

# Fehlerbehebung bei zentraler Webauthentifizierung (CWA) mit Wireless LAN Controller (WLC) 9800 und Identity Services Engine (ISE)

## Inhalt

---

[Einleitung](#)

[Hintergrundinformationen](#)

[Detaillierter Datenfluss](#)

[Fehlerbehebung](#)

[Häufige Symptome: Benutzer wird nicht zur Anmeldeseite weitergeleitet.](#)

- [1 - Ist die erste RADIUS-Authentifizierung erfolgreich?](#)
- [2 - WLC empfängt die URL und ACL für die Umleitung?](#)
- [3 - Ist die Umleitungszugriffskontrollliste korrekt?](#)
- [4 - Wird der Client auf Web-Auth Pending \(Webauthentifizierung ausstehend\) verschoben?](#)
- [5 - Lässt WLC DHCP- und DNS-Datenverkehr zu?](#)
- [6 - Empfängt der DHCP-Server eine DHCP-Erkennung/Anforderung?](#)
- [7 - Wird die automatische Umleitung durchgeführt?](#)
- [8 - Im Browser wird keine Anmeldeseite angezeigt?](#)
- [9 - Kann der Client den ISE-Hostnamen auflösen?](#)
- [10 - Login-Seite immer noch nicht geladen?](#)
- [11 - Warum wird die Sicherheit durch das Zertifikat verletzt?](#)
- [12 - Fehler bei der Gastanmeldung?](#)
- [13 - Anmeldung erfolgreich, aber nicht zu RUN?](#)
- [14 - COA-Fehler?](#)

[Schlussfolgerung](#)

[Referenzen](#)

---

## Einleitung

In diesem Dokument wird die Fehlerbehebung bei der zentralen Webauthentifizierung (CWA) mit dem WLC 9800 und der ISE beschrieben.

## Hintergrundinformationen

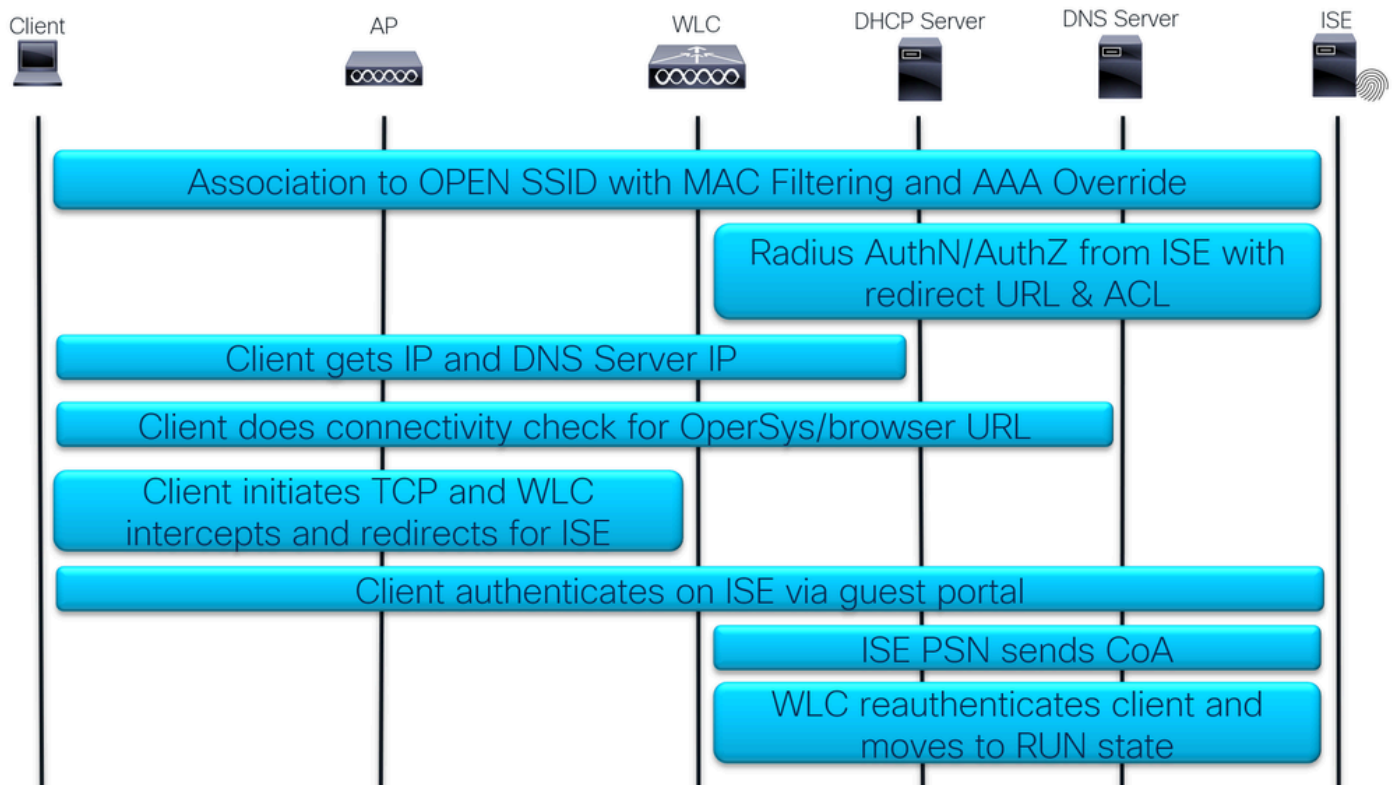
Es gibt derzeit so viele private Geräte, dass Netzwerkadministratoren, die den Wireless-Zugriff sichern möchten, sich normalerweise für Wireless-Netzwerke entscheiden, die CWA verwenden. In diesem Dokument konzentrieren wir uns auf das Flussdiagramm von CWA, das bei der Fehlerbehebung von häufigen Problemen hilft, die uns betreffen.

Wir betrachten die allgemeinen Punkte des Prozesses, wie Protokolle im Zusammenhang mit dem CWA gesammelt werden, wie diese Protokolle analysiert werden und wie eine eingebettete

Paketerfassung auf dem WLC gesammelt wird, um den Datenverkehrsfluss zu bestätigen.

CWA ist die gängigste Konfiguration für Unternehmen, die Benutzern die Verbindung mit dem Unternehmensnetzwerk über ihre privaten Geräte, auch BYOD genannt, ermöglichen. Jeder Netzwerkadministrator ist an den erforderlichen Schritten zur Fehlerbehebung und -behebung interessiert, die er durchführen kann, um seine Probleme zu beheben, bevor er ein TAC-Ticket erstellt.

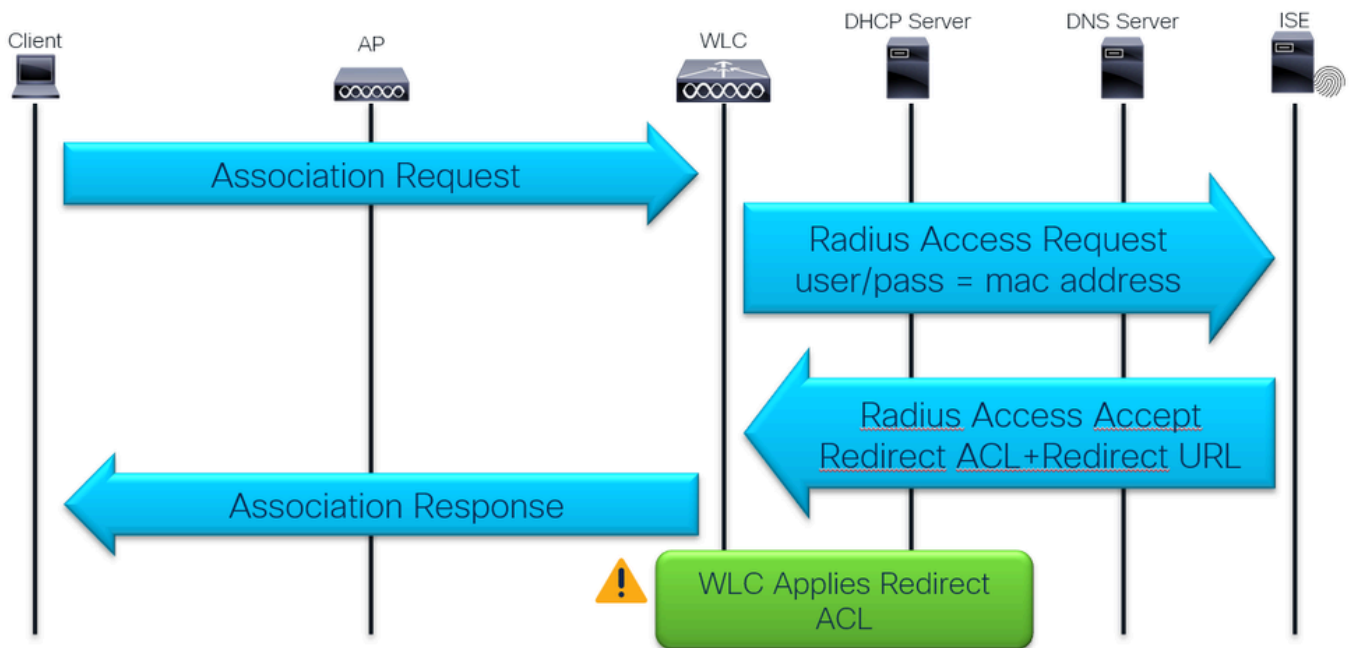
Dies ist der CWA-Paketfluss:



