在Catalyst 9800上配置可下载ACL并对其进行故障排除

目录

简介

背景信息

先决条件

- 要求
- 使用的组件

配置

将dACL与802.1x SSID一起使用

- 网络图
- WLC 配置
- ISE 配置
  - 每结果dACL

将dACL与CWA SSID配合使用的说明

验证

故障排除

- 核对清单
- WLC一站式反射
- WLC Show命令
- 条件调试和无线电主动跟踪
- 数据包捕获
  - RADIUS客户端身份验证
  - DACL下载
- ISE操作日志
  - RADIUS客户端身份验证
  - DACL下载

简介

本文档介绍如何在Catalyst 9800无线LAN控制器(WLC)上配置可下载ACL(dACL)并对其进行故障排除。

背景信息

dACL是指在发生身份验证时从RADIUS服务器动态下载ACL条目的网络设备，而不是具有ACL的本地副本并分配ACL名称。更完整的Cisco ISE配置示例可用。本文档重点介绍自17.10版本以来支持用于中央交换的dACL的Cisco Catalyst 9800。

先决条件

本文档旨在通过基本SSID配置示例演示Catalyst 9800上的dACL使用情况，展示如何完全自定义这些dACL。

在Catalyst 9800无线控制器上，可下载ACL包括：

- 从Cisco IOS XE Dublin 17.10.1版本开始支持。
- 仅支持具有本地模式接入点的集中式控制器（或Flexconnect集中式交换）。
    - FlexConnect本地交换不支持dACL。

要求

Cisco 建议您了解以下主题：

- Catalyst 无线 9800 配置模型。
- 思科IP访问控制列表(ACL)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

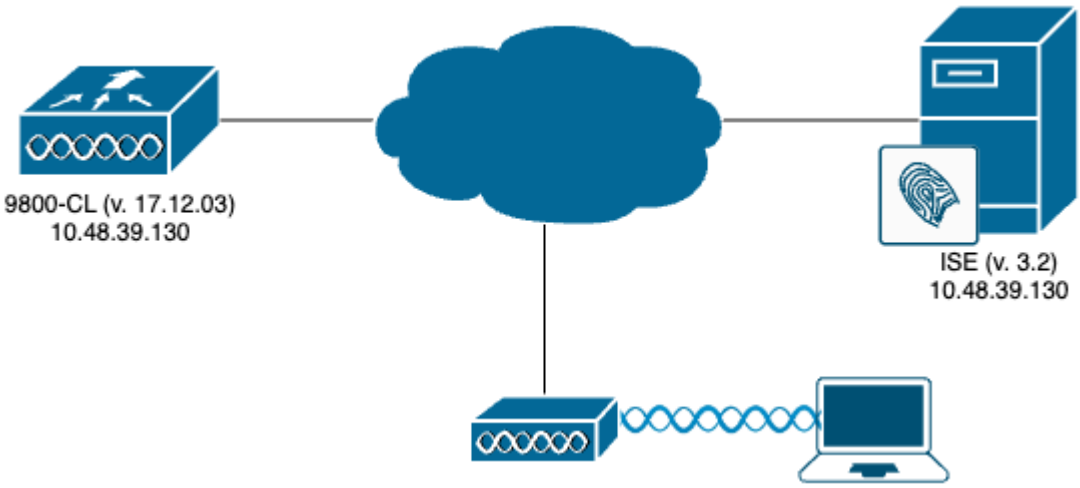
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

在本配置指南中，即使方法不同（例如，WLAN身份验证、策略配置等），最终结果也是相同的。在下一个场景中，两个用户身份定义为USER1和USER2。两者均被授予无线网络的访问权限。每个ACL_USER1和ACL_USER2都分配为dACL，由Catalyst 9800从ISE下载。

将dACL与802.1x SSID一起使用

网络图



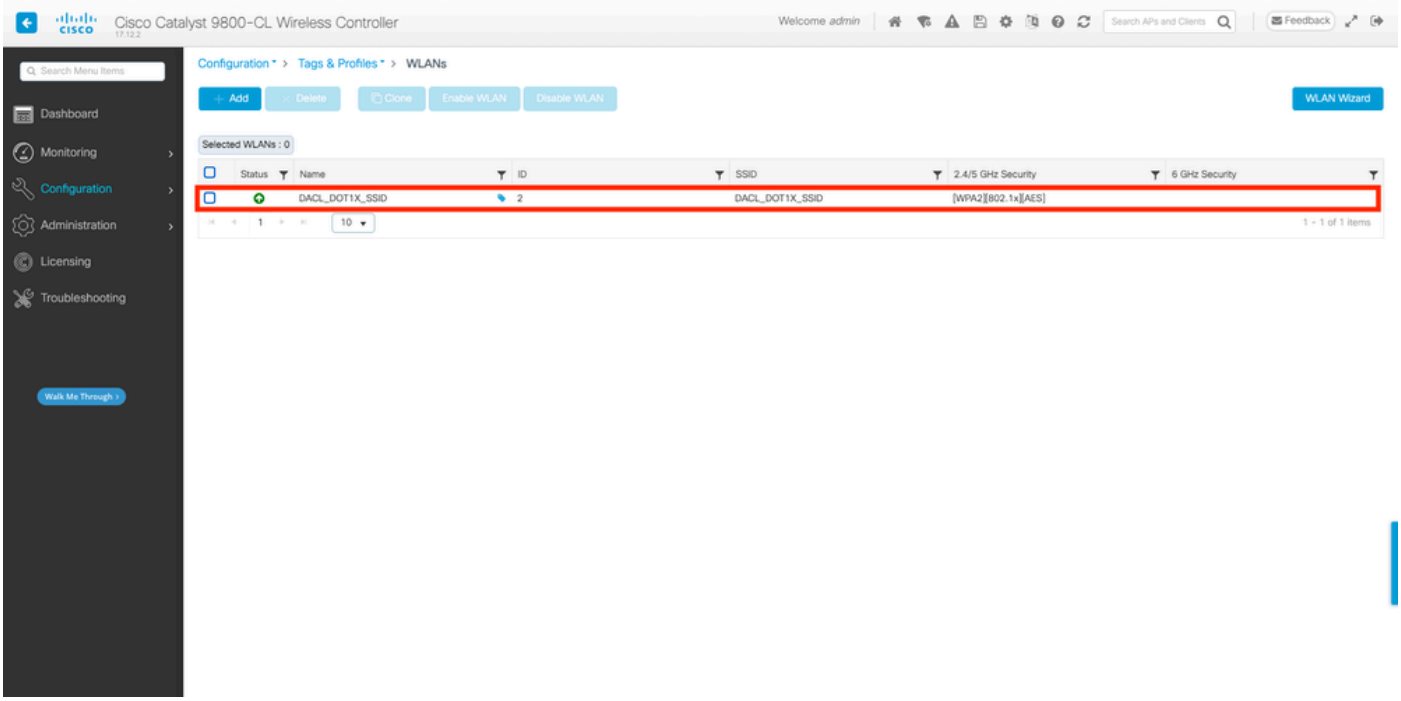
WLC 配置

有关Catalyst 9800上的802.1x SSID配置和故障排除的详细信息，请参阅在Catalyst 9800无线控制器系列上配置802.1X身份验证指南。

1.配置SSID。使用ISE作为RADIUS服务器配置802.1x身份验证SSID。在本文档中，SSID的名称为DACL_DOT1X_SSID。

从 GUI：

2.导航到配置>标签和配置文件> WLAN并创建WLAN:



从 CLI：

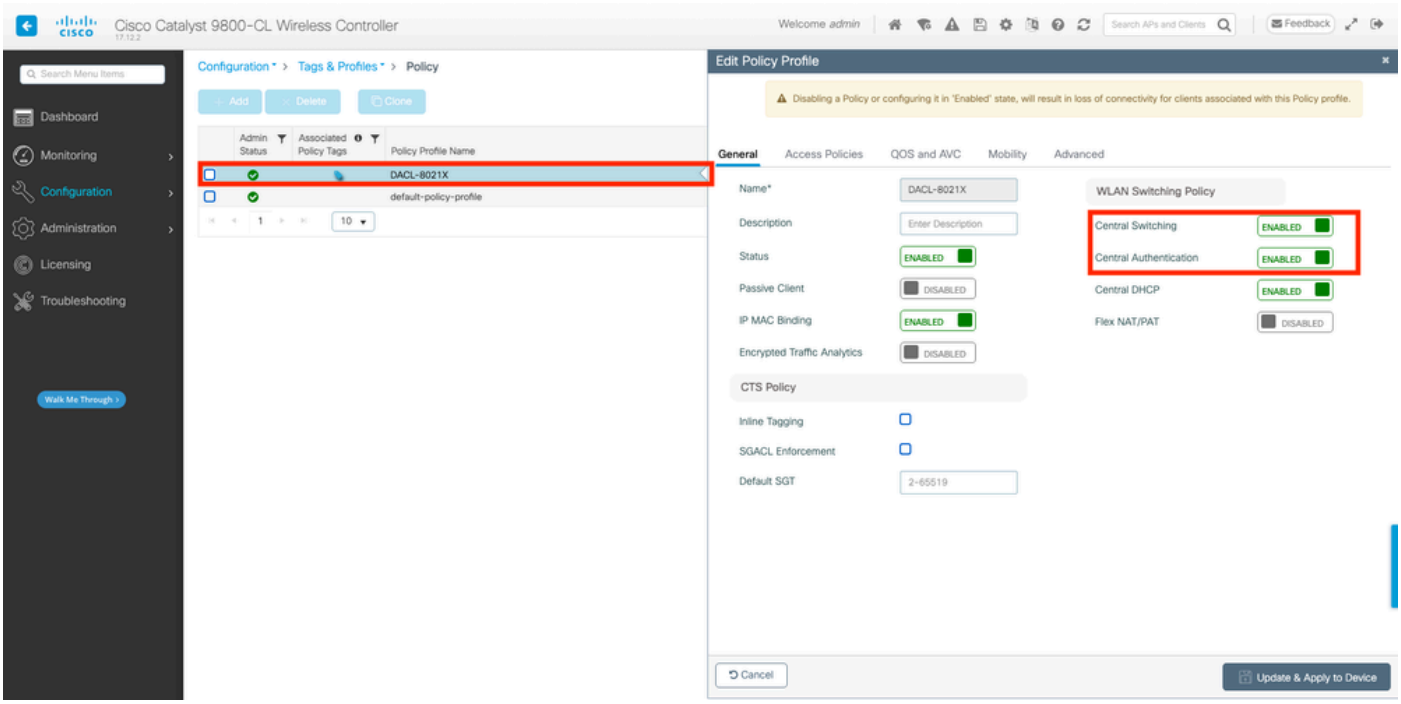
```
WLC#configure terminal
WLC(config)#wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
WLC(config-wlan)#security dot1x authentication-list DOT1X
WLC(config-wlan)#no shutdown
```

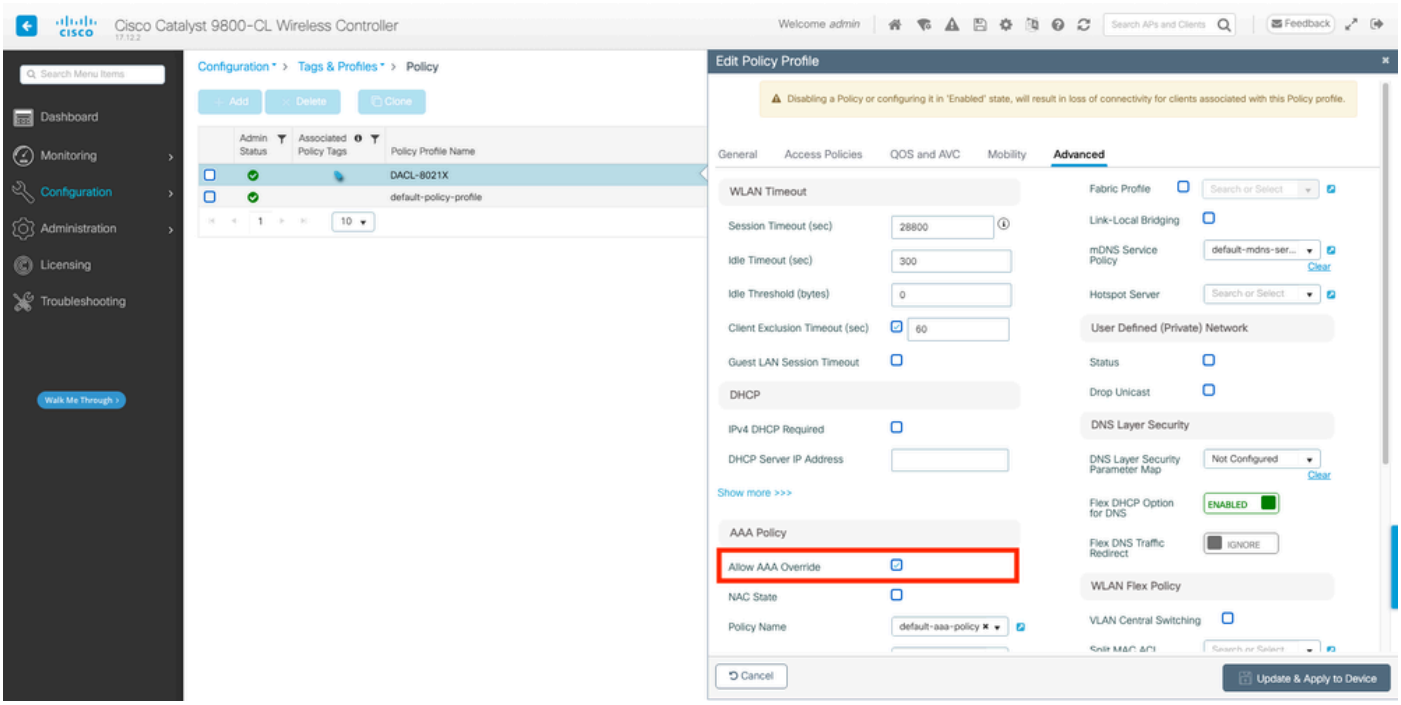
3.配置策略配置文件。配置与之前定义的SSID一起使用的策略配置文件。在此策略配置文件上，确保从高级选项卡配置AAA覆盖，如屏幕截图所示。在本文档中，使用的策略配置文件是DACL-8021X。

