

Konfigurieren von 9800 WLC und Aruba ClearPass - Gastzugriff und FlexConnect

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Datenverkehrsfluss für CWA Guest Enterprise-Bereitstellung](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Konfigurieren der C9800-Parameter für den Wireless-Gastzugriff](#)

[C9800 - AAA-Konfiguration für Gast](#)

[C9800 - Konfigurieren der Umleitungs-ACL](#)

[C9800 - Konfiguration des Gast-WLAN-Profiles](#)

[C9800 - Definition des Gastrichtlinienprofils](#)

[C9800 - Richtlinien-Tag](#)

[C9800 - AP-Beitrittsprofil](#)

[C9800 - Flex Profile](#)

[C9800 - Site-Tag](#)

[C9800 - RF-Profil](#)

[C9800 - Zuweisen von Tags zu AP](#)

[Aruba CPPM-Instanz konfigurieren](#)

[Aruba ClearPass Server - Erstkonfiguration](#)

[Lizenzen beantragen](#)

[Hostname des Servers](#)

[CPPM-Webserverzertifikat \(HTTPS\) generieren](#)

[Definieren des C9800 WLC als Netzwerkgerät](#)

[Gastportalseite und CoA-Timer](#)

[ClearPass - Gast-CWA-Konfiguration](#)

[Metadatenattribut für ClearPass-Endpunkt: Gast-Internet zulassen](#)

[Konfiguration der ClearPass-Richtlinie zur erneuten Authentifizierung](#)

[Konfiguration des Durchsetzungsprofils für die ClearPass-Gastportal-Umleitung](#)

[Konfiguration des Durchsetzungsprofils für ClearPass-Metadaten](#)

[Richtlinienkonfiguration für die Durchsetzungsrichtlinie für den Gastzugriff mit ClearPass](#)

[Konfiguration der Durchsetzungsrichtlinie für ClearPass-Gastzugriff nach AUP](#)

[Konfiguration des ClearPass MAB-Authentifizierungsdiensts](#)

[Konfiguration des ClearPass-Webauthentifizierungsdiensts](#)

[ClearPass - Webanmeldung](#)

[Verifizierung - CWA-Gastautorisierung](#)

[Anhang](#)

Einleitung

In diesem Dokument wird die Integration des Catalyst 9800 Wireless LAN Controller (WLC) mit Aruba ClearPass zur Bereitstellung von Guest Wireless Service Set Identifier (SSID) beschrieben. Diese Funktion nutzt die zentrale Webauthentifizierung (CWA) für Wireless-Clients im Flexconnect-Modus bei Access Point-Bereitstellungen.

Die Wireless-Gastauthentifizierung wird vom Gastportal mit einer Seite für anonyme akzeptable Benutzerrichtlinien (AUP) unterstützt, die auf Aruba Clearpass in einem DMZ-Segment (Secure Demilitarized Zone) gehostet wird.

Voraussetzungen

In diesem Leitfaden wird davon ausgegangen, dass diese Komponenten konfiguriert und verifiziert wurden:

- Alle relevanten Komponenten werden mit dem Network Time Protocol (NTP) synchronisiert und auf korrekte Uhrzeit überprüft (für die Zertifikatsvalidierung erforderlich).
- Operativer DNS-Server (für Datenverkehrsflüsse von Gästen erforderlich, Validierung der Zertifikatsperrliste (Certificate Revocation List, CRL))
- Betriebs-DHCP-Server
- Eine optionale Zertifizierungsstelle (Certificate Authority, CA) (zum Signieren des vom CPPM gehosteten Gastportals erforderlich)
- Catalyst 9800 WLC
- Aruba ClearPass Server (erfordert Plattformlizenz, Zugriffslizenz, Onboard-Lizenz)
- VMware ESXi

Anforderungen

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

- C9800-Bereitstellung und neues Konfigurationsmodell
- Flexconnect-Switching beim C9800
- 9800 CWA-Authentifizierung (siehe: <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>)

Verwendete Komponenten

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

- Cisco Catalyst C9800-L-C mit 17.3.4c
- Cisco Catalyst Serie C9130AX
- Aruba ClearPass, Patch 6-8-0-109592 und 6.8-3
- MS Windows-Server Active Directory (GP konfiguriert für die automatisierte, computerbasierte

Zertifikatsausgabe an verwaltete Endpunkte)DHCP-Server mit Option 43 und Option 60DNS-ServerNTP-Server zur Zeitsynchronisierung aller KomponentenCA

