

Konfigurieren von Central Web Authentication und Mobility Anchor auf Catalyst 9800 WLC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren eines Catalyst 9800, verbunden mit einem anderen Catalyst 9800](#)

[Netzwerkdiagramm](#)

[Konfigurieren von AAA auf beiden 9800-Geräten](#)

[WLANs auf den WLCs konfigurieren](#)

[Erstellen des Richtlinienprofils und des Richtlinien-Tags auf dem externen WLC](#)

[Erstellen Sie das Richtlinienprofil auf dem Anker-WLC.](#)

[Umleiten der ACL-Konfiguration auf beiden 9800s](#)

[ISE konfigurieren](#)

[Konfigurieren eines Catalyst 9800, verankert in einem AireOS WLC](#)

[Catalyst 9800 - Fremdkonfiguration](#)

[AAA-Konfigurationen auf dem Anker AireOS WLC](#)

[WLAN-Konfiguration auf dem AireOS WLC](#)

[Umleitung der ACL auf dem AireOS WLC](#)

[ISE konfigurieren](#)

[Unterschiede in der Konfiguration, wenn der AireOS-WLC der Fremdhersteller ist und der Catalyst 9800 der Auslöser ist](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Informationen zur Fehlerbehebung beim Catalyst 9800](#)

[Clientdetails](#)

[Integrierte Paketerfassung](#)

[RadioActive Traces](#)

[Informationen zur Fehlerbehebung in AireOS](#)

[Clientdetails](#)

[Debugger von der CLI](#)

[Referenzen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine zentrale Webauthentifizierung (CWA) auf dem Catalyst 9800 konfigurieren und Fehler bei der Suche nach einem anderen Wireless LAN Controller (WLC) als Mobilitätsanker beheben. Dabei werden sowohl der Anker auf AireOS als auch ein anderer 9800 WLC abgedeckt.

Voraussetzungen

Anforderungen

Es wird empfohlen, sich mit den 9800 WLC, AireOS WLC und der Cisco ISE vertraut zu machen. Es wird davon ausgegangen, dass Sie vor Beginn der CWA-Ankerkonfiguration den Mobility Tunnel zwischen den beiden WLCs bereits aufgerufen haben. Dies ist nicht Bestandteil des Konfigurationsbeispiels. Wenn Sie Hilfe hierzu benötigen, lesen Sie das Dokument "[Building Mobility Tunnels on Catalyst 9800 Controller](#)".

Verwendete Komponenten

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 potenziellen Auswirkungen eines Befehls verstehen.

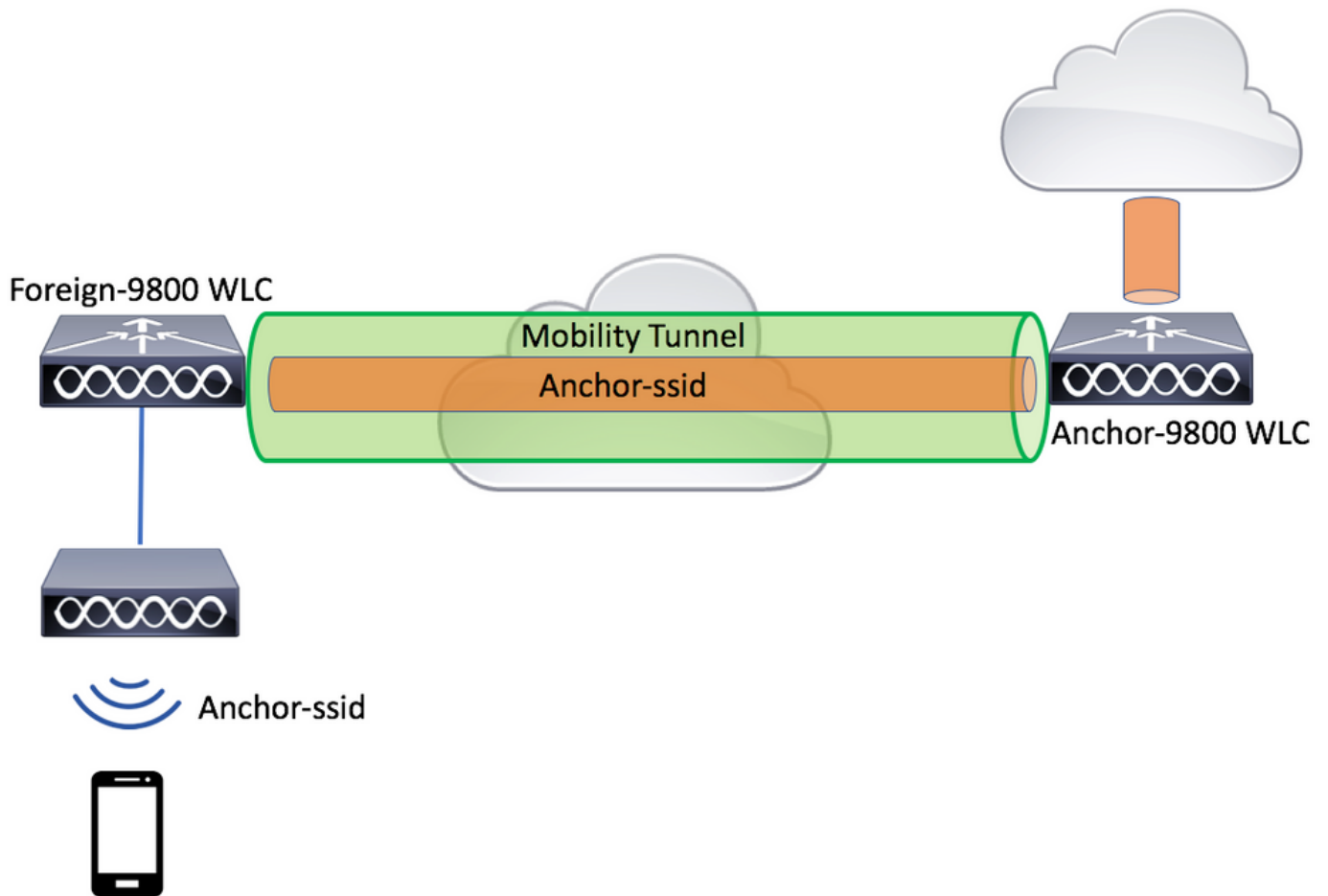
9800 17,2,1

5520 8.5.164 IRCM-Image

ISE 2.4

Konfigurieren eines Catalyst 9800, verbunden mit einem anderen Catalyst 9800

Netzwerkdiagramm



Konfigurieren von AAA auf beiden 9800-Geräten

Sowohl beim Anker als auch im Ausland müssen Sie zuerst den RADIUS-Server hinzufügen und sicherstellen, dass CoA aktiviert ist. Dies können Sie hier tun: **Configuration>Security>AAA>Servers/Groups>Servers>** Klicken Sie auf die Schaltfläche **Add (Hinzufügen)**.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Welcome admin
Last login Fri, May 15 2020 16:56:51 ...

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups

+ Add Delete

RADIUS Servers

TACACS+ Server Groups

LDAP

Create AAA Radius Server

Name* CLUS-Server

Server Address* X.X.X.X

PAC Key

Key Type Clear Text

Key*

Confirm Key*

Auth Port 1812

Acct Port 1813

Server Timeout (seconds) 1-1000

Retry Count 0-100

Support for CoA **ENABLED**

Cancel Apply to Device

Sie müssen nun eine Servergruppe erstellen und den Server, den Sie gerade konfiguriert haben, in diese Gruppe einfügen. Dies erfolgt hier **Configuration>Security>AAA>Servers/Groups>Server Groups>+Add**.

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add X Delete

RADIUS Servers Server Groups

TACACS+

LDAP

Create AAA Radius Server Group

Name* CLUS-Server-Group

Group Type RADIUS

MAC-Delimiter none

MAC-Filtering none

Dead-Time (mins) 1-1440

Available Servers Assigned Servers

CLUS-Server

Cancel Apply to Device

Erstellen Sie jetzt eine **Autorisierungsmethodenliste** (eine Authentifizierungsmethodenliste ist für CWA nicht erforderlich), wobei der Typ das Netzwerk und der Gruppentyp die Gruppe ist. Fügen Sie der Methodenliste die Servergruppe aus der vorherigen Aktion hinzu.

