# RADIUS voor apparaatbeheer met Identity Services Engine gebruiken

## Inhoud



## Inleiding

Dit document beschrijft de compilatie van kenmerken die verschillende Cisco- en niet-Cisco-producten verwachten te ontvangen van een AAA-server zoals een Cisco ISE.

## Achtergrondinformatie

Cisco- en niet-Cisco-producten verwachten een compilatie van kenmerken van een verificatie-, autorisatie- en accounting (AAA) server te ontvangen. In dit geval is de server een Cisco ISE-processor en geeft de ISE deze eigenschappen, samen met een Access-Accept, terug als deel van een autorisatieprofiel (RADIUS).

Dit document bevat stapsgewijze instructies voor het toevoegen van aangepaste attribuutautorisatieprofielen en bevat ook een lijst met apparaten en de RADIUS-kenmerken waarvan de apparaten verwachten dat deze worden teruggestuurd vanaf de AAA-server. Alle onderwerpen bevatten voorbeelden.

De lijst van eigenschappen in dit document is niet uitputtend noch gezaghebbend en kan te allen tijde worden gewijzigd zonder dat dit document hoeft te worden bijgewerkt.

Apparaatbeheer van een netwerkapparaat wordt over het algemeen bereikt met het TACACS+ protocol, maar als het netwerkapparaat geen TACACS+ ondersteunt of als ISE geen apparaatbeheerlicentie heeft, kan dit ook met RADIUS worden bereikt als het netwerkapparaat RADIUS-apparaatbeheer ondersteunt. Sommige apparaten ondersteunen beide protocollen en het is aan de gebruikers om te beslissen welk protocol te gebruiken, maar TACACS+ kan gunstig zijn omdat het functies heeft zoals opdrachtautorisatie en opdrachtaccounting.

# Voorwaarden

## Vereisten

Cisco raadt u aan hiervan op de hoogte te zijn:

- Cisco ISE als Radius-server in het netwerk van belang
- De workflow van het Radius-protocol - RFC2865

## Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Identity Services Engine (ISE) 3.x en hogere versies van ISE.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Configureren

**Stap 1.** De leverancierspecifieke kenmerken maken (VSA)

Er kunnen verschillende woordenboeken worden gemaakt voor elk van de leveranciers, en attributen kunnen aan elk van deze woordenboeken worden toegevoegd. Elk woordenboek kan meerdere kenmerken hebben die in de autorisatieprofielen kunnen worden gebruikt. Elke eigenschap, in het algemeen, bepaalt de verschillende rol van apparatenbeleid een gebruiker kon krijgen wanneer hij aan het netwerkapparaat het programma opent. Dit kenmerk kan echter zijn bedoeld voor verschillende doeleinden van bediening of configuratie op het netwerkapparaat.

ISE wordt geleverd met vooraf gedefinieerde kenmerken voor een paar leveranciers. Als de verkoper niet in de lijst staat, kan deze worden toegevoegd als een woordenboek met eigenschappen. Voor sommige netwerkapparaten zijn de kenmerken configureerbaar en kunnen deze voor verschillende soorten toegang worden gewijzigd. Als dat het geval is, moet ISE worden geconfigureerd met de kenmerken die het netwerkapparaat verwacht voor verschillende soorten toegang.

De attributen die naar verwachting met een Radius Access-Accept verzonden zullen worden, worden als volgt gedefinieerd:

1. Ga naar **Beleid > Beleidselementen > Woordenboeken > Systeem > Straal > Verkopers van Straal > Toevoegen**.

2. De naam en de leveranciers-ID's moeten worden ingevoerd en opgeslagen.

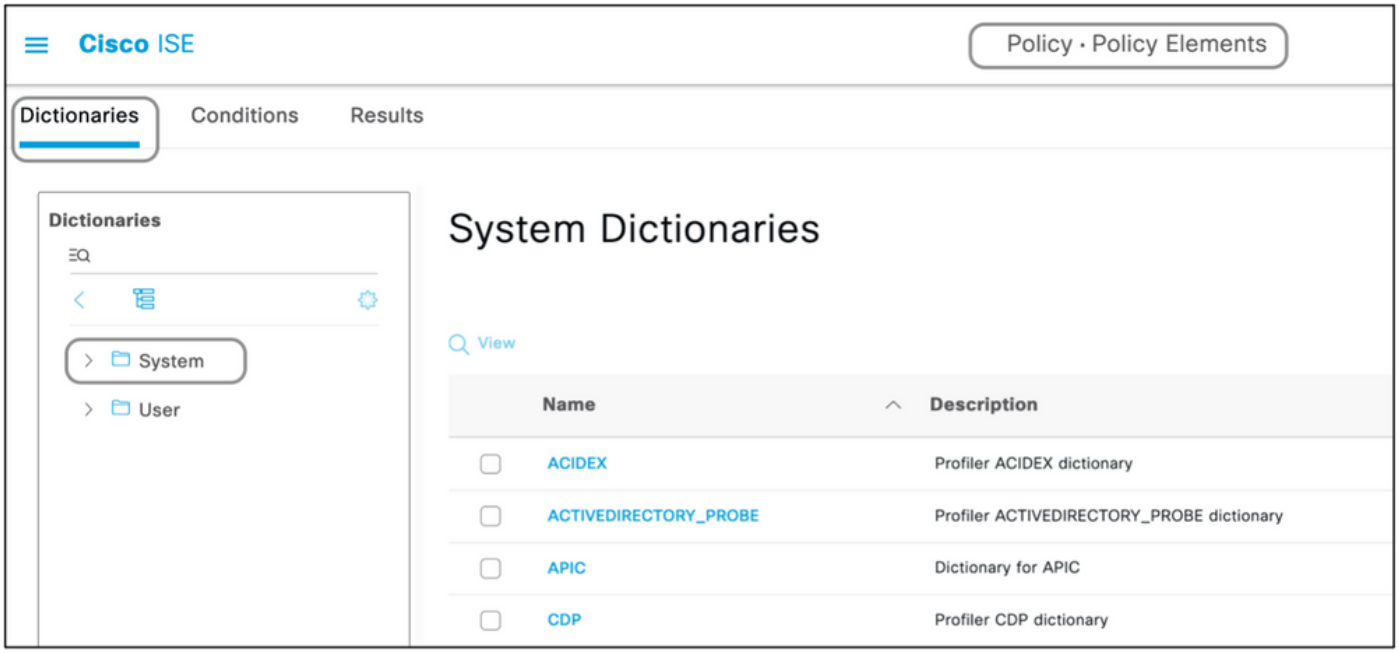
3. Klik op de opgeslagen **RADIUS-leverancier** en navigeer naar **woordenboekkenmerken**.

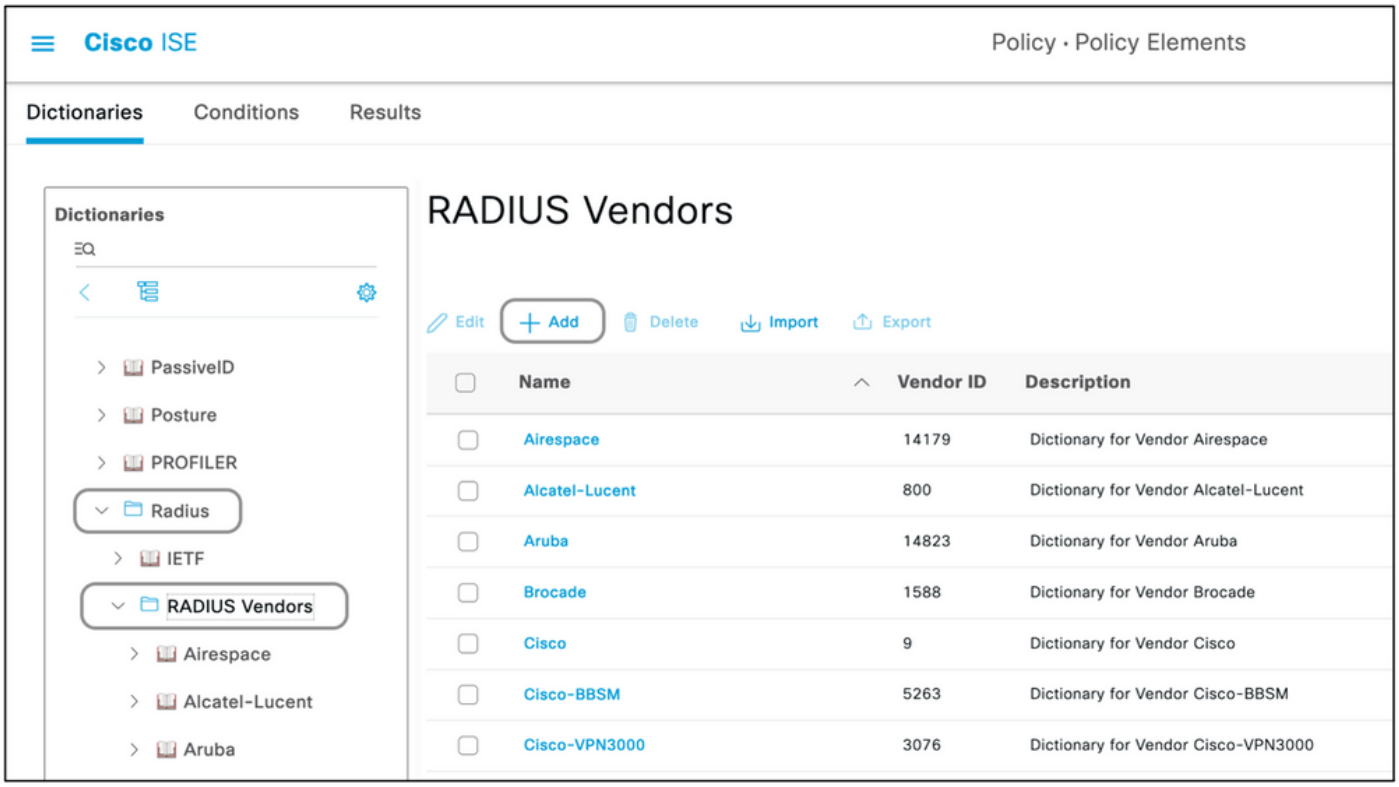
4. Klik op **Add** en vul de casegevoelige naam, het gegevenstype, de richting en de id in.

