

Configuration de l'authentification TACACS+ sur le commutateur Arista avec ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration de TACACS+ sur ISE](#)

[Configuration du commutateur Arista](#)

[Étape 1 : activation de l'authentification TACACS+](#)

[Étape 2 : enregistrement de la configuration](#)

[Vérifier](#)

[Évaluation ISE](#)

[Dépannage](#)

[Problème 1](#)

[Causes possibles](#)

[Problème 2](#)

[Causes possibles](#)

[Solution](#)

Introduction

Ce document décrit comment intégrer Cisco ISE TACACS+ avec un commutateur Arista pour un AAA centralisé d'accès administrateur.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE et le protocole TACACS+.
- commutateurs Arista

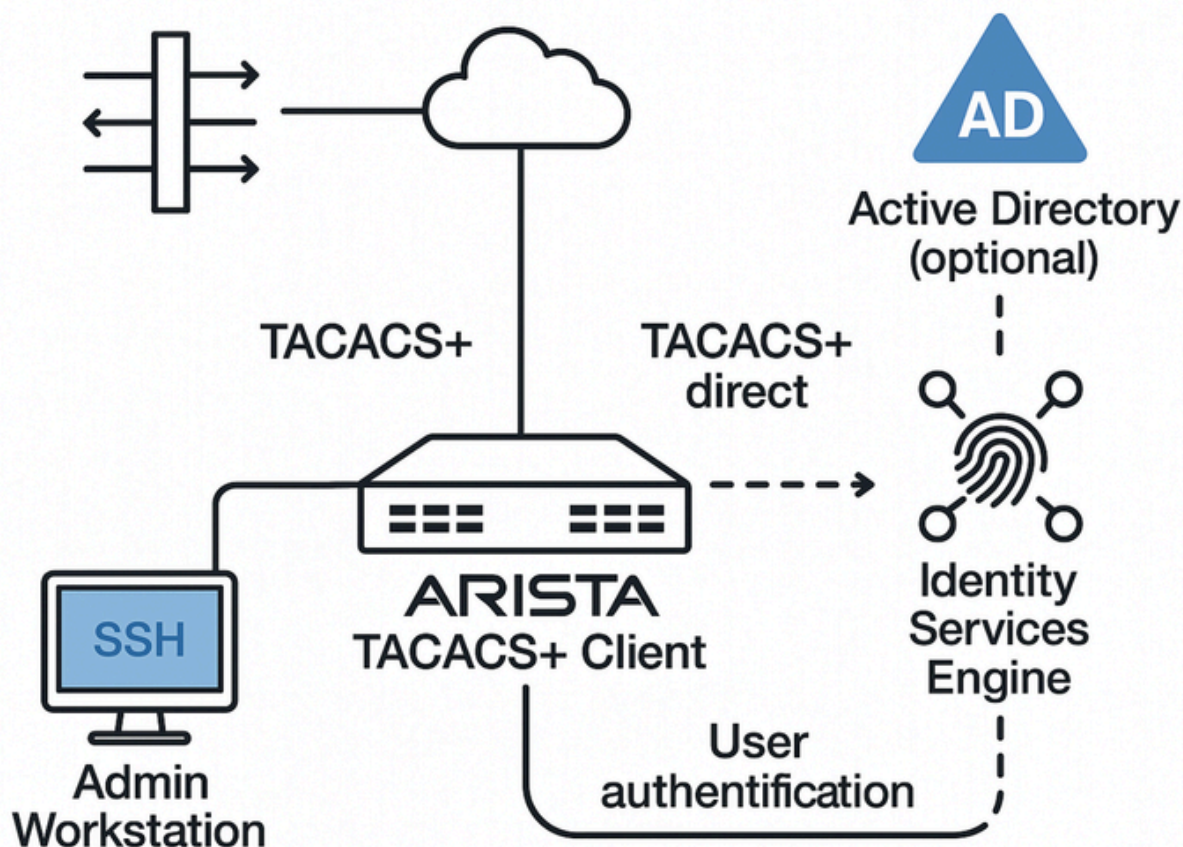
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de l'image logicielle du commutateur Arista : 4,33,2 F
- Cisco Identity Services Engine (ISE) version 3.3 Patch 4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes

Diagramme du réseau

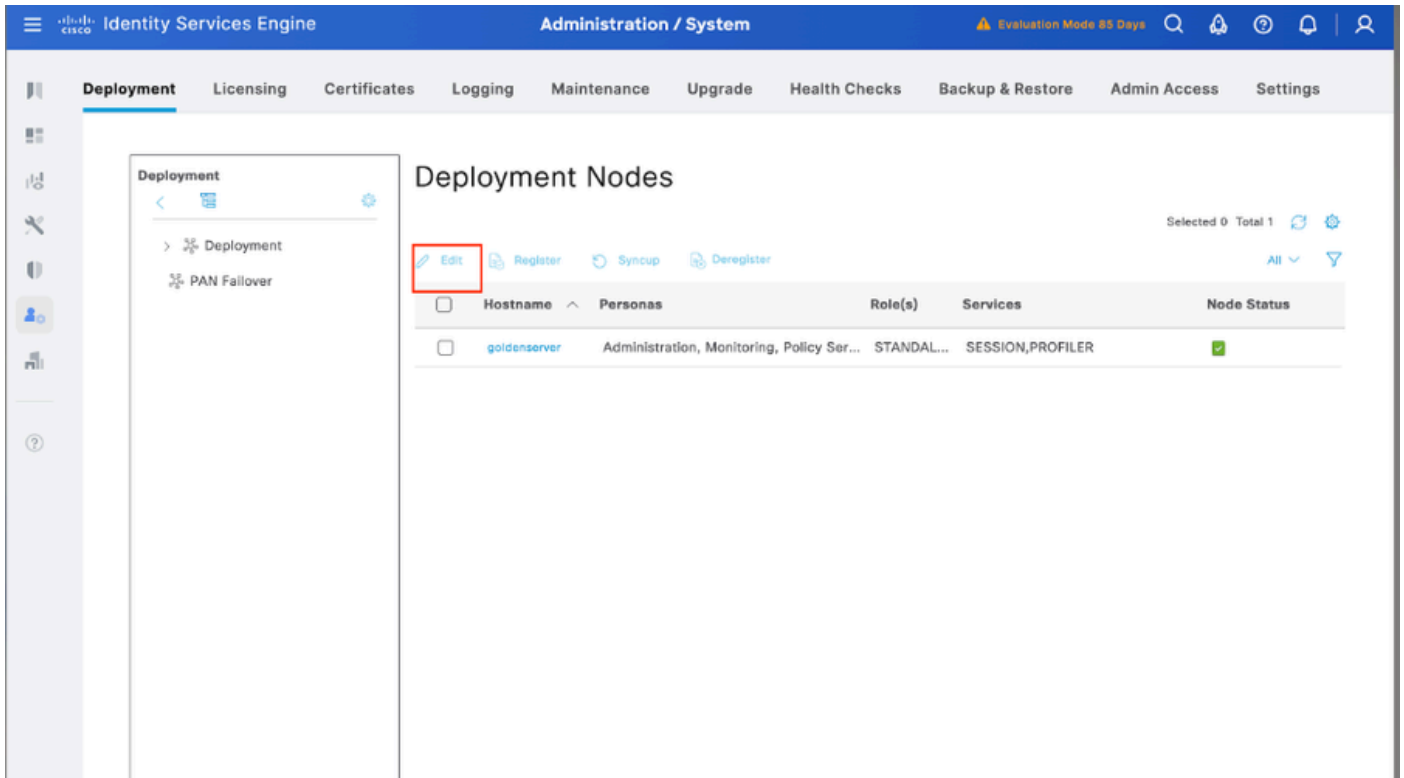


Configurations

Configuration de TACACS+ sur ISE

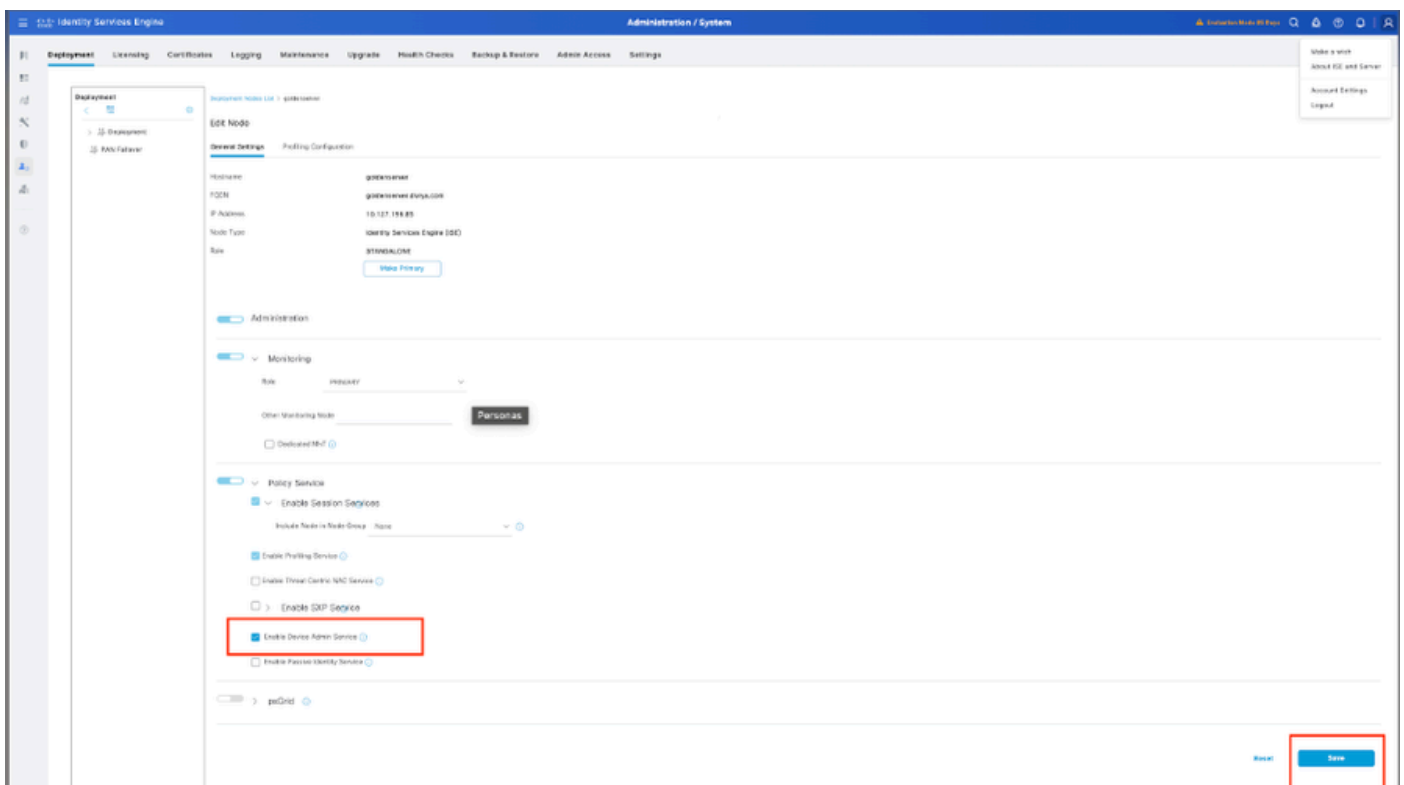
Étape 1. L'étape initiale consiste à vérifier si Cisco ISE dispose des capacités nécessaires pour gérer l'authentification TACACS+. Pour ce faire, vérifiez que la fonctionnalité Device Admin Service est activée sur le noeud Service de stratégie (PSN) souhaité.

