

# Catalyst 9800での& ; の設定とダウンロード可能ACLのトラブルシューティング

## 内容

---

[はじめに](#)

[背景説明](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[802.1x SSIDでのdACLの使用](#)

[ネットワーク図](#)

[WLC の設定](#)

[ISE 設定](#)

[ユーザごとのdACL](#)

[結果ごとのdACL](#)

[CWA SSIDでのdACLの使用についての注意](#)

[確認](#)

[トラブルシューティング](#)

[Checklist](#)

[WLCワンストップシヨップリフレックス](#)

[WLCのshowコマンド](#)

[条件付きデバッグとラジオアクティブトレース](#)

[パケットキャプチャ](#)

[RADIUSクライアント認証](#)

[DACLのダウンロード](#)

[ISE操作ログ](#)

[RADIUSクライアント認証](#)

[DACLのダウンロード](#)

---

## はじめに

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(WLC)でのダウンロード可能ACL(dACL)の設定とトラブルシューティングの方法について説明します。

## 背景説明

dACLは、Cisco IOS®およびIOS XE®スイッチで長年にわたりサポートされてきました。dACLとは、認証が発生したときに、ACLのローカルコピーが存在してACL名が割り当てられるのではな

く、ネットワークデバイスがRADIUSサーバからACLエントリを動的にダウンロードすることを指します。より完全な[Cisco ISEの設定例](#)を使用できます。このドキュメントでは、17.10リリース以降、中央スイッチング用にdACLをサポートしているCisco Catalyst 9800に焦点を当てています。

## 前提条件

このドキュメントの目的は、基本的なSSID設定の例を使用して、Catalyst 9800でのdACLの使用を示し、これらを完全にカスタマイズできる方法を示すことです。

Catalyst 9800ワイヤレスコントローラでは、ダウンロード可能ACLは次のとおりです

- [Cisco IOS XE Dublin 17.10.1](#)リリース以降でサポートされます。
- ローカルモードのアクセスポイントのみを使用した集中型コントローラ（またはFlexconnect中央スイッチング）でサポートされます。FlexConnectローカルスイッチングはdACLをサポートしていません。

## 要件

次の項目に関する知識があることが推奨されます。

- Catalyst Wireless 9800設定モデル。
- Cisco IPアクセスコントロールリスト(ACL)。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

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

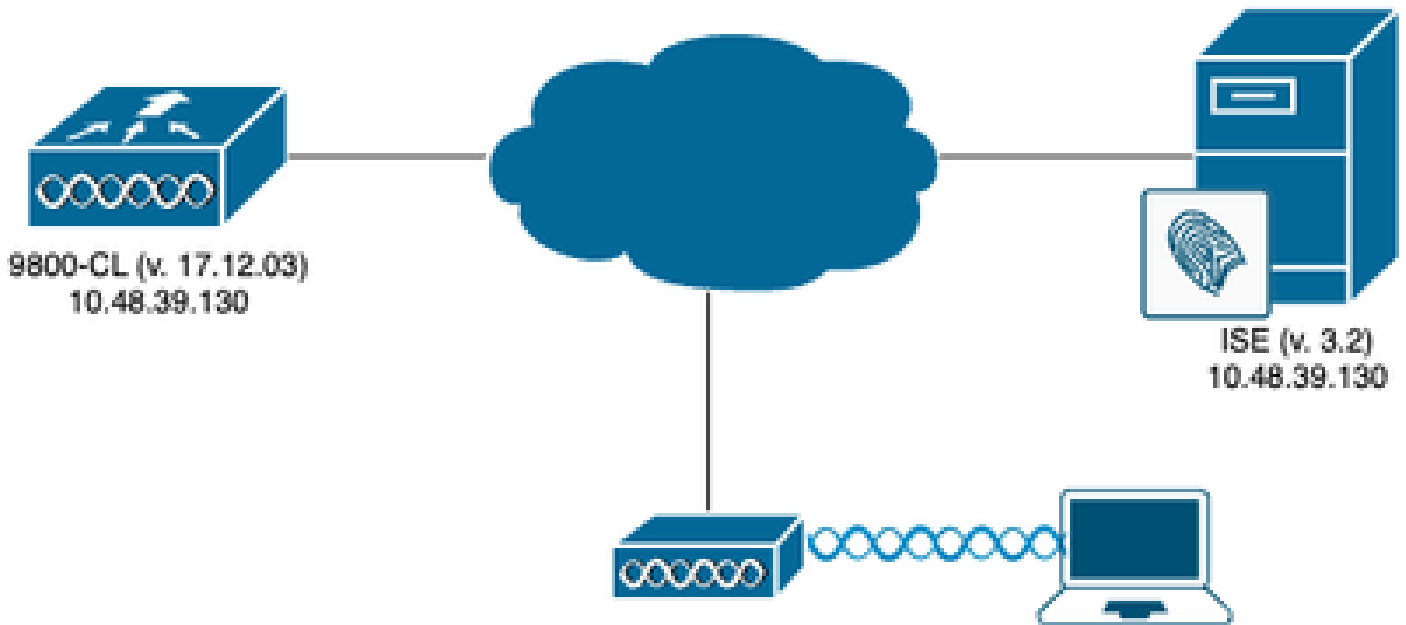
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

この設定ガイドでは、方式（WLAN認証、ポリシー設定など）が異なる場合でも、最終的な結果は同じです。ここで説明するシナリオでは、USER1とUSER2という2つのユーザIDが定義されています。どちらもワイヤレスネットワークへのアクセスを許可されます。それぞれに、ACL\_USER1とACL\_USER2がそれぞれ割り当てられます。これらは、Catalyst 9800によってISEからダウンロードされるdACLです。