CWA-Paketfluss

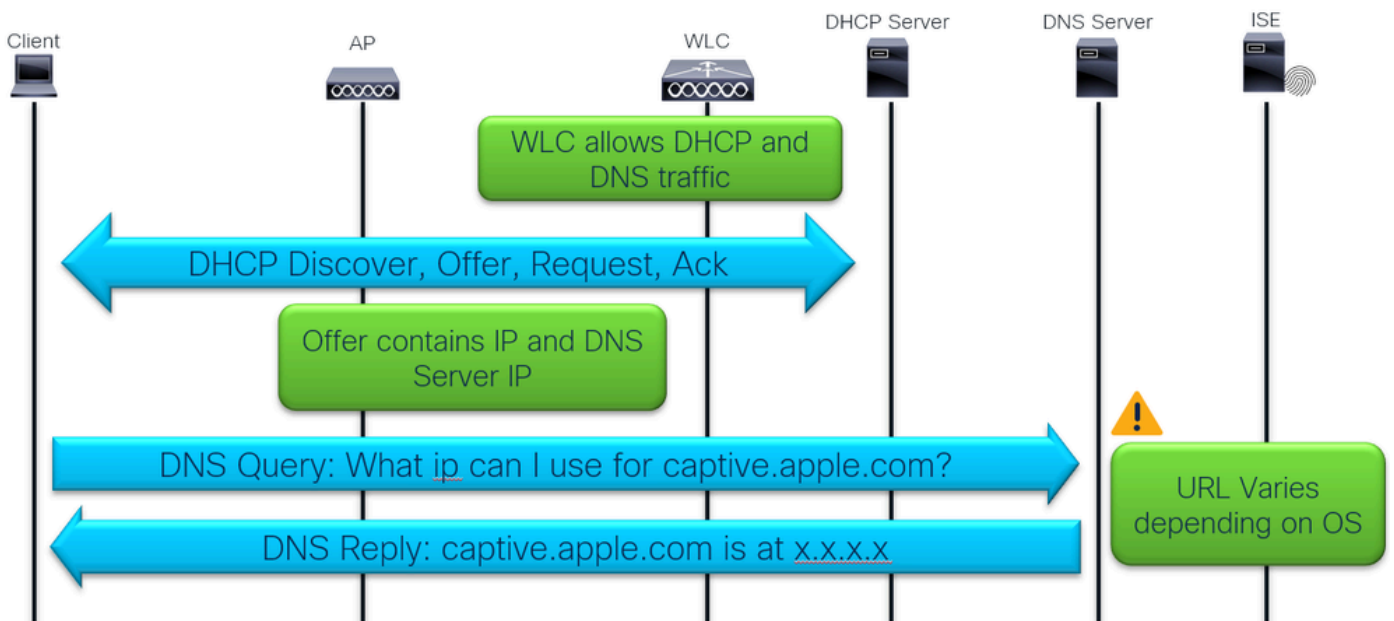
## Detaillierter Datenfluss

Erste Zuordnung und RADIUS-Authentifizierung:



Erste Zuordnung und RADIUS-Authentifizierung

DHCP, DNS und Verbindungsüberprüfung:



DHCP, DNS und Konnektivitätsprüfung

Die Konnektivitätsprüfung wird mithilfe der Captive Portal-Erkennung durch das Betriebssystem oder den Browser des Client-Geräts durchgeführt.

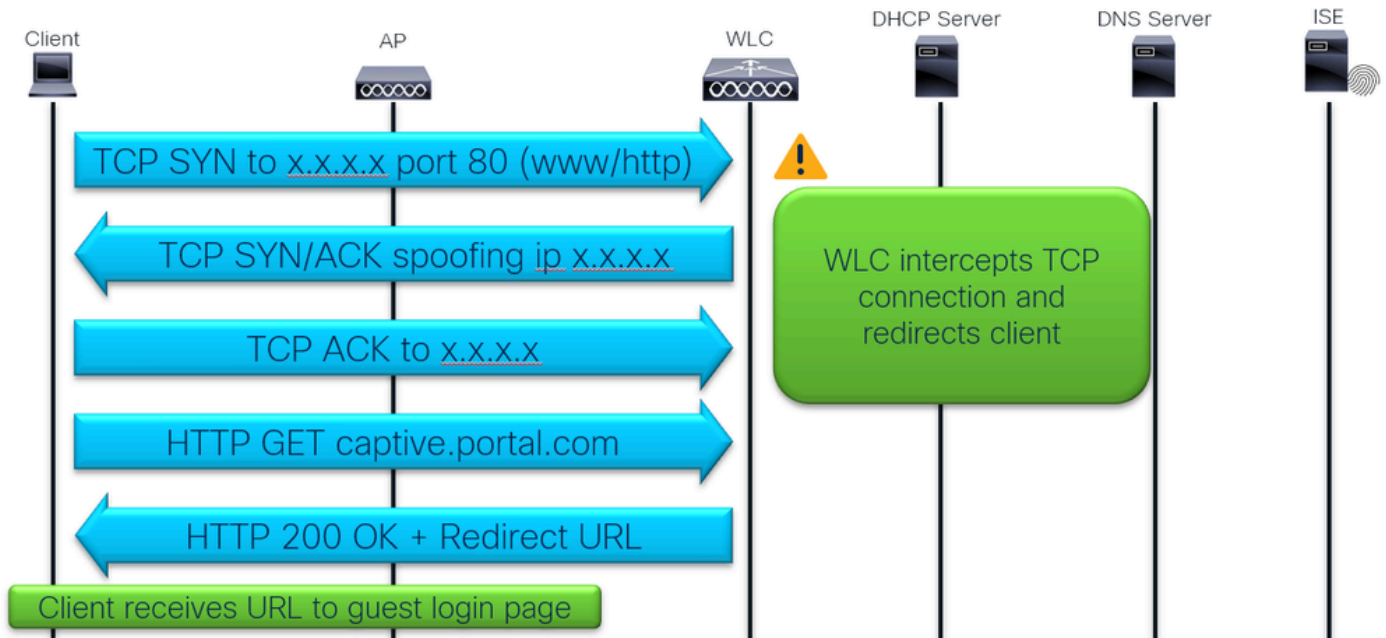
Es gibt ein Betriebssystem für Geräte, das für HTTP GET für eine bestimmte Domäne vorprogrammiert ist.

- Apple = captive.apple.com
- Android = connectivitycheck.gstatic.com
- Windows = msftconnecttest.com

Browser führen diese Prüfung auch beim Öffnen aus:

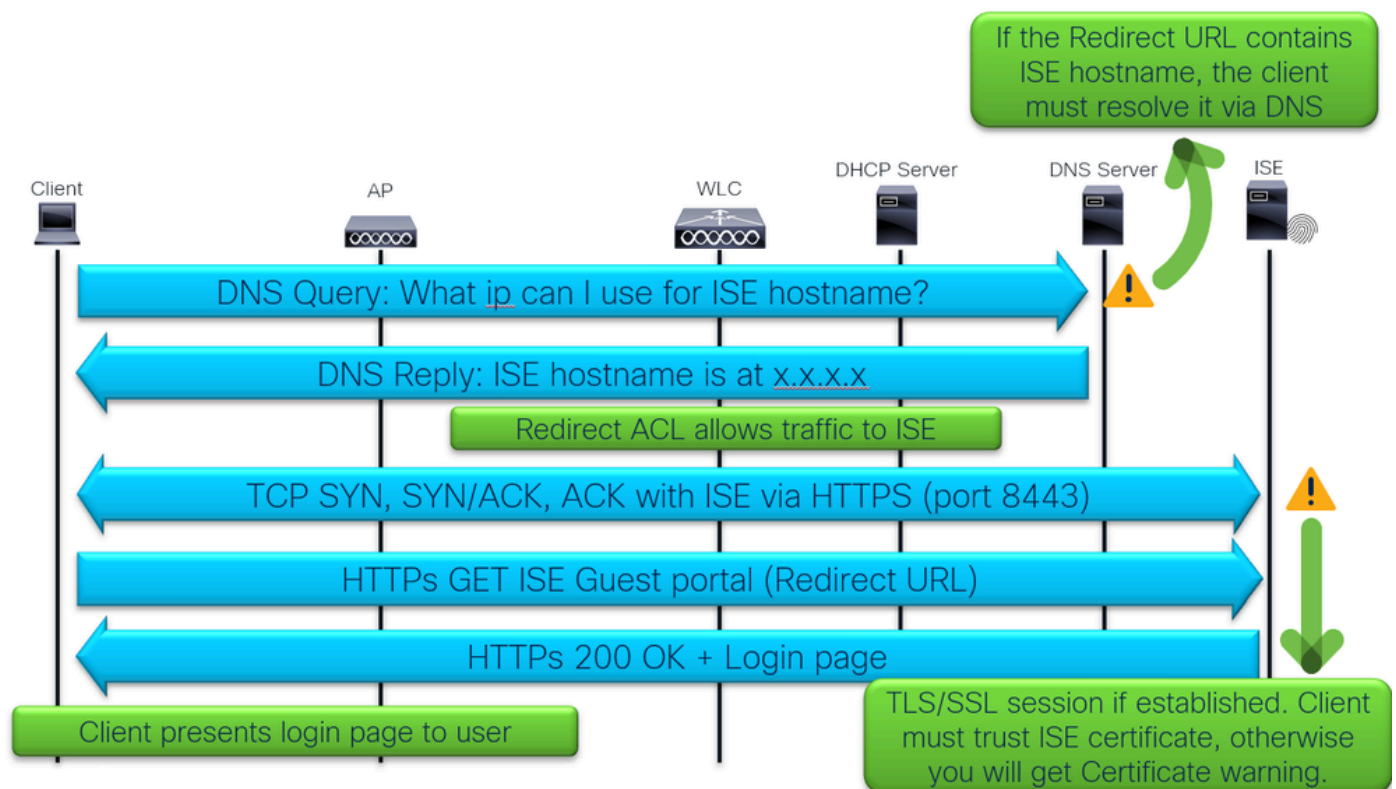
- Chrome = clients3.google.com
- Firefox = detectportal.firefox.com