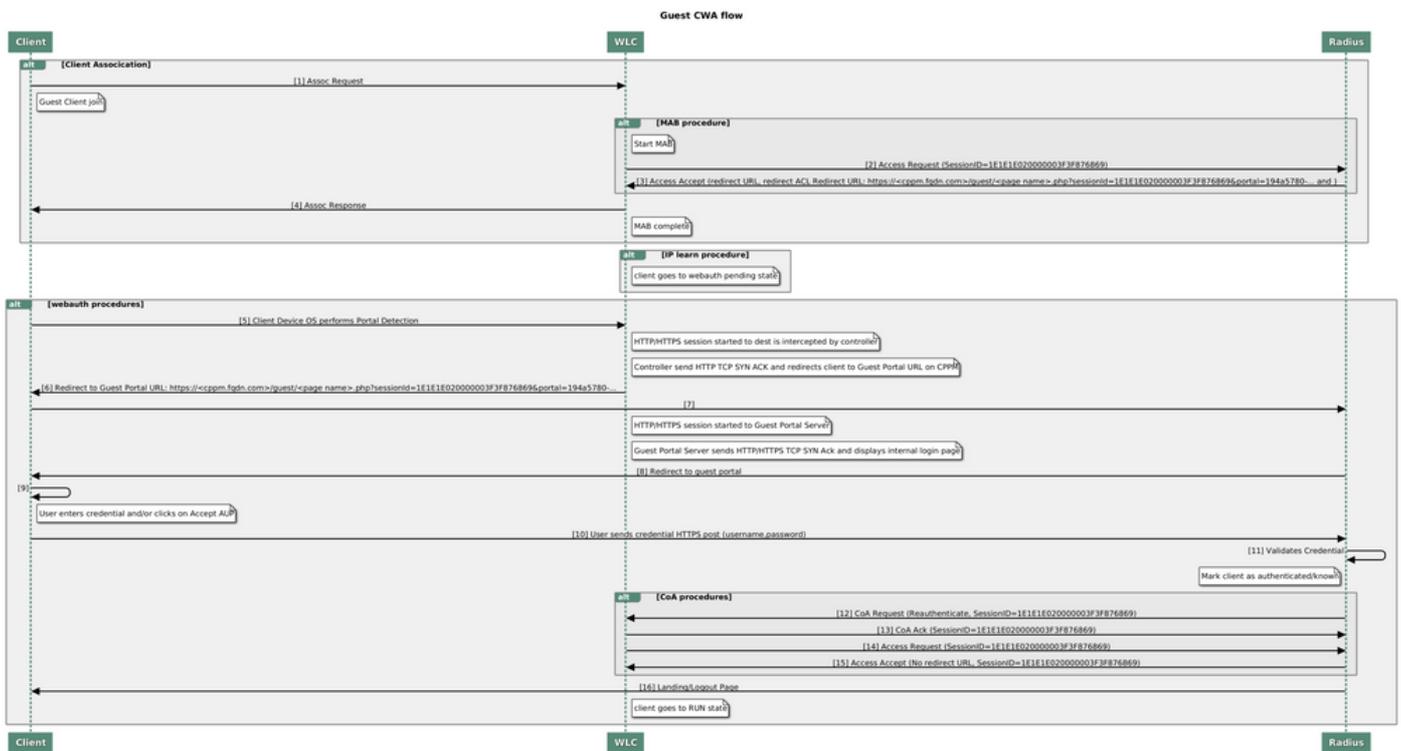
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Das Diagramm zeigt die Einzelheiten des Wi-Fi-Gastzugriffsaustauschs, bevor der Gastbenutzer Zugang zum Netzwerk erhält:

1. Der Gastbenutzer wird dem Gast-Wi-Fi in einer Außenstelle zugewiesen.
2. Die ursprüngliche RADIUS-Zugriffsanforderung wird vom C9800 an den RADIUS-Server weitergeleitet.
3. Der Server sucht die angegebene Gast-MAC-Adresse in der lokalen MAC-Endpunktdatenbank. Wenn die MAC-Adresse nicht gefunden wird, antwortet der Server mit einem MAB-Profil (MAC Authentication Bypass). Diese RADIUS-Antwort umfasst:
 - ACL (URL Redirect Access Control List)
 - URL-Umleitung
4. Der Client durchläuft den IP-Lernprozess, bei dem ihm eine IP-Adresse zugewiesen wird.
5. C9800 setzt den Gastclient (gekennzeichnet durch seine MAC-Adresse) in den Status "Web Auth Pending" (Webauthentifizierung ausstehend) um.
6. Die meisten modernen Geräte-Betriebssysteme in Verbindung mit Gast-WLANs führen eine Art Captive Portal Detection durch.
Der genaue Erkennungsmechanismus hängt von der jeweiligen Betriebssystemimplementierung ab. Das Client-Betriebssystem öffnet ein Popup-Dialogfeld (Pseudo-Browser) mit einer Seite, die von C9800 an die Gastportal-URL umgeleitet wird, die vom RADIUS-Server gehostet wird, der als Teil der RADIUS Access-Accept-Antwort bereitgestellt wird.
7. Der Gastbenutzer akzeptiert die Geschäftsbedingungen des angezeigten Popup-Fensters ClearPass, das die Client-MAC-Adresse in der Endpunktdatenbank (DB) markiert, um anzugeben, dass der Client eine Authentifizierung abgeschlossen hat und eine RADIUS-Autorisierungsänderung (CoA) initiiert, indem eine Schnittstelle auf Basis der Routing-Tabelle ausgewählt wird (wenn auf ClearPass mehrere Schnittstellen vorhanden sind).
8. WLC wechselt den Guest Client in den 'Run'-Status und der Benutzer erhält ohne weitere Umleitungen Zugang zum Internet.

