# Procédure de traitement des anomalies

Opérations mondiales de l'infrastructure et des systèmes • Services aux utilisateurs finaux et à l'infrastructure • **Services à la clientèle**

Version 1.1 • 10.01.2025

faurecia
inspiring mobility

faurecia

# Contenu

**Introduction** ..... **2**

**Conditions préalables** ..... **2**

**Matériel pris en charge** ..... **3**

**Mise à niveau sur place vers Windows 11 SAC 23H2** ..... **4**

**Dépannage** ..... **7**

**Foire aux questions** ..... **9**

# Introduction

Ce document explique comment détecter les anomalies d'authentification et comment les traiter

# Installation de la console Forescout

## 1. Comment demander des autorisations d'accès

Les autorisations sont accordées en fonction de l'appartenance aux groupes de sécurité CC-SSS-Network. Tout membre d'un groupe de sécurité CC-SSS-Network disposera d'un accès en lecture seule au segment de site/usine correspondant et de certaines fonctionnalités d'écriture limitées.

## 2. Comment installer la console Forescout

### 2.1 Télécharger le package d'installation

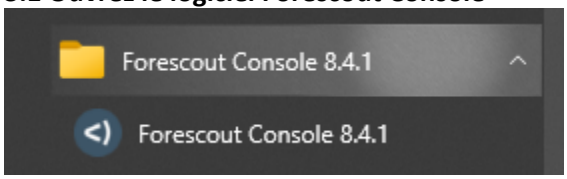
Le logiciel n'est disponible que pour le système d'exploitation Windows
URL de téléchargement : https://wwgrpnac0001.dc.ege.ds/install

### 2.2 Exécuter le paquet d'installation

Le logiciel est installé au niveau de l'utilisateur (uniquement sur le compte d'utilisateur qui exécute le package d'installation). Vous devez l'installer en tant qu'utilisateur régulier, ne l'élevez pas en tant qu'administrateur.
Si vous installez le logiciel sur un ordinateur partagé, le package d'installation doit être exécuté individuellement sur chaque compte utilisateur.

