

# Utiliser RADIUS pour l'administration des périphériques avec Identity Services Engine

## Table des matières

---

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Créer un profil d'acceptation d'accès](#)

[Créer un profil de refus d'accès](#)

[Liste des périphériques](#)

[Routeurs à services d'agrégation \(ASR\)](#)

[Commutateurs Cisco IOS® et Cisco IOS® XE](#)

[Formeur de paquets BlueCoat](#)

[Serveur proxy BlueCoat \(AV/SG\)](#)

[Commutateurs Brocade](#)

[Infoblox](#)

[Cisco Firepower Management Center](#)

[Commutateurs Nexus](#)

[Contrôleur LAN sans fil \(WLC\)](#)

[Data Center Network Manager \(DCNM\)](#)

[Codes audio](#)

---

## Introduction

Ce document décrit la compilation des attributs que divers produits Cisco et non Cisco attendent d'un serveur AAA comme un Cisco ISE.

## Informations générales

Les produits Cisco et non Cisco s'attendent à recevoir une compilation d'attributs d'un serveur AAA (Authentication, Authorization, and Accounting). Dans ce cas, le serveur est un Cisco ISE et l'ISE renvoie ces attributs avec un Access-Accept dans le cadre d'un profil d'autorisation (RADIUS).

Ce document fournit des instructions détaillées sur la façon d'ajouter des profils d'autorisation d'attribut personnalisés et contient également une liste des périphériques et les attributs RADIUS que les périphériques s'attendent à voir renvoyés par le serveur AAA. Tous les sujets incluent des exemples.

La liste des attributs fournie dans ce document n'est ni exhaustive ni faisant autorité et peut être modifiée à tout moment sans mise à jour de ce document.

L'administration de périphériques d'un périphérique réseau est généralement réalisée avec le protocole TACACS+, mais si le périphérique réseau ne prend pas en charge TACACS+ ou si ISE ne dispose pas d'une licence d'administration de périphériques, elle peut également être réalisée avec RADIUS si le périphérique réseau prend en charge l'administration de périphériques RADIUS. Certains périphériques prennent en charge les deux protocoles et c'est aux utilisateurs de décider quel protocole utiliser, mais TACACS+ peut être favorable car il dispose de fonctionnalités telles que l'autorisation et la comptabilisation des commandes.

## Conditions préalables

### Exigences

Cisco vous recommande d'avoir connaissance des éléments suivants :

- Cisco ISE en tant que serveur Radius sur le réseau concerné
- Le workflow du protocole Radius - RFC2865

### Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Identity Services Engine (ISE) 3.x et les versions ultérieures d'ISE.

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.

## Configurer

### Étape 1. Créer les attributs spécifiques au fournisseur (VSA)


Plusieurs dictionnaires peuvent être créés pour chacun des fournisseurs et des attributs peuvent être ajoutés à chacun de ces dictionnaires. Chaque dictionnaire peut avoir plusieurs attributs qui peuvent être utilisés dans les profils d'autorisation. Chaque attribut, en général, définit le rôle différent de l'administration de périphérique qu'un utilisateur peut obtenir lorsqu'il se connecte au périphérique réseau. Cependant, l'attribut peut être destiné à différentes fins de fonctionnement ou de configuration sur le périphérique réseau.

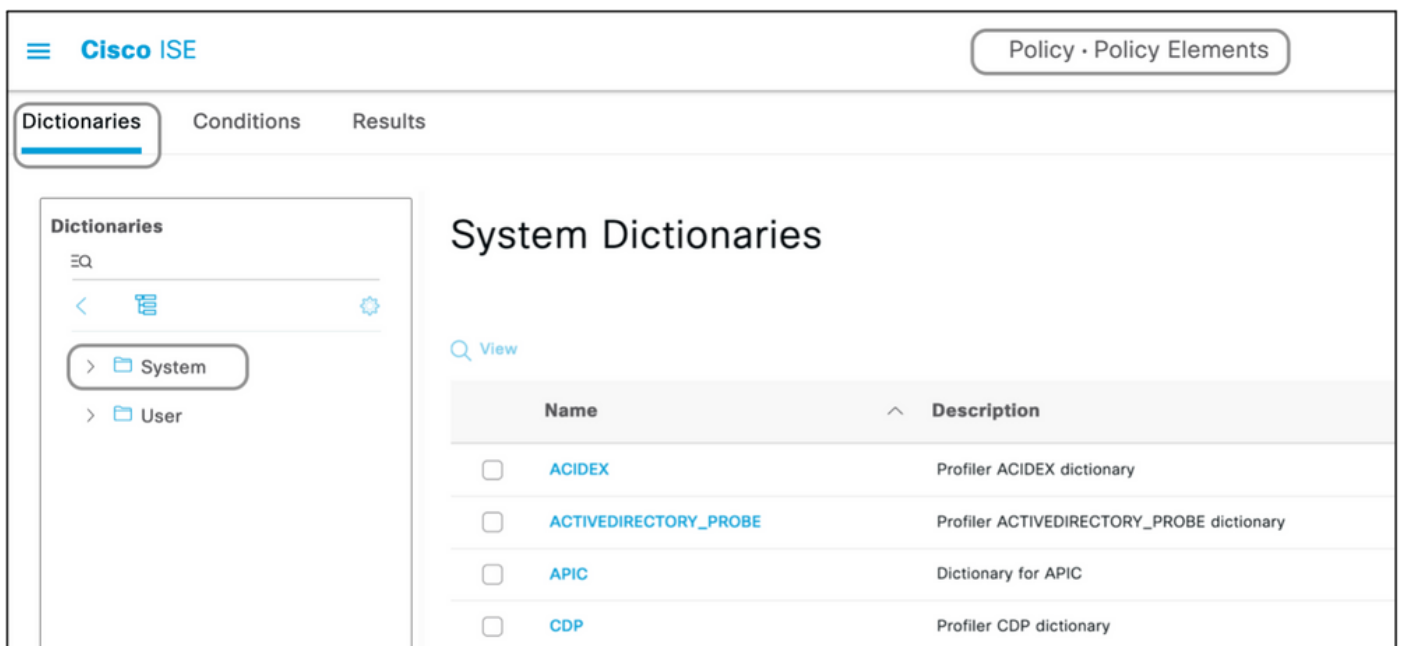
ISE est livré avec des attributs prédéfinis pour quelques fournisseurs. Si le fournisseur n'est pas répertorié, il peut être ajouté en tant que dictionnaire avec des attributs. Pour certains périphériques réseau, les attributs sont configurables et peuvent être modifiés pour différents types d'accès. Dans ce cas, ISE doit être configuré avec les attributs que le périphérique réseau attend pour différents types d'accès.

