

# ISEを使用したCatalyst 9800 WLC iPSKの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[iPSKとは何か、どのシナリオに適合するかを理解する](#)

[9800 WLCの設定](#)

[ISE の設定](#)

[トラブルシューティング](#)

[9800 WLCのトラブルシューティング](#)

[ISEのトラブルシューティング](#)

## 概要

このドキュメントでは、Cisco ISEをRADIUSサーバとして使用するCisco 9800ワイヤレスLANコントローラ(WLC)でのiPSKで保護されたWLANの設定について説明します。

## 前提条件

### 要件

このドキュメントでは、読者が9800上のWLANの基本設定に精通し、その設定を導入に適応できることを前提としています。

### 使用するコンポーネント

- 17.6.3が稼働するCisco 9800-CL WLC
- 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、初期（デフォルト）設定の状態から起動しています。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。

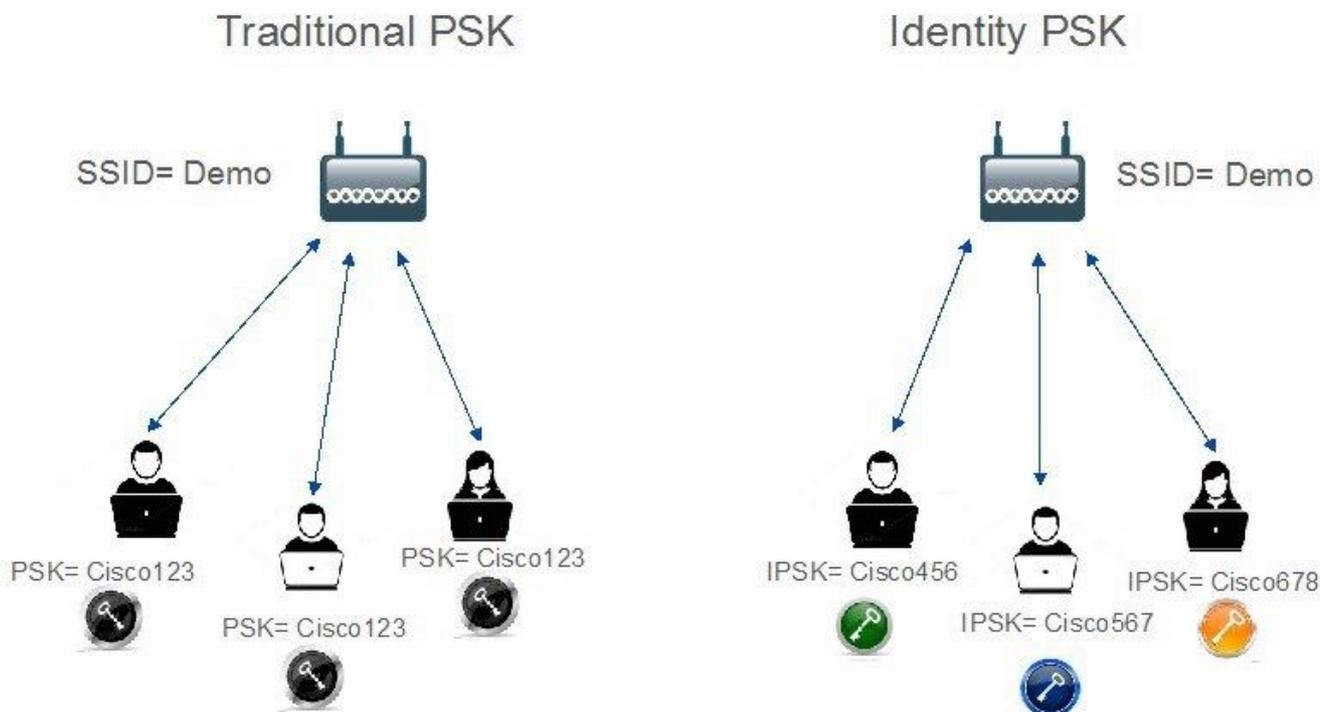
## iPSKとは何か、どのシナリオに適合するかを理解する

従来の事前共有キー(PSK)で保護されたネットワークでは、接続されたすべてのクライアントに同じパスワードが使用されます。その結果、不正ユーザとキーを共有することで、セキュリティ違反やネットワークへの不正アクセスが発生する可能性があります。この侵害の最も一般的な緩和策は、PSK自体の変更です。この変更は、ネットワークに再びアクセスするために多くのエンドデバイスを新しいキーで更新する必要があるため、すべてのユーザに影響を与えます。

