# Configuration et dépannage des listes de contrôle d'accès téléchargeables sur Catalyst 9800

## Table des matières


- Introduction
- Informations générales
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
- Utilisation de dACL avec des SSID 802.1x
  - Diagramme du réseau
  - Configuration WLC
  - Configuration ISE
    - dACL par résultat
- Remarques sur l'utilisation des dACL avec les SSID CWA
- Vérifier
- Dépannage
  - Liste De Contrôle
  - WLC One Stop-Shop Reflex
  - Commandes show du WLC
  - Débogage conditionnel et suivi radioactif
  - Capture de paquets
    - Authentification du client RADIUS
    - Téléchargement DACL
  - Journaux des opérations ISE
    - Authentification du client RADIUS
    - Téléchargement DACL


## Introduction

Ce document décrit comment configurer et dépanner les ACL téléchargeables (dACL) sur le contrôleur LAN sans fil (WLC) Catalyst 9800.

---

## Informations générales

Une dACL fait référence au périphérique réseau qui télécharge dynamiquement les entrées de la liste de contrôle d'accès à partir du serveur RADIUS lors de l'authentification, plutôt que d'avoir une copie locale de la liste de contrôle d'accès et de se voir attribuer le nom de la liste. Un exemple de configuration Cisco ISE plus complet est disponible. Ce document se concentre sur le Cisco Catalyst 9800 qui prend en charge les dACL pour la commutation centrale depuis la version 17.10.

---

# Conditions préalables

Ce document vise à démontrer l'utilisation des dACL sur Catalyst 9800 à travers des exemples de configuration SSID de base, montrant comment ceux-ci peuvent être entièrement personnalisables.

Sur le contrôleur sans fil Catalyst 9800, les listes de contrôle d'accès téléchargeables sont :

- Pris en charge à partir de la version Cisco IOS XE Dublin 17.10.1.
- Prise en charge pour contrôleur centralisé avec points d'accès en mode local uniquement (ou commutation centrale Flexconnect).
    - La commutation locale FlexConnect ne prend pas en charge dACL.

---

## Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Modèle de configuration Catalyst Wireless 9800.
- Listes de contrôle d'accès IP (ACL) Cisco.

---

## Composants utilisés

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

- Catalyst 9800-CL (v. Dublin 17.12.03)

- ISE (v. 3.2)

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.

---

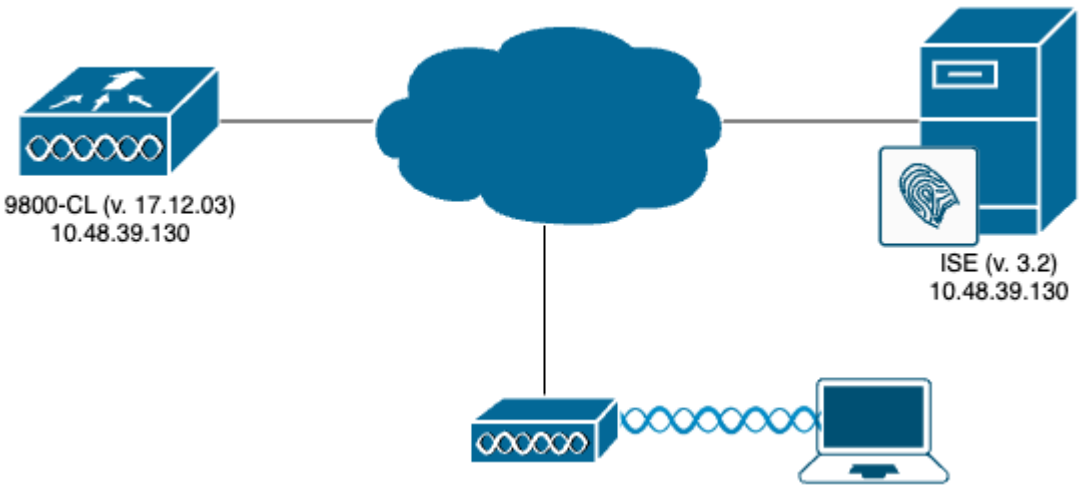
# Configurer

Tout au long de ce guide de configuration, même si les méthodes sont différentes (par exemple, authentification WLAN, configuration des politiques, etc.), le résultat final est le même. Dans le scénario suivant, deux identités utilisateur sont définies comme USER1 et USER2. L'accès au réseau sans fil est accordé aux deux utilisateurs. Chacune se voit attribuer ACL_USER1 et ACL_USER2 en tant que dACL téléchargées par le Catalyst 9800 depuis ISE.

---

# Utilisation de dACL avec des SSID 802.1x

## Diagramme du réseau




---

## Configuration WLC

Pour plus de détails sur la configuration des SSID 802.1x et le dépannage sur Catalyst 9800, référez-vous au guide Configurer l'authentification 802.1x sur le contrôleur sans fil de la gamme Catalyst 9800.

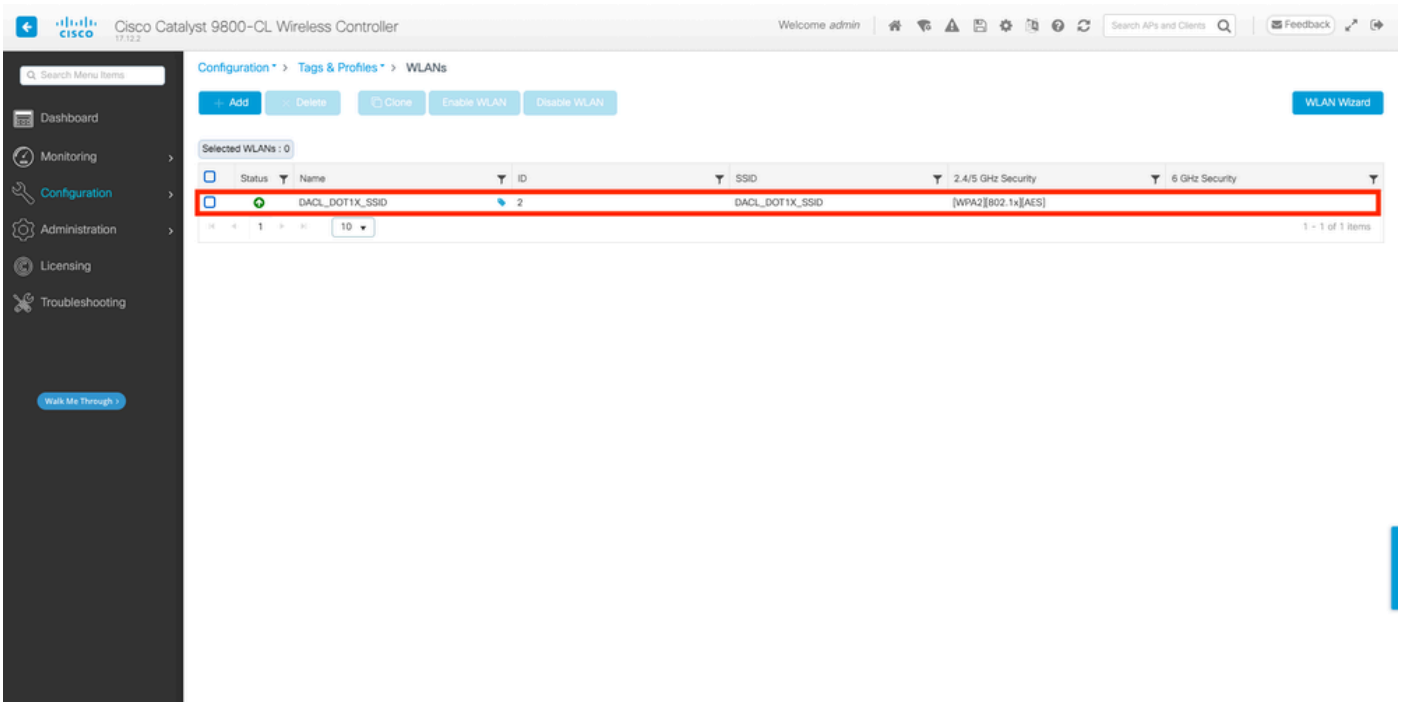
1. Configurez le SSID. Configurez un SSID authentifié 802.1x, en utilisant ISE comme serveur RADIUS. Dans ce document, le SSID a été nommé DACL_DOT1X_SSID.

---

À partir de l'interface utilisateur :

2. Accédez à Configuration > Tags & Profiles > WLAN et créez un WLAN :

---




---

À partir de la 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
```

---

3. Configurez le profil de stratégie. Configurez le profil de stratégie utilisé avec le SSID défini précédemment. Sur ce profil de stratégie, assurez-vous que AAA Override est configuré à partir de l'onglet Avancé, comme indiqué dans la capture d'écran. Dans ce document, le profil de stratégie utilisé est DACL-8021X.

---

3 bis. Comme indiqué dans la section des conditions préalables, les dACL sont uniquement prises

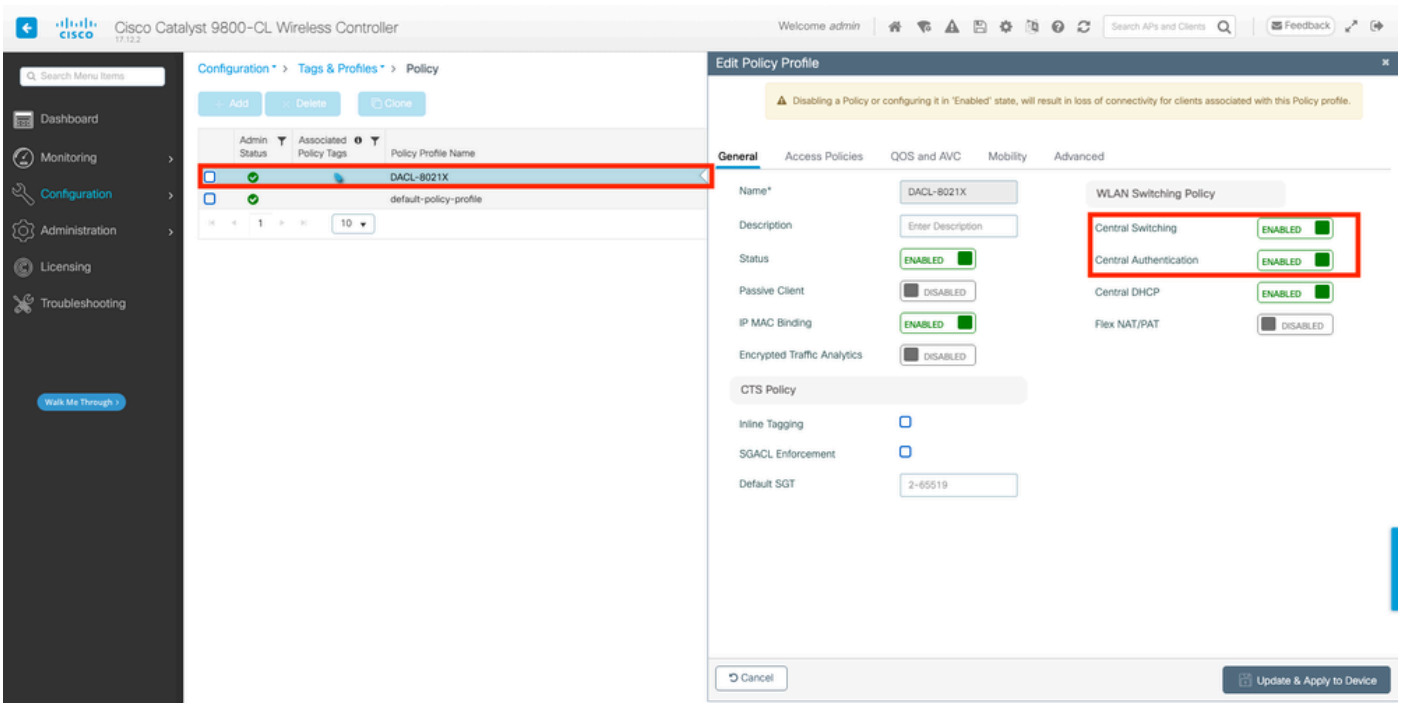
en charge pour les déploiements de commutation/d'authentification centralisés. Assurez-vous que le profil de stratégie est configuré de cette façon.

---

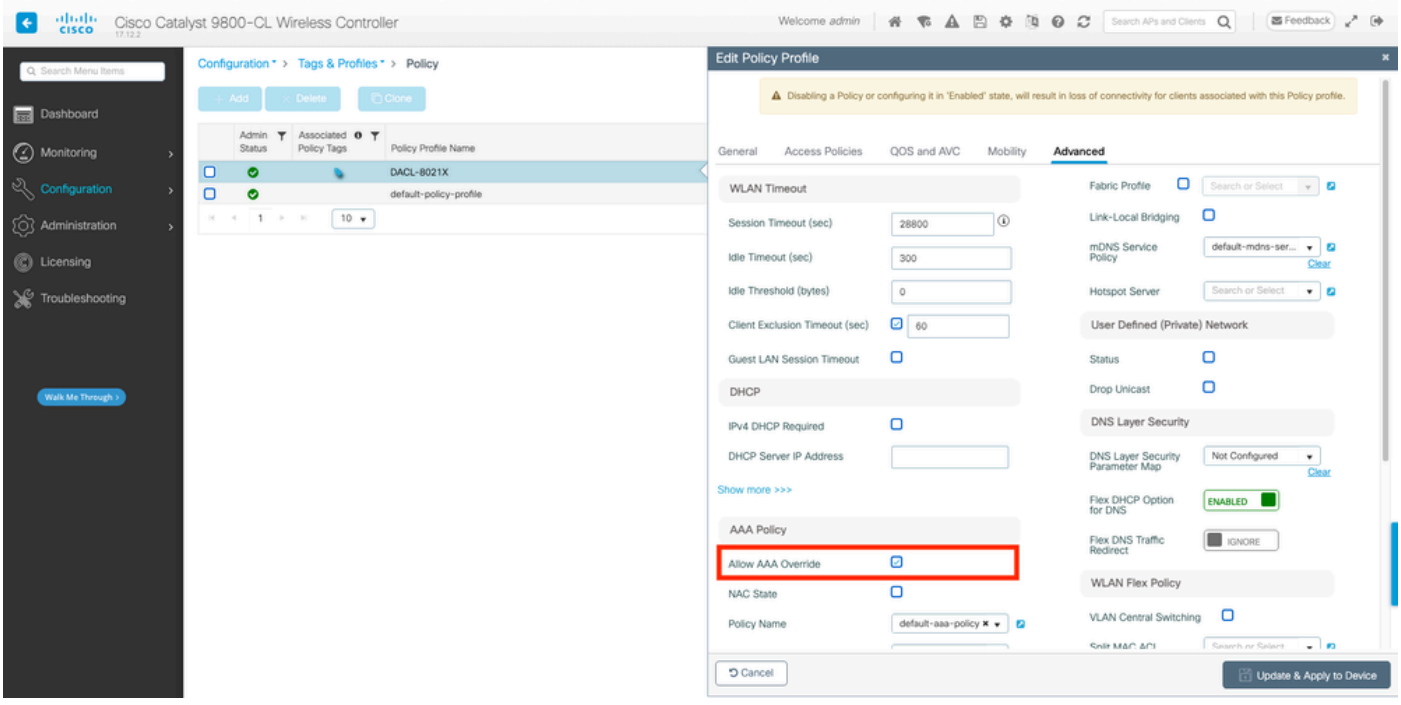
À partir de l'interface utilisateur :

1. Accédez à Configuration > Tags & Profiles > Policy, sélectionnez le profil de stratégie utilisé et configurez comme indiqué dans la capture d'écran suivante :

---




---




---

À partir de la 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
```

