Konfigurieren von & Fehlerbehebung für herunterladbare ACLs auf Catalyst 9800

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie herunterladbare Zugriffskontrolllisten (dACLs) auf dem Catalyst 9800 Wireless LAN Controller (WLC) konfiguriert werden und Fehler bei diesen behoben werden.

Hintergrundinformationen

Die dACLs werden seit vielen Jahren von Cisco IOS®- und IOS XE®-Switches unterstützt. Eine

dACL bezieht sich darauf, dass das Netzwerkgerät die ACL-Einträge bei der Authentifizierung dynamisch vom RADIUS-Server herunterlädt, anstatt eine lokale Kopie der ACL zu besitzen und nur den ACL-Namen zuzuweisen. Ein ausführlicheres Konfigurationsbeispiel für die Cisco ISE ist verfügbar. Der Schwerpunkt dieses Dokuments liegt auf dem Cisco Catalyst 9800, der seit der Version 17.10 dACLs für zentrales Switching unterstützt.

Voraussetzungen

In diesem Dokument wird die Verwendung von dACLs für Catalyst 9800 anhand eines Beispiels für eine grundlegende SSID-Konfiguration veranschaulicht. Dabei wird erläutert, wie diese vollständig angepasst werden können.

Auf dem Catalyst 9800 Wireless Controller werden die ACLs heruntergeladen.

- Unterstützt ab Cisco IOS XE Dublin 17.10.1 Version
- Unterstützt für zentralisierten Controller, der nur lokale Zugangspunkte (oder Flexconnect Central Switching) verwendet. FlexConnect Local Switching unterstützt dACL nicht.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Catalyst Wireless 9800-Konfigurationsmodell.
- Cisco IP Access Control Lists (ACLs)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9800-CL (gegen Dublin 17.12.03)
- ISE (V. 3.2).

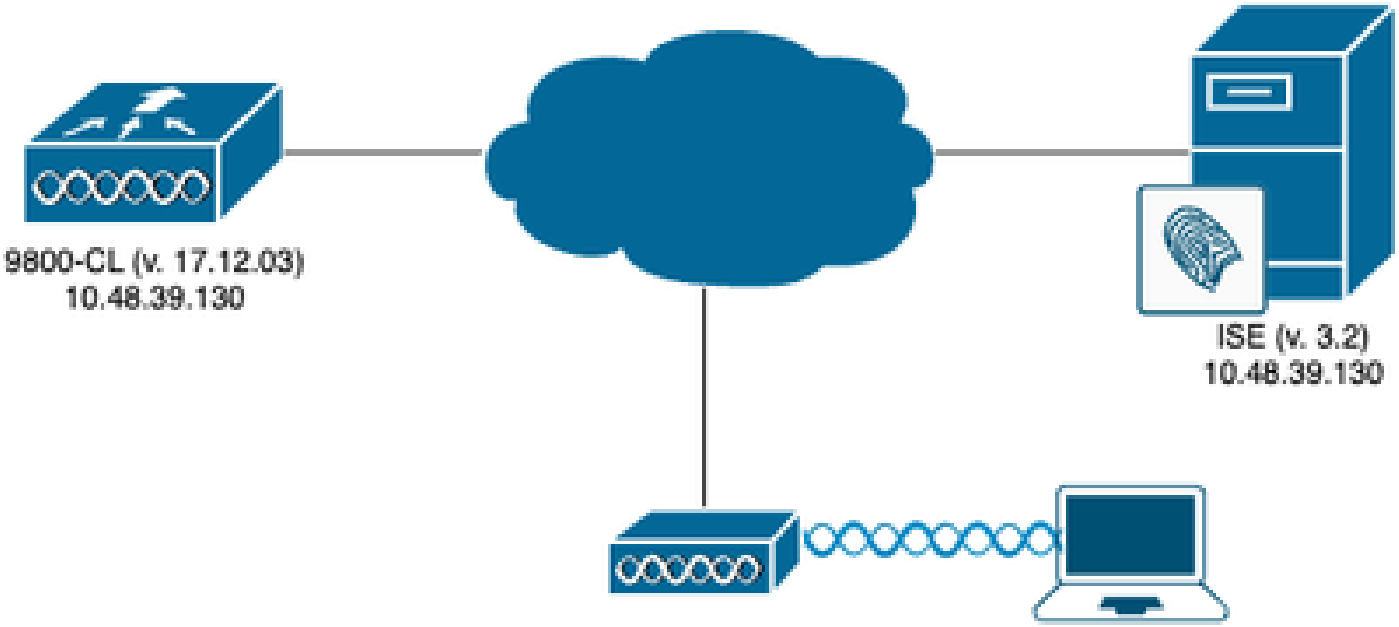
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Auch wenn unterschiedliche Methoden (z. B. WLAN-Authentifizierung, Richtlinienkonfiguration usw.) verwendet werden, bleibt das Endergebnis in diesem Konfigurationsleitfaden unverändert. In dem hier gezeigten Szenario werden zwei Benutzeridentitäten definiert: USER1 und USER2. Beiden wird der Zugriff auf das Wireless-Netzwerk gewährt. Jedem dieser Access Points werden ACL_USER1 und ACL_USER2 als dACLs zugewiesen, die vom Catalyst 9800 von der ISE heruntergeladen werden.

Verwenden von dACLs mit 802.1x-SSIDs

Netzwerkdiagramm



WLC-Konfiguration

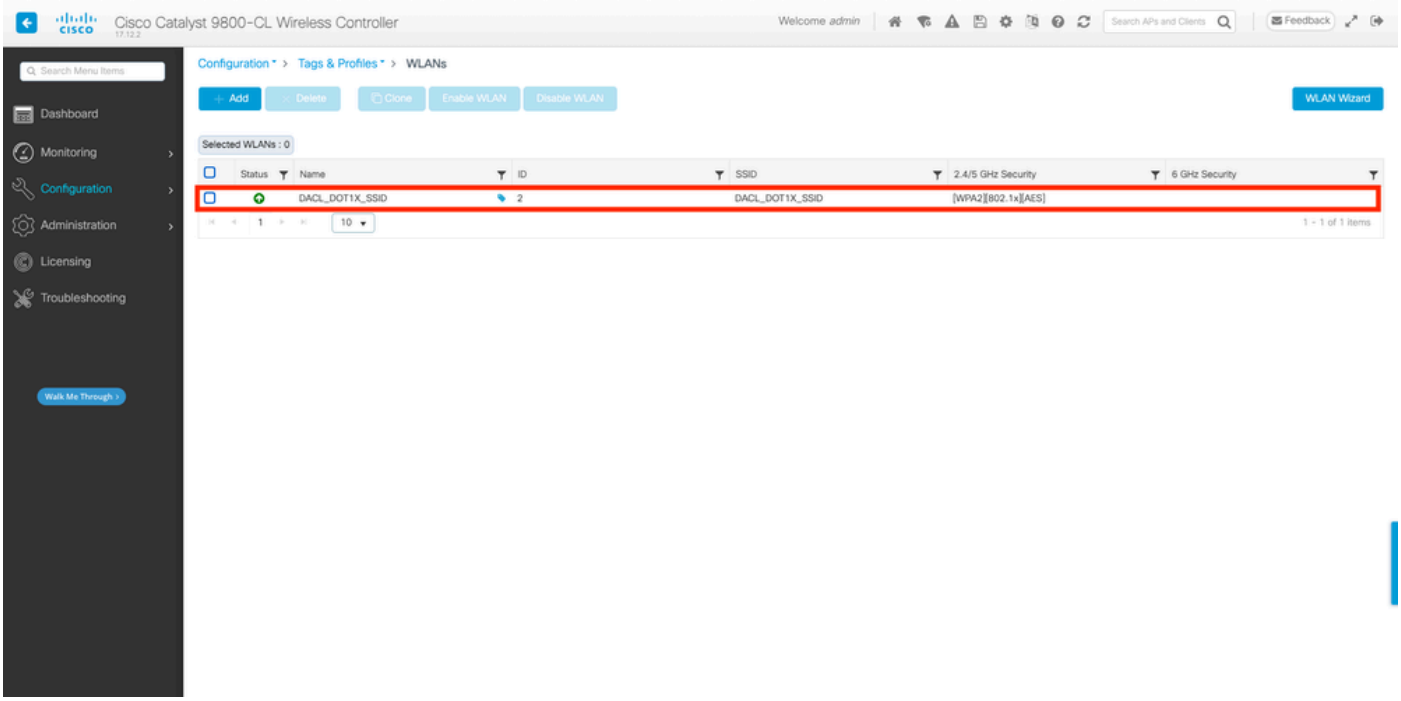
Weitere Informationen zur 802.1x SSID-Konfiguration und Fehlerbehebung für den Catalyst 9800 finden Sie im Konfigurationsleitfaden Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series (Konfigurieren der 802.1X-Authentifizierung auf Catalyst 9800 Wireless-Controllern).

Schritt 1: Konfigurieren der SSID

Konfigurieren einer 802.1x-authentifizierten SSID unter Verwendung der ISE als RADIUS-Server In diesem Dokument erhält die SSID den Namen "DACL_DOT1X_SSID".

Über die GUI:

Navigieren Sie zu Configuration > Tags & Profiles > WLAN, und erstellen Sie ein WLAN ähnlich dem hier gezeigten:



Über die 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
```

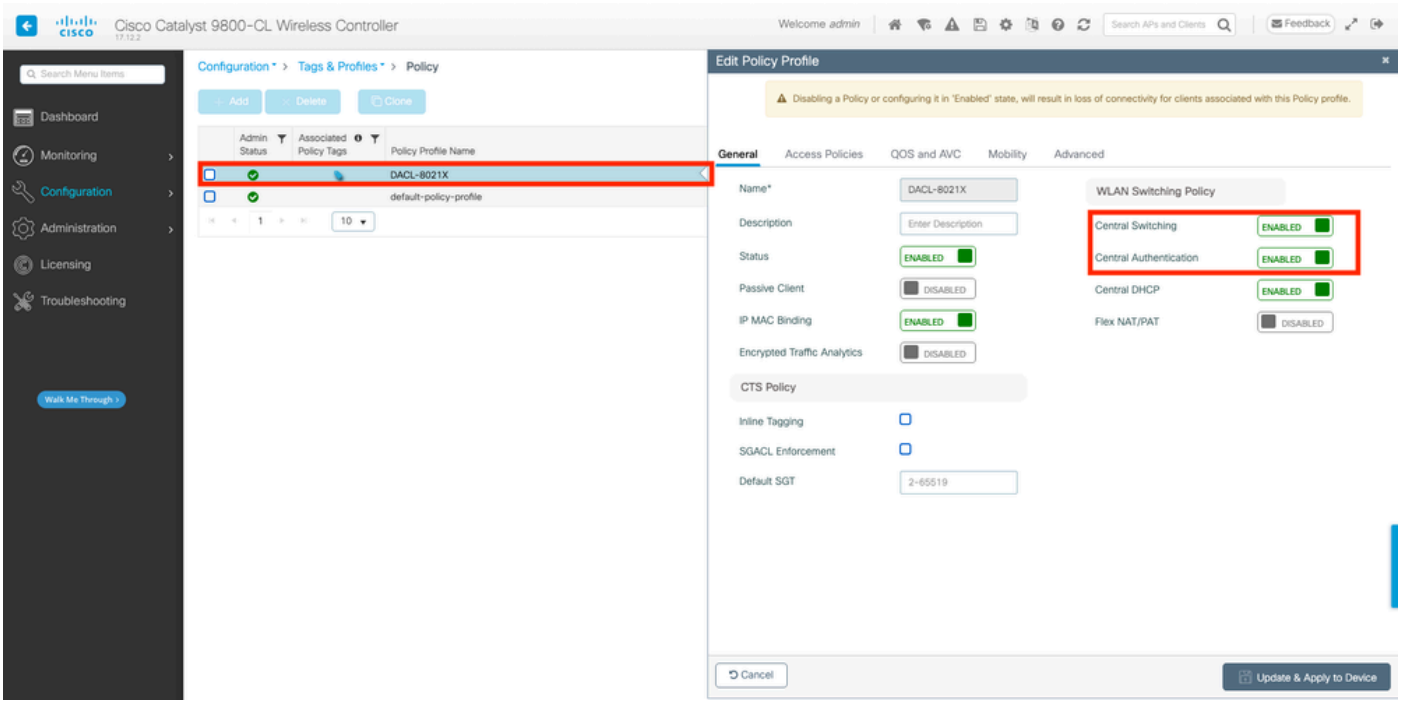
Schritt 2: Konfigurieren Sie das Richtlinienprofil.

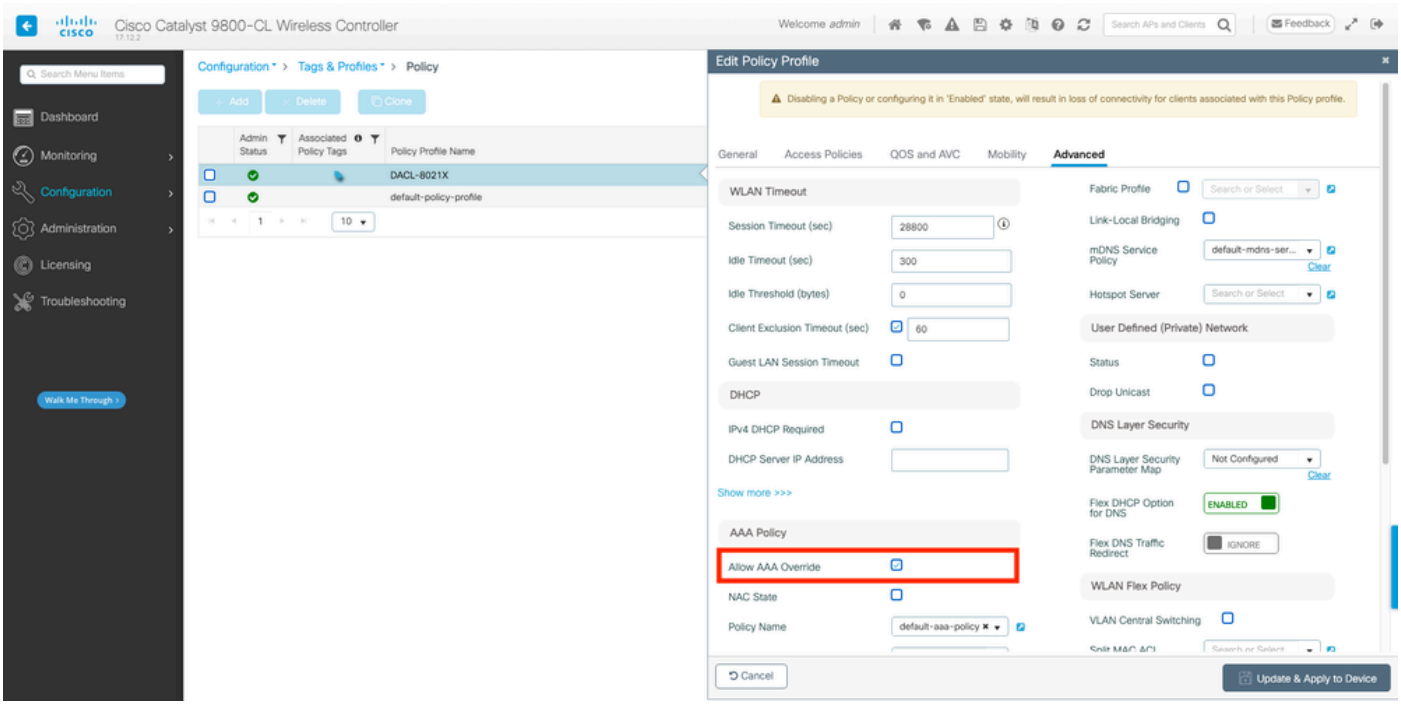
Konfigurieren Sie das Richtlinienprofil, das zusammen mit der oben definierten SSID verwendet wird. Stellen Sie in diesem Richtlinienprofil sicher, dass AAA Override auf der Registerkarte "Advanced" (Erweitert) konfiguriert ist, wie im Screenshot gezeigt. In diesem Dokument wird das Richtlinienprofil "DACL-8021X" verwendet.

Wie im Abschnitt über die Voraussetzungen angegeben, werden dACLs nur für zentrale Switching-/Authentifizierungsbereitstellungen unterstützt. Vergewissern Sie sich, dass das Richtlinienprofil entsprechend konfiguriert ist.

Über die GUI:

Navigieren Sie zu Configuration > Tags & Profiles > Policy, wählen Sie das verwendete Richtlinienprofil aus, und konfigurieren Sie es wie dargestellt.





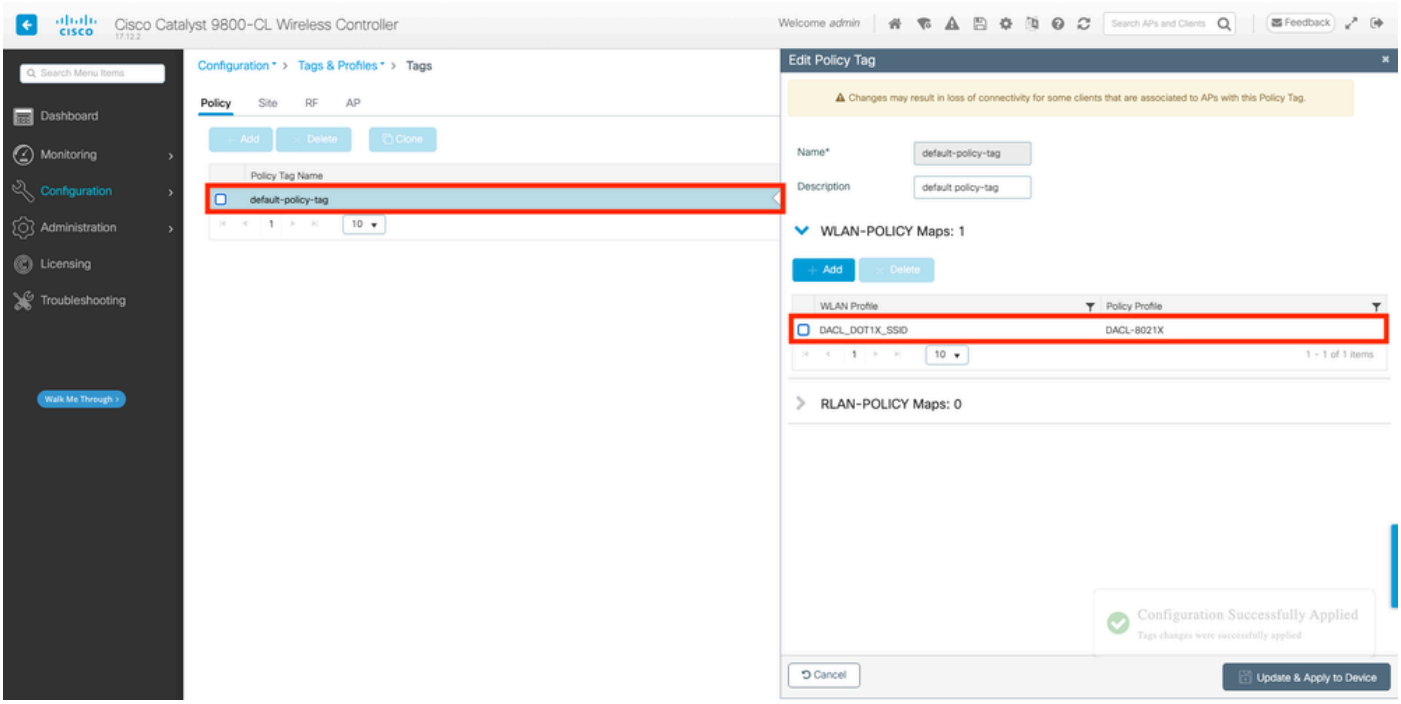
Über die CLI:

