

配置 & 對 Catalyst 9800 上的可下載 ACL 進行故障排除

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[將 dACL 與 802.1x SSID 一起使用](#)

[網路圖表](#)

[WLC 配置](#)

[ISE 組態](#)

[每使用者 dACL](#)

[基於結果的 dACL](#)

[有關將 dACL 與 CWA SSID 一起使用的說明](#)

[驗證](#)

[疑難排解](#)

[檢查清單](#)

[WLC One Stop-Shop 反射](#)

[WLC Show 命令](#)

[條件式偵錯和無線電主動式追蹤](#)

[資料包捕獲](#)

[RADIUS 客戶端身份驗證](#)

[dACL 下載](#)

[ISE 操作日誌](#)

[RADIUS 客戶端身份驗證](#)

[dACL 下載](#)

簡介

本檔案介紹如何在 Catalyst 9800 無線 LAN 控制器 (WLC) 上設定可下載 ACL (dACL) 並對其進行疑難排解。

背景資訊

Cisco IOS® 和 IOS XE® 交換機已支援 dACL 多年。dACL 是指網路裝置在進行身份驗證時從 RADIUS 伺服器動態下載 ACL 條目，而不是僅獲取 ACL 的本地副本並分配 ACL 名稱。有更完整的

[Cisco ISE配置示例](#)可用。本文檔重點介紹自17.10版以來支援用於集中交換的dACL的Cisco Catalyst 9800。

必要條件

本文檔的思想是透過基本SSID配置示例演示Catalyst 9800上的dACL使用情況，展示如何完全自定義這些dACL。

在Catalyst 9800無線控制器上，可下載ACL是

- 支援從[Cisco IOS XE都柏林17.10.1](#)版本開始。
- 僅支援具有本地模式存取點的集中控制器（或Flexconnect集中交換）。FlexConnect本地交換不支援dACL。

需求

思科建議您瞭解以下主題：

- Catalyst無線9800配置型號。
- Cisco IP Access Control Lists (ACL)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9800-CL（v.都柏林17.12.03）。
- ISE (v. 3.2)。

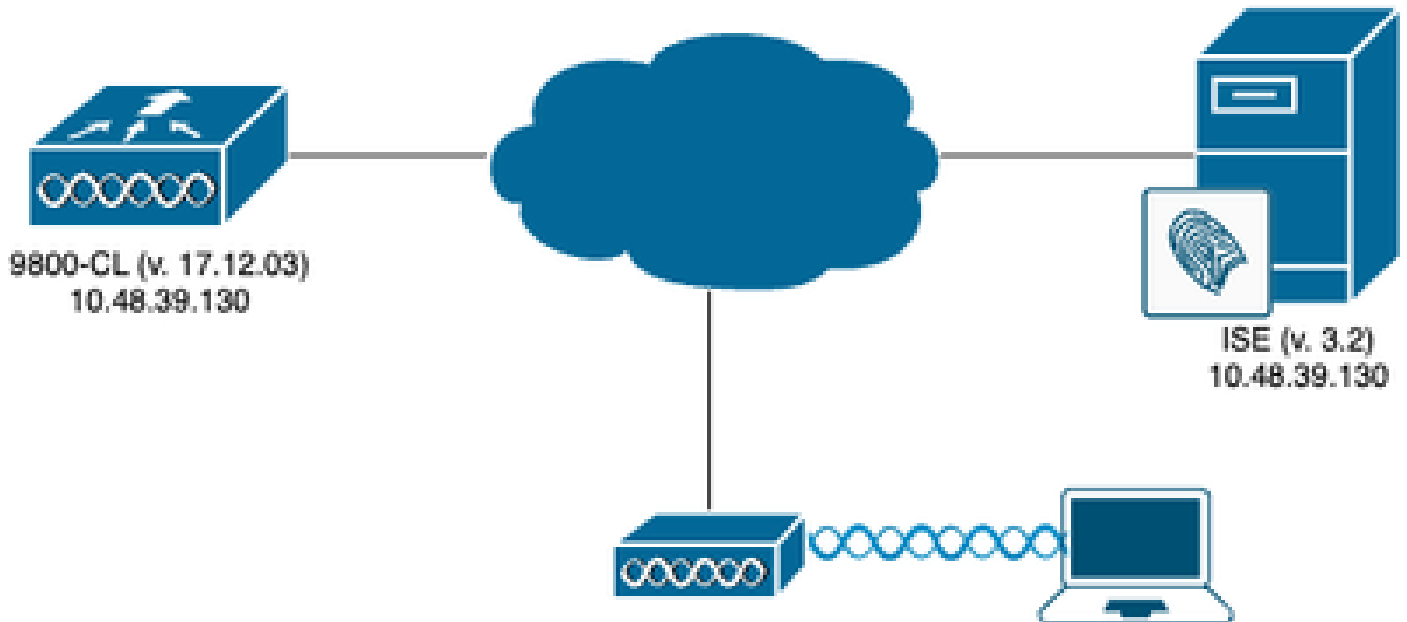
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

在本配置指南中，即使方法不同（例如WLAN身份驗證、策略配置等），最終結果也相同。在此顯示的方案中，定義了兩個使用者身份：USER1和USER2。兩者都被授予了無線網路的訪問許可權。ACL_USER1和ACL_USER2是Catalyst 9800從ISE下載的dACL。

將dACL與802.1x SSID一起使用

網路圖表



WLC配置

有關Catalyst 9800上的802.1x SSID配置和故障排除的詳細資訊，請參閱[在Catalyst 9800無線控制器系列上配置802.1X身份驗證](#)配置指南。

步驟 1. 配置SSID。

使用ISE作為RADIUS伺服器配置經過身份驗證的802.1x SSID。在本文檔中，SSID被命名為「DACL_DOT1X_SSID」。

在 GUI 上：

導航到配置>標籤和配置檔案> WLAN，然後建立如下所示的WLAN：

Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
<input type="checkbox"/>	DACL_DOT1X_SSID	2	DACL_DOT1X_SSID	[WPA2]802.1x[[AES]]	

在CLI上：

```
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
```

步驟 2. 配置策略配置檔案。

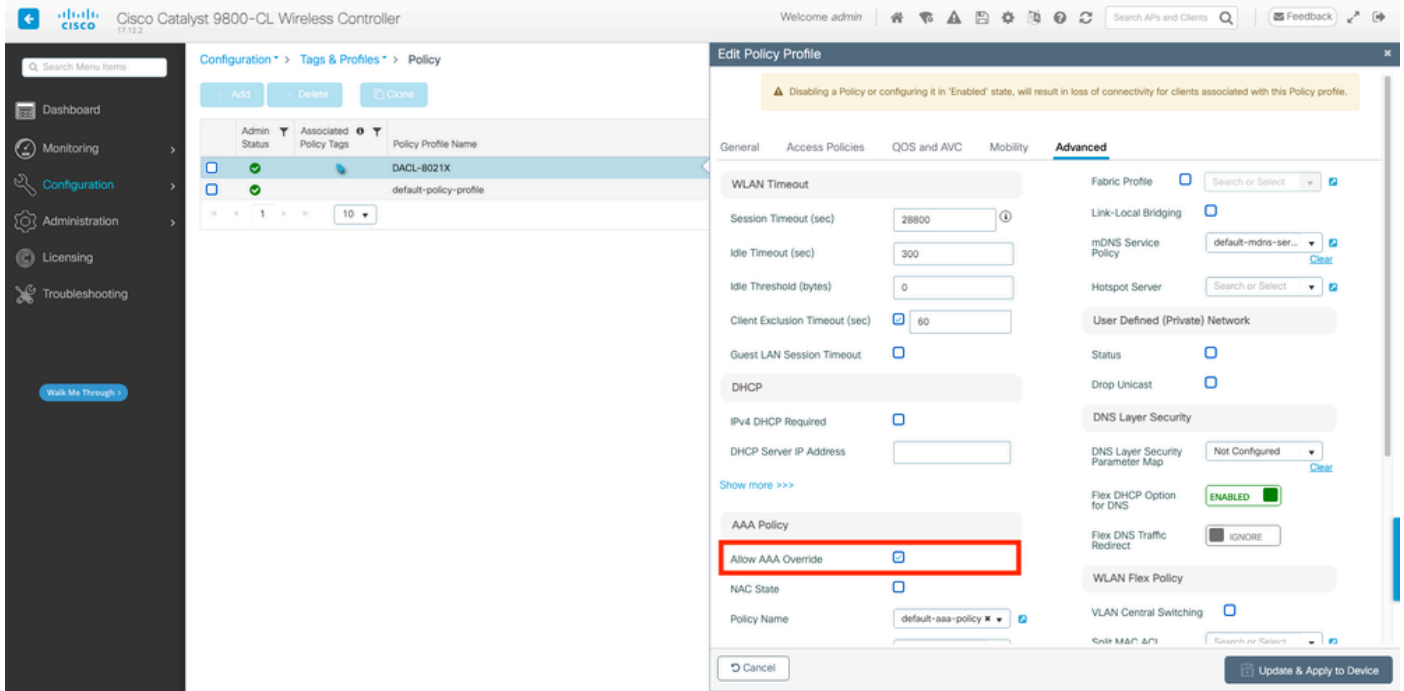
配置與上述定義的SSID一起使用的策略配置檔案。在此策略配置檔案上，確保從「高級」頁籤配置AAA覆蓋，如螢幕截圖所示。在本文檔中，使用的策略配置檔案為「DACL-8021X」。

如前提條件部分所述，dACL僅支援集中交換/身份驗證部署。確保策略配置檔案以這種方式配置。

在 GUI 上：

導航到配置>標籤和配置檔案>策略，選擇使用的策略配置檔案並如圖配置。

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. The left sidebar shows navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Tags & Profiles > Policy'. A table lists policy profiles, with 'DACL-8021X' selected and highlighted by a red box. The 'Edit Policy Profile' window is open, showing the 'General' tab. The 'Name' field is 'DACL-8021X'. The 'Status' is 'ENABLED'. The 'WLAN Switching Policy' section is highlighted with a red box, showing 'Central Switching' and 'Central Authentication' both set to 'ENABLED'. Other settings include 'Passive Client' (DISABLED), 'IP MAC Binding' (ENABLED), 'Encrypted Traffic Analytics' (DISABLED), 'CTS Policy' (Inline Tagging and SGACL Enforcement are unchecked), and 'Default SGT' (2-65519). The bottom right corner has 'Cancel' and 'Update & Apply to Device' buttons.



