

# Konfigurieren von Catalyst 9800 WLC iPSK mithilfe der ISE

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Verständnis von iPSK und den passenden Szenarien](#)

[Konfigurieren des 9800 WLC](#)

[ISE-Konfiguration](#)

[Fehlerbehebung](#)

[Fehlerbehebung am 9800 WLC](#)

[Fehlerbehebung bei ISE](#)

## Einleitung

Dieses Dokument beschreibt die Konfiguration eines durch iPSK gesicherten WLAN auf einem Cisco Wireless LAN Controller der Serie 9800 mit der Cisco ISE als RADIUS-Server.

## Voraussetzungen

### Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie bereits mit der Basiskonfiguration eines WLAN auf dem 9800 vertraut sind und diese Konfiguration an Ihre Bereitstellung anpassen können.

### Verwendete Komponenten

- Cisco 9800-CL WLC mit 17.6.3
- Cisco ISE 3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

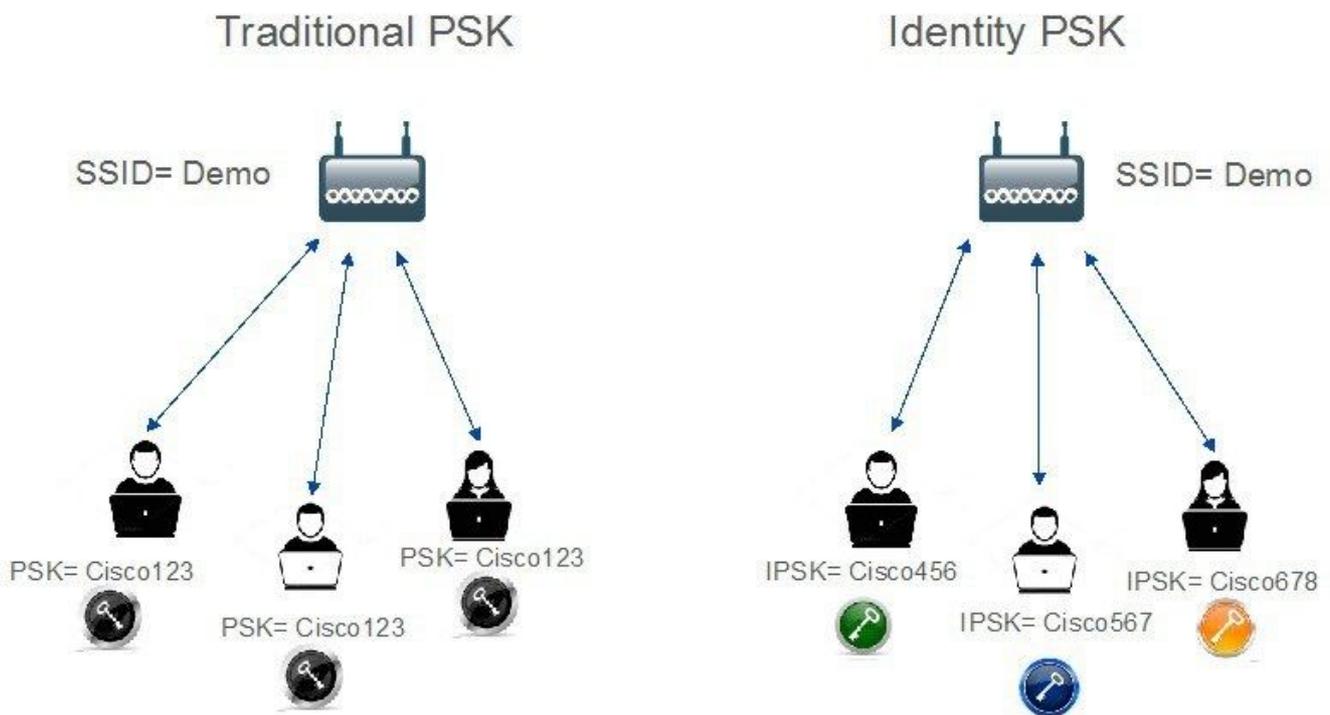
## Verständnis von iPSK und den passenden Szenarien