3a。如必备条件部分所述，dACL仅支持集中交换/身份验证部署。确保策略配置文件以这种方式配置。

从 GUI：

1.导航至配置>标签和配置文件>策略，选择使用的策略配置文件并按下一屏幕截图所示进行配置：





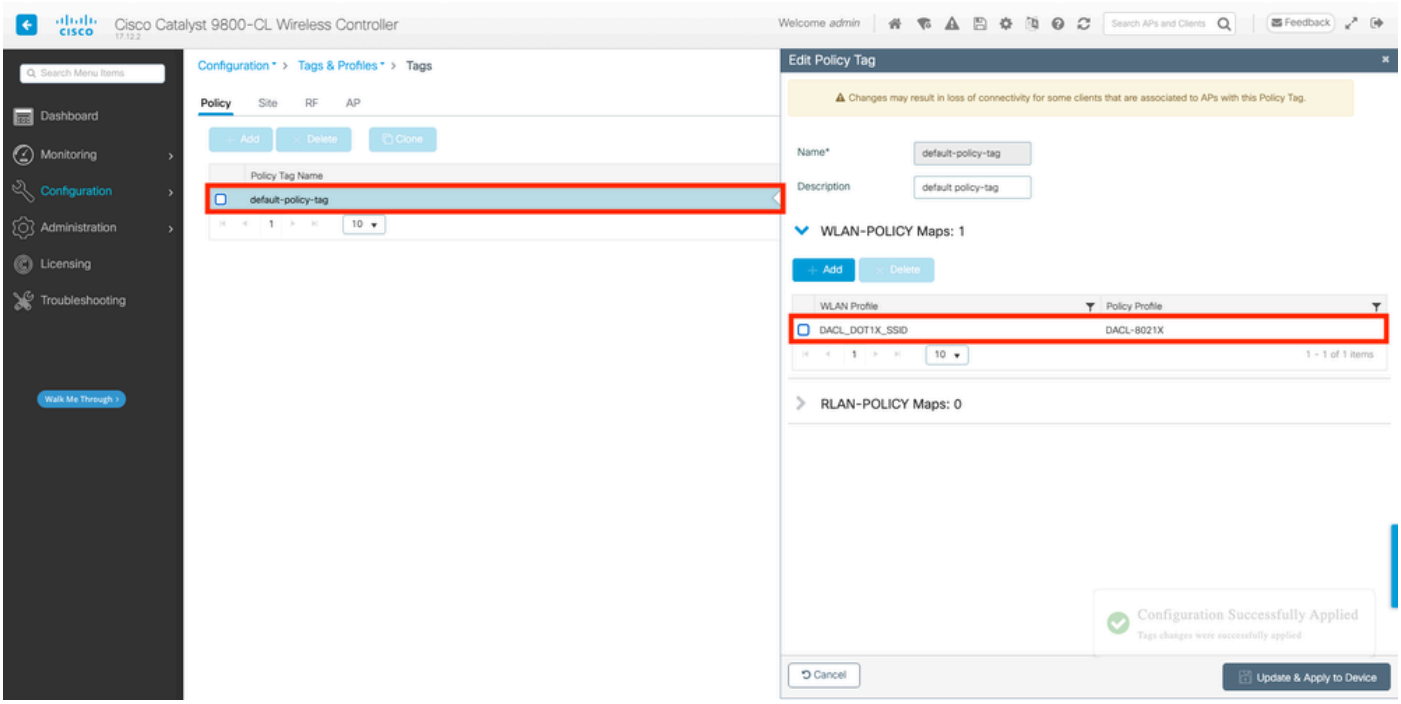
从 CLI：

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

2.将策略配置文件和SSID分配给使用的策略标记。

从 GUI：

3.定位至配置>标签和配置文件>标签。在Policy tags选项卡中，创建（或选择）使用的标记，并分配在步骤1-2期间定义的WLAN和策略配置文件。



从 CLI：

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

4.允许供应商特定属性。可下载ACL通过ISE和WLC之间的RADIUS交换中的供应商特定属性(VSA)传递。通过运行这些CLI命令，可以在WLC上启用对这些属性的支持。

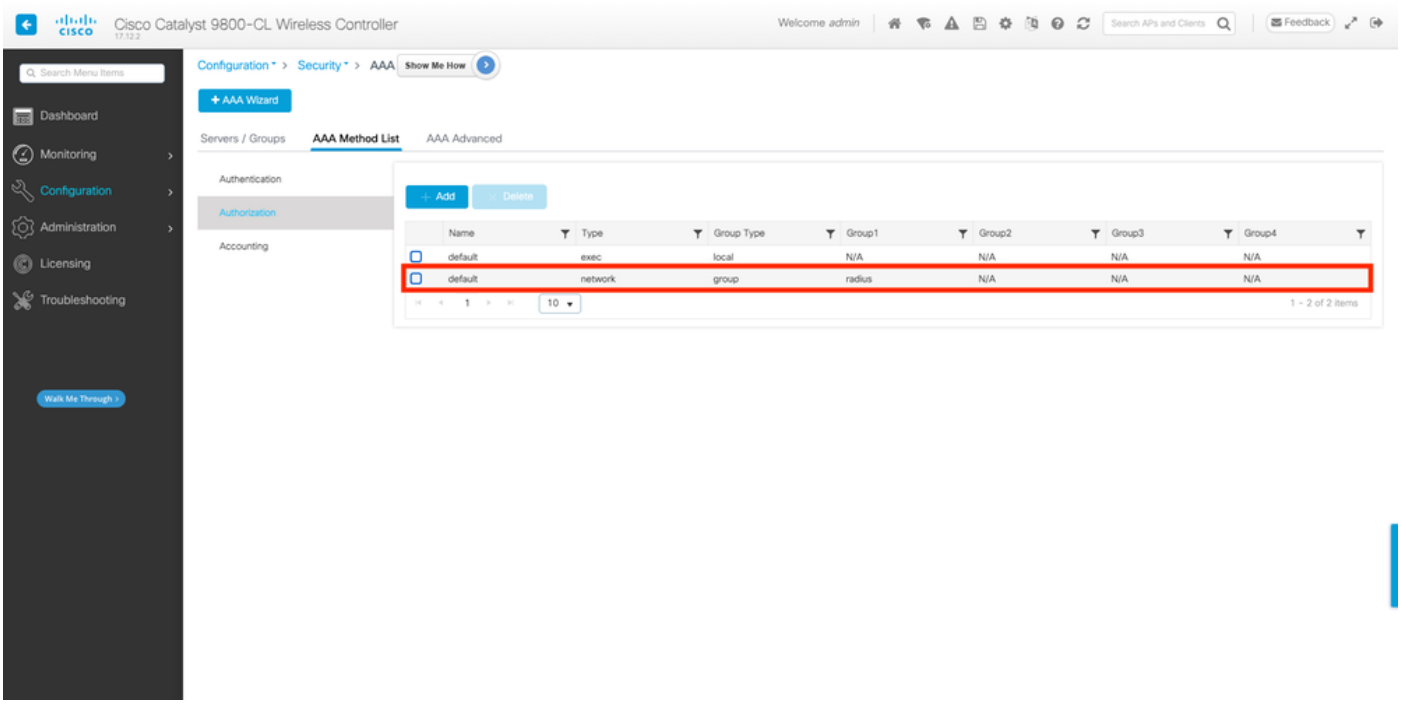
从 CLI：

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

5.配置默认授权列表。当使用dACL时，必须通过RADIUS实施网络授权，WLC才能授权对配置的802.1x SSID进行身份验证的任何用户。授权阶段在RADIUS服务器端处理。因此，需要授权列表。dACL需要使用aaa授权网络方法。您可以使用命令aaa authorization network default group radius使用默认组radius:

从 GUI：

1.定位至配置>安全> AAA，然后从“AAA方法列表”>“授权”标签创建与下一个屏幕截图类似的授权方法：



从 CLI：

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

如果不想定义缺省方法，则必须定义命名方法。在这种情况下，必须调用ISE必须使用的AAA授权方法列表，否则WLC无法下载ACL:

在WLC上：

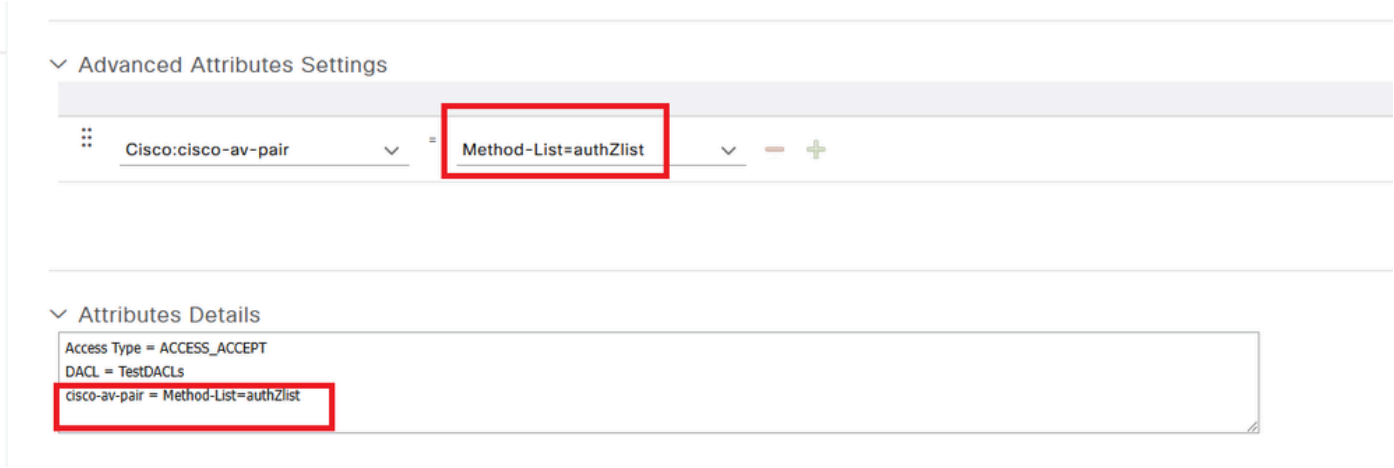
<#root>

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

authZlist

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

在ISE上，将此属性与dACL一起发送：cisco-av-pair = Method-List=authZlist



ISE 配置

在使用ISE的无线环境中实施dACL时，可能会进行两种常见配置：

1.每用户dACL配置:这样，由于自定义身份字段，每个特定身份都分配了一个dACL。

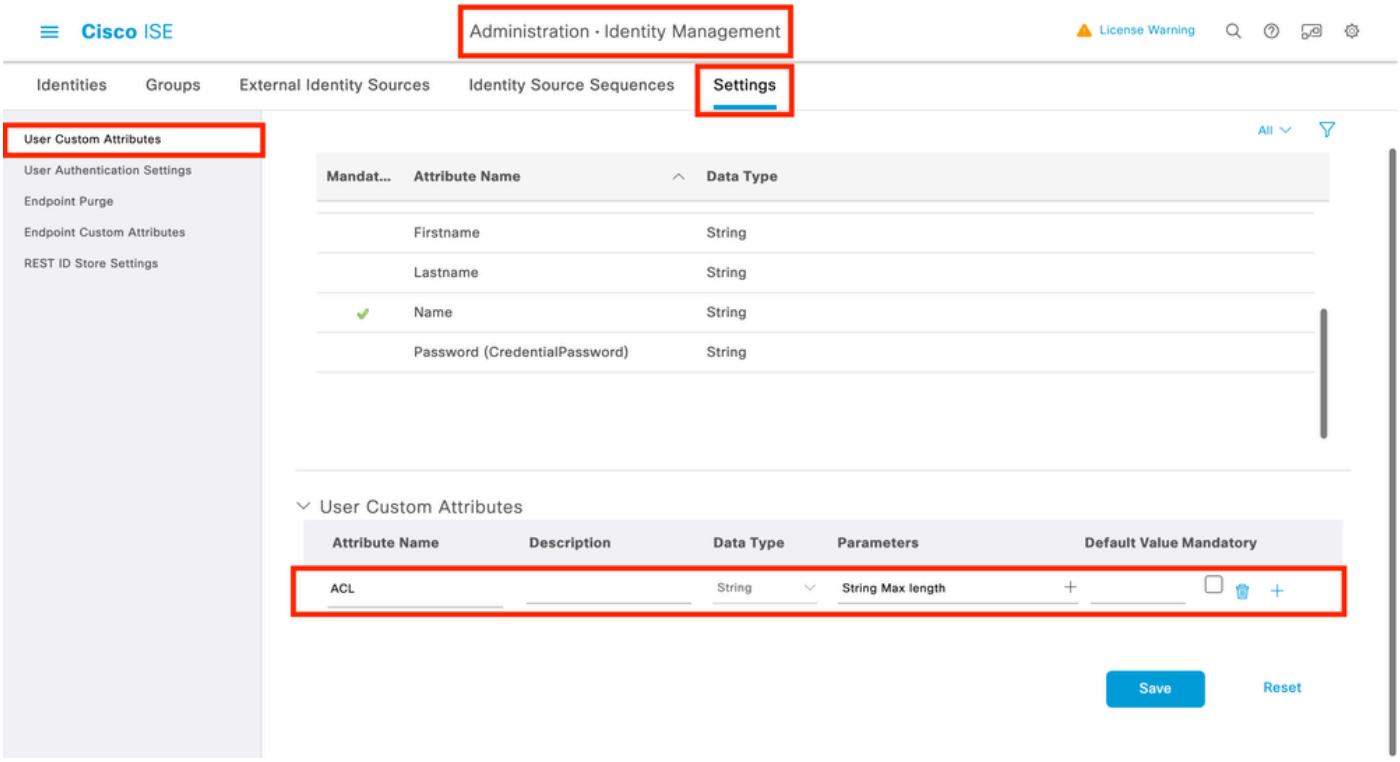
2.每结果dACL配置:当选择此方法时，会根据用户与使用的策略集匹配的授权策略为其分配特定dACL。

