

# Configura & Risoluzione dei problemi relativi agli ACL scaricabili su Catalyst 9800

## Sommario

---

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

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

[Esempio di rete](#)

[Configurazione WLC](#)

[Configurazione di ISE](#)

[dACL per utente](#)

[dACL per risultato](#)

[Note sull'utilizzo di ACL con SSID CWA](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Elenco di controllo](#)

[WLC One Stop-Shop Reflex](#)

[Comandi Show WLC](#)

[Debug condizionale e traccia Radioactive \(RA\)](#)

[Acquisizione pacchetti](#)

[Autenticazione client RADIUS](#)

[Download DACL](#)

[Registri delle operazioni ISE](#)

[Autenticazione client RADIUS](#)

[Download DACL](#)

---

## Introduzione

In questo documento viene descritto come configurare gli ACL (dACL) scaricabili su Catalyst 9800 Wireless LAN Controller (WLC) e come risolvere i relativi problemi.

## Premesse

Gli ACL sono supportati da molti anni sugli switch Cisco IOS® e IOS XE®. Per dACL si intende il fatto che il dispositivo di rete scarica dinamicamente le voci ACL dal server RADIUS quando viene

eseguita l'autenticazione, anziché avere una copia locale dell'ACL a cui viene semplicemente assegnato il nome. È disponibile un [esempio di configurazione](#) più completo di [Cisco ISE](#). Questo documento si concentra su Cisco Catalyst 9800 che supporta gli dACL per lo switching centrale dalla versione 17.10.

## Prerequisiti

Lo scopo di questo documento è dimostrare l'utilizzo degli dACL su Catalyst 9800 tramite un esempio di configurazione SSID di base, illustrando come questi elementi possano essere completamente personalizzabili.

Sul controller wireless Catalyst 9800, gli ACL scaricabili sono

- Supportato [a partire da Cisco IOS XE versione 17.10.1](#).
- Supportato solo per controller centralizzato con access point in modalità locale (o switching centrale Flexconnect). Lo switching locale FlexConnect non supporta dACL.

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Catalyst Wireless 9800 modello di configurazione.
- Cisco IP Access Control Lists (ACLs).

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

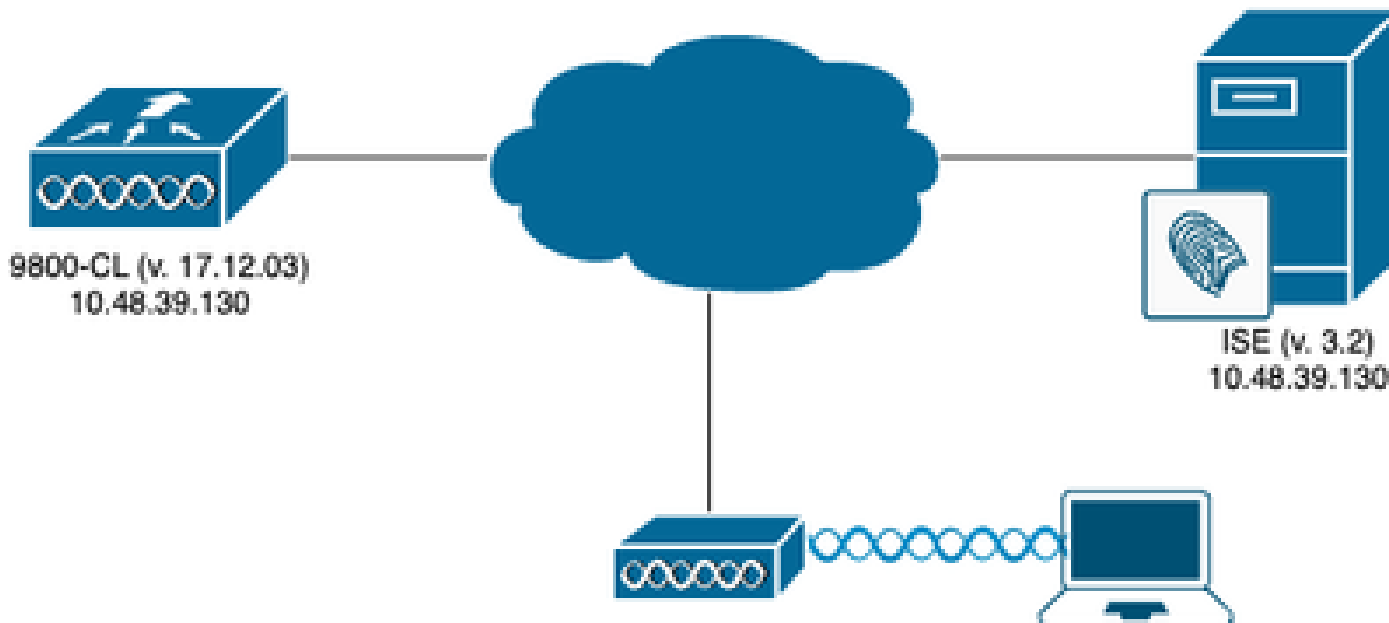
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

In questa guida alla configurazione, anche se i metodi sono diversi (ad esempio, l'autenticazione WLAN, la configurazione delle policy e così via), il risultato finale è lo stesso. Nello scenario illustrato di seguito vengono definite due identità utente, USER1 e USER2. A entrambi è concesso l'accesso alla rete wireless. A ciascuno di essi vengono assegnati, rispettivamente, ACL\_USER1 e ACL\_USER2 scaricati da Catalyst 9800 da ISE.