## 802.1x SSIDでのdACLの使用

## ネットワーク図



## WLC の設定

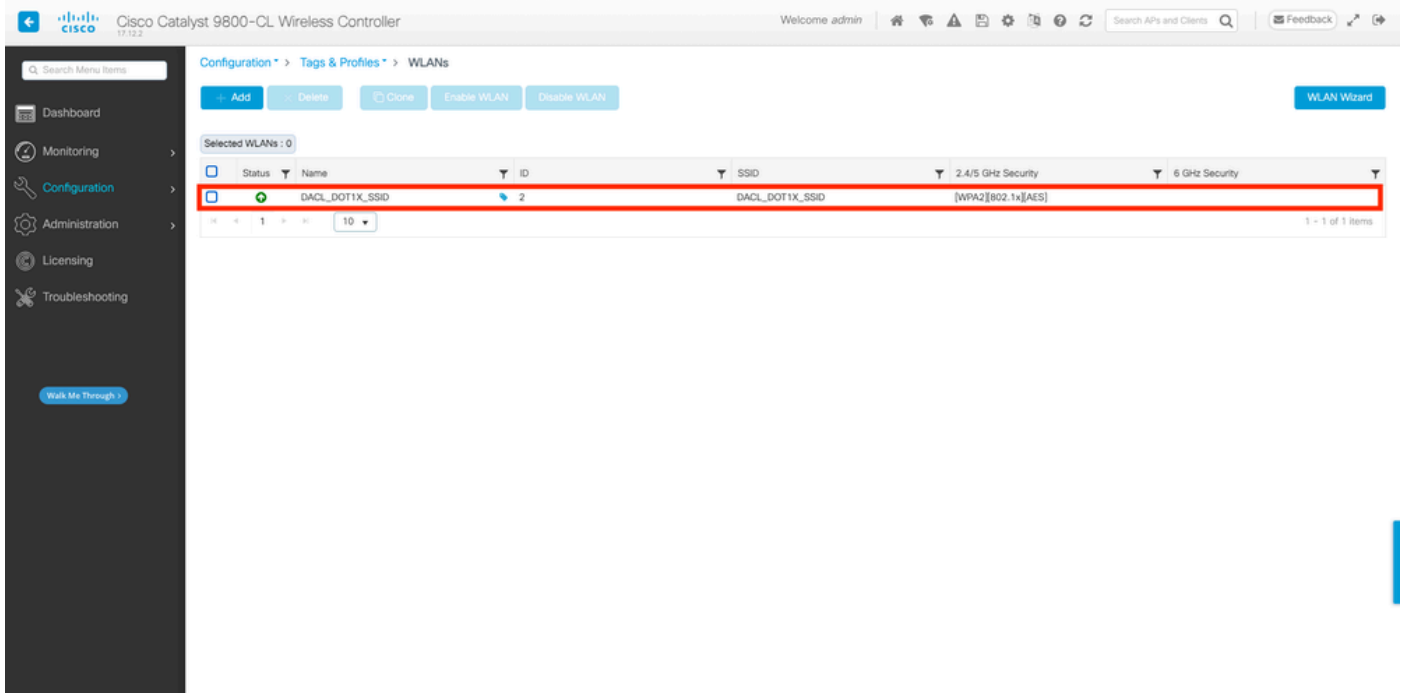
Catalyst 9800での802.1x SSIDの設定とトラブルシューティングの詳細については、『[Catalyst 9800ワイヤレスコントローラシリーズでの802.1X認証の設定](#)』コンフィギュレーションガイドを参照してください。

ステップ 1 : SSID を設定します。

RADIUSサーバとしてISEを使用して、802.1x認証済みSSIDを設定します。このドキュメントでは、SSIDは「DAACL\_DOT1X\_SSID」という名前になっています。

GUI で次の手順を実行します。

Configuration > Tags & Profiles > WLANの順に移動し、次に示すようなWLANを作成します。



CLI から、

```
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
```

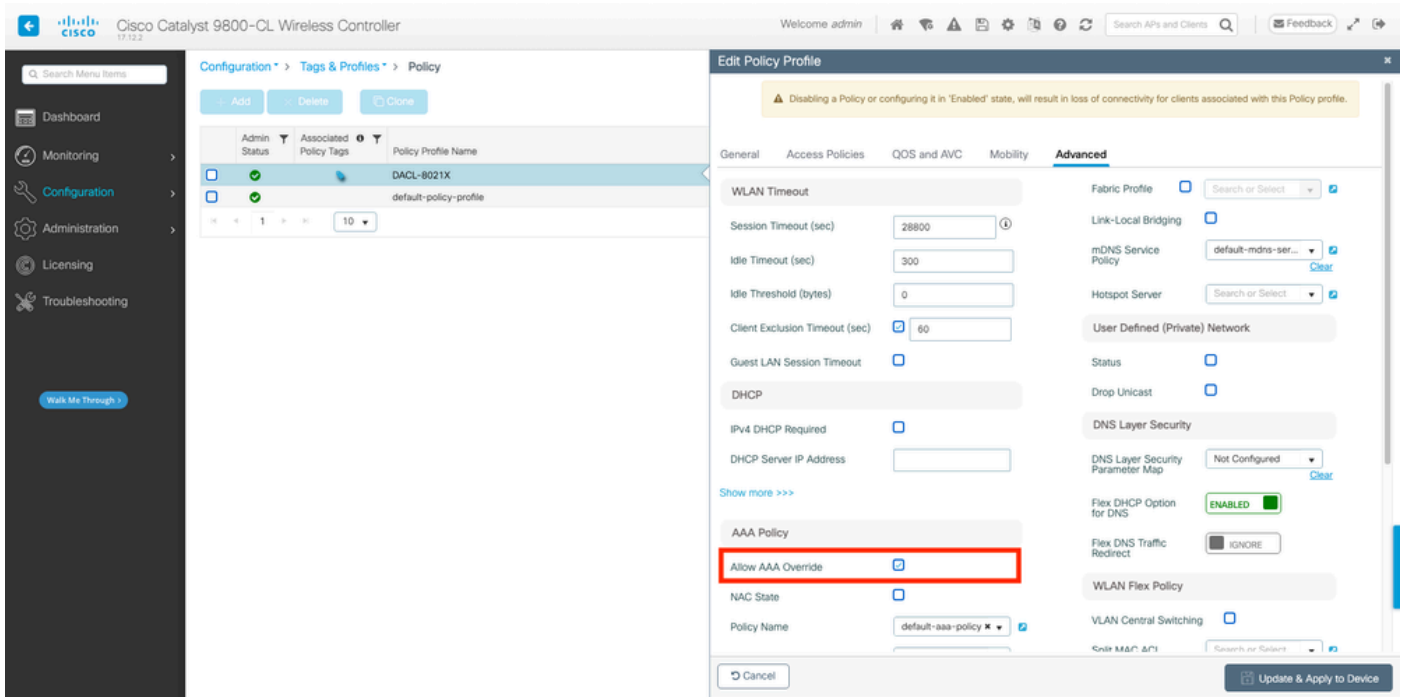
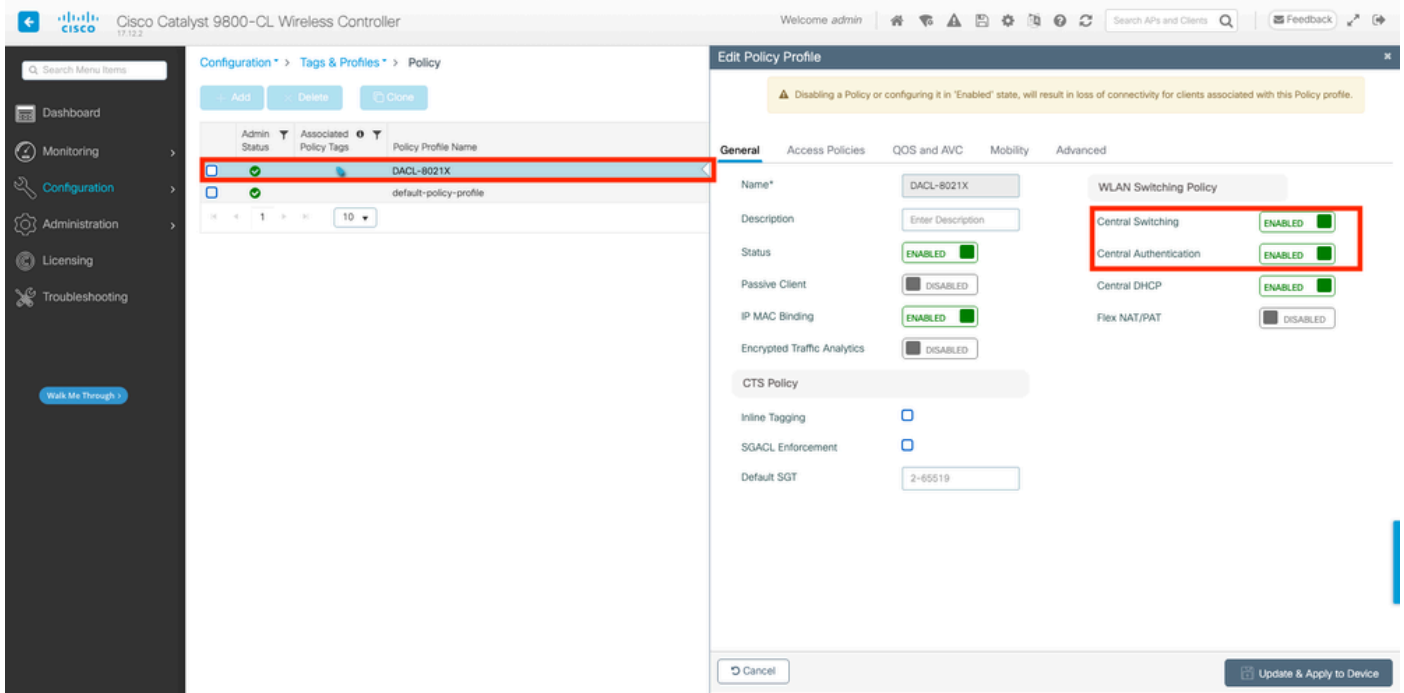
ステップ 2 : ポリシープロファイルを設定します。

