& Catalyst 9800에서 다운로드 가능한 ACL 문제 해결 구성

목차

소개

이 문서에서는 Catalyst 9800 WLC(Wireless LAN Controller)에서 dACL(downloadable ACL)을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

dACL은 수년간 Cisco IOS® 및 IOS XE® 스위치에서 지원되어 왔습니다. dACL은 ACL의 로컬 복사본이 있고 ACL 이름만 할당되는 것이 아니라 인증이 발생할 때 네트워크 디바이스가 RADIUS 서버

에서 ACL 항목을 동적으로 다운로드한다는 사실을 의미합니다. 보다 완벽한 Cisco ISE 컨피그레이션 예를 사용할 수 있습니다. 이 문서에서는 17.10 릴리스 이후 중앙 스위칭을 위해 dACL을 지원하는 Cisco Catalyst 9800에 대해 중점적으로 살펴봅니다.

사전 요구 사항

이 문서의 목적은 기본 SSID 컨피그레이션 예를 통해 Catalyst 9800의 dACL 사용을 시연하는 것으로, 이를 완벽하게 사용자 정의할 수 있는 방법을 보여줍니다.

Catalyst 9800 무선 컨트롤러에서 다운로드 가능한 ACL은

- Cisco IOS XE Dublin 17.10.1 릴리스부터 지원됩니다.

- 로컬 모드 액세스 포인트(또는 Flexconnect 중앙 스위칭)가 있는 중앙 집중식 컨트롤러에서만 지원됩니다. FlexConnect 로컬 스위칭은 dACL을 지원하지 않습니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Catalyst Wireless 9800 컨피그레이션 모델.
- Cisco IP ACL(Access Control List).

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9800-CL(더블린 17.12.03 버전).
- ISE(v. 3.2).

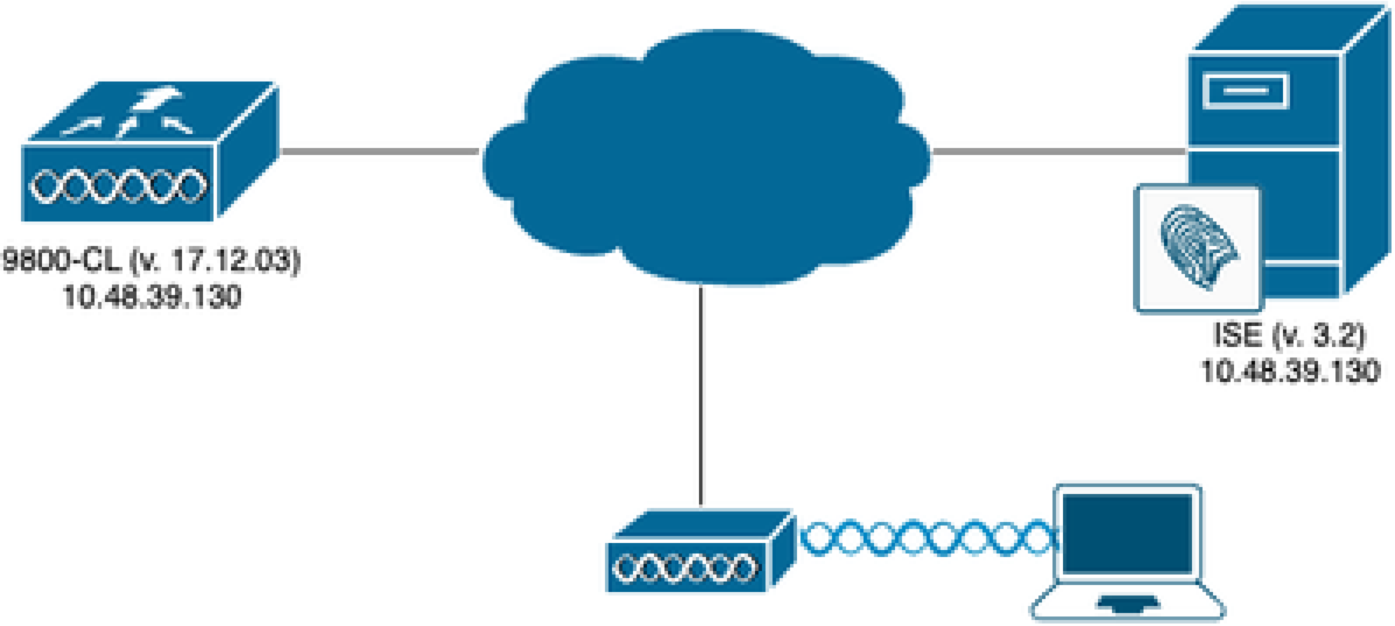
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 컨피그레이션 가이드에서는 방법이 다른 경우에도(예: WLAN 인증, 정책 컨피그레이션 등) 최종 결과는 동일합니다. 여기에 표시되는 시나리오에서는 두 개의 사용자 ID가 USER1 및 USER2로 정의됩니다. 둘 다 무선 네트워크에 대한 액세스 권한이 부여됩니다. ACL_USER1 및 ACL_USER2는 각각 Catalyst 9800이 ISE에서 다운로드한 dACL입니다.

802.1x SSID와 함께 dACL 사용

네트워크 다이어그램



WLC 컨피그레이션

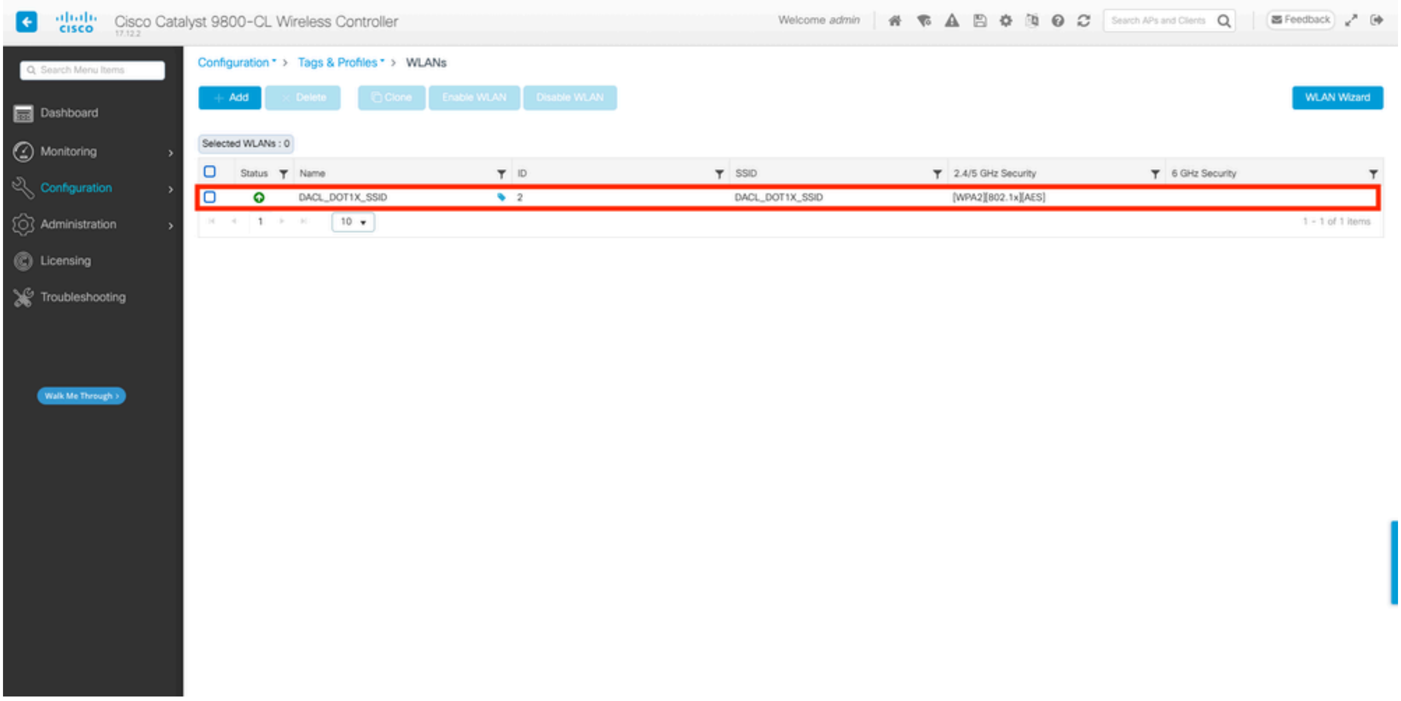
Catalyst 9800의 802.1x SSID 컨피그레이션 및 문제 해결에 대한 자세한 내용은 Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series 컨피그레이션 가이드를 참조하십시오.

1단계. SSID를 구성합니다.

ISE를 RADIUS 서버로 사용하여 802.1x 인증 SSID를 구성합니다. 이 문서에서 SSID의 이름은 "DACL_DOT1X_SSID"입니다.

GUI에서 다음과 같이 표시되어야 합니다.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > WLAN으로 이동하여 여기에 표시된 것과 유사한 WLAN을 생성합니다.



Selected WLANs : 0

Status	Name	ID	SSID	2.4/5 GHz Security	6 GHz Security
●	DACL_DOT1X_SSID	2	DACL_DOT1X_SSID	[WPA2][802.1x][AES]	

1 - 1 of 1 items

CLI에서:

```
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
```

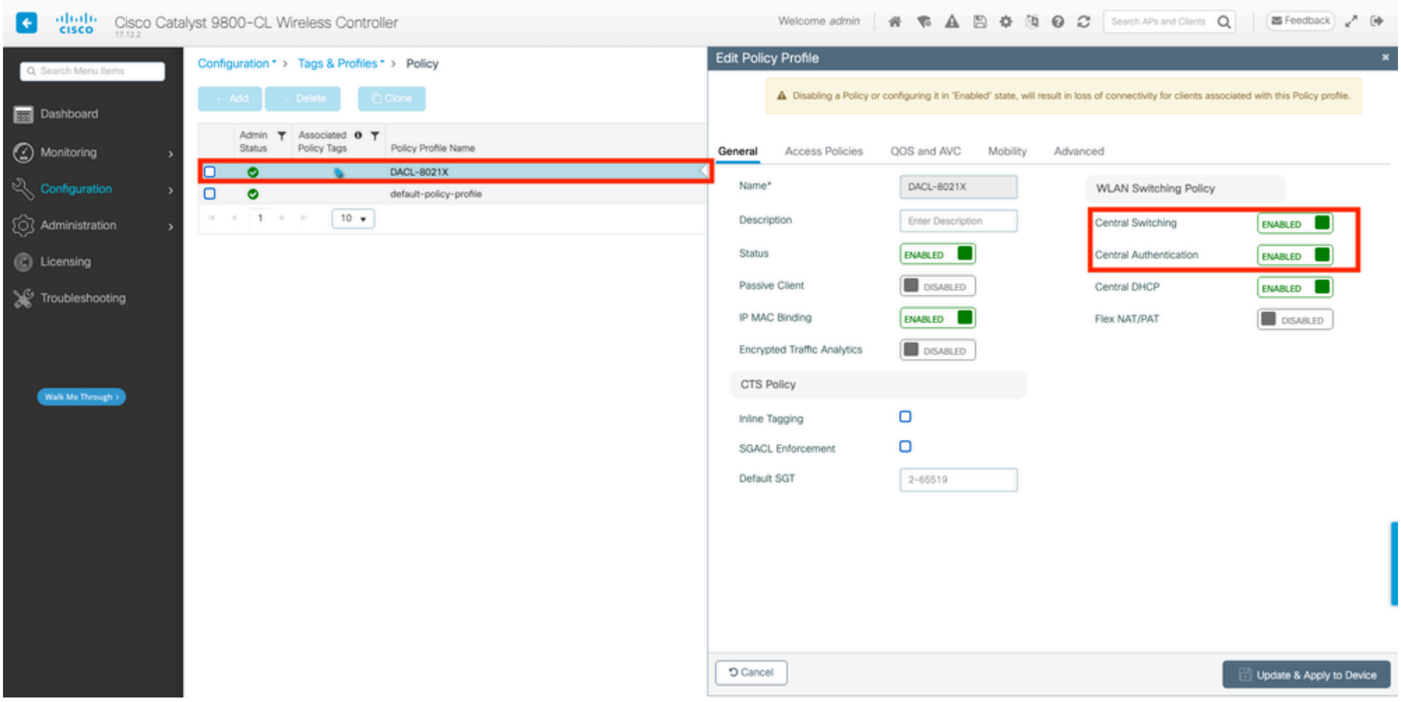
2단계. 정책 프로필을 구성합니다.

위에 정의된 SSID와 함께 사용되는 정책 프로필을 구성합니다. 이 정책 프로필에서 스크린샷과 같이 "Advanced(고급)" 탭에서 AAA Override(AAA 재정의)가 구성되어 있는지 확인합니다. 이 문서에서 사용된 정책 프로필은 "DACL-8021X"입니다.

사전 요구 사항 섹션에서 설명한 대로 dACL은 중앙 스위칭/인증 구축에만 지원됩니다. 정책 프로필이 해당 방식으로 구성되었는지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > Policy(정책)로 이동하여 사용되는 정책 프로필을 선택하고 표시된 대로 구성합니다.



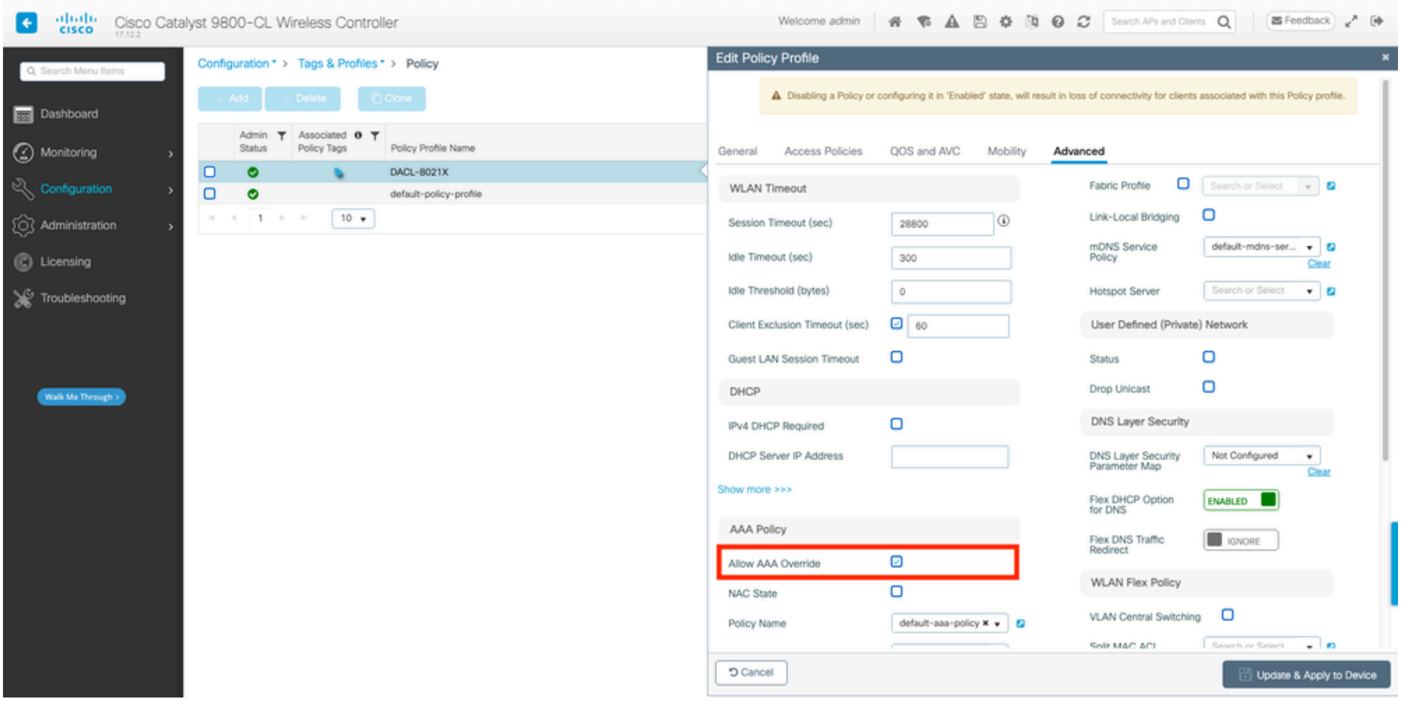
	Admin Status	Associated Policy Tags	Policy Profile Name
□	✓		DACL-8021X
□	✓		default-policy-profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

Name* DACL-8021X
Description Enter Description
Status ENABLED
Passive Client DISABLED
IP MAC Binding ENABLED
Encrypted Traffic Analytics DISABLED

CTS Policy
Inline Tagging □
SGACL Enforcement □
Default SGT 2-65519

WLAN Switching Policy
Central Switching ENABLED
Central Authentication ENABLED
Central DHCP ENABLED
Flex NAT/PAT DISABLED



⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

WLAN Timeout

Session Timeout (sec): 28800

Idle Timeout (sec): 300

Idle Threshold (bytes): 0

Client Exclusion Timeout (sec): ☑ 60

Guest LAN Session Timeout: □

DHCP

IPv4 DHCP Required: □

DHCP Server IP Address:

AAA Policy

Allow AAA Override: ☑

NAC State: □

Policy Name: default-aaa-policy

Fabric Profile: □ Search or Select

Link-Local Bridging: □

mDNS Service Policy: default-mdns-ser...

