& Configureer probleemoplossing in downloadbare ACL's op Catalyst 9800

Inhoud

Inleiding

Dit document beschrijft hoe u downloadbare ACL's (dACL's) op Catalyst 9800 draadloze LAN-controller (WLC) kunt configureren en problemen kunt oplossen.

Achtergrondinformatie

ACL's worden al vele jaren ondersteund in Cisco IOS® en IOS XE® switches. Een dACL verwijst naar het feit dat het netwerkapparaat dynamisch de ACL-vermeldingen van de RADIUS-server

downloadt wanneer verificatie plaatsvindt, in plaats van een lokale kopie van de ACL te hebben en gewoon de ACL-naam te krijgen. Er is een completer voorbeeld van Cisco ISE-configuratie beschikbaar. Dit document concentreert zich op Cisco Catalyst 9800 die dACL's voor centrale switching sinds de 17.10-release ondersteunt.

Voorwaarden

Het idee achter dit document is het gebruik van dACL's op Catalyst 9800 aan te tonen door middel van een eenvoudig voorbeeld van de SSID-configuratie, dat laat zien hoe deze volledig aanpasbaar kunnen zijn.

Op Catalyst 9800 draadloze controller zijn downloadbare ACL's

- Ondersteund vanaf de Cisco IOS XE Dublin 17.10.1 release.
- Alleen ondersteund voor gecentraliseerde controller met Local Mode Access points (of Flexconnect Central-switching). FlexConnect Local Switching ondersteunt geen dACL.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Catalyst draadloze 9800 configuratiemodel.
- Cisco IP-toegangscontrolelijsten (ACL's).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9800-CL (v. Dublin 17.12.03).
- ISE (v. 3.2).

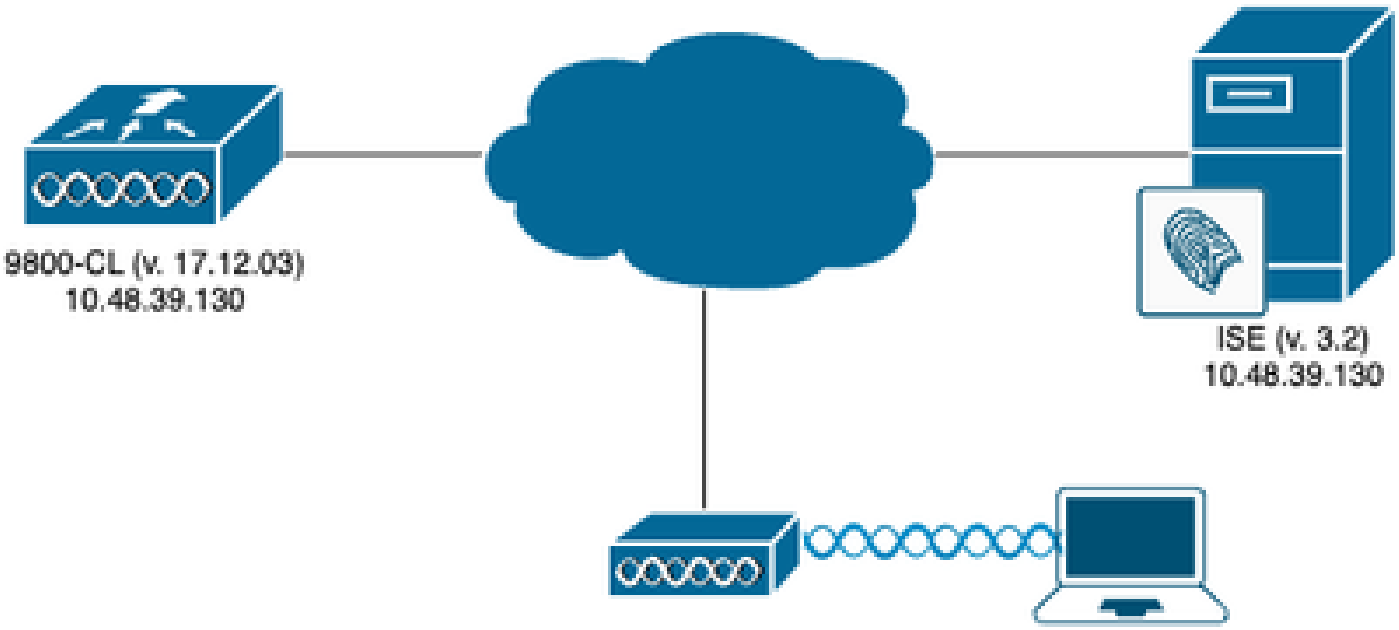
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Door deze configuratiegids, zelfs als de methodes verschillend zijn (bijvoorbeeld WLAN-verificatie, beleidsconfiguratie, enzovoort), is het eindresultaat hetzelfde. In het hier weergegeven scenario worden twee gebruikersidentiteiten gedefinieerd als GEBRUIKER1 en GEBRUIKER2. Beiden krijgen toegang tot het draadloze netwerk. Aan elk van hen wordt, respectievelijk, ACL_USER1 en ACL_USER2 toegewezen die dACLs zijn die door Catalyst 9800 van ISE worden gedownload.

DACL's met 802.1x SSID's gebruiken

Netwerkdiagram



WLC-configuratie

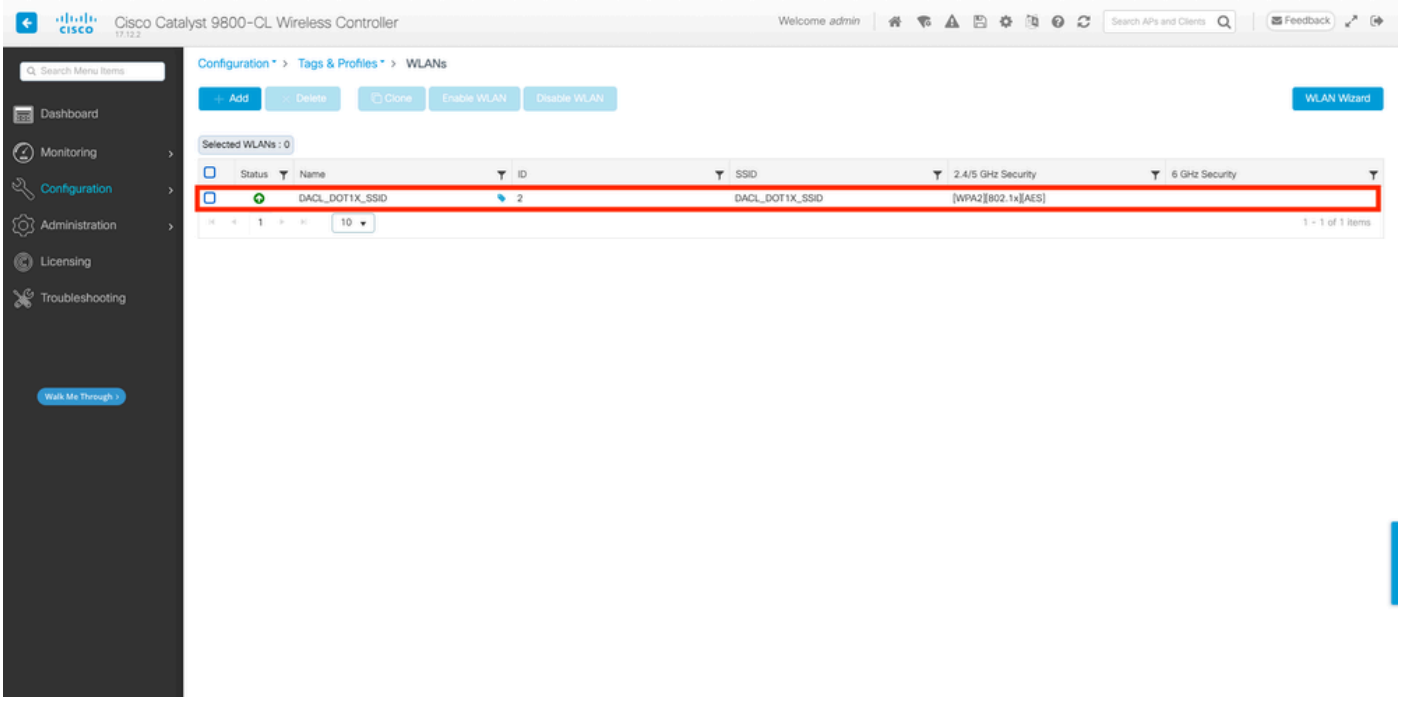
Raadpleeg voor meer informatie over de configuratie en probleemoplossing van 802.1x SID's op Catalyst 9800 de configuratiehandleiding Configure 802.1X verificatie op Catalyst 9800 Wireless Controller Series.

Stap 1. Configureer de SSID.

Configureer een 802.1x geverifieerde SSID met ISE als RADIUS-server. In dit document is de SSID aangeduid als "DACL_DOT1X_SSID".

Via de GUI:

Navigeer naar Configuration > Tags & profielen > WLAN en maak een WLAN dat vergelijkbaar is met de hier weergegeven WLAN:



Van de CLI:

```
WLC#configure terminal
WLC(config)#wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
WLC(config-wlan)#security dot1x authentication-list DOT1X
WLC(config-wlan)#no shutdown
```

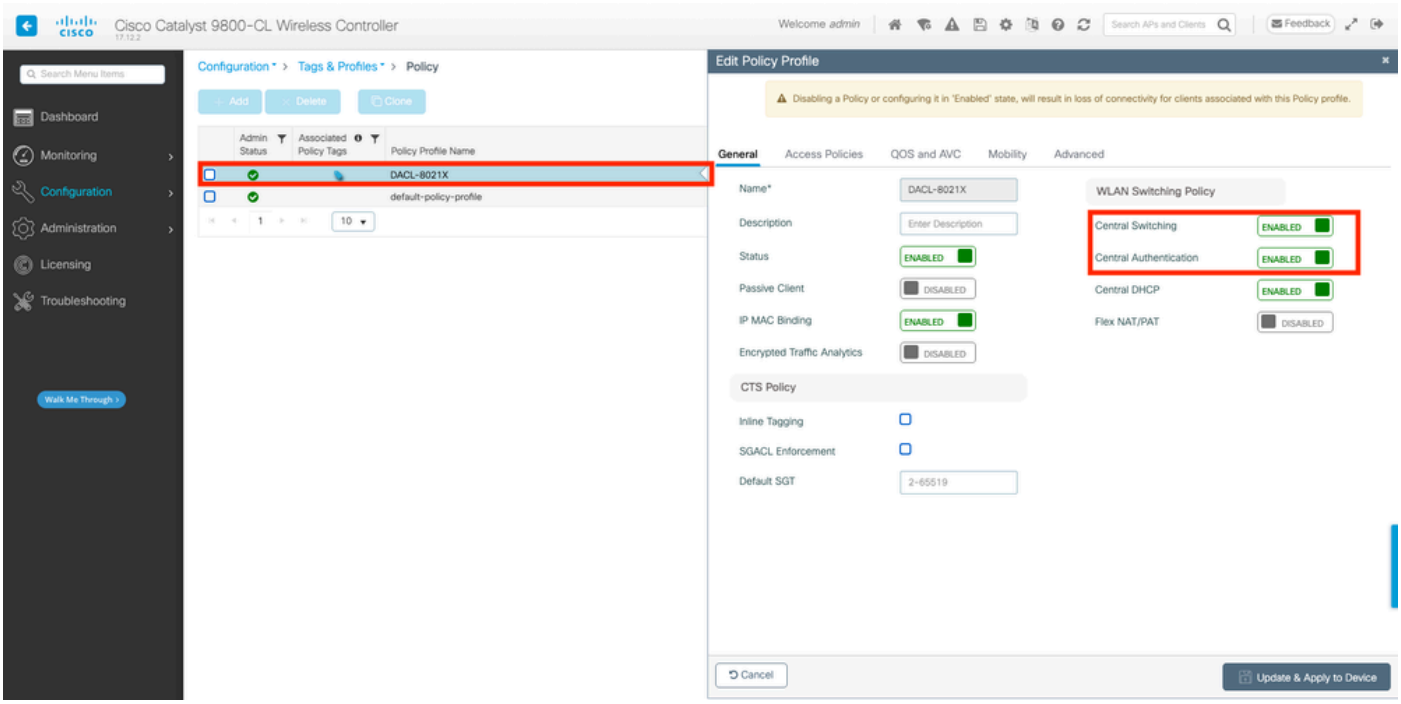
Stap 2. Configureer het beleidsprofiel.

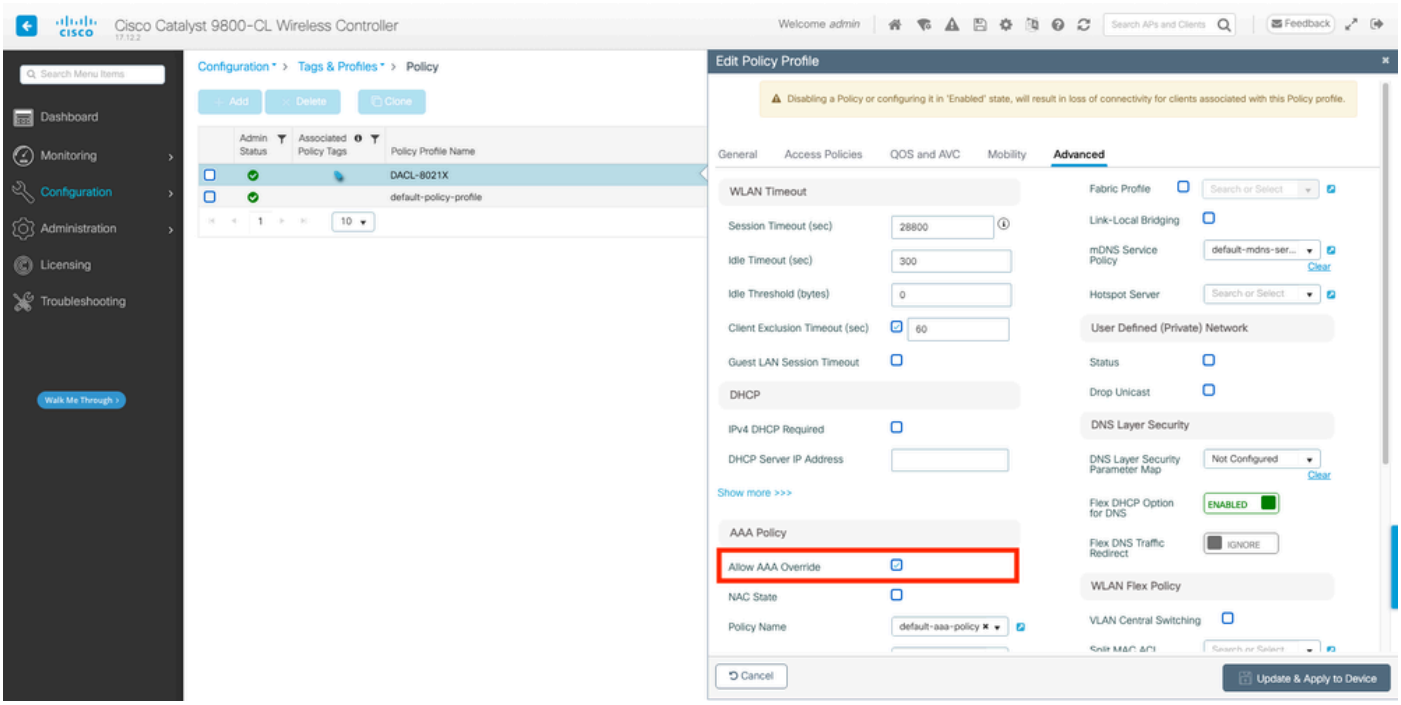
Configureer het beleidsprofiel dat samen met de hierboven gedefinieerde SSID wordt gebruikt. Zorg er in dit beleidsprofiel voor dat AAA Override is geconfigureerd vanuit het tabblad "Geavanceerd", zoals wordt weergegeven in de screenshot. In dit document is het gebruikte beleidsprofiel "DACL-8021X".

Zoals in het gedeelte Voorwaarden wordt vermeld, worden dACL's alleen ondersteund voor centrale switching/verificatie-implementaties. Zorg ervoor dat het beleidsprofiel op die manier is geconfigureerd.

Via de GUI:

Navigeer naar Configuratie > Tags & profielen > Beleid, selecteer het gebruikte beleidsprofiel en configureer het zoals getoond.





