

Konfigurieren der Catalyst 9800 Wireless Controller AP-Autorisierungsliste

Inhalt

- [Einleitung](#)
- [Hintergrundinformationen](#)
- [Voraussetzungen](#)
- [Anforderungen](#)
- [Verwendete Komponenten](#)
- [Konfigurieren](#)
- [Netzwerkdiagramm](#)
- [Konfigurationen](#)
- [MAC AP-Autorisierungsliste - Lokal](#)
- [MAC AP-Autorisierungsliste - Externer RADIUS-Server](#)
- [9800 WLC-Konfiguration](#)
- [ISE-Konfiguration](#)
- [Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Endpunkte](#)
- [Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Benutzername/Kennwort](#)
- [Autorisierungsrichtlinie zur Authentifizierung von APs](#)
- [Überprüfung](#)
- [Fehlerbehebung](#)
- [Referenzen](#)

Einleitung

In diesem Dokument wird die Konfiguration der Authentifizierungsrichtlinie für den Catalyst 9800 Wireless LAN Controller Access Point (AP) beschrieben.

Hintergrundinformationen

Um einen Access Point (AP) zu autorisieren, muss die Ethernet-MAC-Adresse des AP für die lokale Datenbank mit dem Wireless LAN Controller 9800 oder für einen externen RADIUS-Server (Remote Authentication Dial-In User Service) autorisiert werden.

Diese Funktion stellt sicher, dass nur autorisierte Access Points (APs) einem Catalyst 9800 Wireless LAN-Controller beitreten können. In diesem Dokument wird nicht auf vernetzte (1500-Serie) APs eingegangen, die einen MAC-Filtereintrag benötigen, um mit dem Controller verbunden zu werden, jedoch nicht den typischen AP-Autorisierungsfluss verfolgen (siehe Referenzen).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- 9800 WLC
- Zugriff auf die Wireless Controller über eine Kommandozeile (CLI)

Verwendete Komponenten

9800 WLC v16.12

AP 1810 W

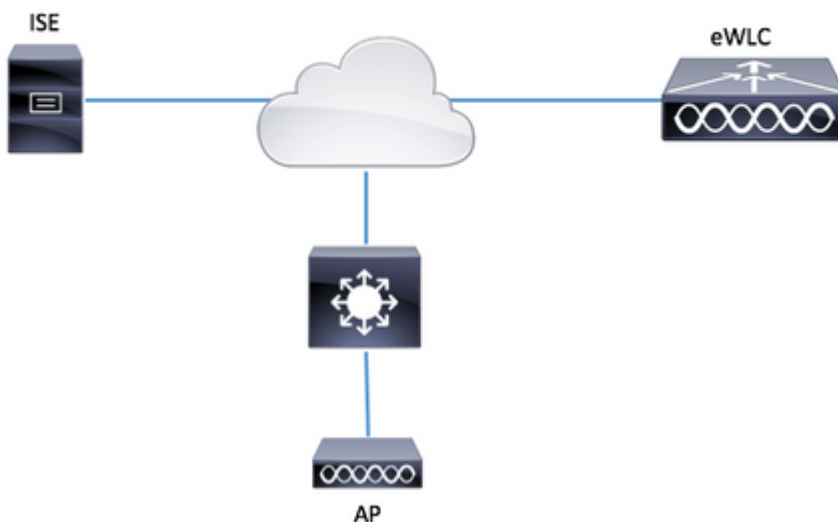
AP 1700

Identity Service Engine (ISE) Version 2.2

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 kennen.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

MAC AP-Autorisierungsliste - Lokal

Die MAC-Adresse der autorisierten Access Points wird lokal im 9800 WLC gespeichert.

Schritt 1: Erstellen Sie eine Liste mit lokalen Methoden zum Herunterladen von Autorisierungsanmeldeinformationen.

Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authorization > + Add.**

Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Troubleshooting

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List

Servers / Groups

AA

General

Authentication

Authorization

Accounting

+ Add

Name
<input type="checkbox"/> default
<input type="checkbox"/> AuthZ-Netw

Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-KCG-grp
- ISE-grp-name

Assigned Server Groups

>

<

Schritt 2: Aktivieren Sie die AP-MAC-Autorisierung.

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA Advanced > AP-Richtlinie**. Aktivieren Sie **die Autorisierung von APs für MAC**, und wählen Sie die in Schritt 1 erstellte **Liste** der **Autorisierungsmethoden** aus.

+ AAA Wizard

AAA Method List

Servers / Groups

AAA Advanced

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC

ENABLED

Authorize APs against Serial Number

DISABLED

Authorization Method List

AP-auth

Schritt 3: Fügen Sie die MAC-Adresse des AP-Ethernets hinzu.

