

Überprüfung konfigurieren und Fehler bei Web Auth bei MAC-Filter beheben

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Webparameter konfigurieren](#)

[Richtlinienprofil konfigurieren](#)

[WLAN-Profil konfigurieren](#)

[AAA-Einstellungen konfigurieren:](#)

[ISE-Konfiguration:](#)

[Überprüfung](#)

[Controller-Konfiguration](#)

[Client-Richtlinienstatus auf Controller](#)

[Fehlerbehebung](#)

[Erfassung radioaktiver Spuren](#)

[Integrierte Paketerfassung:](#)

[Verwandter Artikel](#)

Einleitung

In diesem Dokument wird die Funktion zum Konfigurieren, Beheben von Fehlern und Überprüfen der lokalen Webauthentifizierung unter "Mac Filter Failure" beschrieben, bei der ISE für die externe Authentifizierung verwendet wird.

Voraussetzungen

Konfigurieren der ISE für die MAC-Authentifizierung

Auf ISE/Active Directory konfigurierte gültige Benutzeranmeldeinformationen

Anforderungen

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

Grundlegendes Verständnis für die Navigation durch die Webbenutzeroberfläche des Controllers

Konfiguration von Richtlinien, WLAN-Profil und Richtlinien-Tags

Konfiguration von Servicerichtlinien auf der ISE

Verwendete Komponenten

9800 WLC Version 17.12.2

C9120 AXI-AP

Switch 9300

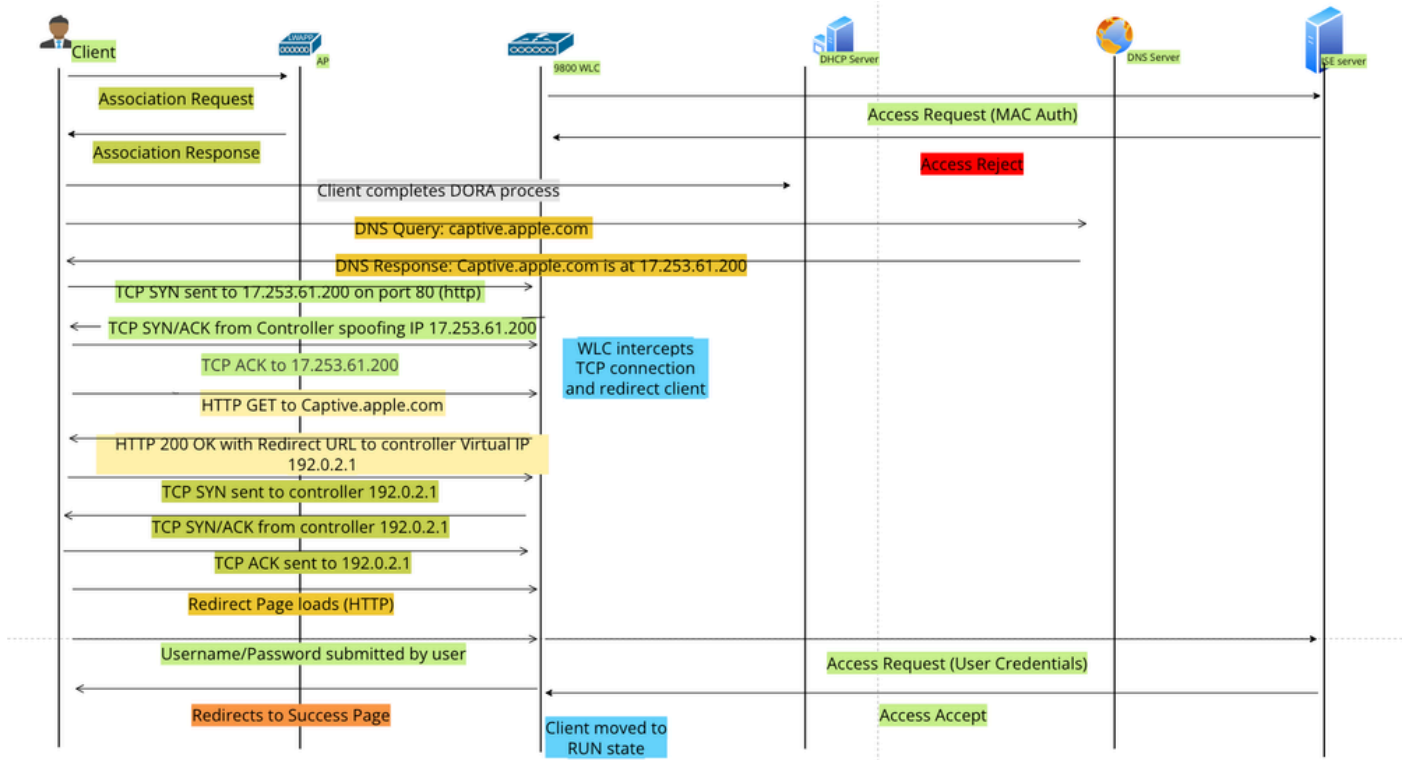
ISE Version 3.1.0.518

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.

Hintergrundinformationen

Die Web Auth-Funktion "On Mac Failure Filter" (Filter bei Mac-Ausfällen) dient als Fallback-Mechanismus in WLAN-Umgebungen, die sowohl MAC Authentication als auch Web Authentication verwenden.