```
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
```

Schritt 3: Weisen Sie das Richtlinienprofil und die SSID dem verwendeten Richtlinien-Tag zu.

Über die GUI:

Navigieren Sie zu Konfiguration > Tags & Profile > Tags. Erstellen (oder wählen) Sie auf der Registerkarte Policy Tags (Richtlinientags) den verwendeten Tag, und weisen Sie ihm das WLAN und das Richtlinienprofil zu, die in den Schritten 1-2 definiert wurden.



Über die 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
```

Schritt 4: Herstellerspezifisches Attribut zulassen.

Herunterladbare ACLs werden über anbieterspezifische Attribute (VSA) im RADIUS-Austausch zwischen ISE und WLC weitergeleitet. Die Unterstützung dieser Attribute kann mithilfe des CLI-Befehls auf dem WLC aktiviert werden.

Über die CLI:

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

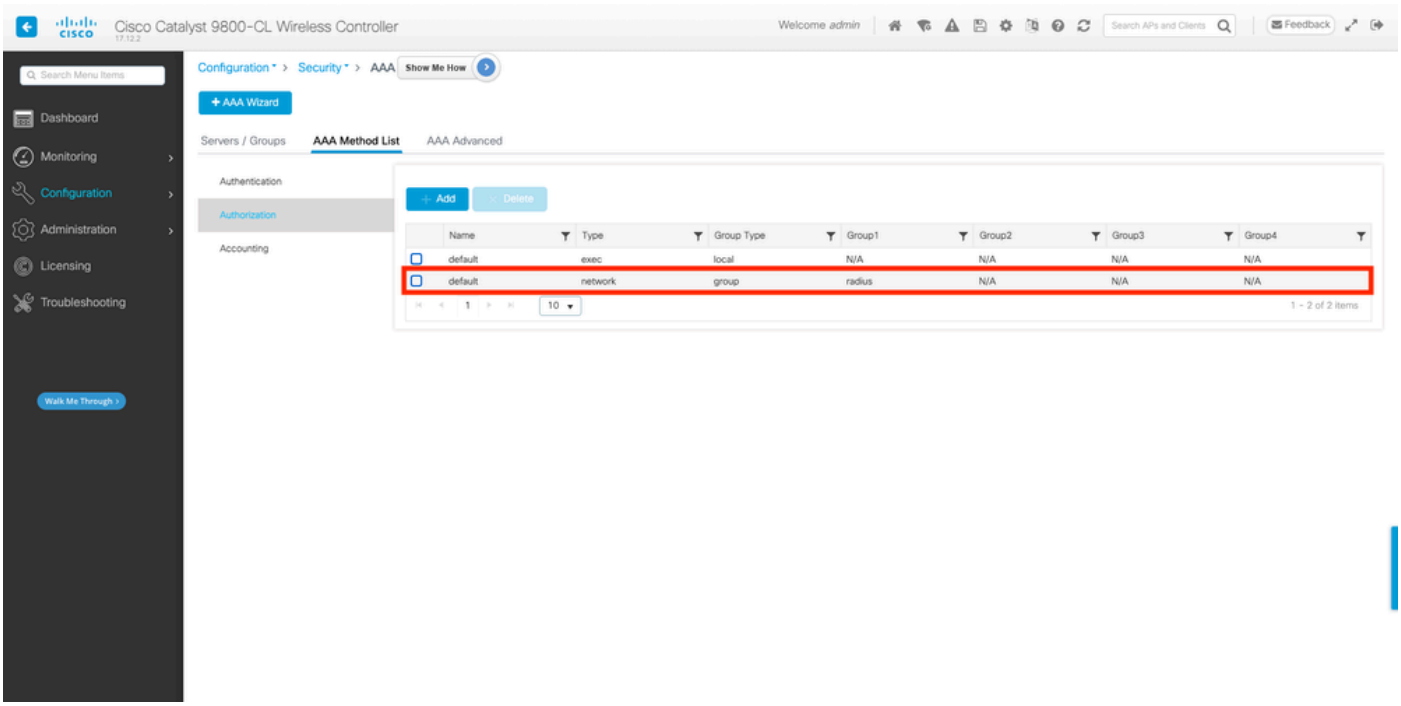
Schritt 5: Autorisierungsliste konfigurieren

Bei Verwendung von dACL muss die Netzwerkautorisierung über RADIUS erzwungen werden, damit der WLC alle Benutzer autorisieren kann, die sich an der konfigurierten 802.1x-SSID authentifizieren. Hier wird nicht nur die Authentifizierungs-, sondern auch die Autorisierungsphase auf der RADIUS-Serverseite behandelt. Daher ist in diesem Fall die Autorisierungsliste erforderlich.

Vergewissern Sie sich, dass die Standard-Netzwerkautorisierungsmethode Teil der 9800-Konfiguration ist.

Über die GUI:

Navigieren Sie zu Configuration > Security > AAA, und erstellen Sie auf der Registerkarte AAA Method List > Authorization (AAA-Methodenliste > Autorisierung) eine Autorisierungsmethode, die der gezeigten ähnelt.



Über die CLI:

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

ISE-Konfiguration

Bei der Implementierung von dACLs in Wireless-Umgebungen mit ISE sind zwei gängige Konfigurationen möglich:

1. dACL-Konfiguration pro Benutzer. Dabei wird jeder Identität eine dACL durch ein

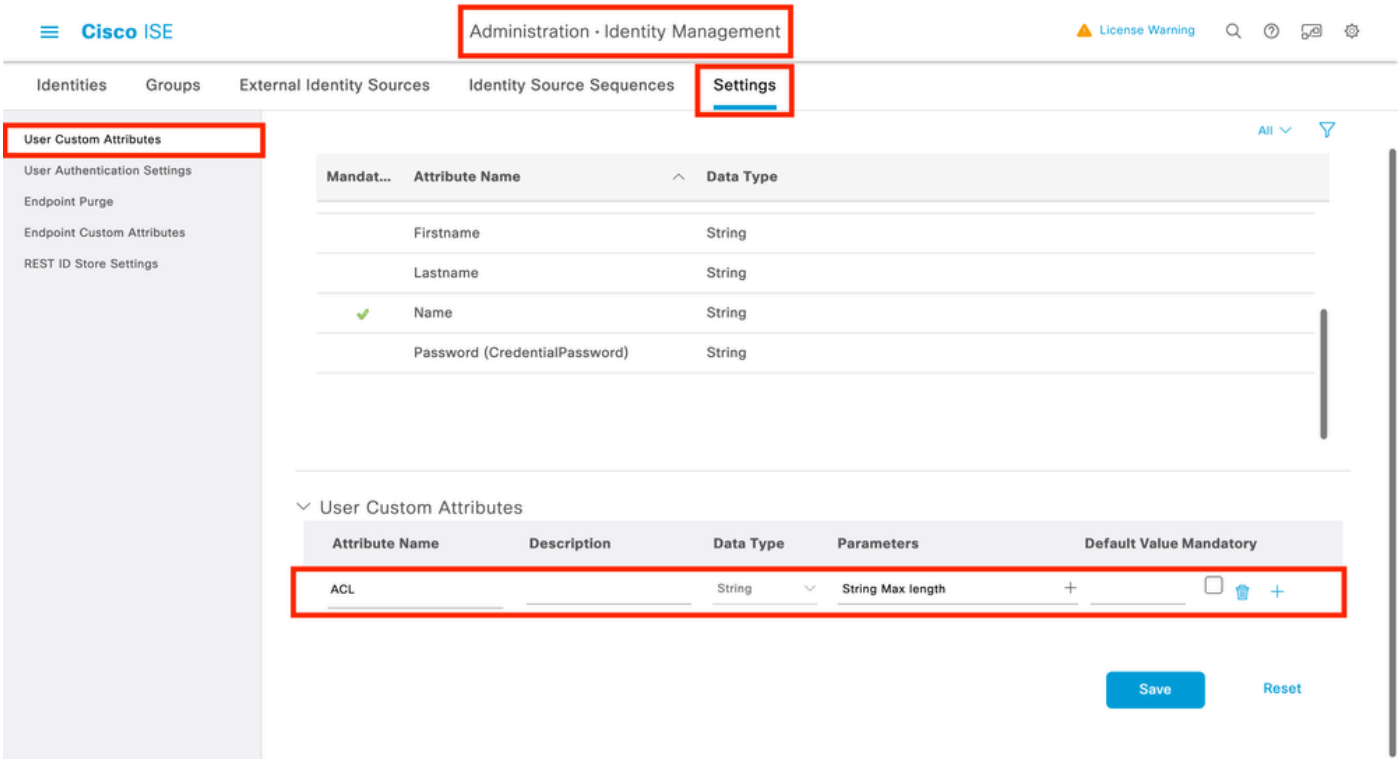
benutzerdefiniertes Identitätsfeld zugewiesen.

2. dACL-Konfiguration nach Ergebnis Bei der Auswahl dieser Methode wird einem Benutzer eine bestimmte dACL zugewiesen, und zwar basierend auf der Autorisierungsrichtlinie, die dem verwendeten Richtliniensatz entspricht.