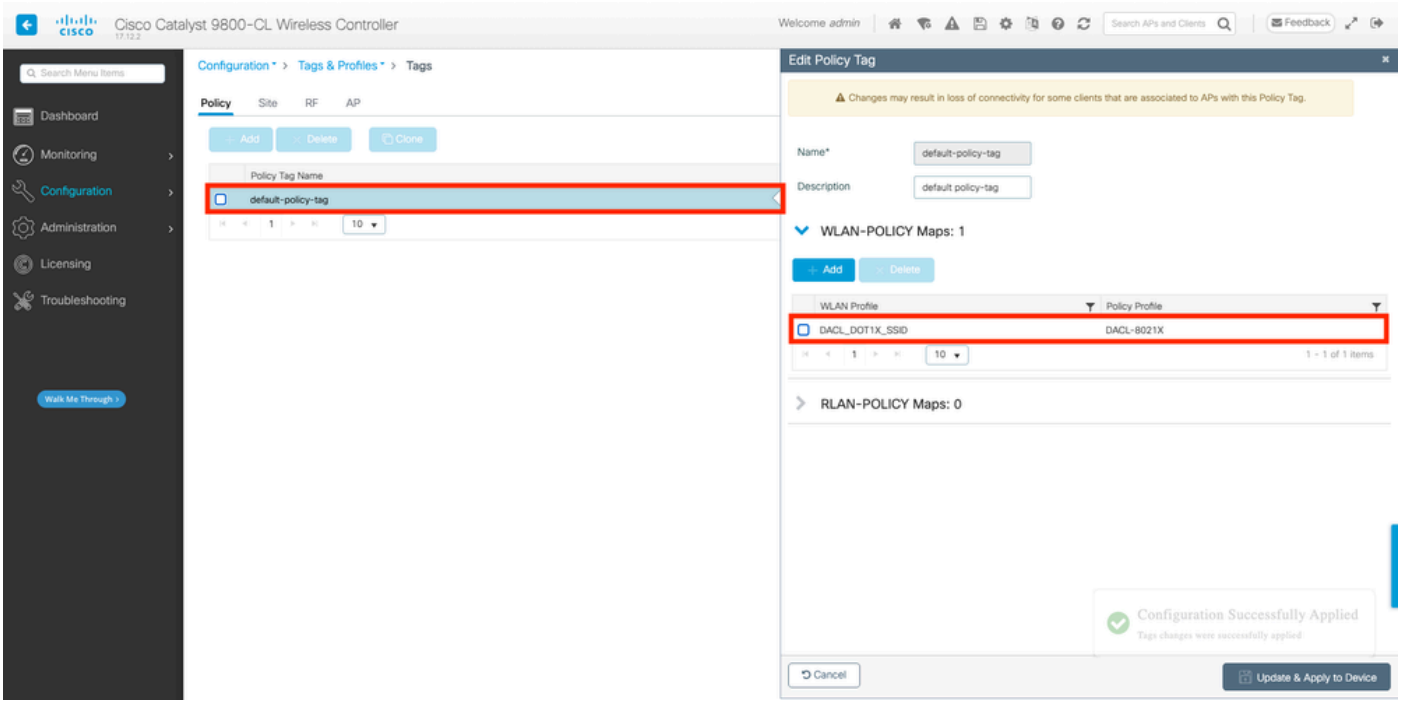
Van de CLI:

```
WLC#configure terminal
WLC(config)#wireless profile policy DACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown
```

Stap 3. Wijs het beleidsprofiel en de SSID toe aan de gebruikte beleidstag.

Via de GUI:

Navigeren naar Configuratie > Tags & profielen > Tags. Maak (of selecteer) de gebruikte tag op het tabblad Policy en wijs er het WLAN- en beleidsprofiel aan toe dat tijdens stap 1-2 is gedefinieerd.



Van de CLI:

```
WLC#configure terminal
WLC(config)#wireless tag policy default-policy-tag
WLC(config-policy-tag)#description "default policy-tag"
WLC(config-policy-tag)#wlan DACL_DOT1X_SSID policy DACL-8021X
```

Stap 4. Sta leverancierspecifieke kenmerken toe.

Downloadbare ACL's worden via leverancierspecifieke kenmerken (VSA) doorgegeven in de RADIUS-uitwisseling tussen ISE en WLC. De ondersteuning van deze eigenschappen kan worden ingeschakeld op de WLC, met behulp van deze CLI opdracht.

Van de CLI:

```
WLC#configure terminal
WLC(config)#radius-server vsa send authentication
```

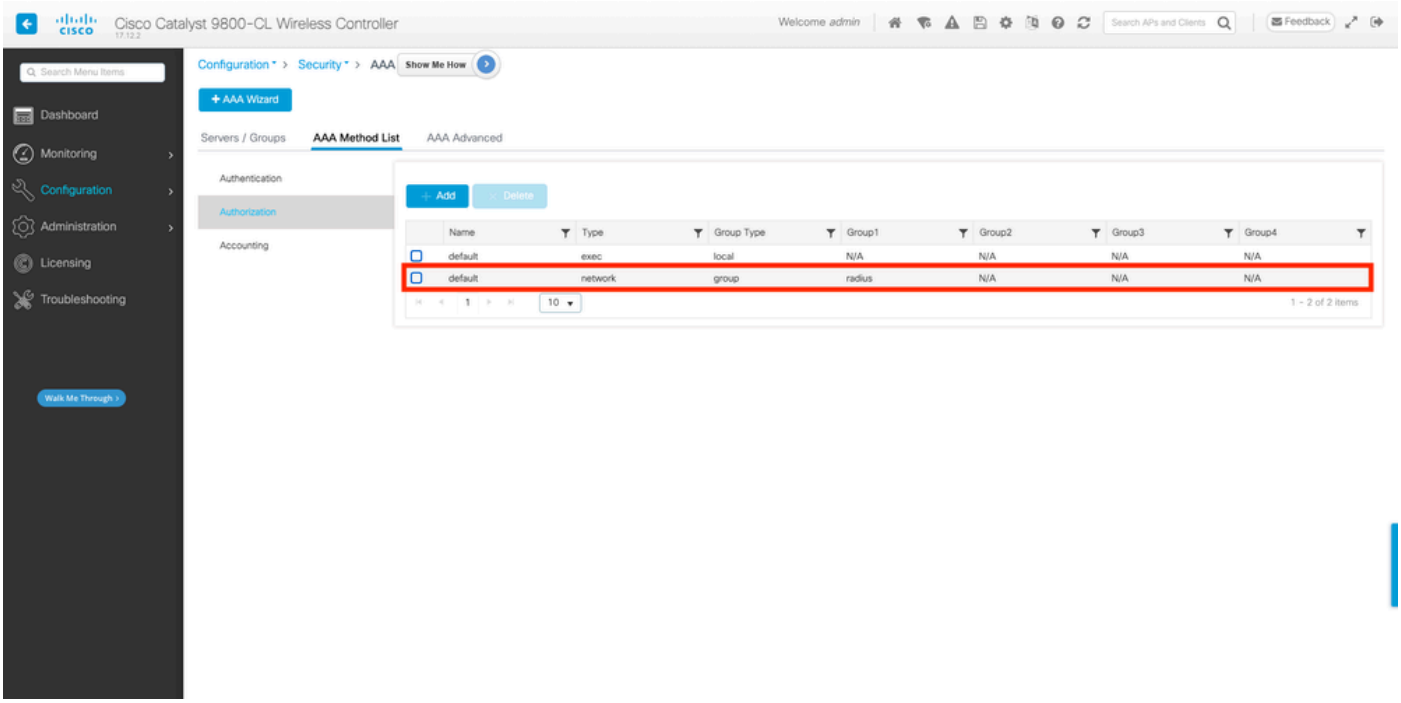
Stap 5. Standaardautorisatielijst configureren.

Wanneer het werken met dACL, moet de netwerkvergunning door RADIUS voor WLC worden afgedwongen om het even welke gebruiker te machtigen die aan 802.1x SSID wordt gevormd voor authentiek verklaart. Niet alleen de verificatie, maar ook de autorisatiefase wordt hier aan de kant van de RADIUS-server afgehandeld. Daarom is in dit geval een toelatingslijst vereist.

Zorg ervoor dat de standaardmethode voor netwerkautorisatie deel uitmaakt van de 9800-configuratie.

Via de GUI:

Navigeer naar Configuratie > Beveiliging > AAA en creëer vanuit het tabblad AAA-methodelijst > Autorisatie een autorisatiemethode die vergelijkbaar is met de methode die wordt getoond.



Van de CLI:

```
WLC#configure terminal
WLC(config)#aaa authorization network default group radius
```

ISE-configuratie

Wanneer het uitvoeren van dACLs in draadloos milieu met ISE, zijn twee gemeenschappelijke configuraties mogelijk, om te weten:

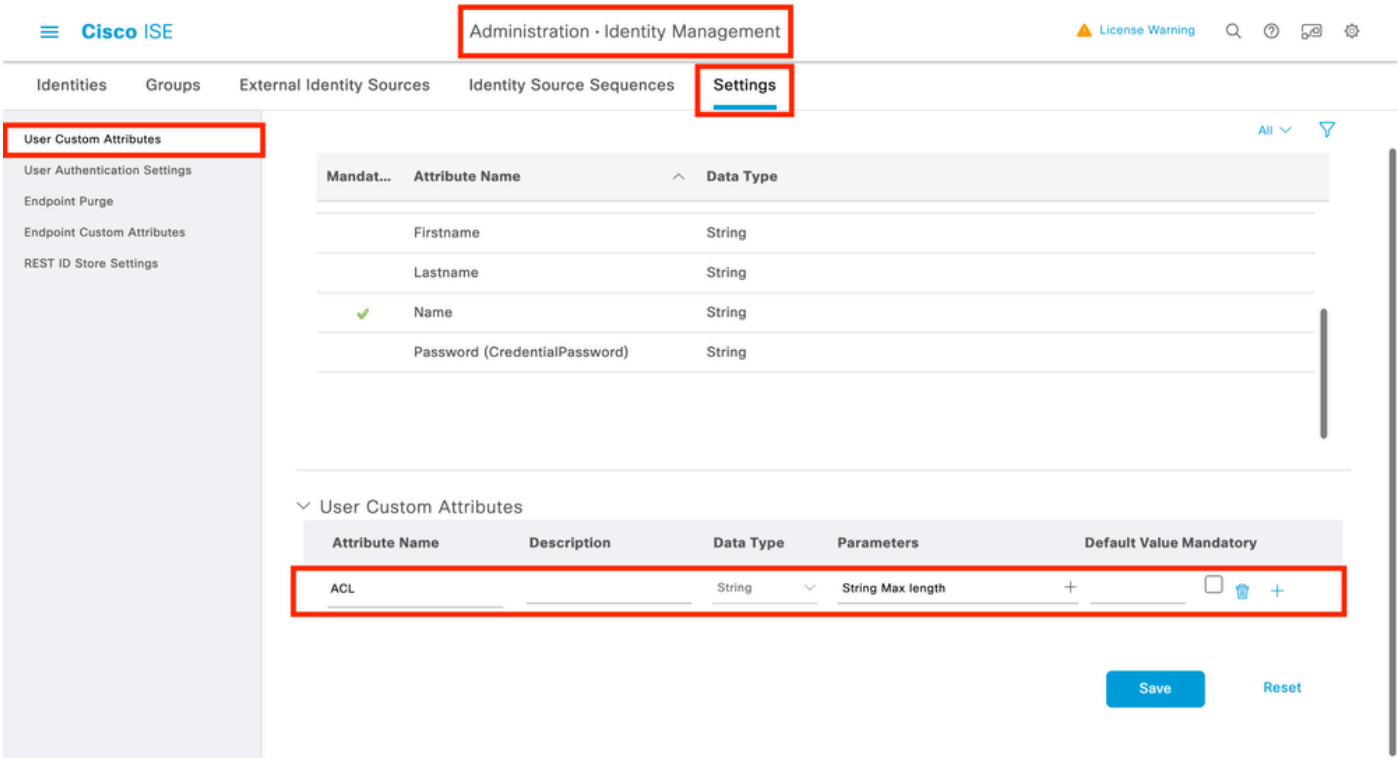
1. Configuratie per gebruiker van dACL. Met dit, heeft elke bepaalde identiteit een dACL toegewezen dankzij een gebied van de douaneidentiteit.
2. Configuratie van dACL per resultaat. Terwijl het kiezen voor deze methode, wordt een

bepaalde dACL toegewezen aan een gebruiker die op het vergunningsbeleid wordt gebaseerd het op de gebruikte beleidsreeks aanpaste.

dACL's per gebruiker

Stap 1. Een aangepast dACL-gebruikerskenmerk definiëren

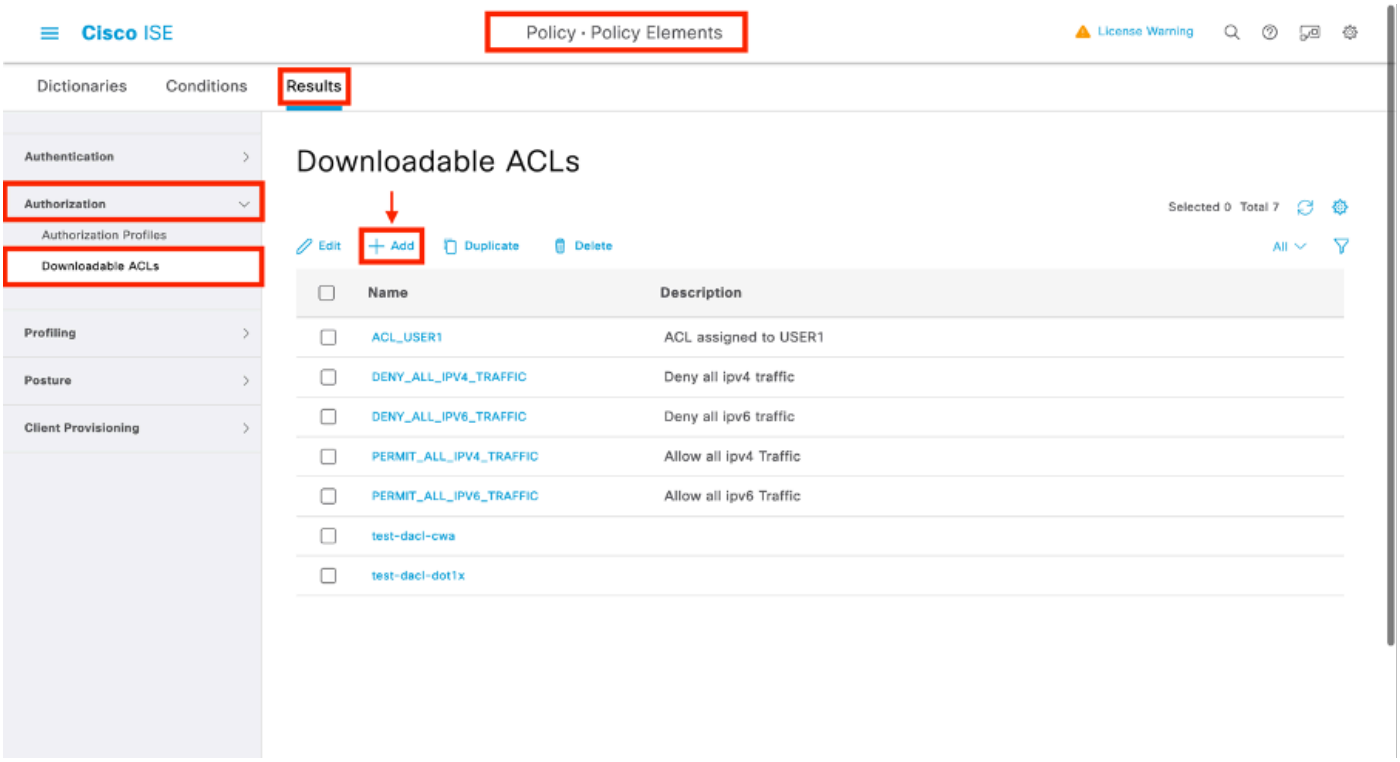
Om dACL aan een gebruikersidentiteit te kunnen toewijzen, moet eerst dit veld op de gecreëerde identiteit configureerbaar zijn. Standaard wordt op ISE het veld "ACL" niet gedefinieerd voor een nieuwe identiteit die wordt gemaakt. Om dit te overwinnen, kan men de "Custom User Attribute" gebruiken en een nieuw configuratieveld definiëren. Ga hiervoor naar Beheer > Identity Management > Instellingen > Aangepaste gebruikerskenmerken. Gebruik de knop "+" om een nieuw kenmerk toe te voegen dat gelijk is aan het kenmerk dat wordt weergegeven. In dit voorbeeld is de naam van het aangepaste kenmerk ACL.



Als dit is ingesteld, gebruikt u de knop "Opslaan" om de wijzigingen op te slaan.

Stap 2. Configureer de dACL

Navigeer naar Beleid > Beleidselementen > Resultaten > Autorisatie > Downloadbare ACL's om dACL op ISE te zien en te definiëren. Gebruik de knop "Toevoegen" om een nieuwe te maken.