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA Advanced > Geräteauthentifizierung > MAC-Adresse > + Hinzufügen**

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

AP Policy

Password Policy

AAA Interface

MAC Address

Serial Number

+ Add

× Delete

MAC Address

0

10 items per

Quick Setup: MAC Filtering ✕

MAC Address*

Attribute List Name

Hinweis: Die MAC-Adresse des AP-Ethernets muss in einem der folgenden Formate, wenn diese in Version 16.12 in die Webbenutzeroberfläche eingegeben wurden (xx:xx:xx:xx:xx:xx (oder) xxxx.xxxx.xxxx (oder) xx-xx-xx-xx-xx). In Version 17.3 müssen sie das Format xxxxxxxxxxxx ohne Trennzeichen haben. Das CLI-Format ist immer xxxxxxxxxxxx in jeder beliebigen Version (in Version 16.12 werden die Trennzeichen in der Konfiguration von der Webbenutzeroberfläche entfernt). Die Cisco Bug-ID [CSCvv43870](#) ermöglicht die Verwendung beliebiger Formate in der CLI oder der Webbenutzeroberfläche in späteren Versionen.

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local

# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP-Autorisierungsliste - Externer RADIUS-Server

9800 WLC-Konfiguration

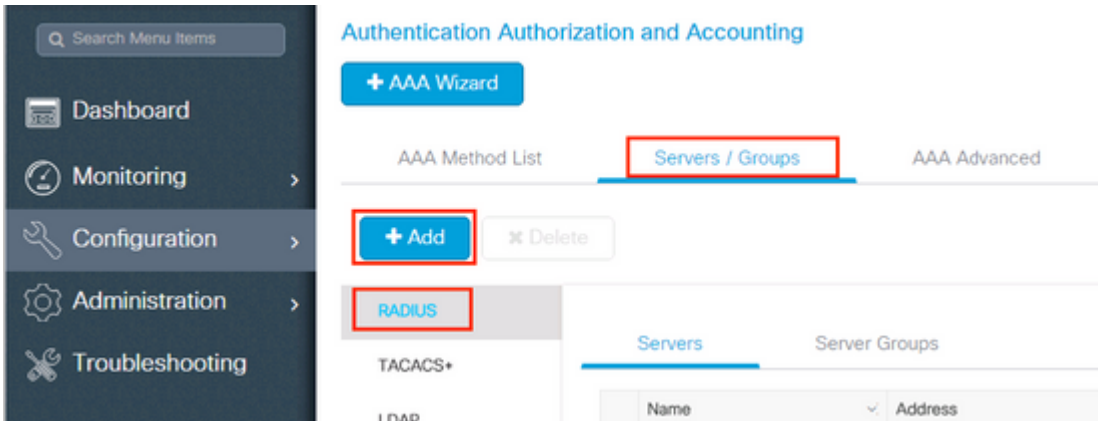
Die MAC-Adresse der autorisierten Access Points wird auf einem externen RADIUS-Server gespeichert, in diesem Beispiel ISE.

Auf der ISE können Sie die MAC-Adresse der Access Points entweder als Benutzername/Kennwort oder als Endpunkte registrieren. Entlang der Schritte werden Sie angewiesen, wie Sie die eine oder die andere Art zu verwenden.

GUI:

Schritt 1: Deklarieren des RADIUS-Servers

Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add (Konfiguration > Sicherheit > AAA > Server/Gruppen > RADIUS > Server > + Hinzufügen)**, und geben Sie die RADIUS-Serverinformationen ein.



Stellen Sie sicher, dass die Unterstützung für CoA aktiviert ist, wenn Sie zukünftig Central Web Authentication (oder irgendeine Art der Sicherheit, die CoA erfordert) verwenden möchten.

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		

Schritt 2: Hinzufügen eines RADIUS-Servers zu einer RADIUS-Gruppe

Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**.

Damit die ISE die MAC-Adresse des Access Points authentifiziert, wenn Benutzernamen keine MAC-Filterung zulassen.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Damit die ISE die AP-MAC-Adresse authentifiziert, wenn Endpunkte die MAC-Filterung in mac ändern.

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

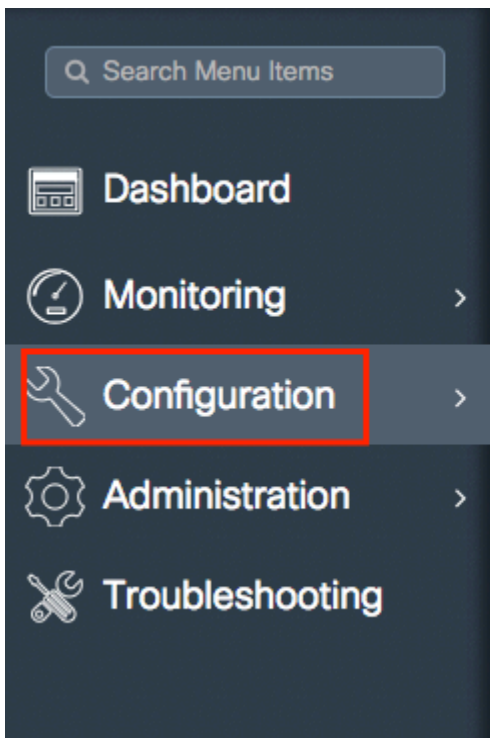
Dead-Time (mins)

Available Servers

Assigned Servers

Schritt 3: Erstellen Sie eine Liste der Autorisierungsanmeldeinformationen-Downloadmethoden.

Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authorization > + Add.**



Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List

Servers / Groups

AA

General

Authentication

Authorization

Accounting

+ Add

Name
<input type="checkbox"/> default
<input type="checkbox"/> AuthZ-Netw

Quick Setup: AAA Authorization

Method List Name*

Type*

Group Type

Fallback to local

Available Server Groups: radius, ldap, tacacs+, ISE-KCG-grp

Assigned Server Groups: ISE-grp-name

Cancel Save & Apply to Dev

Schritt 4: Aktivieren Sie die AP-MAC-Autorisierung.

Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA Advanced > AP-Richtlinie**. Aktivieren Sie die **Autorisierung von APs für MAC**, und wählen Sie die in Schritt 3 erstellte **Liste der Autorisierungsmethoden** aus.

Authentication Authorization and Accounting

+ AAA Wizard

AAA Method List Servers / Groups **AAA Advanced**

RADIUS Fallback

Attribute List Name

AP Authentication

AP Policy

Password Policy

Authorize APs against MAC ENABLED

Authorize APs against Serial Number DISABLED

Authorization Method List

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 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>

# aaa authorization credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISE-Konfiguration

Schritt 1: So fügen Sie der ISE den 9800 WLC hinzu:

[9800 WLC auf der ISE angeben](#)

Legen Sie fest, dass die MAC-Adresse der Access Points anhand der Authentifizierung konfiguriert werden soll. Führen Sie hierzu die folgenden Schritte aus:

[Konfigurieren von USE zur Authentifizierung von MAC-Adressen als Endpunkte](#)

[Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Benutzername/Kennwort](#)

Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Endpunkte

Schritt 2. (Optional) Erstellen einer Identitätsgruppe für Access Points

Da der 9800 das NAS-Port-Type-Attribut nicht mit AP-Autorisierung sendet, hat Cisco einen Fehler [IDCSCvy74904](#).) erkennt die ISE eine AP-Autorisierung nicht als MAB-Workflow und daher ist es nicht möglich, einen AP zu authentifizieren, wenn die MAC-Adresse des AP in der Endpunktliste platziert wird, es sei denn, Sie ändern die MAB-Workflows so, dass das NAS-PORT-Attribut auf der ISE nicht erforderlich ist.

Navigieren Sie zu **Administrator > Network device profile**, und erstellen Sie ein neues Geräteprofil. Aktivieren Sie RADIUS, und fügen Sie service-type=call-check für Wired MAB hinzu. Den Rest können Sie aus dem ursprünglichen Cisco Profil kopieren. Es soll keine Bedingung für den "nas-port-type" für den Wired MAB geben.

* Name

Description

Icon



[Change icon...](#)

[Set To Default](#)



Vendor

Supported Protocols

- RADIUS
- TACACS+
- TrustSec

RADIUS Dictionaries

Templates

[Expand All](#) / [Collapse All](#)

∨ Authentication/Authorization

∨ Flow Type Conditions

Wired MAB detected if the following condition(s) are met :