Diese Konfiguration erfolgt hier: **Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add**

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

Authentication

Authorization + Add - Delete

Accounting

Name	Type	Group Type
------	------	------------

Quick Setup: AAA Authorization

Method List Name* CLUS-AuthZ-Meth-List

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- ISE1

Assigned Server Groups

- CLUS-Server-Group

Cancel Apply to Device

(Optional) Erstellen Sie eine Accounting-Methodenliste unter Verwendung derselben Servergruppe wie die Autorisierungsmethodenliste. Die Accounting-Liste kann hier erstellt werden: **Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add**

The screenshot displays the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation at the top reads "Configuration > Security > AAA". The left sidebar contains navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled "AAA Method List" and includes tabs for "Servers / Groups", "AAA Method List", and "AAA Advanced". Under the "AAA Method List" tab, there are sections for "Authentication", "Authorization", and "Accounting". The "Accounting" section is highlighted, and a "+ Add" button is visible. A modal window titled "Quick Setup: AAA Accounting" is open, showing the following configuration details:

- Method List Name*: CLUS-Acct-Meth-List
- Type*: identity
- Available Server Groups: radius, ldap, tacacs+, ISE1
- Assigned Server Groups: CLUS-Server-Group

Buttons for "Cancel" and "Apply to Device" are located at the bottom of the modal.

WLANs auf den WLCs konfigurieren

Erstellen und konfigurieren Sie die WLANs auf beiden WLCs. Die WLANs sollten auf beiden übereinstimmen. Der Sicherheitstyp sollte MAC-Filterung sein, und die Liste der Autorisierungsmethoden aus dem vorherigen Schritt sollte angewendet werden. Diese Konfiguration wird unter **Configuration>Tags & Profiles>WLANs>+Add** vorgenommen.

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Profile Name* CLUS-WLAN-Name Radio Policy All

SSID* CLUS-SSID Broadcast SSID ENABLED

WLAN ID* 2

Status ENABLED

Cancel Apply to Device

Cisco Catalyst 9800-L Wireless Controller 17.2.1

Configuration > Tags & Profiles > WLANs

+ Add Delete Enable WLAN Disable WLAN

Number of WLANs selected : 0

<input type="checkbox"/>	Status	Name	ID
--------------------------	--------	------	----

Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode None Lobby Admin Access

MAC Filtering Fast Transition Adaptive Enab...

OWE Transition Mode Over the DS

Authorization List* CLUS-AuthZ-Meth-l Reassociation Timeout 20

Cancel Apply to Device

Erstellen des Richtlinienprofils und des Richtlinien-Tags auf dem externen WLC

Rufen Sie die externe WLC-Webbenutzeroberfläche auf.

Um das Richtlinienprofil zu erstellen, gehen Sie zu **Configuration>Tags & Profiles>Policy>+Add**

Beim Verankern müssen Sie das zentrale Switching verwenden.

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Tags & Profiles > Policy**. The **+ Add** button is highlighted. The **Add Policy Profile** dialog box is open, showing the **General** tab. The **Status** is set to **ENABLED**. The **WLAN Switching Policy** section is expanded, showing **Central Switching**, **Central Authentication**, **Central DHCP**, and **Central Association** all set to **ENABLED**. The **Flex NAT/PAT** option is set to **DISABLED**. The **CTS Policy** section shows **Inline Tagging** and **SGACL Enforcement** as unchecked, and **Default SGT** as **2-65519**. The **Apply to Device** button is visible at the bottom right.

Auf der Registerkarte "**Erweitert**" sind AAA-Überschreibungen und RADIUS NAC für CWA obligatorisch. Hier können Sie auch die Accounting-Methodenliste anwenden, wenn Sie eine wählen.

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add 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) 60

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

NAC Type RADIUS

Policy Name default-aaa-policy x

Accounting List CLUS-Acct-Meth-x

Fabric Profile Search or Select

mDNS Service Policy Search or Select

Hotspot Server Search or Select

User Private Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map Not Configured Clear

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

Aktivieren Sie auf der Registerkarte "Mobilität" **NICHT** das Kontrollkästchen "Exportanker", sondern fügen Sie den Anker-WLC zur Ankerliste hinzu. Klicken Sie auf "Apply to Device" (Auf Gerät anwenden). Zur Erinnerung: Es wird davon ausgegangen, dass Sie bereits einen Mobility Tunnel zwischen den beiden Controllern eingerichtet haben.

Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add × Delete

Status Policy Profile Name Description

Add Policy Profile

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

Mobility Anchors

Export Anchor

Static IP Mobility **DISABLED**

Adding Mobility Anchors will cause the enabled VLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (0)

Anchor IP

No anchors available

Selected (1)

Anchor IP	Anchor Priority
192.168.160.18	Primary (1)

Cancel Apply to Device

Damit die APs dieses Richtlinienprofil verwenden können, müssen Sie ein Richtlinien-Tag

erstellen und auf die APs anwenden, die Sie verwenden möchten.

Um das Richtlinien-Tag zu erstellen, gehen Sie zu **Configuration>Tags & Profiles>Tags?Richtlinie>+Hinzufügen**

The screenshot shows the Cisco Catalyst 9800-L Wireless Controller configuration interface. The breadcrumb navigation path is **Configuration > Tags & Profiles > Tags**. The main menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The 'Policy' tab is selected, and the '+ Add' button is highlighted. The 'Add Policy Tag' dialog box is open, showing the following fields and options:

- Name***: CLUS-Policy-Tag
- Description**: Policy Tag for CLUS
- WLAN-POLICY Maps: 0**
- WLAN Profile**: CLUS-WLAN-Name
- Policy Profile**: CLUS-Policy-Profile
- Map WLAN and Policy**: A table with columns for WLAN Profile and Policy Profile, showing 0 items per page and 'No items to display'.
- WLAN Profile***: CLUS-WLAN-Name
- Policy Profile***: CLUS-Policy-Profile
- RLAN-POLICY Maps: 0**
- Buttons**: '+ Add', 'Delete', 'Cancel', and 'Apply to Device'.

Um dies mehreren APs gleichzeitig hinzuzufügen, gehen Sie zu **Configuration>Wireless Setup>Advanced>Start Now**. Klicken Sie auf die Aufzählungsbalken neben "Tag APs", und fügen Sie den gewünschten APs das Tag hinzu.

Configuration > Wireless Setup > Advanced

+ Tag APs

Number of APs: 3
Selected Number of APs: 3

AP Name	AP Model	AP MAC	AP Mode
<input checked="" type="checkbox"/> Jays2800	AIR-AP2802I-B-K9	002a.10f3.6b60	Local
<input checked="" type="checkbox"/> Jays3800	AIR-AP3802I-B-K9	70b3.1755.0520	Local
<input checked="" type="checkbox"/> AP0062.ec20.122c	AIR-CAP2702I-B-K9	cc16.7e6c.3cf0	Local

1 10 items per page

Tag APs

Tags

Policy:

Site:

RF:

Changing AP Tag(s) will cause associated AP(s) to reconnect

Cancel Apply to Device

Erstellen Sie das Richtlinienprofil auf dem Anker-WLC.

Gehen Sie zur WLC-Webbenutzeroberfläche mit Anker. Fügen Sie unter **Configuration>Tags & Profiles>Tags>Policy>+Add** das Richtlinienprofil für den Anker 9800 hinzu. Vergewissern Sie sich, dass dies mit dem Richtlinienprofil im Ausland übereinstimmt, mit Ausnahme der Registerkarte "Mobilität" und der Accounting-Liste.

Sie fügen hier keinen Anker hinzu, aktivieren aber das Kontrollkästchen "Anker exportieren". Fügen Sie hier nicht die Accounting-Liste hinzu. Zur Erinnerung: Es wird davon ausgegangen, dass Sie bereits einen Mobility Tunnel zwischen den beiden Controllern eingerichtet haben.

Anmerkung: Es gibt keinen Grund, dieses Profil einem WLAN in einem Richtlinien-Tag zuzuordnen. Dies führt bei Bedarf zu Problemen. Wenn Sie dasselbe WLAN für APs in diesem WLC verwenden möchten, erstellen Sie ein anderes Richtlinienprofil für dieses WLAN.