Benutzerspezifische dACLs

Schritt 1: Benutzerdefiniertes dACL-Benutzerattribut definieren

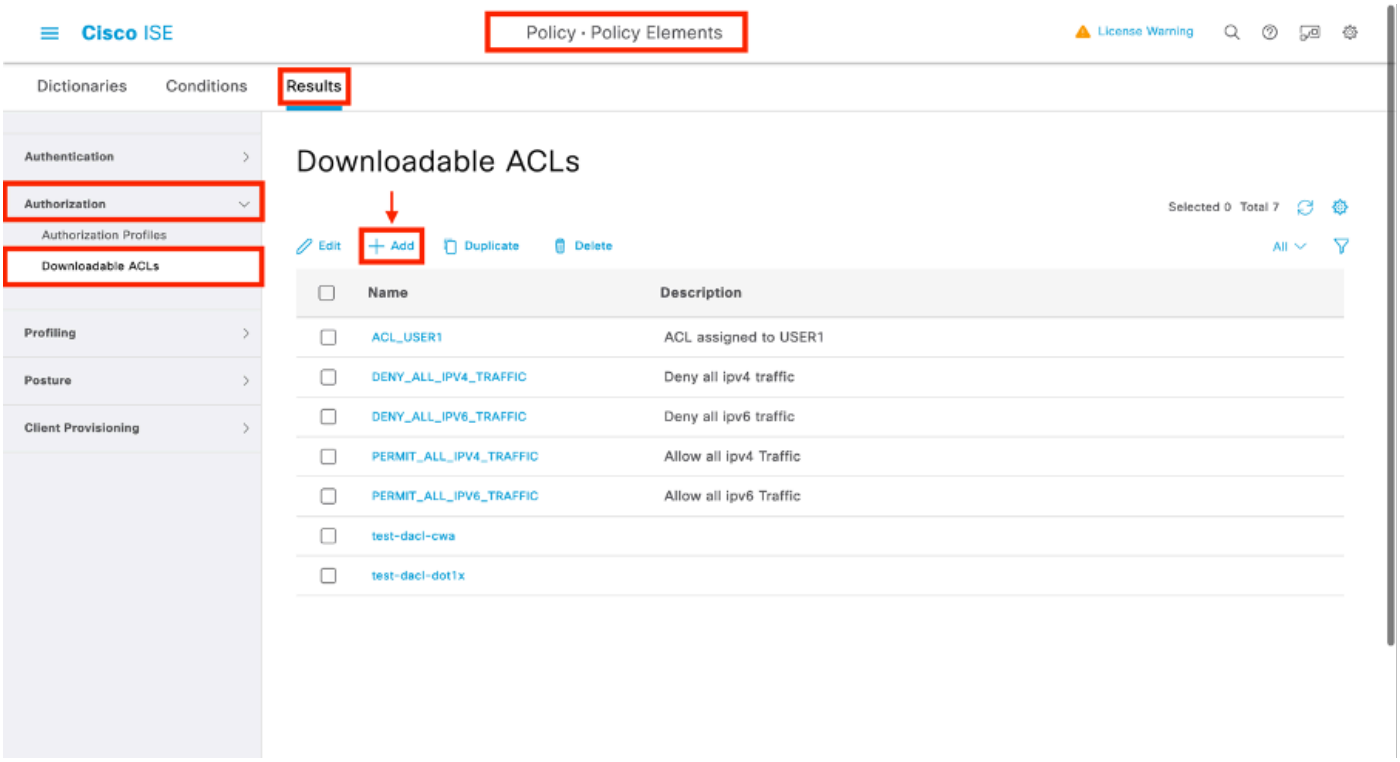
Um einer Benutzeridentität eine dACL zuweisen zu können, muss dieses Feld zunächst für die erstellte Identität konfigurierbar sein. Standardmäßig ist auf der ISE das Feld "ACL" für keine neu erstellte Identität definiert. Um dies zu umgehen, kann man das "Custom User Attribute" verwenden und ein neues Konfigurationsfeld definieren. Navigieren Sie dazu zu Administration > Identity Management > Settings > User Custom Attributes. Verwenden Sie die "+"-Schaltfläche, um ein neues Attribut hinzuzufügen, das dem angezeigten ähnelt. In diesem Beispiel lautet der Name des benutzerdefinierten Attributs ACL.



Speichern Sie die Änderungen mithilfe der Schaltfläche "Save" (Speichern).

Schritt 2: Konfigurieren der dACL

Navigieren Sie zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Herunterladbare ACLs, um dACL auf der ISE anzuzeigen und zu definieren. Verwenden Sie die Schaltfläche "Hinzufügen", um eine neue hinzuzufügen.



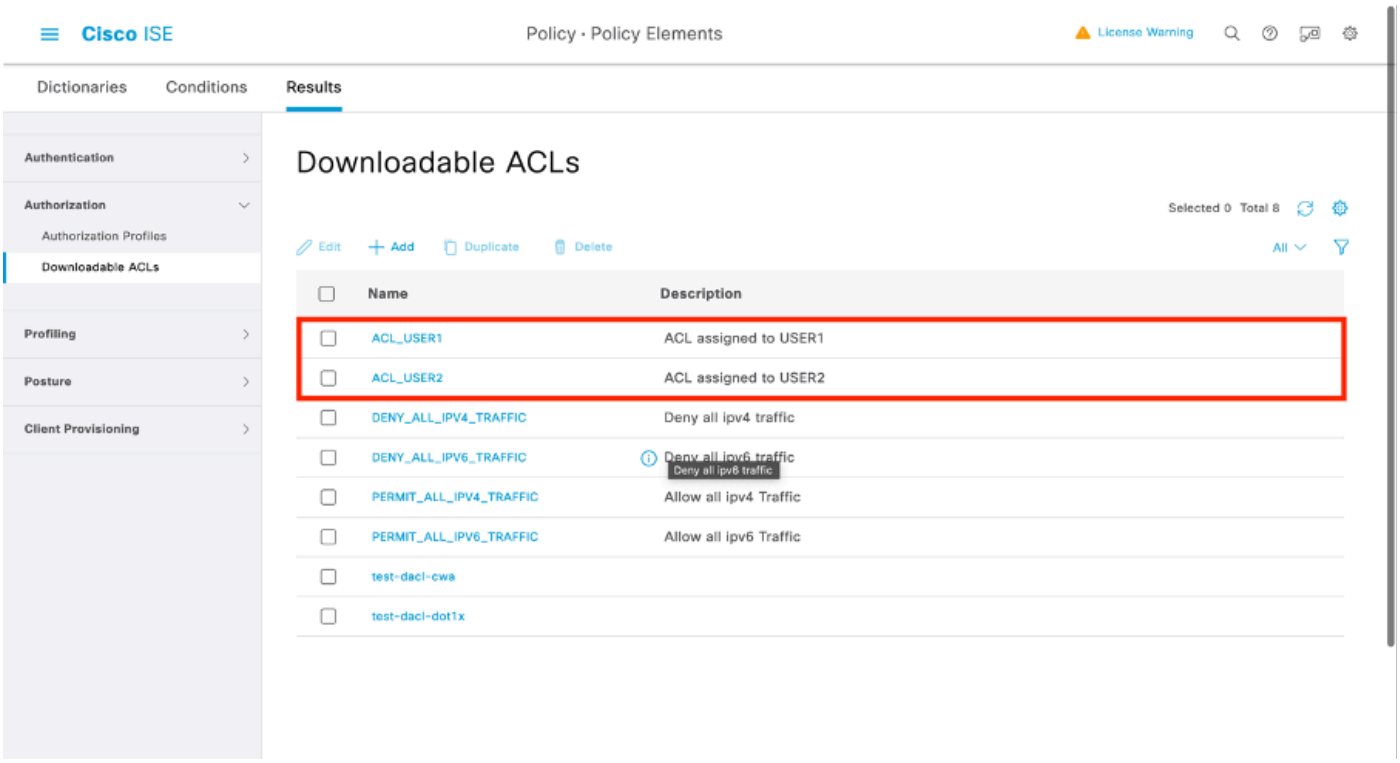
Daraufhin wird das Konfigurationsformular "Neue herunterladbare ACL" geöffnet. Konfigurieren Sie in diesem Feld die folgenden Felder:

- Name: Der Name der definierten dACL.
- Beschreibung (optional): eine kurze Beschreibung der Verwendung der erstellten dACL.
- IP-Version: die in der definierten dACL verwendete IP-Protokollversion (Version 4, 6 oder beide).
- DACL-Inhalt: der Inhalt der dACL gemäß der Cisco IOS XE ACL-Syntax.

In diesem Dokument wird als dACL "ACL_USER1" verwendet. Diese dACL lässt jeglichen Datenverkehr zu, mit Ausnahme des Datenverkehrs, der an 10.48.39.186 und 10.48.39.13 gerichtet ist.

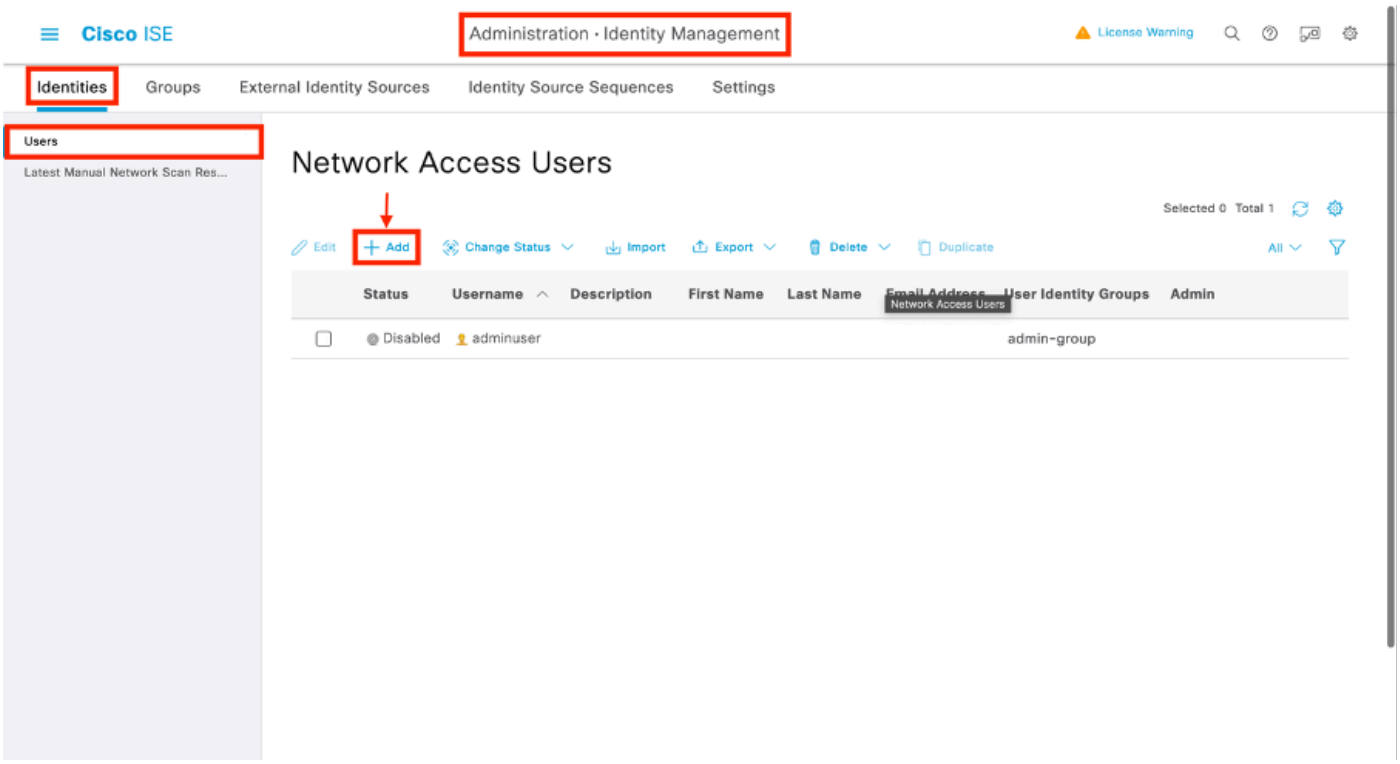
Verwenden Sie nach der Konfiguration der Felder die Schaltfläche "Submit" (Senden), um die dACL zu erstellen.

Wiederholen Sie den Schritt zum Definieren der dACL für den zweiten Benutzer, ACL_USER2, wie in der Abbildung dargestellt.



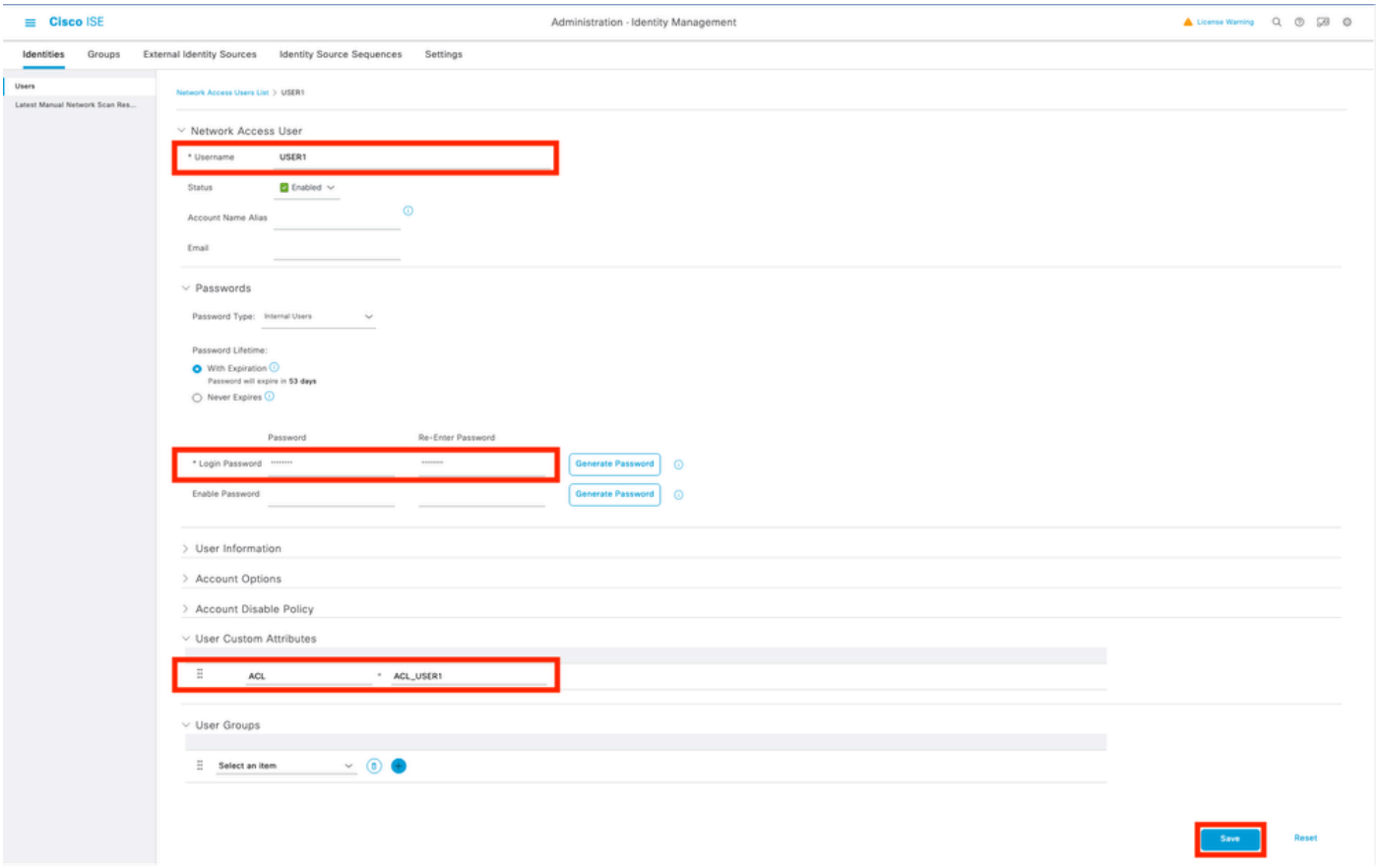
Schritt 3: Zuweisen der dACL zu einer erstellten Identität

Nachdem die dACL erstellt wurde, kann sie mithilfe der in Schritt 1 erstellten benutzerdefinierten Benutzerattribute jeder ISE-Identität zugewiesen werden. Navigieren Sie dazu zu Administration > Identity Management > Identities > Users. Verwenden Sie wie üblich die Schaltfläche "Hinzufügen", um einen Benutzer zu erstellen.



