

# Configure & Troubleshoot Downloadable ACLs on Catalyst 9800

## Contents

---

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[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](#)

[Verify](#)

[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 [Cisco ISE configuration example](#) 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 [starting from Cisco IOS XE Dublin 17.10.1](#) 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).

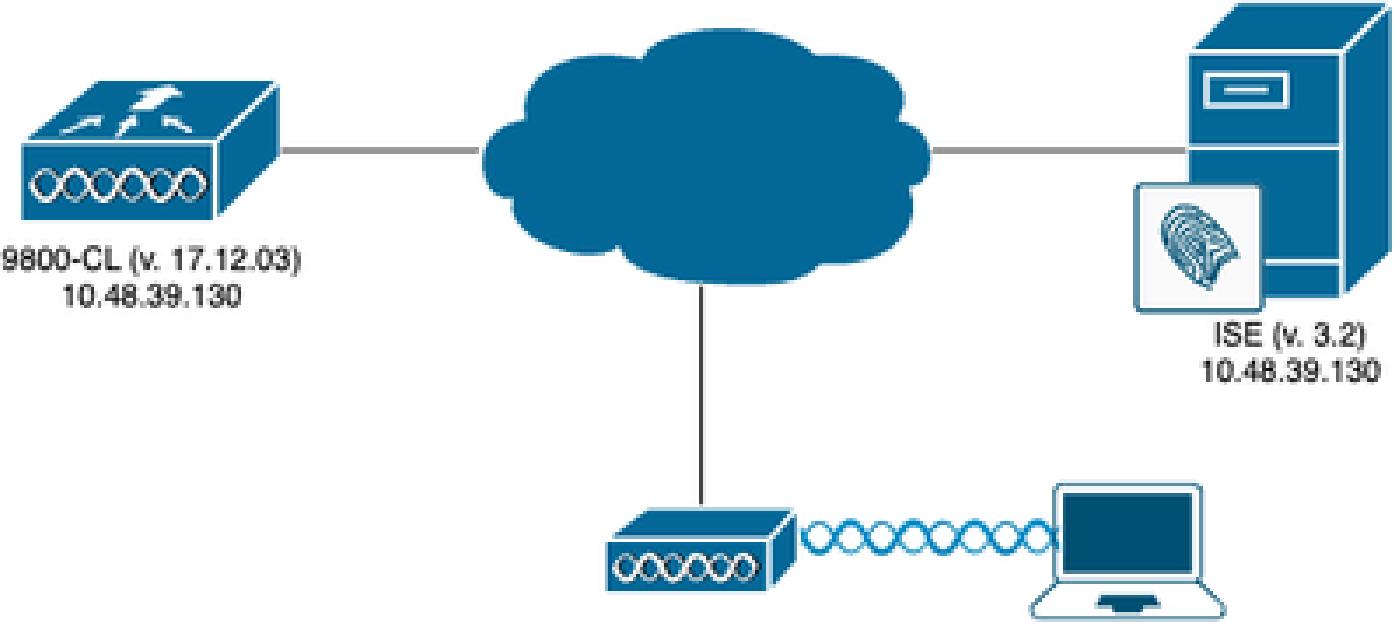
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## 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 [Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series](#) 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:

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

#### 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.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. On the left, the navigation menu includes Dashboard, Monitoring, Configuration (selected), Administration, Licensing, and Troubleshooting. A 'Walk Me Through' button is also present. The main area shows the 'Edit Policy Profile' dialog for 'DACL-8021X'. The 'General' tab is selected, displaying fields for Name\* (DACL-8021X), Description (Enter Description), Status (ENABLED), and other settings like Passive Client (DISABLED), IP MAC Binding (ENABLED), and Encrypted Traffic Analytics (DISABLED). The 'WLAN Switching Policy' section has two options: Central Switching (ENABLED) and Central Authentication (ENABLED), both highlighted with red boxes. The 'CTS Policy' section includes Inline Tagging and SGACL Enforcement checkboxes, both of which are unchecked. The 'Default SGT' field contains the value 2-65519. At the bottom, there are 'Cancel' and 'Update & Apply to Device' buttons.

The screenshot shows the 'Edit Policy Profile' dialog box from the Cisco Catalyst 9800-CL Wireless Controller. The 'Advanced' tab is active. In the 'AAA Policy' section, there is a checkbox labeled 'Allow AAA Override' which is checked and has a red box drawn around it. Other sections visible include 'WLAN Timeout', 'DHCP', 'DNS Layer Security', and 'Flex DHCP Option for DNS'.