Identity PSK(iPSK)では、RADIUSサーバを使用して、同じSSID上の個人またはユーザグループに

対して一意の事前共有キーが作成されます。この種の設定は、エンドクライアントデバイスが dot1x認証をサポートしないが、よりセキュアで詳細な認証方式が必要なネットワークで非常に便利です。クライアントの観点からは、このWLANは従来のPSKネットワークと同じように見えます。いずれかのPSKが侵害された場合、影響を受ける個人またはグループだけがPSKを更新する必要があります。WLANに接続されている残りのデバイスは影響を受けません。

## Traditional Vs Identity PSK



## 9800 WLCの設定

[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Servers] で、ISEをRADIUSサーバとして追加します。

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Address	Auth Port	Acct Port
<input type="checkbox"/> ISE_IPSK	10.48.39.126	1812	1813

1 - 1 of 1 items

[Configuration] > [Security] > [AAA] > [Servers/Groups] > [Server Groups] で、RADIUSサーバグループを作成し、以前に作成したISEサーバを追加します。

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

+ Add

× Delete

RADIUS

TACACS+

LDAP

Servers

Server Groups

Name	Server 1	Server 2	Server 3
<input type="checkbox"/> ISE_IPSK_Group	ISE_IPSK	N/A	N/A

1 - 1 of 1 items

[AAA Method List] タブで、以前に作成したRADIUSサーバグループを指すタイプ「network」とグループタイプ「group」を持つAuthorizationリストを作成します。

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type	Group Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Authz_List_IPSK	network	group	ISE_IPSK_Group	N/A	N/A	N/A

1 - 1 of 1 items

アカウントिंगの設定はオプションですが、タイプを「identity」に設定し、同じRADIUSサーバグループを指定することで実行できます。

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

Name	Type	Group1	Group2	Group3	Group4
<input type="checkbox"/> Acc_List_IPSK	identity	ISE_IPSK_Group	N/A	N/A	N/A

1 - 1 of 1 items

これは、次のコマンドを使用してコマンドラインから実行することもできます。

radius server

[Configuration] > [Tags & Profiles] > [WLANs] で、新しいWLANを作成します。[Layer 2 configuration]で、次の操作を実行します。

- MACフィルタリングを有効にし、以前に作成した許可リストを設定します
- [Auth Key Mgmt] で[PSK] を有効にします。
- 事前共有キーフィールドには、任意の値を入力できます。これは、Webインターフェイス設計の要件を満たすためだけに行われます。ユーザはこのキーを使用して認証できません。こ

の場合、事前共有キーは「12345678」に設定されています。

### Add WLAN

General **Security** Advanced

Layer2 **Layer3** AAA

Layer 2 Security Mode WPA + WPA2

MAC Filtering

Authorization List\* Authz\_List...

Protected Management Frame

PMF Disabled

WPA Parameters

WPA Policy

WPA2 Policy

GTK Randomize

OSEN Policy

WPA2 Encryption  AES(CCMP128)  
 CCMP256  
 GCMP128  
 GCMP256

Auth Key Mgmt  802.1x  
 PSK  
 Easy-PSK  
 CCKM  
 FT + 802.1x  
 FT + PSK  
 802.1x-SHA256  
 PSK-SHA256

PSK Format ASCII

PSK Type Unencrypted

Pre-Shared Key\* .....

