# **Configure & Troubleshoot Downloadable ACLs on Catalyst 9800**

## Contents

Introduction
Background Information
Prerequisites
Requirements
Components Used
<u>Configure</u>
Using dACLs with 802.1x SSIDs
Network Diagram
WLC Configuration
ISE Configuration
Per-user dACLs
Per-result dACLs
Notes About Using dACLs with CWA SSIDs
<u>Verify</u>
Troubleshoot
Checklist
WLC One Stop-Shop Reflex
WLC Show Commands
Conditional Debugging and Radio Active Tracing
Packet capture
RADIUS client authentication
DACL Download
ISE Operation Logs
RADIUS client authentication
DACL Download

# Introduction

This document describes how to configure and troubleshoot downloadable ACLs (dACLs) on Catalyst 9800 Wireless LAN Controller (WLC).

# **Background Information**

dACLs have been supported for many years in Cisco IOS® and IOS XE® switches. A dACL refers to the fact that the network device dynamically downloads the ACL entries from the RADIUS server when authentication occurs, rather than having a local copy of the ACL and just being assigned the ACL name. A more complete <u>Cisco ISE configuration example</u> is available. This document focuses on the Cisco Catalyst

9800 which supports dACLs for central switching since the 17.10 release.

## Prerequisites

The idea behind this document is to demonstrate dACLs usage on Catalyst 9800 through a basic SSID configuration example, showing how these can be fully customizable.

On Catalyst 9800 wireless controller, downloadable ACLs are

- Supported <u>starting from Cisco IOS XE Dublin 17.10.1</u> release.
- Supported for centralized controller with Local mode Access Points only (or Flexconnect central switching). FlexConnect Local Switching does not support dACL.

### Requirements

Cisco recommends that you have knowledge of these topics:

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

### **Components Used**

The information in this document is based on these software and hardware versions:

- Catalyst 9800-CL (v. Dublin 17.12.03).
- ISE (v. 3.2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configure

Throughout this configuration guide, even if methods are different (for example WLAN authentication, policy configuration, and so on), the end result is the same. In the scenario exposed here, two user identities are defined being USER1 and USER2. Both are granted access to the wireless network. To each of them is assigned, respectively, ACL\_USER1 and ACL\_USER2 being dACLs downloaded by the Catalyst 9800 from ISE.

# Using dACLs with 802.1x SSIDs

### **Network Diagram**



### **WLC Configuration**

For details about 802.1x SSIDs configuration and troubleshooting on the Catalyst 9800, please refer to the <u>Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series</u> configuration guide.

Step 1. Configure the SSID.

Configure a 802.1x authenticated SSID, using ISE as RADIUS server. In this document, the SSID has been named "DACL\_DOT1X\_SSID".

#### From the GUI:

Navigate to **Configuration > Tags & Profiles > WLAN** and create a WLAN similar to the one showed here:

Cisco	Cisco Cata	lyst 9800-CL Wi	reless Controller		Welcome admin	***	Search APs and Clients Q	Feedback 🖌
Q. Search Menu Iter	ims	Configuration * >	Tags & Profiles * > W	/LANs				
Dashboard		+ Add	Delete 🔂 Clone	Enable WLAN Disable WLAN				WLAN Wizard
Monitoring	,	Selected WLANs : 0						
Configuration	•	Status Y	Name	T ID	▼ SSID	Y 2.4/5 GHz Security	▼ 6 GHz Security	т
Administration	n >	□ <b>⊙</b> ∺ 4 1 ≯	H 10 +	2	DACL_DOT1X_SSID	[WPA2][802.1x][AES]		1 - 1 of 1 items
C Licensing								
💥 Troubleshooti	ing							
Walk Me Through	•							

From the 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

Step 2. Configure the policy profile.

Configure the policy profile that is used along with the SSID defined above. On this policy profile, make sure AAA Override is configured from the "Advanced" tab, as showed in the screenshot. In this document, the policy profile used is "DACL-8021X".

As stated in the prerequisites section, dACLs are only supported for central switching/authentication deployments. Make sure the policy profile is configured that way.

From the GUI:

Navigate to **Configuration > Tags & Profiles > Policy**, select the policy profile used and configure it as showed.





