

Konfigurieren von ISE Wireless CWA- und Hotspot-Datenflüssen mit AireOS und WLCs der nächsten Generation

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Unified 5508 WLC konfigurieren](#)

[Globale Konfiguration](#)

[Konfigurieren Sie den Service Set Identifier \(SSID\) des Gasts:](#)

[Konfigurieren der Umleitungs-ACL](#)

[HTTPS-Umleitung](#)

[Aggressives Failover](#)

[Captive Bypass](#)

[Konfigurieren von konvergentem 3850 NGWC](#)

[Globale Konfiguration](#)

[SSID-Konfiguration](#)

[Umleiten der ACL-Konfiguration](#)

[Konfiguration der Befehlszeilenschnittstelle \(CLI\)](#)

[Konfigurieren der ISE](#)

[Allgemeine ISE-Konfigurationsaufgaben](#)

[Anwendungsfall 1: CWA mit Gastauthentifizierung in jeder Benutzerverbindung](#)

[Anwendungsfall 2: CWA mit Geräteregistrierung zur Durchsetzung der Gastauthentifizierung einmal täglich](#)

[Anwendungsfall 3: HostSpot-Portal](#)

[Überprüfung](#)

[Anwendungsfall 1](#)

[Anwendungsfall 2](#)

[Anwendungsfall 3](#)

[FlexConnect Local-Switching in AireOS](#)

[Szenario ausländischer Anker](#)

[Fehlerbehebung](#)

[Häufig auftretende unterbrochene Zustände auf AireOS und dem WLC mit konvergentem Zugriff](#)

[AireOS-WLC](#)

[NGWC](#)

[ISE](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die Konfiguration von drei Gastgeräten in der Identity Services Engine mit Cisco AireOS und den Wireless LAN Controllern der nächsten Generation beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco Wireless LAN Controller (Unified und Converged Access)
- Identity Services Engine (ISE)

Verwendete Komponenten

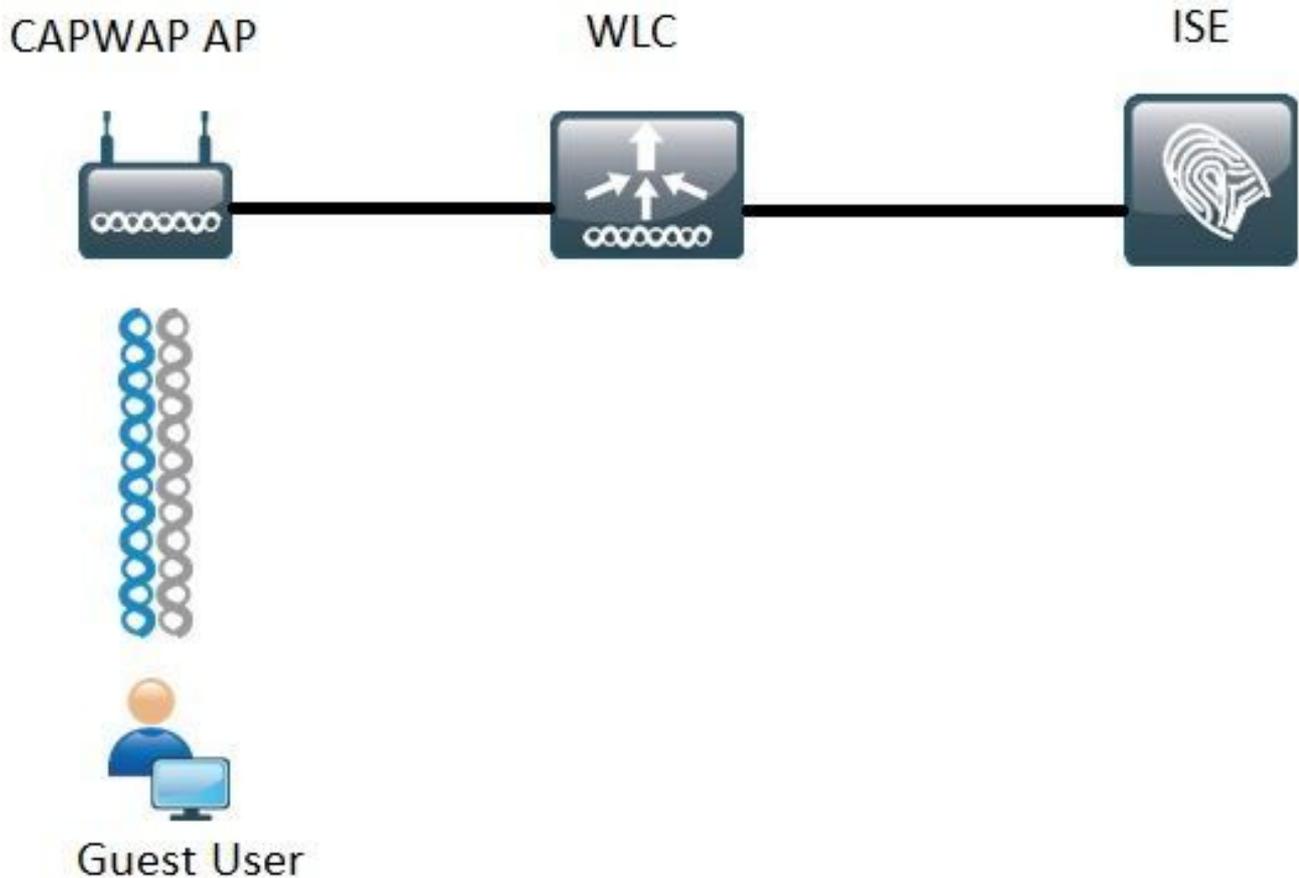
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine Version 2.1
- Cisco Wireless LAN Controller 5508 mit 8.0.121.0
- Next-Generation Wireless Controller (NGWC) Catalyst 3850 (WS-C3850-24P) mit 03.06.04.E

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 verstehen.

Konfigurieren

Netzwerkdiagramm



In den in diesem Dokument beschriebenen Schritten wird die typische Konfiguration auf Unified Access- und Converged Access-WLCs beschrieben, um jeden Gastdatenfluss mit der ISE zu unterstützen.

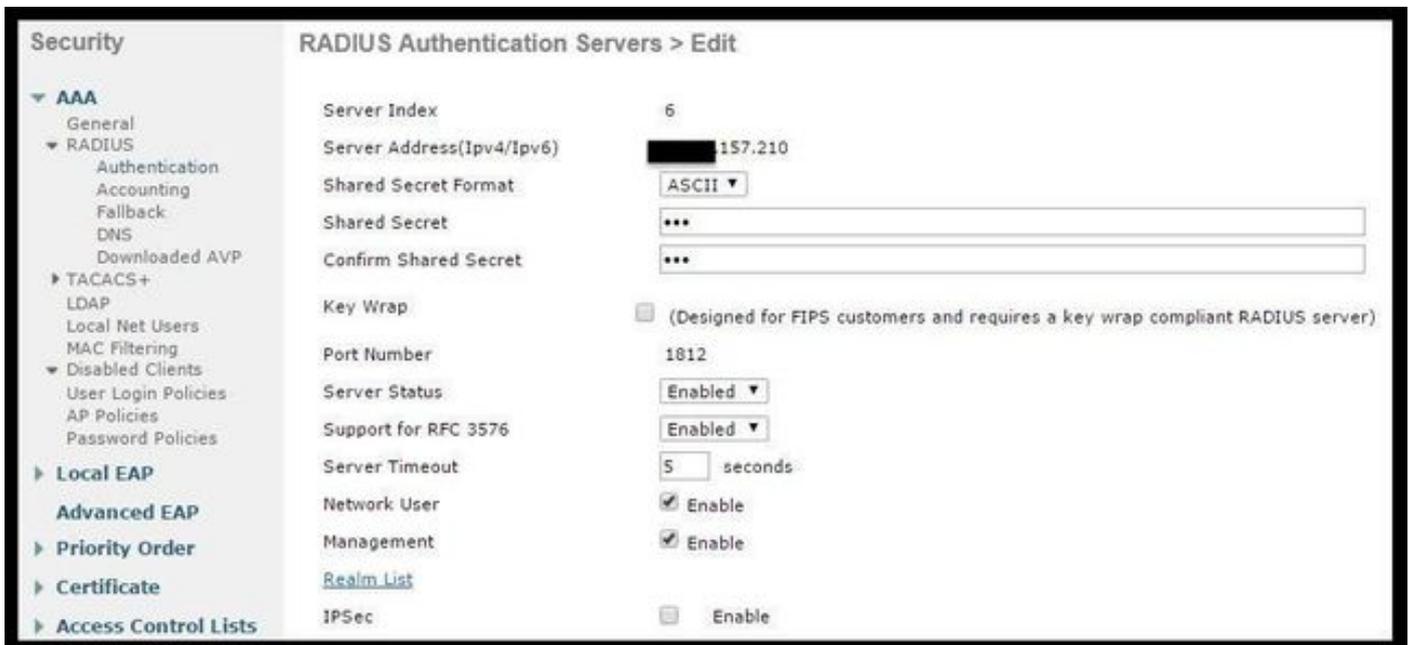
Unified 5508 WLC konfigurieren

Unabhängig vom in der ISE konfigurierten Anwendungsfall beginnt alles aus WLC-Sicht mit einem Wireless-Endpunkt, der sich mit einer offenen SSID mit aktivierter MAC-Filterung verbindet (plus AAA-Übersteuerung und RADIUS NAC), die auf die ISE als Authentifizierungs- und Abrechnungsserver verweist. So wird sichergestellt, dass die ISE die erforderlichen Attribute dynamisch an den WLC weiterleiten kann, um eine Umleitung zum Gastportal der ISE erfolgreich durchzuführen.

Globale Konfiguration

1. ISE global als Authentifizierungs- und Abrechnungsserver hinzufügen

- Navigieren Sie zu **Sicherheit > AAA > Authentifizierung**, und klicken Sie auf **Neu**



- Geben Sie die IP-Adresse und den gemeinsamen geheimen Schlüssel des ISE-Servers ein
- Stellen Sie sicher, dass Serverstatus und **Unterstützung für RFC 3676** (Autorisierungsänderung oder CoA-Unterstützung) beide auf **Aktiviert** eingestellt sind.
- Unter Serverzeitüberschreitung haben AireOS WLCs standardmäßig 2 Sekunden. Berücksichtigen Sie dabei die Netzwerkmerkmale (Latenz, ISE und WLC an unterschiedlichen Standorten), kann es von Vorteil sein, die Server-Zeitüberschreitung auf mindestens 5 Sekunden zu erhöhen, um unnötige Failover-Ereignisse zu vermeiden.
- Klicken Sie auf **Apply** (Anwenden).
- Wenn mehrere zu konfigurierende Policy Services Nodes (PSN) vorhanden sind, fahren Sie mit der Erstellung zusätzlicher Servereinträge fort.

Hinweis: Dieses Konfigurationsbeispiel umfasst 2 ISE-Instanzen.

- Navigieren Sie zu **Security > AAA > RADIUS > Accounting**, und klicken Sie auf **New**
- Geben Sie die IP-Adresse und den gemeinsamen geheimen Schlüssel des ISE-Servers ein
- Stellen Sie sicher, dass der Serverstatus auf Aktiviert eingestellt ist.
- Erhöhen Sie ggf. die Server-Zeitüberschreitung (Standardwert: 2 Sekunden).

2. Fallback-Konfiguration.

In einer einheitlichen Umgebung wird der WLC nach Auslösung des Server-Timeouts zum nächsten konfigurierten Server verschoben. Als Nächstes in der Reihe aus dem WLAN. Wenn keine andere Option verfügbar ist, wählt der WLC die nächste in der Liste der globalen Server aus. Wenn mehrere Server auf der SSID konfiguriert werden (primär, sekundär), nachdem der Failover erfolgt ist, sendet der WLC standardmäßig weiterhin den Authentifizierungs- und (oder) Accounting-Datenverkehr dauerhaft an die sekundäre Instanz, selbst wenn der primäre Server wieder online ist.

Um dieses Verhalten abzuschwächen, aktivieren Sie Fallback. Navigieren Sie zu **Security > AAA > RADIUS > Fallback**. Das Standardverhalten ist "off" (Aus). Die einzige Möglichkeit zur Wiederherstellung nach einem Serverausfall erfordert einen Administrator-Eingriff (globales Bounce des Server-Admin-Status).