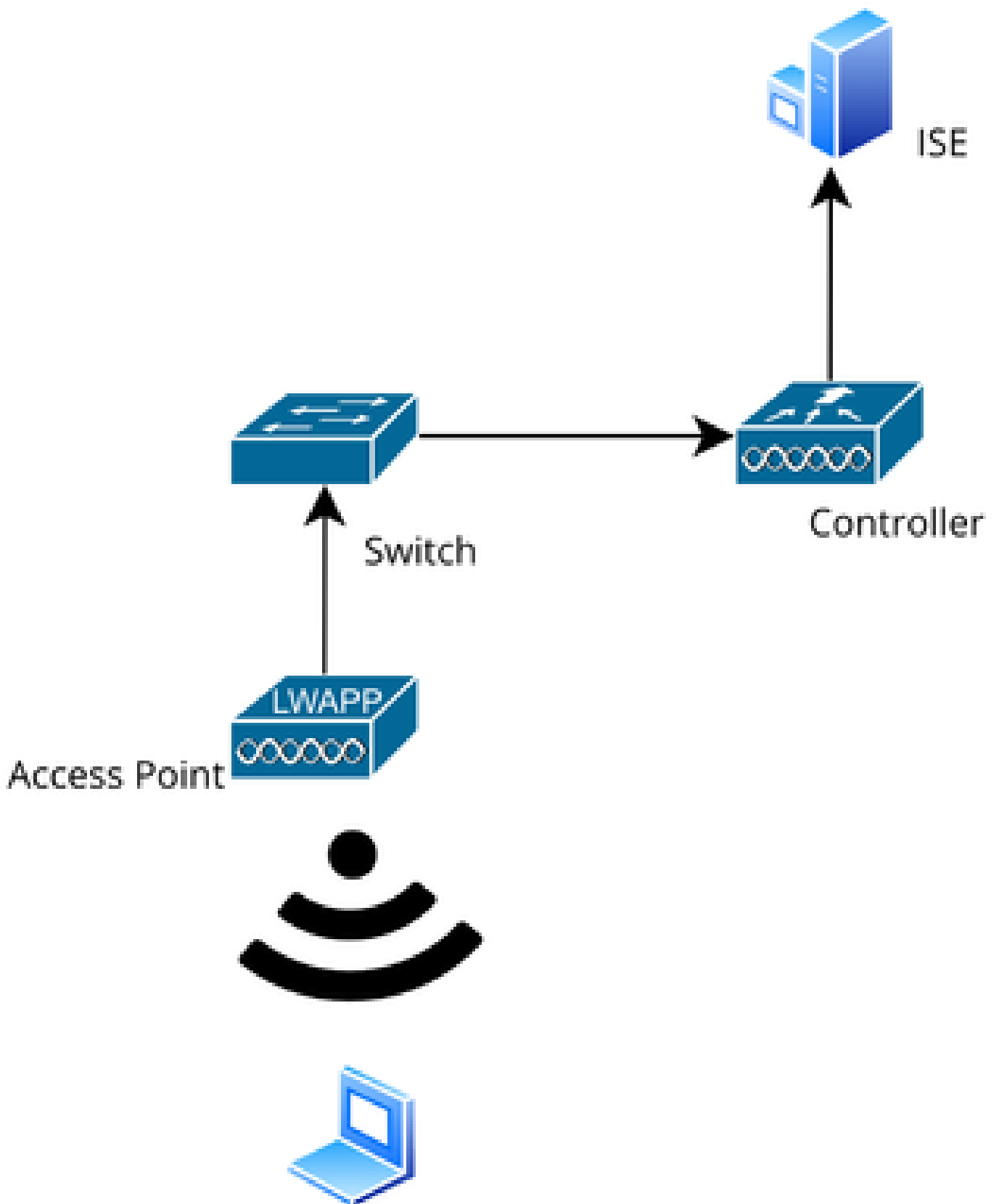
- **Fallback-Mechanismus:** Wenn ein Client versucht, über einen externen RADIUS-Server (ISE) oder lokalen Server eine Verbindung zu einem WLAN mit MAC-Filter herzustellen, und sich nicht authentifiziert, initiiert diese Funktion automatisch eine Layer-3-Webauthentifizierung.
- **Erfolgreiche Authentifizierung:** Wenn sich ein Client erfolgreich über den MAC-Filter authentifiziert, wird die Web-Authentifizierung umgangen, sodass der Client direkt eine Verbindung mit dem WLAN herstellen kann.
- **Vermeiden von Diszuordnungen:** Diese Funktion hilft, Diszuordnungen zu vermeiden, die sonst aufgrund von Fehlern bei der MAC-Filterauthentifizierung auftreten können.



Web-Auth-Fluss

Konfigurieren

Netzwerkdiagramm



Netzwerktopologie

Konfigurationen

Webparameter konfigurieren

Navigieren Sie zu Configuration > Security > Web Auth, und wählen Sie die globale Parameterzuordnung aus.

Überprüfen Sie die Konfiguration der virtuellen IP-Adresse und des Vertrauenspunkts aus der globalen Parameterzuordnung. Alle benutzerdefinierten Web Auth-Parameterprofile übernehmen die Konfiguration der virtuellen IP und des Vertrauenspunkts aus der globalen Parameterzuordnung.

Edit Web Auth Parameter

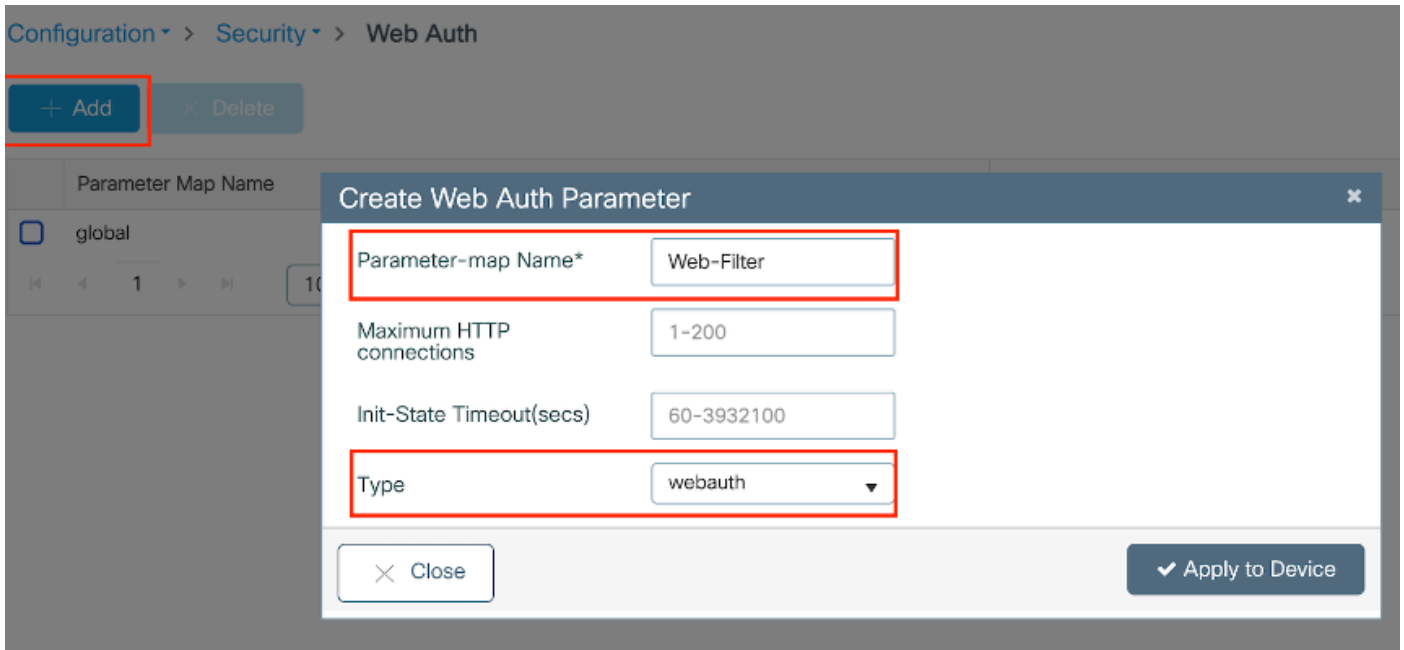
General Advanced

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	:::X:::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"/>		
Sleeping Client Status	<input type="checkbox"/>		

Banner Configuration

Globales Webauthentifizierungsparameterprofil

Schritt 1: Wählen Sie "Hinzufügen", um eine benutzerdefinierte Web-Authentifizierungsparameterzuordnung zu erstellen. Geben Sie den Profilnamen ein, und wählen Sie als Typ "Webauth" aus.