Lobby Admin Access

Fast Transition Adaptive Enabled

Over the DS

Reassociation Timeout 20

MPSK Configuration

MPSK

ユーザの分離は、[Advanced] タブで実行できます。[Allow Private Group]に設定すると、同じPSKを使用しているユーザが相互に通信できるようになりますが、異なるPSKを使用しているユーザはブロックされます。

General	Security	<b>Advanced</b>	Add To Policy Tags
Coverage Hole Detection	<input checked="" type="checkbox"/>		Universal Admin <input type="checkbox"/>
Aironet IE ⓘ	<input type="checkbox"/>		OKC <input checked="" type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>		Load Balance <input type="checkbox"/>
<b>P2P Blocking Action</b>	<input type="checkbox"/>	<b>Allow Private Group</b> ▼	Band Select <input type="checkbox"/>
Multicast Buffer	<input type="checkbox"/>	<input type="checkbox"/>	IP Source Guard <input type="checkbox"/>

[Configuration] > [Tags & Profiles] > [Policy] で、新しいポリシープロファイルを作成します。  
 [Access Policies] タブで、このWLANが使用しているVLANまたはVLANグループを設定します。

**Add Policy Profile** ×

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General	<b>Access Policies</b>	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
<b>WLAN Local Profiling</b>				
Global State of Device Classification ⓘ	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="checkbox"/>			
<b>VLAN</b>				
VLAN/VLAN Group	<input type="checkbox"/>			
Multicast VLAN	<input type="checkbox"/>			

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**URL Filters**

Pre Auth

Post Auth

[Advanced] タブで、[AAA Override]を有効にし、作成済みの場合はアカウントिंगリストを追加します。

## Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General   Access Policies   QOS and AVC   Mobility   **Advanced**

**WLAN Timeout**

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

**AAA Policy**

Allow AAA Override

NAC State

Policy Name

Accounting List  ⓘ ✕

**Fabric Profile**

Link-Local Bridging

mDNS Service Policy

Hotspot Server

**User Defined (Private) Network**

Status

Drop Unicast

**DNS Layer Security**

DNS Layer Security Parameter Map  [Clear](#)

Flex DHCP Option for DNS  **ENABLED**

Flex DNS Traffic Redirect

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

[Configuration] > [Tags & Profiles] > [Tags] > [Policy] で、作成したポリシープロファイルにWLANがマッピングされていることを確認します。

Configuration > Tags & Profiles > Tags

**Policy**   Site   RF   AP

+ Add   ✕ Delete

Policy Tag Name

default-policy-tag

1   10 Items per page

**Edit Policy Tag**

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name\*

Description

▼ **WLAN-POLICY Maps: 1**

+ Add   ✕ Delete

WLAN Profile	Policy Profile
<input checked="" type="checkbox"/> WLAN_iPSK	Policy_Profile_iPSK

1   10 Items per page   1 - 1 of 1 items

これは、次のコマンドを使用してコマンドラインから実行することもできます。

wlan

[Configuration] > [Wireless] > [Access Points] で、WLANをブロードキャストする必要があるアクセスポイントに次のタグが適用されていることを確認します。

### Edit AP

- General
- Interfaces
- High Availability
- Inventory
- ICap
- Advanced
- Support Bundle

General		Tags	
AP Name*	AP70DF.2F8E.184A	Policy	default-policy-tag ▼
Location*	default location	Site	default-site-tag ▼
Base Radio MAC	500f.8004.eea0	RF	default-rf-tag ▼
Ethernet MAC	70df.2f8e.184a	Write Tag Config to AP	<input type="checkbox"/> ⓘ

## ISE の設定

この設定ガイドでは、クライアントのMACアドレスに基づいてデバイスのPSKが決定されるシナリオについて説明します。[Administration] > [Network Resources] > [Network Devices] で、新しいデバイスを追加し、IPアドレスを指定し、RADIUS認証設定を有効にし、RADIUS共有秘密を指定します。

Cisco ISE Administration - Network Resources

Network Devices

Network Devices List > New Network Device

Network Devices

\* Name 9800-WLC

Description

IP Address \* IP: 10.48.38.86 / 32

\* Device Profile Cisco

Model Name

Software Version

\* Network Device Group

Location All Locations [Set To Default](#)