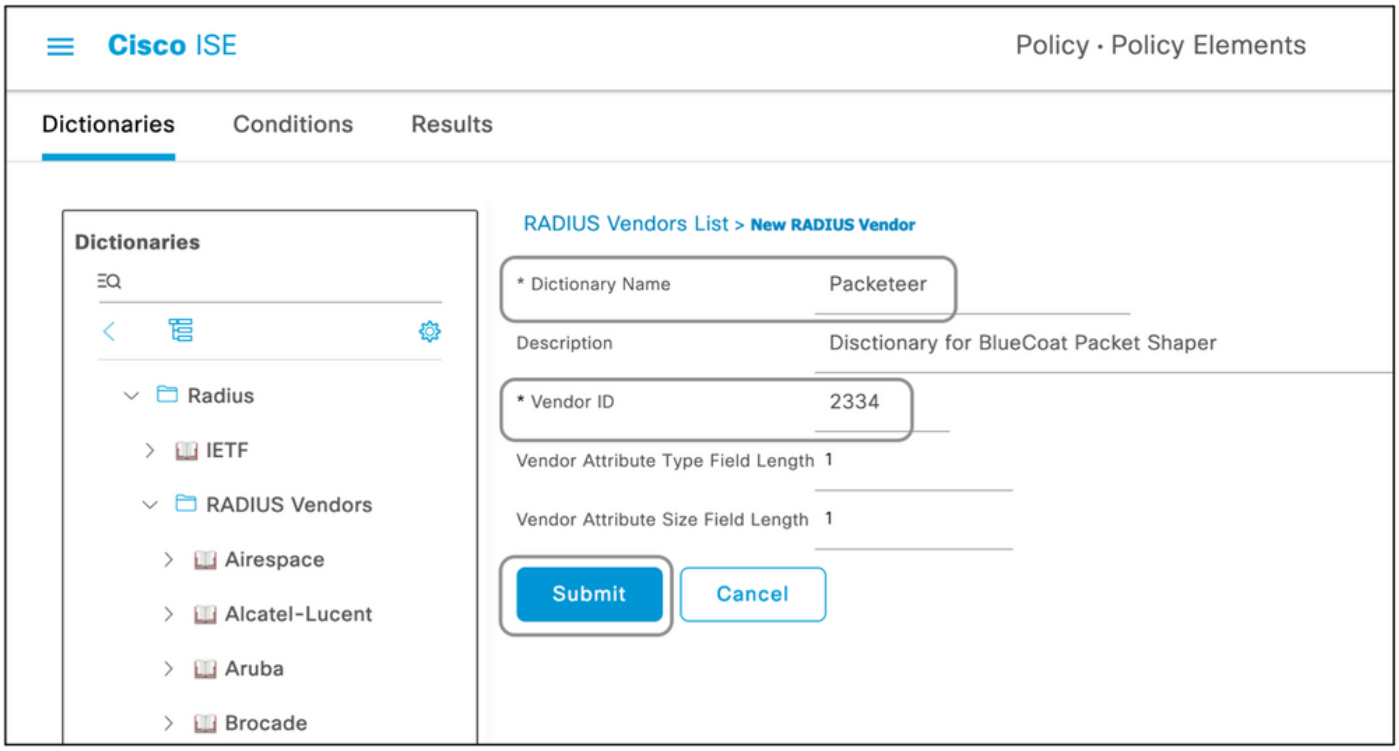
5. **Sla** het kenmerk op.

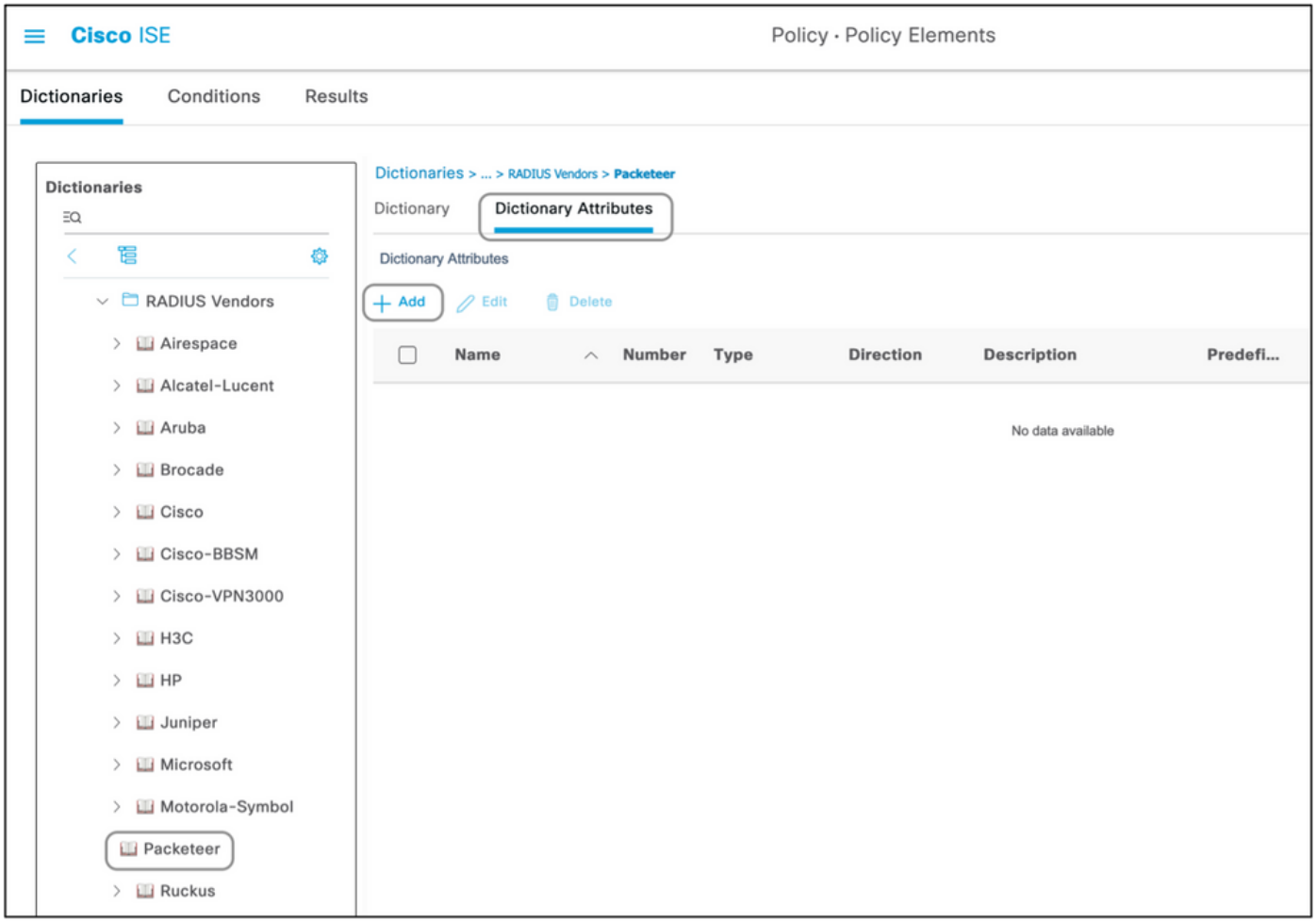
6. Voeg andere kenmerken toe op dezelfde pagina als er meerdere kenmerken zijn die aan hetzelfde woordenboek moeten worden toegevoegd.

   **Opmerking**: elk van de velden die in deze sectie als waarde worden ingevoerd, moet door de verkoper zelf worden ingevuld. De websites van de leveranciers kunnen worden bezocht of er kan contact worden opgenomen met de ondersteuning van de leveranciers als deze niet bekend zijn.




Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
PassiveID
Posture
PROFILER
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
RADIUS Vendors
Edit
Add
Delete
Import
Export
Name
Vendor ID
Description
Airespace 14179 Dictionary for Vendor Airespace
Alcatel-Lucent 800 Dictionary for Vendor Alcatel-Lucent
Aruba 14823 Dictionary for Vendor Aruba
Brocade 1588 Dictionary for Vendor Brocade
Cisco 9 Dictionary for Vendor Cisco
Cisco-BBSM 5263 Dictionary for Vendor Cisco-BBSM
Cisco-VPN3000 3076 Dictionary for Vendor Cisco-VPN3000


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Dictionaries
Radius
IETF
RADIUS Vendors
Airespace
Alcatel-Lucent
Aruba
Brocade
RADIUS Vendors List > New RADIUS Vendor
* Dictionary Name
Packeteer
Description
Disctionary for BlueCoat Packet Shaper
* Vendor ID
2334
Vendor Attribute Type Field Length
1
Vendor Attribute Size Field Length
1
Submit
Cancel





**Opmerking**: niet alle leveranciers hebben een specifiek woordenboek nodig. Als de verkoper de radiuskenmerken kan gebruiken die door IETF zijn gedefinieerd en die al op ISE bestaan, kan deze stap worden overgeslagen.

**Stap 2.** Een profiel voor een netwerkapparaat maken

Dit punt is niet verplicht. Met een profiel voor een netwerkapparaat kunt u het type netwerkapparaat dat wordt toegevoegd, scheiden en geschikte autorisatieprofielen voor deze apparaten maken. Net als de straalwoordenboeken heeft ISE enkele vooraf gedefinieerde

profielen die kunnen worden gebruikt. Als het profiel nog niet bestaat, kan er een nieuw apparaatprofiel worden gemaakt.

Dit is de procedure voor het toevoegen van een netwerkprofiel:

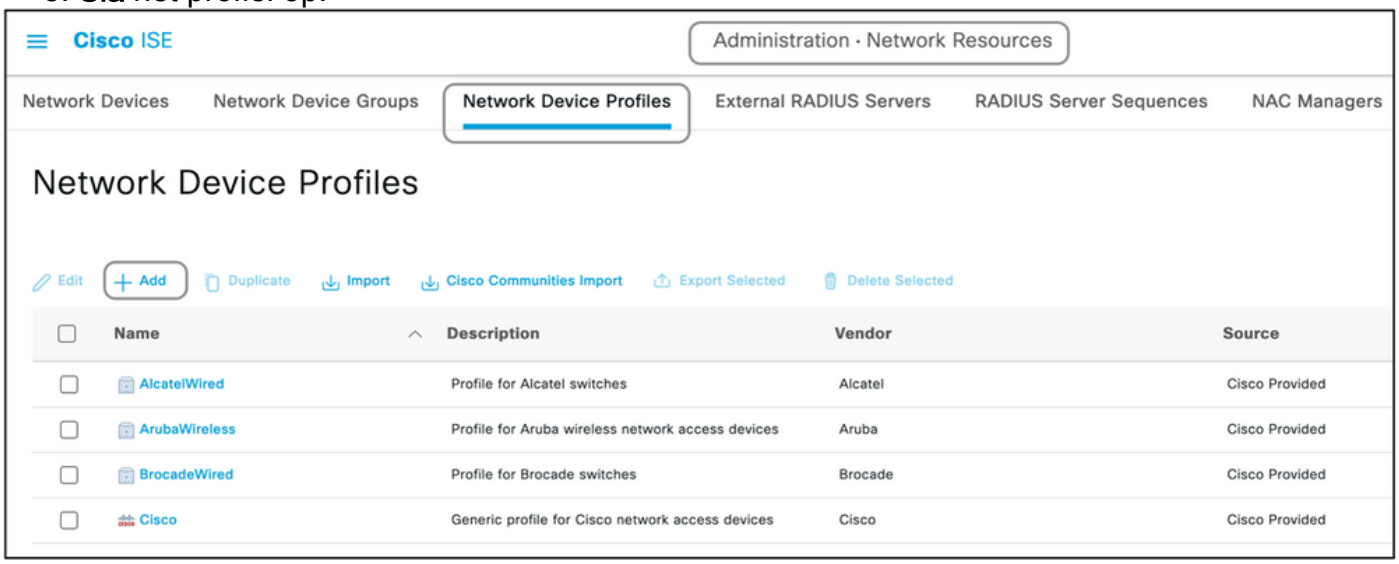
1. Naar navigeren **Beheer > Netwerkbronnen > Netwerkapparaatprofielen > Toevoegen.**

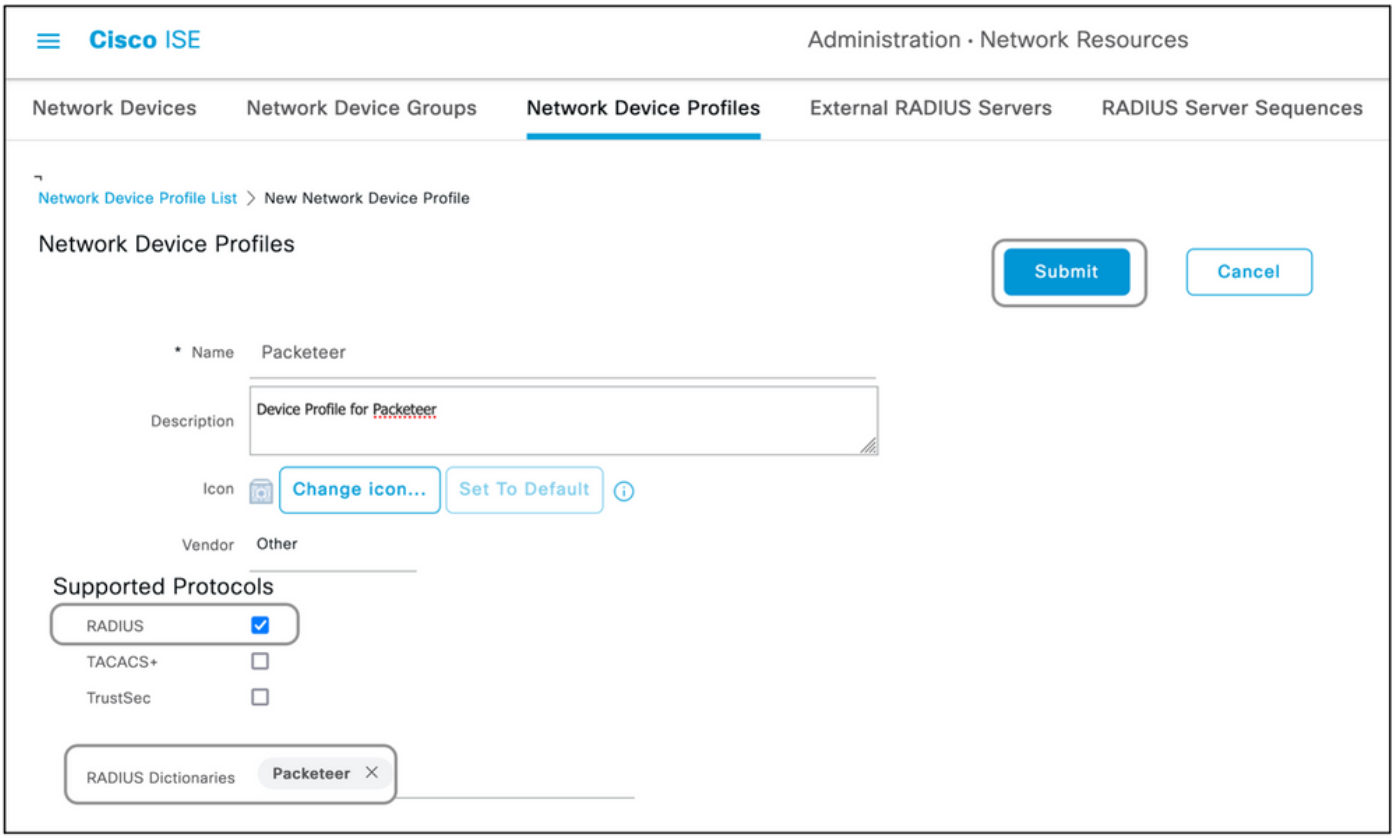
2. Geef een naam en controleer het vakje voor **RADIUS**.

3. Selecteer onder de **RADIUS-woordenboeken** het woordenboek dat in de vorige sectie is gemaakt.

4. Als er meerdere woordenboeken zijn gemaakt voor hetzelfde type apparaat, kunnen deze allemaal worden geselecteerd onder **RADIUS-woordenboeken**.

5. **Sla** het profiel op.






**Stap 3.** Voeg het netwerkapparaat toe aan ISE

Het netwerkapparaat waarop apparaatbeheer wordt bereikt, moet worden toegevoegd aan ISE, samen met een toets die op het netwerkapparaat is gedefinieerd. Op het netwerkapparaat wordt ISE toegevoegd als een AAA-radius met deze toets.