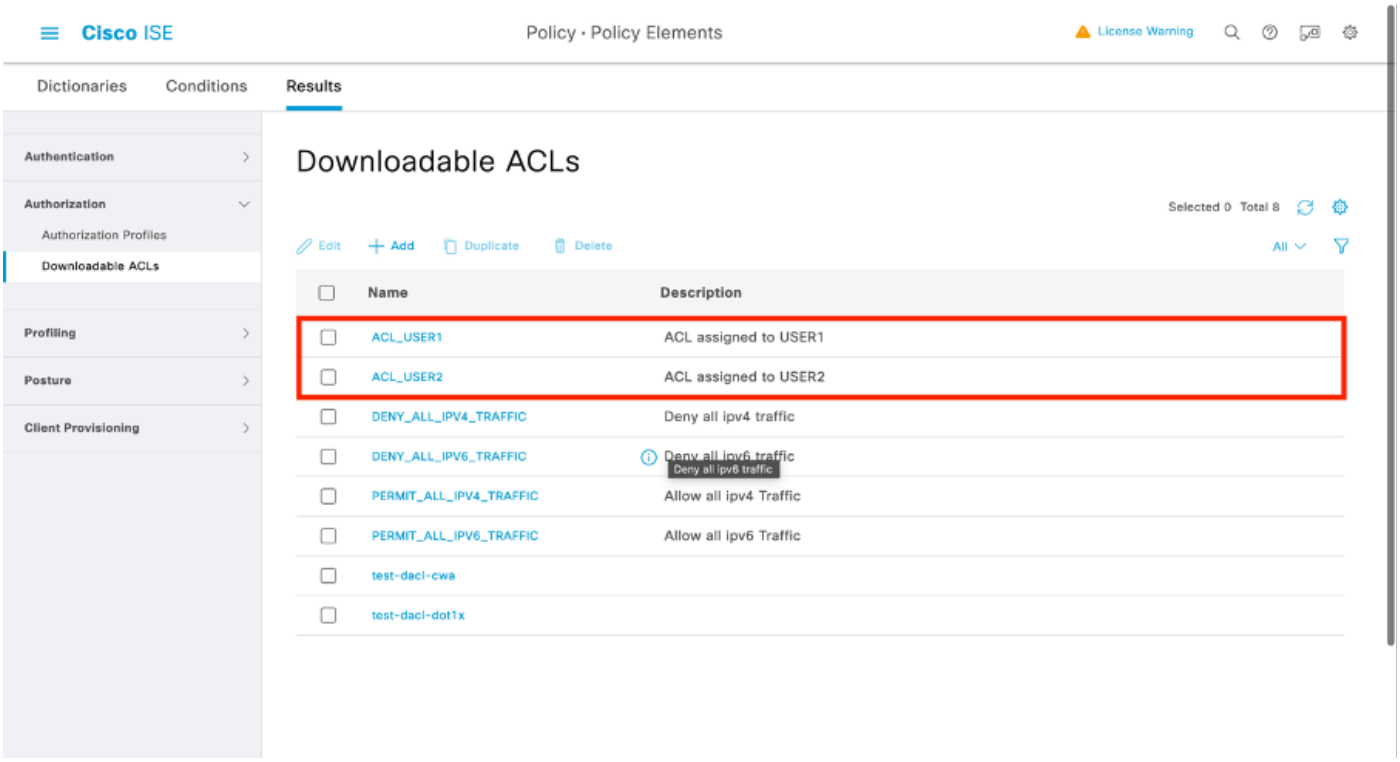
Hiermee opent u het configuratieformulier "Nieuwe downloadbare ACL". Configureer de volgende velden:

- Naam: de naam van de gedefinieerde dACL.
- Beschrijving (optioneel): een korte beschrijving over het gebruik van de gemaakte dACL.
- IP-versie: de IP-protocolversie die in de gedefinieerde dACL wordt gebruikt (versie 4, 6 of beide).
- DACL-inhoud: de inhoud van de dACL, zoals per Cisco IOS XE ACL-syntaxis

In dit document is de gebruikte dACL "ACL_USER1" en deze dACL staat elk verkeer toe behalve het verkeer dat bestemd is voor 10.48.39.186 en 10.48.39.13.

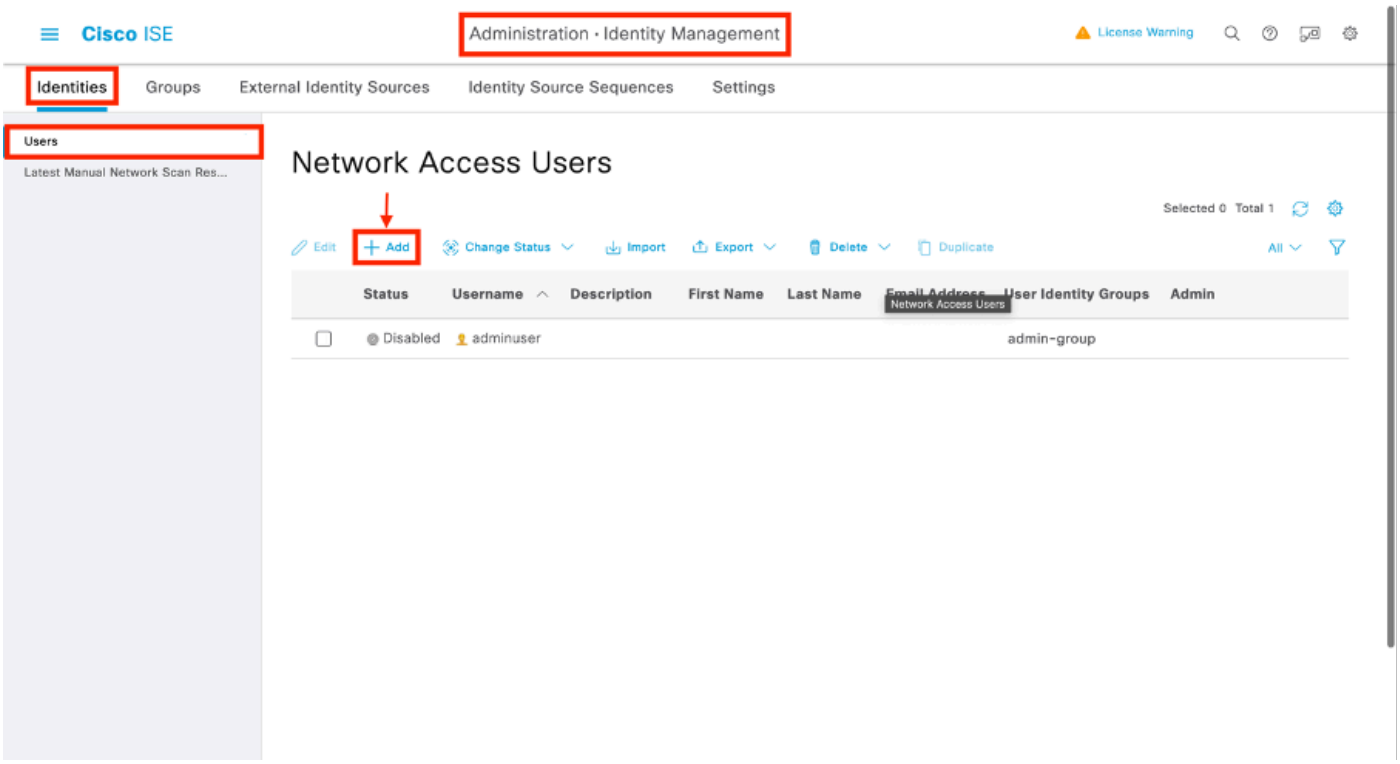
Zodra de velden geconfigureerd zijn, gebruikt u de knop "Indienen" om de dACL te maken.

Herhaal de stap om de dACL voor de tweede gebruiker, ACL_USER2, te definiëren zoals in de afbeelding.



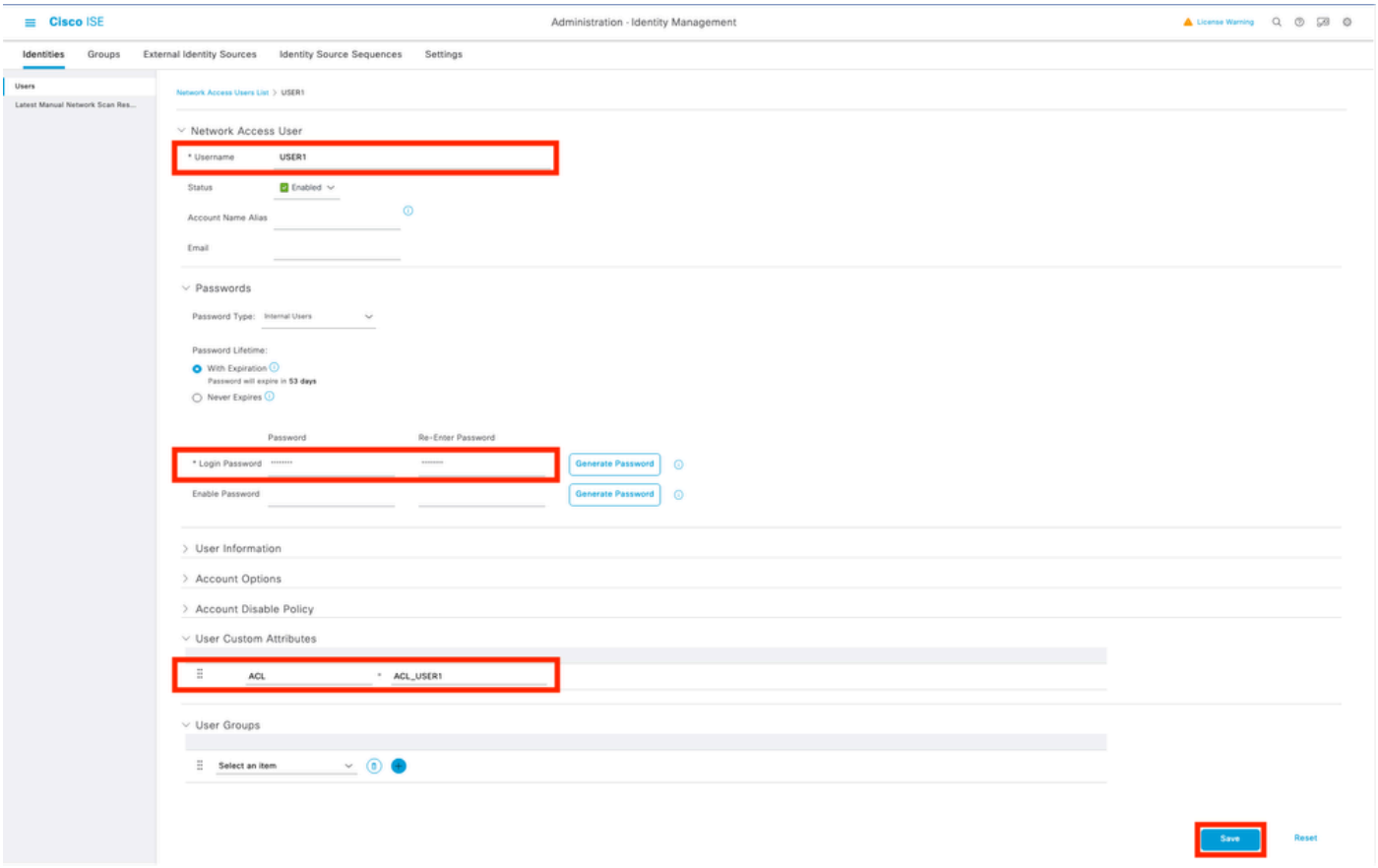
Stap 3. Wijs de dACL toe aan een gemaakte identiteit

Nadat de dACL is gemaakt, kan deze aan elke ISE-identiteit worden toegewezen met behulp van de aangepaste gebruikerskenmerken die in Stap 1 zijn gemaakt. Ga hiervoor naar Beheer > Identity Management > Identity > Identities > Gebruikers. Gebruik zoals gebruikelijk de knop "Toevoegen" om een gebruiker aan te maken.



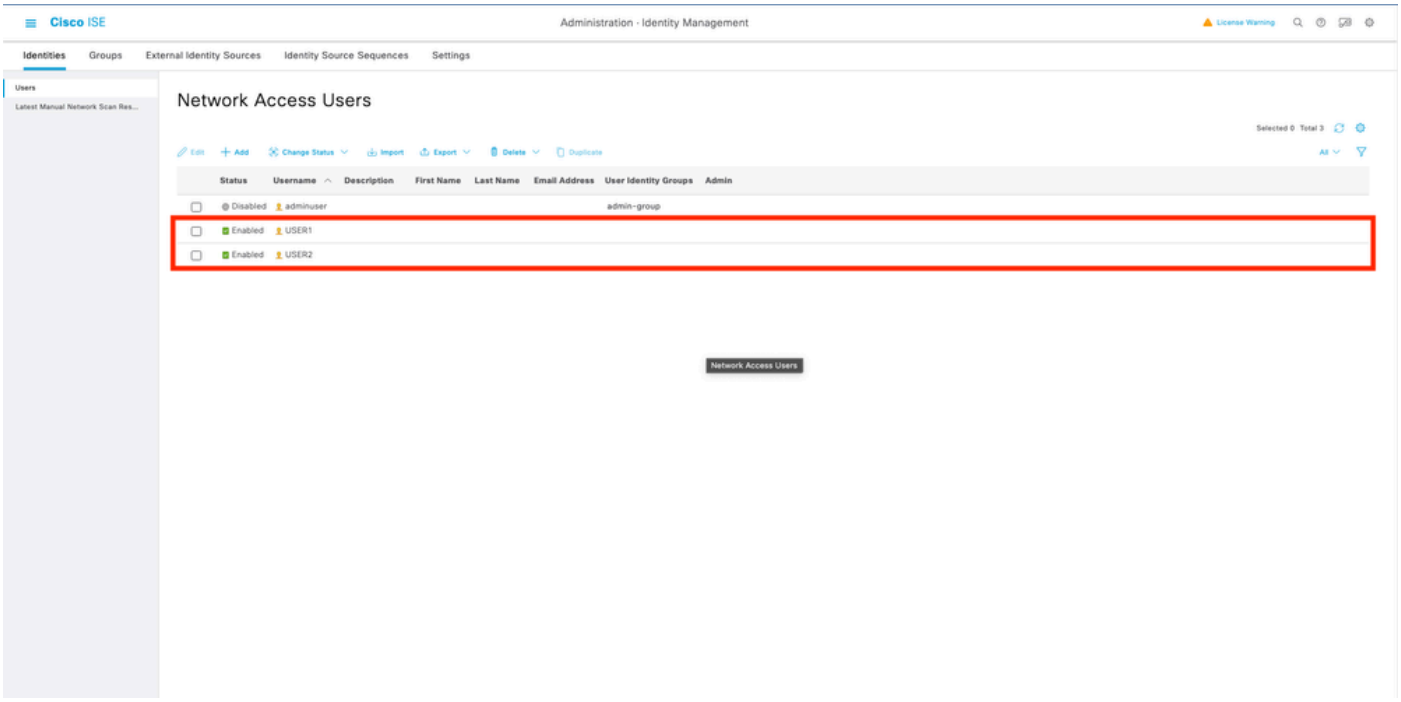
Definieer op het configuratieformulier "Nieuwe gebruiker netwerktoegang" de gebruikersnaam en het wachtwoord voor de gemaakte gebruiker. Gebruik het aangepaste kenmerk "ACL" om de

dACL die in Stap 2 is gemaakt, aan de identiteit toe te wijzen. In het voorbeeld, wordt de identiteit USER1 die ACL_USER1 gebruikt bepaald.



Zodra de velden goed zijn geconfigureerd kunt u de knop "Verzenden" gebruiken om de identiteit aan te maken.

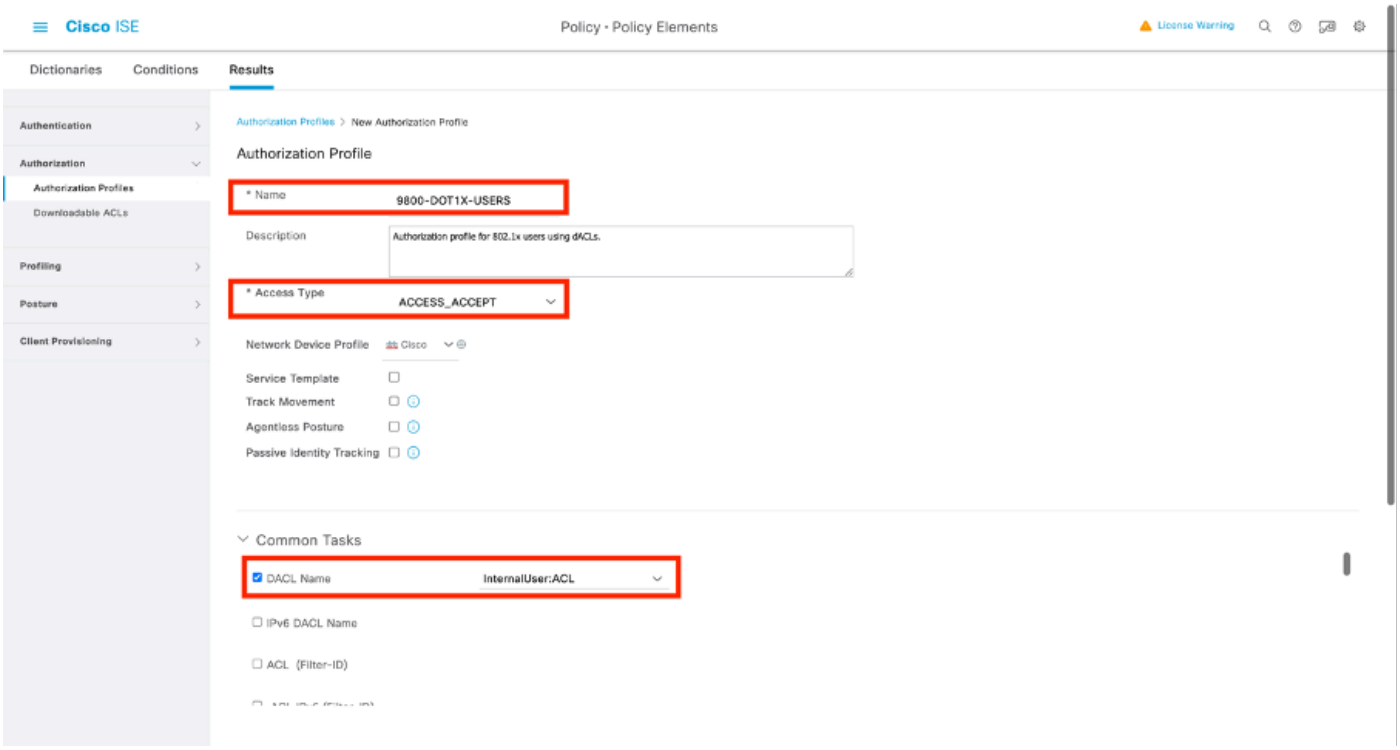
Herhaal deze stap om USER2 te maken en ACL_USER2 hieraan toe te wijzen.