Les attributs qui sont censés être envoyés avec une acceptation d'accès Radius sont définis

comme suit :

1. Accédez à Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors > Add.
2. Le nom et les ID fournisseur doivent être saisis et enregistrés.
3. Cliquez sur le fournisseur Radius enregistré et accédez à Attributs du dictionnaire.
4. Cliquez sur Add et remplissez les champs Attribute Name, Data Type, Direction et ID, qui respectent la casse.
5. Enregistrez l'attribut.
6. Ajoutez d'autres attributs sur la même page s'il y a plusieurs attributs à ajouter au même dictionnaire.

 Note : Chacun des champs saisis comme valeurs dans cette section doit être fourni par le fournisseur lui-même. Les sites Web des fournisseurs peuvent être consultés ou le support des fournisseurs peut être contacté au cas où ils ne seraient pas connus.



The screenshot displays the Cisco ISE interface. At the top, the Cisco ISE logo is on the left, and 'Policy · Policy Elements' is on the right. Below the logo, there are tabs for 'Dictionaries', 'Conditions', and 'Results', with 'Dictionaries' being the active tab. On the left side, there is a sidebar with a search bar and a tree view showing 'System' and 'User' folders. The main area is titled 'System Dictionaries' and features a 'View' button. Below this is a table with the following data:

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX dictionary
<input type="checkbox"/> ACTIVEDIRECTORY_PROBE	Profiler ACTIVEDIRECTORY_PROBE dictionary
<input type="checkbox"/> APIC	Dictionary for APIC
<input type="checkbox"/> CDP	Profiler CDP dictionary

Dictionaries

EQ



- > PassiveID
- > Posture
- > PROFILER
- Radius
    - > IETF
    - RADIUS Vendors
      - > Airespace
      - > Alcatel-Lucent
      - > Aruba

## RADIUS Vendors

[Edit](#)

[Delete](#)
[Import](#)
[Export](#)

<input type="checkbox"/>	Name	Vendor ID	Description
<input type="checkbox"/>	Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/>	Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/>	Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/>	Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/>	Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/>	Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/>	Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000

Dictionaries

EQ



- Radius
  - > IETF
  - RADIUS Vendors
    - > Airespace
    - > Alcatel-Lucent
    - > Aruba
    - > Brocade

RADIUS Vendors List > New RADIUS Vendor

\* Dictionary Name

Description

---

\* Vendor ID

Vendor Attribute Type Field Length

Vendor Attribute Size Field Length

Cisco ISE Policy · Policy Elements

Dictionary Attributes

Dictionary Attributes

+ Add Edit Delete

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefi...
No data available						

Cisco ISE Policy · Policy Elements License Warning

Dictionary Attributes

Dictionary Attributes

\*\* Attribute Name\* Packeteer-AVPair

Description Used in order to specify Access Level

\* Data Type STRING Enable MAC option


\* Direction OUT

\* ID 1 (0-255)