← Cisco 17.2.1 Cisco Catalyst 9800-L Wireless Controller

Configuration > Tags & Profiles > Policy

+ Add × Delete

Add Policy Profile

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

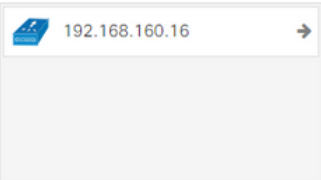
Mobility Anchors

Export Anchor

Static IP Mobility DISABLED

Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (1)	Selected (0)	
Anchor IP	Anchor IP	Anchor Priority
 192.168.160.16 →	Anchors not assigned	

Cancel Apply to Device

Umleiten der ACL-Konfiguration auf beiden 9800s

Als Nächstes müssen Sie die Umleitungskonfiguration für die ACL auf beiden 9800er-Geräten erstellen. Die Einträge im Ausland sind unerheblich, da es sich um den Anker-WLC handelt, der die ACL auf den Datenverkehr anwendet. Die einzige Voraussetzung ist, dass es vorhanden ist und einen Eintrag hat. Die Einträge auf dem Anker müssen den Zugriff auf die ISE an Port 8443 "verweigern" und alles andere "zulassen". Diese ACL wird nur auf Datenverkehr angewendet, der vom Client "eingeht", sodass keine Regeln für den Rückverkehr erforderlich sind. DHCP und DNS werden ohne Einträge in der ACL weitergeleitet.

Cisco Catalyst 9800-L Wireless Controller 17.2.1 Welcome admin
Last login None

Configuration > Security > ACL

+ Add × Delete Associate Interfaces

Add ACL Setup

ACL Name* ACL Type

Rules

Sequence* Action

Source Type

Destination Type

Protocol

Log DSCP

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 10	deny	any		192.168.160.99		tcp	None	eq 8443	None	Disabled
<input type="checkbox"/> 100	permit	any		any		ip	None	None	None	Disabled

10 items per page 1 - 2 of 2 items

Cancel Apply to Device

ISE konfigurieren

Der letzte Schritt ist die Konfiguration der ISE für CWA. Für dieses Beispiel gibt es zahlreiche Optionen, in diesem Beispiel werden jedoch die Grundlagen beibehalten und das standardmäßig selbst registrierte Gastportal verwendet.

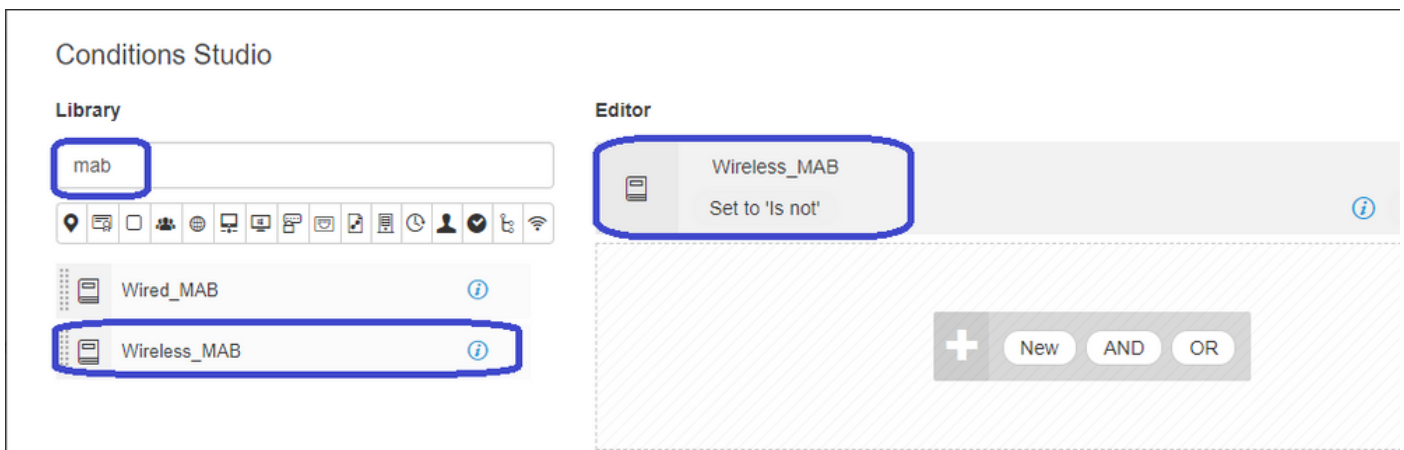
Auf der ISE müssen Sie ein Autorisierungsprofil, einen Richtlinienatz mit einer Authentifizierungsrichtlinie und einer Autorisierungsrichtlinie erstellen, die das Autorisierungsprofil verwendet, die 9800(fremd) zur ISE als Netzwerkgerät hinzufügen und einen Benutzernamen und ein Kennwort für die Anmeldung am Netzwerk erstellen.

Um das Autorisierungsprofil zu erstellen, gehen Sie zu **Richtlinien > Richtlinienelemente > Autorisierung > Ergebnisse > Autorisierungsprofile > +Hinzufügen**. Stellen Sie sicher, dass der zurückgegebene Zugriffstyp "access_accept" lautet, und legen Sie dann die AVPs (Attribut-Wert-Paare) fest, die Sie zurücksenden möchten. Für CWA sind die Umleitungs-ACL und die Umleitungs-URL obligatorisch, Sie können jedoch auch Dinge wie VLAN-ID und Sitzungs-Timeout zurücksenden. Es ist wichtig, dass der ACL-Name mit dem Namen der Umleitungszugriffskontrollliste auf dem Fremd- und dem Anker 9800 übereinstimmt.

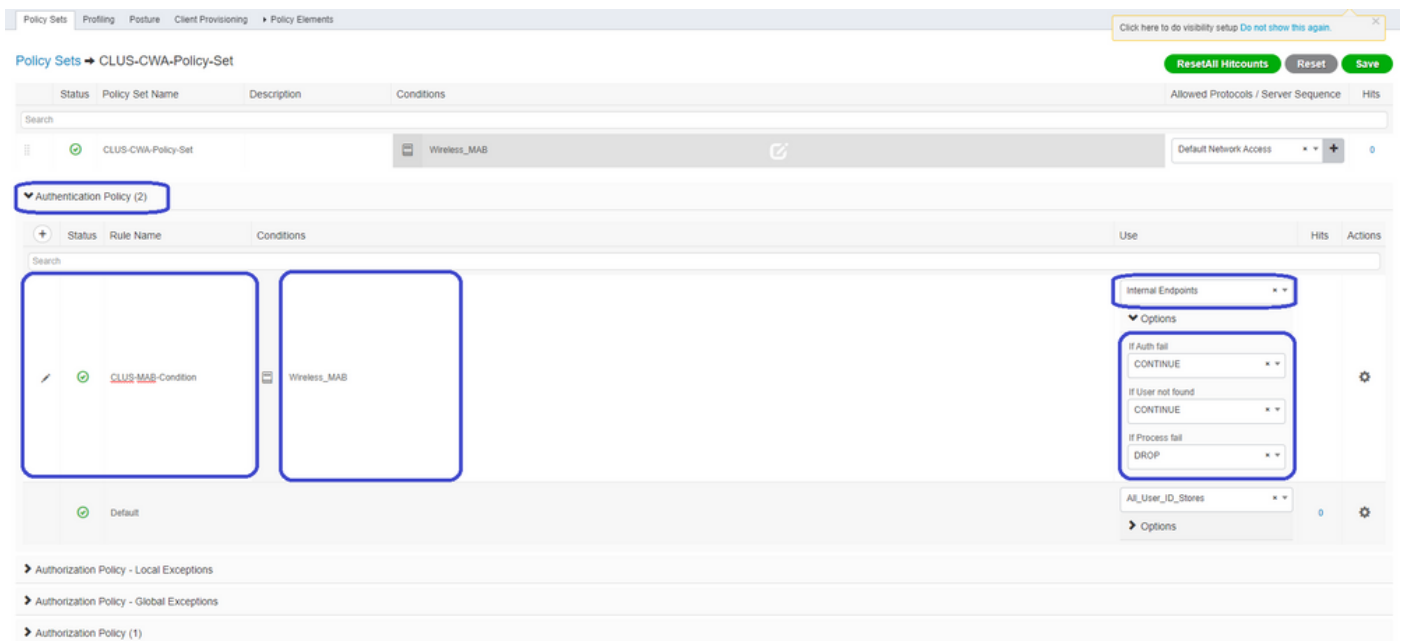
Anschließend müssen Sie eine Möglichkeit konfigurieren, das soeben erstellte Autorisierungsprofil auf die Clients anzuwenden, die CWA durchlaufen. Dazu können Sie einen Richtlinienatz erstellen, der die Authentifizierung bei Verwendung von MAB umgeht, und das Autorisierungsprofil bei Verwendung der in der angerufenen Station-ID gesendeten SSID anwenden. Auch hier gibt es viele Möglichkeiten, dies zu erreichen. Wenn Sie also etwas Spezifischeres oder Sichereres brauchen, dann ist das nur der einfachste Weg.