Accédez à **Administration > System > Deployment**, sélectionnez le noeud approprié où ISE traite l'authentification TACACS+, et cliquez sur **Edit** pour revoir sa configuration.



Étape 2. Faites défiler la page vers le bas pour localiser la fonction Device Administration Service. Notez que l'activation de cette fonctionnalité nécessite que le personnel Policy Service soit actif sur le noeud, ainsi que les licences TACACS+ disponibles dans le déploiement.

Cochez la case pour activer la fonction, puis enregistrez la configuration.

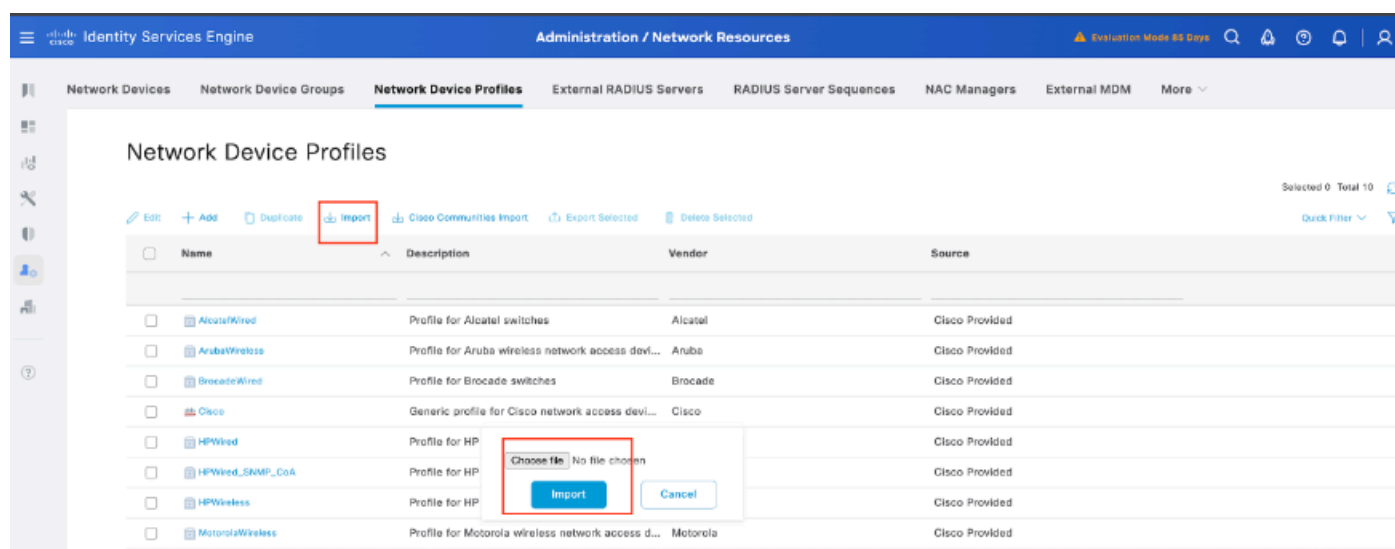


Étape 3. Obtention du profil de périphérique réseau Arista pour Cisco ISE

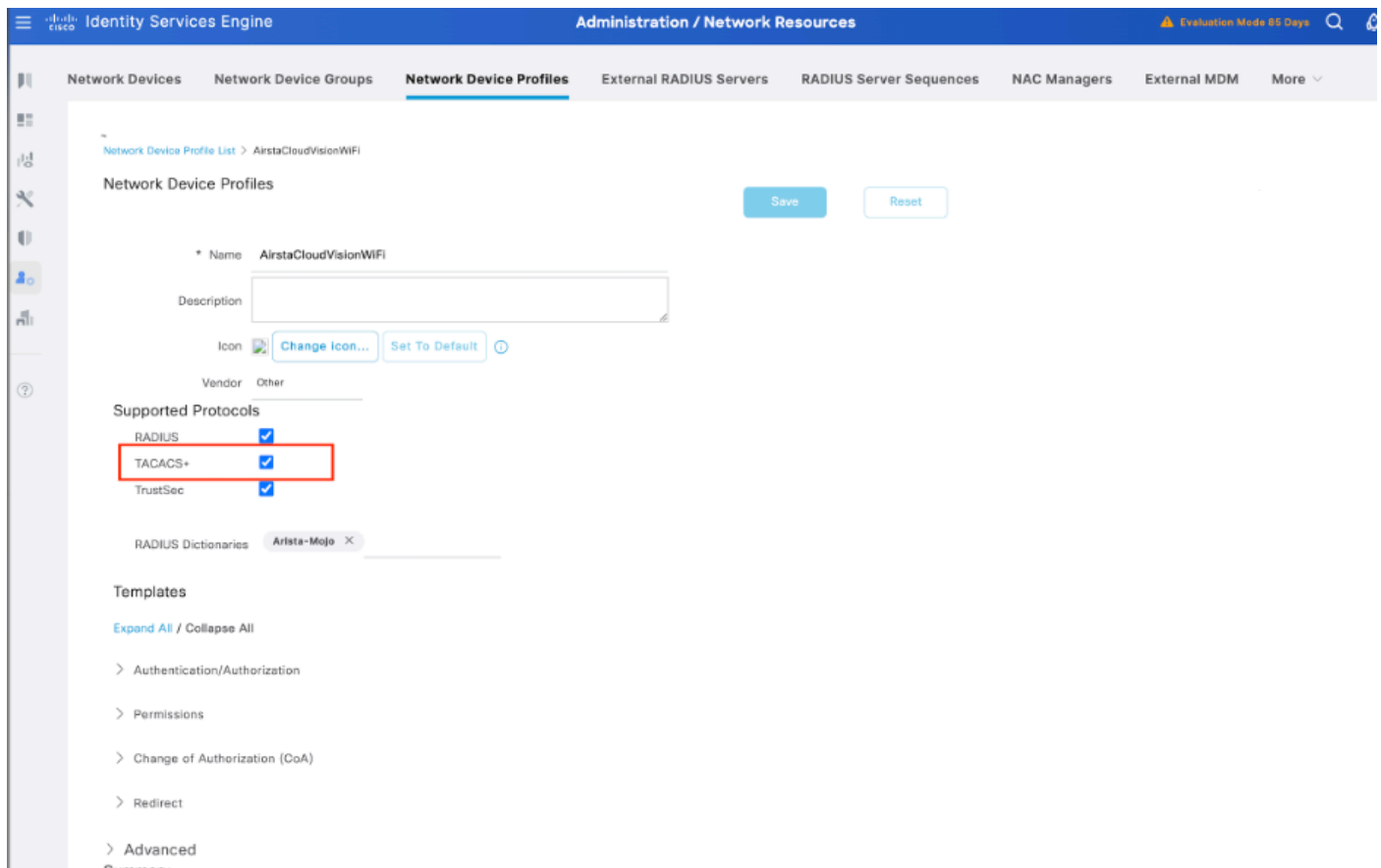
La communauté Cisco a partagé un profil NAD dédié pour les périphériques Arista. Ce profil, ainsi que les fichiers de dictionnaire nécessaires, se trouvent dans l'article [Arista CloudVision WiFi Dictionary and NAD Profile for ISE Integration](#). Le téléchargement et l'importation de ce profil dans votre configuration ISE facilitent l'intégration