每用户dACL

1.定义dACL自定义用户属性。要将dACL分配给用户身份，此字段必须在创建的身份上配置。默认情况下，在ISE上，未为创建的任何新身份定义ACL字段。要解决此问题，您可以使用自定义用户属

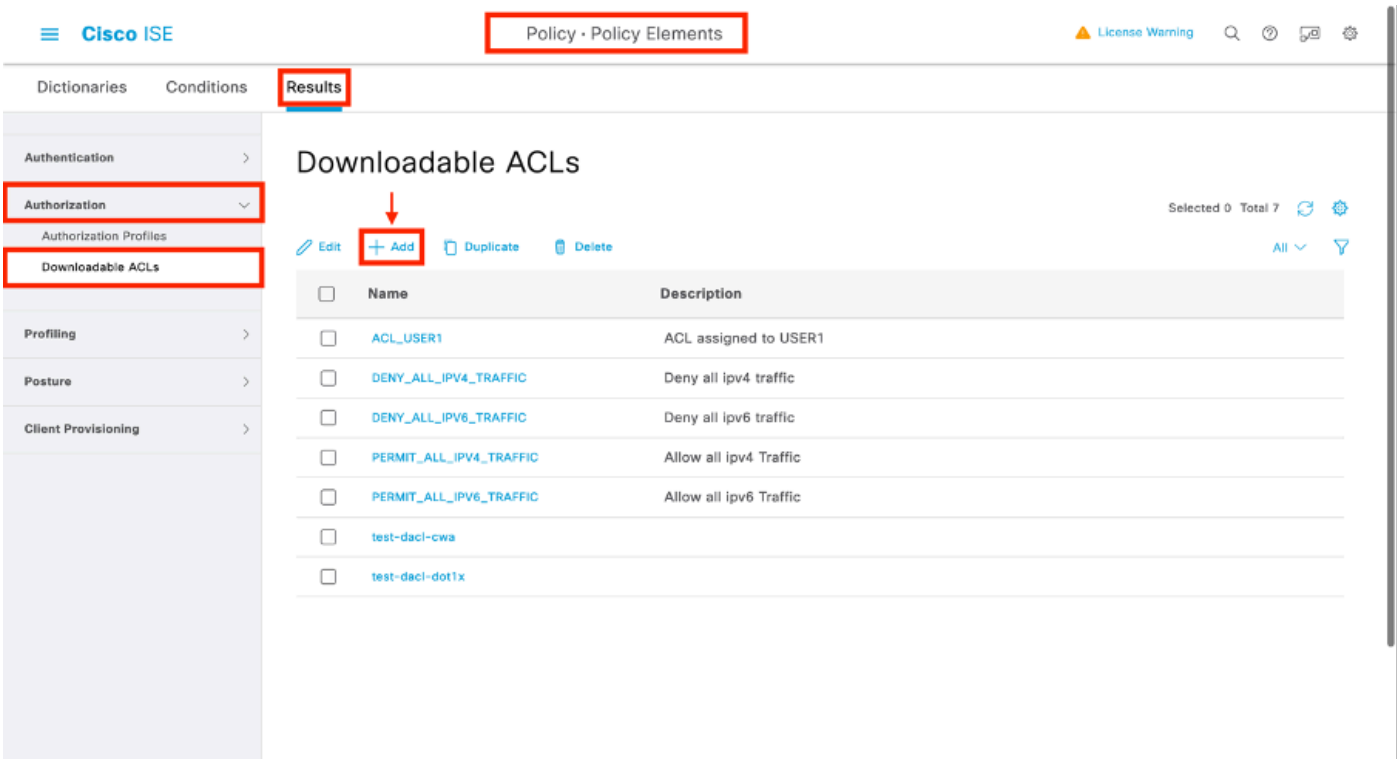
性并定义新的配置字段。

2.导航到管理>身份管理>设置>用户自定义属性。使用+按钮添加新属性，在本示例中，自定义属性的名称为ACL:



3.配置完成后，单击Save。

4.配置dACL。导航到Policy > Policy Elements > Results > Authorization > Downloadable ACLs以查看和定义ISE上的dACL。单击Add按钮以创建新按钮。

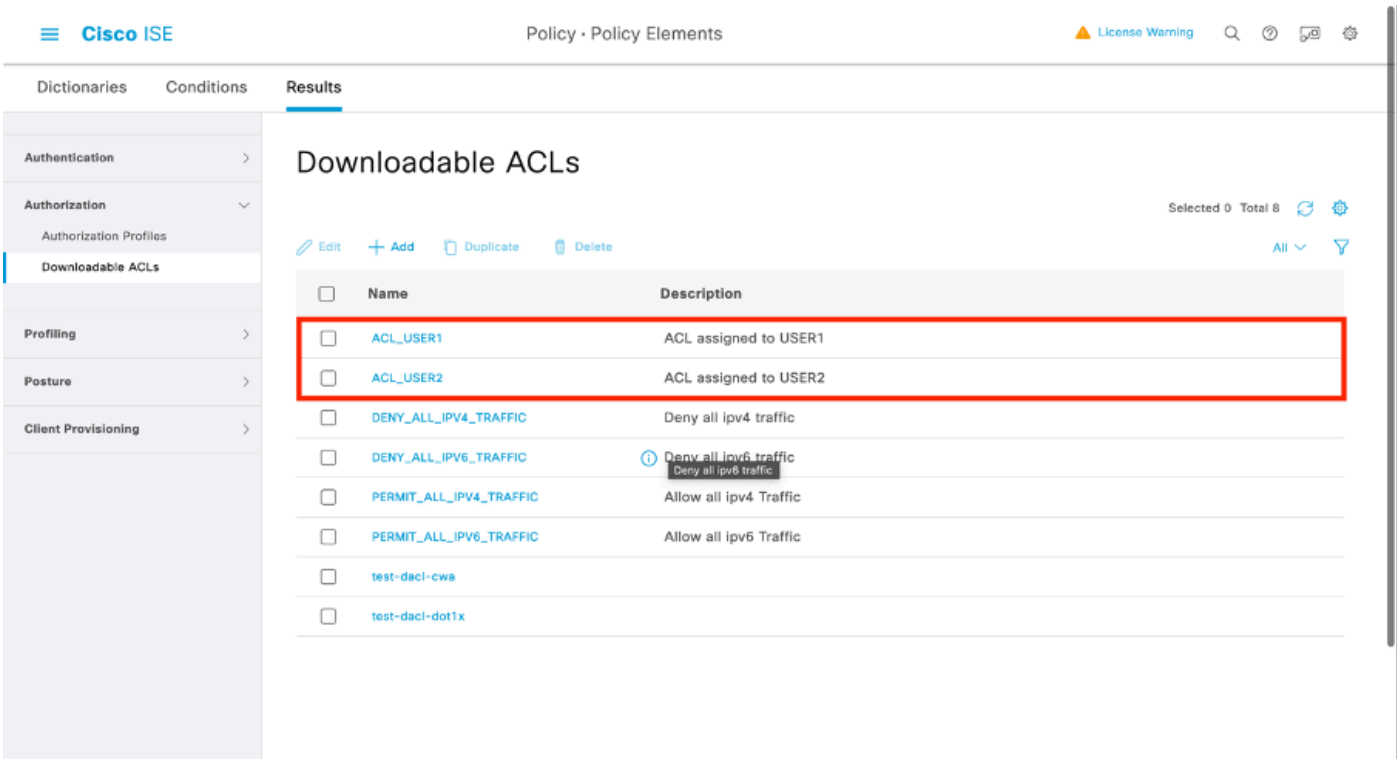


5.这将打开新的可下载ACL配置表。在此表单上，配置以下字段：

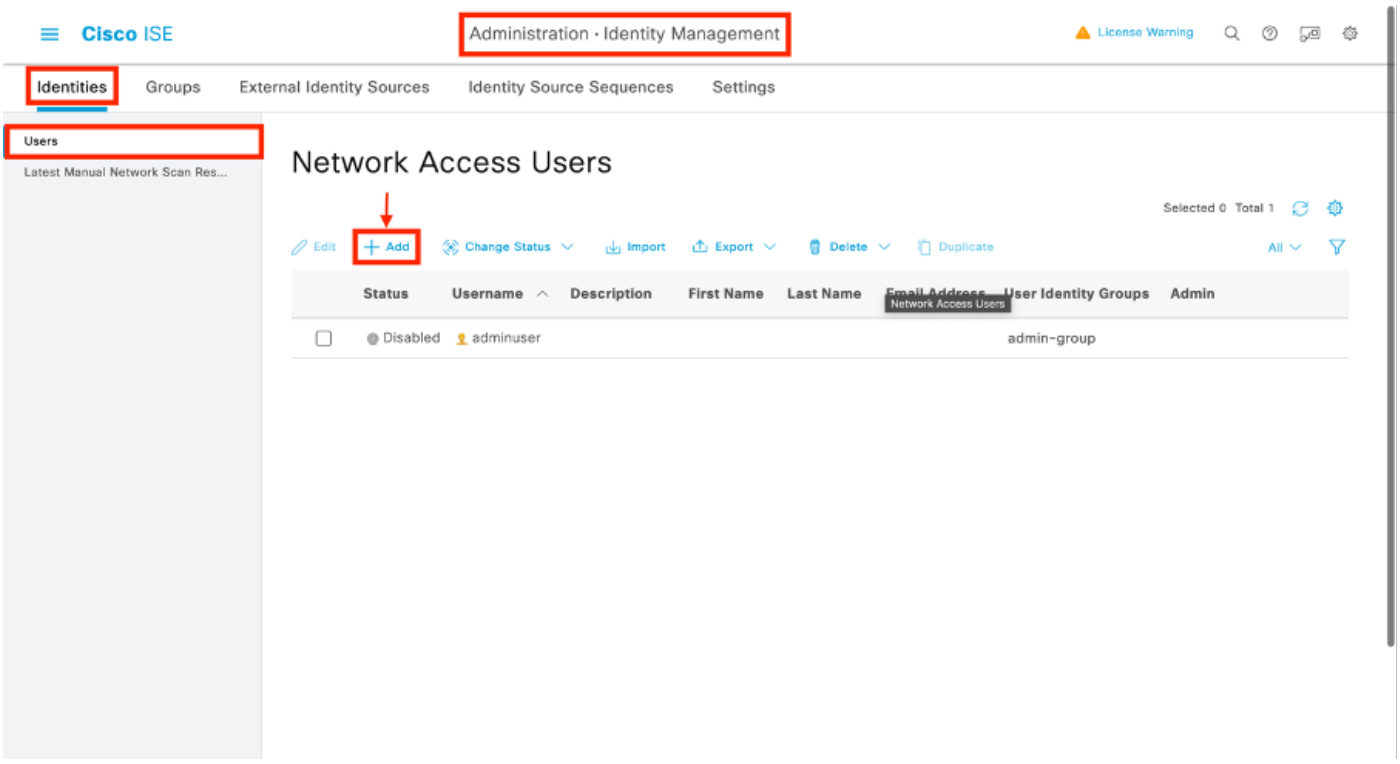
- 名称：定义的dACL的名称。
- 说明（可选）：所创建dACL的使用情况的简要说明。
- IP版本:定义的dACL中使用的IP协议版本（版本4、6或两者）。
- DACL内容:根据Cisco IOS XE® ACL语法，dACL的内容。