在CLI上：

```

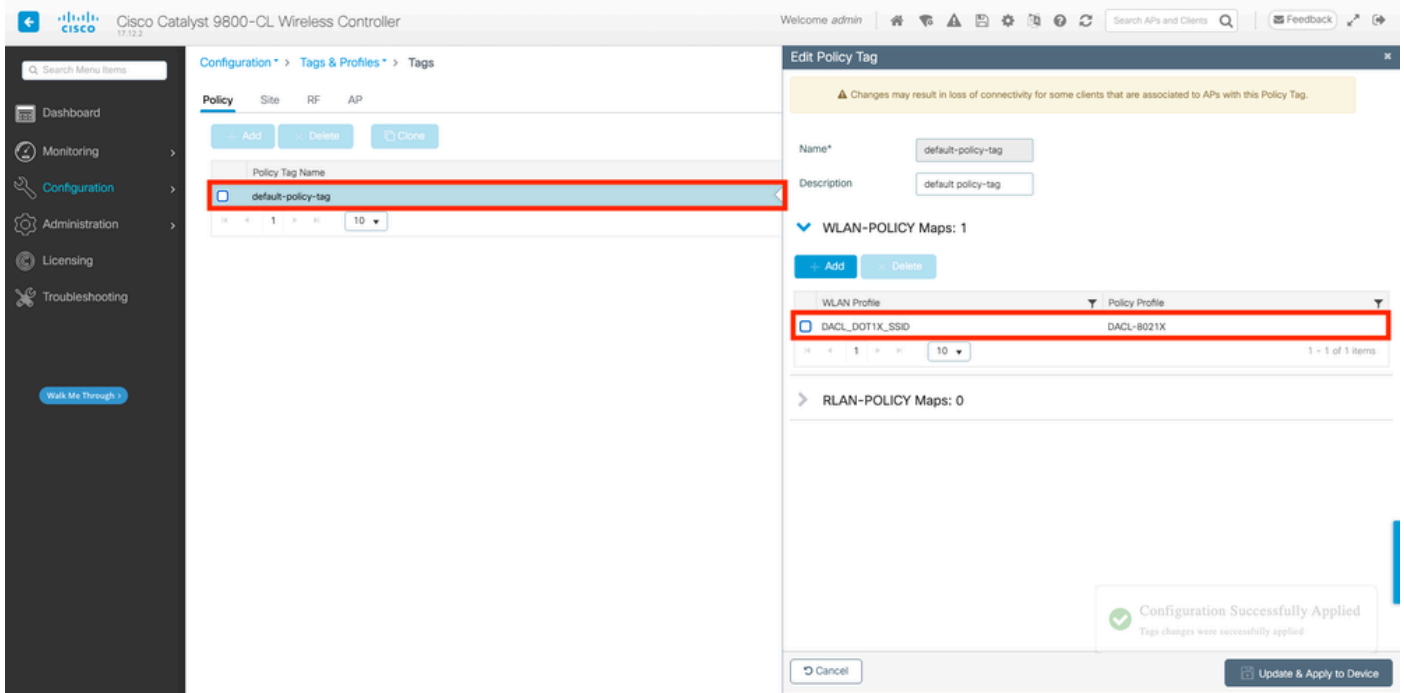
WLC#configure terminal
WLC(config)#wireless profile policy DACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown

```

步驟 3.將策略配置檔案和SSID分配給使用的策略標籤。

在 GUI 上：

導航到配置>標籤和配置檔案>標籤。在Policy tags頁籤中，建立（或選擇）使用的標籤，並為其分配步驟1-2期間定義的WLAN和策略配置檔案。



在CLI上：

```
WLC#configure terminal
WLC(config)#wireless tag policy default-policy-tag
WLC(config-policy-tag)#description "default policy-tag"
WLC(config-policy-tag)#wlan DAACL_DOT1X_SSID policy DAACL-8021X
```

步驟 4. 允許供應商特定屬性。

可下載ACL透過ISE和WLC之間的RADIUS交換中的供應商特定屬性(VSA)傳遞。可使用以下CLI命令，在WLC上啟用對這些屬性的支援。

在CLI上：

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

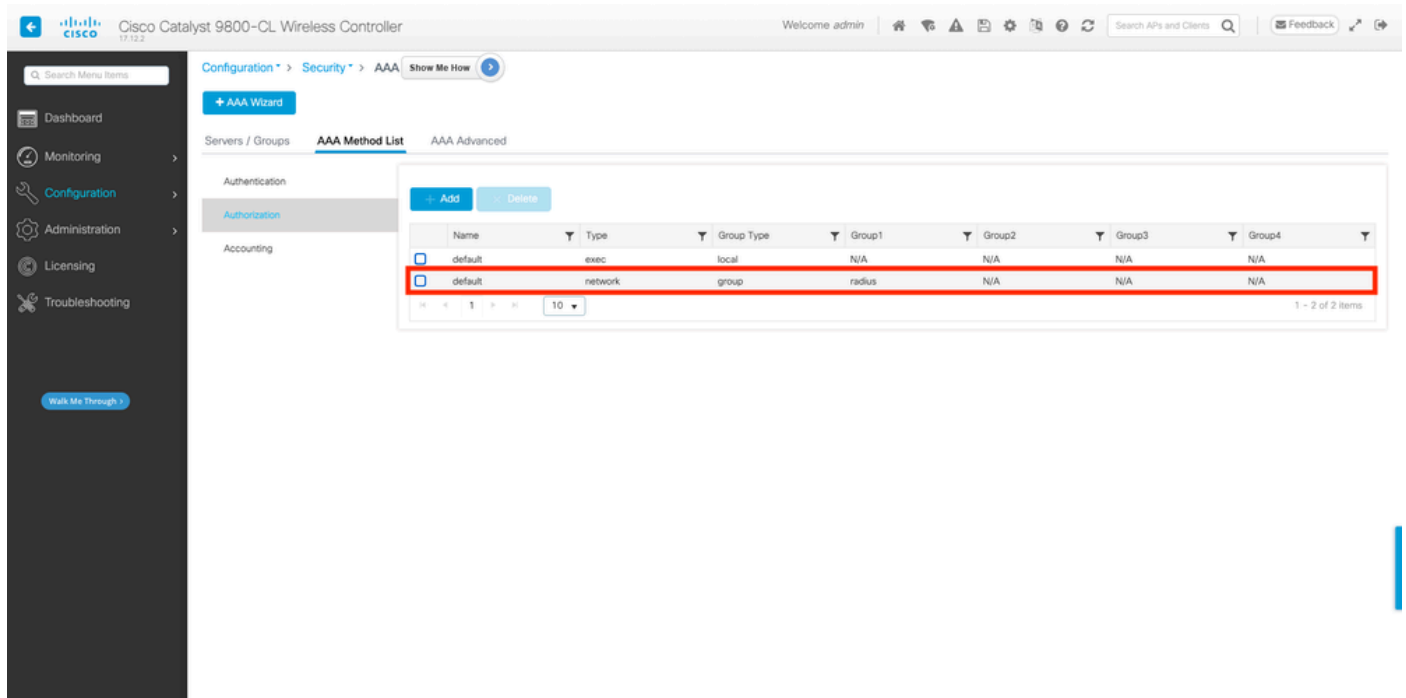
步驟 5. 配置預設授權清單。

使用dACL時，必須透過RADIUS強制執行網路授權，WLC才能授權對設定的802.1x SSID進行驗證的任何使用者。實際上，此處的RADIUS伺服器端不僅會處理驗證，而且會處理授權階段。因此，這種情況下需要授權清單。

確保預設網路授權方法是9800配置的一部分。

在 GUI 上：

導航到Configuration > Security > AAA，然後從AAA Method List > Authorization頁籤建立與所示類似的授權方法。



在CLI上：

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

ISE 組態

在採用ISE的無線環境中實施dACL時，可以採用兩種常見配置：

1. 每使用者dACL配置。藉此，每個特定辨識都會有一個透過自訂辨識欄位指定的dACL。
2. 按結果配置dACL。當選擇此方法時，系統會根據與所用策略集匹配的授權策略，將特定dACL分配給使用者。

每使用者dACL

步驟 1. 定義dACL自訂使用者屬性

要能夠將dACL分配給使用者身份，首先必須在建立的身份上配置此欄位。預設情況下，在ISE上，「ACL」欄位不會為建立的任何新身份定義。要克服這種情況，可以使用「自定義使用者屬性」並定義新的配置欄位。為此，請導航到Administration > Identity Management > Settings > User Custom Attributes。使用「+」按鈕來新增與顯示的屬性類似的新屬性。在本示例中，自定義屬性的名稱是ACL。

Administration · Identity Management

License Warning

Identities Groups External Identity Sources Identity Source Sequences **Settings**

User Custom Attributes

Mandat...	Attribute Name	Data Type
	Firstname	String
	Lastname	String
✓	Name	String
	Password (CredentialPassword)	String

▼ User Custom Attributes

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
ACL		String	String Max length	+	<input type="checkbox"/>