Um den Richtlinienatz zu erstellen, gehen Sie zu **Policy>Policy Sets**, und drücken Sie auf der linken Seite des Bildschirms die Schaltfläche +. Nennen Sie den neuen Richtlinienatz, und stellen Sie sicher, dass er auf "default network access" (Standard-Netzwerkzugriff) oder eine beliebige zulässige Protokollliste gesetzt ist, die "Process Host Lookup" für MAB(ermöglicht, die zulässige Protokollliste zu überprüfen, gehen Sie zu Policy>Policy Elements>Results>Authentication>Allowed Protocols). Drücken Sie jetzt das +-Zeichen in der Mitte des neuen Richtlinienatzes, den Sie erstellt haben.

Für diesen Richtlinienatz wird jedes Mal, wenn MAB in der ISE verwendet wird, dieser Richtlinienatz angewendet. Später können Sie Autorisierungsrichtlinien festlegen, die mit der angerufenen Station-ID übereinstimmen, sodass je nach verwendetem WLAN unterschiedliche Ergebnisse angewendet werden können. Dieser Prozess ist sehr anpassbar, mit einer Vielzahl von Dingen, die Sie abgleichen können.



Erstellen Sie im Richtlinienatz die Richtlinien. Die Authentifizierungsrichtlinie kann auf der MAB erneut übereinstimmen. Sie müssen jedoch den ID-Speicher so ändern, dass "interne Endpunkte" verwendet werden. Außerdem müssen die Optionen geändert werden, damit die Authentifizierung fehlschlägt und der Benutzer nicht gefunden wird.



Nachdem die Authentifizierungsrichtlinie festgelegt wurde, müssen Sie in der Autorisierungsrichtlinie zwei Regeln erstellen. Diese Richtlinie liest sich wie eine ACL, sodass die Regel nach der Authentifizierung oben und die Regel vor der Autorisierung unten angezeigt werden müssen. Die Regel nach der Autorisierung vergleicht Benutzer, die bereits einen Gastdatenfluss durchlaufen haben. Das heißt, wenn sie bereits angemeldet sind, werden sie diese Regel treffen und dort aufhören. Wenn sie sich nicht angemeldet haben, werden sie die Liste weiter herunterfahren und die Vorauth-Regel für die Umleitung drücken. Es empfiehlt sich, die Autorisierungsrichtlinien mit der angerufenen Station-ID abzugleichen, die mit der SSID endet, sodass sie nur auf WLANs zutrifft, die dafür konfiguriert sind.

Status	Policy Set Name	Description	Conditions	Results	Security Groups
✓	CLUS-CWA-Policy-Set		Wireless_MAB		Default Network Access
Authentication Policy (2) Authorization Policy - Local Exceptions Authorization Policy - Global Exceptions Authorization Policy (4)					
+	Status	Rule Name	Conditions	Results	Security Groups
+	✓	Post-CWA	AND Network Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	Select from list
+	✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	Select from list
+	✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	Select from list
+	✓	Default		DenyAccess	Select from list

Nachdem der Richtlinienatz konfiguriert wurde, müssen Sie die ISE über den 9800 (ausländisch) informieren, damit die ISE ihr als Authentifizierer vertrauen kann. Dies kann unter **Admin>Network Resources>Network Device>+** erfolgen. Sie müssen den Namen eingeben, die IP-Adresse (oder in diesem Fall das gesamte Admin-Subnetz) festlegen, RADIUS aktivieren und den gemeinsamen geheimen Schlüssel festlegen. Das gemeinsam genutzte Geheimnis der ISE muss mit dem gemeinsam genutzten geheimen Schlüssel des 9800 übereinstimmen. Andernfalls schlägt dieser Prozess fehl. Nachdem die Konfiguration hinzugefügt wurde, drücken Sie die Schaltfläche zum Senden, um sie zu speichern.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device
Device Security Settings

Network Devices List > JaysNet

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

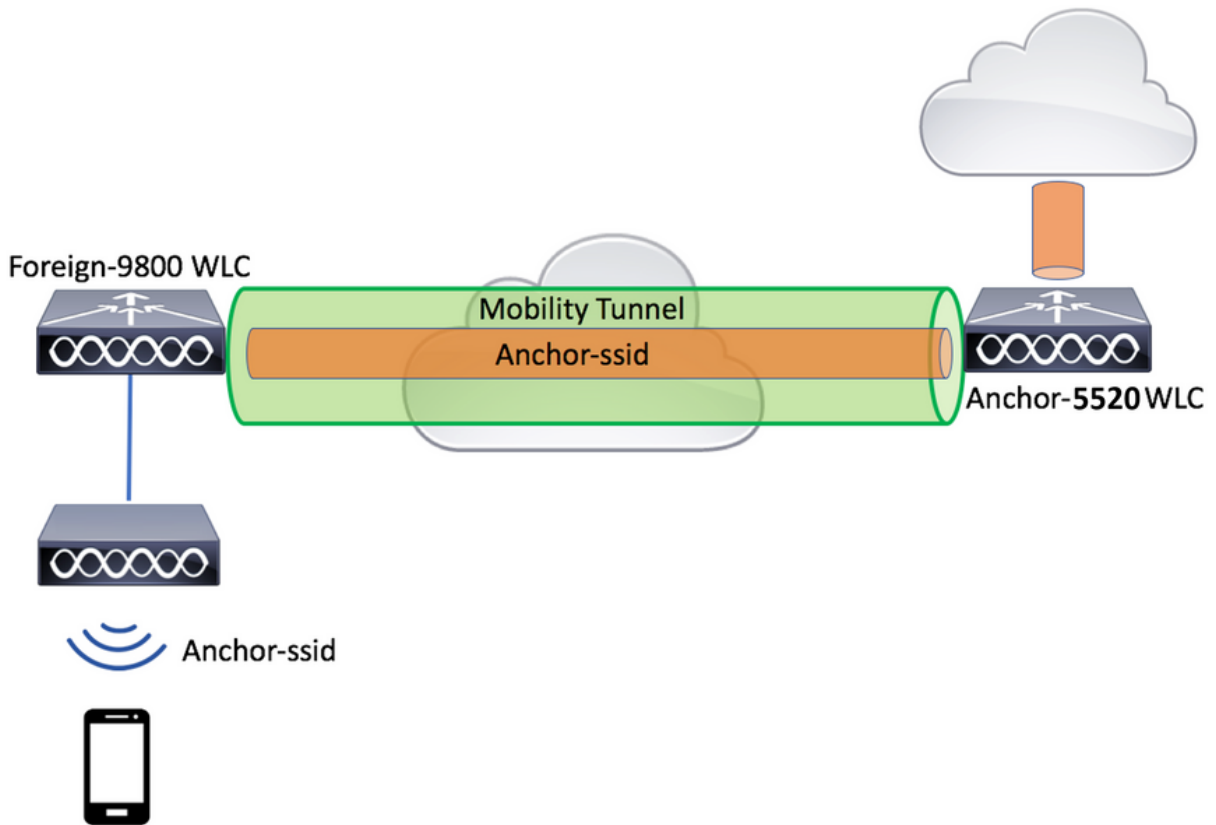
Schließlich müssen Sie den Benutzernamen und das Kennwort hinzufügen, die der Client auf der Anmeldeseite eingeben wird, um zu überprüfen, ob er Zugriff auf das Netzwerk haben soll. Dies erfolgt unter **Admin>Identity Management>Identity>Users>+Add**, und klicken Sie nach dem Hinzufügen auf Submit (Senden). Wie bei allen anderen ISE-Lösungen ist auch diese benutzerdefinierbar und muss kein lokal gespeicherter Benutzer sein, sondern die einfachste Konfiguration.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Identity Management' section is expanded to show 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Users' section is selected, and the 'New Network Access User' configuration page is shown. The page is divided into several sections:

- Network Access User:** The 'Name' field is set to 'CLUS-User'. The 'Status' is 'Enabled'. The 'Email' field is empty.
- Passwords:** The 'Password Type' is 'Internal Users'. The 'Login Password' and 'Re-Enter Password' fields are filled with masked characters. There are 'Generate Password' buttons next to each password field.
- User Information:** The 'First Name' and 'Last Name' fields are empty.
- Account Options:** The 'Description' field is empty. The 'Change password on next login' checkbox is unchecked.
- Account Disable Policy:** The 'Disable account if date exceeds' checkbox is unchecked. The date is set to '2020-07-17' (yyyy-mm-dd).
- User Groups:** The 'Select an item' dropdown menu is empty.

The 'Submit' button is highlighted in blue.