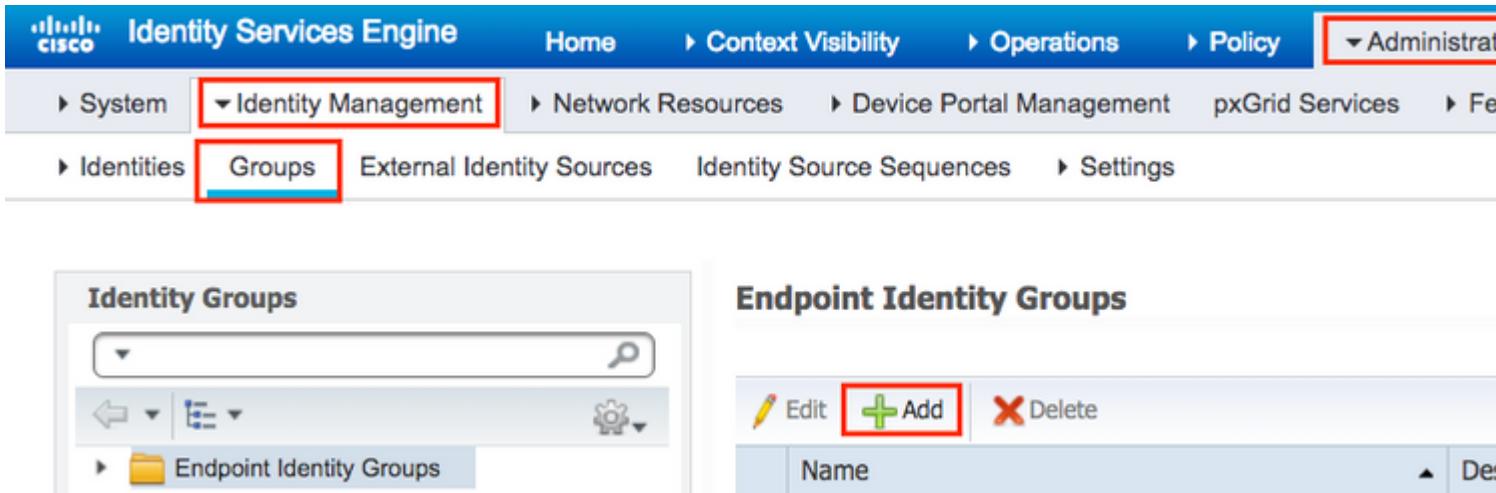


=



Kehren Sie zum Eintrag für das Netzwerkgerät für den 9800 zurück, und legen Sie dessen Profil auf das neu erstellte Geräteprofil fest.

Navigieren Sie zu **Administration > Identity Management > Groups > Endpoint Identity Groups > + Add.**



Wählen Sie einen Namen aus, und klicken Sie auf **Senden**.

The screenshot shows the 'New Endpoint Group' form in the Cisco ISE interface. The form has the following fields and buttons:

- Name:** * Name (required), value: AccessPoints
- Description:** (empty text area)
- Parent Group:** (empty dropdown menu)
- Buttons:** Submit (highlighted with a red box), Cancel

Schritt 3: Fügen Sie die MAC-Adresse des AP-Ethernets der Endgerätidentitätsgruppe hinzu.

Navigieren Sie zu **Work Centers > Network Access > Identities > Endpoints > +**

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > Id Groups > Ext Id Sources > Network Resources > Policy Elements > Authentication Policy > Authorization Policy

Endpoints

Network Access Users

Identity Source Sequences

INACTIVE ENDPOINTS ¹

0 Selected

Refresh + Delete Edit ANC Change Authorization Clear Threats & Vulnerabilities

MAC Address	Status	IPv4 Address	Username
-------------	--------	--------------	----------

Geben Sie die erforderlichen Informationen ein.

Add Endpoint



General Attributes

Mac Address * 00:B0:E1:8C:49:E8

Description Access Point

Static Assignment

Policy Assignment Unknown

Static Group Assignment

Identity Group Assignment AccessPoints

Cancel

Save

Schritt 4: Überprüfen Sie, ob der in der Standardauthentifizierungsregel verwendete Identitätsspeicher die

internen Endpunkte enthält.

A. Navigieren Sie zu **Richtlinie > Authentifizierung**, und notieren Sie sich den Identitätsspeicher.

Identity Services Engine Home Context Visibility Operations Policy

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MAB	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use :

B. Navigieren Sie zu **Administration > Identity Management > Identity Source Sequences > Identity Name**.

Identity Source Sequences

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit	Add	Duplicate	Delete
<input type="checkbox"/> Name	Description		
<input type="checkbox"/> All_User_ID_Stores	A built-in Identity Sequence to include all User		
<input type="checkbox"/> Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Requ		
<input type="checkbox"/> Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Porta		
<input type="checkbox"/> MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices		
<input type="checkbox"/> Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Po		

C. Stellen Sie sicher, dass interne Endpunkte dazu gehören, und fügen Sie sie gegebenenfalls hinzu.

Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

Selected

Internal Users
All_AD_Join_Points
Guest Users

▼ Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

Konfigurieren der ISE zur Authentifizierung der MAC-Adresse als Benutzername/Kennwort

Diese Methode wird nicht empfohlen, da sie niedrigere Kennwortrichtlinien erfordert, damit dasselbe Kennwort wie der Benutzername zulässig ist.

Es kann jedoch eine Problemumgehung sein, falls Sie Ihr Netzwerkgeräteprofil nicht ändern können.

Schritt 2. (Optional) Erstellen einer Identitätsgruppe für Access Points

Navigieren Sie zu **Administration > Identity Management > Groups > User Identity Groups > + Add.**

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', and 'Policy'. Below it, a secondary menu shows 'System', 'Identity Management' (highlighted with a red box), 'Network Resources', 'Device Portal Management', and 'pxGrid S'. A third menu shows 'Identities', 'Groups' (highlighted with a red box), 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The main content area is split into two panels. The left panel, titled 'Identity Groups', shows a search bar and a list of folders: 'Endpoint Identity Groups' and 'User Identity Groups' (highlighted with a red box). The right panel, titled 'User Identity Groups', shows a toolbar with 'Edit', '+ Add' (highlighted with a red box), 'Delete', and 'Import' buttons. Below the toolbar is a table with a header 'Name' and one row containing a checkbox, a person icon, and the text 'ALL_ACCOUNTS (default)'.