Überwachung und Umleitung des Datenverkehrs:



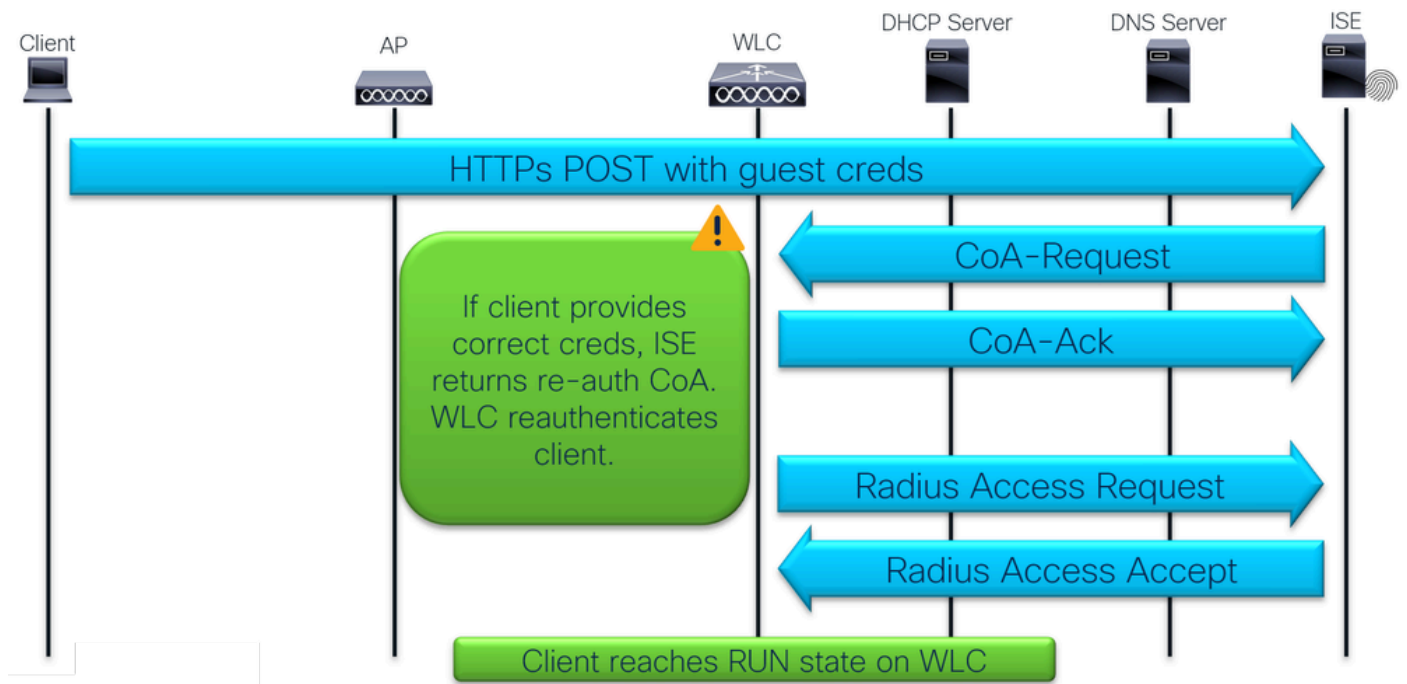
Überwachung und Weiterleitung des Datenverkehrs

Client-Anmeldung beim ISE-Gastanmeldeportal:



Client-Anmeldung beim ISE-Gastanmeldeportal

## Client-Anmeldung und CoA:

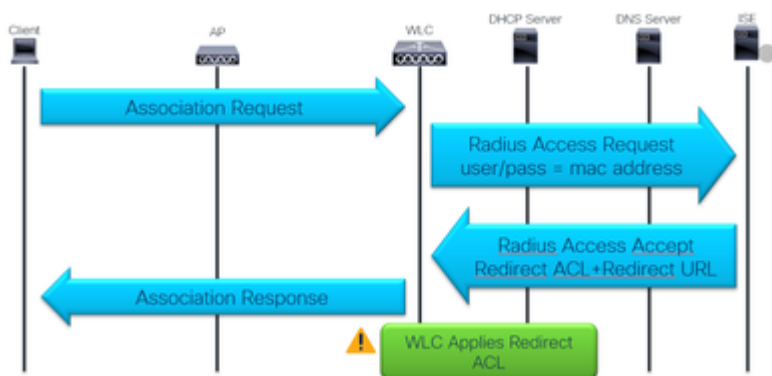


Client-Anmeldung und CoA

## Fehlerbehebung

Häufige Symptome: Benutzer wird nicht zur Anmeldeseite weitergeleitet.

Beginnen wir mit dem ersten Teil des Flusses:



Erste Zuordnung und RADIUS-Authentifizierung

1 - Ist die erste RADIUS-Authentifizierung erfolgreich?

Ergebnis der MAC-Filterauthentifizierung überprüfen:

The screenshot displays the Cisco ISE Operations - RADIUS interface. It includes sections for 'Misconfigured Supplicants' and 'Misconfigured Network Devices', both showing 0 items. The 'Live Logs' section contains a table with columns: Time, Status, Details, Repeats, Identity, and Endpoint ID. A log entry for Jan 13, 2023 09:42:37.4... is highlighted with a red box. The 'Authentication Details' section shows a failure reason: '22056 Subject not found in the applicable identity store(s)'. The 'Steps' section shows a sequence of events, with step 22056 highlighted by a red box.

ISE-Live-Protokolle mit MAC-Filterauthentifizierungsergebnis

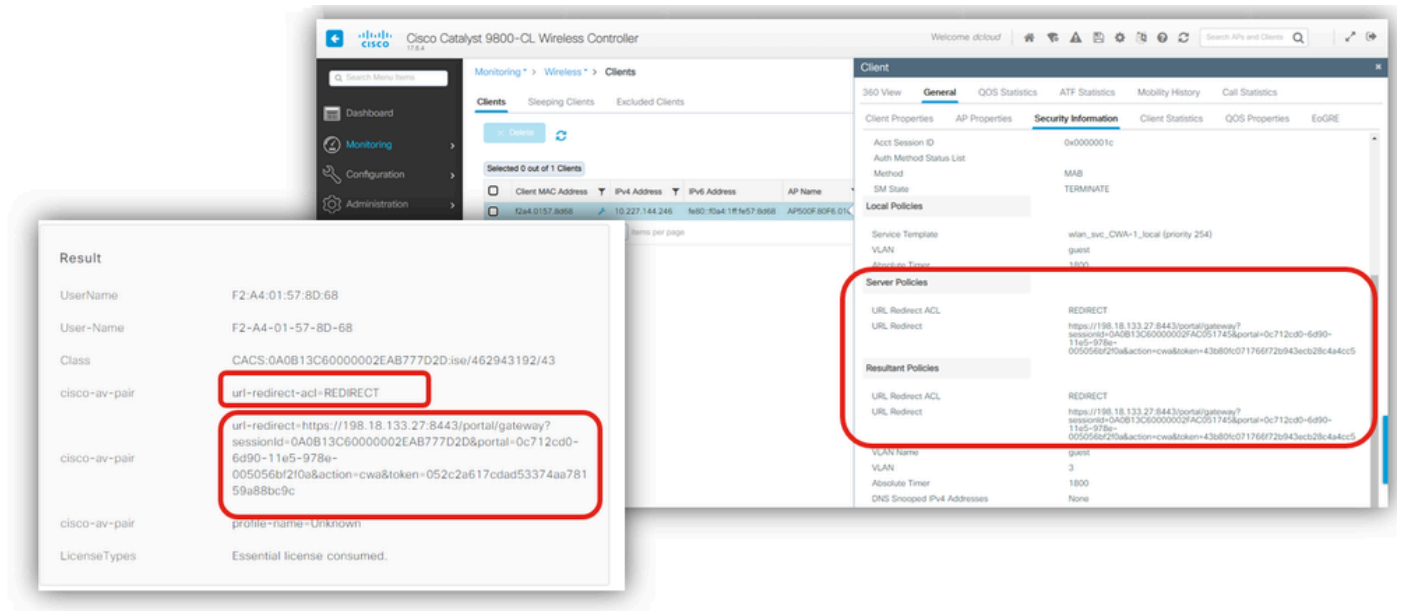
Stellen Sie sicher, dass die erweiterte Option für die Authentifizierung auf "Weiter" gesetzt ist, wenn der Benutzer nicht gefunden wurde:

The screenshot displays the Cisco ISE Policy - Policy Sets interface. It shows a table of Policy Sets with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. A policy set named 'Default' is highlighted. Below this, the 'Authentication Policy (2)' rule is shown. The rule is named 'CWA' and has a condition 'Wireless\_MAB'. The 'Options' section shows a dropdown menu with 'CONTINUE' selected, highlighted by a red box.