### From the CLI:

```

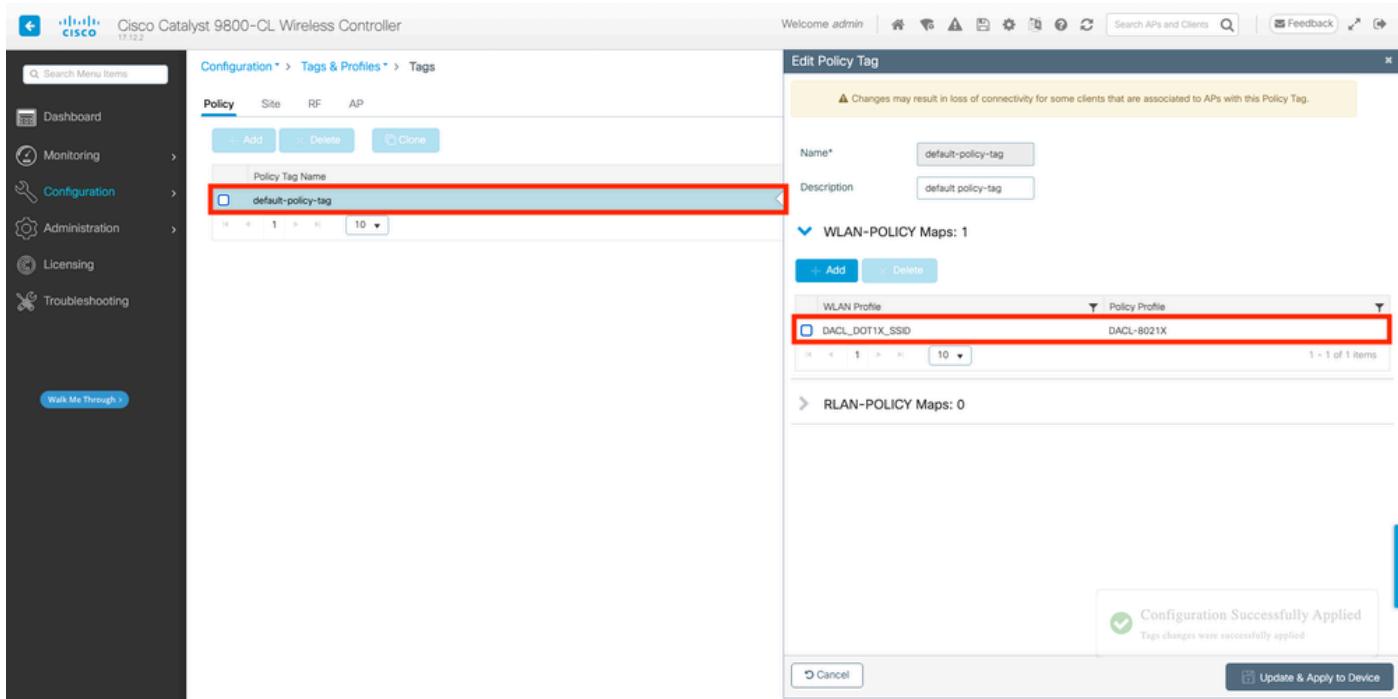
WLC#configure terminal
WLC(config)#wireless profile policy DACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown

```

### **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.

In other words: dACLs require the usage of "aaa authorization network" method.

One can use the default group radius with the command "aaa authorization network default group radius":

#### 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.

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

### From the CLI:

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

### NOTE:

If you do not want to define a default method, then you need to define a named method. In this case, it is a mandatory step to call out the AAA Authorization Method List that ISE needs to use, otherwise the WLC will be unable to download the ACL.

### On the WLC:

```
<#root>  
WLC(config)# aaa authorization network  
authZlist  
group authz-server-group
```

### On the ISE:

Send this attribute along with the dACL: cisco-av-pair = Method-List=**authZlist**

The screenshot shows two parts of the Cisco ISE configuration interface. The top part, 'Advanced Attributes Settings', displays a dropdown menu with 'Cisco:cisco-av-pair' selected, followed by an equals sign and a red-bordered input field containing 'Method-List=authZlist'. Below this is a minus sign and a plus sign. The bottom part, 'Attributes Details', shows a table with three rows: 'Access Type = ACCESS\_ACCEPT', 'DACL = TestDACLs', and 'cisco-av-pair = Method-List=authZlist', with the last row also red-bordered.

## 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**.

The screenshot shows the Cisco ISE Administration interface under the Identity Management section. The 'Settings' tab is selected. On the left, a sidebar lists 'User Custom Attributes' and other settings like 'User Authentication Settings' and 'Endpoint Purge'. The main area displays a table of attributes with columns: Mandatory, Attribute Name, and Data Type. The 'Name' attribute is highlighted with a green checkmark. Below this is a detailed view of 'User Custom Attributes' with columns: Attribute Name, Description, Data Type, Parameters, and Default Value Mandatory. A row for 'ACL' is selected and highlighted with a red box. At the bottom right are 'Save' and 'Reset' buttons.

Once this configured, use the "Save" button to save the 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.

The screenshot shows the Cisco ISE Policy - Policy Elements interface under the 'Results' tab. The 'Authorization' category is selected in the sidebar. The 'Downloadable ACLs' option is highlighted with a red box. The main area shows a list of existing ACLs with columns: Name and Description. An 'Edit' button, a red 'Add' button (which has a red arrow pointing to it), a 'Duplicate' button, and a 'Delete' button are at the top. A status bar at the bottom right indicates 'Selected 0 Total 7'.

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 allIpv4 Traffic
PERMIT_ALL_IPV6_TRAFFIC	Allow allIpv6 Traffic
test-dacl-cwa	
test-dacl-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 destined 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.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	ACL_USER1	ACL assigned to USER1
<input type="checkbox"/>	ACL_USER2	ACL assigned to USER2
<input type="checkbox"/>	DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
<input type="checkbox"/>	DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic Deny all ipv6 traffic
<input type="checkbox"/>	PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
<input type="checkbox"/>	PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic
<input type="checkbox"/>	test-dacl-cwa	
<input type="checkbox"/>	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.

The screenshot shows the Cisco ISE Administration - Identity Management interface. The top navigation bar includes 'Cisco ISE', 'Administration - Identity Management', 'License Warning', and various system icons. Below the navigation is a secondary menu with 'Identities' (highlighted with a red box), 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. On the left, a sidebar menu has 'Users' highlighted with a red box. The main content area is titled 'Network Access Users' and displays a table with one row. The table columns are Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. The single row shows 'Enabled' for Status, 'adminuser' for Username, and 'admin-group' for Admin. At the top of the table header, there are buttons for Edit, + Add (highlighted with a red box and an arrow pointing to it), Change Status, Import, Export, Delete, and Duplicate. To the right of the table, there are filters for 'Selected 0 Total 1' and 'All'.