---

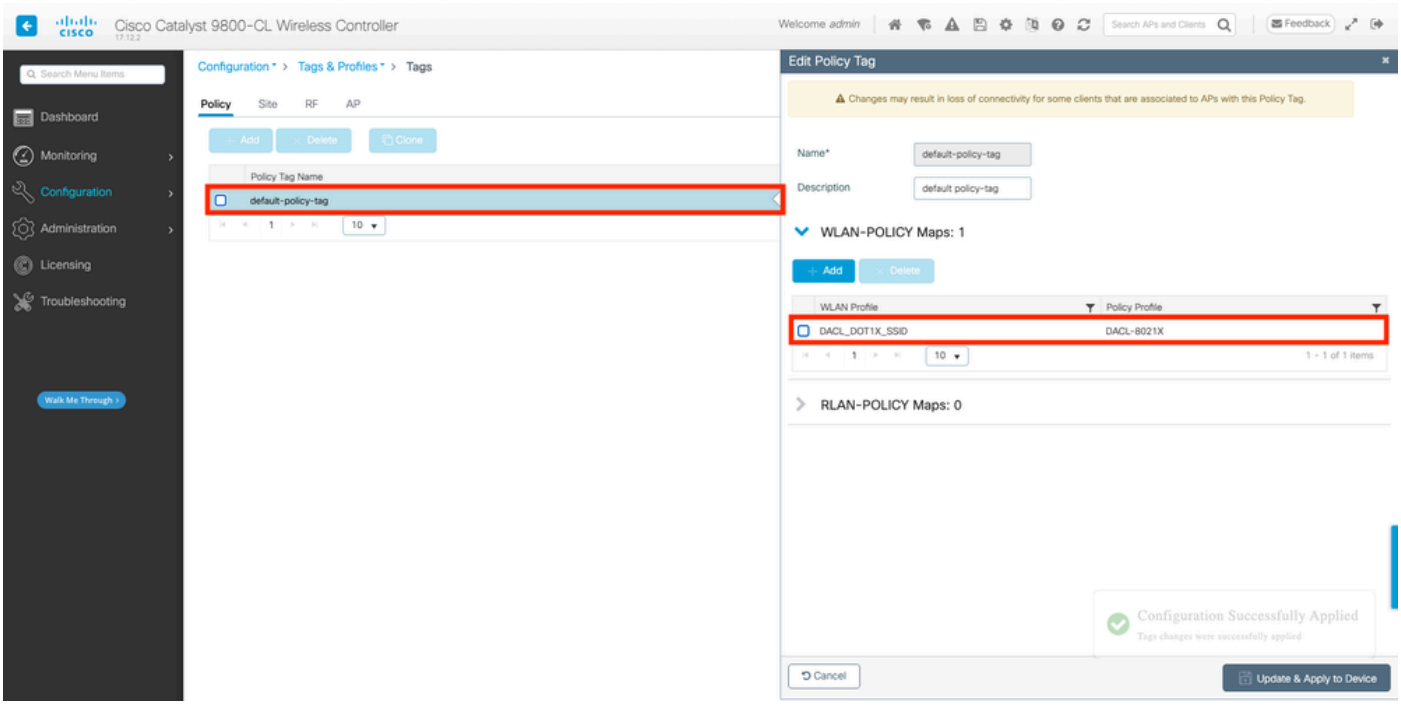
2. Attribuez le profil de stratégie et le SSID à la balise de stratégie utilisée.

---

À partir de l'interface utilisateur :

3. Accédez à Configuration > Tags & Profiles > Tags. Dans l'onglet Balises de stratégie, créez (ou sélectionnez) la balise utilisée et attribuez le WLAN et le profil de stratégie définis au cours des étapes 1 à 2.

---




---

À partir de la 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
```

4. Autorisez les attributs spécifiques au fournisseur. Les listes de contrôle d’accès téléchargeables sont transmises via les attributs spécifiques au fournisseur (VSA) dans l’échange RADIUS entre ISE et le WLC. La prise en charge de ces attributs peut être activée sur le WLC en exécutant ces commandes CLI.

---

À partir de la CLI :

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

---

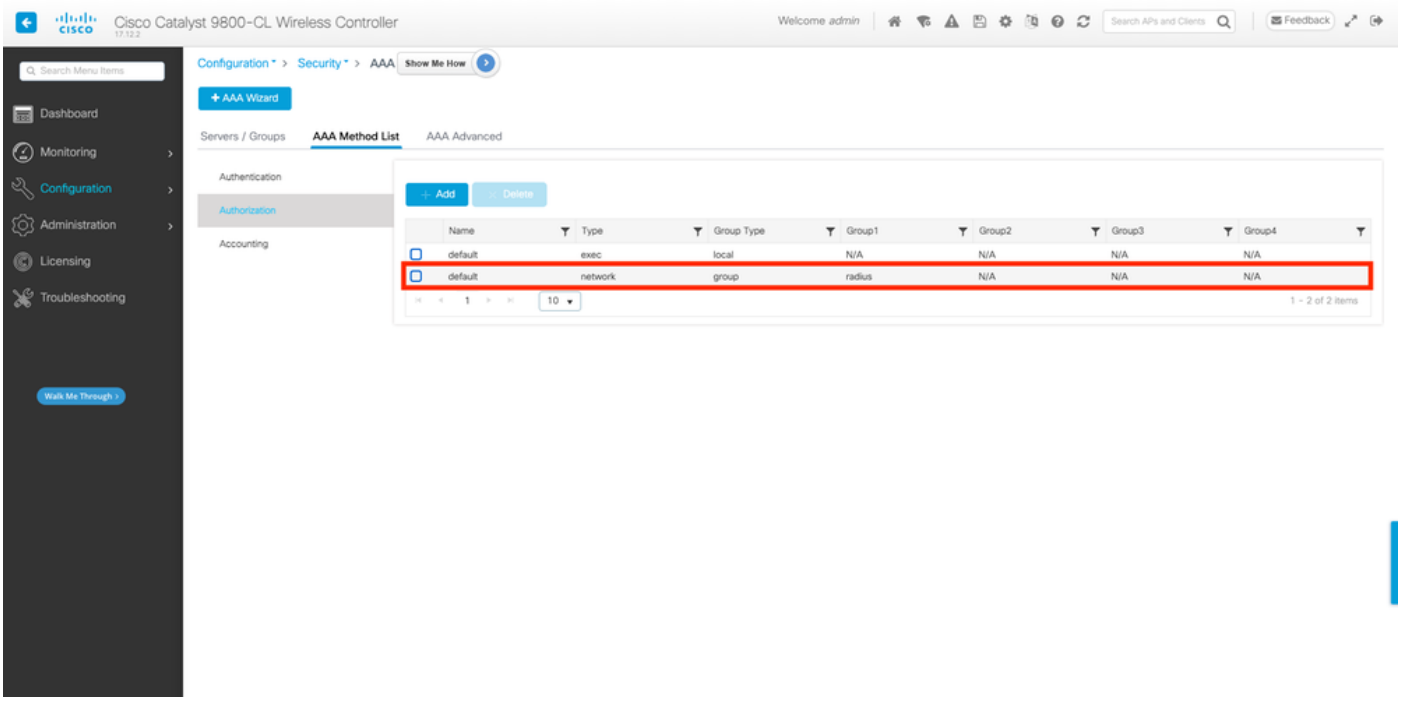
5. Configurez la liste d’autorisations par défaut. Lors de l'utilisation d'une dACL, l'autorisation réseau via RADIUS doit être appliquée pour que le WLC autorise tout utilisateur s'authentifiant sur le SSID 802.1x configuré. La phase d'autorisation est gérée du côté du serveur RADIUS. Par conséquent, la liste d'autorisation est requise. Les dACL nécessitent l'utilisation de la méthode aaa authorization network. Vous pouvez utiliser le rayon du groupe par défaut avec la commande aaa authorization network default group radius :

---

À partir de l'interface utilisateur :

1. Accédez à Configuration **>** Security **>** AAA et à partir de la Liste de méthodes AAA **>** Autorisation onglet, créez une méthode d'autorisation semblable à la capture d'écran suivante :

---




---

À partir de la CLI :

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

---

Si vous ne souhaitez pas définir de méthode par défaut, vous devez définir une méthode nommée. Dans ce cas, il est obligatoire d'appeler la liste de méthodes d'autorisation AAA qu'ISE doit utiliser, sinon le WLC ne peut pas télécharger la liste de contrôle d'accès :

Sur le WLC :

<#root>

```
WLC(config)# aaa authorization network
```

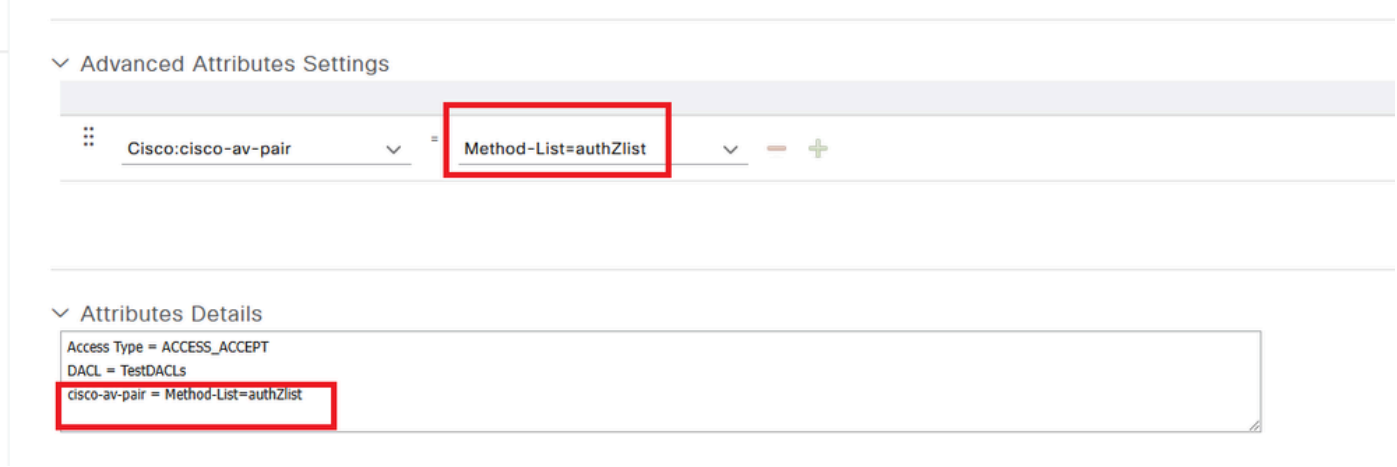
**authZlist**