In herkömmlichen PSK-Netzwerken (Pre-Shared Key) wird für alle verbundenen Clients dasselbe Kennwort verwendet. Dies kann dazu führen, dass der Schlüssel für nicht autorisierte Benutzer freigegeben wird und eine Sicherheitsverletzung sowie nicht autorisierter Zugriff auf das Netzwerk verursacht werden. Die häufigste Abschwächung dieser Sicherheitsverletzung ist die Änderung

des PSK selbst, eine Änderung, die sich auf alle Benutzer auswirkt, da viele Endgeräte mit dem neuen Schlüssel aktualisiert werden müssen, um wieder auf das Netzwerk zugreifen zu können.

Mit Identity PSK (iPSK) werden mithilfe eines RADIUS-Servers eindeutige vorinstallierte Schlüssel für Einzelpersonen oder eine Gruppe von Benutzern auf derselben SSID erstellt. Diese Art von Konfiguration ist äußerst nützlich in Netzwerken, in denen Endclientgeräte keine 802.1x-Authentifizierung unterstützen, aber ein sichereres und präziseres Authentifizierungsschema erforderlich ist. Aus Client-Sicht ist dieses WLAN mit dem herkömmlichen PSK-Netzwerk identisch. Bei Kompromittierung eines PSKs muss nur dessen PSK aktualisiert werden. Die übrigen mit dem WLAN verbundenen Geräte sind davon nicht betroffen.

## Traditional Vs Identity PSK



## Konfigurieren des 9800 WLC

Fügen Sie unter **Configuration > Security > AAA > Servers/Groups > Servers** die ISE als RADIUS-Server hinzu:

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

10 items per page 1 - 1 of 1 items

Erstellen Sie unter **Configuration > Security > AAA > Servers/Groups > Server Groups** eine

RADIUS-Servergruppe, und fügen Sie ihr den zuvor erstellten ISE-Server hinzu:

Configuration > Security > AAA

+ 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 10 items per page 1 - 1 of 1 items

Erstellen Sie auf der Registerkarte **AAA Method List** eine Autorisierungsliste mit dem Typ "network" und dem Gruppentyp "group", der auf die zuvor erstellte RADIUS-Servergruppe verweist:

Configuration > Security > AAA

+ 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 10 items per page 1 - 1 of 1 items

Das Einrichten der Kontoführung ist optional, kann jedoch durch Konfigurieren von Type auf "identity" und Verweisen auf dieselbe RADIUS-Servergruppe erfolgen:

Configuration > Security > AAA

+ 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 10 items per page 1 - 1 of 1 items

Dies kann auch über die Befehlszeile mit folgenden Befehlen durchgeführt werden:

```
radius server
```

Erstellen Sie unter **Configuration > Tags & Profiles > WLANs** ein neues WLAN. Unter Layer 2-Konfiguration:

- Aktivieren Sie die MAC-Filterung, und legen Sie die Autorisierungsliste auf die zuvor erstellte

fest.

- Aktivieren Sie unter **Auth Key Mgmt (Auth-Schlüsselverwaltung) PSK**.
- Das Feld für den vorinstallierten Schlüssel kann mit einem beliebigen Wert gefüllt werden. Dies geschieht nur, um die Anforderungen des Web-Interface-Designs zu erfüllen. Kein Benutzer kann sich mit diesem Schlüssel authentifizieren. In diesem Fall wurde der vorinstallierte Schlüssel auf "12345678" gesetzt.