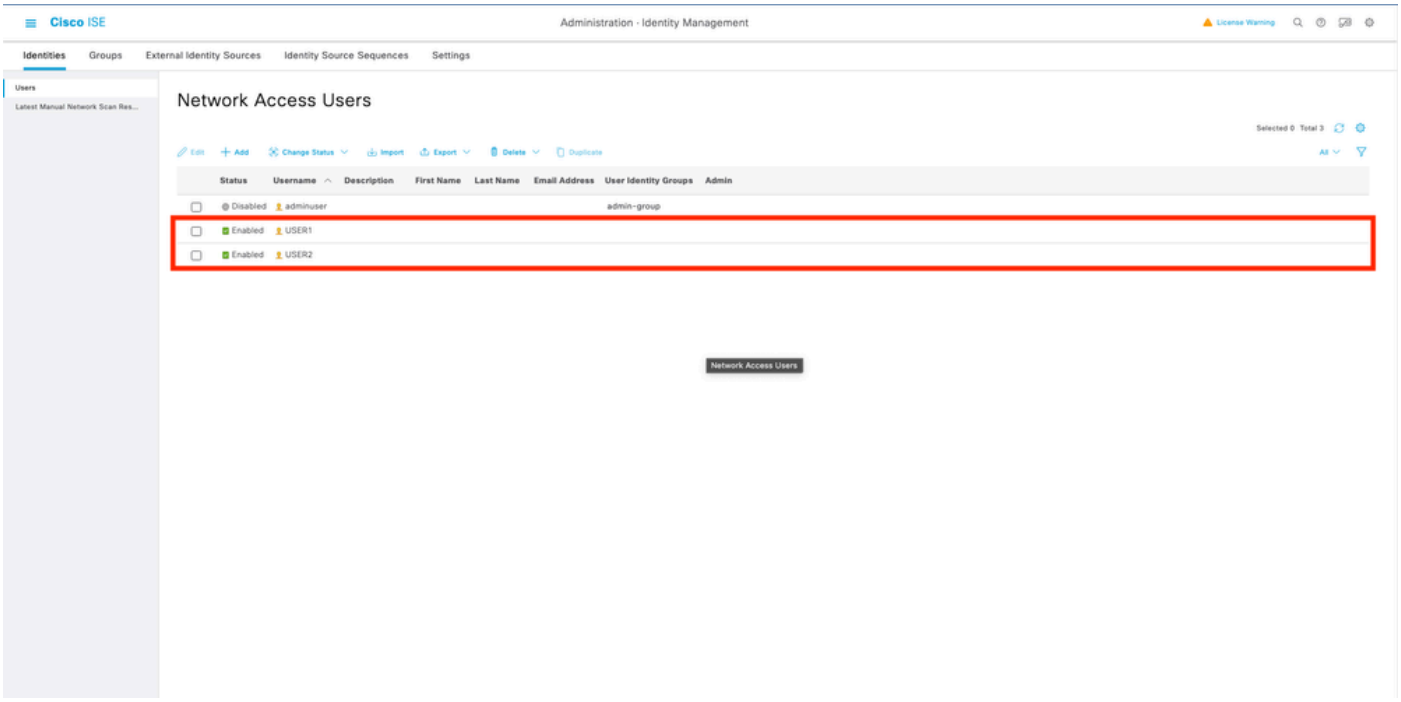
Legen Sie im Konfigurationsformular "New Network Access User" (Neuer Netzwerkzugriffsbenutzer) den Benutzernamen und das Kennwort für den erstellten Benutzer fest.

Verwenden Sie das benutzerdefinierte Attribut "ACL", um die in Schritt 2 erstellte dACL der Identität zuzuweisen. Im Beispiel wird die Identität USER1 mit ACL_USER1 definiert.



Verwenden Sie nach der korrekten Konfiguration der Felder die Schaltfläche "Submit" (Senden), um die Identität zu erstellen.

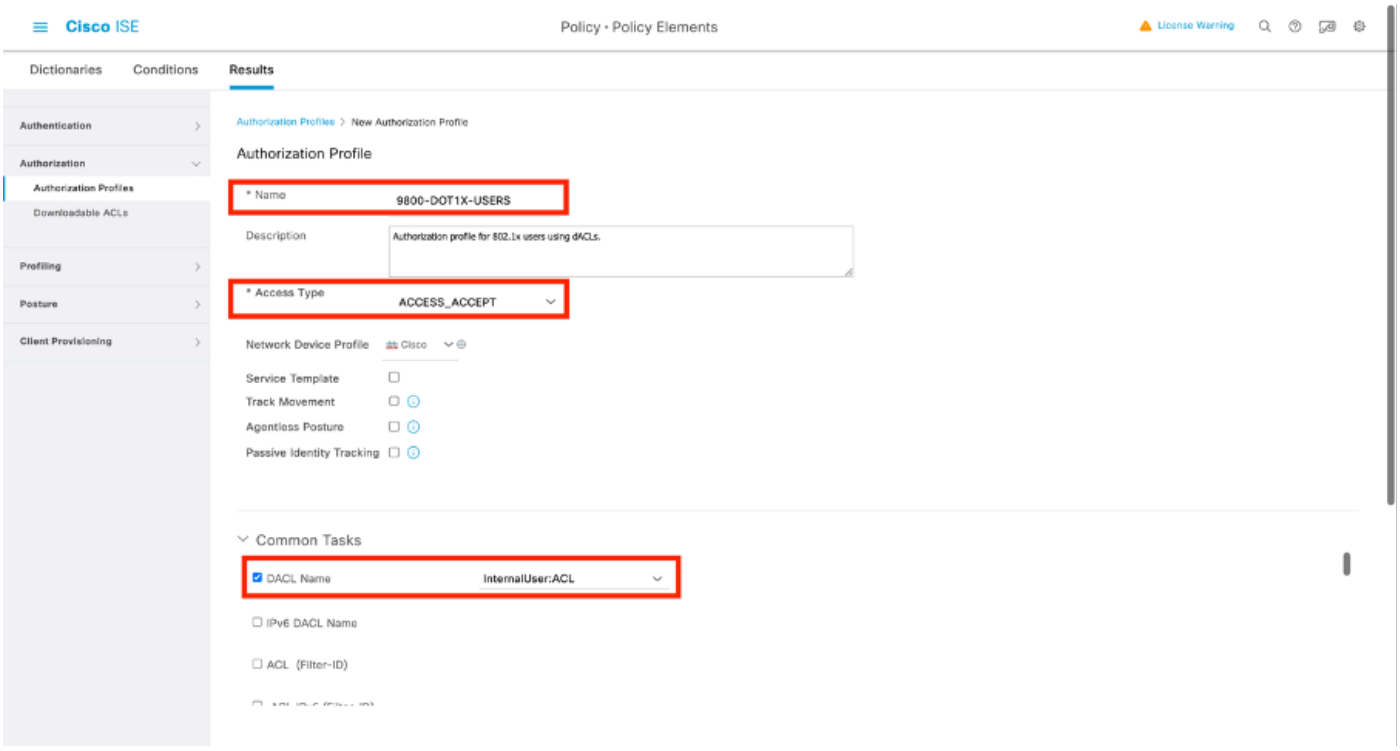
Wiederholen Sie diesen Schritt, um USER2 zu erstellen und ihm ACL_USER2 zuzuweisen.



Schritt 4: Ergebnis der Autorisierungsrichtlinie konfigurieren

Nach der Konfiguration der Identität und der Zuweisung der dACL muss die Autorisierungsrichtlinie weiterhin konfiguriert werden, damit das benutzerdefinierte Benutzerattribut "ACL" einer vorhandenen allgemeinen Autorisierungsaufgabe zugeordnet wird. Navigieren Sie dazu zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile. Verwenden Sie die Schaltfläche "Hinzufügen", um eine neue Autorisierungsrichtlinie zu definieren.

- Name: der Name der Autorisierungsrichtlinie, hier "9800-DOT1X-USERS".
- Access Type (Zugriffstyp): der Zugriffstyp, der beim Abgleich dieser Richtlinie verwendet wird, hier ACCESS_ACCEPT.
- Allgemeine Aufgabe: Ordnen Sie "DACL Name" InternalUser zu:<Name des erstellten benutzerdefinierten Attributs> für internen Benutzer.Entsprechend den in diesem Dokument verwendeten Namen wird das Profil 9800-DOT1X-USERS mit der dACL konfiguriert, die als InternalUser:ACL konfiguriert ist.

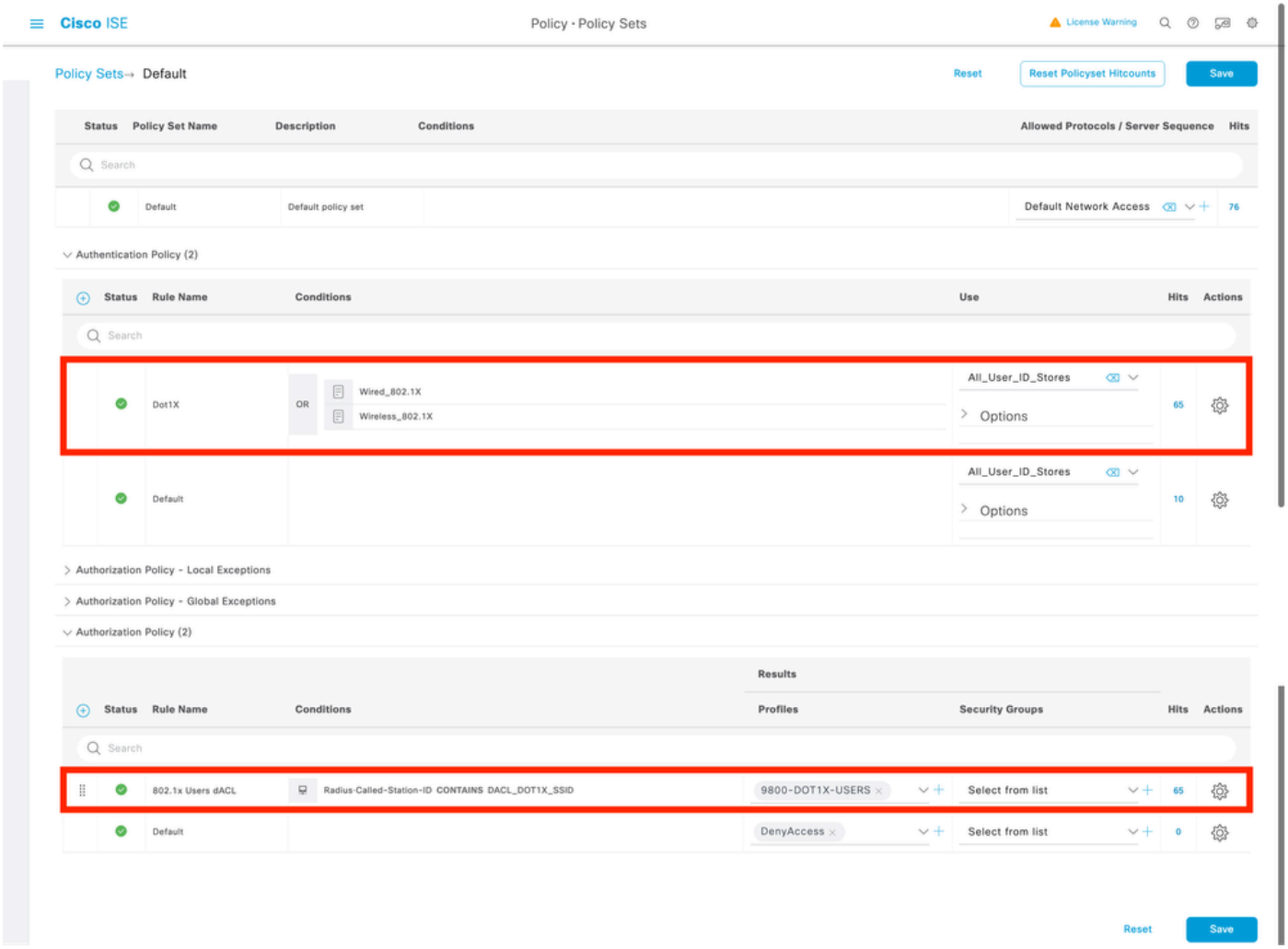


Schritt 5: Autorisierungsprofil im Richtliniensatz verwenden.

Wenn das Autorisierungsprofil korrekt definiert wurde, muss es weiterhin Teil des Richtliniensatzes sein, der für die Authentifizierung und Autorisierung von Wireless-Benutzern verwendet wird. Navigieren Sie zu Policy > Policy Sets, und öffnen Sie den verwendeten Policy Set.

Hier entspricht die Authentifizierungsrichtlinienregel "Dot1X" jeder Verbindung, die über kabelgebundene oder drahtlose 802.1x-Verbindungen hergestellt wird. Die Autorisierungsrichtlinienregel "802.1x Users dACL" implementiert eine Bedingung für die verwendete SSID (d. h. Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID). Wenn eine Autorisierung für das WLAN "DACL_DOT1X_SSID" erfolgt, wird das in Schritt 4 definierte Profil

"9800-DOT1X-USERS" zur Autorisierung des Benutzers verwendet.



