

# Überprüfung und Fehlerbehebung für kabelgebundenen Gast im Wireless LAN-Controller konfigurieren

## Inhalt

---

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie den kabelgebundenen Gastzugriff des 9800 und den IRCM mit externer Web-Authentifizierung konfigurieren, überprüfen und Fehler beheben.

## Voraussetzungen

### Anforderungen

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

9800 WLC

AireOS-WLC

Mobility-Tunnel

ISE

Es wird davon ausgegangen, dass vor der Konfiguration des kabelgebundenen Gastzugriffs ein Mobility Tunnel zwischen den beiden WLCs eingerichtet wurde.

Dieser Aspekt wird in diesem Konfigurationsbeispiel nicht behandelt. Detaillierte Anweisungen finden Sie im beigefügten Dokument mit dem Titel [Configuring Mobility Topology on 9800 \(Konfigurieren von Mobilitätstopologien für 9800\)](#).

### Verwendete Komponenten

9800 WLC Version 17.12.1

5520 WLC Version 8.10.185.0

ISE Version 3.1.0.518

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 von Wired Guest auf Catalyst 9800, verankert in einem anderen Catalyst 9800

Netzwerkdiagramm



Netzwerktopologie

## Konfiguration auf dem 9800 WLC

Webparameterzuordnung konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Security > Web Auth, wählen Sie Global aus, überprüfen Sie die virtuelle IP-Adresse des Controllers und die Vertrauenspunktzuordnung, und stellen Sie sicher, dass der Typ auf webauth eingestellt ist.

Parameter Map Name

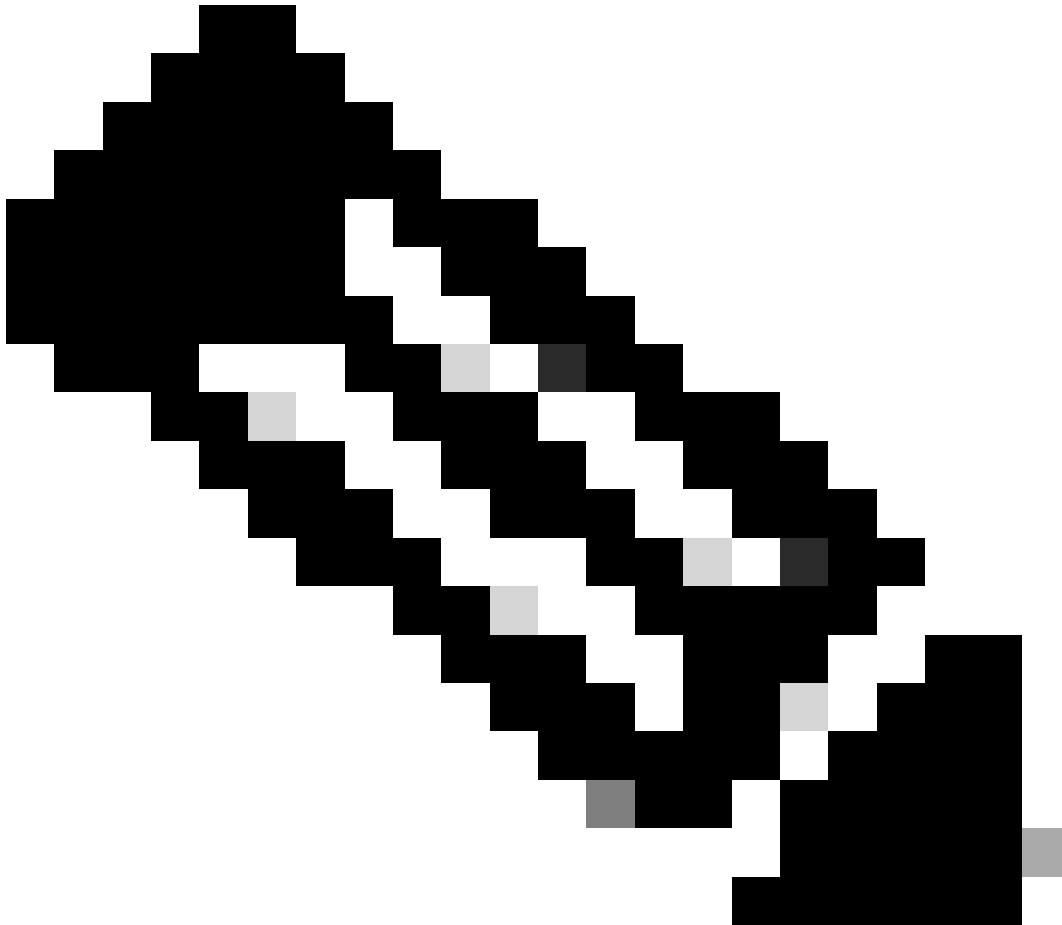
- global
- Web-Filter

1 10

**General** Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	<b>Banner Configuration</b>	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

Globale Parameterzuordnung



Hinweis: Web Auth Intercept-HTTPSs sind eine optionale Einstellung. Wenn HTTPS-Umleitung erforderlich ist, muss die Option Web Auth intercept HTTPS aktiviert sein. Diese Konfiguration wird jedoch nicht empfohlen, da sie die CPU-Auslastung erhöht.

Schritt 2: Konfigurieren Sie auf der Registerkarte Erweitert die URL der externen Webseite für die Client-Umleitung. Legen Sie "Redirect URL for Login" (URL für Anmeldung umleiten) und "Redirect On-Failure" (Bei Fehler umleiten) fest. "Redirect On-Success" ist optional. Nach der Konfiguration wird im Web Auth-Profil eine Vorschau der Umleitungs-URL angezeigt.

General **Advanced**

 Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Registerkarte Erweitert

## CLI-Konfiguration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

Hinweis: In diesem Szenario wird die globale Parameterzuordnung verwendet. Konfigurieren Sie eine benutzerdefinierte Web-Parameterzuordnung, indem Sie Add (Hinzufügen) auswählen und auf der Registerkarte Advanced (Erweitert) die Umleitungs-URL festlegen. Die Einstellungen für Vertrauenspunkt und virtuelle IP werden vom globalen Profil übernommen.

## AAA-Einstellungen:

### Schritt 1: Erstellen eines Radius-Servers:

Navigieren Sie zu Configuration > Security > AAA, klicken Sie im Abschnitt Server/Gruppe auf "Add" (Hinzufügen), und geben Sie auf der Seite "Create AAA Radius Server" (AAA Radius-Server erstellen) den Servernamen, die IP-Adresse und den gemeinsamen Schlüssel ein.

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Add' button is highlighted in red. The 'Servers' tab is selected. The form contains the following fields and options:

- Name\* (text input)
- Server Address\* (text input, placeholder: IPv4/IPv6/Hostname)
- PAC Key (checkbox, unchecked)
- Key Type (dropdown menu, selected: Clear Text)
- Key\* (text input)
- Confirm Key\* (text input)
- Auth Port (text input, value: 1812)
- Acct Port (text input, value: 1813)
- Server Timeout (seconds) (text input, value: 1-1000)
- Retry Count (text input, value: 0-100)
- Support for CoA (toggle, status: ENABLED)
- CoA Server Key Type (dropdown menu, selected: Clear Text)
- CoA Server Key (text input)
- Confirm CoA Server Key (text input)
- Automate Tester (checkbox, unchecked)

Buttons: Cancel, Apply to Device

Radius-Serverkonfiguration

## CLI-Konfiguration

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

## Schritt 2: Erstellen einer RADIUS-Servergruppe:

Wählen Sie im Abschnitt "Server Groups" (Servergruppen) die Option "Add" (Hinzufügen) aus, um eine Servergruppe zu definieren und die Server umzuschalten, die in die Gruppenkonfiguration einbezogen werden sollen.

The screenshot shows the 'Create AAA Radius Server Group' dialog in the Cisco configuration interface. The dialog is titled 'Create AAA Radius Server Group' and is located under the 'Server Groups' tab. The 'Name\*' field is highlighted with a red box and contains the text 'ISE-Group'. A warning message 'Name is required' is displayed next to it. The 'Group Type' is set to 'RADIUS'. The 'MAC-Delimiter' and 'MAC-Filtering' are both set to 'none'. The 'Dead-Time (mins)' is set to '5'. The 'Load Balance' is set to 'DISABLED'. The 'Source Interface VLAN ID' is set to '2074' and is also highlighted with a red box. Below the dialog, the 'Assigned Servers' list contains the server 'ISE-Auth', which is also highlighted with a red box.

