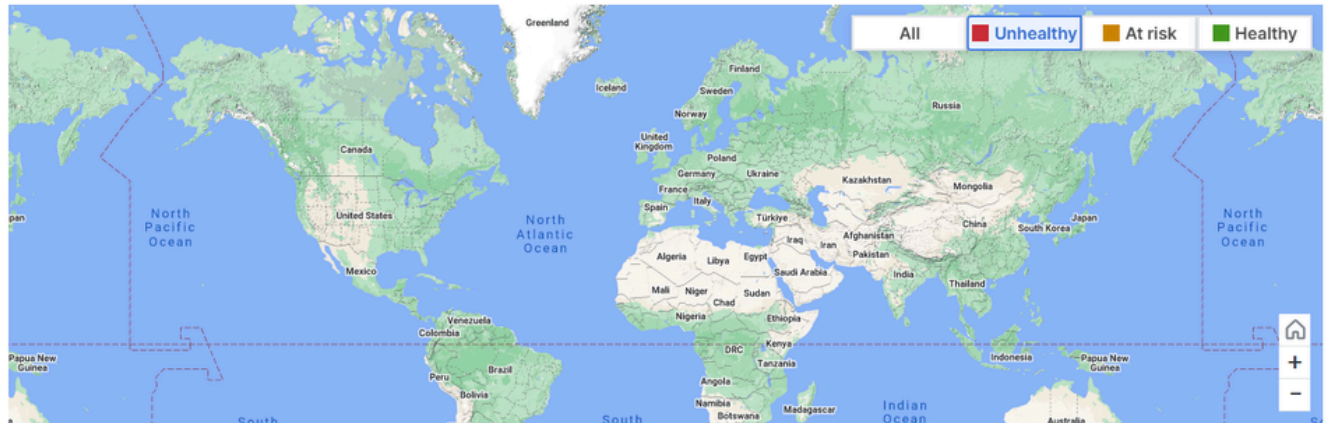
### Health status

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	—

You can see when it was last connected, and no Performance data is available, which is expected because the device is **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

Turn on the monitored PC with the Thousand Eyes agent installed. Then, go back to Experience Insights > Management.

1. Then, you see the updated number of endpoints online
2. Health status shows one endpoint is **At Risk**
3. In the table you can see dashes
4. However, these dashes are expected if you did not configure the NPCAP version permitted