Ergebnisbasierte dACLs

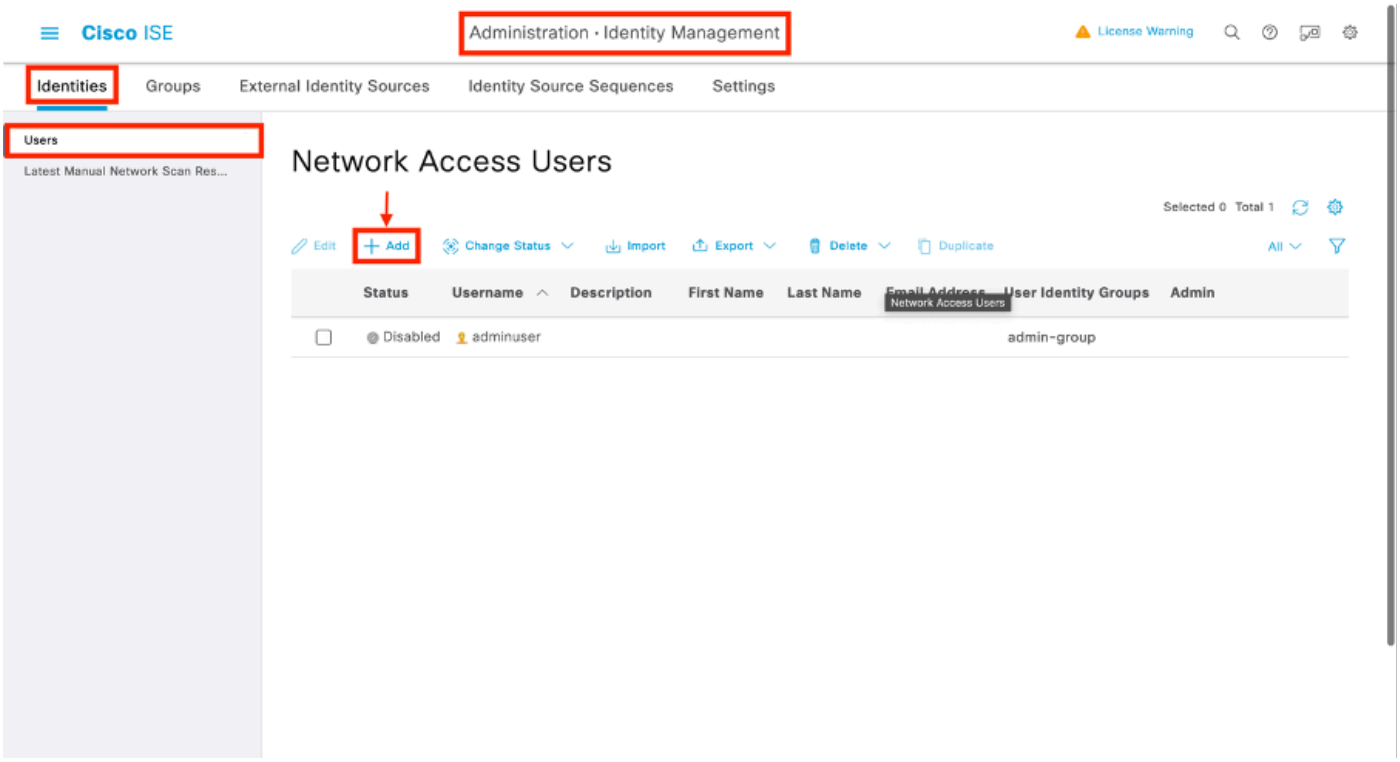
Um zu vermeiden, dass jeder auf der ISE erstellten Identität eine bestimmte dACL zugewiesen wird, kann die dACL auf ein bestimmtes Richtlinienergebnis angewendet werden. Dieses Ergebnis wird dann auf Grundlage einer Bedingung angewendet, die mit den Autorisierungsregeln aus dem verwendeten Richtliniensatz abgeglichen wurde.

Schritt 1: Konfigurieren der dACL

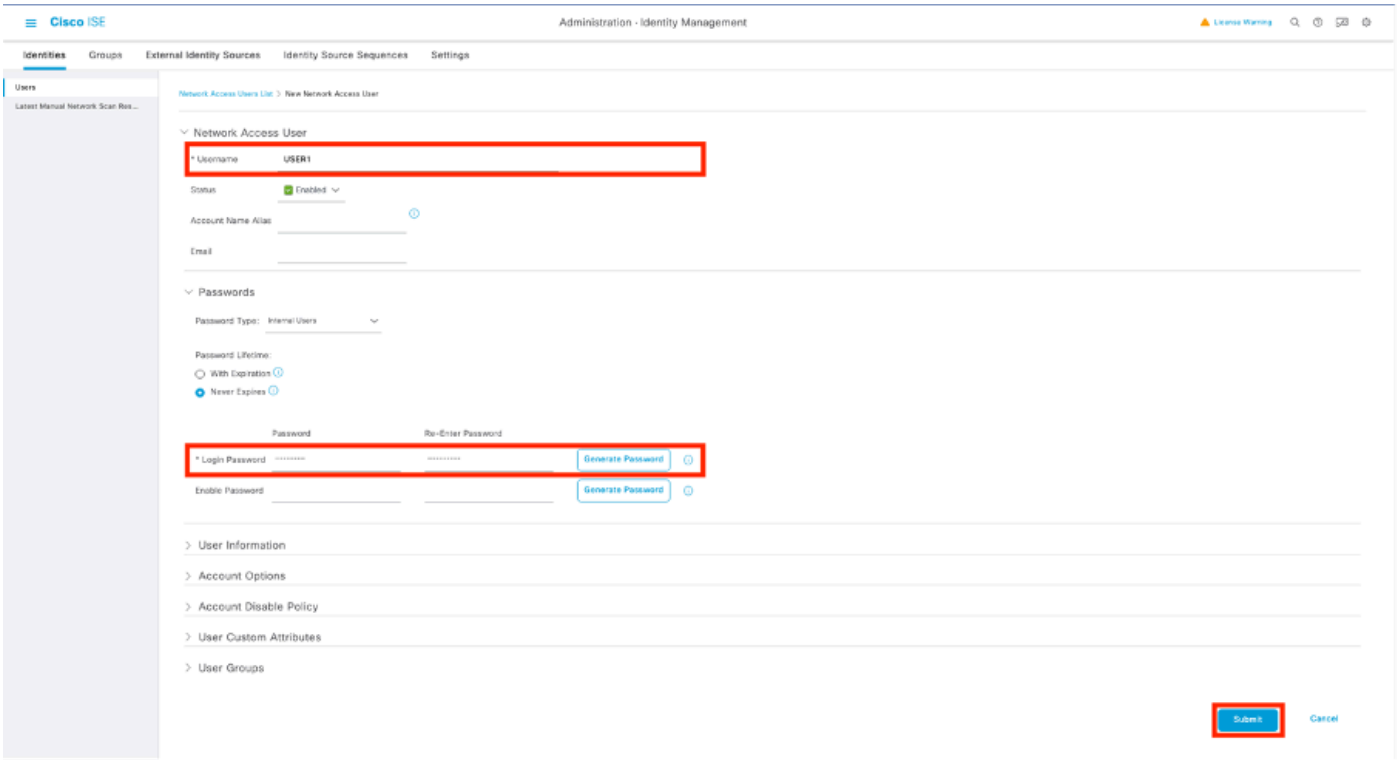
Führen Sie denselben Schritt 2 aus dem Abschnitt "Benutzerspezifische dACLs" aus, um die erforderlichen dACLs zu definieren. Dies sind ACL_USER1 und ACL_USER2.

Schritt 2: Identitäten erstellen

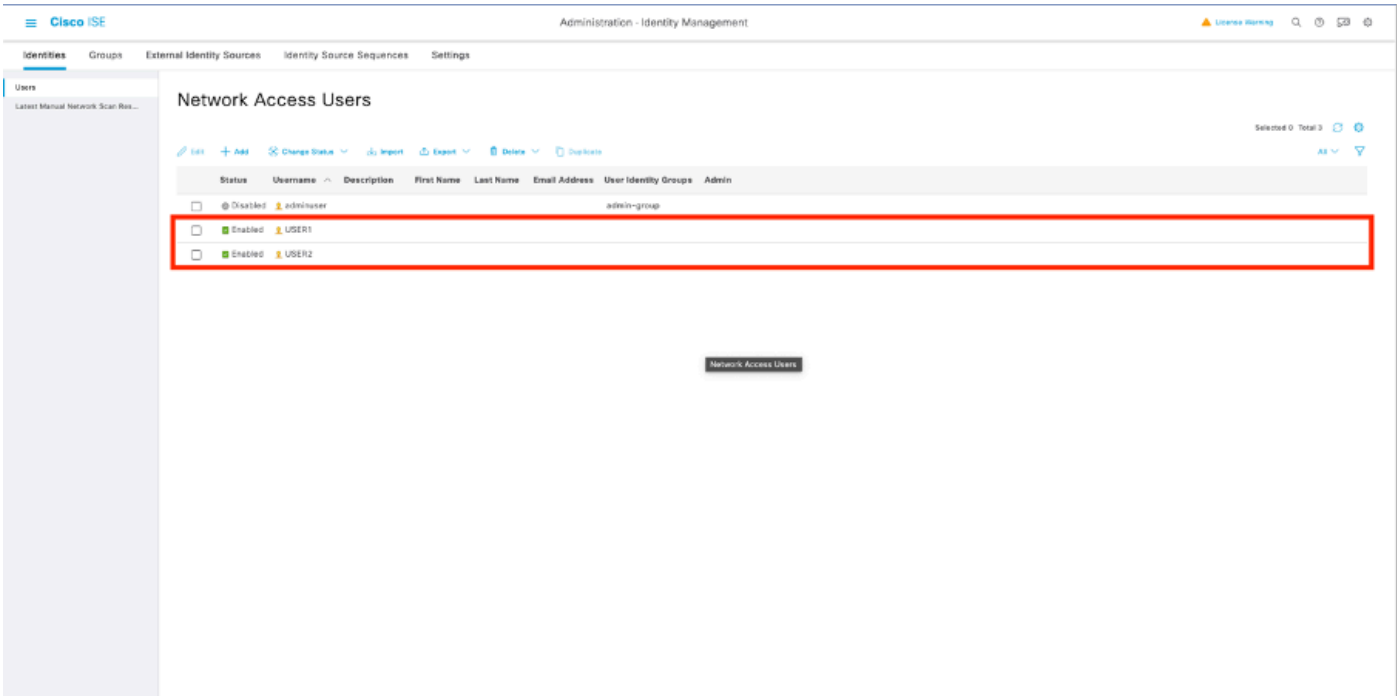
Navigieren Sie zu Administration > Identity Management > Identities > Users, und erstellen Sie mit der Schaltfläche "Add" einen Benutzer.



Legen Sie im Konfigurationsformular "New Network Access User" (Neuer Netzwerkzugriffsbenutzer) den Benutzernamen und das Kennwort für den erstellten Benutzer fest.



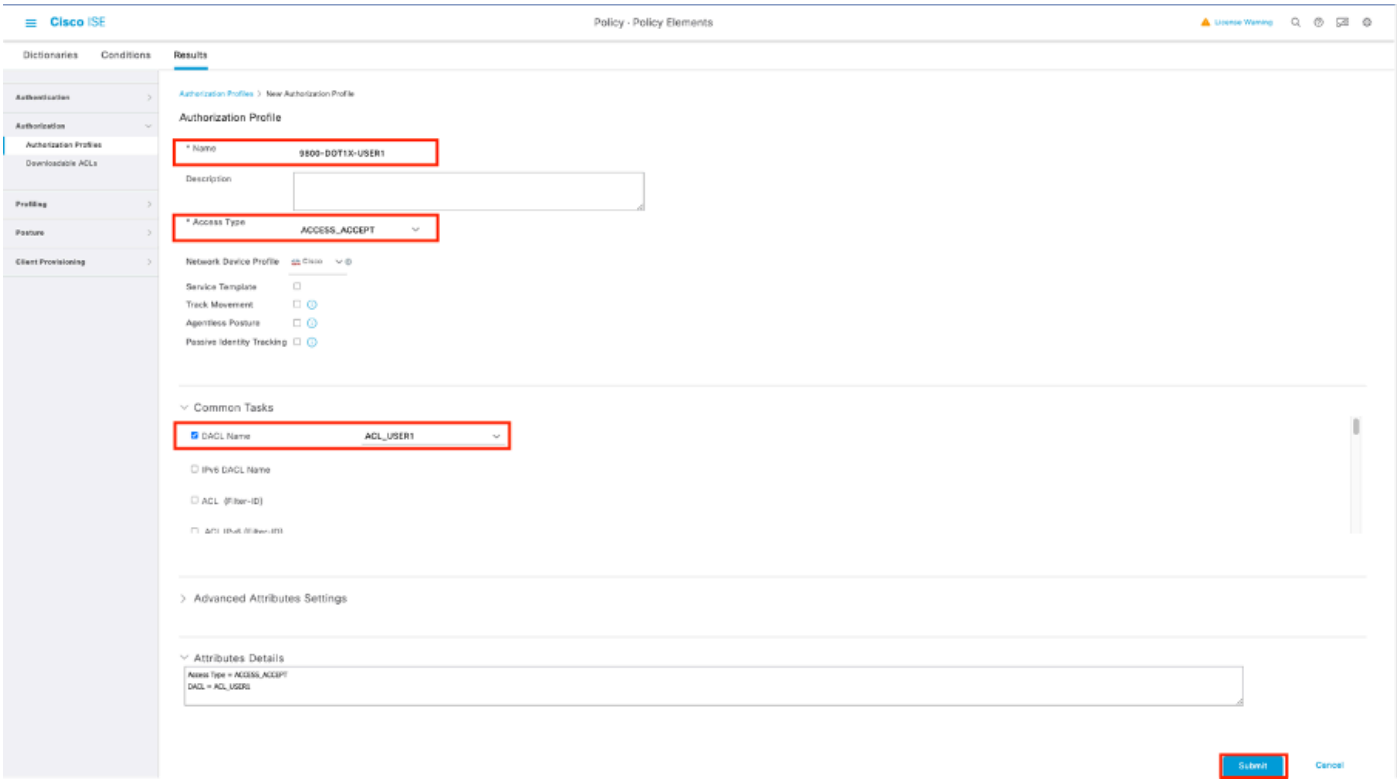
Wiederholen Sie diesen Schritt, um USER2 zu erstellen.



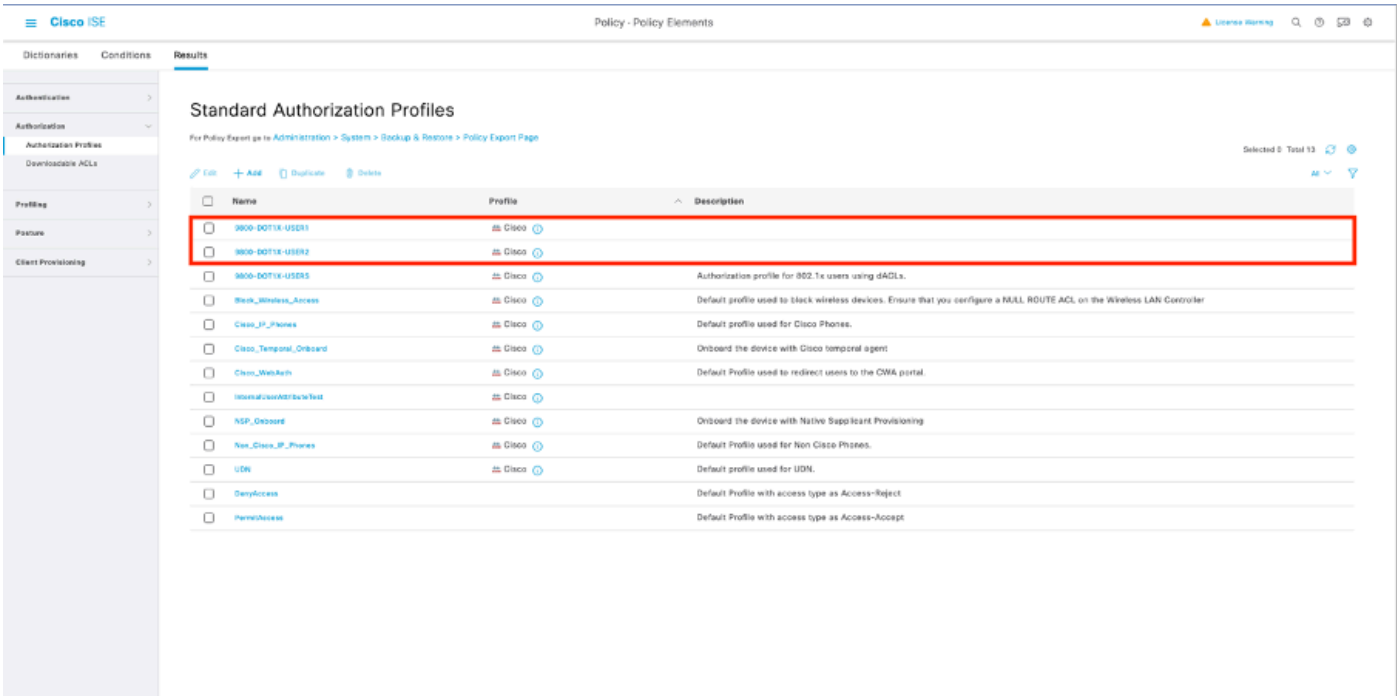
Schritt 4: Konfigurieren Sie das Ergebnis der Autorisierungsrichtlinie.