Um das Fallback zu aktivieren, haben Sie zwei Möglichkeiten:

- **Passiv** - Wenn ein Server im passiven Modus nicht auf die WLC-Authentifizierungsanforderung reagiert, verschiebt der WLC den Server in die inaktive Warteschlange und legt einen Timer fest (Option "Intervall in Sekunde"). Wenn der Timer abläuft, verschiebt der WLC den Server in die aktive Warteschlange, unabhängig vom tatsächlichen Serverstatus. Wenn die Authentifizierungsanforderung zu einem Timeout-Ereignis führt (d. h. der Server ist noch nicht verfügbar), wird der Servereintrag wieder in die Warteschlange für inaktive Geräte verschoben, und der Timer tritt wieder ein. Wenn der Server erfolgreich antwortet, verbleibt er in der Warteschlange "Aktiv". Die konfigurierbaren Werte reichen hier von 180 bis 3600 Sekunden.
- **Aktiv** - Wenn ein Server im aktiven Modus nicht auf die WLC-Authentifizierungsanforderung reagiert, markiert der WLC den Server als ausgefallen. Anschließend wird der Server in den nicht aktiven Serverpool verschoben und es werden regelmäßig Testnachrichten gesendet, bis der Server antwortet. Wenn der Server antwortet, verschiebt der WLC den ausgefallenen Server in den aktiven Pool und beendet das Senden von Testnachrichten.

In diesem Modus müssen Sie im WLC einen Benutzernamen und ein Testintervall in Sekunden (180 bis 3600) eingeben.

Hinweis: Die WLC-Überprüfung erfordert keine erfolgreiche Authentifizierung. In beiden Fällen werden erfolgreiche oder fehlgeschlagene Authentifizierungen als Serverantwort betrachtet, die ausreicht, um den Server in die aktive Warteschlange zu versetzen.

Konfigurieren Sie den Service Set Identifier (SSID) des Gasts:

- Navigieren Sie zur Registerkarte WLANs, und klicken Sie unter Neue Option erstellen auf **Los**:



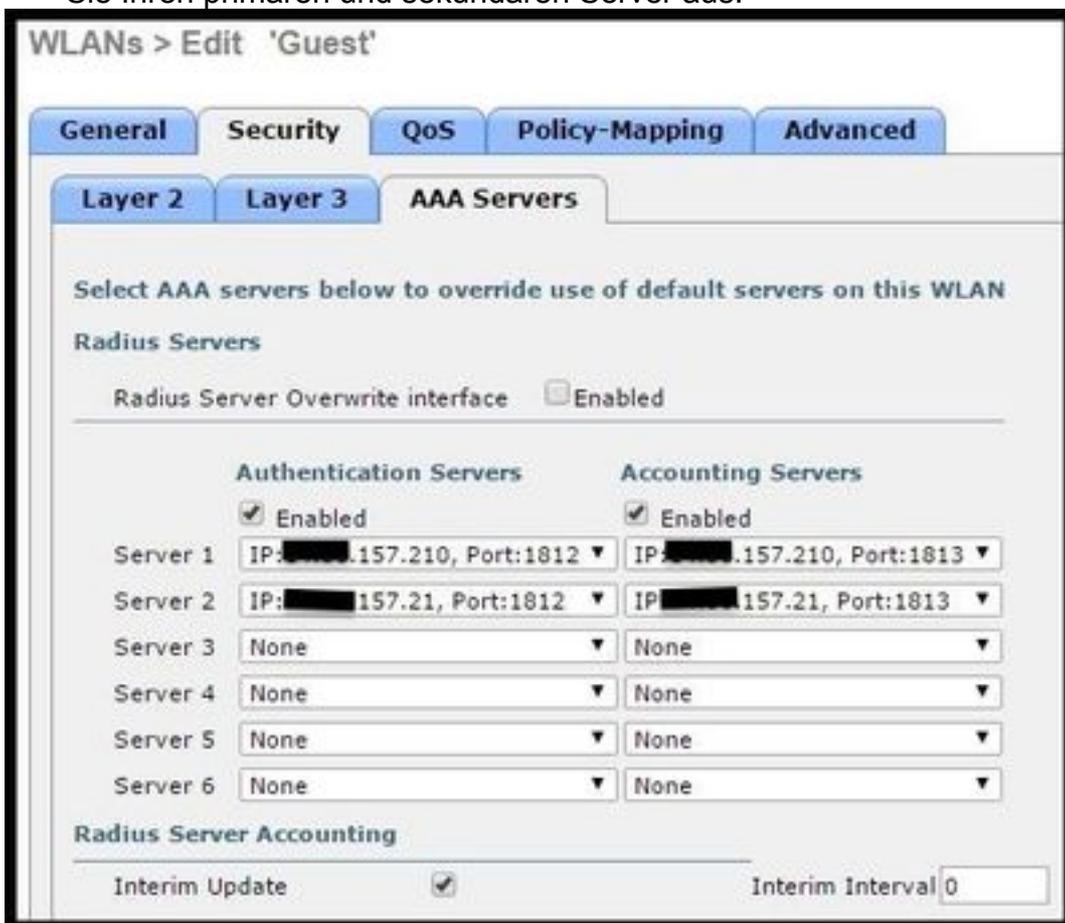
- Geben Sie den Profilnamen und den SSID-Namen ein. Klicken Sie auf **Apply** (Anwenden).
- Wählen Sie auf der Registerkarte Allgemein die zu verwendende Schnittstelle oder Schnittstellengruppe (Gast-VLAN) aus.



- Wählen Sie unter **Sicherheit > Layer 2 > Layer 2-Sicherheit** die Option **Keine aus**, und aktivieren Sie das Kontrollkästchen **Mac Filtering**.



- Legen Sie auf der Registerkarte **AAA-Server** die Option "Authentication and Accounting Servers" (Authentifizierungs- und Abrechnungsserver) auf **enabled (aktiviert)** fest, und wählen Sie Ihren primären und sekundären Server aus.



- **Zwischenaktualisierung:** Dies ist eine optionale Konfiguration, die diesem Fluss keine Vorteile hinzufügt. Wenn Sie diese Option aktivieren möchten, muss der WLC i Code 8.x oder höher ausführen:

Disabled (Deaktiviert): Die Funktion ist vollständig deaktiviert.

Aktiviert mit 0-Intervall: Der WLC sendet Accounting-Updates an die ISE, sobald sich der Mobile Station Control Block (MSCB)-Eintrag des Clients ändert (d. h. IPv4- oder IPv6-Adresszuweisung

oder -änderung, Client-Roaming-Ereignis.) Es werden keine weiteren regelmäßigen Updates versendet.

Aktiviert mit konfiguriertem Interim Interval: In diesem Modus sendet der WLC bei Änderungen am MSCB-Eintrag des Clients Benachrichtigungen an die ISE und im konfigurierten Intervall (unabhängig von Änderungen) weitere periodische Abrechnungsbenachrichtigungen.

- Wählen Sie auf der Registerkarte Erweitert die Option **AAA-Außerkraftsetzung zulassen** und unter **NAC-Status** die Option **RADIUS NAC aus**. Dadurch wird sichergestellt, dass der WLC alle Attributwertpaare (AVPs) anwendet, die von der ISE stammen.
- Navigieren Sie zur Registerkarte SSID General (SSID - Allgemein), und setzen Sie den SSID-Status auf **Enabled (Aktiviert)**.

WLANs > Edit 'Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	Guest			
Type	WLAN			
SSID	Guest			
Status	<input checked="" type="checkbox"/> Enabled			

- Wenden Sie die Änderungen an.

Konfigurieren der Umleitungs-ACL

Diese ACL wird von der ISE referenziert und bestimmt, welcher Datenverkehr umgeleitet wird und durch welchen Datenverkehr zugelassen wird.

- Wechseln Sie zur Registerkarte **Sicherheit > Zugriffskontrolllisten**, und klicken Sie auf **Neu**
- Dies ist ein Beispiel für eine ACL.

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	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

Diese ACL muss den Zugriff auf und von DNS-Diensten und ISE-Knoten über den TCP-Port 8443 ermöglichen. Unten ist eine implizite "deny" (Ablehnen) angegeben, die bedeutet, dass der restliche Datenverkehr an die Gastportal-URL der ISE umgeleitet wird.

HTTPS-Umleitung

Diese Funktion wird in AireOS 8.0.x und höher unterstützt, ist jedoch standardmäßig deaktiviert. Um die HTTPS-Unterstützung zu aktivieren, gehen Sie zu **WLC Management > HTTP-HTTPS >**

HTTPS Redirection (WLC-Verwaltung > HTTP-HTTPS > HTTPS-Umleitung), und legen Sie diese Option auf **Enabled (Aktiviert) fest**, oder wenden Sie den folgenden Befehl in CLI an:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Zertifikatwarnungen nach Aktivierung der HTTPS-Umleitung

Wenn die HTTPS-Umleitung aktiviert ist, kann es während der Umleitung zu Problemen mit der Zertifikatvertrauensstellung kommen. Dies wird selbst dann erkannt, wenn auf dem Controller ein gültiges verkettetes Zertifikat vorhanden ist, und auch dann, wenn dieses Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle eines Drittanbieters signiert wurde. Der Grund hierfür ist, dass das auf dem WLC installierte Zertifikat an den Hostnamen oder die IP-Adresse der virtuellen Schnittstelle ausgegeben wird. Wenn der Client <https://cisco.com> ausprobiert, erwartet der Browser, dass das Zertifikat an cisco.com ausgegeben wird. Damit der WLC jedoch den vom Client ausgegebenen GET abfangen kann, muss er zunächst die HTTPS-Sitzung einrichten, für die der WLC während der SSL-Handshake-Phase sein Virtual Interface Certificate vorlegt. Dies veranlasst den Browser, eine Warnung anzuzeigen, da das während des SSL-Handshakes ausgestellte Zertifikat nicht an die ursprüngliche Website ausgegeben wurde, auf die der Client zugreifen möchte (d. h. cisco.com im Gegensatz zum Hostnamen der virtuellen Schnittstelle von WLC). Sie können verschiedene Zertifikatfehlermeldungen in verschiedenen Browsern sehen, aber alle beziehen sich auf das gleiche Problem.

Aggressives Failover

Diese Funktion ist in AireOS-WLCs standardmäßig aktiviert. Wenn aggressives Failover aktiviert ist, markiert der WLC den AAA-Server als nicht reagierend und wechselt zum nächsten konfigurierten AAA-Server, nachdem ein RADIUS-Timeout-Ereignis einen Client beeinträchtigt hat.

Wenn die Funktion deaktiviert ist, wird der WLC nur dann auf den nächsten Server umgeleitet, wenn das RADIUS-Timeout-Ereignis bei mindestens 3 Clientsitzungen auftritt. Diese Funktion kann mit diesem Befehl deaktiviert werden (für diesen Befehl ist kein Neustart erforderlich):

```
(Cisco Controller) >config radius aggressive-failover disable
```

So überprüfen Sie den aktuellen Status der Funktion:

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Captive Bypass

Die Endgeräte, die einen Captive Network Assistant (CNA)-Mechanismus zum Erkennen eines Captive-Portals und zum automatischen Starten einer Anmeldeseite unterstützen, führen dies in

der Regel über einen Pseudo-Browser in einem kontrollierten Fenster aus, während andere Endgeräte einen voll funktionsfähigen Browser starten, um dies auszulösen. Bei Endpunkten, auf denen die CNA einen Pseudo-Browser startet, kann dies den Fluss unterbrechen wenn sie an ein eigenständiges ISE-Portal umgeleitet werden. Dies wirkt sich in der Regel auf Apple IOS-Geräte aus und hat besonders negative Auswirkungen auf Datenflüsse, die eine Geräteregistrierung, VLAN DHCP-Release und eine Compliance-Prüfung erfordern.

Beachten Sie die Komplexität des verwendeten Datenflusses. Es kann empfohlen werden, Captive Bypass zu aktivieren. In einem solchen Szenario ignoriert der WLC den Mechanismus zur Erkennung des CNA-Portals, und der Client muss einen Browser öffnen, um den Umleitungsprozess zu initiieren.