Konfigurieren eines Catalyst 9800, verankert in einem AireOS WLC



Catalyst 9800 - Fremdkonfiguration

Führen Sie die gleichen Schritte aus wie zuvor, und überspringen Sie den Abschnitt "Erstellen Sie das Richtlinienprofil für den Anker-WLC".

AAA-Konfigurationen auf dem Anker AireOS WLC

Fügen Sie den Server zum WLC hinzu, indem Sie **Security>AAA>RADIUS>Authentication>New wählen**. Fügen Sie die Server-IP-Adresse, den gemeinsamen geheimen Schlüssel und die CoA-Unterstützung hinzu.

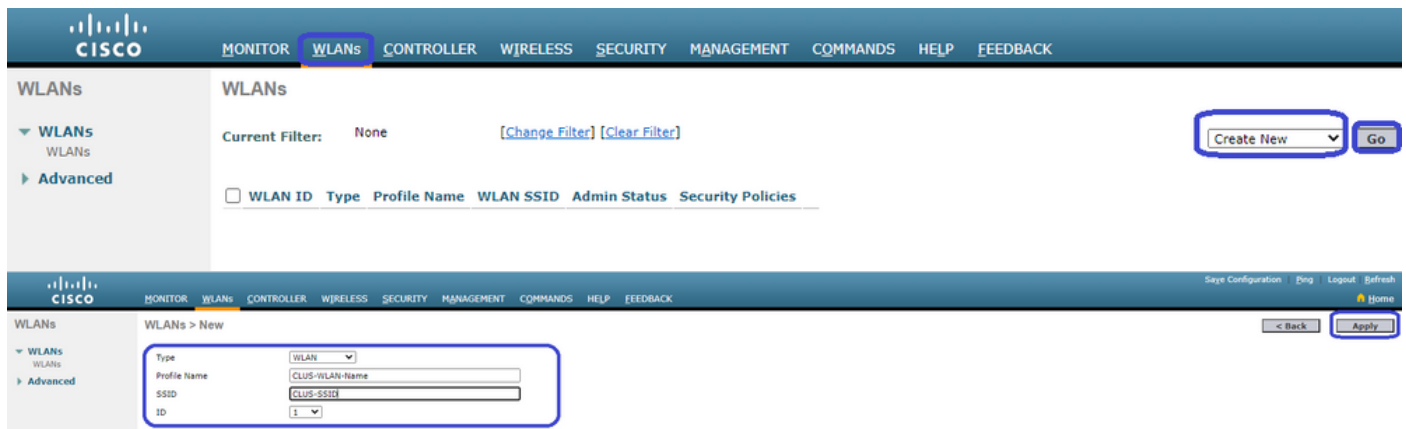
The first screenshot shows the Cisco Catalyst 9800 configuration interface for RADIUS Authentication Servers. The 'Auth Called Station ID Type' is set to 'AP MAC Address:SSID'. The 'Use AES Key Wrap' checkbox is unchecked. The 'MAC Delimiter' is set to 'Hyphen' and the 'Framed MTU' is set to '1300'. A table with columns for Network User, Management, Tunnel Proxy, Server Index, Server Address(Ipv4/Ipv6), Port, IPsec, and Admin Status is visible.

The second screenshot shows the 'RADIUS Authentication Servers > New' configuration page. The 'Server Index (Priority)' is set to '1'. The 'Server IP Address(Ipv4/Ipv6)' is '192.168.160.99'. The 'Shared Secret Format' is 'ASCII' and the 'Shared Secret' is masked with asterisks. The 'Confirm Shared Secret' field is also masked. The 'Apply Cisco ISE Default settings' checkbox is checked. The 'Key Wrap' checkbox is unchecked. The 'Port Number' is '1812' and the 'Server Status' is 'Enabled'. The 'Support for CoA' is set to 'Enabled'. The 'Server Timeout' is '5' seconds. The 'Network User' checkbox is checked. The 'Management' checkbox is checked. The 'Management Retransmit Timeout' is '5' seconds. The 'Tunnel Proxy' checkbox is unchecked. The 'PAC Provisioning' checkbox is unchecked. The 'IPsec' checkbox is unchecked.

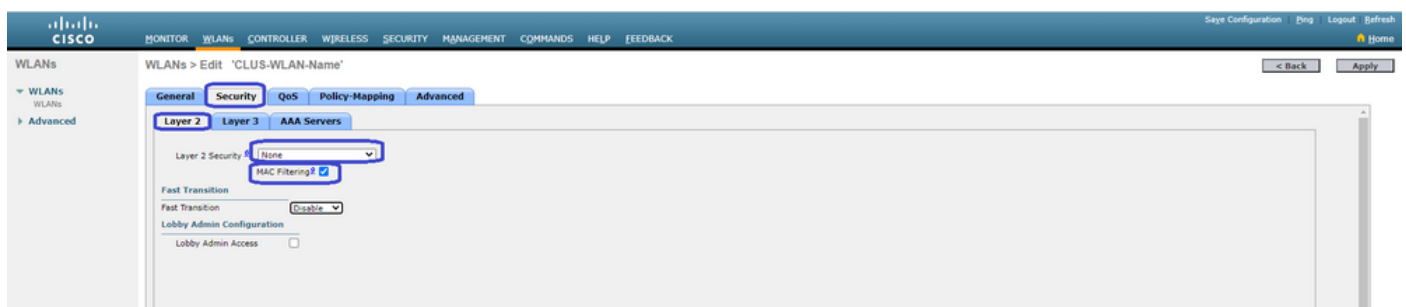
WLAN-Konfiguration auf dem AireOS WLC

Um das WLAN zu erstellen, gehen Sie zu **WLANs>Create New>Go**.

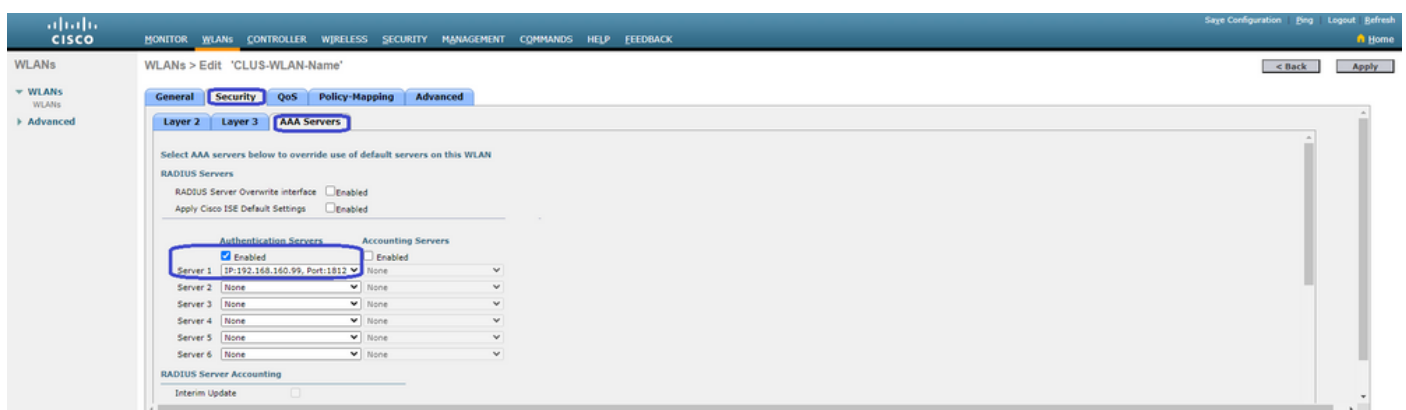
Konfigurieren Sie den Profilnamen, die WLAN-ID und die SSID, und klicken Sie auf "Apply" (Anwenden).