Allow Tagging

Allow multiple instances of this attribute in a profile

Submit

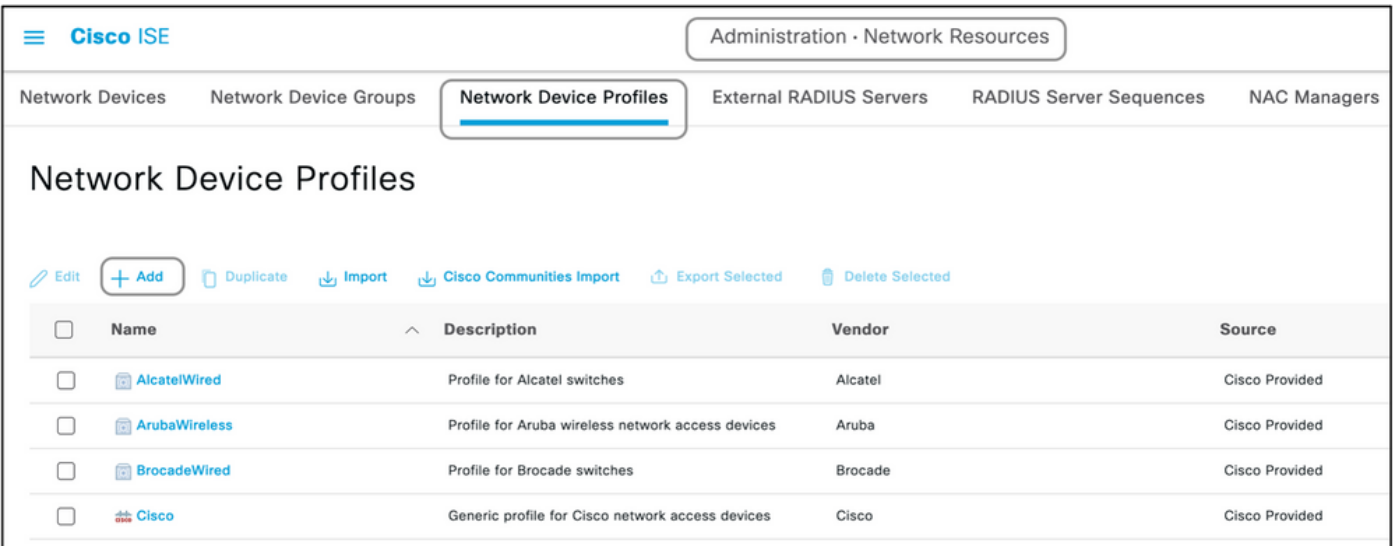
 Remarque : tous les fournisseurs n'ont pas besoin d'ajouter un dictionnaire spécifique. Si le fournisseur peut utiliser les attributs radius définis par l'IETF, qui existent déjà sur ISE, cette étape peut être ignorée.

## Étape 2. Créer un profil de périphérique réseau

Cette section n'est pas obligatoire. Un profil de périphérique réseau permet de distinguer le type de périphérique réseau ajouté et de créer les profils d'autorisation appropriés pour celui-ci. Tout comme les dictionnaires radius, ISE possède quelques profils prédéfinis qui peuvent être utilisés. S'il n'est pas déjà présent, un nouveau profil de périphérique peut être créé.

Voici la procédure à suivre pour ajouter un profil réseau :

1. Accédez à Administration > Network Resources > Network Device Profiles > Add.
2. Donnez un nom et cochez la case pour RADIUS.
3. Sous Dictionnaires RADIUS, sélectionnez le dictionnaire créé dans la section précédente.
4. Si plusieurs dictionnaires ont été créés pour le même type de périphérique, ils peuvent tous être sélectionnés sous Dictionnaires RADIUS.
5. Enregistrez le profil.



The screenshot displays the Cisco ISE interface for managing Network Device Profiles. The breadcrumb navigation is Administration > Network Resources > Network Device Profiles. The page title is "Network Device Profiles". Below the title, there are several action buttons: Edit, Add (highlighted), Duplicate, Import, Cisco Communities Import, Export Selected, and Delete Selected. A table lists the following profiles:

<input type="checkbox"/>	Name	Description	Vendor	Source
<input type="checkbox"/>	AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
<input type="checkbox"/>	ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
<input type="checkbox"/>	BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
<input type="checkbox"/>	Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences

Network Device Profile List > New Network Device Profile

Network Device Profiles Submit Cancel

\* Name Packeteer

Description Device Profile for Packeteer

Icon Change icon... Set To Default

Vendor Other

Supported Protocols

RADIUS

TACACS+

TrustSec

RADIUS Dictionaries Packeteer

### Étape 3. Ajout du périphérique réseau sur ISE

Le périphérique réseau sur lequel l'administration est effectuée doit être ajouté sur ISE avec une clé définie sur le périphérique réseau. Sur le périphérique réseau, ISE est ajouté en tant que serveur RADIUS AAA avec cette clé.

Voici la procédure à suivre pour ajouter un périphérique sur ISE :

1. Accédez à Administration > Network Resources > Network Devices > Add.
2. Donnez un nom et une adresse IP.
3. Le profil de périphérique peut être choisi dans la liste déroulante pour être celui défini dans la section précédente. Si aucun profil n'a été créé, le profil Cisco par défaut peut être utilisé tel quel.
4. Vérifiez les paramètres d'authentification Radius.
5. Saisissez la clé secrète partagée et enregistrez le périphérique.