Stap 4. Configureer het resultaat van het autorisatiebeleid.

Zodra de identiteit is geconfigureerd en de dACL is toegewezen, moet het autorisatiebeleid nog steeds worden geconfigureerd om het aangepaste gebruikerskenmerk "ACL" te matchen dat is gedefinieerd voor een bestaande autorisatie en gemeenschappelijke taak. Hiervoor navigeer je naar Policy > Policy Elements > Results > Authorisation > Authorisation Profiles. Gebruik de knop "Toevoegen" om een nieuw autorisatiebeleid te definiëren.

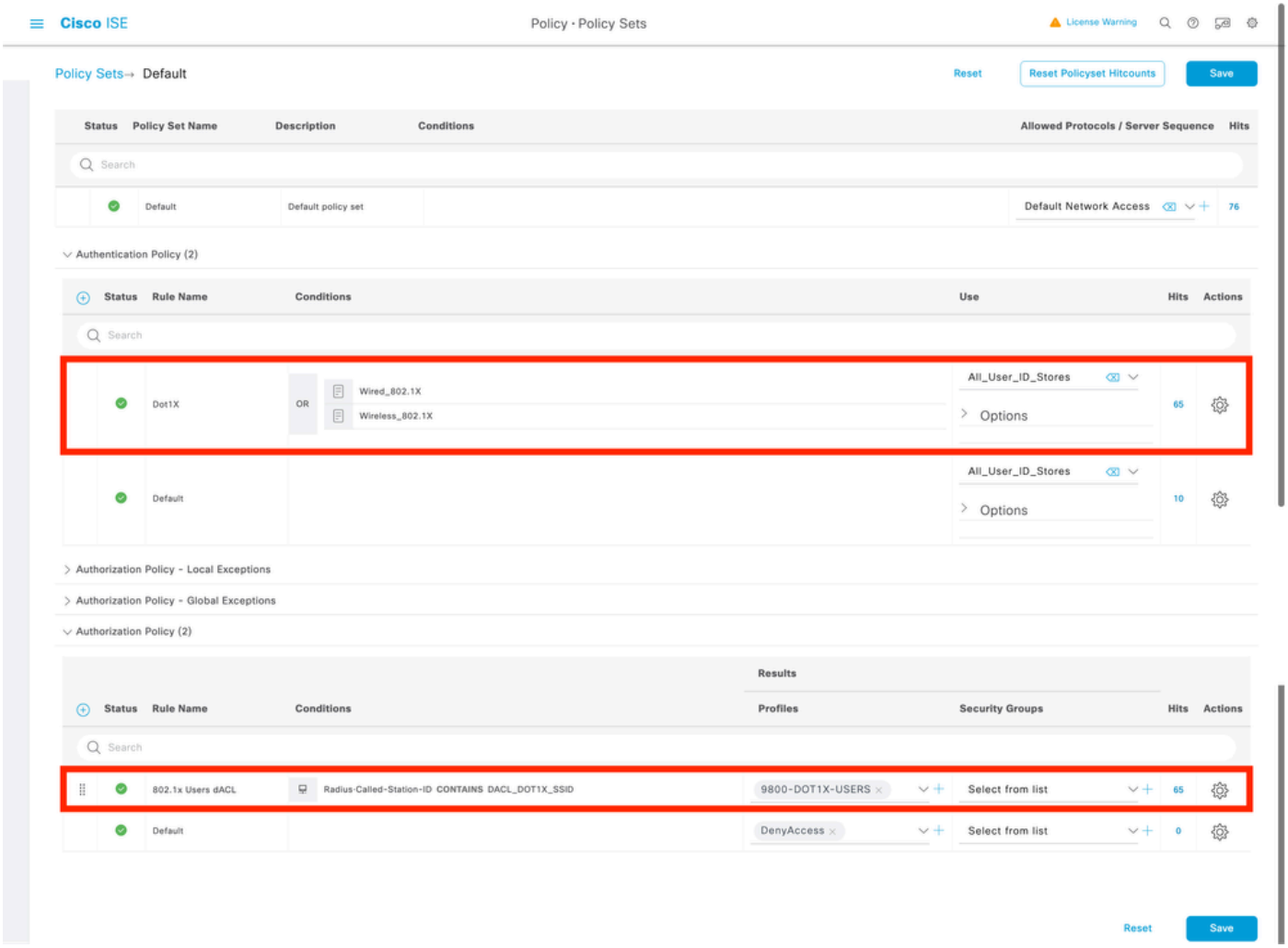
- Naam: de naam van het vergunningsbeleid, hier "9800-DOT1X-GEBRUIKERS".
- Toegangstype: het type toegang dat wordt gebruikt wanneer dit beleid wordt aangepast, hier ACCESS_ACCEPTEREN.
- Gemeenschappelijke taak: stem "DACL-naam" af op Interne Gebruiker:<naam van aangepaste attribuut gemaakt> voor interne gebruiker.Volgens de namen die in dit document worden gebruikt, wordt het profiel 9800-DOT1X-GEBRUIKERS geconfigureerd met de dACL geconfigureerd als Interne Gebruiker:ACL.



Stap 5. Gebruik het autorisatieprofiel in de beleidsset.

Zodra het autorisatieprofiel correct is gedefinieerd, moet dit deel uitmaken van de beleidsset die wordt gebruikt voor het verifiëren en autoriseren van draadloze gebruikers. Navigeer naar Policy > Policy Sets en open de gebruikte policy set.

In dit geval komt de verificatieregel "Dot1X" overeen met elke verbinding die via bekabelde of draadloze 802.1x wordt gemaakt. De autorisatieregel "802.1x Gebruikers dACL" implementeert een voorwaarde op de gebruikte SSID (dat is Radius-Calling-ID bevat DACL_DOT1X_SSID). Als een autorisatie wordt uitgevoerd op het "DACL_DOT1X_SSID" WLAN, wordt het profiel "9800-DOT1X-GEBRUIKERS", gedefinieerd in stap 4, gebruikt om de gebruiker te autoriseren.



dACL's per resultaat

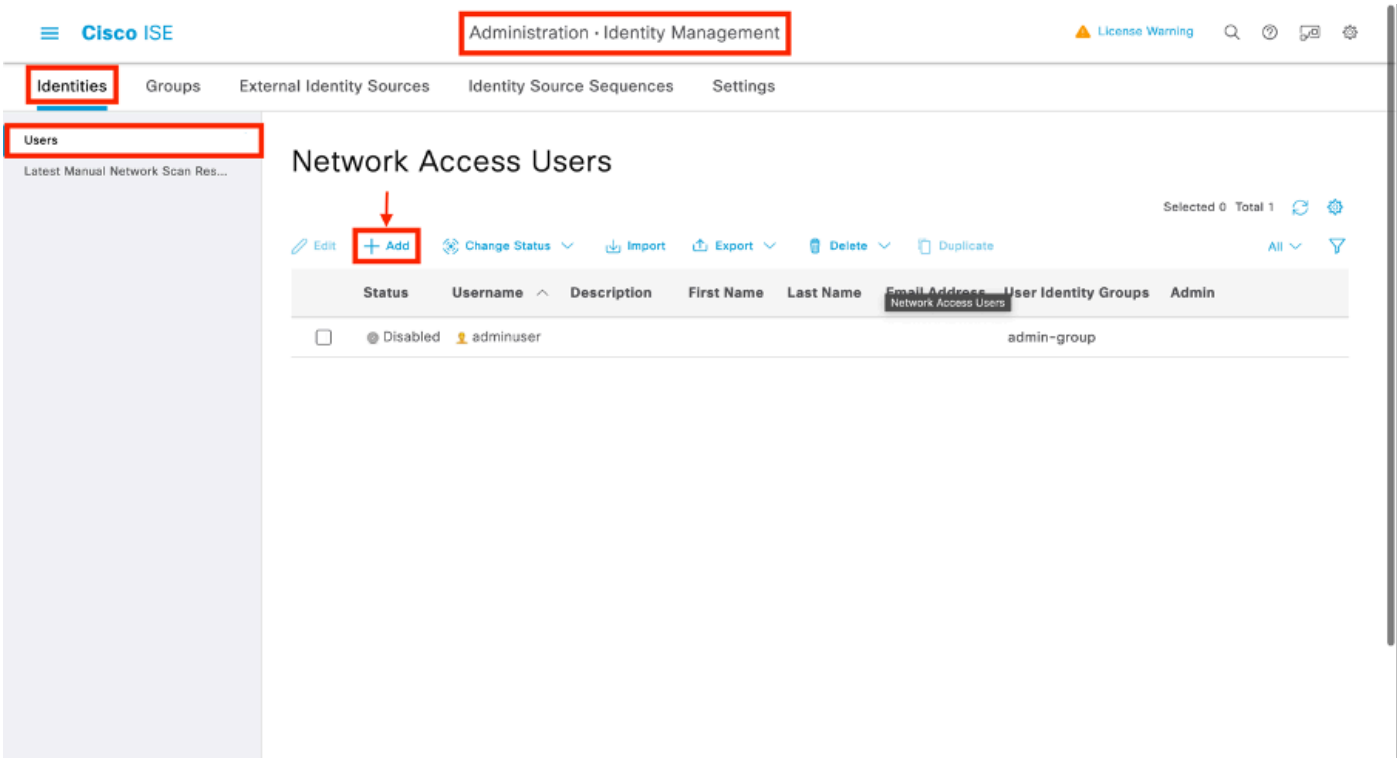
Om de enorme taak te vermijden om een bepaalde dACL aan elke identiteit toe te wijzen die op ISE wordt gemaakt, kan men kiezen voor het toepassen van dACL op een bepaald beleidsresultaat. Dit resultaat wordt vervolgens toegepast op basis van elke voorwaarde die wordt afgemeten aan de vergunningsregels uit de gebruikte beleidsreeks.

Stap 1. Configureer de dACL

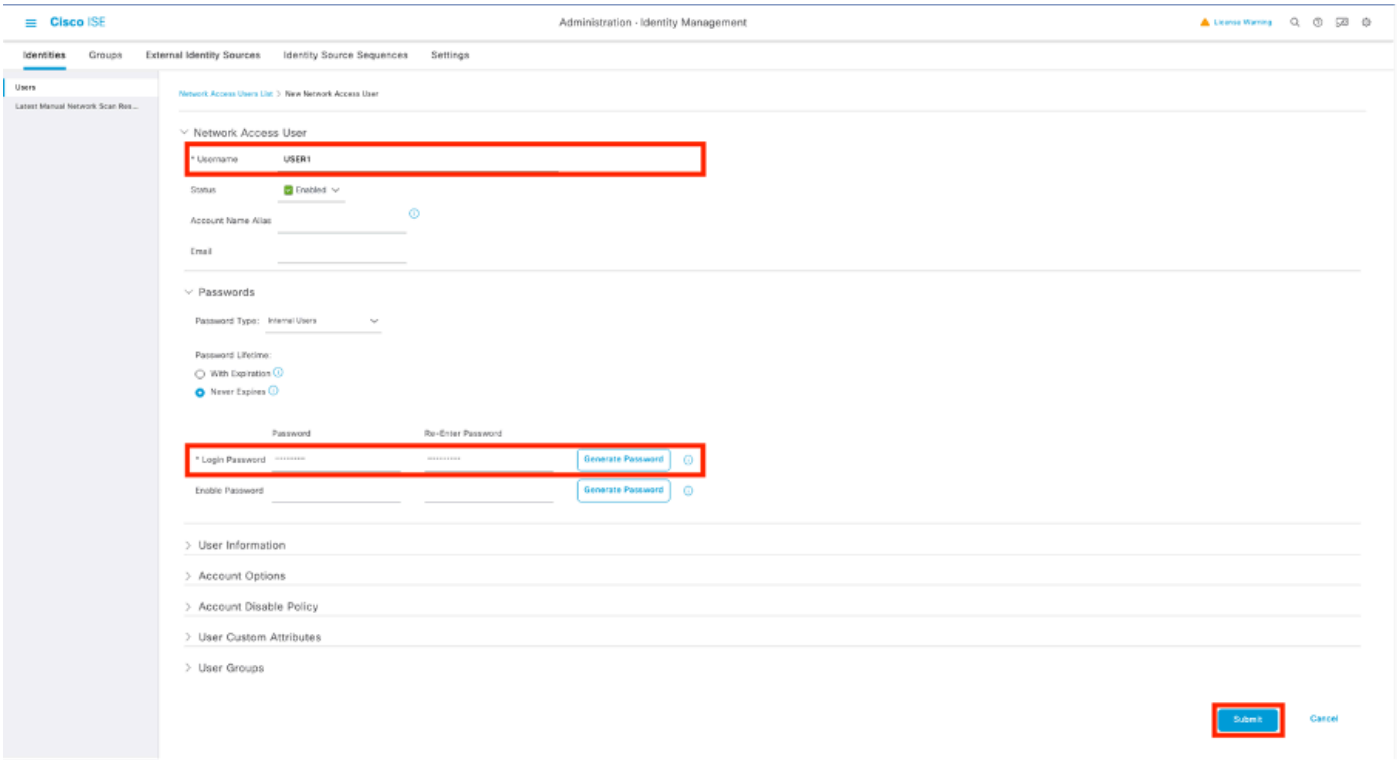
Voer dezelfde stap 2 uit vanuit de sectie Per-gebruiker dACL's om de benodigde dACL's te definiëren. Hier, zijn dit ACL_USER1 en ACL_USER2.

Stap 2. Identiteiten maken

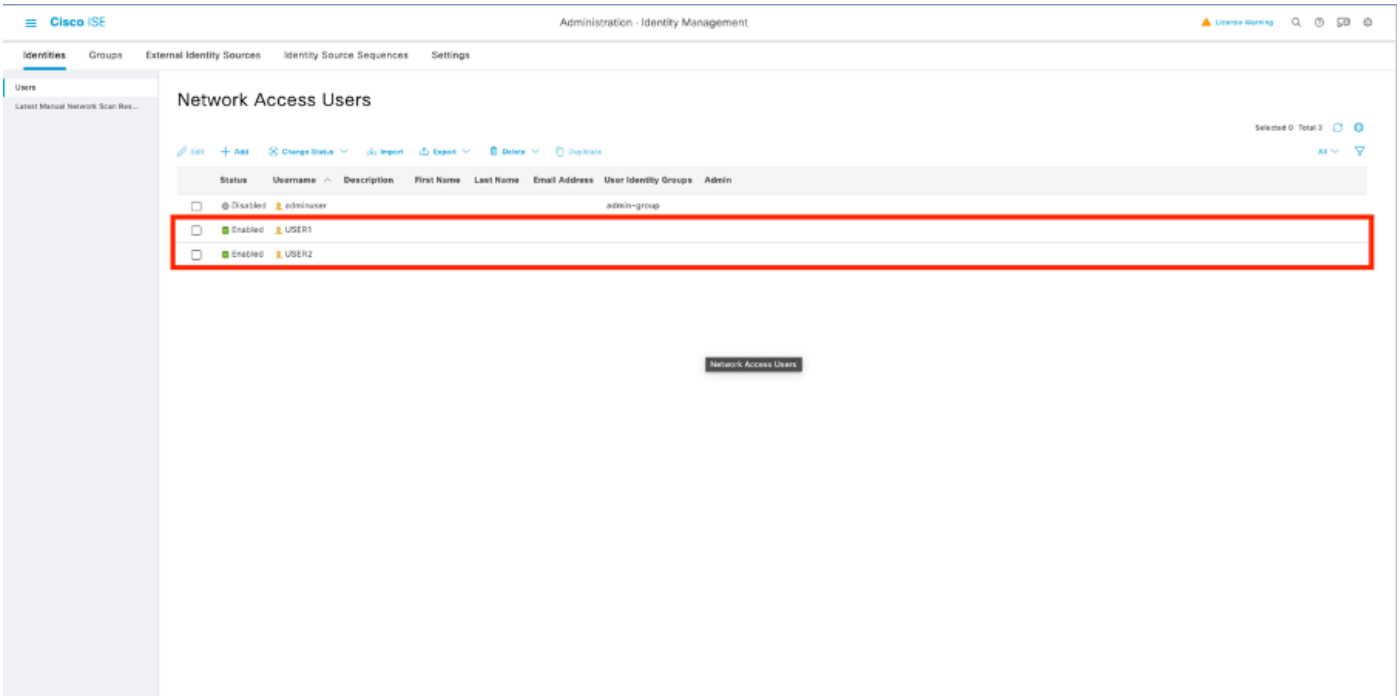
Ga naar Beheer > Identity Management > Identity > Gebruikers en gebruik de knop "Add" om een gebruiker aan te maken.



Definieer op het configuratieformulier "Nieuwe gebruiker netwerktoegang" de gebruikersnaam en het wachtwoord voor de gemaakte gebruiker.



