

# Configuración de & Resolución de problemas de ACL descargables en Catalyst 9800

## Contenido

---

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Uso de dACL con SSID 802.1x](#)

[Diagrama de la red](#)

[Configuración de WLC](#)

[Configuración de ISE](#)

[dACL por usuario](#)

[dACL por resultado](#)

[Notas sobre el uso de dACL con SSID de CWA](#)

[Verificación](#)

[Troubleshoot](#)

[Lista de Verificación](#)

[WLC One Stop-Shop Reflex](#)

[Comandos Show de WLC](#)

[Depuración condicional y seguimiento activo por radio](#)

[Captura de paquete](#)

[autenticación de cliente RADIUS](#)

[Descarga de DACL](#)

[Registros de funcionamiento de ISE](#)

[autenticación de cliente RADIUS](#)

[Descarga de DACL](#)

---

## Introducción

Este documento describe cómo configurar y resolver problemas de ACL descargables (dACL) en el controlador de LAN inalámbrica (WLC) Catalyst 9800.

## Antecedentes

Los dACL han sido soportados durante muchos años en los switches Cisco IOS® e IOS XE®. Una dACL se refiere al hecho de que el dispositivo de red descarga dinámicamente las entradas

ACL del servidor RADIUS cuando ocurre la autenticación, en lugar de tener una copia local de la ACL y simplemente se le asigna el nombre ACL. Está disponible un ejemplo más completo de [configuración de Cisco ISE](#). Este documento se centra en Cisco Catalyst 9800, que soporta dACL para el switching central desde la versión 17.10.

## Prerequisites

La idea detrás de este documento es demostrar el uso de dACL en Catalyst 9800 a través de un ejemplo de configuración SSID básico, mostrando cómo estos pueden ser completamente personalizables.

En el controlador inalámbrico Catalyst 9800, las ACL descargables son

- Compatible [a partir de Cisco IOS XE Dublin 17.10.1](#) release.
- Compatible únicamente con controladores centralizados con puntos de acceso de modo local (o switching central Flexconnect). El switching local de FlexConnect no admite dACL.

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modelo de configuración de Catalyst Wireless 9800.
- Listas de control de acceso (ACL) IP de Cisco.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

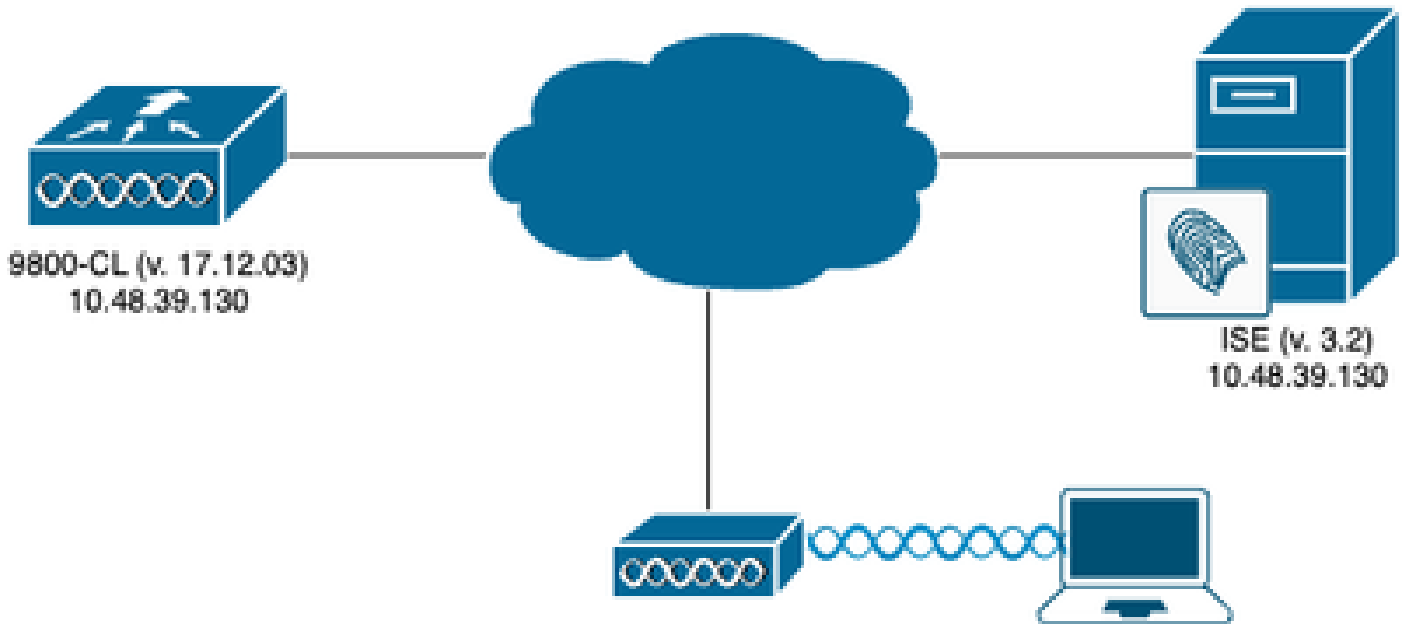
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

En esta guía de configuración, incluso si los métodos son diferentes (por ejemplo, autenticación WLAN, configuración de políticas, etc.), el resultado final es el mismo. En el escenario expuesto aquí, se definen dos identidades de usuario: USER1 y USER2. Ambos tienen acceso a la red inalámbrica. A cada uno de ellos se le asigna, respectivamente, ACL\_USER1 y ACL\_USER2 siendo dACL descargadas por el Catalyst 9800 desde ISE.

# Uso de dACL con SSID 802.1x

## Diagrama de la red



## Configuración de WLC

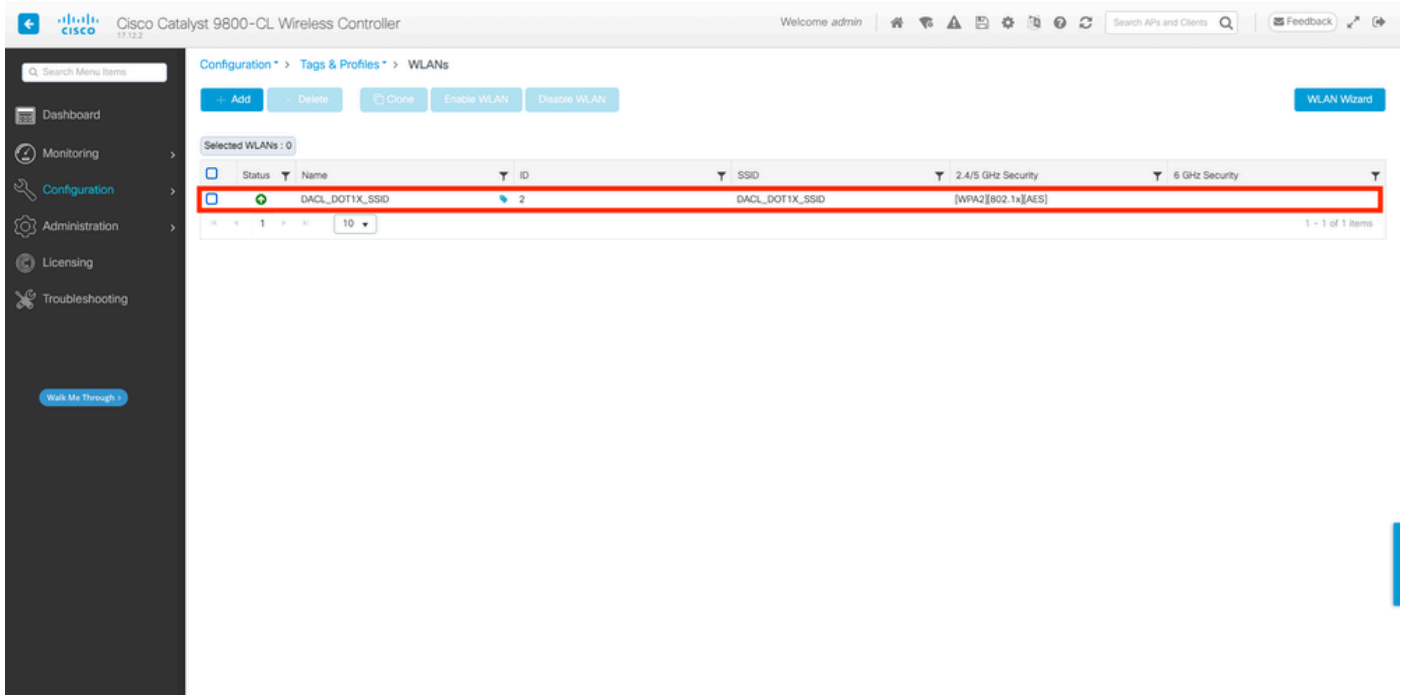
Para obtener detalles sobre la configuración de SSID 802.1x y la resolución de problemas en el Catalyst 9800, consulte la guía de configuración [Configure 802.1X Authentication on Catalyst 9800 Wireless Controller Series](#).

Paso 1. Configure el SSID.

Configure un SSID autenticado 802.1x mediante ISE como servidor RADIUS. En este documento, el SSID se ha denominado "DACL\_DOT1X\_SSID".