Étapes d'importation du profil NAD Arista dans Cisco ISE :

1. Téléchargez le profil :
 - Obtenez le profil NAD Arista à partir du lien Communauté Cisco fourni ci-dessus.
[Communauté Cisco](#)
2. Accédez à Cisco ISE :
 - Connectez-vous à votre console d'administration Cisco ISE
3. Importer le profil NAD :
 - Accédez à Administration > Network Resources > Network Device Profiles.
 - Cliquez sur le bouton Importer
 - Téléchargez le fichier de profil Arista NAD.

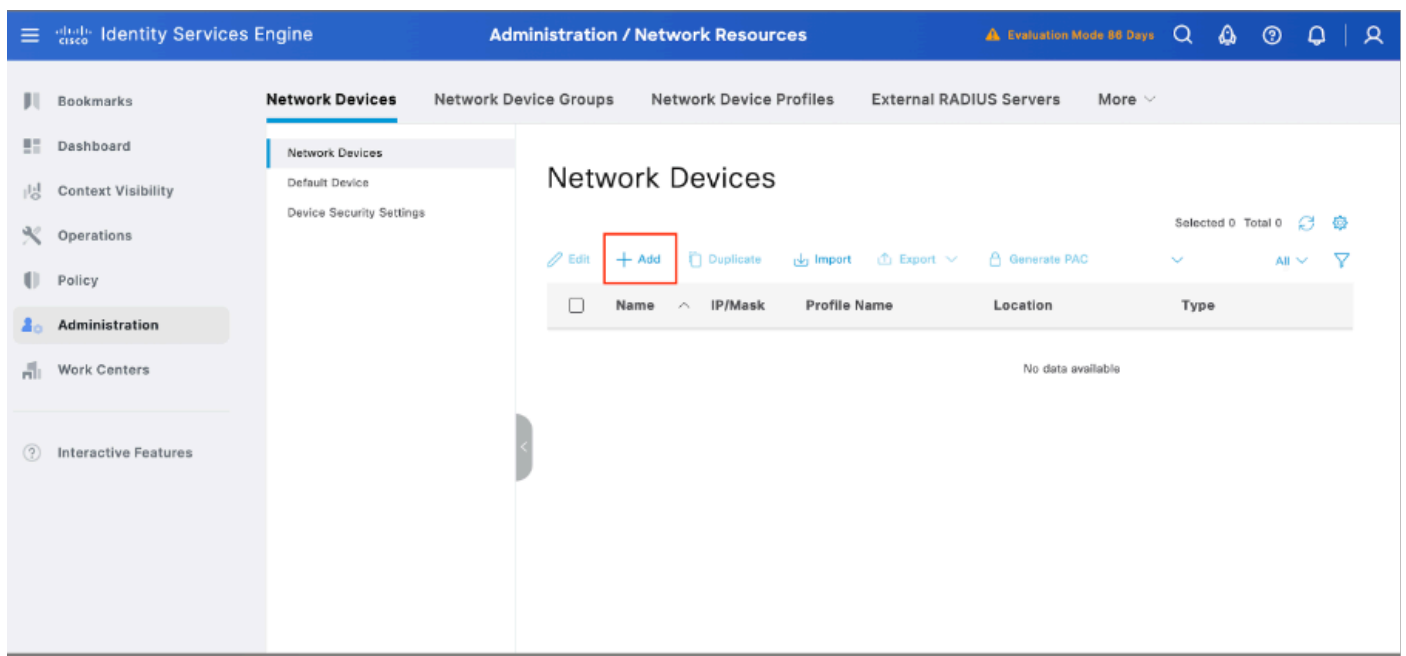


Une fois le téléchargement terminé, accédez à l'option Edit et activez TACACS+ comme protocole pris en charge.



Étape 2 : Ajoutez un commutateur Arista en tant que périphérique réseau.

1. Accédez à Administration > Network Resources > Network Devices > +Add:



2. Cliquez sur Add et entrez ces détails :

- Adresse IP: <IP du commutateur>
- Type de périphérique : Choisir un autre câblé
- Profil de périphérique réseau : sélectionnez AristaCloudVisionWiFi.