#### From the 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
```

Step 3. Assign the policy profile and SSID to the policy tag used.

#### From the GUI:

Navigate to **Configuration > Tags & Profiles > Tags**. From the Policy tags tab, create (or select) the tag used and assign to it the WLAN and policy profile defined during steps 1-2.



#### From the 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

Step 4. Allow Vendor Specific Attribute.

Downloadable ACLs are passed via vendor specific attributes (VSA) in the RADIUS exchange between ISE and the WLC. The support of these attributes can be enabled on the WLC, using these CLI command.

From the CLI:

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

Step 5. Configure Default Authorization List.

When working with dACL, network authorization through RADIUS must be enforced for the WLC to authorize any user authenticating to the 802.1x SSID configured. Indeed, not only the authentication but the authorization phase is handled on the RADIUS server side here. Therefore, the authorization list is required in this case.

Make sure the default network authorization method is part of the 9800 configuration.

From the GUI:

Navigate to Configuration > Security > AAA and from the AAA Method List > Authorization tab, create

an authorization method similar to the one showed.

Cisco Cata	lyst 9800-CL Wireless Controlle	r		Welcom	e admin 🛛 🖨 🐔	A B ¢ % Ø	C Search APs and Clien	C Q SFeedback e <sup>A</sup>
Q. Search Menu Items	Configuration * > Security * > AAA + AAA Wizard	Show Me How 🧿						
<ul> <li>Dashboard</li> <li>Monitoring</li> </ul>	Servers / Groups AAA Method Li	t AAA Advanced						
Configuration	Authentication	+ Add × Delete						
C Licensing	Accounting	default default	Type exec network	Group Type     local     group	Group1 N/A radius	Group2 N/A N/A	Group3 N/A N/A	▼ Group4 ▼ N/A N/A
X Troubleshooting		H 4 1 H H 10	1					1 - 2 of 2 items
Walk Me Through >								

From the CLI:

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

### **ISE Configuration**

When implementing dACLs in wireless environment with ISE, two common configurations are possible, to know:

- 1. Per-user dACL configuration. With this, each particular identity has a dACL assigned thanks to a custom identity field.
- 2. Per-result dACL configuration. While opting for this method, a particular dACL is assigned to a user based on the authorization policy it matched on the policy set used.

#### Per-user dACLs

Step 1. Define a dACL Custom User Attribute

To be able to assign a dACL to a user identity, first this field must be configurable on the identity created. By default, on ISE, the "ACL" field is not defined for any new identity created. To overcome this, one can use the "Custom User Attribute" and define a new configuration field. To do so, navigate to Administration > Identity Management > Settings > User Custom Attributes. Use the "+"button to add a new attribute similar to the one showed. In this example, the name of the custom attribute is ACL.

≡ Cisc	o ISE			Α	dministration •	Identity M	anagement		🔺 License Wa	rning Q	0	ø o
Identities	Groups	External l	dentity Sour	ces lo	dentity Source Se	equences	Settings					
User Custom Attri	ibutes										$\rm All \sim$	$\nabla$
User Authentication	on Settings		Mandat	Attribute	Name	^	Data Type					
Endpoint Purge	Attributes			Firstname			String					
REST ID Store Set	ttings			Lastname			String					
			× .	Name			String					1
				Password	(CredentialPasswo	ord)	String					
		~	User Cust	om Attril	outes							
			Attribute I	Name	Description	n	Data Type	Parameters	Default Val	ue Mandator	у	
		Г	ACL				String ~	String Max length	+	_ C 👔	+	
									Sav	Ð	Reset	

Once this configured, use the "Save" button to savethe changes.

### Step 2. Configure the dACL

Navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** to see and define dACL on ISE. Use the "Add" button to create a new one.

≡ Cisco IS	SE	Policy · Policy Elements					🔺 License Warning	ର ୧	) ja 🎄
Dictionaries	Conditions	Results							
Authentication Authorization Authorization Profile	> ~		Jable ACL	_S			Sele	ected 0 Total	7 (2) (\$) All ~ 17
Downloadable ACLs	,	Name		De	escription				
Profiling	>	ACL_US	R1	A	CL assigned to USER1				
Posture	>	DENY_A	L_IPV4_TRAFFIC	D	eny all ipv4 traffic				
Client Provisioning	>	DENY_A	L_IPV6_TRAFFIC	D	eny all ipv6 traffic				
		PERMIT_	ALL_IPV4_TRAFFIC	A	llow all ipv4 Traffic				
		PERMIT_	ALL_IPV6_TRAFFIC	A	llow all ipv6 Traffic				
		test-dac	-cwa						
		test-dac	-dot1x						

This opens the "New Downloadable ACL" configuration form. On this one, configure these fields:

- Name: the name of the dACL defined.
- Description (optional): a brief description about the usage of the created dACL.
- IP version: the IP protocol version used in the defined dACL (version 4, 6 or both).
- DACL Content: the content of the dACL, as per Cisco IOS XE ACL syntax.

In this document, the dACL used is "ACL\_USER1" and this dACL allows any traffic except the one destinated to 10.48.39.186 and 10.48.39.13.

Once the fields configured, use the "Submit" button to create the dACL.

Repeat the step to define the dACL for the second user, ACL\_USER2, as showed in the figure.

■ Cisco ISE	Policy · Pol	🔺 License Warning 🔍 ⊘ 💭 🐡	
Dictionaries Conditions	Results		
Authentication >	Downloadable ACLs		
Authorization $\checkmark$			Selected 0 Total 8 📿 🚸
Authorization Profiles	🖉 Edit 🕂 Add 📋 Duplicate 🚦 Delete		all $\sim$ $\nabla$
Downloadable ACLs			
	Name	Description	
Profiling >	ACL_USER1	ACL assigned to USER1	
Posture >	ACL_USER2	ACL assigned to USER2	
Client Provisioning	DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic	
	DENY_ALL_IPV6_TRAFFIC	Deny all joy6 traffic     Deny all joy6 traffic     Deny all joy6 traffic	
	PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic	
	PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic	
	test-dacl-cwa		
	test-dacl-dot1x		

Step 3. Assign the dACL to a Created Identity

Once the dACL created, one can assign it to any ISE identity using the User Custom Attributes created in Step 1. To do so, navigate to Administration > Identity Management > Identities > Users. As usual, use the "Add" button to create a user.



On the "New Network Access User" configuration form, define the username and password for the created user. Use the custom attribute "ACL" to assign the dACL created in Step 2 to the identity. In the example, the identity USER1 using ACL\_USER1 is defined.

E Cisco ISE		Administration - Identity Management	🔺 License Warning Q 🔘 🕫 Ø
Identities Groups Ext	rnal identity Sources Identity Source Sequences Settings		
Users Latest Manual Network Scan Res	Natwork 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	Generate Password	
	Enable Password	Generate Password	
	> User Information		
	> Account Ontions		
	> Account Disable Policy		
	<ul> <li>User Custom Attributes</li> </ul>		
		-	
	ACL - ACL_USER1		
	✓ User Groups		
	ii Salart an Jam		
			Save Roset

Once the fields configured properly, use the "Submit" button to create the identity.

Repeat this step to create USER2 and assign ACL\_USER2 to it.

E Cisco ISE	Administration - Identity Management	🔺 License Warning 🔍 💮 🗔 🖗
Identities Groups E	ernal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected 0 Total 3 🧷 🔕
	🖉 Gill 🕂 Add 🛞 Change Status Y 🎂 Import 💩 Export Y 🔲 Delete Y 🗍 Duplicate	As $\vee$ $\nabla$
	Status Username $\wedge$ Description First Name Last Name Email Address User Identity Groups Admin	
	Olisabled 1 adminuser     adminuser	
	Enabled 1 USER1	
	Cabled 1 USER	
	Network Access Users	

Step 4. Configure authorization policy result.

Once the identity configured and the dACL assigned to it, the authorization policy must still be configured in order to match the custom user attribute "ACL" defined to an existing authorization common task. To do so, navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. Use the "Add" button to define a new authorization policy.

- Name: the name of the authorization policy, here "9800-DOT1X-USERS".
- Access Type: the type of access used when this policy is matched, here ACCESS\_ACCEPT.
- Common Task: match "DACL Name" to InternalUser:<name of custom attribute created> for internal user.According to the names used in this document, the profile 9800-DOT1X-USERS is configured with the dACL configured as InternalUser:ACL.

≡ Cisco ISE	Policy • Policy Elements	🔺 License Warning	Q (1)	9 ¢
Dictionaries Conditions	Results			
Authentication >	Authorization Profiles > New Authorization Profile Authorization Profile			
Authorization Profiles	* Name			
Downloadable ACLs	9800-DOTIX-USERS Description Authorization and/e for 400.1x users using 440.1x.			
Profiling >				
Posture >	* Access Type ACCESS_ACCEPT ~			
Client Provisioning >	Network Device Profile 🗰 Cloco 🗸 😑			
	Service Template        Track Movement        Agentiless Posture        Passive Identity Tracking			
	Common Tasks DACL Name InternalUser:ACL IPV6 DACL Name ACL (Filter-ID)			I

Step 5. Use authorization profile in policy set.

Once the authorization profile result correctly defined, it still needs to be part of the policy set used to authenticate and authorize wireless users. Navigate to **Policy Sets** and open the policy set used.