```
 group authz-server-group
```

---

Sur l'ISE, envoyez cet attribut avec la dACL : cisco-av-pair = Method-List=authZlist

---




---

## Configuration ISE

Lors de la mise en oeuvre de dACL dans un environnement sans fil avec ISE, deux configurations communes sont possibles :

1. Configuration de la dACL par utilisateur : Ainsi, une dACL est attribuée à chaque identité particulière en raison d'un champ d'identité personnalisé.

2. Configuration dACL par résultat : Lorsque vous optez pour cette méthode, une dACL particulière est attribuée à un utilisateur en fonction de la stratégie d'autorisation qu'elle a trouvée dans le jeu de stratégies utilisé.

---

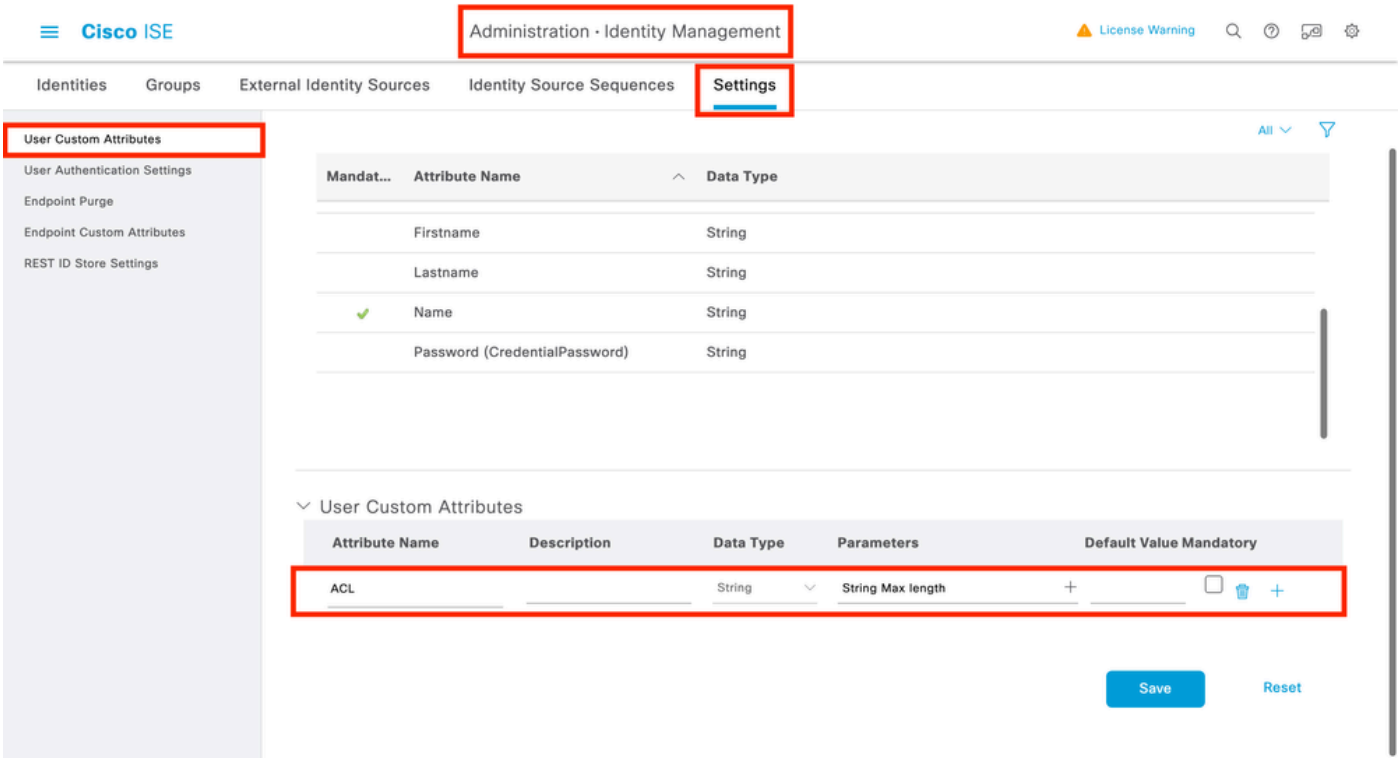
dACL par utilisateur

1. Définissez un attribut utilisateur personnalisé dACL. Pour attribuer une dACL à une identité d'utilisateur, ce champ doit être configurable sur l'identité créée. Par défaut, sur ISE, le champ ACL n'est pas défini pour toute nouvelle identité créée. Pour remédier à cela, vous pouvez utiliser l'attribut d'utilisateur personnalisé et définir un nouveau champ de configuration.

---

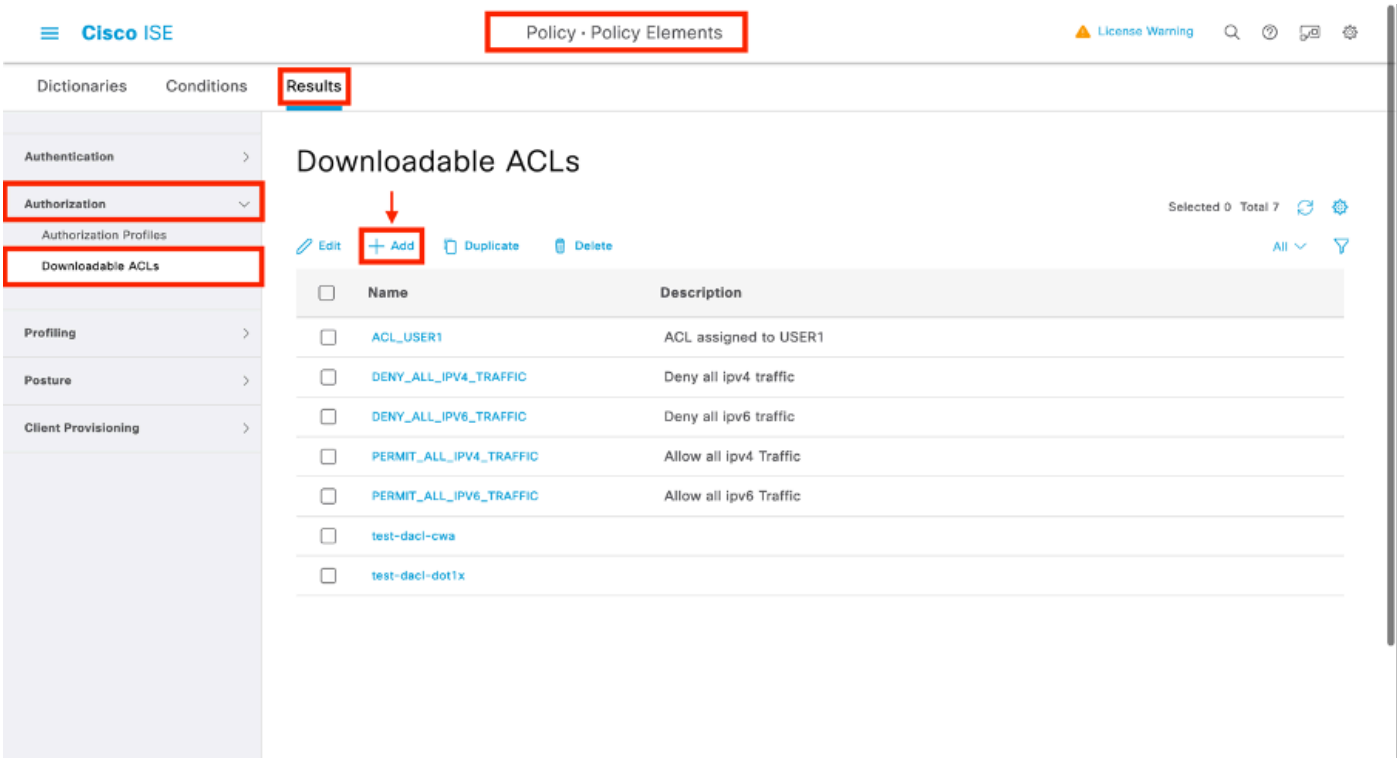
2. Accédez à Administration > Gestion des identités > Paramètres > Attributs personnalisés utilisateur. Utilisez le bouton + pour ajouter un nouvel attribut. Dans cet exemple, le nom de l'attribut personnalisé est ACL:

---




3. Une fois configuré, cliquez sur Enregistrer.

4. Configurez la dACL. Accédez à Policy > Policy Elements > Results > Authorization > Downloadable ACLs pour afficher et définir dACL sur ISE. Cliquez sur le bouton Add pour en créer un nouveau.



5. Un formulaire de configuration Nouvelle liste de contrôle d'accès téléchargeable s'ouvre. Dans ce formulaire, configurez ces champs :

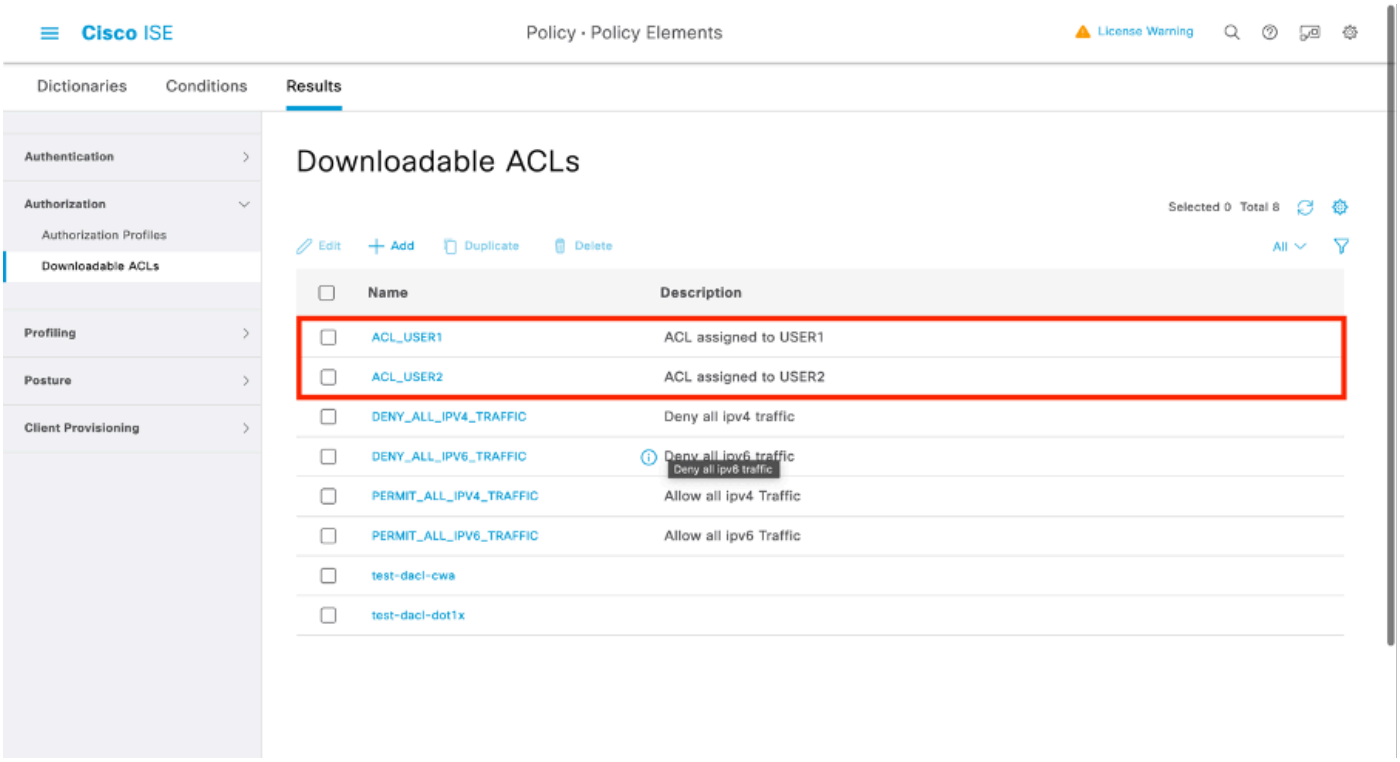
- Name : Nom de la dACL définie.
- Description (facultatif) : Brève description de l'utilisation de la dACL créée.
- Version IP : Version du protocole IP utilisée dans la dACL définie (version 4, 6 ou les deux).
- Contenu DACL : Le contenu de la dACL, conformément à la syntaxe de la liste de contrôle d'accès Cisco IOS XE®.

---

Dans ce document, la dACL utilisée est ACL_USER1 et cette dACL autorise tout trafic sauf celui destiné à 10.48.39.186 et 10.48.39.13. Une fois les champs configurés, cliquez sur le bouton Submit pour créer la dACL.