# Uso di dACL con SSID 802.1x

## Esempio di rete



## Configurazione WLC

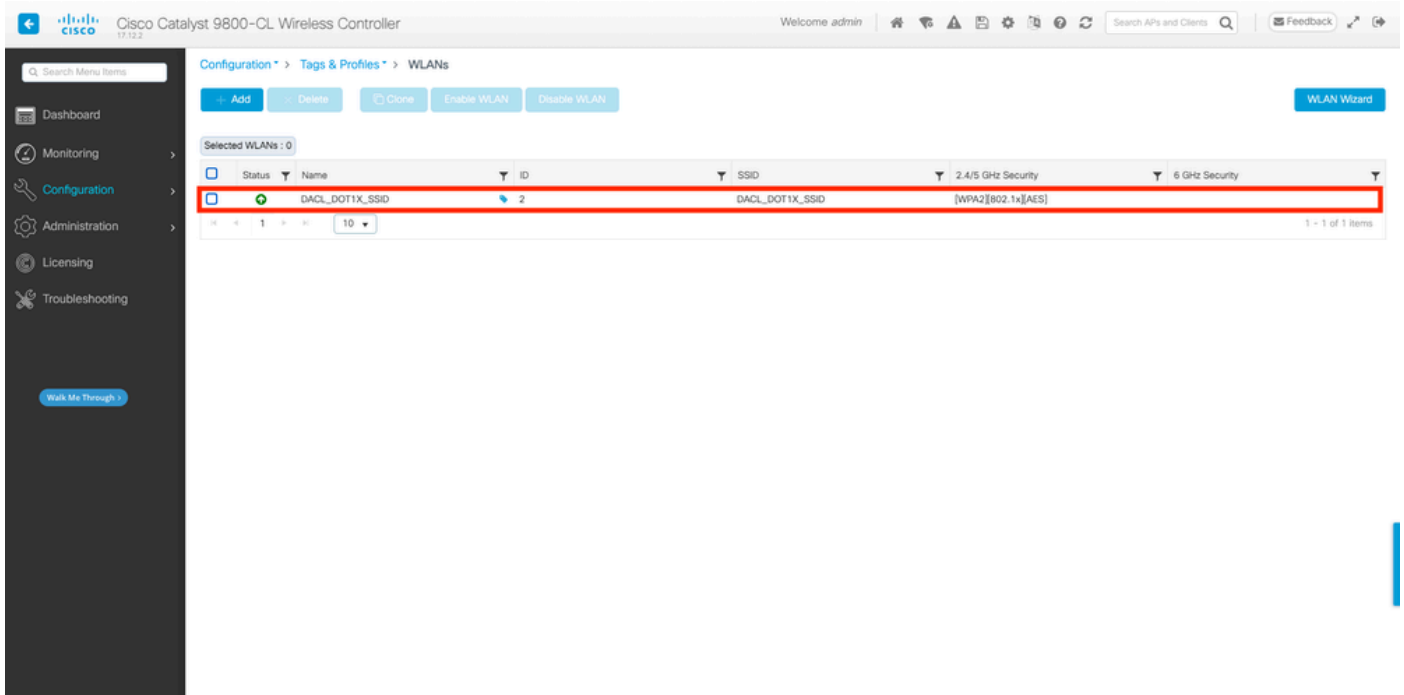
Per i dettagli sulla configurazione degli SSID 802.1x e la risoluzione dei problemi su Catalyst 9800, fare riferimento alla guida alla configurazione dell'[autenticazione 802.1X su Catalyst serie 9800 Wireless Controller](#).

Passaggio 1. Configurare il SSID.

Configurare un SSID autenticato 802.1x utilizzando ISE come server RADIUS. In questo documento, il nome dell'SSID è "DACL\_DOT1X\_SSID".

Dall'interfaccia grafica:

Selezionare Configurazione > Tag e profili > WLAN e creare una WLAN simile a quella mostrata di seguito:



## Dalla 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
```

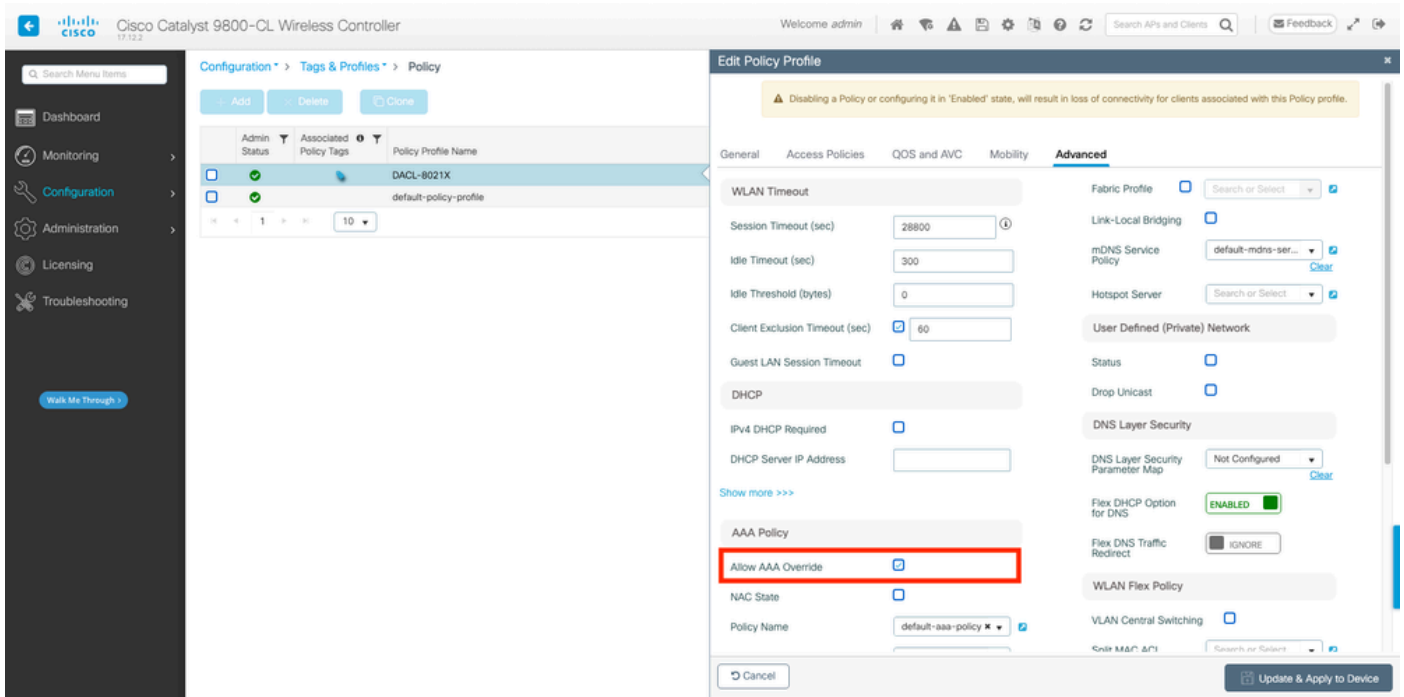
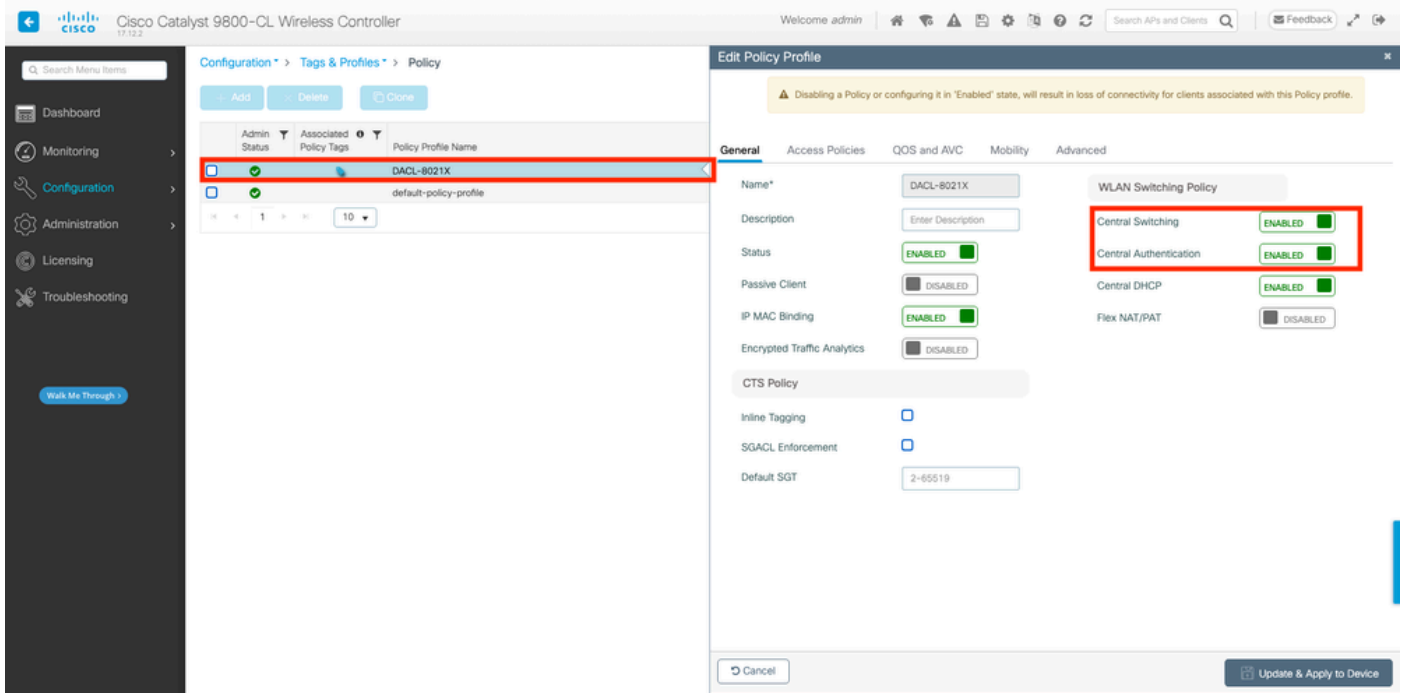
Passaggio 2. Configurare il profilo dei criteri.

Configurare il profilo criteri utilizzato insieme al SSID definito in precedenza. In questo profilo di criteri, verificare che la sostituzione AAA sia configurata dalla scheda "Avanzate", come mostrato nella schermata. In questo documento, il profilo del criterio utilizzato è "DACL-8021X".

Come indicato nella sezione dei prerequisiti, gli dACL sono supportati solo per le distribuzioni di switching/autenticazione centralizzate. Verificare che il profilo dei criteri sia configurato in questo modo.

## Dall'interfaccia grafica:

Passare a Configurazione > Tag e profili > Criterio, selezionare il profilo criterio utilizzato e configurarlo come mostrato.



## Dalla CLI:

```

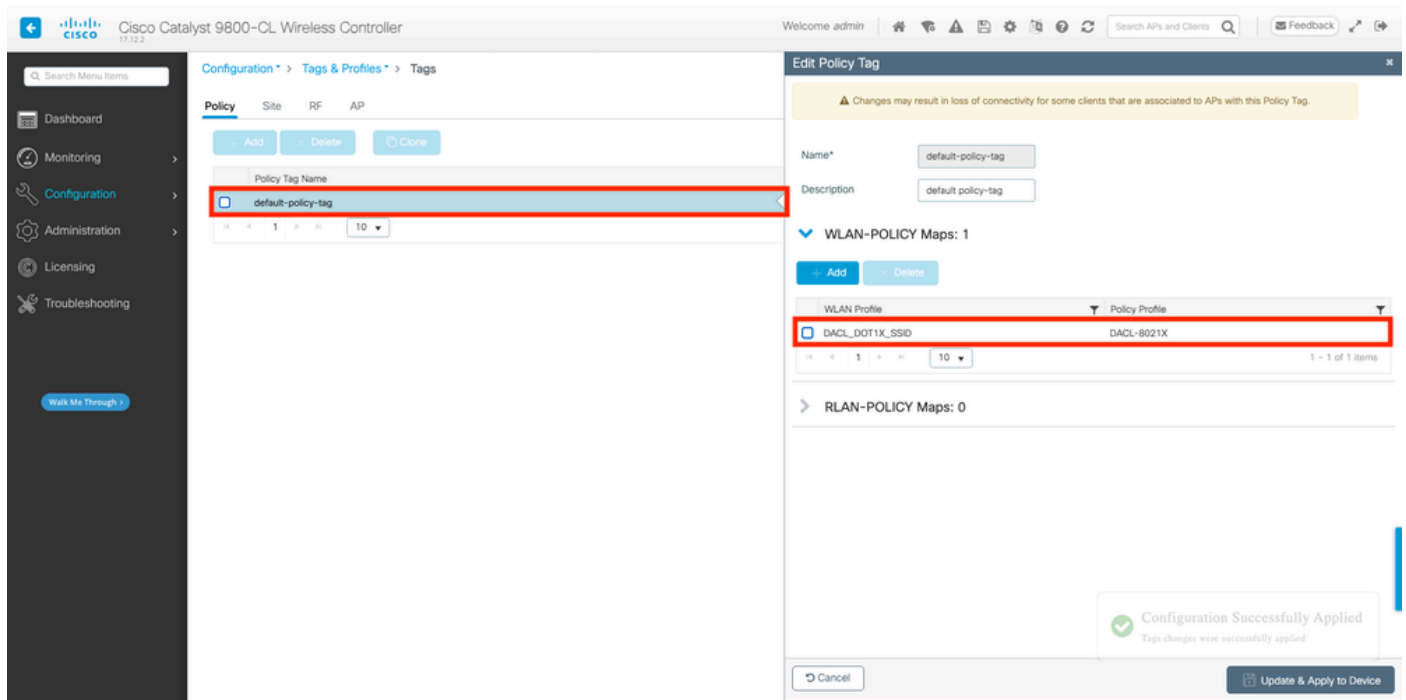
WLC#configure terminal
WLC(config)#wireless profile policy DAACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown

```

Passaggio 3. Assegnare il profilo dei criteri e l'SSID al tag dei criteri utilizzato.

Dall'interfaccia grafica:

Selezionare Configurazione > Tag e profili > Tag. Dalla scheda Tag criteri, creare (o selezionare) il tag utilizzato e assegnargli il profilo WLAN e criteri definito durante i passaggi 1-2.



Dalla 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
```

Passaggio 4. Consenti attributo specifico del fornitore.

Gli ACL scaricabili vengono passati tramite attributi specifici del fornitore (VSA) nello scambio RADIUS tra ISE e WLC. Il supporto di questi attributi può essere abilitato sul WLC, utilizzando questo comando CLI.

Dalla CLI:

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

Passaggio 5. Configurare l'elenco di autorizzazioni predefinito.

Quando si utilizza dACL, è necessario applicare l'autorizzazione di rete tramite RADIUS affinché il

WLC autorizzi qualsiasi utente che esegue l'autenticazione al SSID 802.1x configurato. In questo caso, infatti, non solo l'autenticazione, ma anche la fase di autorizzazione vengono gestite sul lato server RADIUS. Pertanto, in questo caso è necessario l'elenco delle autorizzazioni.

Accertarsi che il metodo di autorizzazione di rete predefinito faccia parte della configurazione 9800.

Dall'interfaccia grafica:

Selezionare Configurazione > Sicurezza > AAA e dalla scheda Elenco metodi AAA > Autorizzazione creare un metodo di autorizzazione simile a quello mostrato.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' tab is active. Under the 'Authorization' section, there is a table with the following data:

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> default	exec	local	N/A	N/A	N/A	N/A
<input type="checkbox"/> default	network	group	radius	N/A	N/A	N/A

Dalla CLI:

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

## Configurazione di ISE

Quando si implementano gli dACL in un ambiente wireless con ISE, è possibile avere due configurazioni comuni:

1. Configurazione dACL per utente. In questo modo, a ogni identità specifica viene assegnato un dACL tramite un campo di identità personalizzato.
2. Configurazione dACL per risultato. Quando si sceglie questo metodo, un determinato dACL viene assegnato a un utente in base al criterio di autorizzazione corrispondente al set di

criteri utilizzato.

## dACL per utente

### Passaggio 1. Definizione di un attributo utente personalizzato dACL

Per poter assegnare un dACL a un'identità utente, è necessario innanzitutto che questo campo sia configurabile per l'identità creata. Per impostazione predefinita, su ISE, il campo "ACL" non è definito per nessuna nuova identità creata. Per risolvere questo problema, è possibile utilizzare "Attributo utente personalizzato" e definire un nuovo campo di configurazione. A tale scopo, selezionare Amministrazione > Gestione delle identità > Impostazioni > Attributi utente personalizzati. Utilizzare il pulsante "+" per aggiungere un nuovo attributo simile a quello mostrato. Nell'esempio, il nome dell'attributo personalizzato è 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 'ACL' is being added. The configuration row is highlighted with a red box:

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 volta configurata questa opzione, utilizzare il pulsante "Salva" per salvare le modifiche.