在本文档中，使用的dACL是ACL_USER1，此dACL允许除发往10.48.39.186和10.48.39.13的流量以外的任何流量。配置字段后，单击Submit按钮创建dACL。

重复该步骤以定义第二个用户ACL_USER2的dACL。

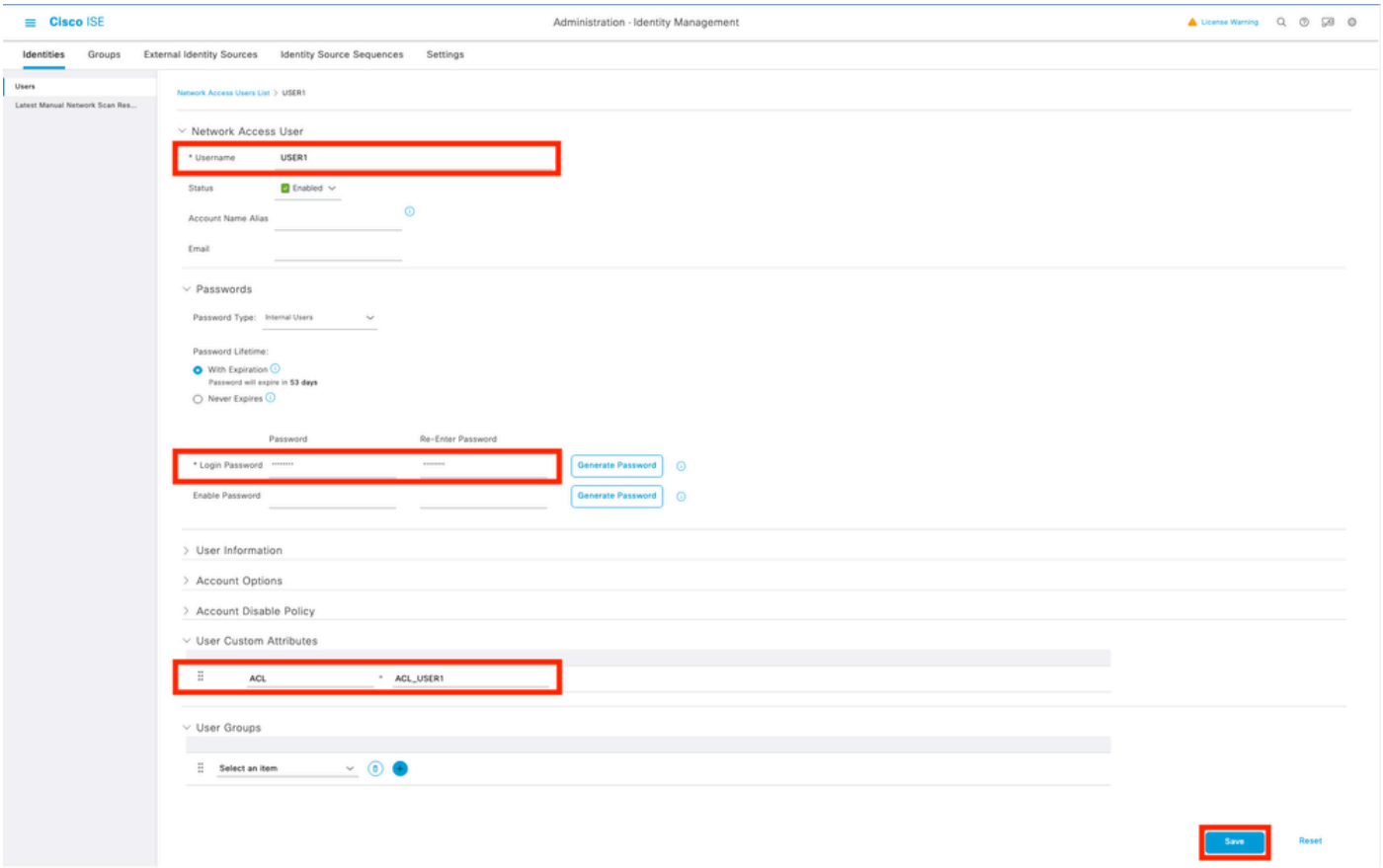


6.将dACL分配给创建的身份。创建dACL后，可以使用步骤1中创建的用户自定义属性将其分配到任何ISE身份。导航到管理>身份管理>身份>用户。单击Add以创建用户。

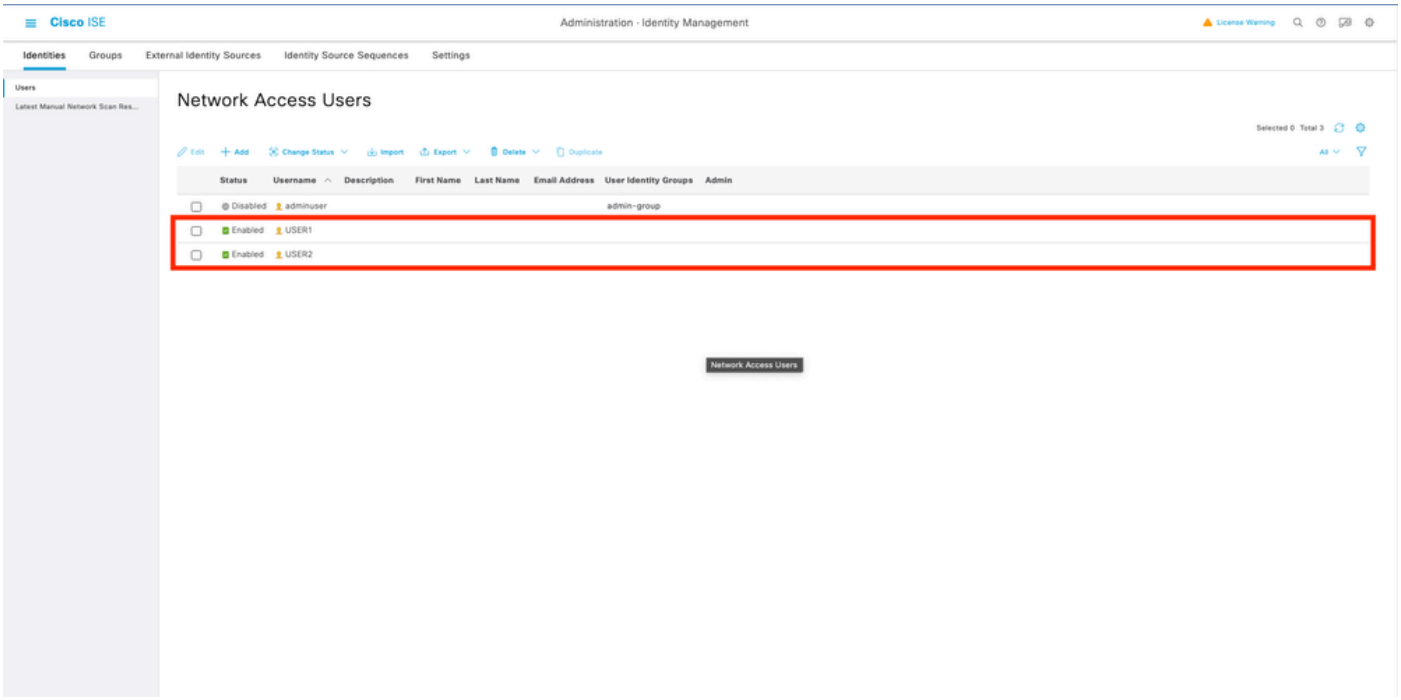


7.在New Network Access User配置表单上，定义所创建用户的用户名和密码。使用自定义属性

ACL将在第2步中创建的dACL分配给身份。在本示例中，定义使用ACL_USER1的身份标识USER1。



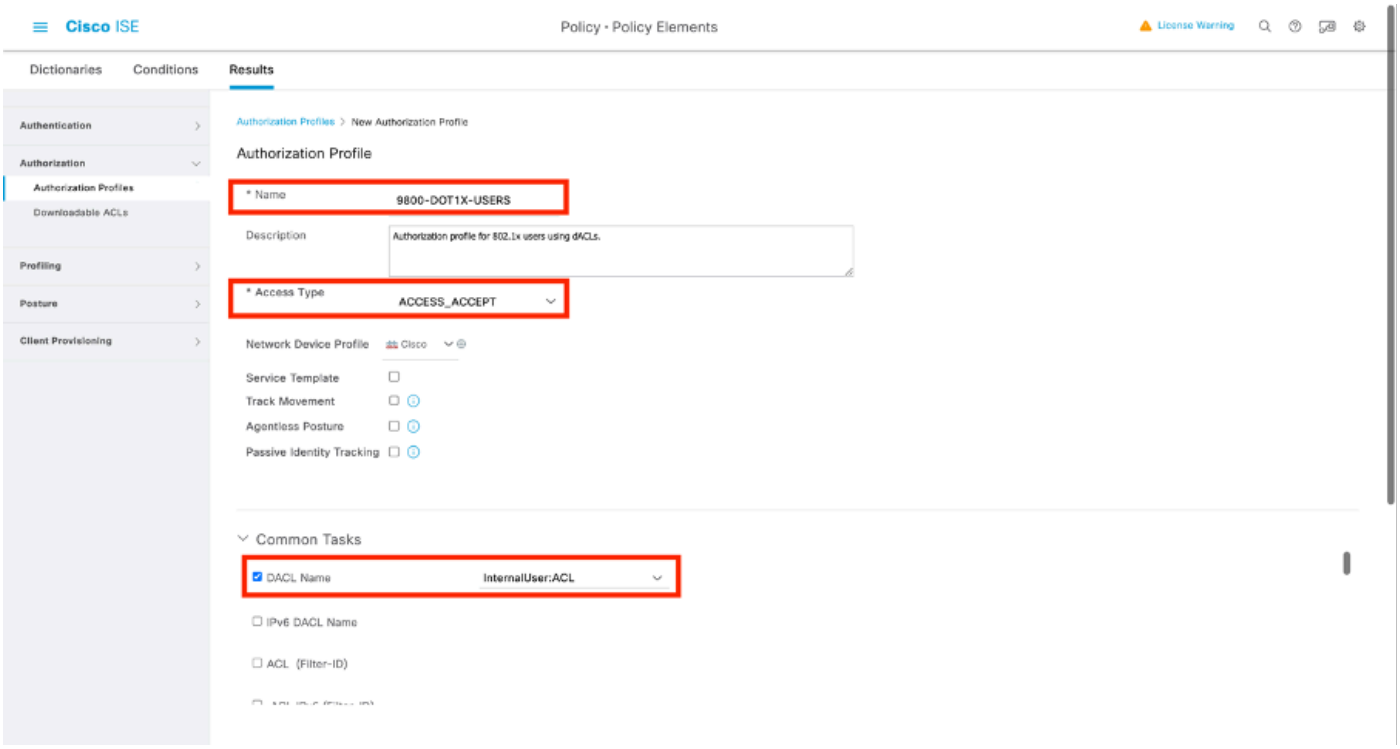
8.正确配置字段后，单击Submit按钮创建身份。重复此步骤以创建USER2并为其分配ACL_USER2。