Wählen Sie einen Namen aus, und klicken Sie auf **Senden**.

The screenshot shows the 'New User Identity Group' form in the Cisco ISE interface. The breadcrumb navigation is 'User Identity Groups > New User Identity Group'. The form title is 'Identity Group'. It contains two input fields: '* Name' with the value 'AccessPoints' and 'Description'. At the bottom, there are two buttons: 'Submit' (highlighted with a red box) and 'Cancel'.

Schritt 3: Vergewissern Sie sich, dass Sie mit Ihrer aktuellen Kennwortrichtlinie eine MAC-Adresse als Benutzername und Kennwort hinzufügen können.

Navigieren Sie zu **Administration > Identity Management > Settings > User Authentication Settings > Password Policy**, und stellen Sie sicher, dass mindestens diese Optionen deaktiviert sind:

Cisco Identity Services Engine Home > Context Visibility > Operations > Policy > Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed

Identities Groups External Identity Sources Identity Source Sequences Settings

User Custom Attributes

User Authentication Settings

Endpoint Purge

Endpoint Custom Attributes

Password Policy Account Disable Policy

Password Policy

- Minimum Length: characters (Valid Range 4 to 127)

Password must not contain:

- User name or its characters in reverse order
- "cisco" or its characters in reverse order
- This word or its characters in reverse order:
- Repeated characters four or more times consecutively
- Dictionary words, their characters in reverse order or their letters replaced w

Default Dictionary ⓘ

Custom Dictionary ⓘ No file chosen

The newly added custom dictionary file will replace the existing cust

Password must contain at least one character of each of the selected types

- Lowercase alphabetic characters
- Uppercase alphabetic characters
- Numeric characters
- Non-alphanumeric characters

Password History

- Password must be different from the previous versions (Valid Range
- Password change delta characters (Valid Range 3 to 10)
- Cannot reuse password within days (Valid Range 0 to 365)

Password Lifetime

Users can be required to periodically change password

- Disable user account after days if password was not
- Display reminder days prior to password expiration (
- Lock/Suspend Account with Incorrect Login Attempts

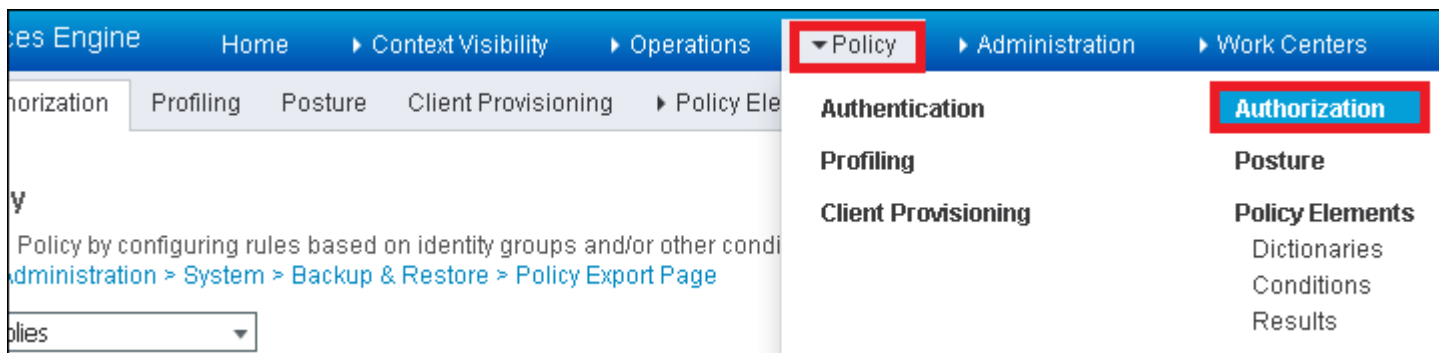
- # (Valid Range 3 to 20)
- Suspend account for minutes (Valid Range 15 to 1440) D

Hinweis: Sie können die Option **Benutzerkonto nach XX**
Tagen deaktivieren, wenn das Kennwort nicht geändert