Dit is de procedure voor het toevoegen van een apparaat aan ISE:

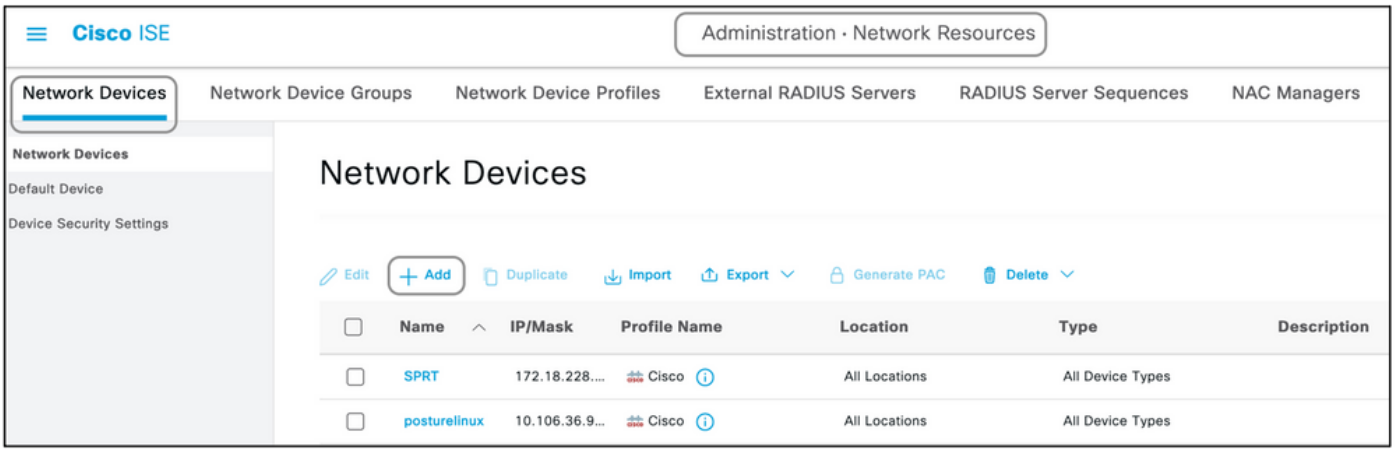
1. Naar navigeren **Beheer > Netwerkbronnen > Netwerkapparaten > Toevoegen.**

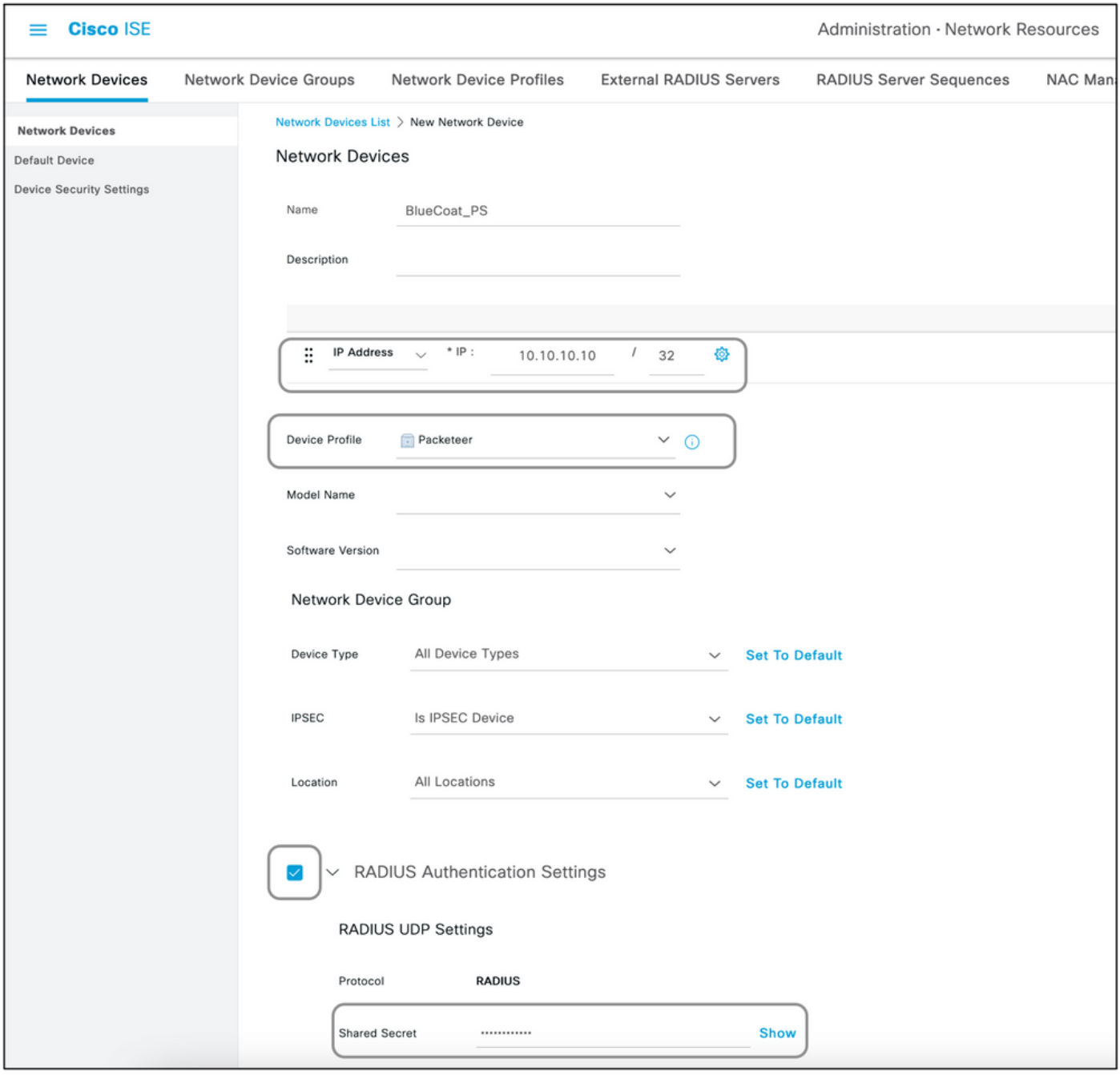
2. Geef een naam en het IP-adres op.

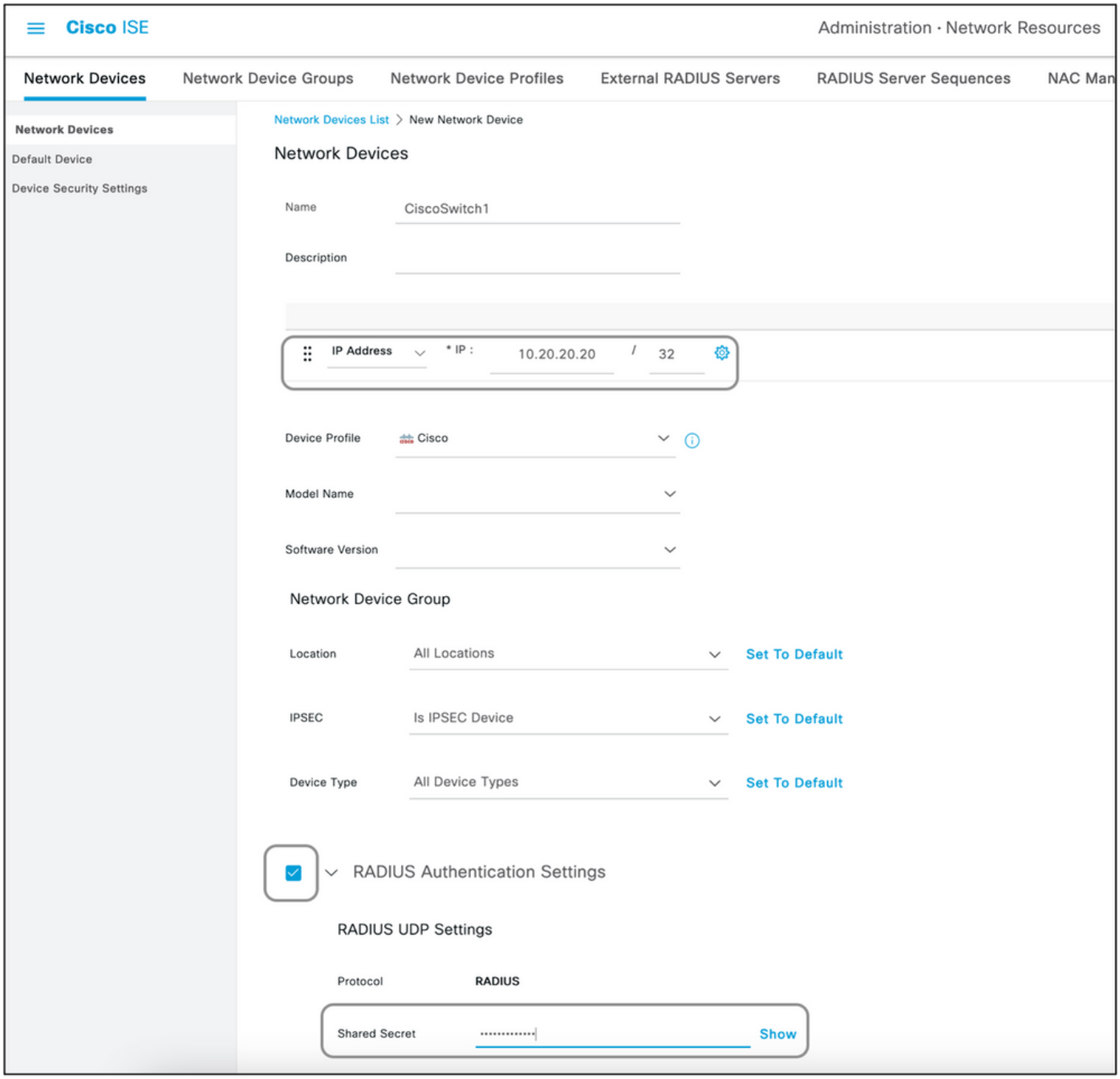
3. Het profiel van het apparaat kan uit de vervolgkeuzelijst worden gekozen om te worden gedefinieerd in de vorige sectie. Als er geen profiel is gemaakt, kan het standaard Cisco-profiel worden gebruikt zoals het is.