Desde la GUI:

Navigue hasta Configuration > Tags & Profiles > WLAN y cree una WLAN similar a la que se muestra aquí:



### Desde la 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
```

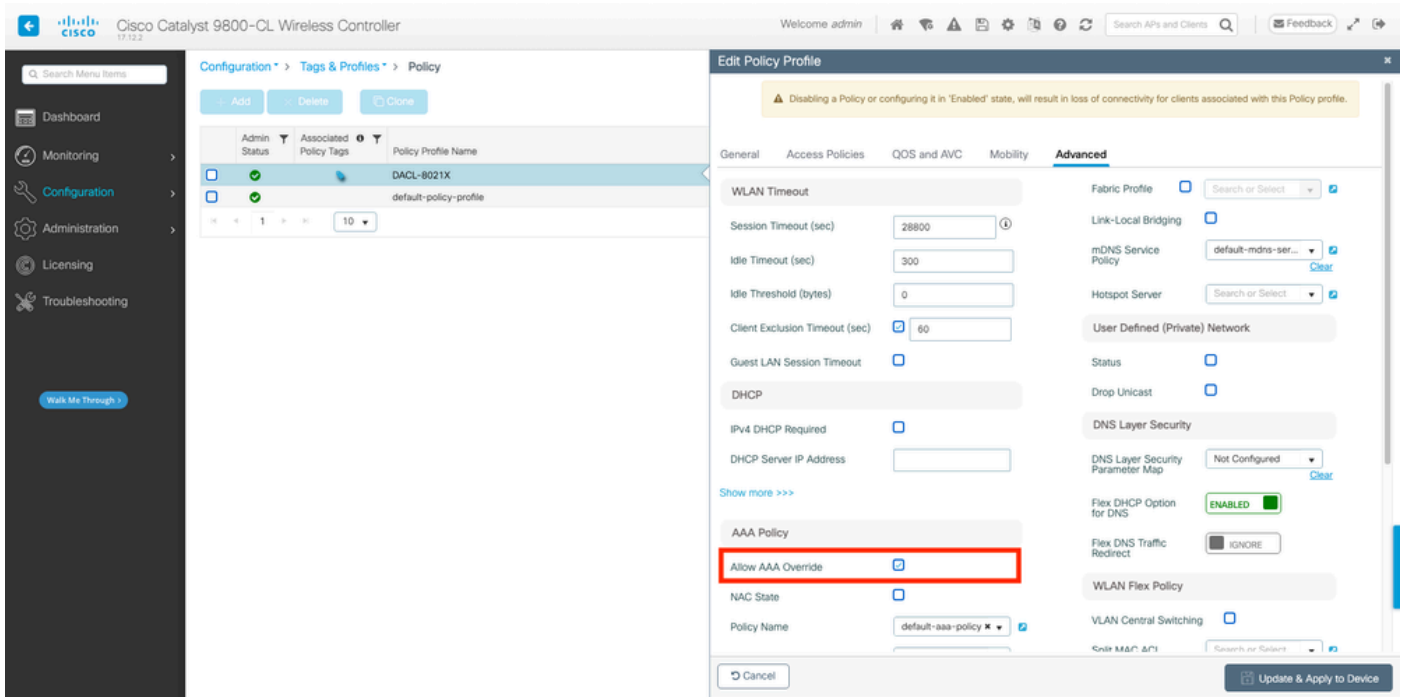
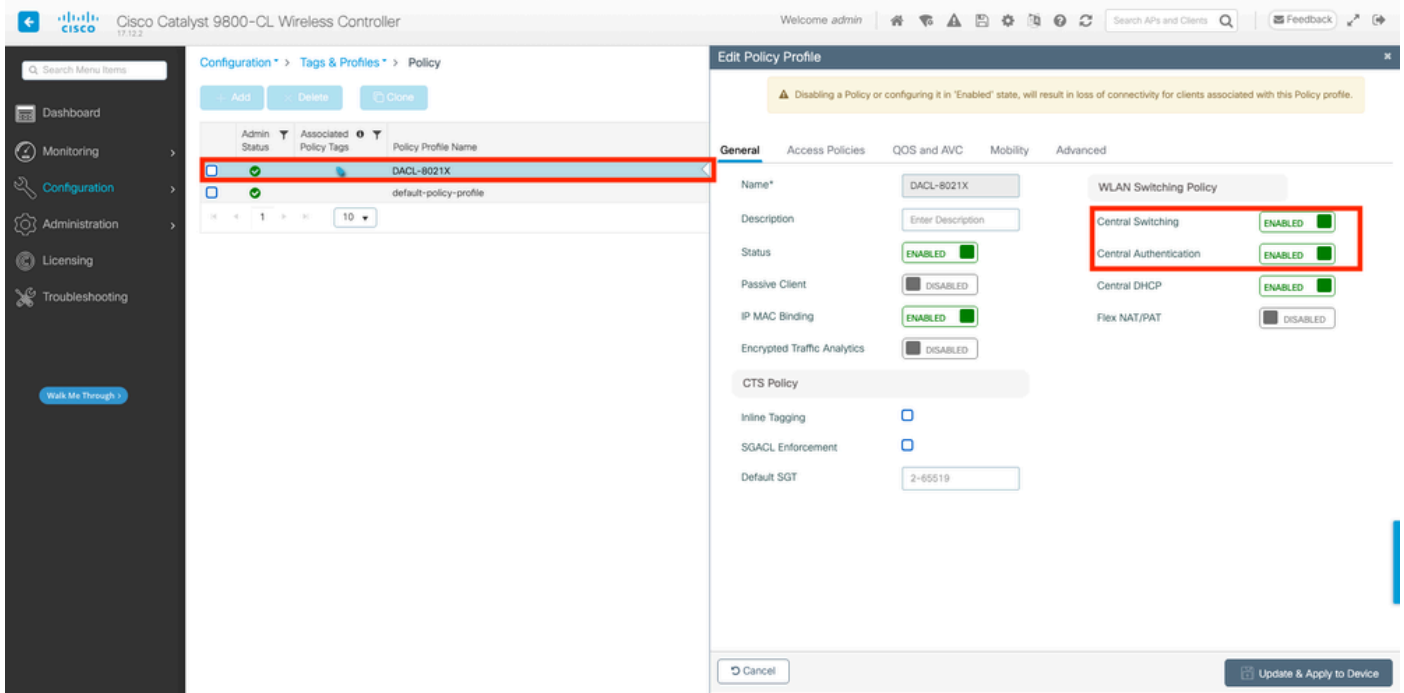
### Paso 2. Configure el perfil de directiva.

Configure el perfil de política que se utiliza junto con el SSID definido anteriormente. En este perfil de política, asegúrese de que la anulación de AAA esté configurada desde la ficha "Avanzado", como se muestra en la captura de pantalla. En este documento, el perfil de política utilizado es "DACL-8021X".

Como se indica en la sección de requisitos previos, las dACL solo son compatibles con implementaciones de switching/autenticación centrales. Asegúrese de que el perfil de directiva esté configurado de esa manera.

### Desde la GUI:

Vaya a Configuration > Tags & Profiles > Policy, seleccione el perfil de política utilizado y configúrelo como se muestra.



Desde la CLI:

```

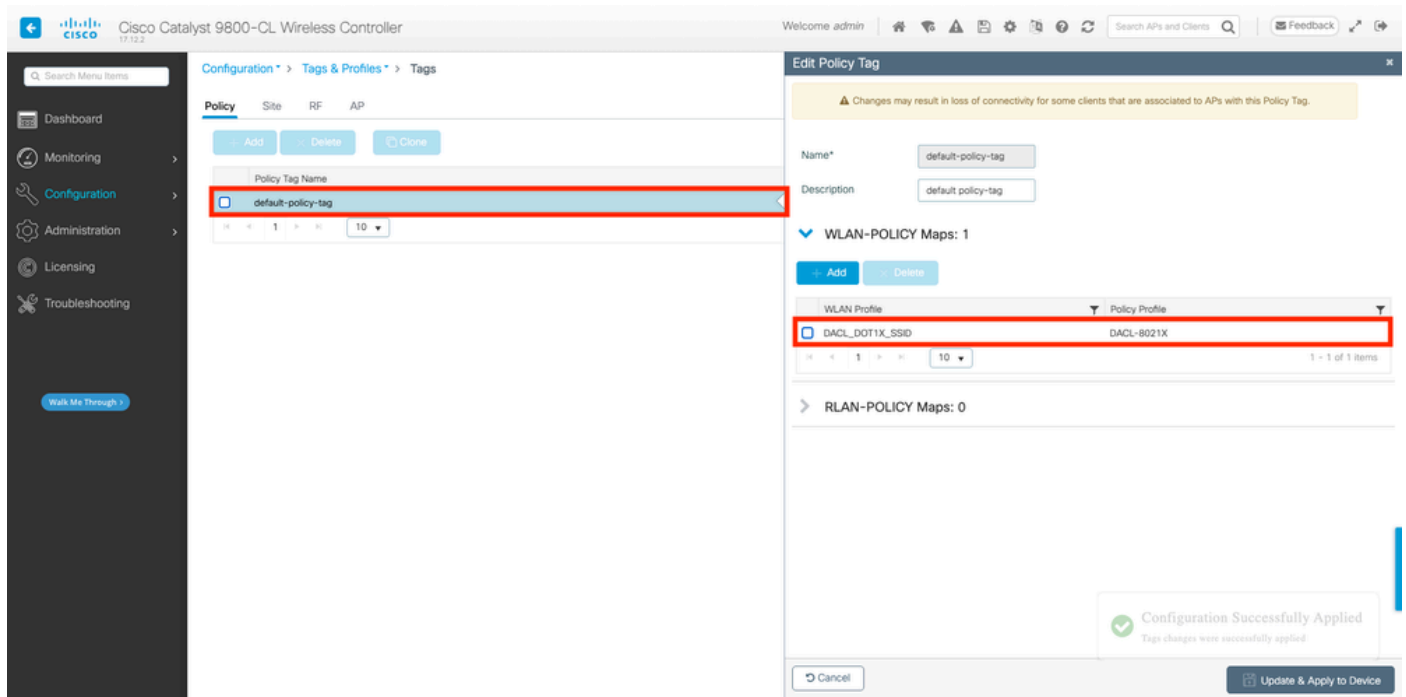
WLC#configure terminal
WLC(config)#wireless profile policy DAACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown

```

Paso 3. Asigne el perfil de directiva y el SSID a la etiqueta de directiva utilizada.

## Desde la GUI:

Vaya a Configuration > Tags & Profiles > Tags. En la ficha Etiquetas de directiva, cree (o seleccione) la etiqueta utilizada y asíguele el perfil de directiva y WLAN definido durante los pasos 1-2.



## Desde la 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 DAACL_DOT1X_SSID policy DAACL-8021X
```

Paso 4. Permitir atributo específico del proveedor.

Las ACL descargables se transfieren a través de atributos específicos del proveedor (VSA) en el intercambio RADIUS entre ISE y el WLC. El soporte de estos atributos se puede habilitar en el WLC, usando estos comandos CLI.