Save Reset

配置完成後，使用「儲存」按鈕儲存更改。

步驟 2. 配置dACL

導航到策略>策略元素>結果>授權>可下載ACL檢視並定義ISE上的dACL。使用「增加」按鈕建立新按鈕。

Policy · Policy Elements

License Warning

Dictionarys Conditions **Results**

Authentication >

Authorization ▼

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Downloadable ACLs

Selected 0 Total 7

Edit **+ Add** Duplicate Delete

Name	Description
ACL_USER1	ACL assigned to USER1
DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic
PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic
test-dacl-cwa	
test-dacl-dot1x	

這將打開「New Downloadable ACL」（新的可下載ACL）配置表。在本示例中，請配置以下欄位

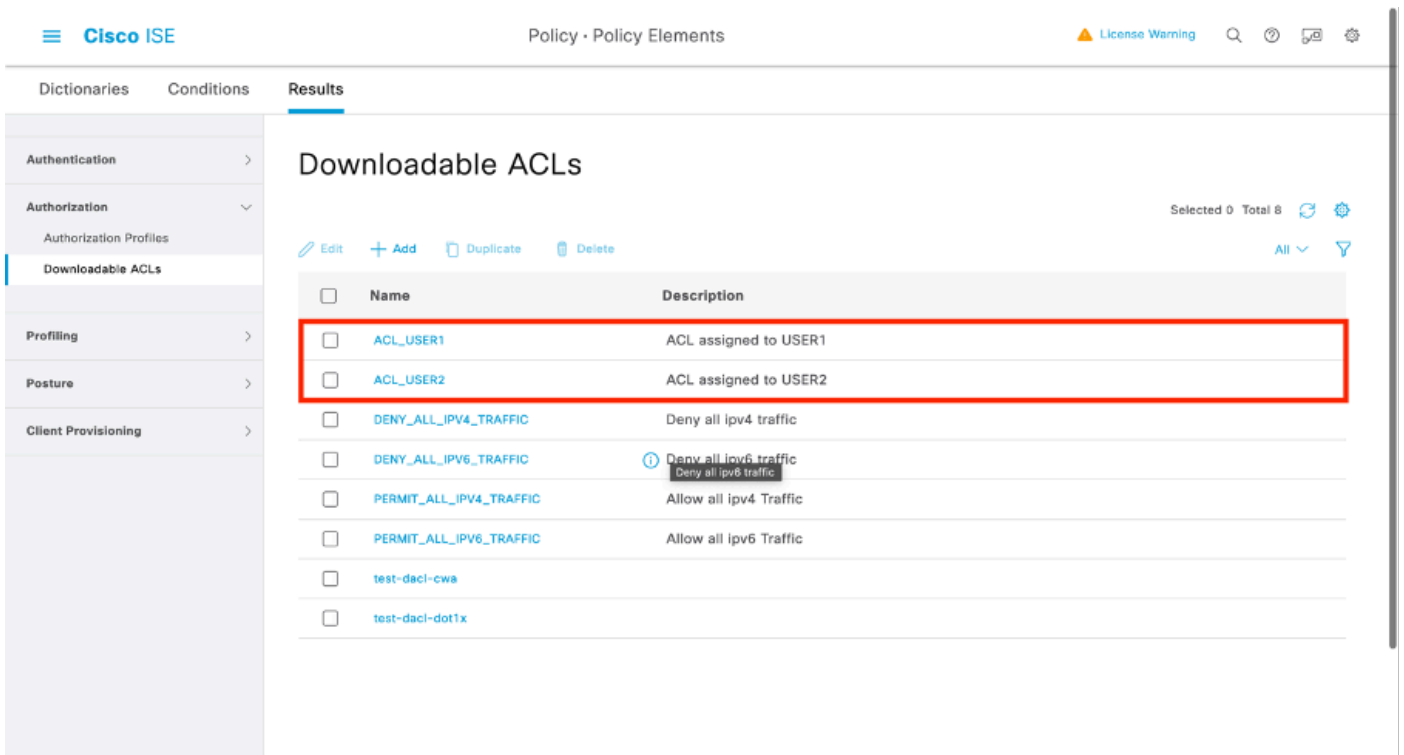
:

- 名稱：定義的dACL的名稱。
- 說明（可選）：建立之dACL的使用方法簡短說明。
- IP版本：定義的dACL中使用的IP協定版本（版本4、6或兩者）。
- DACL內容：根據Cisco IOS XE ACL語法的dACL內容。