上で定義したSSIDとともに使用されるポリシープロファイルを設定します。このポリシープロファイルで、スクリーンショットに示すように、「Advanced」タブからAAA Overrideが設定されていることを確認します。このドキュメントでは、使用するポリシープロファイルは「DACL-8021X」です。

「前提条件」セクションで説明したように、dACLは中央スイッチング/認証導入でのみサポートされます。ポリシープロファイルがそのように設定されていることを確認します。

GUI で次の手順を実行します。

Configuration > Tags & Profiles > Policyの順に移動し、使用するポリシープロファイルを選択して、ここに示すように設定します。



CLI から、

```

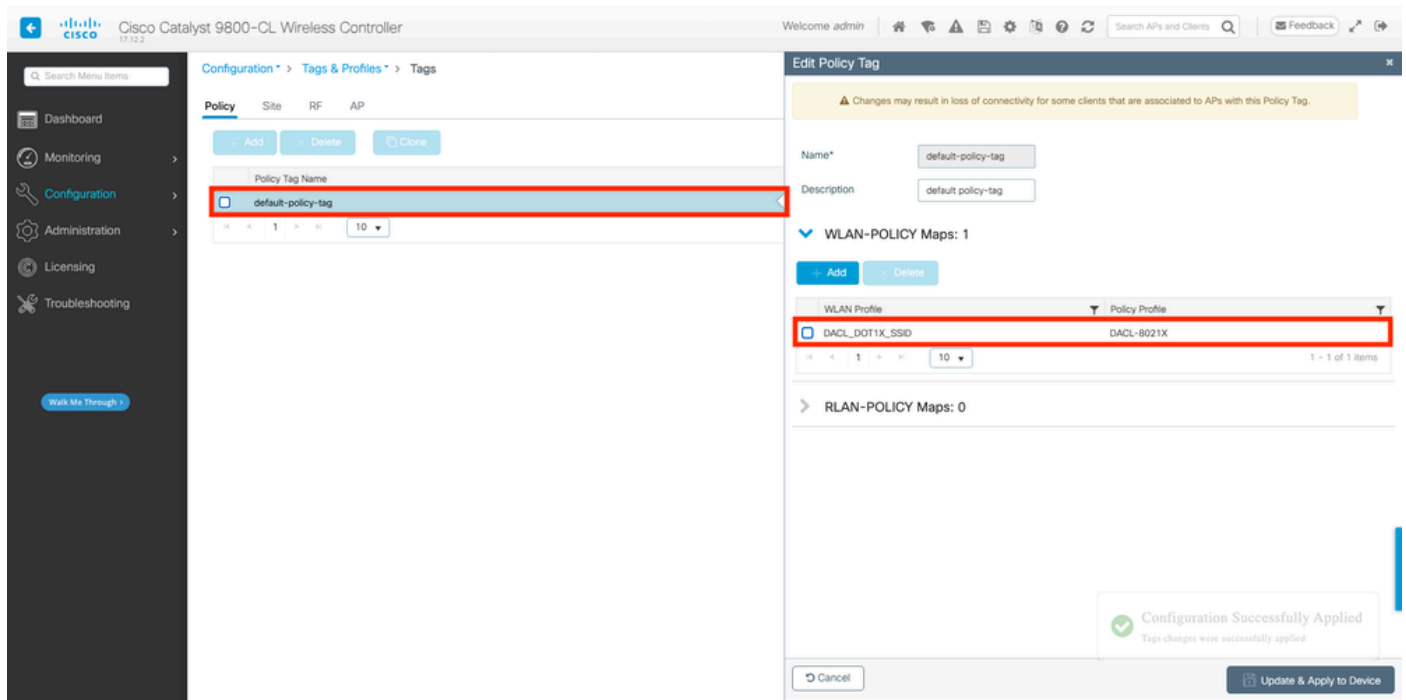
WLC#configure terminal
WLC(config)#wireless profile policy DAACL-8021X
WLC(config-wireless-policy)#aaa-override
WLC(config-wireless-policy)#vlan VLAN_1413
WLC(config-wireless-policy)#no shutdown

