

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

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[WLCの設定](#)

[9800 WLCでのAAAの設定](#)

[WLANプロファイルの設定](#)

[ポリシープロファイルの設定](#)

[ポリシータグの設定](#)

[ポリシータグの割り当て](#)

[ISE設定](#)

[WLConISEの宣言](#)

[ISEでの新しいユーザの作成](#)

[認証プロファイルの作成](#)

[ポリシーセットの作成](#)

[認証ポリシーの作成](#)

[許可ポリシーの作成](#)

[確認](#)

[トラブルシューティング](#)

[WLCでのトラブルシューティング](#)

[ISEでのトラブルシューティング](#)

はじめに

このドキュメントでは、Cisco Catalyst 9800シリーズワイヤレスコントローラで802.1Xセキュリティを使用してWLANを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 802.1X

使用するコンポーネント

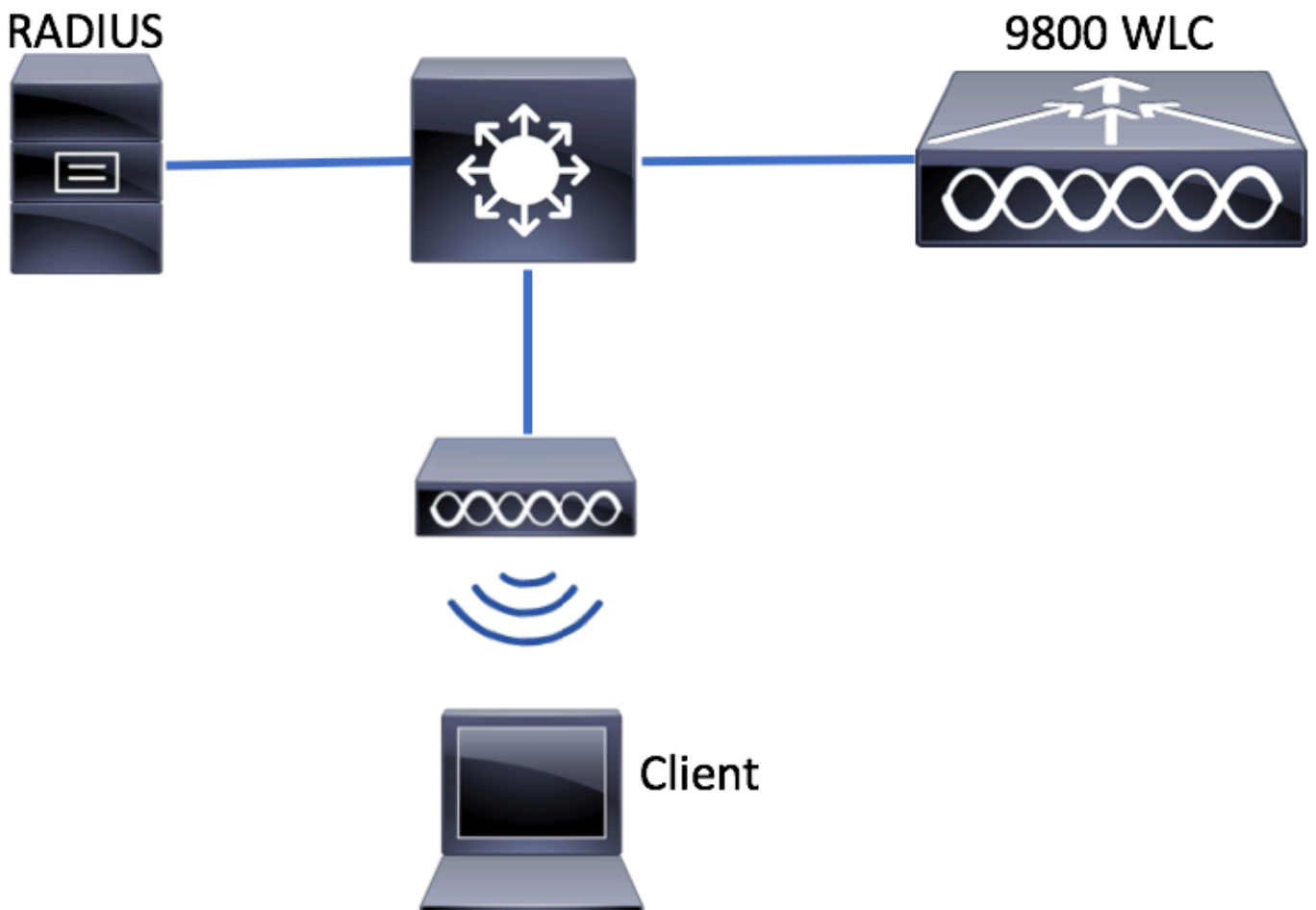
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9800ワイヤレスコントローラシリーズ(Catalyst 9800-CL)
- Cisco IOS® XEジブラルタル17.3.x
- Cisco ISE 3.0