Répétez l'étape pour définir la dACL pour le deuxième utilisateur, ACL_USER2.

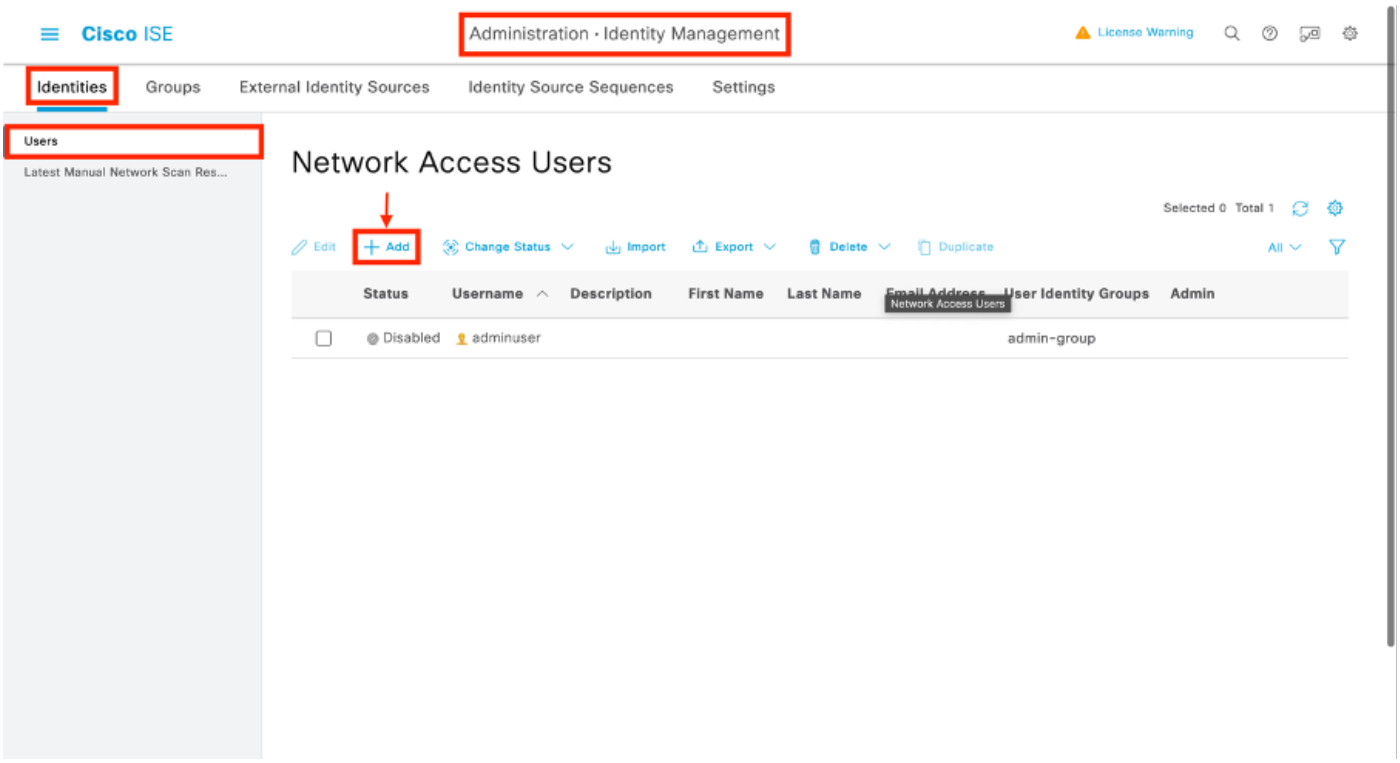
---




---

6. Attribuez la dACL à une identité créée. Une fois la dACL créée, vous pouvez l'attribuer à n'importe quelle identité ISE en utilisant les Attributs personnalisés utilisateur créés à l'étape 1. TNavigate to Administration > Identity Management > Identities > Users. Cliquez sur Add pour créer un utilisateur.

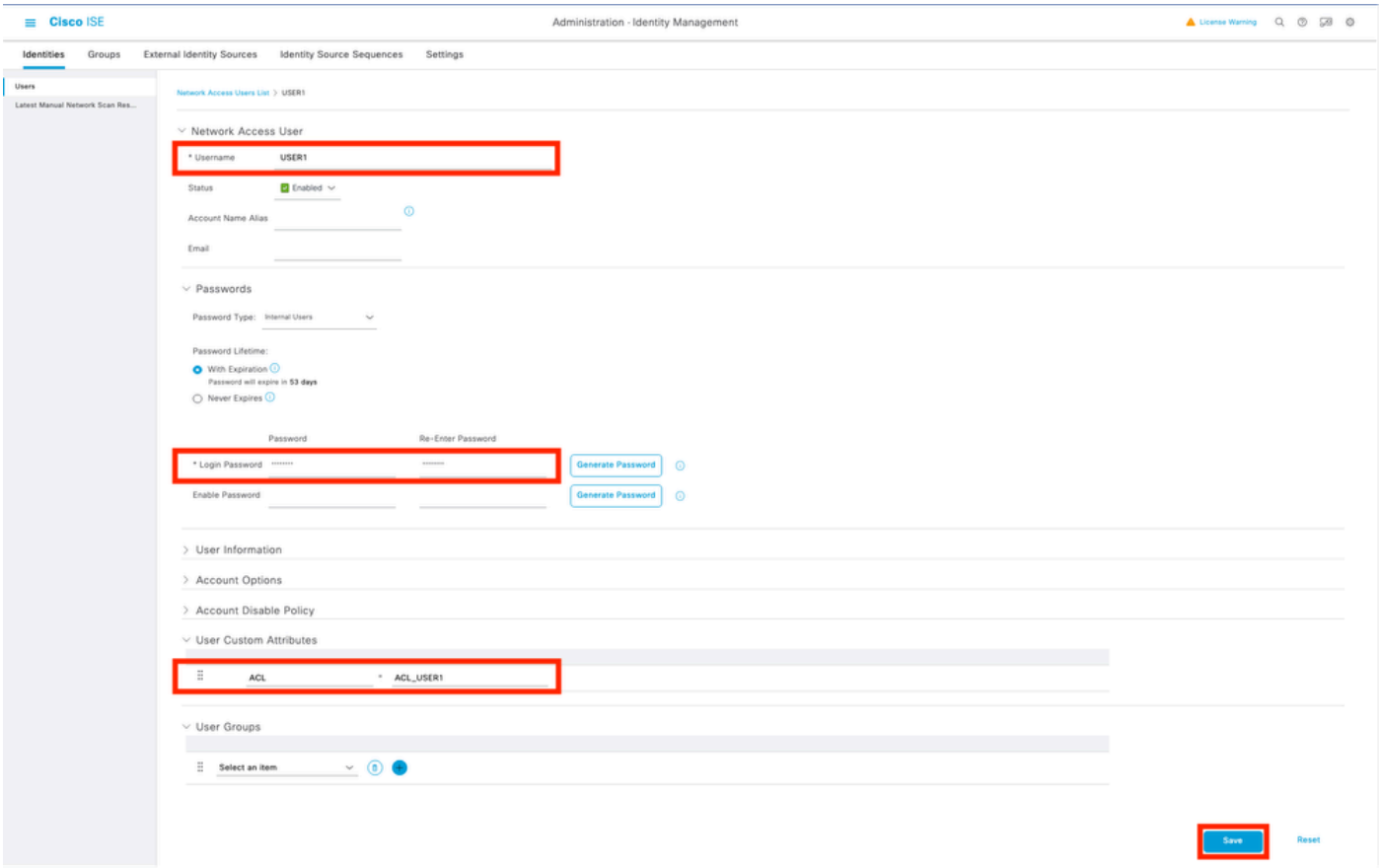
---



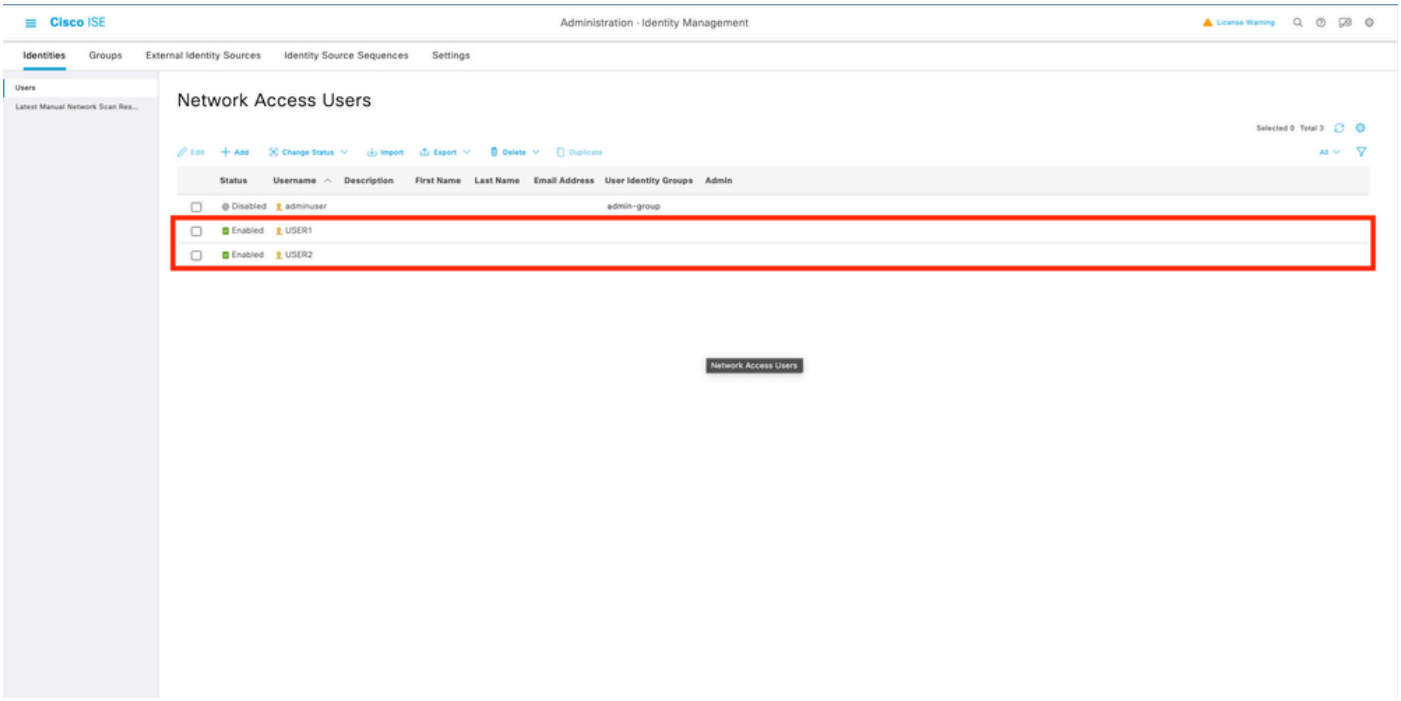

---

7. Dans l'écran de configuration Nouvel utilisateur d'accès au réseau, définissez le nom d'utilisateur et le mot de passe de l'utilisateur créé. Utilisez l'ACL d'attribut personnalisé pour affecter la dACL créée à l'étape 2 à l'identité. Dans l'exemple, l'identité USER1 utilisant ACL_USER1 est définie.

---




8. Une fois les champs correctement configurés, cliquez sur Submit pour créer l'identité. Répétez cette étape pour créer USER2 et lui attribuer ACL_USER2.



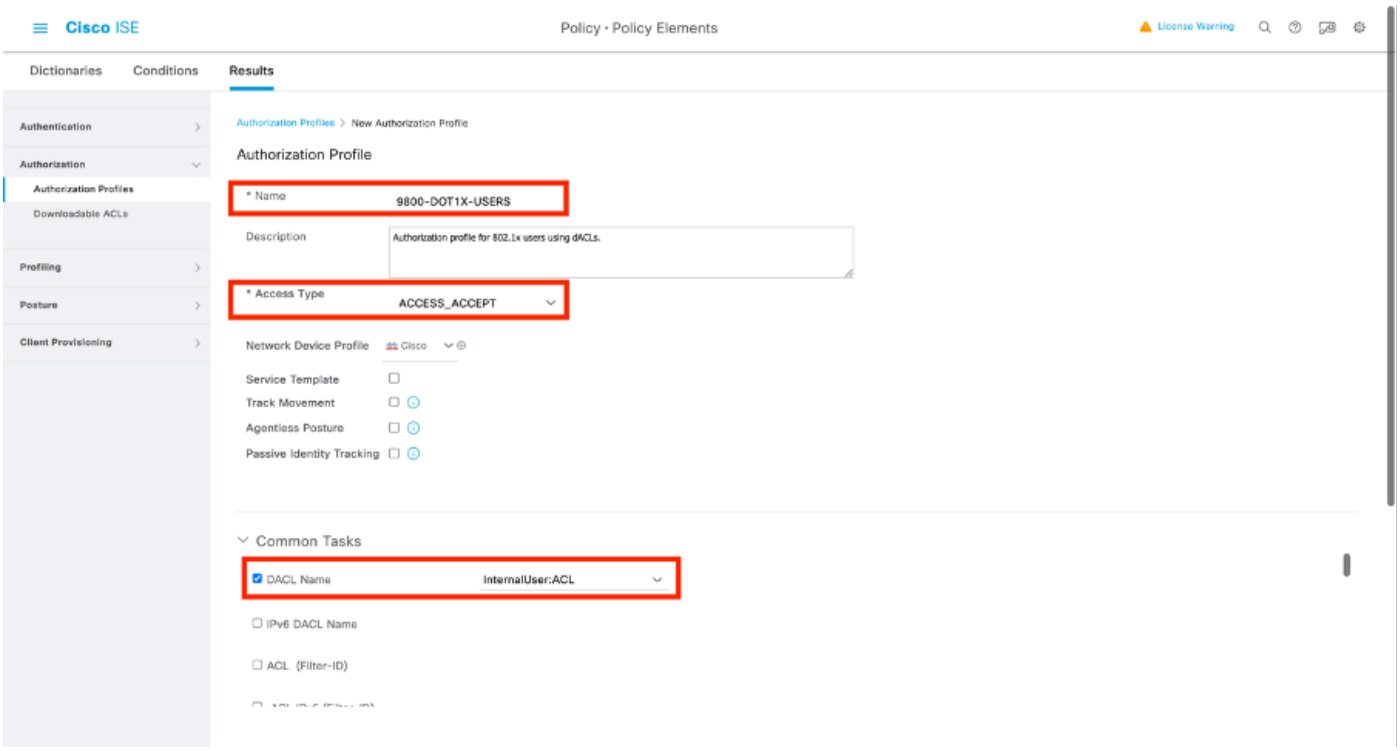
9. Configurez le résultat de la stratégie d'autorisation. Une fois l'identité configurée et la dACL attribuée, la stratégie d'autorisation doit toujours être configurée pour faire correspondre la liste de contrôle d'accès d'attribut utilisateur personnalisée définie à une tâche commune d'autorisation existante.

---

10. Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles. Cliquez sur Add pour définir une nouvelle stratégie d'autorisation.

- Name : Le nom de la stratégie d'autorisation, dans cet exemple, 9800-DOT1X-USERS est utilisé.
- Type d'accès : Le type d'accès utilisé lorsque cette stratégie est mise en correspondance, dans cet exemple ACCESS_ACCEPT est utilisé.
- Tâche courante : Associez DACL Name à InternalUser:<nom de l'attribut personnalisé créé> pour l'utilisateur interne. Selon les noms utilisés dans ce document, le profil 9800-DOT1X-USERS est configuré avec la dACL configurée comme InternalUser:ACL.

---




---

11. Utilisez le profil d'autorisation dans l'ensemble de stratégies. Une fois le résultat du profil d'autorisation correctement défini, il doit faire partie du jeu de stratégies utilisé pour authentifier et autoriser les utilisateurs sans fil.