4. Controleer RADIUS-verificatie-instellingen.

5. Voer de **gedeelde geheime sleutel in** en **sla** het apparaat op.


Cisco ISE
Administration · Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
Network Devices
Default Device
Device Security Settings
Network Devices
Edit
Add
Duplicate
Import
Export
Generate PAC
Delete
Name
IP/Mask
Profile Name
Location
Type
Description
SPRT
172.18.228....
Cisco
All Locations
All Device Types
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
Network Devices
Default Device
Device Security Settings
Network Devices List > New Network Device
Network Devices
Name
BlueCoat_PS
Description
IP Address
* IP :
10.10.10.10
/
32
Device Profile
Packeteer
Model Name
Software Version
Network Device Group
Device Type
All Device Types
Set To Default
IPSEC
Is IPSEC Device
Set To Default
Location
All Locations
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
Shared Secret
Show



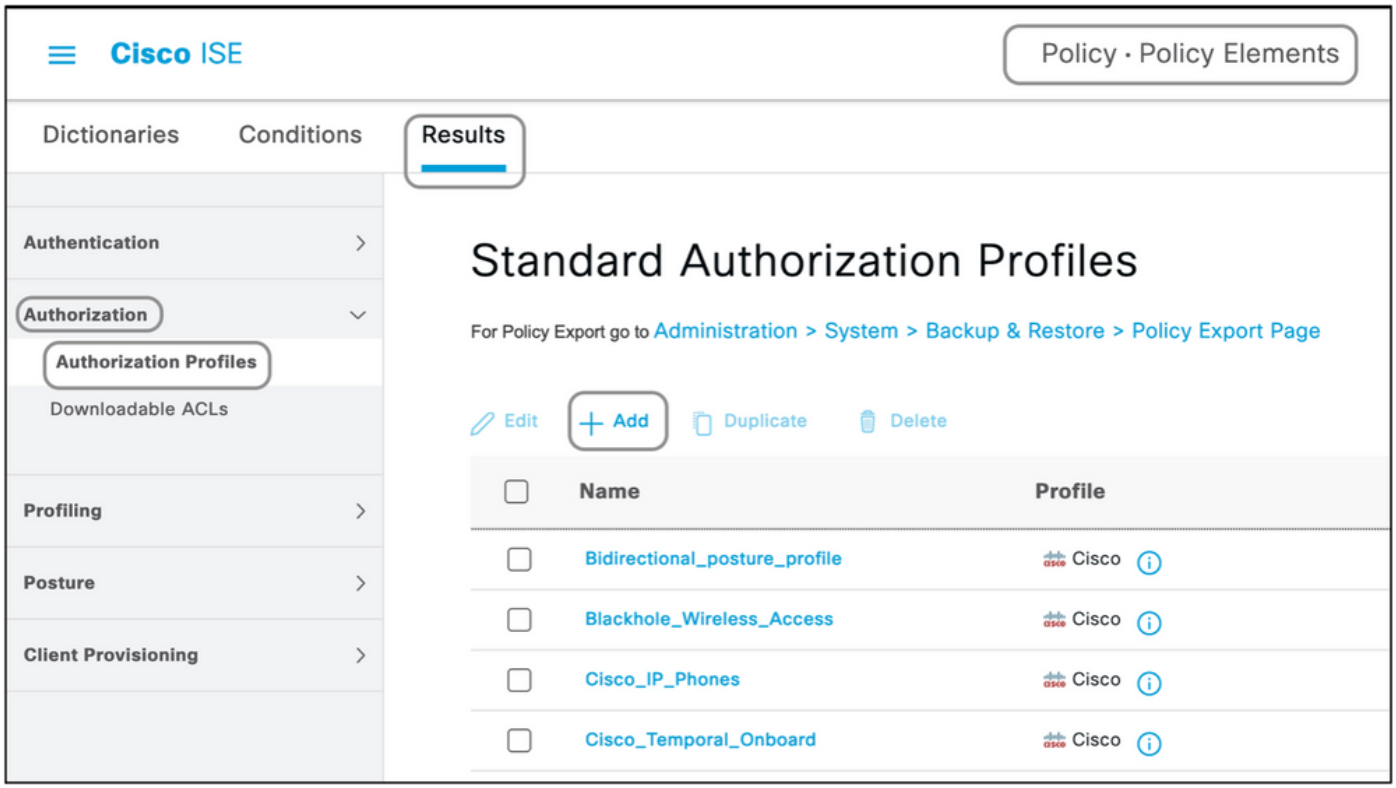

**Stap 4.** Autorisatieprofielen maken

Het eindresultaat dat van ISE wordt gedrukt als een access-acceptatie of access-reject, wordt gedefinieerd in een autorisatieprofiel. Met elk autorisatieprofiel kunt u extra kenmerken doordrukken die het netwerkapparaat verwacht.

Dit is de procedure voor het maken van een autorisatieprofiel:

1. Naar navigeren **Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen.**

2. Klik onder de **standaard autorisatieprofielen** op **Toevoegen**.




De typen profielen die kunnen worden toegevoegd zijn Access-Accept en Access-Reject.

### Een profiel voor toegangsgoedkeuring maken

Dit profiel wordt gebruikt voor een of andere vorm van toegang tot het netwerkapparaat. In dit profiel kunnen meerdere attributen tegelijk worden doorgegeven. Dit zijn de stappen:

1. Geef een zinnige naam en kies Toegangstype te zijn Access-Accepteren.

2. Kies het profiel van het netwerkapparaat dat in een van de vorige secties is gemaakt. Als er geen profiel is gemaakt, kan de standaard Cisco worden gebruikt.

3. Met verschillende types van gekozen profielen, beperkt de pagina hier de opties van configuratie.

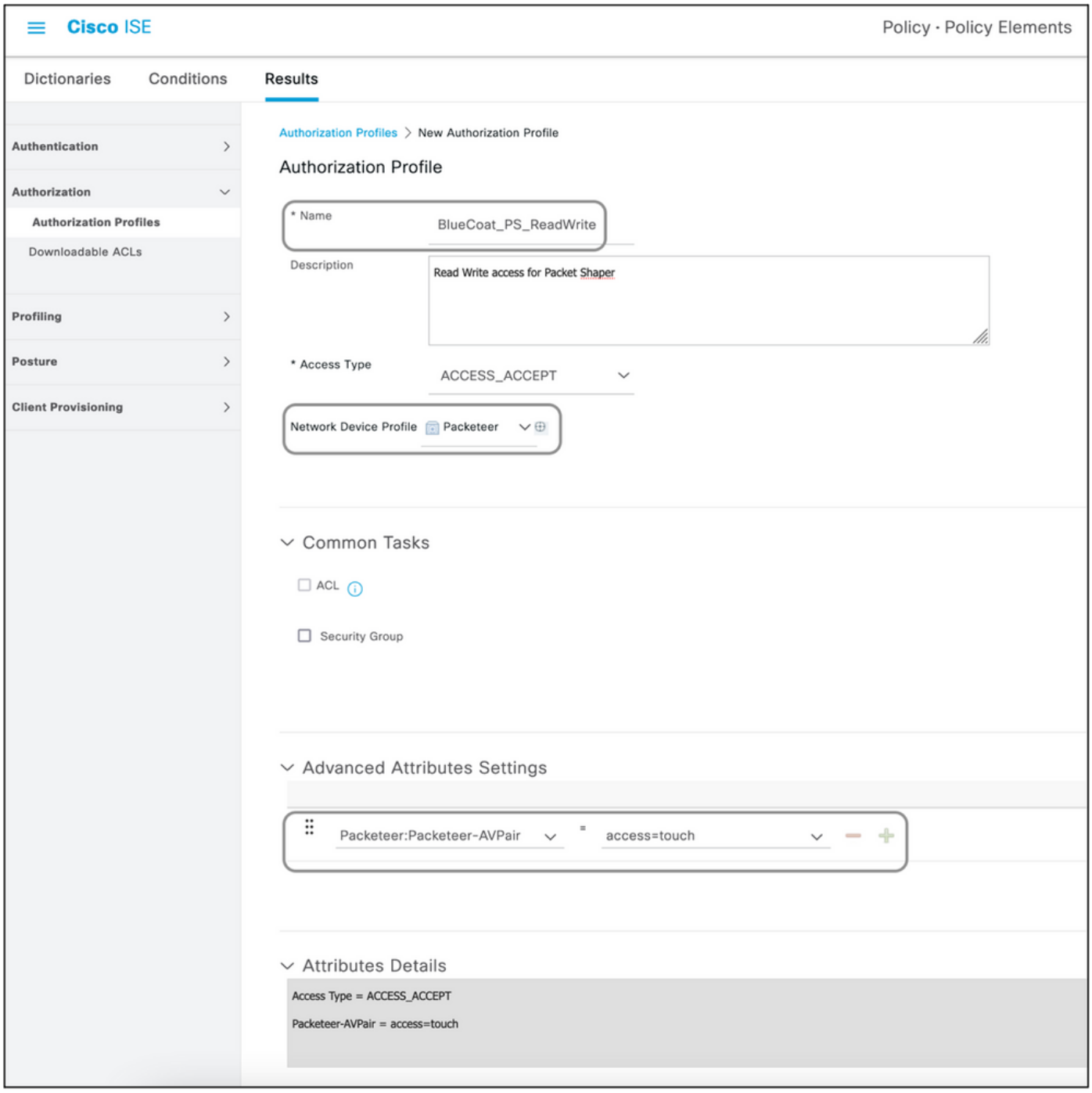
4. Kies onder **Instellingen geavanceerde kenmerken** het woordenboek en het toepasselijke kenmerk (LHS).