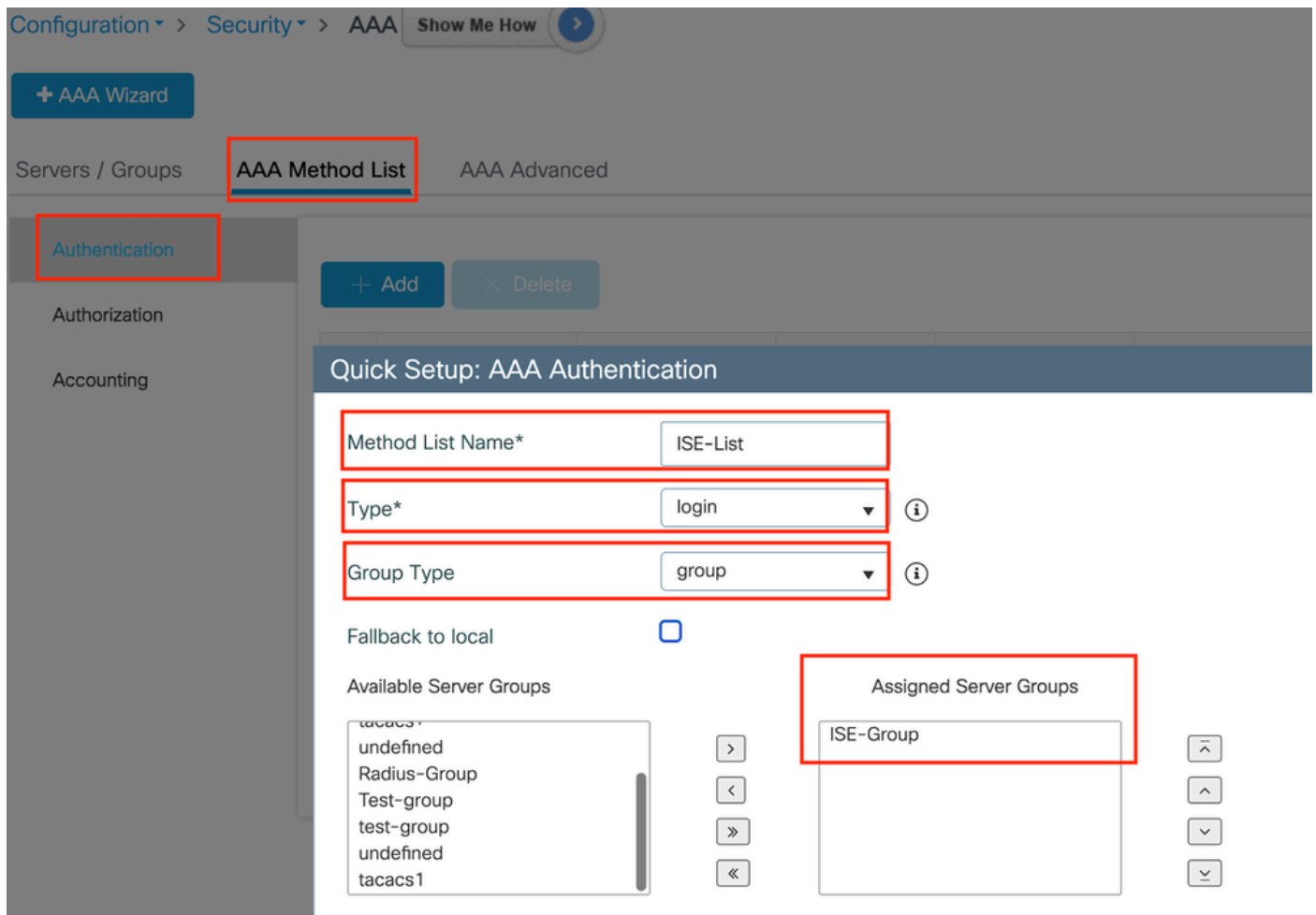
Radius-Servergruppe

CLI-Konfiguration

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5
```

### Schritt 3: Konfigurieren der AAA-Methodenliste:

Navigieren Sie zur Registerkarte AAA-Methodenliste, wählen Sie unter Authentifizierung Hinzufügen aus, definieren Sie einen Methodenlistennamen mit Typ als "login" und Gruppentyp als "Group", und ordnen Sie die konfigurierte Authentifizierungsservergruppe im Abschnitt Zugewiesene Servergruppe zu.



Liste der Authentifizierungsmethoden

### CLI-Konfiguration

```
aaa authentication login ISE-List group ISE-Group
```

### Richtlinienprofil konfigurieren

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profile > Richtlinie, benennen Sie Ihr neues Profil auf der Registerkarte Allgemein, und aktivieren Sie es mithilfe des Statusschalters.

Configuration > Tags & Profiles > Policy

+ Add   × Delete   Clone

### 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

Name*	<input type="text" value="GuestLANPolicy"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input checked="" type="checkbox" value="ENABLED"/>
Status	<input checked="" type="checkbox" value="ENABLED"/>	Central Authentication	<input checked="" type="checkbox" value="ENABLED"/>
Passive Client	<input type="checkbox" value="DISABLED"/>	Central DHCP	<input checked="" type="checkbox" value="ENABLED"/>
IP MAC Binding	<input checked="" type="checkbox" value="ENABLED"/>	Flex NAT/PAT	<input type="checkbox" value="DISABLED"/>
Encrypted Traffic Analytics	<input type="checkbox" value="DISABLED"/>		
CTS Policy			
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Richtlinienprofil

Schritt 2: Weisen Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) ein zufälliges VLAN zu, wenn die VLAN-Zuordnung auf dem Anker-Controller abgeschlossen ist. In diesem Beispiel wird VLAN 1 konfiguriert.



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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

**WLAN Local Profiling**

Global State of Device Classification **Disabled** ⓘ

Local Subscriber Policy Name

**VLAN**

VLAN/VLAN Group

Multicast VLAN

**WLAN ACL**

IPv4 ACL

IPv6 ACL

**URL Filters** ⓘ

Pre Auth

Post Auth

Registerkarte "Zugriffsrichtlinie"

Schritt 3: Schalten Sie auf der Registerkarte Mobility (Mobilität) den Anchor-Controller auf Primary (1) um, und konfigurieren Sie optional sekundäre und tertiäre Mobility-Tunnel, um die Redundanzanforderungen zu erfüllen

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

**Mobility Anchors**

Export Anchor

Static IP Mobility

*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 (3)	Selected (1)
Anchor IP	Anchor IP   Anchor Priority
<ul style="list-style-type: none"> <li> 10.106.40.11 →</li> <li> 10.76.118.75 →</li> <li> 10.76.118.74 →</li> </ul>	<ul style="list-style-type: none"> <li> 10.76.118.70 Primary (1) ←</li> </ul>

Mobility-Karte

CLI-Konfiguration

```
wireless profile policy GuestLANPolicy
mobility anchor 10.76.118.70 priority 1
no shutdown
```

## Konfigurieren des Gast-LAN-Profiles

Schritt 1: Navigieren Sie zu Configuration > Wireless > Guest LAN, wählen Sie Add aus, konfigurieren Sie einen eindeutigen Profilnamen, aktivieren Sie Wired VLAN, geben Sie die VLAN-ID für Wired Guest-Benutzer ein, und schalten Sie den Profilstatus auf Enabled (Aktiviert).

General	Security
Profile Name*	Client Association Limit
Guest LAN ID*	Wired VLAN Status
mDNS Mode	Wired VLAN ID*
Status	

Profile Name\*  Client Association Limit

Guest LAN ID\*  Wired VLAN Status  ENABLE

mDNS Mode  Wired VLAN ID\*

Status  ENABLE

Gast-LAN-Profil

Schritt 2: Aktivieren Sie auf der Registerkarte Sicherheit die Option Web Auth (Webauthentifizierung), ordnen Sie die Web Auth-Parameterzuordnung zu, und wählen Sie den Radius-Server aus der Dropdown-Liste Authentifizierung aus.

# Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



Registerkarte "Guest LAN Security"

## CLI-Konfiguration

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Gast-LAN-ZUORDNUNG

Navigieren Sie zu Konfiguration > Wireless > Gast-LAN.

Wählen Sie im Konfigurationsabschnitt Guest LAN MAP die Option Add (Hinzufügen) aus, und ordnen Sie das Richtlinienprofil und das Gast-LAN-Profil zu.

## ➤ Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map: GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page    0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save    Cancel

Gast-LAN-ZUORDNUNG

## CLI-Konfiguration

```
wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy
```

## Konfiguration auf Anchor 9800 WLC

### Webparameterzuordnung konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Security > Web Auth, wählen Sie Global aus, überprüfen Sie die virtuelle IP-Adresse des Controllers und die Vertrauenspunktzuordnung, und stellen Sie sicher, dass der Typ auf webauth eingestellt ist.

Configuration > Security > Web Auth

+ Add    × Delete

Parameter Map Name

- global
- Web-Filter

1    10

### Edit Web Auth Parameter

General    Advanced

Parameter-map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal:

Disable Success Window:

Disable Logout Window:

Disable Cisco Logo:

Sleeping Client Status:

Sleeping Client Timeout (minutes): 720

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-3...

Virtual IPv4 Hostname:

Virtual IPv6 Address: x::x::x::x

Web Auth intercept HTTPs:

Enable HTTP server for Web Auth:

Disable HTTP secure server for Web Auth:

#### Banner Configuration

Banner Title:

Banner Type:  None     Banner Text

Schritt 2: Konfigurieren Sie auf der Registerkarte Erweitert die URL der externen Webseite für die Client-Umleitung. Legen Sie "Redirect URL for Login" (URL für Anmeldung umleiten) und "Redirect On-Failure" (Bei Fehler umleiten) fest. "Redirect On-Success" ist optional.

Nach der Konfiguration wird im Web Auth-Profil eine Vorschau der Umleitungs-URL angezeigt.

General **Advanced**

**i** Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

Registerkarte Erweitert

## CLI-Konfiguration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
intercept-https-enable.
trustpoint TP-self-signed-3915430211
webauth-http-enable
```

## AAA-Einstellungen:

### Schritt 1: Erstellen eines Radius-Servers:

Navigieren Sie zu Configuration > Security > AAA, klicken Sie im Abschnitt Server/Gruppe auf Add, und geben Sie auf der Seite "Create AAA Radius Server" (AAA Radius-Server erstellen) den Servernamen, die IP-Adresse und den gemeinsamen Schlüssel ein.

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Add' button is highlighted in red. The 'Name\*' field is also highlighted in red. The 'Server Address\*' field is highlighted in red. The 'Key Type' dropdown is highlighted in red. The 'Key\*' and 'Confirm Key\*' fields are highlighted in red. The 'Support for CoA' option is enabled. The 'Auth Port' is 1812, 'Acct Port' is 1813, 'Server Timeout (seconds)' is 1-1000, and 'Retry Count' is 0-100.

Radius-Serverkonfiguration

## CLI-Konfiguration

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

### Schritt 2: Erstellen einer RADIUS-Servergruppe:

Wählen Sie im Abschnitt "Server Groups" die Option Add aus, um eine Servergruppe zu definieren und die Server umzuschalten, die in die Gruppenkonfiguration einbezogen werden sollen.