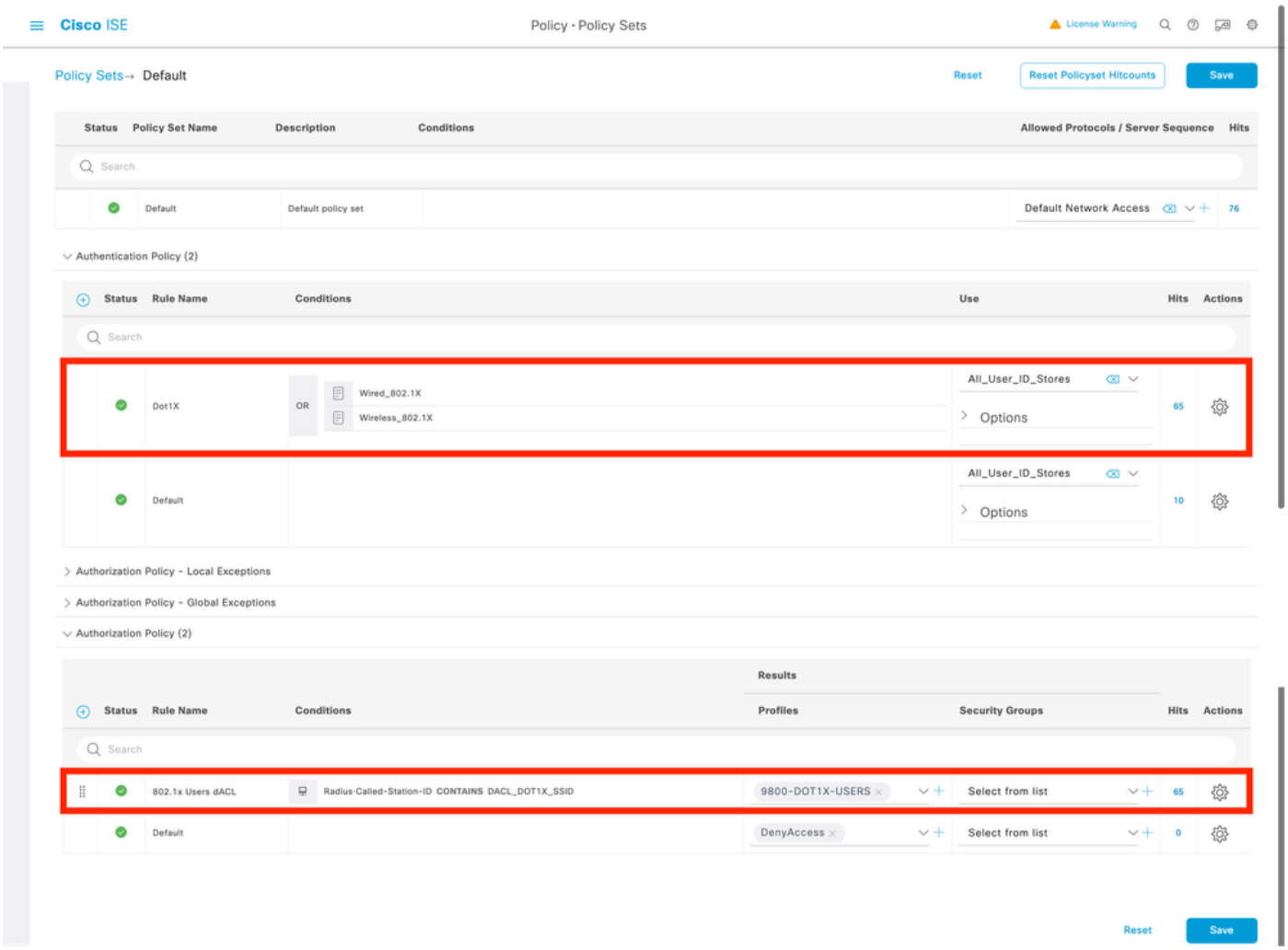
---

12. Accédez à Policy > Policy Sets et ouvrez le jeu de stratégies utilisé.

---

13. La règle de stratégie d'authentification Dot1X correspond à toute connexion établie via la norme 802.1x câblée ou sans fil. La règle de stratégie d'autorisation 802.1x Users dACL implémente une condition sur le SSID utilisé (c'est-à-dire Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID). Si une autorisation est effectuée sur le WLAN DACL_DOT1X_SSID, le profil 9800-DOT1X-USERS défini à l'étape 4 est utilisé pour autoriser l'utilisateur.

---




---

dACL par résultat

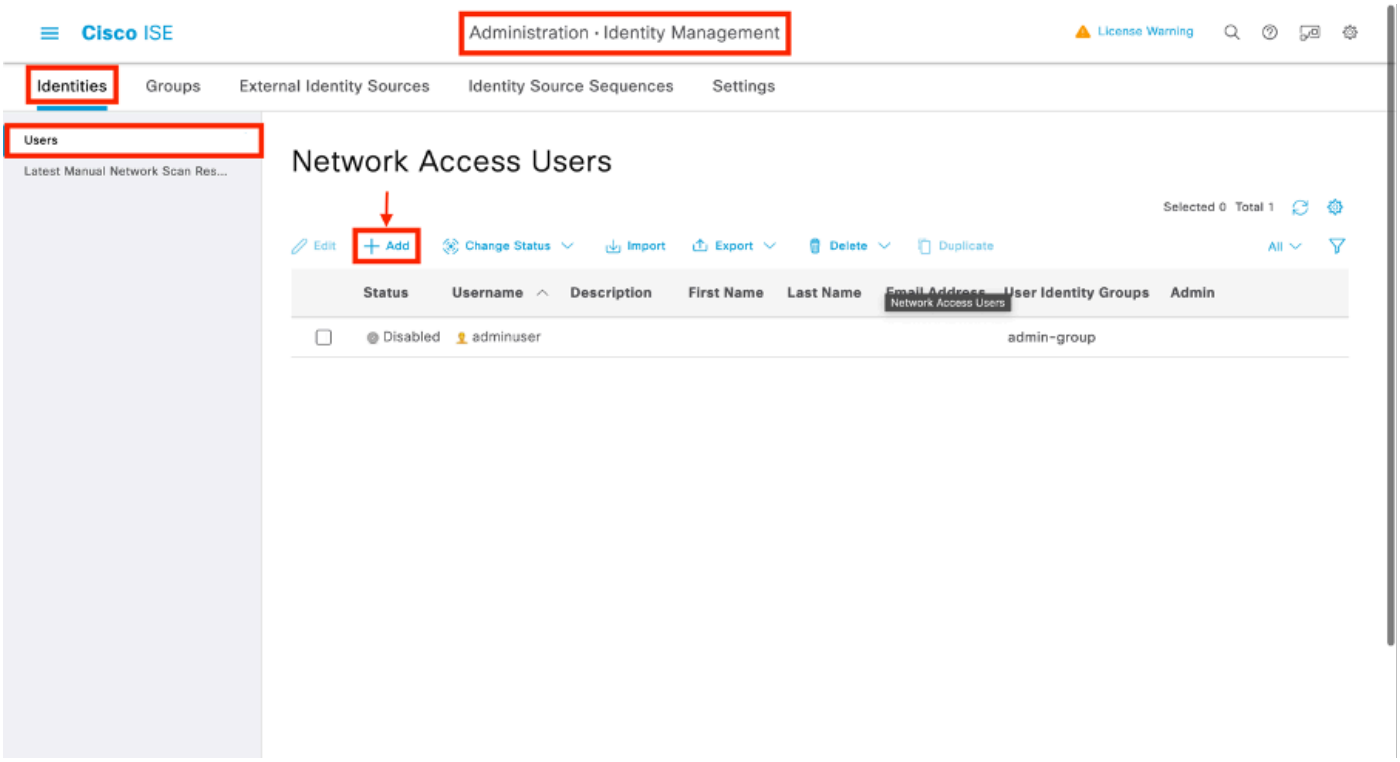
Pour éviter d'attribuer une dACL particulière à chaque identité créée sur ISE, vous pouvez choisir d'appliquer la dACL à un résultat de stratégie spécifique. Ce résultat est ensuite appliqué en fonction de toute condition correspondant aux règles d'autorisation du jeu de stratégies utilisé.

---

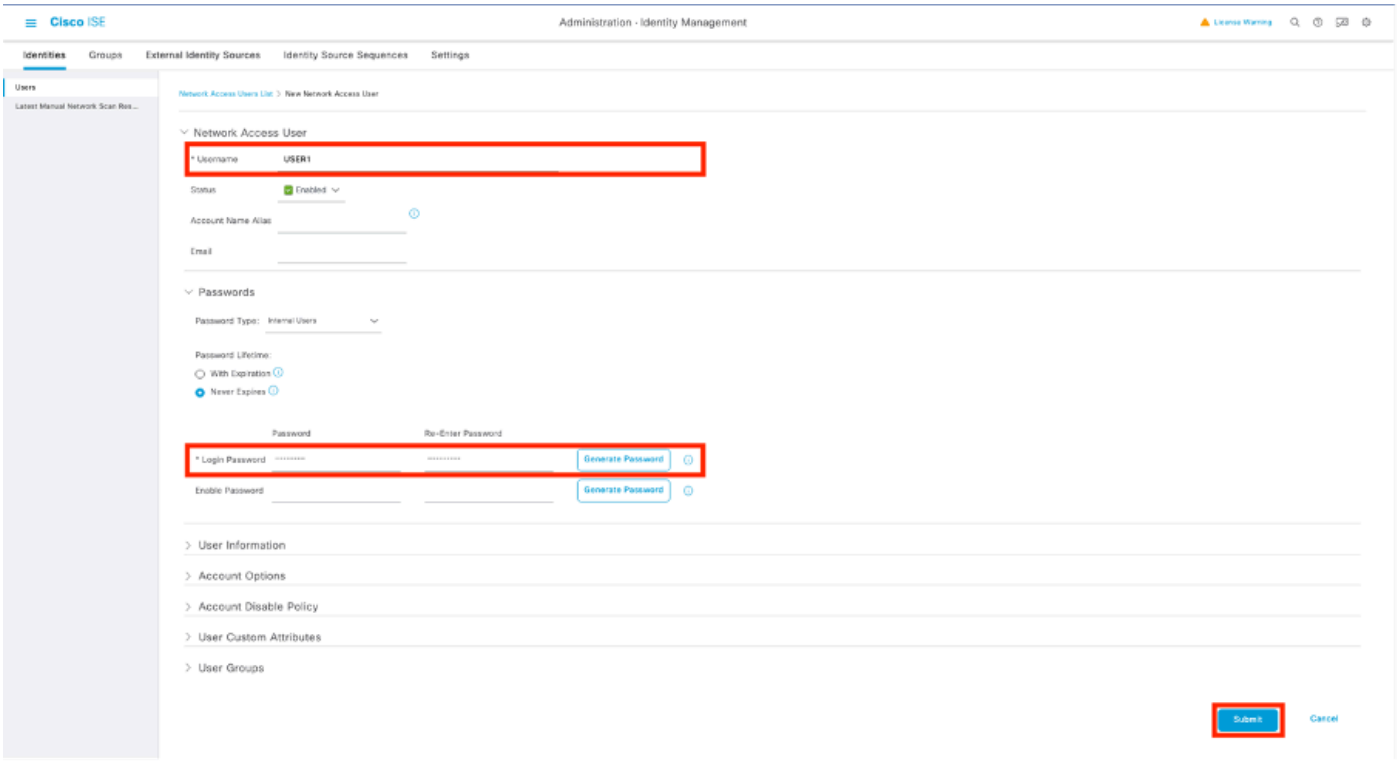
1. Configurez la dACL. Exécutez les mêmes étapes à partir de l'étape 2 de la section dACL par utilisateur pour définir les dACL requises. Il s'agit de ACL_USER1 et ACL_USER2.

---

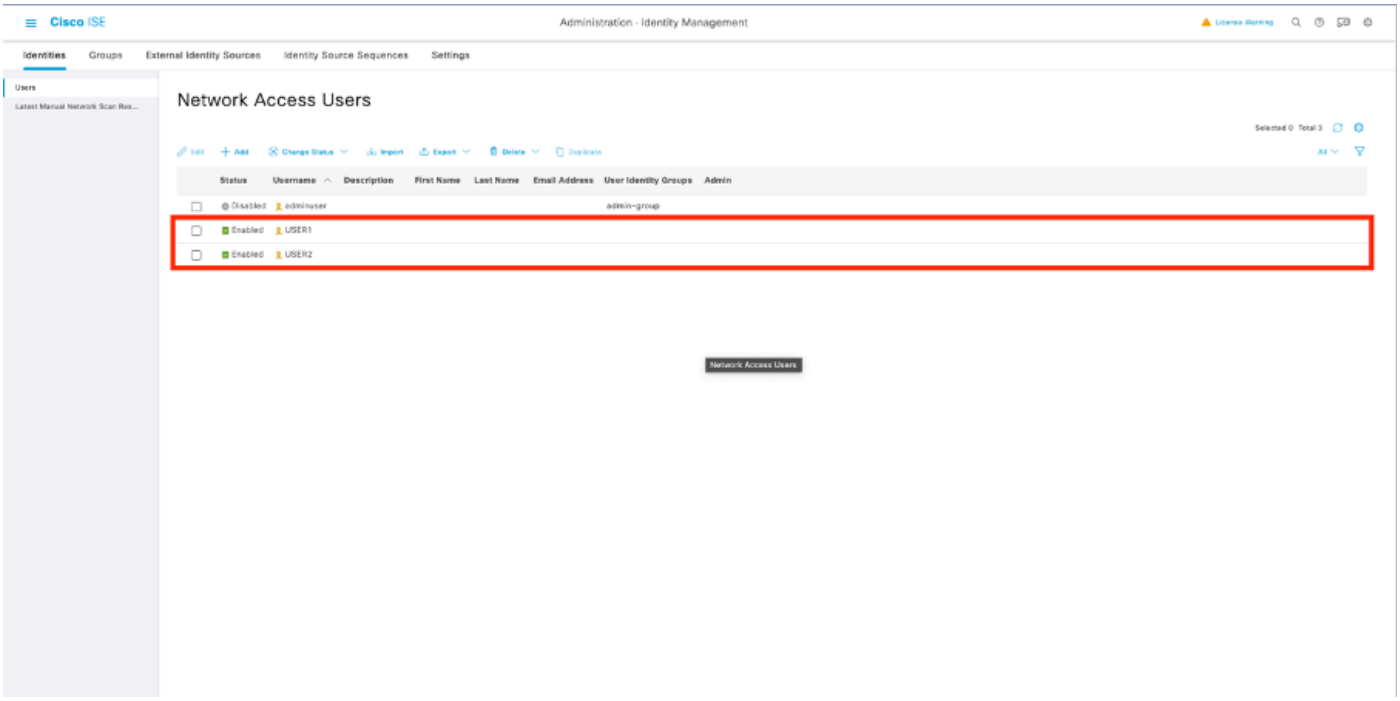
2. Créez des identités. Accédez à Administration > Identity Management > Identities > Users et cliquez sur le bouton Add pour créer un utilisateur.




3. Dans l'écran de configuration Nouvel utilisateur d'accès au réseau, définissez le nom d'utilisateur et le mot de passe de l'utilisateur créé.



4. Répétez cette étape pour créer USER2.




---

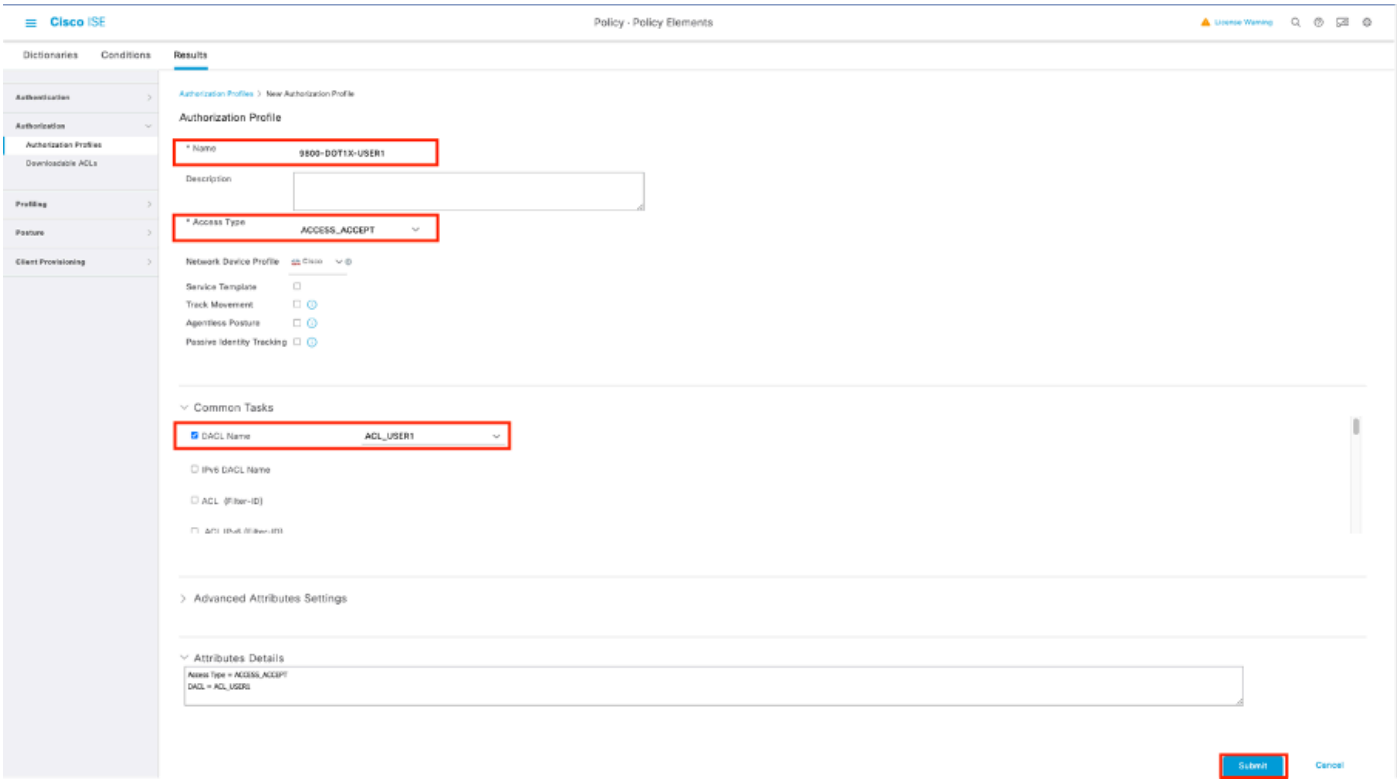
5. Configurez le résultat de la stratégie d'autorisation. Une fois l'identité et la dACL configurées, la stratégie d'autorisation doit toujours être configurée pour attribuer une dACL spécifique à l'utilisateur correspondant à la condition d'utilisation de cette stratégie.

---

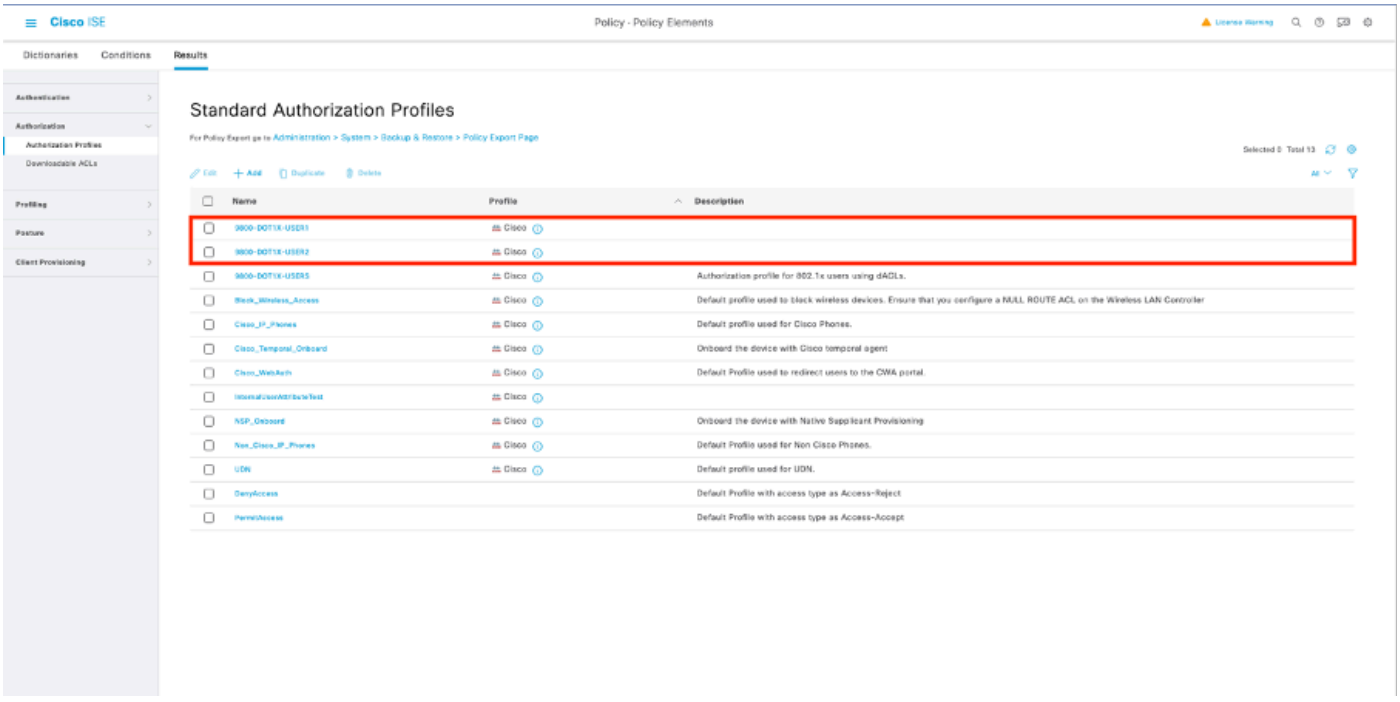
6. Pour ce faire, accédez à Stratégie > Eléments de stratégie > Résultats > Autorisation > Profils d'autorisation. Cliquez sur Add pour définir une nouvelle stratégie d'autorisation et renseignez les champs suivants :

- Name : Le nom de la stratégie d'autorisation, dans cet exemple 9800-DOT1X-USER1 est utilisé.
- Type d'accès : Type d'accès utilisé lorsque cette stratégie est mise en correspondance. Dans cet exemple, ACCESS_ACCEPT est utilisé.
