

# Ajout/modification d'une entrée de périphérique d'accès réseau dans ISE par Catalyst Center

## Table des matières

---

[Introduction](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

---

## Introduction

Ce document décrit la procédure de reconfiguration de l'entrée Network Access Device (NAD) dans ISE qui est soit modifiée soit supprimée d'ISE.

## Informations générales

Il peut y avoir plusieurs scénarios dans lesquels l'entrée NAD d'un périphérique réseau (qui est géré par Catalyst Center) doit être modifiée. Exemple : un périphérique est renvoyé, le numéro de série a changé et un nouveau numéro de série doit être mis à jour dans l'entrée NAD de ce périphérique réseau (Advanced TrustSec Settings).

Dans le cas contraire, l'authentification TrustSec du périphérique n'aurait pas lieu, ce qui aurait empêché le téléchargement des données PAC/env.

Il peut y avoir un autre scénario où l'entrée NAD est supprimée d'Identity Services Engine (ISE) (en raison d'une erreur manuelle ou d'une autre cause). et maintenant, toute l'authentification du périphérique échoue car il n'y a pas d'entrée NAD dans ISE.

## Problème

Le problème dans les scénarios mentionnés ci-dessus est qu'il n'y a pas d'option prédéfinie dans Catalyst Center pour créer l'entrée NAD directement une fois que le périphérique réseau est affecté au site et que l'entrée NAD est créée pour la première fois, ce qui oblige les utilisateurs à configurer/modifier manuellement l'entrée NAD dans ISE, ce qui peut prendre du temps et entraîner des erreurs.

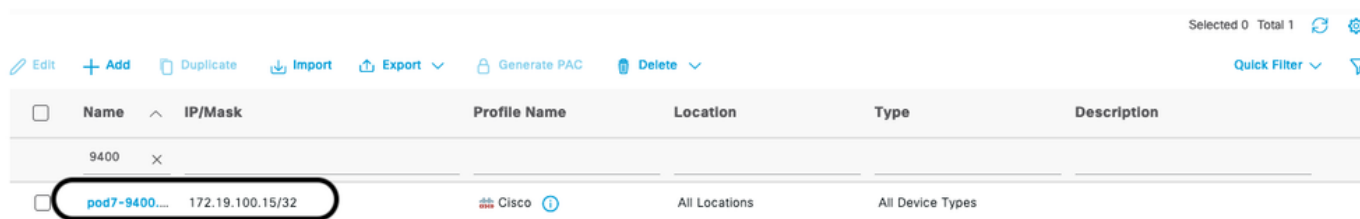
Ce document décrit la procédure/les étapes pour reconfigurer l'entrée NAD (Network Access Device) pour tout périphérique réseau dans ISE qui est soit modifié soit supprimé d'ISE NAD. Cette procédure s'applique à tout périphérique réseau géré par Catalyst Center.

# Solution

Pour que Catalyst Center configure l'entrée NAD dans ISE, nous devons changer l'adresse IP de gestion du périphérique (en n'importe quelle adresse IP factice) qui est le moteur qui déclenche le workflow de création d'entrée NAD.

Cette procédure s'applique à tout périphérique réseau géré par Catalyst Center. L'entrée NAD sera créée avec l'adresse IP d'origine (car le workflow se déclenche avant la modification de l'adresse IP de gestion). Dans cet exemple, les paramètres TrustSec avancés d'une entrée NAD sont désactivés dans ISE :

## Network Devices



Selected 0 Total 1

Edit + Add Duplicate Import Export Generate PAC Delete Quick Filter

Name	IP/Mask	Profile Name	Location	Type	Description
9400	x				
pod7-9400...	172.19.100.15/32	Cisco	All Locations	All Device Types	

Entrée NAD ISE pour un périphérique réseau

Network Devices   Network Device Groups   Network Device Profiles   External RADIUS Servers   RADIUS Servers

Network Devices

Default Device

Device Security Settings

TACACS Authentication Settings

**SNMP Settings**

SNMP Version 2c ▼

SNMP RO Community \*\* [Show](#)

SNMP Username

Security Level  ▼

Auth Protocol  ▼

Auth Password  [Show](#)

Privacy Protocol  ▼

Privacy Password  [Show](#)

Polling Interval 0 seconds(Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

Originating Policy Services Node Auto ▼

**Advanced TrustSec Settings**

Les paramètres TrustSec avancés sont désactivés pour cette entrée NAD

Comme le montre cette image, les paramètres avancés TrustSec de l'entrée NAD du périphérique sont désactivés (généralement, lorsque Catalyst Center crée l'entrée NAD, cette section est activée). Dans Catalyst Center, modifiez l'adresse IP de gestion en IP factice qui déclenche le workflow pour reconfigurer l'entrée NAD dans ISE. Lorsque vous modifiez l'adresse IP de gestion, elle fait passer l'état de gestion du périphérique à Synchronisation et l'entrée NAD ISE doit être modifiée.