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

ネットワーク図

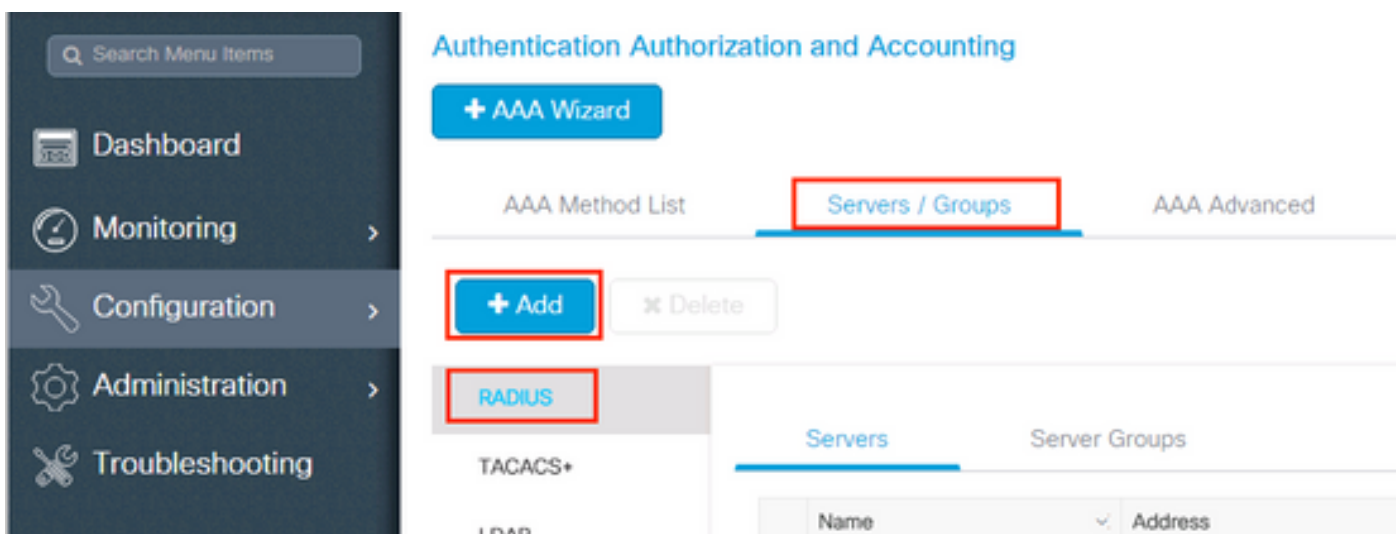


WLC の設定

9800 WLCでのAAAの設定

GUI :

ステップ 1 : RADIUSサーバを宣言します。 Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add に移動し、RADIUSサーバ情報を入力します。



今後、中央Web認証（または認可変更[CoA]を必要とするあらゆる種類のセキュリティ）を使用する予定の場合は、CoAのサポートが有効になっていることを確認します。

Create AAA Radius Server

Name*	<input type="text" value="ISE-kcg"/>	Clear PAC Key	<input type="checkbox"/>
IPV4/IPv6 Server Address*	<input type="text" value="172.16.0.11"/>	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	<input type="password" value="....."/>		
Confirm Shared Secret*	<input type="password" value="....."/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		
Support for CoA	<input checked="" type="checkbox"/> ENABLED		

ステップ 2 : RADIUSサーバをRADIUSグループに追加します。[グループに名前を付ける]に移 Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add. 動し、以前に作成したサーバーを Assigned Servers.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

ステップ 3 : 認証方式リストを作成します。移動先 **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

The screenshot shows the 'Authentication Authorization and Accounting' configuration page. On the left is a dark sidebar menu with options: Dashboard, Monitoring, Configuration (highlighted with a red box), and Administration. The main content area has a blue header and a '+ AAA Wizard' button. Below that, 'AAA Method List' is highlighted with a red box. Underneath, the 'General' tab is selected, and 'Authentication' is highlighted with a red box. On the right side of the 'Authentication' section, a '+ Add' button is highlighted with a red box. A table with a 'Name' column is partially visible at the bottom.