9.配置授权策略结果。配置身份并分配dACL后，仍必须配置授权策略，使其与定义到现有授权通用任务的自定义用户属性ACL匹配。

10.定位至策略>策略要素>结果>授权>授权配置文件。单击Add以定义新的授权策略。

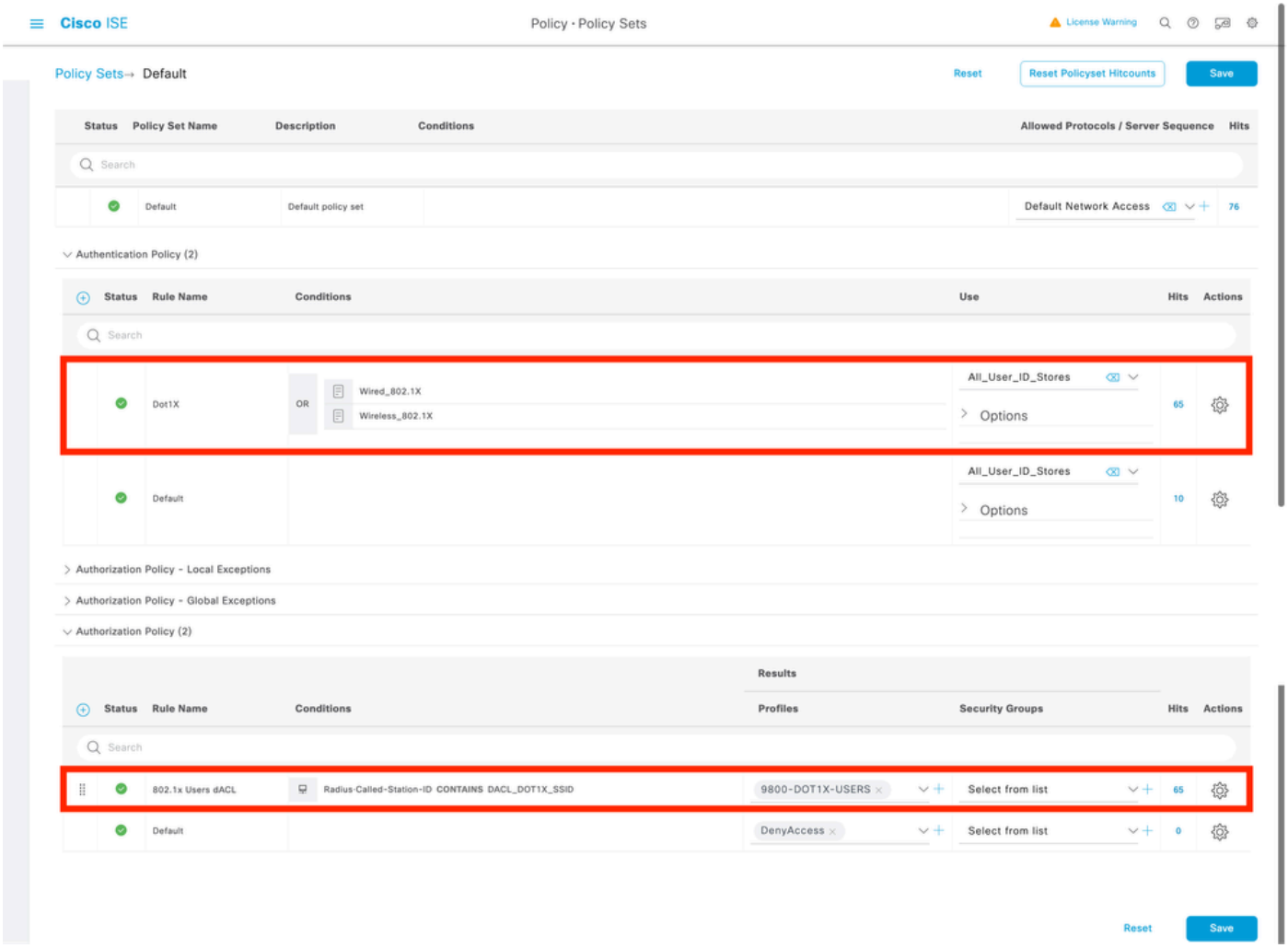
- 名称：授权策略的名称，在本例中为9800-DOT1X-USERS。
- 访问类型:匹配此策略时使用的访问类型，在本示例中使用ACCESS_ACCEPT。
- 常见任务：将DACL Name与InternalUser:<name of custom attribute created>与内部用户进行匹配。根据本文档中使用的名称，配置文件9800-DOT1X-USERS配置了dACL，该dACL配置为InternalUser:ACL。



11.使用策略集中的授权配置文件。授权配置文件结果定义正确后，它必须成为用于验证和授权无线用户的策略集的一部分。

12.定位至策略>策略集，然后打开使用的策略集。

13.身份验证策略规则Dot1X与通过有线或无线802.1x建立的任何连接匹配。授权策略规则802.1x Users dACL对使用的SSID实施一个条件（即Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID）。 如果在DACL_DOT1X_SSID WLAN上执行授权，将使用步骤4中定义的配置文件9800-DOT1X-USERS对用户进行授权。

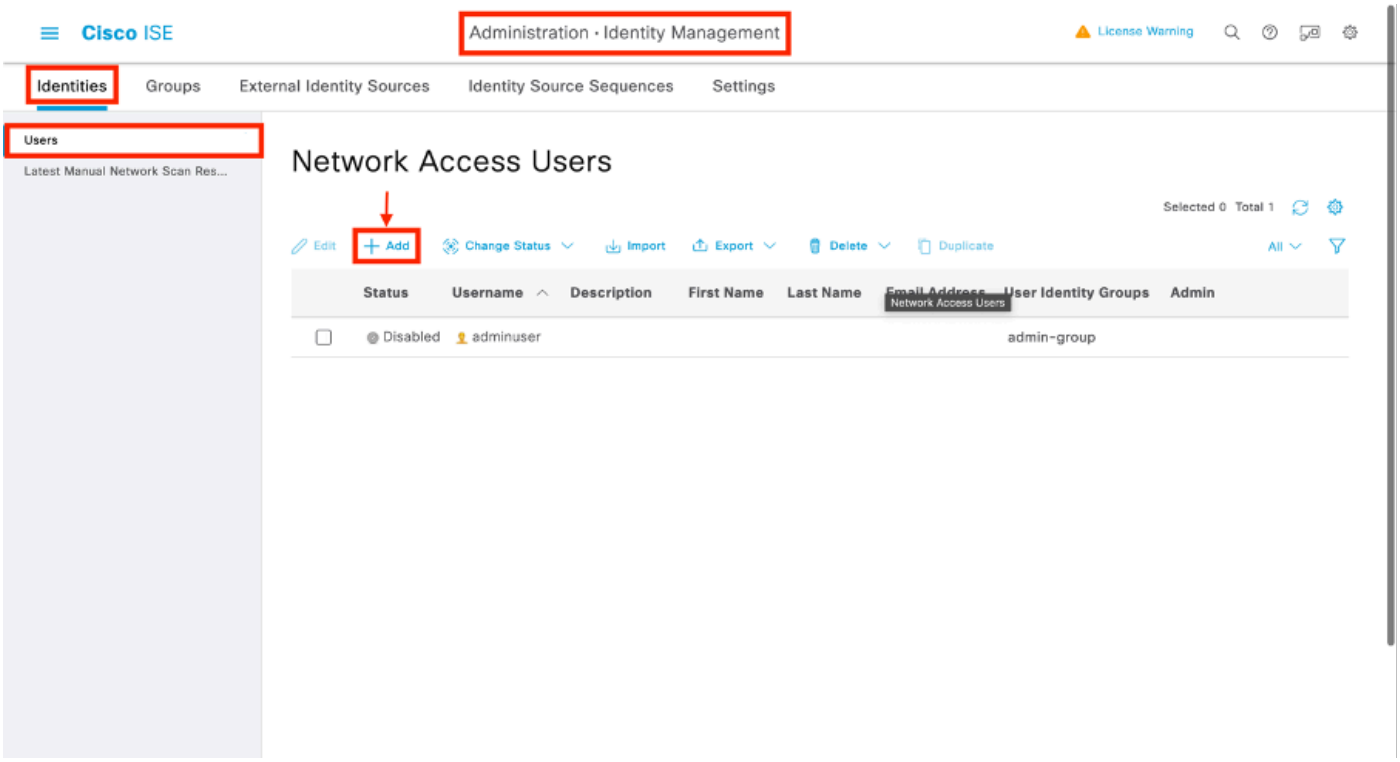


每结果dACL

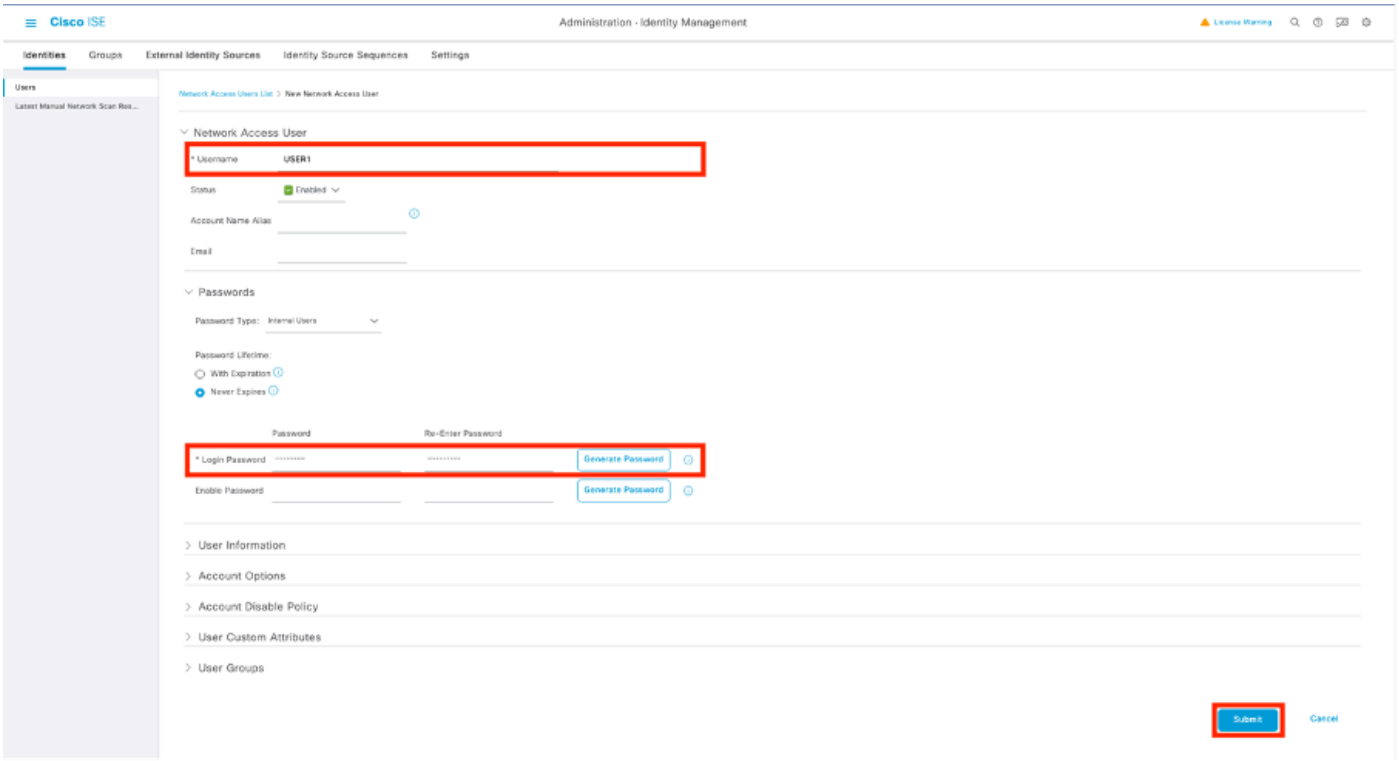
为了避免将特定dACL分配给ISE上创建的每个身份的任务，您可以选择将dACL应用于特定策略结果。然后，根据与所用策略集的授权规则匹配的任何条件应用此结果。