Name*	ISE-Group
Group Type	RADIUS

MAC-Delimiter	none ▼
---------------	--------

MAC-Filtering	none ▼
---------------	--------

Dead-Time (mins)	5
------------------	---

Load Balance	<input type="checkbox"/> DISABLED
--------------	-----------------------------------

Source Interface VLAN ID	2081 ▼ 
--------------------------	--

Available Servers

Assigned Servers

--



ISE-Auth
----------

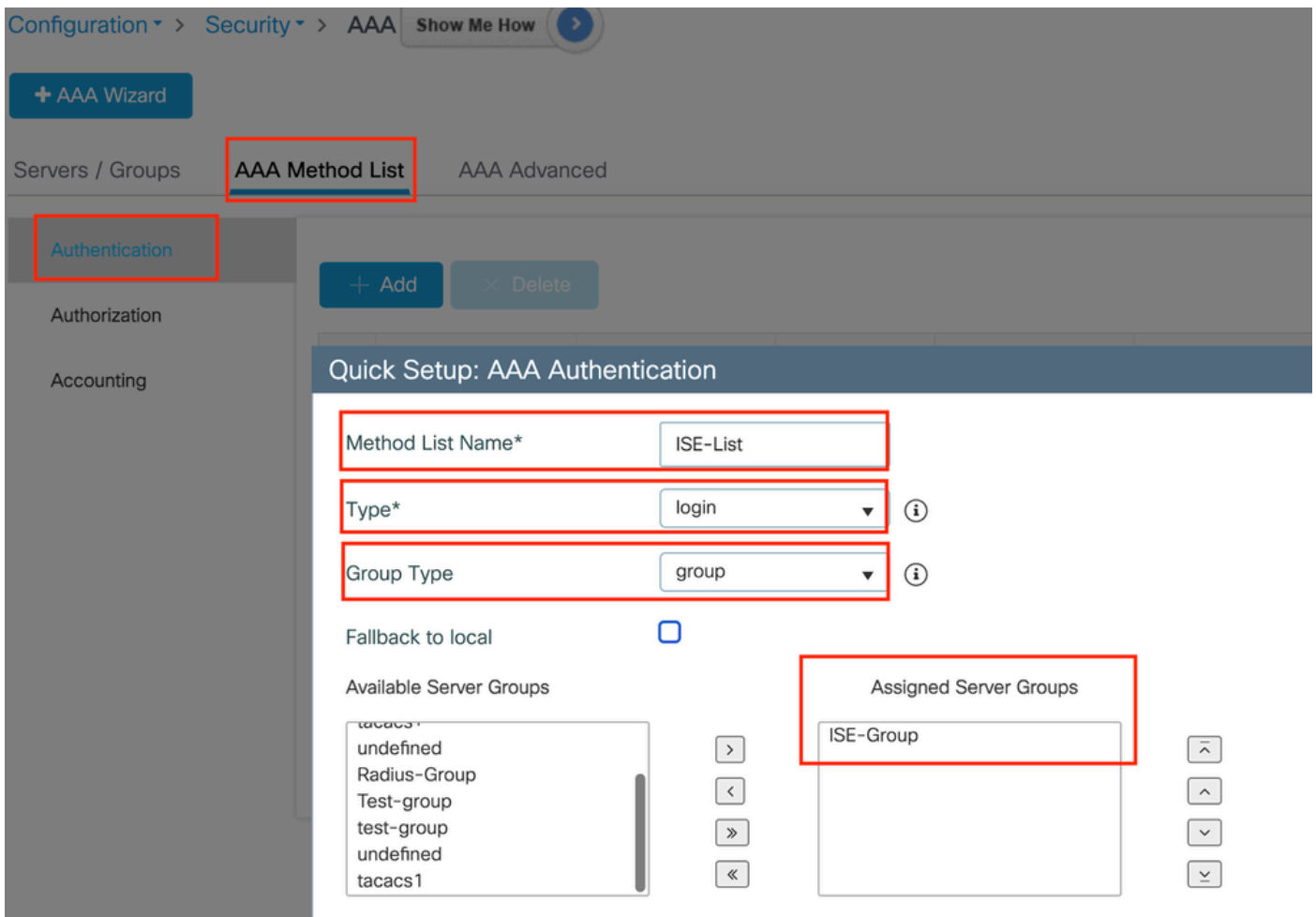
Ankerradiusgruppe

### CLI-Konfiguration

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2081
deadtime 5
```

### Schritt 3: Konfigurieren der AAA-Methodenliste:

Navigieren Sie zur Registerkarte AAA Method List (AAA-Methodenliste), wählen Sie Add unter Authentication (Authentifizierung) aus, definieren Sie einen Methodenlistennamen mit Type als "login" (Anmelden) und Group Type als "Group" (Gruppe), und ordnen Sie die konfigurierte Authentifizierungsservergruppe im Abschnitt Assigned Server Group (Zugewiesene Servergruppe) zu.



Liste der Authentifizierungsmethoden

## CLI-Konfiguration

```
aaa authentication login ISE-List group ISE-Group
```

## Richtlinienprofil konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Tag & Profiles > Policy, konfigurieren Sie das Richtlinienprofil mit demselben Namen wie auf dem Fremdcontroller, und aktivieren Sie das Profil.



**General**

Access Policies

QOS and AVC

Mobility

Advanced

Name*	GuestLANPolicy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
IP MAC Binding	ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy	
Central Switching	ENABLED <input checked="" type="checkbox"/>
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	ENABLED <input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/> DISABLED

Ankerrichtlinienprofil

Schritt 2: Ordnen Sie unter "Access Policies" (Zugriffsrichtlinien) das kabelgebundene Client-VLAN aus der Dropdown-Liste zu.

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



### VLAN

VLAN/VLAN Group

VLAN2024





Hinweis: Die Konfiguration des Richtlinienprofils muss auf dem Foreign-Controller und dem Anchor-Controller mit Ausnahme des VLAN übereinstimmen.

---

Schritt 3: Aktivieren Sie auf der Registerkarte Mobilität das Kontrollkästchen Anker exportieren.

### Mobility Anchors

Export Anchor



Static IP Mobility



*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 (2)

Selected (0)

Anchor IP

Anchor IP

Anchor IP

Anker exportieren



Hinweis: Bei dieser Konfiguration wird der Wireless LAN Controller 9800 (WLC) als Anker-WLC für alle WLANs festgelegt, die dem angegebenen Richtlinienprofil zugeordnet sind. Wenn ein ausländischer 9800-WLC Clients an den Anker-WLC umleitet, enthält er Details zum WLAN und zum Richtlinienprofil, die dem Client zugewiesen sind. Auf diese Weise kann der Anker-WLC auf Basis der empfangenen Informationen das entsprechende lokale Richtlinienprofil anwenden.

---

## CLI-Konfiguration

```
wireless profile policy GuestLANPolicy
  mobility anchor
  vlan VLAN2024
  no shutdown
```

## GastLAN-Profil konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Wireless > Guest LAN, und wählen Sie Add aus, um das Profil für das Gast-LAN zu erstellen und zu konfigurieren. Stellen Sie sicher, dass der Profilename mit dem des Fremdcontrollers übereinstimmt. Beachten Sie, dass das kabelgebundene VLAN auf dem Anker-Controller deaktiviert sein muss.

Configuration > Wireless > Guest LAN

> Guest LAN Configuration

+ Add × Delete

### Add Guest LAN Profile

**General** Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

Gast-LAN-Profil

Schritt 2: Aktivieren Sie in den Sicherheitseinstellungen die Webauthentifizierung, und konfigurieren Sie dann die Webauthentifizierungsparameterzuordnung und die Authentifizierungsliste.

## Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List





Hinweis: Die Konfiguration des Gast-LAN-Profiles muss mit Ausnahme des Status des kabelgebundenen VLAN zwischen dem Fremd- und dem Anker-Controller identisch sein.

---

## CLI-Konfiguration

```
guest-lan profile-name Guest-Profile 1
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Gast-LAN-ZUORDNUNG

Schritt 1: Navigieren Sie zu Konfiguration > Wireless > Gast-LAN. Wählen Sie im Konfigurationsabschnitt "Gast-LAN-MAP" die Option Hinzufügen aus, und ordnen Sie das Richtlinienprofil dem Gast-LAN-Profil zu.



## > Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map : GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	
10 items per page    0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save    Cancel

Gast-LAN-ZUORDNUNG

wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy

## Konfigurieren von Wired Guest auf Catalyst 9800, verankert in AireOS 5520 Controller



Netzwerktopologie

## Konfiguration auf dem 9800 WLC

## Webparameterzuordnung konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Security > Web Auth, und wählen Sie Global aus. Überprüfen Sie, ob die virtuelle IP-Adresse des Controllers und der Vertrauenspunkt im Profil korrekt zugeordnet sind, und stellen Sie sicher, dass der Typ "webauth" (Webauthentifizierung) lautet.

General		Advanced	
Parameter-map Name	<input type="text" value="global"/>	Virtual IPv4 Address	<input type="text" value="192.0.2.1"/>
Maximum HTTP connections	<input type="text" value="100"/>	Trustpoint	<input type="text" value="TP-self-signed-3..."/>
Init-State Timeout(secs)	<input type="text" value="120"/>	Virtual IPv4 Hostname	<input type="text"/>
Type	<input type="text" value="webauth"/>	Virtual IPv6 Address	<input type="text" value=":::XX:XX::X"/>
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	<b>Banner Configuration</b>	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	<input type="text"/>
Sleeping Client Timeout (minutes)	<input type="text" value="720"/>	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Webparameterübersicht

Schritt 2: Geben Sie auf der Registerkarte Erweitert die URL der externen Webseite an, zu der Clients umgeleitet werden müssen. Konfigurieren Sie die Umleitungs-URL für Anmeldung und Umleitung bei Ausfall. Die Einstellung "Redirect On-Success" (Bei Erfolg umleiten) ist eine optionale Konfiguration.

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X"/>

Registerkarte Erweitert

### CLI-Konfiguration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Hinweis: Informationen zur AAA-Konfiguration finden Sie im Abschnitt "" unter den Konfigurationsdetails für den Foreign 9800 WLC.