Here, the authentication policy rule "Dot1X" matches any connection made via wired or wireless 802.1x. The authorization policy rule "802.1x Users dACL" implements a condition on the SSID used (that is Radius-Called-Station-ID CONTAINS DACL\_DOT1X\_SSID). If an authorization is performed on the "DACL\_DOT1X\_SSID" WLAN, then the profile "9800-DOT1X-USERS" defined in Step 4 is used to authorize the user.

Cisco ISE	Policy · Policy Sets		🔺 License Warnin	
Policy Sets→ Default			Reset Policyset Hitco	unts Save
Status Policy Set Name	Description Conditions		Allowed Protocols / S	erver Sequence Hits
Q Search				
😕 Default	Default policy set		Default Network Acc	BSS ⟨S ∨ + 76
$\sim$ Authentication Policy (2)				
(+) Status Rule Name	Conditions		Use	Hits Actions
Q Search				
			All_User_ID_Stores	
Dot1X	OR E Wireless_802.1X		> Options	65 (弥 ——
			All_User_ID_Stores	
Default			> Options	10 {ô}
> Authorization Policy - Local Exceptions				
> Authorization Policy - Global Exceptions				
$\lor$ Authorization Policy (2)				
		Results		
+ Status Rule Name	Conditions	Profiles	Security Groups	Hits Actions
Q Search				
1 802.1x Users dACL	Radius-Called-Station-ID CONTAINS DACL_DOTIX_SSID	9800-DOT1X-USERS ×	+ Select from list	· + 65 {}
Ø Default		DenyAccess ×	+ Select from list	·+ • ô

#### Per-result dACLs

To avoid the tremendous task of assigning a particular dACL to each identity created on ISE, one can opt for applying the dACL to a particular policy result. This result is then applied based on any condition matched on the authorization rules from the policy set used.

Step 1. Configure the dACL

Execute the same Step 2 from the <u>Per-user dACLs section</u> in order to define the dACLs needed. Here, these are ACL\_USER1 and ACL\_USER2.

#### Step 2. Create identities

Navigate to Administration > Identity Management > Identities > Users and use the "Add" button to

create a user.



On the "New Network Access User" configuration form, define the username and password for the created user.

≡ Cisco IS	SE			Ac	dministration - Identity	Management	🔺 License Warring	0.0	() 52 ()
Identities G	Groups Exte	mal Identity Sources	Identity Source Sequences	Settings					
Users Latert Manual Network	k Scan Res	Network Access Users List	> New Network Access User						
		V Network Acces	s User						
		* Usomarne	USER1						
		Status	🗧 Enabled 🗸						
		Account Name Allas		0					
		Ernal							
		- Passuorda							
		Password Type: k	temel Users						
		-							
		Password Lifetime:     With Expiration							
		O Never Expires (	D						
			Password	Re-Enter Password					
		* Login Password			Generate Password	0			
		Enoble Password			Generate Password	0			
		> User Informati	on						
		> Account Optio	ns						
		> Account Disab	le Policy						
		> User Custom A	Attributes						
		> User Groups							
							Submit	Car	ncel

Repeat this step to create USER2.

E Cisco ISE	E	Administration - Identity Management	🔺 License Marrieg O, O 53 @
Identities Gro	oupa	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network S	Scan Res	Network Access Users	
			Selected O Total 3 [
		∕ Eil + A44 - S Change Status ∨ do legent - Δ Eigent ∨ - Π Deles ∨ - Π Deles ∨ - Π Deles	$\sim \Delta$
		Status Username 🔿 Description Finst Name Last Name Email Address User Identity Groups Admin	
		O Saabed 1 edminuser     admin-group	
		Network Access Users	

Step 4. Configure the authorization policy result.

Once the identity and the dACL configured, the authorization policy must still be configured in order to assign a particular dACL to user matching the condition to use this policy. To do so, navigate to **Policy** > **Policy Elements** > **Results** > **Authorization** > **Authorization Profiles**. Use the "Add" button to define a new authorization policy and complete these fields.

- Name: the name of the authorization policy, here "9800-DOT1X-USER1".
- Access Type: the type of access used when this policy is matched, here ACCESS\_ACCEPT.
- **Common Task:** match "DACL Name" to "ACL\_USER1" for internal user. According to the names used in this document, the profile 9800-DOT1X-USER1 is configured with the dACL configured as "ACL\_USER1".

≡ Cisco ISE	Policy · Policy Elements	A Usense Warring	Q (	8 52 C	þ
Dictionaries Conditions	Results				
Astheediadles     >       Astheediadles     ~       Astheediadles     ~       Develoadleth ACLs     ~       PredBag     >       Pastare     >       Client Profiliation     >	Azere/zation Profile         * Notro       9809-00718-03881         Description				
	Common Tasks Common Tasks Common Tasks Could Name OLCLUSEN OLVANNE OLCLUSEN OLVANNE OLCLUSEN OLVANNE ACLUSEN ACUITAL ACCENTS ACUITAL				
	V Attributes Details Axes free - KCSSE, ACEPT DACL = AQL, ISSTR	Submit	]	Cencel	

Repeat this step to create the policy result "9800-DOT1X-USER2" and assign "ACL\_USER2" as DACL to it.

E Cisco ISE		Polic	y - Policy Elements 🔺 Literate Running Q, 🕐 52
Dictionaries Conditions	Results		
Asthemication >	Standard Authorization P	rofiles	
Authorization ~	for finite faces on a Administration & Contem & Backs	n & Remove > Doliny Execut Rane	
Authorization Profiles	For Pointy Capital Series Advantagement > Capital > Const	the or supporting in a county of the state of the state	Selected 0 Total 13 🦪 🄇
Dewnlosdable ACLs	/ Edit + Add () Displayers () Debits		м× 1
Profiling	Neme	Profile	
Pasture	Seco-portix-uspai	m Cisco 🕕	
Client Provisioning	9800-D011X-U36R2	# Cisca 🕡	
	aeco-bottx-usbas	# Ciaca 🕦	Authorization profile for 802.1x users using dADLs.
	Bleck_Windess_Access	# Cisco 🕦	Default profile used to black wireless devices. Ensure that you configure a NULL ROUTE ACL on the Wireless LAN Controller
	Cisco_JP_Phones	tte Classo 🕥	Default profile used for Cloca Phones.
	Cisco_Temporal_Onboard	tti Cisca 🕕	Oriboard the device with Clisco temporal agent
	Ches_WebAsth	the Cisco 🕥	Default Profile used to redirect users to the CWA portal.
	Internal Confector Activities Test	# Ciaco 🕥	
	NSP_Onboard	tte Cisco 🕕	Onboard the dovice with Native Supplicant Provisioning
	Non_Close_JP_Phones	the Cisco 🕕	Default Profile used for Non Close Phones.
	UDN	# Ciaca 🕠	Default profile used for UDN.
	DenyAccess		Default Profile with access type as Access-Reject
	Permithecess		Default Profile with access type as Access-Accept

Step 5. Use authorization profiles in policy set.

Once the authorization profile results correctly defined, it still needs to be part of the policy set used to authenticate and authorize wireless users. Navigate to **Policy** > **Policy** Sets and open the policy set used.

Here, the authentication policy rule "Dot1X" matches any connection made via wired or wireless 802.1X. The authorization policy rule "802.1X User 1 dACL" implements a condition on the username used (that is InternalUser-Name CONTAINS USER1). If an authorization is performed using the username USER1, then the profile "9800-DOT1X-USER1" defined in Step 4 is used to authorize the user and thus, the dACL from this result (ACL\_USER1) is applied as well to the user. The same is configure for username USER2, for which "9800-DOT1X-USER1" is used.

Cisco ISE							
			Policy - Policy Sets		📥 License Warring	Q. (	5 57
olicy Sets-+	Default				Reset Policyset Hitsourts		Sav
Status P	ulicy Set Name I	escription Conditions			Allowed Protocols / Server	Sequi	ence
Q Search							
	Defeut	Default rolls s set			Default Network Access		×+
-							
<ul> <li>Authenticatio</li> </ul>	n Palicy (2)						
<ul> <li>Status</li> </ul>	Ruie Name	Conditions			Use	Hits	Acti
Q Search							_
		Wined_B82.1X			All_User_ID_Stores 🛛 🗠		
۰	Det1X	CR Windows, MAB			> Options		43
		Wired_WAB					
					All_User_ID_Stores 02 V		
•	Defeat				> Options	10	67
Authorization	Balina - Local Paramitera						
> Authorization	Policy - Global Exceptions						
~ Authorization	Pelicy (3)						
				Results			
<ul> <li>Status</li> </ul>	Rule Name	Conditions		Profiles	Security Groups	Hits	Acti
<ul> <li>Status</li> <li>Q Search</li> </ul>	Rule Name	Conditions		Results Profiles	Security Groups	Hits	Act
<ul> <li>Status</li> <li>Q Search</li> </ul>	Rule Name	Conditions		Profiles 9800-DOT1X-USER2 × +	Security Groups Select from list ~ ~ +	Hits	Act
<ul> <li>Status</li> <li>Q Search</li> <li>Q</li> <li>Search</li> <li>Q</li> </ul>	Bule Name           892.1x liner 2 dAOL           892.1x liner 1 dAOL	Conditions  Condit		Results           Profiles           1900-DOT1X-USER2 ×         >+           9800-DOT1X-USER2 ×         >+	Security Groups Select from list $\sim$ + Select from list $\sim$ +	нітя 0 86	Acti

# Notes About Using dACLs with CWA SSIDs

As described in the <u>Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE</u> configuration guide, CWA relies on MAB and particular result to authenticate and authorize users. Downloadables ACLs can be added to the CWA configuration from ISE side identically as what has been described above.



**Warning**: Downloadable ACLs can only be used as network access list and are not supported as pre-authentication ACLs. Therefore, any pre-authentication ACL used in a CWA workflow must be defined in the WLC configuration.

## Verify

To verify the configuration made, these commands can be used.

# 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 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 }

Here is referenced the relevant part of the WLC configuration corresponding to this example.