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.

The screenshot shows the 'New Network Access User' configuration form. The 'Username' field is set to 'USER1' (highlighted with a red box). Under 'Passwords', the 'Login Password' and 'Re-Enter Password' fields are shown, both highlighted with red boxes. In the 'User Custom Attributes' section, the 'ACL' attribute is assigned to 'ACL\_USER1' (highlighted with a red box). At the bottom right of the form, the 'Save' button is highlighted with a red box.

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.

The screenshot shows the Cisco ISE Administration interface under the 'Identity Management' section. On the left, there's a sidebar with 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The main area is titled 'Network Access Users'. It has a toolbar with 'Edit', '+ Add', 'Change Status', 'Import', 'Export', 'Delete', and 'Duplicate'. Below the toolbar is a table header with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. Under the 'Status' column, there are three entries: 'Disabled' for 'adminuser', and 'Enabled' for 'USER1' and 'USER2'. A red box highlights these three entries. The 'User Identity Groups' column shows 'admin-group' for all users. The 'Admin' column shows a checkmark for 'USER1' and 'USER2', while 'adminuser' is not checked.

#### 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.

The screenshot shows the Cisco ISE Policy - Policy Elements interface. The left sidebar includes 'Dictionaries', 'Conditions', and 'Results'. Under 'Results', 'Authorization Profiles' is selected, showing a sub-menu for 'New Authorization Profile'. The 'Name' field is filled with '9800-DOT1X-USERS'. The 'Access Type' dropdown is set to 'ACCESS\_ACCEPT'. In the 'Common Tasks' section, there's a checkbox for 'DACL Name' which is checked and set to 'InternalUser:ACL'. Other options like 'IPv6 DACL Name' and 'ACL (Filter-ID)' are also present but not selected. A red box highlights the 'DACL Name' field and its value.

## 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 > 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.

The screenshot shows the Cisco ISE Policy Set interface. The top navigation bar includes 'Cisco ISE', 'Policy - Policy Sets', 'License Warning', and 'Save' buttons. The main area displays the 'Default' policy set with two sections highlighted:

- Authentication Policy (2):** Contains a 'Dot1X' rule with conditions 'Wired\_802.1X' and 'Wireless\_802.1X'. This section is highlighted with a red box.
- Authorization Policy (2):** Contains an '802.1x Users dACL' rule with a condition 'Radius-Called-Station-ID CONTAINS DACL\_DOT1X\_SSID'. This section is also highlighted with a red box.

Both sections show results for 'All\_User\_ID\_Stores' with hits counts of 65 and 10 respectively, and 'Options' buttons.

## 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 [Per-user dACLs section](#) 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.

The screenshot shows the Cisco ISE Administration - Identity Management interface. The top navigation bar includes 'Administration - Identity Management' and a 'License Warning' icon. Below the navigation, there are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' tab is selected and highlighted with a red box. On the left sidebar, the 'Users' section is also highlighted with a red box. The main content area displays a list titled 'Network Access Users' with one entry: 'adminuser'. The list includes columns for Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. A red arrow points to the '+ Add' button in the toolbar above the list. The toolbar also contains buttons for Edit, Change Status, Import, Export, Delete, and Duplicate. A status bar at the bottom right indicates 'Selected 0 Total 1'.

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

The screenshot shows the 'New Network Access User' configuration form. The top navigation bar includes 'Administration - Identity Management' and a 'License Warning' icon. Below the navigation, there are tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Identities' tab is selected and highlighted with a red box. On the left sidebar, the 'Users' section is also highlighted with a red box. The main content area shows a configuration form for a 'Network Access User'. The 'Username' field is set to 'USER1' and is highlighted with a red box. The 'Status' dropdown is set to 'Enabled'. The 'Passwords' section includes fields for 'Login Password' and 'Re-Enter Password', both of which are highlighted with a red box. There is also a 'Generate Password' button. At the bottom right of the form, there are 'Submit' and 'Cancel' buttons, with the 'Submit' button highlighted with a red box.

Repeat this step to create USER2.

The screenshot shows the Cisco ISE Administration interface under the Identity Management section. The left sidebar has 'Identities' selected. The main area is titled 'Network Access Users'. It includes a toolbar with 'Edit', '+ Add', 'Change Status', 'Import', 'Export', 'Delete', and 'Duplicate' buttons. Below the toolbar is a table header with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. Under the 'Status' column, there are three rows: 'Disabled' (checkbox), 'Enabled' (checkbox) for 'USER1', and 'Enabled' (checkbox) for 'USER2'. A red box highlights the 'Enabled' rows for both 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”.

The screenshot shows the Cisco ISE Policy - Policy Elements interface. The left sidebar has 'Authorization Profiles' selected. The main area is titled 'Results' and shows the 'Authorization Profile' configuration screen. The 'Name' field is set to '9800-DOT1X-USER1' (highlighted by a red box). The 'Access Type' dropdown is set to 'ACCESS\_ACCEPT' (highlighted by a red box). In the 'Common Tasks' section, the 'DACL Name' dropdown is set to 'ACL\_USER1' (highlighted by a red box). At the bottom right, there are 'Submit' and 'Cancel' buttons, with 'Submit' highlighted by a red box.