Webauthentifizierungs-Parameterprofil

Wenn Ihre Clients auch eine IPv6-Adresse erhalten, müssen Sie der Parameterzuordnung auch eine virtuelle IPv6-Adresse hinzufügen. Verwenden Sie eine IP im Dokumentationsbereich 2001:db8::/32

Wenn Ihre Clients eine IPv6-Adresse erhalten haben, ist es gut möglich, dass sie versuchen, die HTTP-Web-Authentifizierungsumleitung in V6 und nicht in V4 zu erhalten. Aus diesem Grund müssen Sie auch das virtuelle IPv6 festlegen.

CLI-Konfiguration:

```
parameter-map type webauth Web-Filter
 type webauth
```

Richtlinienprofil konfigurieren

Schritt 1: Richtlinienprofil erstellen

Navigieren Sie zu Konfiguration > Tags & Profile > Richtlinie. Wählen Sie "Hinzufügen". Geben Sie auf der Registerkarte Allgemein einen Namen für das Profil an, und aktivieren Sie den Statusschalter.

Configuration > Tags & Profiles > Policy

+ Add 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.

Admin Status

General Access Policies QOS and AVC Mobility Advanced

Name* Web-Filter-Policy

Description Enter Description

Status **ENABLED**

Passive Client **DISABLED**

IP MAC Binding **ENABLED**

Encrypted Traffic Analytics **DISABLED**

CTS Policy

Inline Tagging

SGACL Enforcement

WLAN Switching Policy

Central Switching **ENABLED**

Central Authentication **ENABLED**

Central DHCP **ENABLED**

Flex NAT/PAT **DISABLED**

Richtlinienprofil

Schritt 2:

Wählen Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) das Client-VLAN aus der Dropdown-Liste im VLAN-Abschnitt aus.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select

VLAN

VLAN/VLAN Group **VLAN2074** ⓘ

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select ⓘ

IPv6 ACL Search or Select ⓘ

URL Filters ⓘ

Pre Auth Search or Select ⓘ

Post Auth Search or Select ⓘ

Registerkarte "Zugriffsrichtlinie"

CLI-Konfiguration:

```
wireless profile policy Web-Filter-Policy
vlan VLAN2074
no shutdown
```

WLAN-Profil konfigurieren

Schritt 1: Navigieren Sie zu Configuration > Tags and Profiles > WLANs. Wählen Sie "Hinzufügen", um ein neues Profil zu erstellen. Definieren Sie einen Profilnamen und einen SSID-Namen, und aktivieren Sie das Statusfeld.

The screenshot shows the 'Add WLAN' configuration page in Cisco ISE. The breadcrumb navigation is 'Configuration > Tags & Profiles > WLANs'. A red box highlights the '+ Add' button. Below it, the 'Add WLAN' form is shown with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is active. The form fields are: 'Profile Name*' (Mac_Filtering_Wlan), 'SSID*' (Mac_Filtering_Wlan), 'WLAN ID*' (9), 'Status' (ENABLED with a green toggle), and 'Broadcast SSID' (ENABLED with a green toggle). To the right, the 'Radio Policy' section is visible, showing '6 GHz Status' (ENABLED with a red toggle), '5 GHz Status' (ENABLED with a green toggle), and '2.4 GHz Status' (ENABLED with a green toggle). The '802.11b/g Policy' is set to '802.11b/g'. A 'Show slot configuration' link is also present.

WLAN-Profil

Schritt 2: Aktivieren Sie auf der Registerkarte Sicherheit das Kontrollkästchen "Mac Filtering", und konfigurieren Sie den RADIUS-Server in der Autorisierungsliste (ISE oder lokaler Server). Bei dieser Konfiguration wird ISE sowohl für die Mac-Authentifizierung als auch für die Web-Authentifizierung verwendet.

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Authorization List*

network

OWE Transition Mode

Lobby Admin Access

Fast Transition

Status

Disabled

Over the DS

Reassociation Timeout *

20

WLAN Layer 2-Sicherheit

Schritt 3: Navigieren Sie zu Security > Layer 3. Aktivieren Sie die Webrichtlinie, und ordnen Sie sie dem Profil Web Authentication Parameter Map zu. Aktivieren Sie das Kontrollkästchen "On Mac Filter Failure" (Bei Mac-Filterfehler), und wählen Sie den RADIUS-Server aus der Dropdown-Liste "Authentication" (Authentifizierung) aus.

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map

Web-Filter

Authentication List

ISE-List

<< Hide

On MAC Filter Failure

Splash Web Redirect

DISABLED

Preauthentication ACL

For Local Login Method List to work, please make sure

Registerkarte "WLAN Layer3-Sicherheit"

CLI-Konfiguration

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
mac-filtering network
radio policy dot11 24ghz
radio policy dot11 5ghz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list ISE-List
security web-auth on-macfilter-failure
security web-auth parameter-map Web-Filter
no shutdown
```

Schritt 4: Konfigurieren von Richtlinien-Tags, Erstellen eines WLAN-Profiles und Zuordnung von Richtlinienprofilen

Navigieren Sie zu Konfiguration > Tags & Profile > Tags > Policy. Klicken Sie auf "Hinzufügen", um einen Namen für das Policy Tag (Richtlinien-Tag) zu definieren. Wählen Sie unter WLAN-Policy Maps (WLAN-Richtlinienzuordnungen) die Option Add (Hinzufügen) aus, um das zuvor erstellte WLAN- und Richtlinienprofil zuzuordnen.

The screenshot shows the Cisco ISE configuration interface for Policy Tags. At the top, there are tabs for 'Policy', 'Site', 'RF', and 'AP'. Below these tabs are buttons for '+ Add', 'Delete', and 'Clone'. The 'Add Policy Tag' dialog is open, with the following fields:

- Name*: default-policy-tag
- Description: Enter Description

Below the fields, there is a section for 'WLAN-POLICY Maps: 0' with '+ Add' and 'Delete' buttons. A table below this section shows 0 items. A red box highlights the 'Map WLAN and Policy' section, which contains two search/select dropdowns for 'WLAN Profile*' and 'Policy Profile*', and 'X' and 'Check' buttons.

CLI-Konfiguration:

```
wireless tag policy default-policy-tag  
  description "default policy-tag"  
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

Schritt 5: Navigieren Sie zu Configuration > Wireless > Access Point. Wählen Sie den Access Point aus, der für die Übertragung dieser SSID verantwortlich ist. Weisen Sie im Menü Edit AP (AP bearbeiten) die erstellte Policy Tag (Richtlinien-Tag) zu.