```

ステップ 3 : 使用するポリシータグにポリシープロファイルとSSIDを割り当てます。

GUI で次の手順を実行します。

Configuration > Tags & Profiles > Tagsの順に移動します。Policy tagsタブで、使用するタグを作成 (または選択) し、ステップ1 ~ 2で定義したWLANとポリシープロファイルを割り当てます。



CLI から、

```
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
```

ステップ 4 : ベンダー固有の属性を許可します。

ダウンロード可能ACLは、ISEとWLC間のRADIUS交換でベンダー固有属性(VSA)を介して渡されます。これらの属性のサポートは、次のCLIコマンドを使用してWLCでイネーブルにできます。

CLI から、

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

ステップ 5 : デフォルトの許可リストを設定します。

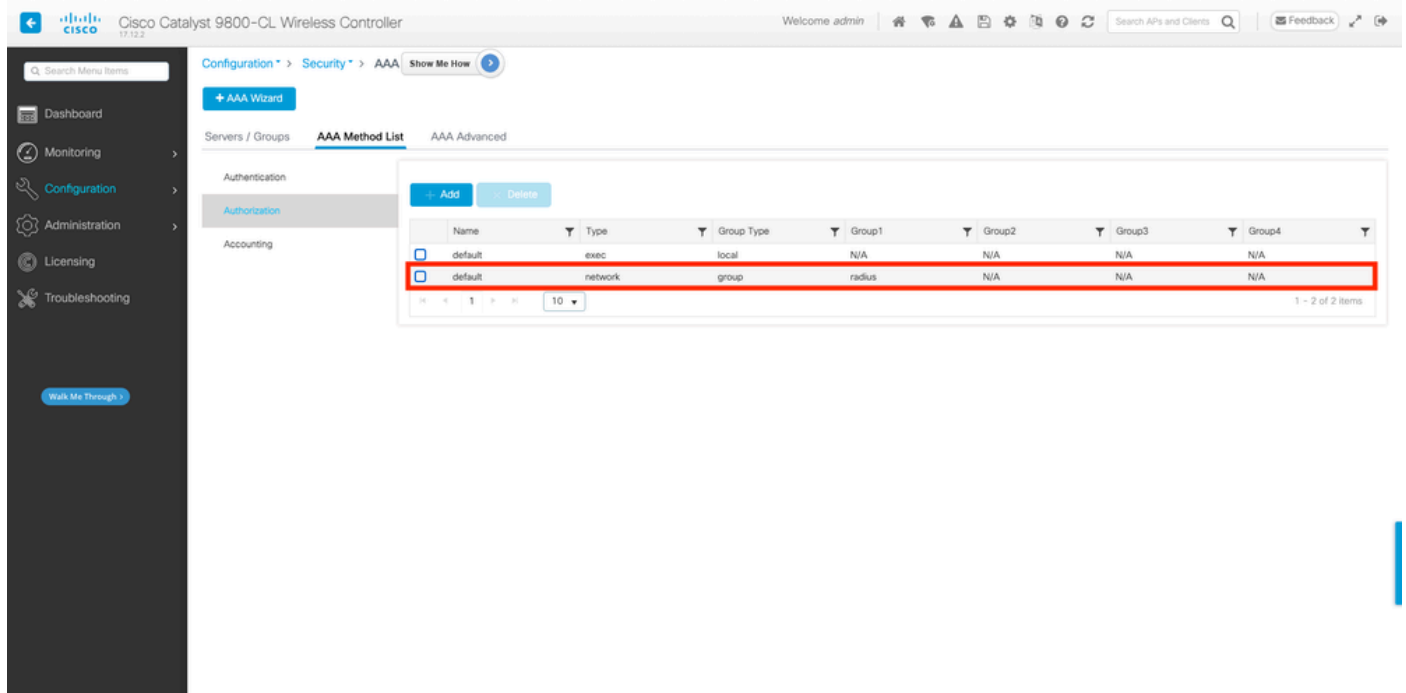
dACLを使用する場合、設定された802.1x SSIDに対して認証するすべてのユーザをWLCで認可するためには、RADIUSによるネットワーク認可を適用する必要があります。実際に、ここでは認

証だけでなく、認可フェーズもRADIUSサーバ側で処理されます。したがって、この場合は認証リストが必要です。

デフォルトのネットワーク許可方式が9800設定の一部であることを確認します。

GUIで次の手順を実行します。

Configuration > Security > AAAの順に移動し、AAA Method List > Authorizationタブで、表示されているような許可方式を作成します。



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Security > AAA. The 'AAA Method List' page is displayed, with the 'Authorization' tab selected. A table lists two entries:

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

The second row is highlighted with a red box. The table also includes checkboxes for each entry and a 'Walk Me Through' button at the bottom left of the main content area.

CLIから、

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

## ISE 設定

ISEを使用してワイヤレス環境にdACLを実装する場合、次の2つの一般的な設定を知ることができます。

1. ユーザごとのdACL設定。これにより、カスタムIDフィールドを使用して特定の各IDにdACLが割り当てられます。
2. 結果ごとのdACL設定。この方式を選択すると、使用するポリシーセットに一致した許可ポリシーに基づいて、特定のdACLがユーザに割り当てられます。

## ユーザごとのdACL

## ステップ 1 : dACLカスタムユーザ属性の定義

ユーザIDにdACLを割り当てるには、最初にこのフィールドを、作成したIDで設定可能にする必要があります。デフォルトでは、ISEで作成された新しいIDに対して「ACL」フィールドは定義されていません。これを解決するには、「カスタムユーザ属性」を使用して、新しい設定フィールドを定義します。これを行うには、Administration > Identity Management > Settings > User Custom Attributesの順に移動します。「+」ボタンを使用して、表示されているのと同じような新しい属性を追加します。この例では、カスタム属性の名前はACLです。

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is Administration > Identity Management > Settings > User Custom Attributes. The left sidebar shows the navigation menu with 'User Custom Attributes' selected. The main content area displays a table of existing attributes and a table for adding new ones. The 'ACL' attribute is highlighted in red in the second table.