Nach der Konfiguration der Identität und der dACL muss die Autorisierungsrichtlinie weiterhin konfiguriert werden, damit dem Benutzer, der die Bedingung für die Verwendung dieser Richtlinie erfüllt, eine bestimmte dACL zugewiesen werden kann. Navigieren Sie dazu zu Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile. Verwenden Sie die Schaltfläche "Hinzufügen", um eine neue Autorisierungsrichtlinie zu definieren, und füllen Sie diese Felder aus.

- Name: der Name der Autorisierungsrichtlinie, hier "9800-DOT1X-USER1".
- Access Type (Zugriffstyp): Der beim Abgleich dieser Richtlinie verwendete Zugriffstyp, hier ACCESS_ACCEPT.
- Allgemeine Aufgabe: Für internen Benutzer "DACL Name" mit "ACL_USER1" abgleichen. Entsprechend den in diesem Dokument verwendeten Namen wird das Profil 9800-DOT1X-USER1 mit der dACL konfiguriert, die als "ACL_USER1" konfiguriert ist.



Wiederholen Sie diesen Schritt, um das Richtlinienergebnis "9800-DOT1X-USER2" zu erstellen und ihm "ACL_USER2" als DACL zuzuweisen.

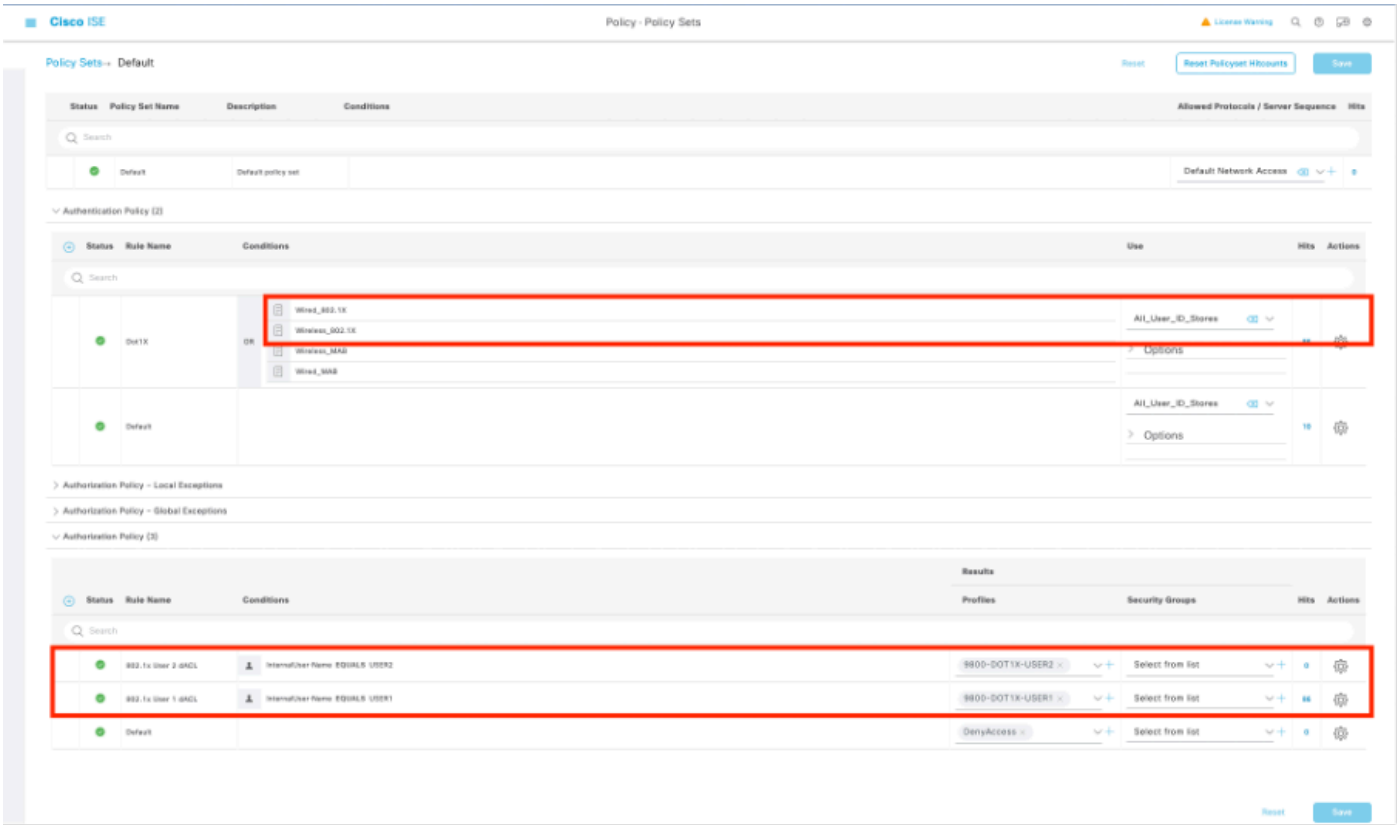


Schritt 5: Autorisierungsprofile im Richtliniensatz verwenden.

Sobald das Autorisierungsprofil korrekt definiert wurde, muss es weiterhin Teil des Richtliniensatzes sein, der für die Authentifizierung und Autorisierung von Wireless-Benutzern verwendet wird. Navigieren Sie zu Policy > Policy Sets, und öffnen Sie den verwendeten Policy Set.

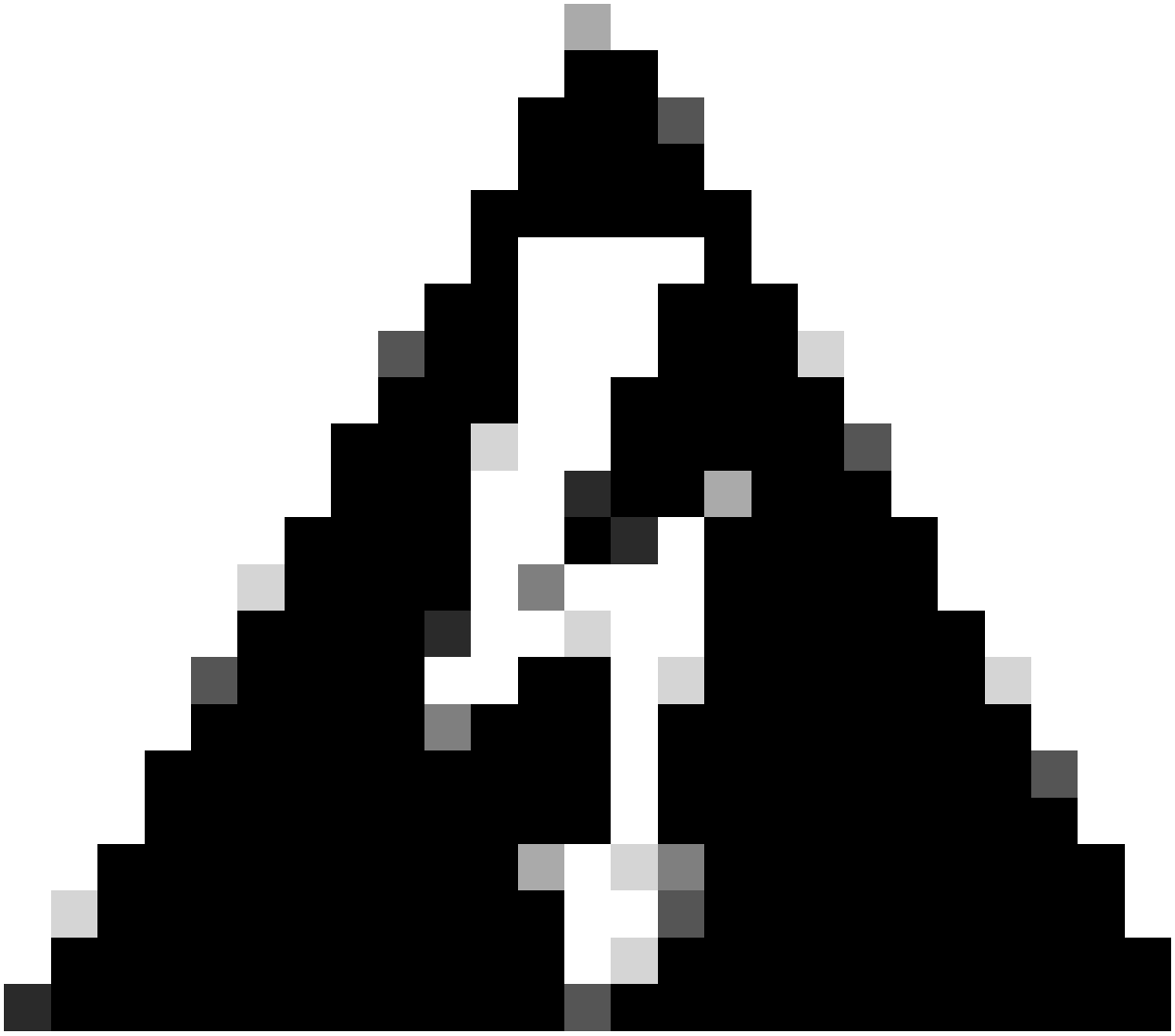
Hier entspricht die Authentifizierungsrichtlinienregel "Dot1X" jeder über kabelgebundene oder

drahtlose 802.1X-Verbindungen hergestellten Verbindung. Die Autorisierungsrichtlinienregel "802.1X User 1 dACL" implementiert eine Bedingung für den verwendeten Benutzernamen (d. h. InternalUser-Name CONTAINS USER1). Wird eine Autorisierung unter Verwendung des Benutzernamens USER1 durchgeführt, wird das in Schritt 4 definierte Profil "9800-DOT1X-USER1" zur Autorisierung des Benutzers verwendet und somit die aus diesem Ergebnis resultierende dACL (ACL_USER1) auch auf den Benutzer angewendet. Dasselbe gilt für den Benutzernamen USER2, für den "9800-DOT1X-USER1" verwendet wird.



Hinweise zur Verwendung von dACLs mit CWA-SSIDs

Wie im Configure Central Web Authentication (CWA) auf dem Catalyst 9800 WLC und in der ISE-Konfigurationsanleitung beschrieben, stützt sich CWA bei der Authentifizierung und Autorisierung von Benutzern auf MAB und bestimmte Ergebnisse. Herunterladbare ACLs können der CWA-Konfiguration von der ISE-Seite aus genau wie oben beschrieben hinzugefügt werden.



Warnung: Herunterladbare ACLs können nur als Netzwerkzugriffslisten verwendet werden und werden nicht als Pre-Authentication-ACLs unterstützt. Daher muss jede in einem CWA-Workflow verwendete ACL vor der Authentifizierung in der WLC-Konfiguration definiert werden.

Überprüfung

Zur Verifizierung der vorgenommenen Konfiguration können diese Befehle verwendet werden.

```
# 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 }
```

Es wird auf den entsprechenden Teil der WLC-Konfiguration für dieses Beispiel verwiesen.

```
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
```

Die RADIUS-Serverkonfiguration wird mit dem Befehl show running-config all angezeigt.

```
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
```

Fehlerbehebung

Checkliste

- Stellen Sie sicher, dass die Clients eine Verbindung mit der konfigurierten 802.1X-SSID herstellen können.
- Stellen Sie sicher, dass die RADIUS-Zugriffsanforderung/-akzeptiert die richtigen Attribut-Wert-Paare (AVPs) enthält.
- Stellen Sie sicher, dass die Clients das richtige WLAN-/Richtlinienprofil verwenden.

WLC One Stopp Shop Reflex

Um zu überprüfen, ob die dACL einem bestimmten Wireless-Client ordnungsgemäß zugewiesen ist, können Sie den Befehl **show wireless client mac-address <H.H.H> detail** verwenden. Daraus sind verschiedene nützliche Informationen zur Fehlerbehebung ersichtlich, nämlich: der Client-Benutzername, der Status, das Richtlinienprofil, das WLAN und hier vor allem die 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

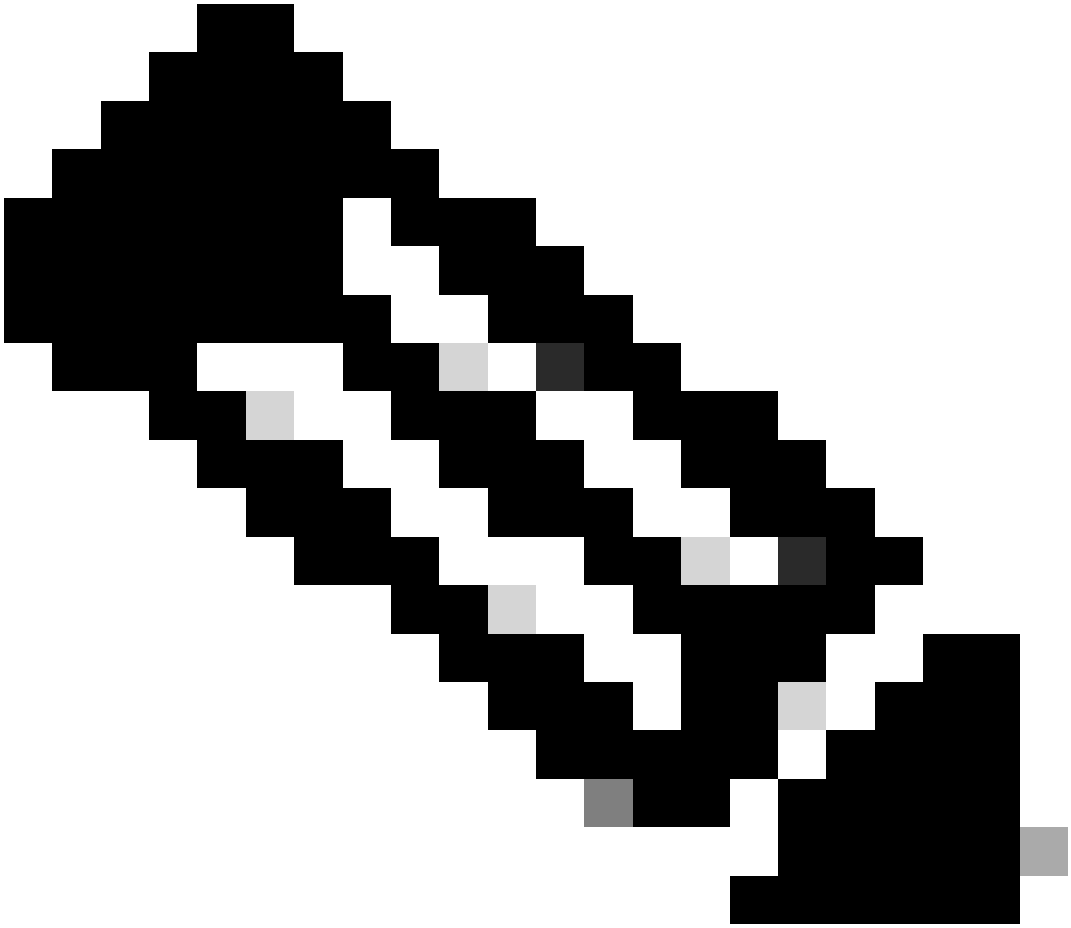
Resultant Policies:

ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab VLAN Name : VLAN_1413 VLAN : 1413 Absolute-Timer : 28800

[...]