The screenshot shows the 'Edit AP' configuration page in the Meraki dashboard. The breadcrumb navigation is 'Configuration > Wireless > Access Points'. On the left, there is a list of 'All Access Points' with a table showing AP Name, AP Model, and a status icon. The selected AP is 'AP2-AIR-AP3802I-D-K9-2'. Below the list are sections for '6 GHz Radios' and '5 GHz Radios'. The main configuration area is titled 'Edit AP' and has several tabs: 'General', 'Interfaces', 'High Availability', 'Inventory', 'Geolocation', 'ICap', 'Advanced', and 'Support Bundle'. The 'General' tab is active. It contains fields for 'AP Name*' (AP2-AIR-AP3802I-D-K9), 'Location*' (default location), 'Base Radio MAC' (1880.902b.05e0), 'Ethernet MAC' (a023.9fd9.0834), 'Admin Status' (ENABLED), 'AP Mode' (Local), 'Operation Status' (Registered), 'Fabric Status' (Disabled), and 'CleanAir NSI Key'. The 'Tags' section is highlighted with a red box and contains a 'Policy' dropdown menu set to 'default-policy-tag', a 'Site' dropdown menu set to 'default-site-tag', and an 'RF' dropdown menu set to 'default-rf-tag'. There is also a 'Write Tag Config to AP' button. The 'Version' section shows 'Primary Software Version' as 17.12.2.35, 'Predownloaded Status' as N/A, 'Predownloaded Version' as N/A, and 'Next Retry Time' as N/A.

Richtlinienbasierte TAGs werden AP zugeordnet

AAA-Einstellungen konfigurieren:

Schritt 1: Erstellen eines Radius-Servers:

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

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

[+ Add](#) [Delete](#)

RADIUS **Servers** Server Groups

Create AAA Radius Server

Name*	<input type="text"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	<input type="text"/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="text"/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		

[Cancel](#) [Apply to Device](#)

Serverkonfiguration

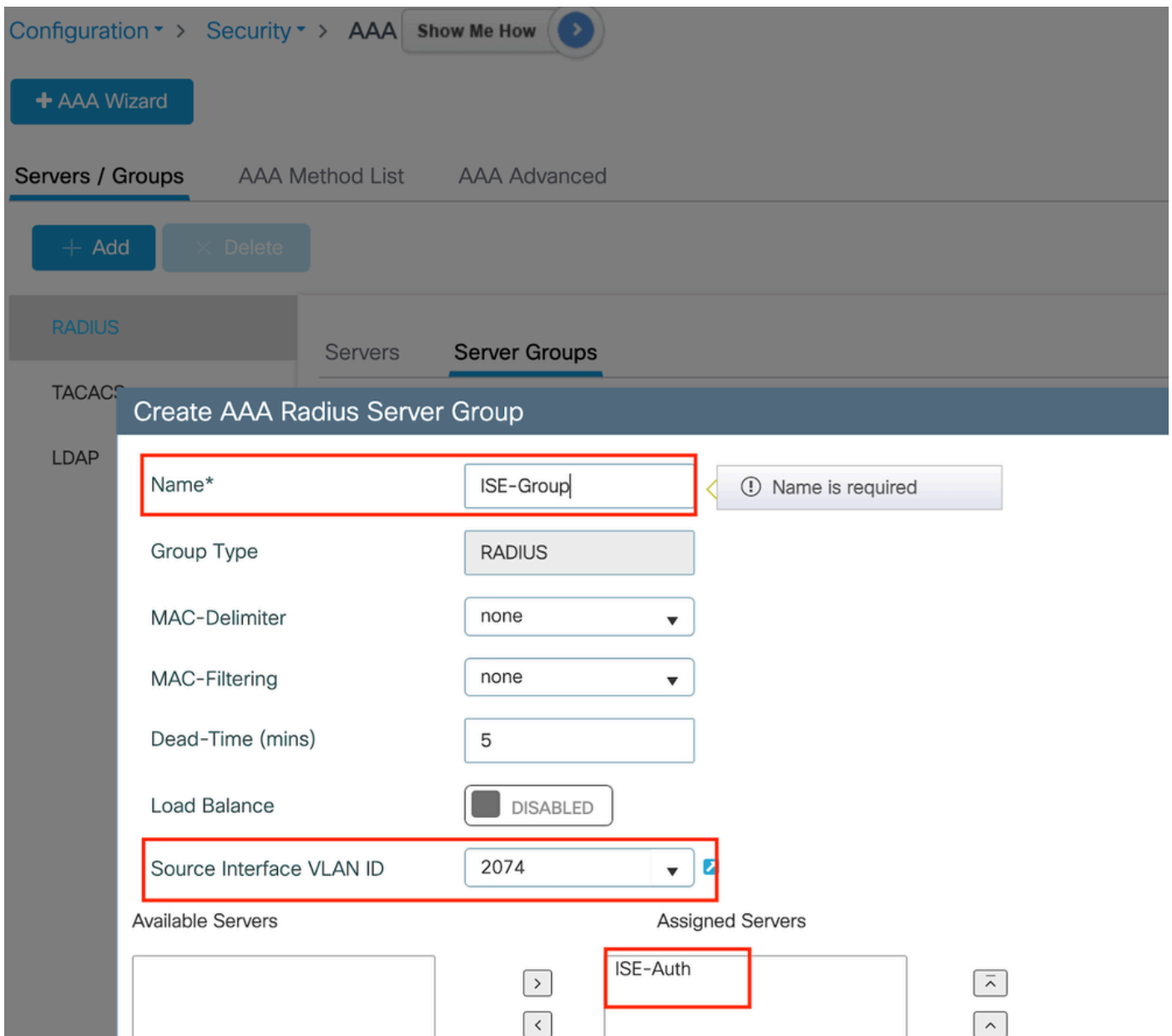
CLI-Konfiguration

```
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" (Hinzufügen) aus, um eine Servergruppe zu definieren. Schalten Sie zwischen den Servern um, die in der gleichen Gruppenkonfiguration enthalten sein sollen.

Es ist nicht erforderlich, die Quellschnittstelle festzulegen. Standardmäßig verwendet der 9800 seine Routing-Tabelle, um die Schnittstelle zu ermitteln, über die der RADIUS-Server erreicht werden kann, und verwendet in der Regel das Standard-Gateway.



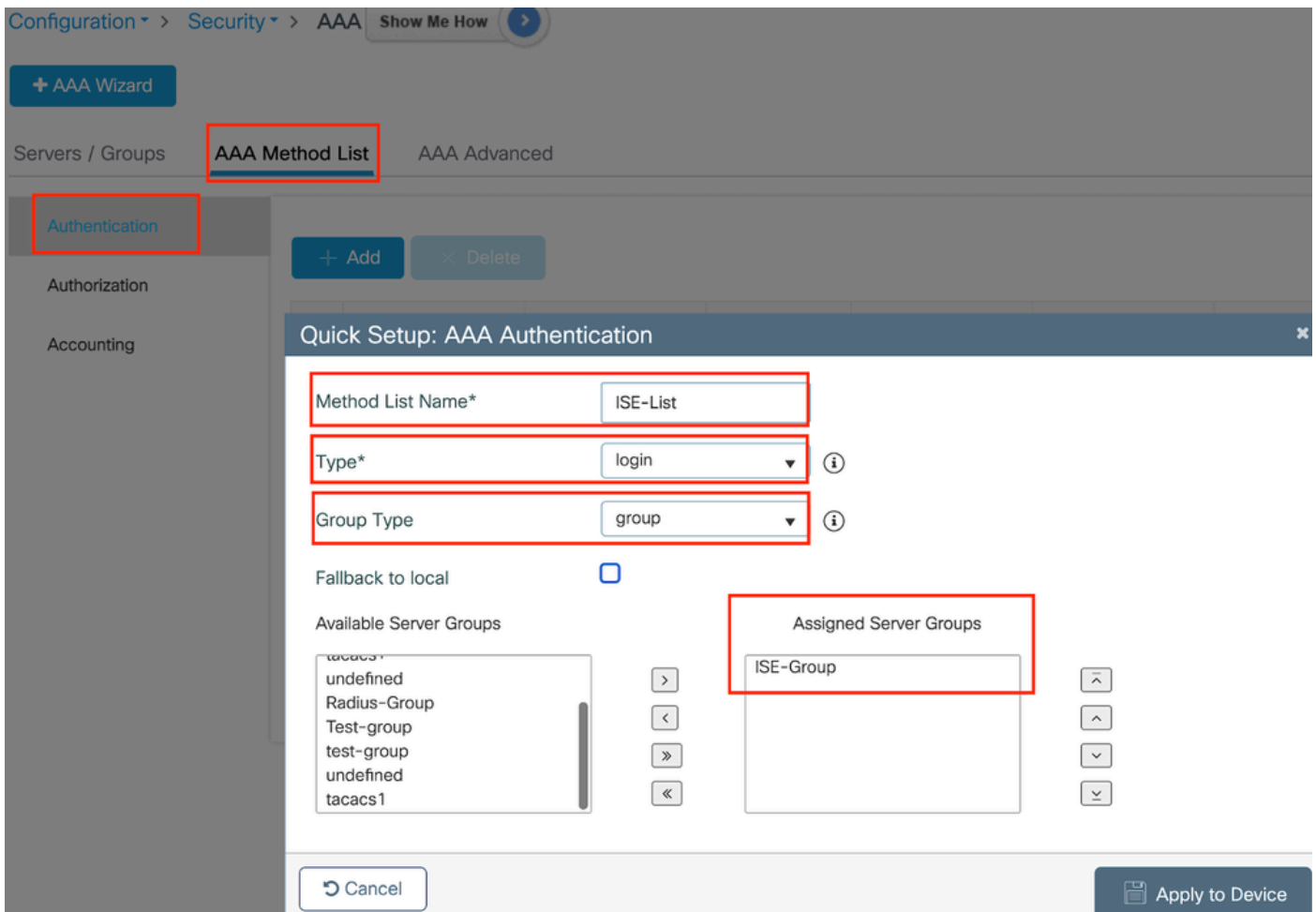
Servergruppe

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. Klicken Sie unter Authentifizierung auf Hinzufügen. Definieren Sie einen Methodenlistennamen mit Type als "login" und Group type als "Group". Ordnen Sie die konfigurierte Authentifizierungsservergruppe im Abschnitt Zugewiesene Servergruppe zu.



Liste der Authentifizierungsmethoden

CLI-Konfiguration

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

Navigieren Sie zum Abschnitt "Autorisierungsmethodenliste", und klicken Sie auf "Hinzufügen". Definieren Sie einen Methodenlistennamen, und setzen Sie den Typ auf "network", wobei Gruppentyp "Group" ist. Schalten Sie den konfigurierten RADIUS-Server in den Abschnitt Zugewiesene Servergruppen um.

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add × Delete

Quick Setup: AAA Authorization

Method List Name* network

Type* network i

Group Type group i

Fallback to local

Authenticated

Available Server Groups

Assigned Server Groups

ISE-Group

tacacs1
undefined
Radius-Group
Test-group
test-group
undefined
tacacs1

Liste der Autorisierungsmethoden

CLI-Konfiguration