Überprüfen Sie den Status der Funktion:

```
(Cisco Controller) >show network summary
```

```
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

Geben Sie den folgenden Befehl ein, um diese Funktion zu aktivieren:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

Der WLC weist den Benutzer darauf hin, dass ein Reset-System (Neustart) erforderlich ist, damit die Änderungen wirksam werden.

Eine **Netzwerkübersicht** zeigt an, **dass** die Funktion aktiviert ist. Damit die Änderungen wirksam werden, muss der WLC jedoch neu gestartet werden.

Konfigurieren von konvergentem 3850 NGWC

Globale Konfiguration

1. ISE global als Authentifizierungs- und Abrechnungsserver hinzufügen

- Navigieren Sie zu **Konfiguration > Sicherheit > RADIUS > Server**, und klicken Sie auf **Neu**
- Geben Sie die **IP-Adresse** des ISE-Servers, den **gemeinsamen geheimen Schlüssel**, das **Server-Timeout** und die **Anzahl der Wiederholungen** ein, die Ihre Umgebungsbedingungen widerspiegeln.
- Stellen Sie sicher, dass **Unterstützung für RFC 3570** (CoA-Unterstützung) aktiviert ist.
- Wiederholen Sie den Vorgang, um einen sekundären Servereintrag hinzuzufügen.

RADIUS Servers

Radius Servers > **New**

Server Name

Server IP Address

Shared Secret

Confirm Shared Secret

Auth Port (0-65535)

Acct Port (0-65535)

Server Timeout (1-1000)secs

Retry Count (0-100)

Support for RFC 3576 ▾

2. Servergruppe der ISE erstellen

- Navigieren Sie zu **Konfiguration > Sicherheit > Servergruppen**, und klicken Sie auf **Neu**.
- Weisen Sie der Gruppe einen Namen zu, und geben Sie einen Wert für **die Totzeit** in Minuten ein. Dies ist die Zeit, zu der der Controller den Server in der inaktiven Warteschlange hält, bevor er wieder zur Liste der aktiven Server hochgestuft wird.
- Fügen Sie sie aus der Liste **Verfügbare Server** der Spalte **Zugewiesene Server** hinzu.

Radius Server Group

Radius Server Group > **New**

Name

MAC-delimiter ▾

MAC-filtering ▾

Dead-time (0-1440) in minutes

Group Type

Servers In This Group

Available Servers

Assigned Servers

ISE2

ISE1

3. Dot1x global aktivieren

- Navigieren Sie zu **Configuration > AAA > Method Lists > General**, und aktivieren Sie **Dot1x**

System Auth Control.

The screenshot shows the 'General' configuration page for System Auth Control. The 'Dot1x System Auth Control' checkbox is checked and highlighted with a yellow border. Below it, the 'Local Authentication' and 'Local Authorization' dropdown menus are both set to 'None'.

4. Konfigurieren von Methodenlisten

- Navigieren Sie zu **Configuration > AAA > Method Lists > Authentication**, und erstellen Sie eine neue Method List. In diesem Fall ist dies der Typ Punkt1x und die Gruppe ISE_Group (Gruppe, die im vorherigen Schritt erstellt wurde). Klicken Sie dann auf **Übernehmen**

The screenshot shows the 'Authentication > New' configuration page. The 'Method List Name' is 'ISE_Method'. The 'Type' is 'dot1x' (selected) and 'login'. The 'Group Type' is 'group' (selected) and 'local'. The 'Fallback to local' checkbox is unchecked. The 'Available Server Groups' list is empty, and the 'Assigned Server Groups' list contains 'ISE_Group'.

- Führen Sie die gleichen Schritte für die Abrechnung (**Konfiguration > AAA > Methodenlisten > Abrechnung**) und Autorisierung (**Konfiguration > AAA > Methodenlisten > Autorisierung**) durch. Sie müssen so aussehen

The screenshot shows the 'Accounting > New' configuration page. The 'Method List Name' is 'ISE_Method'. The 'Type' is 'identity' (selected), 'dot1x', 'exec', 'network', and 'commands'. The 'Available Server Groups' list is empty, and the 'Assigned Server Groups' list contains 'ISE_Group'.

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups: [Empty list]

Assigned Server Groups:

Groups In This Method: [Empty list]

5. Erstellen Sie die Autorisierungs-MAC-Filtermethode.

Dieser wird später aus den SSID-Einstellungen aufgerufen.

- Navigieren Sie zu **Konfiguration > AAA > Methodenlisten > Autorisierung**, und klicken Sie auf **Neu**.
- Geben Sie den **Namen der Methodenliste** ein. Wählen Sie **Type = Network** and **Group Type Group** (Typ = Netzwerk und Gruppentyp Gruppe).
- Fügen Sie ISE_Group zum Feld **Zugewiesene Servergruppen** hinzu.

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups: [Empty list]

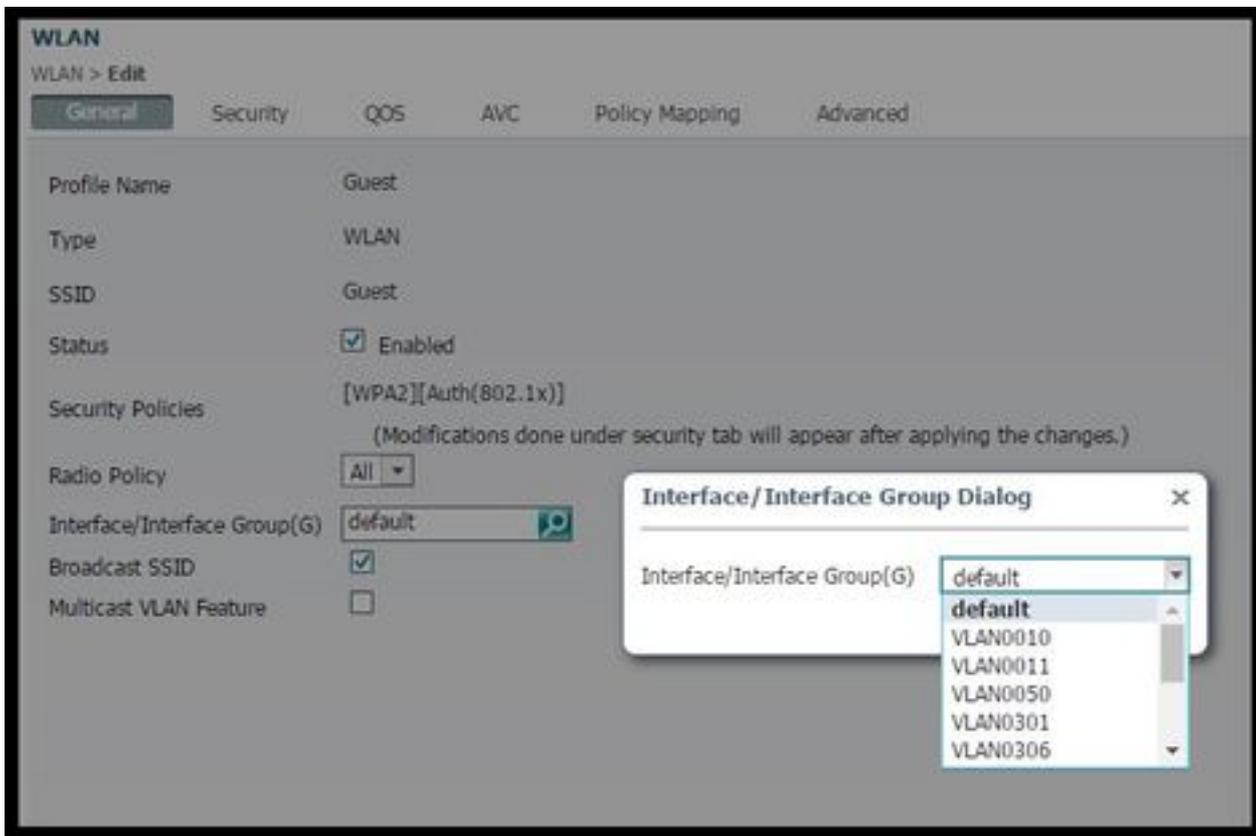
Assigned Server Groups:

Groups In This Method: [Empty list]

SSID-Konfiguration

1. Erstellen der Gast-SSID

- Navigieren Sie zu **Configuration > Wireless > WLANs**, und klicken Sie auf **New**.
- Geben Sie die WLAN-ID, die SSID und den Profilnamen ein, und klicken Sie auf **Apply**.
- Sobald Sie die SSID-Einstellungen unter "Interface / Interface Group" (Schnittstelle/Schnittstellengruppe) vorgenommen haben, wählen Sie die Layer 3-Schnittstelle des Gast-VLAN aus.

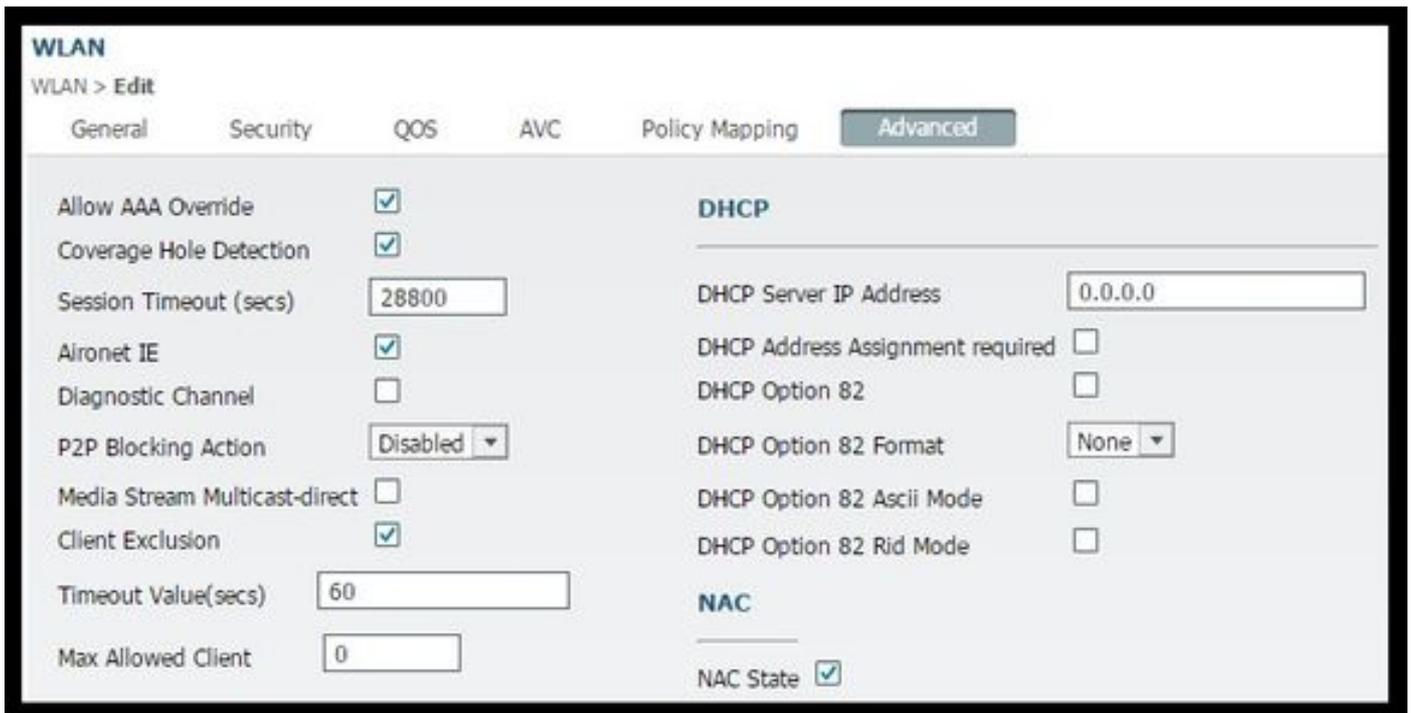


- Wählen Sie unter **Sicherheit > Schicht 2** die Option **Keine** aus, und geben Sie neben **Mac Filtering** den zuvor konfigurierten Namen der MAC-Filtermethodenliste (MacFilterMethod) ein.
- Wählen Sie auf der Registerkarte **Sicherheit > AAA-Server** die entsprechenden Listen der Authentifizierungs- und Abrechnungsmethoden (ISE_Method) aus.



- Aktivieren Sie auf der Registerkarte **"Erweitert"** die Option **"AAA-Außerkräftsetzung und NAC-Status zulassen"**. Die übrigen Einstellungen müssen entsprechend den jeweiligen Bereitstellungsanforderungen (Sitzungs-Timeout, Client-Ausschluss, Unterstützung für Aironet

Extensions) angepasst werden.



- Navigieren Sie zur Registerkarte Allgemein, und setzen Sie den Status auf Aktiviert. Klicken Sie dann auf **Übernehmen**.

Umleiten der ACL-Konfiguration

Auf diese ACL wird später von der ISE im "access-accept"-Modus als Reaktion auf die ursprüngliche MAB-Anfrage verwiesen. Das NGWC bestimmt damit, welcher Datenverkehr umgeleitet werden soll und welcher Datenverkehr durchgelassen werden muss.

- Navigieren Sie zu **Configuration > Security > ACL > Access Control Lists**, und klicken Sie auf **Add New**.
- Wählen Sie Erweitert aus, und geben Sie den ACL-Namen ein.
- Dieses Bild zeigt ein Beispiel für eine typische Umleitungszugriffskontrollliste:



Hinweis: Leitung 10 ist optional. Dies wird in der Regel für Vorschläge zur Fehlerbehebung hinzugefügt. Diese ACL muss den Zugriff auf DHCP, DNS-Dienste sowie auf ISE-Server-Ports mit TCP 8443(ACEs verweigern) ermöglichen. HTTP- und HTTPS-Datenverkehr wird umgeleitet (ACEs zulassen).

Konfiguration der Befehlszeilenschnittstelle (CLI)

Alle in den vorherigen Schritten beschriebenen Konfigurationen können auch über die CLI angewendet werden.

802.1x global aktiviert

```
dot1x system-auth-control
```

Globale AAA-Konfiguration

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

WLAN-Konfiguration

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
```

```
mac-filtering MacFilterMethod
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

ACL umleiten - Beispiel

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

HTTP- und HTTPS-Unterstützung