Hotspot Server: Search or Select

User Defined (Private) Network

Status: □

Drop Unicast: □

DNS Layer Security

DNS Layer Security Parameter Map: Not Configured

Flex DHCP Option for DNS: ENABLED

Flex DNS Traffic Redirect: IGNORE

WLAN Flex Policy

VLAN Central Switching: □

Split MAC ACL: Search or Select

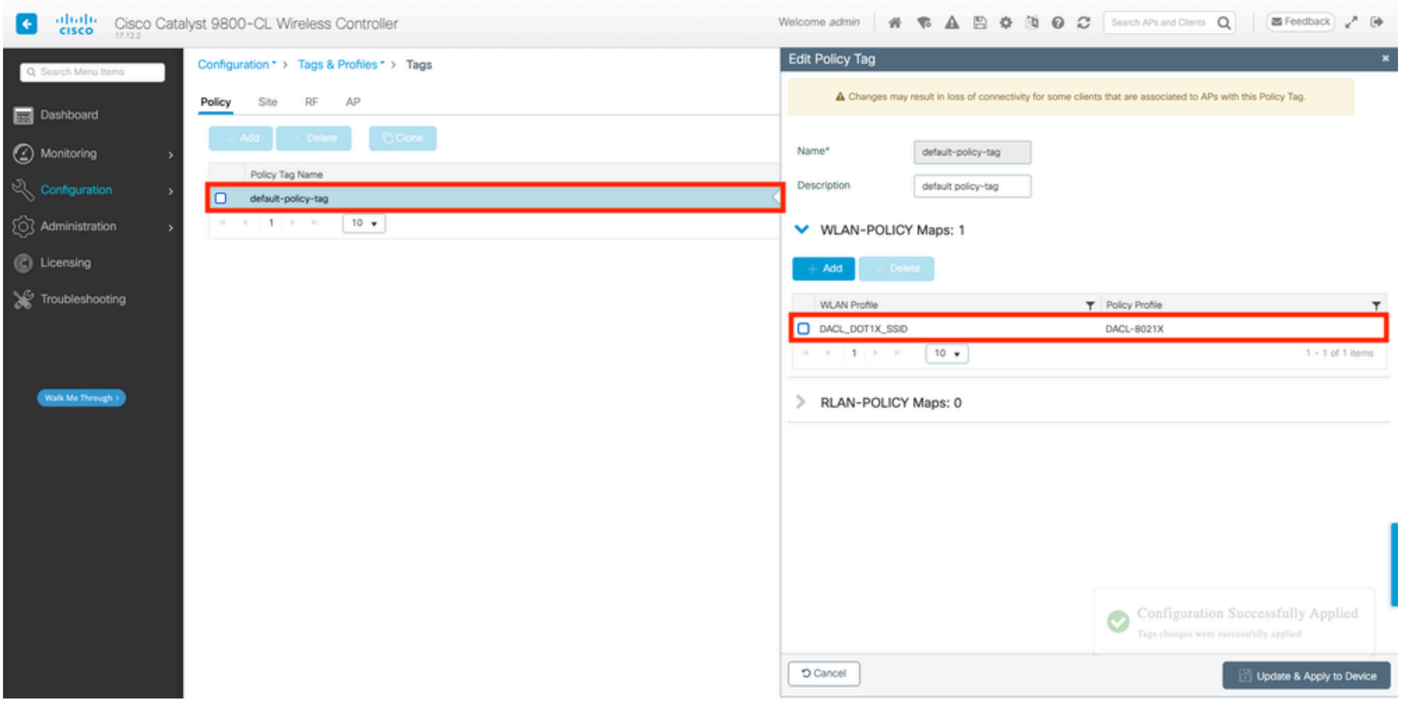
<u>CLI에서:</u>

```
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
```

3단계. 정책 프로파일과 SSID를 사용된 정책 태그에 할당합니다.

<u>GUI에서 다음과 같이 표시되어야 합니다.</u>

Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로파일) > Tags(태그)로 이동합니다. Policy tags(정책 태그) 탭에서 사용된 태그를 생성(또는 선택)하고 1-2단계에서 정의한 WLAN 및 정책 프로필을 할당합니다.



	Policy Tag Name
□	default-policy-tag

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*: default-policy-tag

Description: default policy-tag

WLAN-POLICY Maps: 1

	WLAN Profile	Policy Profile
□	DACL_DOT1X_SSID	DACL-8021X

1 - 1 of 1 items

RLAN-POLICY Maps: 0

CLI에서:

```
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
```

4단계. 공급업체별 특성 허용

다운로드 가능한 ACL은 ISE와 WLC 간의 RADIUS 교환에서 VSA(Vendor Specific Attributes)를 통해 전달됩니다. 이러한 특성의 지원은 WLC에서 이 CLI 명령을 사용하여 활성화할 수 있습니다.

CLI에서:

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

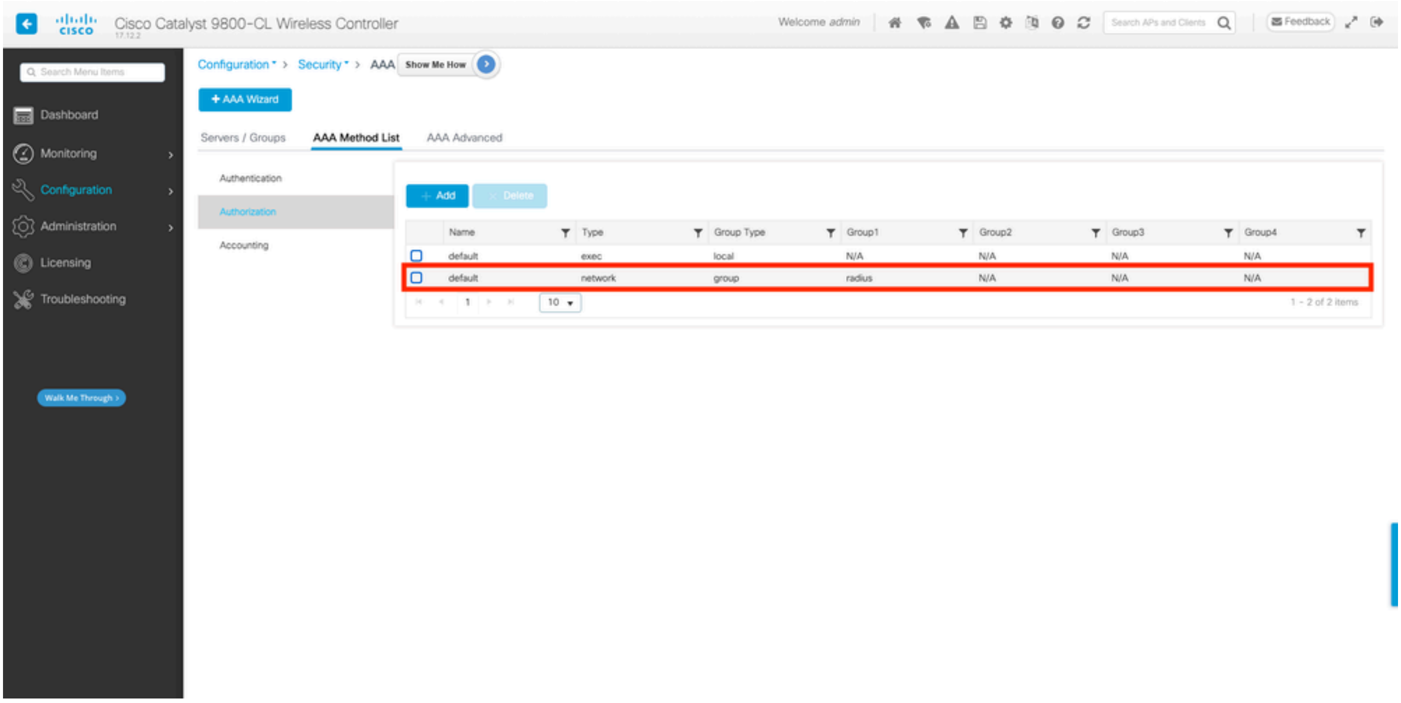
5단계. 기본 권한 부여 목록을 구성합니다.

dACL로 작업할 때 구성된 802.1x SSID에 대해 인증되는 모든 사용자에게 권한을 부여하려면 RADIUS를 통한 네트워크 권한 부여를 WLC에 적용해야 합니다. 실제로 인증뿐만 아니라 권한 부여 단계도 RADIUS 서버 측에서 처리됩니다. 따라서 이 경우 권한 부여 목록이 필요합니다.

기본 네트워크 권한 부여 방법이 9800 컨피그레이션의 일부인지 확인합니다.

GUI에서 다음과 같이 표시되어야 합니다.

Configuration(컨피그레이션) > Security(보안) > AAA로 이동하고 AAA Method List(AAA 메서드 목록) > Authorization(권한 부여) 탭에서 표시된 것과 유사한 권한 부여 메서드를 생성합니다.



	Name	Type	Group Type	Group1	Group2	Group3	Group4
□	default	exec	local	N/A	N/A	N/A	N/A
□	default	network	group	radius	N/A	N/A	N/A

CLI에서:

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

ISE 구성

ISE를 사용하는 무선 환경에서 dACL을 구현할 때 다음 두 가지 공통 컨피그레이션이 가능합니다.

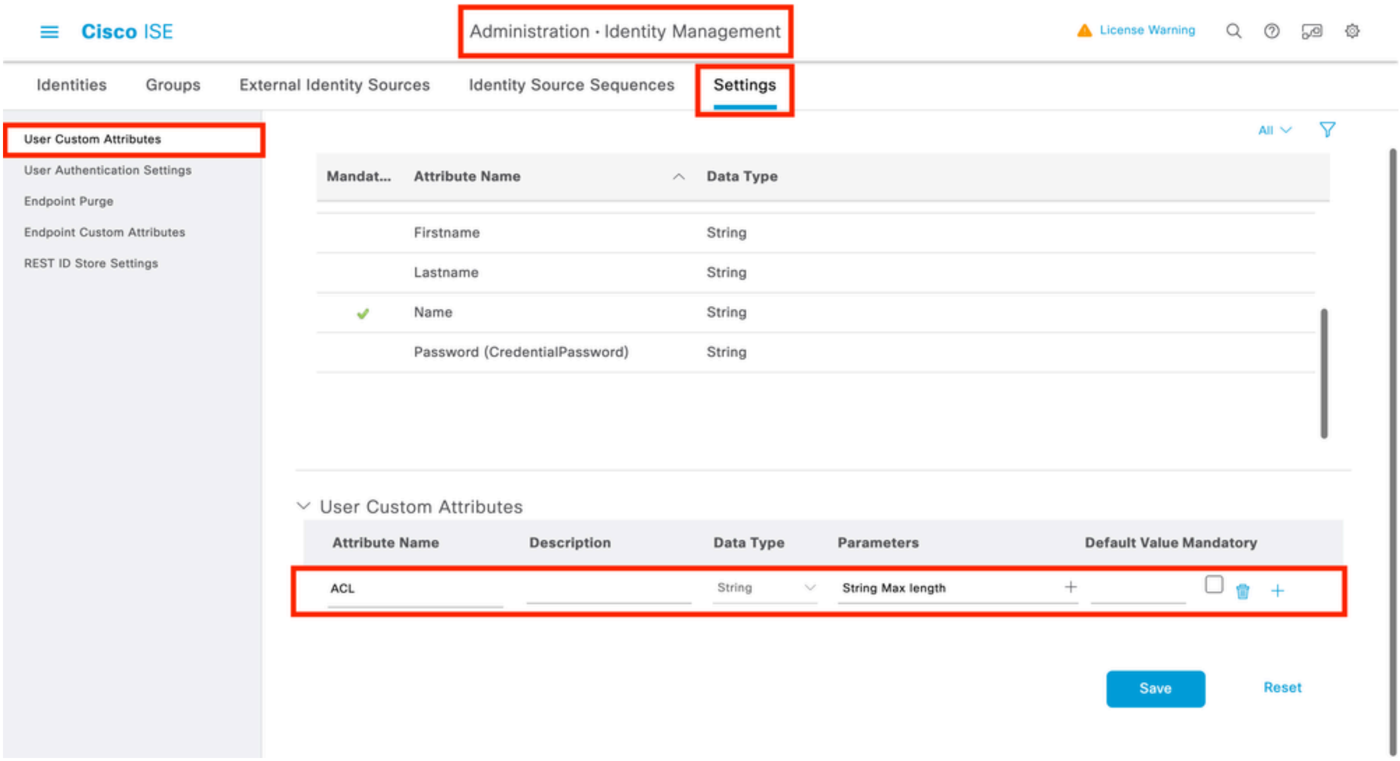
1. 사용자별 dACL 컨피그레이션 이를 통해 각 특정 ID에는 사용자 지정 ID 필드 덕분에 dACL이 할당됩니다.
2. 결과별 dACL 컨피그레이션 이 방법을 선택하는 동안 사용된 정책 집합과 일치하는 권한 부여 정책에 따라 특정 dACL이 사용자에게 할당됩니다.

사용자별 dACL

1단계. dACL 사용자 지정 사용자 특성 정의

사용자 ID에 dACL을 할당할 수 있으려면 먼저 생성된 ID에서 이 필드를 구성해야 합니다. 기본적으로 ISE에서 "ACL" 필드는 새로 생성된 ID에 대해 정의되지 않습니다. 이를 극복하기 위해 "Custom User Attribute(사용자 지정 사용자 특성)"를 사용하고 새 컨피그레이션 필드를 정의할 수 있습니다. 이렇게 하려면 Administration(관리) > Identity Management(ID 관리) > Settings(설정) > User

Custom Attributes(사용자 지정 특성)로 이동합니다. "+" 버튼을 사용하여 표시된 것과 유사한 새 속성을 추가합니다. 이 예에서 사용자 지정 특성의 이름은 ACL입니다.