WLC Befehle anzeigen

Mit dem Befehl **show access-lists** können Sie alle ACLs anzeigen, die derzeit Teil der Catalyst 9800 WLC-Konfiguration sind. Mit diesem Befehl werden alle lokal definierten ACLs oder vom WLC heruntergeladenen dACLs aufgelistet. Alle vom WLC von der ISE heruntergeladenen dACLs haben das Format xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.



Hinweis: Herunterladbare ACLs verbleiben in der Konfiguration, solange ein Client zugeordnet ist und sie in der Wireless-Infrastruktur verwendet. Sobald der letzte Client, der die dACL verwendet, die Infrastruktur verlässt, wird die dACL aus der Konfiguration entfernt.

```
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
[...]
```

Bedingtes Debugging und Radio Active Tracing

Während der Fehlerbehebung können Sie radioaktive Spuren für einen Client sammeln, der mit der definierten dACL zugewiesen werden soll. Hier sind die Protokolle hervorgehoben, die den interessanten Teil der radioaktiven Spuren während des Client-Assoziierungsprozesses für Client 08be.ac14.137d zeigen.

<#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 [31]
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[1
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 fa
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 th
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_9000

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_9000

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

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=

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

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=

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

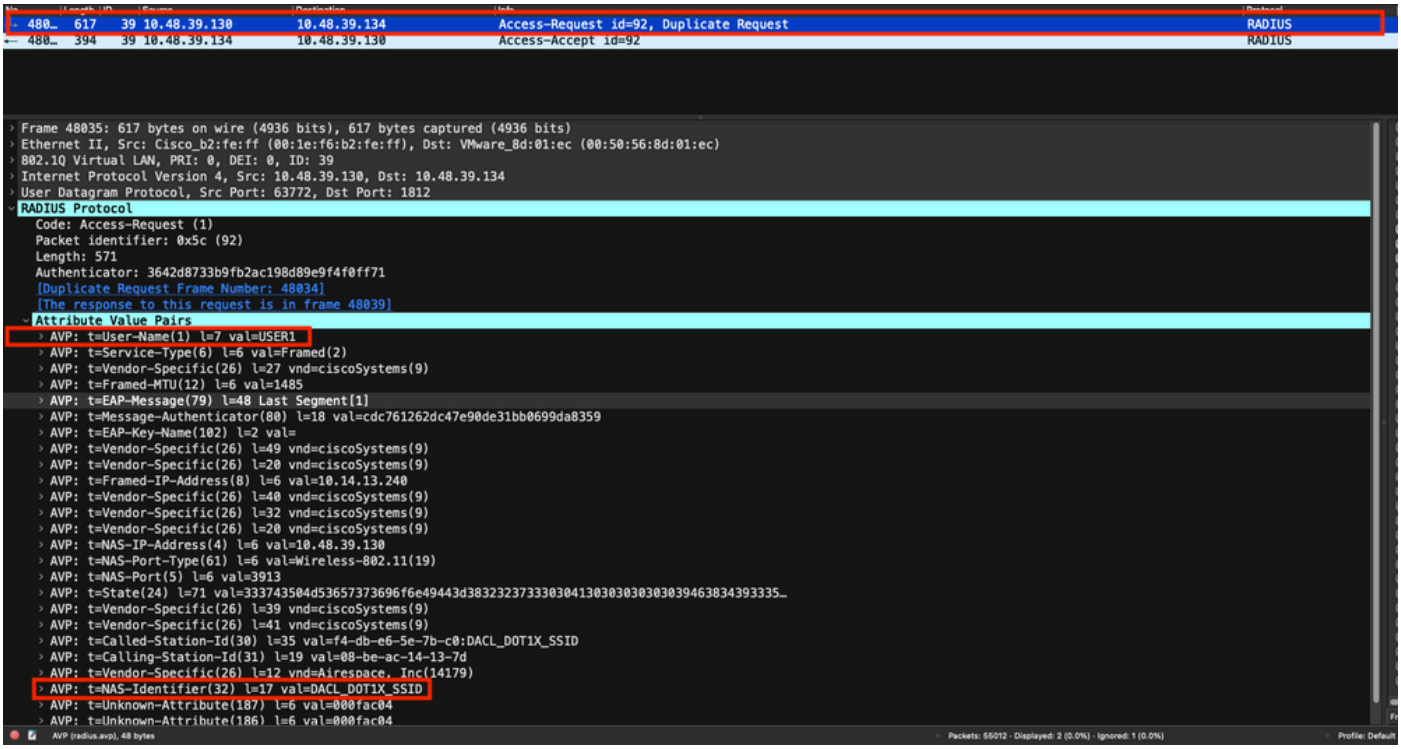
```
2024/03/28 10:43:04.789642576 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute :Cis

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
```

Paketerfassung

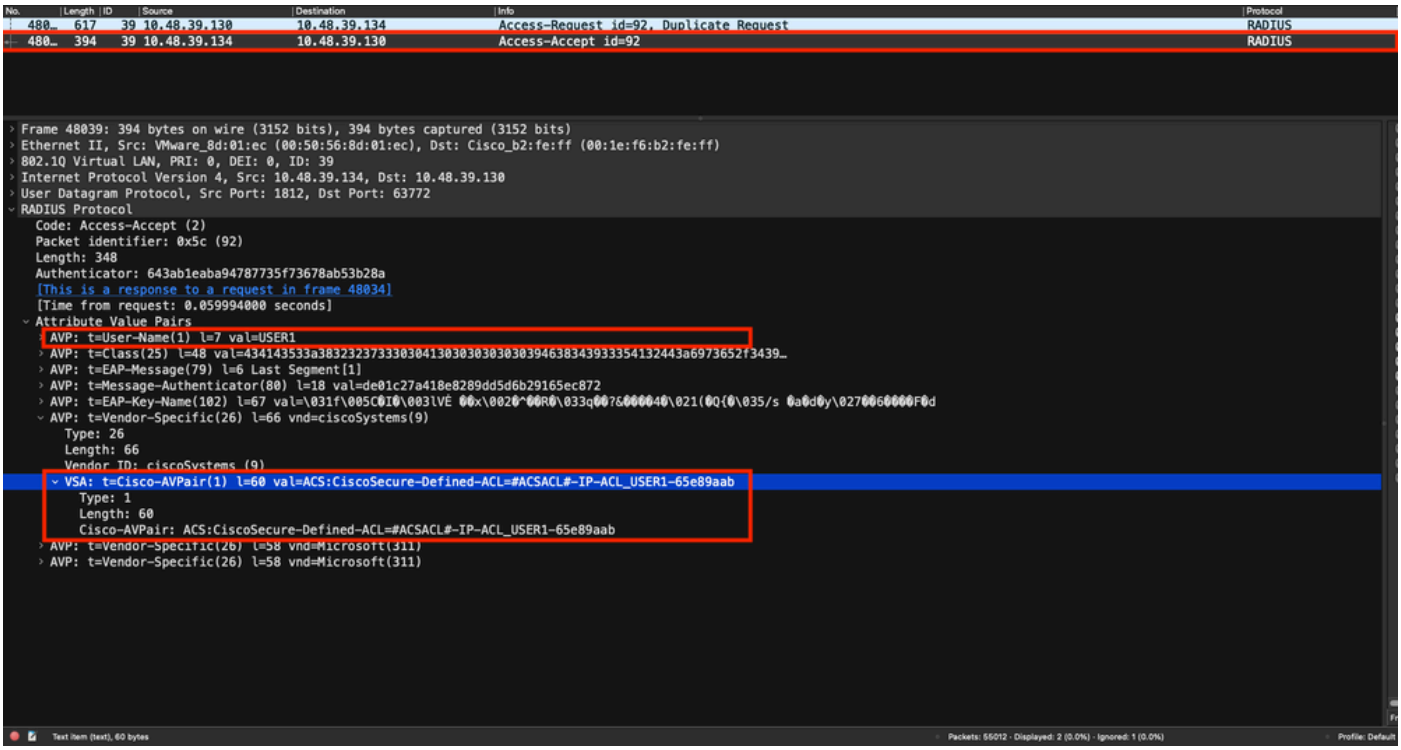
Ein weiterer interessanter Reflex besteht darin, die Paketerfassung des RADIUS-Flusses für eine Client-Zuordnung zu analysieren. Herunterladbare ACLs basieren nicht nur auf RADIUS, um einem Wireless-Client zugewiesen zu werden, sondern auch, um vom WLC heruntergeladen zu werden. Während der Paketerfassung für die Fehlerbehebung der dACL-Konfiguration müssen Sie daher die Erfassung auf der Schnittstelle vornehmen, die vom Controller für die Kommunikation mit dem RADIUS-Server verwendet wird. In diesem Dokument wird die Konfiguration der einfach eingebetteten Paketerfassung auf dem Catalyst 9800 erläutert, mit der die in diesem Artikel analysierte Erfassung erfasst wurde.

RADIUS-Client-Authentifizierung

Sie können die vom WLC an den RADIUS-Server gesendete RADIUS-Clientzugriffsanforderung sehen, um den Benutzer USER1 (AVP User-Name) auf der DACL_DOT1X_SSID-SSID (AVP NAS-Identifier) zu authentifizieren.

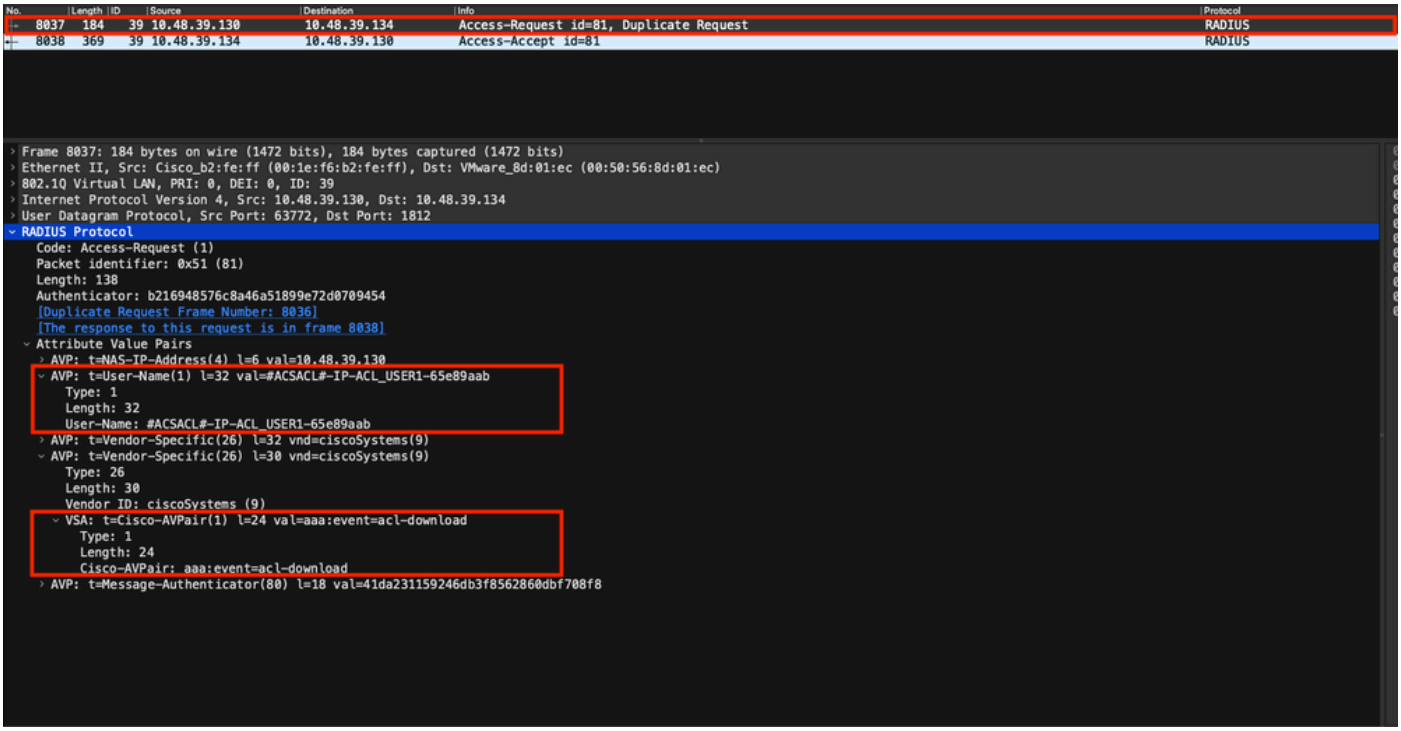


Wenn die Authentifizierung erfolgreich ist, antwortet der RADIUS-Server mit einem "access-accept", also nach wie vor für den Benutzer USER1 (AVP User-Name), und wendet die AAA-Attribute an, wobei insbesondere der anbieterspezifische AVP ACS:CiscoSecure-Defined-ACL hier "#ACSACL#-IP-ACL_USER1-65e89aab" ist.