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

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

この設定が完了したら、「Save」ボタンを使用して変更を保存します。

## ステップ 2 : dACLの設定

ISEでdACLを表示および定義するには、Policy > Policy Elements > Results > Authorization > Downloadable ACLsの順に選択します。「追加」ボタンを使用して新しいボタンを作成します。



The screenshot shows the Cisco ISE interface with the 'Policy · Policy Elements' header. The 'Results' tab is active, and the 'Downloadable ACLs' menu item is selected. The main content area displays a table of Downloadable ACLs. The table has two columns: 'Name' and 'Description'. The table contains the following entries:

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	

これにより、「新しいダウンロード可能ACL」設定フォームが開きます。この場合は、次のフィールドを設定します。

- 名前：定義されたdACLの名前。
- 説明（オプション）：作成されたdACLの使用に関する簡単な説明。
- IPバージョン：定義されたdACLで使用されるIPプロトコルのバージョン（バージョン4、6、またはその両方）。
- DACLコンテンツ：Cisco IOS XE ACL構文に従ったdACLのコンテンツ。

このドキュメントで使用するdACLは「ACL\_USER1」であり、このdACLでは、10.48.39.186および10.48.39.13宛てのトラフィック以外のトラフィックを許可します。

フィールドを設定したら、「Submit」ボタンを使用してdACLを作成します。

図に示すように、手順を繰り返して2番目のユーザACL\_USER2のdACLを定義します。

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	

ステップ 3 : 作成したアイデンティティへのdACLの割り当て

dACLを作成したら、ステップ1で作成したユーザカスタム属性を使用して、任意のISEアイデンティティに割り当てることができます。これを行うには、Administration > Identity Management > Identities > Usersの順に移動します。いつものように、「追加」ボタンを使用してユーザーを作成します。

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	

「New Network Access User」設定フォームで、作成したユーザのユーザ名とパスワードを定義します。カスタム属性「ACL」を使用して、手順2で作成したdACLをアイデンティティに割り当

てます。この例では、ACL\_USER1を使用するアイデンティティUSER1が定義されています。

The screenshot shows the configuration page for a Network Access User in Cisco ISE. The 'Username' field is set to 'USER1'. The 'Status' is 'Enabled'. The 'Password Type' is 'Internal Users'. The 'Password Lifetime' is set to 'With Expiration' (53 days). The 'Login Password' field is highlighted in red. The 'ACL' dropdown menu is set to 'ACL\_USER1', which is also highlighted in red. The 'Save' button is highlighted in red.

フィールドが正しく設定されたら、「Submit」ボタンを使用してIDを作成します。

この手順を繰り返してUSER2を作成し、ACL\_USER2を割り当てます。

The screenshot shows the 'Network Access Users' list in Cisco ISE. 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						

ステップ 4 : 許可ポリシーの結果を設定します。

IDが設定され、dACLが割り当てられても、既存の許可の共通タスクに定義されたカスタムユーザ属性「ACL」に一致するように、許可ポリシーを設定する必要があります。これを行うには、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動します。[Add]ボタンを使用して、新しい許可ポリシーを定義します。

- Name：許可ポリシーの名前。ここでは、「9800-DOT1X-USERS」です。
- アクセスタイプ：このポリシーが一致したときに使用するアクセスのタイプ。ここではACCESS\_ACCEPTです。
- 共通タスク：内部ユーザの「DACL名」をInternalUser:<作成されたカスタム属性の名前>に一致させます。このドキュメントで使用されている名前に従い、プロファイル9800-DOT1X-USERSは、InternalUser:ACLとして設定されたdACLを使用して設定されています

The screenshot shows the Cisco ISE configuration interface for a new Authorization Profile. The 'Name' field is highlighted with a red box and contains '9800-DOT1X-USERS'. The 'Access Type' dropdown is also highlighted with a red box and set to 'ACCESS\_ACCEPT'. The 'Description' field contains 'Authorization profile for 802.1x users using dACLs.'. In the 'Common Tasks' section, the 'DACL Name' dropdown is highlighted with a red box and set to 'InternalUser:ACL'. Other options like 'Track Movement', 'Agentless Posture', and 'Passive Identity Tracking' are visible but not selected.

ステップ 5：ポリシーセットで許可プロファイルを使用します。

認可プロファイルの結果を正しく定義した後も、ワイヤレスユーザの認証と認可に使用するポリシーセットにその認可プロファイルを含める必要があります。Policy > Policy Setsの順に移動し、使用するポリシーセットを開きます。

ここで、認証ポリシールール「Dot1X」は、有線または無線802.1xを介して行われたすべての接続と一致します。認可ポリシールール「802.1x Users dACL」は、使用されるSSIDに条件を実装します（つまり、Radius-Called-Station-IDにはDACL\_DOT1X\_SSIDが含まれます）。「DACL\_DOT1X\_SSID」WLANで認可が実行される場合、ステップ4で定義されたプロファイル「9800-DOT1X-USERS」を使用してユーザが認可されます。

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	⚙️

## 結果ごとのdACL

ISEで作成された各IDに特定のdACLを割り当てるという大変なタスクを回避するために、特定のポリシー結果にdACLを適用することができます。この結果は、使用されるポリシーセットの許可ルールに一致する条件に基づいて適用されます。

### ステップ 1 : dACLの設定

「[ユーザごとのdACL](#)」セクションと同じステップ2を実行し、必要なdACLを定義します。ここで、これらはACL\_USER1とACL\_USER2です。

### ステップ 2 : IDの作成

Administration > Identity Management > Identities > Usersの順に移動し、Addボタンを使用してユーザを作成します。