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

The screenshot shows the Cisco ISE Policy - Policy Elements interface. On the left, there's a navigation sidebar with sections like Dictionaries, Conditions, Results, Authorization, Authentication, Authorization Profiles, Downloadable ACLs, Profiling, Feature, and Client Provisioning. The 'Results' tab is selected. In the center, under 'Standard Authorization Profiles', there's a table with columns: Name, Profile, and Description. Two profiles are highlighted with a red box: '9800-DOT1X-USER1' and '9800-DOT1X-USER2'. Both are associated with the 'Cisco' profile. The descriptions for these two profiles mention they are for '802.1x users using dACLs'. Other profiles listed include '802-DOT1X-USERS', 'Block\_Wireless\_Access', 'Cisco\_IP\_Phones', 'Cisco\_Temporal\_Onboard', 'Cisco\_WiFiAuth', 'InternalUserAttributeTest', 'NAP\_Onboard', 'Non\_Cisco\_IP\_Phones', 'UDN', 'DenyAccess', and 'PermitAccess'. A status bar at the top right indicates 'Selected 0 Total 13'.

Name	Profile	Description
9800-DOT1X-USER1	Cisco	Authorization profile for 802.1x users using dACLs.
9800-DOT1X-USER2	Cisco	Authorization profile for 802.1x users using dACLs.
802-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_WiFiAuth	Cisco	Default Profile used to redirect users to the CWA portal.
InternalUserAttributeTest	Cisco	
NAP_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.

### 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 configured for username USER2, for which "9800-DOT1X-USER1" is used.

The screenshot shows the Cisco ISE Policy Sets interface. At the top, there's a header with 'Cisco ISE' and 'Policy - Policy Sets'. Below the header, the 'Default' policy set is selected. The interface is divided into two main sections: 'Authentication Policy' and 'Authorization Policy'.

**Authentication Policy:** This section lists rules based on conditions like 'dot1X' or 'Default'. One rule, 'dot1X', has its conditions expanded, showing 'Wired\_802.1X' and 'Wireless\_802.1X' under 'OR'. These conditions are highlighted with a red box. To the right, there are columns for 'Use', 'Hits', and 'Actions'.

**Authorization Policy:** This section lists rules for users like '802.1x user 2 dACL' and '802.1x user 1 dACL'. These rules also have their conditions expanded, showing 'InterUser Name EQUALS USER2' and 'InterUser Name EQUALS USER1'. These conditions are also highlighted with a red box. To the right, there are columns for 'Results', 'Profiles', 'Security Groups', 'Hits', and 'Actions'.

## Notes About Using dACLs with CWA SSIDs

As described in the [Configure Central Web Authentication \(CWA\) on Catalyst 9800 WLC and ISE](#) 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 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
!
!
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]^PVANfcbR0b
!
!
[...]
wireless profile policy DACL-8021X
    aaa-override
    wlan 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
```

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
IIF ID           : 0x90000012
Authorized       : TRUE
Session timeout   : 28800
Common Session ID: 8227300A0000000C8484A22F
Acct Session ID  : 0x00000000
Last Tried Aaa Server Details:
```

```
    Server IP : 10.48.39.134
```

#### Auth Method Status List

```
    Method : Dot1x
```

```
        SM State      : AUTHENTICATED
```

```
        SM Bend State : IDLE
```

#### Local Policies:

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

#### Server Policies:

```
ACS ACL          : xACSAACLx-IP-ACL_USER1-65e89aab
```

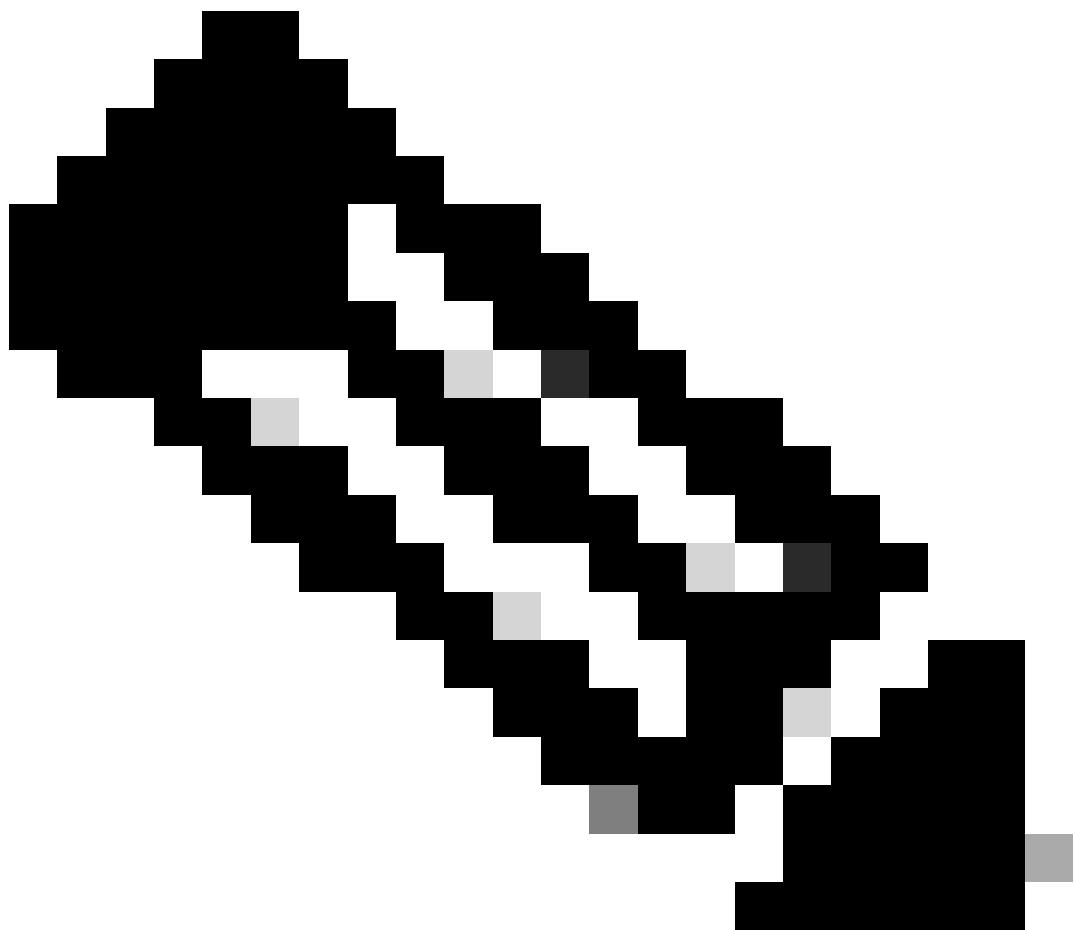
#### Resultant Policies:

```
ACS ACL          : xACSAACLx-IP-ACL_USER1-65e89aab
VLAN Name        : VLAN_1413
VLAN             : 1413
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 xACSAACLx-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 xACSAACLx-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 [radioactive traces](#) 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 Association

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

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

[...]

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

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

[...]

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

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 Client

[...]

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

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

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

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

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