次の情報を入力します。

Quick Setup: AAA Authentication
✕

Method List Name*

Type* dot1x ▼

Group Type group ▼

Fallback to local

Available Server Groups

radius
 ldap
 tacacs+
 ISE-kcg-grp

Assigned Server Groups

ISE-grp-name

CLI :

```
# config t # aaa new-model # radius server <radius-server-name> # address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813 # timeout 300 # retransmit 5
# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

AAAデッドサーバ検出についての注意


RADIUSサーバを設定したら、それが「ALIVE」と見なされるかどうかを確認できます。

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current
```

特に複数のRADIUSサーバを使用する場合、WLCで **dead criteria**, および **deadtime** を設定できます。

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

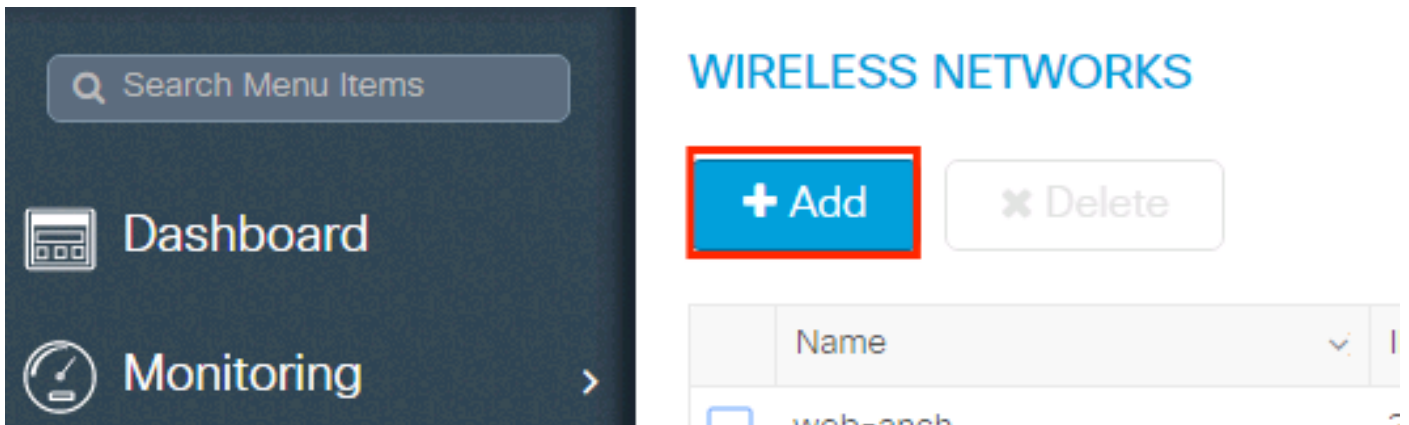
注: **dead criteria** は、RADIUSサーバをデッドとしてマークするために使用される基準です。構成は次のとおりです。 1.コントローラが最後にRADIUSサーバから有効なパケットを受信してから、サーバが停止したとマークされるまでの経過時間を示すタイムアウト (秒単位)。 2.カウンタ。RADIUSサーバが停止とマークされるまでにコントローラで発生する必要がある連続タイムアウトの数を表します。

 **注：** **deadtime**は、dead基準によってサーバがdeadとしてマークされた後、サーバがdeadステータスのままになる時間（分単位）を指定します。デッドタイムが経過すると、コントローラはサーバをUP(ALIVE)としてマークし、登録されたクライアントに状態変更を通知します。状態がUPとマークされた後もサーバに到達できず、デッド基準を満たしている場合、サーバはデッドタイムインターバルの間に再びデッドとマークされます。

WLANプロファイルの設定

GUI：

ステップ 1：WLANを作成します。**Configuration > Wireless > WLANs > + Add**の順に移動し、必要に応じてネットワークを設定します。



ステップ 2：WLAN情報を入力します

Add WLAN

General Security Advanced

Profile Name*	<input type="text" value="prof-name"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

ステップ 3：Securityタブに移動し、必要なセキュリティ方式を選択します。この例では、WPA2 + 802.1xです。

Add WLAN [Close]

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode WPA + WPA2 ▼

MAC Filtering

Protected Management Frame

Fast Transition Adaptive Enab... ▼

Over the DS

Reassociation Timeout 20

PMF Disabled ▼

WPA Parameters

WPA Policy

Cancel Save & Apply to Device

Add WLAN [Close]