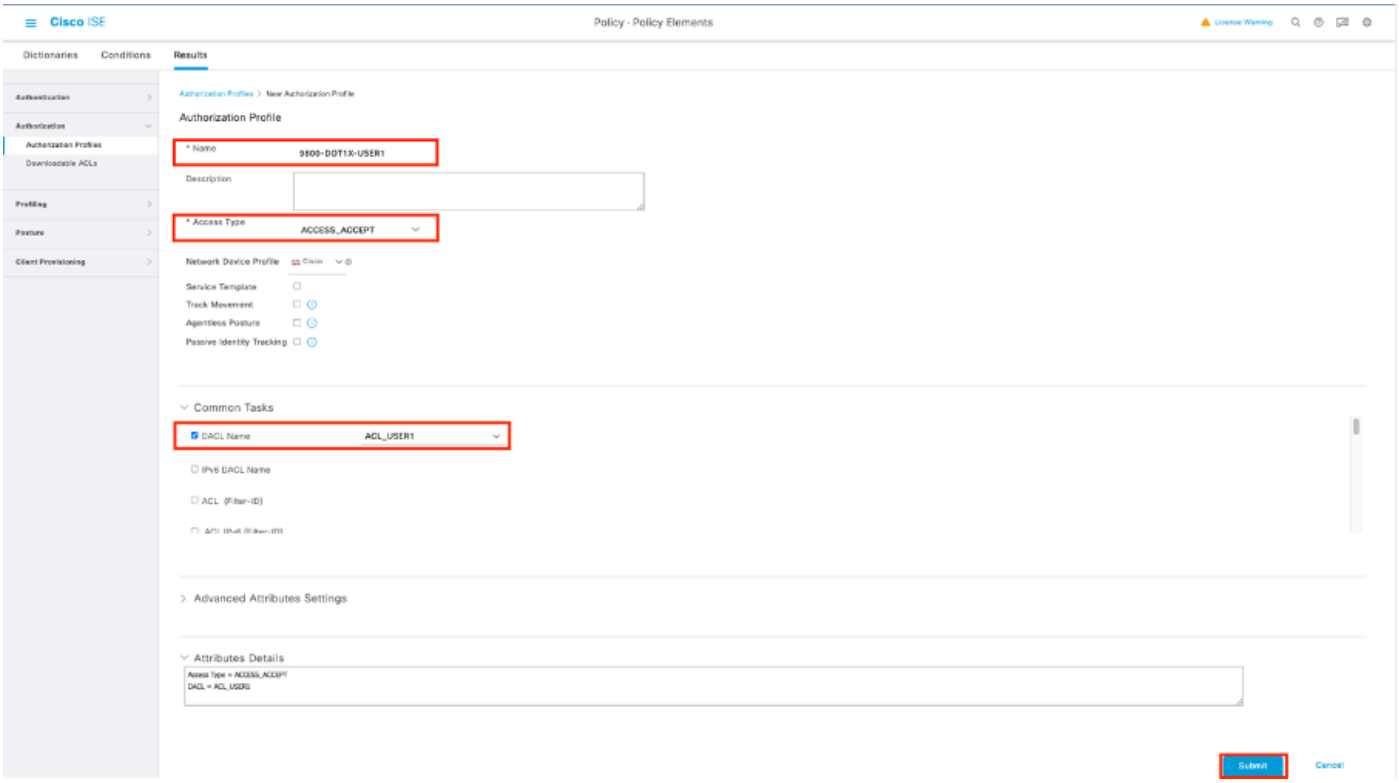
Herhaal deze stap om USER2 te maken.



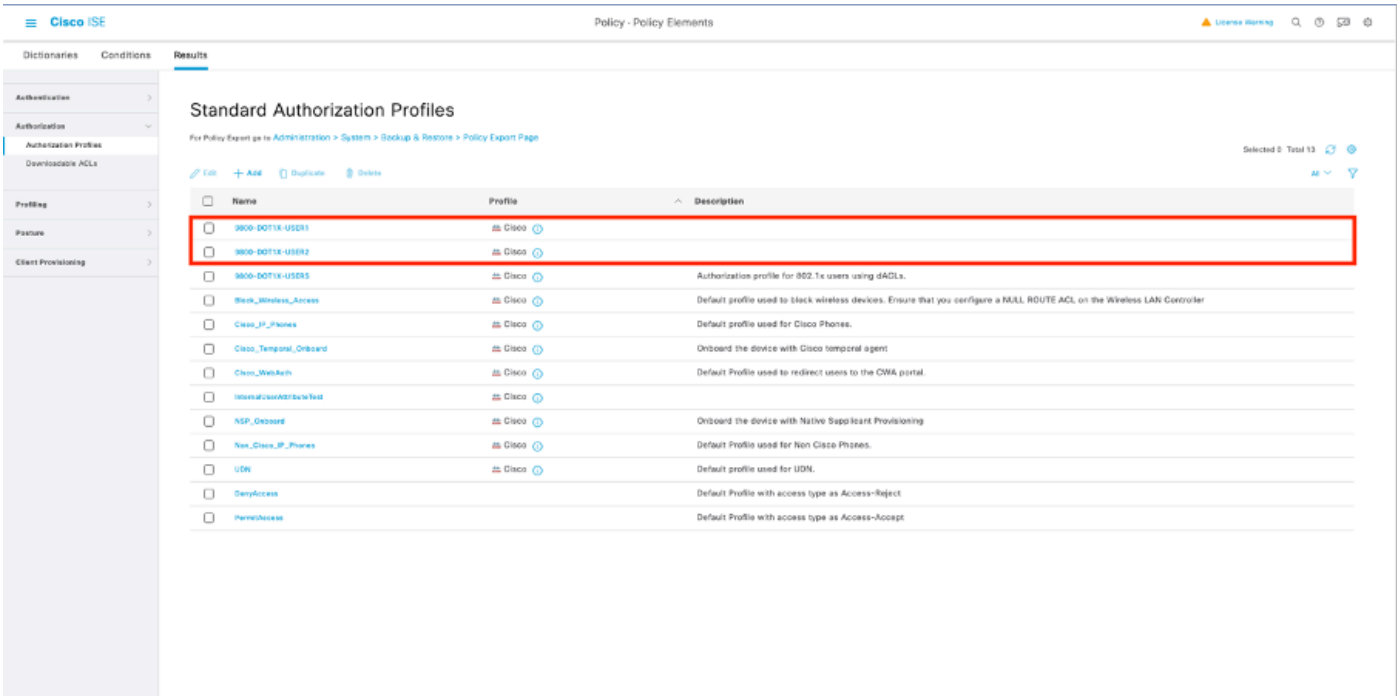
Stap 4. Configureer het resultaat van het autorisatiebeleid.

Zodra de identiteit en de dACL zijn geconfigureerd, moet het autorisatiebeleid nog steeds worden geconfigureerd om een bepaalde dACL toe te wijzen aan gebruiker die de voorwaarde aanpast om dit beleid te gebruiken. Hiervoor navigeer je naar Policy > Policy Elements > Results > Authorisation > Authorisation Profiles. Gebruik de knop "Toevoegen" om een nieuw autorisatiebeleid te definiëren en deze velden te voltooien.

- Naam: de naam van het vergunningsbeleid, hier "9800-DOT1X-USER1".
- Toegangstype: het type toegang dat wordt gebruikt wanneer dit beleid wordt aangepast, hier ACCESS_ACCEPTEERT.
- Gemeenschappelijke Taak: pas "DACL Naam"aan "ACL_USER1"voor interne gebruiker aan. Volgens de namen die in dit document worden gebruikt, wordt het profiel 9800-DOT1X-USER1 geconfigureerd met de dACL geconfigureerd als "ACL_USER1".



Herhaal deze stap om het beleidsresultaat "9800-DOT1X-USER2" te maken en wijs "ACL_USER2" als DACL toe aan het.

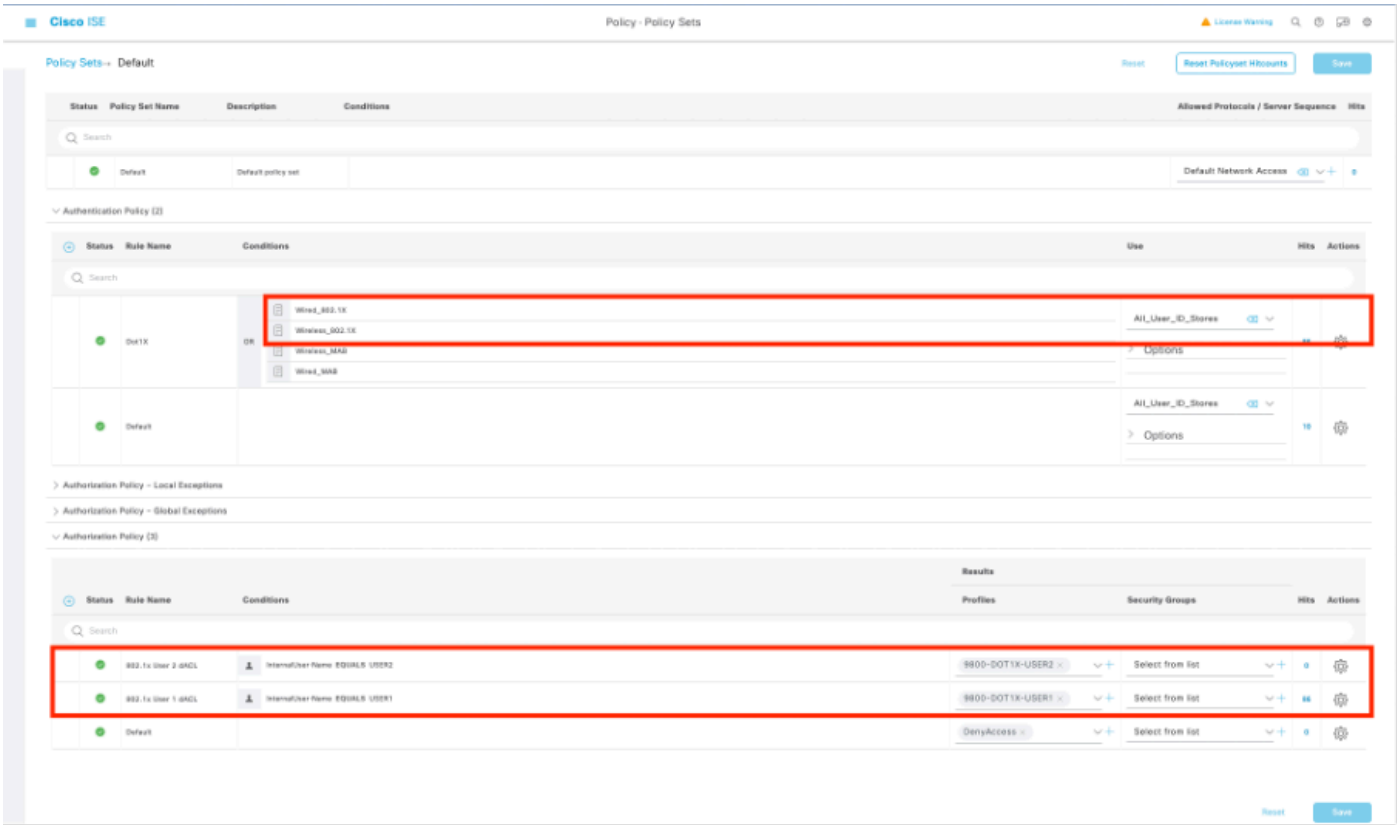


Stap 5. Gebruik autorisatieprofielen in de beleidsset.

Zodra het autorisatieprofiel correct is gedefinieerd, moet het nog steeds deel uitmaken van de beleidsset die wordt gebruikt voor het verifiëren en autoriseren van draadloze gebruikers. Navigeer naar Policy > Policy Sets en open de gebruikte policy set.

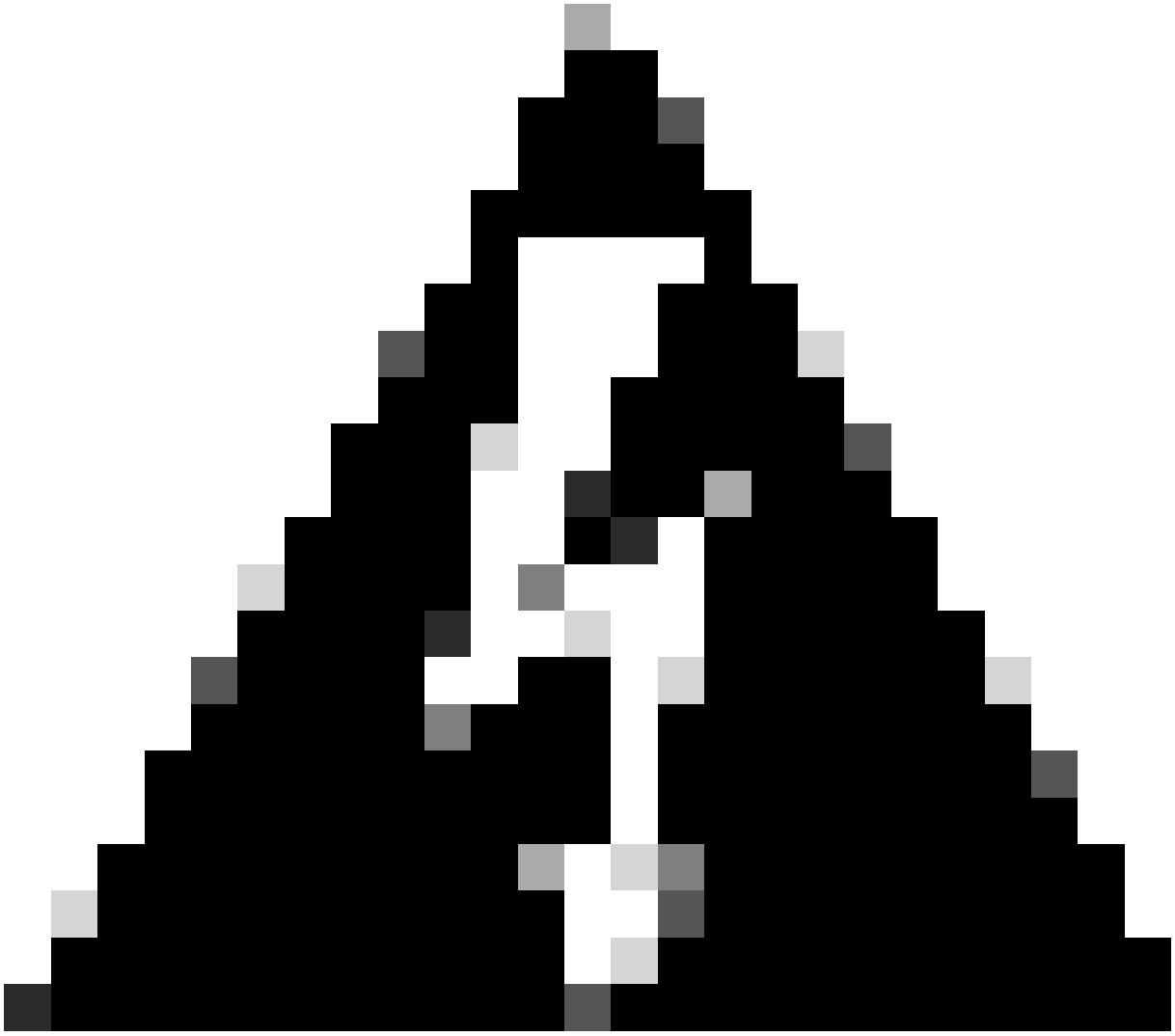
In dit geval komt de verificatieregel "Dot1X" overeen met elke verbinding die via bekabelde of draadloze 802.1X wordt gemaakt. De autorisatieregel "802.1X Gebruiker 1 dACL" implementeert

een voorwaarde op de gebruikte gebruikersnaam (dat is Interne Gebruiker-Naam BEVAT USER1). Als een autorisatie wordt uitgevoerd met de gebruikersnaam USER1, dan wordt het profiel "9800-DOT1X-USER1", gedefinieerd in Stap 4, gebruikt om de gebruiker te autoriseren en wordt dus ook de dACL uit dit resultaat (ACL_USER1) toegepast op de gebruiker. Hetzelfde wordt ingesteld voor de gebruikersnaam USER2, waarvoor "9800-DOT1X-USER1" wordt gebruikt.



Opmerkingen over het gebruik van dACL's met CWA-SSID's

Zoals beschreven in de Configure Central Web Verification (CWA) op Catalyst 9800 WLC en ISE-configuratiehandleiding, maakt CWA gebruik van MAB en bepaalde resultaten om gebruikers te verifiëren en te autoriseren. Downloadbare ACL's kunnen aan de CWA-configuratie vanuit ISE-zijde op dezelfde manier worden toegevoegd als wat hierboven is beschreven.



Waarschuwing: downloadbare ACL's kunnen alleen worden gebruikt als netwerktoegangslijst en worden niet ondersteund als pre-verificatie ACL's. Daarom moet elke pre-authenticatie ACL die gebruikt wordt in een CWA-workflow worden gedefinieerd in de WLC-configuratie.

Verifiëren

Om de gemaakte configuratie te controleren, kunnen deze opdrachten worden gebruikt.

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name <ap-name> config general
# show ap tag summary
# show ap name <AP-name> tag detail
# show wlan { summary | id | nme | all }
```

```
# show wireless tag policy detailed <policy-tag-name>
# show wireless profile policy detailed <policy-profile-name>
# show access-lists { acl-name }
```

Hier wordt verwezen naar het relevante deel van de WLC-configuratie die overeenkomt met dit voorbeeld.

```
aaa new-model
!
!
aaa group server radius authz-server-group
 server name DACL-RADIUS
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authentication dot1x DOT1X group radius
aaa authorization exec default local
aaa authorization network default group radius
!
!
aaa server radius dynamic-author
 client <ISE IP>
!
aaa session-id common
!
[...]
vlan 1413
 name VLAN_1413
!
[...]
radius server DACL-RADIUS
 address ipv4 <ISE IP> auth-port 1812 acct-port 1813
 key 6 aHaOSX[QbbEHURGW`cXiG^UE]CR]^PVANfcbROb
!
!
[...]
wireless profile policy DACL-8021X
 aaa-override
 vlan VLAN_1413
 no shutdown
[...]
wireless tag policy default-policy-tag
 description "default policy-tag"
 wlan DACL_DOT1X_SSID policy DACL-8021X
[...]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
 security dot1x authentication-list DOT1X
 no shutdown
```

De RADIUS-serverconfiguratie wordt weergegeven met de opdracht all in werking stellen-config van de show.