IPSEC Is IPSEC Device [Set To Default](#)

Device Type All Device Types [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

\* Shared Secret [Show](#)

[Context Visibility] > [Endpoints] > [Authentication] で、iPSKネットワークに接続しているすべてのデバイス (クライアント) のMACアドレスを追加します。

Cisco ISE Context Visibility - Endpoints

Authentication

INACTIVE ENDPOINTS

AUTHENTICATION STATUS

AUTHENTIFICATIONS

NETWORK DE

Rows/Page 1 / 1 Total Rows

MAC Address	Status	IP Address	Username	Hostname	Location	Endpoint Profile	Authentication Failure Re...	Authentication ...	Authorization P..
08.BE.AC:27:85:7E	*		08beac278...		Location...	Unknown	-	MAB	Basic_Authenticate.

[Administration] > [Identity Management] > [Groups] > [Endpoint Identity Groups] で、1つ以上のグループを作成し、それらにユーザを割り当てます。各グループは、後でネットワークに接続するために異なるPSKを使用するように設定できます。

Cisco ISE Administration - Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

Selected 0 Total 18

Edit + Add Delete

Name	Description
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iDevice	Identity Group for Profile: Apple-iDevice

Cisco ISE Administration - Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Endpoint Identity Group List > New Endpoint Group

Endpoint Identity Group

\* Name Identity\_Group\_IPSK

Description

Parent Group

Submit Cancel

グループが作成されたら、ユーザをグループに割り当てることができます。作成したグループを選択し、[Edit]をクリックします。

Cisco ISE Administration - Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

Selected 1 Total 19

Edit + Add Delete

Name	Description
<input type="checkbox"/> Epson-Device	Identity Group for Profile: Epson-Device
<input type="checkbox"/> GuestEndpoints	Guest Endpoints Identity Group
<input checked="" type="checkbox"/> Identity_Group_IPSK	
<input type="checkbox"/> Iusiner-Device	Identity Group for Profile: Iusiner-Device

グループ設定で、[Add]ボタンをクリックして、このグループに割り当てるクライアントのMACアドレスを追加します。

The screenshot shows the Cisco ISE Administration interface for Identity Management. The breadcrumb trail is: Endpoint Identity Group List > Identity\_Group\_IPSK. The main form is titled 'Endpoint Identity Group' and contains the following fields:

- \* Name: Identity\_Group\_IPSK
- Description: (empty text area)
- Parent Group: (empty dropdown)

Below the form are 'Save' and 'Reset' buttons. Underneath, there is a section for 'Identity Group Endpoints' with a '+ Add' button and a 'Remove' button. A table below shows one endpoint:

MAC Address	Static Group Assignment	Endpoint Profile
<input type="checkbox"/> 08:BE:AC:27:85:7E	true	Unknown