```
aaa new-model
1
I
aaa group server radius authz-server-group
server name DACL-RADIUS
I
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
1
!
aaa server radius dynamic-author
client <ISE IP>
aaa session-id common
I
[...]
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
T
1
[...]
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
ſ...]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
security dot1x authentication-list DOT1X
no shutdown
```

The RADIUS server configuration is presented, displayed using the show running-config all command.

```
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
```

### Troubleshoot

### Checklist

- Ensure clients can connect properly to the 802.1X SSID configured.
- Ensure the RADIUS access-request/accept contain the proper attribute-value pairs (AVPs).
- Ensure clients use the proper WLAN/policy profile.

### WLC One Stop-Shop Reflex

To check if the dACL is properly assigned to a particular wireless client, one can use the **show wireless** client mac-address <H.H.H> detail command as shown. From there, different useful troubleshooting information can be seen, namely: the client username, state, policy profile, WLAN and, most importantly here, the 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
           : 0x90000012
 IIF ID
 Authorized : TRUE
Session timeout : 28800
 Common Session ID: 8227300A000000C8484A22F
 Acct Session ID : 0x0000000
 Last Tried Aaa Server Details:
     Server IP : 10.48.39.134
 Auth Method Status List
     Method : Dot1x
                  : AUTHENTICATED
         SM State
         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
                         : 1413
         VLAN
         Absolute-Timer : 28800
[...]
```