Cisco ISE
Administration · Identity Management
License Warning
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
User Custom Attributes
User Authentication Settings
Endpoint Purge
Endpoint Custom Attributes
REST ID Store Settings
All
User Custom Attributes
Save
Reset

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

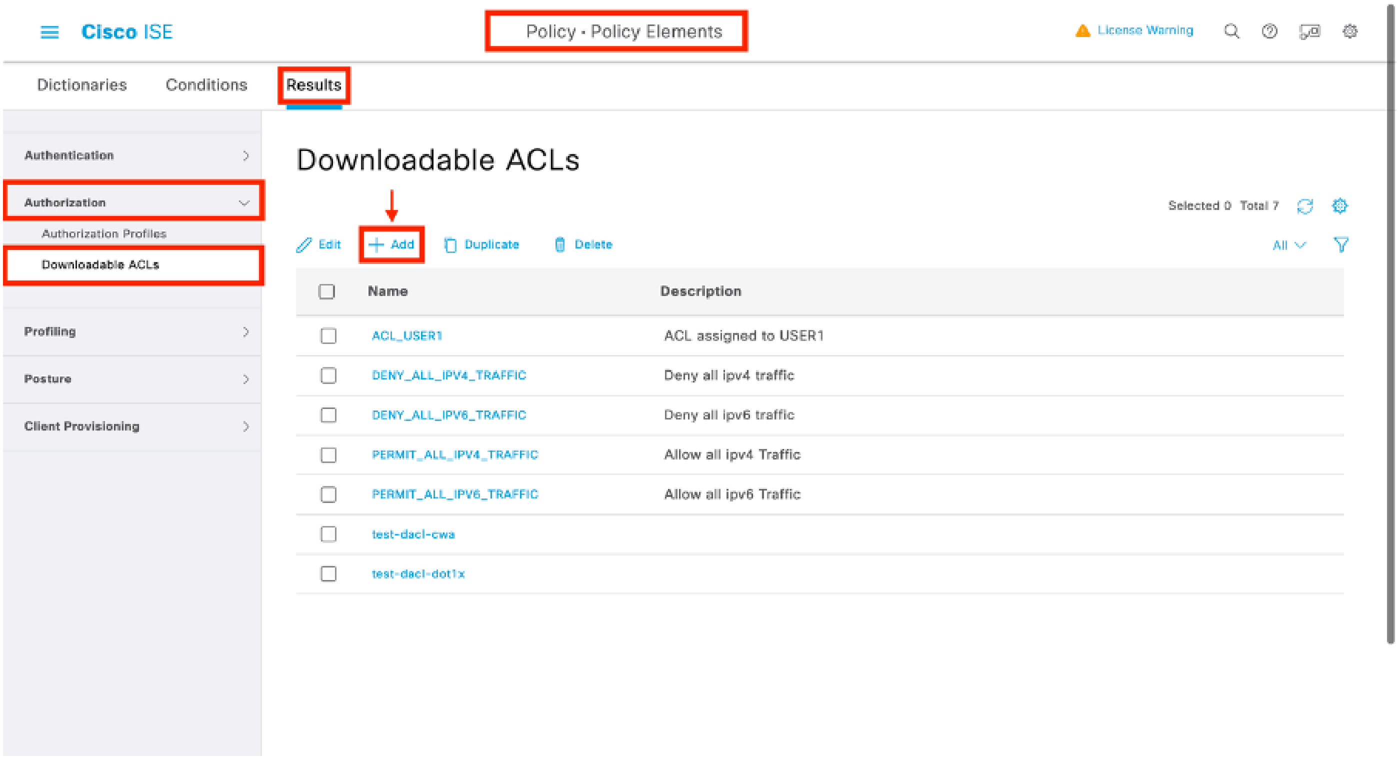
User Custom Attributes

Attribute Name	Description	Data Type	Parameters	Default Value	Mandatory
ACL		String	String Max length +		□

구성이 완료되면 "Save(저장)" 버튼을 사용하여 변경 사항을 저장합니다.

2단계. dACL 구성

Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Downloadable ACLs(다운로드 가능 ACL)로 이동하여 ISE에서 dACL을 보고 정의합니다. "Add(추가)" 버튼을 사용하여 새 항목을 생성합니다.



☐	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	

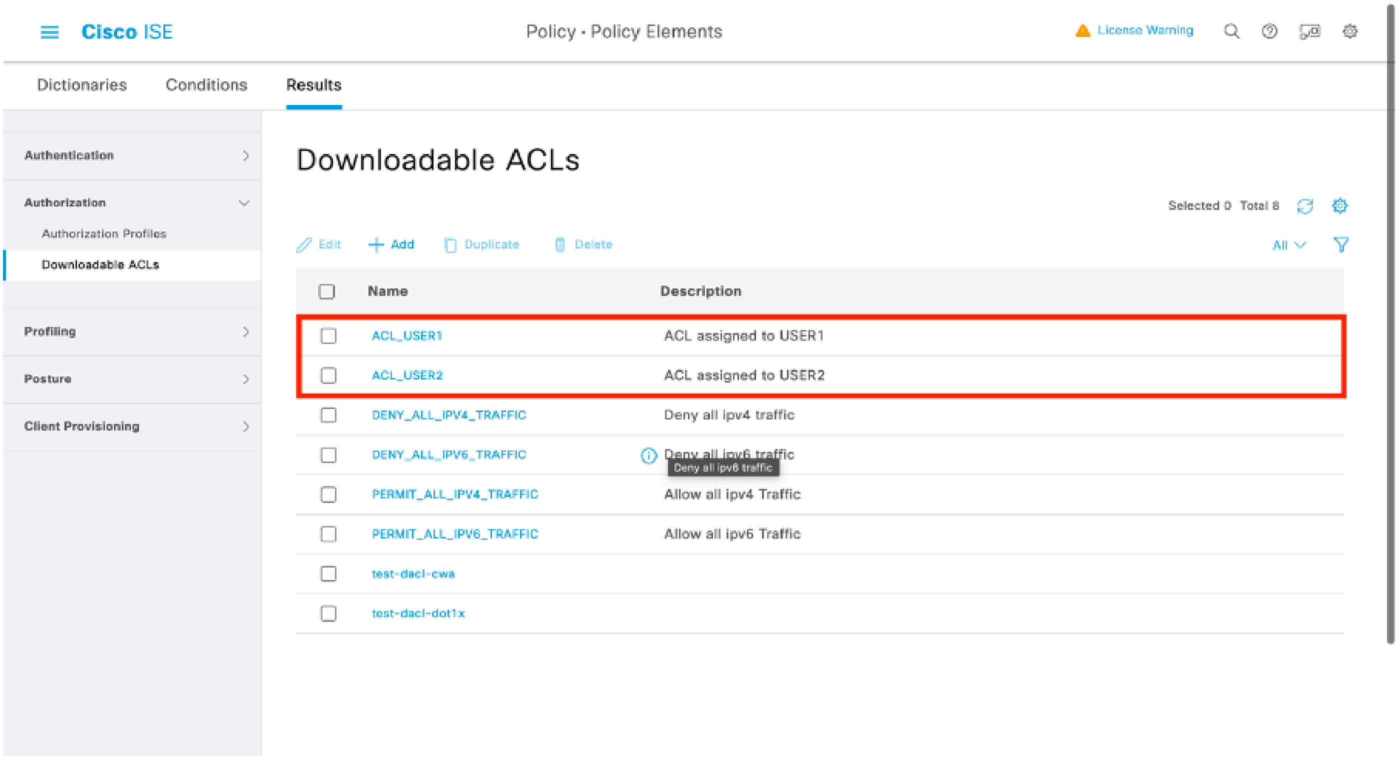
이렇게 하면 "새 다운로드 가능 ACL" 컨피그레이션 양식이 열립니다. 이 필드에서 다음 필드를 구성합니다.

- Name(이름): 정의된 dACL의 이름입니다.
- 설명(선택 사항): 생성된 dACL 사용에 대한 간략한 설명입니다.
- IP version(IP 버전): 정의된 dACL에 사용되는 IP 프로토콜 버전(버전 4, 6 또는 둘 다)입니다.
- DACL Content(DACL 콘텐츠): Cisco IOS XE ACL 구문에 따른 dACL의 내용입니다.

이 문서에서 사용된 dACL은 "ACL_USER1"이며 이 dACL은 10.48.39.186 및 10.48.39.13으로 대상 트래픽을 제외한 모든 트래픽을 허용합니다.

필드가 구성되었으면 "Submit(제출)" 버튼을 사용하여 dACL을 생성합니다.

그림과 같이 두 번째 사용자 ACL_USER2에 대해 dACL을 정의하려면 이 단계를 반복합니다.



Cisco ISE — Policy · Policy Elements — License Warning

Dictionaries | Conditions | Results

Authentication
Authorization
- Authorization Profiles
- Downloadable ACLs

Profiling
Posture
Client Provisioning

Downloadable ACLs

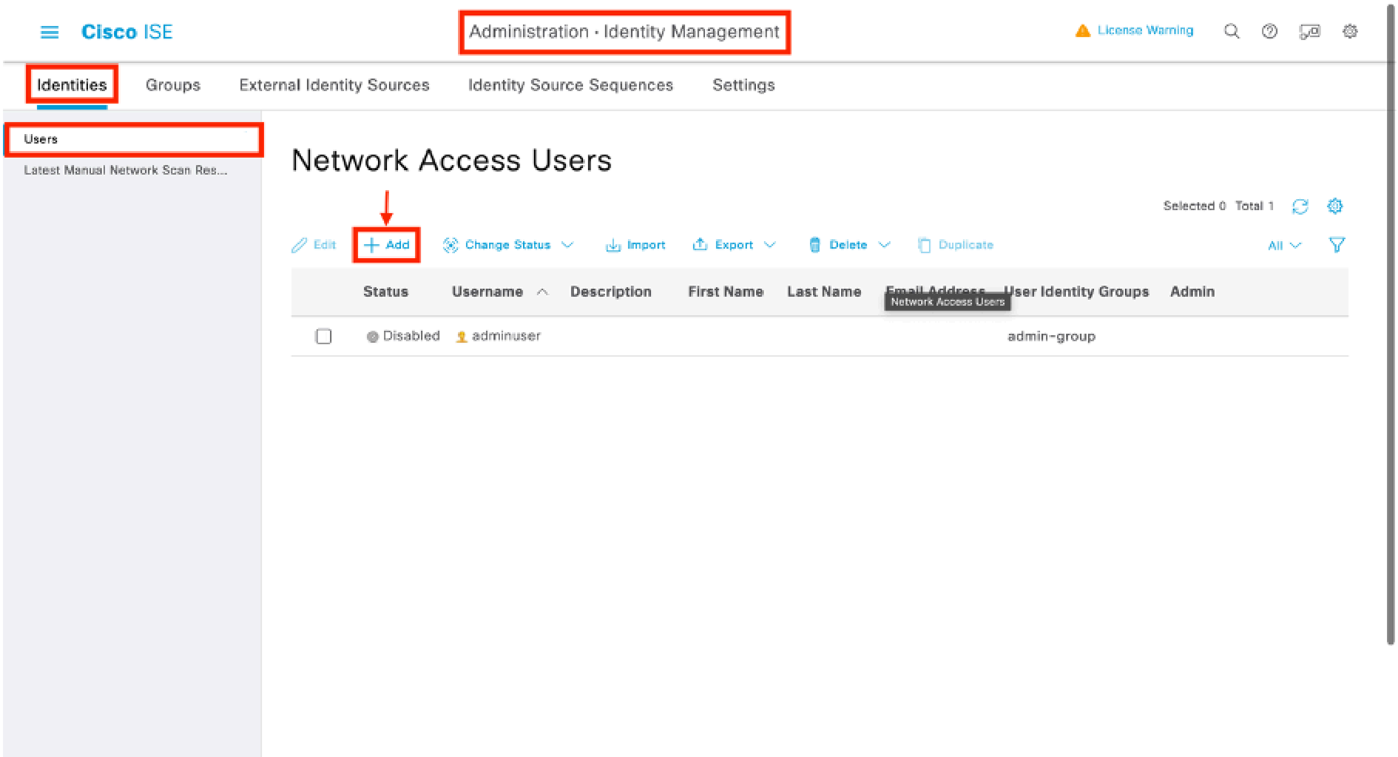
Selected 0 Total 8

Edit | + Add | Duplicate | Delete | All

☐	Name	Description
☐	ACL_USER1	ACL assigned to USER1
☐	ACL_USER2	ACL assigned to USER2
☐	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	

3단계. 생성된 ID에 dACL 할당

dACL이 생성되면 1단계에서 생성한 사용자 지정 특성을 사용하여 모든 ISE ID에 이를 할당할 수 있습니다. 이렇게 하려면 Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자)로 이동합니다. 평소와 같이 "Add(추가)" 버튼을 사용하여 사용자를 생성합니다.



Cisco ISE — Administration · Identity Management — License Warning

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

Users
Latest Manual Network Scan Res...

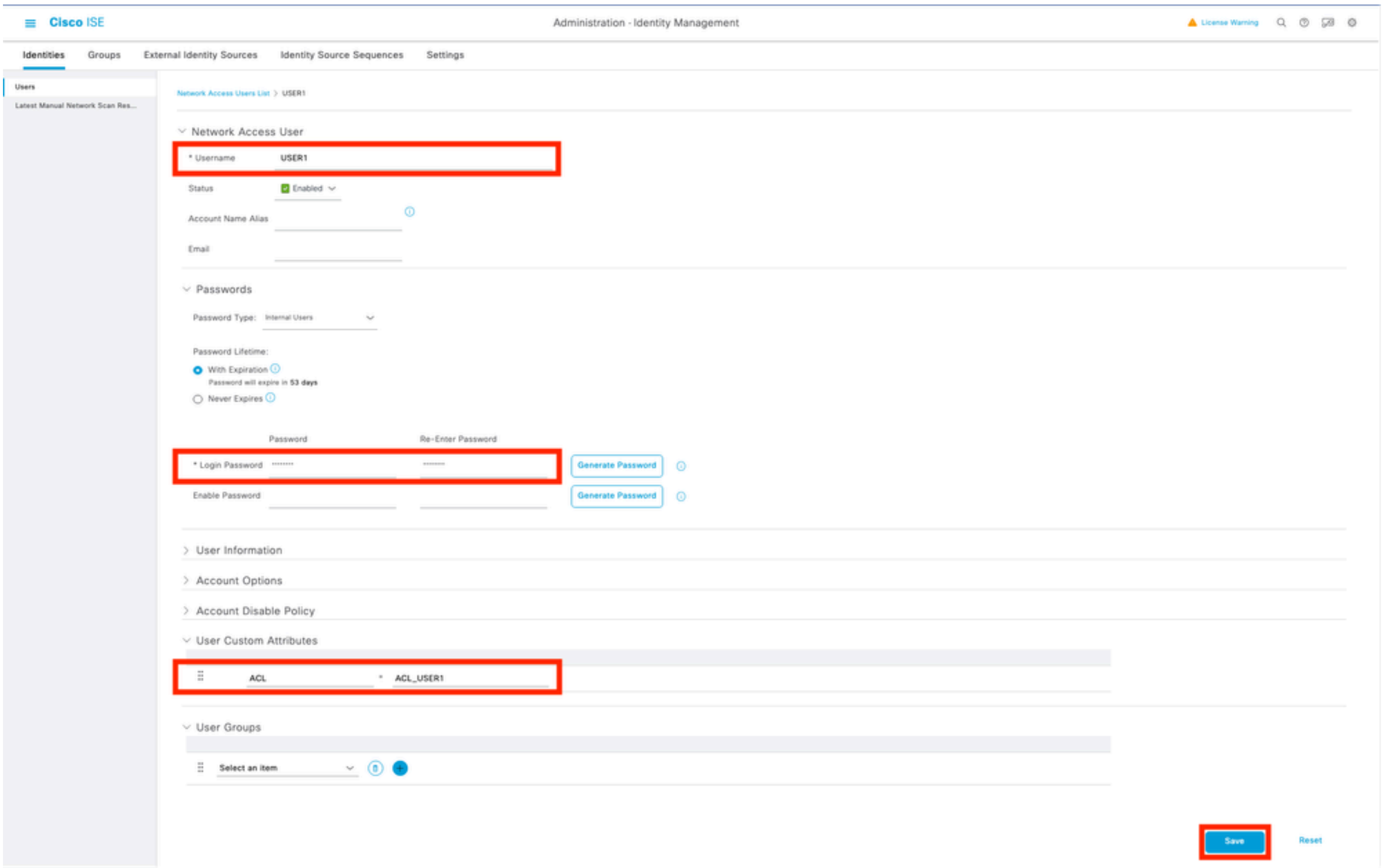
Network Access Users

Selected 0 Total 1

Edit | + Add | Change Status | Import | Export | Delete | Duplicate | All

☐	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
☐	Disabled	adminuser					admin-group	

"New Network Access User(새 네트워크 액세스 사용자)" 컨피그레이션 양식에서 생성된 사용자의 사용자 이름 및 비밀번호를 정의합니다. 사용자 지정 특성 "ACL"을 사용하여 2단계에서 생성한 dACL을 ID에 할당합니다. 이 예에서는 ACL_USER1을 사용하는 ID USER1이 정의됩니다.