**Cisco ISE** Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers

## Network Devices

[Edit](#)
[+ Add](#)
[Duplicate](#)
[Import](#)
[Export](#)
[Generate PAC](#)
[Delete](#)

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	SPRT	172.18.228....	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	posturelinux	10.106.36.9...	Cisco	All Locations	All Device Types	

**Cisco ISE** Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers

Network Devices List > New Network Device

## Network Devices

Name:

Description:

IP Address:  /

Device Profile:

Model Name:

Software Version:

Network Device Group

Device Type:  [Set To Default](#)

IPSEC:  [Set To Default](#)

Location:  [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol:

Shared Secret:  [Show](#)



**Cisco ISE** Administration · Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Man

Network Devices List > New Network Device

### Network Devices

Name

Description

IP Address  /

Device Profile

Model Name

Software Version

Network Device Group

Location  [Set To Default](#)

IPSEC  [Set To Default](#)

Device Type  [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret  [Show](#)

#### Étape 4. Créer des profils d'autorisation

Le résultat final qui est transmis à partir d'ISE en tant qu'Access-Accept ou Access-Reject est défini dans un profil d'autorisation. Chaque profil d'autorisation peut transmettre des attributs supplémentaires attendus par le périphérique réseau.

Voici la procédure de création d'un profil d'autorisation :

1. Allez à Policy > Policy Elements > Results > Authorization > Authorization Profiles (politique > éléments de politique > résultats > autorisation > profils d'autorisation).
2. Sous Profils d'autorisation standard, cliquez sur Ajouter.

The screenshot shows the Cisco ISE interface. At the top, there is a navigation bar with 'Cisco ISE' and 'Policy · Policy Elements'. Below this, there are tabs for 'Dictionaries', 'Conditions', and 'Results', with 'Results' being the active tab. On the left, a sidebar menu shows 'Authentication', 'Authorization' (selected), 'Downloadable ACLs', 'Profiling', 'Posture', and 'Client Provisioning'. Under 'Authorization', 'Authorization Profiles' is highlighted. The main content area is titled 'Standard Authorization Profiles' and includes a link for 'Policy Export'. Below the title, there are action buttons: 'Edit', '+ Add', 'Duplicate', and 'Delete'. A table lists several profiles:

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Bidirectional_posture_profile	Cisco ⓘ
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco ⓘ
<input type="checkbox"/>	Cisco_IP_Phones	Cisco ⓘ
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco ⓘ

Les types de profils pouvant être ajoutés sont Access-Accept et Access-Reject.

Créer un profil d'acceptation d'accès

Ce profil est utilisé pour un certain type d'accès au périphérique réseau. Plusieurs attributs peuvent être transmis avec ce profil. Voici les étapes à suivre :

1. Donnez un nom pertinent et choisissez Access Type (Type d'accès) pour Access-Accept (Acceptation d'accès).
2. Sélectionnez le profil de périphérique réseau qui a été créé dans l'une des sections précédentes. Si aucun profil n'a été créé, le profil Cisco par défaut peut être utilisé.
3. Avec différents types de profils choisis, la page limite les options de configuration.
4. Sous Advanced Attributes Settings, choisissez le dictionnaire et l'attribut applicable (LHS).
5. Attribuez une valeur (RHS) à l'attribut à partir de la liste déroulante, si disponible, ou tapez la valeur attendue.
6. Si d'autres attributs doivent être envoyés dans le cadre du même résultat, cliquez sur l'icône + et répétez les étapes 4 et 5.

Créez plusieurs profils d'autorisation pour chacun des résultats/rôles/autorisations qu'ISE est censé envoyer.

---

 Note : Les attributs consolidés peuvent être vérifiés dans le champ Détails de l'attribut.

---

Dictionaries   Conditions   **Results**

- Authentication >
- Authorization ▾
  - Authorization Profiles**
  - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Authorization Profiles > New Authorization Profile

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

#### Common Tasks

ACL ⓘ

Security Group

#### Advanced Attributes Settings

#### Attributes Details

Access Type = ACCESS\_ACCEPT  
Packeteer-AVPair = access=touch

The screenshot displays the Cisco ISE web interface for configuring an Authorization Profile. The breadcrumb path is "Authorization Profiles > New Authorization Profile". The profile name is "Cisco\_Switches" and the description is "Access to Cisco switches". The access type is set to "ACCESS\_ACCEPT". The network device profile is "Cisco". The service template, track movement, agentless posture, and passive identity tracking options are all unchecked. The advanced attributes settings section shows a configuration: "Cisco:cisco-av-pair" equals "shell:priv-lvl=15". The attributes details section shows "Access Type = ACCESS\_ACCEPT" and "cisco-av-pair = shell:priv-lvl=15".