```
3850#show run | inc http
ip http server
ip http secure-server
```

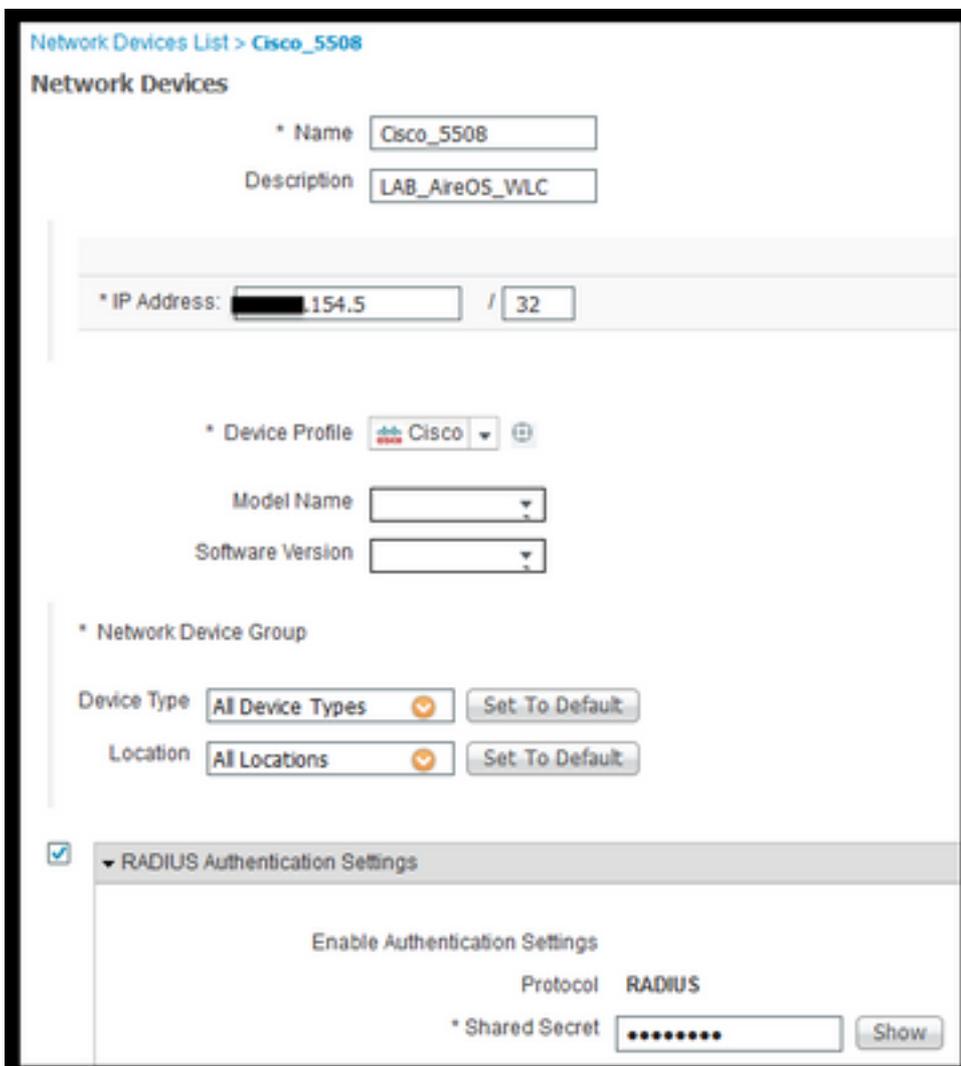
Hinweis: Wenn Sie eine ACL anwenden, um den Zugriff auf den WLC über HTTP zu beschränken, wirkt sich dies auf die Umleitung aus.

Konfigurieren der ISE

In diesem Abschnitt wird die erforderliche Konfiguration für die ISE zur Unterstützung aller in diesem Dokument beschriebenen Anwendungsfälle beschrieben.

Allgemeine ISE-Konfigurationsaufgaben

1. Melden Sie sich bei der ISE an, navigieren Sie zu **Administration > Network Resources > Network Devices**, und klicken Sie auf **Add**.
2. Geben Sie den **Namen** für den WLC und die **IP-Adresse** des Geräts ein.
3. Aktivieren Sie das Kontrollkästchen **RADIUS authentication settings**, und geben Sie den auf der WLC-Seite konfigurierten **Shared Secret** ein. Klicken Sie dann auf **Senden**.

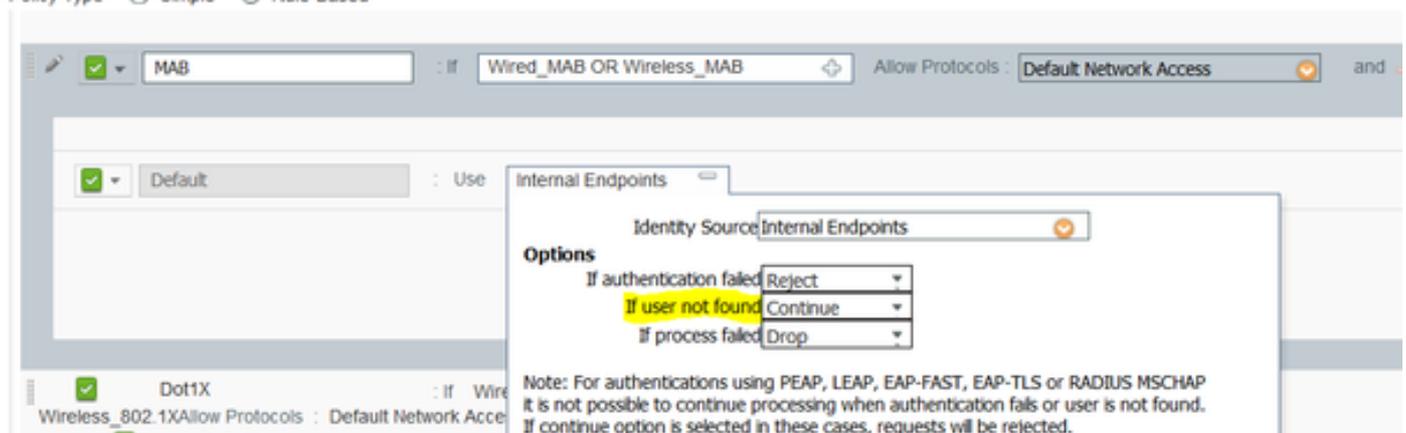


4. Navigieren Sie zu Richtlinie > Authentifizierung und klicken Sie unter MAB auf Bearbeiten, und stellen Sie sicher, dass unter **Verwendung: Interne Endpunkte** die Option **Wenn der Benutzer nicht gefunden wird** auf **Weiter** gesetzt ist (sie muss standardmäßig vorhanden sein).

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based



Anwendungsfall 1: CWA mit Gastauthentifizierung in jeder Benutzerverbindung

Flussübersicht

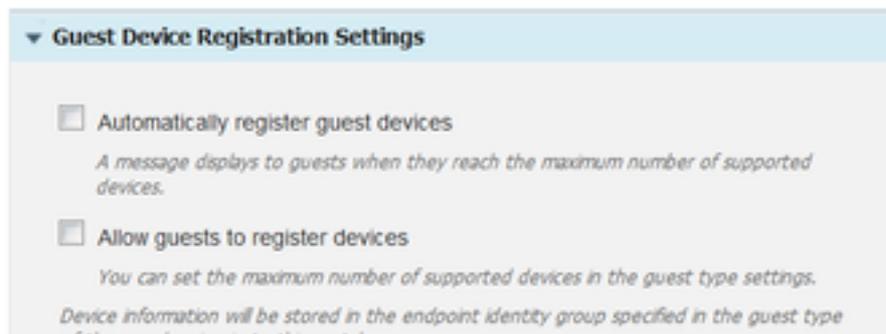
1. Wireless-Benutzer stellt eine Verbindung zum Gast-SSID her.

2. WLC authentifiziert den Endpunkt anhand seiner MAC-Adresse auf der ISE als AAA-Server.
3. Die ISE kehrt zurück und akzeptiert den Zugriff mit zwei Attributwertpaaren (AVPs): url-redirect und url-redirect-acl. Sobald der WLC diese AVPs auf die Endpunktsitzung anwendet, wechselt die Station zu DHCP-Required, und sobald sie eine IP-Adresse erfasst, verbleibt sie in CENTRAL_WEB_AUTH. In diesem Schritt ist der WLC bereit, den HTTP-/HTTPS-Datenverkehr des Clients umzuleiten.
4. Der Endbenutzer öffnet den Webbrowser, und nach Generierung von HTTP- oder HTTPS-Datenverkehr leitet der WLC den Benutzer zum ISE-Gastportal um.
5. Sobald der Benutzer das Gastportal aufruft, fordert er zur Eingabe der Gastanmeldeinformationen auf (in diesem Fall von einem Sponsor erstellt).
6. Bei der Validierung der Anmeldeinformationen zeigt die ISE die AUP-Seite an. Sobald der Client akzeptiert, wird ein dynamischer CoA-Typ "Re-Authenticate" an den WLC gesendet.
7. Der WLC verarbeitet die MAC-Filterauthentifizierung erneut, ohne der Mobilstation eine Deauthentifizierung zu übermitteln. Dies muss nahtlos zum Endpunkt erfolgen.
8. Nach der erneuten Authentifizierung wertet die ISE die Autorisierungsrichtlinien erneut aus. Diesmal erhält der Endpunkt eine Berechtigung für den Zugriff, da zuvor eine erfolgreiche Gastauthentifizierung stattgefunden hat.

Dieser Prozess wiederholt sich jedes Mal, wenn der Benutzer eine Verbindung mit der SSID herstellt.

Konfiguration

1. Navigieren Sie zur ISE, und navigieren Sie zu **Work Centers > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal** (oder erstellen Sie einen neuen Portaltyp "Sponsored-Guest").
2. Deaktivieren Sie unter **Einstellungen für die Gastgeräteregistrierung** alle Optionen, und klicken Sie auf **Speichern**.



3. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**. Klicken Sie auf **Hinzufügen**.

4. Dieses Profil wird als Antwort auf die ursprüngliche MAB-Anfrage (Mac Authentication Bypass) an den WLC, die **Redirect-URL** und die **Redirect-URL-ACL** weitergeleitet.

- Nachdem die Webumleitung (CWA, MDM, NSP, CPP) aktiviert wurde, wählen Sie **Zentrale Webauthentifizierung** aus, geben Sie dann den Namen der Umleitungs-ACL in das Feld **ACL** ein, und wählen Sie unter **Wert** das **gesponserte Gastportal (Standard)** aus (oder ein anderes spezifisches Portal, das in vorherigen Schritten erstellt wurde).

Das Profil muss dem in diesem Bild gezeigten ähneln. Klicken Sie dann auf **Speichern**.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) (i)

Centralized Web Auth ACL Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

Attributdetails am unteren Seitenrand die Attributwertpaare (AVPs), während sie an den WLC übertragen werden

Attributes Details

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
    
```

5. Navigieren Sie zu **Richtlinie > Autorisierung**, und fügen Sie eine neue Regel ein. Diese Regel löst den Umleitungsprozess als Reaktion auf die ursprüngliche MAC-Authentifizierungsanforderung vom WLC aus (in diesem Fall **Wireless_Guest_Redirect**).

6. Unter **Bedingungen** wählen **Bestehende Bedingung aus Bibliothek auswählen**, dann unter **Bedingungsname Zusammengesetzte Bedingung** wählen. Wählen Sie eine vordefinierte zusammengesetzte Bedingung mit der Bezeichnung **Wireless_MAB** aus.

Hinweis: Diese Bedingung umfasst 2 Radius-Attribute, die in der vom WLC erstellten Zugriffsanfrage erwartet werden (NAS-Port-Type= IEEE 802.11 <in allen Wireless-Anfragen vorhanden> und Service-Type = Call Check < bezieht sich auf eine bestimmte Anforderung für eine Umgehung der MAC-Authentifizierung).

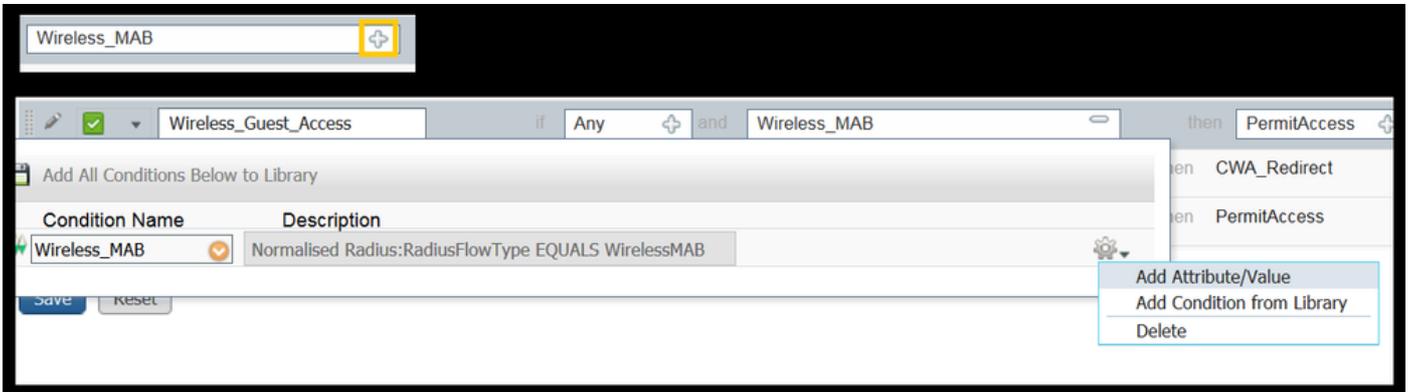
7. Wählen Sie unter Ergebnisse die Option **Standard > CWA_Redirect** (Autorisierungsprofil, das im vorherigen Schritt erstellt wurde). Klicken Sie dann auf **Fertig** und **Speichern**.

Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect Edit | ▾

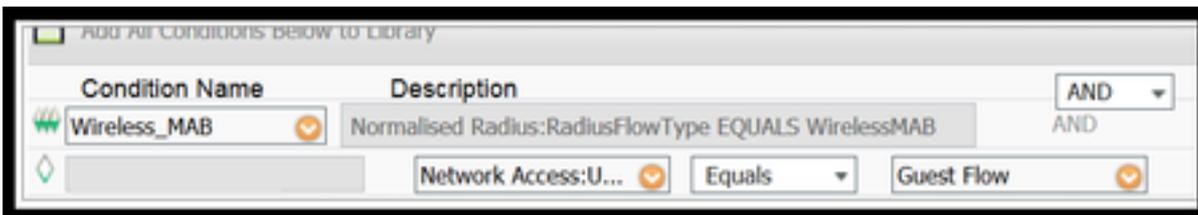
8. Navigieren Sie zum Ende der **CWA_Redirect**-Regel, und klicken Sie auf den Pfeil neben **Bearbeiten**. Dann wählen Sie **Duplikat oben**.

9. Ändern Sie den Namen, da es sich hierbei um die Richtlinie handelt, die der Endpunkt nach der erneuten Authentifizierung der Sitzung durch die ISE-CoA (in diesem Fall Wireless_Guest_Access) erfüllt.

10. Klicken Sie neben **Wireless_MAB** Compound Condition auf das Symbol +, um die Bedingungen zu erweitern, und klicken Sie am Ende der **Wireless_MAB**-Bedingung auf **Attribut/Wert hinzufügen**.



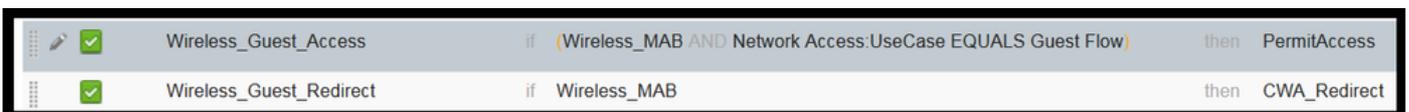
11. Unter "Attribut auswählen" wählen Sie **Netzwerkzugriff > UseCase** gleich **Gastdatenfluss**



12. Wählen Sie unter **Berechtigungen** die Option **Zugriff zulassen**. Klicken Sie dann auf **Fertig** und **Speichern**.



Die beiden Richtlinien müssen ähnlich aussehen:



Anwendungsfall 2: CWA mit Geräteregistrierung zur Durchsetzung der Gastauthentifizierung einmal täglich

Flussübersicht

1. Wireless-Benutzer stellt eine Verbindung zum Gast-SSID her.
2. WLC authentifiziert den Endpunkt anhand seiner MAC-Adresse auf der ISE als AAA-Server.
3. Die ISE gibt zwei Attributwertpaare (AVPs) (url-redirect und url-redirect-acl) zurück und akzeptiert diese.
4. Sobald der WLC diese AVPs auf die Endpunktsitzung anwendet, wechselt die Station zu DHCP-Required, und sobald sie eine IP-Adresse erfasst, verbleibt sie in CENTRAL_WEB_AUTH. In diesem Schritt ist der WLC bereit, den HTTP-/HTTPS-Datenverkehr des Clients umzuleiten.

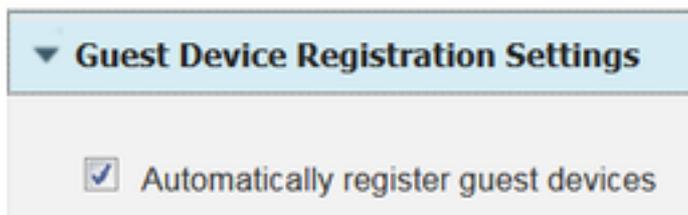
5. Der Endbenutzer öffnet den Webbrowser, und nach Generierung von HTTP- oder HTTPS-Datenverkehr leitet der WLC den Benutzer zum ISE-Gastportal um.
6. Sobald der Benutzer das Gastportal aufruft, wird er aufgefordert, die vom Sponsor erstellten Anmeldeinformationen einzugeben.
7. Bei der Validierung der Anmeldeinformationen fügt die ISE diesen Endpunkt einer bestimmten (vorkonfigurierten) Endpunkt-Identitätsgruppe (Gerätregistrierung) hinzu.
8. Die AUP-Seite wird angezeigt. Sobald der Client akzeptiert, wird ein dynamischer CoA-Typ "Re-Authenticate" angezeigt. Wird an den WLC gesendet.
9. Der WLC verarbeitet die MAC-Filterauthentifizierung erneut, ohne die Mobilstation von der Authentifizierung zu befreien. Dies muss nahtlos zum Endpunkt erfolgen.
10. Nach der erneuten Authentifizierung wertet die ISE die Autorisierungsrichtlinien erneut aus. Dieses Mal, da das Endgerät Mitglied der richtigen Endpoint Identity Group ist, gibt die ISE eine Zugriffsgenehmigung ohne Einschränkungen zurück.
11. Da der Endpunkt in Schritt 6 registriert wurde, kann er jedes Mal, wenn der Benutzer zurückkommt, mit dem Netzwerk verbunden werden, bis er manuell aus der ISE entfernt wird, oder eine Richtlinie zum Löschen von Endpunkten führt eine Leerung der Endpunkte aus, die die Kriterien erfüllen.

In diesem Übungsszenario wird die Authentifizierung einmal täglich durchgesetzt. Der Auslöser für die erneute Authentifizierung ist eine Endpunkt-Bereinigungsrichtlinie, die täglich alle Endpunkte der verwendeten Endpunkt-Identitätsgruppe entfernt.

Hinweis: Es ist möglich, das Gastauthentifizierungsereignis basierend auf der seit der letzten AUP-Annahme verstrichenen Zeit durchzusetzen. Dies kann eine Option sein, wenn Sie die Gastanmeldung häufiger als einmal täglich (z. B. alle 4 Stunden) durchsetzen müssen.

Konfiguration

1. Navigieren Sie auf der ISE zu **Work Centers > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal** (oder erstellen Sie einen neuen Portaltyp "Sponsored-Guest").
2. Überprüfen Sie unter **Guest Device Registration settings**, ob die Option **Automatically register guest devices (Gastgerätregistrierung automatisch registrieren)** aktiviert ist. Klicken Sie auf **Speichern**.



3. Navigieren Sie zu **Work Center > Guest Access > Configure > Guest Types**, oder klicken Sie einfach auf die Verknüpfung, die unter Guest Device Registration Settings im Portal angegeben ist.

▼ Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

4. Wenn der Sponsor-Benutzer ein Gastkonto erstellt, weist er diesem einen Gasttyp zu. Jeder einzelne Gasttyp kann über einen registrierten Endpunkt verfügen, der zu einer anderen Endpunkt-Identitätsgruppe gehört. Um die Endpunkt-Identitätsgruppe zuzuweisen, der das Gerät hinzugefügt werden muss, wählen Sie den Gasttyp aus, den der Sponsor für diese Gastbenutzer verwendet (Dieses Anwendungsbeispiel basiert auf "Wöchentlich" (Standard)).

5. Wählen Sie im Gasttyp unter **Anmeldeoptionen** die Endpunktgruppe aus dem Dropdown-Menü **Endpunktidentitätsgruppe für die Gastgerätregistrierung** aus.

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

6. Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**. Klicken Sie auf **Hinzufügen**.

7. Dieses Profil wird als Antwort auf die ursprüngliche MAB-Anfrage (Mac Authentication Bypass) an den WLC, die **Redirect-URL** und die **Redirect-URL-ACL** weitergeleitet.

- Nachdem die Webumleitung (CWA, MDM, NSP, CPP) aktiviert wurde, wählen Sie **Zentrale Webauthentifizierung** aus, geben Sie dann den Namen der Umleitungs-ACL in das Feld **ACL** ein, und wählen Sie unter **Value** das für diesen Fluss erstellte Portal aus (**CWA_DeviceRegistration**).

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth ACL Value

8. Navigieren Sie zu **Richtlinie > Autorisierung**, und fügen Sie eine neue Regel ein. Diese Regel löst den Umleitungsprozess als Reaktion auf die ursprüngliche MAC-Authentifizierungsanforderung vom WLC aus (in diesem Fall **Wireless_Guest_Redirect**).

9. Unter **Bedingungen** wählen **Bestehende Bedingung aus Bibliothek auswählen**, dann unter **Bedingungsname Zusammengesetzte Bedingung** wählen. Wählen Sie eine vordefinierte zusammengesetzte Bedingung mit der Bezeichnung **Wireless_MAB aus**.

10. Wählen Sie unter Ergebnisse die Option **Standard > CWA_DeviceRegistration** (Autorisierungsprofil, das im vorherigen Schritt erstellt wurde) aus. Klicken Sie dann auf **Fertig** und **Speichern**.

Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

11. Duplizieren Sie die obige Richtlinie, ändern Sie ihren Namen, da dies die Richtlinie ist, auf die der Endpunkt nach der Rückgabe vom Ereignis für die erneute Authentifizierung (**Wireless_Guest_Access**) zugreift.

12. Wählen Sie im Feld **Identitätsgruppendetails** die Option **Endpoint Identity Group** aus, und wählen Sie die Gruppe aus, auf die Sie unter Gasttyp (GuestEndpoints) verwiesen haben.

13. Wählen Sie unter Ergebnisse die Option **PermitAccess aus**. Klicken Sie auf **Fertig**, und **speichern Sie** die Änderungen.

Wireless_Guest_Access if GuestEndpoints AND Wireless_MAB then PermitAccess

Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

14. Erstellen Sie eine Richtlinie zum Löschen von Endpunkten, die die GuestEndpoint Group

täglich löscht.

- Navigieren Sie zu **Administration > Identity Management > Settings > Endpoint Purge**.
- Unter **Purge** rules (Regeln löschen) muss es standardmäßig eine geben, die das Löschen von GuestEndpoints auslöst, wenn die abgelaufene Zeit länger als 30 Tage ist.
- Ändern Sie die vorhandene Richtlinie für GuestEndpoints, oder erstellen Sie eine neue Richtlinie (falls die Standardrichtlinie entfernt wurde). Beachten Sie, dass die Löschrichtlinien täglich zu einer definierten Zeit ausgeführt werden.

In diesem Fall ist die Bedingung Mitglieder von GuestEndpoints mit abgelaufenen Tagen unter 1 Tag.

Anwendungsfall 3: HostSpot-Portal

Flussübersicht

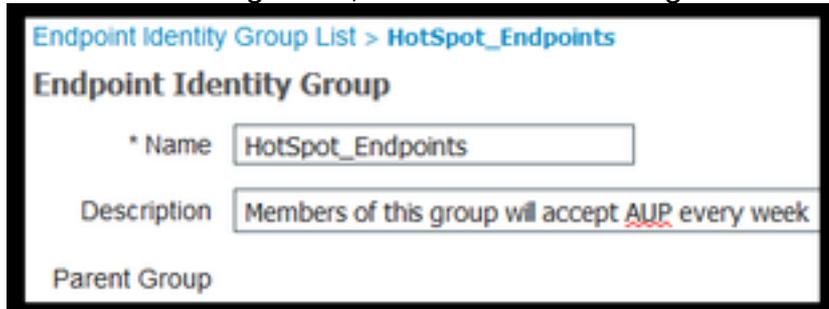
1. Wireless-Benutzer stellt eine Verbindung zum Gast-SSID her.
2. WLC authentifiziert den Endpunkt anhand seiner MAC-Adresse und verwendet die ISE als AAA-Server.
3. Die ISE gibt mit zwei Attribut-Wertepaaren (AVPs) einen Wert für access-accept zurück: url-redirect und url-redirect-acl.
4. Sobald der WLC diese AVPs auf die Endpunktsitzung anwendet, wechselt die Station zu DHCP-Required, und sobald sie eine IP-Adresse erfasst, verbleibt sie in CENTRAL_WEB_AUTH. In diesem Schritt ist der WLC bereit, den HTTP-/HTTPS-Datenverkehr des Clients umzuleiten.
5. Der Endbenutzer öffnet den Webbrowser, und der WLC leitet den Benutzer nach Generierung von HTTP- oder HTTPS-Datenverkehr zum ISE HotSpot-Portal weiter.
6. Sobald der Benutzer das Portal betritt, wird er aufgefordert, eine Richtlinie für die akzeptable Nutzung zu akzeptieren.
7. Die ISE fügt der konfigurierten Endpunkt-Identitätsgruppe die Endpunkt-MAC-Adresse (Endpunkt-ID) hinzu.
8. Der Policy Services Node (PSN), der die Anfrage verarbeitet, sendet ein dynamisches CoA-**Zurücksetzen** vom Typ **Admin-Reset** an den WLC.
9. Sobald der WLC die Verarbeitung der eingehenden CoA abgeschlossen hat, sendet er eine Deauthentifizierung an den Client (die Verbindung geht für die Zeit verloren, die der Client benötigt, um wiederzukommen).
10. Sobald der Client die Verbindung wieder herstellt, wird eine neue Sitzung erstellt, sodass auf ISE-Seite keine Sitzungskontinuität besteht. Das bedeutet, dass die Authentifizierung als neuer Thread verarbeitet wird.
11. Da der Endpunkt der konfigurierten Endpunkt-Identitätsgruppe hinzugefügt wird und eine Autorisierungsrichtlinie vorhanden ist, die überprüft, ob der Endpunkt zu dieser Gruppe gehört, entspricht die neue Authentifizierung dieser Richtlinie. Das Ergebnis ist der uneingeschränkte Zugriff auf das Gastnetzwerk.
12. Der Benutzer darf die AUP nicht erneut akzeptieren müssen, es sei denn, das Endpunkt-Identitätsobjekt wird als Ergebnis einer Richtlinie zum Löschen von Endpunkten aus der ISE-Datenbank gelöscht.