---

## Richtlinienprofil konfigurieren

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profile > Richtlinie. Wählen Sie Hinzufügen aus, geben Sie auf der Registerkarte Allgemein einen Namen für das Profil an, und aktivieren Sie den Statusschalter.

**General**

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Richtlinienprofil

Schritt 2: Zuweisen eines zufälligen VLAN auf der Registerkarte Access Policies (Zugriffsrichtlinien)

General

**Access Policies**

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device  
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



### VLAN

VLAN/VLAN Group

1



Multicast VLAN

Enter Multicast VLAN

Zugriffsrichtlinien

Schritt 3: Schalten Sie auf der Registerkarte Mobility (Mobilität) den Anchor-Controller um, und legen Sie dessen Priorität auf Primary (1) fest.

### Mobility Anchors

Export Anchor



Static IP Mobility




*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)



Anchor IP

 10.76.6.156 
---

#### Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) 
--	---

Registerkarte "Mobilität"



Hinweis: Das Richtlinienprofil des 9800 Foreign WLC muss mit dem Gast-LAN-Profil des 5520 Anchor WLC übereinstimmen, mit Ausnahme der VLAN-Konfiguration.

---

## CLI-Konfiguration

```
wireless profile policy Guest
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor 10.76.118.74 priority 1
no shutdown
```

## Konfigurieren des Gast-LAN-Profiles

Schritt 1: Navigieren Sie zu Configuration > Wireless > Guest LAN, und wählen Sie Add



(Hinzufügen). Konfigurieren Sie einen eindeutigen Profilnamen, und aktivieren Sie das kabelgebundene VLAN. Geben Sie dabei die dedizierte VLAN-ID für kabelgebundene Gastbenutzer an. Schalten Sie zuletzt den Profilstatus auf Enabled (Aktiviert) um.

**General** Security

Profile Name*	Guest	Client Association Limit	2000
Guest LAN ID*	2	Wired VLAN Status	ENABLE <input checked="" type="checkbox"/>
mDNS Mode	Bridging ▼	Wired VLAN ID*	11
Status	ENABLE <input checked="" type="checkbox"/>		

Gast-LAN-Richtlinie

Schritt 2: Aktivieren Sie auf der Registerkarte Sicherheit die Webauthentifizierung, ordnen Sie die Webauthentifizierungsparameterzuordnung zu, und wählen Sie den RADIUS-Server aus der Dropdown-Liste Authentifizierung aus.

General **Security**

Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global ▼
Authentication List	ISE-List ▼

Registerkarte Sicherheit



Hinweis: Der Gast-LAN-Profilname muss für den 9800 Foreign Controller und den 5520 Anchor Controller identisch sein.

---

## CLI-Konfiguration

```
guest-lan profile-name Guest 2 wired-vlan 11
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Gast-LAN-ZUORDNUNG

Schritt 1: Navigieren Sie zu Konfiguration > Wireless > Gast-LAN. Wählen Sie im Konfigurationsabschnitt Guest LAN MAP die Option Add (Hinzufügen) aus, und ordnen Sie das Richtlinienprofil dem Gast-LAN-Profil zu.

➤ Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map : GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page    0 - 0 of 0 items

Profile Name: Guest

Policy Name: Guest

✓ Save    ↻ Cancel

Gast-LAN-ZUORDNUNG

## CLI-Konfiguration

```
wireless guest-lan map GuestMap
guest-lan Guest policy Guest
```

# Konfiguration auf Anchor 5520 WLC

## Webauthentifizierung konfigurieren

Schritt 1: Navigieren Sie zu Security > Web Auth > Web Login Page. Legen Sie den Webauthentifizierungstyp auf "Extern" (An externen Server umleiten) fest, und konfigurieren Sie die externe Webauthentifizierungs-URL. Die Umleitungs-URL nach der Anmeldung ist optional und kann konfiguriert werden, wenn Clients nach erfolgreicher Authentifizierung auf eine dedizierte Seite umgeleitet werden müssen.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Save Configuration Ping Logout Refresh User: admin(ReadWrite) Home

Security

Web Login Page

Preview... Apply

Web Authentication Type: External (Redirect to external server)

Redirect URL after login: http://10.127.196.171/webauth/logout.html

Login Success Page Type: None

External Webauth URL: http://10.127.196.171/webauth/login.html

QrCode Scanning Bypass Timer: 0

QrCode Scanning Bypass Count: 0

AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Auth Cached Users
  - Failback
  - DNS
  - Downloaded AVP
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
- Web Auth
  - Web Login Page
  - Certificate

## AAA-Einstellungen:

### Schritt 1: Konfigurieren des Radius-Servers

Navigieren Sie zu Security > Radius > Authentication > New.



### Radius-Server

Schritt 2: Konfigurieren der RADIUS-Server-IP und des gemeinsamen geheimen Schlüssels auf dem Controller. Schalten Sie den Serverstatus auf Aktiviert um, und aktivieren Sie das Kontrollkästchen Netzwerkbenutzer.

## RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Serverkonfiguration

### Zugriffskontrollliste konfigurieren

Schritt 1: Navigieren Sie zu Sicherheit > Zugriffskontrollliste, und wählen Sie Neu aus. Erstellen

Sie eine Pre-Authentication-ACL, die den Datenverkehr an DNS und den externen Webserver zulässt.

The screenshot shows the Cisco ISE Security configuration page for Access Control Lists. The 'SECURITY' tab is highlighted in the top navigation bar. In the left sidebar, 'Access Control Lists' is selected. The main content area shows the 'General' configuration for an Access List named 'Pre-Auth\_ACL'. The 'Deny Counters' are set to 0. Below this is a table with 6 rows of rules, all set to 'Permit'.

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Zugriffsliste zum Zulassen des Datenverkehrs zum Webserver

## Konfigurieren des Gast-LAN-Profiles

Schritt 1: Navigieren Sie zu WLANs > wählen Sie Neu erstellen aus.

Wählen Sie Type as Guest LAN aus, und konfigurieren Sie den gleichen Namen wie das Richtlinienprofil des 9800 Foreign-Controllers.

The screenshot shows the Cisco ISE WLANs configuration page. The 'WLANs' tab is highlighted in the top navigation bar. In the top right corner, there is a 'Create New' dropdown menu and a 'Go' button, both highlighted with a red box. Below this, there is a table with columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

Gast-LAN erstellen

The screenshot shows the Cisco ISE 'WLANs > New' configuration page. The 'WLANs' tab is highlighted in the top navigation bar. In the top right corner, there is a '< Back' button and an 'Apply' button, both highlighted with a red box. Below this, there is a form with fields for 'Type', 'Profile Name', and 'ID'. The 'Type' field is set to 'Guest LAN', 'Profile Name' is 'Guest', and 'ID' is '2'.

Gast-LAN-Profil

Schritt 2: Zuordnen der Eingangs- und Ausgangsschnittstellen zum Gast-LAN-Profil

Die Eingangsschnittstelle ist in diesem Fall keine Eingangsschnittstelle, da es sich bei der Eingangsschnittstelle um den EoIP-Tunnel des Foreign-Controllers handelt.

Die Ausgangsschnittstelle ist das VLAN, mit dem der kabelgebundene Client eine physische Verbindung herstellt.

**General** **Security** **QoS** **Advanced**

Profile Name: Guest  
Type: Guest LAN  
Status:  Enabled

Security Policies: **Web-Auth**  
(Modifications done under security tab will appear after applying the changes.)

Ingress Interface: None  
Egress Interface: wired-vlan-11  
NAS-ID: none

Gast-LAN-Profil

Schritt 3: Wählen Sie auf der Registerkarte Sicherheit die Option Layer-3-Sicherheit als Webauthentifizierung aus, und ordnen Sie die ACL vor der Authentifizierung zu.

## WLANs > Edit 'Guest'

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 3 Security: Web Authentication  
Preauthentication ACL: IPv4 Pre-Auth\_ACL IPv6 None  
Override Global Config<sup>20</sup>:  Enable

Registerkarte "Guest LAN Security"

Schritt 4: Navigieren Sie zu Sicherheit > AAA-Server.

Wählen Sie das Dropdown-Menü aus, und ordnen Sie den Radius-Server dem Gast-LAN-Profil zu.

Authentication Servers		Accounting Servers	
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.197.224.122, Port:1812	<input type="checkbox"/> Enabled	None
Server 2	None		None
Server 3	None		None
Server 4	None		None

Zuordnung des Radius-Servers zum Gast-LAN-Profil

Schritt 5: Navigieren Sie zu WLAN. Bewegen Sie den Mauszeiger über das Dropdown-Symbol des Gast-LAN-Profiles, und wählen Sie Mobility Anchors aus.

2 Guest LAN Guest --- Disabled Web-Auth

- Remove
- Mobility Anchors

Schritt 6: Wählen Sie Mobility Anchor Create (Mobilitätsanker erstellen) aus, um den Controller als Exportanker für dieses Gast-LAN-Profil zu konfigurieren.

WLAN SSID Guest

Switch IP Address (Anchor)  
local

Mobility Anchor Create

Data Path	Control Path
up	up

Erstellung von Mobility Anchors

Konfigurieren von Wired Guest auf AireOS 5520 (verankert in



# Catalyst 9800)



Netzwerktopologie

## Konfiguration auf dem Foreign 5520 WLC

### Konfiguration der Controller-Schnittstelle

Schritt 1: Navigieren Sie zu Controller > Interfaces > New. Konfigurieren Sie einen Schnittstellennamen und eine VLAN-ID, und aktivieren Sie das Gast-LAN.

Für den kabelgebundenen Gast sind zwei dynamische Schnittstellen erforderlich.

Erstellen Sie zunächst eine dynamische Layer-2-Schnittstelle, und weisen Sie sie als Gast-LAN zu. Diese Schnittstelle dient als Eingangsschnittstelle für das Gast-LAN, über die kabelgebundene Clients eine physische Verbindung herstellen.

The screenshot shows the Cisco Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANS', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANA'. The left sidebar lists various configuration categories, with 'Interfaces' highlighted in red. The main content area is titled 'Interfaces > Edit' and is divided into several sections:

- General Information:** Interface Name is 'wired-guest' (highlighted in red), and MAC Address is 'a0:e0:af:32:d9:ba'.
- Configuration:** 'Guest Lan' is checked (highlighted in red), and NAS-ID is 'none'.
- Physical Information:** Port Number is '1', Backup Port is '0', and Active Port is '1'.
- Interface Address:** VLAN Identifier is '2020' (highlighted in red), DHCP Proxy Mode is 'Global', and 'Enable DHCP Option 82' is unchecked.

Eingangsschnittstelle

Schritt 2: Navigieren Sie zu Controller > Interfaces > New. Konfigurieren eines Schnittstellennamen und einer VLAN-ID

Bei der zweiten dynamischen Schnittstelle muss es sich um eine Layer 3-Schnittstelle auf dem Controller handeln. Die verkabelten Clients erhalten die IP-Adresse von diesem VLAN-Subnetz. Diese Schnittstelle dient als Ausgangsschnittstelle für das Gast-LAN-Profil.

**Controller**

**Interfaces > Edit**

**General Information**

Interface Name	vlan2024
MAC Address	a0:e0:af:32:d9:ba

**Configuration**

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

**Interface Address**

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

Ausgangs-Schnittstelle

## Switch-Port-Konfiguration

Kabelgebundene Gastbenutzer stellen eine Verbindung mit dem Access Layer-Switch her. Diese zugewiesenen Ports müssen mit einem VLAN konfiguriert werden, in dem Guest LAN auf dem Controller aktiviert ist.

Access Layer-Switch-Port-Konfiguration