## Créer un profil de refus d'accès

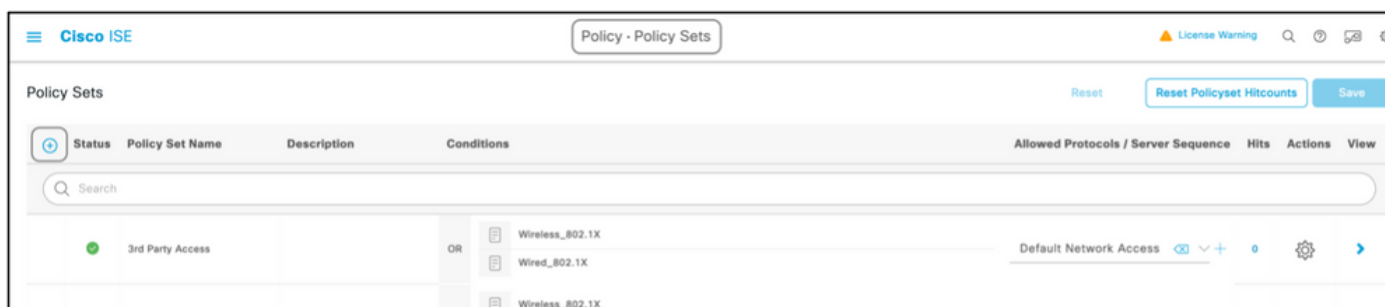
Ce profil est utilisé pour envoyer un refus pour l'administration des périphériques, mais peut toujours être utilisé pour envoyer des attributs avec lui. Il est utilisé pour envoyer un paquet Radius Access-Reject. Les étapes restent les mêmes, à l'exception de l'étape 1 où Access-Reject doit être choisi au lieu de Access-Accept pour le type d'accès.

## Étape 5. Créer un ensemble de stratégies

Les ensembles de politiques sur ISE sont évalués de haut en bas et le premier qui satisfait la condition définie dans les ensembles de politiques est responsable de la réponse de l'ISE au paquet de demande d'accès Radius envoyé par le périphérique réseau. Cisco recommande un jeu de stratégies unique pour chaque type de périphérique. La condition pour évaluer l'authentification et l'autorisation de l'utilisateur se produit lors de l'évaluation. Si ISE a des sources d'identité externes, il peut être utilisé pour le type d'autorisation.

Un jeu de stratégies type est créé de cette façon :

1. Accédez à Policy > Policy Sets > +.
2. Renommez le nouvel ensemble de stratégies 1.
3. Définissez la condition pour qu'elle soit unique pour ce périphérique.
4. Développez l'ensemble de stratégies.
5. Développez la stratégie d'authentification pour définir une règle d'authentification. La source externe ou les utilisateurs internes sont des exemples qui peuvent être utilisés comme séquence source d'identité par rapport à laquelle ISE vérifierait l'identité de l'utilisateur.
6. La stratégie d'authentification est entièrement définie. La stratégie peut être enregistrée à ce stade.
7. Développez la stratégie d'autorisation pour ajouter les conditions d'autorisation pour les utilisateurs. Par exemple, vous pouvez rechercher un groupe AD ou un groupe d'identité interne ISE particulier. Nommez la règle de la même manière.
8. Le résultat de la règle d'autorisation peut être sélectionné dans la liste déroulante.
9. Créez plusieurs règles d'autorisation pour différents types d'accès pris en charge par le fournisseur.



Cisco ISE Policy - Policy Sets License Warning

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	Packet Shaper		DEVICE-Network Device Profile EQUALS Packeteer	Default Network Access	0		

Cisco ISE Policy - Policy Sets License Warning

Packet Shaper DEVICE-Network Device Profile EQUALS Packeteer Default Network Access

Authentication Policy (1)

Status	Rule Name	Conditions	Use
✔	Any authentication condition	DEVICE-Network Device Profile EQUALS Packeteer	All_User_ID_Stores > Options All_User_ID_Stores > Options
✔	Default		All_User_ID_Stores > Options