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

### Network Access Users

Selected 0 Total 1

Edit + Add Change Status Import Export Delete Duplicate

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

「New Network Access User」設定フォームで、作成したユーザのユーザ名とパスワードを定義します。

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

#### Network Access Users List > New Network Access User

Network Access User

Username **USER1**

Status  Enabled

Account Name Alias

Email

Passwords

Password Type: Internal Users

Password Lifetime

With Expiration

Never Expires

Password Re-Enter Password

\* Login Password Generate Password

Enable Password Generate Password

> User Information

> Account Options

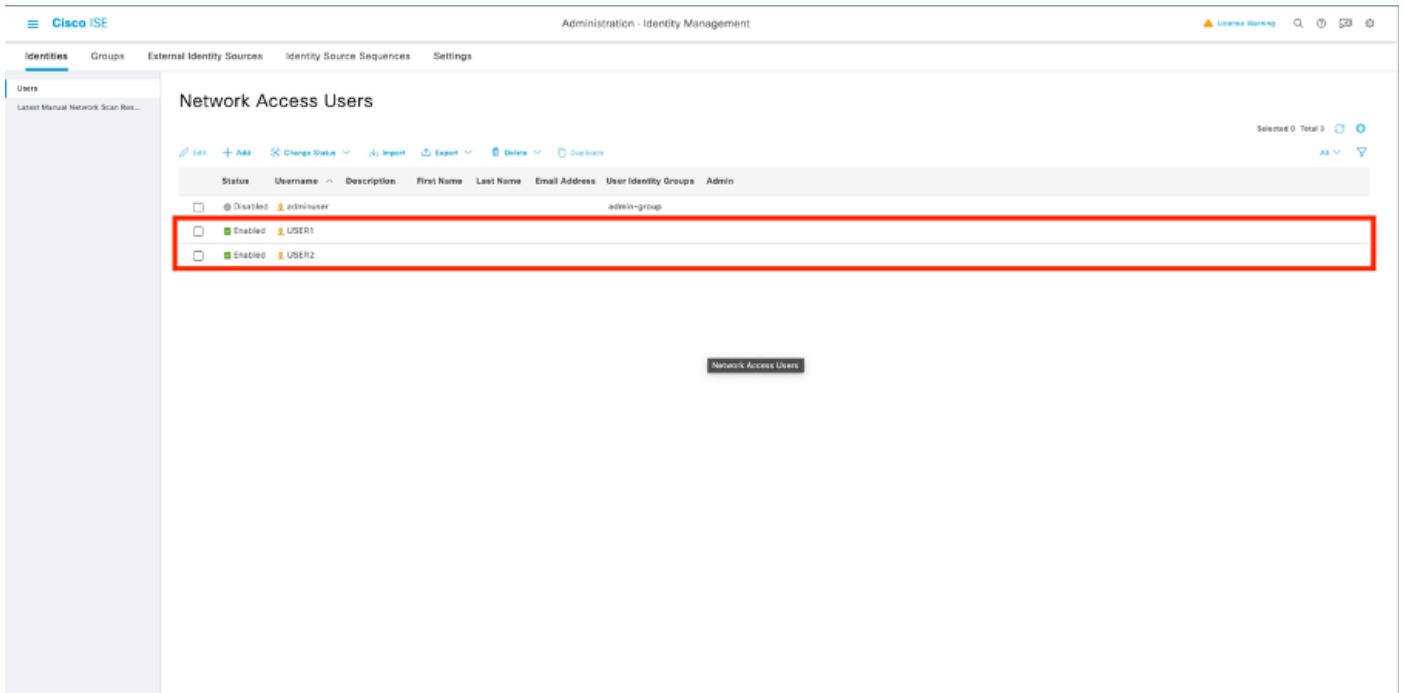
> Account Disable Policy

> User Custom Attributes

> User Groups

Submit Cancel

この手順を繰り返して、USER2を作成します。



ステップ 4：許可ポリシーの結果を設定します。

IDとdACLを設定した後も、特定のdACLを条件に一致するユーザに割り当ててこのポリシーを使用するには、認可ポリシーを設定する必要があります。これを行うには、Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動します。「Add」ボタンを使用して新しい認可ポリシーを定義し、次のフィールドに入力します。

- Name:許可ポリシーの名前。ここでは、「9800-DOT1X-USER1」です。
- アクセスタイプ：このポリシーが一致したときに使用するアクセスのタイプ。ここでは ACCESS\_ACCEPTです。
- 共通タスク：内部ユーザの「dACL名」を「ACL\_USER1」に一致させます。このドキュメントで使用されている名前によると、プロファイル9800-DOT1X-USER1は「ACL\_USER1」として設定されたdACLを使用して設定されています。

The screenshot shows the configuration for a new Authorization Profile in Cisco ISE. The profile name is '9800-DOT1X-USER1' and the access type is 'ACCESS\_ACCEPT'. A dACL named 'ACL\_USER1' is assigned to the profile. The attributes are set to 'Access Type = ACCESS\_ACCEPT' and 'dACL = ACL\_USER1'.

この手順を繰り返して、ポリシー結果「9800-DOT1X-USER2」を作成し、dACLとして「ACL\_USER2」を割り当てます。

The screenshot displays a table of Standard Authorization Profiles. Two profiles, '9800-DOT1X-USER1' and '9800-DOT1X-USER2', are highlighted with a red box. The table includes columns for Name, Profile, and Description.

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.
ISEAdminUserWebAuthTest	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

ステップ 5：ポリシーセットで許可プロファイルを使用する。

認可プロファイルを正しく定義した後も、ワイヤレスユーザの認証と認可に使用するポリシーセットに認可プロファイルを含める必要があります。Policy > Policy Setsの順に移動し、使用するポリシーセットを開きます。

ここで、認証ポリシールール「Dot1X」は、有線または無線802.1X経由で行われたすべての接続と一致します。認可ポリシールール「802.1X User 1 dACL」は、使用されるユーザ名



(InternalUser-Name CONTAINS USER1)に条件を実装します。ユーザ名USER1を使用して認可が実行される場合は、ステップ4で定義したプロファイル「9800-DOT1X-USER1」を使用してユーザが認可されるため、この結果(ACL\_USER1)からのdACLもユーザに適用されます。ユーザ名USER2も同様に設定し、「9800-DOT1X-USER1」を使用します。

The screenshot displays the Cisco ISE Policy Sets configuration interface. It is divided into several sections:

- Policy Sets - Default:** Shows a table with columns for Status, Policy Set Name, Description, and Conditions. A search bar is present.
- Authentication Policy (2):** Contains a table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. A red box highlights the 'Dot1X' rule, which has conditions 'Wired\_802.1X', 'Wired\_802.1X', 'Wired\_MAB', and 'Wired\_WAP'. The 'Use' column for this rule is set to 'All\_User\_ID\_Stores'.
- Authorization Policy (2):** Contains a table with columns for Status, Rule Name, Conditions, Results, Profiles, Security Groups, Hits, and Actions. A red box highlights two rules: '802.1x User 2 dACL' (condition: InternalUser-Name EQUALS USER2) and '802.1x User 1 dACL' (condition: InternalUser-Name EQUALS USER1). Both have profiles set to '9800-DOT1X-USER2' and '9800-DOT1X-USER1' respectively, and security groups set to 'Select from list'.