1.配置dACL。从每个用户dACLs部分执行步骤2中的相同步骤，以定义所需的dACL。它们是ACL_USER1和ACL_USER2。

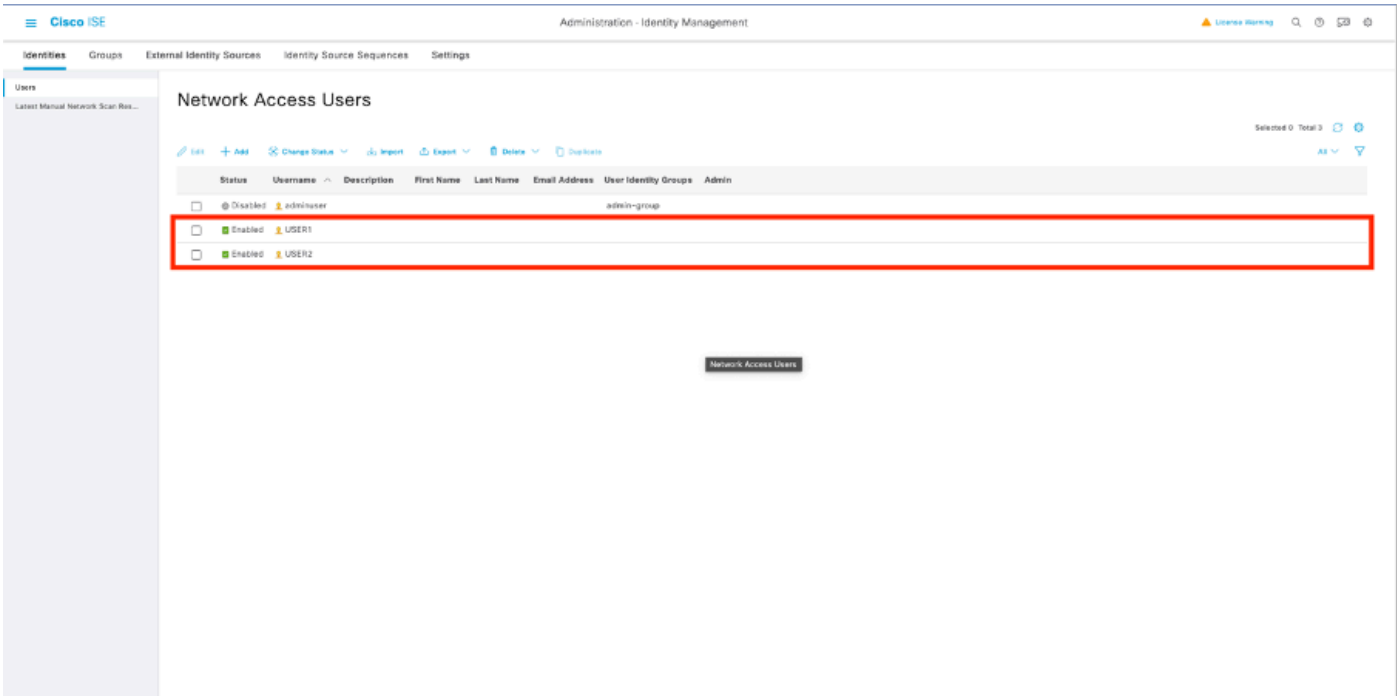
2.创建身份。导航到管理>身份管理>身份>用户，然后单击添加按钮以创建用户。



3.在New Network Access User配置表单上，定义所创建用户的用户名和密码。



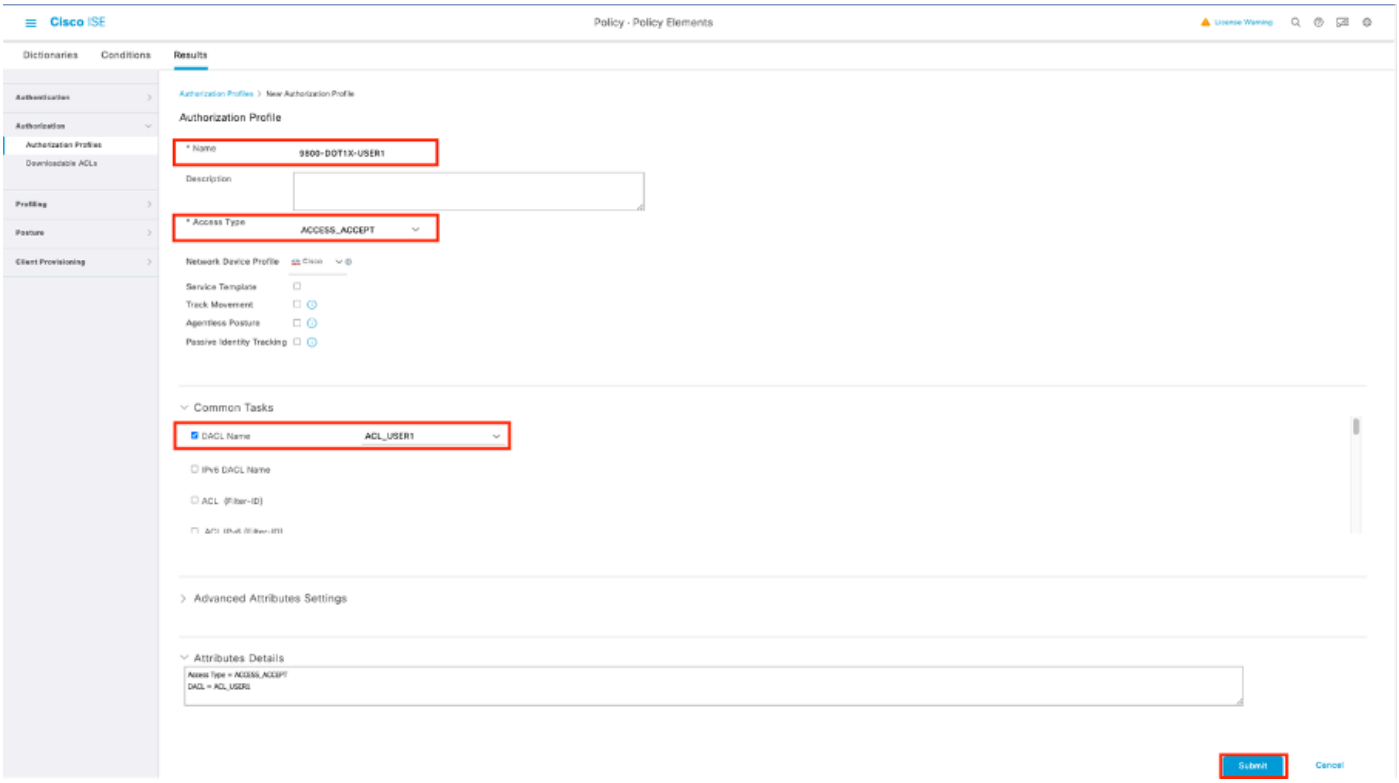
4.重复此步骤以创建USER2。



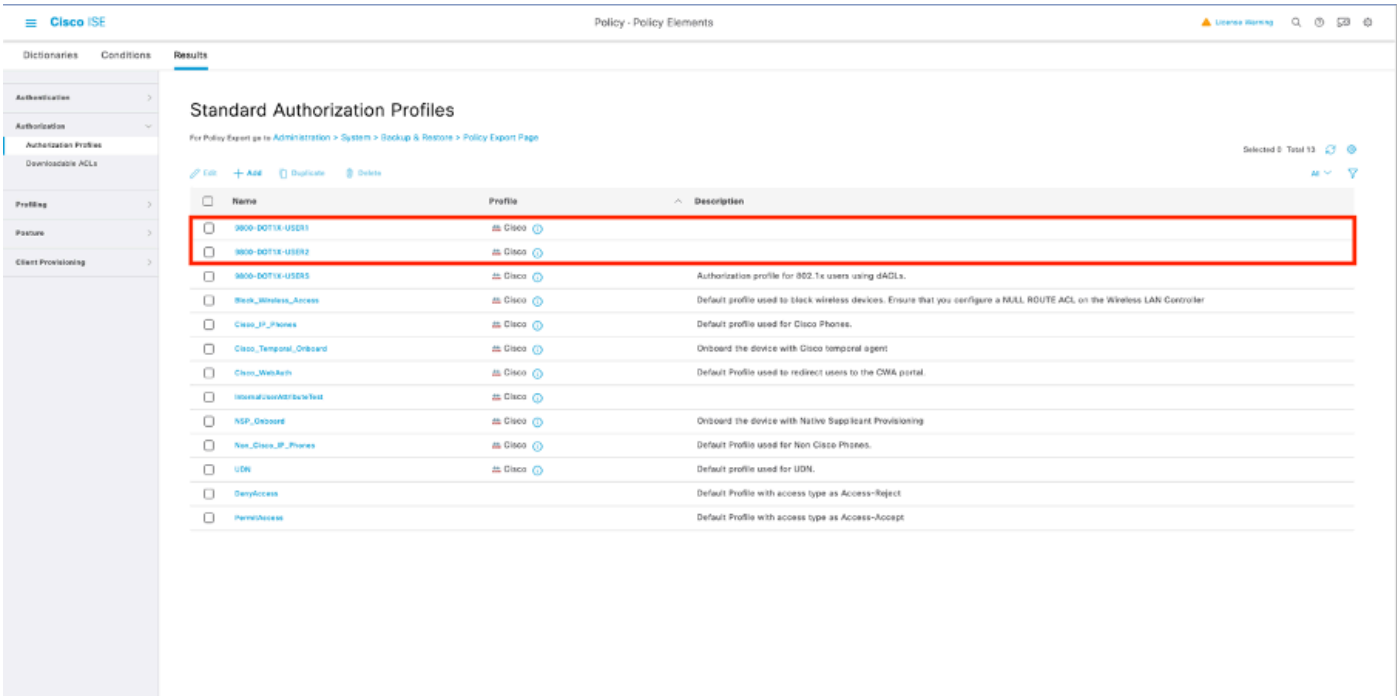
5.配置授权策略结果。配置身份和dACL后，仍然必须配置授权策略，以便为符合条件的用户分配特定dACL才能使用此策略。

6.要执行此操作，请定位至策略>策略元素>结果>授权>授权配置文件。单击Add以定义新的授权策略并填写以下字段：

- 名称：授权策略的名称，在本例中为9800-DOT1X-USER1。
- 访问类型:匹配此策略时使用的访问类型，在本例中使用ACCESS_ACCEPT。
- 常见任务:将内部用户的DACL Name与ACL_USER1进行匹配。根据本文档中使用的名称，配置文件9800-DOT1X-USER1已配置为ACL_USER1的dACL。



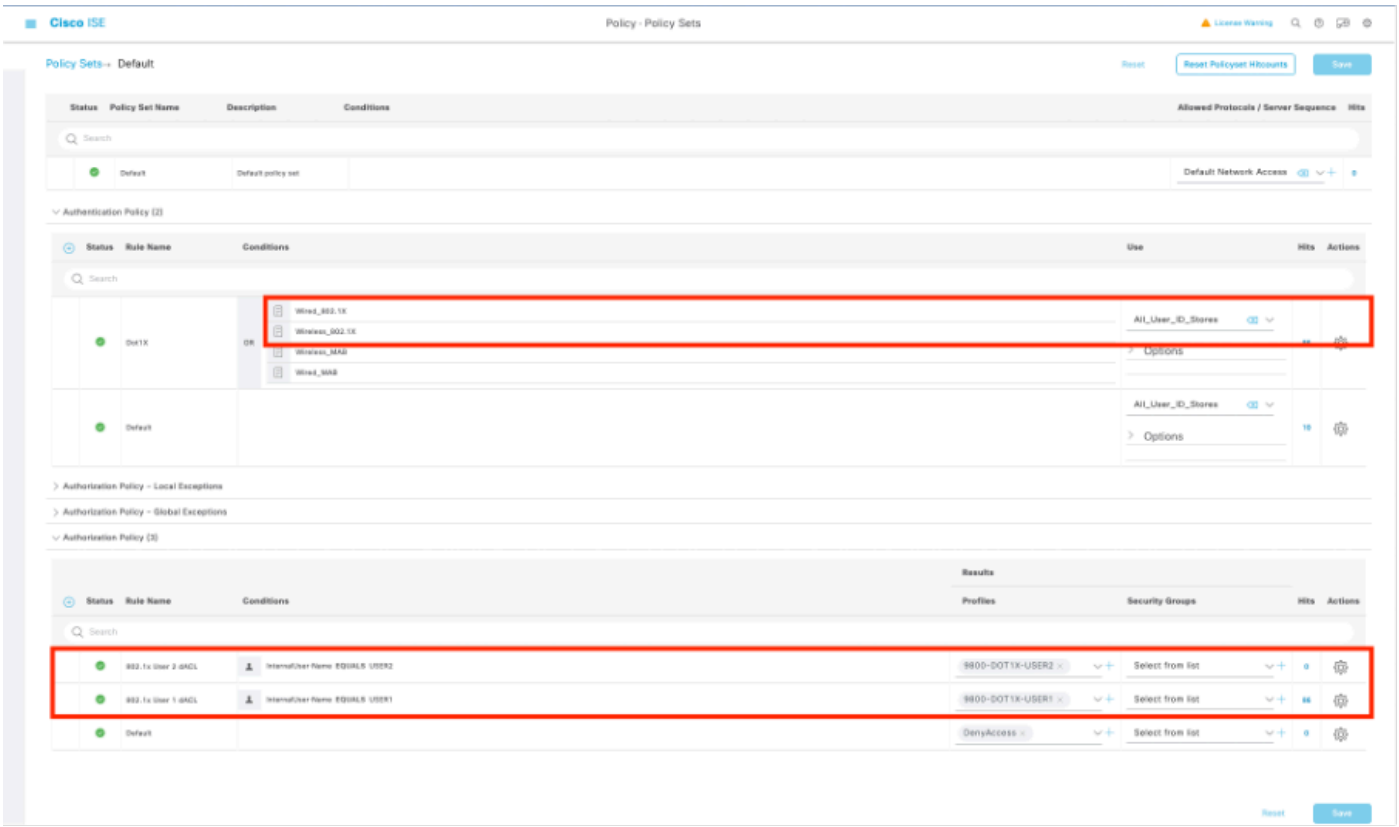
7.重复此步骤，创建策略结果9800-DOT1X-USER2，并将ACL_USER2分配为DACL。



8.在策略集中使用授权配置文件。授权配置文件结果定义正确后，它仍必须成为用于验证和授权无线用户的策略集的一部分。

9.定位至策略>策略集，然后打开使用的策略集。

10.身份验证策略规则Dot1X匹配通过有线或无线802.1X建立的任何连接。授权策略规则802.1X User 1 dACL对使用的用户名实施条件（即InternalUser-Name CONTAINS USER1）。 如果使用USER1执行授权，则使用第4步中定义的配置文件9800-DOT1X-USER1对用户进行授权，并将此结果中的dACL(ACL_USER1)应用于用户。对用户名USER2（使用9800-DOT1X-USER1）配置相同操作。



将dACL与CWA SSID配合使用的说明

如[在Catalyst 9800 WLC和ISE配置指南上配置中心Web身份验证(CWA)中所述，CWA依赖MAB和特定结果对用户进行身份验证和授权。](#)可下载的ACL可以从ISE端添加到CWA配置中，与之前介绍的相同。

警告：可下载ACL只能用作网络访问列表，不支持用作预身份验证ACL。因此，必须在WLC配置中定义CWA工作流程中使用的所有预身份验证ACL。

验证

要检验配置，可以使用以下命令：

```
# show run wlan
# show run aaa
# show aaa servers
# show ap config general
# show ap name



      config general
# show ap tag summary
# show ap name



       tag detail
# show wlan { summary | id | nme | all }
# show wireless tag policy detailed




# show wireless profile policy detailed




# show access-lists { acl-name }
```

在本示例中，显示了与此示例对应的WLC配置的参考相关部分：

```
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
```

```
!
aaa session-id common
!
[...]
vlan 1413
 name VLAN_1413
!
[...]
radius server DACL-RADIUS
 address ipv4



       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
```

显示RADIUS服务器配置，运行show running-config all命令：

```
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
```

故障排除

核对清单

- 确保客户端可以正确连接到配置的802.1X SSID。
- 确保RADIUS access-request/accept包含适当的属性值对(AVP)。
- 确保客户端使用正确的WLAN/策略配置文件。

WLC一站式反射

要检查dACL是否正确分配到特定无线客户端，可以运行show wireless client mac-address <H.H.H> detail命令。从中可以找到一些有用的故障排除信息，即：客户端用户名、状态、策略配置文件、WLAN，最重要的是此处，即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 DUID: NA
Client IPv4 Address : 10.14.13.240

Client Username : USER1

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

Client State : Associated Policy Profile : DACL-8021X

Wireless LAN Id: 2

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

BSSID : f4db.e65e.7bc0
Association Id : 1
Authentication Algorithm : Open System
Client Active State : In-Active
[...]
Client Join Time:
  Join Time Of Client : 03/28/2024 10:04:30 UTC

Client ACLs : None Policy Manager State: Run

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

VLAN : VLAN_1413

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

 SM State : AUTHENTICATED

          SM Bend State    : IDLE
  Local Policies:

 Service Template : wlan_svc_DACL-8021X_local (priority 254) VLAN : VLAN_1413 Absolute-Timer : 28800

  Server Policies:

 ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab

  Resultant Policies:

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

[...]
```

WLC Show命令

要查看属于Catalyst 9800 WLC配置的所有ACL，您可以运行show access-lists命令。此命令列出本地定义的所有ACL或由WLC下载的dACL。WLC从ISE下载的任何dACL都有xACSACLx-IP-<ACL_NAME>-<ACL_HASH> format.

注意：如果客户端已关联并在无线基础设施中使用可下载ACL，可下载ACL将保留在配置中

。使用dACL的最后一个客户端离开基础设施后，将从配置中删除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
[...]
```

条件调试和无线电主动跟踪

在对配置进行故障排除时，您可以收集已分配定义dACL的客户端的放射性踪迹。以下是一些突出显示的日志，其中显示客户端08be.ac14.137d的关联过程中的部分放射性痕迹：

<#root>

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

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

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

[...]