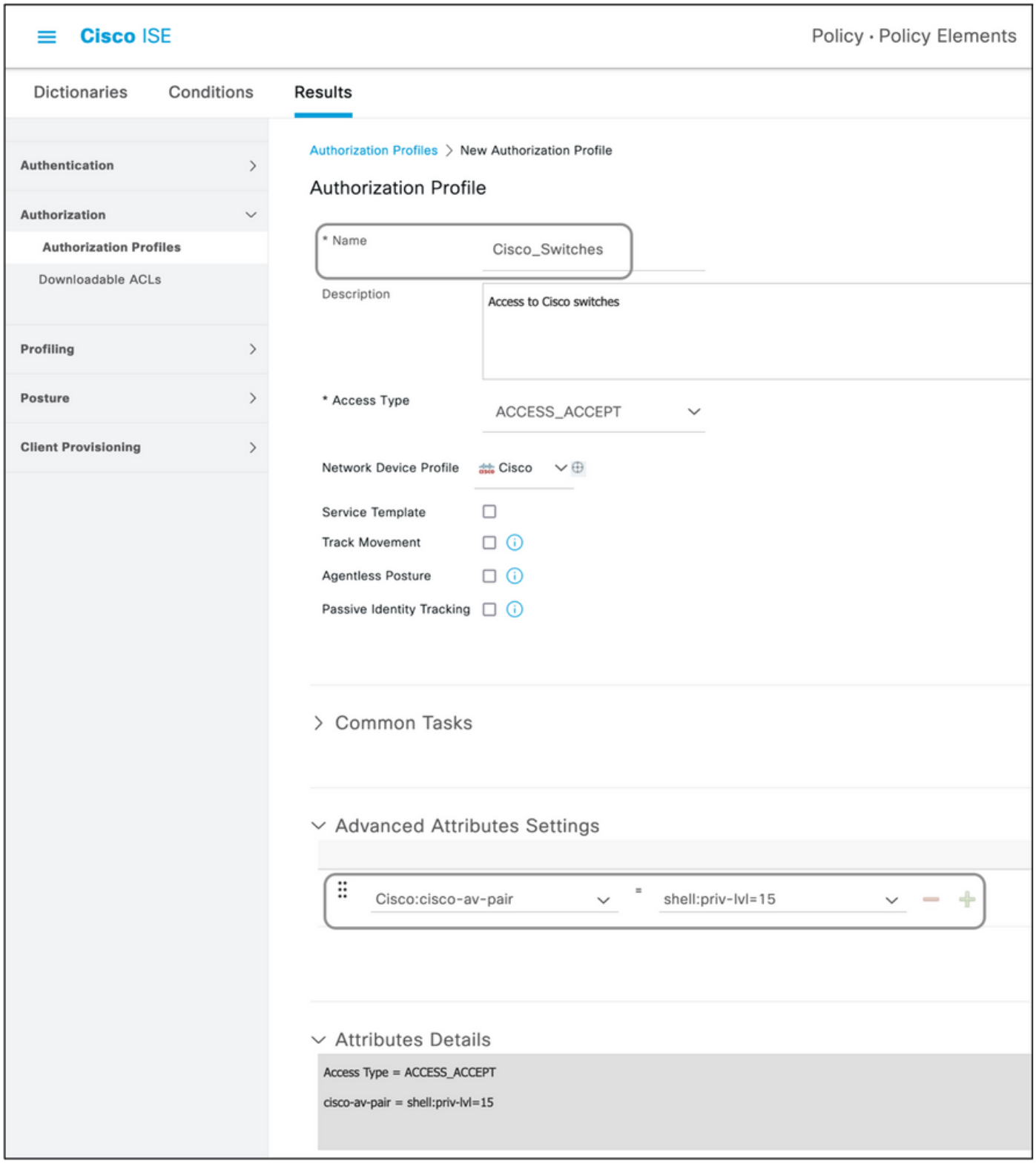
5. Ken een waarde (RHS) toe aan het kenmerk, hetzij vanaf de vervolgkeuzelijst indien beschikbaar, hetzij typ de verwachte waarde.

6. Als er meer attributen moeten worden verzonden als deel van hetzelfde resultaat, klik dan op het **+** pictogram en herhaal stap 4 en 5.

Meerdere autorisatieprofielen maken voor elk van de resultaten/rollen/autorisaties die ISE naar verwachting zal verzenden.

> **Opmerking**: De geconsolideerde eigenschappen kunnen worden geverifieerd onder het veld Eigenschappen en details.


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
BlueCoat_PS_ReadWrite
Description
Read Write access for Packet Shaper
* Access Type
ACCESS_ACCEPT
Network Device Profile
Packeteer
Common Tasks
ACL
Security Group
Advanced Attributes Settings
Packeteer:Packeteer-AVPair
=
access=touch
Attributes Details
Access Type = ACCESS_ACCEPT
Packeteer-AVPair = access=touch




### Een profiel voor toegangsweigering maken

Dit profiel wordt gebruikt om een afwijzing voor apparaatbeheer te verzenden, maar kan nog steeds worden gebruikt om attributen mee te sturen. Dit wordt gebruikt om een Radius Access-Reject-pakket te verzenden. De stappen blijven hetzelfde behalve stap één, waarbij access-reject moet worden gekozen in plaats van Access-Accept voor het access type.

**Stap 5.** Een beleidsset maken

Beleidssets op ISE worden van boven naar beneden beoordeeld en de eerste die voldoet aan de voorwaarde die in de beleidssets is ingesteld, is verantwoordelijk voor de reactie van de ISE op

het Radius Access-request-pakket dat door het netwerkapparaat wordt verzonden. Cisco raadt een unieke beleidsset aan voor elk type apparaat. De voorwaarde om de authenticatie en autorisatie van de gebruiker te evalueren gebeurt bij de evaluatie. Indien ISE externe identiteitsbronnen heeft, kan zij worden gebruikt voor het soort vergunning.

Op deze manier wordt een typische beleidsset gecreëerd:

1. Ga naar **Beleid > Beleidssets > +**.

2. De naam wijzigen **Nieuwe beleidsreeks 1.**

3. Stel de voorwaarde in op uniek voor dit apparaat.

4. Breid de **beleidsset uit**.

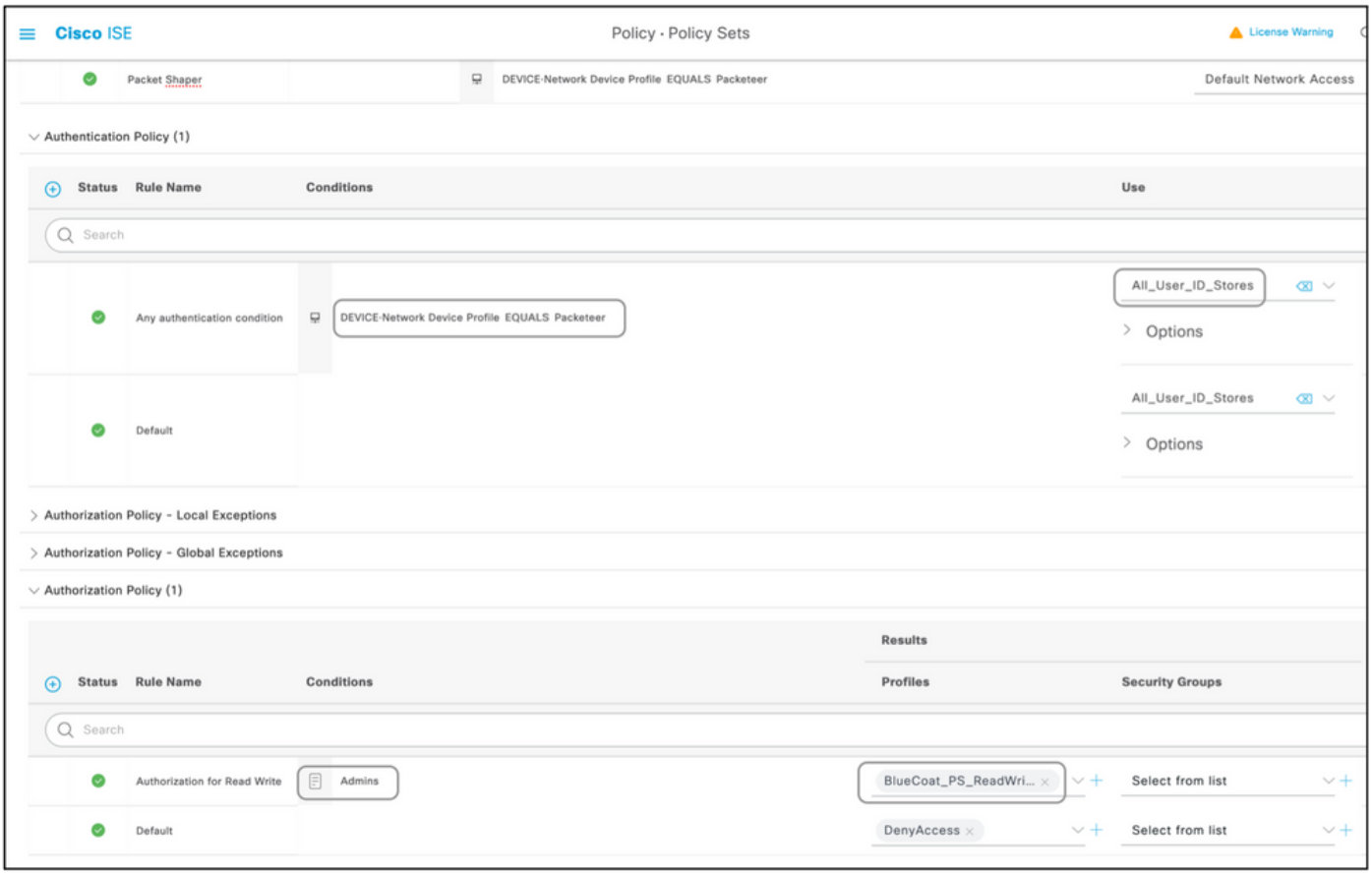
5. Breid het **verificatiebeleid uit** om een verificatieregel in te stellen. De externe bron of de interne gebruikers zijn voorbeelden die kunnen worden gebruikt als een opeenvolging van identiteitsbronnen waartegen ISE de gebruiker zou controleren.