PMF Disabled ▼

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x ▼

Cancel Save & Apply to Device

ステップ 4 : Security > AAA タブで、手順3で作成した認証方式を「9800 WLCでのAAA設定」セクションから選択します。

The screenshot shows the 'Add WLAN' configuration window with the following settings:

- General tab selected
- Security sub-tab selected
- Layer3 sub-tab selected
- AAA sub-tab selected
- Authentication List: list-name
- Local EAP Authentication:
- Buttons: Cancel, Save & Apply to Device

CLI :

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # security dot1x authentication-list <dot1x-list-name> # no shutdown
```

ポリシープロファイルの設定

ポリシープロファイル内では、他の設定 (アクセスコントロールリスト[ACL]、Quality of Service [QoS]、モビリティアンカー、タイマーなど) の中から、クライアントに割り当てるVLANを決定できます。

デフォルトのポリシープロファイルを使用することも、新しいプロファイルを作成することもできます。

GUI :

Configuration > Tags & Profiles > Policy Profile の順に移動し、**default-policy-profile** を設定するか、新しいプロファイルを作成します。

プロファイルを有効にします。

また、アクセスポイント(AP)がローカルモードの場合、ポリシープロファイルで中央スイッチングと中央認証が有効になっていることを確認します。

Access Policiesタブで、クライアントを割り当てる必要があるVLANを選択します。

Edit Policy Profile

General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

Search or Select



VLAN

VLAN/VLAN Group

VLAN2602



Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select



IPv6 ACL

Search or Select



URL Filters

Pre Auth

Search or Select



Post Auth

Search or Select



VLAN割り当てなどの属性をアクセス承認で返すようにISEを設定する場合は、**Advanced** タブでAAA Overrideを有効にしてください。

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

WLAN Timeout

Session Timeout (sec)	1800
Idle Timeout (sec)	300
Idle Threshold (bytes)	0
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> 60

DHCP

IPv4 DHCP Required	<input checked="" type="checkbox"/>
DHCP Server IP Address	

Show more >>>

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	default-aaa-policy ✕ ▼

Fabric Profile	<input type="checkbox"/> Search or Select ▼
Umbrella Parameter Map	Not Configured ▼
mDNS Service Policy	default-mdns-service ▼ Clear

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	Search or Select ▼

Air Time Fairness Policies

2.4 GHz Policy	Search or Select ▼
5 GHz Policy	Search or Select ▼

↶ Cancel

↵ Update & Apply to Device

CLI :

```
# config # wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> # no shutdown
```

ポリシータグの設定

Policy Tagは、SSIDとポリシープロファイルをリンクするために使用されます。新しいポリシータグを作成するか、default-policyタグを使用します。

注:default-policy-tagは、1 ~ 16のWLAN IDを持つSSIDをdefault-policy-profileに自動的にマッピングします。変更も削除もできません。 ID 17以上のWLANがある場合、default-policy-tagは使用できません。

GUI :

必要に応じて、**Configuration > Tags & Profiles > Tags > Policy** に移動し、新しいプロファイルを追加します。

Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

Manage Tags

Policy Site RF AP

+ Add x Delete

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

WLAN プロファイルを目的のポリシープロファイルにリンクします。

Add Policy Tag

Name* PolicyTagName

Description Enter Description

+ Add x Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶	10 items per page
No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

✕ ✓

↶ Cancel 📄 Save & Apply to Device

Add Policy Tag ✕

Name*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
◀ ◁ 1 ▷ ▶	10 items per page
1 - 1 of 1 items	

↶ Cancel 📄 Save & Apply to Device

CLI :