- Paramètres d'authentification RADIUS :
 - Activez l'authentification RADIUS.
 - Entrez le secret partagé (il doit correspondre à la configuration du commutateur).

3. Cliquez sur Enregistrer :

Identity Services Engine Administration / Network Resources

Network Devices

Name: Arista_switch

Description: Arista_switch for device login TACACS and

IP Address: 32

Device Profile: AristaCloudVisionWiFi

Model Name: 4-33-2F

Software Version: 4-33-2F

Network Device Group: All Locations

Location: All Locations

IPSEC: No

Device Type: All Device Types

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: RADIUS

Shared Secret: -----

☐ Use Second Shared Secret

Étape 3. Validez le nouveau périphérique comme indiqué sous Network Devices :

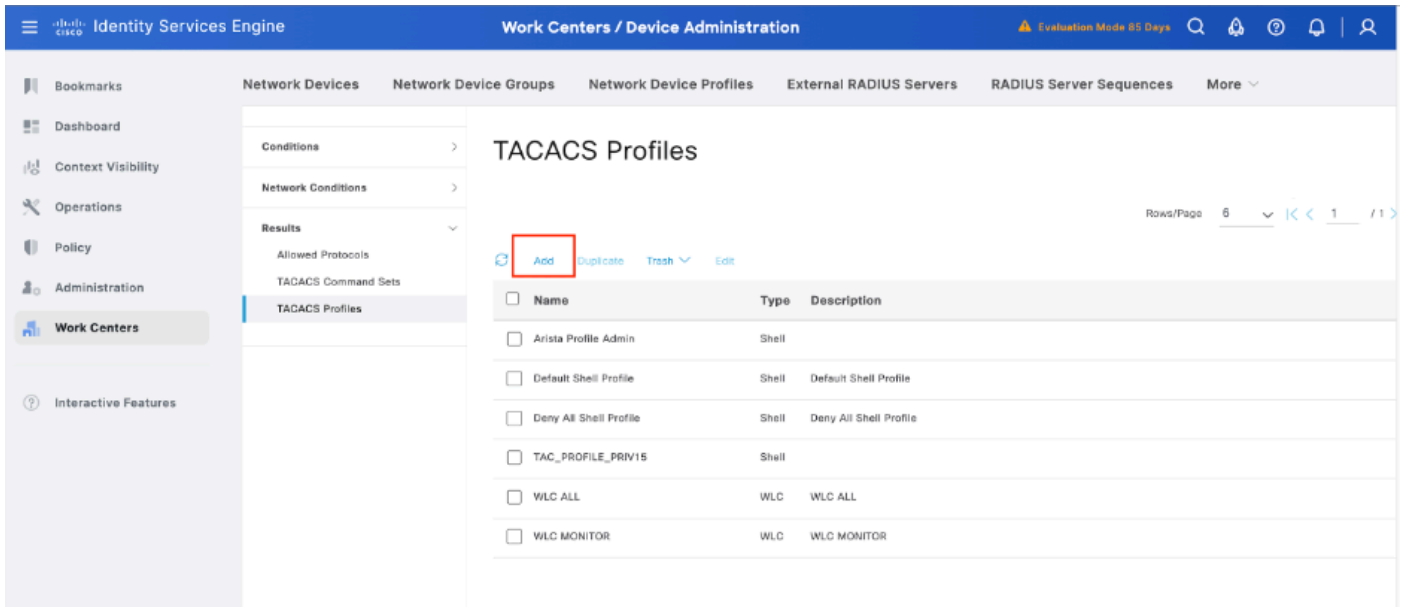
Identity Services Engine Administration / Network Resources

Network Devices

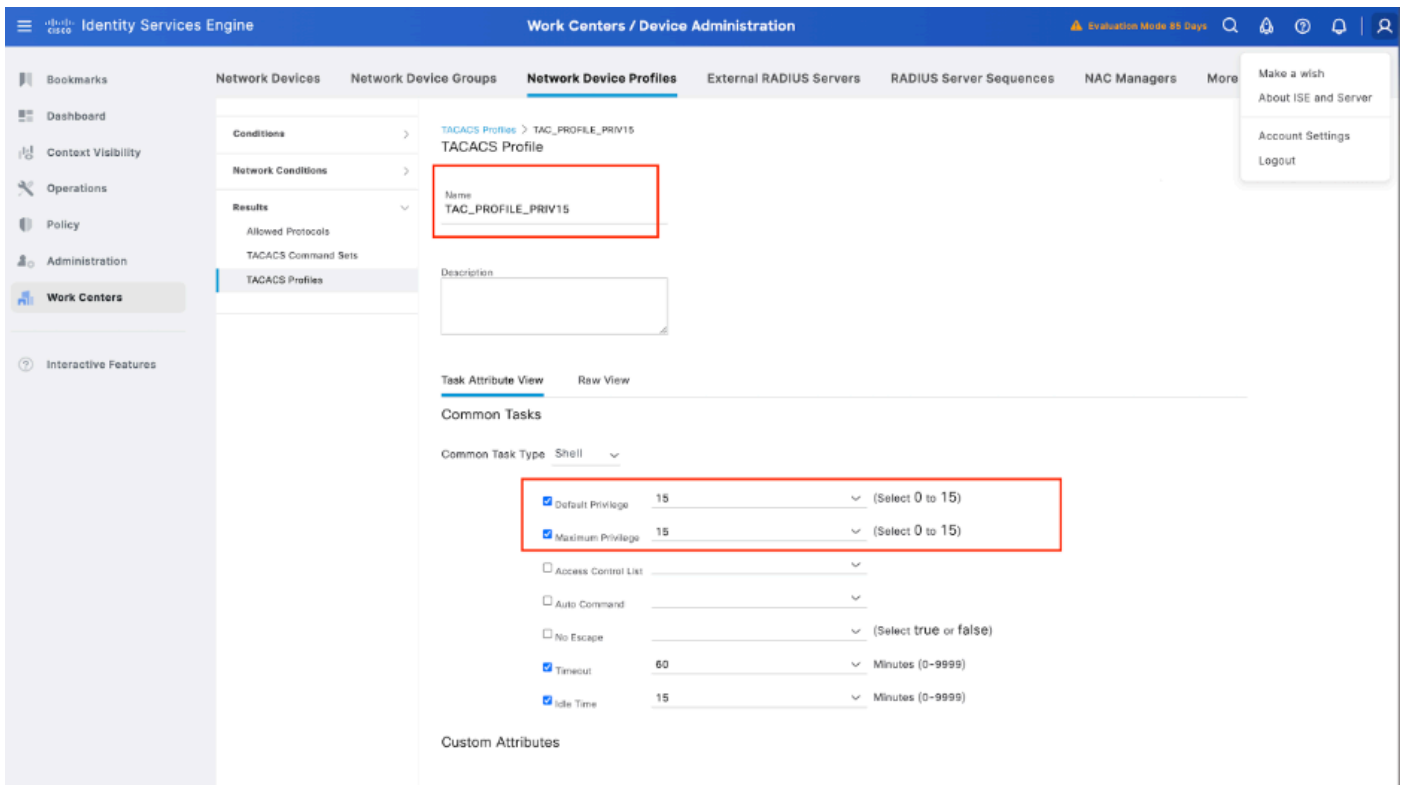
Name	IP/Mask	Profile Name	Location	Type	Description
☐ Arista_switch	32	AristaCloudVisionWiFi	All Locations	All Device Types	Arista_switch f