```
aaa authorization network network group ISE-Group
```

ISE-Konfiguration:

WLC als Netzwerkgerät zur ISE hinzufügen

Schritt 1: Navigieren Sie zu Administration > Network Devices, und klicken Sie auf Add. Geben Sie die IP-Adresse, den Hostnamen und den gemeinsamen geheimen Schlüssel des Controllers in die Radius-Authentifizierungseinstellungen ein.

Network Devices

Name

Description

IP Address * IP : / 32

Netzwerkgerät hinzufügen

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Show

Gemeinsamer Schlüssel

Schritt 2: Benutzereintrag erstellen

Wählen Sie unter Identity Management > Identities die Option Add (Hinzufügen) aus.

Konfigurieren Sie den Benutzernamen und das Kennwort, die der Client für die Webauthentifizierung verwenden muss.

✓ Network Access User

* Username

Status Enabled

Email

✓ Passwords

Password Type:

* Login Password

Hinzufügen von Benutzeranmeldeinformationen

Schritt 3: Navigieren Sie zu Administration > Identity Management > Groups > Registered Devices, und klicken Sie auf Add.

Geben Sie die MAC-Adresse des Geräts ein, um einen Eintrag auf dem Server zu erstellen.

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

Identity Groups

- Endpoint Identity Groups
 - Blocked List
 - GuestEndpoints
 - Profiled
 - RegisteredDevices**
 - Unknown
- User Identity Groups

Endpoint Identity Group List > RegisteredDevices

Endpoint Identity Group

* Name: **RegisteredDevices**

Description: Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints Select

+ Add Remove

MAC Address Static Group Assignment Endpoint Profile

Save

MAC-Adresse des Geräts hinzufügen

Schritt 4: Erstellen einer Servicerichtlinie

Navigieren Sie zu Policy > Policy sets, und wählen Sie das Pluszeichen aus, um einen neuen Policy Set zu erstellen.

Dieser Richtlinienatz ist für die Web-Benutzerauthentifizierung vorgesehen, bei der ein Benutzername und ein Kennwort für den Client in Identity Management erstellt werden.

Policy Sets → User-Webauth Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users		Options

Richtlinie für den Webauthentifizierungsdienst

Erstellen Sie auf ähnliche Weise eine MAB-Dienstrichtlinie, und ordnen Sie interne Endpunkte

unter der Authentifizierungsrichtlinie zu.

Policy Sets -> Test-MAB Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Test-MAB		Normalised Radius-RadiusFlowType EQUALS WirelessMAB	Default Network Access ✕ +	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Endpoints ✕ v	0	> Options

Richtlinie für MAB-Authentifizierungsdienst

Überprüfung

Controller-Konfiguration

<#root>

```
show wireless tag policy detailed
```

```
default-policy-tag
```

```
Policy Tag Name : default-policy-tag  
Description      : default policy-tag  
Number of WLAN-POLICY maps: 1  
WLAN Profile Name      Policy Name
```

Mac_Filtering_Wlan

Web-Filter-Policy

<#root>