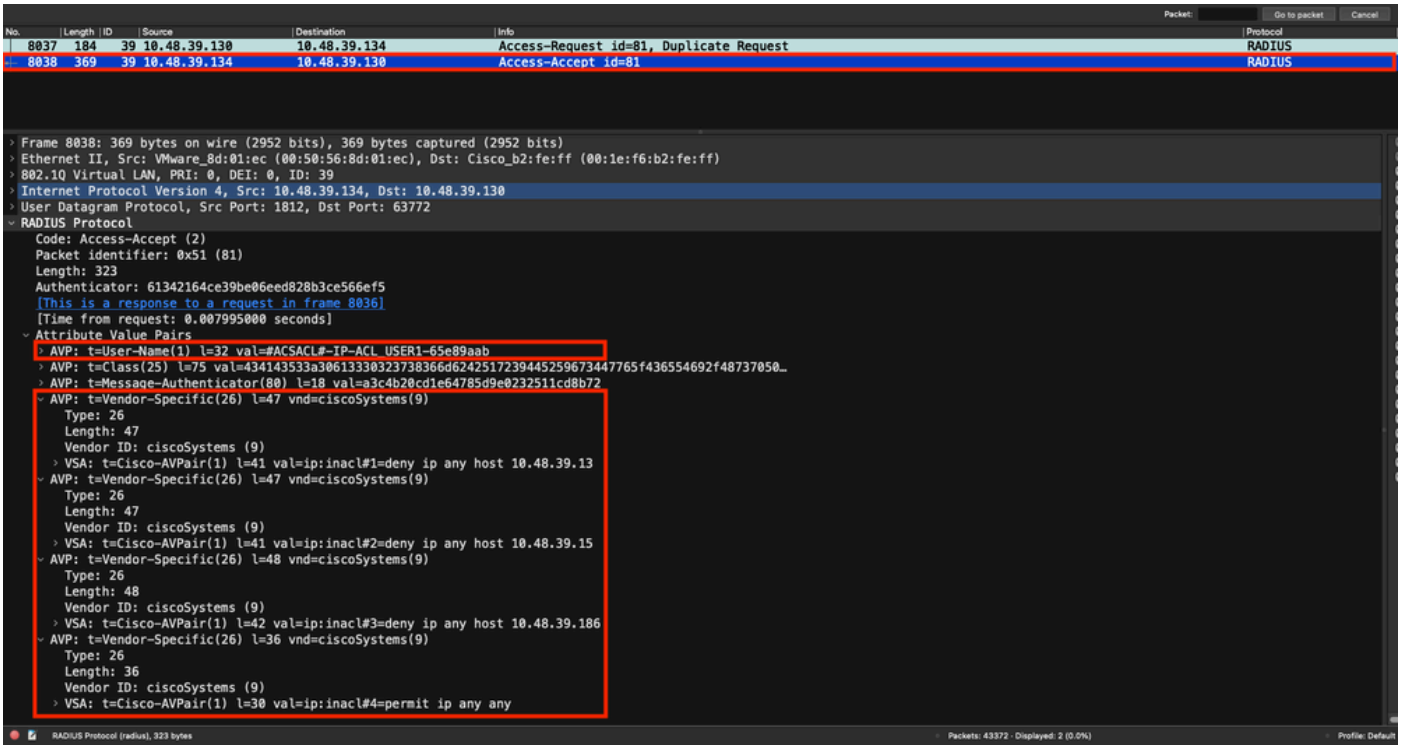


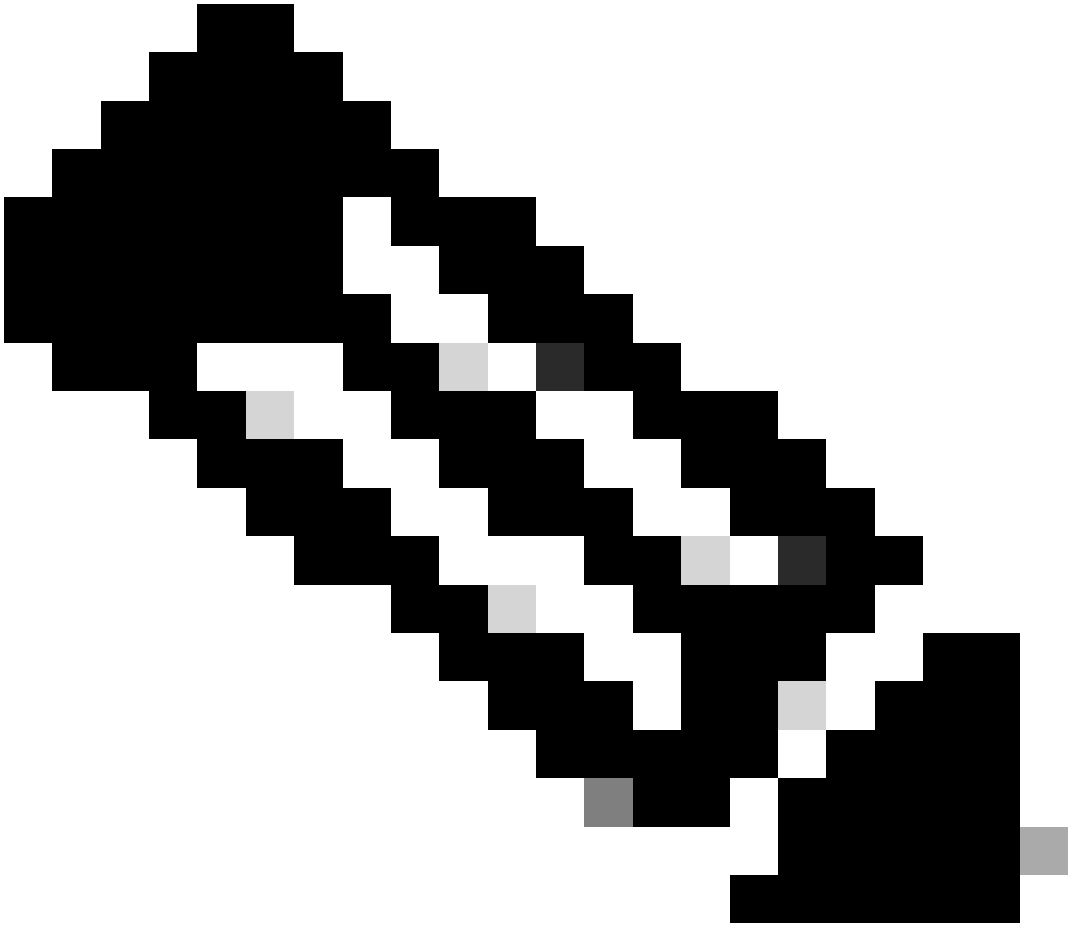
DACL-Download

Wenn die dACL bereits Teil der WLC-Konfiguration ist, wird sie einfach dem Benutzer zugewiesen, und die RADIUS-Sitzung wird beendet. Andernfalls lädt der WLC die ACL herunter, wobei weiterhin RADIUS verwendet wird. Dazu stellt der WLC eine RADIUS-Zugriffsanforderung aus, diesmal unter Verwendung des dACL-Namens ("#ACSACL#-IP-ACL_USER1-65e89aab") für den AVP-Benutzernamen. Darüber hinaus informiert der WLC den RADIUS-Server, dass dieser "access-accept" einen ACL-Download mit dem Cisco AV-Paar aaa:event=acl-download initiiert.



Die RADIUS-Zugriffsbestätigung, die an den Controller zurückgesendet wird, enthält die angeforderte dACL (siehe Abbildung). Jede ACL-Regel ist in einer anderen Cisco AVP vom Typ "ip:inacl#**<X>**=<ACL_RULE>" enthalten, wobei <X> die Regelnummer ist.



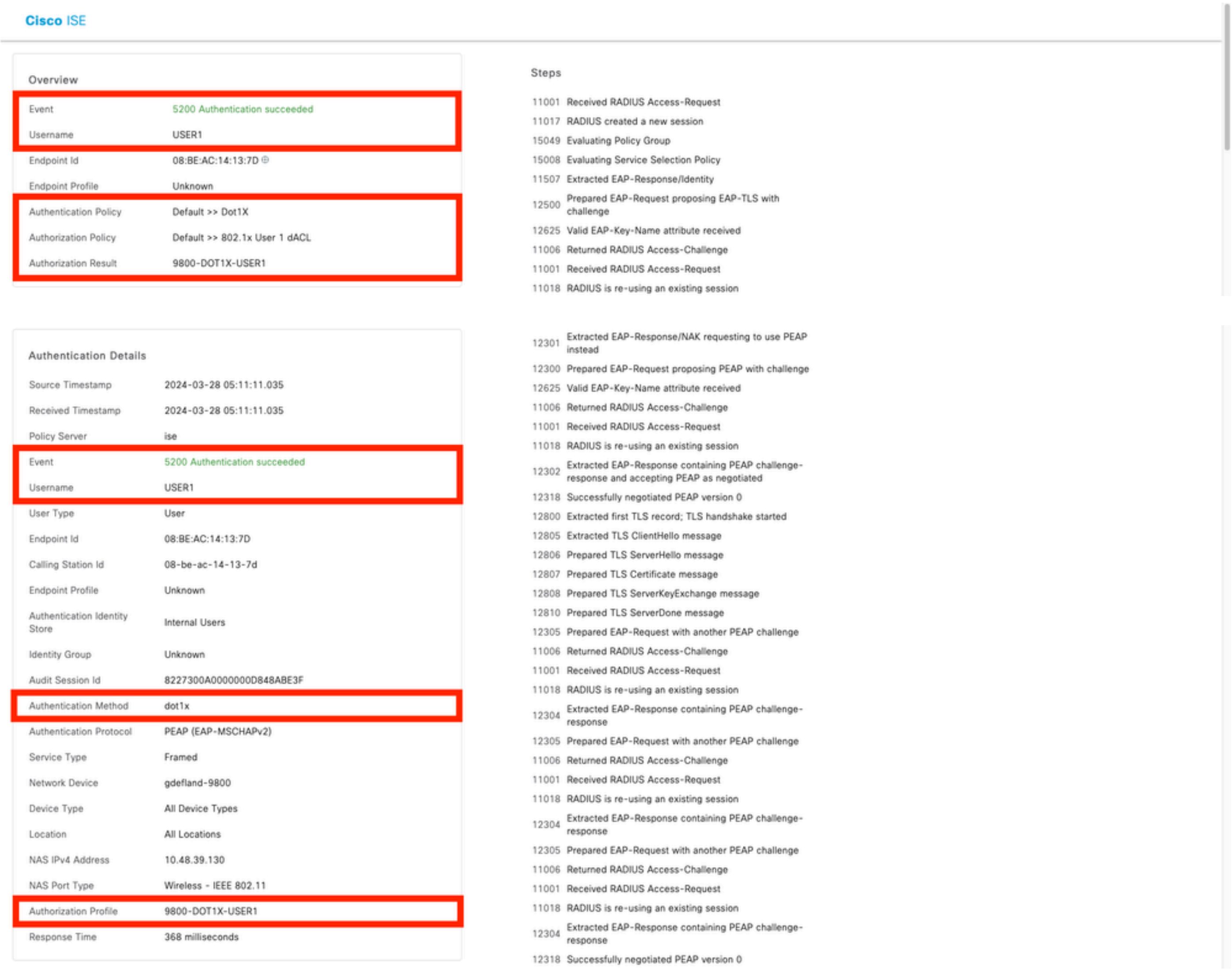


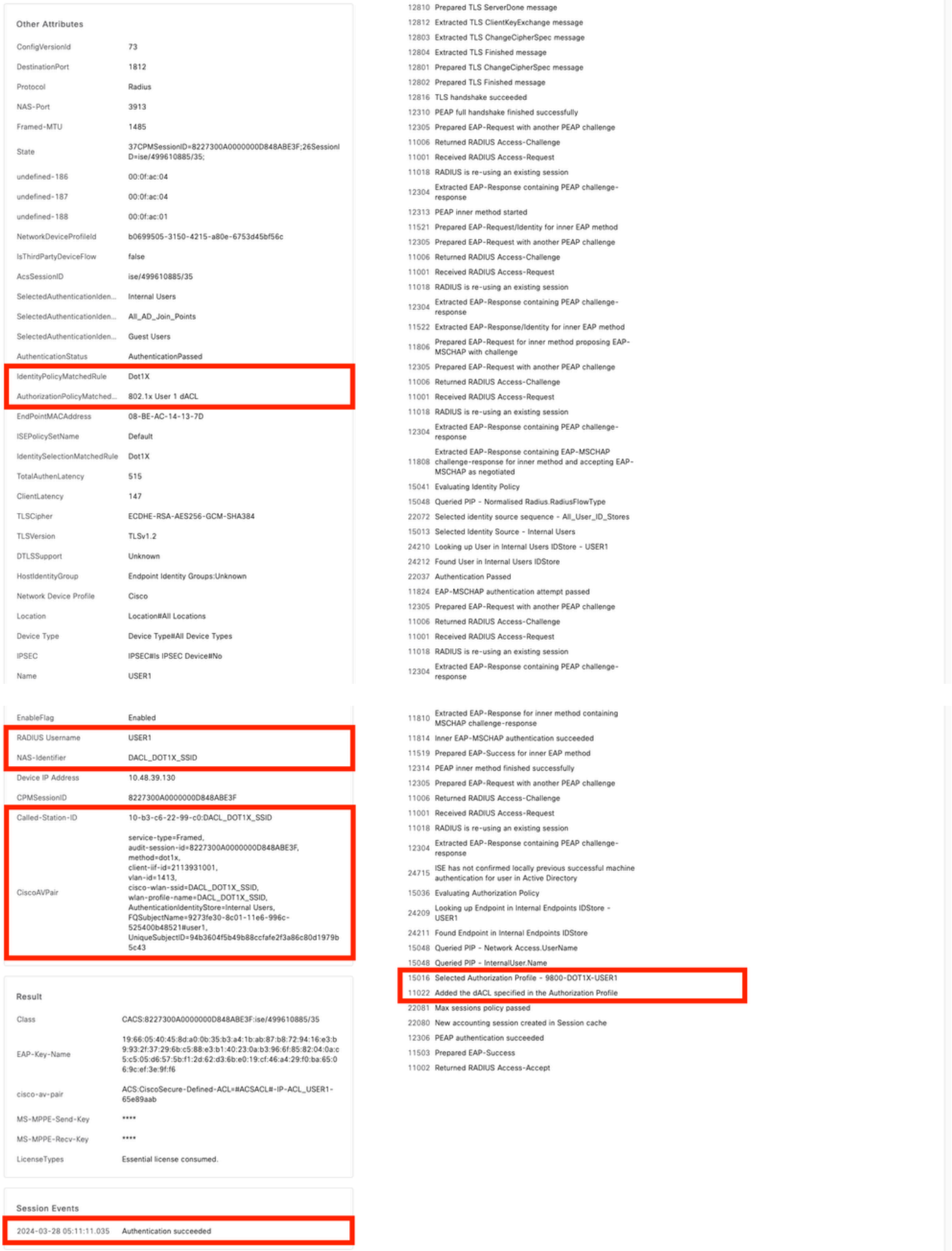
Hinweis: Wenn der Inhalt einer Download-ACL geändert wird, nachdem sie auf den WLC heruntergeladen wurde, wird die Änderung für diese ACL erst übernommen, wenn sich ein Benutzer, der diese verwendet, erneut authentifiziert (und der WLC führt für einen solchen Benutzer erneut eine RADIUS-Authentifizierung durch). Eine Änderung der ACL spiegelt sich auch im Hash-Teil des ACL-Namens wider. Wenn diese ACL einem Benutzer das nächste Mal zugewiesen wird, muss ihr Name daher anders sein, und die ACL darf daher nicht Teil der WLC-Konfiguration sein und soll heruntergeladen werden. Clients, die sich vor der Änderung in der ACL authentifizieren, verwenden die vorherige jedoch so lange weiter, bis sie sich vollständig erneut authentifizieren.

ISE-Betriebsprotokolle

RADIUS-Client-Authentifizierung

Die Betriebsprotokolle zeigen eine erfolgreiche Authentifizierung des Benutzers "USER1" an, auf den die herunterladbare ACL "ACL_USER1" angewendet wird. Die für die Fehlerbehebung interessanten Bereiche sind rot eingerahmt.


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

Die Betriebsprotokolle zeigen an, dass die ACL "ACL_USER1" erfolgreich heruntergeladen wurde. Die für die Fehlerbehebung interessanten Bereiche sind rot eingerahmt.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.