- Tâche courante : Associez le nom de la DACL à ACL_USER1 pour un utilisateur interne. Selon les noms utilisés dans ce document, le profil 9800-DOT1X-USER1 est configuré avec la dACL configurée comme ACL_USER1.

---




7. Répétez cette étape pour créer le résultat de stratégie 9800-DOT1X-USER2 et lui affecter ACL_USER2 comme DACL.



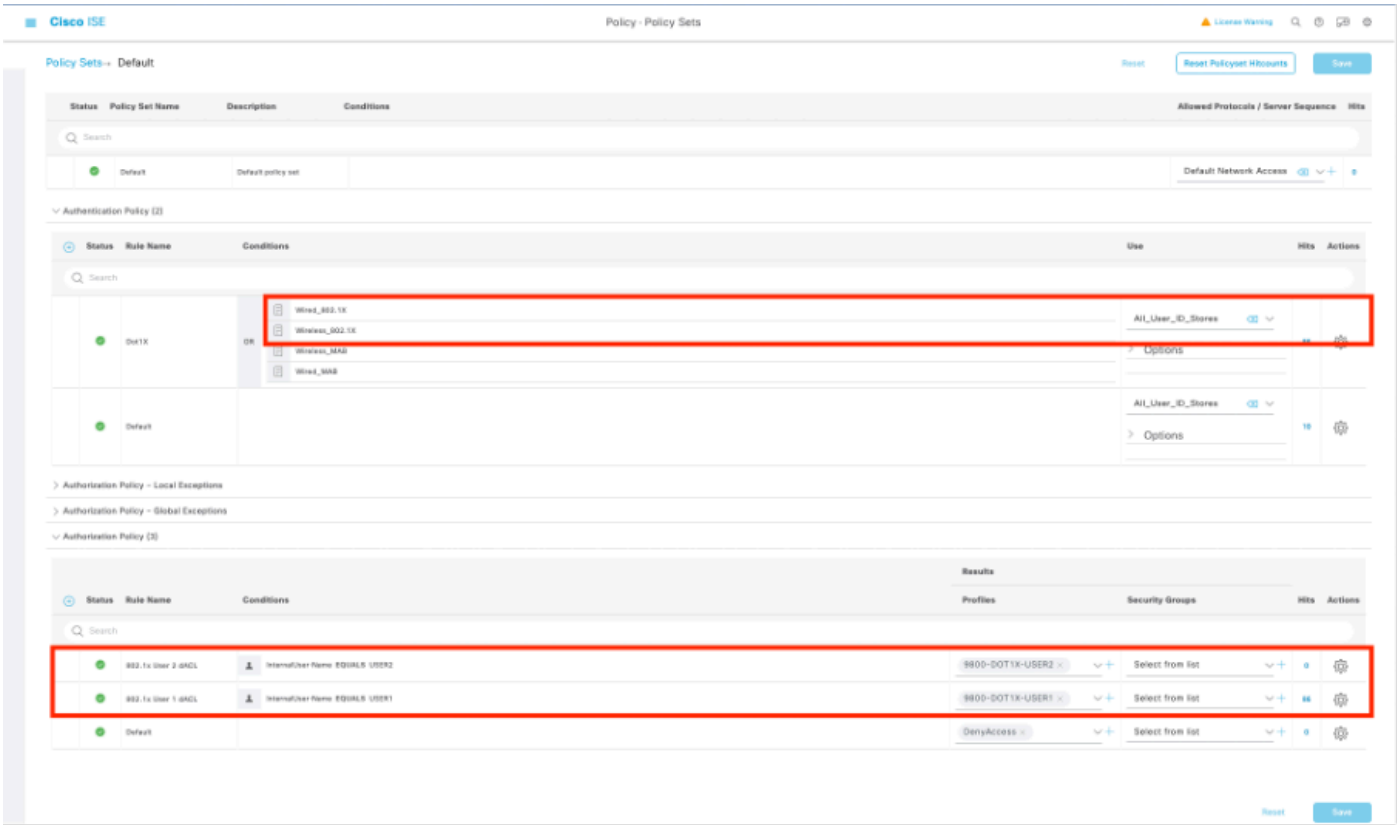

8. Utilisez des profils d'autorisation dans un jeu de stratégies. Une fois que les résultats du profil d'autorisation sont correctement définis, ils doivent toujours faire partie du jeu de stratégies utilisé pour authentifier et autoriser les utilisateurs sans fil.

9. Accédez à Policy > Policy Sets et ouvrez le jeu de stratégies utilisé.

---

10. La règle de stratégie d'authentification Dot1X correspond à toute connexion établie via 802.1X filaire ou sans fil. La règle de stratégie d'autorisation 802.1X User 1 dACL implémente une condition sur le nom d'utilisateur utilisé (c'est-à-dire InternalUser-Name CONTAINS USER1). Si une autorisation est effectuée à l'aide du nom d'utilisateur USER1, le profil 9800-DOT1X-USER1 défini à l'étape 4 est utilisé pour autoriser l'utilisateur et la dACL de ce résultat (ACL_USER1) est appliquée à l'utilisateur. La même chose est configurée pour le nom d'utilisateur USER2 où 9800-DOT1X-USER1 est utilisé.

---




---

# Remarques sur l'utilisation des dACL avec les SSID CWA

Comme décrit dans le guide de configuration Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE, CWA se base sur MAB et des résultats spécifiques pour authentifier et autoriser les utilisateurs. Les listes de contrôle d'accès téléchargeables peuvent être ajoutées à la configuration CWA du côté ISE de la même manière que ce qui a été décrit précédemment.

---

Avertissement : Les listes de contrôle d'accès téléchargeables peuvent uniquement être

---

utilisées comme listes d’accès réseau et ne sont pas prises en charge comme listes de contrôle d’accès de pré-authentification. Par conséquent, toutes les listes de contrôle d'accès de pré-authentification utilisées dans un workflow CWA doivent être définies dans la configuration du WLC.

## Vérifier

Pour vérifier la configuration, vous pouvez utiliser les commandes suivantes :