## Desde la CLI:

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

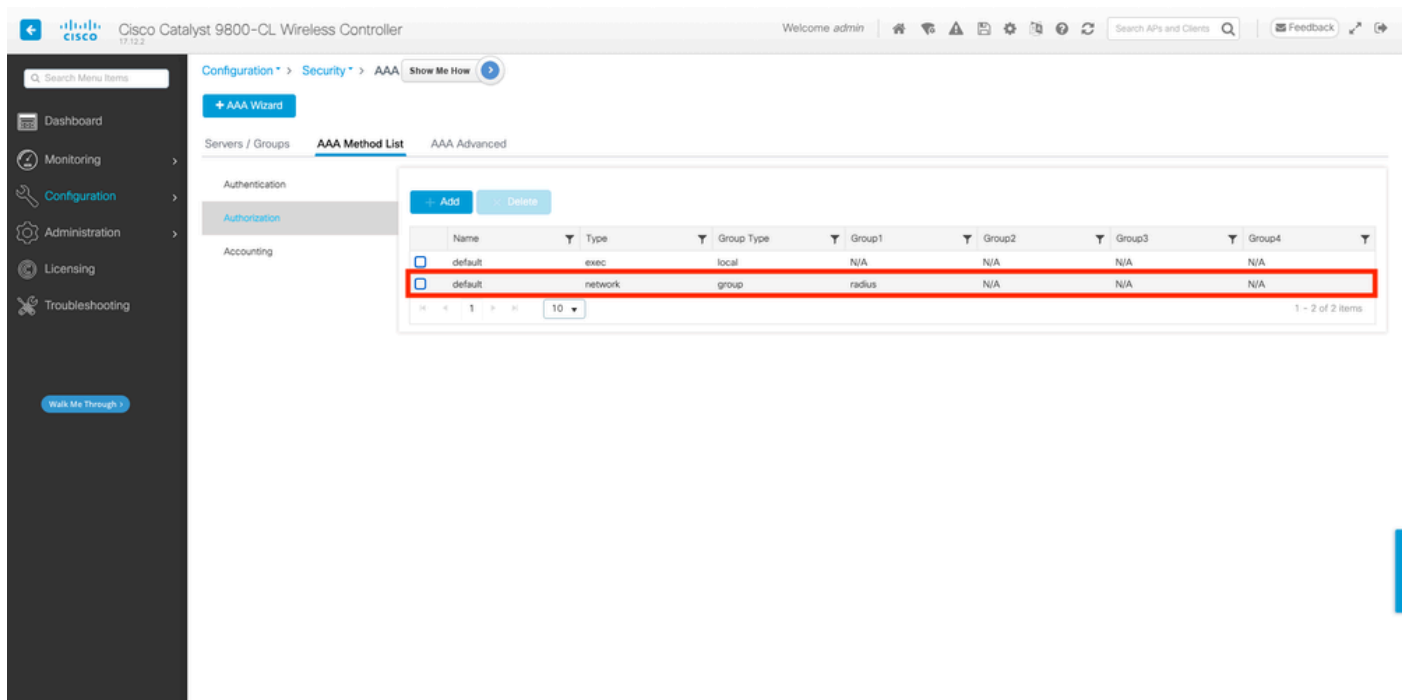
Paso 5. Configurar lista de autorización predeterminada.

Cuando se trabaja con dACL, la autorización de red a través de RADIUS se debe aplicar para que el WLC autorice a cualquier usuario que autentique al SSID 802.1x configurado. De hecho, no sólo la autenticación sino la fase de autorización se maneja aquí en el lado del servidor RADIUS. Por lo tanto, en este caso se requiere la lista de autorización.

Asegúrese de que el método de autorización de red predeterminado forme parte de la configuración de 9800.

Desde la GUI:

Vaya a Configuration > Security > AAA y desde la ficha AAA Method List > Authorization, cree un método de autorización similar al que se muestra.



Desde la CLI:

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

## Configuración de ISE

Al implementar dACL en entornos inalámbricos con ISE, se pueden realizar dos configuraciones comunes, a saber:

1. Configuración dACL por usuario. Con esto, cada identidad particular tiene una dACL asignada gracias a un campo de identidad personalizado.
2. Configuración dACL por resultado. Al optar por este método, se asigna una dACL

determinada a un usuario en función de la política de autorización que coincide en el conjunto de políticas utilizado.

## dACL por usuario

### Paso 1. Definir un atributo de usuario personalizado de dACL

Para poder asignar una dACL a una identidad de usuario, primero este campo debe ser configurable en la identidad creada. De forma predeterminada, en ISE, el campo "ACL" no está definido para ninguna identidad nueva creada. Para superar esto, se puede utilizar el "Atributo de usuario personalizado" y definir un nuevo campo de configuración. Para hacerlo, navegue hasta Administration > Identity Management > Settings > User Custom Attributes. Utilice el botón "+" para añadir un nuevo atributo similar al que se muestra. En este ejemplo, el nombre del atributo personalizado es ACL.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management > Settings > User Custom Attributes. The 'User Custom Attributes' section is active, showing a table of existing attributes:

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

Below this table, a new attribute is being added:

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

At the bottom right, there are 'Save' and 'Reset' buttons.

Una vez configurado, utilice el botón "Guardar" para guardar los cambios.

### Paso 2. Configuración de dACL

Navegue hasta Política > Elementos de política > Resultados > Autorización > ACL descargables para ver y definir dACL en ISE. Utilice el botón "Agregar" para crear uno nuevo.



The screenshot shows the Cisco ISE interface. At the top, there is a navigation bar with 'Cisco ISE' on the left and 'Policy · Policy Elements' in the center. On the right, there are icons for 'License Warning', search, refresh, and settings. Below the navigation bar, there are tabs for 'Dictionaries', 'Conditions', and 'Results'. The 'Results' tab is active. On the left side, there is a sidebar menu with categories: 'Authentication', 'Authorization', 'Authorization Profiles', 'Downloadable ACLs', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Authorization' category is expanded, and 'Downloadable ACLs' is selected. The main content area is titled 'Downloadable ACLs'. It features a toolbar with 'Edit', '+ Add', 'Duplicate', and 'Delete' buttons. A red box highlights the '+ Add' button, and a red arrow points to it. Below the toolbar is a table with the following data:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	ACL_USER1	ACL assigned to USER1
<input type="checkbox"/>	DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
<input type="checkbox"/>	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	

Se abrirá el formulario de configuración "Nueva ACL descargable". En este, configure estos campos:

- Nombre: el nombre de la dACL definida.
- Descripción (opcional): una breve descripción del uso de la dACL creada.
- Versión IP: la versión del protocolo IP utilizada en la dACL definida (versión 4, 6 o ambas).
- Contenido DACL: el contenido de la dACL, según la sintaxis de la ACL de Cisco IOS XE.

En este documento, la dACL utilizada es "ACL\_USER1" y esta dACL permite cualquier tráfico excepto el destinado a 10.48.39.186 y 10.48.39.13.

Una vez configurados los campos, utilice el botón "Enviar" para crear la dACL.

Repita el paso para definir la dACL para el segundo usuario, ACL\_USER2, como se muestra en la figura.

Downloadable ACLs

Name	Description
ACL_USER1	ACL assigned to USER1
ACL_USER2	ACL assigned to USER2
DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic
PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic
test-dacl-cwa	
test-dacl-dot1x	

### Paso 3. Asignar dACL a una identidad creada

Una vez creada la dACL, se puede asignar a cualquier identidad ISE mediante los atributos personalizados del usuario creados en el paso 1. Para hacerlo, navegue hasta Administration > Identity Management > Identities > Users. Como de costumbre, utilice el botón "Agregar" para crear un usuario.

Administration · Identity Management

Identities

Users

### Network Access Users

Status	Username	Description	First Name	Last Name	Small Address	User Identity Groups	Admin
Disabled	adminuser				Network Access Users	admin-group	

En el formulario de configuración "Nuevo usuario de acceso a la red", defina el nombre de usuario y la contraseña del usuario creado. Utilice el atributo personalizado "ACL" para asignar la dACL

creada en el paso 2 a la identidad. En el ejemplo, se define la identidad USER1 que utiliza ACL\_USER1.

The screenshot shows the Cisco ISE Administration interface for Identity Management. The main content area is titled "Network Access Users List > USER1". Under "Network Access User", the "Username" field is set to "USER1" and is highlighted with a red box. The "Status" is "Enabled". Under "Passwords", the "Password Type" is "Internal Users". The "Password Lifetime" is set to "With Expiration" (53 days). The "Login Password" field is highlighted with a red box, and there are "Generate Password" buttons next to it. Under "User Custom Attributes", the "ACL" field is set to "ACL\_USER1" and is highlighted with a red box. At the bottom right, the "Save" button is highlighted with a red box.

Una vez configurados correctamente los campos, utilice el botón "Enviar" para crear la identidad.

Repita este paso para crear USER2 y asignarle ACL\_USER2.

The screenshot shows the "Network Access Users" list in the Cisco ISE Administration interface. The table has columns for Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. The rows are:

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

The USER1 and USER2 rows are highlighted with a red box. Below the table, there is a "Network Access Users" label.

Paso 4. Configurar resultado de directiva de autorización.

Una vez configurada la identidad y asignada la dACL, la política de autorización se debe seguir configurando para hacer coincidir el atributo de usuario personalizado "ACL" definido con una tarea común de autorización existente. Para hacerlo, navegue hasta Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización. Utilice el botón "Agregar" para definir una nueva directiva de autorización.

- Nombre: el nombre de la directiva de autorización, aquí "9800-DOT1X-USERS".
- Tipo de acceso: el tipo de acceso utilizado cuando esta política coincide, aquí ACCESS\_ACCEPT.
- Tarea común: haga coincidir "DACL Name" con InternalUser:<nombre del atributo personalizado creado> para el usuario interno. Según los nombres utilizados en este documento, el perfil 9800-DOT1X-USERS está configurado con el dACL configurado como InternalUser:ACL.

The screenshot shows the Cisco ISE interface for configuring a new Authorization Profile. The interface is titled "Policy - Policy Elements" and has tabs for "Dictionaries", "Conditions", and "Results". The "Results" tab is active, and the "Authorization Profiles" section is selected. The "New Authorization Profile" form is displayed, with the following fields and values:

- Name:** 9800-DOT1X-USERS
- Description:** Authorization profile for 802.1x users using dACLs.
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**
- Agentless Posture:**
- Passive Identity Tracking:**
- Common Tasks:**
  - DACL Name: InternalUser:ACL
  - IPv6 DACL Name
  - ACL (Filter-ID)

Paso 5. Usar perfil de autorización en conjunto de políticas.