Cisco ISE
Administration - Identity Management
License Warning
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Res...
Network Access Users List > USER1

Network Access User

* Username: USER1

Status: Enabled

Account Name Alias:

Email:

Passwords

Password Type: Internal Users

Password Lifetime:

● With Expiration
Password will expire in 53 days

○ Never Expires

	Password	Re-Enter Password
* Login Password	••••••••	••••••••
Enable Password		

Generate Password
Generate Password
User Information
Account Options
Account Disable Policy

User Custom Attributes

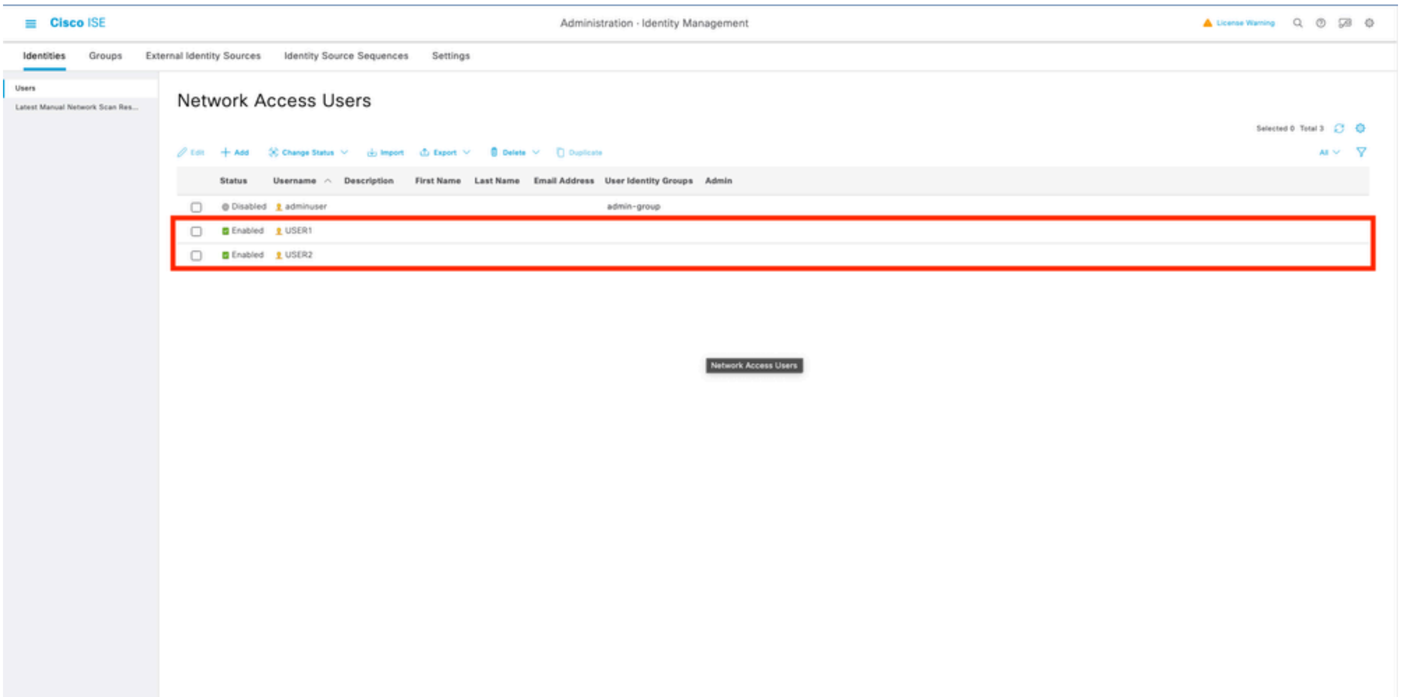
ACL = ACL_USER1

User Groups

Select an item

필드가 올바르게 구성되면 "Submit(제출)" 버튼을 사용하여 ID를 생성합니다.

USER2를 생성하고 ACL_USER2를 할당하려면 이 단계를 반복합니다.



Network Access Users

Selected 0 Total 3

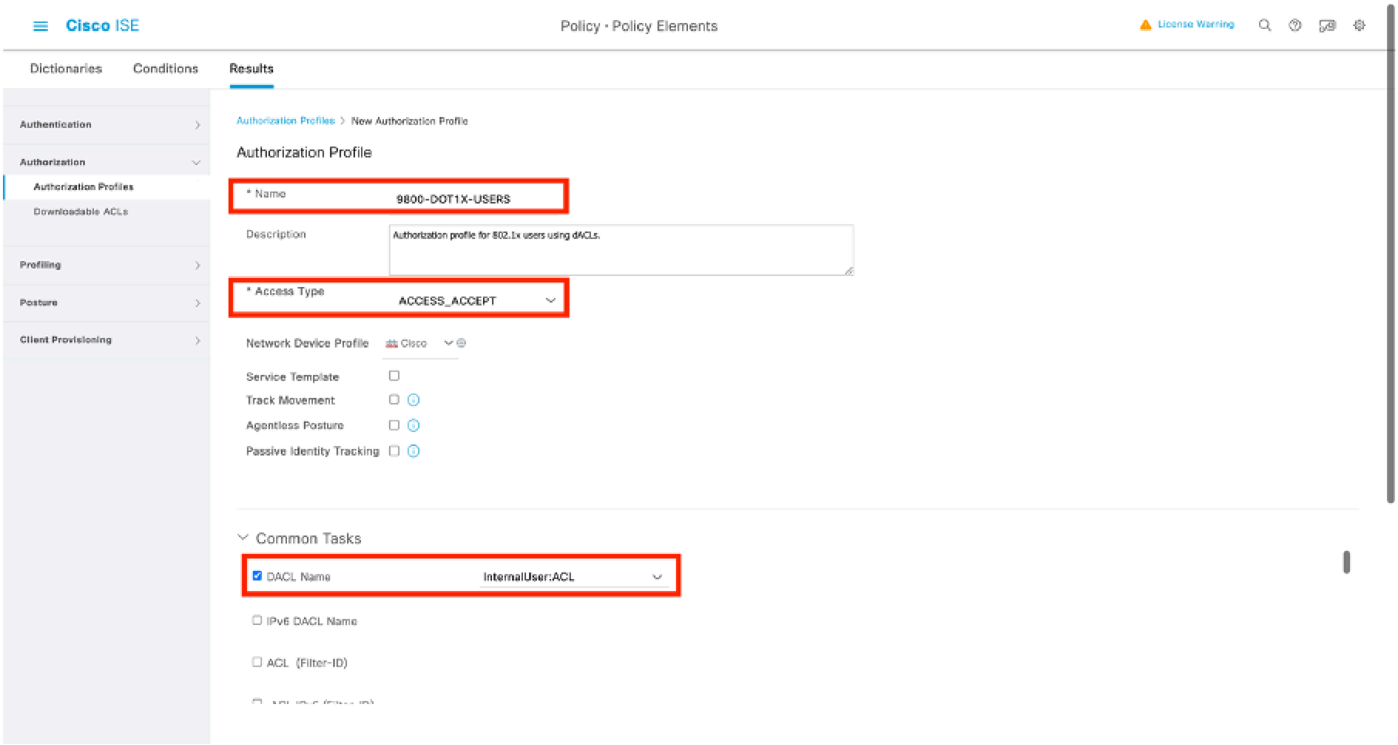
	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
☐	Disabled	adminuser					admin-group	
☐	Enabled	USER1						
☐	Enabled	USER2						

4단계. 권한 부여 정책 결과를 구성합니다.

ID가 구성되고 dACL이 할당되면 기존 권한 부여 공통 작업에 정의된 사용자 지정 사용자 특성 "ACL"과 매칭하려면 권한 부여 정책을 계속 구성해야 합니다. 이렇게 하려면 정책 > 정책 구성 요소

> 결과 > 권한 부여 > 인증 프로파일로 이동합니다. "Add(추가)" 버튼을 사용하여 새 권한 부여 정책을 정의합니다.

- Name(이름): 권한 부여 정책의 이름(여기서는 "9800-DOT1X-USERS")입니다.
- Access Type(액세스 유형): 이 정책이 일치할 때 사용되는 액세스 유형(ACCESS_ACCEPT)입니다.
- 일반 작업: 내부 사용자의 경우 "DACL Name"을 InternalUser:<사용자 지정 특성의 이름이 생성됨>과 일치시킵니다.이 문서에 사용된 이름에 따라 프로필 9800-DOT1X-USERS는 InternalUser:ACL로 구성된 dACL로 구성됩니다.



Authorization Profile

* Name 9800-DOT1X-USERS

Description Authorization profile for 802.1x users using dACLs.

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Common Tasks

☑ DACL Name InternalUser:ACL

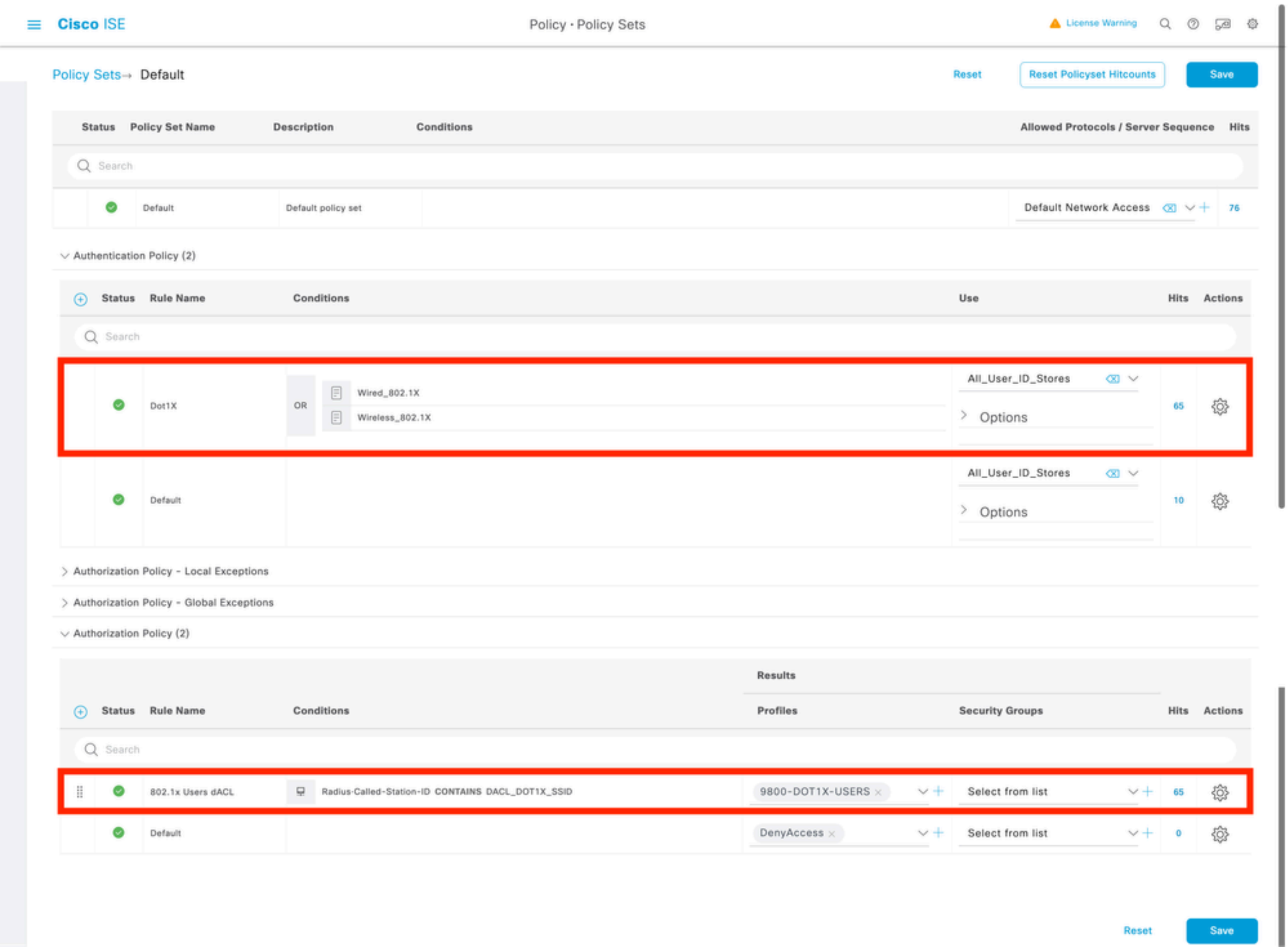
☐ IPv6 DACL Name

☐ ACL (Filter-ID)

5단계. 정책 집합에서 권한 부여 프로파일을 사용합니다.

권한 부여 프로파일 결과가 올바르게 정의되면, 무선 사용자를 인증하고 권한을 부여하는 데 사용되는 정책 세트의 일부여야 합니다. Policy(정책) > Policy Sets(정책 세트)로 이동하여 사용된 정책 세트를 엽니다.

여기서 인증 정책 규칙 "Dot1X"는 유선 또는 무선 802.1x를 통해 이루어지는 모든 연결과 일치합니다. 권한 부여 정책 규칙 "802.1x Users dACL"은 사용되는 SSID(즉, Radius-Called-Station-ID는 DACL_DOT1X_SSID를 포함함)에 대한 조건을 구현합니다. "DACL_DOT1X_SSID" WLAN에서 권한 부여를 수행하는 경우 4단계에서 정의된 "9800-DOT1X-USERS" 프로파일이 사용자에게 권한을 부여하는 데 사용됩니다.



Policy Sets→ Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	76

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	65	
✓	Default		All_User_ID_Stores Options	10	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	802.1x Users dACL	Radius-Called-Station-ID CONTAINS DACL_DOT1X_SSID	9800-DOT1X-USERS	Select from list	65	
✓	Default		DenyAccess	Select from list	0	

결과당 dACL

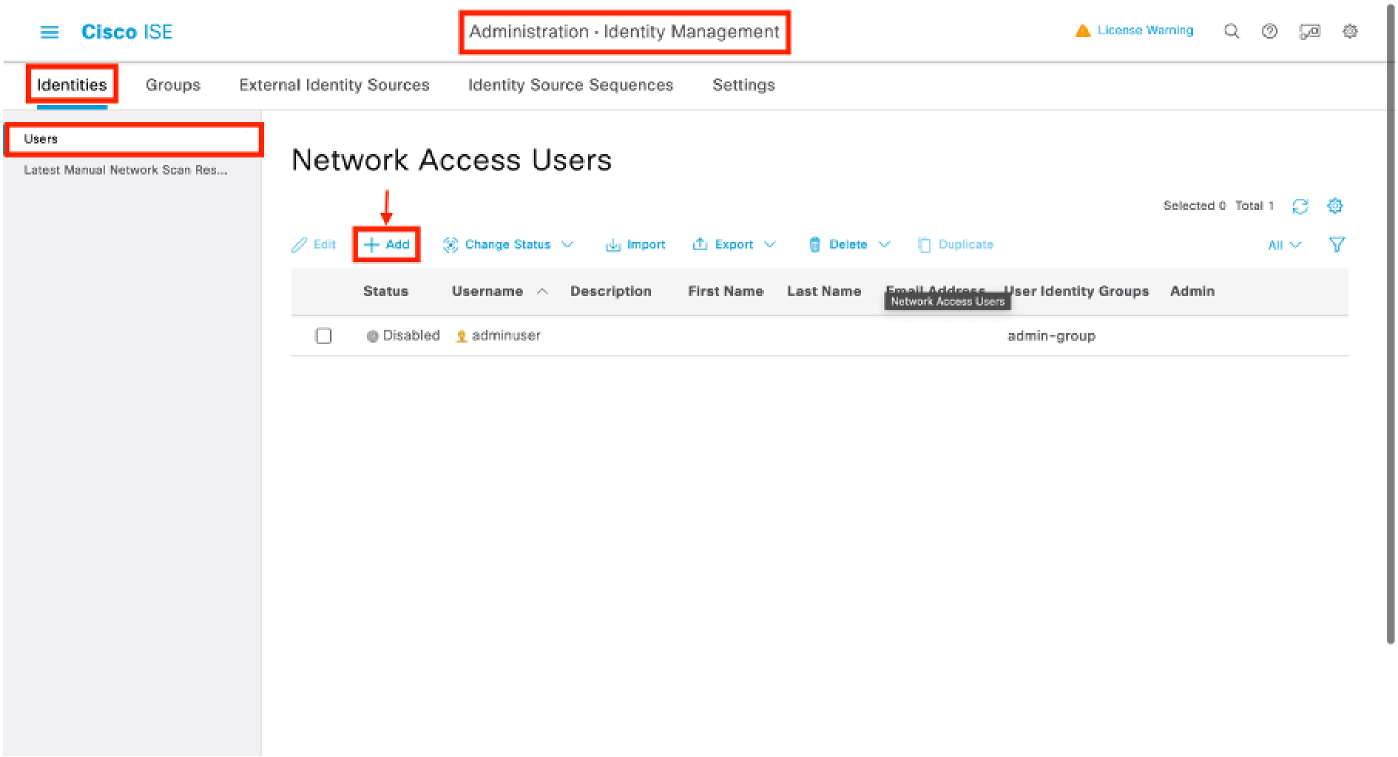
ISE에서 생성된 각 ID에 특정 dACL을 할당하는 엄청난 작업을 방지하기 위해 특정 정책 결과에 dACL을 적용하도록 선택할 수 있습니다. 그런 다음 이 결과는 사용된 정책 세트의 권한 부여 규칙과 일치하는 조건을 기반으로 적용됩니다.