### Passaggio 2. Configurazione di dACL

Selezionare Policy > Policy Elements > Results > Authorization > Downloadable ACLs (Policy > Elementi della policy > Risultati > Autorizzazione > ACL scaricabili) per visualizzare e definire gli ACL su ISE. Utilizzare il pulsante "Aggiungi" per crearne uno nuovo.



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 is a 'License Warning' icon and several utility icons. Below the navigation bar, there are tabs for 'Dictionaries', 'Conditions', and 'Results', with 'Results' being the active tab. 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' and shows a table of existing ACLs. The table has two columns: 'Name' and 'Description'. The table contains seven rows of ACLs. Above the table, there are action buttons: 'Edit', '+ Add', 'Duplicate', and 'Delete'. A red box highlights the '+ Add' button, and a red arrow points to it. The table data is as follows:

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

Verrà aperto il modulo di configurazione "New Downloadable ACL" (Nuovo ACL scaricabile). In questo caso, configurare i seguenti campi:

- Nome: il nome dell'ACL definito.
- Description (facoltativo): breve descrizione dell'uso dell'elenco di controllo di accesso creato.
- Versione IP: la versione del protocollo IP utilizzata nell'elenco ACL definito (versione 4, 6 o entrambe).
- Contenuto DACL: il contenuto dell'elenco di controllo di accesso (ACL) di Cisco IOS XE, in base alla sintassi.

Nel presente documento, il valore dACL utilizzato è "ACL\_USER1" e questo dACL consente tutto il traffico eccetto quello destinato alle versioni 10.48.39.186 e 10.48.39.13.

Una volta configurati i campi, usare il pulsante "Submit" (Invia) per creare l'ACL.

Ripetere la procedura per definire l'ACL per il secondo utente, ACL\_USER2, come mostrato nella figura.

The screenshot shows the Cisco ISE interface for Policy Elements. The left sidebar contains a navigation menu with categories: Authentication, Authorization (with sub-items Authorization Profiles and Downloadable ACLs), Profiling, Posture, and Client Provisioning. The main content area is titled "Downloadable ACLs" and shows a table of ACLs. The table has columns for Name and Description. Two rows are highlighted with a red box: ACL\_USER1 (ACL assigned to USER1) and ACL\_USER2 (ACL assigned to USER2). Other ACLs include DENY\_ALL\_IPV4\_TRAFFIC, DENY\_ALL\_IPV6\_TRAFFIC, PERMIT\_ALL\_IPV4\_TRAFFIC, PERMIT\_ALL\_IPV6\_TRAFFIC, test-dacl-cwa, and test-dacl-dot1x. At the top right, there are options for "Selected 0 Total 8" and a search icon.

Passaggio 3. Assegnare il dACL a un'identità creata

Una volta creato l'ACL, è possibile assegnarlo a qualsiasi identità ISE utilizzando gli attributi personalizzati dell'utente creati nel passo 1. A tale scopo, selezionare Amministrazione > Gestione delle identità > Identità > Utenti. Come al solito, utilizzare il pulsante "Aggiungi" per creare un utente.

The screenshot shows the Cisco ISE Administration - Identity Management interface. The top navigation bar includes "Administration - Identity Management" and "License Warning". The left sidebar has "Identities" selected, with "Users" highlighted. The main content area is titled "Network Access Users" and shows a table of users. The table has columns for Status, Username, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. One user is listed: Disabled, adminuser, admin-group. At the top right, there are options for "Selected 0 Total 1" and a search icon. A red box highlights the "+ Add" button, with a red arrow pointing to it.

Nel modulo di configurazione "Nuovo utente di accesso alla rete", definire il nome utente e la password per l'utente creato. Utilizzare l'attributo personalizzato "ACL" per assegnare l'ACL creato

nel passaggio 2 all'identità. Nell'esempio, viene definita l'identità USER1 che utilizza 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 the "Network Access User" section, the "Username" field is set to "USER1". The "Status" is "Enabled". The "Password" section shows "Password Type: Internal Users" and "Password Lifetime: With Expiration (53 days)". The "Login Password" field is highlighted in red, along with the "Generate Password" button. The "ACL" field is set to "ACL\_USER1" and is also highlighted in red. At the bottom right, the "Save" button is highlighted in red.

Una volta configurati correttamente i campi, utilizzare il pulsante "Invia" per creare l'identità.

Ripetere questo passaggio per creare USER2 e assegnarvi ACL\_USER2.

The screenshot shows the "Network Access Users" list in the Cisco ISE Administration interface. The table has the following columns: 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 in red. Below the table, there is a "Network Access Users" button.

Passaggio 4. Configura risultato criteri di autorizzazione.

Dopo aver configurato l'identità e avergli assegnato l'ACL, è necessario configurare i criteri di autorizzazione in modo che corrispondano all'attributo utente personalizzato "ACL" definito per un'attività comune di autorizzazione esistente. A tale scopo, selezionare Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. Utilizzare il pulsante "Aggiungi" per definire un nuovo criterio di autorizzazione.

- Nome: il nome del criterio di autorizzazione, qui "9800-DOT1X-USERS".
- Tipo di accesso: il tipo di accesso utilizzato quando viene stabilita una corrispondenza con questo criterio, in questo caso ACCESS\_ACCEPT.
- Attività comune: associare "Nome DACL" a InternalUser:<nome dell'attributo personalizzato creato> per l'utente interno. In base ai nomi utilizzati in questo documento, il profilo 9800-DOT1X-USERS è configurato con dACL configurato come InternalUser:ACL.