Erweiterte Option wurde nicht gefunden

2 - WLC empfängt die URL und ACL für die Umleitung?

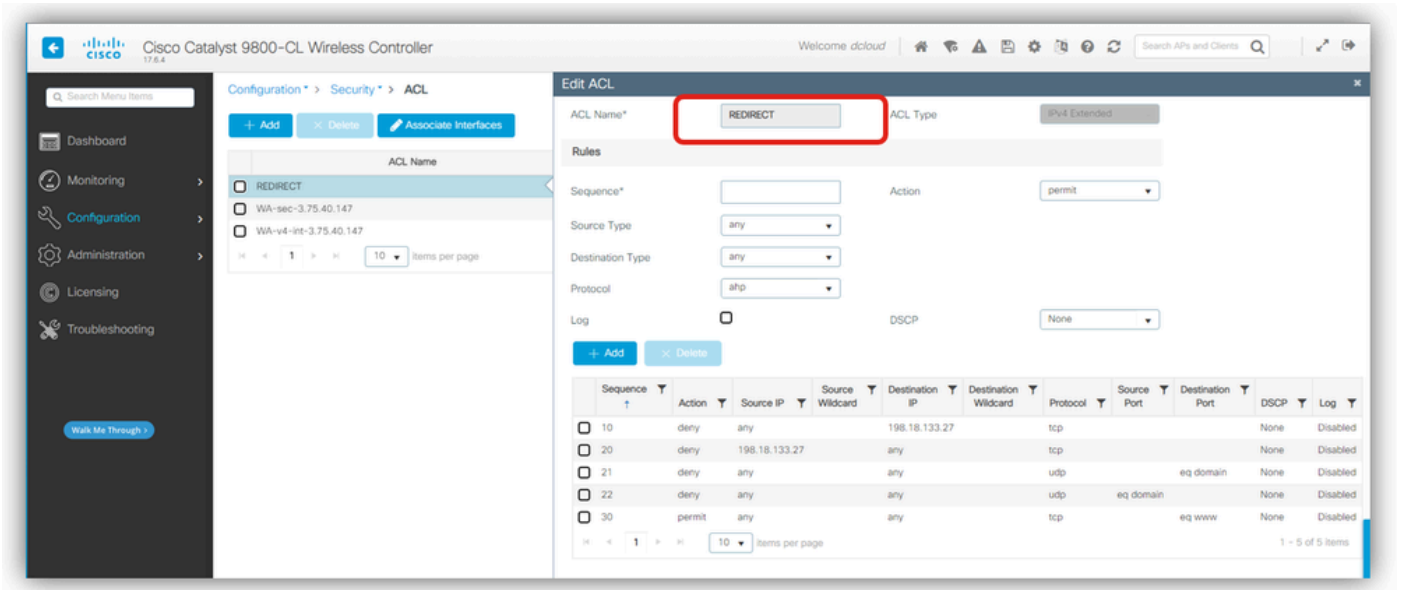
Überprüfen Sie die ISE-Live-Protokolle und die WLC-Client-Sicherheitsinformationen unter Überwachung. Überprüfen Sie, ob die ISE eine Umleitungs-URL und ACL im Access Accept sendet und diese vom WLC empfangen und in den Client-Details auf den Client angewendet werden:



ACL und URL umleiten

### 3 - Ist die Umleitungszugriffskontrollliste korrekt?

Überprüfen Sie den ACL-Namen für einen beliebigen Tippfehler. Vergewissern Sie sich, dass es genau so ist, wie es von der ISE gesendet wurde:



ACL-Überprüfung umleiten

### 4 - Wird der Client auf Web-Auth Pending (Webauthentifizierung ausstehend) verschoben?

Überprüfen Sie die Clientdetails auf den Status "Webauthentifizierung ausstehend". Wenn sich der Status nicht in diesem Zustand befindet, überprüfen Sie, ob AAA override und Radius NAC im Richtlinienprofil aktiviert sind:

Monitoring > Wireless > Clients

Clients
Sleeping Clients
Excluded Clients

Delete
Refresh

Selected 0 out of 1 Clients

|                          | Client MAC Address | IPv4 Address | IPv6 Address             | AP Name          | SSID  | WLAN ID | Client Type | State            |
|--------------------------|--------------------|--------------|--------------------------|------------------|-------|---------|-------------|------------------|
| <input type="checkbox"/> | f2a4.0157.8d68     | 198.19.1.11  | fe80::f0a4:1ff:fe57:8d68 | AP500F.80F6.0168 | CWA-1 | 4       | WLAN        | Web Auth Pending |

1
10 Items per page

Edit Policy Profile

IPv4 DHCP Required
☐

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override
☒

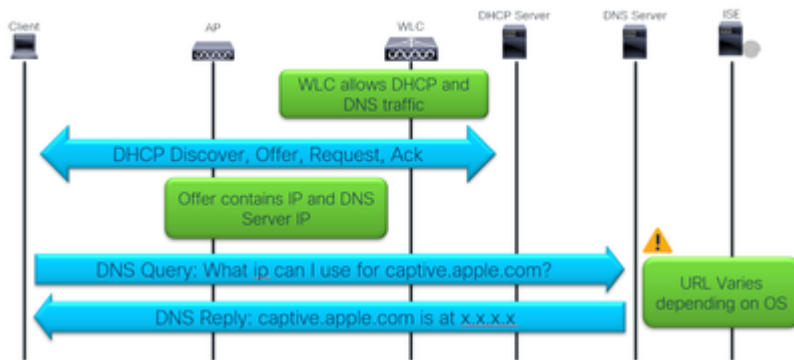
NAC State
☒

NAC Type
RADIUS

Client-Details, aaa override und RADIUS NAC

Funktioniert es immer noch nicht?

Sehen wir uns nun den Ablauf noch einmal an ...



DHCP, DNS und Konnektivitätsprüfung

5 - Lässt WLC DHCP- und DNS-Datenverkehr zu?

Überprüfen Sie den Inhalt der Umleitungszugriffskontrollliste im WLC:

Cisco Catalyst 9800-CL Wireless Controller
Welcome dcloud

Configuration > Security > ACL

Add
Delete
Associate Interfaces

ACL Name

☐ REDIRECT
☐ WA-sec-3.75.40.147
☐ WA-v4-int-3.75.40.147

1
10 Items per page

Edit ACL

ACL Name\*
REDIRECT
ACL Type
IPv4 Extended

Rules

Sequence\*
Action
permit

Source Type
any

Destination Type
any

Protocol
shp

Log
☐
DSCP
None

Add
Delete

| Sequence                    | Action | Source IP     | Source Wildcard | Destination IP | Destination Wildcard | Protocol | Source Port | Destination Port | DSCP | Log      |
|-----------------------------|--------|---------------|-----------------|----------------|----------------------|----------|-------------|------------------|------|----------|
| <input type="checkbox"/> 10 | deny   | any           |                 | 198.18.133.27  |                      | tcp      |             |                  | None | Disabled |
| <input type="checkbox"/> 20 | deny   | 198.18.133.27 |                 | any            |                      | tcp      |             |                  | None | Disabled |
| <input type="checkbox"/> 21 | deny   | any           |                 | any            |                      | udp      |             | eq domain        | None | Disabled |
| <input type="checkbox"/> 22 | deny   | any           |                 | any            |                      | udp      |             | eq domain        | None | Disabled |
| <input type="checkbox"/> 30 | permit | any           |                 | any            |                      | tcp      |             | eq www           | None | Disabled |

1
10 Items per page

ACL-Inhalte im WLC umleiten



Die Umleitungs-ACL definiert, welcher Datenverkehr von der permit-Anweisung abgefangen und umgeleitet wird und welcher Datenverkehr von der Interception und Umleitung mit einer deny-Anweisung ignoriert wird.