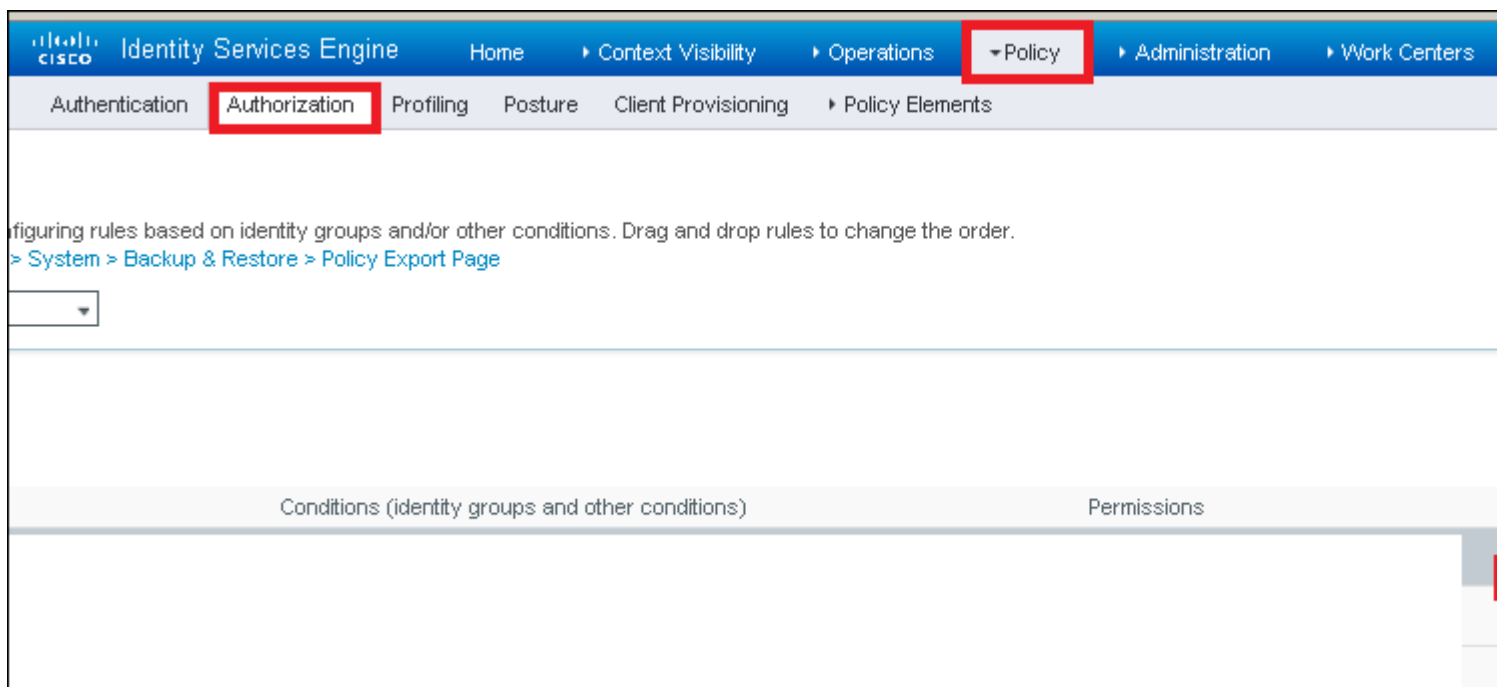
-Passwortfeld muss die Ethernet-MAC-Adresse des APs sein, nur Kleinbuchstaben und keine Trennzeichen.

Autorisierungsrichtlinie zur Authentifizierung von APs

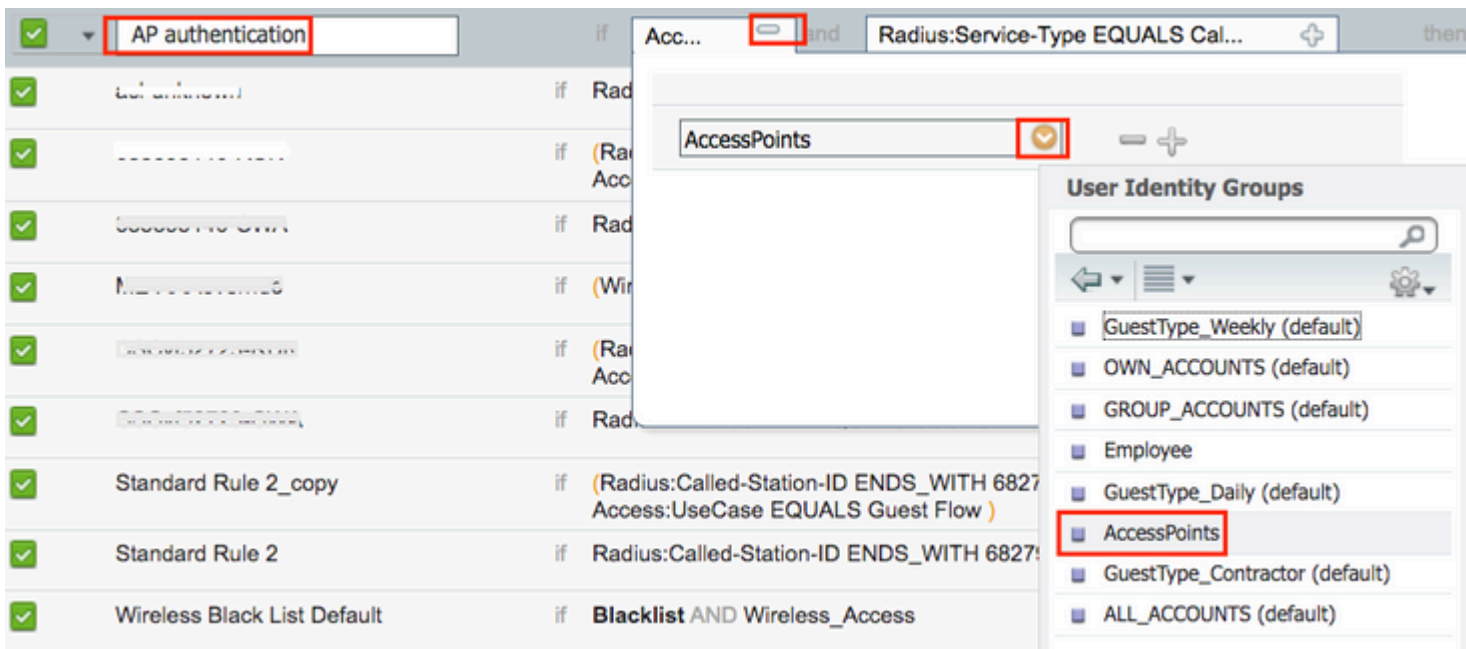
Navigieren Sie wie im Bild dargestellt **zu Richtlinie > Autorisierung**.