```
interface gigabitEthernet <x/x/x>
```

```
description Kabelgebundener Gastzugriff
```

```
switchport access vlan 2020
```

```
switchport mode access
```

```
end
```

Uplink-Port-Konfiguration des Fremdcontrollers

```
interface TenGigabitEthernet<x/x/x>
```

Beschreibung Trunk port to the Foreign WLC

```
switchport mode trunk
```

```
switchport trunk native vlan 2081
```

```
switchport trunk allowed vlan 2081.2020
```

```
end
```

Uplink-Port-Konfiguration des Ankercontrollers

```
interface TenGigabitEthernet<x/x/x>
```

Beschreibung Trunk port to the Anchor WLC

```
switchport mode trunk
```

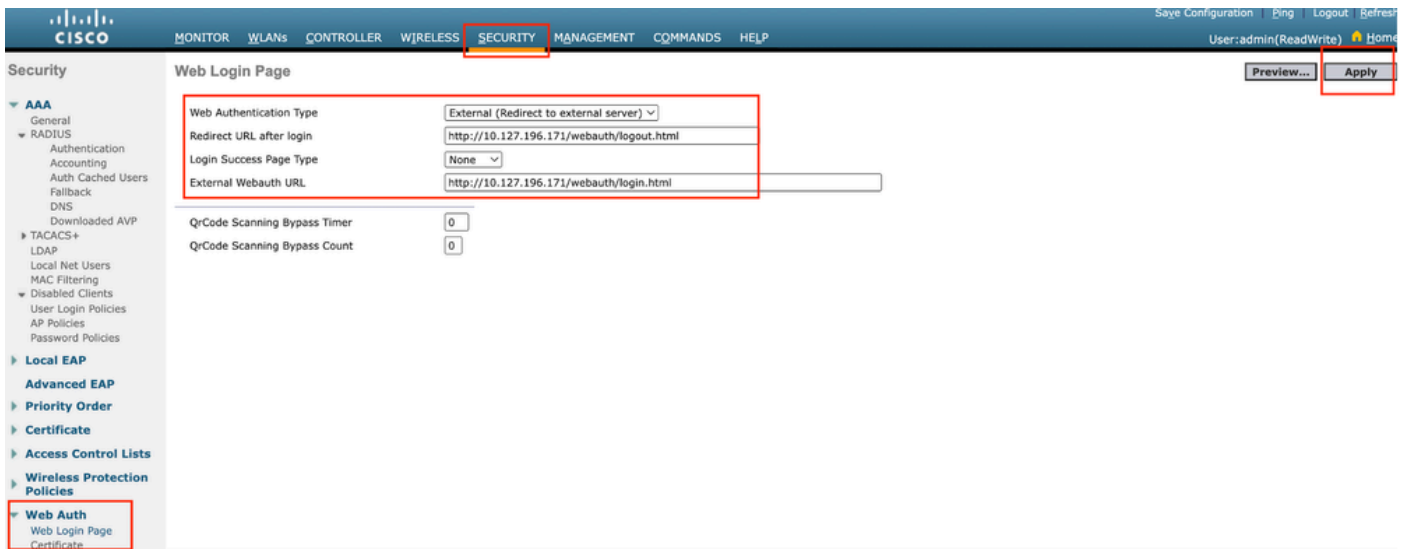
```
switchport trunk native vlan 2081
```

```
switchport trunk allowed vlan 2081.2024
```

```
end
```

## Webauthentifizierung konfigurieren

Schritt 1: Navigieren Sie zu Security > Web Auth > Web Login Page. Legen Sie den Webauthentifizierungstyp auf "Extern" (An externen Server umleiten) fest, und konfigurieren Sie die externe Webauthentifizierungs-URL. Die Umleitungs-URL nach der Anmeldung ist optional und kann konfiguriert werden, wenn Clients nach erfolgreicher Authentifizierung auf eine dedizierte Seite umgeleitet werden müssen.



Webauthentifizierungseinstellungen

## AAA-Einstellungen:

### Schritt 1: Konfigurieren des Radius-Servers

Navigieren Sie zu Security > Radius > Authentication > New.



Radius-Server

Schritt 2: Konfigurieren der RADIUS-Server-IP und des gemeinsamen geheimen Schlüssels auf dem Controller Schalten Sie den Serverstatus auf Aktiviert um, und aktivieren Sie das Kontrollkästchen Netzwerkbenutzer.

## RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

Serverkonfiguration

### Zugriffskontrollliste konfigurieren

Schritt 1: Navigieren Sie zu Sicherheit > Zugriffskontrollliste, und wählen Sie Neu aus. Erstellen

Sie eine Pre-Authentication-ACL, die den Datenverkehr an DNS und den externen Webserver zulässt.

Security

Access Control Lists > Edit

General

Access List Name: Pre-Auth\_ACL

Deny Counters: 0

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	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

Zugriffsliste zum Zulassen des Datenverkehrs zum Webserver

## Konfigurieren des Gast-LAN-Profiles

Schritt 1: Navigieren Sie zu WLAN > Create New > Go.

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

Current Filter: None [Change Filter] [Clear Filter]

Create New [Go]

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
---------	------	--------------	-----------	--------------	-------------------

Gast-LAN-Profil

Wählen Sie Als Gast-LAN eingeben aus, und konfigurieren Sie einen Profilnamen. Derselbe Name muss im Richtlinienprofil und im Gast-LAN-Profil des 9800 Anchor-Controllers konfiguriert werden.

## WLANs > New

Type

Guest LAN ▾

Profile Name

Guest-Profile

ID

3 ▾

Gast-LAN-Profil

Schritt 2: Ordnen Sie auf der Registerkarte General (Allgemein) die Eingangs- und Ausgangsschnittstelle des Gast-LAN-Profiles zu.

Die Eingangsschnittstelle ist das VLAN, mit dem die kabelgebundenen Clients physisch verbunden sind.

Die Ausgangsschnittstelle ist das VLAN-Subnetz, das die Clients für die IP-Adresse anfordern.

General	Security	QoS	Advanced
Profile Name	Guest-Profile		
Type	Guest LAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	<b>Web-Auth</b> (Modifications done under security tab will appear after applying th		
Ingress Interface	wired-guest ▾		
Egress Interface	vlan2024 ▾		
NAS-ID	none		

Gast-LAN-Profil

Schritt 3: Navigieren Sie zu Sicherheit > Layer 3.



Wählen Sie Layer-3-Sicherheit als Webauthentifizierung aus, und ordnen Sie die ACL vor der Authentifizierung zu.

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security

Preauthentication ACL IPv4 Pre-Auth\_ACL IPv6 None Web Authentication

Override Global Config<sup>20</sup>  Enable

Registerkarte "Layer 3 Security"

Schritt 4:

Ordnen Sie auf der Registerkarte AAA-Server den Radius-Server zu, und aktivieren Sie das Kontrollkästchen Enabled (Aktiviert).

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on the

**RADIUS Servers**

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.197.224.122, Port:1812	<input type="checkbox"/> Enabled None
Server 2	None	None
Server 3	None	None
Server 4	None	None

Zuordnung von Radius-Servern zum Gast-LAN-Profil

Schritt 5: Navigieren Sie zur Seite WLAN, zeigen Sie mit der Maus auf das Dropdown-Symbol für das Gast-LAN-Profil, und wählen Sie Mobility Anchors (Mobilitätsanker) aus.

<input type="checkbox"/>	30	WLAN	guest-1665	guest-1665	Disabled	[WPA + WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>
<input type="checkbox"/>	1	Guest LAN	Guest-Profile	---	Enabled	Web-Auth	<input type="button" value="Remove"/> <input type="button" value="Mobility Anchors"/>
<input type="checkbox"/>	2	Guest LAN	Guest	---	Disabled	Web-Auth	

Mobility-Anker

Schritt 6: Zuordnen des Mobility Anchor aus der Dropdown-Liste zum Gast-LAN-Profil

### Mobility Anchors

WLAN SSID    Guest-Profile

---

Switch IP Address (Anchor)    Data Path    Co

local  
 10.106.39.41  
 10.76.6.156

Switch IP Address (Anchor)

**Foot Notes**

Zuordnung des Mobilitätsankers zum Gast-LAN

## Konfiguration auf Anchor 9800 WLC

### Webparameterzuordnung konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Security > Web Auth, und wählen Sie Global aus. Überprüfen Sie, ob die virtuelle IP-Adresse des Controllers und der Vertrauenspunkt im Profil korrekt zugeordnet sind, und stellen Sie sicher, dass der Typ "webauth" (Webauthentifizierung) lautet.

**General**

## Advanced

Parameter-map Name Maximum HTTP connections Init-State Timeout(secs) Type Captive Bypass Portal Disable Success Window Disable Logout Window Disable Cisco Logo Sleeping Client Status Sleeping Client Timeout (minutes) Virtual IPv4 Address Trustpoint Virtual IPv4 Hostname Virtual IPv6 Address Web Auth intercept HTTPs Enable HTTP server for Web Auth Disable HTTP secure server for Web Auth **Banner Configuration**Banner Title Banner Type  None  Banner Text  Read From File

## Webparameterübersicht

Schritt 2: Geben Sie auf der Registerkarte Erweitert die URL der externen Webseite an, zu der Clients umgeleitet werden müssen. Konfigurieren Sie die Umleitungs-URL für Anmeldung und Umleitung bei Ausfall. Die Einstellung "Redirect On-Success" (Bei Erfolg umleiten) ist eine optionale Konfiguration.

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X::X"/>

Registerkarte Erweitert

### CLI-Konfiguration

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```



Hinweis: Informationen zur AAA-Konfiguration finden Sie im Abschnitt "Configure Wired Guest on Catalyst 9800 anchored to another Catalyst 9800" (Konfigurieren von kabelgebundenen Gastgeräten an einem anderen Catalyst 9800) für den Foreign 9800 WLC.

---

## Richtlinienprofil konfigurieren

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profile > Richtlinie. Konfigurieren Sie das Richtlinienprofil mit demselben Namen, der auch für das Gast-LAN-Profil des Foreign-Controllers verwendet wird.

**General**

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Guest-Profile

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

Richtlinienprofil

Schritt 2: Ordnen Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) das kabelgebundene Client-VLAN aus der Dropdown-Liste zu.

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

**WLAN Local Profiling**Global State of Device  
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

**VLAN**

VLAN/VLAN Group

VLAN2024



Multicast VLAN

Enter Multicast VLAN

Zugriffsrichtlinien

Schritt 3: Aktivieren Sie auf der Registerkarte Mobilität das Kontrollkästchen Anker exportieren.

### Mobility Anchors

Export Anchor



Static IP Mobility



*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

Registerkarte "Mobilität"

### CLI-Konfiguration

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

### Konfigurieren des Gast-LAN-Profiles

Schritt 1: Navigieren Sie zu Configuration > Wireless > Guest LAN, und wählen Sie Add aus, um das Profil für das Gast-LAN zu konfigurieren und den Status für das kabelgebundene VLAN zu deaktivieren.

Der Name des Gast-LAN-Profiles auf dem Anker muss mit dem des Gast-LAN-Profiles auf dem ausländischen WLC übereinstimmen.



**General**

## Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

Gast-LAN-Profil

Schritt 2: Aktivieren Sie auf der Registerkarte "Sicherheit" die Option "Web Auth". Wählen Sie die Web Auth-Parameterzuordnung und die Authentifizierungsliste aus der Dropdown-Liste aus.

## Edit Guest LAN Profile

## General

**Security**

## Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global
Authentication List	ISE-List

Registerkarte "Guest LAN Security"

## CLI-Konfiguration