In diesem Beispiel lassen wir zu, dass DNS- und Datenverkehr zu/von der ISE-IP-Adresse fließt, und unterbrechen den TCP-Datenverkehr auf Port 80 (www).

6 - Empfängt der DHCP-Server eine DHCP-Erkennung/Anforderung?

Mit EPC überprüfen, ob DHCP-Austausch erfolgt. EPC kann mit internen Filtern wie dem DHCP-Protokoll und/oder der inneren Filter-MAC-Adresse verwendet werden, wobei die MAC-Adresse des Client-Geräts verwendet werden kann und nur DHCP-Pakete vom EPC gesendet oder an die MAC-Adresse des Client-Geräts gesendet werden.

In diesem Beispiel werden die DHCP Discover-Pakete angezeigt, die als Broadcast über VLAN 3 gesendet wurden:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Packet Capture' section is active, displaying a list of captured packets. A red box highlights the 'Edit Packet Capture' configuration, showing 'Capture Name: test', 'Filter: any', 'Monitor Control Plane: On', 'Inner Filter Protocol: DHCP', and 'Inner Filter MAC: f2a4.0157.8958'. A blue cloud callout points to this configuration with the text 'Inner filters !!'. Below the configuration, a table lists captured packets. A red box highlights a specific packet (Frame 2) with details: '352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface 1/0/24, Src: f2a4:0157:8d68 (f2a4:0157:8d68), Dst: Broadcast (ff:ff:ff:ff:ff:ff), Internet Protocol Version 4, Src: 10.10.10.1, Dst: 255.255.255.255, User Datagram Protocol, Src Port: 68, Dst Port: 67, Dynamic Host Configuration Protocol (Discover)'. An orange cloud callout points to this packet with the text 'Sent as broadcast on VLAN 3'.

WLC-EPC zur DHCP-Verifizierung

Bestätigen Sie das erwartete Client-VLAN im Richtlinienprofil:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Configuration' section is active, displaying the 'Tags & Profiles' view. The 'Policy' section is selected, showing a list of policy profiles. A red box highlights the 'Edit Policy Profile' configuration for the 'CWA-1' profile. The 'Access Policies' tab is active, showing the 'WLAN' section. The 'VLAN/VLAN Group' is set to 'guest', and the 'Multicast VLAN' is set to 'Enter Multicast VLAN'. A red box highlights this configuration.

## Überprüfen der WLC-VLAN- und Switch-Port-Trunk-Konfiguration und des DHCP-Subnetzes

```
WLC1#show vlan

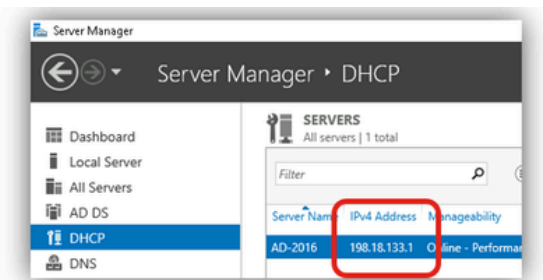
VLAN Name                Status    Ports
-----
1    default                active    Gi2, Gi3
2    employee                active
3    guest                   active
11   mgmt                     active

WLC1#show ip int br

Interface                IP-Address      OK? Method Status    Protocol
GigabitEthernet1         unassigned      YES unset  up        up
GigabitEthernet2         unassigned      YES unset  administratively down down
GigabitEthernet3         unassigned      YES unset  administratively down down
Vlan1                     unassigned      YES NVRAM  up        up
Vlan2                     198.19.2.2      YES NVRAM  up        up
Vlan3                     198.19.1.2      YES NVRAM  up        up
Vlan11                    198.19.11.10   YES NVRAM  up        up

WLC1#show run int vlan 3
Building configuration...

Current configuration : 109 bytes
!
interface Vlan3
 description guest
 ip address 198.19.1.2 255.255.255.0
 no mop enabled
 no mop sysid
end
```



If DHCP server is on different subnet we need **ip helper address** on SVI

### VLAN, Switch-Port und DHCP-Subnetz

Wie wir sehen können, ist VLAN 3 im WLC vorhanden und verfügt auch über SVI für VLAN 3. Wenn wir jedoch die IP-Adresse des DHCP-Servers in einem anderen Subnetz überprüfen, benötigen wir die IP Helper-Adresse auf der SVI.

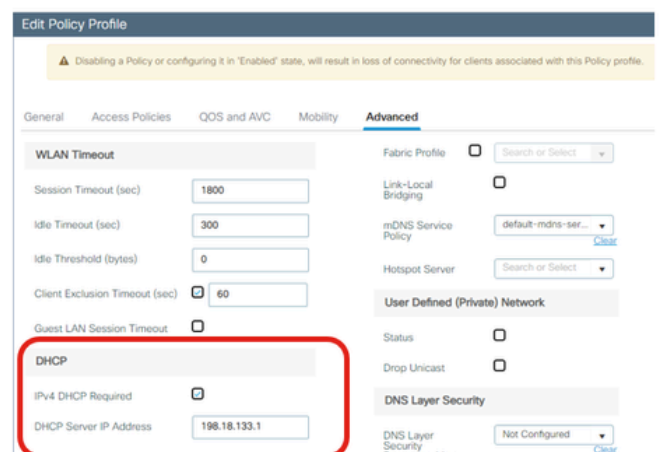
Best Practices schreiben vor, dass SVI für Client-Subnetze in der kabelgebundenen Infrastruktur konfiguriert werden muss, um sie am WLC zu vermeiden.

In allen Fällen muss der Befehl `ip helper-address` zur SVI hinzugefügt werden, unabhängig davon, wo sich diese befindet.

Eine Alternative besteht darin, die IP-Adresse des DHCP-Servers im Richtlinienprofil zu konfigurieren:

```
WLC1#show run int vlan 3
Building configuration...

Current configuration : 141 bytes
!
interface Vlan3
 description guest
 ip address 198.19.1.2 255.255.255.0
 ip helper-address 198.18.133.1
 no mop enabled
 no mop sysid
end
```



SVI can be at the WLC itself or in the Wired network

IP-Hilfsadresse bei SVI oder Richtlinienprofil

Anschließend können Sie mit EPC überprüfen, ob der DHCP-Austausch jetzt in Ordnung ist und ob der DHCP-Server eine oder mehrere DNS-Server-IP(s) bereitstellt:

Full DHCP exchange and DHCP server offering IP and DNS servers

DHCP-Angebotsdetails der DNS-Server-IP

7 - Wird die automatische Umleitung durchgeführt?

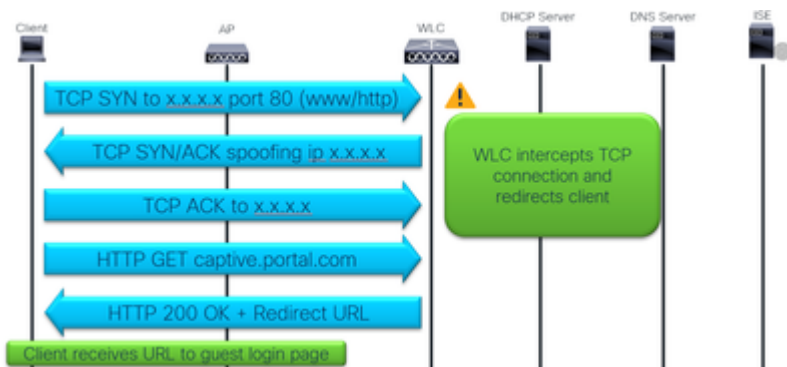
Mit WLC EPC überprüfen, ob der DNS-Server Abfragen beantwortet:

DNS-Abfrage und -Antworten

- Wenn die Umleitung nicht automatisch erfolgt, öffnen Sie einen Browser, und versuchen Sie eine zufällige IP-Adresse. Beispiel: 10.0.0.1.
- Wenn die Umleitung dann funktioniert, ist es möglich, dass Sie ein DNS-Auflösungsproblem haben.

Funktioniert es immer noch nicht?

Sehen wir uns nun den Ablauf noch einmal an ...



Überwachung und Weiterleitung des Datenverkehrs

## 8 - Im Browser wird keine Anmeldeseite angezeigt?

Überprüfen Sie, ob der Client das TCP-SYN an Port 80 sendet und der WLC es abfängt:

So many retransmissions to port 80 without interception from WLC??

TCP-Neuübertragungen an Port 80

Hier können wir sehen, dass der Client TCP SYN Pakete an Port 80 sendet, aber keine Antwort erhält und TCP erneut sendet.