```
show wireless profile policy detailed
```

Web-Filter-Policy

```
Policy Profile Name      :
```

Web-Filter-Policy

Description :
Status :
ENABLED
VLAN :
2074
Multicast VLAN : 0

<#root>

show wlan name

Mac_Filtering_Wlan

WLAN Profile Name :

Mac_Filtering_Wlan

=====
Identifier : 9
Description :
Network Name (SSID) :

Mac_Filtering_Wlan

Status :

Enabled

Broadcast SSID :

Enabled

Mac Filter Authorization list name :

network

Webauth On-mac-filter Failure :

Enabled

Webauth Authentication List Name :

ISE-List

Webauth Authorization List Name : Disabled

Webauth Parameter Map :

Web-Filter

<#root>

show parameter-map type webauth name Web-Filter

Parameter Map Name :

Web-Filter

Type :

webauth

Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window :

Enabled

Webauth success-window :

Enabled

Consent Email : Disabled
Activation Mode : Replace
Sleeping-Client : Disabled
Webauth login-auth-bypass:

<#root>

show ip http server status

HTTP server status:

Enabled

HTTP server port:

80

HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:

Enabled

HTTP secure server port:

443

show ap name AP2-AIR-AP3802I-D-K9-2 tag detail

Policy tag mapping



WLAN Profile Name	Policy Name	VLAN	Flex
Mac_Filtering_Wlan	Web-Filter-Policy	2074	ENAB

Client-Richtlinienstatus auf Controller

Navigieren Sie zum Abschnitt Dashboard > Clients, um den Status der verbundenen Clients zu bestätigen.

Der Client befindet sich derzeit im ausstehenden Webauthentifizierungsstatus.

[Clients](#)
[Sleeping Clients](#)
[Excluded Clients](#)

[Delete](#)



Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

1 - 1 of 1 clients

Client-Details

```
show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type	ID	State	Protocol	Method
6c7e.67e3.6db9	AP2-AIR-AP3802I-D-K9-2	WLAN	9	Webauth Pending	11ac	Web

```
<#root>
```

```
show wireless client mac-address 6c7e.67e3.6db9 detail
```

```
Client MAC Address :
```

```
6c7e.67e3.6db9
```

```
Client MAC Type : Universally Administered Address
```

```
Client DUID: NA
```

```
Client IPv4 Address :
```

```
10.76.6.150
```

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
```

```
Client Username :
```

```
6c7e67e36db9
```

```
AP MAC Address : 1880.902b.05e0
```

```
AP Name: AP2-AIR-AP3802I-D-K9-2
```

```
AP slot : 1
```

```
Client State : Associated
```

```
Policy Profile :
```

Web-Filter-Policy

Flex Profile : N/A
Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List

Method : Web Auth
Webauth State :

Get Redirect

Webauth Method :

Webauth

Nach erfolgreicher Web-Authentifizierung wechselt der Client Policy Manager-Status zu RUN

<#root>

show wireless client mac-address 6c7e.67e3.6db9 detail

Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A

Fehlerbehebung

Die Funktion "Web Auth on MAC Failure" (Webauthentifizierung bei MAB-Ausfall) setzt voraus, dass der Controller bei einem MAB-Ausfall die Webauthentifizierung auslöst. Unser vorrangiges Ziel ist es, RA-Traces effizient vom Controller zur Fehlerbehebung und Analyse zu erfassen.

Erfassung radioaktiver Spuren

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 Debugdatei im Controller-Bootflash 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.

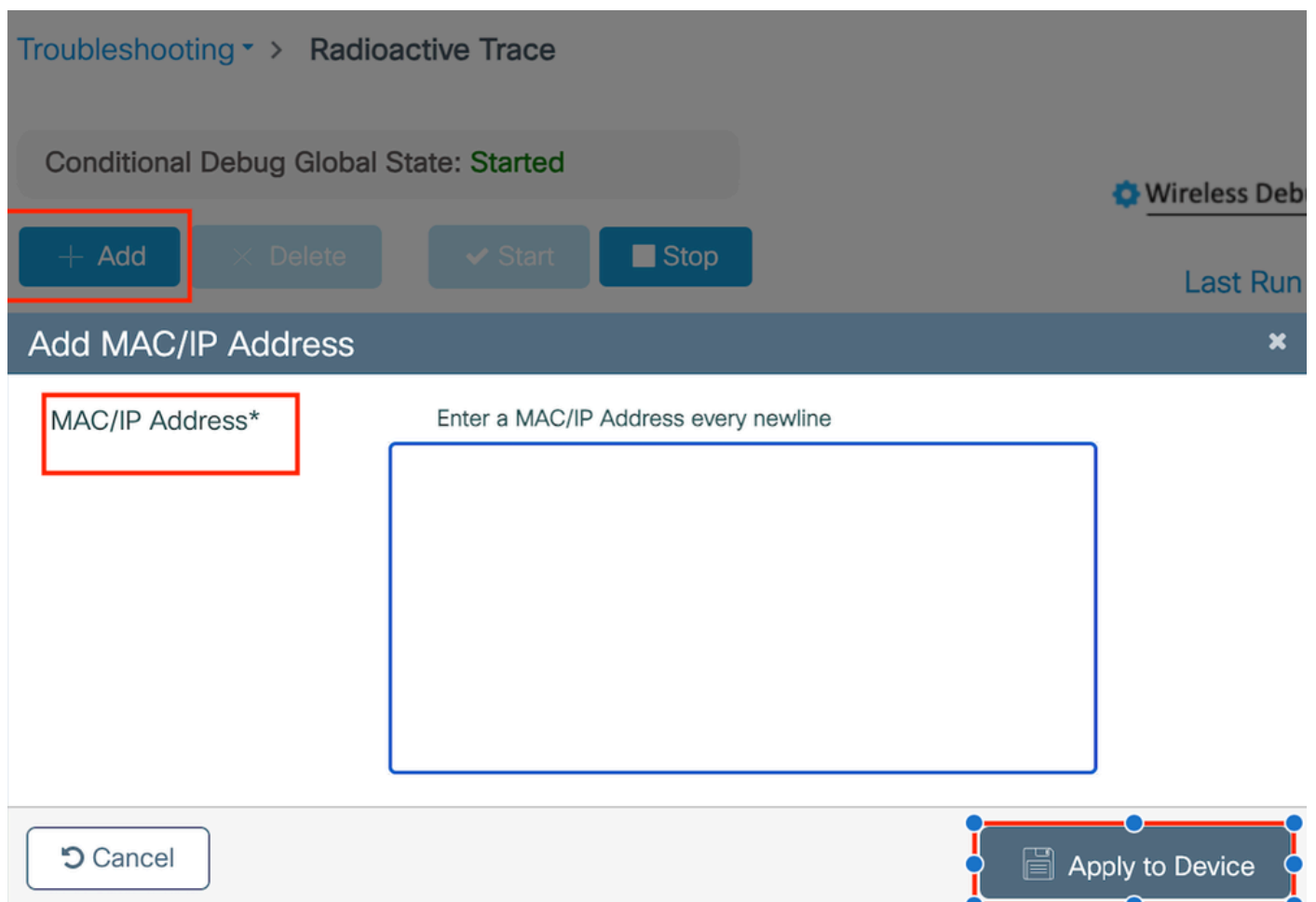
```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

Debug-Protokoll anzeigen:

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

RA Trace in GUI aktivieren,

Schritt 1: Navigieren Sie zu Troubleshooting > Radioactive Trace. Wählen Sie die Option zum Hinzufügen eines neuen Eintrags aus, und geben Sie dann die Client-MAC-Adresse auf der entsprechenden Registerkarte Add MAC/IP Address (MAC/IP-Adresse hinzufügen) ein.