```

[...]

2024/03/28 10:43:04.381397739 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to [redacted]  
2024/03/28 10:43:04.381411901 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator e9 8b e [redacted]  
2024/03/28 10:43:04.381425481 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 7 "USERID  
2024/03/28 10:43:04.381430559 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Service-Type [6] 6 Fr [redacted]  
2024/03/28 10:43:04.381433583 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 27 [redacted]  
2024/03/28 10:43:04.381437476 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 21 " [redacted]  
2024/03/28 10:43:04.381440925 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Framed-MTU [12] 6 148 [redacted]  
2024/03/28 10:43:04.381452676 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 12 . [redacted]  
2024/03/28 10:43:04.381466839 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator [redacted]  
2024/03/28 10:43:04.381482891 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Key-Name [102] 2 [redacted]  
2024/03/28 10:43:04.381486879 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 49 [redacted]  
2024/03/28 10:43:04.381489488 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 43 " [redacted]  
2024/03/28 10:43:04.381491463 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20 [redacted]  
2024/03/28 10:43:04.381494016 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 " [redacted]  
2024/03/28 10:43:04.381495896 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32 [redacted]  
2024/03/28 10:43:04.381498320 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 " [redacted]  
2024/03/28 10:43:04.381500186 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20 [redacted]  
2024/03/28 10:43:04.381502409 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 " [redacted]  
  
2024/03/28 10:43:04.381506029 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6 1 [redacted]  
  
2024/03/28 10:43:04.381509052 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port-Type [61] 6 [redacted]  
2024/03/28 10:43:04.381511493 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port [5] 6 3913 [redacted]  
2024/03/28 10:43:04.381513163 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 39 [redacted]  
2024/03/28 10:43:04.381515481 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 33 " [redacted]  
  
2024/03/28 10:43:04.381517373 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 41 [redacted]  
2024/03/28 10:43:04.381519675 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 35 " [redacted]  
  
2024/03/28 10:43:04.381522158 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Called-Station-Id [30] [redacted]  
2024/03/28 10:43:04.381524583 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Calling-Station-Id [30] [redacted]  
2024/03/28 10:43:04.381532045 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Airespace [26] [redacted]  
2024/03/28 10:43:04.381534716 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Airespace-WLAN-ID [1] [redacted]  
2024/03/28 10:43:04.381537215 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Nas-Identifier [32] 17 [redacted]  
  
2024/03/28 10:43:04.381539951 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [188] [redacted]  
2024/03/28 10:43:04.381542233 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[188] [redacted]  
2024/03/28 10:43:04.381544465 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188] [redacted]  
2024/03/28 10:43:04.381619890 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout [redacted]  
[...]  
2024/03/28 10:43:04.392544173 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812 [redacted]  
  
2024/03/28 10:43:04.392557998 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 08 6d f [redacted]  
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\_90000012]  
  
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\_90000012]  
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\_90000012]  
  
2024/03/28 10:43:04.727164223 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
2024/03/28 10:43:04.727169069 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
  
2024/03/28 10:43:04.727223736 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : user  
  
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\$®vf9JØ«¤ý0@≤™ÇÑbWü6\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\_90000012]  
  
2024/03/28 10:43:04.727513133 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
  
2024/03/28 10:43:04.727607738 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: SVM Apply user profile  
2024/03/28 10:43:04.728003638 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: Activating EPM feature  
  
2024/03/28 10:43:04.728144450 {wncd\_x\_R0-0}{1}: [epm-misc] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
  
2024/03/28 10:43:04.728161361 {wncd\_x\_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
2024/03/28 10:43:04.728177773 {wncd\_x\_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
2024/03/28 10:43:04.728184975 {wncd\_x\_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
  
2024/03/28 10:43:04.728218783 {wncd\_x\_R0-0}{1}: [epm-acl] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
  
2024/03/28 10:43:04.729005675 {wncd\_x\_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
2024/03/28 10:43:04.729019215 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: Response of epm is 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 30

2024/03/28 10:43:04.729432771 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6 1

2024/03/28 10:43:04.729435487 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.729437912 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32

2024/03/28 10:43:04.729440782 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "a

2024/03/28 10:43:04.729442854 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 30

2024/03/28 10:43:04.729445280 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 24 "a

2024/03/28 10:43:04.729447530 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator

2024/03/28 10:43:04.729529806 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout

2024/03/28 10:43:04.731972466 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812/

2024/03/28 10:43:04.731979444 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 2a 24 8

2024/03/28 10:43:04.731983966 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.731986470 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Class [25] 75 ...