**Add WLAN** [Close]

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode: WPA + WPA2

MAC Filtering:

Authorization List\*: Authz\_List... [Info]

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\*: [Masked Key]

Lobby Admin Access:

Fast Transition: Adaptive Enabled

Over the DS:

Reassociation Timeout: 20

MPSK Configuration

MPSK:

Die Benutzersegregation kann auf der Registerkarte **Erweitert** erreicht werden. Wenn Sie diese Einstellung auf Allow Private Group (Private Gruppe zulassen) festlegen, können Benutzer, die den gleichen PSK verwenden, miteinander kommunizieren, während Benutzer, die einen anderen PSK verwenden, blockiert werden:

The screenshot shows the 'Advanced' tab of a configuration interface. The 'P2P Blocking Action' dropdown menu is highlighted with a red box and is set to 'Allow Private Group'. Other settings include 'Coverage Hole Detection' (checked), 'Aironet IE' (unchecked), 'Advertise AP Name' (unchecked), 'Multicast Buffer' (DISABLED), 'Universal Admin' (unchecked), 'OKC' (checked), 'Load Balance' (unchecked), 'Band Select' (unchecked), and 'IP Source Guard' (unchecked).

Erstellen Sie unter **Configuration > Tags & Profiles > Policy** (Konfiguration > Tags & Profile > Richtlinie) ein neues Richtlinienprofil. Legen Sie auf der Registerkarte **Access Policies** (Zugriffsrichtlinien) die VLAN- oder VLAN-Gruppe fest, die von diesem WLAN verwendet wird:

The screenshot shows the 'Add Policy Profile' dialog box. A warning message states: 'Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.' The 'Access Policies' tab is selected. The 'VLAN/VLAN Group' dropdown menu is highlighted with a red box and is set to 'VLAN0039'. Other settings include 'RADIUS Profiling' (unchecked), 'HTTP TLV Caching' (unchecked), 'DHCP TLV Caching' (unchecked), 'Global State of Device Classification' (info icon), 'Local Subscriber Policy Name' (Search or Select), 'WLAN ACL' (WLAN ACL), 'IPv4 ACL' (Search or Select), 'IPv6 ACL' (Search or Select), 'URL Filters' (URL Filters), 'Pre Auth' (Search or Select), and 'Post Auth' (Search or Select).

Aktivieren Sie auf der Registerkarte **Erweitert** die Option AAA-Überschreiben, und fügen Sie die Abrechnungsliste hinzu, falls zuvor erstellt:

## 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  IGNORE

### WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Vergewissern Sie sich unter **Configuration > Tags & Profiles > Tags > Policy**, dass das WLAN dem von Ihnen erstellten Richtlinienprofil zugeordnet ist:

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

WLAN\_iPSK Policy\_Profile\_iPSK

1 10 Items per page

1 - 1 of 1 items

Dies kann auch über die Befehlszeile mit folgenden Befehlen durchgeführt werden:

wlan

Vergewissern Sie sich unter **Konfiguration > Wireless > Access Points**, dass dieser Tag auf die Access Points angewendet wurde, auf die das WLAN übertragen werden muss:

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"/>	i		

## ISE-Konfiguration

In diesem Konfigurationsleitfaden wird ein Szenario beschrieben, in dem der PSK des Geräts anhand der Client-MAC-Adresse bestimmt wird. Unter **Administration > Netzwerkressourcen > Netzwerkgeräte** fügen Sie ein neues Gerät hinzu, geben die IP-Adresse an, aktivieren die RADIUS-Authentifizierungseinstellungen und geben einen gemeinsamen RADIUS-Schlüssel an:

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]

Fügen Sie unter **Context Visibility > Endpoints > Authentication** (Kontextsichtbarkeit > Endpunkte > Authentifizierung) die MAC-Adressen aller Geräte (Clients) hinzu, die eine Verbindung zum iPSK-Netzwerk herstellen:

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.

Erstellen Sie unter **Administration > Identity Management > Groups > Endpoint Identity Groups** eine oder mehrere Gruppen, und weisen Sie ihnen Benutzer zu. Jede Gruppe kann später für die Verwendung eines anderen PSK für die Verbindung mit dem Netzwerk konfiguriert werden.

The screenshot shows the Cisco ISE Administration console. The breadcrumb is "Administration - Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area shows a table of Endpoint Identity Groups:

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

Buttons for "Edit", "+ Add", and "Delete" are visible above the table. The "Add" button is highlighted with a red box.