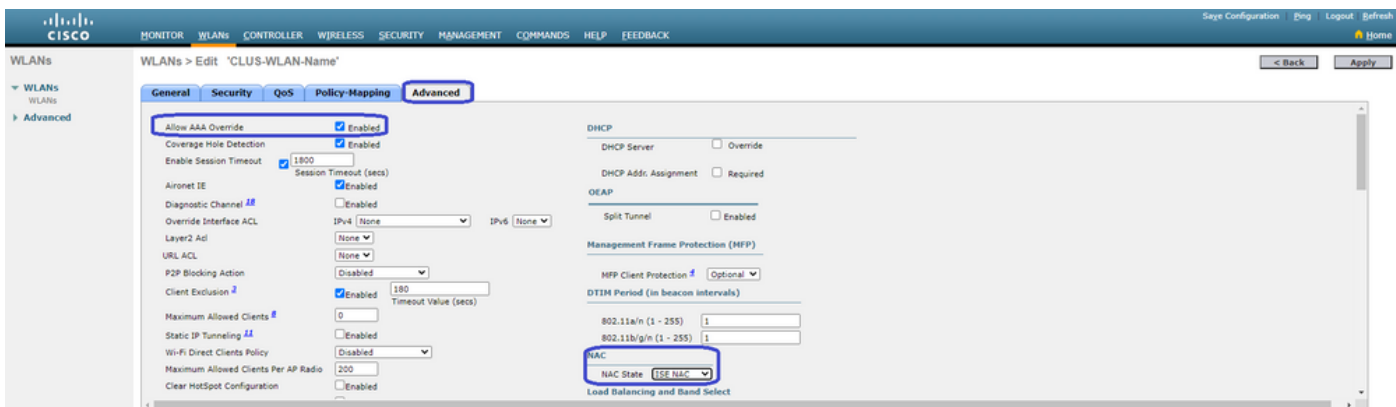
Dadurch gelangen Sie zur WLAN-Konfiguration. Auf der Registerkarte "Allgemein" können Sie die Schnittstelle hinzufügen, die die Clients verwenden sollen, wenn Sie die ISE nicht so konfigurieren möchten, dass sie in den AVPs gesendet wird. Wechseln Sie anschließend zum Register **Security>Layer2** und stimmen Sie mit der Konfiguration für Layer-2-Sicherheit überein, die Sie auf dem 9800 verwendet haben, und aktivieren Sie "MAC-Filterung".



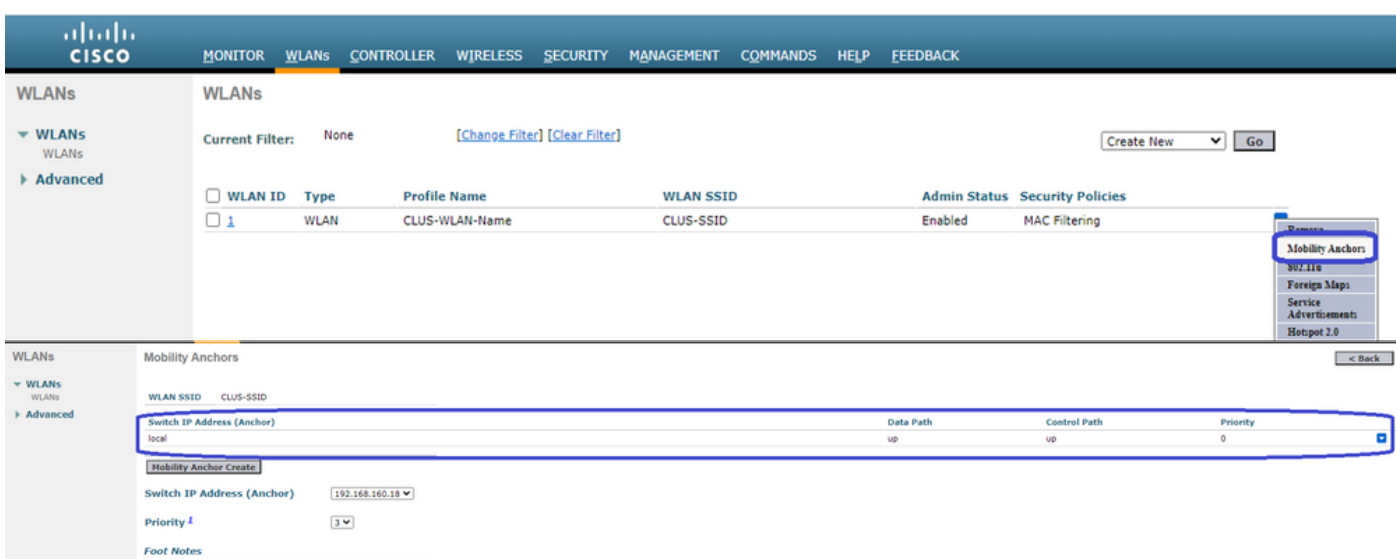
Wechseln Sie nun zur Registerkarte **Security>AAA Servers** und setzen Sie den ISE-Server als "Authentication Servers" ein. Legen Sie **keine** Einstellungen für die "Buchhaltungsserver" fest. Deaktivieren Sie das Kontrollkästchen "Aktivieren" für die Rechnungsstellung.



Wechseln Sie zur Registerkarte **Erweitert**, und aktivieren Sie "AAA-Außerkräftsetzung zulassen", und ändern Sie den "NAC-Status" in "ISE NAC".

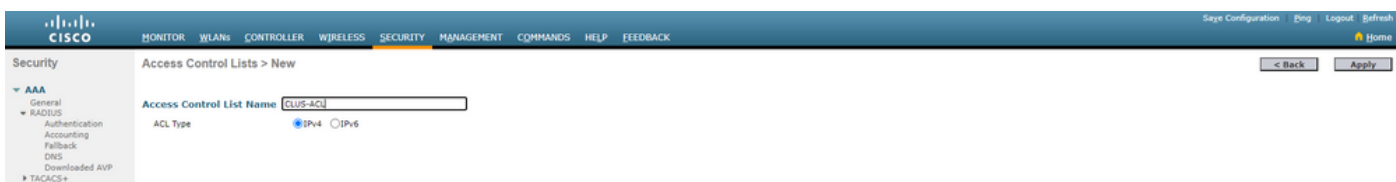


Das Letzte ist, es selbst zu verankern. Gehen Sie zurück zur **WLANs**-Seite, und bewegen Sie den Mauszeiger über das blaue Kästchen rechts neben WLAN>Mobility Anchors. Legen Sie "Switch IP Address (Anchor)" auf local fest, und drücken Sie die Schaltfläche "Mobility Anchor Create" (Mobility-Anker erstellen). Es sollte dann mit der Priorität 0 lokal verankert angezeigt werden.



Umleitung der ACL auf dem AireOS WLC

Dies ist die letzte erforderliche Konfiguration für den AireOS WLC. Um die Umleitungsliste zu erstellen, gehen Sie zu **Security>Access Control Lists>Access Control Lists>New**. Geben Sie den Namen der Zugriffskontrollliste ein (dieser muss mit dem in den AVPs gesendeten Inhalt übereinstimmen), und drücken Sie "Apply" (Anwenden).



Klicken Sie nun auf den Namen der gerade erstellten ACL. Klicken Sie auf die Schaltfläche Neue Regel hinzufügen. Im Gegensatz zum 9800 stellt der AireOS WLC eine Sicherheits-ACL dar, wenn sie auf den Client angewendet wird. Das heißt, wir müssen den Datenverkehr zur ISE **zulassen** und den Rückverkehr zulassen. DHCP und DNS sind standardmäßig zulässig.

Security

Access Control Lists > Edit

General

Access List Name: CLUS-ACL

Deny Counters: 5

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.160.99 / 255.255.255.255	TCP	Any	8443	Any	Any	273
2	Permit	192.168.160.99 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	566

ISE konfigurieren

Der letzte Schritt ist die Konfiguration der ISE für CWA. Für dieses Beispiel gibt es zahlreiche Optionen, in diesem Beispiel werden jedoch die Grundlagen beibehalten und das standardmäßig selbst registrierte Gastportal verwendet.

Auf der ISE müssen Sie ein Autorisierungsprofil, einen Richtlinienatz mit einer Authentifizierungsrichtlinie und einer Autorisierungsrichtlinie erstellen, die das Autorisierungsprofil verwendet, die 9800(fremd) zur ISE als Netzwerkgerät hinzufügen und einen Benutzernamen und ein Kennwort für die Anmeldung am Netzwerk erstellen.

Um das Autorisierungsprofil zu erstellen, gehen Sie **zu Richtlinien > Richtlinienelemente > Autorisierung > Ergebnisse > Autorisierungsprofile > +Hinzufügen**. Stellen Sie sicher, dass der zurückgegebene Zugriffstyp "access_accept" lautet, und legen Sie dann die AVPs (Attribut-Wert-Paare) fest, die Sie zurücksenden möchten. Für CWA sind die Umleitungs-ACL und die Umleitungs-URL obligatorisch, Sie können jedoch auch Dinge wie VLAN-ID und Sitzungs-Timeout zurücksenden. Es ist wichtig, dass der ACL-Name mit dem Namen der Umleitungszugriffskontrollliste auf dem Fremd- und dem Anker-WLC übereinstimmt.