Étape 4 : configuration du profil TACACS

Créez un profil TACACS, accédez au menu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles, puis sélectionnez Add :



Saisissez un nom, cochez la case Privilège par défaut et définissez la valeur sur 15. En outre, sélectionnez Privilège maximal, définissez sa valeur sur 15, puis cliquez sur Soumettre :



Étape 5. Créez un ensemble de stratégies d'administration de périphériques à utiliser pour votre commutateur Arista, accédez au menu Work Centers > Device Administration > Device Admin Policy Sets, puis, à partir d'un ensemble de stratégies existant, sélectionnez l'icône d'engrenage pour ensuite sélectionner Insert new row above.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27		
+	Default	Tacacs Default policy set		Default Device Admin			

Context menu options: Insert new row above, Insert new row below, Duplicate above, Duplicate below, Delete.

Étape 6. Nommez ce nouvel ensemble de stratégies, ajoutez des conditions en fonction des caractéristiques des authentifications TACACS+ en cours à partir du commutateur Arista, et sélectionnez Allowed Protocols > Default Device Admin, enregistrez votre configuration.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27		
+	Default	Tacacs Default policy set					

Allowed Protocols dropdown: Default Device Admin, Default Network Access.

Étape 7. Sélectionnez l'option > view, puis dans la section Authentication Policy, sélectionnez la source d'identité externe que Cisco ISE utilise pour interroger le nom d'utilisateur et les informations d'identification pour l'authentification sur le commutateur Arista. Dans cet exemple, les informations d'identification correspondent aux utilisateurs internes stockés dans ISE.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is selected. The 'Policy Sets' section displays 'Arista Switch Access' with a status of 'On'. Below this, the 'Authentication Policy(1)' section shows a 'Default' rule with a status of 'On'. The 'Internal Users' option is highlighted with a red box.

Étape 8. Faites défiler la page jusqu'à la section intitulée Authorization Policy to Default policy, sélectionnez l'icône du rapport, puis insérez une règle ci-dessus.

Étape 9. Attribuez un nom à la nouvelle règle d'autorisation, ajoutez des conditions concernant l'utilisateur qui est déjà authentifié en tant qu'appartenance à un groupe et, dans la section Profils Shell, ajoutez le profil TACACS que vous avez configuré précédemment, enregistrez la configuration.

The screenshot shows the Cisco ISE Work Centers / Device Administration interface. The 'Device Admin Policy Sets' tab is selected. The 'Policy Sets' section displays 'Arista Switch Access' with a status of 'On'. Below this, the 'Authorization Policy(2)' section shows a 'Default' rule with a status of 'On'. The 'Internal Users' option is highlighted with a red box.

Configuration du commutateur Arista

Étape 1 : activation de l'authentification TACACS+

Connectez-vous au commutateur Arista et passez en mode de configuration :

configurer

!

```
tacacs-server host <ISE-IP> key <TACACS-SECRET>
```

!

```
aaa group server tacacs+ ISE_TACACS
```

serveur <|SE-IP>

!

```
aaa authentication login default group ISE_TACACS local
```

```
aaa authorization exec default group ISE_TACACS local
```

```
aaa accounting commands 15 default start-stop group ISE_TACACS
```

!

Tranche

Étape 2 : enregistrement de la configuration

Pour conserver la configuration lors des redémarrages :

mémoire d'écriture

OU

```
# copy running-config startup-config
```

Vérifier

Évaluation ISE

Étape 1. Vérifiez si la facilité de maintenance TACACS+ est en cours d'exécution. Vous pouvez l'intégrer :