```
WLC#show running-config all | s radius-server
radius-server attribute 77 include-in-acct-req
radius-server attribute 77 include-in-access-req
radius-server attribute 11 default direction out
radius-server attribute nas-port format a
radius-server attribute wireless authentication call-station-id ap-macaddress-ssid
radius-server dead-criteria time 10 tries 10
radius-server cache expiry 24 enforce hours
radius-server transaction max-tries 8
radius-server retransmit 3
radius-server timeout 5
radius-server ipc-limit in 10
radius-server ipc-limit done 10
radius-server vsa send accounting
radius-server vsa send authentication
```

Problemen oplossen

Checklist

- Zorg ervoor dat de clients goed kunnen aansluiten op de 802.1X SSID die is geconfigureerd.
- Verzeker dat het RADIUS-toegangsverzoek/acceptatie de juiste attribuut-waarde paren (AVP's) bevat.
- Zorg ervoor dat clients het juiste WLAN/beleidsprofiel gebruiken.

WLC One Stop-Shop Reflex

Om te controleren of de dACL correct aan een bepaalde draadloze client is toegewezen, kan men de opdracht **show wireless client mac-address <H.H.H> detail** gebruiken zoals getoond. Van daar, kan de verschillende nuttige het oplossen van probleeminformatie worden gezien, namelijk: de cliëntgebruikersbenaming, staat, beleidsprofiel, WLAN en, het belangrijkst hier, ACS-ACL.

<#root>

WLC#show wireless client mac-address 08be.ac14.137d detail Client MAC Address : 08be.ac14.137d Client MAC Type : Universally Administered Addre

Client Username : USER1

AP MAC Address : f4db.e65e.7bc0 AP Name: AP4800-E

Client State : Associated Policy Profile : DACL-8021X

Wireless LAN Id: 2

WLAN Profile Name: DACL_DOT1X_SSID Wireless LAN Network Name (SSID): DACL_DOT1X_SSID

BSSID : f4db.e65e.7bc0 Association Id : 1 Authentication Algorithm : Open System Client Active State :

Client ACLs : None Policy Manager State: Run

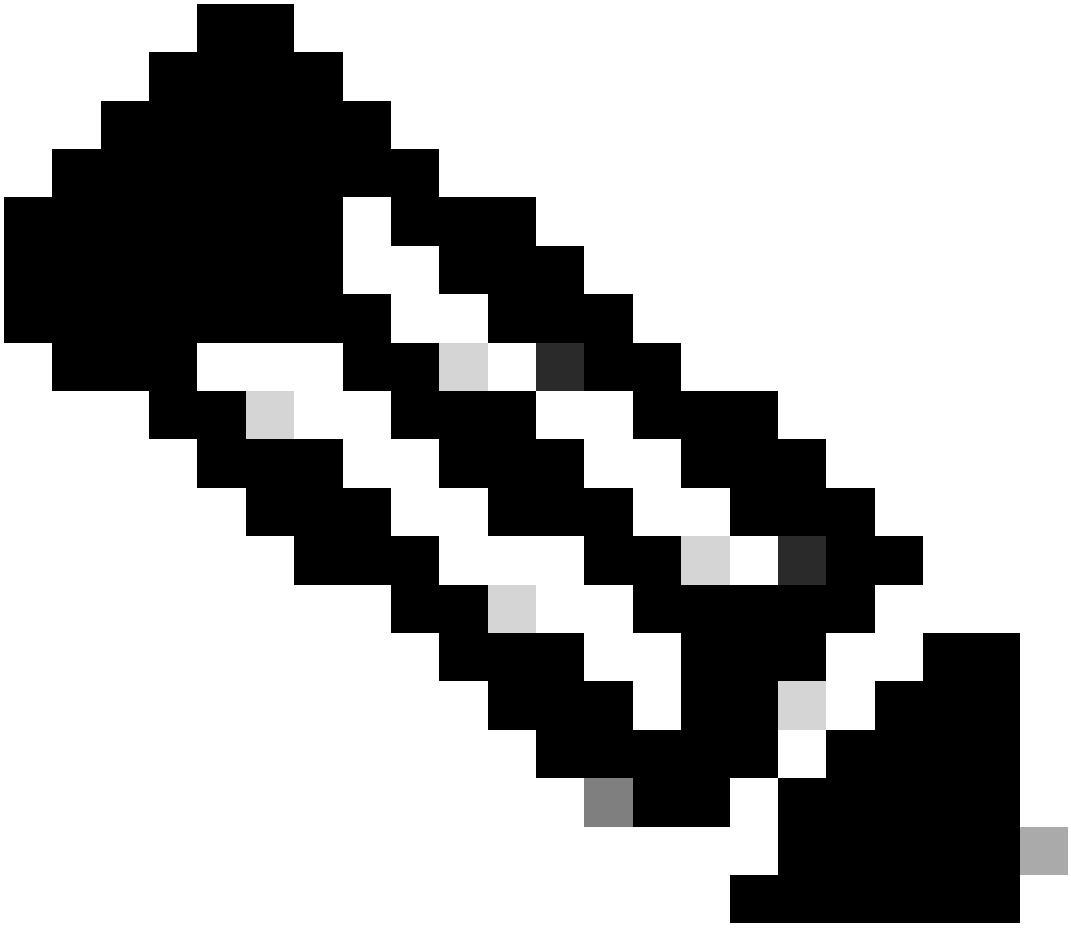
Last Policy Manager State : IP Learn Complete Client Entry Create Time : 35 seconds Policy Type : WPA2

VLAN : VLAN_1413

```
[...] Session Manager: Point of Attachment : capwap_90000012 IIF ID : 0x90000012 Authorized : TRUE Sess
 SM State : AUTHENTICATED
 SM Bend State : IDLE Local Policies:
 Service Template : wlan_svc_DACL-8021X_local (priority 254) VLAN : VLAN_1413 Absolute-Timer : 28800
 Server Policies:
 ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab
 Resultant Policies:
 ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab VLAN Name : VLAN_1413 VLAN : 1413 Absolute-Timer : 28800
 [...]
```

WLC-opdrachten weergeven

Om alle ACL's te zien die momenteel deel uitmaken van de Catalyst 9800 WLC-configuratie, kunt u de opdracht **toegangslijsten tonen** gebruiken. Dit bevel maakt een lijst van alle plaatselijk bepaalde ACLs of dACLs die door WLC wordt gedownload. Om het even welke dACLs die van ISE door WLC wordt gedownload heeft het formaat xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.



Opmerking: downloadbare ACL's blijven in de configuratie zolang een client is gekoppeld en gebruikt in de draadloze infrastructuur. Zodra de laatste client die gebruik maakt van de dACL de infrastructuur verlaat, wordt de dACL verwijderd uit de configuratie.

```
WLC#show access-lists
Extended IP access list IP-Adm-V4-Int-ACL-global
[...]
Extended IP access list IP-Adm-V4-LOGOUT-ACL
[...]
Extended IP access list implicit_deny
[...]
Extended IP access list implicit_permit
[...]
```

```
Extended IP access list meraki-fqdn-dns
[...]
Extended IP access list preauth-ise
[...]
Extended IP access list preauth_v4
[...]
Extended IP access list xACSACLx-IP-ACL_USER1-65e89aab
    1 deny ip any host 10.48.39.13
    2 deny ip any host 10.48.39.15
    3 deny ip any host 10.48.39.186
    4 permit ip any any (56 matches)
IPv6 access list implicit_deny_v6
[...]
IPv6 access list implicit_permit_v6
[...]
IPv6 access list preauth_v6
[...]
```

Voorwaardelijke debugging en radio actieve tracering

Tijdens het oplossen van problemen configuratie, kunt u radioactieve sporen verzamelen voor een client die verondersteld wordt te worden toegewezen met de gedefinieerde dACL. Hier worden de logboeken benadrukt die het interessante deel van de radioactieve sporen tijdens het proces van de cliëntenvereniging voor cliënt 08be.ac14.137d tonen.

```
<#root>

24/03/28 10:43:04.321315612 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (note): MAC: 08be.ac14.137d Asso

2024/03/28 10:43:04.321414308 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d

2024/03/28 10:43:04.321464486 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

[...]