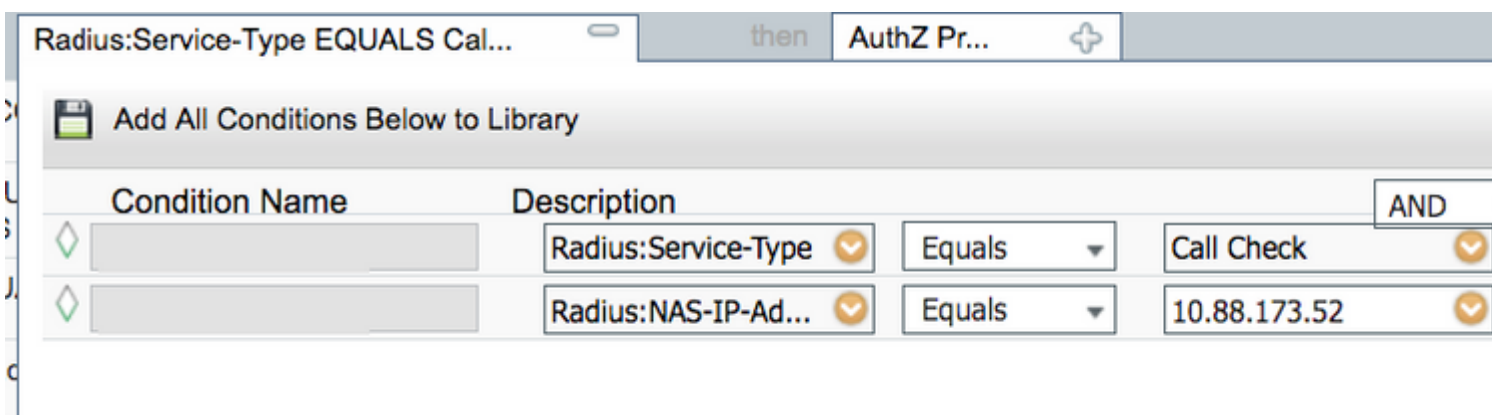
Fügt eine neue Regel wie im Bild dargestellt ein.



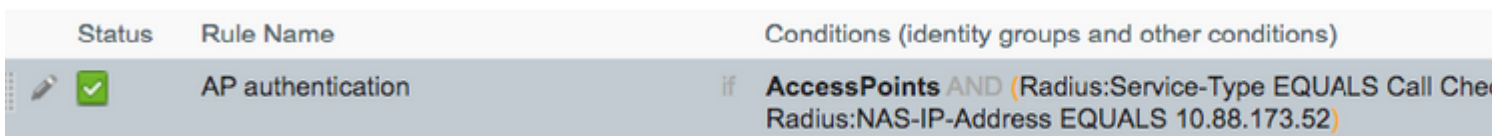
Wählen Sie zunächst einen Namen für die Regel und die Identitätsgruppe aus, in der der Access Point gespeichert ist (AccessPoints). Wählen Sie **Benutzeridentitätsgruppen** aus, wenn Sie die MAC-Adresse als Benutzername und Kennwort authentifizieren möchten, oder **Endpunkt-Identitätsgruppen**, wenn Sie die AP-MAC-Adresse als Endpunkte authentifizieren möchten.



Wählen Sie anschließend andere Bedingungen für den Autorisierungsprozess aus, um in diese Regel zu fallen. In diesem Beispiel greift der Autorisierungsprozess auf diese Regel zu, wenn der Dienstyp "Anrufprüfung" verwendet wird und die Authentifizierungsanforderung von der IP-Adresse 10.88.173.52 stammt.