The screenshot shows the Cisco ISE interface for configuring a new Authorization Profile. The page title is "Policy - Policy Elements". The left sidebar shows navigation options: Dictionaries, Conditions, Results, Authentication, Authorization, Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled "Authorization Profile" and contains the following fields:

- 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:**

Under the "Common Tasks" section, the "dACL Name" field is set to "InternalUser:ACL". Other options like "IPv6 DACL Name", "ACL (Filter-ID)", and "Filter-ID" are present but not selected.

Passaggio 5. Usa profilo di autorizzazione nel set di criteri.

Dopo aver definito correttamente il risultato del profilo di autorizzazione, è necessario che faccia ancora parte del set di criteri utilizzato per autenticare e autorizzare gli utenti wireless. Passare a Criterio > Set di criteri e aprire il set di criteri utilizzato.

In questo caso, la regola dei criteri di autenticazione "Dot1X" corrisponde a qualsiasi connessione effettuata tramite cavo o wireless 802.1x. La regola dei criteri di autorizzazione "802.1x Users dACL" implementa una condizione nell'SSID utilizzato (ovvero Radius-Called-Station-ID CONTIENE DACL\_DOT1X\_SSID). Se viene eseguita un'autorizzazione sulla WLAN "DACL\_DOT1X\_SSID", per autorizzare l'utente viene utilizzato il profilo "9800-DOT1X-USERS" definito al passaggio 4.

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 > Options	65	⚙️
✓	Default		All_User_ID_Stores > Options	10	⚙️

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (2)

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

## dACL per risultato

Per evitare l'enorme compito di assegnare un particolare dACL a ciascuna identità creata con ISE, si può scegliere di applicare il dACL a un particolare risultato della policy. Questo risultato viene quindi applicato in base a qualsiasi condizione corrispondente alle regole di autorizzazione del set di criteri utilizzato.

### Passaggio 1. Configurazione di dACL

Eeguire lo stesso passaggio 2 dalla [sezione dACL per utente](#) per definire gli dACL necessari. Si tratta di ACL\_USER1 e ACL\_USER2.

### Passaggio 2. Creare identità

Selezionare Amministrazione > Gestione delle identità > Identità > Utenti e utilizzare il pulsante "Aggiungi" per creare un utente.

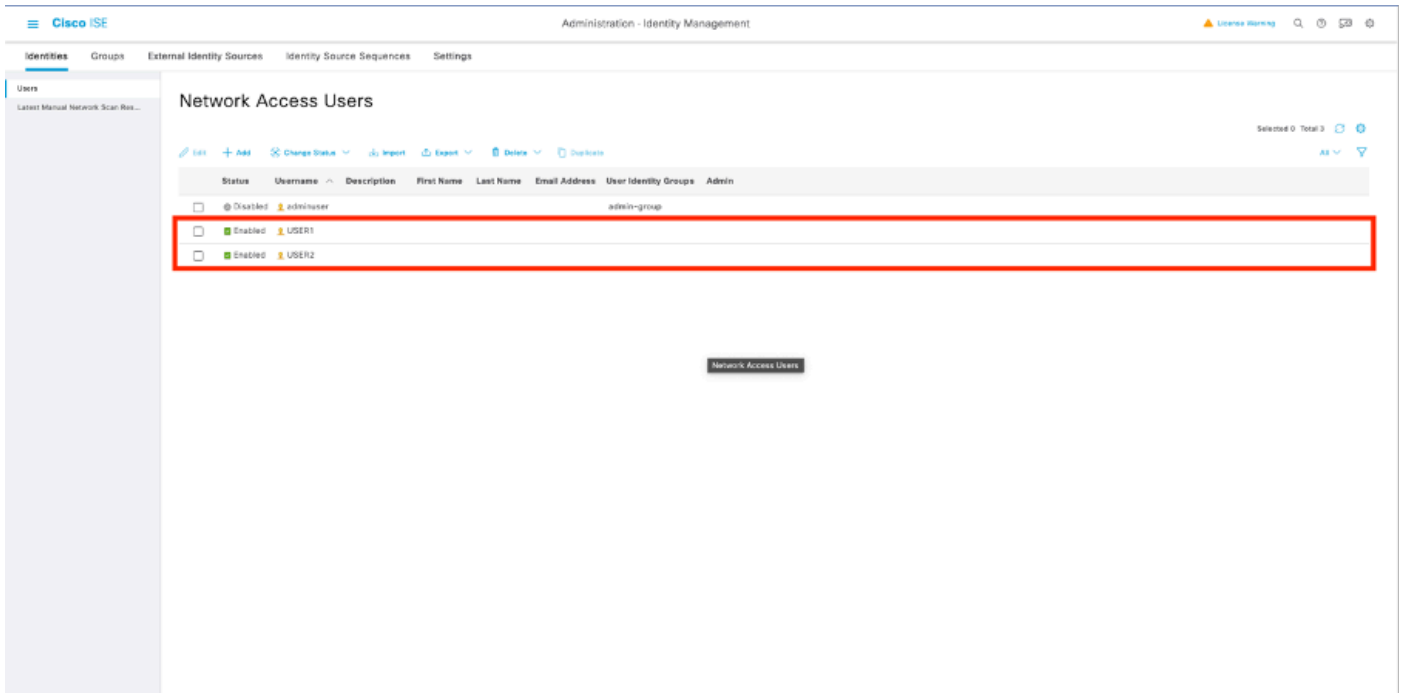
The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Administration - Identity Management' and 'License Warning'. The left sidebar has 'Identities' selected. The main content area is titled 'Network Access Users' and features a toolbar with 'Add', 'Change Status', 'Import', 'Export', 'Delete', and 'Duplicate' buttons. A table lists the following user:

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Disabled	adminuser				admin-group	

Nel modulo di configurazione "Nuovo utente di accesso alla rete", definire il nome utente e la password per l'utente creato.