2024/03/28 10:43:04.732032438 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator

2024/03/28 10:43:04.732048785 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732051657 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 "i

2024/03/28 10:43:04.732053782 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732056351 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 "i

2024/03/28 10:43:04.732058379 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 48

2024/03/28 10:43:04.732060673 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 42 "i

2024/03/28 10:43:04.732062574 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 36

2024/03/28 10:43:04.732064854 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 30 "i

2024/03/28 10:43:04.732114294 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t  
[...]

2024/03/28 10:43:04.733046258 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): [08be.ac14.137d] Applied User Pr

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\$®vf9jØø«%ÿ0ä@≤™CÑbWï6\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\_9000001234567890]  
  
2024/03/28 10:43:04.733486604 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 A  
2024/03/28 10:43:04.734665244 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client  
  
2024/03/28 10:43:04.734894043 {wncd\_x\_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d E  
2024/03/28 10:43:04.734904452 {wncd\_x\_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d C  
  
2024/03/28 10:43:04.734915743 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_9000001234567890]  
  
  
2024/03/28 10:43:04.740499944 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= o  
  
  
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= o  
  
[...]  
  
2024/03/28 10:43:04.745245318 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl 1  
  
2024/03/28 10:43:04.745294050 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Allocated  
2024/03/28 10:43:04.745326416 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in  
  
  
2024/03/28 10:43:04.751291844 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= o  
  
  
2024/03/28 10:43:04.751943577 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A  
  
  
2024/03/28 10:43:04.752686055 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client  
  
  
2024/03/28 10:43:04.755505991 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= o

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 I  
2024/03/28 10:43:04.758843625 {wncd\_x\_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d IE  
  
2024/03/28 10:43:04.759064834 {wncd\_x\_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d IE  
  
2024/03/28 10:43:04.761186727 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl I  
  
2024/03/28 10:43:04.761241972 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in  
  
2024/03/28 10:43:04.763131516 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client  
  
2024/03/28 10:43:04.764575895 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c  
  
2024/03/28 10:43:04.764755847 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A  
  
2024/03/28 10:43:04.769965195 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c  
  
2024/03/28 10:43:04.770727027 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c  
  
2024/03/28 10:43:04.772314586 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl I  
  
2024/03/28 10:43:04.772362837 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in  
  
2024/03/28 10:43:04.773070456 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c  
  
2024/03/28 10:43:04.773661861 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A  
  
2024/03/28 10:43:04.775537766 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c  
  
2024/03/28 10:43:04.777154567 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c  
  
2024/03/28 10:43:04.778756670 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl I  
  
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 notification received from interface wncd_x_R0-0

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

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

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

2024/03/28 10:43:04.786433419 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interface wncd_x_R0-0
2024/03/28 10:43:04.786523172 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interface wncd_x_R0-0
2024/03/28 10:43:04.787787313 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interface wncd_x_R0-0
2024/03/28 10:43:04.788160929 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interface wncd_x_R0-0
2024/03/28 10:43:04.788491833 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (note): MAC: 08be.ac14.137d Client IP Learned
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, old: 08be.ac14.137d:capwap_9000, new: 08be.ac14.137d:capwap_9000
2024/03/28 10:43:04.788761575 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [19620]: (info): [08be.ac14.137d:capwap_9000]
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 Learned

2024/03/28 10:43:04.789410101 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d Client IP Learned
2024/03/28 10:43:04.789622587 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute : user_name : user_name ]
2024/03/28 10:43:04.789632684 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute : cipher_suite : cipher_suite ]
2024/03/28 10:43:04.789642576 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute : cipher_suite : cipher_suite ]
2024/03/28 10:43:04.789651931 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute : bsn : bsn ]

2024/03/28 10:43:04.789653490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute : t1 : t1 ]
2024/03/28 10:43:04.789735556 {wncd_x_R0-0}{1}: [ewlc-qos-client] [19620]: (info): MAC: 08be.ac14.137d Client IP Learned
2024/03/28 10:43:04.789800998 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [19620]: (debug): Managed client RADIUS authentication successful

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

## 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).

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
> 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]
> 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=Frame-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=Vendor-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=Frame-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=333743504d53657373696f6e49443d383232373330304130303030303039463834393335...
  > 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(32) 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
  
```

Packets: 56012 - Displayed: 2 (0.0%) - Ignored: 1 (0.0%) 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	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: 63772, Dst Port: 1812
> 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]
> Attribute Value Pairs
  > AVP: t=User-Name(1) l=7 val=USER1
  > AVP: t=Class(25) l=48 val=a34143533a38323237333030413030303030394638343933354132443a6973652f3439...
  > AVP: t=EAP-Message(79) l=6 Last Segment[1]
  > AVP: t=Message-Authenticator(80) l=18 val=de01c27a418e8289d5d6b2916sec872
  > AVP: t=Vendor-Key-Name(102) l=67 val=031f\005c01\0031VE 00\x\0020\00R0\033q\0076\000040\021(0Q\0\035/s 0a\0d0y\0270060000F0d
  > AVP: t=Vendor-Specific(26) l=66 vnd=ciscoSystems(9)
    Type: 26
    Length: 66
    Vendor ID: ciscoSvstems (9)
  > 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)
  