Wählen Sie anschließend das Autorisierungsprofil aus, das den Clients zugewiesen ist, die diese Regel aufgerufen haben, klicken Sie auf Weiter, und speichern Sie es, wie im Bild dargestellt.



Hinweis: APs, die dem Controller bereits beigetreten sind, verlieren ihre Zuordnung nicht. Wenn sie jedoch nach der Aktivierung der Autorisierungsliste die Kommunikation mit dem Controller verlieren und versuchen, sich wieder anzuschließen, durchlaufen sie den Authentifizierungsprozess. Wenn ihre MAC-Adressen nicht lokal oder im RADIUS-Server aufgeführt werden, können sie keine Verbindung zum Controller herstellen.

Überprüfung

Überprüfen Sie, ob der 9800 WLC eine Liste zur Authentifizierung von APs aktiviert hat.

```
<#root>
```

```
# show ap auth-list
```

```
Authorize APs against MAC : Disabled  
Authorize APs against Serial Num : Enabled  
Authorization Method List : <auth-list-name>
```

Radius-Konfiguration überprüfen:

```
<#root>
```

```
#
```

```
show run aaa
```

Fehlerbehebung

Der WLC 9800 bietet IMMER-EIN-Ablaufverfolgungsfunktionen. Dadurch wird sichergestellt, dass alle mit dem AP-Beitritt zusammenhängenden Fehler, Warnungen und Meldungen auf Benachrichtigungsebene ständig protokolliert werden und Sie nach einem Vorfall oder Ausfall Protokolle anzeigen können.

Hinweis: Die Anzahl der generierten Protokolle variiert von einigen Stunden bis zu mehreren Tagen.

Um die Traces anzuzeigen, die der 9800 WLC standardmäßig erfasst, können Sie über SSH/Telnet eine Verbindung zum 9800 WLC herstellen (stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle Uhrzeit des Controllers, damit Sie die Protokolle bis zum Auftreten des Problems nachverfolgen können.

```
# show clock
```

Schritt 2: Erfassen Sie die Syslogs aus dem Controller-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie einen schnellen Überblick über den Systemzustand und eventuelle Fehler.

```
# show logging
```

Schritt 3: Überprüfen Sie, ob Debug-Bedingungen aktiviert sind.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Trace Configs:

Packet Infra debugs:
```

```
Ip Address _____ Port
-----|-----
```

Hinweis: Wenn eine Bedingung aufgelistet ist, bedeutet dies, dass die Traces für alle Prozesse, bei denen die aktivierten Bedingungen (MAC-Adresse, IP-Adresse usw.) auftreten, auf Debugging-Ebene protokolliert werden. Dies würde das Protokollvolumen erhöhen. Daher wird empfohlen, alle Bedingungen zu löschen, wenn gerade kein Debugging aktiv ist

Schritt 4: Angenommen, die zu testende MAC-Adresse wurde in Schritt 3 nicht als Bedingung aufgeführt. Sammeln Sie die stets verfügbaren Traces auf Benachrichtigungsebene für die jeweilige MAC-Adresse.

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

Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

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

Bedingtes Debugging und Radio Active Tracing

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu bestimmen, können Sie bedingtes Debuggen aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellt, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse).

Schritt 5: Stellen Sie sicher, dass keine Debug-Bedingungen aktiviert sind.

```
# clear platform condition all
```

Schritt 6: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesen Befehlen wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

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

Hinweis: Um mehr als einen Client gleichzeitig zu überwachen, führen Sie den Befehl `debug wireless mac <aaaa.bbbb.cccc>` für jede MAC-Adresse aus.

Hinweis: Sie sehen die Ausgabe der Client-Aktivität in der Terminalsitzung nicht, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 7. Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 8: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

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

Sobald die Monitoring-Zeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 9. Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie können entweder die Datei `ra_trace.log` auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA-Tracing-Datei

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

Datei auf externen Server kopieren:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d
```

Inhalt anzeigen:

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

Schritt 10. Wenn die Ursache immer noch nicht offensichtlich ist, rufen Sie die internen Protokolle ab, die eine ausführlichere Ansicht der Protokolle auf Debug-Ebene darstellen. Sie müssen den Client nicht noch einmal debuggen, da wir uns nur die Debug-Protokolle genauer ansehen, die bereits gesammelt und intern gespeichert wurden.

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

Hinweis: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Nachverfolgungen zu analysieren.

Sie können entweder die Datei `ra-internal-FILENAME.txt` auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Datei auf externen Server kopieren:

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

Inhalt anzeigen:

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

Schritt 11. Entfernen Sie die Debug-Bedingungen.

```
# clear platform condition all
```

Hinweis: Stellen Sie sicher, dass Sie die Debug-Bedingungen immer nach einer Fehlerbehebungsitzung entfernen.

Referenzen

[Verbindung von Mesh-APs mit 9800 WLC](#)

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.