The screenshot shows the 'New Network Access User' configuration page. The 'Username' field is set to 'USER1'. The 'Status' is 'Enabled'. The 'Password' field is highlighted, showing a 'Generate Password' button. The 'Submit' button is highlighted at the bottom right.

Ripetere questo passaggio per creare USER2.



Passaggio 4. Configurare il risultato del criterio di autorizzazione.

Dopo aver configurato l'identità e l'ACL, è necessario configurare il criterio di autorizzazione per assegnare un determinato dACL all'utente che soddisfa la condizione per l'utilizzo del criterio. A tale scopo, selezionare Criteri > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. Utilizzare il pulsante "Aggiungi" per definire un nuovo criterio di autorizzazione e completare questi campi.

- Nome: il nome del criterio di autorizzazione, qui "9800-DOT1X-USER1".
- Tipo di accesso: il tipo di accesso utilizzato quando viene trovata una corrispondenza con questo criterio, in questo caso ACCESS\_ACCEPT.
- Attività comune: associare "Nome DACL" a "ACL\_USER1" per l'utente interno. In base ai nomi utilizzati nel documento, il profilo 9800-DOT1X-USER1 è configurato con il dACL configurato come "ACL\_USER1".

The screenshot shows the configuration page for a new Authorization Profile in Cisco ISE. The profile name is "9800-DOT1X-USER1". The Access Type is set to "ACCESS\_ACCEPT". Under Common Tasks, the DACL Name is set to "ACL\_USER1". The Attributes Details section shows "Access Type = ACCESS\_ACCEPT" and "DACL = ACL\_USER1".

Ripetere questo passaggio per creare il risultato del criterio "9800-DOT1X-USER2" e assegnare ad esso "ACL\_USER2" come DACL.

The screenshot shows the "Standard Authorization Profiles" list in Cisco ISE. Two profiles are highlighted with a red box: "9800-DOT1X-USER1" and "9800-DOT1X-USER2".

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

Passaggio 5. Usa profili di autorizzazione nel set di criteri.

Dopo aver definito correttamente il profilo di autorizzazione, è necessario che faccia parte del set di criteri utilizzato per autenticare e autorizzare gli utenti wireless. Passare a Criterio > Set di criteri e aprire il set di criteri utilizzato.

In questo caso, la regola dei criteri di autenticazione "Dot1X" corrisponde a qualsiasi connessione effettuata tramite cavo o wireless 802.1X. La regola dei criteri di autorizzazione "802.1X User 1



dACL" implementa una condizione sul nome utente utilizzato (ovvero InternalUser-Name CONTAINS USER1). Se si esegue un'autorizzazione utilizzando il nome utente USER1, per autorizzare l'utente viene utilizzato il profilo "9800-DOT1X-USER1" definito nel passaggio 4. Di conseguenza, all'utente viene applicato anche il dACL risultante da questo risultato (ACL\_USER1). La stessa configurazione viene effettuata per il nome utente USER2, per il quale viene utilizzato "9800-DOT1X-USER1".

The screenshot displays the Cisco ISE Policy Sets configuration interface. It is divided into two main sections: Authentication Policy and Authorization Policy.

**Authentication Policy (2):**

Status	Rule Name	Conditions	Use	Hits	Actions
On	Dot1X	Wired_802.1X Wired_802.1X Wired_802.1X Wired_802.1X	All_User_ID_Stores		Options
On	Default		All_User_ID_Stores		Options

**Authorization Policy (3):**

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
On	802.1x User 2 dACL	InternalUser-Name EQUALS USER2	9800-DOT1X-USER2	Select from list		Options
On	802.1x User 1 dACL	InternalUser-Name EQUALS USER1	9800-DOT1X-USER1	Select from list		Options
On	Default		DenyAccess	Select from list		Options

## Note sull'utilizzo di ACL con SSID CWA

Come descritto nella [guida alla configurazione di Configure Central Web Authentication \(CWA\) su Catalyst 9800 WLC e ISE](#), CWA si basa sul protocollo MAB e su risultati particolari per autenticare e autorizzare gli utenti. Gli ACL scaricabili possono essere aggiunti alla configurazione CWA dal lato ISE nello stesso modo in cui sono stati descritti sopra.



Avviso: gli ACL scaricabili possono essere utilizzati solo come elenco degli accessi alla rete e non sono supportati come ACL di preautenticazione. Pertanto, tutti gli ACL di preautenticazione utilizzati in un flusso di lavoro CWA devono essere definiti nella configurazione WLC.

---

## Verifica

Per verificare la configurazione effettuata, è possibile utilizzare questi comandi.

```
# 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 }
```

Di seguito viene riportata la parte corrispondente della configurazione WLC corrispondente a questo esempio.

```
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
```

Viene presentata la configurazione del server RADIUS, visualizzata con il 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
```

Risoluzione dei problemi

Elenco di controllo

- Verificare che i client possano connettersi correttamente all'SSID 802.1X configurato.
- Verificare che la richiesta/accettazione di accesso RADIUS contenga le coppie attributo-valore corrette.
- Verificare che i client utilizzino il profilo WLAN/criterio appropriato.

WLC One Stop-Shop Reflex

Per verificare che l'ACL sia assegnato correttamente a un client wireless specifico, usare il comando **show wireless client mac-address <H.H.H>detail** come mostrato. Da qui è possibile visualizzare diverse informazioni utili per la risoluzione dei problemi, ossia il nome utente del client, lo stato, il profilo della policy, la WLAN e, cosa più importante, l'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 : Associated
```

```
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  
[...]
```

Comandi Show WLC

Per visualizzare tutti gli ACL che fanno attualmente parte della configurazione Catalyst 9800 WLC, è possibile usare il comando **show access-lists**. Con questo comando vengono elencati tutti gli ACL definiti localmente o gli ACL scaricati dal WLC. Ogni dACL scaricato dall'ISE dal WLC ha il formato xACSACLx-IP-<ACL\_NAME>-<ACL\_HASH>.