```
# config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>
```

ポリシータグの割り当て


必要な AP にポリシータグを割り当てます。

GUI :

タグを1つのAPに割り当てるには、関連するポリシータグを割り **Configuration > Wireless > Access Points > AP Name > General Tags**, 当てるように移動し、 **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration window with the 'General' tab selected. The 'Policy' dropdown menu is highlighted with a red box, showing 'default-policy-tag' as the selected option. The 'Update & Apply to Device' button at the bottom right is also highlighted with a red box.

Field	Value
AP Name*	AP3802-02-WS
Location*	default location
Base Radio MAC	00:42:68:c6:41:20
Ethernet MAC	00:42:68:a0:d0:22
Admin Status	Enabled
AP Mode	Local
Operation Status	Registered
Fabric Status	Disabled
Version	
Primary Software Version	10.0.200.50
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.0.0
IOS Version	10.0.200.52
Mini IOS Version	0.0.0.0
IP Config	
IP Address	172.16.0.207
Static IP	<input type="checkbox"/>
Time Statistics	
Up Time	9 days 1 hrs 17 mins 24 secs
Controller Associated Time	0 days 3 hrs 26 mins 41 secs
Controller Association Latency	8 days 21 hrs 50 mins 33 secs

 注：APのポリシータグが変更されると、9800 WLCへの関連付けがドロップされ、数分後に元に戻ることに注意してください。

複数のAPに同じポリシータグを割り当てるには、 **Configuration > Wireless Setup > Advanced > Start Now > Apply.**

Start

Tags & Profiles



WLAN Profile



Policy Profile



Policy Tag



AP Join Profile



Start Now →



Flex Profile



Site Tag



RF Profile



RF Tag



Apply



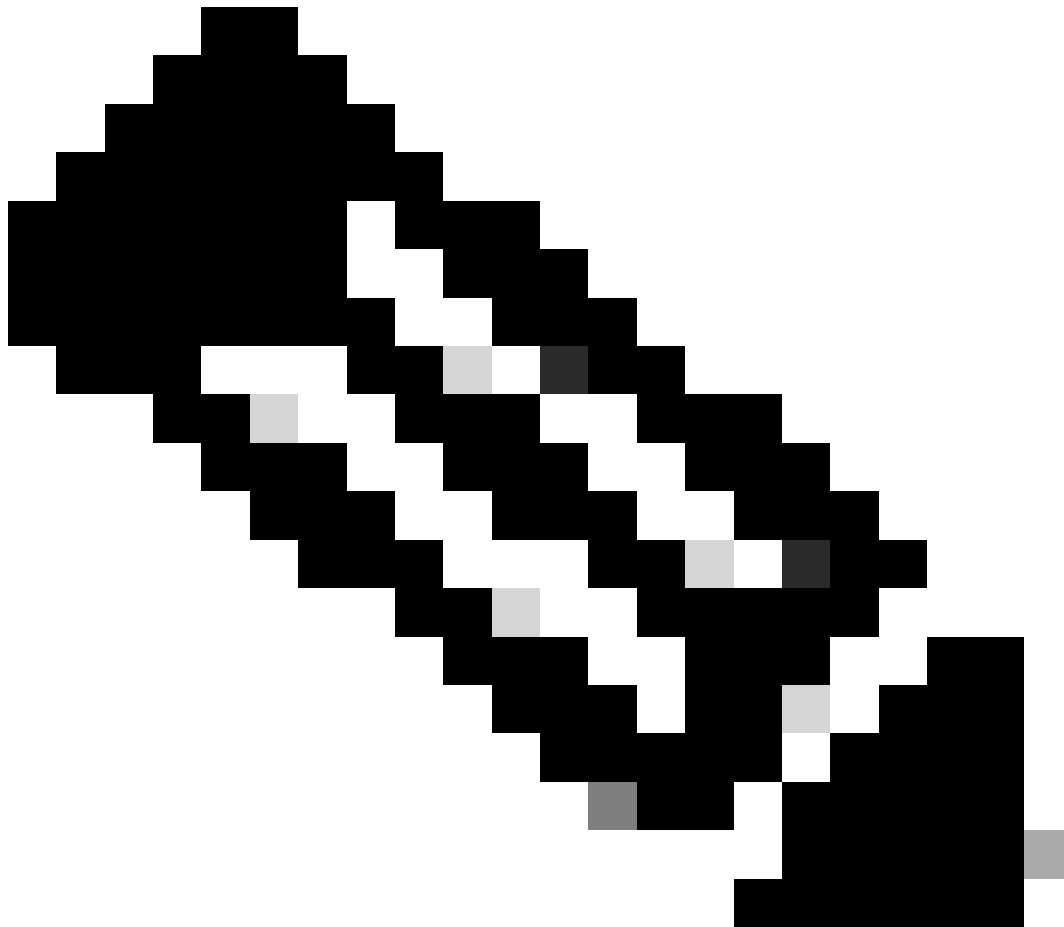
Tag APs



Done