在本文檔中，使用的dACL是「ACL_USER1」，此dACL允許除發往10.48.39.186和10.48.39.13的資料流以外的任何資料流。

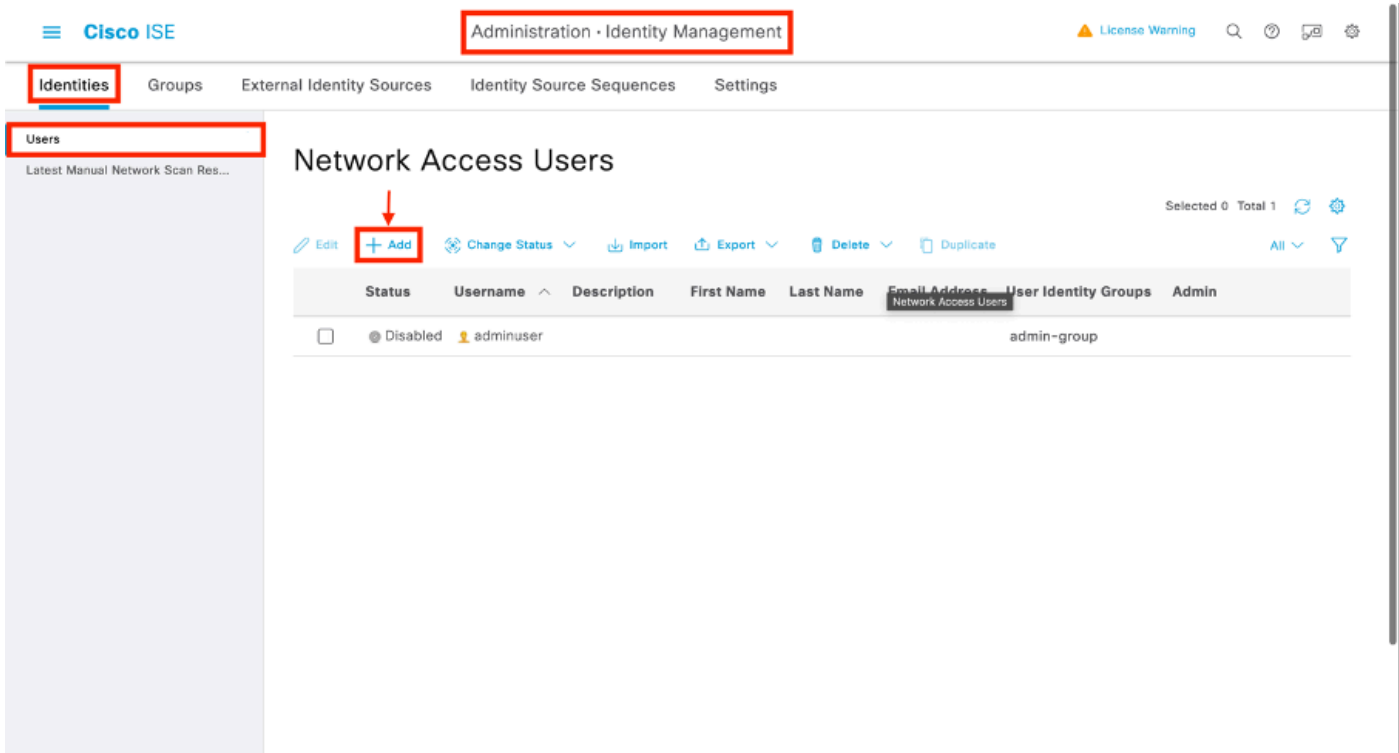
配置欄位後，使用「提交」按鈕建立dACL。

重複該步驟，為第二個使用者ACL_USER2定義dACL，如圖所示。

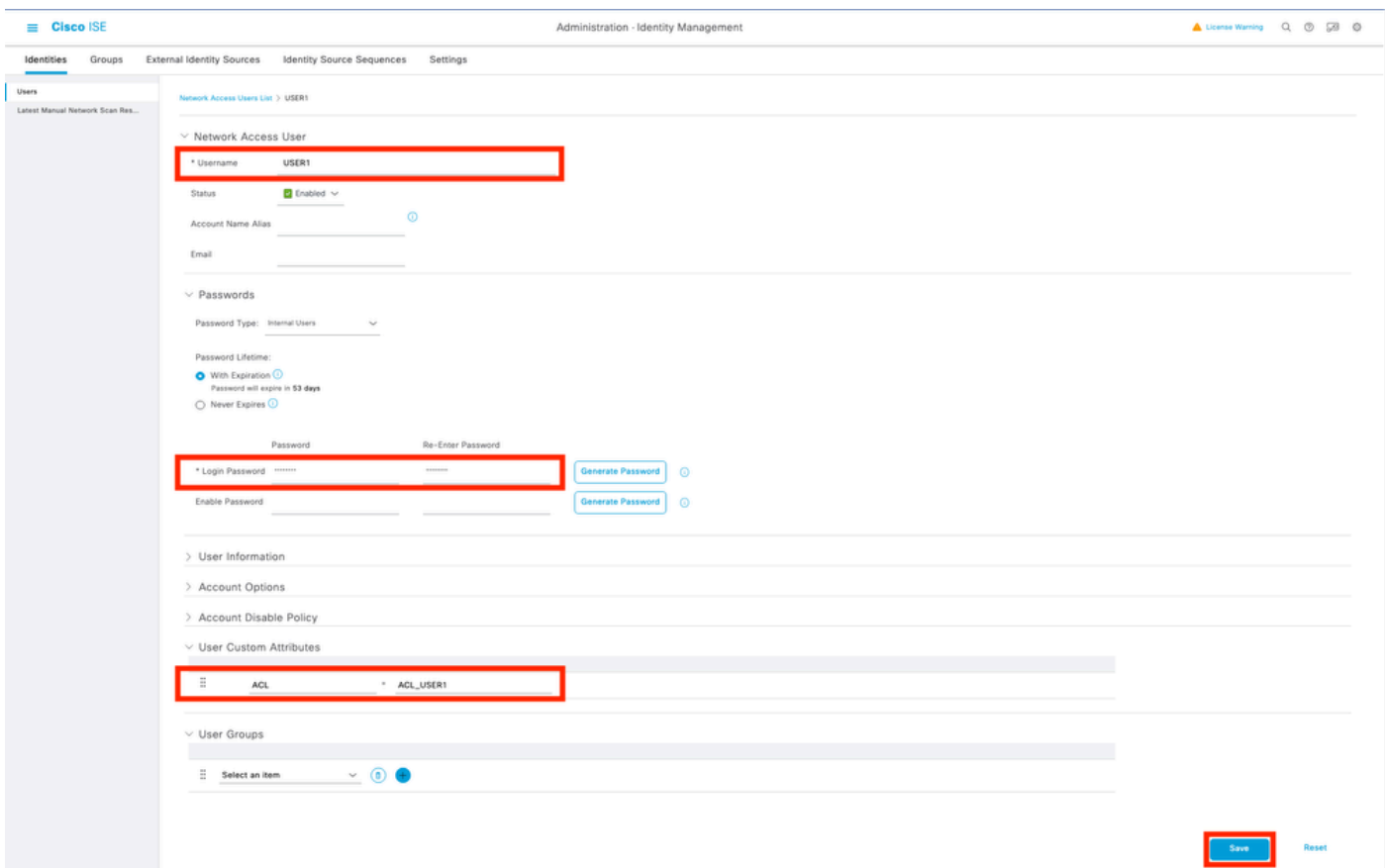


步驟 3.將dACL分配給已建立的身份

建立dACL後，可以使用第1步中建立的使用者自定義屬性將其分配到任何ISE身份。為此，請導航到管理>身份管理>身份>使用者。像往常一樣，使用「增加」按鈕建立使用者。

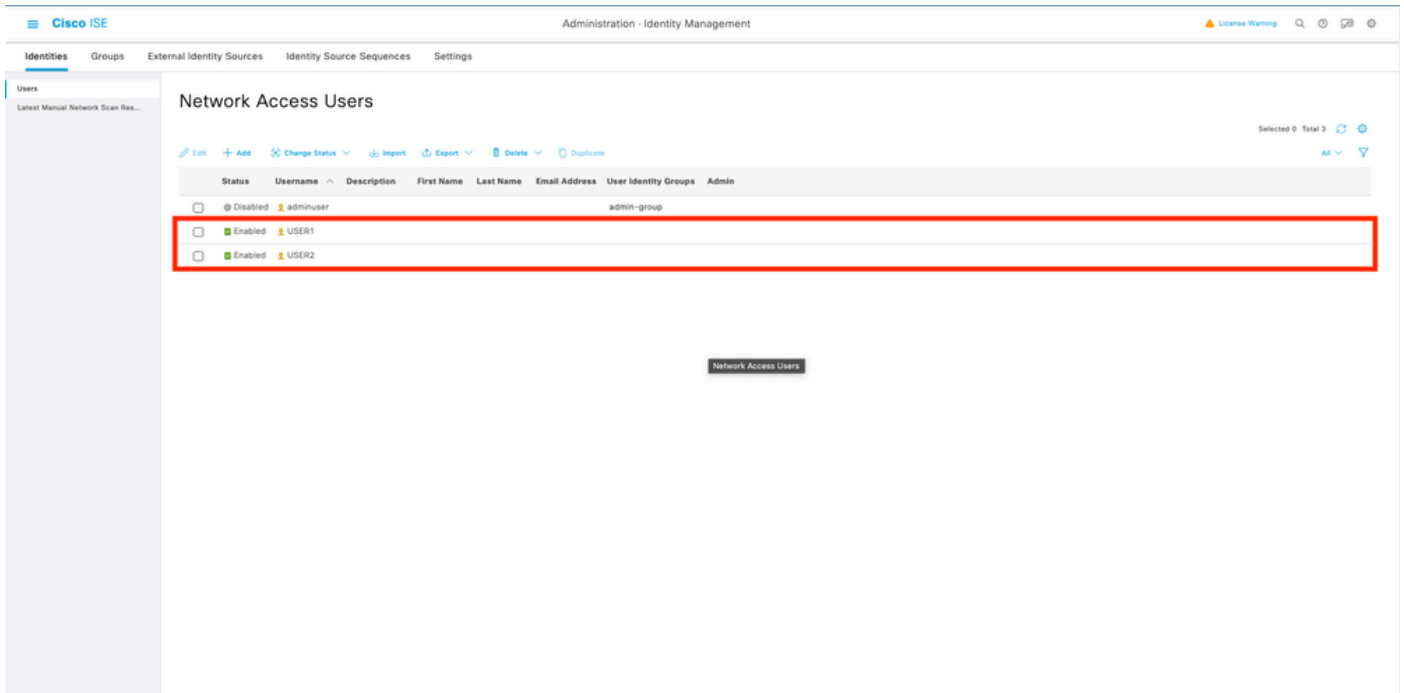


在「新網路訪問使用者」配置表單上，定義所建立使用者的使用者名稱和密碼。使用自定義屬性「ACL」將步驟2中建立的dACL分配給身份。在本示例中，定義了使用ACL_USER1的身份USER1。



欄位配置正確後，使用「提交」按鈕建立身份。

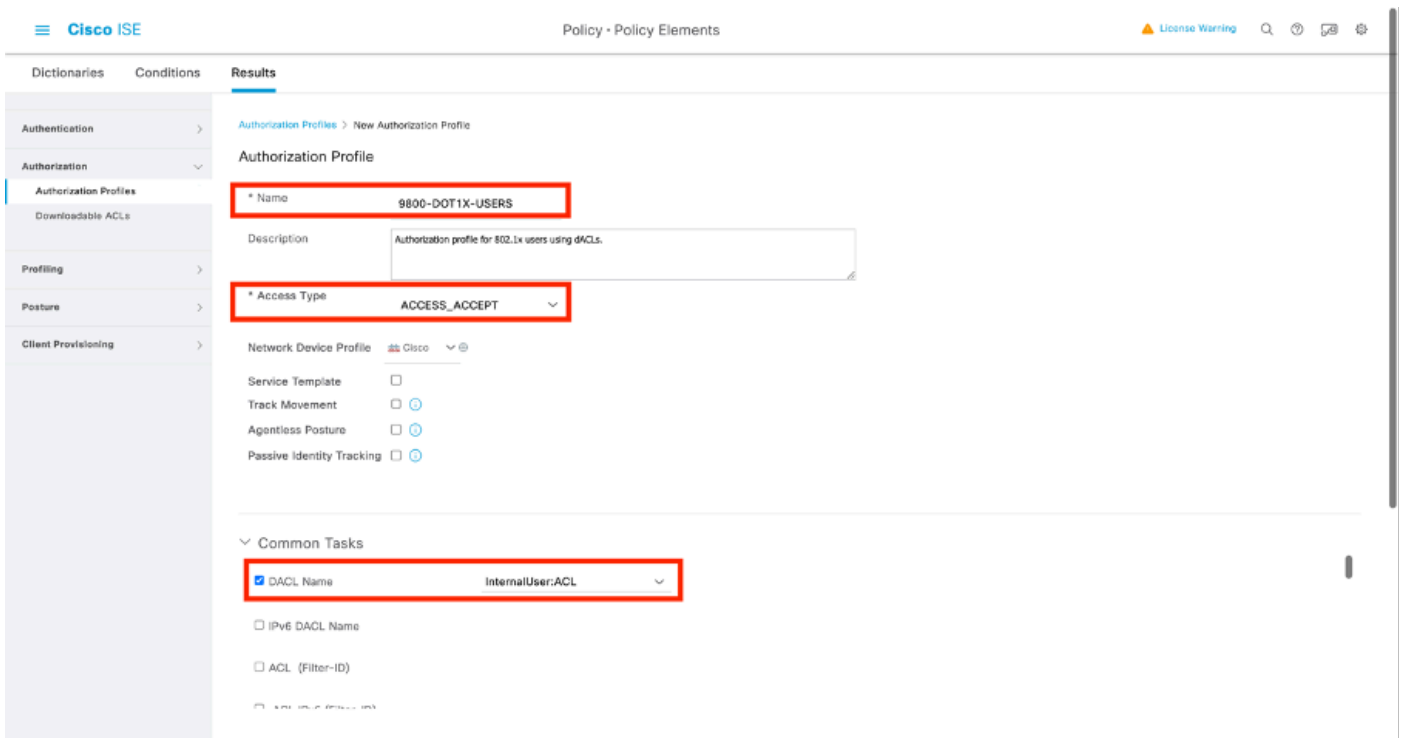
重複此步驟以建立USER2並為其分配ACL_USER2。



步驟 4. 配置授權策略結果。

配置身份並為其分配dACL後，仍必須配置授權策略，以便匹配與現有授權常見任務定義的自定義使用者屬性「ACL」。為此，請導航到策略>策略元素>結果>授權>授權配置檔案。使用「增加」按鈕定義新的授權策略。