2024/03/28 10:43:04.322185953 {wncd_x_R0-0}{1}: [dot11] [19620]: (note): MAC: 08be.ac14.137d Association
```

2024/03/28 10:43:04.322199665 {wncd_x_R0-0}{1}: [dot11] [19620]: (info): MAC: 08be.ac14.137d DOT11 state

[...]

2024/03/28 10:43:04.322860054 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d S

2024/03/28 10:43:04.322881795 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

[...]

2024/03/28 10:43:04.323379781 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

[...]

2024/03/28 10:43:04.330181613 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.353413199 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.13
2024/03/28 10:43:04.353414496 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.13

2024/03/28 10:43:04.353438621 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 Au

2024/03/28 10:43:04.353443674 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

[...]

2024/03/28 10:43:04.381397739 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.381411901 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator e9 8b e

2024/03/28 10:43:04.381425481 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 7 "USER1

2024/03/28 10:43:04.381430559 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Service-Type [6] 6 Fra
2024/03/28 10:43:04.381433583 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 27
2024/03/28 10:43:04.381437476 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 21 "
2024/03/28 10:43:04.381440925 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Framed-MTU [12] 6 148
2024/03/28 10:43:04.381452676 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 12 .
2024/03/28 10:43:04.381466839 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator
2024/03/28 10:43:04.381482891 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Key-Name [102] 2
2024/03/28 10:43:04.381486879 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 49
2024/03/28 10:43:04.381489488 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 43 "
2024/03/28 10:43:04.381491463 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381494016 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "m

2024/03/28 10:43:04.381495896 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32
2024/03/28 10:43:04.381498320 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "

2024/03/28 10:43:04.381500186 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381502409 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "v

2024/03/28 10:43:04.381506029 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6 1

2024/03/28 10:43:04.381509052 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port-Type [61] 6
2024/03/28 10:43:04.381511493 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port [5] 6 3913
2024/03/28 10:43:04.381513163 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 39

2024/03/28 10:43:04.381515481 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 33 "c

2024/03/28 10:43:04.381517373 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 41

2024/03/28 10:43:04.381519675 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 35 "w

2024/03/28 10:43:04.381522158 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Called-Station-Id [30]
2024/03/28 10:43:04.381524583 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Calling-Station-Id [3
2024/03/28 10:43:04.381532045 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Airespace [26]
2024/03/28 10:43:04.381534716 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Airespace-WLAN-ID [1]

2024/03/28 10:43:04.381537215 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Nas-Identifier [32] 17

2024/03/28 10:43:04.381539951 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [18

2024/03/28 10:43:04.381542233 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[
2024/03/28 10:43:04.381544465 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188]
2024/03/28 10:43:04.381619890 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout
[...]

2024/03/28 10:43:04.392544173 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812/

2024/03/28 10:43:04.392557998 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 08 6d f
2024/03/28 10:43:04.392564273 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: State [24] 71 ...
2024/03/28 10:43:04.392615218 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 8 ..
2024/03/28 10:43:04.392628179 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator
2024/03/28 10:43:04.392738554 {wncd_x_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t
2024/03/28 10:43:04.726798622 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.726801212 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.726896276 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.726905248 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

[...]

2024/03/28 10:43:04.727138915 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.727148212 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.727164223 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000
2024/03/28 10:43:04.727169069 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727223736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : use

2024/03/28 10:43:04.727233018 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : cl
2024/03/28 10:43:04.727234046 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA
2024/03/28 10:43:04.727234996 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Me
2024/03/28 10:43:04.727236141 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA
M$®vf9∫Ø◇«? %ÿO?ã@≤™ÇÑbWï6\Ë&\q·lU+QB–º®”≠∫JÑv?"

2024/03/28 10:43:04.727246409 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Cis

[...]

2024/03/28 10:43:04.727509267 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.727513133 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.727607738 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: SVM Apply user profile
2024/03/28 10:43:04.728003638 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: Activating EPM feature

2024/03/28 10:43:04.728144450 {wncd_x_R0-0}{1}: [epm-misc] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.728161361 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012]
2024/03/28 10:43:04.728177773 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012]
2024/03/28 10:43:04.728184975 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012]

2024/03/28 10:43:04.728218783 {wncd_x_R0-0}{1}: [epm-acl] [19620]: (info): [08be.ac14.137d:capwap_900000

2024/03/28 10:43:04.729005675 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012]
2024/03/28 10:43:04.729019215 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: Response of epm is ASY
[...]

2024/03/28 10:43:04.729422929 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.729428175 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 20 06 3

2024/03/28 10:43:04.729432771 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6 1

2024/03/28 10:43:04.729435487 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.729437912 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32

2024/03/28 10:43:04.729440782 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "a

2024/03/28 10:43:04.729442854 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 30

2024/03/28 10:43:04.729445280 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 24 "a

2024/03/28 10:43:04.729447530 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator
2024/03/28 10:43:04.729529806 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout

2024/03/28 10:43:04.731972466 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812/

2024/03/28 10:43:04.731979444 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 2a 24 8

2024/03/28 10:43:04.731983966 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.731986470 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Class [25] 75 ...
2024/03/28 10:43:04.732032438 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator

2024/03/28 10:43:04.732048785 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732051657 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 "i

2024/03/28 10:43:04.732053782 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732056351 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 "i

2024/03/28 10:43:04.732058379 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 48

2024/03/28 10:43:04.732060673 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 42 "i

2024/03/28 10:43:04.732062574 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 36

2024/03/28 10:43:04.732064854 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 30 "i

2024/03/28 10:43:04.732114294 {wncd_x_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t
[...]

2024/03/28 10:43:04.733046258 {wncd_x_R0-0}{1}: [svm] [19620]: (info): [08be.ac14.137d] Applied User Pro

2024/03/28 10:43:04.733058380 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M
2024/03/28 10:43:04.733064555 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M
2024/03/28 10:43:04.733065483 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e
2024/03/28 10:43:04.733066816 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: m
2024/03/28 10:43:04.733068704 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c
2024/03/28 10:43:04.733069947 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: i

2024/03/28 10:43:04.733070971 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: us

2024/03/28 10:43:04.733079208 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c
2024/03/28 10:43:04.733080328 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: E
M$®vf9∫Ø◇«? %ÿO?ã@≤™ÇÑbWï6\Ë&\q·lU+QB-º®”≠∫JÑv?"
2024/03/28 10:43:04.733091441 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e

2024/03/28 10:43:04.733092470 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile:Cis

[...]

2024/03/28 10:43:04.733396045 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.733486604 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 A

2024/03/28 10:43:04.734665244 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.734894043 {wncd_x_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d E
2024/03/28 10:43:04.734904452 {wncd_x_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d C

2024/03/28 10:43:04.734915743 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.740499944 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.742238941 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.744387633 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

[...]

2024/03/28 10:43:04.745245318 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.745294050 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Allocate

2024/03/28 10:43:04.745326416 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.751291844 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.751943577 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.752686055 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.755505991 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.756746153 {wncd_x_R0-0}{1}: [mm-transition] [19620]: (info): MAC: 08be.ac14.137d MM
2024/03/28 10:43:04.757801556 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d ADD

2024/03/28 10:43:04.758843625 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

2024/03/28 10:43:04.759064834 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d IP

2024/03/28 10:43:04.761186727 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.761241972 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.763131516 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.764575895 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.764755847 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.769965195 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.770727027 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.772314586 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.772362837 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.773070456 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.773661861 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.775537766 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.777154567 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.778756670 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.778807076 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.778856100 {iosrp_R0-0}{1}: [mpls_ldp] [26311]: (info): LDP LLAF: Registry notificati

2024/03/28 10:43:04.779401863 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.779879864 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.780510740 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.786433419 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interfac
2024/03/28 10:43:04.786523172 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interfac
2024/03/28 10:43:04.787787313 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interfac
2024/03/28 10:43:04.788160929 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interfac