### WLC Show Commands

To see all ACLs which are currently part of the Catalyst 9800 WLC configuration, you can use the **show access-lists** command. This command lists all ACLs defined locally or dACLs downloaded by the WLC. Any dACLs downloaded from ISE by the WLC has the format xACSACLx-IP-<ACL\_NAME>-<ACL\_HASH>.



**Note**: Downloadable ACLs remain in the configuration as long as a client is associated and uses it in the wireless infrastructure. As soon as the last client using the dACL leaves the infrastructure, the dACL is removed from the configuration.

```
WLC#show access-lists
Extended IP access list IP-Adm-V4-Int-ACL-global
[...]
Extended IP access list IP-Adm-V4-LOGOUT-ACL
[...]
Extended IP access list implicit_deny
[...]
Extended IP access list implicit_permit
[...]
Extended IP access list meraki-fqdn-dns
[...]
Extended IP access list preauth-ise
[...]
Extended IP access list preauth_v4
[...]
Extended IP access list xACSACLx-IP-ACL_USER1-65e89aab
```

```
1 deny ip any host 10.48.39.13
2 deny ip any host 10.48.39.15
3 deny ip any host 10.48.39.186
4 permit ip any any (56 matches)
IPv6 access list implicit_deny_v6
[...]
IPv6 access list implicit_permit_v6
[...]
IPv6 access list preauth_v6
[...]
```