Una vez definido correctamente el resultado del perfil de autorización, debe seguir formando parte del conjunto de políticas utilizado para autenticar y autorizar a los usuarios inalámbricos. Navegue hasta Policy > Policy Sets y abra el conjunto de políticas utilizado.

Aquí, la regla de política de autenticación "Dot1X" coincide con cualquier conexión realizada a través de 802.1x por cable o inalámbrica. La regla de política de autorización "802.1x Users dACL" implementa una condición en el SSID utilizado (que es Radius-Called-Station-ID CONTAINS DACL\_DOT1X\_SSID). Si se realiza una autorización en la WLAN "DACL\_DOT1X\_SSID", se utiliza el perfil "9800-DOT1X-USERS" definido en el paso 4 para autorizar al usuario.

Cisco ISE Policy · Policy Sets

Policy Sets → Default

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

Authentication Policy (2)

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

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

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

## dACL por resultado

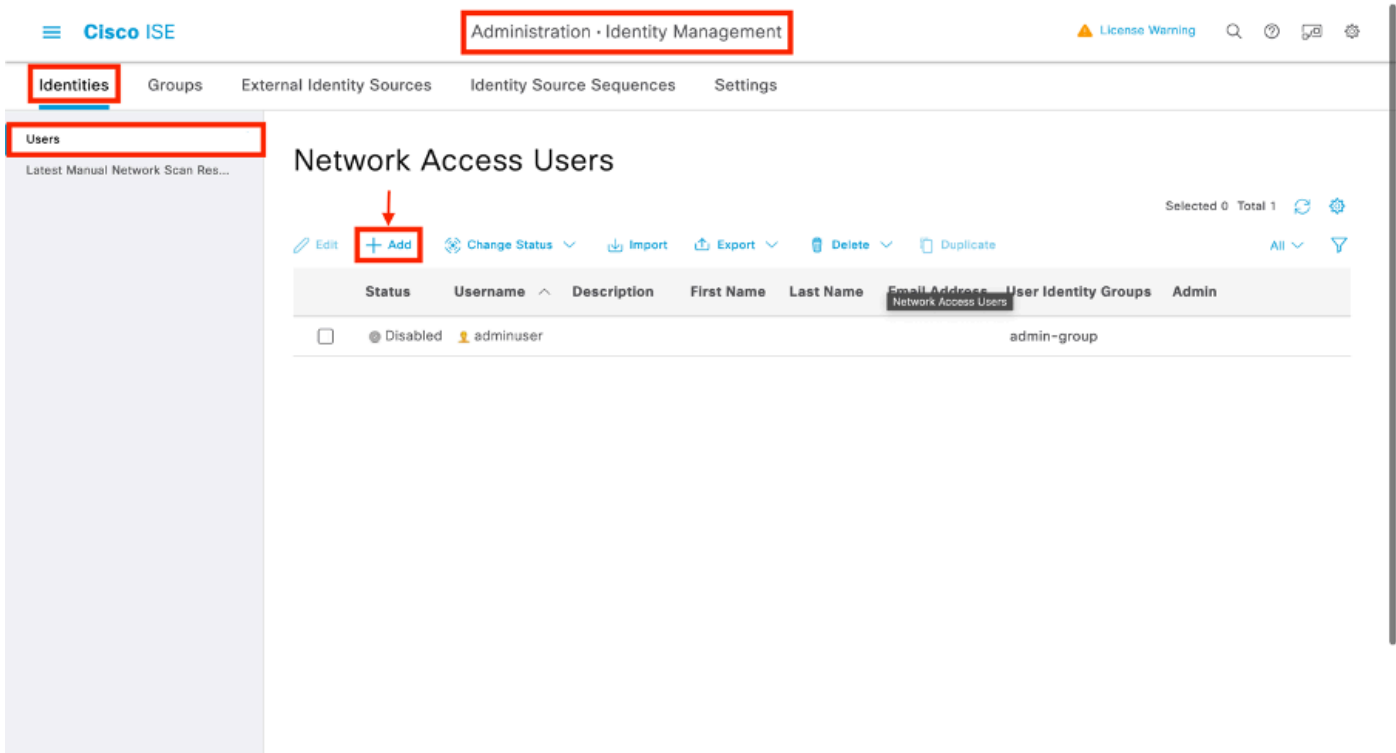
Para evitar la enorme tarea de asignar una dACL concreta a cada identidad creada en ISE, se puede optar por aplicar la dACL a un resultado de política concreto. A continuación, este resultado se aplica en función de cualquier condición que coincida con las reglas de autorización del conjunto de directivas utilizado.

### Paso 1. Configuración de dACL

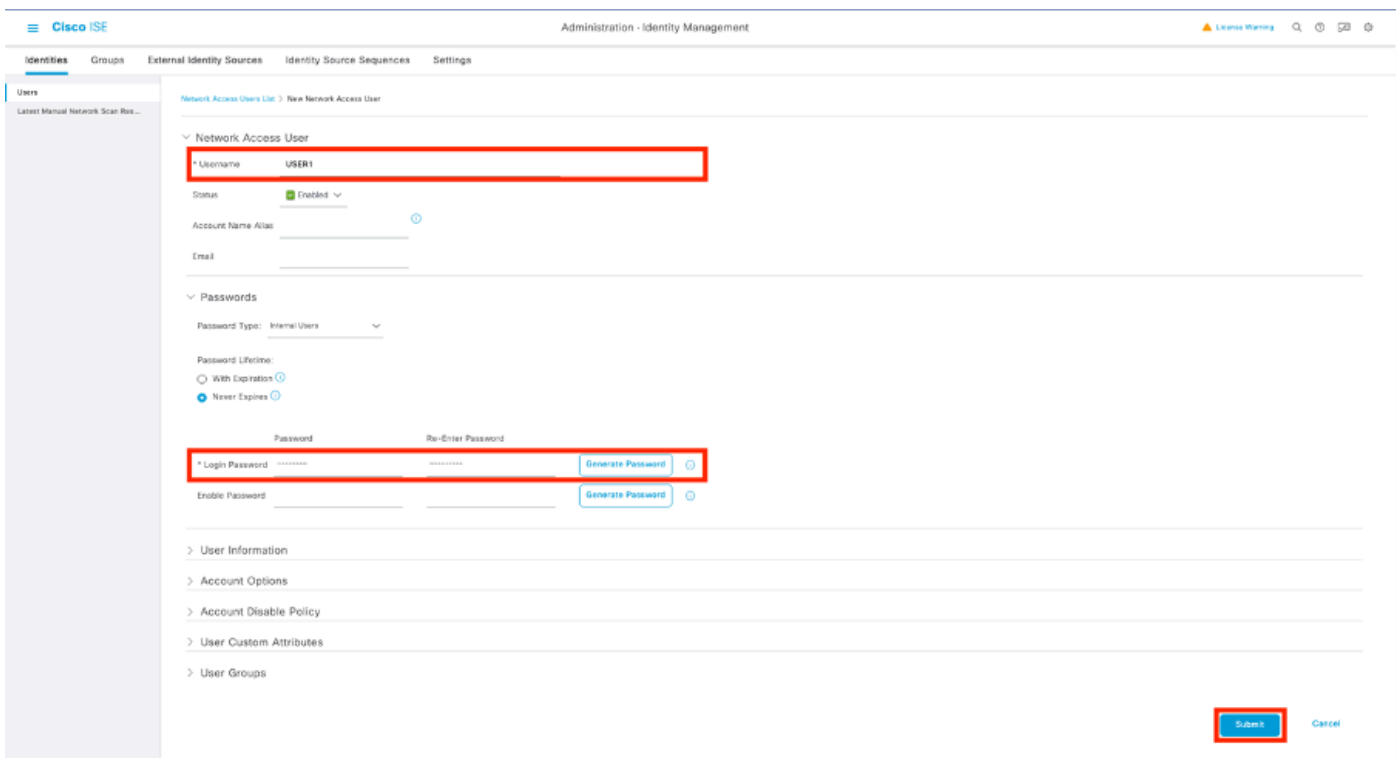
Ejecute el mismo Paso 2 desde la [sección dACLs por usuario](#) para definir las dACLs necesarias. Aquí, estos son ACL\_USER1 y ACL\_USER2.

### Paso 2. Crear identidades

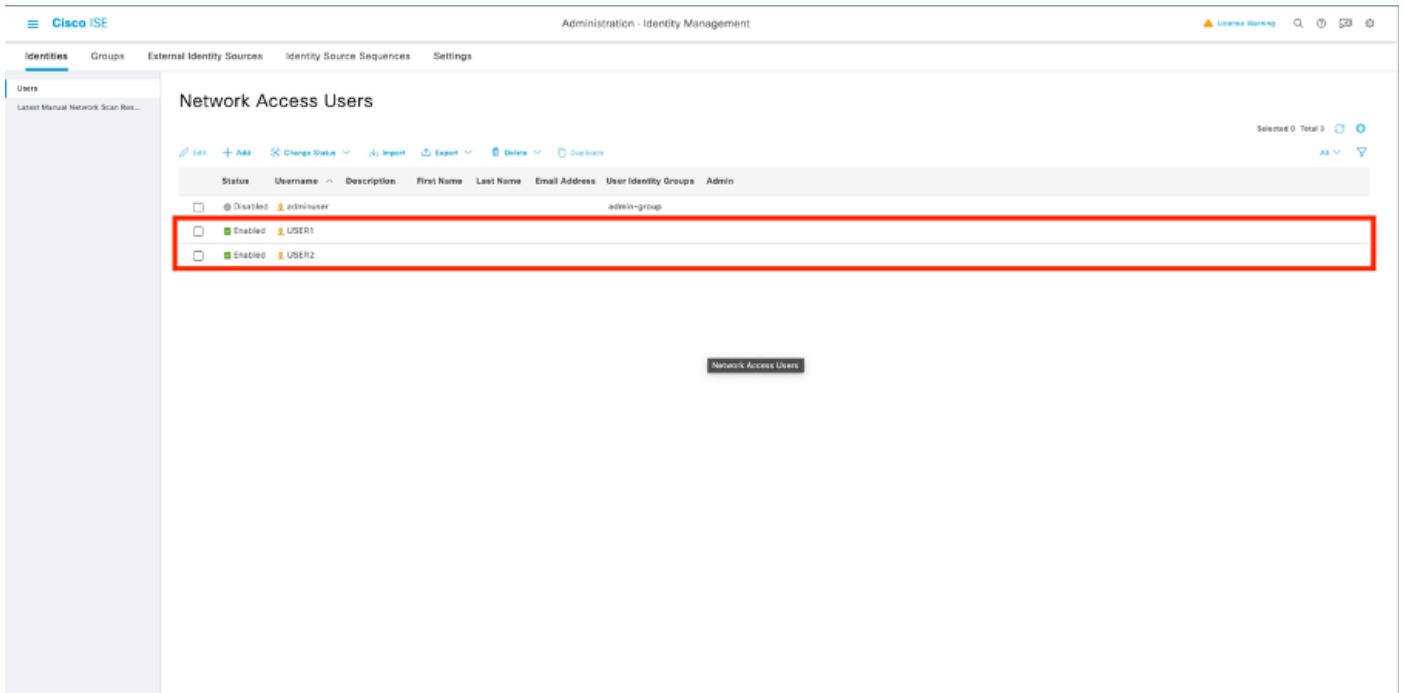
Navegue hasta Administration > Identity Management > Identities > Users y utilice el botón "Add" para crear un usuario.