## CWA SSIDでのdACLの使用についての注意

「[Catalyst 9800 WLCおよびISEでの中央Web認証\(CWA\)の設定](#)」の設定ガイドで説明されているように、CWAはMABと特定の結果に基づいてユーザを認証および許可します。ダウンロード可能ACLは、前述と同じようにISE側からCWA設定に追加できます。



警告：ダウンロード可能ACLはネットワークアクセスリストとしてのみ使用でき、事前認証ACLとしてはサポートされていません。したがって、CWAワークフローで使用される事前認証ACLは、WLC設定で定義する必要があります。

---

## 確認

設定を確認するには、次のコマンドを使用できます。

```
# 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 }
```

次に、この例に対応するWLC設定の関連部分を示します。

```
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]^PVANfcbR0b
!
!
[...]
wireless profile policy DACL-8021X
 aaa-override
 vlan VLAN_1413
 no shutdown
[...]
wireless tag policy default-policy-tag
 description "default policy-tag"
 wlan DACL_DOT1X_SSID policy DACL-8021X
[...]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
 security dot1x authentication-list DOT1X
 no shutdown
```

RADIUSサーバの設定は、show running-config allコマンドを使用して表示します。

```
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
```

## トラブルシューティング

### Checklist

- クライアントが設定済みの802.1X SSIDに正しく接続できることを確認します。
- RADIUS access-request/acceptに適切なattribute-value pairs ( AVP ; 属性値ペア ) が含まれていることを確認します。
- クライアントが適切なWLAN/ポリシープロファイルを使用していることを確認します。

### WLCワンストップシヨップリフレックス

dACLが特定の無線クライアントに正しく割り当てられているかどうかを確認するには、次に示すようにshow wireless client mac-address <H.H.H> detailコマンドを使用します。そこから、さまざまな有用なトラブルシューティング情報、つまり、クライアントのユーザ名、状態、ポリシープロファイル、WLAN、最も重要な点として、ACS-ACLを確認できます。

<#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 Enterprise
```

```
VLAN : VLAN_1413
```

```
[...] Session Manager: Point of Attachment : capwap_90000012 IIF ID : 0x90000012 Authorized : TRUE Session
```

```
SM State : AUTHENTICATED
```

SM Bend State : IDLE Local Policies:

Service Template : wlan\_svc\_DACL-8021X\_local (priority 254) VLAN : VLAN\_1413 Absolute-Timer : 28800

Server Policies:

ACS ACL : xACSACLx-IP-ACL\_USER1-65e89aab

Resultant Policies:

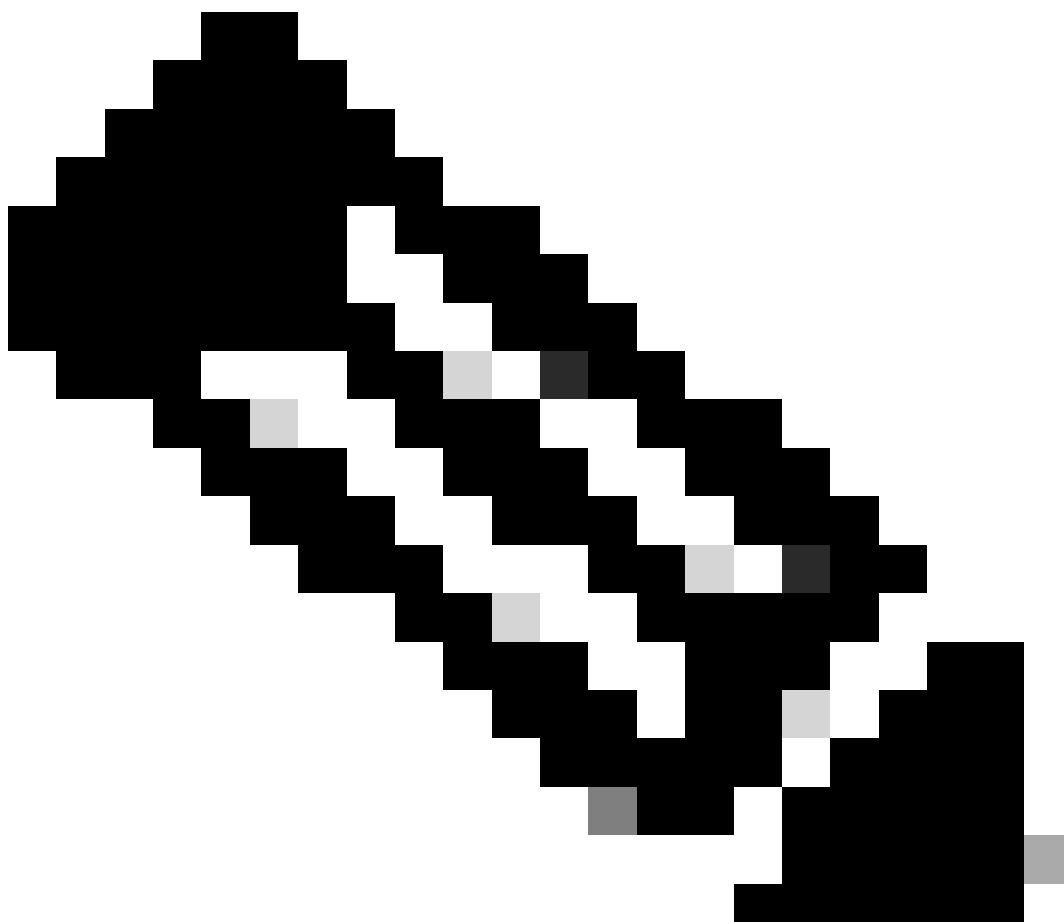
ACS ACL : xACSACLx-IP-ACL\_USER1-65e89aab VLAN Name : VLAN\_1413 VLAN : 1413 Absolute-Timer : 28800

[...]

#### WLCのshowコマンド

現在Catalyst 9800 WLC設定の一部になっているすべてのACLを表示するには、`show access-lists`コマンドを使用します。このコマンドは、ローカルで定義されたすべてのACL、またはWLCによってダウンロードされたdACLをリストします。WLCによってISEからダウンロードされたdACLの形式は、`xACSACLx-IP-<ACL_NAME>-<ACL_HASH>`.

---



---

注：ダウンロード可能ACLは、クライアントが関連付けられ、ワイヤレスインフラストラクチャで使用されている限り、設定に残ります。dACLを使用している最後のクライアントがインフラストラクチャから送信されるとすぐに、dACLが設定から削除されます。

---