← → ↻ Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element

Identity Services Engine

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

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Authentication Profiles > test

Authorization Profile

* Name: CLUS-AuthZ-Profile-ISE

Description: []

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: []

Track Movement: []

Passive Identity Tracking: []

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) []

Centralized Web Auth ACL: CLUS-ACL Value: Self-Registered Guest Portal []

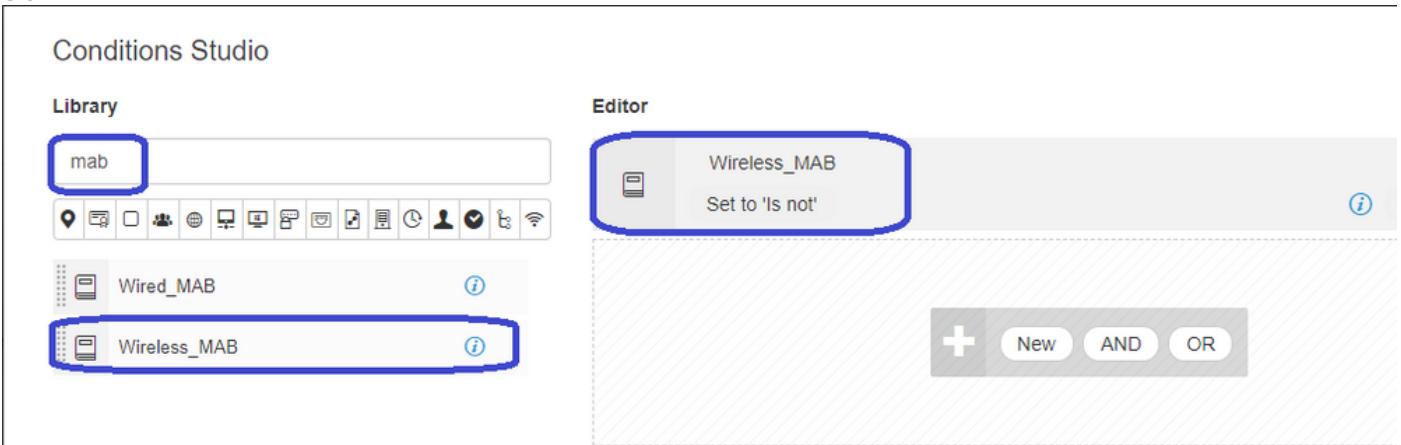
Anschließend müssen Sie eine Möglichkeit konfigurieren, das soeben erstellte Autorisierungsprofil auf die Clients anzuwenden, die

CWA durchlaufen. Dazu können Sie einen Richtlinienatz erstellen, der die Authentifizierung bei Verwendung von MAB umgeht, und das Autorisierungsprofil bei Verwendung der in der angerufenen Station-ID gesendeten SSID anwenden. Auch hier gibt es viele Möglichkeiten, dies zu erreichen. Wenn Sie also etwas Spezifischeres oder Sichereres brauchen, dann ist das nur der einfachste Weg.

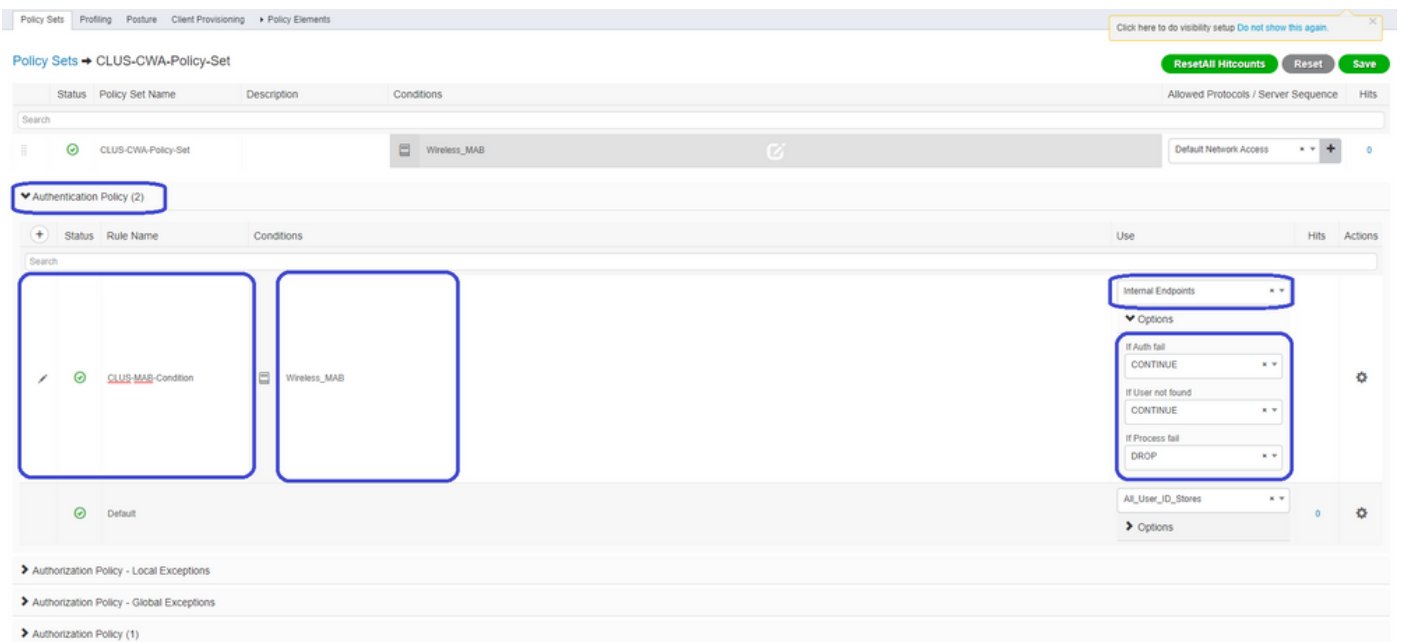
Um den Richtlinienatz zu erstellen, gehen Sie zu **Policy>Policy Settings**, und drücken Sie auf der linken Seite des Bildschirms die Taste +. Nennen Sie den neuen Richtlinienatz, und stellen Sie sicher, dass er auf "default network access" (Standard-Netzwerkzugriff) oder eine beliebige zulässige Protokollliste gesetzt ist, die "Process Host Lookup" für MAB(ermöglicht, die zulässige Protokollliste zu überprüfen, gehen Sie zu **Policy>Policy Elements>Results>Authentication>Allowed Protocols**). Drücken Sie jetzt das +-Zeichen in der Mitte des neuen Richtlinienatzes, den Sie erstellt haben.



Für diesen Richtlinienatz wird jedes Mal, wenn MAB in der ISE verwendet wird, dieser Richtlinienatz angewendet. Später können Sie Autorisierungsrichtlinien festlegen, die mit der angerufenen Station-ID übereinstimmen, sodass je nach verwendetem WLAN unterschiedliche Ergebnisse angewendet werden können. Dieser Prozess kann mit einer Vielzahl von Elementen individuell angepasst werden, die Sie



Erstellen Sie im Richtlinienatz die Richtlinien. Die Authentifizierungsrichtlinie kann auf der MAB erneut übereinstimmen. Sie müssen jedoch den ID-Speicher so ändern, dass "interne Endpunkte" verwendet werden. Außerdem müssen die Optionen geändert werden, damit die Authentifizierung fehlschlägt und der Benutzer nicht gefunden wird.



Nachdem die Authentifizierungsrichtlinie festgelegt wurde, müssen Sie in der Autorisierungsrichtlinie zwei Regeln erstellen. Diese Richtlinie liest sich wie eine ACL, sodass die Regel nach der Authentifizierung oben und die Regel vor der Autorisierung unten angezeigt werden müssen. Die Regel nach der Autorisierung vergleicht Benutzer, die bereits einen Gastdatenfluss durchlaufen haben. Das heißt, wenn sie bereits angemeldet sind, werden sie diese Regel treffen und dort aufhören. Wenn sie sich nicht angemeldet haben, werden sie die Liste weiter herunterfahren und die Vorauth-Regel für die Umleitung drücken. Es empfiehlt sich, die Autorisierungsrichtlinien mit der angerufenen Station-ID abzugleichen, die mit der SSID endet, sodass sie nur auf WLANs zutrifft, die dafür konfiguriert sind.