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

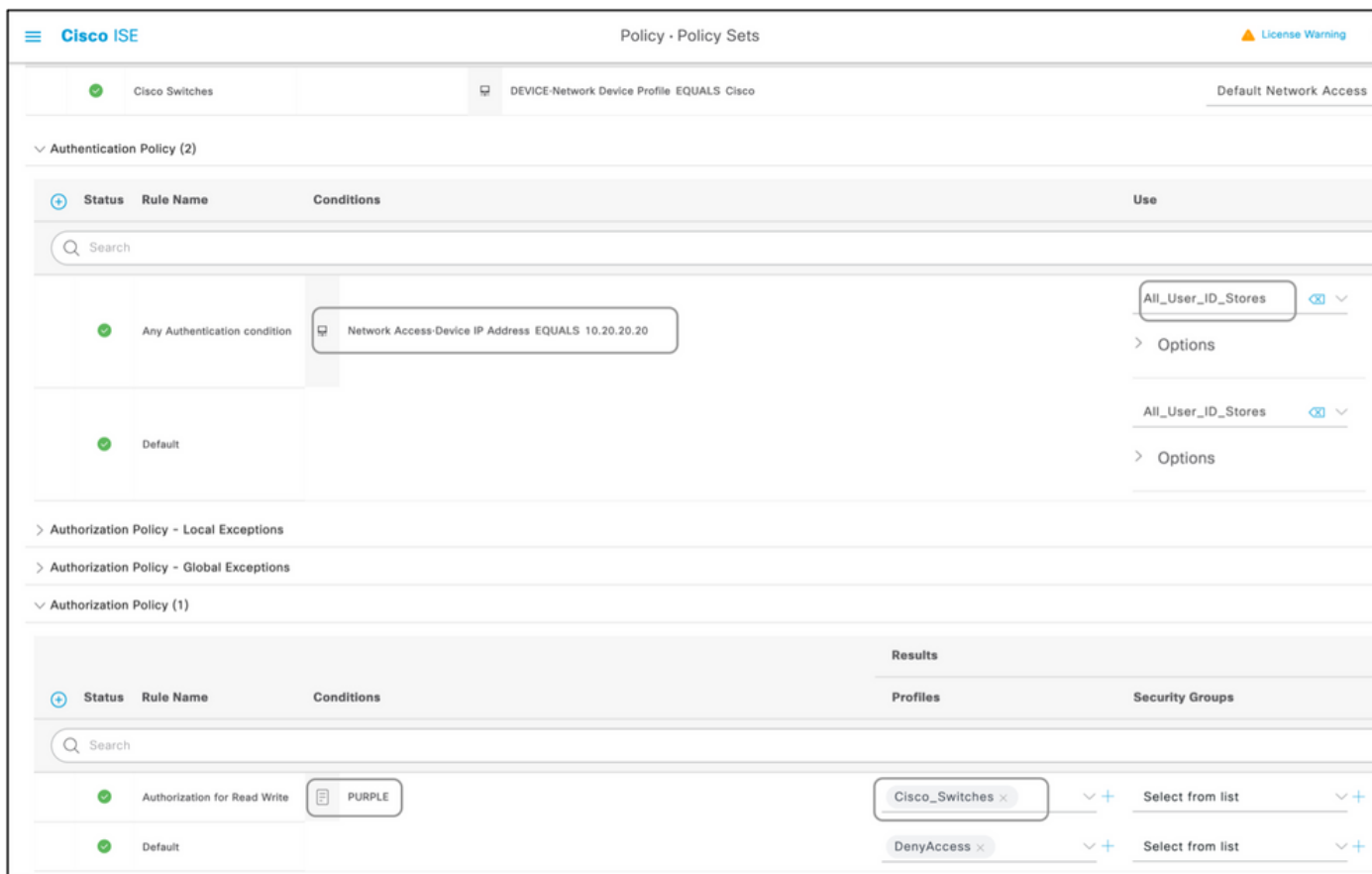
Authorization Policy (1)

Status	Rule Name	Conditions	Results	
			Profiles	Security Groups
✔	Authorization for Read Write	Admins	BlueCoat_PS_ReadWri...	Select from list
✔	Default		DenyAccess	Select from list

Cisco ISE Policy - Policy Sets License Warning

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✔	Cisco Switches		DEVICE-Network Device Profile EQUALS Cisco	Default Network Access	0		



## Liste des périphériques

Tout périphérique prenant en charge l'administration de périphériques avec Radius peut être ajouté sur ISE avec quelques modifications à toutes les étapes mentionnées dans la section précédente. Par conséquent, ce document contient une liste de périphériques qui fonctionnent avec les informations fournies dans cette section. La liste des attributs et des valeurs fournie dans ce document n'est ni exhaustive ni faisant autorité et peut être modifiée à tout moment sans mise à jour de ce document. Veuillez consulter les sites Web des fournisseurs et le support technique pour la validation.

### Routeurs à services d'agrégation (ASR)

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des paires Cisco AV déjà présentes sur ISE.

Attribut(s) : cisco-av-pair

Valeur(s) : shell : tasks="#<nom-rôle>,<permission>:<process>"

Utilisation : Définissez les valeurs de <role-name> sur le nom d'un rôle défini localement sur le routeur. La hiérarchie des rôles peut être décrite sous la forme d'une arborescence, où le rôle #root se trouve en haut de l'arborescence et le rôle #leaf ajoute des commandes supplémentaires. Ces deux rôles peuvent être combinés et repassés si : shell : tasks="#root,#leaf".

Les autorisations peuvent également être retransmises sur un processus individuel, de sorte qu'un utilisateur peut se voir accorder des privilèges de lecture, d'écriture et d'exécution pour certains processus. Par exemple, afin d'accorder à un utilisateur des privilèges de lecture et d'écriture pour le processus BGP, définissez la valeur sur : shell : tasks="#root, rw : bgp". L'ordre des attributs n'a pas d'importance ; le résultat est le même si la valeur est définie sur shell : tasks="#root, rw : bgp" ou toshell : tasks="rw : bgp, #root".

Exemple : Ajouter l'attribut à un profil d'autorisation.

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Cisco	paire cisco-av	Chaîne (string)	shell : tasks="#root, #leaf, rwx : bgp, r : ospf"

## Commutateurs Cisco IOS® et Cisco IOS® XE

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des attributs RADIUS déjà présents sur ISE.