Vergewissern Sie sich, dass der Befehl `ip http server` in der globalen Konfiguration oder `webauth-http-enable` in der globalen Parameterzuordnung vorhanden ist:

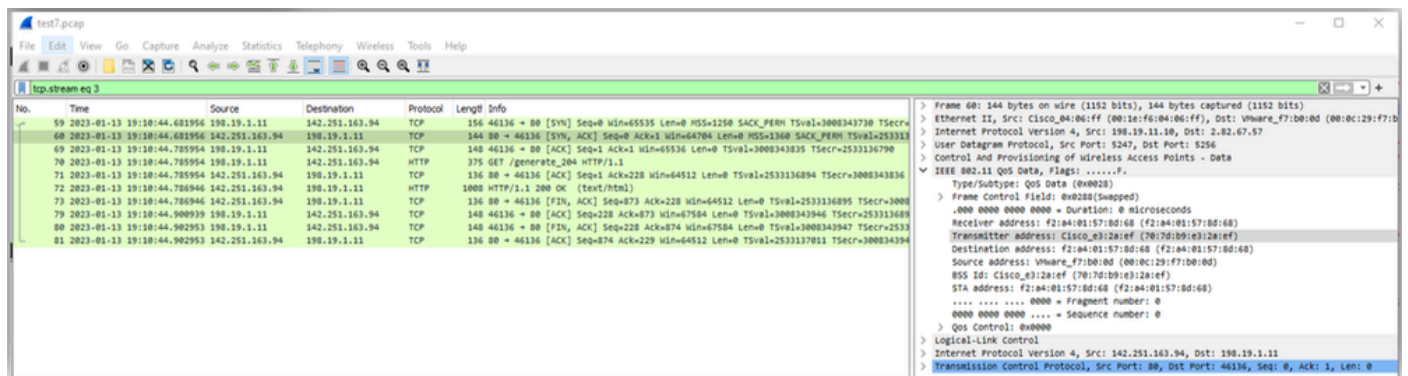
No need for `ip http server`

HTTP-Interception-Befehle

Nach dem Befehl fängt der WLC das TCP ab und sendet Spoofs an die Ziel-IP-Adresse, um dem



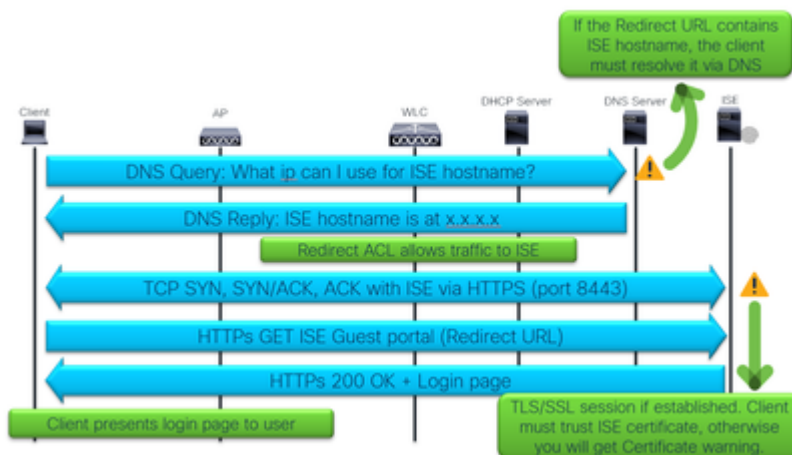
Client zu antworten und eine Umleitung vorzunehmen.



TCP-Abfragen durch WLC

Funktioniert es immer noch nicht?

Es ist mehr im Fluss...



Client-Anmeldung beim ISE-Gastanmeldeportal

9 - Kann der Client den ISE-Hostnamen auflösen?

Überprüfen Sie, ob die Umleitungs-URL IP oder Hostnamen verwendet und ob der Client den ISE-Hostnamen auflöst:

The screenshot shows the Cisco ISE Policy Elements configuration page. In the 'Common Tasks' section, the 'Static IP/Host name/FQDN' checkbox is selected, and the value 'ise.thewifilab.org' is entered. In the 'Advanced Attributes Settings' section, the 'Access Type' is set to 'ACCESS\_ACCEPT'. In the 'Attributes Details' section, the 'Access Type' is set to 'ACCESS\_ACCEPT' and the 'Cisco-av-pair' is set to 'url-redirect=https://ise.thewifilab.org/port/gateway/sessionId=SessionId/uea/port=0712:00-6d90-11a5-478e-005056f2f1a6/daysToExpiry=value&action=oa'. A terminal window on the right shows the command 'nslookup ise.thewifilab.org' and the output: 'Server: localhost', 'Address: 127.0.0.1', 'Non-authoritative answer:', 'Name: ise.thewifilab.org', 'Address: 198.18.133.27'.

## ISE-Hostnamenaufösung

Ein häufiges Problem tritt auf, wenn die Umleitungs-URL den ISE-Hostnamen enthält. Das Client-Gerät kann diesen Hostnamen jedoch nicht in die ISE-IP-Adresse auöösen. Wenn ein Hostname verwendet wird, stellen Sie sicher, dass dieser über DNS aufgelöst werden kann.

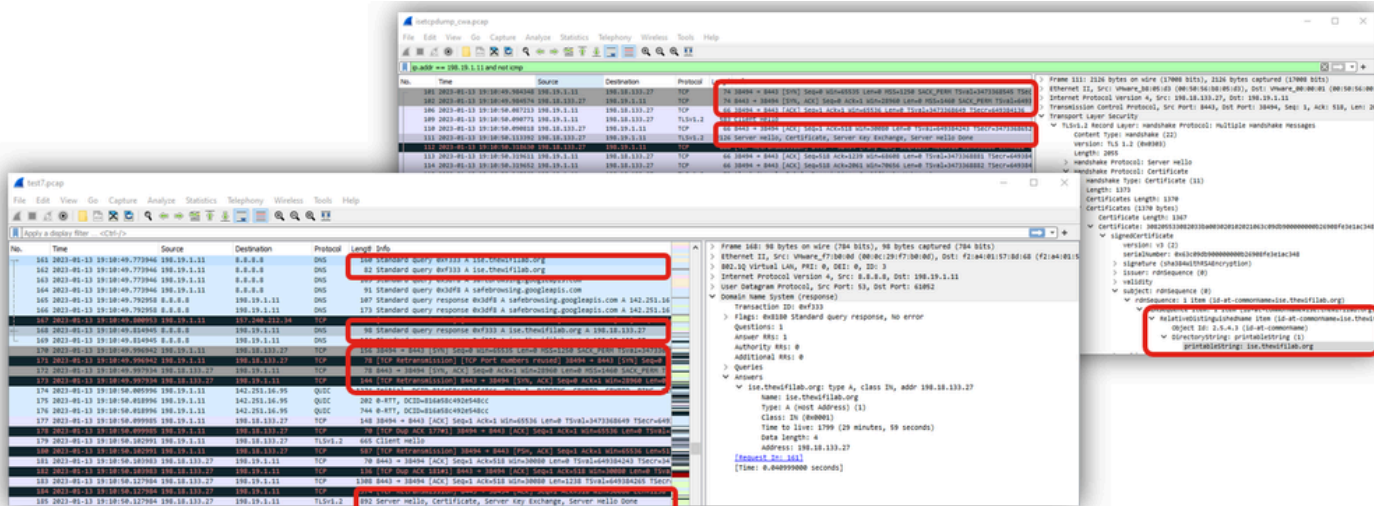
10 - Login-Seite immer noch nicht geladen?

Überprüfen Sie dies mit WLC EPC und ISE TCPdump, wenn der Client-Datenverkehr ISE PSN erreicht. Konfigurieren und Initiieren der Erfassungen auf WLC und ISE:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller Packet Capture configuration page. The 'Capture Name' is 'test', the 'Filter' is 'any', and the 'Inner Filter MAC' is 'f2a4.0157.8d58'. The 'Buffer Size (MB)' is '10' and the 'Limit by' is 'Duration'. The 'Available' list shows 'GigabitEthernet2', 'GigabitEthernet3', and 'GigabitEthernet1'. The 'Selected' list shows 'GigabitEthernet1'. The Cisco ISE Diagnostic Tools TCP Dump configuration page shows the 'Host Name' as 'ise', the 'Network Interface' as 'GigabitEthernet 0', and the 'File Name' as 'testtcpdump\_cwa'.