Policy Sets → CLUS-CWA-Policy-Set Reset All Hitcounts

Allowed Protocols / Server S

Status	Policy Set Name	Description	Conditions	Results	Profiles	Security Groups
✓	CLUS-CWA-Policy-Set		Wireless_MAB			Default Network Access
<p>Authentication Policy (2)</p> <p>Authorization Policy - Local Exceptions</p> <p>Authorization Policy - Global Exceptions</p> <p>Authorization Policy (4)</p>						
+	Status	Rule Name	Conditions	Results	Profiles	Security Groups
+	✓	Post-CWA	AND Network.Access UseCase EQUALS Guest Flow Radius Called-Station-ID ENDS_WITH CLUS-SSID	CLUS-Post-Auth	+	Select from list
	✓	MAB on WLAN	AND Radius Called-Station-ID ENDS_WITH CLUS-SSID Wireless_MAB	CLUS-AuthZ-Profile-ISE	+	Select from list
	✓	Flex AuthZ	Radius Called-Station-ID ENDS_WITH FLEX-CWA	CLUS-Flex_CWA	+	Select from list
	✓	Default		DenyAccess	+	Select from list

Nachdem der Richtliniensatz konfiguriert wurde, müssen Sie die ISE über den 9800 (ausländisch) informieren, damit die ISE ihr als Authentifizierer vertrauen kann. Dies kann unter **Admin > Netzwerkressourcen > Netzwerkgerät > +** Sie müssen den Namen eingeben, die IP-Adresse (oder in diesem Fall das gesamte Admin-Subnetz) festlegen, RADIUS aktivieren und den gemeinsamen geheimen Schlüssel festlegen. Das gemeinsam genutzte Geheimnis der ISE muss mit dem gemeinsam genutzten geheimen Schlüssel des 9800 übereinstimmen. Andernfalls schlägt dieser Prozess fehl. Nachdem die Konfiguration hinzugefügt wurde, drücken Sie die Schaltfläche zum Senden, um sie zu speichern.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

Default Device

Device Security Settings

Network Devices List > JaysNet

Network Devices

* Name

Description

IP Address * IP:

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings

Schließlich müssen Sie den Benutzernamen und das Kennwort hinzufügen, die der Client auf der Anmeldeseite eingeben wird, um zu überprüfen, ob er Zugriff auf das Netzwerk haben soll. Dies geschieht unter **Admin > Identitätsverwaltung > Identität > Benutzer > +Hinzufügen** und klicken Sie auf Submit (Senden), nachdem Sie sie hinzugefügt haben. Wie bei allen anderen ISE-Lösungen ist auch diese benutzerdefinierbar und muss kein lokal gespeicherter Benutzer sein, sondern die einfachste Konfiguration.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The current page is 'Network Access Users List > New Network Access User'. The form contains the following sections:

- Network Access User:**
 - * Name: CLUS-User
 - Status: Enabled
 - Email: [Empty field]
- Passwords:**
 - Password Type: Internal Users
 - * Login Password: [Masked with dots]
 - Re-Enter Password: [Masked with dots]
 - Enable Password: [Empty field]
- User Information:**
 - First Name: [Empty field]
 - Last Name: [Empty field]
- Account Options:**
 - Description: [Empty field]
 - Change password on next login:
- Account Disable Policy:**
 - Disable account if date exceeds 2020-07-17 (yyyy-mm-dd)
- User Groups:**
 - Select an item [Dropdown menu]

At the bottom, there are 'Submit' and 'Cancel' buttons.

Unterschiede in der Konfiguration, wenn der AireOS-WLC der Fremdhersteller ist und der Catalyst 9800 der Auslöser ist

Wenn Sie möchten, dass der AireOs WLC der ausländische Controller ist, ist die Konfiguration identisch mit der vorherigen Konfiguration mit nur zwei Unterschieden.

1. Die AAA-Abrechnung erfolgt niemals am Anker, sodass der 9800 über keine Accounting-Methodenliste verfügt und der AireOS WLC die Accounting-Funktion aktiviert hätte und auf die ISE verweist.
2. Das AireOS müsste auf dem 9800-Gerät verankert werden, anstatt sich selbst zu bedienen. Im Richtlinienprofil des 9800-Geräts ist kein Anker ausgewählt, aber das Kontrollkästchen "Export Anchor" (Anker exportieren) ist aktiviert.
3. Beachten Sie, dass beim Exportieren von AireOS-WLCs in den 9800 kein Konzept für Richtlinienprofile existiert, sondern nur der WLAN-Profilname gesendet wird. Daher wendet der 9800 den von AireOS gesendeten WLAN-Profilnamen sowohl auf den WLAN-Profilnamen als auch auf den Richtlinienprofilnamen an. Bei der Verankerung von einem AireOS-WLC an einen 9800-WLC müssen jedoch der WLAN-Profilname auf beiden WLCs und der Name des Richtlinienprofils auf dem 9800 übereinstimmen.

Überprüfung

Um die Konfigurationen auf dem **9800 WLC** zu überprüfen, führen Sie die Befehle aus.

- AAA

```
Show Run | section aaa|radius
```

- WLAN

```
Show wlan id <wlan id>
```

- Richtlinienprofil

```
Show wireless profile policy detailed <profile name>
```

- Richtlinien-Tag

```
Show wireless tag policy detailed <policy tag name>
```

- ACL

```
Show IP access-list <ACL name>
```

- Überprüfen Sie, ob die Mobilität mit dem Anker verbunden ist.

```
Show wireless mobility summary
```

Führen Sie die Befehle aus, um die Konfigurationen auf dem AireOS WLC zu überprüfen.

- AAA

```
Show radius summary
```

Anmerkung: RFC3576 ist die CoA-Konfiguration.

- WLAN

```
Show WLAN <wlan id>
```

- ACL

```
Show acl detailed <acl name>
```

- Überprüfen Sie, ob die Mobilität mit dem Ausland verbunden ist.

```
Show mobility summary
```

Fehlerbehebung

Die Fehlerbehebung sieht je nach dem Punkt, an dem der Client anhält, anders aus. Wenn der WLC beispielsweise nie eine Antwort von der ISE auf der MAB erhält, bleibt der Client im "Policy Manager State: Zuordnen" und nicht in den Anker exportiert. In dieser Situation führen Sie nur

eine Fehlerbehebung für das Ausland durch, und Sie können eine RA-Ablaufverfolgung und eine Paketerfassung für den Datenverkehr zwischen dem WLC und der ISE sammeln. Ein weiteres Beispiel wäre, dass MAB erfolgreich übergeben wurde, aber der Client die Umleitung nicht erhält. In diesem Fall müssen Sie sicherstellen, dass der Fremdhersteller die Umleitung in den AVPs erhalten und auf den Client angewendet hat. Sie müssen auch den Anker überprüfen, um sicherzustellen, dass der Client mit der richtigen ACL vorhanden ist. Dieser Umfang der Fehlerbehebung ist nicht Bestandteil des Designs dieses technischen Dokuments (überprüfen Sie die Referenzen für allgemeine Richtlinien zur Client-Fehlerbehebung).

Weitere Hilfe bei der Fehlerbehebung für CWA auf dem 9800 WLC finden Sie in der Cisco Live! Präsentation: DGTL-TSCENT-404

Informationen zur Fehlerbehebung beim Catalyst 9800

Clientdetails

```
show wireless client mac-address
```

Hier sehen Sie "Policy Manager State", "Session Manager > Auth Method", "Mobility Role".

Sie finden diese Informationen auch in der GUI unter Monitoring>Clients

Integrierte Paketerfassung

Über die Kommandozeile startet der Befehl *#monitor capture <capture name>*, danach folgen die Optionen.

Gehen Sie in der GUI zu Troubleshoot>Packet Capture>+Add

RadioActive Traces

Über die CLI

```
debug wireless mac/ip
```

Beenden Sie den Befehl mit der Form no (Nein). Diese wird in einer Datei im Bootflash "ra_trace" protokolliert, dann in der MAC- oder IP-Adresse des Clients sowie in Datum und Uhrzeit.

Gehen Sie in der GUI zu Troubleshoot>Radioactive Trace>+Add. Fügen Sie die MAC- oder IP-Adresse des Clients hinzu, klicken Sie auf "Anwenden", und drücken Sie dann auf "Start".

Nachdem Sie den Prozess einige Male beendet haben, erstellen Sie das Protokoll und laden es auf Ihr Gerät herunter.

Informationen zur Fehlerbehebung in AireOS

Clientdetails

In der CLI zeigen Sie *Client-Details an*.

Über GUI Monitor>Clients

Debugger von der CLI

Debug client

Debug mobility handoff

Debug mobility config

Referenzen

[Gebäude für Mobility-Tunnel mit 9800 Controllern](#)

[Wireless-Debuggen und Protokollerfassung für 9800](#)