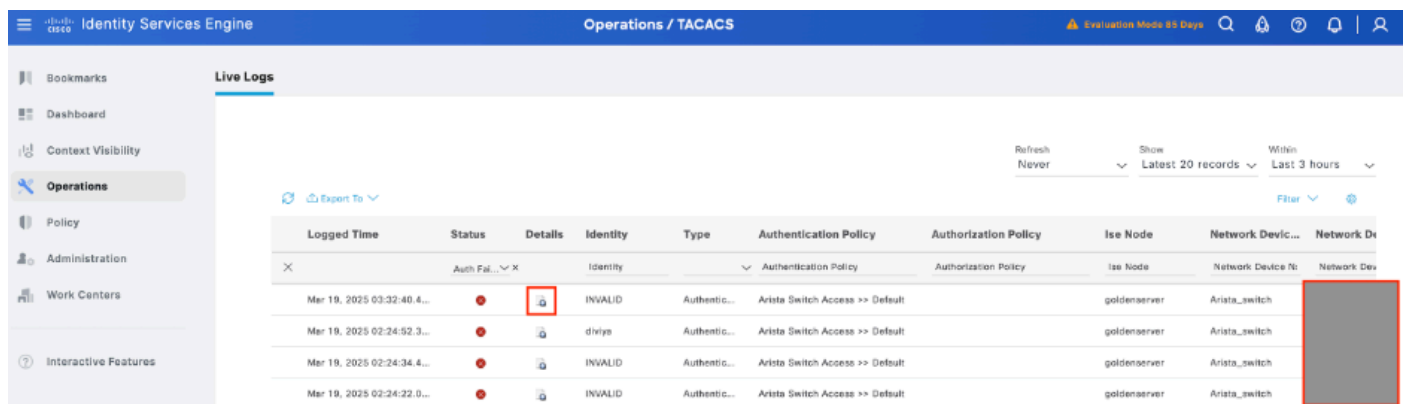
- IUG: Vérifiez si le noeud est répertorié avec le service DEVICE ADMIN dans > System > Deployment.
- CLI : Exécutez la commande `show ports | include 49` pour confirmer que le port TCP contient des connexions appartenant à TACACS+

```
goldenserver/admin#show ports | include 49
```

```
tcp: [REDACTED]
```

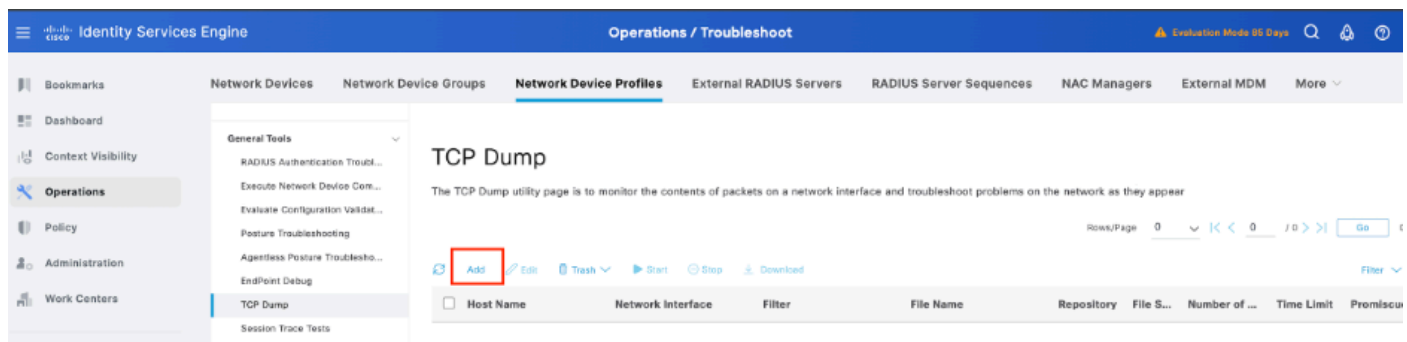
Étape 2. Vérifier s'il existe des journaux en direct concernant les tentatives d'authentification TACACS+ : vous pouvez le vérifier dans le menu Operations > TACACS > Live logs,

En fonction de la raison de l'échec, vous pouvez ajuster votre configuration ou résoudre la cause de l'échec.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device	Network Device ID
Mar 19, 2025 03:32:40.4...	Auth Fail	INVALID	diviya	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	
Mar 19, 2025 02:24:52.3...		INVALID	diviya	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	
Mar 19, 2025 02:24:34.4...		INVALID	diviya	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	
Mar 19, 2025 02:24:22.0...		INVALID	diviya	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	

Étape 3. Si vous ne voyez pas de journal en direct, passez à la capture de paquets. Accédez au menu Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump , sélectionnez Add:



Host Name	Network Interface	Filter	File Name	Repository	File Size	Number of ...	Time Limit	Promiscuous
The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear Rows/Page 0 < > 0 / 0 > > Go Add Edit Trash Start Stop Download Filter								

Identity Services Engine Operations / Troubleshoot Evaluation Mode 85 Days

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxGrid Direct Connectors More

General Tools
 RADIUS Authentication Troubleshooting
 Evaluate Network Device Configuration
 Evaluate Configuration Validation
 Posture Troubleshooting
 Agentless Posture Troubleshooting
 Endpoint Debug
TCP Dump
 Session Trace Tests
 TrustSec Tools

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*
 goldenserver

Network Interface*
 GigabitEthernet 0 ([Up, Running])

Filter
 ip host
 E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
 tcpdump_issue

Repository

File Size
 10 Mb

Limit to
 1 File(s)

Time Limit
 5 Minute(s)

☐ Privileges Mode

Cancel Save **Save and Run**

Étape 4. Activez le composant runtime-AAA dans debug dans le PSN à partir de l'endroit où l'authentification est effectuée dans Operations > Troubleshoot > Debug Wizard > Debug log configuration, sélectionnez PSN node, puis sélectionnez le bouton Edit :

Identity Services Engine Operations / Troubleshoot Evaluation Mode 85 Days

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

Node List

Selected 0 Total 1

Edit Reset to Default

Node Name	Replication Role
goldenserver	STANDALONE

Identity Services Engine Operations / Troubleshoot Evaluation Mode 85 Days

Diagnostic Tools Download Logs **Debug Wizard**

Node List > goldenserver.diviya.com

Debug Level Configuration

Edit Reset to Default Log Filter Enable Log Filter Disable Quick Filter

Component Name	Log Level	Description	Log file Name	Log Filter
runtime-AAA	DEBUG	AAA runtime messages (prnt)	prnt-server.log	Disabled

Save Cancel

Identifiez le composant runtime-AAA, définissez son niveau de journalisation sur debug, reproduisez le problème et analysez les journaux pour une enquête plus approfondie.