Konfiguration

1. Erstellen Sie eine neue Endpunkt-Identitätsgruppe, in die diese Geräte nach der

Registrierung verschoben werden. Navigieren Sie zu **Work Centers > Guest Access > Identity Groups > Endpoint Identity Groups**, und klicken Sie auf  .

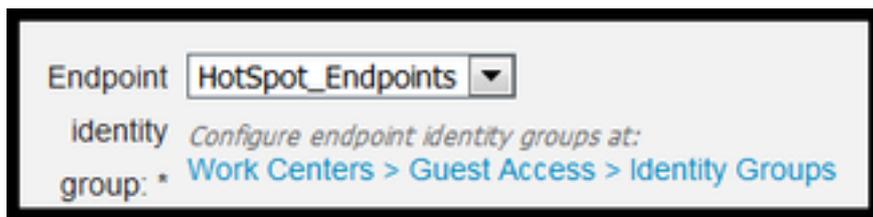
- Geben Sie einen Gruppennamen ein (in diesem Fall Hotspot_Endpoints). Fügen Sie eine Beschreibung hinzu, und es ist keine übergeordnete Gruppe erforderlich.



The screenshot shows the configuration page for an Endpoint Identity Group. The breadcrumb navigation is "Endpoint Identity Group List > HotSpot_Endpoints". The title is "Endpoint Identity Group". There are three input fields: "Name" with the value "HotSpot_Endpoints", "Description" with the value "Members of this group will accept AUP every week", and "Parent Group" which is currently empty.

2. Navigieren Sie zu **Work Centers > Guest Access > Configure > Guest Portals** > wählen Sie **Hotspot Portal (Standard)**.

3. Erweitern Sie Portal Settings, und wählen Sie unter Endpoint Identity Group (Endpunkt-Identitätsgruppe) die Gruppe **HotSpot_Endpoints** unter **Endpoint Identity Group (Endpunkt-Identitätsgruppe)** aus. Dadurch werden die registrierten Geräte an die angegebene Gruppe gesendet.



The screenshot shows a dropdown menu for selecting an Endpoint Identity Group. The selected value is "HotSpot_Endpoints". Below the dropdown, there is a label "Identity" and a link "Configure endpoint identity groups at: Work Centers > Guest Access > Identity Groups".

4. **Speichern Sie** die Änderungen.

5. Erstellen Sie das Autorisierungsprofil, das das HotSpot-Portal nach der vom WLC generierten MAB-Authentifizierung aufruft.

- Navigieren Sie zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**, und erstellen Sie ein Profil (HotSpotRedirect).
- Nachdem die **Webumleitung (CWA, MDM, NSP, CPP)** aktiviert wurde, wählen Sie **Hot Spot aus**, geben Sie dann den Namen der Umleitungszugriffskontrollliste in das Feld ACL (Guest_Redirect) ein, und wählen Sie als Wert das richtige Portal aus (**Hotspot-Portal (Standard)**).

Add New Standard Profile

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot: ACL: Value:

Static IP/Host name/FQDN

Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = url-redirect-ad=Guest_Redirect
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. Erstellen Sie die Autorisierungsrichtlinie, die das HotSpotRedirect-Ergebnis bei der ersten MAB-Anfrage vom WLC auslöst.

- Navigieren Sie zu **Richtlinie > Autorisierung**, und fügen Sie eine neue Regel ein. Diese Regel löst den Umleitungsprozess als Reaktion auf die ursprüngliche MAC-Authentifizierungsanforderung vom WLC aus (in diesem Fall **Wireless_HotSpot_Redirect**).
- Wählen Sie unter **Bedingungen Bestehende Bedingung aus Bibliothek auswählen**, und wählen Sie dann unter **Bedingungsname Zusammengesetzte Bedingung** aus.
- Wählen Sie unter Ergebnisse die Option **Standard > HotSpotRedirect** (Autorisierungsprofil, das im vorherigen Schritt erstellt wurde) aus. Klicken Sie dann auf **Fertig** und **Speichern**.

7. Erstellen Sie die zweite Autorisierungsrichtlinie

- Duplizieren Sie die obige Richtlinie, und ändern Sie ihren Namen, da dies die Richtlinie ist, die der Endpunkt nach der Rückgabe durch das Ereignis zur erneuten Authentifizierung trifft (**Wireless_HotSpot_Access**).
- Wählen Sie im Feld **Identitätsgruppendetails** die Option **Endpoint Identity Group** und dann die zuvor erstellte Gruppe aus (**HotSpot_Endpoints**).
- Wählen Sie unter Ergebnisse die Option **PermitAccess** aus. Klicken Sie auf **Fertig**, und **speichern Sie** die Änderungen.

<input checked="" type="checkbox"/>	Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
<input checked="" type="checkbox"/>	Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

8. Konfigurieren Sie die Bereinigungsrichtlinie, die Endpunkte mit einer abgelaufenen Zeit von mehr als 5 Tagen löscht.

- Navigieren Sie zu **Administration > Identity Management > Settings > Endpoint Purge**, und erstellen Sie unter Purge rules (Bereinigungsregeln) eine neue.
- Wählen Sie im Feld **Identitätsgruppendetails** die Option **Endpunkt-Identitätsgruppe > HotSpot_Endpoints** aus.

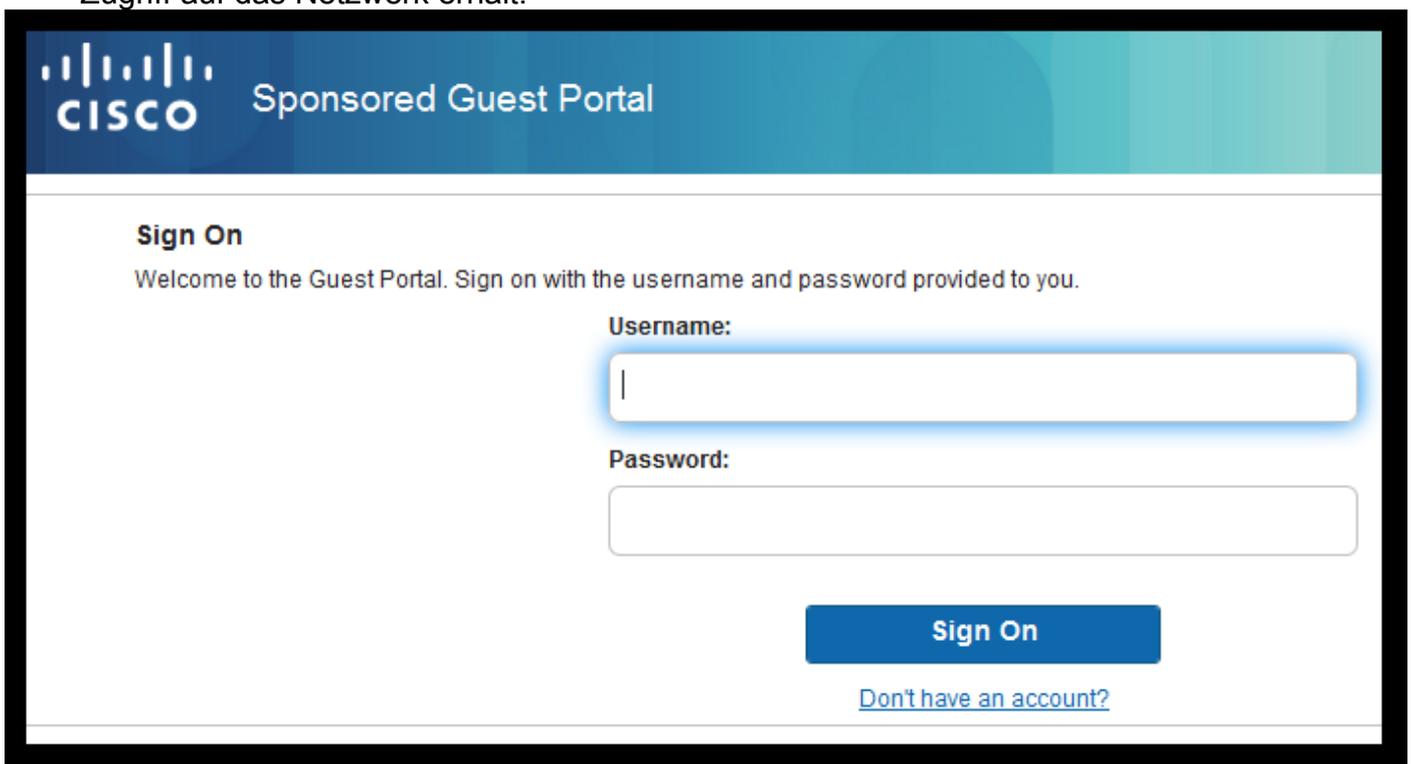
- Klicken Sie unter **Bedingungen** auf **Neue Bedingung erstellen (erweiterte Option)** .
- Wählen Sie unter Attribut auswählen die Option *ENDPUNTPURGE: ElapsedDays GREATER THAN 5 days*

```
HotSpot_Endpoints_PurgeRule if HotSpot_Endpoints AND ENDPUNTPURGE:ElapsedDays GREATER THAN 5
```

Überprüfung

Anwendungsfall 1

1. Der Benutzer stellt eine Verbindung zum Gast-SSID her.
2. Er öffnet den Browser und sobald HTTP-Datenverkehr generiert wird, wird das Gastportal angezeigt.
3. Sobald sich der Gastbenutzer authentifiziert und die AUP akzeptiert, wird eine Erfolgsseite angezeigt.
4. Ein Re-Authenticate CoA wird ausgesendet (transparent für den Client).
5. Die Endpunktsitzung wird mit vollem Zugriff auf das Netzwerk erneut authentifiziert.
6. Jede nachfolgende Gastverbindung muss die Gast-Authentifizierung bestehen, bevor sie Zugriff auf das Netzwerk erhält.





Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Success

You now have Internet access through this network.