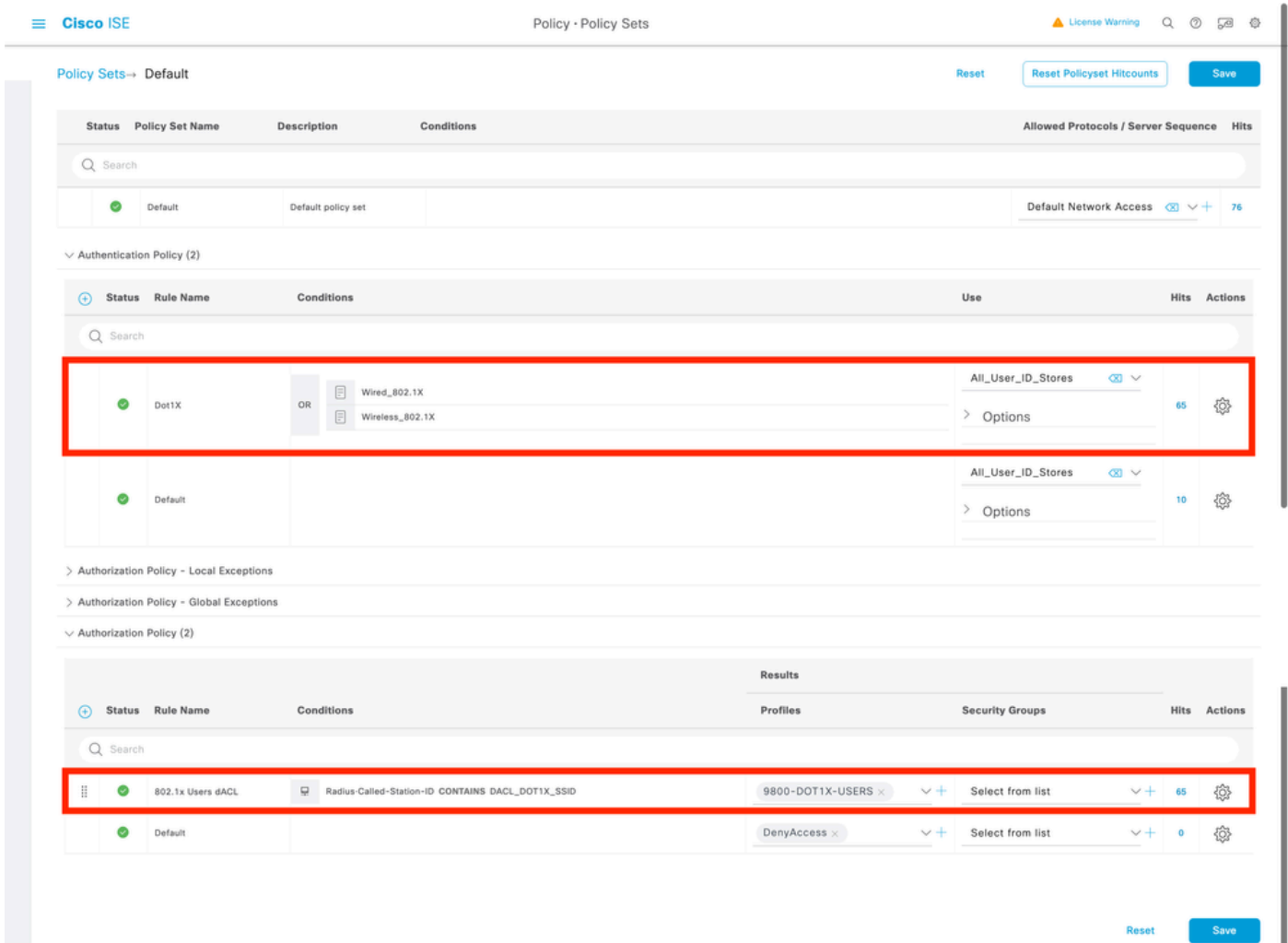
- 名稱：授權策略的名稱，此處「9800-DOT1X-USERS」。
- 存取型別：此原則相符時使用的存取型別，此處為ACCESS_ACCEPT。
- 常見任務：將「DACL名稱」與內部使用者的InternalUser：<建立的自定義屬性的名稱>進行匹配。根據本文檔中使用的名稱，配置檔案9800-DOT1X-USERS配置為InternalUser：ACL的dACL。



步驟 5.使用策略集中的授權配置檔案。

一旦授權配置檔案得到正確定義，它仍需要成為用於驗證和授權無線使用者的策略集的一部分。導航到策略>策略集，打開使用的策略集。

此處，身份驗證策略規則「Dot1X」匹配透過有線或無線802.1x建立的任何連線。授權原則規則「802.1x使用者dACL」實作所用SSID的條件（即Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID）。如果在「DACL_DOT1X_SSID」WLAN上執行授權，則會使用步驟4中定義的設定檔「9800-DOT1X-USERS」來授權使用者。



基於結果的dACL

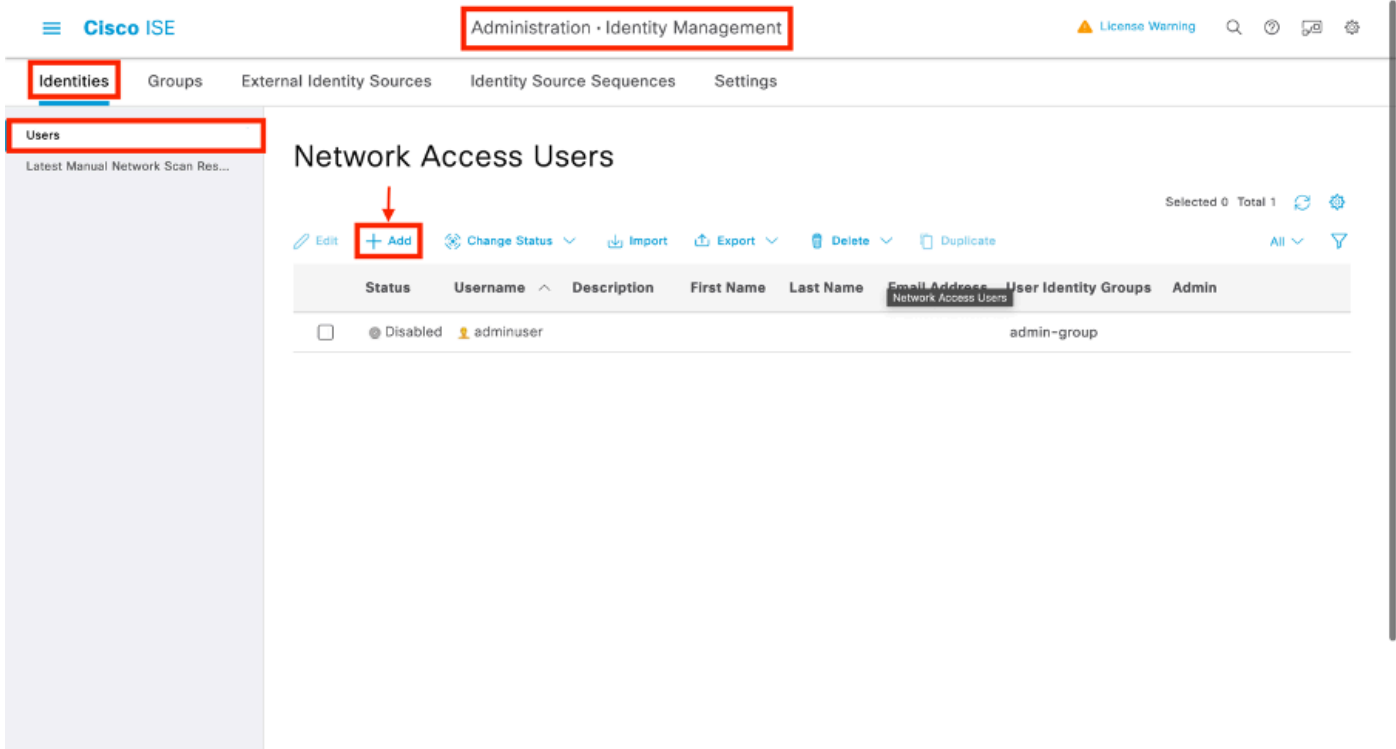
為避免將特定dACL分配給ISE上建立的每個身份這一艱鉅任務，您可以選擇將dACL應用於特定策略結果。然後，根據與所用策略集的授權規則匹配的任何條件應用此結果。