```
# show ap tag summary // Tag information for AP'S
# show wlan { summary | id | name | all } // WLAN details
# show wireless tag policy detailed <policy-tag name> // Detailed information on given policy tag
# show wireless profile policy detailed <policy-profile name> // Detailed information on given policy profile
```

トラブルシューティング



注：外部ロードバランサの使用には問題はありません。ただし、calling-station-id RADIUS属性を使用して、ロードバランサがクライアントごとに動作することを確認してください。UDP送信元ポートに依存するメカニズムは、9800からのRADIUS要求のバランシングではサポートされていません。

WLCでのトラブルシューティング

WLC 9800には常時トレース機能があります。これにより、クライアント接続に関連するすべてのエラー、警告、および通知レベルのメッセージが継続的にログに記録され、発生後にインシデントまたは障害状態のログを表示できます。

生成されるログの量によって異なりますが、通常は数時間から数日に戻ることができます。

9800 WLCがデフォルトで収集したトレースを表示するには、SSH/Telnetで9800 WLCに接続し、次の手順を実行します (セッションをテキストファイルに記録していることを確認します)。

ステップ 1 : WLCの現在の時刻を確認して、問題が発生した時刻までログを追跡できるようにします。


```
# show clock
```

ステップ 2 : システム設定に従って、WLCバッファまたは外部syslogからsyslogを収集します。これにより、システムの正常性とエラー (発生している場合) をすぐに確認できます。

```
# show logging
```

ステップ 3 : デバッグ条件が有効になっているかどうかを確認します。

```
# show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Add
```

 注 : 条件が一覧表示されている場合は、有効な条件 (MACアドレス、IPアドレスなど) に遭遇するすべてのプロセスについて、トレースがデバッグレベルで記録されていることを意味します。これにより、ログの量が増加します。そのため、アクティブにデバッグを行っていない場合は、すべての条件をクリアすることを推奨します。

ステップ 4 : テスト対象のMACアドレスがステップ3の条件としてリストされていないとすると、特定のMACアドレスのalways-on notice levelトレースを収集します。

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>
```

セッションの内容を表示するか、ファイルを外部TFTPサーバにコピーできます。

```
# more bootflash:always-on-<FILENAME.txt>  
or
```

```
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

条件付きデバッグとラジオアクティブトレース

常時接続トレースで、調査中の問題のトリガーを判別するのに十分な情報が得られない場合は、条件付きデバッグを有効にして、無線アクティブ(RA)トレースをキャプチャできます。これにより、指定された条件（この場合はクライアントMACアドレス）と対話するすべてのプロセスにデバッグレベルのトレースが提供されます。これは、GUIまたはCLIを使用して実行できます。

CLI：

条件付きデバッグを有効にするには、次の手順を実行します。


ステップ 5：有効なデバッグ条件がないことを確認します。


```
# clear platform condition all
```

手順 6：監視するワイヤレスクライアントのMACアドレスのデバッグ条件を有効にします。

このコマンドは、指定されたMACアドレスを30分間（1800秒）モニタし始めます。オプションでこの時間を最大2085978494秒まで増やすことができます。

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

 注:複数のクライアントを同時にモニタするには、MACアドレスごとにdebug wireless mac <aaaa.bbbb.cccc>コマンドを実行します。

 注:ターミナルセッションでは、すべてが後で表示できるように内部でバッファされるため、クライアントアクティビティの出力は表示されません。

手順 7：監視する問題または動作を再現します。

ステップ 8：デフォルトまたは設定されたモニタ時間が経過する前に問題が再現した場合は、デバッグを停止します。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

モニター時間が経過するか、debug wireless が停止すると、9800 WLC では次の名前のローカルファイルが生成されます。

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

ステップ 9： MAC アドレスアクティビティのファイルを収集します。 ra trace.log を外部サーバーにコピーするか、出力を画面に直接表示できます。

RA トレースファイルの名前を確認します。

```
# dir bootflash: | inc ra_trace
```

ファイルを外部サーバーにコピーします。


```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt
```

内容を表示します。

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

ステップ 10： 根本原因がまだ明らかでない場合は、デバッグレベルのログのより詳細なビューである内部ログを収集します。すでに収集されて内部で保存されているデバッグログの詳細を確認するため、クライアントを再度デバッグする必要はありません。

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

 注：このコマンド出力は、すべてのプロセスのすべてのログレベルのトレースを返し、非常に大量です。これらのトレースを解析する場合は、Cisco TAC にお問い合わせください。

ra-internal-FILENAME.txt を外部サーバーにコピーするか、出力を画面に直接表示できます。

ファイルを外部サーバーにコピーします。

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

内容を表示します。