---

**Nota:** gli ACL scaricabili rimangono nella configurazione finché un client è associato e lo utilizza nell'infrastruttura wireless. Non appena l'ultimo client che utilizza dACL lascia l'infrastruttura, dACL viene rimosso dalla configurazione.

---

```
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
[...]
```

### Debug condizionale e traccia Radioactive (RA)

Durante la risoluzione dei problemi relativi alla configurazione, è possibile raccogliere [tracce radioattive](#) per un client che si suppone debba essere assegnato con l'ACL definito. Qui sono evidenziati i log che mostrano la parte interessante delle tracce radioattive durante il processo di associazione del client 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\$®vf9JØ«? %ÿ0?ã@≤™ÇÑbWi6\È&\q·1U+QB-º®”#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] 6 192

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] 30

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

## Acquisizione pacchetti

Un altro riflesso interessante è quello di prendere e analizzare le acquisizioni dei pacchetti del flusso RADIUS per un'associazione client. Gli ACL scaricabili si basano su RADIUS, non solo per essere assegnati a un client wireless, ma anche per essere scaricati dal WLC. Durante l'acquisizione dei pacchetti per la risoluzione dei problemi relativi alla configurazione degli ACL, è necessario eseguire l'acquisizione sull'interfaccia utilizzata dal controller per comunicare con il server RADIUS. [Questo documento](#) mostra come configurare un'acquisizione dei pacchetti facilmente integrabile in Catalyst 9800, che è stato usato per raccogliere l'acquisizione analizzata in questo articolo.

## Autenticazione client RADIUS

È possibile visualizzare la richiesta di accesso RADIUS del client inviata dal WLC al server RADIUS per autenticare l'utente USER1 (nome utente AVP) sul DACL\_DOT1X\_SSID SSID (identificatore NAS AVP).

```
480...617...39 10.48.39.130...10.48.39.134...Access-Request id=92, Duplicate Request...RADIUS
480...594...39 10.48.39.134...10.48.39.130...Access-Request 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=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=333743504d53657373696f6e49443d3832323733303041303030303039463834393335..
  > 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
```

Quando l'autenticazione ha esito positivo, il server RADIUS risponde con un messaggio di accettazione dell'accesso, sempre per l'utente USER1 (nome utente AVP), e applica gli attributi AAA, in particolare l'ACS AVP: CiscoSecure-Defined-ACL specifico del fornitore indicato qui "#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)
  
```

### Download DACL

Se l'ACL fa già parte della configurazione WLC, viene semplicemente assegnato all'utente e la sessione RADIUS termina. In caso contrario, il WLC scarica l'ACL, usando ancora RADIUS. A tale scopo, il WLC effettua una richiesta di accesso RADIUS, questa volta utilizzando il nome dACL ("#ACSACL#-IP-ACL\_USER1-65e89aab") per il nome utente AVP. Inoltre, il WLC informa il server RADIUS che questa opzione di accettazione dell'accesso avvia il download di un ACL utilizzando la coppia Cisco AV 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
  
```

L'autorizzazione di accesso RADIUS inviata al controller contiene l'ACL richiesto, come mostrato. Ogni regola ACL è contenuta in un altro Cisco AVP di tipo "ip:inacl#<X>=<ACL\_RULE>", dove <X> è il numero della regola.



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=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

▼ RADIUS Protocol (radius), 323 bytes

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



**Nota:** se il contenuto di un ACL di download viene modificato dopo essere stato scaricato sul WLC, la modifica apportata a questo ACL non viene applicata finché un utente che utilizza questo ACL non esegue nuovamente l'autenticazione RADIUS per questo utente. Infatti, una modifica nell'ACL si riflette nella parte hash del nome dell'ACL. Pertanto, alla successiva assegnazione di questo ACL a un utente, il suo nome deve essere diverso e quindi l'ACL non deve far parte della configurazione WLC e deve essere scaricato. Tuttavia, i client che eseguono l'autenticazione prima della modifica nell'ACL continuano a utilizzare quello precedente fino a quando non eseguono di nuovo l'autenticazione.

---

## Registri delle operazioni ISE

### Autenticazione client RADIUS

I log delle operazioni mostrano un'autenticazione riuscita dell'utente "USER1", a cui è applicato l'ACL "ACL\_USER1" scaricabile. Le parti di interesse per la risoluzione dei problemi sono evidenziate in rosso.

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=94b3604f5b49b88ccf9e2f3a86c80d1979b5c43

Result	
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.

Session Events	
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

```

## Download DACL

I log delle operazioni mostrano che il download dell'ACL "ACL\_USER1" è riuscito. Le parti di interesse per la risoluzione dei problemi sono evidenziate in rosso.

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:inacl#1=deny ip any host 10.48.39.13
cisco-av-pair	ip:inacl#2=deny ip any host 10.48.39.15
cisco-av-pair	ip:inacl#3=deny ip any host 10.48.39.186
cisco-av-pair	ip:inacl#4=permit ip any any

Steps

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

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).