2024/03/28 10:43:04.788491833 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (note): MAC: 08be.ac14.137d C
2024/03/28 10:43:04.788576063 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000
2024/03/28 10:43:04.788741337 {wncd_x_R0-0}{1}: [webauth-sess] [19620]: (info): Change address update,
2024/03/28 10:43:04.788761575 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [19620]: (info): [08be.ac14.137d:c
2024/03/28 10:43:04.788877999 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [0000.0000.0000:unknown] HDL = 0

2024/03/28 10:43:04.789333126 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d IP

2024/03/28 10:43:04.789410101 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d

2024/03/28 10:43:04.789622587 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : us

2024/03/28 10:43:04.789632684 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : c

2024/03/28 10:43:04.789642576 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute :Cis

2024/03/28 10:43:04.789651931 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute :bsn

2024/03/28 10:43:04.789653490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : t
2024/03/28 10:43:04.789735556 {wncd_x_R0-0}{1}: [ewlc-qos-client] [19620]: (info): MAC: 08be.ac14.137d
2024/03/28 10:43:04.789800998 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [19620]: (debug): Managed client RUN

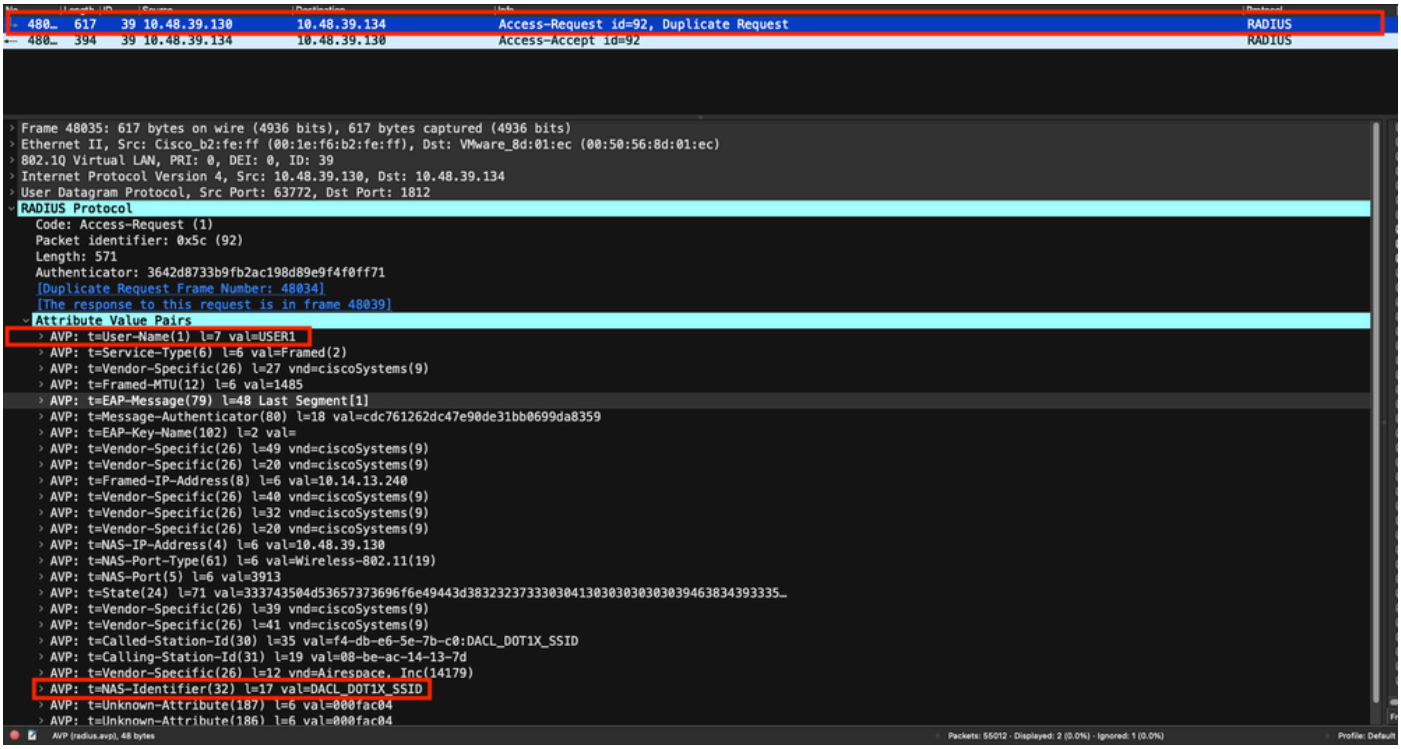
```
2024/03/28 10:43:04.789886011 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d
```

PacketCapture

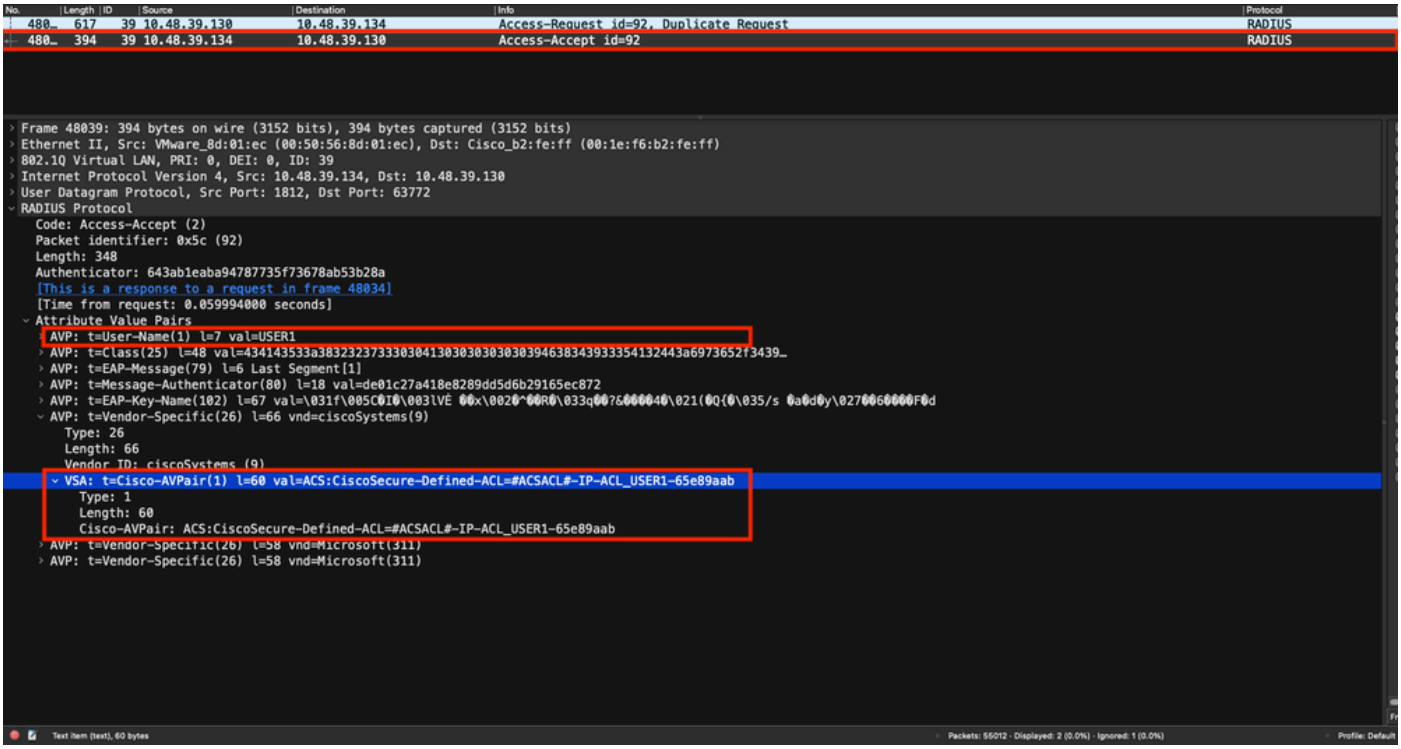
Een andere interessante reflex is pakketopnamen van de RADIUS-stroom voor een clientassociatie te nemen en te analyseren. Downloadbare ACL's zijn afhankelijk van RADIUS, niet alleen om te worden toegewezen aan een draadloze client, maar ook om te worden gedownload door de WLC. Terwijl u pakketopname neemt voor het oplossen van problemen met de configuratie van dACL's, moet u daarom op de interface opnemen die door de controller wordt gebruikt om met de RADIUS-server te communiceren. Dit document toont hoe u gemakkelijk ingesloten pakketvastlegging op Catalyst 9800 kunt configureren, die zijn gebruikt om de in dit artikel geanalyseerde opname te verzamelen.

RADIUS-clientverificatie

U kunt de client-RADIUS-toegangsaanvraag zien die van de WLC naar de RADIUS-server wordt verzonden om de gebruiker USER1 (AVP-gebruikersnaam) op de DACL_DOT1X_SSID SSID (AVP NAS-Identifier) te verifiëren.

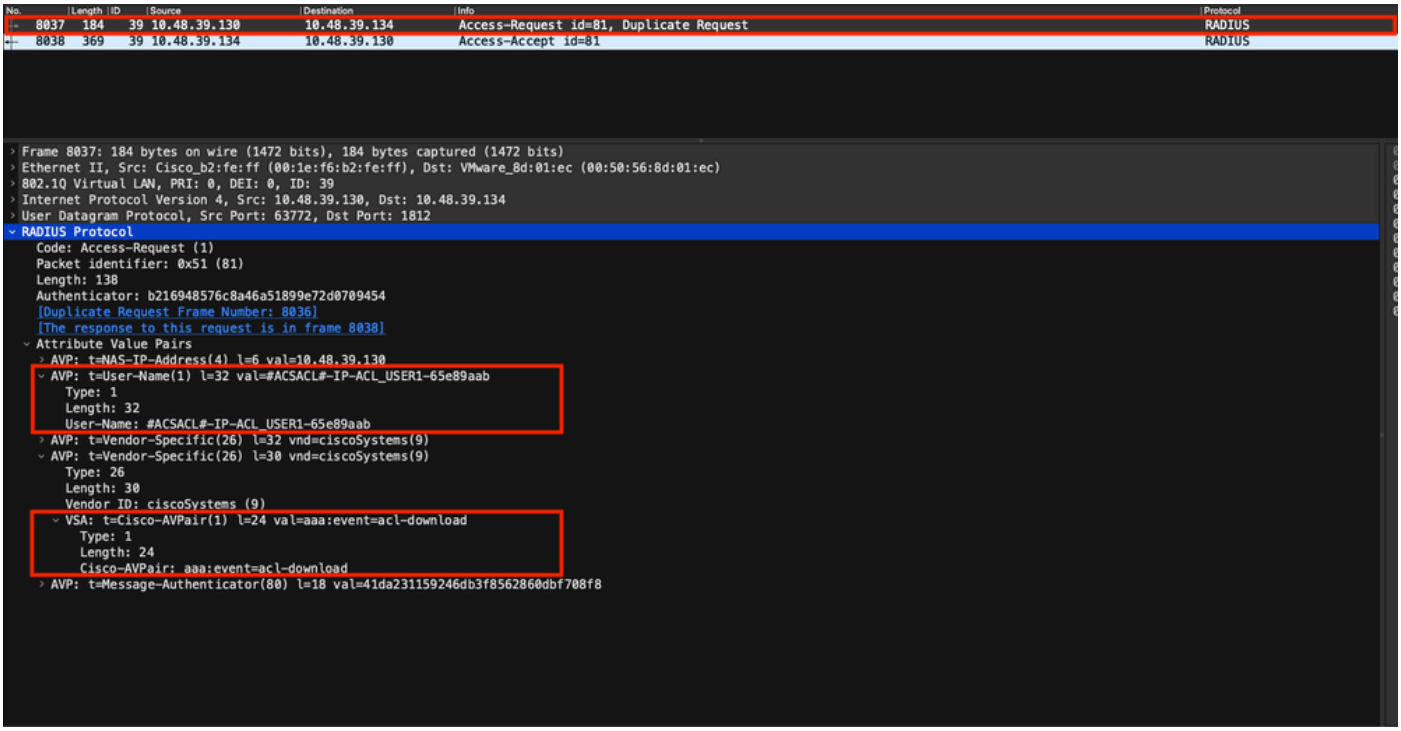


Wanneer de verificatie slaagt, antwoordt de RADIUS-server met een access-accept, nog steeds voor gebruiker USER1 (AVP-gebruikersnaam) en past de AAA-kenmerken toe, in het bijzonder de verkoper-specifieke AVP ACS:CiscoSecure-Defined-ACL die hier "#ACSACL#-IP-ACL_USER1-65e89aab" is.

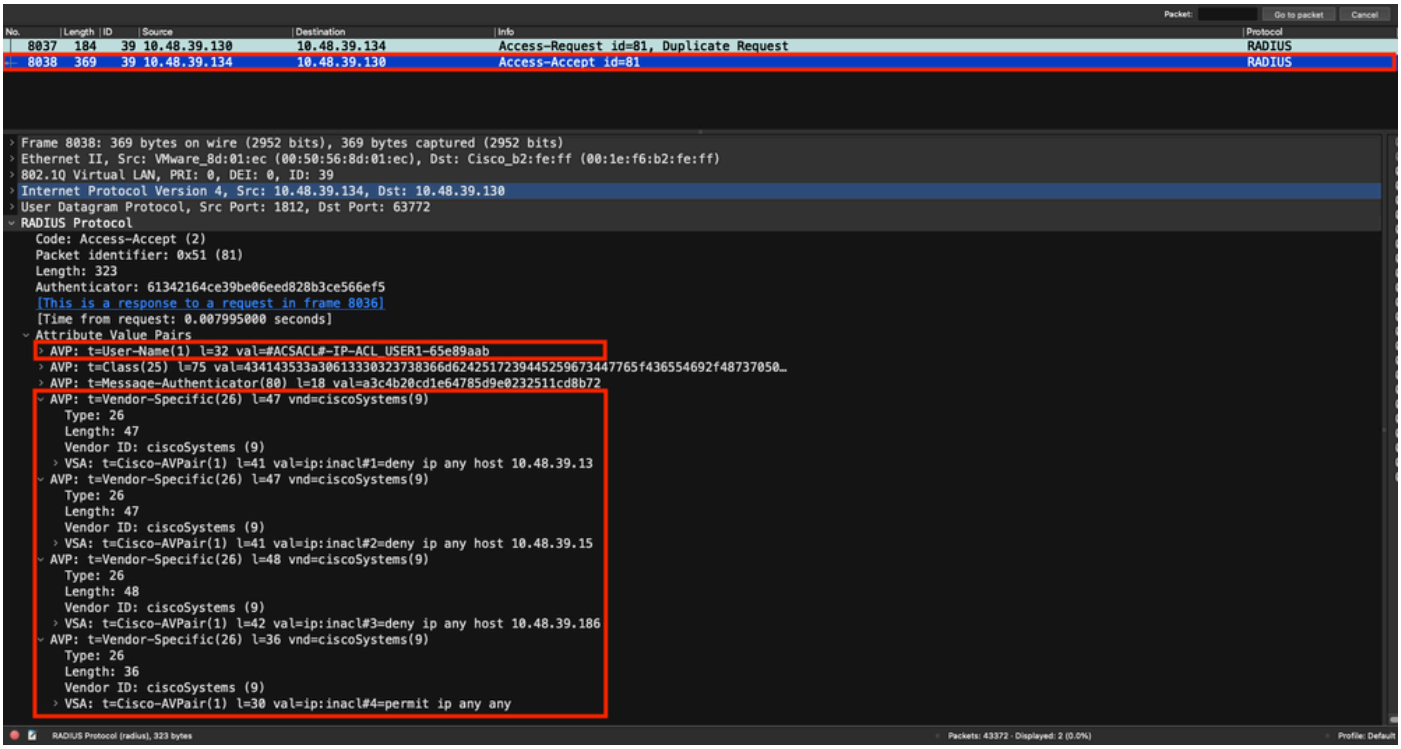


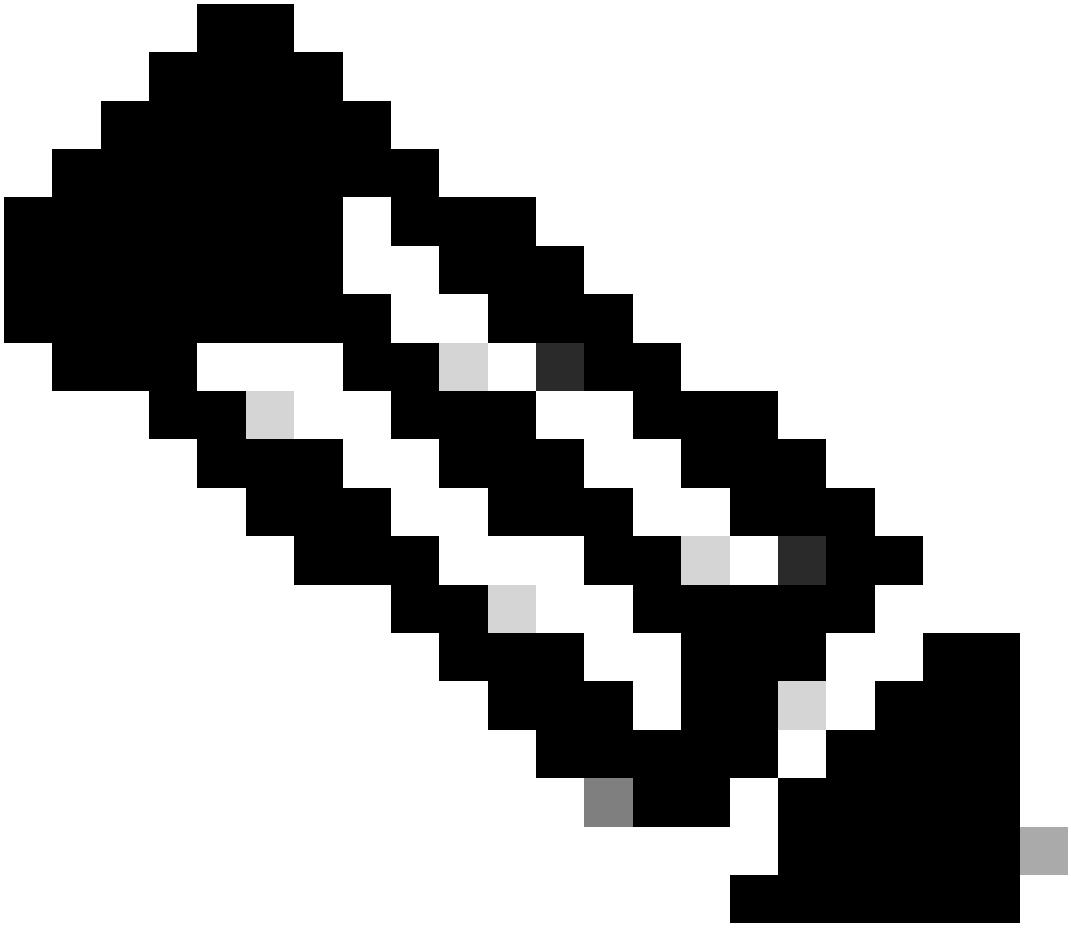
DACL-download

Als dACL al deel uitmaakt van de WLC-configuratie, wordt deze simpelweg toegewezen aan de gebruiker en worden de RADIUS-sessies beëindigd. Anders downloadt de WLC de ACL, nog steeds met RADIUS. Om dit te doen, doet de WLC een RADIUS access-request, dit keer met behulp van de dACL naam ("#ACSACL#-IP-ACL_USER1-65e89aab") voor de AVP User-Name. Tegelijkertijd informeert de WLC de RADIUS-server dat deze access-acceptatie een ACL-download initieert met behulp van het Cisco AV-paar aaa:event=acl-download.



De RADIUS-toegang-acceptatie die is teruggestuurd naar de controller bevat de gevraagde dACL, zoals aangegeven op de afbeelding. Elke ACL-regel bevindt zich in een andere Cisco AVP van het type "ip:inacl#<**X**>=<ACL_REGEL>", waarbij <X> het regelnummer is.


Packet:
Go to packet
Cancel
No. | Length | ID | Source | Destination | Info | Protocol
8037 184 39 10.48.39.130 10.48.39.134 Access-Request id=81, Duplicate Request RADIUS
8038 369 39 10.48.39.134 10.48.39.130 Access-Accept id=81 RADIUS
Frame 8038: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)
Ethernet II, Src: VMware_8d:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130
User Datagram Protocol, Src Port: 1812, Dst Port: 63772
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0x51 (81)
Length: 323
Authenticator: 61342164ce39be06eed828b3ce566ef5
[This is a response to a request in frame 8036]
[Time from request: 0.007995000 seconds]
Attribute Value Pairs
AVP: t=User-Name(1) l=32 val=#ACSACL#-IP-ACL_USER1-65e89aab
AVP: t=Class(25) l=75 val=434143533a3061333032373836366d624251723944525967344776 5f436554692f48737050…
AVP: t=Message-Authenticator(80) l=18 val=a3c4b20cd1e64785d9e0232511cd8b72
AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)
Type: 26
Length: 47
Vendor ID: ciscoSystems (9)
VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#1=deny ip any host 10.48.39.13
AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)
Type: 26
Length: 47
Vendor ID: ciscoSystems (9)
VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#2=deny ip any host 10.48.39.15
AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)
Type: 26
Length: 48
Vendor ID: ciscoSystems (9)
VSA: t=Cisco-AVPair(1) l=42 val=ip:inacl#3=deny ip any host 10.48.39.186
AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
Type: 26
Length: 36
Vendor ID: ciscoSystems (9)
VSA: t=Cisco-AVPair(1) l=30 val=ip:inacl#4=permit ip any any
RADIUS Protocol (radius), 323 bytes
Packets: 43372 · Displayed: 2 (0.0%)
Profile: Default

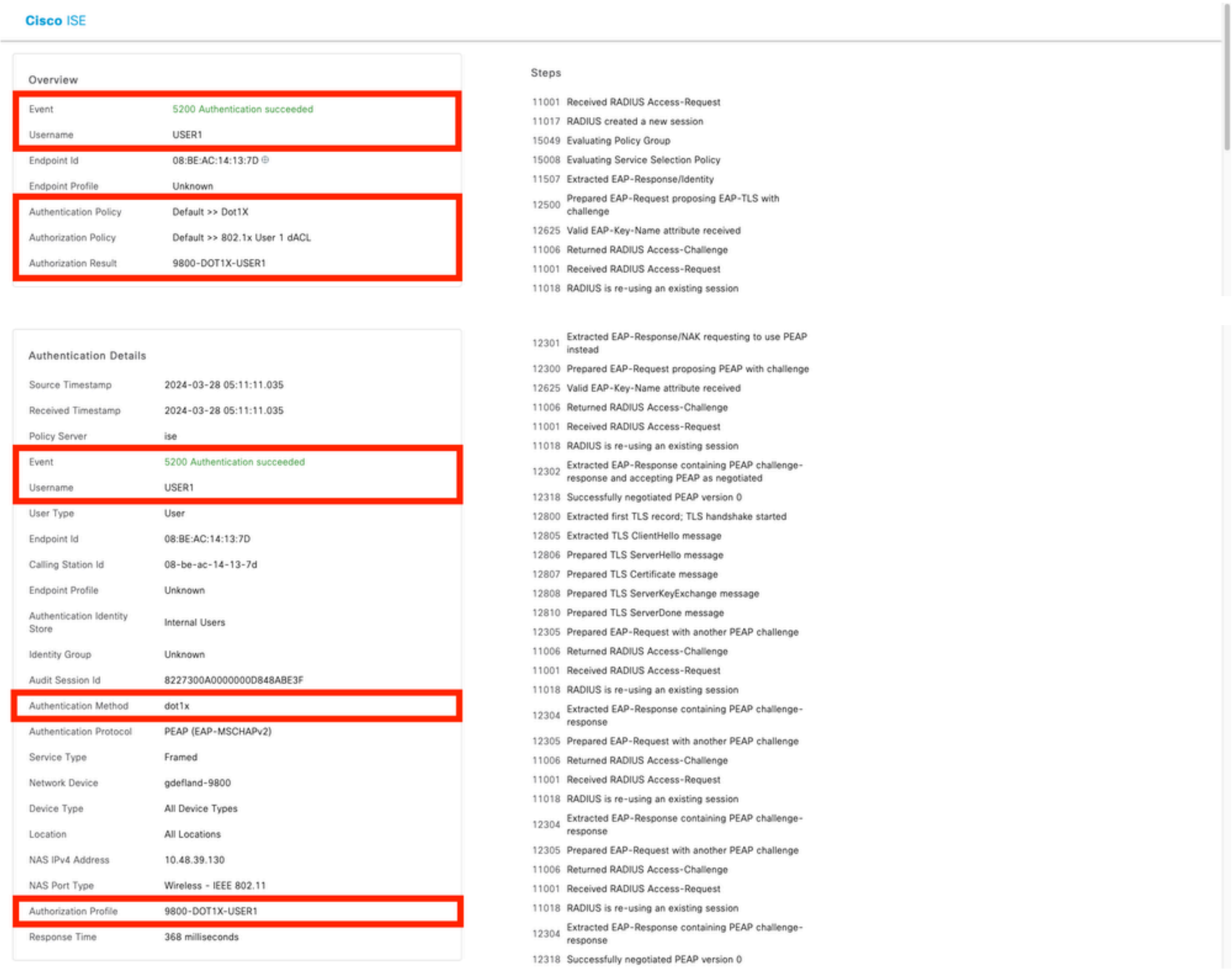


Opmerking: Als de inhoud van een download ACL wordt gewijzigd nadat deze op de WLC is gedownload, wordt de wijziging voor deze ACL niet weergegeven tot een gebruiker die deze gebruikt opnieuw authenticeert (en de WLC voert opnieuw een RADIUS-verificatie uit voor zo'n gebruiker). Een wijziging in de ACL wordt weerspiegeld door een wijziging in het hashgedeelte van de ACL-naam. Daarom moet de volgende keer dat deze ACL aan een gebruiker wordt toegewezen, de naam anders zijn en moet de ACL dus geen deel uitmaken van de WLC-configuratie en moet worden gedownload. Clients die voor de wijziging op de ACL authenticeren, blijven echter de vorige gebruiken totdat ze volledig opnieuw worden geauthenticeerd.

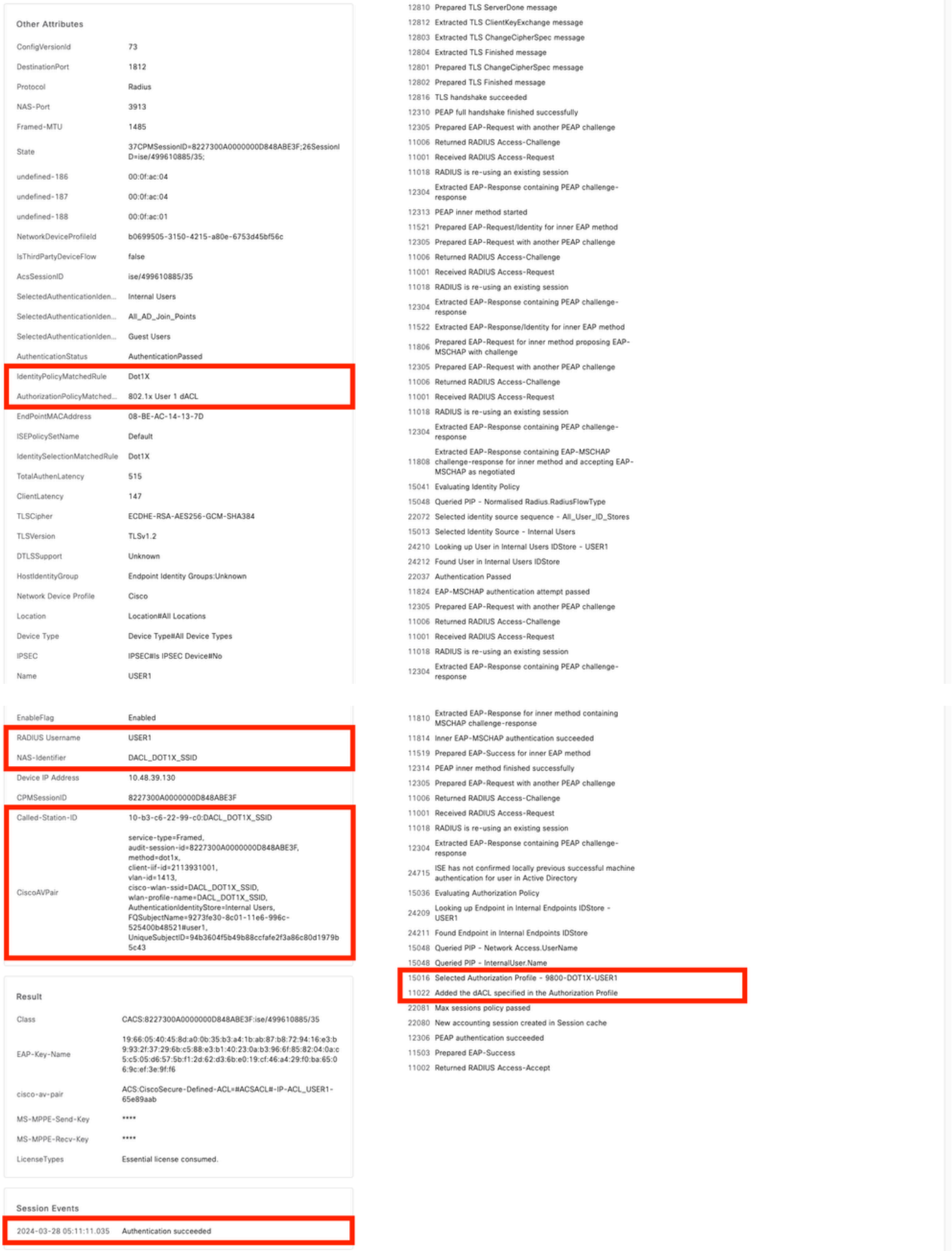
ISE-functielogboeken

RADIUS-clientverificatie

De verrichtingslogbestanden tonen een succesvolle verificatie van de gebruiker "USER1", waarop de downloadbare ACL "ACL_USER1" wordt toegepast. Delen van belang voor het oplossen van problemen worden in rood weergegeven.



Cisco ISE
Overview
Event
5200 Authentication succeeded
Username
USER1
Endpoint Id
08:BE:AC:14:13:7D
Endpoint Profile
Unknown
Authentication Policy
Default >> Dot1X
Authorization Policy
Default >> 802.1x User 1 dACL
Authorization Result
9800-DOT1X-USER1
Authentication Details
Source Timestamp
2024-03-28 05:11:11.035
Received Timestamp
2024-03-28 05:11:11.035
Policy Server
ise
Event
5200 Authentication succeeded
Username
USER1
User Type
User
Endpoint Id
08:BE:AC:14:13:7D
Calling Station Id
08-be-ac-14-13-7d
Endpoint Profile
Unknown
Authentication Identity Store
Internal Users
Identity Group
Unknown
Audit Session Id
8227300A0000000D848ABE3F
Authentication Method
dot1x
Authentication Protocol
PEAP (EAP-MSCHAPv2)
Service Type
Framed
Network Device
gdefland-9800
Device Type
All Device Types
Location
All Locations
NAS IPv4 Address
10.48.39.130
NAS Port Type
Wireless - IEEE 802.11
Authorization Profile
9800-DOT1X-USER1
Response Time
368 milliseconds
Steps
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
11507 Extracted EAP-Response/Identity
12500 Prepared EAP-Request proposing EAP-TLS with challenge
12625 Valid EAP-Key-Name attribute received
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12301 Extracted EAP-Response/NAK requesting to use PEAP instead
12300 Prepared EAP-Request proposing PEAP with challenge
12625 Valid EAP-Key-Name attribute received
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12302 Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated
12318 Successfully negotiated PEAP version 0
12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12810 Prepared TLS ServerDone message
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12318 Successfully negotiated PEAP version 0



Other Attributes

ConfigVersionId	73
DestinationPort	1812
Protocol	Radius
NAS-Port	3913
Framed-MTU	1485
State	37CPMSessionID=8227300A0000000D848ABE3F;26SessionID=ise/499610885/35;
undefined-186	00:0f:ac:04
undefined-187	00:0f:ac:04
undefined-188	00:0f:ac:01
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ise/499610885/35
SelectedAuthenticationIden...	Internal Users
SelectedAuthenticationIden...	All_AD_Join_Points
SelectedAuthenticationIden...	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Dot1X
AuthorizationPolicyMatched...	802.1x User 1 dACL
EndPointMACAddress	08-BE-AC-14-13-7D
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Dot1X
TotalAuthenLatency	515
ClientLatency	147
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Name	USER1

12810	Prepared TLS ServerDone message
12812	Extracted TLS ClientKeyExchange message
12803	Extracted TLS ChangeCipherSpec message
12804	Extracted TLS Finished message
12801	Prepared TLS ChangeCipherSpec message
12802	Prepared TLS Finished message
12816	TLS handshake succeeded
12310	PEAP full handshake finished successfully
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
12313	PEAP inner method started
11521	Prepared EAP-Request/Identity for inner EAP method
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
11522	Extracted EAP-Response/Identity for inner EAP method
11806	Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore - USER1
24212	Found User in Internal Users IDStore
22037	Authentication Passed
11824	EAP-MSCHAP authentication attempt passed
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response

EnableFlag	Enabled
RADIUS Username	USER1
NAS-Identifier	DACL_DOT1X_SSID
Device IP Address	10.48.39.130
CPMSessionID	8227300A0000000D848ABE3F
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID
CiscoAVPair	service-type=Framed, audit-session-id=8227300A0000000D848ABE3F, method=dot1x, client-iif-id=2113931001, vlan-id=1413, cisco-wlan-ssid=DACL_DOT1X_SSID, wlan-profile-name=DACL_DOT1X_SSID, AuthenticationIdentityStore=Internal Users, FQSubjectName=9273fe30-8c01-11e6-996c-525400b48521#user1, UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b5c43

11810	Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814	Inner EAP-MSCHAP authentication succeeded
11519	Prepared EAP-Success for inner EAP method
12314	PEAP inner method finished successfully
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge-response
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
24209	Looking up Endpoint in Internal Endpoints IDStore - USER1
24211	Found Endpoint in Internal Endpoints IDStore
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - InternalUser.Name
15016	Selected Authorization Profile - 9800-DOT1X-USER1
11022	Added the dACL specified in the Authorization Profile
22081	Max sessions policy passed
22080	New accounting session created in Session cache
12306	PEAP authentication succeeded
11503	Prepared EAP-Success
11002	Returned RADIUS Access-Accept

Result

Class	CACS:8227300A0000000D848ABE3F:ise/499610885/35
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:87:b8:72:94:16:e3:b9:93:2f:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:c5:c5:05:d6:57:5b:f1:2d:62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:06:9c:ef:3e:9f:f6
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1-65e89aab
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.

Session Events

2024-03-28 05:11:11.035	Authentication succeeded

DACL-download

De verrichtingslogboeken tonen een succesvolle download van ACL "ACL_USER1". Delen van belang voor het oplossen van problemen worden in rood weergegeven.

Cisco ISE

Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-ACL_USER1-65e89aab
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

Source Timestamp	2024-03-28 05:43:04.755
Received Timestamp	2024-03-28 05:43:04.755
Policy Server	ise
Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-ACL_USER1-65e89aab
Network Device	gdefland-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.48.39.130
Response Time	1 milliseconds

Other Attributes

ConfigVersionId	73
DestinationPort	1812
Protocol	Radius
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ise/499610885/48
TotalAuthenLatency	1
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	#ACSACL#-IP-ACL_USER1-65e89aab
Device IP Address	10.48.39.130
CPMSessionID	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcseM
CiscoAVPair	aaa:service=ip_admission, aaa:event=acl-download

Result

Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcseM:ise/499610885/48
cisco-av-pair	ip:inacl#1=deny ip any host 10.48.39.13
cisco-av-pair	ip:inacl#2=deny ip any host 10.48.39.15
cisco-av-pair	ip:inacl#3=deny ip any host 10.48.39.186
cisco-av-pair	ip:inacl#4=permit ip any any

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11117	Generated a new session ID
11002	Returned RADIUS Access-Accept

1

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.