```

Packets: 56012 - Displayed: 2 (0.0%) - Ignored: 1 (0.0%) Profile: Default

## 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.

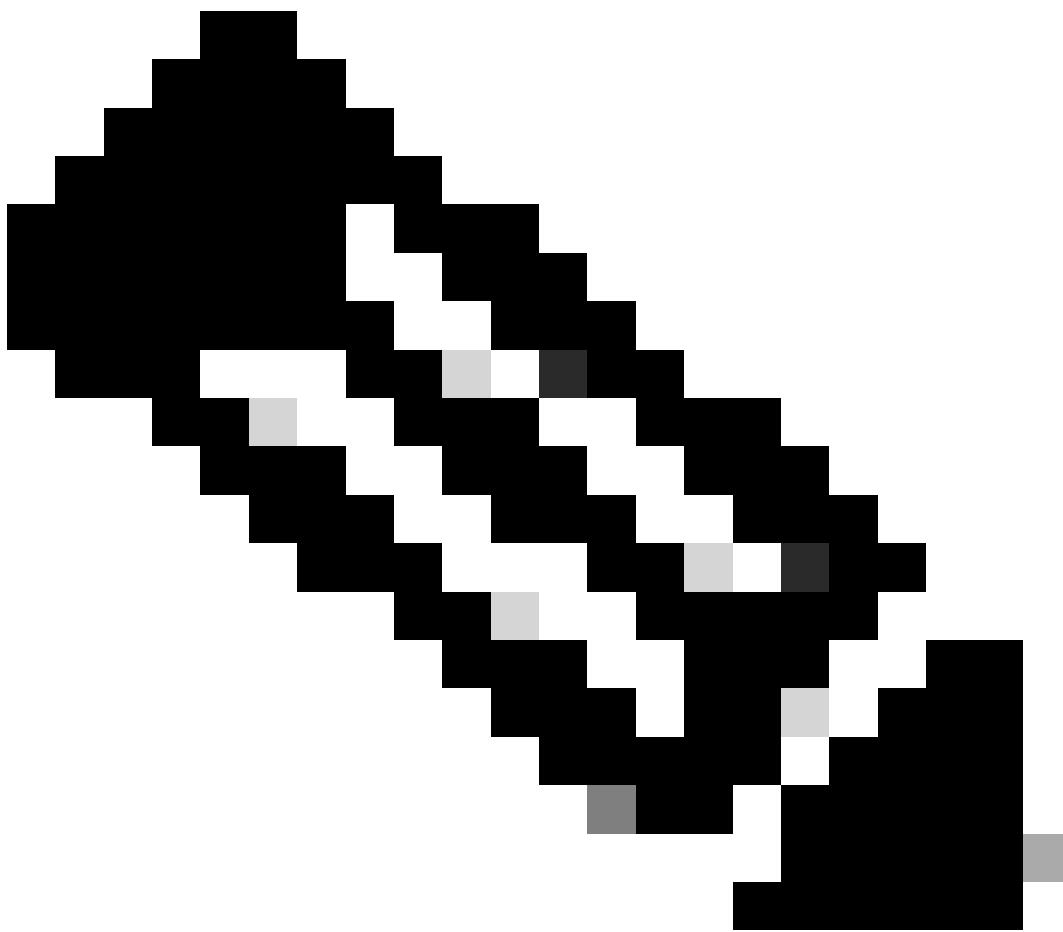
No.	Length	ID	Source	Destination	Info	Protocol
8037	184	39	10.48.39.130	10.48.39.134	Access-Request id=81, Duplicate Request	RADIUS
8038	369	39	10.48.39.134	10.48.39.130	Access-Accept id=81	RADIUS

> 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  
+ RADIUS Protocol  
Code: Access-Request (1)  
Packet identifier: 0x51 (81)  
Length: 138  
Authenticator: b216948576c8a46a51899e72d070945a  
[Duplicate Request Frame Number: 8036]  
[The response to this request is in frame 8038]  
- Attribute Value Pairs  
> AVP: t=NAS-IP-Address(4) l=6 val=10.48.39.130  
- AVP: t=User-Name(1) l=32 val=#ACSAACL#-IP-ACL\_USER1-65e89aab  
Type: 1  
Length: 32  
User-Name: #ACSAACL#-IP-ACL\_USER1-65e89aab  
> AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)  
- AVP: t=Vendor-Specific(26) l=30 vnd=ciscoSystems(9)  
Type: 26  
Length: 30  
Vendor ID: ciscoSystems (9)  
- 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

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.