En el formulario de configuración "Nuevo usuario de acceso a la red", defina el nombre de usuario y la contraseña del usuario creado.



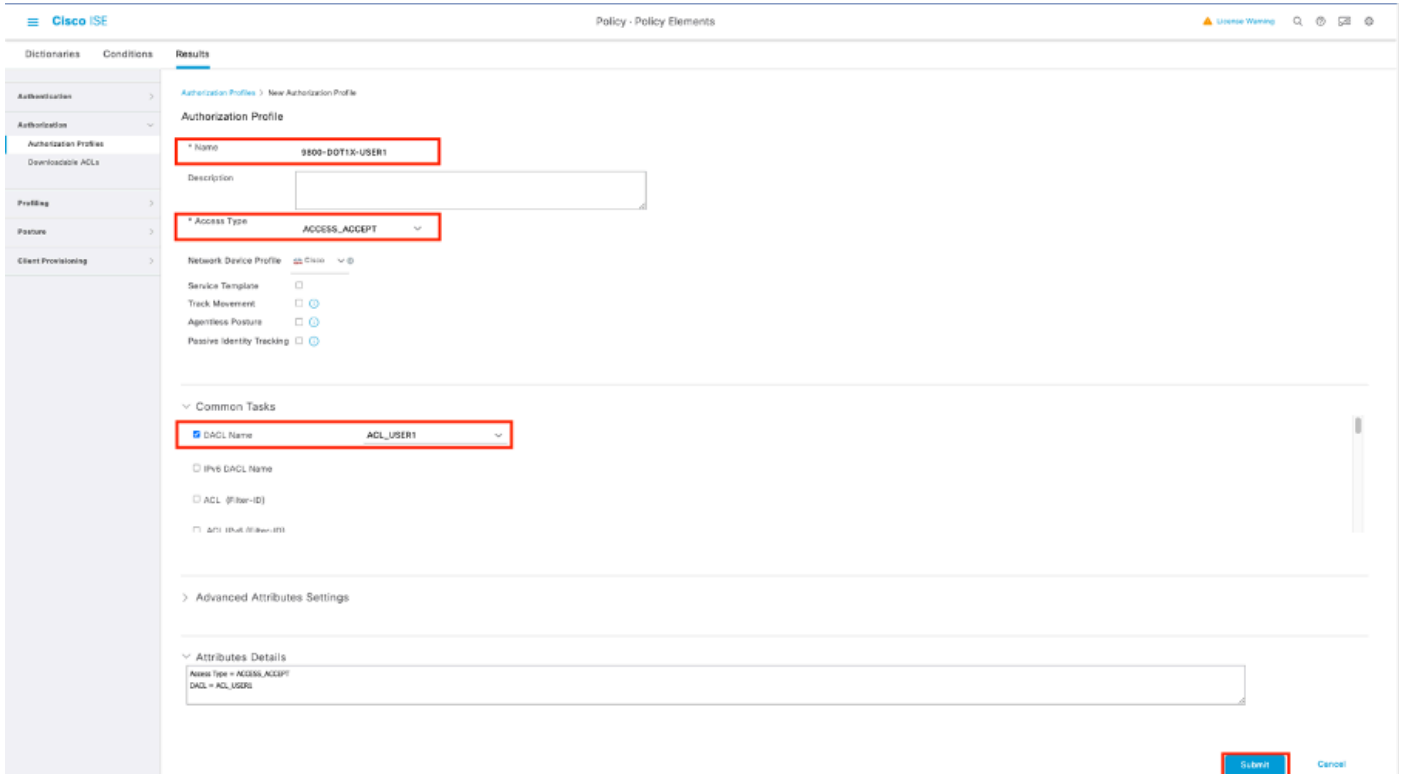
Repita este paso para crear USER2.



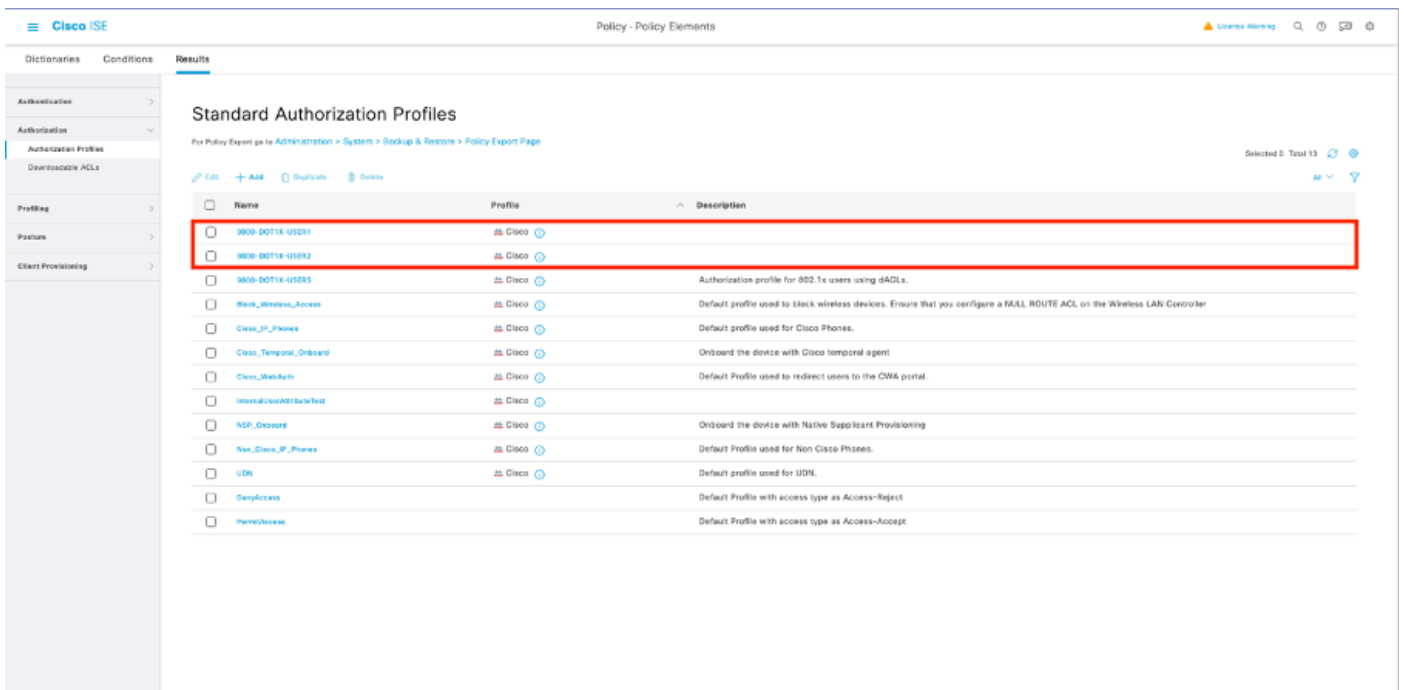
Paso 4. Configure el resultado de la directiva de autorización.

Una vez configuradas la identidad y la dACL, la política de autorización se debe seguir configurando para asignar una dACL determinada a un usuario que coincida con la condición para utilizar esta política. Para hacerlo, navegue hasta Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización. Utilice el botón "Agregar" para definir una nueva directiva de autorización y rellene estos campos.

- Nombre: nombre de la directiva de autorización, aquí "9800-DOT1X-USER1".
- Tipo de acceso: el tipo de acceso utilizado cuando esta política coincide, aquí ACCESS\_ACCEPT.
- Tarea común: haga coincidir "DACL Name" con "ACL\_USER1" para el usuario interno. Según los nombres utilizados en este documento, el perfil 9800-DOT1X-USER1 se configura con la dACL configurada como "ACL\_USER1".



Repita este paso para crear el resultado de la política "9800-DOT1X-USER2" y asignarle "ACL\_USER2" como DACL.