Attribut(s) : cisco-av-pair

Valeur(s) : shell : priv-lvl=<niveau>

Utilisation : Définissez les valeurs de <level> sur les nombres qui sont essentiellement le nombre de privilèges à envoyer. Typiquement, si 15 est envoyé, cela signifie lecture-écriture, si 7 est envoyé, cela signifie lecture seule.

Exemple : Ajouter l'attribut à un profil d'autorisation.

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Cisco	paire cisco-av	Chaîne (string)	shell:priv-lvl=15

## Formeur de paquets BlueCoat

Attribut(s) : Packeter-AVPair

Valeur(s) : access=<level>

Utilisation : <level> est le niveau d'accès à accorder. L'accès tactile est équivalent à l'accès en lecture-écriture, tandis que l'accès en lecture est équivalent à l'accès en lecture seule.

Créez un dictionnaire comme indiqué dans ce document avec les valeurs suivantes :

- Nom : Packeter
- ID du fournisseur : 2334
- Taille du champ Longueur du fournisseur : 1
- Taille du champ Type de fournisseur : 1



Entrez les détails de l'attribut :

- Attribut:Packeter-AVPair
- Description : utilisée afin de spécifier le niveau d'accès
- ID d'attribut fournisseur : 1
- Direction : OUT
- Multiple autorisé : faux
- Autoriser le balisage : décoché
- Type d'attribut : chaîne

Exemple : Ajouter l'attribut à un profil d'autorisation (pour un accès en lecture seule).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Packeter	Packeter-AVPair	Chaîne (string)	access=regarder

Exemple : Ajouter l'attribut à un profil d'autorisation (pour un accès en lecture/écriture).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Packeter	Packeter-AVPair	Chaîne (string)	access=toucher

## Serveur proxy BlueCoat (AV/SG)

Attribut(s) : Blue-Coat-Authorization

Valeur(s) : <level>

Utilisation : <level>est le niveau d'accès à accorder. 0 signifie pas d'accès, 1 signifie un accès en lecture seule, tandis que 2 signifie un accès en lecture-écriture. L'attribut Blue-Coat-Authorization est celui responsable du niveau d'accès.

Créez un dictionnaire comme indiqué dans ce document avec les valeurs suivantes :

- Nom : BlueCoat
- ID du fournisseur : 14501
- Taille du champ Longueur du fournisseur : 1
- Taille du champ Type de fournisseur : 1

Entrez les détails de l'attribut :

- Attribut : Blue-Coat-Group
- ID d'attribut fournisseur : 1
- Direction : LES DEUX
- Multiple autorisé : faux
- Autoriser le balisage : décoché
- Type d'attribut : Entier non signé 32 (UINT32)

Entrez les détails du deuxième attribut :

- Attribut : Blue-Coat-Authorization
- Description : utilisée afin de spécifier le niveau d'accès
- ID d'attribut fournisseur : 2
- Direction : LES DEUX
- Multiple autorisé : faux
- Autoriser le balisage : décoché
- Type d'attribut : Entier non signé 32 (UINT32)

Exemple : Ajouter l'attribut à un profil d'autorisation (sans accès).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	0

Exemple : Ajouter l'attribut à un profil d'autorisation (pour un accès en lecture seule).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	1

Exemple : Ajouter l'attribut à un profil d'autorisation (pour un accès en lecture/écriture).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-BlueCoat	Blue-Coat-Group	UINT32	2

## Commutateurs Brocade

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des attributs RADIUS déjà présents sur ISE.

Attribut(s) : Tunnel-Private-Group-ID

Valeur(s) : U:<VLAN1>; T:<VLAN2>

Utilisation : Définissez<VLAN1>sur la valeur du VLAN de données. Définissez<VLAN2>sur la valeur du VLAN voix. Dans cet exemple, le VLAN de données est le VLAN 10 et le VLAN voix est le VLAN 21.

Exemple : Ajouter l'attribut à un profil d'autorisation.

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-IETF	ID-groupe-privé-tunnel	Chaîne marquée	U:10 ; T:21

## Infoblox

Attribut(s) : Infoblox-Group-Info

Valeur(s) : <nom-groupe>

Utilisation : <nom-groupe>est le nom du groupe disposant des privilèges accordés à l'utilisateur.

Ce groupe doit être configuré sur le périphérique Infoblox. Dans cet exemple de configuration, le nom du groupe est MyGroup.

Créez un dictionnaire comme indiqué dans ce document avec les valeurs suivantes :

- Nom : Infoblox
- ID du fournisseur : 7779
- Taille du champ Longueur du fournisseur : 1
- Taille du champ Type de fournisseur : 1

Entrez les détails de l'attribut :

- Attribut : Infoblox-Group-Info
- ID attribut fournisseur : 009
- Direction : OUT
- Multiple autorisé : faux
- Autoriser le balisage : décoché
- Type d'attribut : chaîne

Exemple : Ajouter l'attribut à un profil d'autorisation.