1단계. dACL 구성

필요한 dACL을 정의하려면 Per-user dACLs(사용자별 dACL) 섹션에서 동일한 2단계를 실행합니다. ACL_USER1 및 ACL_USER2입니다.

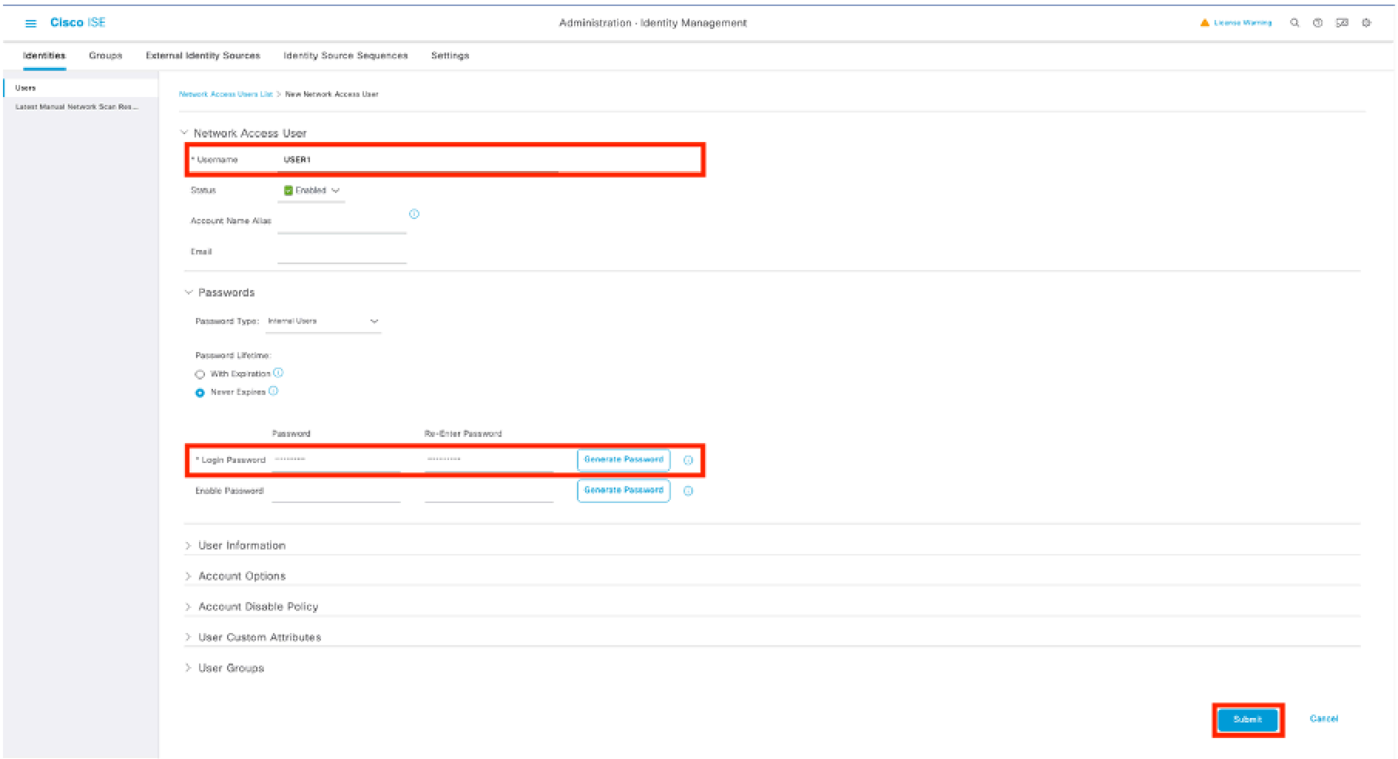
2단계. ID 생성

Administration(관리) > Identity Management(ID 관리) > Identities(ID) > Users(사용자)로 이동하고 "Add(추가)" 버튼을 사용하여 사용자를 생성합니다.



Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
Disabled	adminuser					admin-group	

"New Network Access User(새 네트워크 액세스 사용자)" 컨피그레이션 양식에서 생성된 사용자의 사용자 이름 및 비밀번호를 정의합니다.



* Username USER1

Status Enabled

Account Name Alias

Email

Password Type: Internal Users

Password Lifetime:

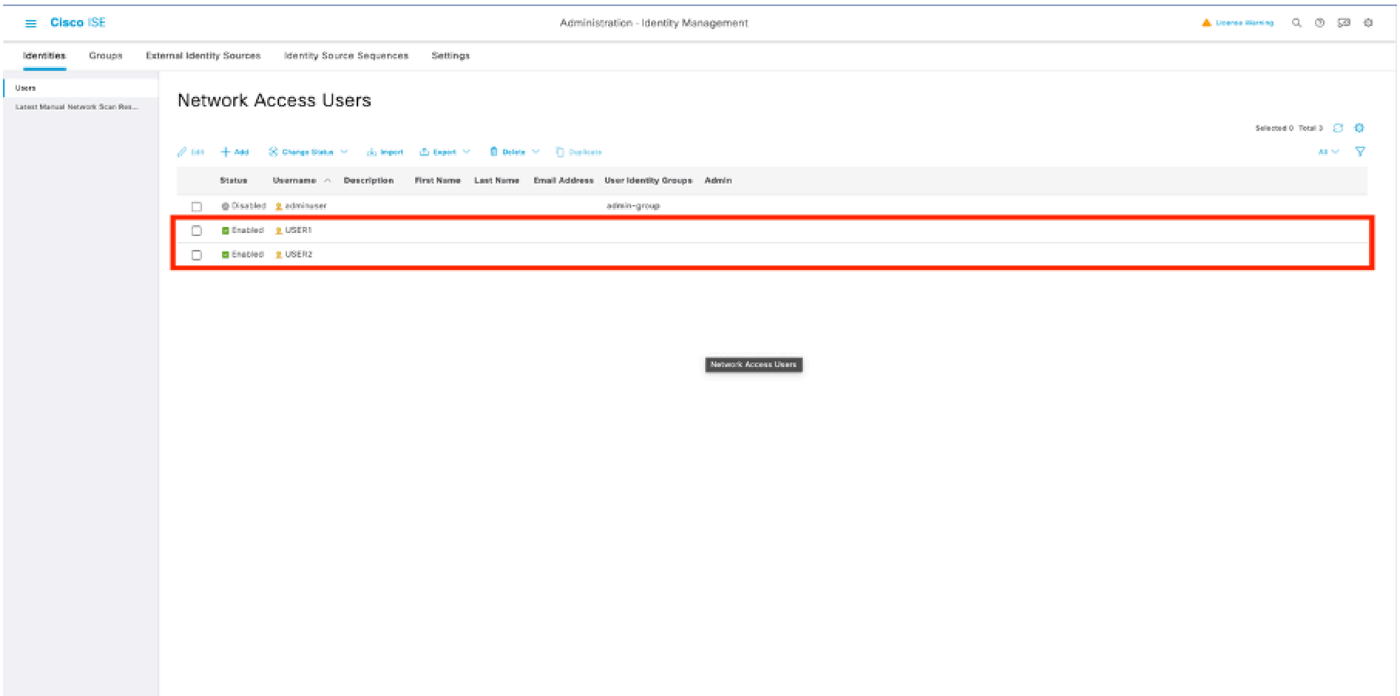
○ With Expiration

● Never Expires

* Login Password ········· ·········

Enable Password

USER2를 생성하려면 이 단계를 반복합니다.



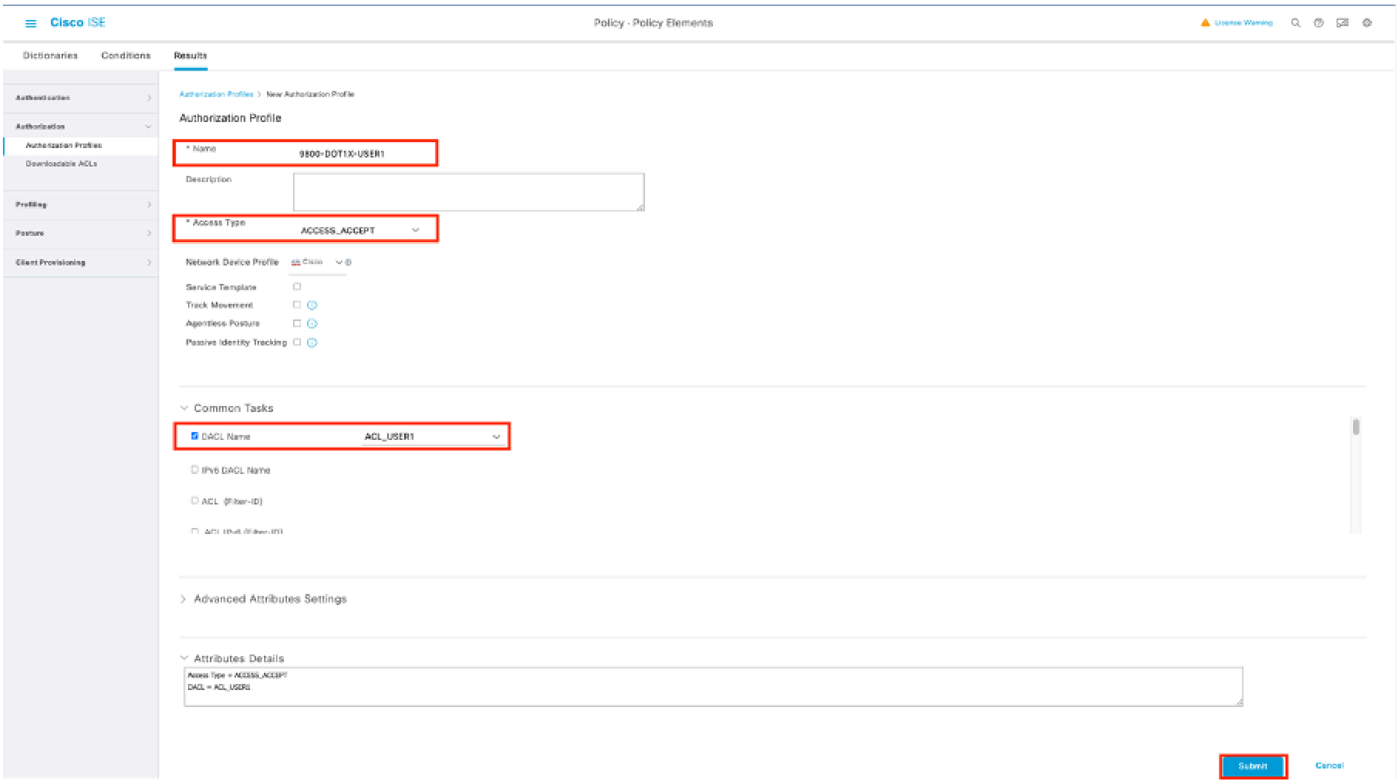
Network Access Users

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
□	Disabled	adminuser					admin-group	
□	Enabled	USER1						
□	Enabled	USER2						

4단계. 권한 부여 정책 결과를 구성합니다.

ID 및 dACL이 구성되었으면 이 정책을 사용하기 위해 조건과 일치하는 사용자에게 특정 dACL을 할당하려면 권한 부여 정책을 계속 구성해야 합니다. 이렇게 하려면 정책 > 정책 구성 요소 > 결과 > 인증 > 인증 프로파일로 이동 합니다. "Add(추가)" 버튼을 사용하여 새 권한 부여 정책을 정의하고 이 필드를 완성합니다.

- Name(이름): 권한 부여 정책의 이름(여기서는 "9800-DOT1X-USER1")입니다.
- 액세스 유형: 이 정책이 일치할 때 사용되는 액세스 유형(여기서는 ACCESS_ACCEPT)입니다.
- 일반 작업: 내부 사용자의 경우 "DACL Name"을 "ACL_USER1"과 일치시킵니다. 이 문서에 사용된 이름에 따라 프로파일 9800-DOT1X-USER1은 "ACL_USER1"로 구성된 dACL로 구성됩니다.



Authorization Profile

* Name 9800-DOT1X-USER1

Description

* Access Type ACCESS_ACCEPT

Network Device Profile Cisco

Service Template □

Track Movement □

Agentless Posture □

Passive Identity Tracking □

Common Tasks

☑ DACL Name ACL_USER1

□ IPv6 DACL Name

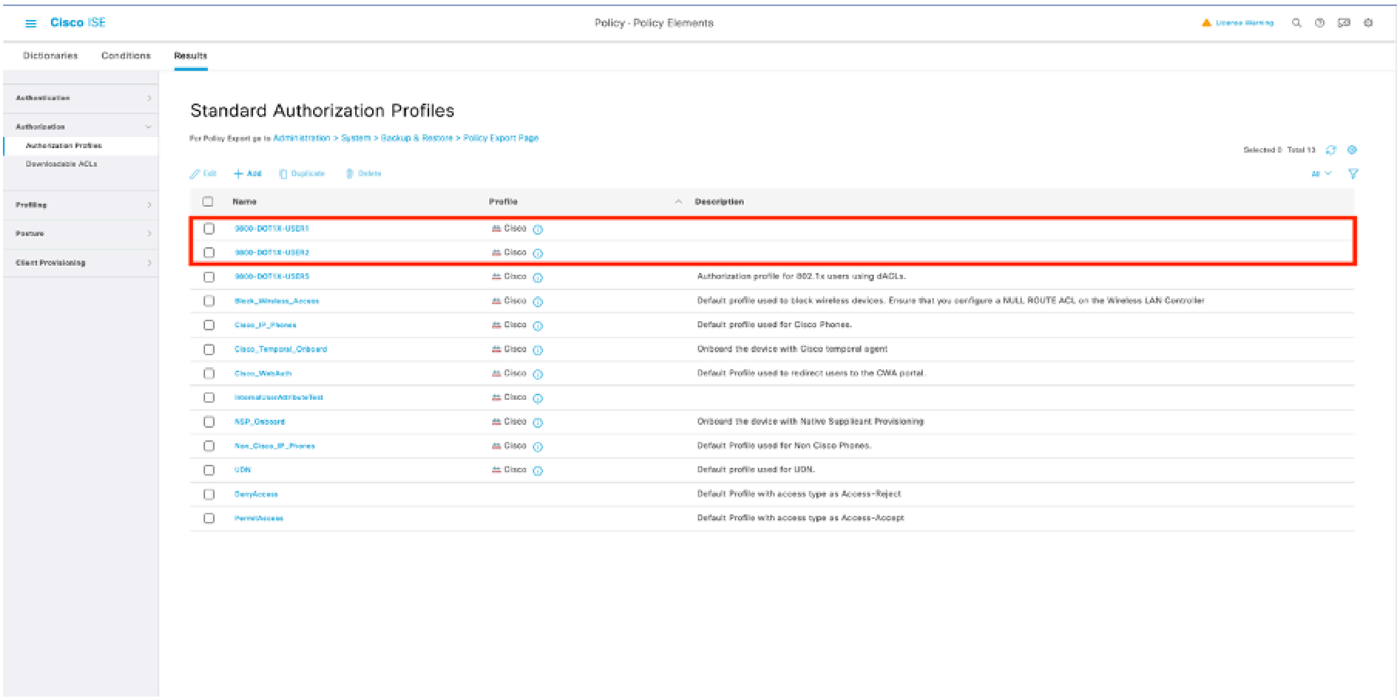
□ ACL (Filter-ID)