```
# more bootflash:ra-internal-<FILENAME>.txt
```

ステップ 11 デバッグ条件を削除します。

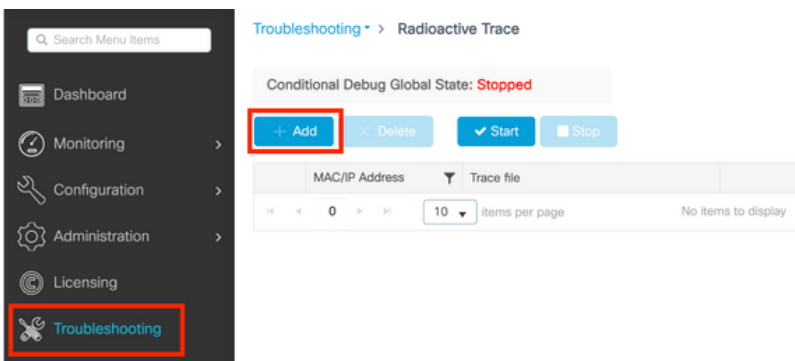
```
# clear platform condition all
```



注：トラブルシューティングセッションの後は、必ずデバッグ条件を削除してください。

GUI：

ステップ 1： **Troubleshooting > Radioactive Trace > + Add** に移動して、トラブルシューティングを行うクライアントのMAC/IPアドレスを指定します。

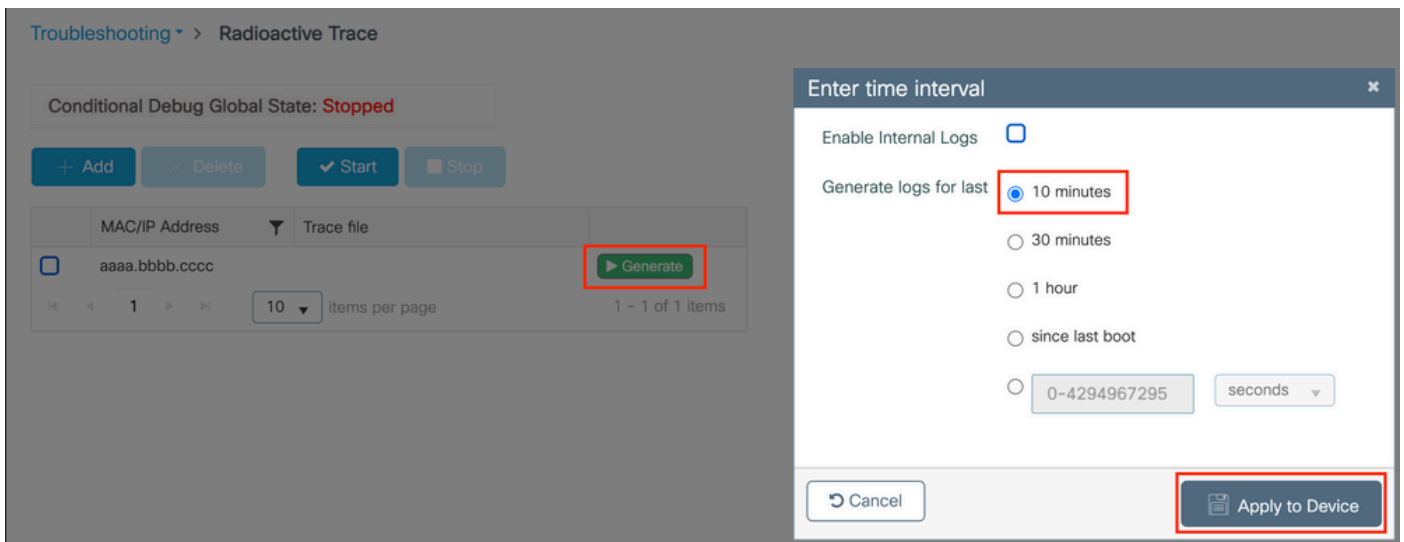


ステップ 2： [Start (スタート)] をクリックします。

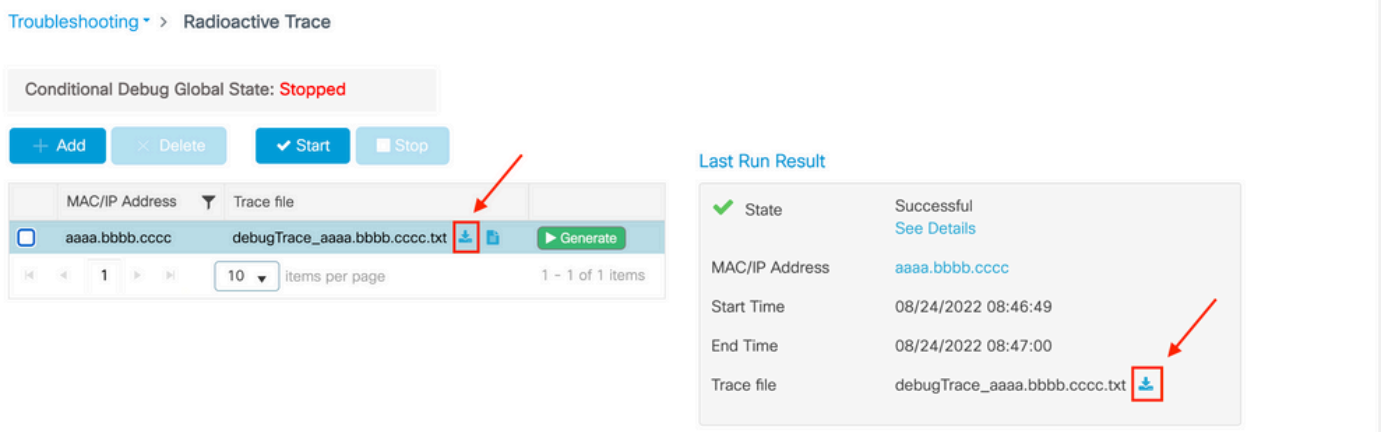
ステップ 3： 問題を再現します。

ステップ 4： [Stop] をクリックします。