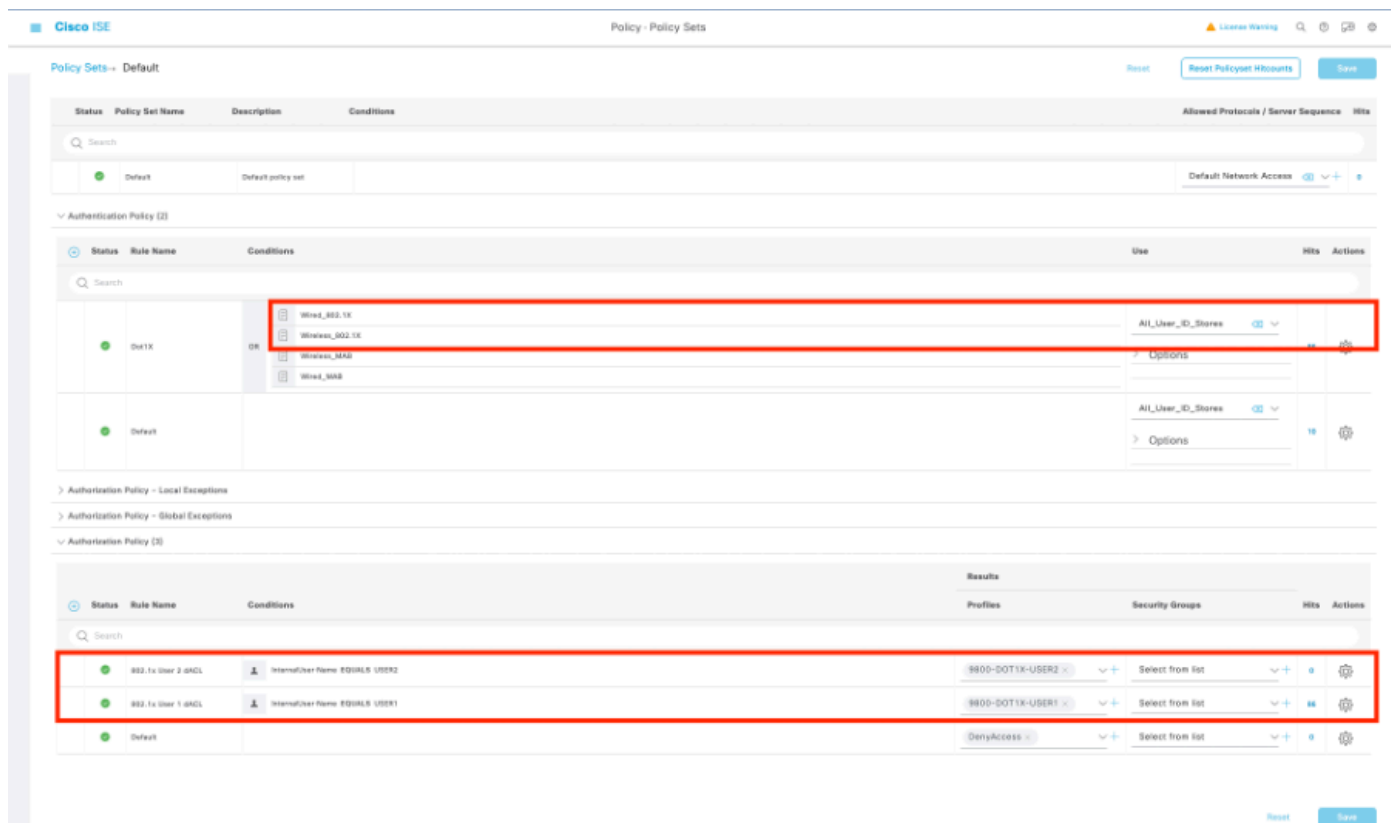
Paso 5. Utilice perfiles de autorización en el conjunto de políticas.

Una vez que se hayan definido correctamente los resultados del perfil de autorización, aún debe formar parte del conjunto de políticas utilizado para autenticar y autorizar a los usuarios inalámbricos. Navegue hasta Policy > Policy Sets y abra el conjunto de políticas utilizado.

Aquí, la regla de política de autenticación "Dot1X" coincide con cualquier conexión realizada a través de 802.1X por cable o inalámbrica. La regla de política de autorización "802.1X User 1



dACL" implementa una condición en el nombre de usuario utilizado (InternalUser-Name CONTAINS USER1). Si se realiza una autorización utilizando el nombre de usuario USER1, se utiliza el perfil "9800-DOT1X-USER1" definido en el paso 4 para autorizar al usuario y, por lo tanto, se aplica también al usuario la dACL de este resultado (ACL\_USER1). Lo mismo se configura para el nombre de usuario USER2, para el cual se utiliza "9800-DOT1X-USER1".



## Notas sobre el uso de dACL con SSID de CWA

Como se describe en la guía de configuración de [Configure Central Web Authentication \(CWA\) on Catalyst 9800 WLC and ISE](#), CWA se basa en el MAB y el resultado particular para autenticar y autorizar a los usuarios. Las ACL descargables se pueden agregar a la configuración de CWA desde el lado de ISE de manera idéntica a lo que se ha descrito anteriormente.



Advertencia: las ACL descargables sólo se pueden utilizar como lista de acceso a la red y no se admiten como ACL previas a la autenticación. Por lo tanto, cualquier ACL de autenticación previa utilizada en un flujo de trabajo de CWA debe definirse en la configuración del WLC.

---

## Verificación

Para verificar la configuración realizada, se pueden utilizar estos comandos.

```
# 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 }
```

Aquí se hace referencia a la parte relevante de la configuración del WLC correspondiente a este ejemplo.

```
aaa new-model
!
!
aaa group server radius authz-server-group
  server name DACL-RADIUS
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authentication dot1x DOT1X group radius
aaa authorization exec default local
aaa authorization network default group radius
!
!
aaa server radius dynamic-author
  client <ISE IP>
!
aaa session-id common
!
[...]
vlan 1413
  name VLAN_1413
!
[...]
radius server DACL-RADIUS
  address ipv4 <ISE IP> auth-port 1812 acct-port 1813
  key 6 aHa0SX[QbbEHURGW`cXiG^UE]CR]^PVANfcbROb
!
!
[...]
wireless profile policy DACL-8021X
  aaa-override
  vlan VLAN_1413
  no shutdown
[...]
wireless tag policy default-policy-tag
  description "default policy-tag"
  wlan DACL_DOT1X_SSID policy DACL-8021X
[...]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
  security dot1x authentication-list DOT1X
  no shutdown
```

Se presenta la configuración del servidor RADIUS, mostrada mediante el comando show running-config all.

```
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

Lista de Verificación

- Asegúrese de que los clientes puedan conectarse correctamente al SSID 802.1X configurado.
- Asegúrese de que la solicitud/aceptación de acceso de RADIUS contenga los pares atributo-valor (AVP) adecuados.
- Asegúrese de que los clientes utilizan el perfil de WLAN/política adecuado.

WLC One Stop-Shop Reflex

Para verificar si la dACL está asignada correctamente a un cliente inalámbrico en particular, se puede utilizar el comando **show wireless client mac-address <H.H.H>detail** como se muestra. A partir de ahí, se puede ver diferente información útil de troubleshooting, a saber: el nombre de usuario del cliente, el estado, el perfil de política, la WLAN y, lo más importante aquí, la ACS-ACL.

<#root>

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

```
Client Username : USER1
```

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

```
Client State : Associated Policy Profile : DACL-8021X
```

```
Wireless LAN Id: 2
```

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

```
BSSID : f4db.e65e.7bc0 Association Id : 1 Authentication Algorithm : Open System Client Active State : Active
```

```
Client ACLs : None Policy Manager State: Run
```

```
Last Policy Manager State : IP Learn Complete Client Entry Create Time : 35 seconds Policy Type : WPA2
```

```
VLAN : VLAN_1413
```

```
[...] Session Manager: Point of Attachment : capwap_90000012 IIF ID : 0x90000012 Authorized : TRUE Sess  
SM State : AUTHENTICATED  
SM Bend State : IDLE Local Policies:  
Service Template : wlan_svc_DACL-8021X_local (priority 254) VLAN : VLAN_1413 Absolute-Timer : 28800  
Server Policies:  
ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab  
Resultant Policies:  
ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab VLAN Name : VLAN_1413 VLAN : 1413 Absolute-Timer : 28800  
[...]
```

#### Comandos Show de WLC

Para ver todas las ACL que actualmente forman parte de la configuración del WLC del Catalyst 9800, puede utilizar el comando **show access-lists**. Este comando enumera todas las ACL definidas localmente o las dACL descargadas por el WLC. Cualquier dACL descargada desde ISE por el WLC tiene el formato xACSACLx-IP-<ACL\_NAME>-<ACL\_HASH>.

---

**Nota:** Las ACL descargables permanecen en la configuración mientras un cliente esté asociado y lo utilice en la infraestructura inalámbrica. Tan pronto como el último cliente que utiliza la dACL abandona la infraestructura, la dACL se elimina de la configuración.

---

```
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
[...]
```

## Depuración condicional y seguimiento activo por radio

Mientras se soluciona el problema de configuración, puede recopilar [rastros radiactivos](#) para un cliente que se supone debe asignarse con la dACL definida. Aquí están resaltados los registros que muestran la parte interesante de los rastros radiactivos durante el proceso de asociación de clientes para el cliente 08be.ac14.137d.

<#root>