Radio Active Tracing

Integrierte Paketerfassung:

Navigieren Sie zu Fehlerbehebung > Paketerfassung. Geben Sie den Erfassungsnamen ein, und geben Sie die Client-MAC-Adresse 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.

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane

Inner Filter Protocol DHCP

Inner Filter MAC

Buffer Size (MB)* 100

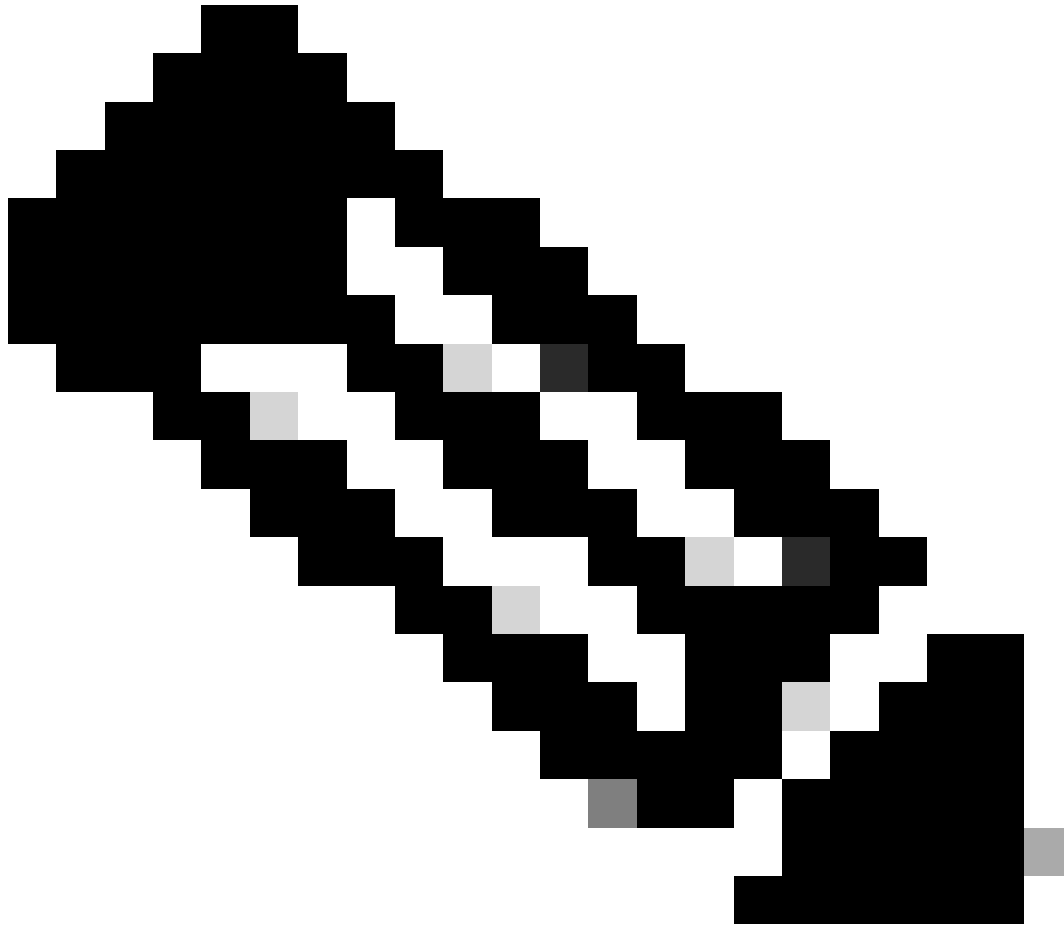
Limit by* Duration 3600 secs ≈ 1.00 hour

Available (12) Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0



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

Wählen Sie Start zum Erfassen von Paketen

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	<input type="button" value="Start"/>

Erfassung 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

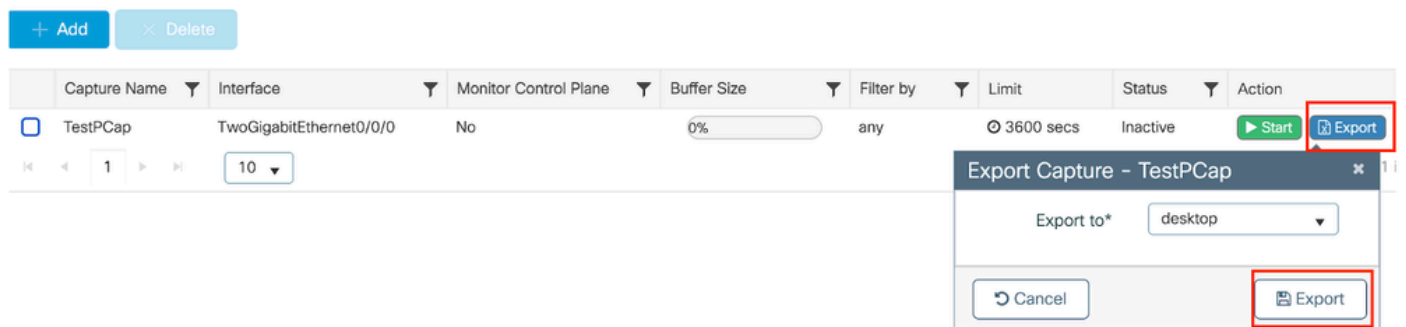
Packet Size to capture: 0 (no limit)

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
```



Paketerfassung exportieren

Beispielszenario bei erfolgreicher MAC-Authentifizierung: Ein Client-Gerät stellt eine Verbindung mit dem Netzwerk her, seine MAC-Adresse wird durch konfigurierte Richtlinien vom RADIUS-Server validiert, und bei der Verifizierung wird der Zugriff durch das Netzwerkzugriffsgerät gewährt, wodurch die Netzwerkkonnektivität ermöglicht wird.

Sobald der Client eine Zuweisung hergestellt hat, sendet der Controller eine Access-Request an den ISE-Server.

Der Benutzername ist die MAC-Adresse des Clients, da es sich um die MAB-Authentifizierung handelt.

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request to
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
```

ISE sendet Access-Accept, da ein gültiger Benutzereintrag vorliegt

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

Der Client-Richtlinienstatus wurde in Mac Auth abgeschlossen.