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Infoblox	Info-Groupe-Infoblox	Chaîne (string)	MonGroupe

## Cisco Firepower Management Center

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des attributs RADIUS déjà présents sur ISE.

Attribut(s) : cisco-av-pair

Valeur(s) : Class-[25]=<role>

Utilisation : définissez les valeurs de <role> sur les noms des rôles définis localement sur le FMC. Créez plusieurs rôles, tels que admin et utilisateur en lecture seule sur le FMC et attribuez les valeurs aux attributs sur ISE pour qu'ils soient également reçus par le FMC.

Exemple : Ajouter l'attribut à un profil d'autorisation.

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Cisco	paire cisco-av	Chaîne (string)	Class-[25]=AdministrateursRéseau

## Commutateurs Nexus

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des attributs RADIUS déjà présents sur ISE.

Attribut(s) : cisco-av-pair

Valeur(s) : shell : roles="<role1> <role2>"

Utilisation : Définissez les valeurs de <role1> et <role2> sur les noms des rôles définis localement sur le commutateur. Lorsque plusieurs rôles sont créés, séparez-les par un espace. Lorsque plusieurs rôles sont repassés du serveur AAA au commutateur Nexus, l'utilisateur a accès aux commandes définies par l'union des trois rôles.

Les rôles intégrés sont définis [dans Configurer les comptes d'utilisateurs et RBAC](#).

Exemple : Ajouter l'attribut à un profil d'autorisation.

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-Cisco	paire cisco-av	Chaîne (string)	shell : roles="network-admin vdc-admin vdc-operator"

## Contrôleur LAN sans fil (WLC)

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des attributs RADIUS déjà présents sur ISE.

Attribut(s) : Service-Type

Valeur(s) : Administrative (6) / NAS-Prompt (7)

Utilisation : Pour accorder à l'utilisateur un accès en lecture/écriture au contrôleur de réseau local sans fil (WLC), la valeur doit être Administrative ; pour un accès en lecture seule, la valeur doit être NAS-Prompt.

Pour plus d'informations, [consultez Exemple de configuration de l'authentification serveur RADIUS des utilisateurs de gestion sur un contrôleur LAN sans fil \(WLC\)](#)

Exemple : Ajouter l'attribut à un profil d'autorisation (pour un accès en lecture seule).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-IETF	Type de service	Énumération	Invite NAS

Exemple : Ajouter l'attribut à un profil d'autorisation (pour un accès en lecture/écriture).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-IETF	Type de service	Énumération	Administratif

## Data Center Network Manager (DCNM)

DCNM doit être redémarré après la modification de la méthode d'authentification. Sinon, il peut attribuer le privilège d'opérateur de réseau au lieu de network-admin.

Il n'est pas nécessaire de créer un dictionnaire et des VSA distincts pour cela, car il utilise des attributs RADIUS déjà présents sur ISE.

Attribut(s) : cisco-av-pair

Valeur(s) : shell : roles=<role>

Rôle DCNM	Paire RADIUS Cisco-AV
Utilisateur	shell : rôles = "opérateur réseau"
administrateur	shell : rôles = "admin-réseau"

## Codes audio

Attribut(s) : ACL-Auth-Level

Valeur(s) : ACL-Auth-Level = "<entier>"

Utilisation : <entier>est le niveau d'accès à accorder. Valeur de l'attribut ACL-Auth-Level avec le nom ACL-Auth-UserLevel de 50 pour l'utilisateur, valeur de l'attribut ACL-Auth-Level avec le nom ACL-Auth-AdminLevel de la valeur 100 pour l'administrateur et valeur de ACL-Auth-Level avec le nom ACL-Auth-SecurityAdminLevel de la valeur 200 pour l'administrateur de sécurité. Les noms peuvent être ignorés et les valeurs des attributs peuvent être données directement en tant que valeur pour la paire AV avancée de profil d'autorisation.

Créez un dictionnaire comme indiqué dans ce document avec les valeurs suivantes :

- Nom : AudioCodes
- ID du fournisseur : 5003
- Taille du champ Longueur du fournisseur : 1
- Taille du champ Type de fournisseur : 1

Entrez les détails de l'attribut :

- Attribut : ACL-Auth-Level
- Description : utilisée afin de spécifier le niveau d'accès
- ID d'attribut fournisseur : 35
- Direction : OUT
- Multiple autorisé : faux
- Autoriser le balisage : décoché
- Type d'attribut : Entier

Exemple : Ajouter l'attribut à un profil d'autorisation (pour l'utilisateur).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-AudioCodes	ACL-Auth-Level	Entier	50

Exemple : Ajouter l'attribut à un profil d'autorisation (pour admin).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-AudioCodes	ACL-Auth-Level	Entier	100

Exemple : Ajouter l'attribut à un profil d'autorisation (pour l'administrateur de sécurité).

Type de dictionnaire	Attribut RADIUS	Type d'attribut	Valeur d'attribut
RADIUS-AudioCodes	ACL-Auth-Level	Entier	200

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.