Dépannage

Problème 1

L'authentification TACACS+ entre Cisco ISE et le commutateur Arista (ou tout périphérique réseau) échoue avec le message d'erreur suivant :

"Le profil d'interpréteur de commandes 13036 sélectionné est DenyAccess"

Overview		Steps	
Request Type	Authentication	13013	Received TACACS+ Authentication START Request
Status	Fail	15049	Evaluating Policy Group (🔴 Step latency=1ms)
Session Key	goldenserver/541265148/80	15008	Evaluating Service Selection Policy (🔴 Step latency=0ms)
Message Text	Failed-Attempt: Authentication failed	15048	Queried PIP - DEVICE.Device Type (🔴 Step latency=2ms)
Username	diviya	15041	Evaluating Identity Policy (🔴 Step latency=3ms)
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth	15048	Queried PIP - Network Access.Protocol (🔴 Step latency=2ms)
Selected Authorization Profile	Deny All Shell Profile	15013	Selected Identity Source - Internal Users (🔴 Step latency=2ms)
Authentication Details		24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
Generated Time	2025-07-27 16:06:30.094000 +05:30	24212	Found User in Internal Users IDStore (🔴 Step latency=37ms)
Logged Time	2025-07-27 16:06:30.094	13045	TACACS+ will use the password prompt from global TACACS+ configuration (🔴 Step latency=0ms)
Epoch Time (sec)	1753612590	13015	Returned TACACS+ Authentication Reply (🔴 Step latency=0ms)
ISE Node	goldenserver	13014	Received TACACS+ Authentication CONTINUE Request (🔴 Step latency=68ms)
Message Text	Failed-Attempt: Authentication failed	15041	Evaluating Identity Policy (🔴 Step latency=0ms)
Failure Reason	13036 Selected Shell Profile is DenyAccess	15013	Selected Identity Source - Internal Users (🔴 Step latency=4ms)
Resolution	Check whether the Device Administration Authorization Policy rules are correct	24210	Looking up User in Internal Users IDStore (🔴 Step latency=0ms)
Root Cause	Selected Shell Profile fails for this request	24212	Found User in Internal Users IDStore (🔴 Step latency=7ms)
Username	diviya	22037	Authentication Passed (🔴 Step latency=0ms)
		15036	Evaluating Authorization Policy (🔴 Step latency=0ms)
		15048	Queried PIP - Network Access.UserName (🔴 Step latency=4ms)

L'erreur « 13036 Selected Shell Profile is DenyAccess » dans Cisco ISE signifie typiquement que pendant une tentative d'administration de périphérique TACACS+, la stratégie d'autorisation correspondait à un profil d'interpréteur de commandes défini sur DenyAccess. Ce n'est généralement pas le résultat d'un profil d'interpréteur de commandes mal configuré lui-même, mais indique plutôt qu'aucune des règles d'autorisation configurées ne correspondait aux attributs d'utilisateur entrant (tels que l'appartenance à un groupe, le type de périphérique ou l'emplacement). Par conséquent, ISE revient à une règle par défaut ou à une règle de refus explicite, ce qui entraîne le refus de l'accès.

Causes possibles

- Examinez les règles de stratégie d'autorisation dans ISE. Vérifiez que l'utilisateur ou le périphérique correspond à la règle qui attribue le profil d'environnement souhaité, par exemple celle qui autorise un accès approprié.
- Assurez-vous que le mappage AD ou de groupe d'utilisateurs interne est correct et que les conditions de stratégie, telles que l'appartenance à un groupe d'utilisateurs, le type de périphérique et le protocole, sont spécifiées avec précision.
- Utilisez les journaux en direct ISE et les détails de l'échec de la tentative pour voir exactement quelle règle correspond et pourquoi.

Problème 2

L'authentification TACACS+ entre Cisco ISE et le commutateur Arista (ou tout périphérique

réseau) échoue avec le message d'erreur suivant :

"13017 Paquet TACACS+ reçu d'un périphérique réseau inconnu ou d'un client AAA"

Cisco ISE

Overview

Request Type

Authentication

Status

Fail

Session Key

Message Text

Failed-Attempt: TACACS+ Request dropped

Username

Authentication Policy

Selected Authorization Profile

Steps

13017

Received TACACS+ packet from unknown Network Device or AAA Client

Authentication Details

Generated Time

2025-07-27 17:50:17.705000 +05:30

Logged Time

2025-07-27 17:50:17.705

Epoch Time (sec)

1753618817

ISE Node

goldenserver

Message Text

Failed-Attempt: TACACS+ Request dropped

Failure Reason

13017 Received TACACS+ packet from unknown Network Device or AAA Client

Resolution

Root Cause

Username

Causes possibles

- La raison la plus courante est que l'adresse IP du commutateur n'est pas ajoutée en tant que périphérique réseau dans ISE (sous Administration > Network Resources > Network Devices).
- Assurez-vous que l'adresse IP ou la plage correspond exactement à l'adresse IP source utilisée par le commutateur Arista pour envoyer des paquets TACACS+.
- Si votre commutateur utilise une interface de gestion, vérifiez que son adresse IP exacte (et pas seulement un sous-réseau/une plage) est ajoutée dans ISE.

Solution

- Accédez à Administration > Network Resources > Network Devices dans l'interface utilisateur graphique ISE.
- Vérifiez si l'adresse IP source exacte sur le commutateur Arista est utilisée pour la communication TACACS+ (le plus souvent l'adresse IP de l'interface de gestion).
- Spécifiez le secret partagé (il doit correspondre à celui défini sur le commutateur Arista).

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.