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  
+ 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]  
- Attribute Value Pairs  
> AVP: t=User-Name(1) l=32 val=#ACSAACL#-IP-ACL\_USER1-65e89aab  
> AVP: t=Class(25) l=75 val=434143533a061330323738366d624251723945259673447765f436554692f48737050..  
> AVP: t=Message-Authenticator(80) l=18 val=a3c4b20cd1e64785d9e0232511cd8b72  
- AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)  
Type: 26  
Length: 47  
Vendor ID: ciscoSystems (9)  
> VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#1=deny ip any host 10.48.39.13  
- AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)  
Type: 26  
Length: 47  
Vendor ID: ciscoSystems (9)  
> VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#2=deny ip any host 10.48.39.15  
- AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)  
Type: 26  
Length: 48  
Vendor ID: ciscoSystems (9)  
> VSA: t=Cisco-AVPair(1) l=42 val=ip:inacl#3=deny ip any host 10.48.39.186  
- AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)  
Type: 26  
Length: 36  
Vendor ID: ciscoSystems (9)  
> VSA: t=Cisco-AVPair(1) l=30 val=ip:inacl#4=permit ip any any



**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.

Overview		Steps
Event	5200 Authentication succeeded	11001 Received RADIUS Access-Request
Username	USER1	11017 RADIUS created a new session
Endpoint Id	08:BE:AC:14:13:7D ⓘ	15049 Evaluating Policy Group
Endpoint Profile	Unknown	15008 Evaluating Service Selection Policy
Authentication Policy	Default >> Dot1X	11507 Extracted EAP-Response/Identity
Authorization Policy	Default >> 802.1x User 1 dACL	12500 Prepared EAP-Request proposing EAP-TLS with challenge
Authorization Result	9800-DOT1X-USER1	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
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	12301 Extracted EAP-Response/NAK requesting to use PEAP instead
Username	USER1	12300 Prepared EAP-Request proposing PEAP with challenge
User Type	User	12625 Valid EAP-Key-Name attribute received
Endpoint Id	08:BE:AC:14:13:7D	11006 Returned RADIUS Access-Challenge
Calling Station Id	08-be-ac-14-13-7d	11001 Received RADIUS Access-Request
Endpoint Profile	Unknown	11018 RADIUS is re-using an existing session
Authentication Identity Store	Internal Users	12302 Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated
Identity Group	Unknown	12318 Successfully negotiated PEAP version 0
Audit Session Id	8227300A0000000D848ABE3F	12800 Extracted first TLS record; TLS handshake started
Authentication Method	dot1x	12805 Extracted TLS ClientHello message
Authentication Protocol	PEAP (EAP-MSCHAPv2)	12806 Prepared TLS ServerHello message
Service Type	Framed	12807 Prepared TLS Certificate message
Network Device	gdefland-9800	12808 Prepared TLS ServerKeyExchange message
Device Type	All Device Types	12810 Prepared TLS ServerDone message
Location	All Locations	12305 Prepared EAP-Request with another PEAP challenge
NAS IPv4 Address	10.48.39.130	11006 Returned RADIUS Access-Challenge
NAS Port Type	Wireless - IEEE 802.11	11001 Received RADIUS Access-Request
Authorization Profile	9800-DOT1X-USER1	11018 RADIUS is re-using an existing session
Response Time	368 milliseconds	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		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 - Normalized 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
IdentityPolicyMatchedRule	Dot1X	11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response
AuthorizationPolicyMatched...	802.1x User 1 dACL	11814 Inner EAP-MSCHAP authentication succeeded 11519 Prepared EAP-Success for inner EAP method
EndPointMACAddress	08-BE-AC-14-13-7D	12314 PEAP inner method finished successfully 12305 Prepared EAP-Request with another PEAP challenge
ISEPolicySetName	Default	11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request
IdentitySelectionMatchedRule	Dot1X	11018 RADIUS is re-using an existing session 12304 Extracted EAP-Response containing PEAP challenge-response
TotalAuthenLatency	515	15041 Evaluating Identity Policy 15048 Queried PIP - Normalized Radius.RadiusFlowType
ClientLatency	147	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
TLSVersion	TLSv1.2	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
DTLSSupport	Unknown	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
HostIdentityGroup	Endpoint Identity Groups:Unknown	
Network Device Profile	Cisco	
Location	Location>All Locations	
Device Type	Device TypeAll Device Types	
IPSEC	IPSEC#Is IPSEC Device#No	
Name	USER1	
EnableFlag	Enabled	
RADIUS Username	USER1	
NAS-Identifier	DACL_DOT1X_SSID	
Device IP Address	10.48.39.130	
CPMSessionID	8227300A0000000D848ABE3F	
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID	
CiscoAVPair		service-type=Frameless, audit-session-id=8227300A0000000D848ABE3F, method=dot1x, client-if-id=2113931001, vlan-id=1413, cisco-wlan-ssid=DACL_DOT1X_SSID, wlan-profile-name=DACL_DOT1X_SSID, AuthenticationIdentityStore=Internal Users, FQSubjectName=9273fe30-8c01-11e6-996c- 525400b48521#user1, UniqueSubjectID=94b3604f5b49b88ccfabe2f3a86c80d1979b 5c43
Result		
Class	CACS:8227300A0000000D848ABE3F:ise/499610885/35 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:f6:85:82:04:0a:c 5:c5:05:d6:57:5b:f1:d2:62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:0 6:9:c:ef:3e:9f:f6	
EAP-Key-Name	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

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	#ACSAACL#-IP-ACL_USER1-65e89aab	11017 RADIUS created a new session
Endpoint Id		11117 Generated a new session ID
Endpoint Profile		11002 Returned RADIUS Access-Accept
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	#ACSAACL#-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 TypeAll Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	#ACSAACL#-IP-ACL_USER1-65e89aab
Device IP Address	10.48.39.130
CPMSessionID	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcseM:ise/499610885/48eM
CiscoAVPair	aaa:service=ip_admission, aaa:event=acl-download

Result	
Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcseM:ise/499610885/48
cisco-av-pair	ip:inac1#1<deny ip any host 10.48.39.13
cisco-av-pair	ip:inac1#2<deny ip any host 10.48.39.15
cisco-av-pair	ip:inac1#3<deny ip any host 10.48.39.186
cisco-av-pair	ip:inac1#4<permit ip any any