ステップ 5： **Generate** ボタンをクリックし、ログを取得する時間間隔を選択して、**Apply to Device**. In this example, the logs for the last 10 minutes are requested.

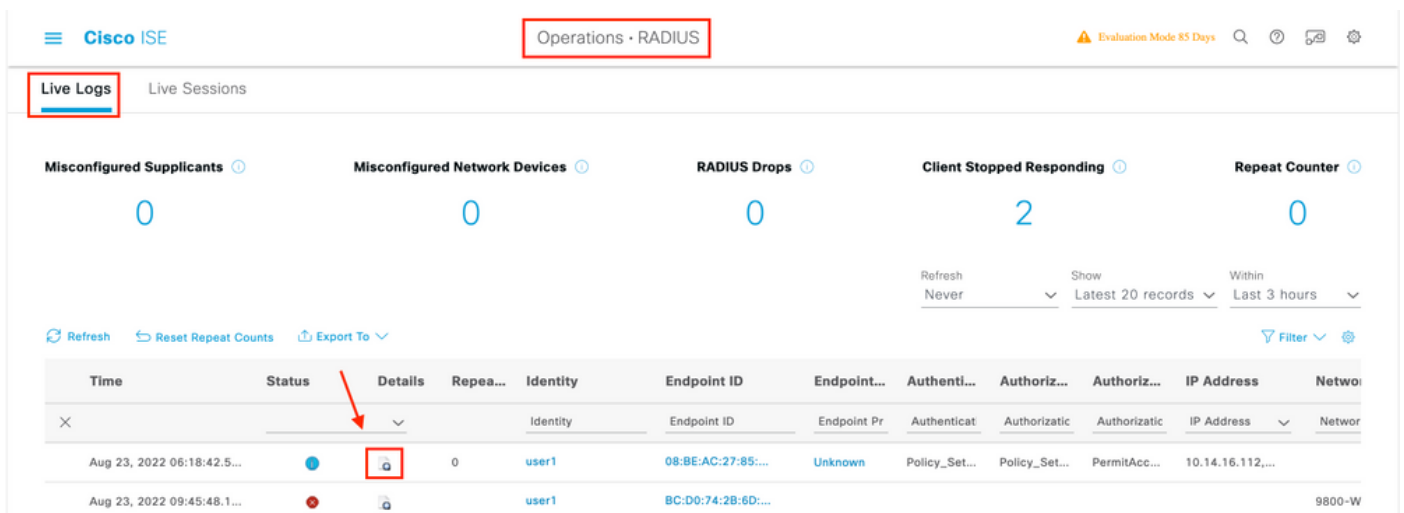


手順 6 : コンピュータに放射性トレースをダウンロードし、ダウンロードボタンをクリックして検査します。



ISEでのトラブルシューティング

クライアント認証の問題が発生した場合は、ISEサーバでログを確認できます。Operations > RADIUS > Live Logs に移動すると、認証要求のリスト、一致したポリシーセット、各要求の結果などが表示されます。図に示すように、各行の Details タブの下にある虫眼鏡をクリックすると、詳細が表示されます。



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。