步驟 1.配置dACL

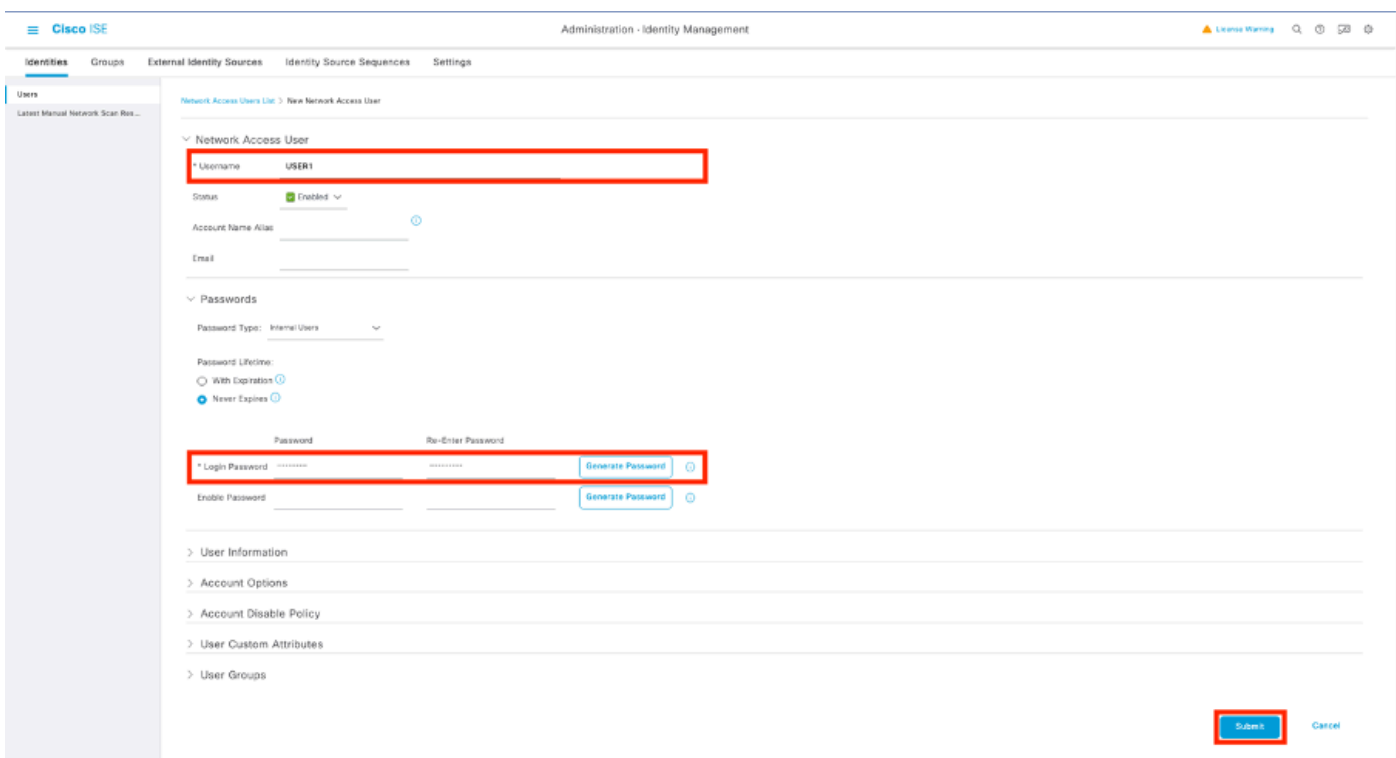
從每使用者dACL部分執行相同的步驟2以定義所需的dACL。此處是ACL_USER1和ACL_USER2。