6. Het verificatiebeleid is ingesteld. Het beleid kan op dit punt worden opgeslagen.

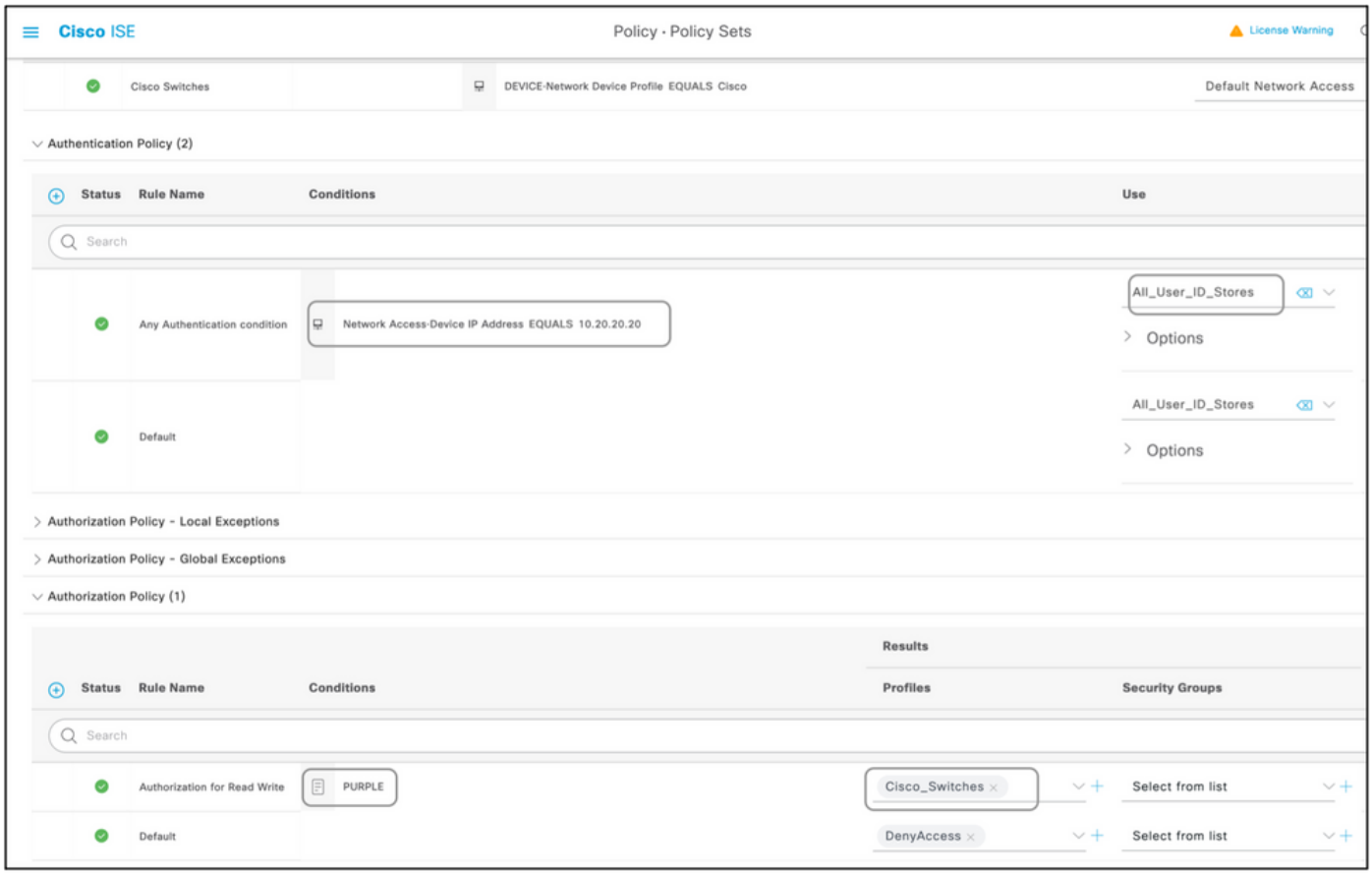
7. Breid het **beleid** van de **Vergunning uit** om de vergunningsvoorwaarden voor de gebruikers toe te voegen. Een voorbeeld is te controleren op een bepaalde AD-groep of een interne ISE-identiteitsgroep. Noem de regel ook.

8. Het resultaat voor de autorisatieregel kan uit de vervolgkeuzelijst worden geselecteerd.

9. Meerdere autorisatieregels maken voor verschillende soorten toegang die de verkoper ondersteunt.



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
Search
Any authentication condition
DEVICE-Network Device Profile EQUALS Packeteer
All_User_ID_Stores
Options
Default
All_User_ID_Stores
Options
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (1)
Results
Status
Rule Name
Conditions
Profiles
Security Groups
Search
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
Search
Cisco Switches
DEVICE-Network Device Profile EQUALS Cisco
Default Network Access
0




# Apparatenlijst

Om het even welk apparaat dat apparatenbeleid met Straal steunt kan op ISE met een paar wijzigingen aan alle die stappen worden toegevoegd in de vorige sectie worden vermeld. Vandaar dat dit document een lijst van apparaten heeft die met de informatie werken die in deze sectie wordt verstrekt. De lijst van eigenschappen en waarden in dit document is niet uitputtend noch gezaghebbend en kan op elk moment worden gewijzigd zonder dat dit document hoeft te worden bijgewerkt. Raadpleeg de websites van de leveranciers en de verkoopondersteuning voor validatie.

## Aggregation Services routers (ASR)

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, omdat Cisco AV-paren worden gebruikt die al op ISE aanwezig zijn.

Attributen: **cisco-av-pair**

Waarde(n): **shell:task="#<role-name>,<permissie>:<process>"**

Gebruik:Stel de waarden van <role-name>in op de naam van een rol die lokaal op de router is gedefinieerd. De rolhiërarchie kan in termen van een boom worden beschreven, waar de rol#rootis bovenaan de boom, en de rol#leafadd extra bevelen. Deze twee rollen kunnen worden gecombineerd en teruggegeven als:**shell:task="#root,#leaf"**.

De rechten kunnen ook op een individuele procesbasis worden teruggegeven, zodat een gebruiker lees-, schrijf-, en uitvoerende voorrechten voor bepaalde processen kan worden verleend. Om een gebruiker bijvoorbeeld lees- en schrijfrechten voor het BGP-proces te verlenen, stelt u de waarde in op:**shell:task="#root,rw:bgp"**. De volgorde van de eigenschappen is niet van

belang; het resultaat is hetzelfde of de waarde is ingesteld **op shell:task="#root,rw:bgp"**of **toshell:task="rw:bgp,#root"**.

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel.

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Cisco | Cisco Av-paar | String | shell:task="#root,#leaf,rwx:bgp,r:ospf" |

## Cisco Switches IOS® en Cisco IOS® XE

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, aangezien hiervoor RADIUS-kenmerken worden gebruikt die al op ISE aanwezig zijn.

Kenmerken(en):**cisco-av-paar**

Waarde(n):**shell:priv-lvl=<level>**

Gebruik:Stel de waarden van <level>in op de getallen die in wezen het aantal te verzenden rechten zijn. Typisch, als 15 wordt verzonden, betekent het read-write, als 7 wordt verzonden betekent het read-only.

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel.