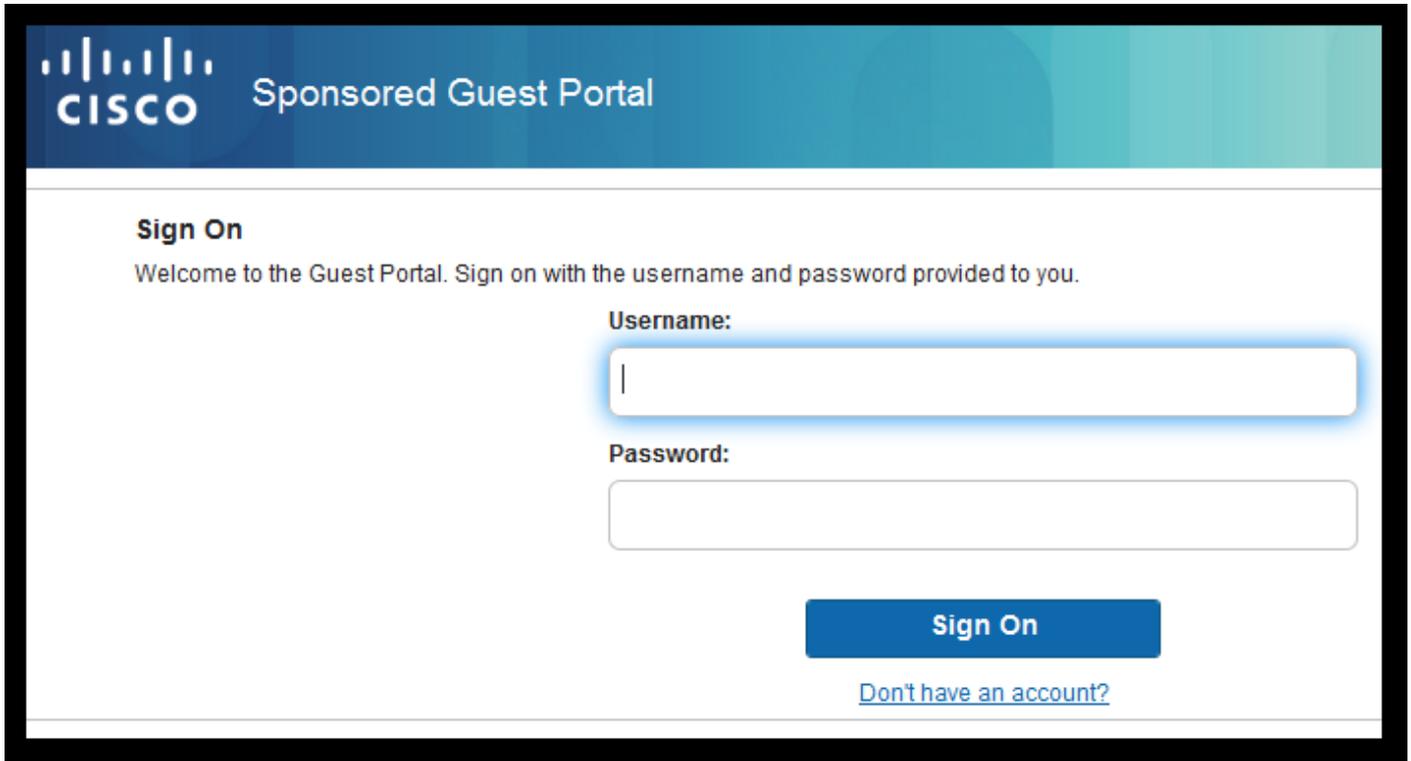
Fluss aus ISE RADIUS Live-Protokollen:

🔍	🔒	1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
✅	🔒	1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
✅	🔒		68:7F:74:72:18:2E					← CoA Event
✅	🔒	1001	68:7F:74:72:18:2E					← Guest Authentication Event
✅	🔒	68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

Anwendungsfall 2

1. Der Benutzer stellt eine Verbindung zum Gast-SSID her.
2. Er öffnet den Browser und sobald HTTP-Datenverkehr generiert wird, wird das Gastportal angezeigt.

3. Sobald sich der Gastbenutzer authentifiziert und die AUP akzeptiert, wird das Gerät registriert.
4. Es wird eine Erfolgsseite angezeigt, und eine CoA für erneute Authentifizierung wird gesendet (für den Client transparent).
5. Die Endpunktsitzung wird mit vollem Zugriff auf das Netzwerk erneut authentifiziert.
6. Alle nachfolgenden Böenverbindungen (9) sind ohne Erzwingung der Gastauthentifizierung zulässig, solange sich das Endgerät noch in der konfigurierten Endpunkt-Identitätsgruppe befindet.



The image shows a screenshot of the Cisco Sponsored Guest Portal sign-on page. The header features the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". A blue "Sign On" button is positioned below the password field, and a link for "Don't have an account?" is located at the bottom right of the form area.

CISCO Sponsored Guest Portal

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

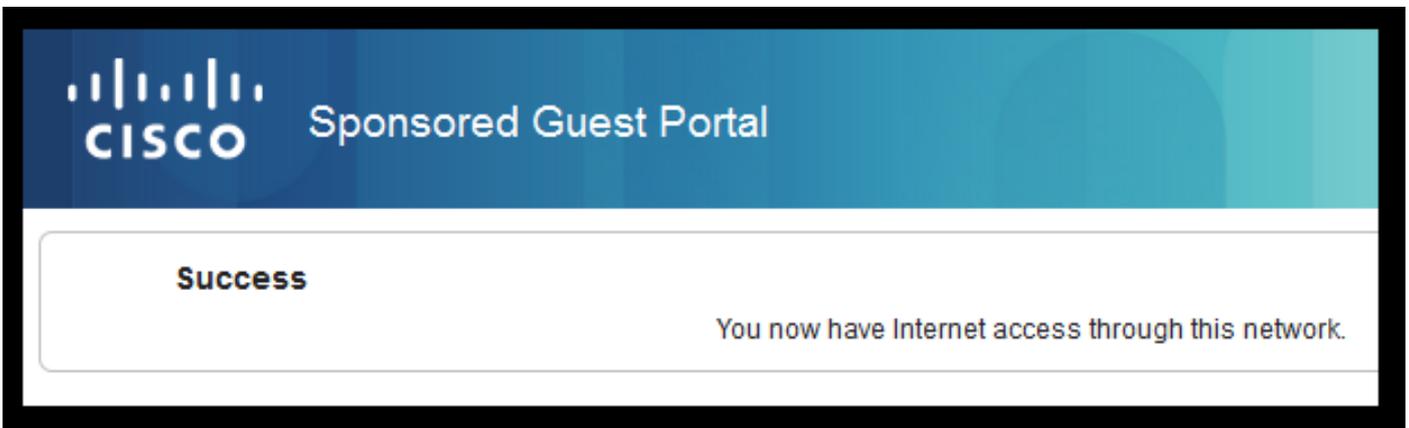


Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



Fluss aus ISE RADIUS Live-Protokollen:

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	
		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	GuestEndpoints
		hfr592	68.7F:74.72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
			68.7F:74.72:...		
		hfr592	68.7F:74.72:...		GuestType_Contractor (default)
		68.7F:74.72:1...	68.7F:74.72:...	CWA_DeviceRegistration	Profiled

Accounting Start

Subsequent MAB request(no redirect to guest portal)

Re-Authentication Event

CoA Reauth Event

Guest Authentication and Device Registration

Initial MAB request

Anwendungsfall 3

1. Der Benutzer stellt eine Verbindung zum Gast-SSID her.
2. Er öffnet den Browser und sobald HTTP-Verkehr generiert wird, wird eine AUP-Seite angezeigt.
3. Sobald der Gastbenutzer die AUP akzeptiert, wird das Gerät registriert.
4. Es wird eine Erfolgsseite angezeigt und eine Admin-Reset CoA gesendet (transparent für den Client).
5. Der Endpunkt stellt erneut eine Verbindung mit vollständigem Netzwerkzugriff her.
6. Alle nachfolgenden Gastverbindungen sind ohne Erzwingung der AUP-Akzeptanz zulässig (sofern nicht anders konfiguriert), solange der Endpunkt in der konfigurierten Endpunkt-Identitätsgruppe verbleibt.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

FlexConnect Local-Switching in AireOS

Wenn das lokale FlexConnect-Switching konfiguriert ist, muss der Netzwerkadministrator Folgendes sicherstellen:

- Die Umleitungs-ACL wird als FlexConnect-ACL konfiguriert.
- Die Umleitungszugriffskontrollliste wurde als Richtlinie entweder über den Access Point selbst auf der Registerkarte **FlexConnect > External Web Authentication ACLs > Policies > Select Redirect ACL** (Umleitungszugriffskontrollliste auswählen) und dann auf **Apply (Anwenden)** angewendet

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

[Local Split ACLs](#)

[Central DHCP Processing](#)

[Layer2 ACLs](#)

Policies

Policy ACL CWA_Redirect

Policy Access Control Lists

CWA_Redirect

Oder indem Sie die Richtlinien-ACL zur FlexConnect-Gruppe hinzufügen, zu der gehört (Wireless > FlexConnect-Gruppen > Wählen Sie die richtige Gruppe aus > ACL-Zuordnung > Richtlinien Wählen Sie die Umleitungs-ACL aus, und klicken Sie auf Hinzufügen)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL CWA_Redirect

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

Durch Hinzufügen einer Richtlinien-ACL überträgt der WLC die konfigurierte ACL an die AP(s) der FlexConnect-Gruppe. Wenn Sie dies nicht tun, liegt ein Problem mit der Webumleitung vor.

Szenario ausländischer Anker

In auto-anchor (Foreign-Anchor) Szenarien ist es wichtig, diese Fakten hervorzuheben:

- Die Umleitungszugriffskontrollliste muss sowohl auf dem Fremd- als auch auf dem Anker-WLC definiert werden. Auch wenn es nur auf dem Anker erzwungen wird.
- Die Layer-2-Authentifizierung wird immer vom ausländischen WLC durchgeführt. Dies ist während der Entwurfsphasen (auch für die Fehlerbehebung) von entscheidender Bedeutung, da der gesamte RADIUS-Authentifizierungs- und Accounting-Datenverkehr zwischen der ISE und dem ausländischen WLC stattfindet.
- Nachdem die Umleitungs-AVPs auf die Client-Sitzung angewendet wurden, aktualisiert der Foreign WLC die Client-Sitzung mithilfe einer Mobility Handoff-Nachricht.
- An diesem Punkt beginnt der Anker-WLC mit der Durchsetzung der Umleitung mithilfe der vorkonfigurierten Umleitungs-ACL.
- Die Abrechnung muss für die Anker-WLC-SSID vollständig deaktiviert werden, um zu verhindern, dass Abrechnungsaktualisierungen für die ISE (die auf dasselbe Authentifizierungsereignis verweisen) sowohl vom Anker als auch vom Fremdsystem eingehen.
- URL-basierte ACLs werden in Foreign-Anchor-Szenarien nicht unterstützt.

Fehlerbehebung

Häufig auftretende unterbrochene Zustände auf AireOS und dem WLC mit konvergentem Zugriff

1. Der Client kann der Gast-SSID nicht beitreten.

Ein "**show client detail xx:xx:xx:xx:xx:xx**" zeigt, dass der Client im **START-Modus** feststeckt. In der Regel ist dies ein Hinweis darauf, dass der WLC ein vom AAA-Server zurückgegebenes Attribut nicht anwenden kann.

Überprüfen Sie, ob der von der ISE weitergeleitete ACL-Name genau mit dem Namen der vordefinierten ACL auf dem WLC übereinstimmt.

Dasselbe Prinzip gilt für alle anderen Attribute, die Sie der ISE für die Übertragung an den WLC konfiguriert haben (VLAN-IDs, Schnittstellennamen, Airespace-ACLs). Der Client muss dann zu DHCP und dann zu **CENTRAL_WEB_AUTH** wechseln.

2. Umleitungs-AVPs werden auf die Client-Sitzung angewendet, aber die Umleitung funktioniert nicht.

Überprüfen Sie, ob der Client-Richtlinien-Manager-Status **CENTRAL_WEB_AUTH** mit einer gültigen IP-Adresse ist, die an der konfigurierten dynamischen Schnittstelle für die SSID ausgerichtet ist, und ob die Attribute "Redirect ACL" (ACL umleiten) und "URL-Redirect" (URL-Umleitung) auf die Sitzung des Clients angewendet werden.

ACL umleiten

In AireOS-WLCs muss die Umleitungszugriffskontrollliste explizit den Datenverkehr zulassen, der nicht umgeleitet werden darf, wie DNS und ISE auf TCP-Port 8443 in beide Richtungen, und die

implizite deny ip any löst die Umleitung des restlichen Datenverkehrs aus.

Beim konvergenten Zugriff ist die Logik umgekehrt. Umleitung durch Deny ACEs umgehen, während permit ACEs die Umleitung auslösen. Aus diesem Grund wird empfohlen, die TCP-Ports 80 und 443 explizit zuzulassen.

Überprüfen des Zugriffs auf die ISE über Port 8443 vom Guest-VLAN Wenn aus Konfigurationsperspektive alles gut aussieht, besteht der einfachste Weg vorwärts darin, eine Aufzeichnung hinter dem Wireless-Adapter des Clients zu machen und zu überprüfen, wo die Umleitung unterbrochen wird.

- Kommt es zur DNS-Auflösung?
- Ist der TCP 3-Wege-Handshake auf der angeforderten Seite beendet?
- Gibt der WLC eine Umleitungsaktion zurück, nachdem der Client die GET-Anforderung initiiert hat?
- Ist der TCP 3-Wege-Handshake gegen ISE über 8443 abgeschlossen?

3. Der Client kann nicht auf das Netzwerk zugreifen, nachdem die ISE eine VLAN-Änderung am Ende des Gastflusses per Push gesendet hat.

Wenn der Client zu Beginn des Datenflusses eine IP-Adresse erfasst hat (Status "Vor der Umleitung") und eine VLAN-Änderung nach der Guest-Authentifizierung nach unten verschoben wird (nach der CoA-erneuten Authentifizierung), ist die einzige Möglichkeit, eine DHCP-Freigabe/Verlängerung im Guest-Datenfluss (ohne Status-Agent) zu erzwingen, über ein Java-Applet, das auf mobilen Geräten nicht funktioniert.

Dadurch bleibt der Client im VLAN X mit einer IP-Adresse von VLAN Y schwarz. Dies muss bei der Planung der Lösung berücksichtigt werden.

4. ISE zeigt während der Umleitung die Meldung "HTTP 500 Internal error, Radius session not found" (Interner HTTP-500-Fehler, Radius-Sitzung nicht gefunden) im Browser des Gastclients an

Dies ist in der Regel ein Indikator für einen Sitzungsverlust bei der ISE (Sitzung wurde beendet). Der häufigste Grund hierfür ist die auf dem Anchor-WLC konfigurierte Abrechnung, wenn Foreign-Anchor bereitgestellt wurde. Um dies zu beheben, deaktivieren Sie die Kontoführung auf dem Anker und lassen den Foreign-Handle "Authentifizierung und Kontoführung".