步驟 2.建立辨識

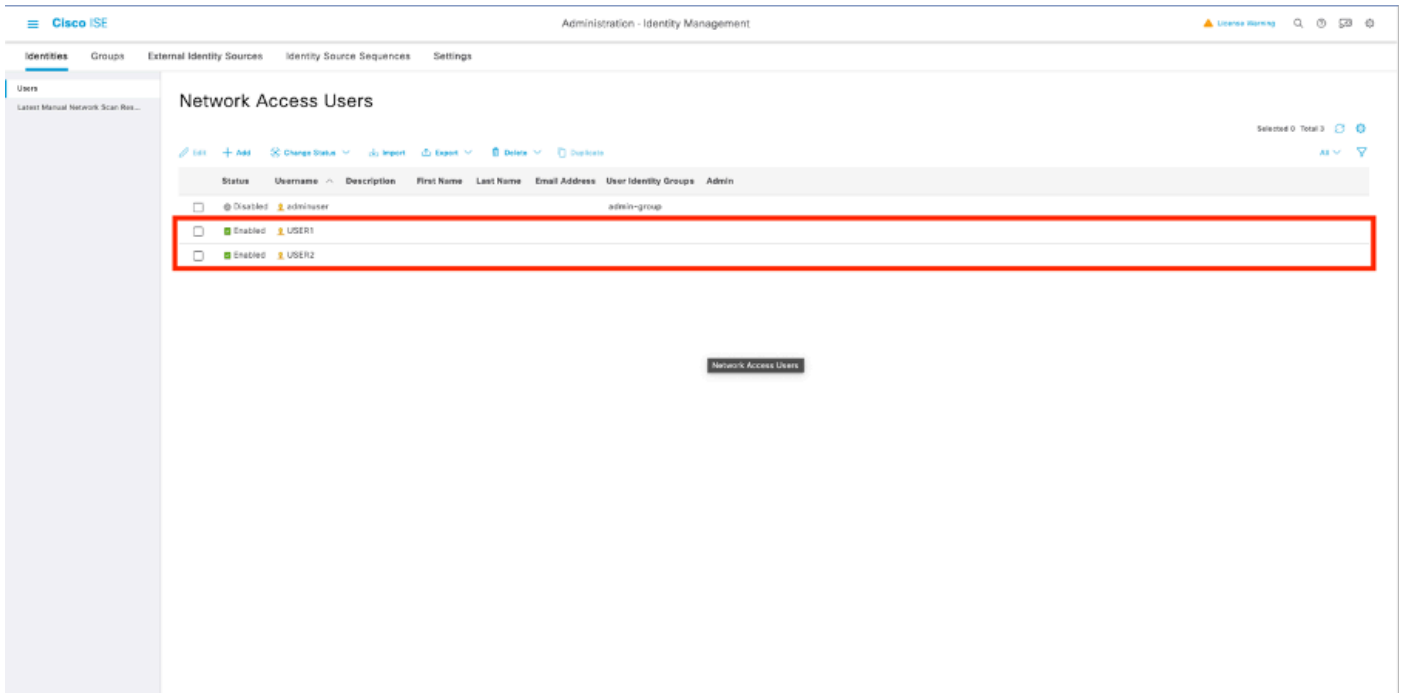
導航到管理>身份管理>身份>使用者，使用「增加」按鈕建立使用者。



在「新網路訪問使用者」配置表單上，定義所建立使用者的使用者名稱和密碼。



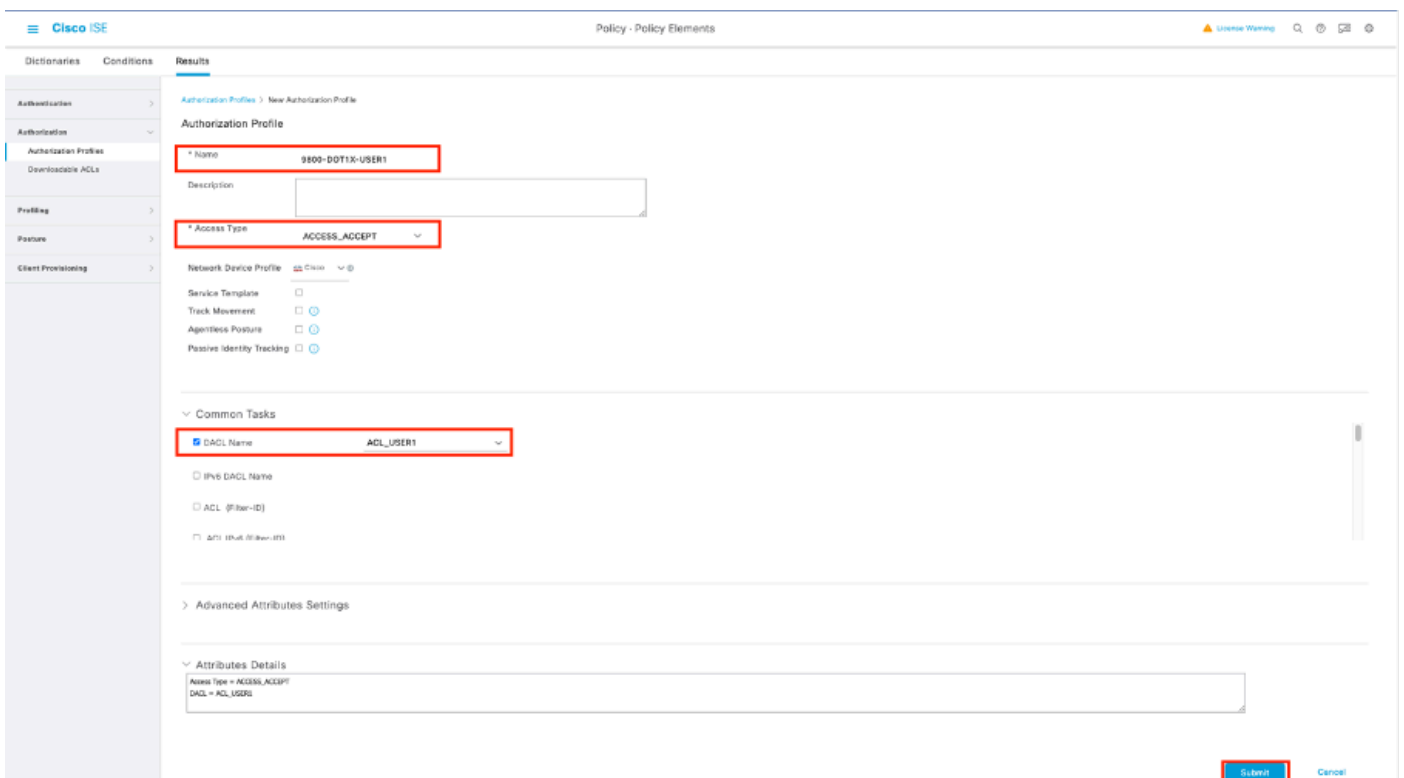
重複此步驟以建立USER2。



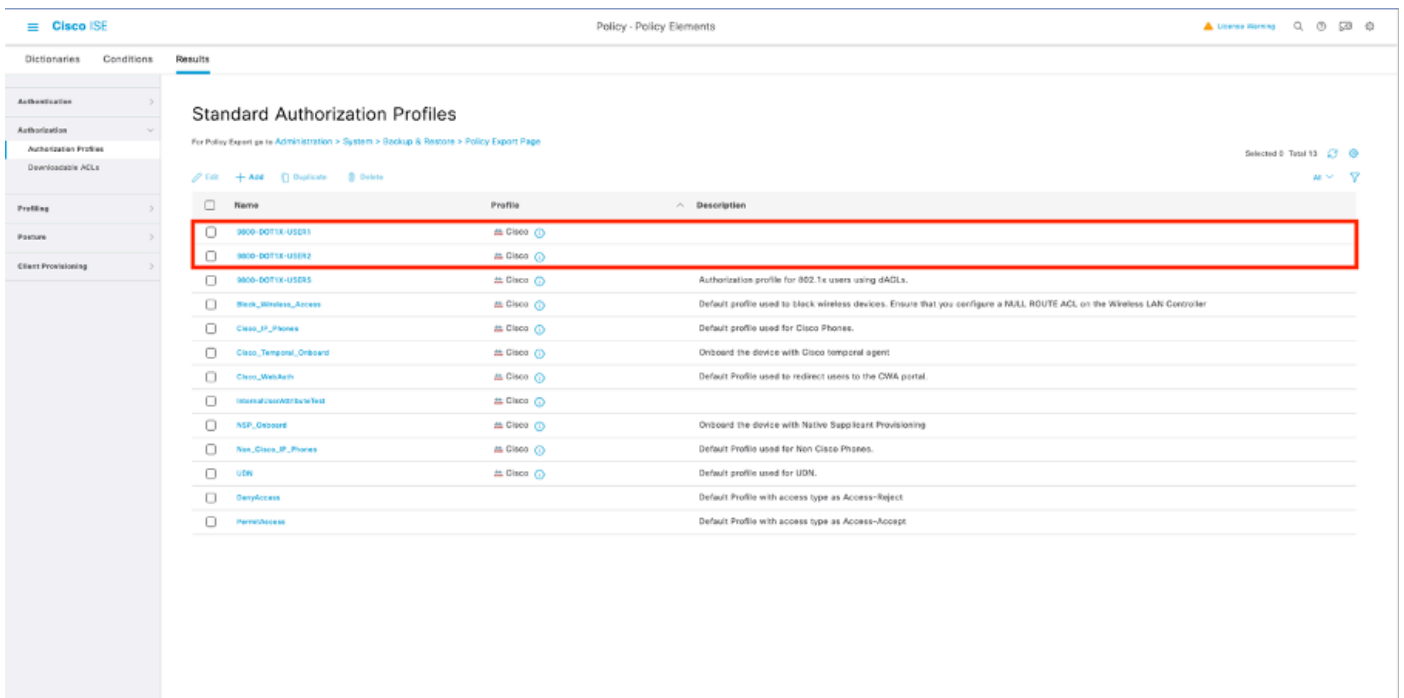
步驟 4. 配置授權策略結果。

配置身份和dACL後，仍必須配置授權策略，以便向符合使用此策略條件的使用者分配特定dACL。為此，請導航到策略>策略元素>結果>授權>授權配置檔案。使用「增加」按鈕定義新的授權策略並填寫這些欄位。

- 名稱：授權策略的名稱，此處「9800-DOT1X-USER1」。
- 訪問型別：匹配此策略時使用的訪問型別，此處為ACCESS_ACCEPT。
- 常見任務：將內部使用者的「DACL名稱」與「ACL_USER1」進行匹配。根據本文檔中使用的名稱，配置檔案9800-DOT1X-USER1配置了配置為「ACL_USER1」的dACL。



重複此步驟，建立策略結果「9800-DOT1X-USER2」，並將「ACL_USER2」分配為DAACL。



步驟 5. 使用策略集中的授權配置檔案。

一旦授權配置檔案得到正確定義，它仍需要成為用於驗證和授權無線使用者的策略集的一部分。導航到策略>策略集，打開使用的策略集。

此處，身份驗證策略規則「Dot1X」匹配透過有線或無線802.1X建立的任何連線。授權原則規則「802.1X User 1 dACL」實作使用之使用者名稱的條件（即InternalUser-Name CONTAINS USER1）。如果使用使用者名稱USER1執行授權，則第4步中定義的配置檔案「9800-DOT1X-USER1」用於授權使用者，因此，此結果中的dACL (ACL_USER1)也應用於該使用者。對使用「9800-DOT1X-USER1」的使用者名稱USER2進行配置也是如此。

The screenshot displays the Cisco ISE Policy Sets configuration interface. At the top, the 'Policy Sets - Policy Sets' header is visible. The main content area is divided into several sections:

- Policy Sets - Default:** A table showing the 'Default' policy set with a search bar and a 'Default Network Access' dropdown.
- Authentication Policy (2):** A table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. A red box highlights the 'Dot1X' rule, which has conditions for 'Wired_802.1X', 'Wired_802.1X', 'Wired_MAB', and 'Wired_SAB'. The 'Use' column for this rule is set to 'All_User_ID_Stores'.
- Authorization Policy (3):** A table with columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. A red box highlights two rules: '802.1x User 2 dACL' and '802.1x User 1 dACL', both with conditions 'InternalUser Name EQUALS USER2' and 'InternalUser Name EQUALS USER1' respectively. The 'Profiles' column for these rules is set to '800-DOT1X-USER2' and '800-DOT1X-USER1', and the 'Security Groups' column is set to 'Select from list'.

有關將dACL與CWA SSID一起使用的說明

如在[Catalyst 9800 WLC和ISE上配置中央Web身份驗證\(CWA\)](#)配置指南中所述，CWA依賴MAB和特定結果對使用者進行身份驗證和授權。可下載的ACL可以從ISE端增加到CWA配置，與上面所述的完全相同。



警告：可下載ACL只能用作網路訪問清單，不支援作為預身份驗證ACL。因此，必須在WLC配置中定義CWA工作流程中使用的所有預身份驗證ACL。

驗證

要檢驗已進行的配置，可以使用以下命令。

```
# 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 }
```

以下參考了與此範例對應的WLC組態相關部分。

```
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 aHa0SX[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
```

此時將顯示RADIUS伺服器配置，使用show running-config all命令顯示。

```
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
```

疑難排解

檢查清單

- 確保客戶端可正確連線到配置的802.1X SSID。
- 確保RADIUS access-request/accept包含正確的屬性值對(AVP)。
- 確保客戶端使用正確的WLAN/策略配置檔案。

WLC One Stop-Shop反射

要檢查dACL是否已正確分配給特定無線客戶端，可以使用**show wireless client mac-address <H.H.H> detail**命令，如下所示。從此處可以看到各種有用的故障排除資訊，即：客戶端使用者名稱、狀態、策略配置檔案、WLAN，最重要的是ACS-ACL。

<#root>

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

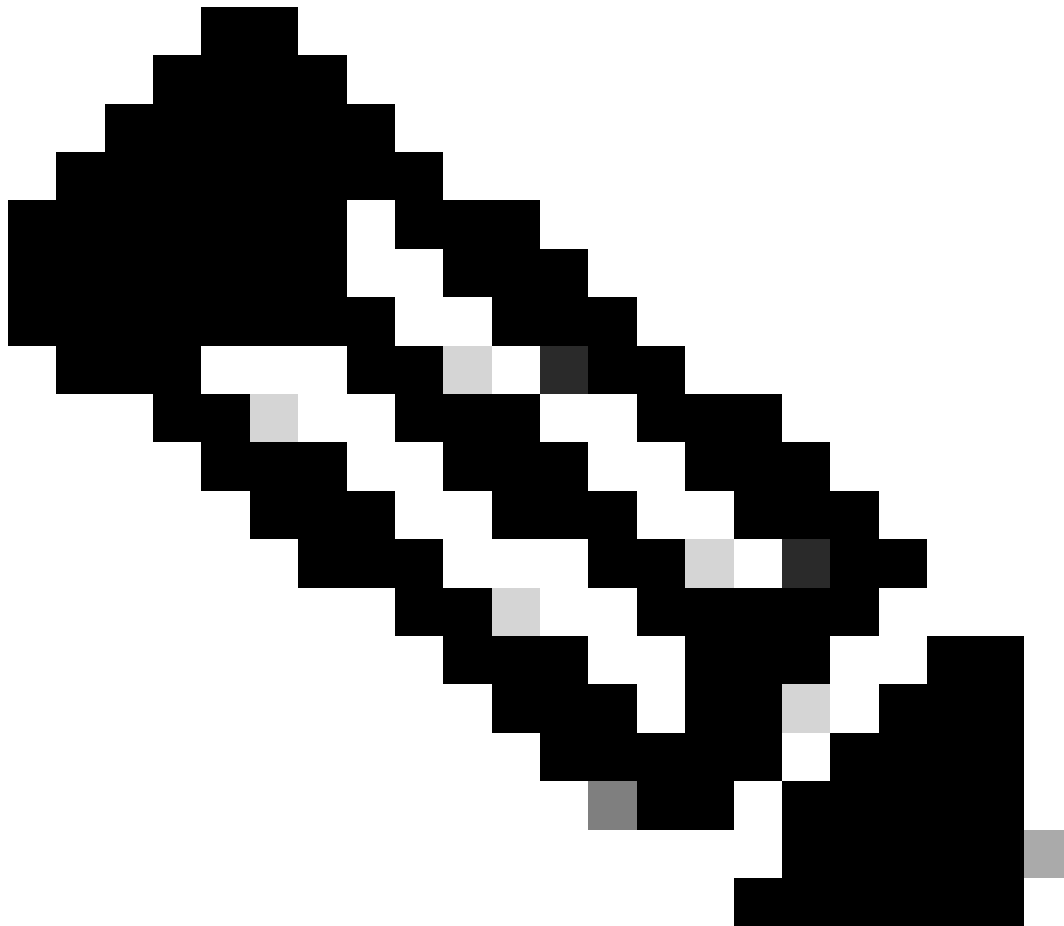
Resultant Policies:

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

[...]