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Cisco | Cisco Av-paar | String | schaal:priv-lvl=15 |

## BlueCoat Packet Shaper

Kenmerken(en):**Packet-AVPair**

Waarde(n):**access=<level>**

Gebruik:<level>is het niveau van toegang tot de subsidie. Aanraaktoegang staat gelijk aan lezen-schrijven, terwijl toegang tot de look gelijk is aan alleen-lezen.

Maak een woordenboek zoals in dit document met de volgende waarden:

- Naam: Verpakker
- Verkoper-ID: 2334
- Veldgrootte leverancier: 1
- Veldgrootte leverancier type: 1

Voer de gegevens van het kenmerk in:

- Kenmerk:Packet-AVPair
- Beschrijving: Gebruikt om het toegangsniveau te specificeren
- Kenmerk van leverancier: 1
- Richting: UIT

- Meervoudige toegestaan: Onjuist
- Tagging toestaan: ongecontroleerd
- Attribuuttype: String

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor alleen-lezen toegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-pakketter | Packet-AVPair | String | access=look |

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor lees-schrijftoegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-pakketter | Packet-AVPair | String | access=touch |

## BlueCoat Proxy-server (AV/SG)

Kenmerk(en): **Blauwe jas-Vergunning**

Waarde(n): **<level>**

Gebruik:<level>is het niveau van toegang tot de subsidie. 0 betekent geen toegang, 1 betekent alleen-lezen toegang en 2 betekent lezen-schrijven toegang. Het kenmerk Blue-Coat-Authorisation is degene die verantwoordelijk is voor het toegangsniveau.

Maak een woordenboek zoals in dit document met de volgende waarden:

- Naam: BlueCoat
- Verkoper-ID: 14501
- Veldgrootte leverancier: 1
- Veldgrootte leverancier type: 1

Voer de gegevens van het kenmerk in:

- Kenmerk: Blauwe jas-groep
- Kenmerk van leverancier: 1
- Richting: BEIDE
- Meervoudige toegestaan: Onjuist
- Tagging toestaan: ongecontroleerd
- Attribuuttype: Unsigned Integer 32 (UINT32)

Voer de gegevens van het tweede kenmerk in:

- Attribuut: Blue-Coat-Authorisation
- Beschrijving: Gebruikt om het toegangsniveau te specificeren
- Kenmerk van leverancier: 2
- Richting: BEIDE
- Meervoudige toegestaan: Onjuist
- Tagging toestaan: ongecontroleerd
- Attribuuttype: Unsigned Integer 32 (UINT32)

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor geen toegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-BlueCoat | Blauwe jas-groep | UINT32 | 0 |

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor alleen-lezen toegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-BlueCoat | Blauwe jas-groep | UINT32 | 1 |

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor lees-schrijftoegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-BlueCoat | Blauwe jas-groep | UINT32 | 2 |

## Brocade-Switches

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, aangezien hiervoor RADIUS-kenmerken worden gebruikt die al op ISE aanwezig zijn.

Attribuut(en): **Tunnel-Private-Group-ID**

Waarde(n):**U:<VLAN1>; T:<VLAN2>**

Gebruik:Stel <VLAN1>in op de waarde van de gegevens VLAN. Stel <VLAN2>in op de waarde van de spraak-VLAN. In dit voorbeeld, zijn de gegevens VLAN VLAN 10, en de stem VLAN is VLAN 21.

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel.

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-IETF | Tunnel-Private-Group-ID | Tekenreeks | U:10;T:21 |

## infoblox

Kenmerk(en):**Infoblox-Group-Info**

Waarde(n):**<group-name>**

Gebruik:<group-name>is de naam van de groep met de rechten die de gebruiker heeft verkregen. Deze groep moet op het Infoblox apparaat worden geconfigureerd. In dit configuratievoorbeeld is de groepsnaam MyGroup.

Maak een woordenboek zoals in dit document met de volgende waarden:

- Naam: Infoblox
- Verkoper-ID: 7779
- Veldgrootte leverancier: 1
- Veldgrootte leverancier type: 1

Voer de gegevens van het kenmerk in:

- Attribuut:Infoblox-Group-Info
- Kenmerk van leverancier: 009

- Richting: UIT
- Meervoudige toegestaan: Onjuist
- Tagging toestaan: ongecontroleerd
- Attribuuttype: String

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel.

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-infoblox | Infoblox-Group-Info | String | Mijn groep |

## Cisco Firepower Management Center

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, aangezien hiervoor RADIUS-kenmerken worden gebruikt die al op ISE aanwezig zijn.

Kenmerken(en):**cisco-av-paar**

Waarde(n): **class-[25]=<role>**

Gebruik:Stel de waarden van <rol>in op de namen van de rollen die lokaal op het VCC zijn gedefinieerd. Creëer meerdere rollen zoals beheer en alleen-lezen gebruiker op het VCC en wijs de waarden toe aan de eigenschappen op ISE die ook door het VCC moeten worden ontvangen.

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel.

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Cisco | Cisco Av-paar | String | Class-[25]=NetAdmins |

## Nexus Switches

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, aangezien hiervoor RADIUS-kenmerken worden gebruikt die al op ISE aanwezig zijn.

Kenmerken(en):**cisco-av-paar**

Waarde(n):**shell:rollen="<role1> <role2>"**

Gebruik:Stel de waarden van <role1>en<role2>in op de namen van de rollen die lokaal op de switch zijn gedefinieerd. Wanneer meerdere rollen worden gemaakt, scheidt u deze van een spatiekarakter. Wanneer meerdere rollen worden doorgegeven van de AAA-server naar de Nexus switch, is het resultaat dat de gebruiker toegang heeft tot opdrachten die worden gedefinieerd door de combinatie van alle drie de rollen.

De ingebouwde rollen worden gedefinieerd inConfigure User Accounts en RBAC.

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel.

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Cisco | Cisco Av-paar | String | shell:rollen="netwerk-admin vdc-admin vdc-operator |

## Draadloze LAN-controller (WLC)

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, aangezien hiervoor RADIUS-kenmerken worden gebruikt die al op ISE aanwezig zijn.

Kenmerk(en):**servicetype**

Waarde(n): **Administratief (6) / NAS-prompt (7)**

Gebruik:Om de gebruiker lees-/schrijftoegang te verlenen tot de draadloze LAN-controller (WLC), moet de waarde Administratief zijn; voor alleen-lezen toegang moet de waarde NAS-prompt zijn.

Zie voor meer informatie RADIUS-serververificatie van beheergebruikers op configuratievoorbeeld van draadloze LAN-controller (WLC)

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor alleen-lezen toegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-IETF | Service-type | opsomming | NAS-prompt |

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor lees-schrijftoegang).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-IETF | Service-type | opsomming | Administratief |

## Data Center Network Manager (DCNM)

DCNM moet opnieuw worden gestart nadat de verificatiemethode is gewijzigd. Anders kan het netwerk-exploitant privilege toekennen in plaats van netwerk-admin.

Hiervoor hoeven geen afzonderlijke woordenboeken en VSA's te worden gemaakt, aangezien hiervoor RADIUS-kenmerken worden gebruikt die al op ISE aanwezig zijn.

Kenmerken(en):**cisco-av-paar**

Waarde(n):**shell:rollen=<role>**

| DCNM-rol | RADIUS Cisco-AV-paar |
|---|---|
| Gebruiker | shell:rollen = "netwerkexploitant" |
| Beheerder | shell:rollen = "netwerk-admin" |

## Audiocodes

Attributen: **ACL-autorisatieniveau**

Waarde(n): **ACL-autorisatieniveau = "<integer>"**

Gebruik:<integer>is het niveau van toegang tot de subsidie. Een waarde van ACL-Auth-Level attribuut met naam ACL-Auth-UserLevel van 50 voor de gebruiker, een waarde van ACL-Auth-Level attribuut met naam ACL-Auth-AdminLevel van waarde100 voor admin en waarde van ACL-Auth-Level met naam ACL-Auth-SecurityAdminLevel van waarde 200 voor security admin. De namen kunnen worden overgeslagen en de waarden voor eigenschappen kunnen direct worden

gegeven als waarde voor het autorisatieprofiel geavanceerde AV-paar.

Maak een woordenboek zoals in dit document met de volgende waarden:

- Naam: AudioCodes
- Verkoper-ID: 5003
- Veldgrootte leverancier: 1
- Veldgrootte leverancier type: 1

Voer de gegevens van het kenmerk in:

- Kenmerk: ACL-autorisatieniveau
- Beschrijving: Gebruikt om het toegangsniveau te specificeren
- Kenmerk van de verkoper: 35
- Richting: UIT
- Meervoudige toegestaan: Onjuist
- Tagging toestaan: ongecontroleerd
- Attribuuttype: Integer

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor gebruiker).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Audio-codes | ACL-autorisatieniveau | geheel | 50 |

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor admin).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Audio-codes | ACL-autorisatieniveau | geheel | 100 |

Voorbeeld: Voeg het kenmerk toe aan een autorisatieprofiel (voor beveiligingsbeheerder).

| Type woordenboek | RADIUS-kenmerk | Type kenmerk | Waarde kenmerk |
|---|---|---|---|
| RADIUS-Audio-codes | ACL-autorisatieniveau | geheel | 200 |

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.