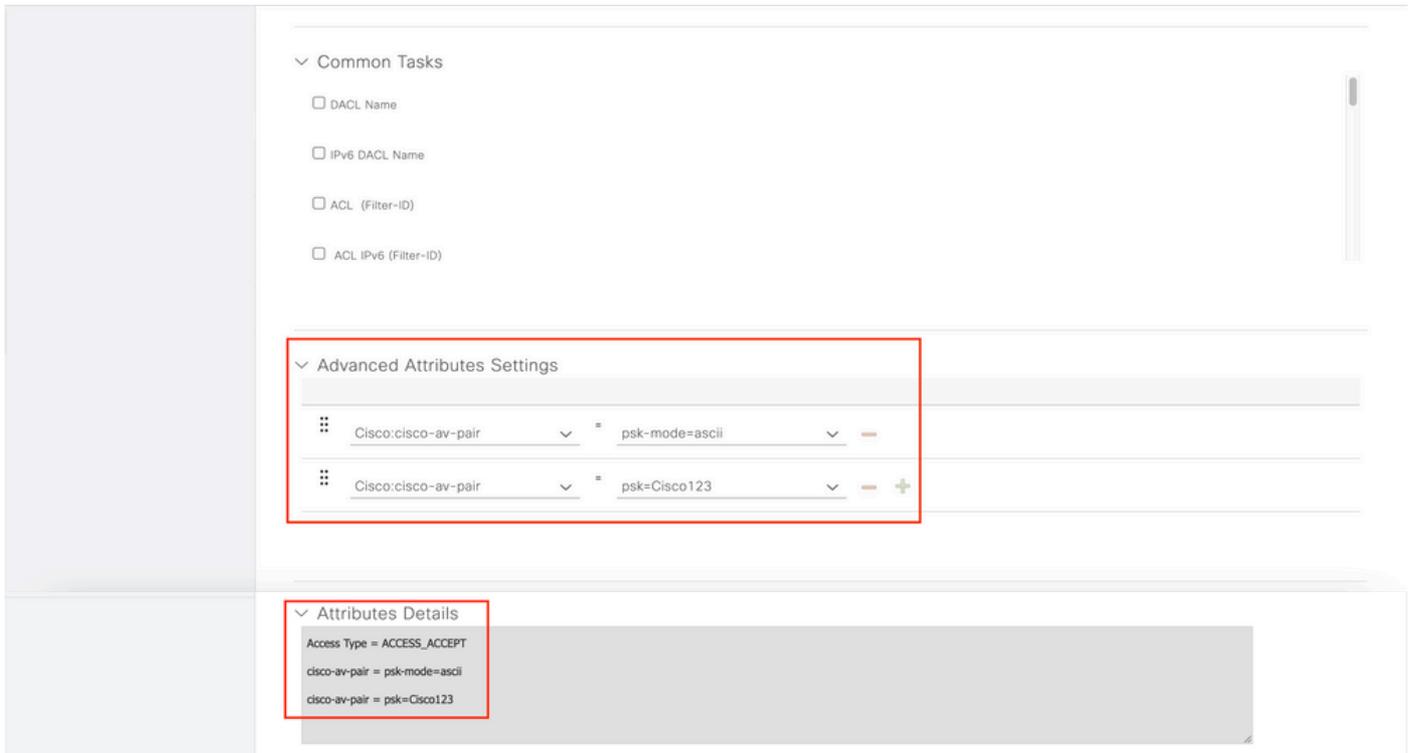
[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] で、新しい認可プロファイルを作成します。属性を次のように設定します。

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

異なるPSKを使用する必要があるユーザグループごとに、異なるpsk avペアを使用して追加の結果を作成します。ACLやVLANオーバーライドなどの追加パラメータもここで設定できます。

The screenshot shows the Cisco ISE Administration interface for Policy Elements. The breadcrumb trail is: Policy > Policy Elements. The main form is titled 'Authorization Profile' and contains the following fields:

- \* Name: Authz\_Profile\_IPSK
- Description: (empty text area)
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:  ⓘ
- Agentless Posture:  ⓘ
- Passive Identity Tracking:  ⓘ



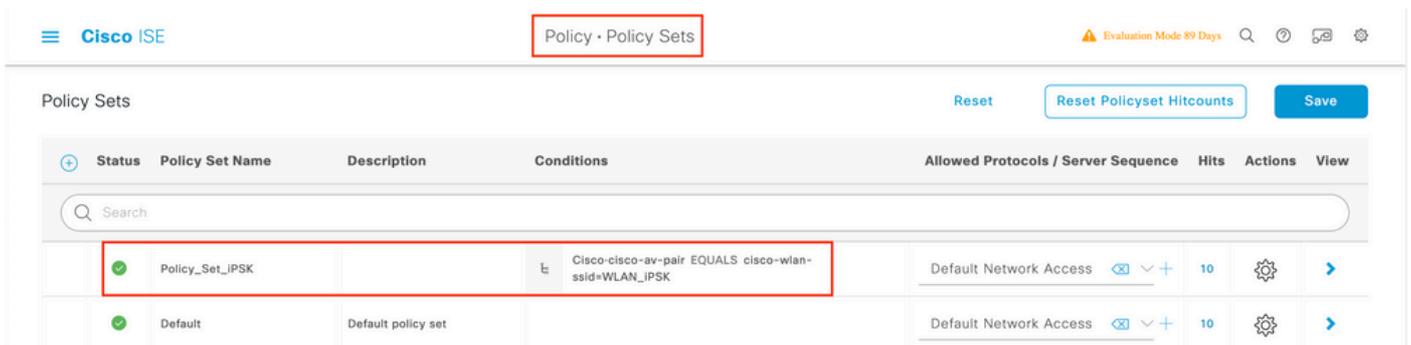
[Policy] > [Policy Sets] で、新しいポリシーを作成します。クライアントがポリシーセットに一致していることを確認するために、次の条件が使用されます。