#### **Conditional Debugging and Radio Active Tracing**

While troubleshooting configuration, you can collect <u>radioactive traces</u> for a client supposed to be assigned with the dACL defined. Here are highlighted the logs showing the interesting part of the radioactive traces during the client association process for client 08be.ac14.137d.

```
<#root>
24/03/28 10:43:04.321315612 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (note): MAC: 08be.ac14.137d Asso
2024/03/28 10:43:04.321414308 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d
2024/03/28 10:43:04.321464486 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376
[...]
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 $
2024/03/28 10:43:04.322881795 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376
[...]
2024/03/28 10:43:04.323379781 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]
[...]
2024/03/28 10:43:04.330181613 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]
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 Clier

[...] 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 "USER 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 "r 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 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 "0 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 "v 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] 1 2024/03/28 10:43:04.381539951 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [18 2024/03/28 10:43:04.381542233 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[ 2024/03/28 10:43:04.381544465 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188] 2024/03/28 10:43:04.381619890 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout [...] 2024/03/28 10:43:04.392544173 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812, 2024/03/28 10:43:04.392557998 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 08 6d f 2024/03/28 10:43:04.392564273 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: State [24] 71 ...

2024/03/28 10:43:04.392615218 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 8 ... 2024/03/28 10:43:04.392628179 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.392738554 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t 2024/03/28 10:43:04.726798622 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_9000001 2024/03/28 10:43:04.726801212 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012 2024/03/28 10:43:04.726896276 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_9000001 2024/03/28 10:43:04.726905248 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012 [...] 2024/03/28 10:43:04.727138915 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012 2024/03/28 10:43:04.727148212 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000 2024/03/28 10:43:04.727164223 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000 2024/03/28 10:43:04.727169069 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000 2024/03/28 10:43:04.727223736 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : use 2024/03/28 10:43:04.727233018 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : cl 2024/03/28 10:43:04.727234046 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA 2024/03/28 10:43:04.727234996 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Me 2024/03/28 10:43:04.727236141 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA M\$®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\_9000 2024/03/28 10:43:04.727513133 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000 2024/03/28 10:43:04.727607738 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: SVM Apply user profile 2024/03/28 10:43:04.728003638 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: Activating EPM feature 2024/03/28 10:43:04.728144450 {wncd\_x\_R0-0}{1}: [epm-misc] [19620]: (info): [08be.ac14.137d:capwap\_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 " 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 " 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 " 2024/03/28 10:43:04.732062574 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 36 2024/03/28 10:43:04.732064854 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 30 " 2024/03/28 10:43:04.732114294 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t [...] 2024/03/28 10:43:04.733046258 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): [08be.ac14.137d] Applied User Pro 2024/03/28 10:43:04.733058380 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M 2024/03/28 10:43:04.733064555 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M 2024/03/28 10:43:04.733065483 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e 2024/03/28 10:43:04.733066816 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: m 2024/03/28 10:43:04.733068704 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c 2024/03/28 10:43:04.733069947 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: i 2024/03/28 10:43:04.733070971 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: us 2024/03/28 10:43:04.733079208 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c 2024/03/28 10:43:04.733080328 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: E M\$®∨f9∫Ø◊« %ÿ0ã@≤™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 A 2024/03/28 10:43:04.734665244 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth] 2024/03/28 10:43:04.734894043 {wncd\_x\_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d E 2024/03/28 10:43:04.734904452 {wncd\_x\_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d C 2024/03/28 10:43:04.734915743 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012 2024/03/28 10:43:04.740499944 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= of the set of the 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= 0 [...] 2024/03/28 10:43:04.745245318 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl ] 2024/03/28 10:43:04.745294050 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Allocate 2024/03/28 10:43:04.745326416 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in 2024/03/28 10:43:04.751291844 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= 0 2024/03/28 10:43:04.751943577 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A 2024/03/28 10:43:04.752686055 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth] 2024/03/28 10:43:04.755505991 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= of the set of the 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.ac14.1376 2024/03/28 10:43:04.759064834 {wncd\_x\_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d II 2024/03/28 10:43:04.761186727 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl ] 2024/03/28 10:43:04.761241972 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in 2024/03/28 10:43:04.763131516 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth] 2024/03/28 10:43:04.764575895 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= 0 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= of the set of the 2024/03/28 10:43:04.770727027 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= o 2024/03/28 10:43:04.772314586 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl ] 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= of the set of the 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= o 2024/03/28 10:43:04.777154567 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= of the set of the 2024/03/28 10:43:04.778756670 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl ] 2024/03/28 10:43:04.778807076 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.778856100 {iosrp\_R0-0}{1}: [mpls\_ldp] [26311]: (info): LDP LLAF: Registry notificat:

2024/03/28 10:43:04.779401863 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= 0

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= of the set of the

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 II 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 :bs 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.ac14.1370

#### Packet capture

Another interesting reflex is to take and analyze packet captures of the RADIUS flow for a client association. Downloadable ACLs rely on RADIUS, not only to be assigned to a wireless client but also to be downloaded by the WLC. While taking packet capture for troubleshooting dACLs configuration, you must therefore capture on the interface used by the controller to communicate with the RADIUS server. This document shows how to configure easily embedded packet capture on the Catalyst 9800, which have been used to collect the capture analyzed in this article.

#### **RADIUS client authentication**

You can see the client RADIUS access-request sent from the WLC to the RADIUS server in order to authenticate the user USER1 (AVP User-Name) on the DACL\_DOT1X\_SSID SSID (AVP NAS-Identifier).

Ma II any	ath UD	Causea	Destination	i kada	Destand
- 480 6	17 3	9 10.48.39.130	10.48.39.134	Access-Request id=92, Duplicate Request	RADIUS
- 480 3	94 3	9 10.48.39.134	10.48.39.130	Access-Accept id=92	RADIUS
Eramo 49	035. G	17 buter on wire (4026	bits) 617 butos conturad	(4026 hitz)	
Ethernet	033: 0 TT C	re. Cisco b2.fo.ff (00	10:16:16:12:10:11 Ditte	(4530 U1(5) c. 04.01.c. (00.50.55.04.01.c.)	
> POD 10 V	irtual	IAN DOT: A DET: A	TD: 20		
Totornot	Droto	col Version 4 Srci 10	10: 39		
> licer Dat	20720	Protocol Src Port: 62	772 Det Doet, 1912	44 	
PADTUS P	agraiii	Protocot, sic Port: 03	772, DSC PORC: 1012		
Coder	Access	Bequest (1)			
Docket	iden+	ifier AvEc (02)			
Length	. 571	11161: 0050 (92)			
Length	: 3/1	2642d9722b0fb2ac109	100-044694471		
Auchen	citato B	1: 304208/33091028C198	0096914101171		
[The r	cate N	equest Frame Number: 4	60034]		
Attrib	ute Va	e to this request is i	II Traile 460591		
A1/D		-Name(1) 1=7 valeUSER	1		
> AVP	t-Ser	(1) = 1	ramed(2)		
AVP	t=Ven	$dor_Specific(26)$ 1=27	und=ciccoSveteme(0)		
AVP	t-Era	$med_MTII(12) = 6 yal = 14$	4110=C13C03y3Cellis(3/		
AVP	+-EAD	Maccaae(70) 1=49 Last	Segment [1]		
	t-Mac	sage_Authenticator(80)	l=18 val=cdc761262dc47e98d	21bb8600d38250	
	+-EAD	Kov_Name(102) 1-2 val	-		
AVP	t=Ven	$dor_Specific(26) = 40$	und=ciccoSystems(0)		
	t-Ven	dor-Specific(26) $1-29$	und=ciscoSystems(9)		
AVP	t=Era	$mod_TP_Addross(R) = 6$	val=10 14 12 240		
	t-Ven	dor_Specific(26) 1-40	val-10.14.13.240		
	t=Ven	dor-Specific(26) $1=22$	und=ciscoSystems(9)		
AVP	t-Ven	dor-Specific(26) $1-20$	und-ciccoSystems(0)		
	+-NAC	$TP_Addrocc(A) = 6 val$	-10 40 20 120		
> AVP	t-NAS	-Port-Type(61) 1=6 val	-Wireless-802 11(10)		
AVP	t=NAS	-Port(5) ]=6 val=3013			
AVP	t=Sta	$t_{e}(24)$ ]=71 va]=333743	504453657373606f6e404434383	222773328284138283838383838383838383833335	
AVP	t=Ven	$dor_{Specific(26)} = 39$	und=ricroSvetame(0)		
> AVP:	t=Ven	dor-Specific(26) $l=41$	vnd=ciscoSystems(9)		
> AVP	t=Cal	led-Station-Id(30) 1=3	5 val=f4-db-e6-5e-7b-c0:DAC	DOT1X SSID	
> AVP	t=Cal	ling-Station-Id(31) 1=	19 val=08-be-ac-14-13-7d		
> AVP	t=Ven	dor-Specific(26) 1=12	vnd=Airespace, Inc(14179)		
> AVP:	t=NAS	-Identifier(32) l=17 v	al=DACL_DOT1X_SSTD		
AVP:	t=link	nown-Attribute(187) ]=	6 val=000fac04		
> AVP:	t=Unk	nown-Attribute(186) l=	6 val=000fac04		
AVP (rat	dius.avp), 4	8 bytes		<ul> <li>Packets: 55012 - Displayed: 2 (0.0%) - Ignored: 1 (0.0%)</li> </ul>	Profile: Default

When the authentication succeeds, the RADIUS server replies with an access-accept, still for user USER1 (AVP User-Name) and applying the AAA attributes, in particular the vendor specific AVP ACS:CiscoSecure-Defined-ACL being here "#ACSACL#-IP-ACL\_USER1-65e89aab".

No.	Length   ID	Source	Destination	Info	Protocol
480	617 3	39 10.48.39.130	10.48.39.134	Access-Request id=92, Duplicate Request	RADIUS
- 480	394 3	39 10.48.39.134	10.48.39.130	Access-Accept id=92	RADIUS
> Frame	48039: 3	94 bytes on wire (31	52 bits), 394 bytes	captured (3152 bits)	
Ethern	et II, S	rc: VMware_8d:01:ec	(00:50:56:8d:01:ec),	Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)	
> 802.10	Virtual	LAN, PRI: 0, DEI: 0	, ID: 39		
> Interr	et Proto	col Version 4, Src:	10.48.39.134, Dst: 1	0.48.39.130	
> User [	atagram	Protocol, Src Port:	1812. Dst Port: 6377	2	
~ RADIUS	Protoco				
Code	Access	-Accept (2)			
Pack	at ident	ifier: Av5c (02)			
Lend	the 249	111211 0030 (92)			
Auth	enticate	c. 642ab1oaba0479772	F72670ab62b20a		
Autr	enticato	1: 043ab1eaba9478773	5173078a033028a		
1102	<u>s is a r</u>	esponse to a request	1n Trame 480341		
[110	e trom r	equest: 0.059994000	seconasj		
~ ATT	ibute va	lue Pairs	504		
	P: t=Use	r-Name(1) L=7 val=US	ERI		
> AV	P: t=Cla	ss(25) l=48 val=43414	43533a38323237333030	41303030303030394638343933354132443a697365213439	
> A\	P: t=EAP	-Message(79) l=6 Las	t Segment[1]		
> A\	P: t=Mes	sage-Authenticator(8	a) l=18 val=de01c27a	418e8289dd5d6b29165ec872	
> A\	P: t=EAP	-Key-Name(102) l=67	val=\031f\005C <b>0I0</b> \00	31VE 00x\0020^00R0\033q00?&000040\021(0Q{0\035/s 0a0d0y\02700	60000F0d
~ A\	P: t=Ven	dor-Specific(26) l=60	<pre>6 vnd=ciscoSystems(9</pre>		
	Type: 26				
	Length: (	66			
_	Vendor II	D: ciscoSystems (9)			
~	VSA: t=C	isco-AVPair(1) l=60 v	val=ACS:CiscoSecure-	Defined-ACL=#ACSACL#-IP-ACL_USER1-65e89aab	
	Type: 3	1			
	Length	: 60			
	Cisco-	AVPair: ACS:CiscoSecu	re-Defined-ACL=#ACS	ACL#-IP-ACL_USER1-65e89aab	
> AV	P: t=Ven	dor-Specific(26) L=5	K vnd=Microsoft(311)		
> 41	P: t=Ven	dor-Specific(26) 1=5	R vnd=Microsoft(311)		
		doi specific(10) (-s			
	+ h (11) - #1				. Declarity (F2015, Disclosed, D.(5.047), Instance, J.(6.047).

### DACL Download

If the dACL is already part of the WLC configuration, then it is simply assigned to the user and the RADIUS session ends. Otherwise, the WLC downloads the ACL, still using RADIUS. To do so, the WLC makes a RADIUS access-request, this time using the dACL name ("#ACSACL#-IP-ACL\_USER1-65e89aab") for the AVP User-Name. Along with this, the WLC informs the RADIUS server that this access-accept initiates an ACL download using the Cisco AV pair aaa:event=acl-download.



The RADIUS access-accept sent back to the controller contains the dACL requested, as shown. Each ACL rule is contained inside a different Cisco AVP of type "ip:inacl# $<X>=<ACL_RULE>$ ", <X> being the rule number.