WLC Show命令

要檢視當前作為Catalyst 9800 WLC配置一部分的所有ACL，您可以使用show access-lists命令。此命令列出本地定義的所有ACL或WLC下載的dACL。WLC從ISE下載的任何dACL的格式為 xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.



注意：只要客戶端建立關聯並在無線基礎架構中使用可下載ACL，可下載ACL就會保留在配置中。一旦最後一個使用

dACL的客戶端離開基礎設施，就會從配置中刪除dACL。

```
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
[...]
```

條件式偵錯和無線電主動式追蹤

在排除配置故障時，您可以為假定使用dACL分配的客戶端收集[放射性蹤跡](#)。這裡突出顯示了在客戶端08be.ac14.137d的客戶端關聯過程中放射性痕跡的相關部分的日誌。

<#root>

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

```
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 Clie

[...]

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

2024/03/28 10:43:04.353413199 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.137d]
2024/03/28 10:43:04.353414496 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.137d]

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 Client

[...]

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 "USERI

2024/03/28 10:43:04.381430559 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Service-Type [6] 6 Fr
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 "

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 "

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 1

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 "

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 "

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_90000012

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_90000012

[...]

2024/03/28 10:43:04.727138915 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

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\$®vf9fjØ◊«? %ÿ0?ã@≤™ÇÑbWi6\È&\q·1U+QB-º®”≠fJÑv?”

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_9000

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_90000012]

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_90000012]

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 ASYNCHRONOUS
[...]

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

2024/03/28 10:43:04.729428175 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 20 06 30

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

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

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 "

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\$®vf9jØ◊«? %ÿ0?ã@≤™ÇÑbWi6\Ë&\q·1U+QB-º®”#fJÑv?”
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_9000

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 Client

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_90000012

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

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

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

[...]

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

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

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 Client

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

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 Client

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 I

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

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, c
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 IF

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 :bsr

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

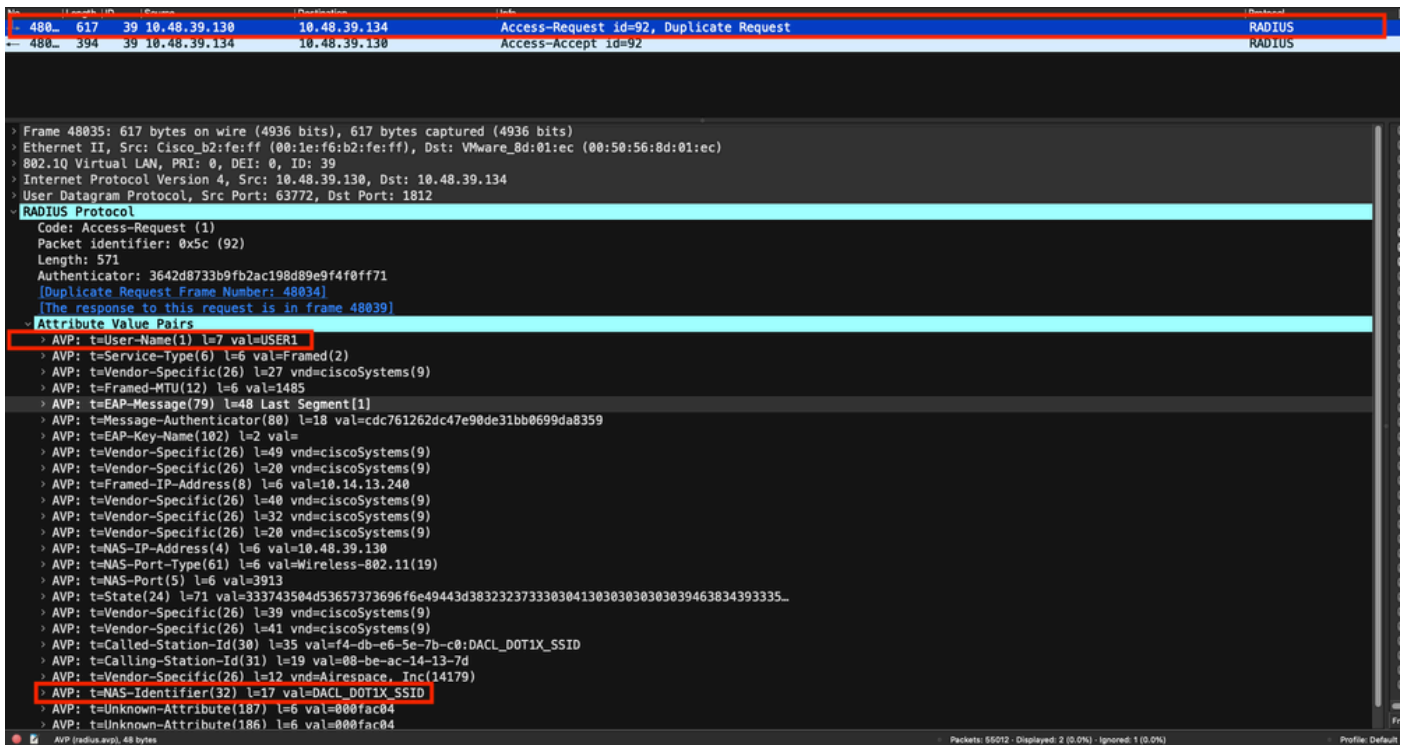
2024/03/28 10:43:04.789886011 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

資料包捕獲

另一個有趣的反射是獲取和分析客戶端關聯的RADIUS流的資料包捕獲。可下載ACL依賴於RADIUS，不僅要分配給無線客戶端，還
要由WLC下載。因此，在進行資料包捕獲以排除dACL配置故障時，必須在控制器用來與RADIUS伺服器通訊的介面上進行捕獲。[本
文檔](#)說明了如何在Catalyst 9800上配置易於嵌入的資料包捕獲，該資料包捕獲已用於收集本文所分析的捕獲。

RADIUS客戶端身份驗證

您可以看到從WLC傳送到RADIUS伺服器的使用者端RADIUS存取要求，以便驗證DACL_DOT1X_SSID SSID (AVP NAS-Identifier)上
的使用者USER1 (AVP使用者名稱)。



No.	Length	ID	Source	Destination	Info	Protocol
8037	184	39	10.48.39.130	10.48.39.134	Access-Request id=81, Duplicate Request	RADIUS
8038	369	39	10.48.39.134	10.48.39.130	Access-Accept id=81	RADIUS

> Frame 8038: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)
 > Ethernet II, Src: VMware_Bd:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)
 > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
 > Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130
 > User Datagram Protocol, Src Port: 1812, Dst Port: 63772
 > RADIUS Protocol
 Code: Access-Accept (2)
 Packet identifier: 0x51 (81)
 Length: 323
 Authenticator: 61342164ce39be06eed028b3ce566ef5
 [This is a response to a request in frame 8036]
 [Time from request: 0.007995000 seconds]
 Attribute Value Pairs
 > AVP: t=User-Name(1) l=32 val=#ACSAcl@-IP-ACL_USER1-65e89aab
 > AVP: t=Class(25) l=75 val=434143533a30613330323738366d6242517239445259673447765f436554692f48737050_
 > AVP: t=Message-Authenticator(80) l=18 val=a3c4b20cd1e64785d9e0232511cd8b72
 > AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)
 Type: 26
 Length: 47
 Vendor ID: ciscoSystems (9)
 > VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#1=deny ip any host 10.48.39.13
 > AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)
 Type: 26
 Length: 47
 Vendor ID: ciscoSystems (9)
 > VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#2=deny ip any host 10.48.39.15
 > AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)
 Type: 26
 Length: 48
 Vendor ID: ciscoSystems (9)
 > VSA: t=Cisco-AVPair(1) l=42 val=ip:inacl#3=deny ip any host 10.48.39.186
 > AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
 Type: 26
 Length: 36
 Vendor ID: ciscoSystems (9)
 > VSA: t=Cisco-AVPair(1) l=30 val=ip:inacl#4=permit ip any any

RADIUS Protocol (radius), 323 bytes Packets: 43372 - Displayed: 2 (0.0%) Profile: Default



注意：如果將下載ACL下載到WLC上後修改其內容，則在使用該ACL的使用者重新進行身份驗證（並且WLC再次對此類使用者執行RADIUS身份驗證）之前，不會反映該ACL的更改。實際上，ACL名稱的雜湊部分發生變化就反映了ACL的變化。因此，下次將此ACL指派給使用者時，其名稱必須不同，因此，ACL不能是WLC組態的一部分，而且應該下載。但是，在ACL更改之前進行身份驗證的客戶端會繼續使用前一個，直到完全重新進行身份驗證。

ISE操作日誌

RADIUS客戶端身份驗證

操作日誌顯示應用了可下載ACL「ACL_USER1」的使用者「USER1」的成功身份驗證。故障排除中值得注意的部分用紅色框住。

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

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-if-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-52540b48521#user1, UniqueSubjectID=94b3604f5b49b8ccfefe2f3a86c80d1979b5c43

Result	
Class	CACS:8227300A0000000D848ABE3F:ise/499610885/35
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:97: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=#ACACL#-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

```

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
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
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 - InternalUserName
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

```

DACL下載

操作日誌顯示ACL「ACL_USER1」已成功下載。故障排除中值得注意的部分用紅色框住。

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	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcs eM
CiscoAVPair	aaa.service=ip_admission, aaa.event=acl-download

Result

Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfd Fbcs eM:ise/499610885/48
cisco-av-pair	ip:inacI#1=deny ip any host 10.48.39.13
cisco-av-pair	ip:inacI#2=deny ip any host 10.48.39.15
cisco-av-pair	ip:inacI#3=deny ip any host 10.48.39.186
cisco-av-pair	ip:inacI#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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。