```
# 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 }
```

Dans cet exemple, la partie pertinente référencée de la configuration WLC correspondant à cet exemple est affichée :

```
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
```

---

La configuration du serveur RADIUS est présentée, exécutant la commande show running-config all :

```
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
```

---

# Dépannage

## Liste De Contrôle

- Vérifiez que les clients peuvent se connecter correctement au SSID 802.1X configuré.
- Assurez-vous que la requête d'accès/acceptation RADIUS contient les paires attribut-valeur (AVP) appropriées.
- Assurez-vous que les clients utilisent le profil WLAN/de stratégie approprié.

---

## WLC One Stop-Shop Reflex

Pour vérifier si la dACL est correctement attribuée à un client sans fil particulier, vous pouvez exécuter la commande show wireless client mac-address <H.H.H> detail. De là, vous trouverez des informations de dépannage utiles, notamment : le nom d'utilisateur du client, son état, son profil de stratégie, son WLAN et, plus important encore, la liste de contrôle d'accès ACS.

### <#root>

WLC#show wireless client mac-address 08be.ac14.137d detail

Client MAC Address : 08be.ac14.137d
Client MAC Type : Universally Administered Address
Client DUID: NA
Client IPv4 Address : 10.14.13.240

**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 : In-Active
[...]
Client Join Time:
  Join Time Of Client : 03/28/2024 10:04:30 UTC

**Client ACLs : None Policy Manager State: Run**

Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 35 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
EAP Type : PEAP
VLAN Override after Webauth : No

**VLAN : VLAN_1413**

[...]