	Packet	Go to packet	Cancel
No.  Length  ID  Source  Destination	Info	Protocol	1
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: Ci	sco_b2:fe:ff (00:1e:f6:b2:fe:ff)		
> 802.10 Virtual LAN, PRI: 0, DEI: 0, ID: 39			
Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.1	130		
User Datagram Protocol, Src Port: 1812, Dst Port: 63772			
RADIUS Protocol			
Code: Access-Accept (2)			
Packet Identifier: 0X51 (81)			
Length: 323 Authenticator: 61242164ce20be86eed828b2ce566ef5			
This is a response to a request in frame 9036			
[Time from request: 0.007995000 seconds]			
Attribute Value Pairs			
> AVP: t=liser-Name(1) ]=32 va]=#ACSACL#-TP-ACL USER1-65e89aal			
<pre>&gt; AVP: t=Class(25) l=75 val=434143533a30613330323738366d6242</pre>	517239445259673447765f436554692f48737050-		
AVP: t=Message-Authenticator(80) l=18 val=a3c4b20cd1e64785	19e0232511cd8b72		
AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSvstems(9)			
Type: 26			
Length: 47			
Vendor ID: ciscoSystems (9)			
> VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#1=denv ip anv ho	pst 10.48.39.13		
<pre>~ AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSvstems(9)</pre>			
Type: 26			
Length: 47			
Vendor ID: ciscoSystems (9)			
> VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#2=deny ip any he	ost 10.48.39.15		
AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)			
Type: 26			
Length: 48			
Vendor ID: ciscoSystems (9)			
> VSA: t=Cisco-AVPair(1) l=42 val=ip:inacl#3=deny ip any he	ost 10.48.39.186		
AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)			
Type: 26			
Length: 36			
Vendor ID: ciscoSystems (9)			
> VSA: t=Cisco-AVPair(1) l=30 val=ip:inacl#4=permit ip any	any		
RADIUS Protocol (radius), 323 bytes	<ul> <li>Packets: 43372 - Displayed: 2 (0.0%)</li> </ul>		Profile: Default



**Note**: If the content of a download ACL is modified after it has been downloaded on the WLC, the change for this ACL is not reflected until a user using this one re-authenticates ( and the WLC perform a RADIUS authentication for such a user again). Indeed, a change in the ACL is reflected by a change in the hash part of the ACL name. Therefore, the next time this ACL is assigned to a user, its name must be different and thus, the ACL must not be part of the WLC configuration and is supposed to be downloaded. However, clients which authenticate before the change on the ACL continue to use the previous one until they fully re-authenticate.

### **ISE Operation Logs**

#### **RADIUS client authentication**

The operation logs show a successful authentication of the user "USER1", to which the downloadable ACL "ACL\_USER1" is applied. Parts of interest for troubleshooting are framed in red.

#### 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
Identity Group Audit Session Id	Unknown 8227300A000000D848ABE3F
Identity Group Audit Session Id Authentication Method	Unknown 8227300A0000000D848ABE3F dot1x
Identity Group Audit Session Id Authentication Method Authentication Protocol	Unknown 8227300A0000000B48ABE3F dol1x PEAP (EAP-MSCHAPv2)
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type	Unknown 8227300A0000000B48ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device	Unknown 8227300A0000000B48ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type	Unknown 8227300A0000000B48ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address	Unknown 8227300A0000000B48ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type	Unknown 8227300A0000000B48ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130 Wireless - IEEE 802.11
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type Authorization Profile	Unknown 8227300A0000000B48ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130 Wireless - IEEE 802.11 9800-DOT1X-USER1

#### 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;26SessionI D=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
AuthenticationStatus IdentityPolicyMatchedRule	AuthenticationPassed Dot1X
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched	AuthenticationPassed Dot1X 802.1x User 1 dACL
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Det1X 515
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147
AuthenticationStatus IdentityPelicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress IISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSSversion DTLSSupport	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSSversion DTLSSupport HostIdentityGroup	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco Locationt#All Locations
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location Device Type	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSV1.2 Unknown Endpoint Identity Groups:Unknown Cisco Locationt#All Locations Device Types/All Device Types
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location Device Type IPSEC	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSV1.2 Unknown Endpoint Identity Groups:Unknown Cisco LocationHAll Locations Device TypesHAII Device Types IPSECHIS IPSEC Device#No

EnableFlag	Enabled
RADIUS Username	USER1
NAS-Identifier	DACL_DOT1X_SSID
Device IP Address	10.48.39.130
CPMSessionID	8227300A000000D848ABE3F
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID
CiscoAVPair	service-type=Framed, audit-session-id=8227300A0000000D848ABE3F, method-dot1x, client-id=id=213031001, vlan-id=1413, cisco-wlan-ssid=DACL_DDT1X_SSID, wlan-profile-name=0ACL_DDT1X_SSID, AuthenticationdentityStore-internal Users, FQSubjectName=9273fs30-8c01-11e6-996c- 5524600485211wuer1, UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b 5c43

Result	
Class	CACS:8227300A000000D848ABE3F: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:b 9:93:27:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:c 5:c5:05:6f:55:bb:12:24:62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:0 6:9c:ef:3e:9f:f6
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1- 65e89aab
MS-MPPE-Send-Key	
MS-MPPE-Recv-Key	
LicenseTypes	Essential license consumed.
Session Events	
2024-03-28 05:11:11.035	Authentication succeeded

### **DACL Download**

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
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

The operation logs show a successful download of the ACL "ACL\_USER1". Parts of interest for troubleshooting are framed in red.

Cisco ISE				
Overview		Steps		
Event	5232 DACL Download Succeeded	11001	Received RADIUS Access-Request	
Username	WACSACL#-IP-ACL_USER1-65e89aab	11017	RADIUS created a new session	
Endpoint Id		11002	Returned RADIUS Access-Accept	
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		1	
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	IPSECHIs IPSEC Device#No			
RADIUS Username	#ACSACL#-IP-ACL_USER1-65e89aab			
Device IP Address	10.48.39.130			
CPMSessionID	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcs eM			
CiscoAVPair	aaa:service=ip_admission, aaa:event=acl=download			
Result				
Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfd FbcseM: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			