Cisco:cisco-av-pair **EQUALS** cisco-wlan-ssid=WLAN\_iPSK // "WLAN\_iPSK" is WLAN name

## Conditions Studio



ポリシー照合をより安全にするために、条件を追加できます。



[Policy Set]行の右側にある青い矢印をクリックして、新しく作成したiPSKポリシーセット設定に移動します。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">✔</span>	Policy_Set_IPSK		Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_IPSK	Default Network Access	77		

[Authentication Policy] が [Internal Endpoints] に設定されていることを確認します。

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Policy Sets → Policy\_Set-IPSK Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
<span style="color: green;">✔</span>	Policy_Set-IPSK		Radius-Called-Station-ID ENDS_WITH WLAN_IPSK	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
<span style="color: green;">✔</span>	Default		Internal Endpoints	0	

[Authorization Policy] で、ユーザグループごとに新しいルールを作成します。条件として、次を使用します。

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK //
"Identity_Group_iPSK" is name of the created endpoint group
```

Resultは、以前に作成した認可プロファイルです。[Default] ルールが一番下に残り、[DenyAccess] をポイントしていることを確認します。

Cisco ISE Policy · Policy Sets Evaluation Mode 89 Days

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions	Results		Hits	Actions
			Profiles	Security Groups		
<span style="color: green;">✔</span>	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_iPSK	Authz_Profile_IPSK	Select from list	0	
<span style="color: green;">✔</span>	Default		DenyAccess	Select from list	0	

すべてのユーザが異なるパスワードを使用する場合、エンドポイントグループとそのエンドポイントグループに一致するルールを作成する代わりに、次の条件を持つルールを作成できます。

Radius-Calling-Station-ID **EQUALS** <client\_mac\_addr>

**注：** MACアドレスデリミタは、WLCの[AAA] > [AAA Advanced] > [Global Config] > [Advanced Settings]で設定できます。この例では、文字「-」が使用されています。

The screenshot shows the Cisco ISE interface for configuring Policy Sets. The 'Authorization Policy (1)' section is expanded, displaying a table of rules. The first rule, 'Authz\_Rule\_Single', is highlighted with a red box. Its condition is 'Radius-Calling-Station-ID EQUALS 08-BE-AC-27-85-7E' and its profile is 'Authz\_Profile\_IPSK'.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Authz_Rule_Single	Radius-Calling-Station-ID EQUALS 08-BE-AC-27-85-7E	Authz_Profile_IPSK ×	Select from list		⚙️
✓	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK ×	Select from list		⚙️
✓	Default		DenyAccess ×	Select from list	0	⚙️

認可ポリシーのルールでは、ユーザが使用しているパスワードを指定するために、他の多くのパラメータを使用できます。最も一般的に使用されるルールは次のとおりです。

### 1. ユーザの場所に基づく照合

このシナリオでは、WLCはAPロケーション情報をISEに送信する必要があります。これにより、ある場所のユーザは1つのパスワードを使用し、別の場所のユーザは別のパスワードを使用できます。これは、[Configuration] > [Security] > [Wireless AAA Policy] で設定できます。