```
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
[...]
```

## 条件付きデバッグとラジオアクティブトレース

設定のトラブルシューティング中に、定義されたdACLで割り当てられると想定されるクライアントの[放射性トレース](#)を収集できます。次に、クライアント08be.ac14.137dのクライアント関連付けプロセス中の放射性トレースの興味深い部分を示すログを強調表示します。

<#root>

24/03/28 10:43:04.321315612 {wncd\_x\_R0-0}{1}: [client-orch-sm] [19620]: (note): MAC: 08be.ac14.137d Assc

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 Client

[...]

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

2024/03/28 10:43:04.353413199 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [19620]: (info): [08be.ac14.137d]

2024/03/28 10:43:04.353414496 {wncd\_x\_R0-0}{1}: [auth-mgr-feat\_wireless] [19620]: (info): [08be.ac14.137d]

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

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

[...]

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

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 "n

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 1

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

2024/03/28 10:43:04.381515481 {wncd\_x\_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 33 "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\_900000

2024/03/28 10:43:04.727164223 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_900000

2024/03/28 10:43:04.727169069 {wncd\_x\_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap\_900000

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\$®vf9j0«? %ÿ0?ã@≤™ÇÑbWï6\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\_900000



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 "#AC

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

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

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

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

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

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

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

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

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

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

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\$®vf9fj0«? %ÿ0?ã@≤™ÇÑbwï6\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\_90000

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

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

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

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

2024/03/28 10:43:04.734915743 {wncd\_x\_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap\_9000001

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

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

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

[...]



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

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 Client

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

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

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

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

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

2024/03/28 10:43:04.761186727 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl

2024/03/28 10:43:04.761241972 {iosrp\_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.763131516 {wncd\_x\_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client

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

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

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

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

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

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

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

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

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

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

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

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

2024/03/28 10:43:04.789800998 {wncd\_x\_R0-0}{1}: [rog-proxy-capwap] [19620]: (debug): Managed client RUN

2024/03/28 10:43:04.789886011 {wncd\_x\_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.137d

## パケット キャプチャ

もう1つの興味深いリフレックスは、クライアントアソシエーションのRADIUSフローのパケットキャプチャを取得して分析することです。ダウンロード可能なACLは、ワイヤレスクライアントへの割り当てだけでなく、WLCによるダウンロードもRADIUSに依存します。dACL設定のトラブルシューティングのためにパケットキャプチャを実行する場合は、コントローラがRADIUSサーバとの通信に使用するインターフェイス上でキャプチャする必要があります。[このドキュメントでは](#)、この記事で分析したキャプチャの収集に使用した、Catalyst 9800での簡単に組み込みパケットキャプチャの設定方法を示します。

## RADIUSクライアント認証

DACL\_DOT1X\_SSID SSID(AVP NAS-Identifier)でユーザUSER1 ( AVPユーザ名 ) を認証するためにWLCからRADIUSサーバに送信されるクライアントRADIUSアクセス要求を確認できます。

```

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

> Frame 48035: 617 bytes on wire (4936 bits), 617 bytes captured (4936 bits)
> Ethernet II, Src: Cisco_b2:fe:ff (00:1e:fe: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=333743504d53657373696f6e49443d383232373330304130303030303039463834393335..
AVP: t=Vendor-Specific(26) l=39 vnd=ciscoSystems(9)
AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
AVP: t=Called-Station-Id(30) l=35 val=f4-db-e6-5e-7b-c0:DACL_DOT1X_SSID
AVP: t=Calling-Station-Id(31) l=19 val=08-be-ac-14-13-7d
AVP: t=Vendor-Specific(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

```

認証が成功すると、RADIUSサーバはユーザUSER1(AVP User-Name)に対するaccess-acceptで応答し、AAA属性 (特にベンダー固有のAVP ACS:CiscoSecure-Defined-ACL) を「#ACSACL#-IP-ACL\_USER1-65e89aab」として適用します。

```

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

> Frame 48039: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
> Ethernet II, Src: Vmware_8d:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:fe: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: 643ab1eaba94787735f73678ab53b28a
[This is a response to a request in frame 48034]
[Time from request: 0.059994000 seconds]
Attribute Value Pairs
AVP: t=User-Name(1) l=7 val=USER1
AVP: t=Class(25) l=48 val=434143533a3832323733303041303030303030394638343933354132443a6973652f3439..
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\027060000F0d
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)

```

## DACLのダウンロード

dACLがすでにWLC設定の一部である場合、そのACLはユーザに割り当てられ、RADIUSセッションは終了します。それ以外の場合、WLCはRADIUSを使用してACLをダウンロードします。これを行うために、WLCはRADIUSアクセス要求を作成します。今回は、AVPユーザ名にdACL名(「#ACSACL#-IP-ACL\_USER1-65e89aab」)を使用します。これに加えて、WLCは、このaccess-acceptがCisco AVペアaaa:event=acl-downloadを使用してACLダウンロードを開始することをRADIUSサーバに通知します。

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

```

> Frame 8037: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits)
> Ethernet II, Src: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff), Dst: VMware_8d:01:ec (00:50:56:8d:01:ec)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.130, Dst: 10.48.39.134
> User Datagram Protocol, Src Port: 63772, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x51 (81)
Length: 138
Authenticator: 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

```

コントローラに返送されたRADIUS access-acceptには、次に示すように、要求されたdACLが含まれています。各ACLルールは、タイプ「ip:inacl#<X>=<ACL\_RULE>」（<X>はルール番号）の異なるCisco AVPに含まれています。

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

```

> Frame 8038: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits)
> Ethernet II, Src: VMware_8d:01:ec (00:50:56:8d:01:ec), Dst: Cisco_b2:fe:ff (00:1e:f6:b2:fe:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 39
> Internet Protocol Version 4, Src: 10.48.39.134, Dst: 10.48.39.130
> User Datagram Protocol, Src Port: 1812, Dst Port: 63772
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0x51 (81)
Length: 323
Authenticator: 61342164ce39be06eed828b3ce566ef5
[This is a response to a request in frame 8036]
[Time from request: 0.007995000 seconds]
Attribute Value Pairs
  > AVP: t=User-Name(1) l=32 val=#ACSACL#-IP-ACL_USER1-65e89aab
  > AVP: t=Class(25) l=75 val=43414353a3061333022738366d6242517239445259673447765f436554692f48737050..
  > 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

```





注：ダウンロードACLの内容が、WLCにダウンロードされた後に変更された場合、このACLの変更は、このACLを使用しているユーザが再認証するまで反映されません（さらにWLCは、そのようなユーザに対して再度RADIUS認証を実行します）。実際、ACLの変更は、ACL名のハッシュ部分の変更によって反映されます。したがって、このACLを次にユーザに割り当てる際には、このACLの名前が異なっている必要があります。そのため、このACLはWLC設定には含めず、ダウンロードする必要があります。ただし、ACLの変更前に認証を行うクライアントは、完全に再認証されるまで以前のクライアントを使用し続けます。

---

## ISE操作ログ

### RADIUSクライアント認証

操作ログには、ダウンロード可能ACL「ACL\_USER1」が適用された、ユーザ「USER1」の認証の成功が示されます。トラブルシューティングの対象となる部分は赤で囲まれています。

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

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

```

## DACLのダウンロード

操作ログには、ACL「ACL\_USER1」の正常なダウンロードが示されます。トラブルシューティングの対象となる部分は赤で囲まれています。

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

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。