```
guest-lan profile-name Guest-Profile 1
```

```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## Gast-LAN-ZUORDNUNG

Schritt 1: Navigieren Sie zu Konfiguration > Wireless > Gast-LAN. Wählen Sie im Konfigurationsabschnitt Guest LAN MAP die Option Add (Hinzufügen) aus, und ordnen Sie das Richtlinienprofil dem Gast-LAN-Profil zu.

### > Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map: GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page    0 - 0 of 0 items

Profile Name: Guest-Profile

Policy Name: Guest-Profile

✓ Save    ↺ Cancel

Gast-LAN-ZUORDNUNG

## Überprüfung

Validierung der Controller-Konfiguration

#show Gast-LAN-Übersicht

GLAN	GLAN Profile Name	Status
1	Guest-Profile	UP
2	Guest	UP

#show Gast-LAN-ID 1

<#root>

Guest-LAN Profile Name : Guest

```
=====
Guest-LAN ID           : 2
Wired-Vlan             :
```

```

Status :
Enabled
Number of Active Clients : 0
Max Associated Clients : 2000
Security
  WebAuth :
Enabled
  Webauth Parameter Map : global
  Webauth Authentication List :
ISE-List
  Webauth Authorization List : Not configured
mDNS Gateway Status : Bridge

```

#show, Parameterzuordnungstyp webauth global

```

<#root>
Parameter Map Name : global
Type :
webauth
  Redirect:
  For Login :
http://10.127.196.171/webauth/login.html
  On Success :
http://10.127.196.171/webauth/logout.html
  On Failure :
http://10.127.196.171/webauth/failed.html
  Portal ipv4 :
10.127.196.171
  Virtual-ipv4 :
192.0.2.1

```

#show parameter-map type webauth name <Profilname> (Bei Verwendung eines benutzerdefinierten Web-Parameterprofils)

#show Übersicht zu Wireless-Gast-LAN

GLAN Profile Name	Policy Name
Guest	Guest

## #show Zusammenfassung der Wireless-Mobilität

IP	Public Ip	MAC Address
10.76.118.70	10.76.118.70	f4bd.9e59.314b

## #show IP HTTP-Serverstatus

HTTP server status: Enabled  
HTTP server port: 80  
HTTP server active supplementary listener ports: 21111  
HTTP server authentication method: local

HTTP secure server capability: Present  
HTTP secure server status: Enabled  
HTTP secure server port: 443  
HTTP secure server trustpoint: TP-self-signed-3010594951

## >Zusammenfassung des Gast-LAN anzeigen

Number of Guest LANs..... 1

GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

## >Gastplan 2 anzeigen

Guest LAN Identifier..... 2  
Profile Name..... Guest  
Status..... Enabled  
Interface..... wired-vlan-11

Radius Servers  
Authentication..... 10.197.224.122 1812 \*  
Web Based Authentication..... Enabled  
Web Authentication Timeout..... 300  
IPv4 ACL..... Pre-Auth\_ACL

Mobility Anchor List

GLAN ID	IP Address	Status
2	10.76.118.74	Up

>Benutzerdefiniertes Web anzeigen

```

Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode..... None
Web Authentication Type..... External
Logout-popup..... Enabled
External Web Authentication URL..... http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer..... 0
QR Code Scanning Bypass Count..... 0

```

>show custom-web guest-lan 2

```

Guest LAN Status..... Enabled
Web Security Policy..... Web Based Authentication
WebAuth Type..... External
Global Status..... Enabled

```

Client-Richtlinienstatus überprüfen

Im Ausland:

#show Zusammenfassung des Wireless Client

Der Status des Client-Richtlinienmanagers auf dem Foreign-Controller wird nach erfolgreicher Zuweisung durch den Client ausgeführt.

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	N/A			

GLAN 1

Run

802.3

Web Auth

Export Foreign

>Client-Details anzeigen a0ce.c8c3.a9b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5  
Client Username ..... N/A  
Client Webauth Username ..... N/A  
Client State..... Associated  
User Authenticated by ..... None  
Client User Group.....  
Client NAC OOB State..... Access  
guest-lan..... 1  
Wireless LAN Profile Name..... Guest-Profile  
Mobility State.....

**Export Foreign**

Mobility Anchor IP Address.....  
10.76.118.70

Security Policy Completed.....

**Yes**

Policy Manager State.....

**RUN**

Pre-auth IPv4 ACL Name..... Pre-Auth\_ACL  
EAP Type..... Unknown  
Interface.....

**wired-guest-egress**

VLAN..... 2024  
Quarantine VLAN..... 0

Auf dem Anker,

Der Client-Statusübergang muss auf dem Anker-Controller überwacht werden.

Der Status des Client-Richtlinienmanagers lautet "Webauthentifizierung ausstehend".

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	10.76.6.156			

**GLAN 1**

Webauth Pending

802.3

Web Auth

**Export Anchor**

Sobald sich der Client authentifiziert, wechselt der Status des Richtlinien-Managers in den Status RUN.

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

#show wireless client mac-adresse a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5  
Client MAC Type : Universally Administered Address  
Client DUID: NA  
Client IPv4 Address :

10.105.211.69

Client State : Associated  
Policy Profile : Guest-Profile  
Flex Profile : N/A  
Guest Lan:  
GLAN Id: 1  
GLAN Name: Guest-Profile

Mobility:

Foreign IP Address :

10.76.118.74

Point of Attachment : 0xA0000003  
Point of Presence : 0  
Move Count : 1  
Mobility Role :

Export Anchor

Mobility Roam Type :

L3 Requested

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:

Point of Attachment : mobility\_a0000003  
IIF ID : 0xA0000003  
Authorized : FALSE

Session timeout : 28800  
Common Session ID: 4a764c0a0000008ea0285466  
Acct Session ID : 0x00000000  
Auth Method Status List  
Method : Web Auth  
Webauth State :

Login

Webauth Method :

Webauth

Server Policies:

Resultant Policies:

URL Redirect ACL :

WA-v4-int-10.127.196.171

Preauth ACL :

WA-sec-10.127.196.171

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

Der Client wechselt nach erfolgreicher Webauthentifizierung in den Status "RUN".

show wireless client mac-address a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5  
Client MAC Type : Universally Administered Address  
Client DUID: NA  
Client IPv4 Address :

10.105.211.69

Client Username :

testuser

Client State : Associated  
Policy Profile : Guest-Profile  
Flex Profile : N/A  
Guest Lan:  
GLAN Id: 1  
GLAN Name: Guest-Profile  
Wireless LAN Network Name (SSID) : N/A  
BSSID : N/A  
Connected For : 81 seconds  
Protocol : 802.3



Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 81 seconds

VLAN : VLAN2024

Last Tried Aaa Server Details:

Server IP :

10.197.224.122

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Resultant Policies:

URL Redirect ACL :

IP-Adm-V4-LOGOUT-ACL

VLAN Name : VLAN2024

VLAN :

2024

Absolute-Timer : 28800

>Client-Detail a0:ce:c8:c3:a9:b5 anzeigen

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5  
Client Username ..... N/A  
Client Webauth Username ..... N/A  
Client State..... Associated  
Wireless LAN Profile Name..... Guest  
WLAN Profile check for roaming..... Disabled  
Hotspot (802.11u)..... Not Supported  
Connected For ..... 90 secs  
IP Address..... 10.105.211.75  
Gateway Address..... 10.105.211.1  
Netmask..... 255.255.255.128  
Mobility State.....