Advanced Attributes Settings

Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = ACL_USER1
```

이 단계를 반복하여 정책 결과 "9800-DOT1X-USER2"를 생성하고 DACL로 "ACL_USER2"를 할당합니다.



Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

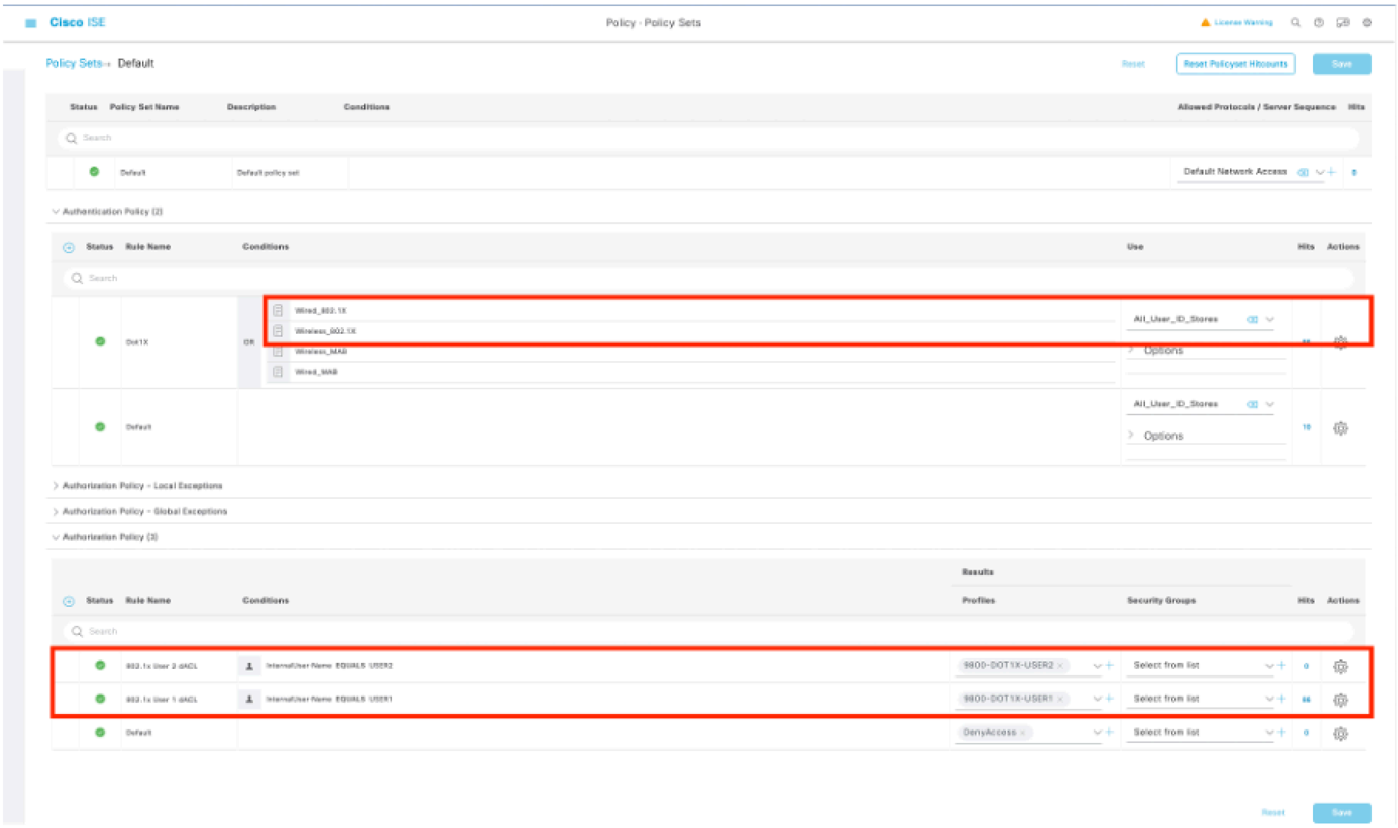
Name	Profile	Description
9800-DOT1X-USER1	Cisco	
9800-DOT1X-USER2	Cisco	
9800-DOT1X-USERS	Cisco	Authorization profile for 802.1x users using dACLs.
Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure a NULL ROUTE ACL on the Wireless LAN Controller
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
InternalUserAttributeTest	Cisco	
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
UDN	Cisco	Default profile used for UDN.
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

5단계. 정책 집합에서 권한 부여 프로파일을 사용합니다.

권한 부여 프로파일이 올바르게 정의되면 무선 사용자를 인증하고 권한을 부여하는 데 사용되는 정책 세트의 일부여야 합니다. Policy(정책) > Policy Sets(정책 세트)로 이동하여 사용된 정책 세트를 엽니다.

여기서 인증 정책 규칙 "Dot1X"는 유선 또는 무선 802.1X를 통해 연결 된 모든 일치 합니다. 권한 부여 정책 규칙 "802.1X User 1 dACL"은 사용된 사용자 이름에 대한 조건을 구현합니다(InternalUser-

Name CONTAINS USER1). 사용자 이름 USER1을 사용하여 권한 부여를 수행하는 경우, 4단계에서 정의된 프로파일 "9800-DOT1X-USER1"을 사용하여 사용자에게 권한을 부여하므로 이 결과의 dACL(ACL_USER1)도 사용자에게 적용됩니다. "9800-DOT1X-USER1"이 사용되는 사용자 이름 USER2에 대해서도 동일하게 구성됩니다.



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	8

Authentication Policy (2)

Status	Rule Name	Conditions		Use	Hits	Actions
●	Dot1X	OR	Wired_802.1X Wireless_802.1X Wireless_MAB Wired_MAB	All_User_ID_Stores Options	55	⚙
●	Default			All_User_ID_Stores Options	18	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (3)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	802.1x User 2 dACL	InternalUser·Name EQUALS USER2	9800-DOT1X-USER2	Select from list	0	⚙
●	802.1x User 1 dACL	InternalUser·Name EQUALS USER1	9800-DOT1X-USER1	Select from list	66	⚙
●	Default		DenyAccess	Select from list	0	⚙

CWA SSID와 함께 dACL 사용에 대한 참고 사항

Catalyst 9800 WLC 및 ISE 컨피그레이션 가이드에서 CWA(Configure Central Web Authentication)에 설명된 것처럼, CWA는 MAB 및 특정 결과를 사용하여 사용자를 인증하고 권한을 부여합니다. 위에서 설명한 것과 동일하게 다운로드 가능한 ACL을 ISE 측에서 CWA 컨피그레이션에 추가할 수 있습니다.

경고: 다운로드 가능한 ACL은 네트워크 액세스 목록으로만 사용할 수 있으며 사전 인증 ACL로 지원되지 않습니다. 따라서 CWA 워크플로에서 사용되는 모든 사전 인증 ACL은 WLC 컨피그레이션에서 정의해야 합니다.

다음을 확인합니다.

컨피그레이션을 확인하기 위해 이 명령을 사용할 수 있습니다.

```
# 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 }
```

여기서는 이 예에 해당하는 WLC 컨피그레이션의 관련 부분을 참조합니다.

```
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
```

RADIUS 서버 컨피그레이션이 표시되며, show running-config all 명령을 사용하여 표시됩니다.

```
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
```

문제 해결

체크리스트

- 클라이언트가 구성된 802.1X SSID에 올바르게 연결할 수 있는지 확인합니다.
- RADIUS access-request/accept에 적절한 AVP(특성-값 쌍)가 포함되어 있는지 확인합니다.
- 클라이언트가 올바른 WLAN/정책 프로필을 사용하는지 확인합니다.

WLC 원 스톱 샵 리플렉스

특정 무선 클라이언트에 dACL이 올바르게 할당되었는지 확인하려면 표시된 대로 **show wireless client mac-address <H.H.H> detail 명령**을 사용합니다. 여기에서 클라이언트 사용자 이름, 상태, 정책 프로필, WLAN 및 가장 중요한 부분인 ACS-ACL과 같은 다양한 유용한 문제 해결 정보를 볼 수 있습니다.

<#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 Show 명령

현재 Catalyst 9800 WLC 컨피그레이션의 일부인 모든 ACL을 보려면 **show access-lists 명령을** 사용할 수 있습니다. 이 명령은 로컬로 정의된 모든 ACL 또는 WLC에서 다운로드한 dACL을 나열합니다. WLC에 의해 ISE에서 다운로드 된 모든 dACL는 형식을 갖습니다 xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.

참고: 다운로드 가능한 ACL은 클라이언트가 연결되어 있고 무선 인프라에서 사용하는 한 컨피그레이션에 남아 있습니다. dACL을 사용하는 마지막 클라이언트가 인프라를 떠나자마자 dACL이 컨피그레이션에서 제거됩니다.

```
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
[...]
```

조건부 디버깅 및 무선 활성 추적

컨피그레이션의 문제를 해결하는 동안 정의된 dACL을 할당해야 하는 클라이언트에 대한 방사성 추적을 수집할 수 있습니다. 클라이언트 08be.ac14.137d에 대한 클라이언트 연결 프로세스 동안 방사성 추적의 흥미로운 부분을 보여주는 로그를 강조 표시합니다.

<#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 Associatio




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 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
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_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_900000012



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_90000
2024/03/28 10:43:04.727169069 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_90000


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◇«? %ÿ0?ã@≤™ÇÑbWï6\Ë&\q·lU+QB–º®”≠∫JÑv?"


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


[...]


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

```
2024/03/28 10:43:04.727513133 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_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_9000

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_90000

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 "#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 "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_9000
```

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

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

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 interface
2024/03/28 10:43:04.786523172 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interface
2024/03/28 10:43:04.787787313 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interface
2024/03/28 10:43:04.788160929 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interface
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:ca
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 : cl
```

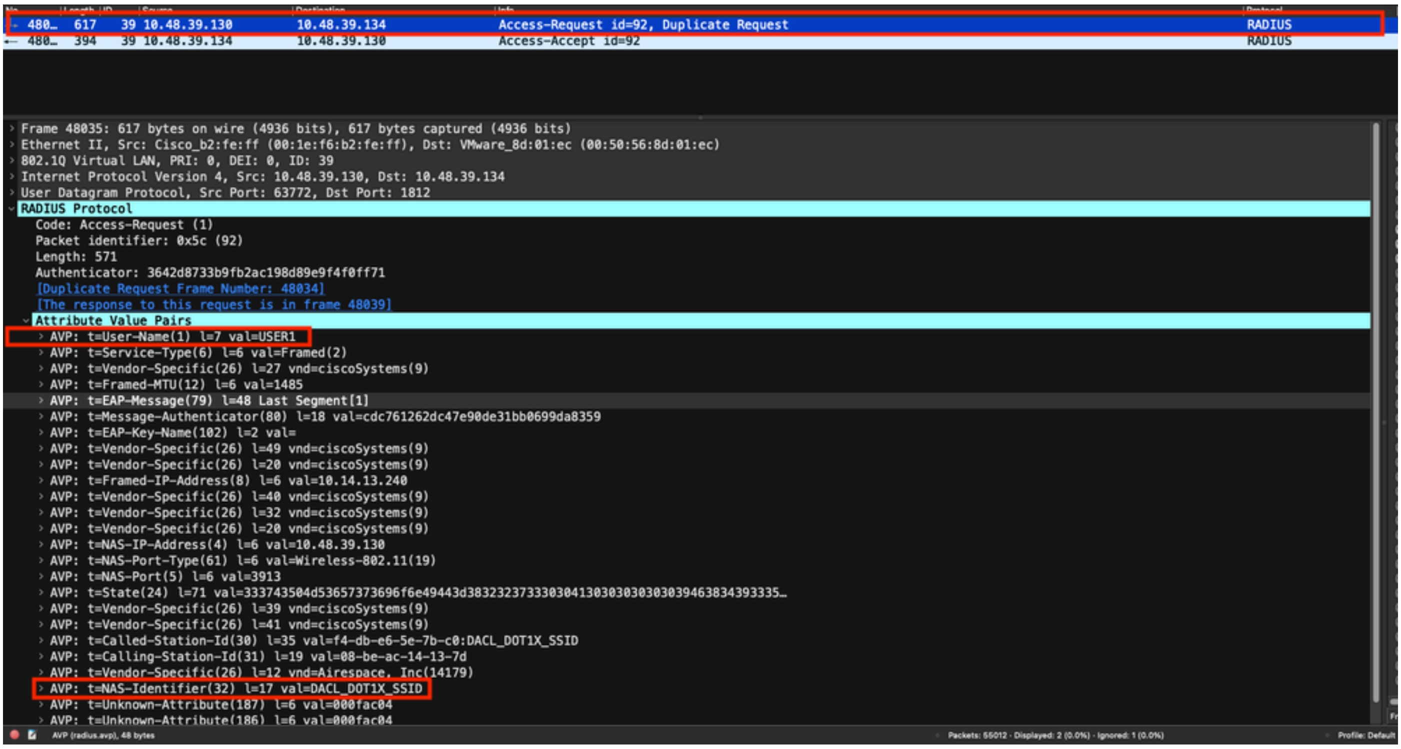
```
2024/03/28 10:43:04.789642576 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute :Cis

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
```

패킷 캡처

또 다른 흥미로운 반향은 클라이언트 연결을 위한 RADIUS 플로우의 패킷 캡처를 취하여 분석하는 것입니다. 다운로드 가능한 ACL은 RADIUS에 의존하며, 무선 클라이언트에 할당될 뿐만 아니라 WLC에 의해 다운로드됩니다. dACL 컨피그레이션 트러블슈팅을 위해 패킷 캡처를 수행하는 동안, RADIUS 서버와 통신하기 위해 컨트롤러에서 사용하는 인터페이스에서 캡처해야 합니다. 이 문서에서는 이 문서에서 분석한 캡처를 수집하는 데 사용된 Catalyst 9800에서 손쉽게 임베드된 패킷 캡처를 구성하는 방법을 보여줍니다.