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29 Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

Client befindet sich nach erfolgreicher MAB-Authentifizierung im IP-Lernstatus

```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d29
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

Client-Richtlinienmanager-Status auf "RUN" aktualisiert; Web-Authentifizierung wird für den Client übersprungen, der die MAB-Authentifizierung abschließt

2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD

Überprüfung mithilfe von Embedded Packet Capture

No.	Time	Source	Destination	Length	Protocol	Info
53	02:42:52.710961	10.76.6.156	10.197.224.122		RADIUS	Access-Request id=0
54	02:42:52.778951	10.197.224.122	10.76.6.156		RADIUS	Access-Accept id=0

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x0 (0)
Length: 422
Authenticator: 19c6635633a7e6b6f30070b02a7f753c
[\[The response to this request is in frame 54\]](#)
Attribute Value Pairs
> AVP: t=User-Name(1) l=14 val=6c7e67b72d29
> AVP: t=User-Password(2) l=18 val=Encrypted
> AVP: t=Service-Type(6) l=6 val=Call-Check(10)
> AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
> AVP: t=Framed-MTU(12) l=6 val=1485

Radius-Paket

Beispiel: MAC-Authentifizierungsfehler für ein Client-Gerät

Mac-Authentifizierung für einen Client nach erfolgreicher Zuordnung initiiert

2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Success
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 C
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]

Die ISE sendet eine Access-Reject-Nachricht, da dieser Geräteeintrag in der ISE nicht vorhanden ist.

2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000

Web-Auth für Client-Gerät initiiert, da MAB fehlgeschlagen ist

```
2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cli
```

Nachdem der Client eine HTTP GET-Anforderung initiiert hat, wird die Umleitungs-URL auf das Client-Gerät weitergeleitet, da die entsprechende TCP-Sitzung vom Controller gespoofed wird.

```
2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6
```

Der Client initiiert einen HTTP-Abruf zur Umleitungs-URL und sendet die Anmeldeinformationen, sobald die Seite geladen wurde.

Der Controller sendet eine Zugriffsanforderung an die ISE.

Dies ist eine Webauthentifizierung, da ein gültiger Benutzername im Access-Accept-Paket festgestellt wird.

```
2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
```

Von ISE erhaltene Zugriffsgenehmigung

```
2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

Die Webauthentifizierung ist erfolgreich, und der Client-Status wechselt in den RUN-Status.

```
2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db
```

Überprüfung durch EPC-Aufzeichnungen

Der Client schließt den TCP-Handshake mit der virtuellen IP-Adresse des Controllers ab, und der Client lädt die Portalseite für die Umleitung. Sobald der Benutzer Benutzername und Passwort übermittelt, können wir eine RADIUS-Zugriffsanfrage von der IP-Adresse des Controllers beobachten.

Nach erfolgreicher Authentifizierung wird die Client-TCP-Sitzung geschlossen, und der Client wechselt auf dem Controller in den RUN-Status.

15649	08:52:51.122979	10.76.6.150	192.0.2.1	TCP	58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650	08:52:51.123986	192.0.2.1	10.76.6.150	TCP	443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=4022788871
15651	08:52:51.125985	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652	08:52:51.126992	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
15653	08:52:51.126992	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654	08:52:51.126992	192.0.2.1	10.76.6.150	85,1,64	TLSv1.2 Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655	08:52:51.129982	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656	08:52:51.129982	10.76.6.150	192.0.2.1	1,64	TLSv1.2 Change Cipher Spec, Encrypted Handshake Message
15657	08:52:51.130989	10.76.6.150	192.0.2.1	640	TLSv1.2 Application Data
15658	08:52:51.130989	10.76.6.150	192.0.2.1	160	TLSv1.2 Application Data
15659	08:52:51.130989	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3
15665	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment i
15667	08:52:51.191976	192.0.2.1	10.76.6.150	2496	TLSv1.2 Application Data
15668	08:52:51.192983	192.0.2.1	10.76.6.150	48	TLSv1.2 Encrypted Alert
15673	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15676	08:52:51.197987	10.76.6.150	192.0.2.1	48	TLSv1.2 Encrypted Alert
15677	08:52:51.197987	10.76.6.150	192.0.2.1	TCP	58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0

TCP-Fluss mit Radius-Paket

15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
 Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
 Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
 User Datagram Protocol, Src Port: 65433, Dst Port: 1812
 RADIUS Protocol

- Code: Access-Request (1)
- Packet identifier: 0x3 (3)
- Length: 457
- Authenticator: fd400f7e3567dc5a63cfefaeaf379eaa
- [\[The response to this request is in frame 15663\]](#)
- Attribute Value Pairs
 - AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
 - AVP: t=User-Name(1) l=10 val=testuser
 - AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
 - AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
 - AVP: t=Message-Authenticator(00) l=16 val=501b124c30216efd5973086d99f3a185
 - AVP: t=Service-Type(6) l=6 val=Dialog-Framed-User(5)
 - AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
 - AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
 - AVP: t=User-Password(2) l=18 val=Encrypted

Radius-Paket wird mit Benutzeranmeldeinformationen an die ISE gesendet

Client-seitige Erfassung von Wireshark-Daten zur Überprüfung, ob der Client-Datenverkehr zur Portalseite umgeleitet wird, und Überprüfung des TCP-Handshakes zur virtuellen IP-Adresse/zum Webserver des Controllers

Time	Source	Destination	Length	Protocol	Info
105	08:51:34.203945	10.76.6.150	10.76.6.145	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
108	08:51:34.206602	10.76.6.145	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)
234	08:51:39.028084	10.76.6.150	7.7.7.7	HTTP	GET / HTTP/1.1
236	08:51:39.031420	7.7.7.7	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)

Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
 Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
 Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
 Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637

Hypertext Transfer Protocol

Line-based text data: text/html (9 lines)

```
<HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
<HEAD>\n
<TITLE> Web Authentication Redirect</TITLE>\n
<META http-equiv="Cache-control" content="no-cache">\n
<META http-equiv="Pragma" content="no-cache">\n
<META http-equiv="Expires" content="-1">\n
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
</HEAD>\n
</HTML>
```

Erfassung auf Clientseite zur Validierung der Umleitungs-URL

Client richtet TCP-Handshake zur virtuellen IP-Adresse des Controllers ein

Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1	TCP	58812 → 443 [SYN, ECE, CW] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_P
117	08:51:34.211190	192.0.2.1	10.76.6.150	TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr=
118	08:51:34.211275	10.76.6.150	192.0.2.1	TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150	TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLSv1.2 Server Hello, Certificate
125	08:51:34.220835	192.0.2.1	10.76.6.150	783,4	TLSv1.2 Server Key Exchange, Server Hello Done

TCP-Handshake zwischen Client und Webserver

Die Sitzung wird nach erfolgreicher Webauthentifizierung beendet.

144	08:51:34.235915	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLSv1.2 Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1	TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLSv1.2 Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150	TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

TCP-Sitzung nach Abschluss der Webauthentifizierung durch den Client geschlossen

Verwandter Artikel

[Wireless-Fehlerbehebungen und Protokollierung auf Catalyst 9800 Wireless LAN-Controllern](#)

[Webbasierte Authentifizierung am 9800](#)

[Lokale Webauthentifizierung auf 9800 konfigurieren](#)

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.