## WLC EPC und ISE TCPDump

Erfassen Sie nach der Problemwiedergabe die erfassten Daten, und korrelieren Sie den Datenverkehr. Hier sehen wir den aufgelösten ISE-Hostnamen und dann die Kommunikation zwischen Client und ISE auf Port 8443:



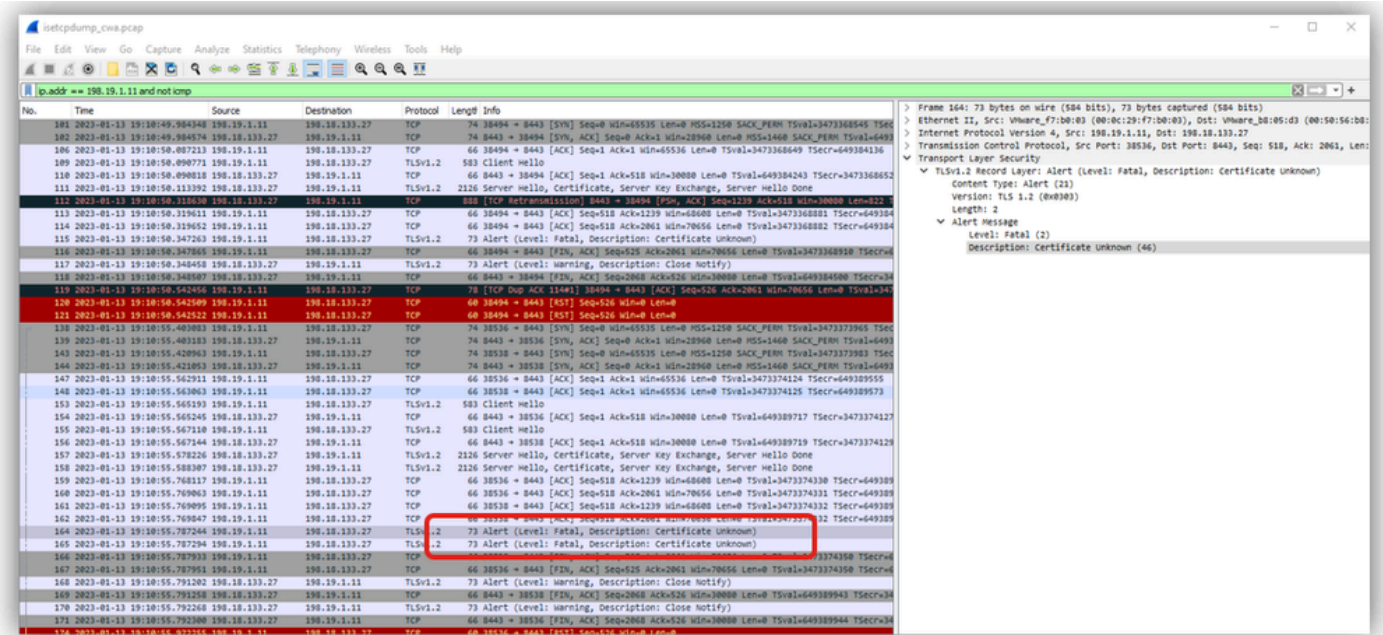
## WLC- und ISE-Verkehr

### 11 - Warum wird die Sicherheit durch das Zertifikat verletzt?

Wenn Sie ein selbstsigniertes Zertifikat auf der ISE verwenden, wird erwartet, dass der Client eine Sicherheitswarnung ausgibt, wenn er versucht, die Anmeldeseite des ISE-Portals anzuzeigen.

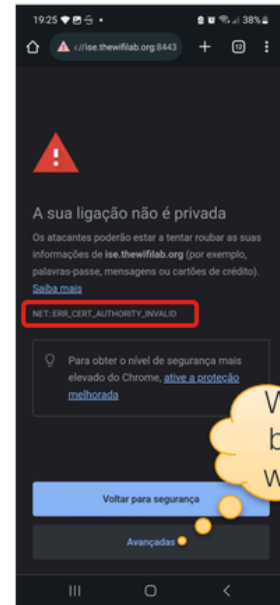
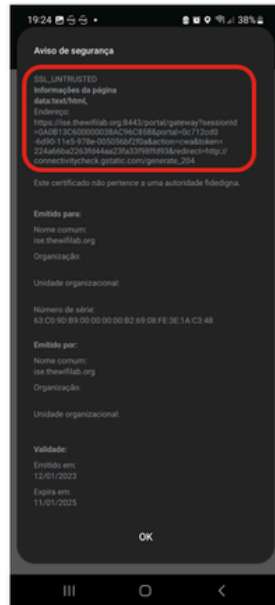
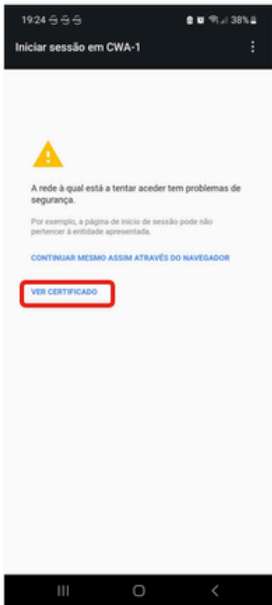
Auf dem WLC EPC oder ISE TCPdump können wir überprüfen, ob das ISE-Zertifikat vertrauenswürdig ist.

In diesem Beispiel sehen wir die Verbindung schließen vom Client mit Alert (Level: Fatal, Beschreibung: certificate Unknown), was bedeutet, dass das ISE-Zertifikat nicht bekannt ist (Trusted):



## Nicht vertrauenswürdiges ISE-Zertifikat

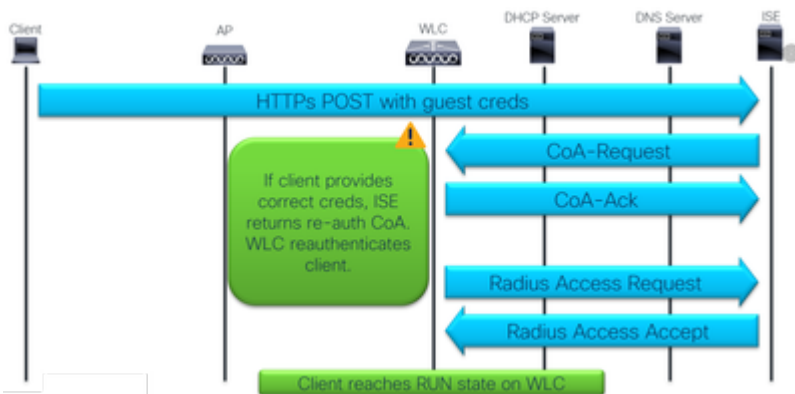
Wenn wir auf der Client-Seite überprüfen, sehen wir diese Beispielausgabe:



Client-Gerät, das dem ISE-Zertifikat nicht vertraut

Die Umleitung funktioniert!! Die Anmeldung schlägt fehl ...

Ein letztes Mal den Fluss prüfen...



Client-Anmeldung und CoA

12 - Fehler bei der Gastanmeldung?

Überprüfen Sie die ISE-Protokolle auf fehlgeschlagene Authentifizierung. Stellen Sie sicher, dass die Anmeldeinformationen korrekt sind.



### Overview

|                      |                                  |
|----------------------|----------------------------------|
| Event                | 5418 Guest Authentication Failed |
| Username             | Cwa                              |
| Endpoint Id          | F2:A4:01:57:8D:68 @              |
| Endpoint Profile     |                                  |
| Authorization Result |                                  |

### Steps

|      |                             |
|------|-----------------------------|
| 5418 | Guest Authentication Failed |
|------|-----------------------------|

### Authentication Details

|                    |                                                                                                                  |
|--------------------|------------------------------------------------------------------------------------------------------------------|
| Source Timestamp   | 2023-01-13 21:32:29.201                                                                                          |
| Received Timestamp | 2023-01-13 21:32:29.201                                                                                          |
| Policy Server      | ise                                                                                                              |
| Event              | 5418 Guest Authentication Failed                                                                                 |
| Failure Reason     | 22040 Wrong password or invalid shared secret                                                                    |
| Resolution         | Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials. |
| Root cause         | Wrong password or invalid shared secret                                                                          |
| Username           | Cwa                                                                                                              |

Make sure you using correct credentials 😊

Fehler bei der Gastauthentifizierung aufgrund falscher Anmeldeinformationen.

### 13 - Anmeldung erfolgreich, aber nicht zu RUN?

Überprüfen Sie die ISE-Protokolle auf Authentifizierungsdetails und Ergebnisse:

### Overview

|                       |                               |
|-----------------------|-------------------------------|
| Event                 | 5236 Authorize-Only succeeded |
| Username              | cwa                           |
| Endpoint Id           | F2:A4:01:57:8D:68 @           |
| Endpoint Profile      | Android                       |
| Authentication Policy | Default                       |
| Authorization Policy  | Default >> Redirect-to-Portal |
| Authorization Result  | CWAredirect                   |

### Steps

|       |                                                                                                       |
|-------|-------------------------------------------------------------------------------------------------------|
| 11001 | Received RADIUS Access-Request                                                                        |
| 11017 | RADIUS created a new session                                                                          |
| 11027 | Detected Host Lookup UseCase (Service-Type = Call Check (10))                                         |
| 15049 | Evaluating Policy Group                                                                               |
| 15008 | Evaluating Service Selection Policy                                                                   |
| 24715 | ISE has not confirmed locally previous successful machine authentication for user in Active Directory |
| 15036 | Evaluating Authorization Policy                                                                       |
| 24209 | Looking up Endpoint in Internal Endpoints IDStore - cwa                                               |
| 24211 | Found Endpoint in Internal Endpoints IDStore                                                          |
| 15016 | Selected Authorization Profile - CWAredirect                                                          |
| 24210 | Looking up User in Internal Users IDStore - cwa                                                       |
| 24212 | Found User in Internal Users IDStore                                                                  |
| 11002 | Returned RADIUS Access-Accept                                                                         |

### Authentication Details

|                    |                               |
|--------------------|-------------------------------|
| Source Timestamp   | 2023-01-13 21:36:01.8         |
| Received Timestamp | 2023-01-13 21:36:01.8         |
| Policy Server      | ise                           |
| Event              | 5236 Authorize-Only succeeded |
| Username           | cwa                           |
| User Type          | User                          |

### Result

|               |                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User-Name     | cwa                                                                                                                                                                                         |
| Class         | CACS:0A0B13C60000003BAD0BF3E4:ise/462943192/128                                                                                                                                             |
| cisco-av-pair | url-redirect=act-REDIRECT                                                                                                                                                                   |
| cisco-av-pair | url-redirect=https://ise.thewifilab.org.8443/portal/gateway?sessionId=0A0B13C60000003BAD0BF3E4&portal=0c712cd0-6d90-11e5-978e-005056b2f0a&action=cwa&token=92eb9963bc6f70c9f82d32ed8a072c6c |
| cisco-av-pair | profile-name=Android                                                                                                                                                                        |
| LicenseTypes  | Essential license consumed.                                                                                                                                                                 |

Still getting Redirect-to-Portal ????