RADIUS 클라이언트 인증

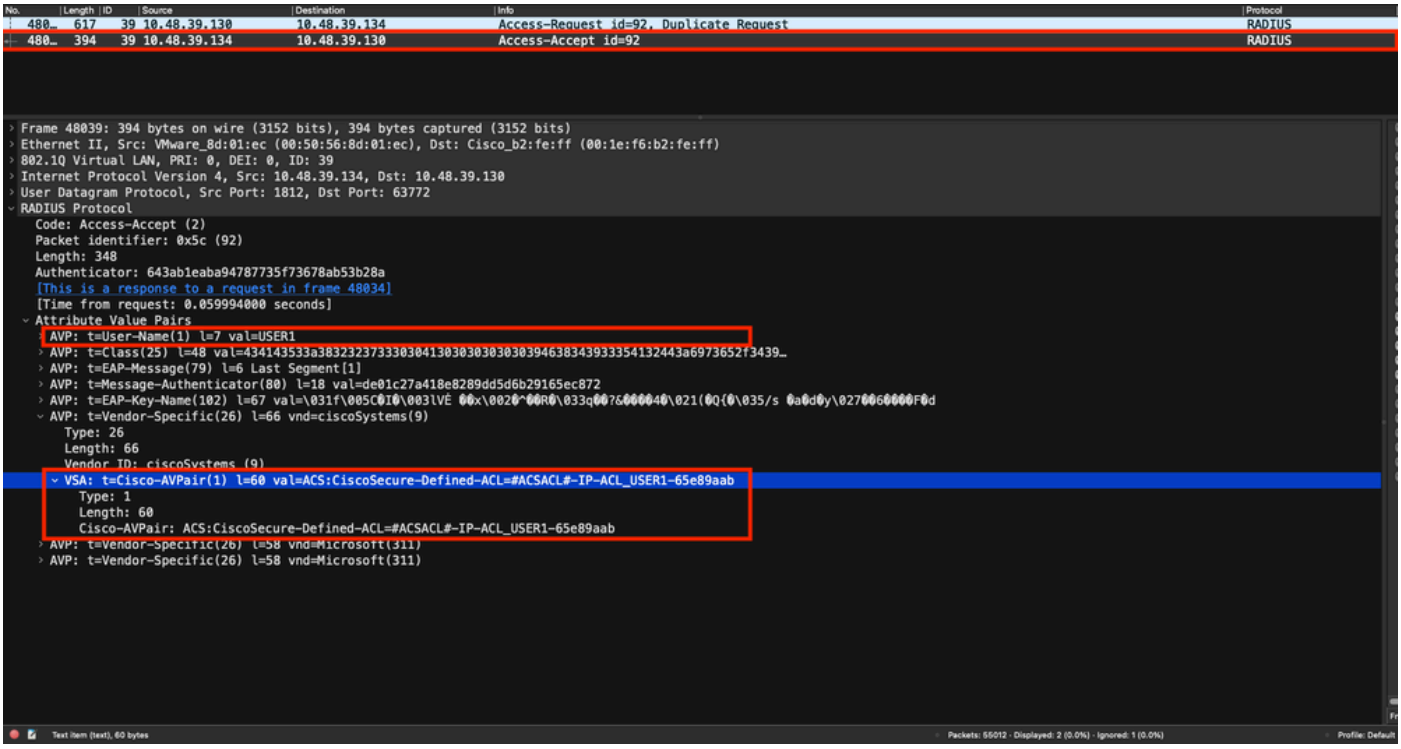
DACL_DOT1X_SSID SSID(AVP NAS-Identifier)에서 사용자 USER1(AVP User-Name)을 인증하기 위해 WLC에서 RADIUS 서버로 전송되는 클라이언트 RADIUS 액세스 요청을 볼 수 있습니다.



```
No.     |Length |ID  |Source          |Destination     |Info                                   |Protocol
→ 480…   617     39  10.48.39.130     10.48.39.134     Access-Request id=92, Duplicate Request   RADIUS
← 480…   394     39  10.48.39.134     10.48.39.130     Access-Accept id=92                       RADIUS

> Frame 48035: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits)
> Ethernet II, Src: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff), Dst: VMware_8d:01:ec (00:50:56:8d:01:ec)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.130, Dst: 10.48.39.134
> User Datagram Protocol, Src Port: 63772, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x5c (92)
    Length: 571
    Authenticator: 3642d8733b9fb2ac198d89e9f4f0ff71
    [Duplicate Request Frame Number: 48034]
    [The response to this request is in frame 48039]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=7 val=USER1
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=1485
    > AVP: t=EAP-Message(79) l=48 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=cdc761262dc47e90de31bb0699da8359
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=Framed-IP-Address(8) l=6 val=10.14.13.240
    > AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
    > AVP: t=NAS-IP-Address(4) l=6 val=10.48.39.130
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=NAS-Port(5) l=6 val=3913
    > AVP: t=State(24) l=71 val=333743504d53657373696f6e49443d38323237333030413030303030303946383439335…
    > AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
    > AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
    > AVP: t=Called-Station-Id(30) l=35 val=f4-db-e6-5e-7b-c0:DACL_DOT1X_SSID
    > AVP: t=Calling-Station-Id(31) l=19 val=08-be-ac-14-13-7d
    > AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
    > AVP: t=NAS-Identifier(32) l=17 val=DACL_DOT1X_SSID
    > AVP: t=Unknown-Attribute(187) l=6 val=000fac04
    > AVP: t=Unknown-Attribute(186) l=6 val=000fac04
```

AVP (radius.avp), 48 bytes
Packets: 55012 · Displayed: 2 (0.0%) · Ignored: 1 (0.0%)
Profile: Default

인증이 성공하면 RADIUS 서버는 여전히 사용자 USER1(AVP User-Name) 및 AAA 특성, 특히 공급업체별 AVP ACS:CiscoSecure-Defined-ACL을 "#ACSACL#-IP-ACL_USER1-65e89aab"에 대해 access-accept로 응답합니다.

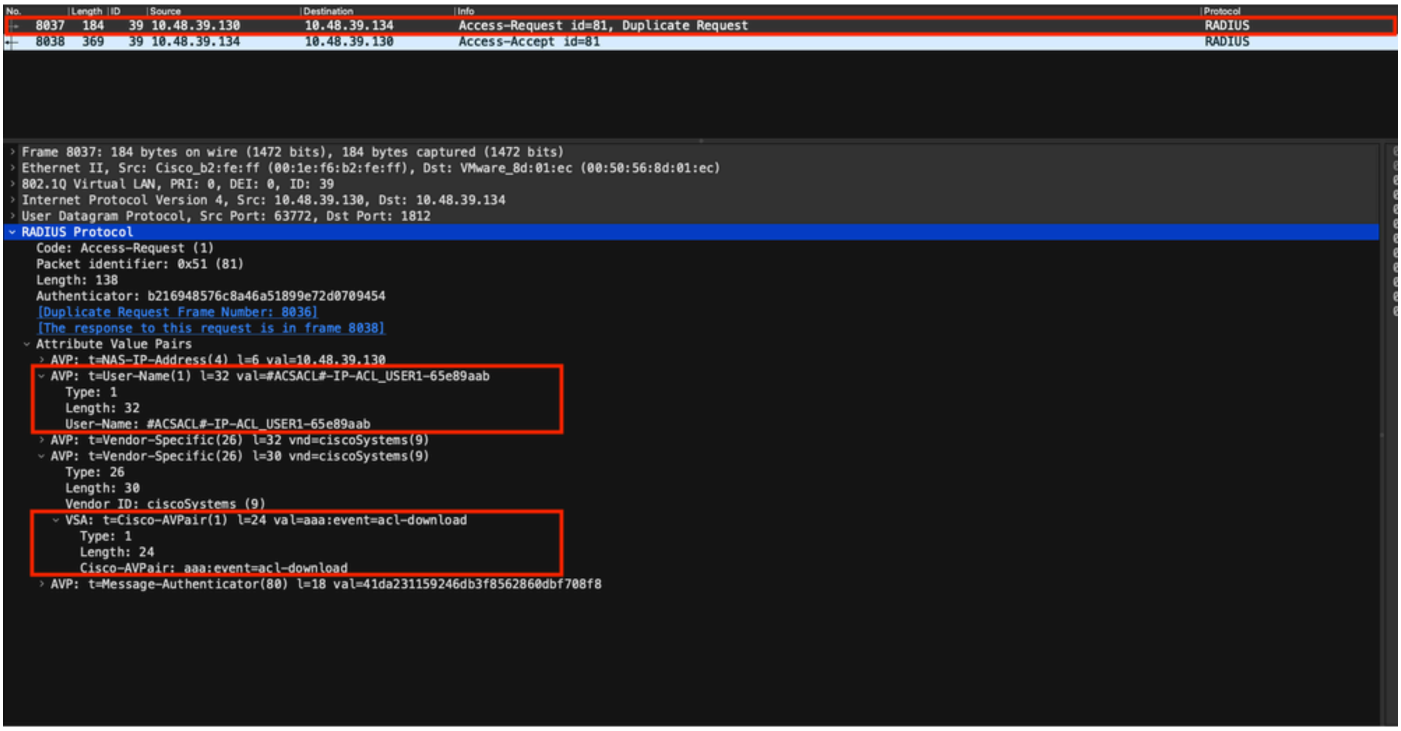


```
No.     |Length |ID  |Source          |Destination     |Info                                   |Protocol
  480…   617     39  10.48.39.130     10.48.39.134     Access-Request id=92, Duplicate Request   RADIUS
← 480…   394     39  10.48.39.134     10.48.39.130     Access-Accept id=92                       RADIUS

> Frame 48039: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
> Ethernet II, Src: VMware_8d:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130
> User Datagram Protocol, Src Port: 1812, Dst Port: 63772
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x5c (92)
    Length: 348
    Authenticator: 643ab1eaba94787735f73678ab53b28a
    [This is a response to a request in frame 48034]
    [Time from request: 0.059994000 seconds]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=7 val=USER1
    > AVP: t=Class(25) l=48 val=434143533a38323237333030413030303030303946383439333354132443a6973652f3439…
    > AVP: t=EAP-Message(79) l=6 Last Segment[1]
    > AVP: t=Message-Authenticator(80) l=18 val=de01c27a418e8289dd5d6b29165ec872
    > AVP: t=EAP-Key-Name(102) l=67 val=\031f\005C�I�\003lVÈ ��x\002�^��R�\033q��7&����4�\021(�Q{�\035/s �a�d�y\027��6����F�d
    v AVP: t=Vendor-Specific(26) l=66 vnd=ciscoSystems(9)
        Type: 26
        Length: 66
        Vendor ID: ciscoSystems (9)
      v VSA: t=Cisco-AVPair(1) l=60 val=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1-65e89aab
          Type: 1
          Length: 60
          Cisco-AVPair: ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1-65e89aab
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
    > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
```

Text item (text), 60 bytes
Packets: 55012 · Displayed: 2 (0.0%) · Ignored: 1 (0.0%)
Profile: Default

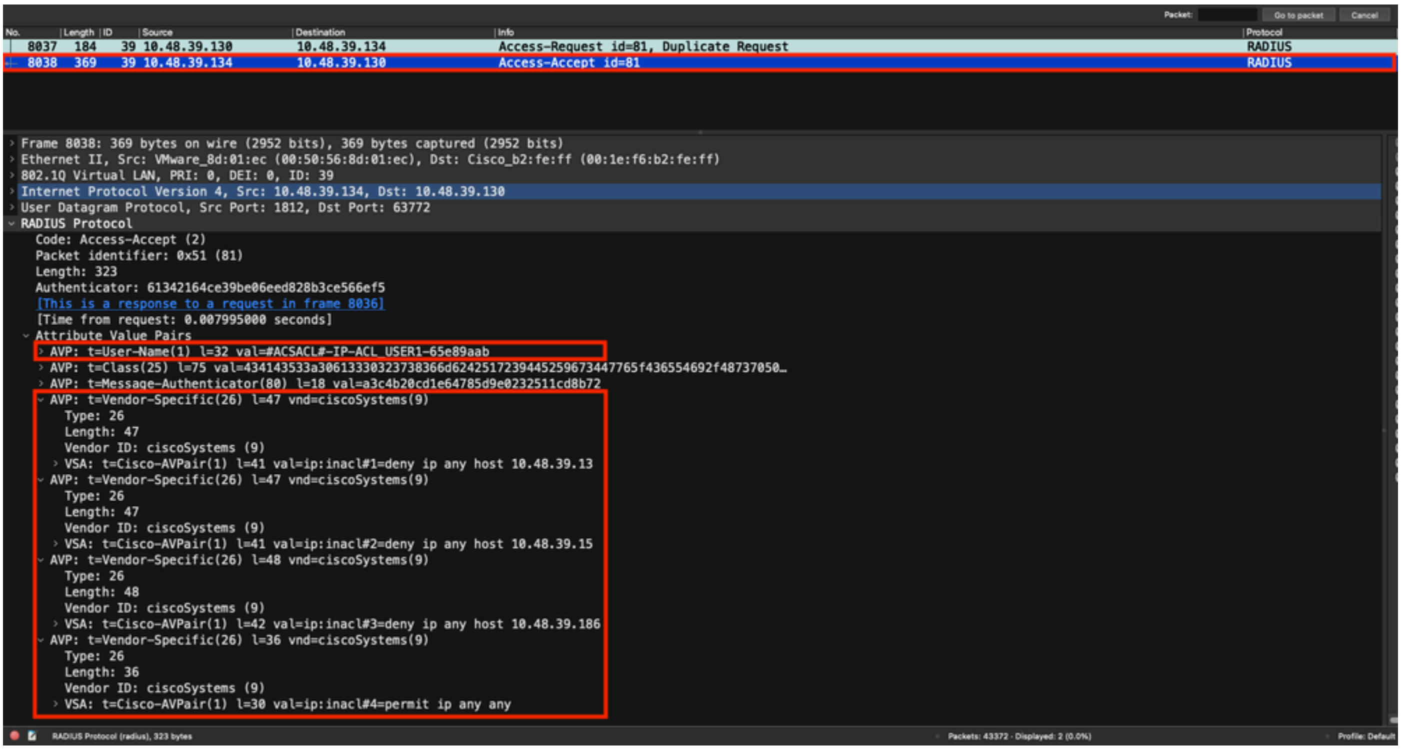
DACL 다운로드

dACL이 이미 WLC 컨피그레이션의 일부인 경우 사용자에게 간단하게 할당되고 RADIUS 세션이 종료됩니다. 그렇지 않은 경우 WLC는 ACL을 다운로드하며 RADIUS를 계속 사용합니다. 이를 위해 WLC는 이번에는 AVP User-Name에 dACL 이름("#ACSACL#-IP-ACL_USER1-65e89aab")을 사용하여 RADIUS 액세스 요청을 생성합니다. 이와 함께 WLC는 이 access-accept가 Cisco AV 쌍 aaa:event=acl-download를 사용하여 ACL 다운로드를 시작한다는 것을 RADIUS 서버에 알립니다.



```
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 8037: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits)
> Ethernet II, Src: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff), Dst: VMware_8d:01:ec (00:50:56:8d:01:ec)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.130, Dst: 10.48.39.134
> User Datagram Protocol, Src Port: 63772, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x51 (81)
    Length: 138
    Authenticator: b216948576c8a46a51899e72d0709454
    [Duplicate Request Frame Number: 8036]
    [The response to this request is in frame 8038]
  v Attribute Value Pairs
    > AVP: t=NAS-IP-Address(4) l=6 val=10.48.39.130
    v AVP: t=User-Name(1) l=32 val=#ACSACL#-IP-ACL_USER1-65e89aab
        Type: 1
        Length: 32
        User-Name: #ACSACL#-IP-ACL_USER1-65e89aab
    > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
    v AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)
        Type: 26
        Length: 30
        Vendor ID: ciscoSystems (9)
      v VSA: t=Cisco-AVPair(1) l=24 val=aaa:event=acl-download
          Type: 1
          Length: 24
          Cisco-AVPair: aaa:event=acl-download
    > AVP: t=Message-Authenticator(80) l=18 val=41da231159246db3f8562860dbf708f8
```

컨트롤러로 다시 전송된 RADIUS 액세스 승인은 표시된 대로 요청된 dACL을 포함합니다. 각 ACL 규칙은 "ip:inacl#<**X**>=<ACL_RULE>" 유형의 다른 Cisco AVP에 포함되어 있으며 <X>는 규칙 번호입니다.