5. Der Client trennt die Verbindung und bleibt getrennt oder stellt eine Verbindung zu einem anderen SSID her, nachdem er AUP im HotSpot-Portal der ISE akzeptiert hat.

Dies ist in HotSpot aufgrund der dynamischen Autorisierungsänderung (Dynamic Change of Authorization, CoA) zu erwarten, die an diesem Fluss (CoA Admin Reset) beteiligt ist, der bewirkt, dass der WLC einen Fehler an die Wireless-Station ausgibt. Bei den meisten Wireless-Endgeräten gibt es nach der Deauthentifizierung keine Probleme, die SSID wiederherzustellen. In einigen Fällen stellt der Client jedoch als Reaktion auf das Deauthentifizierungsereignis eine Verbindung mit einer anderen bevorzugten SSID her. Von der ISE oder dem WLC kann nichts unternommen werden, um dies zu verhindern, da es Sache des Wireless-Clients ist, sich an die ursprüngliche SSID zu halten oder eine Verbindung zu einer anderen verfügbaren (bevorzugten) SSID herzustellen.

In diesem Fall muss der Wireless-Benutzer manuell eine Verbindung zum HotSpot-SSID herstellen.

AireOS-WLC

```
(Cisco Controller) >debug client
```

Der Debug-Client legt eine Reihe von Komponenten fest, die an Änderungen des Client-Zustandscomputers beteiligt sind.

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

```
Debug Flags Enabled:
```

```
  dhcp packet enabled.  
  dot11 mobile enabled.  
  dot11 state enabled  
  dot1x events enabled.  
  dot1x states enabled.  
  mobility client handoff enabled.  
  pem events enabled.  
  pem state enabled.  
  802.11r event debug enabled.  
  802.11w event debug enabled.  
  CCKM client debug enabled.
```

AAA-Komponenten debuggen

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

Dies kann sich je nach Anzahl der Benutzer, die über MAB oder Dot1X SSID eine Verbindung herstellen, auf die Ressourcen auswirken. Diese Komponenten auf DEBUG-Ebene zeichnen AAA-Transaktionen zwischen WLC und ISE auf und drucken die RADIUS-Pakete auf dem Bildschirm aus.

Dies ist von entscheidender Bedeutung, wenn die ISE die erwarteten Attribute nicht liefern kann oder wenn der WLC sie nicht richtig verarbeitet.

Web-Auth-Umleitung

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

Auf diese Weise kann überprüft werden, ob der WLC die Umleitung erfolgreich auslöst. Dies ist ein Beispiel dafür, wie die Umleitung bei Debuggen aussehen muss:

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
```

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

NGWC

Der Debug-Client legt eine Reihe von Komponenten fest, die an Änderungen des Client-Zustandscomputers beteiligt sind.

```
3850#debug client mac-address <client MAC>
```

Diese Komponente druckt die RADIUS-Pakete (Authentication und Accounting) auf dem Bildschirm. Dies ist nützlich, wenn Sie sicherstellen müssen, dass die ISE die richtigen AVPs liefert, und wenn Sie sicherstellen müssen, dass die CoA ordnungsgemäß gesendet und verarbeitet wird.

```
3850#debug radius
```

Dies betrifft alle AAA-Übergänge (Authentifizierung, Autorisierung und Abrechnung), an denen Wireless-Clients beteiligt sind. Dies ist wichtig, um sicherzustellen, dass der WLC die AVPs richtig analysiert und auf die Client-Sitzung anwendet.

```
3850#debug aaa wireless all
```

Dies kann aktiviert werden, wenn Sie ein Umleitungsproblem im NGWC vermuten.

```
3850#debug epm plugin redirect all
3850#debug ip http transactions
3850#debug ip http url
```

ISE

RADIUS-Live-Protokolle

Vergewissern Sie sich, dass die erste MAB-Anfrage in der ISE korrekt verarbeitet wurde und dass die ISE die erwarteten Attribute zurücksetzt. Navigieren Sie zu **Operations > RADIUS > Live logs (Vorgänge > RADIUS > Live-Protokolle)**, und filtern Sie die Ausgabe mithilfe der Client-MAC unter **Endpoint ID (Endpunkt-ID)**. Sobald das Authentifizierungsereignis gefunden wurde, klicken Sie auf **Details**, und überprüfen Sie dann die Ergebnisse, die als Teil des Accept-Prozesses übertragen wurden.



Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

TCPDump

Diese Funktion kann verwendet werden, wenn eine eingehendere Untersuchung des RADIUS-Paketaustauschs zwischen der ISE und dem WLC erforderlich ist. Auf diese Weise können Sie nachweisen, dass die ISE die richtigen Attribute im access-accept-Modus sendet, ohne dass auf der WLC-Seite Debug-Vorgänge aktiviert werden müssen. Um eine Erfassung mit TCDDump zu starten, navigieren Sie zu **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCPDump**.

Dies ist ein Beispiel für einen korrekten Fluss, der über TCPDump erfasst wurde.

Source	Destination	Protocol	Length	Info
████████.154.5	████████.157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
████████.157.13	████████.154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
████████.154.5	████████.157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
████████.157.13	████████.154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
████████.157.13	████████.154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
████████.154.5	████████.157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
████████.154.5	████████.157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
████████.157.13	████████.154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

Nachfolgend sind die AVPs aufgeführt, die als Antwort auf die ursprüngliche MAB-Anfrage gesendet wurden (zweites Paket im obigen Screenshot).

RADIUS Protocol

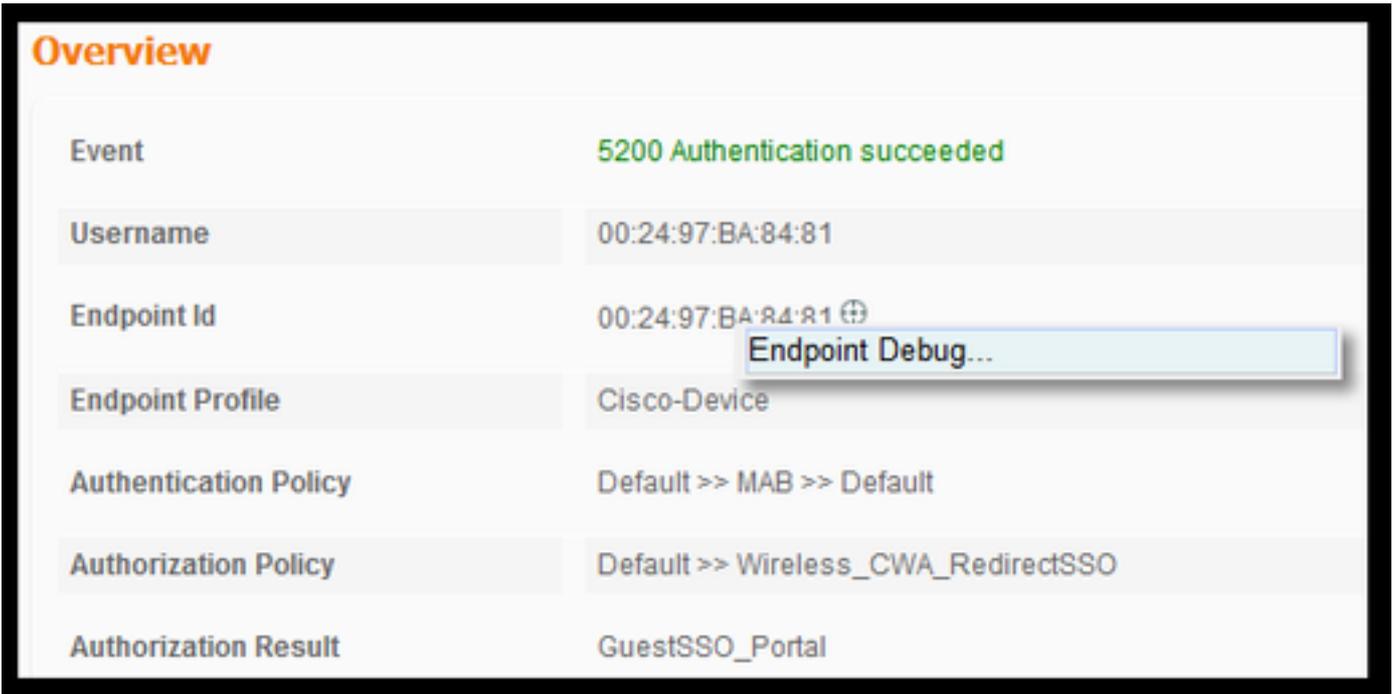
```
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: fleaaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
```

```
VSA: l=189 t=Cisco-AVPair(1): url-redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a050000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622
AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)
```

Endpunktdebugs:

Wenn Sie sich eingehender mit ISE-Prozessen befassen müssen, die Richtlinienentscheidungen, Portalauswahl, Gastauthentifizierung und CoA-Verarbeitung umfassen, besteht der einfachste Weg, dies zu erreichen, darin, **Endpunktdebugs** zu aktivieren, anstatt vollständige Komponenten auf die Debugstufe festlegen zu müssen.

Um dies zu aktivieren, navigieren Sie zu **Operations > Troubleshooting > DiagnosticTools > General Tools > EndPoint Debug**.

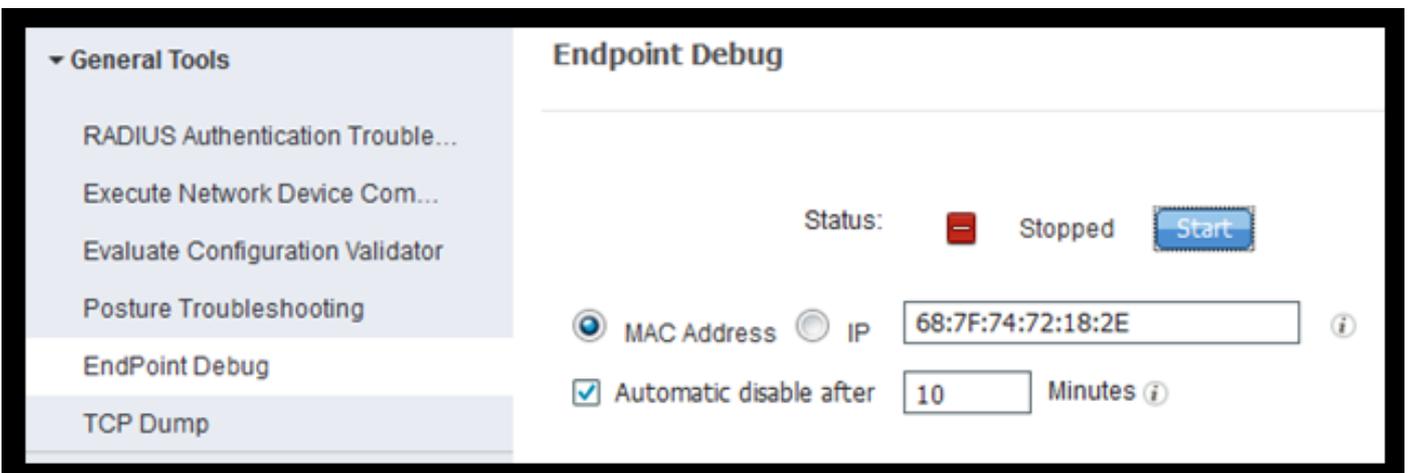


The screenshot shows the 'Overview' page in the ISE interface. It displays the following information:

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

A tooltip labeled 'Endpoint Debug...' is visible over the Endpoint Id field.

Geben Sie auf der Seite Endpoint debug (Endpunktdebuggen) die Endpunkt-MAC-Adresse ein, und klicken Sie auf start (Starten), wenn Sie bereit sind, das Problem neu zu erstellen.



The screenshot shows the 'Endpoint Debug' configuration page. On the left is a sidebar with 'General Tools' expanded, showing options like 'RADIUS Authentication Trouble...', 'Execute Network Device Com...', 'Evaluate Configuration Validator', 'Posture Troubleshooting', 'EndPoint Debug', and 'TCP Dump'. The main area is titled 'Endpoint Debug' and contains the following settings:

- Status: Stopped (with a red stop icon and a 'Start' button)
- MAC Address (selected) or IP: 68:7F:74:72:18:2E ⓘ
- Automatic disable after: 10 Minutes ⓘ

Wenn das Debuggen beendet wurde, klicken Sie auf den Link, der die Endpunkt-ID identifiziert, um die Debugausgabe herunterzuladen.

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

Zugehörige Informationen

[Empfohlene AireOS-Versionen für das TAC](#)

[Konfigurationsanleitung für den Cisco Wireless Controller, Version 8.0.](#)

[Administratorleitfaden für die Cisco Identity Services Engine, Version 2.1](#)

[Universelle NGWC Wireless-Konfiguration mit Identity Services Engine](#)

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.