## 3. Comment se connecter à la console Forescout

### 3.1 Ouvrez le logiciel Forescout Console




Version 8.4.1 dans cet exemple

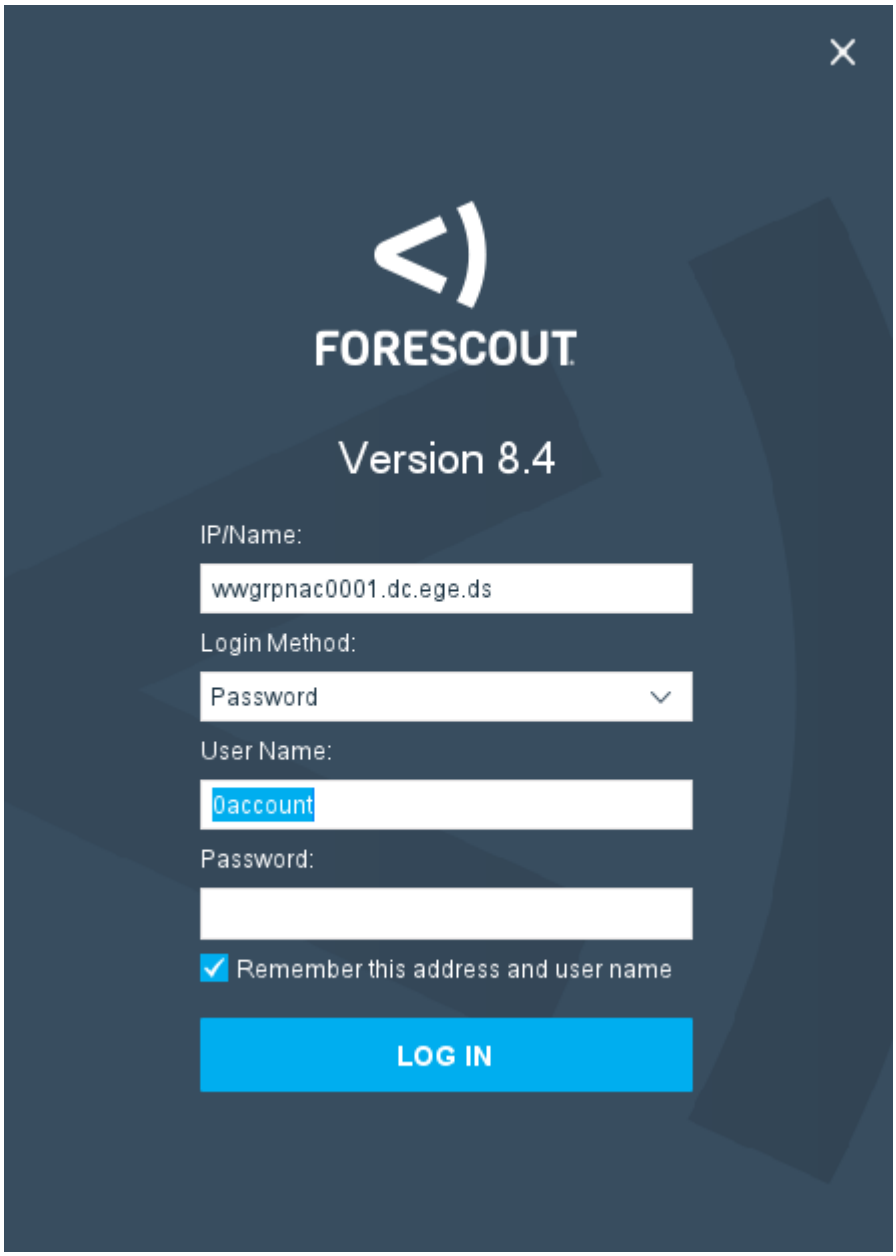
### 3.2 Informations de connexion

IP/Name: wwgrpnac0001.dc.ege.ds

Login Method: Password

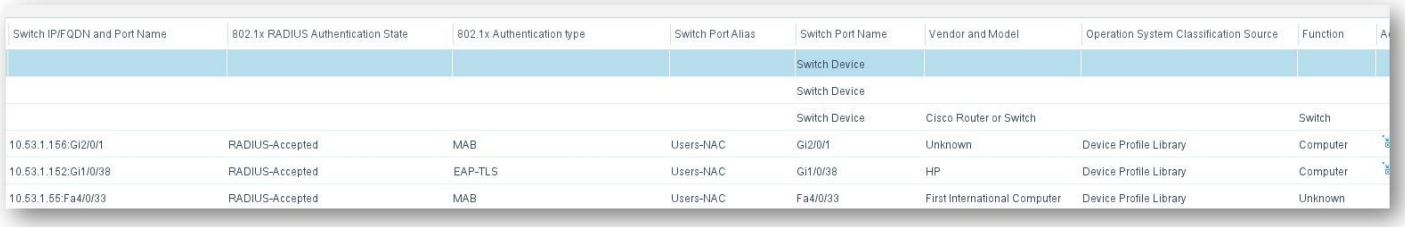
User Name: Your 0account

Password: Your 0account password



# Anomalie sur la console Forescout

Après l'installation on ajoute les colonnes suivantes :



| Switch IP/FQDN and Port Name | 802.1x RADIUS Authentication State | 802.1x Authentication type | Switch Port Alias | Switch Port Name | Vendor and Model | Operation System Classification Source | Function | A |
|---|---|---|---|---|---|---|---|---|
| | | | | Switch Device | | | | |
| | | | | Switch Device | | | | |
| | | | | Switch Device | Cisco Router or Switch | | Switch | |
| 10.53.1.156:Gi2/0/1 | RADIUS-Accepted | MAB | Users-NAC | Gi2/0/1 | Unknown | Device Profile Library | Computer | |
| 10.53.1.152:Gi1/0/38 | RADIUS-Accepted | EAP-TLS | Users-NAC | Gi1/0/38 | HP | Device Profile Library | Computer | |
| 10.53.1.55:Fa4/0/33 | RADIUS-Accepted | MAB | Users-NAC | Fa4/0/33 | First International Computer | Device Profile Library | Unknown | |

Pour ajouter des colonnes, il faut faire « clique droit » sur l'en-tête de l'une d'elles. Dans la fenêtre qui s'affiche vous pouvez rechercher directement le nom de l'en-tête rechercher.

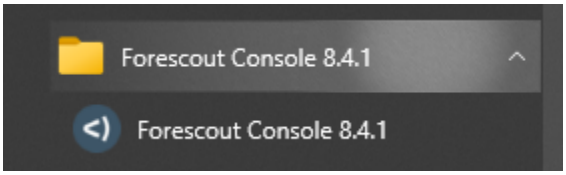


Les pilotes de ces périphériques ont été intégrés dans les sources d'installation.

**Remarque :** La mise à niveau ne fonctionnera pas pour les modèles avec processeur de 7e génération ou inférieur.

# Traitement des ports en MAB2

1. **Ouvrez le logiciel Forescout Console**




2. Dans la console identifier les ports en MAB prenez le nom du switch

| Switch IP/FQDN and Port Name | 802.1x RADIUS Authentication State | 802.1x Authentication type | Switch Port Alias | Switch Port Name | Vendor and Model | Operation System Classification Source | Function |
|---|---|---|---|---|---|---|---|
| | | | | Switch Device | | | |
| | | | | Switch Device | | | |
| | | | | Switch Device | Cisco Router or Switch | | Switch |
| 10.53.1.156:Gi2/0/1 | RADIUS-Accepted | MAB | Users-NAC | Gi2/0/1 | Unknown | Device Profile Library | Computer |
| 10.53.1.152:Gi1/0/38 | RADIUS-Accepted | EAP-TLS | Users-NAC | Gi1/0/38 | HP | Device Profile Library | Computer |
| 10.53.1.55:Fa4/0/33 | RADIUS-Accepted | MAB | Users-NAC | Fa4/0/33 | First International Computer | Device Profile Library | Unknown |

3. La première chose à faire est de mettre ses infos en parallèle avec le DHCP avec une recherche Excel on trouve le nom des appareils en l'occurrence la majorité des anomalies était due à des evoko

| | |
|---|---|
| FRMERWLT3327.ls.ege.ds | #N/A |
| evoko-liso-LF1933011515.ls.ege.ds | ok_a revoir |
| =RECHERCHEV(MAB[@[IPv4 Address]];DHCP!A:B;2;FAUX) | |
| evoko-liso-LF1933011870.ls.ege.ds | ok_a revoir |
| evoko-liso-LF1933011568.ls.ege.ds | ok_a revoir |
| evoko-liso-LF1933011392.ls.ege.ds | ok_a revoir |
| evoko-liso-LF1933011388.ls.ege.ds | ok_a revoir |
| evoko-liso-LF1933011629.ls.ege.ds | ok_a revoir |
| nd-dc1153502689.ls.ege.ds | ok_a revoir |

4. Basculez les ports en question sur le Template « **SANS-NAC** » avec Julie ou autre en fonction du besoin