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

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

[...]

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

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

[...]

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

[...]

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

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

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

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

[...]

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

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

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

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

```
2024/03/28 10:43:04.381486879 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 49
2024/03/28 10:43:04.381489488 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 43 "
2024/03/28 10:43:04.381491463 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

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

2024/03/28 10:43:04.381495896 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32
2024/03/28 10:43:04.381498320 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "
2024/03/28 10:43:04.381500186 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

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

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

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

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

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

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

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

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

2024/03/28 10:43:04.381539951 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [18
2024/03/28 10:43:04.381542233 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[
2024/03/28 10:43:04.381544465 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188]
2024/03/28 10:43:04.381619890 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout
[...]

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

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

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

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

2024/03/28 10:43:04.726905248 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000012

[...]

2024/03/28 10:43:04.727138915 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000012

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

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

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

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

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

[...]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[...]

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

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

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

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

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

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

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

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

[...]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

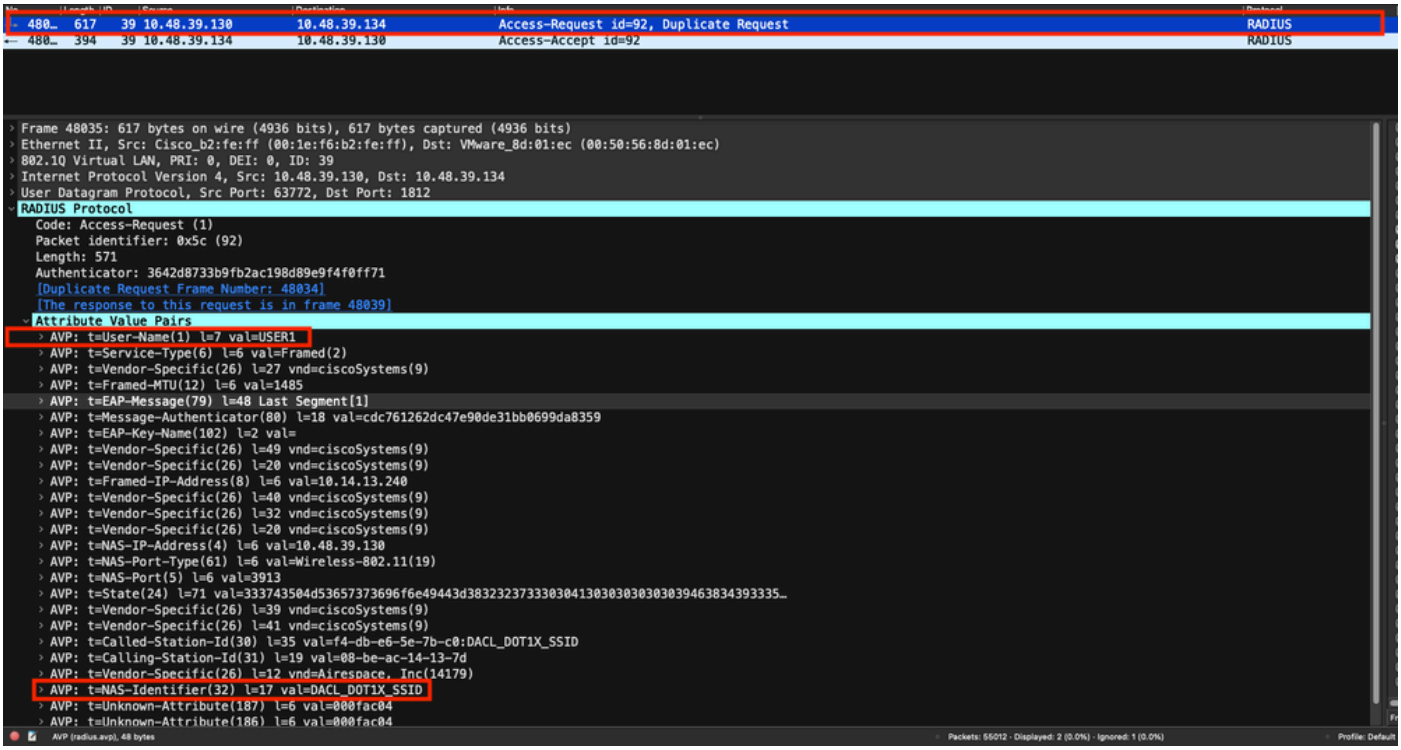
---

数据包捕获

另一个要分析的方法是客户端关联的RADIUS流的数据包捕获。可下载ACL依赖于RADIUS，不仅要分配给无线客户端，还要由WLC下载。在对dACL配置进行故障排除时，必须在控制器用于与RADIUS服务器通信的接口上捕获数据包。本文档展示了如何在Catalyst 9800上配置轻松嵌入的数据包捕获，这些捕获已用于收集本文分析的捕获。

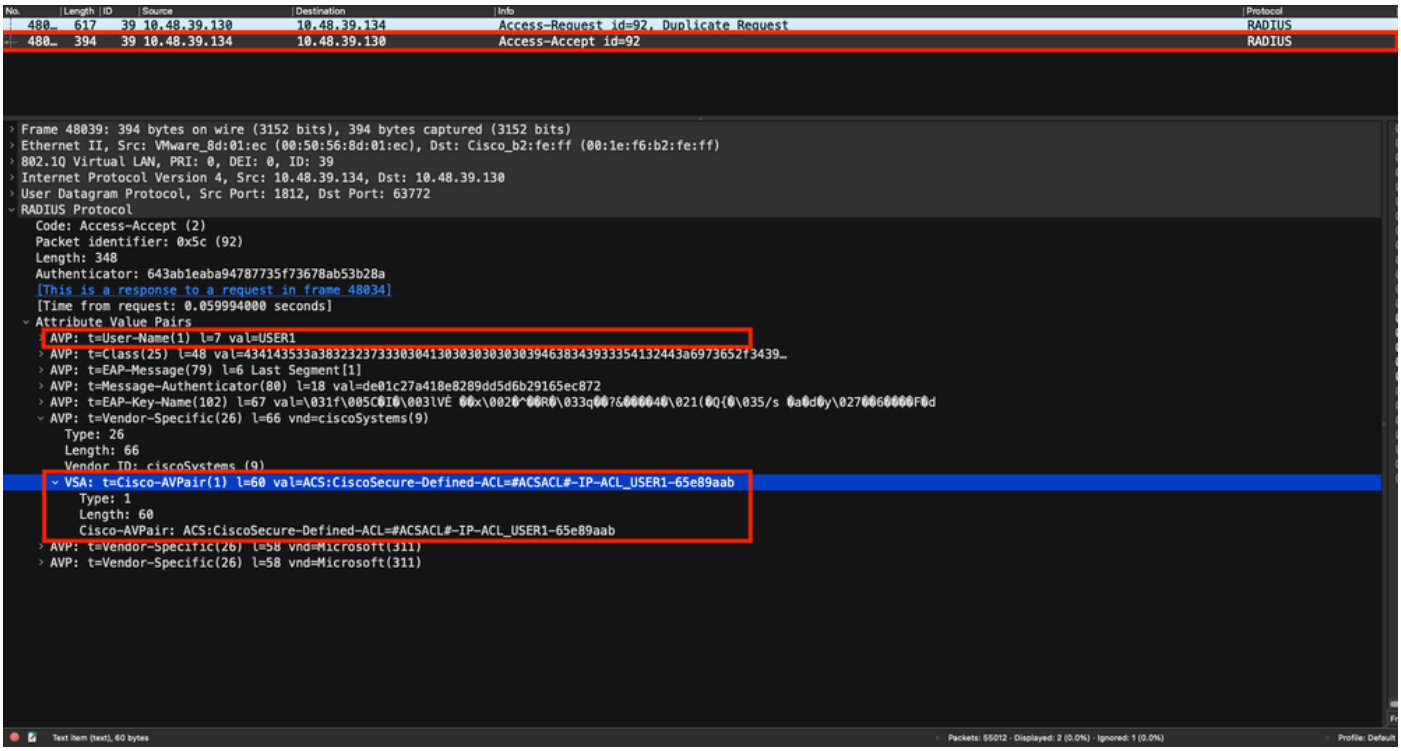
RADIUS客户端身份验证

您可以看到从WLC向RADIUS服务器发送客户端RADIUS访问请求以对DACL_DOT1X_SSID SSID(AVP NAS-Identifier)上的USER1(AVP User-Name)进行身份验证。



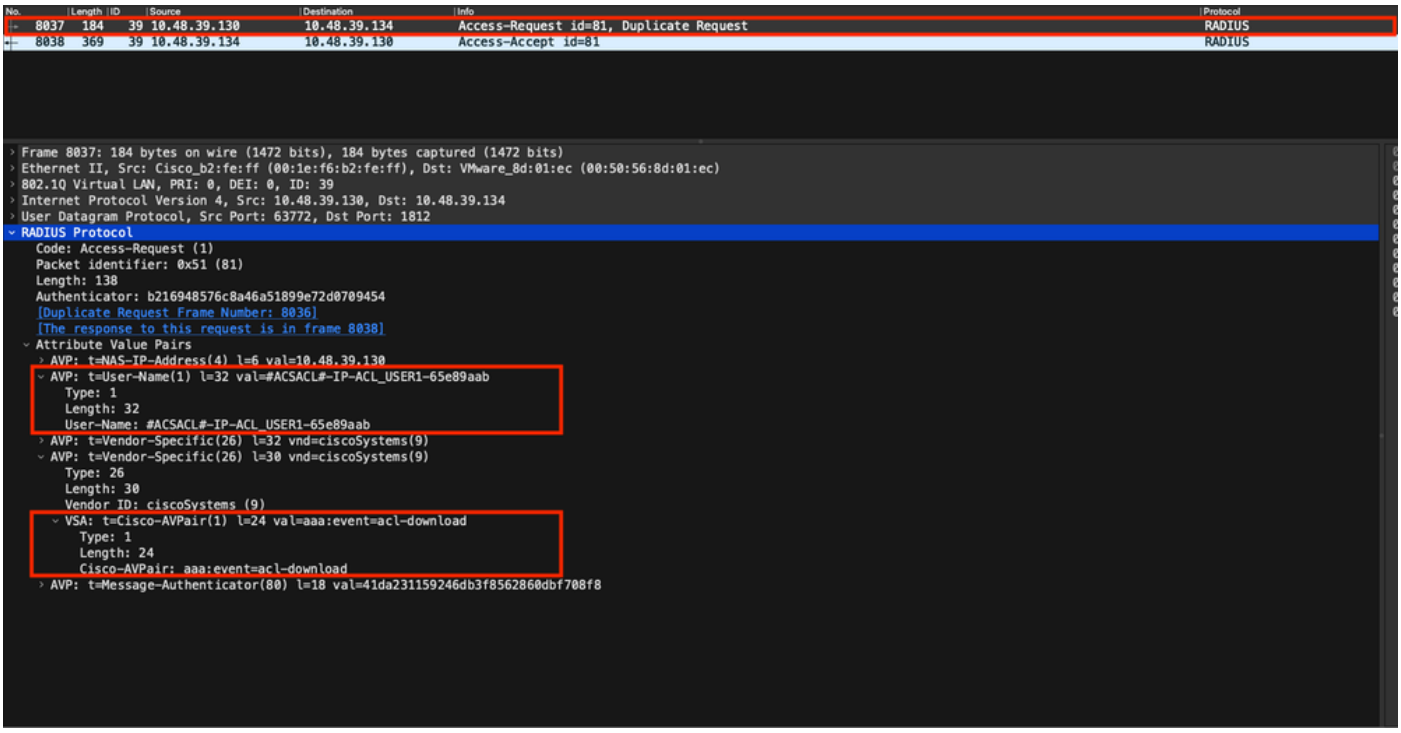
身份验证成功后，RADIUS服务器会以访问接受进行回复。对于用户USER1(AVP User-Name)和应用AAA属性时，供应商特定AVP ACS:CiscoSecure-Defined-ACL为#ACSACL#-IP-ACL_USER1-

65e89aab。

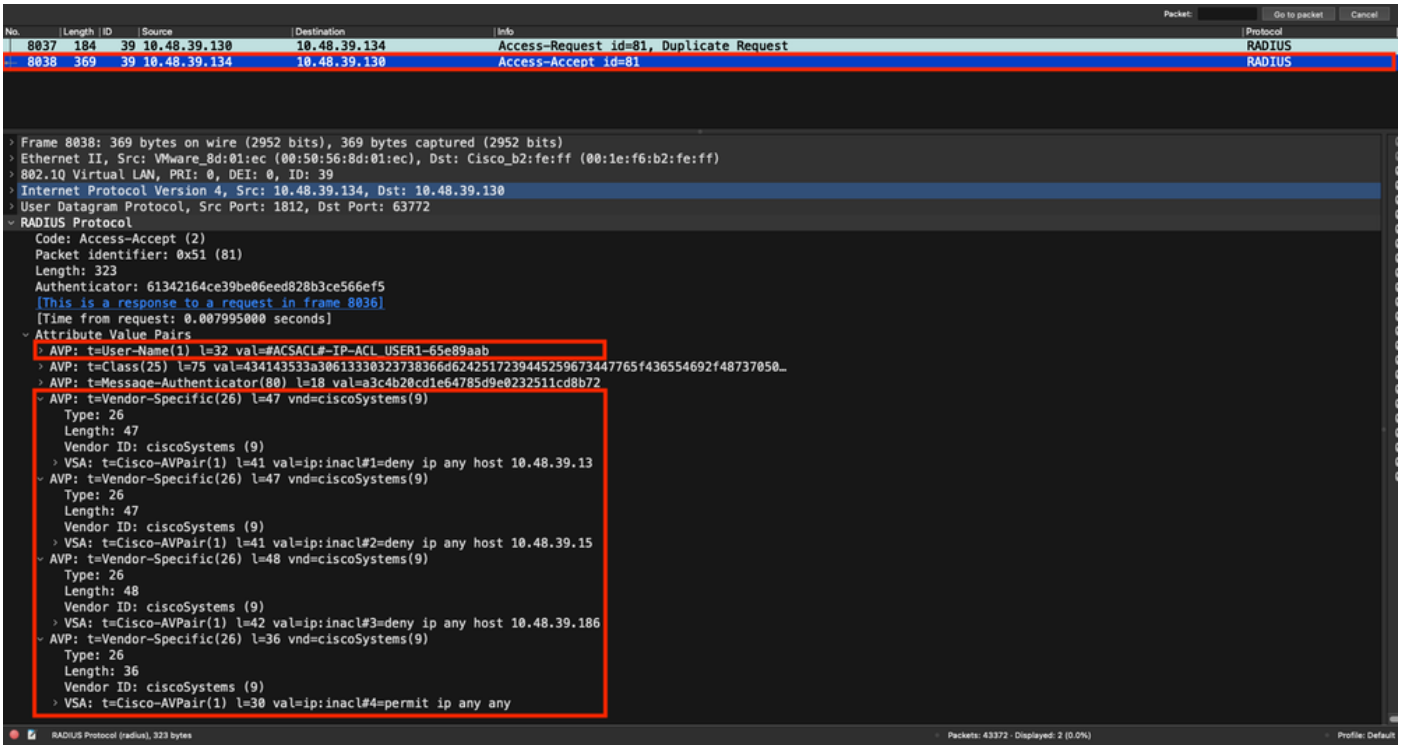


DACL下载

如果dACL已是WLC配置的一部分，则会将其分配给用户，并且RADIUS会话结束。否则，WLC将下载ACL，仍然使用RADIUS。为此，WLC发送RADIUS访问请求，这次使用AVP用户名的dACL名称(#ACSACL#-IP-ACL_USER1-65e89aab)。WLC通知RADIUS服务器此访问接受使用Cisco AV对aaa:event=acl-download启动ACL下载。



发回控制器的RADIUS access-accept包含请求的dACL，如屏幕截图所示。每个ACL规则都包含在ip:inacl#<X>=<ACL_RULE>类型的不同Cisco AVP中， <X>是规则编号。



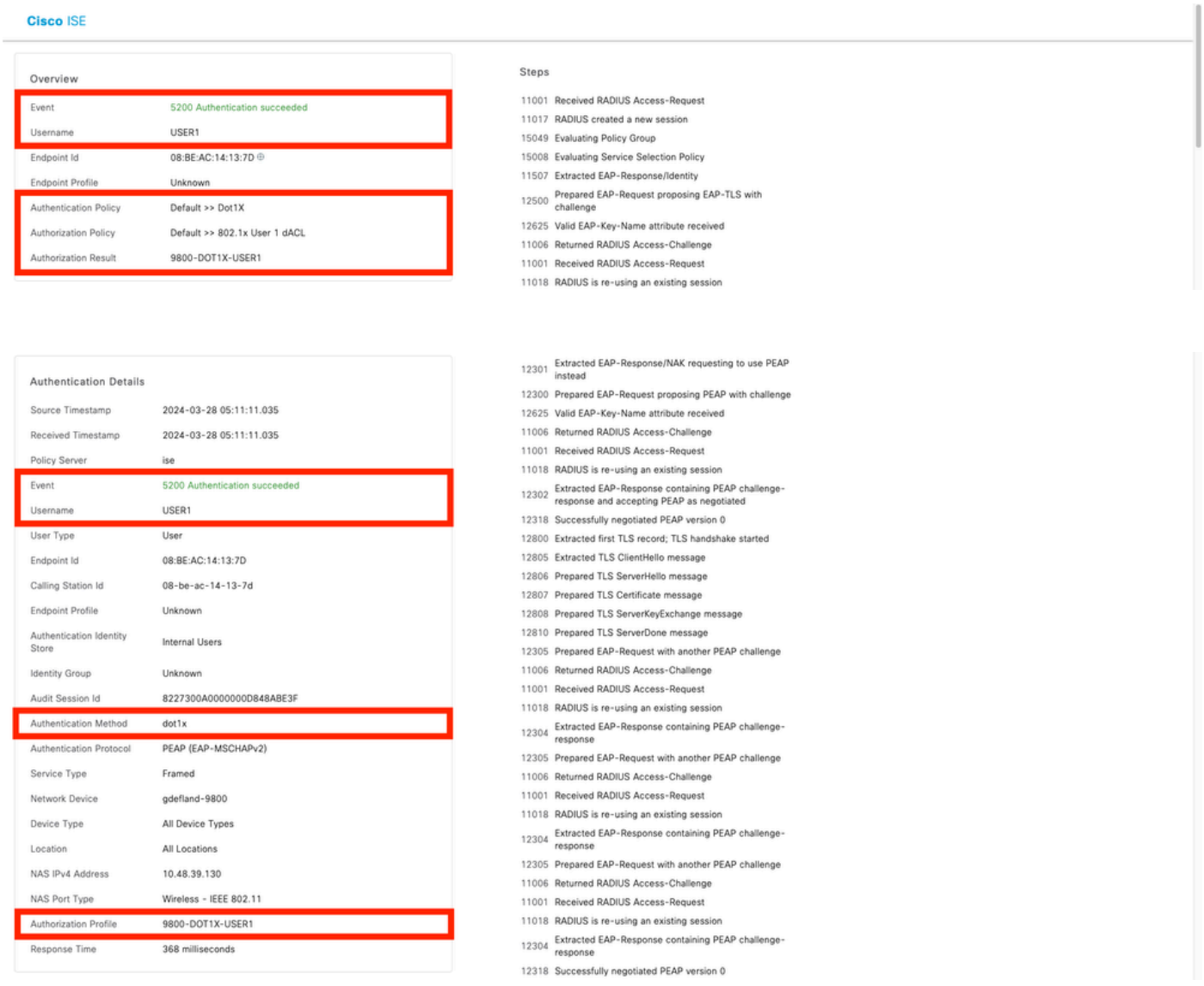
注意：如果ACL的内容在WLC上下载后被修改，则直到用户重新进行身份验证（并且

WLC再次对用户执行RADIUS身份验证），此ACL的更改才会反映出来。ACL名称的散列部分变化反映了ACL的变化。此ACL下次分配给用户时，其名称必须不同，并且ACL不能是WLC配置的一部分。但是，在ACL更改之前进行身份验证的客户端继续使用上一个客户端直到完全重新进行身份验证。

ISE操作日志

RADIUS客户端身份验证

操作日志显示用户USER1的身份验证成功，其中应用了可下载的ACL ACL_USER1。故障排除的兴趣部分以红色框显示。



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

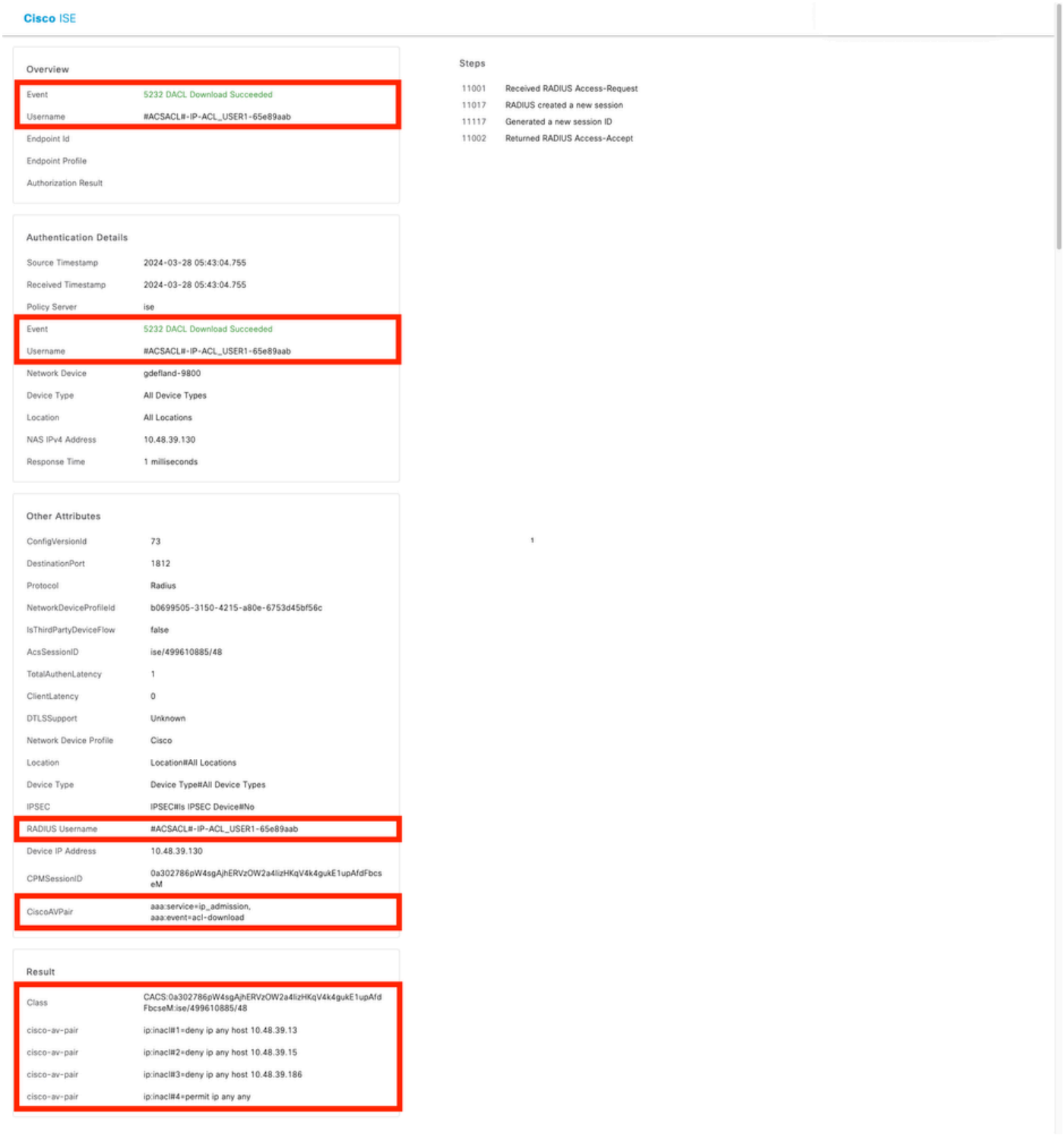
Class	CACS:8227300A0000000D848ABE3F:ise/499610885/35
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:87:b8:72:94:16:e3:b9:93:2f:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:c5:c5:05:d6:57:5b:f1:2d:62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:06:9c:ef:3e:9f:f6
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1-65e89aab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

Session Events

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

DACL下载

操作日志显示ACL ACL_USER1下载成功。故障排除的关注部分以红色显示。



关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。