Devices (1) Focus: Inventory

deviceName: (\*9400\*)

1 Selected

Device Name	IP Address
pod7-9400.dr.com	172.19.100.15

### Edit Device

Credentials | **Management IP** | Resync Interval | Device Role

Device IP / DNS Name\*  
172.19.100.100

- Please ensure that the new IP address is reachable from Cisco DNA Center and device credentials are correct, otherwise the device may go to an unmanaged state.
- Please ensure that the device is re-provisioned if the management interface has changed and IP address of the same has been updated. Failure to do so will cause reachability issues from the device to the network servers.

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. [Learn More](#)

Cancel **Update**

Remplacement de l'adresse IP de gestion du périphérique réseau dans Catalyst Center par une adresse IP fictive

Devices (1) Focus: Inventory

deviceName: (\*9400\*)

0 Selected

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability
pod7-9400.dr.com	172.19.100.100	Switches and Hubs (WLC Capable)	Reachable	Not Scanned	<b>Managed Syncing...</b>

Le périphérique réseau passe en état de synchronisation

Devices (1) Focus: Inventory

deviceName: (\*9400\*)

0 Selected

As of: Jul 7, 2024 7:13 PM

Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance	Health Score	Site
pod7-9400.dr.com	172.19.100.100	Switches and Hubs (WLC Capable)	Unreachable	Not Scanned	Managed Inventory Sync...	Non-Compliant	No Health	...

Le périphérique réseau devient inaccessible et non géré car l'adresse IP de gestion est une adresse IP factice et n'est pas accessible depuis Catalyst Center

L'entrée NAD ISE pour les paramètres TrustSec mis à jour et avancés est maintenant activée :

Network Devices    Network Device Groups    Network Device Profiles    External RADIUS Servers    RA

**Network Devices**

Default Device

Device Security Settings

SNMP Username \_\_\_\_\_

Security Level \_\_\_\_\_ ▾

Auth Protocol \_\_\_\_\_ ▾

Auth Password \_\_\_\_\_ [Show](#)

Privacy Protocol \_\_\_\_\_ ▾

Privacy Password \_\_\_\_\_ [Show](#)

Polling Interval  seconds(Valid Range 600 to 86400 or zero)

Link Trap Query

MAC Trap Query

Originating Policy Services Node  ▾

▾ **Advanced TrustSec Settings**

▾ Device Authentication Settings

Use Device ID for TrustSec Identification

Device Id

Password  [Show](#)

Les paramètres TrustSec avancés ont été activés après la mise à jour de l'adresse IP de gestion depuis Catalyst Center

Une fois cette adresse créée, nous pouvons rétablir l'adresse IP d'origine de la gestion.

Provision / Inventory

🔍 ? 🔄 🔔

---

Devices (1) Focus: Inventory

deviceName: (\*9400\*)

1 Selected Add Device Tag Actions

Device Name	IP Address
pod7-9400.dr.com	172.19.100.15

1 Records

### Edit Device

Credentials
Management IP
Resync Interval
Device Role

Device IP / DNS Name\*

172.19.100.15

- Please ensure that the new IP address is reachable from Cisco DNA Center and device credentials are correct, otherwise the device may go to an unmanaged state.
- Please ensure that the device is re-provisioned if the management interface has changed and IP address of the same has been updated. Failure to do so will cause reachability issues from the device to the network servers.

Device Controllability is **Enabled**. Config changes will be made on network devices during discovery/inventory or when device is associated to a site. [Learn More](#)

Cancel Update

Remplacement de l'adresse IP de gestion par son adresse IP d'origine

Une fois l'adresse IP de gestion mise à jour, le périphérique passe à l'état « Synchronisation » et devient « Géré ».

Voici un autre scénario où l'entrée NAD a été supprimée :

## Network Devices

Selected 0 Total 0 🔄 ⚙️

✎ Edit + Add 📄 Duplicate 📥 Import 📤 Export 🔒 Generate PAC 🗑 Delete Quick Filter ⌵

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	9400	x				

No data available

L'entrée NAD n'existe pas dans ISE pour le périphérique réseau

Comme vous le voyez, l'entrée NAD du même périphérique n'existe pas. Nous utilisons la même procédure, c'est-à-dire que nous modifions l'adresse IP de gestion dans Catalyst Center en IP factice). Après avoir suivi cette procédure, une entrée NAD est créée pour le périphérique réseau avec son adresse IP d'origine.

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.