```
2024/03/28 10:43:04.321315612 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (note): MAC: 08be.ac14.137d Assoc
```

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

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

[...]

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

2024/03/28 10:43:04.322199665 {wncd\_x\_R0-0}{1}: [dot11] [19620]: (info): MAC: 08be.ac14.137d DOT11 state

[...]

2024/03/28 10:43:04.322860054 {wncd\_x\_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d s

2024/03/28 10:43:04.322881795 {wncd\_x\_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

[...]

2024/03/28 10:43:04.323379781 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

[...]

2024/03/28 10:43:04.330181613 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.353413199 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [19620]: (info): [08be.ac14.13

2024/03/28 10:43:04.353414496 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [19620]: (info): [08be.ac14.13



2024/03/28 10:43:04.353438621 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 Au

2024/03/28 10:43:04.353443674 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clie

[...]

2024/03/28 10:43:04.381397739 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.381411901 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator e9 8b e

2024/03/28 10:43:04.381425481 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 7 "USERI

2024/03/28 10:43:04.381430559 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Service-Type [6] 6 Fr

2024/03/28 10:43:04.381433583 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 27

2024/03/28 10:43:04.381437476 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 21 "

2024/03/28 10:43:04.381440925 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Framed-MTU [12] 6 148

2024/03/28 10:43:04.381452676 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 12.

2024/03/28 10:43:04.381466839 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator

2024/03/28 10:43:04.381482891 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Key-Name [102] 2

2024/03/28 10:43:04.381486879 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 49

2024/03/28 10:43:04.381489488 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 43 "

2024/03/28 10:43:04.381491463 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381494016 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "

2024/03/28 10:43:04.381495896 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32

2024/03/28 10:43:04.381498320 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "

2024/03/28 10:43:04.381500186 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381502409 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "v

2024/03/28 10:43:04.381506029 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6 I

2024/03/28 10:43:04.381509052 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port-Type [61] 6  
2024/03/28 10:43:04.381511493 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port [5] 6 3913  
2024/03/28 10:43:04.381513163 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 39

2024/03/28 10:43:04.381515481 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 33 "c

2024/03/28 10:43:04.381517373 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 41

2024/03/28 10:43:04.381519675 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 35 "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] 17

2024/03/28 10:43:04.381539951 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [18]

2024/03/28 10:43:04.381542233 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[  
2024/03/28 10:43:04.381544465 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188]  
2024/03/28 10:43:04.381619890 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout  
[...]

2024/03/28 10:43:04.392544173 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812/

2024/03/28 10:43:04.392557998 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 08 6d f  
2024/03/28 10:43:04.392564273 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: State [24] 71 ...  
2024/03/28 10:43:04.392615218 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 8..  
2024/03/28 10:43:04.392628179 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator  
2024/03/28 10:43:04.392738554 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t  
2024/03/28 10:43:04.726798622 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_9000001

2024/03/28 10:43:04.726801212 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012

2024/03/28 10:43:04.726896276 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_9000001

2024/03/28 10:43:04.726905248 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012

[...]

2024/03/28 10:43:04.727138915 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012

2024/03/28 10:43:04.727148212 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_90000012

2024/03/28 10:43:04.727164223 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000  
2024/03/28 10:43:04.727169069 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000

2024/03/28 10:43:04.727223736 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : use

2024/03/28 10:43:04.727233018 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : cl  
2024/03/28 10:43:04.727234046 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA  
2024/03/28 10:43:04.727234996 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Me  
2024/03/28 10:43:04.727236141 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA  
M\$®vf9fjØ«? %ÿ0?ã@≤™ÇÑbWi6\Ë&\q·1U+QB-°@”≠fJÑv?”

2024/03/28 10:43:04.727246409 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Cis

[...]

2024/03/28 10:43:04.727509267 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000

2024/03/28 10:43:04.727513133 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000

2024/03/28 10:43:04.727607738 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: SVM Apply user profile  
2024/03/28 10:43:04.728003638 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: Activating EPM feature

2024/03/28 10:43:04.728144450 {wncd\_x\_R0-0}{1}: [epm-misc] [19620]: (info): [08be.ac14.137d:capwap\_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-ac1] [19620]: (info): [08be.ac14.137d:capwap\_90000012]

2024/03/28 10:43:04.729005675 {wncd\_x\_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap\_90000012]  
2024/03/28 10:43:04.729019215 {wncd\_x\_R0-0}{1}: [svm] [19620]: (info): SVM\_INFO: Response of epm is ASYNCHRONOUS  
[...]

2024/03/28 10:43:04.729422929 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to NAS

2024/03/28 10:43:04.729428175 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 20 06 30

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2024/03/28 10:43:04.733058380 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M  
2024/03/28 10:43:04.733064555 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M  
2024/03/28 10:43:04.733065483 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e  
2024/03/28 10:43:04.733066816 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: m  
2024/03/28 10:43:04.733068704 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c  
2024/03/28 10:43:04.733069947 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: i

2024/03/28 10:43:04.733070971 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: us

2024/03/28 10:43:04.733079208 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c  
2024/03/28 10:43:04.733080328 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: E  
M\$®vf9f0«? %ÿ0?ã@≤™ÇÑbwî6\Ë&q·1U+QB-°@”≠fJÑv?"  
2024/03/28 10:43:04.733091441 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e

2024/03/28 10:43:04.733092470 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: Cis

[...]

2024/03/28 10:43:04.733396045 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000

2024/03/28 10:43:04.733486604 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 A

2024/03/28 10:43:04.734665244 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.734894043 {wncd\_x\_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d E  
2024/03/28 10:43:04.734904452 {wncd\_x\_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d C



2024/03/28 10:43:04.734915743 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_90000012

2024/03/28 10:43:04.740499944 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.742238941 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A

2024/03/28 10:43:04.744387633 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

[...]

2024/03/28 10:43:04.745245318 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.745294050 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Allocate

2024/03/28 10:43:04.745326416 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.751291844 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.751943577 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A

2024/03/28 10:43:04.752686055 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clien

2024/03/28 10:43:04.755505991 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.756746153 {wncd\_x\_R0-0}{1}: [mm-transition] [19620]: (info): MAC: 08be.ac14.137d MM

2024/03/28 10:43:04.757801556 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d ADD I

2024/03/28 10:43:04.758843625 {wncd\_x\_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

2024/03/28 10:43:04.759064834 {wncd\_x\_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d IF

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 Clien

2024/03/28 10:43:04.764575895 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.764755847 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A

2024/03/28 10:43:04.769965195 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.770727027 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.772314586 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.772362837 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.773070456 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.773661861 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A

2024/03/28 10:43:04.775537766 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.777154567 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.778756670 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl l

2024/03/28 10:43:04.778807076 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

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

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

2024/03/28 10:43:04.779879864 {iosrp\_R0-0}{1}: [og] [26311]: (info): OG\_PI\_ACL\_INFO: ogacl\_configured: A

2024/03/28 10:43:04.780510740 {iosrp\_R0-0}{1}: [parser\_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.786433419 {wncd\_x\_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interfac  
2024/03/28 10:43:04.786523172 {wncd\_x\_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interfac  
2024/03/28 10:43:04.787787313 {wncd\_x\_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interfac  
2024/03/28 10:43:04.788160929 {wncd\_x\_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interfac  
2024/03/28 10:43:04.788491833 {wncd\_x\_R0-0}{1}: [client-iplearn] [19620]: (note): MAC: 08be.ac14.137d C  
2024/03/28 10:43:04.788576063 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_9000  
2024/03/28 10:43:04.788741337 {wncd\_x\_R0-0}{1}: [webauth-sess] [19620]: (info): Change address update, c  
2024/03/28 10:43:04.788761575 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_acct] [19620]: (info): [08be.ac14.137d:c  
2024/03/28 10:43:04.788877999 {wncd\_x\_R0-0}{1}: [epm] [19620]: (info): [0000.0000.0000:unknown] HDL = 0

2024/03/28 10:43:04.789333126 {wncd\_x\_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d IE

2024/03/28 10:43:04.789410101 {wncd\_x\_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d I

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 :Ci

2024/03/28 10:43:04.789651931 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute :bsr

2024/03/28 10:43:04.789653490 {wncd\_x\_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [ Applied attribute : t  
2024/03/28 10:43:04.789735556 {wncd\_x\_R0-0}{1}: [ewlc-qos-client] [19620]: (info): MAC: 08be.ac14.137d c  
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

## Captura de paquete

Otro reflejo interesante es tomar y analizar las capturas de paquetes del flujo RADIUS para una asociación de cliente. Las ACL descargables dependen de RADIUS, no solo para ser asignadas a un cliente inalámbrico sino también para ser descargadas por el WLC. Mientras toma la captura de paquetes para resolver problemas de configuración de dACL, debe capturar en la interfaz utilizada por el controlador para comunicarse con el servidor RADIUS. [Este documento](#) muestra cómo configurar la captura de paquetes fácilmente embebidos en el Catalyst 9800, que se han utilizado para recopilar la captura analizada en este artículo.

## autenticación de cliente RADIUS

Puede ver la solicitud de acceso RADIUS del cliente enviada desde el WLC al servidor RADIUS para autenticar al usuario USER1 (Nombre de usuario AVP) en el SSID DACL\_DOT1X\_SSID (Identificador de NAS AVP).

```
Length: 617  Encaps.  39  10.48.39.130  10.48.39.134  Access-Request id=92, Duplicate Request  RADIUS
--  Length: 594  Encaps.  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) on 0
> 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=Framed-MTU(12) l=6 val=1485
  > AVP: t=EAP-Message(79) l=48 Last Segment[1]
  > AVP: t=Message-Authenticator(80) l=18 val=cdc761262dc47e90de31bb0699da8359
  > AVP: t=EAP-Key-Name(102) l=2 val=
  > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
  > AVP: t=Framed-IP-Address(8) l=6 val=10.14.13.240
  > AVP: t=Vendor-Specific(26) l=40 vnd=ciscoSystems(9)
  > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
  > AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
  > AVP: t=NAS-IP-Address(4) l=6 val=10.48.39.130
  > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
  > AVP: t=NAS-Port(5) l=6 val=3913
  > AVP: t=State(24) l=71 val=333743504d53657373696f6e49443d38323237333030413030303030394638343933335..
  > AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
  > AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
  > AVP: t=Called-Station-Id(30) l=35 val=f4-db-e6-5e-7b-c0:DACL_DOT1X_SSID
  > AVP: t=Calling-Station-Id(31) l=19 val=08-be-ac-14-13-7d
  > AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
  > AVP: t=NAS-Identifier(32) l=17 val=DACL_DOT1X_SSID
  > AVP: t=Unknown-Attribute(187) l=6 val=000fac04
  > AVP: t=Unknown-Attribute(186) l=6 val=000fac04
```

Cuando la autenticación es exitosa, el servidor RADIUS responde con un access-accept, todavía para el usuario USER1 (AVP User-Name) y aplica los atributos AAA, en particular el proveedor específico AVP ACS:CiscoSecure-Defined-ACL estando aquí "#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_Bd:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130
> User Datagram Protocol, Src Port: 1812, Dst Port: 63772
< RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x5c (92)
  Length: 348
  Authenticator: 643ab1eaba9478735f73678ab53b28a
  [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=434143533a38323237333030413030303030394638343933354132443a6973652f3439..
  > AVP: t=EAP-Message(79) l=6 Last Segment[1]
  > AVP: t=Message-Authenticator(80) l=18 val=de01c27a418e8289dd5d6b29165ec872
  > AVP: t=EAP-Key-Name(102) l=67 val=\031f\005c010\0031VE 00x\0020\00R0\033q0076000040\021(0Q(0\035/s 0a0d0y\0270660000F0d
  > AVP: t=Vendor-Specific(26) l=66 vnd=ciscoSystems(9)
    Type: 26
    Length: 66
    Vendor ID: ciscoSystems (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)
  