# 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, 15:59

## Endpoints Overview

Number of endpoints 1 total

1

Online

Health status

2

0

Unhealthy

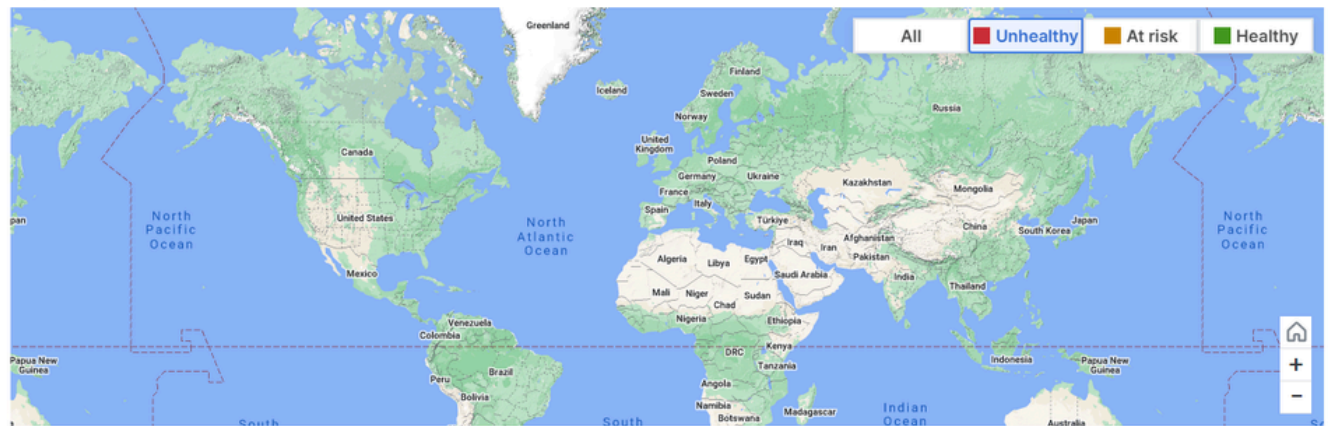
1

At Risk

0

Healthy

## 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-JLL4OS0	—	—	—	—	—	—	—	Microsoft Windows 10 Pro	—

## Solution

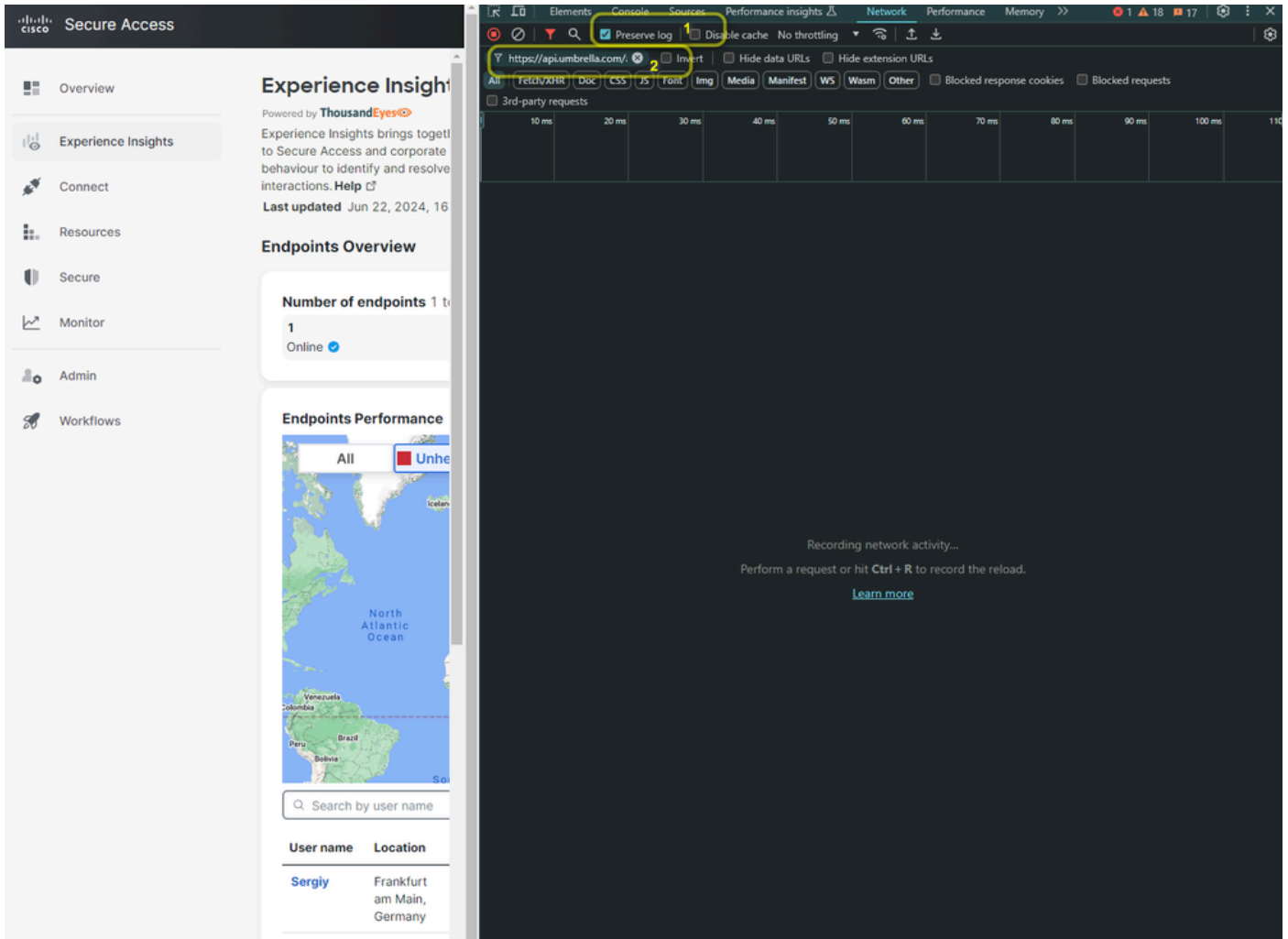
To solve the issue, verify the next steps:

In the browser (in this example, you need to use Chrome)

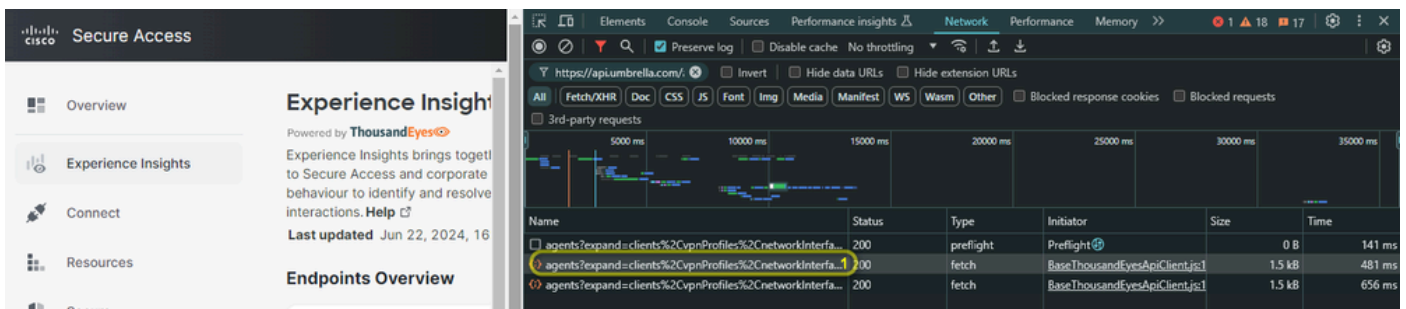
- Click Settings > More Tools > Developer Tools
- Click the checkbox **Preserve log**

In the filter option, put the next string:

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



Then, refresh the page to see the requests in **Developer Tools**.



1. Click **Response**
2. The Response contains the structured JSON format with sections for each monitored PC. You can scroll down to the end of the section for specific PC and note down the npcapVersion, In this example, I have a test PC with npcap version 1.78
3. If you have more **User name** in the table, check the npcap version for each monitored PC

**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, 16:00
- Connect
- Resources
- Secure
- Monitor
- Admin
- Workflows

### Endpoints Overview

Number of endpoints 1 total

1 Online

### Endpoints Performance

All Unhealthy

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`.

Response body (JSON):

```

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

```

Annotations in the image highlight the `asName` field and the `self` object in the response body.



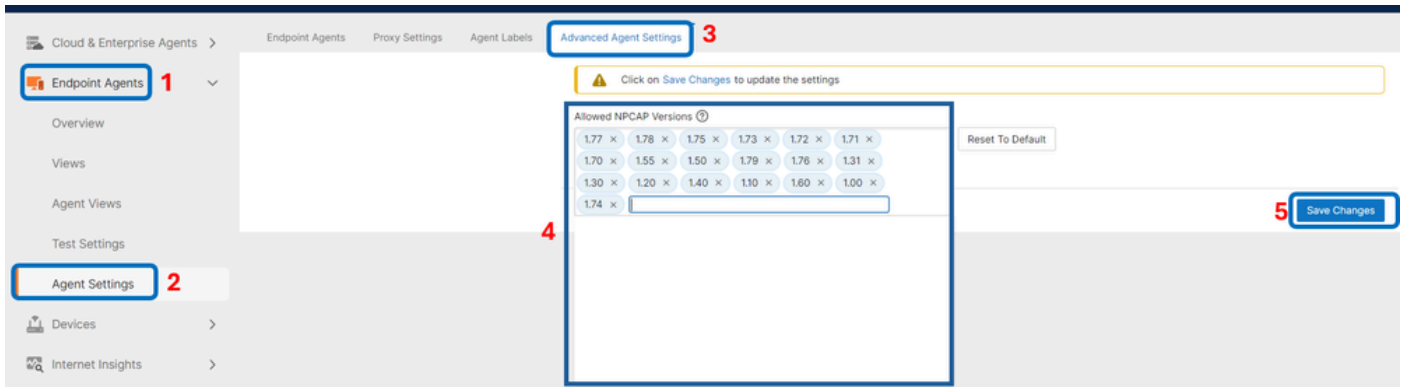
**Note:** The table shows a limit of 10 monitored devices. If you have more than 10 devices, you must do the same on each page.