The screenshot shows the "New Endpoint Group" form. The breadcrumb is "Administration - Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area shows the "Endpoint Identity Group List" with a "New Endpoint Group" form:

Endpoint Identity Group

\* Name: Identity\_Group\_IPSK

Description:

Parent Group:

Buttons for "Submit" and "Cancel" are visible at the bottom. The "Endpoint Identity Group" title and the "Name" field are highlighted with red boxes.

Nachdem die Gruppe erstellt wurde, können Sie ihnen Benutzer zuweisen. Wählen Sie die Gruppe, die Sie erstellt haben, und klicken Sie auf "Bearbeiten":

The screenshot shows the Cisco ISE Administration console. The breadcrumb is "Administration - Identity Management". The "Groups" tab is selected. In the left sidebar, "Endpoint Identity Groups" is highlighted. The main content area shows a table of Endpoint Identity Groups:

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

Buttons for "Edit", "+ Add", and "Delete" are visible above the table. The "Edit" button and the "Identity\_Group\_IPSK" row are highlighted with red boxes.

Fügen Sie in der Gruppenkonfiguration die MAC-Adresse der Clients hinzu, die Sie dieser Gruppe zuweisen möchten. Klicken Sie dazu auf die Schaltfläche "Hinzufügen":

Cisco ISE Administration - Identity Management

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

Identity Groups

Endpoint Identity Group List > Identity\_Group\_IPSK

Endpoint Identity Group

\* Name Identity\_Group\_IPSK

Description

Parent Group

Save Reset

Selected 0 Total 1

+ Add Remove

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

Erstellen Sie unter Policy > **Policy Elements** > Results > Authorization > Authorization Profiles (Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile) ein neues Autorisierungsprofil. Attribute festlegen auf:

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

Erstellen Sie für jede Benutzergruppe, die einen anderen PSK verwenden muss, ein zusätzliches Ergebnis mit einem anderen PSK-AV-Paar. Hier können auch zusätzliche Parameter wie ACL und VLAN Override konfiguriert werden.

Cisco ISE Policy - Policy Elements

Dictionarys Conditions **Results**

Authentication

Authorization

**Authorization Profiles**

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > New Authorization Profile

Authorization Profile

\* Name Authz\_Profile\_IPSK

Description

\* Access Type ACCESS\_ACCEPT

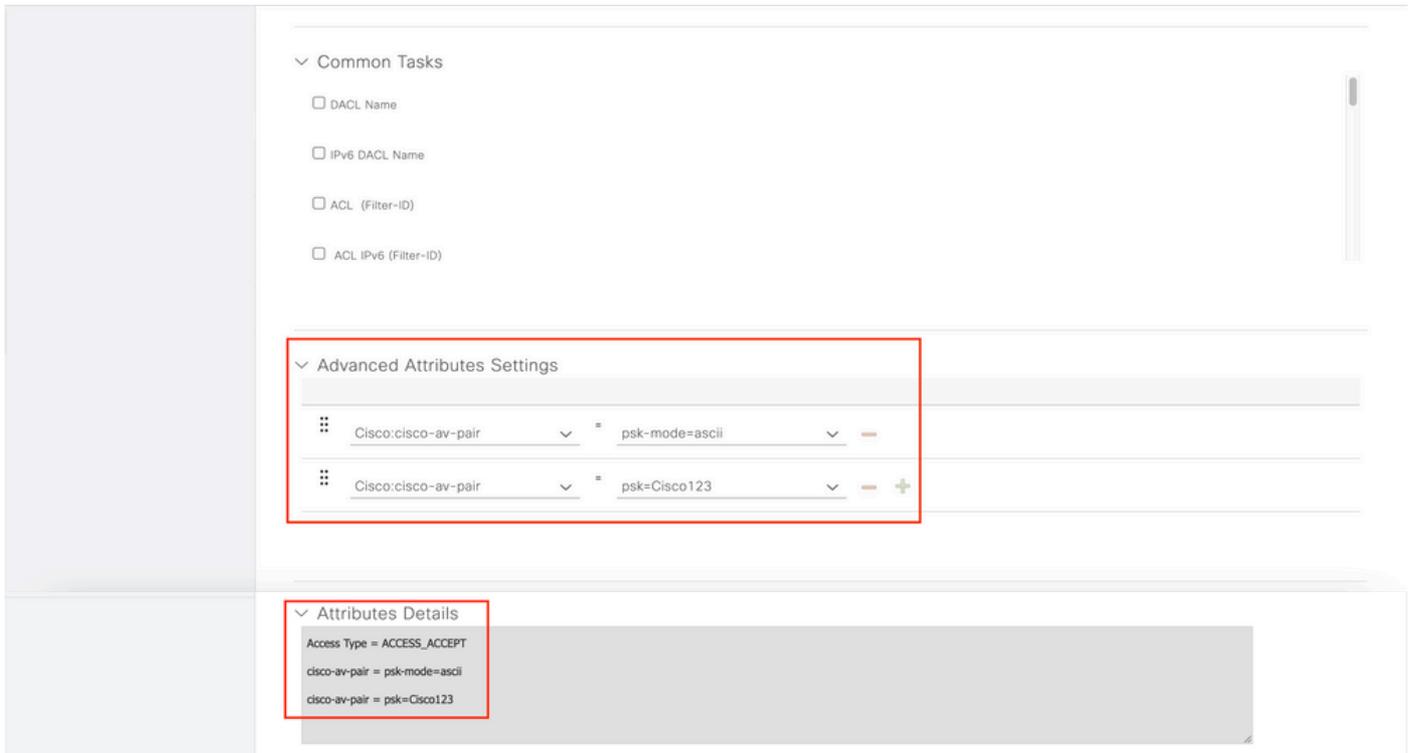
Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking



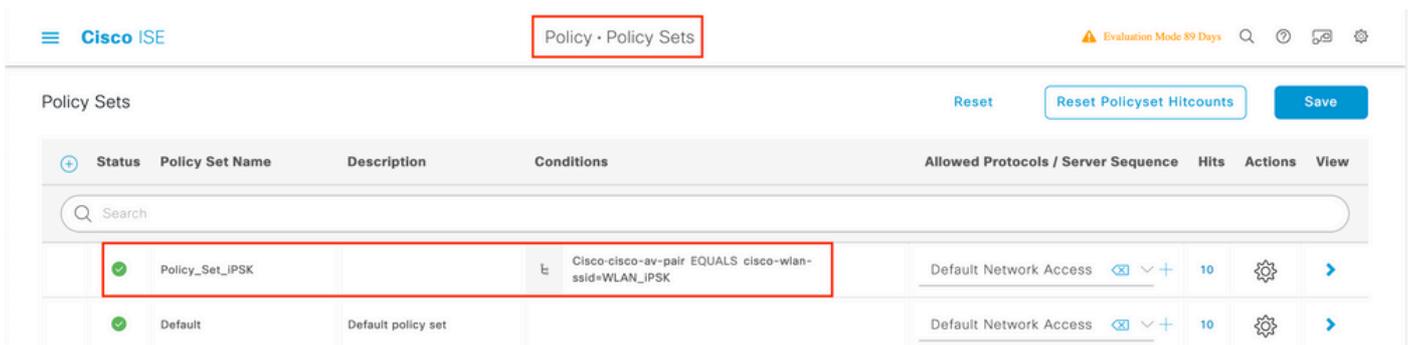
Erstellen Sie unter **Richtlinie > Richtlinienätze** eine neue Richtlinie. Um sicherzustellen, dass der Client mit dem Richtlinienatz übereinstimmt, wird diese Bedingung verwendet:

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

## Conditions Studio



Es können weitere Bedingungen hinzugefügt werden, um die Richtlinienzuordnung sicherer zu machen.



Öffnen Sie die neu erstellte iPSK-Konfiguration für den Richtlinienatz, indem Sie auf den blauen

Pfeil rechts neben der Zeile Richtlinienansatz klicken:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy_Set_IPSK		Cisco-cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_IPSK	Default Network Access	77	 	

Stellen Sie sicher, dass die **Authentifizierungsrichtlinie** auf "Interne Endpunkte" festgelegt ist:

Policy Sets → Policy\_Set-iPSK

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	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
✓	Default		Internal Endpoints	0	Options

Erstellen Sie unter **Autorisierungsrichtlinie** eine neue Regel für jede Benutzergruppe. Als Bedingung:

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

wobei das **Ergebnis** das **Autorisierungsprofil** ist, das zuvor erstellt wurde. Vergewissern Sie sich, dass die **Standardregel** unten beibehalten wird und auf **DenyAccess** zeigt.