```

### Descarga de DACL

Si la dACL ya es parte de la configuración del WLC, entonces se asigna simplemente al usuario y la sesión de RADIUS finaliza. De lo contrario, el WLC descarga la ACL, todavía usando RADIUS. Para ello, el WLC realiza una solicitud de acceso RADIUS, esta vez usando el nombre dACL ("**#ACSACL#-IP-ACL\_USER1-65e89aab**") para el nombre de usuario AVP. Junto con esto, el WLC informa al servidor RADIUS que este access-accept inicia una descarga ACL usando el par AV de Cisco `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_Bd: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: b216948576c8a46a51899e72d0709454
  [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=#ACSACL#-IP-ACL_USER1-65e89aab
    Type: 1
    Length: 32
    User-Name: #ACSACL#-IP-ACL_USER1-65e89aab
  > AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
  > 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
  
```

La aceptación de acceso de RADIUS enviada de vuelta al controlador contiene la dACL solicitada, como se muestra. Cada regla ACL está contenida dentro de un Cisco AVP diferente del tipo "ip:inacl#<X>=<ACL\_RULE>", siendo <X> el número de regla.



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

> Frame 8038: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)  
> Ethernet II, Src: VMware\_Bd:01:ec (00:50:56:8d:01:ec), Dst: Cisco\_b2:fe:ff (00:1e:f6:b2:fe:ff)  
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39  
> Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130  
> User Datagram Protocol, Src Port: 1812, Dst Port: 63772

▼ RADIUS Protocol  
Code: Access-Accept (2)  
Packet identifier: 0x51 (81)  
Length: 323  
Authenticator: 61342164ce39be06eed028b3ce566ef5  
[\[This is a response to a request in frame 8036\]](#)  
[Time from request: 0.007995000 seconds]

▼ Attribute Value Pairs

- > AVP: t=User-Name(1) l=32 val=#ACSAcl@-IP-ACL\_USER1-65e89aab
- > AVP: t=Class(25) l=75 val=434143533a30613330323738366d6242517239445259673447765f436554692f48737050...
- > AVP: t=Message-Authenticator(80) l=18 val=a3c4b20cd1e64785d9e0232511cd0b72
- ▼ AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)
  - Type: 26
  - Length: 47
  - Vendor ID: ciscoSystems (9)
  - > VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#1=deny ip any host 10.48.39.13
- ▼ AVP: t=Vendor-Specific(26) l=47 vnd=ciscoSystems(9)
  - Type: 26
  - Length: 47
  - Vendor ID: ciscoSystems (9)
  - > VSA: t=Cisco-AVPair(1) l=41 val=ip:inacl#2=deny ip any host 10.48.39.15
- ▼ AVP: t=Vendor-Specific(26) l=48 vnd=ciscoSystems(9)
  - Type: 26
  - Length: 48
  - Vendor ID: ciscoSystems (9)
  - > VSA: t=Cisco-AVPair(1) l=42 val=ip:inacl#3=deny ip any host 10.48.39.186
- ▼ AVP: t=Vendor-Specific(26) l=36 vnd=ciscoSystems(9)
  - Type: 26
  - Length: 36
  - Vendor ID: ciscoSystems (9)
  - > VSA: t=Cisco-AVPair(1) l=30 val=ip:inacl#4=permit ip any any

▼ RADIUS Protocol (radius), 323 bytes

Packets: 43372 - Displayed: 2 (0.0%) Profile: Default



**Nota:** Si el contenido de una ACL de descarga se modifica después de que se haya descargado en el WLC, el cambio para esta ACL no se refleja hasta que un usuario que usa esta se reautentica (y el WLC realiza una autenticación RADIUS para ese usuario nuevamente). De hecho, un cambio en la ACL se refleja en un cambio en la parte hash del nombre de la ACL. Por lo tanto, la próxima vez que esta ACL se asigne a un usuario, su nombre debe ser diferente y, por lo tanto, la ACL no debe ser parte de la configuración del WLC y se supone que debe ser descargada. Sin embargo, los clientes que se autentican antes del cambio en la ACL continúan utilizando la anterior hasta que se vuelven a autenticar completamente.

---

## Registros de funcionamiento de ISE

### autenticación de cliente RADIUS

Los registros de operaciones muestran una autenticación correcta del usuario "USER1", al que se aplica la ACL descargable "ACL\_USER1". Las partes de interés para la solución de problemas están enmarcadas en rojo.

Overview

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

Authentication Details

Source Timestamp	2024-03-28 05:11:11.035
Received Timestamp	2024-03-28 05:11:11.035
Policy Server	ise
Event	5200 Authentication succeeded
Username	USER1
User Type	User
Endpoint Id	08:BE:AC:14:13:7D
Calling Station Id	08-be-ac-14-13-7d
Endpoint Profile	Unknown
Authentication Identity Store	Internal Users
Identity Group	Unknown
Audit Session Id	8227300A0000000D848ABE3F
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	gdefland-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.48.39.130
NAS Port Type	Wireless - IEEE 802.11
Authorization Profile	9800-DOT1X-USER1
Response Time	368 milliseconds

Steps

- 11001 Received RADIUS Access-Request
- 11017 RADIUS created a new session
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 11507 Extracted EAP-Response/Identity
- 12500 Prepared EAP-Request proposing EAP-TLS with challenge
- 12625 Valid EAP-Key-Name attribute received
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session
- 12301 Extracted EAP-Response/NAK requesting to use PEAP instead
- 12300 Prepared EAP-Request proposing PEAP with challenge
- 12625 Valid EAP-Key-Name attribute received
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session
- 12302 Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated
- 12318 Successfully negotiated PEAP version 0
- 12800 Extracted first TLS record; TLS handshake started
- 12805 Extracted TLS ClientHello message
- 12806 Prepared TLS ServerHello message
- 12807 Prepared TLS Certificate message
- 12808 Prepared TLS ServerKeyExchange message
- 12810 Prepared TLS ServerDone message
- 12305 Prepared EAP-Request with another PEAP challenge
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session
- 12304 Extracted EAP-Response containing PEAP challenge-response
- 12305 Prepared EAP-Request with another PEAP challenge
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session
- 12304 Extracted EAP-Response containing PEAP challenge-response
- 12305 Prepared EAP-Request with another PEAP challenge
- 11006 Returned RADIUS Access-Challenge
- 11001 Received RADIUS Access-Request
- 11018 RADIUS is re-using an existing session
- 12304 Extracted EAP-Response containing PEAP challenge-response
- 12318 Successfully negotiated PEAP version 0

Other Attributes	
ConfigVersionId	73
DestinationPort	1812
Protocol	Radius
NAS-Port	3913
Framed-MTU	1485
State	37CPMSessionID=8227300A0000000D848ABE3F;26SessionID=ise/499610885/35;
undefined-186	00:0f:ac:04
undefined-187	00:0f:ac:04
undefined-188	00:0f:ac:01
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ise/499610885/35
SelectedAuthenticationIden...	Internal Users
SelectedAuthenticationIden...	All_AD_Join_Points
SelectedAuthenticationIden...	Guest Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Dot1X
AuthorizationPolicyMatched...	802.1x User 1 dACL
EndPointMACAddress	08-BE-AC-14-13-7D
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Dot1X
TotalAuthenLatency	515
ClientLatency	147
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
Name	USER1
EnableFlag	Enabled
RADIUS Username	USER1
NAS-Identifier	DACL_DOT1X_SSID
Device IP Address	10.48.39.130
CPMSessionID	8227300A0000000D848ABE3F
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID
CiscoAVPair	service-type=Framed, audit-session-id=8227300A0000000D848ABE3F, method=dot1x, client-if-id=2113931001, vlan-id=1413, cisco-wlan-ssid=DACL_DOT1X_SSID, wlan-profile-name=DACL_DOT1X_SSID, AuthenticationIdentityStore=Internal Users, FQSubjectName=9273fe30-8c01-11e6-996c-52540b48521#user1, UniqueSubjectID=94b3604f5b49b88ccf2f3a86c80d1979b5c43
<b>Result</b>	
Class	CACS:8227300A0000000D848ABE3F;ise/499610885/35
EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:97:b8:72:94:16:e3:b9:93:2f:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:c5:c5:05:d6:57:5b:f1:2d:62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:06:9c:ef:3e:9f:f6
cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSAcl#-IP-ACL_USER1-65e89aab
MS-MPPE-Send-Key	****
MS-MPPE-Recv-Key	****
LicenseTypes	Essential license consumed.
<b>Session Events</b>	
2024-03-28 05:11:11.035	Authentication succeeded

```

12810 Prepared TLS ServerDone message
12812 Extracted TLS ClientKeyExchange message
12803 Extracted TLS ChangeCipherSpec message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded
12310 PEAP full handshake finished successfully
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
12313 PEAP inner method started
11521 Prepared EAP-Request/Identity for inner EAP method
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11522 Extracted EAP-Response/Identity for inner EAP method
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11522 Extracted EAP-Response/Identity for inner EAP method
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP-MSCHAP as negotiated
15041 Evaluating Identity Policy
15048 Queried PIP - Normalised Radius.RadiusFlowType
22072 Selected identity source sequence - All_User_ID_Stores
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore - USER1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
11824 EAP-MSCHAP authentication attempt passed
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
11810 Extracted EAP-Response for inner method containing MSCHAP challenge-response
11814 Inner EAP-MSCHAP authentication succeeded
11519 Prepared EAP-Success for inner EAP method
12314 PEAP inner method finished successfully
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12304 Extracted EAP-Response containing PEAP challenge-response
24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - USER1
24211 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - InternalUserName
15016 Selected Authorization Profile - 9800-DOT1X-USER1
11022 Added the dACL specified in the Authorization Profile
22081 Max sessions policy passed
22080 New accounting session created in Session cache
12306 PEAP authentication succeeded
11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept

```

### Descarga de DACL

Los registros de operaciones muestran una descarga correcta de la ACL "ACL\_USER1". Las partes de interés para la solución de problemas están enmarcadas en rojo.

Overview

Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-ACL_USER1-65e89aab
Endpoint Id	
Endpoint Profile	
Authorization Result	

Authentication Details

Source Timestamp	2024-03-28 05:43:04.755
Received Timestamp	2024-03-28 05:43:04.755
Policy Server	ise
Event	5232 DACL Download Succeeded
Username	#ACSACL#-IP-ACL_USER1-65e89aab
Network Device	gdefland-9800
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.48.39.130
Response Time	1 milliseconds

Other Attributes

ConfigVersionId	73
DestinationPort	1812
Protocol	Radius
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ise/499610885/48
TotalAuthenLatency	1
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	#ACSACL#-IP-ACL_USER1-65e89aab
Device IP Address	10.48.39.130
CPMSessionID	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcs eM
CiscoAVPair	aaa.service=ip_admission, aaa.event=acl-download

Result

Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfd Fbcs eM:ise/499610885/48
cisco-av-pair	ip:inacI#1=deny ip any host 10.48.39.13
cisco-av-pair	ip:inacI#2=deny ip any host 10.48.39.15
cisco-av-pair	ip:inacI#3=deny ip any host 10.48.39.186
cisco-av-pair	ip:inacI#4=permit ip any any

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11117	Generated a new session ID
11002	Returned RADIUS Access-Accept

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).