Umleitungsschleife

In diesem Beispiel erhält der Client erneut das Autorisierungsprofil, das die Umleitungs-URL und die Umleitungs-ACL enthält. Daraus ergibt sich eine Umleitungsschleife.

Aktivieren Sie Policy Set. Die Regelprüfung für Guest\_Flow muss vor der Umleitung liegen:

Authorization Policy (3)

| Status | Rule Name          | Conditions                                                   | Profiles       | Security Groups | Hits | Actions |
|--------|--------------------|--------------------------------------------------------------|----------------|-----------------|------|---------|
| ✓      | Redirect-to-Portal | AND<br>Wireless_MAB<br>Radius Called-Station-ID CONTAINS CWA | CWRedirect x   |                 |      |         |
| ✓      | Guest-Flow         | AND<br>Wireless_MAB<br>Guest_Flow                            | PermitAccess x |                 |      |         |
| ✓      | Default            |                                                              | DenyAccess x   |                 |      |         |

Other Attributes

|                               |                                         |
|-------------------------------|-----------------------------------------|
| ConfigVersionId               | 83                                      |
| DestinationPort               | 1812                                    |
| Protocol                      | Radius                                  |
| NAS-Port                      | 1115                                    |
| Framed-MTU                    | 1485                                    |
| OriginalUserName              | f2a401578a68                            |
| NetworkDeviceProfileId        | Bade1115-aef1-4a9a-8158-002e835179db    |
| IsThirdPartyDeviceFlow        | false                                   |
| AcctSessionId                 | 0012529311021118                        |
| UseCase                       | Guest-Flow                              |
| AuthorizationPolicyMatched... | Guest-Flow                              |
| EndPointMACAddress            | F2-A4-01-57-8D-68                       |
| ISEPolicySetName              | Default                                 |
| DTLSSupport                   | Unknown                                 |
| HostIdentityGroup             | Endpoint Identity Groups:GuestEndpoints |

Guest\_Flow-Regel

## 14 - CoA-Fehler?

Mit EPC und ISE TCPDump kann der CoA-Datenverkehr überprüft werden. Überprüfen Sie, ob der CoA-Port (1700) zwischen WLC und ISE offen ist. Stellen Sie sicher, dass der freigegebene geheime Schlüssel übereinstimmt.

test.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

radius

| No.  | Time                       | Source        | Destination   | Protocol | Length | Info                       |
|------|----------------------------|---------------|---------------|----------|--------|----------------------------|
| 214  | 2023-01-13 19:38:06.999336 | 198.19.11.10  | 198.18.133.27 | RADIUS   | 468    | Accounting-Request id=212  |
| 215  | 2023-01-13 19:38:06.997934 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 84     | Accounting-Response id=212 |
| 295  | 2023-01-13 19:38:14.104990 | 198.19.11.10  | 198.18.133.27 | RADIUS   | 438    | Access-Request id=213      |
| 296  | 2023-01-13 19:38:14.121987 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 409    | Access-Accept id=213       |
| 310  | 2023-01-13 19:38:14.426964 | 198.19.11.10  | 198.18.133.27 | RADIUS   | 400    | Accounting-Request id=214  |
| 311  | 2023-01-13 19:38:14.427971 | 198.19.11.10  | 198.18.133.27 | RADIUS   | 442    | Accounting-Request id=215  |
| 312  | 2023-01-13 19:38:14.438972 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 66     | Accounting-Response id=215 |
| 313  | 2023-01-13 19:38:14.448971 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 66     | Accounting-Response id=214 |
| 351  | 2023-01-13 19:38:15.224979 | 198.19.11.10  | 198.18.133.27 | RADIUS   | 460    | Accounting-Request id=216  |
| 352  | 2023-01-13 19:38:15.229983 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 66     | Accounting-Response id=216 |
| 3539 | 2023-01-13 19:38:50.416970 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 248    | CoA-Request id=4           |
| 3540 | 2023-01-13 19:38:50.416970 | 198.19.11.10  | 198.18.133.27 | RADIUS   | 475    | Access-Request id=217      |
| 3541 | 2023-01-13 19:38:50.416970 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 111    | CoA-Ack id=4               |
| 3542 | 2023-01-13 19:38:50.428963 | 198.18.133.27 | 198.19.11.10  | RADIUS   | 166    | Access-Accept id=217       |

Frame 3539: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 11, Src: VMware\_F7:08:00 (08:00:27:08:00:00), Dst: Cisco\_04:06:ff (00:1e:f6:04:00:00), Virtual LAN, Prio: 0, Dst: 11

Internet Protocol Version 4, Src: 198.18.133.27, Dst: 198.19.11.10

User Datagram Protocol, Src Port: 14564, Dst Port: 1700

Source Port: 14564

Destination Port: 1700

Length: 210

Checksum: 0x371 [unverified]

Checksum Status: Unverified

Stream Index: 67

[Timestamp]

UDP payload (202 bytes)

RADIUS Protocol

CoA-Datenverkehr



Anmerkung: In Version 17.4.x und höher müssen Sie auch den CoA-Serverschlüssel konfigurieren, wenn Sie den RADIUS-Server konfigurieren. Verwenden Sie denselben Schlüssel wie den gemeinsamen geheimen Schlüssel (bei ISE sind sie standardmäßig identisch). Optional soll ein anderer Schlüssel für CoA als der gemeinsame geheime Schlüssel konfiguriert werden, wenn dies der Grund ist, für den der RADIUS-Server konfiguriert wurde. In Cisco IOS® XE 17.3 wurde für die Webbenutzeroberfläche lediglich derselbe geheime Schlüssel wie für den CoA-Schlüssel verwendet.

Ab Version 17.6.1 wird RADIUS (einschließlich CoA) über diesen Port unterstützt. Wenn Sie den Service-Port für RADIUS verwenden möchten, benötigen Sie folgende Konfiguration:

<#root>

```
aaa server radius dynamic-author  
  client 10.48.39.28
```

vrf

Mgmt-intf

```
  server-key cisco123
```

```
interface GigabitEthernet0
```

vrf

forwarding

Mgmt-intf

```
  ip address x.x.x.x x.x.x.x
```

```
!if using aaa group server:  
aaa group server radius group-name  
  server name nicoISE
```

ip

vrf

forwarding

Mgmt-intf

ip

radius

source

```
-interface GigabitEthernet0
```

## Schlussfolgerung

Dies ist die wiederaufgenommene CWA-Checkliste:

- Vergewissern Sie sich, dass sich der Client im richtigen VLAN befindet und IP-Adresse und DNS erhält.
  - Abrufen von Client-Details am WLC und Ausführen von Paketerfassungen, um den DHCP-Austausch anzuzeigen
- Überprüfen, ob der Client Hostnamen über DNS auflösen kann
  - Pingen Sie den Hostnamen von cmd.
- WLC muss auf Port 80 lauschen
  - Überprüfen Sie den globalen Befehl ip http server oder den globalen Parameterzuordnungsbefehl webauth-http-enable.
- Installieren Sie ein vertrauenswürdiges Zertifikat auf der ISE, um die Zertifikatswarnung loszuwerden.
  - Vertrauenswürdige Zertifikate müssen nicht auf WLC in CWA installiert werden.
- Authentifizierungsrichtlinie bei ISE - Erweiterte Option "Weiter" Wenn Benutzer nicht gefunden wird
  - Um gesponserten Gastbenutzern zu erlauben, sich zu verbinden und URL-Umleitung und ACL zu erhalten.

Die wichtigsten Tools zur Fehlerbehebung:

- WLC-EPC
  - Innenfilter: DHCP-Protokoll, MAC-Adresse
- WLC-Monitor
  - Überprüfen Sie die Details zur Client-Sicherheit.
- WLC RA-Verfolgung
  - Debugging mit detaillierten Informationen auf WLC Seite.
- ISE-Live-Protokolle
  - Authentifizierungsdetails.
- ISE-TCPDump
  - Sammeln von Paketerfassungen an der ISE-PSN-Schnittstelle

## Referenzen

[Konfigurieren von Central Web Authentication \(CWA\) auf Catalyst 9800 WLC und ISE](#)

### 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.