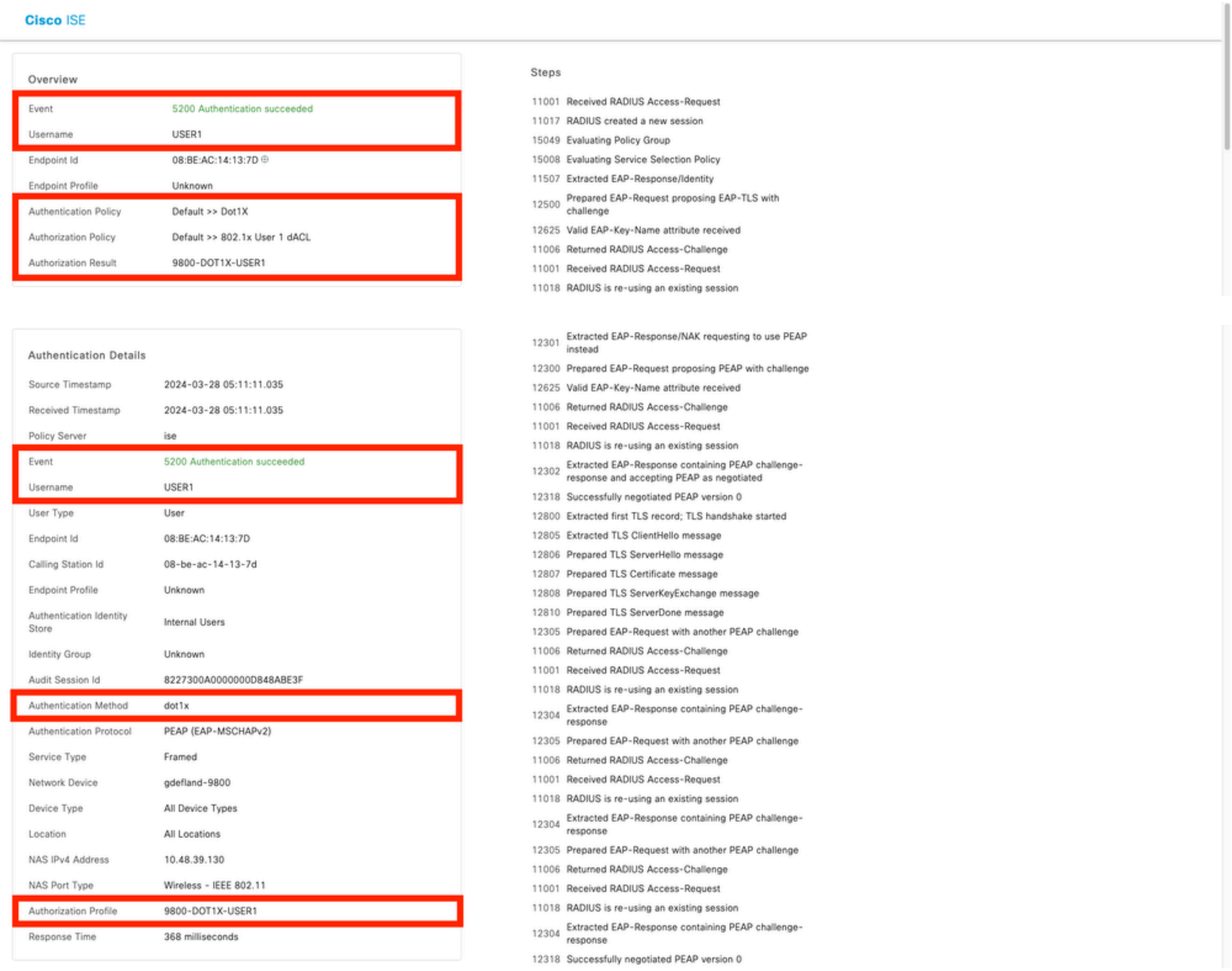
```
No.     |Length |ID   |Source          |Destination       |Info                                       |Protocol
   8037   184    39 10.48.39.130     10.48.39.134       Access-Request id=81, Duplicate Request    RADIUS
   8038   369    39 10.48.39.134     10.48.39.130       Access-Accept id=81   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

> Frame 8038: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)
> Ethernet II, Src: VMware_8d:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130
> User Datagram Protocol, Src Port: 1812, Dst Port: 63772
v RADIUS Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x51 (81)
    Length: 323
    Authenticator: 61342164ce39be06eed828b3ce566ef5
    [This is a response to a request in frame 8036]
    [Time from request: 0.007995000 seconds]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=32 val=#ACSACL#-IP-ACL_USER1-65e89aab
    > AVP: t=Class(25) l=75 val=434143533a30613330323738366d62425172394452596734477765f436554692f48737050…
    > AVP: t=Message-Authenticator(80) l=18 val=a3c4b20cd1e64785d9e0232511cd8b72
    v 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
    v 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
    v 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
    v 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
```

참고: 다운로드 ACL의 내용이 WLC에 다운로드된 후 수정될 경우 이 ACL을 사용하는 사용자가 다시 인증할 때까지 이 ACL의 변경 사항이 반영되지 않습니다(그리고 WLC는 해당 사용자에 대해 RADIUS 인증을 다시 수행). 실제로 ACL의 변경은 ACL 이름의 해시 부분의 변경에 반영됩니다. 따라서 다음에 이 ACL을 사용자에게 할당할 때는 이름이 달라야 하므로 ACL은 WLC 컨피그레이션의 일부가 아니어야 하며 다운로드되어야 합니다. 그러나 ACL에서 변경하기 전에 인증하는 클라이언트는 완전히 다시 인증될 때까지 이전 클라이언트를 계속 사용합니다.

ISE 작업 로그

RADIUS 클라이언트 인증

작업 로그는 다운로드 가능한 ACL "ACL_USER1"이 적용된 사용자 "USER1"의 성공적인 인증을 보여줍니다. 문제 해결에 필요한 부분은 빨간색으로 프레임화되어 있습니다.



Cisco ISE

Overview

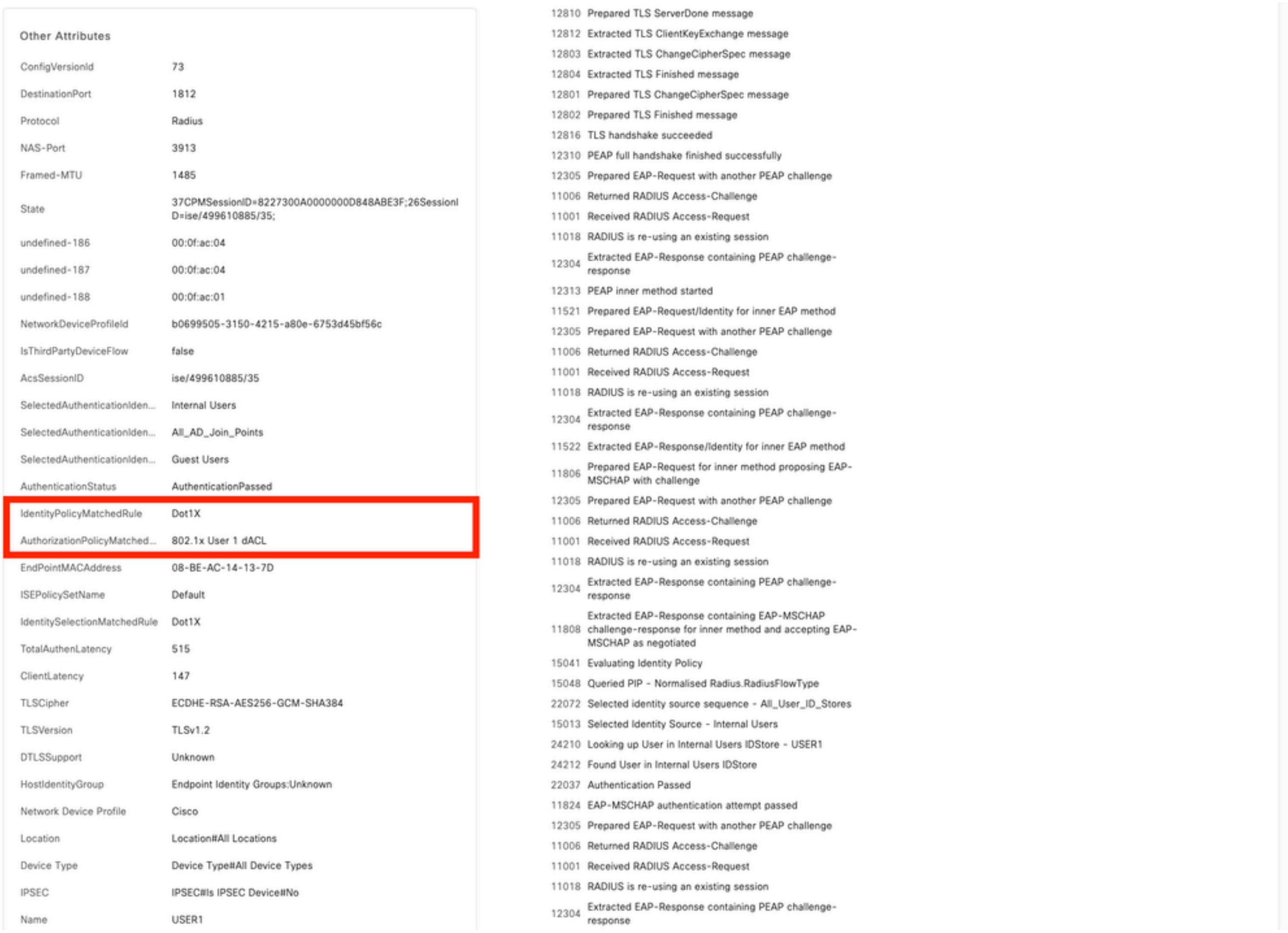
Event	5200 Authentication succeeded
Username	USER1
Endpoint Id	08:BE:AC:14:13:7D ⊕
Endpoint Profile	Unknown
Authentication Policy	Default >> Dot1X
Authorization Policy	Default >> 802.1x User 1 dACL
Authorization Result	9800-DOT1X-USER1

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

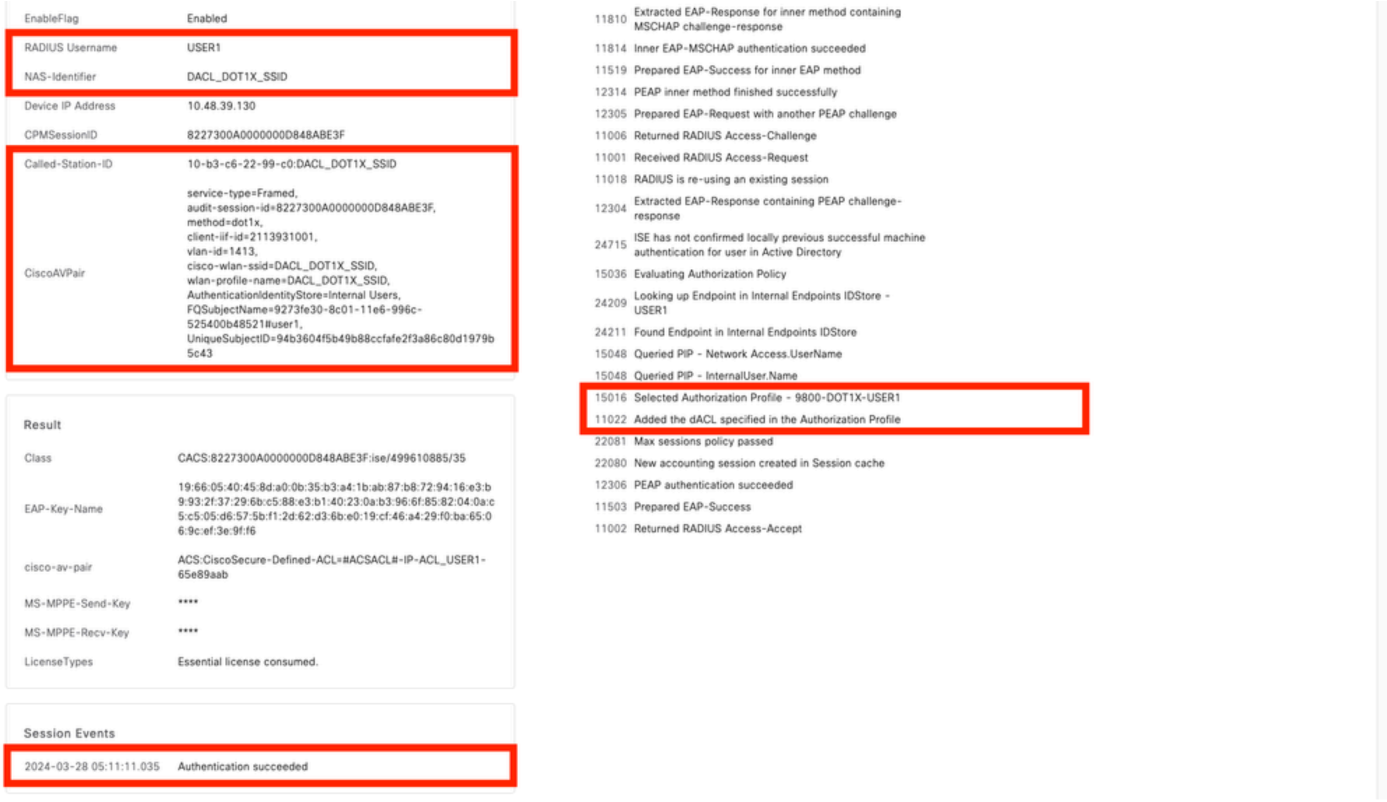
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned 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
      Extracted EAP-Response containing EAP-MSCHAP
11808 challenge-response for inner method and accepting EAP-
      MSCHAP as negotiated
15041 Evaluating Identity Policy
15048 Queried PIP - Normalised Radius.RadiusFlowType
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - USER1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
11824 EAP-MSCHAP authentication attempt passed
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-
      response
```



EnableFlag	Enabled
RADIUS Username	USER1
NAS-Identifier	DACL_DOT1X_SSID
Device IP Address	10.48.39.130
CPMSessionID	8227300A0000000D848ABE3F
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID

CiscoAVPair	service-type=Framed,
	audit-session-id=8227300A0000000D848ABE3F,
	method=dot1x,
	client-iif-id=2113931001,
	vlan-id=1413,
	cisco-wlan-ssid=DACL_DOT1X_SSID,
	wlan-profile-name=DACL_DOT1X_SSID,
	AuthenticationIdentityStore=Internal Users,
	FQSubjectName=9273fe30-8c01-11e6-996c-525400b48521#user1,
	UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b5c43

Result

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

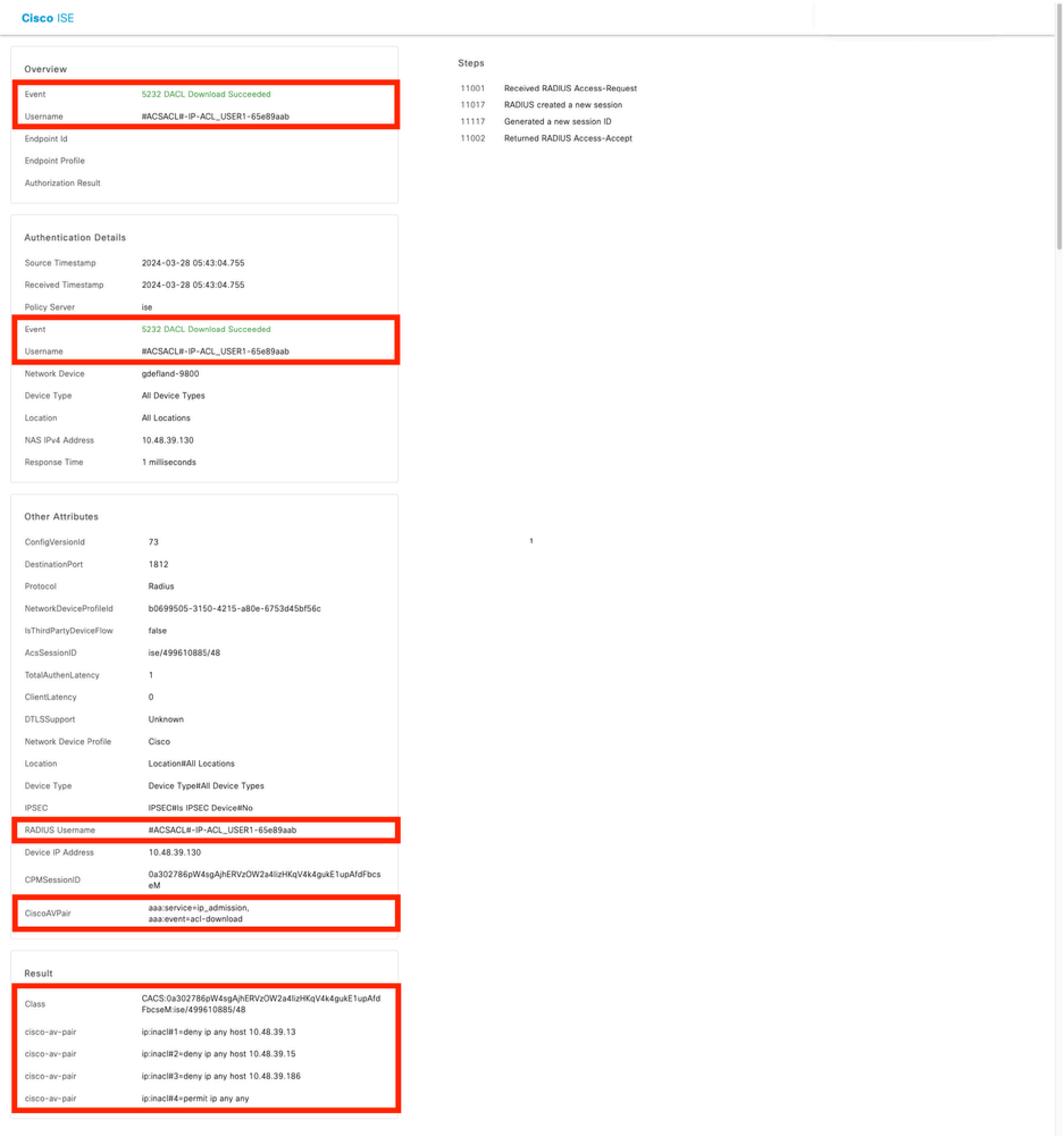
Session Events

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

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

DACL 다운로드

작업 로그는 ACL "ACL_USER1"의 성공적인 다운로드를 보여줍니다. 문제 해결에 필요한 부분은 빨간색으로 프레임화되어 있습니다.



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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.