```
Session Manager:
  Point of Attachment : capwap_90000012
  IIF ID              : 0x90000012
  Authorized          : TRUE
  Session timeout     : 28800
  Common Session ID: 8227300A0000000C8484A22F
  Acct Session ID  : 0x00000000
  Last Tried Aaa Server Details:
      Server IP : 10.48.39.134
  Auth Method Status List
      Method : Dot1x

 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

[...]
```

## Commandes show du WLC

Pour voir toutes les ACL qui font partie de la configuration du WLC Catalyst 9800, vous pouvez exécuter la commande show access-lists. Cette commande répertorie toutes les ACL définies localement ou les dACL téléchargées par le WLC. Toutes les dACL téléchargées depuis ISE par le WLC ont le xACSACLx-IP-<ACL_NAME>-<ACL_HASH> format.

---

Remarque : Les listes de contrôle d'accès téléchargeables restent dans la configuration si un client est associé et les utilise dans l'infrastructure sans fil. Lorsque le dernier client utilisant la dACL quitte l'infrastructure, la dACL est supprimée de la configuration.

---

```
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
[...]
```

---

## Débogage conditionnel et suivi radioactif

Lors du dépannage de la configuration, vous pouvez collecter des traces radioactives pour un client affecté avec la dACL définie. Voici quelques journaux mis en évidence affichant des parties des traces radioactives pendant un processus d'association pour le client 08be.ac14.137d :

<#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.ac14.137

[...]

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◇« %ÿOã@≤™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◇« %ÿOã@≤™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 t**

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 t**

**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**

## Capture de paquets

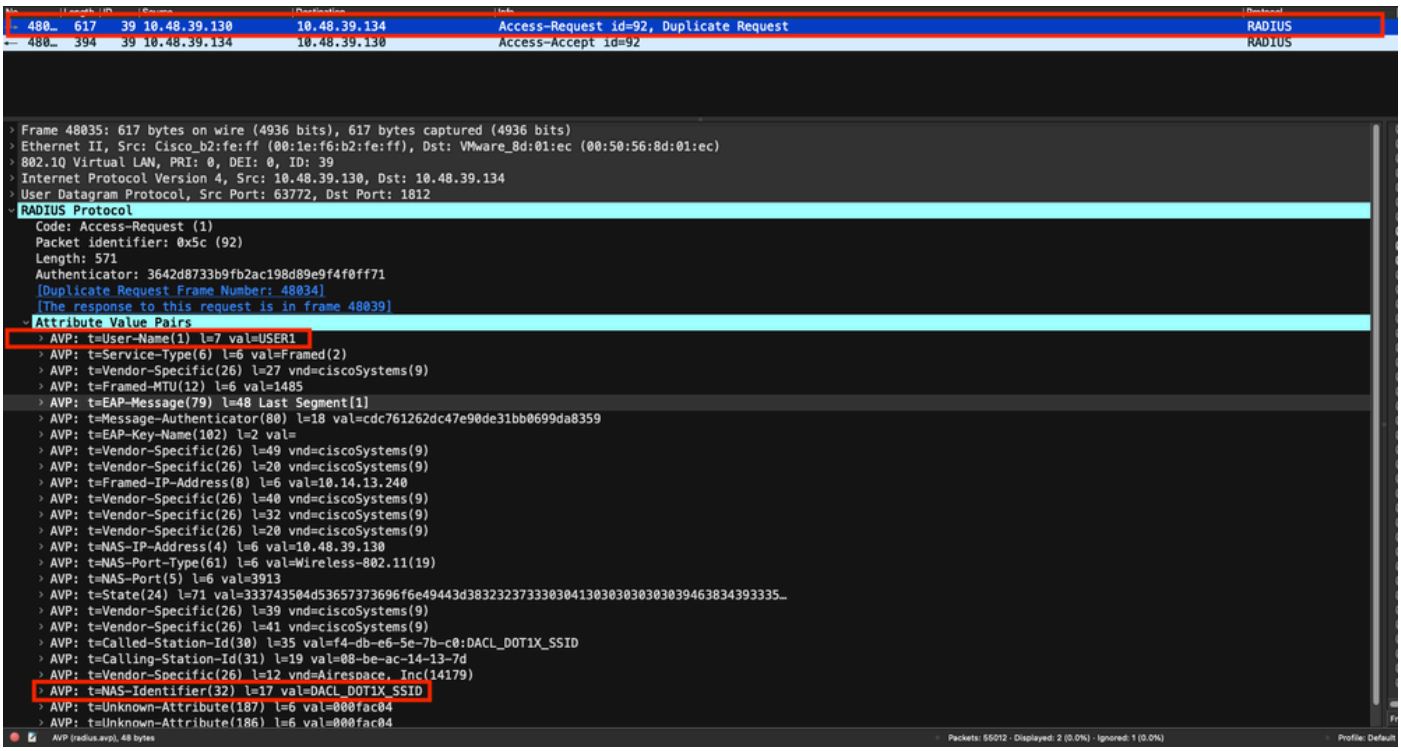
Une autre tâche à effectuer pour analyser est la capture de paquets du flux RADIUS pour l'association client. Les listes de contrôle d'accès téléchargeables dépendent de RADIUS, non seulement pour être attribuées à un client sans fil, mais également pour être téléchargées par le WLC. Lors de la capture de paquets pour le dépannage de la configuration des dACL, vous devez effectuer la capture sur l'interface utilisée par le contrôleur pour communiquer avec le serveur RADIUS. Ce document montre comment configurer facilement les captures de paquets intégrées sur le Catalyst 9800, qui ont été utilisées pour collecter la capture analysée dans cet article.

---

## Authentification du client RADIUS

Vous pouvez voir que la demande d'accès RADIUS du client est envoyée du WLC au serveur RADIUS pour authentifier USER1 (AVP User-Name) sur le SSID DACL_DOT1X_SSID (AVP NAS-Identifier).

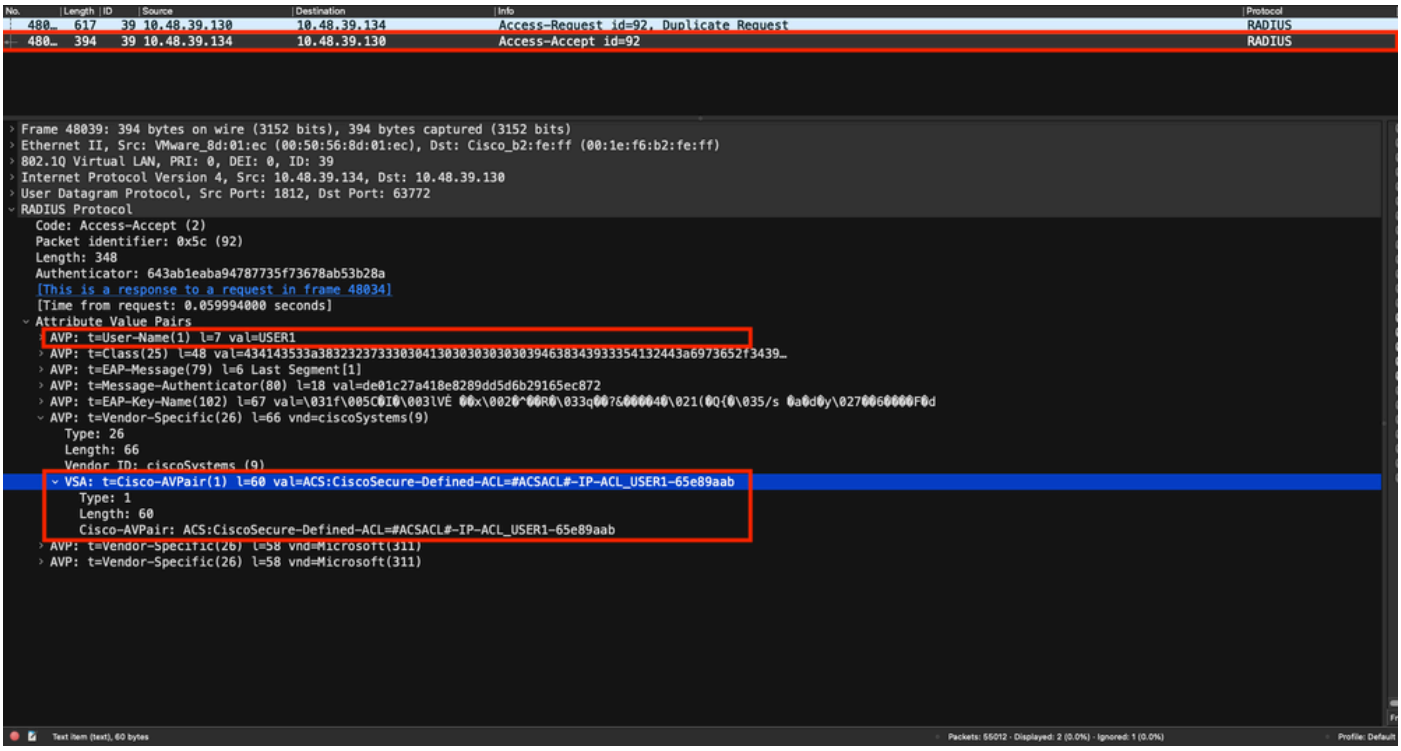
---




---

Lorsque l'authentification réussit, le serveur RADIUS répond avec un access-accept. Pour l'utilisateur USER1 (Nom d'utilisateur AVP) et lors de l'application des attributs AAA, l'AVP spécifique au fournisseur ACS:CiscoSecure-Defined-ACL étant #ACSACL#-IP-ACL_USER1-65e89aab.

---

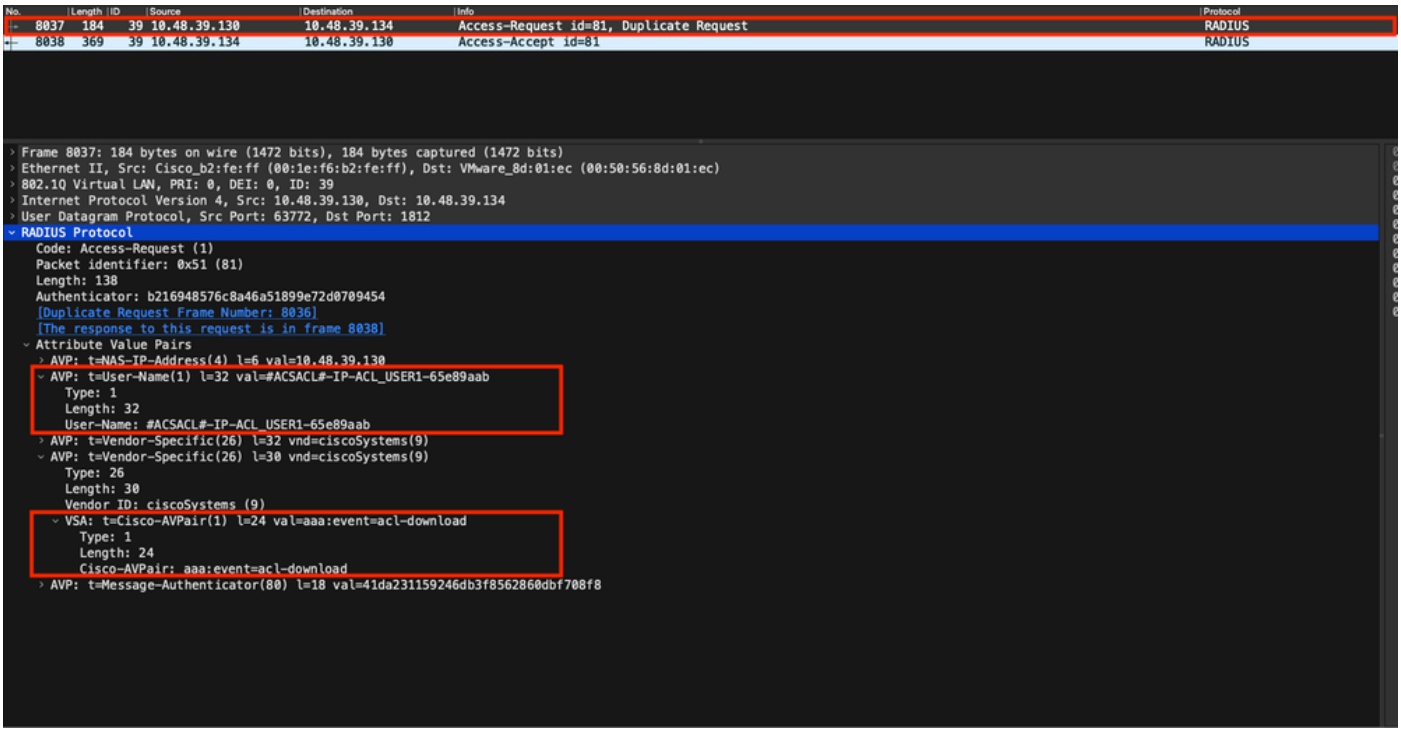



---

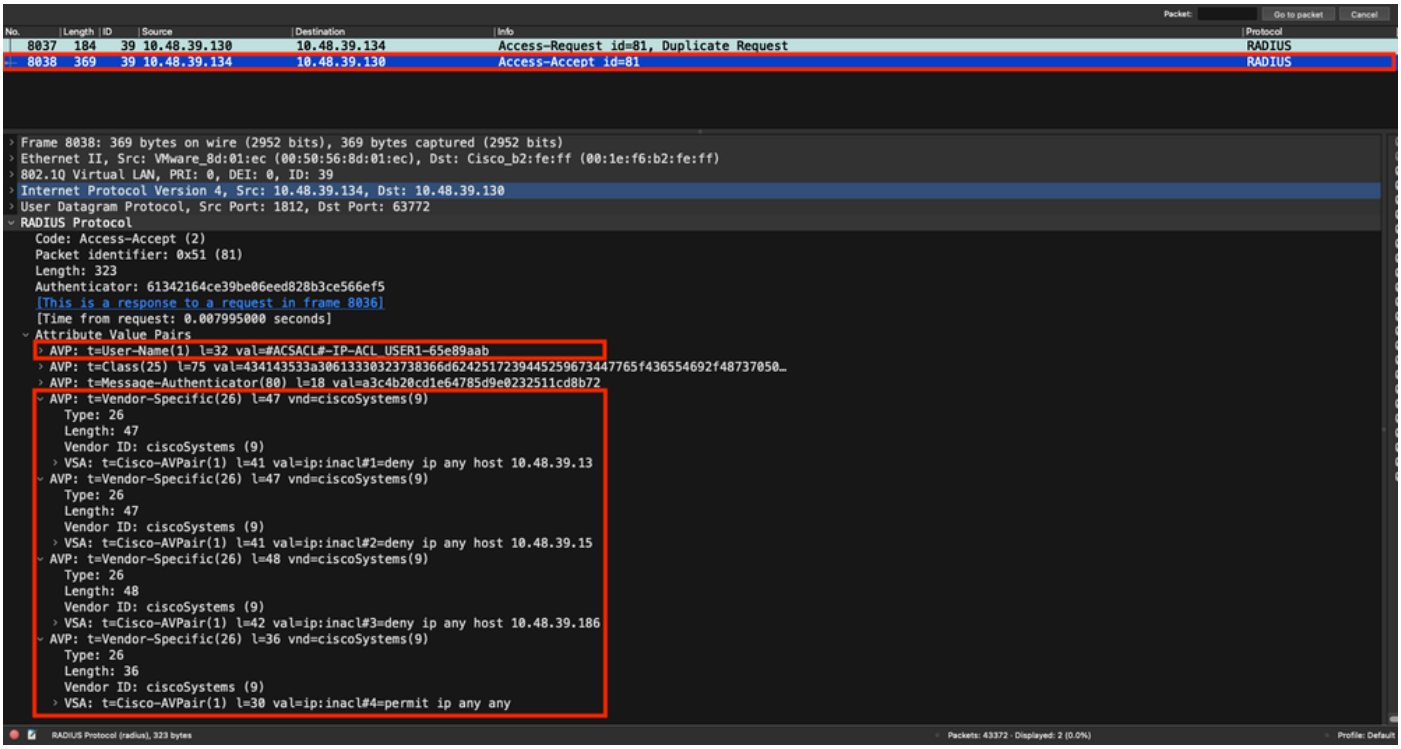
Téléchargement DACL

Si la dACL fait déjà partie de la configuration du WLC, elle est attribuée à l'utilisateur et la session RADIUS se termine. Sinon, WLC télécharge la liste de contrôle d'accès, toujours en utilisant RADIUS. Pour ce faire, le WLC envoie une requête d'accès RADIUS, cette fois en utilisant le nom dACL (#ACSACL#-IP-ACL_USER1-65e89aab) pour le nom d'utilisateur AVP. Le WLC informe le serveur RADIUS que cette acceptation d'accès lance un téléchargement de liste de contrôle d'accès à l'aide de la paire AV Cisco aaa:event=acl-download.

---




L'acceptation d'accès RADIUS renvoyé au contrôleur contient la dACL demandée, comme indiqué dans la capture d'écran. Chaque règle de liste de contrôle d'accès est contenue dans un protocole Cisco AVP différent de type ip : inacl#<X>=<ACL_RULE>, <X> étant le numéro de la règle.

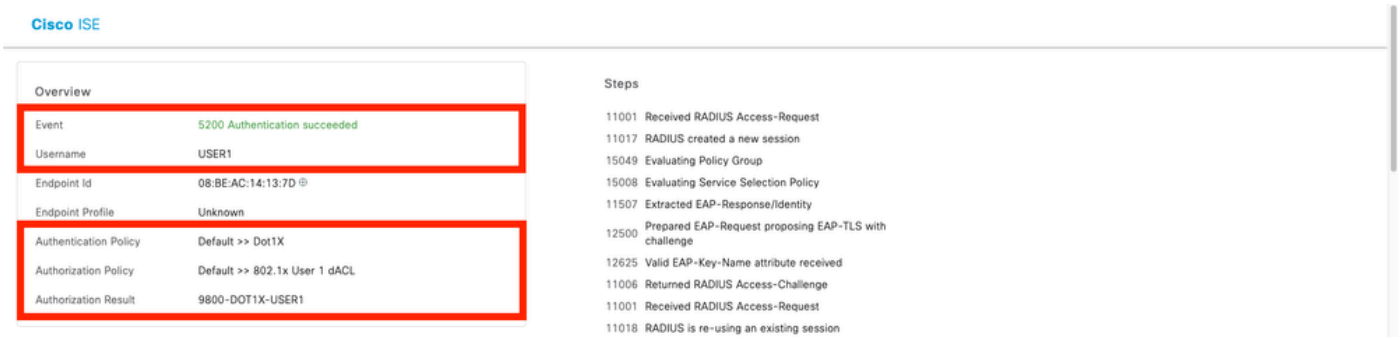


Remarque : Si le contenu d'une ACL est modifié après avoir été téléchargé sur le WLC, la modification pour cette ACL n'est pas reflétée jusqu'à ce qu'un utilisateur s'authentifie à nouveau (et le WLC effectue une authentification RADIUS pour un utilisateur à nouveau). Une modification de la liste de contrôle d'accès se traduit par une modification de la partie hachée du nom de la liste. La prochaine fois que cette liste de contrôle d'accès sera attribuée à un utilisateur, son nom doit être différent et la liste de contrôle d'accès ne doit pas faire partie de la configuration du WLC. Toutefois, les clients qui s'authentifient avant une modification de la liste de contrôle d'accès continuent d'utiliser la précédente jusqu'à ce qu'ils s'authentifient à nouveau complètement.

## Journaux des opérations ISE

### Authentification du client RADIUS

Les journaux d'opérations montrent une authentification réussie de l'utilisateur USER1, où la liste de contrôle d'accès téléchargeable ACL_USER1 est appliquée. Les éléments intéressants pour le dépannage sont encadrés en rouge.



## Authentication Details

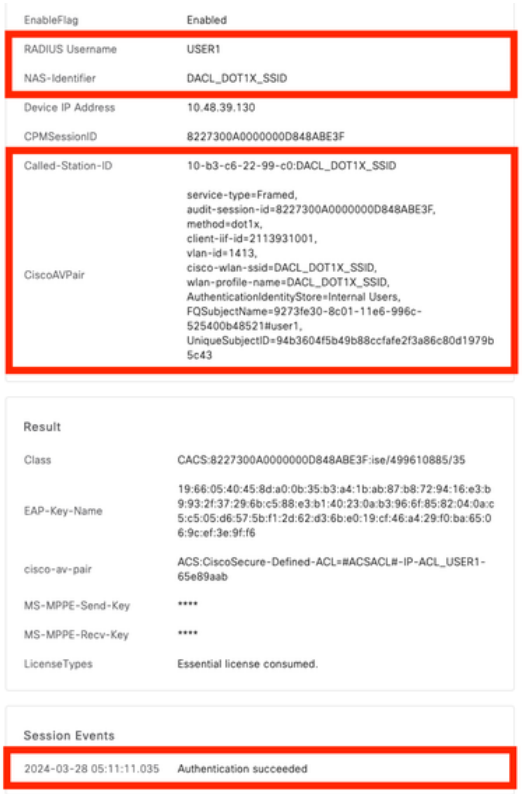
| | |
|---|---|
| Source Timestamp | 2024-03-28 05:11:11.035 |
| Received Timestamp | 2024-03-28 05:11:11.035 |
| Policy Server | ise |
| Event | 5200 Authentication succeeded |
| Username | USER1 |
| User Type | User |
| Endpoint Id | 08:BE:AC:14:13:7D |
| Calling Station Id | 08-be-ac-14-13-7d |
| 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 |

| | |
|---|---|
| 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 |

**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 |

| | |
|---|---|
| 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 |

---

Téléchargement DACL

Les journaux des opérations indiquent que la liste de contrôle d'accès ACL_USER1 a bien été téléchargée. Les parties intéressantes pour le dépannage sont encadrées en rouge.

---

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

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.