---

After you have collected all the agent npcap versions, you need to access TE to add the supported versions.

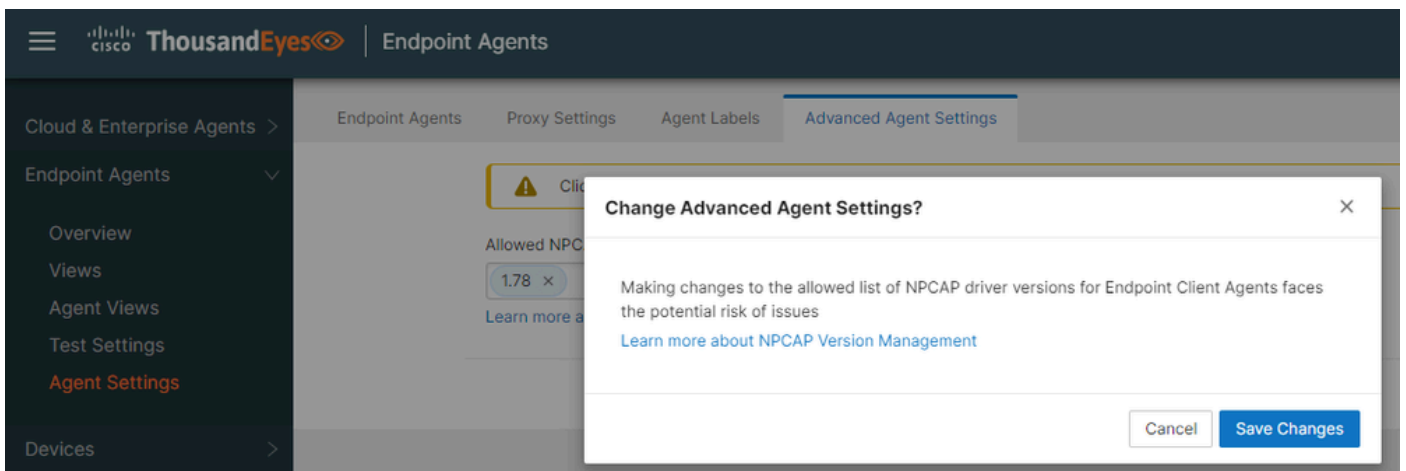
To proceed with the configuration, verify the next steps:

1. Click on **Endpoint Agents**
2. Agent Settings
3. Advanced Agent Settings
4. Choose the versions you found under the developers tools in the previous step
5. Click **Save**



Then you have a pop-up windows that ask you to apply the changes.

- Click **Save**







---

**Note:** The link redirects to the next documentation - [Thousand Eyes - Endpoint Agent - Advanced Settings](#)

---

After some time, the missing metrics show the correct value.

User name	Location	Health status <sup>ⓘ</sup>	Device name	Latency <sup>ⓘ</sup>	Jitter <sup>ⓘ</sup>	Loss <sup>ⓘ</sup>	WiFi <sup>ⓘ</sup>	Ethernet <sup>ⓘ</sup>	CPU	Memory	OS	Test time <sup>ⓘ</sup> 
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

## Related Information

[About Experience Insights](#)

[View Summary of Endpoints](#)

[Advanced Agent Settings](#)

[NPCAP Driver Upgrade Management](#)