Export Anchor

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No

Policy Manager State.....

WEBAUTH\_REQD

Pre-auth IPv4 ACL Name.....

Pre-Auth\_ACLPre-auth

IPv4 ACL Applied Status..... Yes  
Pre-auth IPv4 ACL Applied Status.....

Yes

Nach der Authentifizierung wechselt der Client in den RUN-Status.

<#root>

show client detail a0:ce:c8:c3:a9:b5  
Client MAC Address..... a0:ce:c8:c3:a9:b5  
Client Username .....

testuser

Client Webauth Username .....

testuser

Client State.....

Associated

User Authenticated by .....

RADIUS Server

Client User Group..... testuser  
Client NAC OOB State..... Access  
Connected For ..... 37 secs  
IP Address.....

10.105.211.75

Gateway Address..... 10.105.211.1  
Netmask..... 255.255.255.128  
Mobility State.....

Export Anchor

Mobility Foreign IP Address..... 10.76.118.70  
Security Policy Completed..... Yes  
Policy Manager State.....

RUN

Pre-auth IPv4 ACL Name..... Pre-Auth\_ACL  
Pre-auth IPv4 ACL Applied Status..... Yes  
EAP Type..... Unknown  
Interface.....

wired-vlan-11

VLAN.....

11

Quarantine VLAN..... 0

# Fehlerbehebung

## AireOS Controller-Debugging

Client-Debugging aktivieren

```
>Debug-Client <H.H.H>
```

So überprüfen Sie, ob das Debuggen aktiviert ist

```
>Debugging anzeigen
```

So deaktivieren Sie das Debugging

```
debug disable-all
```

## 9800 Radioaktive Spur

Aktivieren Sie Radio Active Tracing, um Client-Debug-Traces für die angegebene MAC-Adresse in der CLI zu generieren.

Schritte zum Aktivieren der radioaktiven Ablaufverfolgung:

Stellen Sie sicher, dass alle bedingten Debugging-Vorgänge deaktiviert sind.

```
clear platform condition all
```

Debug für angegebene MAC-Adresse aktivieren.

```
debug wireless mac <H.H.H> monitor-time <Time in seconds>
```

Deaktivieren Sie nach dem Reproduzieren des Problems das Debuggen, um die RA-Ablaufverfolgungssammlung anzuhalten.

```
no debug wireless mac <H.H.H>
```

Sobald die RA-Ablaufverfolgung beendet ist, wird die Debug-Datei im Bootflash des Controllers generiert.

```
show bootflash: | include ra_trace
2728          179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

Datei auf externen Server kopieren.

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

Debug-Protokoll anzeigen:

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

RA Trace in GUI aktivieren,

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Started**

+ Add x Delete v Start ■ Stop

Wireless Deb

Last Run

Add MAC/IP Address

MAC/IP Address\*

Enter a MAC/IP Address every newline

Cancel Apply to Device

RA Trace auf WebUI aktivieren

## Integrierte Paketerfassung

Navigieren Sie zu Fehlerbehebung > Paketerfassung. Geben Sie den Erfassungsnamen ein, und geben Sie die MAC-Adresse des Clients als innere Filter-MAC an. Legen Sie die Puffergröße auf

100 fest, und wählen Sie die Uplink-Schnittstelle aus, um eingehende und ausgehende Pakete zu überwachen.

Troubleshooting > Packet Capture

+ Add    × Delete

### Create Packet Capture ×

Capture Name\*    TestPCap

Filter\*    any

Monitor Control Plane ?   

Inner Filter Protocol     DHCP

Inner Filter MAC

Buffer Size (MB)\*    100

Limit by\*    Duration    3600    secs ≈ 1.00 hour

Available (12)    Search

<input type="checkbox"/> Tw0/0/1	→
<input checked="" type="checkbox"/> Tw0/0/2	→
<input checked="" type="checkbox"/> Tw0/0/3	→
<input type="checkbox"/> Te0/1/0	→

Selected (1)

<input checked="" type="checkbox"/> Tw0/0/0	←
---	---

Integrierte Paketerfassung



Hinweis: Wählen Sie die Option "Kontrollverkehr überwachen", um den an die System-CPU umgeleiteten und in die Datenebene zurückgeleiteten Datenverkehr anzuzeigen.

Navigieren Sie zu Troubleshooting > Packet Capture, und wählen Sie Start aus, um Pakete zu erfassen.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	<a href="#">▶ Start</a>

Paketerfassung starten

## CLI-Konfiguration

```
monitor capture TestPCap inner mac <H.H.H>  
monitor capture TestPCap buffer size 100  
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
```

monitor capture TestPCap start

<Reproduce the issue>

monitor capture TestPCap stop

show monitor capture TestPCap

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

## Exportieren der Paketerfassung auf einen externen TFTP-Server

monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap

Navigieren Sie zu Troubleshooting > Packet Capture, und wählen Sie Export aus, um die Erfassungsdatei auf den lokalen Computer herunterzuladen.

The screenshot shows a table of capture configurations. The first row is for 'TestPCap' on interface 'TwoGigabitEthernet0/0/0'. The 'Action' column has a green 'Start' button and a blue 'Export' button. The 'Export' button is highlighted with a red box. Below the table, an 'Export Capture - TestPCap' dialog box is open, showing 'Export to\*' set to 'desktop'. The 'Export' button in this dialog is also highlighted with a red box.

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	Start Export

EPC herunterladen

Funktionierende Protokollausschnitte

## AireOS-Debug-Protokoll für Foreign Controller-Client

### Kabelgebundenes Paket vom kabelgebundenen Client empfangen

\*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobi1

### Export-Ankeranforderung für Außendienstmitarbeiter-Gebäude

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0

Ein ausländischer Controller sendet eine Export-Ankeranforderung an den Anker-Controller.

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70

### Ankercontroller sendet Bestätigung für die Ankeranforderung für Client

\*Dot1x\_NW\_MsgTask\_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c

Die Mobilitätsrolle für die Clients auf dem Foreign-Controller wird aktualisiert, um Foreign zu exportieren.

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) mobility role update requ  
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70

Der Client wechselte in den RUN-Status.

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) State Update from Mobilit

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state

9800 Ausländischer Controller radioaktive Spur



Der Client wird dem Controller zugeordnet.

```
2024/07/15 04:10:29.087608331 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
```

Die Mobilitätserkennung wird nach der Zuordnung durchgeführt.

```
2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
```

```
2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
```

Nach der Verarbeitung der Mobilitätserkennung wird für den Client-Roamingtyp eine Aktualisierung auf L3 angefordert.

```
2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM
```

```
2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t
```

Der ausländische Controller sendet die Exportankeranforderung an den Anchor-WLC.

```
2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
```

```
2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

```
2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For
```

Die Antwort "Export Anchor" wird vom Anchor-Controller empfangen, und das VLAN wird vom Benutzerprofil übernommen.

```
2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5
```

```
2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex
```

```
2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An
```

```
2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr
```

```
2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:
```

Sobald die Anfrage für den Export-Anker verarbeitet wurde, wird die Client-Mobilitätsrolle auf Export Foreign aktualisiert.

```
2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce
```

```
2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20
```

2024/07/15 04:10:32.107592251 {wncd\_x\_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobil

Der Client wechselt in den IP-Lernstatus.

2024/07/15 04:10:32.108210365 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 04:10:32.108293096 {wncd\_x\_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5

Nach dem IP-Lernen wechselt der Client auf dem ausländischen WLC in den Status "RUN".

2024/07/15 04:10:32.108521618 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5

Client-Debug-Protokoll für AireOS Anchor

Anfrage für Export-Anker vom ausländischen Controller empfangen.

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileNa

Das lokale Bridging-VLAN wird für den Client angewendet.

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol

Die Mobilitätsrolle wird aktualisiert auf "Anker exportieren" und "Clientstatus-Transistorzuordnung".

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ

Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74

Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5

add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5

Sent message to add a0:ce:c8:c3:a9:b5 on mer

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm\_listen.c:7933) Changi

Die Mobilität ist abgeschlossen, der Client-Status ist verknüpft, und die Mobilitätsrolle lautet

"Export Anchor".