Cisco ISE Policy - Policy Sets Evaluation Mode 89 Days

Search

Internal Endpoints <v> Options 0

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK x	Select from list	0	+
+	Default		DenyAccess x	Select from list	0	+

Wenn jeder Benutzer über ein anderes Kennwort verfügt, kann statt Endpunktgruppen und Regeln zu erstellen, die mit dieser Endpunktgruppe übereinstimmen, eine Regel mit dieser Bedingung erstellt werden:

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

**Anmerkung:** Das MAC-Adressen-Delimiter kann auf dem WLC unter **AAA > AAA Advanced > Global Config > Advanced Settings** konfiguriert werden. In diesem Beispiel wurde das Zeichen "-" verwendet.

Cisco ISE Policy - Policy Sets Evaluation Mode 89 Days

Search

Internal Endpoints <v> Options 0

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

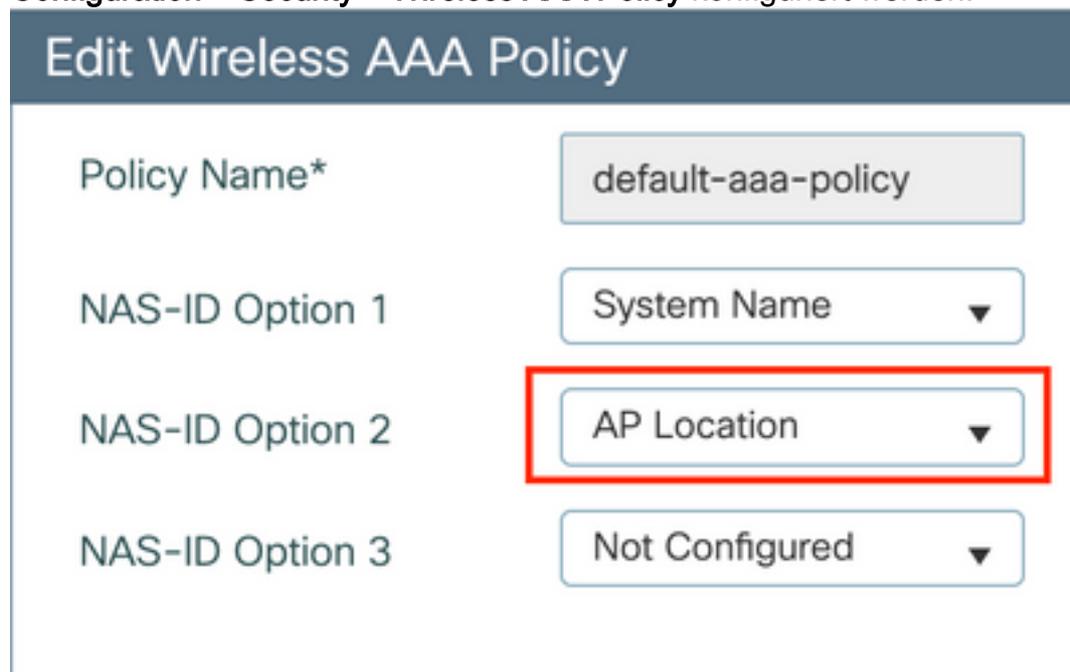
Authorization Policy (1)

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 x	Select from list	0	+
+	Authz_Rule_Group1	IdentityGroup-Name EQUALS Endpoint Identity Groups:Identity_Group_IPSK	Authz_Profile_IPSK x	Select from list	0	+
+	Default		DenyAccess x	Select from list	0	+

Regeln für die Autorisierungsrichtlinie ermöglichen die Verwendung zahlreicher anderer Parameter, um das vom Benutzer verwendete Kennwort festzulegen. Zu den am häufigsten verwendeten Regeln gehören:

### 1. Übereinstimmung basierend auf dem Benutzerstandort

In diesem Szenario muss der WLC Informationen zum AP-Standort an die ISE senden. Dadurch können Benutzer an einem Standort ein Kennwort verwenden, während die Benutzer an einem anderen Standort ein anderes Kennwort verwenden. Dies kann unter **Configuration > Security > Wireless AAA Policy** konfiguriert werden:



The screenshot shows the 'Edit Wireless AAA Policy' configuration page. The 'Policy Name\*' is set to 'default-aaa-policy'. The 'NAS-ID Option 1' is set to 'System Name'. The 'NAS-ID Option 2' is set to 'AP Location', which is highlighted with a red box. The 'NAS-ID Option 3' is set to 'Not Configured'.

## 2. Anpassung anhand der Erstellung von Geräteprofilen

In diesem Szenario muss der WLC so konfiguriert werden, dass ein globales Geräteprofil erstellt wird. Dadurch kann ein Administrator ein anderes Kennwort für Laptops und Telefone konfigurieren. Die globale Geräteklassifizierung kann aktiviert werden unter **Configuration > Wireless > Wireless Global**. Informationen zur Konfiguration der Erstellung von Geräteprofilen auf der ISE finden Sie im [Designleitfaden zur ISE-Profilerstellung](#).

Da diese Autorisierung in der 802.11-Zuordnungsphase erfolgt, ist es nicht nur möglich, den Verschlüsselungsschlüssel zurückzugeben, sondern es können auch andere AAA-Attribute von der ISE wie ACL oder VLAN-ID zurückgegeben werden.

## Fehlerbehebung

### Fehlerbehebung am 9800 WLC

Auf dem WLC muss das Sammeln radioaktiver Spuren mehr als genug sein, um eine Mehrheit der Probleme zu identifizieren. Dies kann über die WLC-Webschnittstelle unter **Troubleshooting > Radioactive Trace** erfolgen. Fügen Sie die MAC-Adresse des Clients hinzu, drücken Sie **Start**, und versuchen Sie, das Problem zu reproduzieren. Klicken Sie auf **Generate (Generieren)**, um die Datei zu erstellen und herunterzuladen:

## 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

**Wichtig:** iPhones auf IOS 14- und Android 10-Smartphones verwenden bei der Verbindung mit dem Netzwerk eine randomisierte MAC-Adresse. Diese Funktion kann die iPSK-Konfiguration vollständig unterbrechen. Stellen Sie sicher, dass diese Funktion deaktiviert ist!

Reicht Radioactive Traces nicht aus, um das Problem zu identifizieren, können Paketerfassungen direkt auf dem WLC erfasst werden. Fügen Sie unter **Troubleshooting > Packet Capture** (Fehlerbehebung > Paketerfassung) einen Erfassungspunkt hinzu. Standardmäßig verwendet WLC eine Wireless-Management-Schnittstelle für die gesamte RADIUS-AAA-Kommunikation. Erhöhen Sie die Puffergröße auf 100 MB, wenn der WLC über eine hohe Anzahl an Clients verfügt:

### 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 ←

Eine Paketerfassung eines erfolgreichen Authentifizierungs- und Abrechnungsversuchs ist in der

Abbildung unten dargestellt. Verwenden Sie diesen Wireshark-Filter, um alle relevanten Pakete für diesen Client herauszufiltern:

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

## Fehlerbehebung bei ISE

Das wichtigste Verfahren zur Fehlerbehebung bei der Cisco ISE ist die Seite **Live Logs** unter **Operations > RADIUS > Live Logs**. Sie können gefiltert werden, indem die MAC-Adresse des Clients in das Feld Endpunkt-ID eingegeben wird. Wenn Sie einen vollständigen ISE-Bericht öffnen, erhalten Sie weitere Details zum Fehlergrund. Stellen Sie sicher, dass der Client die richtige ISE-Richtlinie verwendet:

Operations - RADIUS

Live Logs

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

Refresh: Never, Show: Latest 20 records, Within: Last 3 hours

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	

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.