。

## Edit Wireless AAA Policy

Policy Name*	default-aaa-policy
NAS-ID Option 1	System Name ▼
NAS-ID Option 2	AP Location ▼
NAS-ID Option 3	Not Configured ▼

### 2. デバイスのプロファイリングに基づく照合

このシナリオでは、デバイスをグローバルにプロファイルするようにWLCを設定する必要があります。これにより、管理者はラップトップデバイスと電話デバイスに異なるパスワードを設定できます。グローバルデバイス分類は、[Configuration] > [Wireless] > [Wireless Global] で有効にできます。ISEでのデバイスプロファイリングの設定については、『[ISEプロファイリング設計ガイド](#)』を参照してください。

暗号化キーを返すだけでなく、この認可は802.11アソシエーションフェーズで発生するため、ACLやVLAN IDなど、他のAAA属性をISEから返すことも完全に可能です。

## トラブルシューティング

### 9800 WLCのトラブルシューティング

WLCでは、放射性トレースの収集は、問題の大部分を特定するのに十分な量である必要があります。これは、WLC Webインターフェイスの[Troubleshooting] > [Radioactive Trace] で実行できます。クライアントのMACアドレスを追加し、**Start**を押して問題の再現を試みます。[Generate]をクリックしてファイルを作成し、ダウンロードします。

## Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file	
<input type="checkbox"/>	74da.38f6.76f0	debugTrace_74da.38f6.76f0.txt	<b>▶ Generate</b>

◀ 1 ▶ 20 items per page 1 - 1 of 1 items

**重要** : IOS 14およびAndroid 10スマートフォンのiPhoneは、ネットワークへの関連付けにランダム化されたMACアドレスを使用します。この機能により、iPSK設定が完全に壊れる可能性があります。この機能が無効になっていることを確認してください。

放射性トレースでは問題を特定するのに十分でない場合は、パケットキャプチャをWLCで直接収集できます。[Troubleshooting] > [Packet Capture] で、キャプチャポイントを追加します。デフォルトでは、WLCはすべてのRADIUS AAA通信にワイヤレス管理インターフェイスを使用します。WLCのクライアント数が多い場合は、バッファサイズを100 MBに増やします。

### Edit Packet Capture

Capture Name\*

iPSK

Filter\*

any

Monitor Control Plane

Buffer Size (MB)\*

100

Limit by\*

Duration

3600

secs == 1.00 hour

Available (4)

Search

- GigabitEthernet1 →
- GigabitEthernet2 →
- GigabitEthernet3 →
- Vlan1 →

Selected (1)

- Vlan39 ←

次の図に、認証とアカウントングの試行が成功したときのパケットキャプチャを示します。このクライアントに関連するすべてのパケットをフィルタリングするには、次のWiresharkフィルタを使用します。

ip.addr==

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

## ISEのトラブルシューティング

Cisco ISEの主なトラブルシューティングテクニックは、[Operations] > [RADIUS] > [Live Logs] にある[Live Logs] ページです。これらは、クライアントのMACアドレスを[Endpoint ID]フィールドに入力することでフィルタリングできます。完全なISEレポートを開くと、障害の原因に関する詳細が表示されます。クライアントが正しいISEポリシーにヒットしていることを確認します。

Operations - RADIUS

Live Logs

Misconfigured Supplicants: 0, Misconfigured Network Devices: 0, RADIUS Drops: 0, Client Stopped Responding: 0, Repeat Counter: 1

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentic...	Authoriz...	Authorization Pro...	IP Address
Aug 19, 2022 08:04:20.5...	●	🔒	1	08:BE:AC:27:8...	08:BE:AC:27:85:7E	Unknown	Policy_Set...	Policy_Set...	Authz_Profile_IPSK	fe80::e864:b6
Aug 19, 2022 08:04:13.3...	✅	🔒		08:BE:AC:27:8...	08:BE:AC:27:85:7E	Unknown	Policy_Set...	Policy_Set...	Authz_Profile_IPSK	

## 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。