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

Die Client-IP-Adresse wird vom Controller erfasst, und der Status des Transistors von DHCP ist erforderlich, um die Webauthentifizierung zu ermöglichen.

```
*dt1ArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan
*dt1ArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dt1ArpSetType: Changing ARP Type from 0 ---> 1 for
*dt1ArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

Die Webauth-URL wird durch Hinzufügen der externen Umleitungs-URL und der virtuellen IP-Adresse des Controllers formuliert.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

Client-MAC-Adresse und WLAN zur URL hinzugefügt.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http://
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

Finale URL nach dem Parchen des HTTP-GET-Prozesses für Host 10.105.211.1

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

Die Umleitungs-URL wird im 200-OK-Antwortpaket an den Client gesendet.

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

Der Client stellt eine TCP-Verbindung mit dem Umleitungs-URL-Host her. Sobald die Clients den Benutzernamen und das Kennwort für die Anmeldung im Portal übermitteln, sendet der Controller eine RADIUS-Anfrage an den RADIUS-Server

Sobald der Controller eine Access-Accept-Nachricht empfängt, hat der Client die TCP-Sitzung beendet und wird in den Status RUN verschoben.

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe

*aaaQueueReader: May 28 10:46:59:077: AVP[01] User-Name.....testuser
*aaaQueueReader: May 28 10:46:59:077: AVP[03] Calling-Station-Id.....a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077: AVP[04] Nas-Port.....0x000000
*aaaQueueReader: May 28 10:46:59:077: AVP[05] Nas-IP-Address.....0x0a4c76
*aaaQueueReader: May 28 10:46:59:077: AVP[06] NAS-Identifier.....POD1586-

*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv

*Dot1x_NW_MsgTask_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c

*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state
```

## 9800 Anker Controller radioaktive Spur

Mobility-Ankündigungsnachricht für den Client vom Foreign-Controller.

```
2024/07/15 15:10:20.614677358 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re
```

Die Exportankeranforderung, die vom ausländischen Controller empfangen wird, wenn der Client eine Verknüpfung herstellt, für die die Exportankerantwort vom Ankercontroller gesendet wird. Diese kann über die RA-Folgerung des ausländischen Controllers überprüft werden.

```
2024/07/15 15:10:22.615246594 {mobilityd_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5
```

Der Client wird in den Zuordnungsstatus versetzt, und die Mobilitätsrolle wird in Export Anchor umgewandelt.

```
2024/07/15 15:10:22.616156811 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
2024/07/15 15:10:22.627358367 {wncd_x_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

```
2024/07/15 15:10:22.627462963 {wncd_x_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da
2024/07/15 15:10:22.627490485 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex
2024/07/15 15:10:22.627494963 {mobilityd_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo
```

Die IP-Ermittlung wurde abgeschlossen, die Client-IP-Erkennung erfolgte über ARP .

```
2024/07/15 15:10:22.628124206 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:23.627064171 {wncd_x_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m
2024/07/15 15:10:24.469704913 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470527056 {wncd_x_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470587596 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
2024/07/15 15:10:24.470613094 {wncd_x_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5
```

Der Client-Richtlinienstatus steht in der Webauthentifizierung aus.

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli
```

Der TCP-Handshake wird vom Controller getäuscht. Wenn der Client ein HTTP GET sendet, wird ein 200 OK-Antwortrahmen gesendet, der die Umleitungs-URL enthält.

Der Client muss einen TCP-Handshake mit der Umleitungs-URL einrichten und die Seite laden.

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wnc2024/07/15 15:12:04.280574375 {wncd_x_R0-0}{1}: [webauth-httpd] [1470
```

Wenn der Client die Anmeldeinformationen auf der Webportalseite sendet, wird ein Access-Request-Paket zur Authentifizierung an den Radius-Server gesendet.

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair
```

Access-Accept wird vom Radius-Server empfangen, Webauth ist erfolgreich.

```

2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name

```

Die Authentifizierung war erfolgreich, und der Client-Richtlinienstatus lautet "RUN".

```

2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errormsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b

```

## Integrierte Paketerfassungsanalyse

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)

```

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)
> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156
> User Datagram Protocol, Src Port: 16667, Dst Port: 16667
> Control And Provisioning of Wireless Access Points - Data
> Ethernet II, Src: Cisco_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink_c3:a9:b5 (a0:ce:c8:c3:a9:b5)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095
> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Location: http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n
    Content-Type: text/html\r\n
  < Content-Length: 527\r\n
  < \r\n
  < [HTTP response 1/1]
  < [Time since request: 0.000000000 seconds]
  < [Request in frame: 804]
  < [Request URI: http://10.105.211.1/auth/discovery?architecture=9]
  < File Data: 527 bytes

```

Client wird auf Portalseite umgeleitet

Die Sitzung wird nach Erhalt der Umleitungs-URL geschlossen.

804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
805	15:10:24.826953	10.105.211.1	10.105.211.69		TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)
807	15:10:24.826953	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
812	15:10:24.835955	10.105.211.69	10.105.211.1		TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
813	15:10:24.836947	10.105.211.1	10.105.211.69		TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
814	15:10:24.836947	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

Die TCP-Sitzung wird nach dem Empfang der Umleitungs-URL geschlossen.

Der Client initiiert einen TCP-3-Wege-Handshake an den URL-Umleitungshost und sendet eine HTTP GET-Anforderung.

Nach dem Laden der Seite werden die Anmeldedaten im Portal übermittelt. Der Controller sendet eine Zugriffsanforderung an den Radius-Server, um den Client zu authentifizieren.

Nach erfolgreicher Authentifizierung wird die TCP-Sitzung mit dem Webserver beendet, und auf dem Controller wird der Client-Richtlinienmanager-Status auf "RUN" gesetzt.

Time	Source	Destination	Protocol	Length	Info
2348	15:11:38.598968	10.105.211.69	10.127.196.171	TCP	54381 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2678067533 TSecr=0
2349	15:11:38.599959	10.127.196.171	10.105.211.69	TCP	80 → 54381 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
2350	15:11:38.599959	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2351	15:11:38.600966	10.105.211.69	10.127.196.171	HTTP	GET /webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://3.3.3.3/
2352	15:11:38.602965	10.127.196.171	10.105.211.69	HTTP	[TCP Previous segment not captured] Continuation
2354	15:11:38.602965	10.127.196.171	10.105.211.69	TCP	[TCP Out-Of-Order] 80 → 54381 [ACK] Seq=1 Ack=485 Win=2097408 Len=1380
2355	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	[TCP Dup ACK 2350#1] 54381 → 80 [ACK] Seq=485 Ack=1 Win=262144 Len=0 SLE=1381 SRE=1737
2356	15:11:38.603957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=485 Ack=1737 Win=260352 Len=0
2358	15:11:38.615965	10.105.211.69	10.127.196.171	HTTP	GET /webauth/yourlogo.jpg HTTP/1.1
2359	15:11:38.616957	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2360	15:11:38.616957	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1113 Ack=1880 Win=261952 Len=0
2362	15:11:38.621961	10.105.211.69	10.127.196.171	HTTP	GET /webauth/aup.html HTTP/1.1
2363	15:11:38.623960	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2364	15:11:38.623960	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=1706 Ack=2023 Win=261952 Len=0
2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
2751	15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0
2836	15:12:09.729957	10.105.211.69	10.127.196.171	HTTP	GET /webauth/logout.html HTTP/1.1
2837	15:12:09.731956	10.127.196.171	10.105.211.69	HTTP	HTTP/1.1 304 Not Modified
2838	15:12:09.731956	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2186 Ack=2166 Win=261952 Len=0
4496	15:13:07.964946	10.105.211.69	10.127.196.171	TCP	54381 → 80 [FIN, ACK] Seq=2186 Ack=2166 Win=262144 Len=0
4497	15:13:07.964946	10.127.196.171	10.105.211.69	TCP	80 → 54381 [FIN, ACK] Seq=2166 Ack=2187 Win=2097408 Len=0
4498	15:13:07.965938	10.105.211.69	10.127.196.171	TCP	54381 → 80 [ACK] Seq=2187 Ack=2167 Win=262144 Len=0

Client sendet HTTP GET-Anforderung an die Portalseite und schließt die Authentifizierung erfolgreich ab

## RADIUS Access Request-Paket

Time	Source	Destination	Protocol	Length	Info
2747	15:12:04.280976	10.76.118.70	10.197.224.122	RADIUS	Access-Request id=0
<pre> &gt; Frame 2747: 405 bytes on wire (3240 bits), 405 bytes captured (3240 bits) &gt; Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb) &gt; Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.197.224.122 &gt; User Datagram Protocol, Src Port: 60222, Dst Port: 1812 &lt; RADIUS Protocol   Code: Access-Request (1)   Packet identifier: 0x0 (0)   Length: 363   Authenticator: e3018f5d8e52fccbe0d703dac1a209e6   [The response to this request is in frame 2751]   Attribute Value Pairs     &gt; AVP: t=Calling-Station-Id(31) l=19 val=a0-ce-c8-c3-a9-b5     &gt; AVP: t=User-Name(1) l=10 val=testuser     &gt; AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)     &gt; AVP: t=Framed-IP-Address(8) l=6 val=10.105.211.69     &gt; AVP: t=Message-Authenticator(80) l=18 val=6f469fa30834350d2aed4e4b226cddf7     &gt; AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5)     &gt; AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)     &gt; AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)     &gt; AVP: t=User-Password(2) l=18 val=Encrypted     &gt; AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)     &gt; AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)     &gt; AVP: t=NAS-IP-Address(4) l=6 val=10.76.118.70     &gt; AVP: t=NAS-Port-Type(61) l=6 val=Virtual(5) </pre>					

Zugriffs-Anforderungspaket

## RADIUS Access Accept-Paket

Time	Source	Destination	Protocol	Length	Info
2751	15:12:04.682963	10.197.224.122	10.76.118.70	RADIUS	Access-Accept id=0
<pre> Frame 2751: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) Ethernet II, Src: Cisco_34:90:cb (6c:5e:3b:34:90:cb), Dst: Cisco_59:31:4b (f4:bd:9e:59:31:4b) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2081 Internet Protocol Version 4, Src: 10.197.224.122, Dst: 10.76.118.70 User Datagram Protocol, Src Port: 1812, Dst Port: 60222 RADIUS Protocol   Code: Access-Accept (2)   Packet identifier: 0x0 (0)   Length: 105   Authenticator: 523eb01399aba715577647a1f9e3b899   [This is a response to a request in frame 2747]   [Time from request: 0.401987000 seconds]   Attribute Value Pairs     &gt; AVP: t=User-Name(1) l=10 val=testuser     &gt; AVP: t=Class(25) l=57 val=434143533a303030303030303030303030303030303030303733342354243343437423a697365333167...     &gt; AVP: t=Message-Authenticator(80) l=18 val=223df8645f1387d7137428b20df9e0c1 </pre>					

Access Accept-Paket

## Verwandter Artikel

[Konfigurieren der Mobilitätsfunktion von WLAN Anchor auf dem Catalyst 9800](#)

[Konfigurationsbeispiel für kabelgebundenen Gastzugriff mit AireOS-Controllern](#)



## 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.