Anmerkung: Das Statusdiagramm des Cisco 9800 Foreign, Anchor Wireless Controller mit RADIUS und dem extern gehosteten Gastportal finden Sie im Anhang dieses Artikels.



Zustandsdiagramm zur Guest Central Web Authentication (CWA)

Datenverkehrsfluss für CWA Guest Enterprise-Bereitstellung

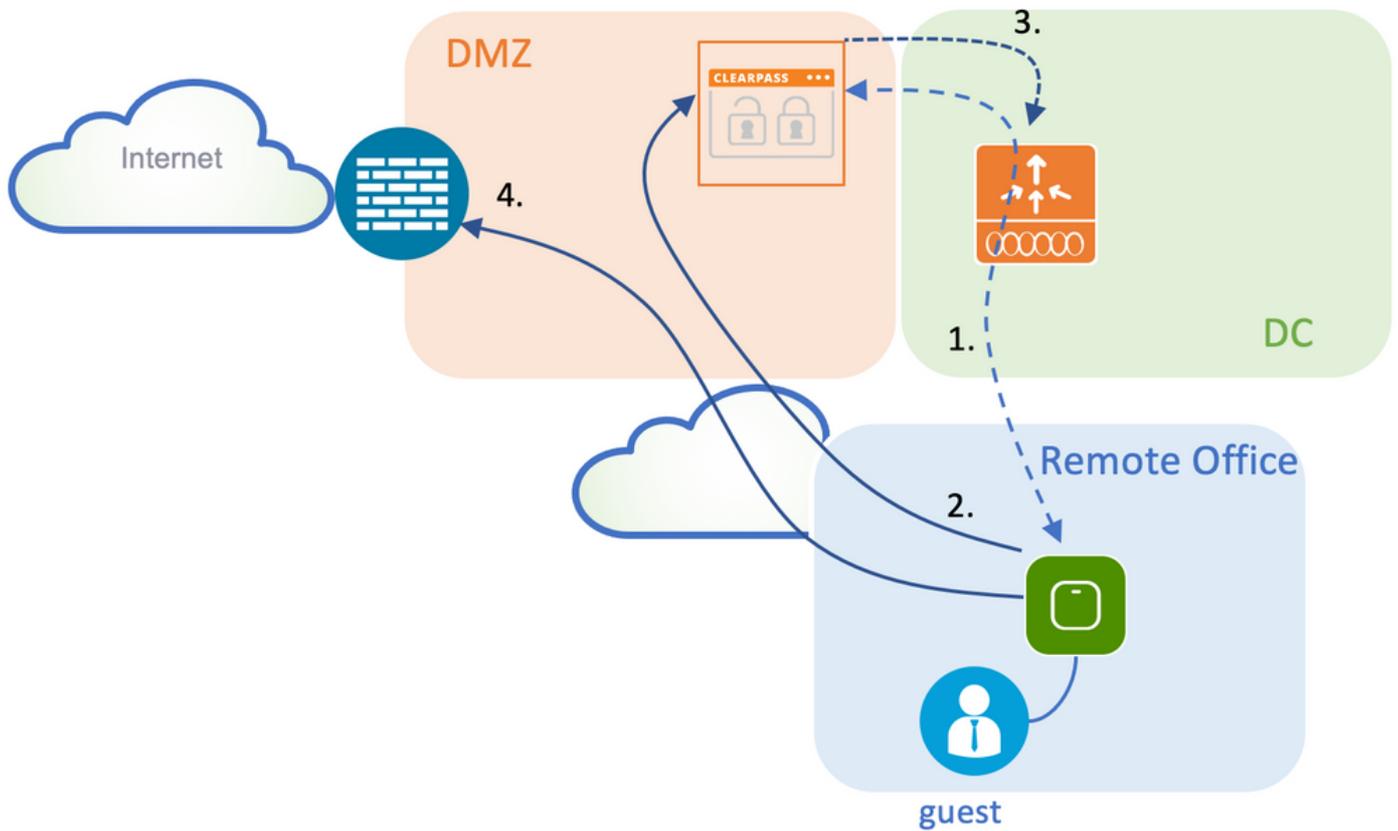
In einer typischen Unternehmensbereitstellung mit mehreren Zweigstellen ist jede Zweigstelle so eingerichtet, dass sie Gästen über ein Gastportal sicheren, segmentierten Zugriff gewährt, sobald der Gast die EULA akzeptiert.

In diesem Konfigurationsbeispiel wird der 9800 CWA für den Gastzugriff über die Integration mit einer separaten ClearPass-Instanz verwendet, die ausschließlich für Gastbenutzer in der sicheren DMZ des Netzwerks bereitgestellt wird.

Die Gäste müssen die Bedingungen akzeptieren, die im Popup-Portal für die Web-Zustimmung des DMZ ClearPass-Servers aufgeführt sind. Dieses Konfigurationsbeispiel konzentriert sich auf die Methode für den anonymen Gastzugriff (d. h., für die Authentifizierung im Gastportal ist kein Gastbenutzername/Kennwort erforderlich).

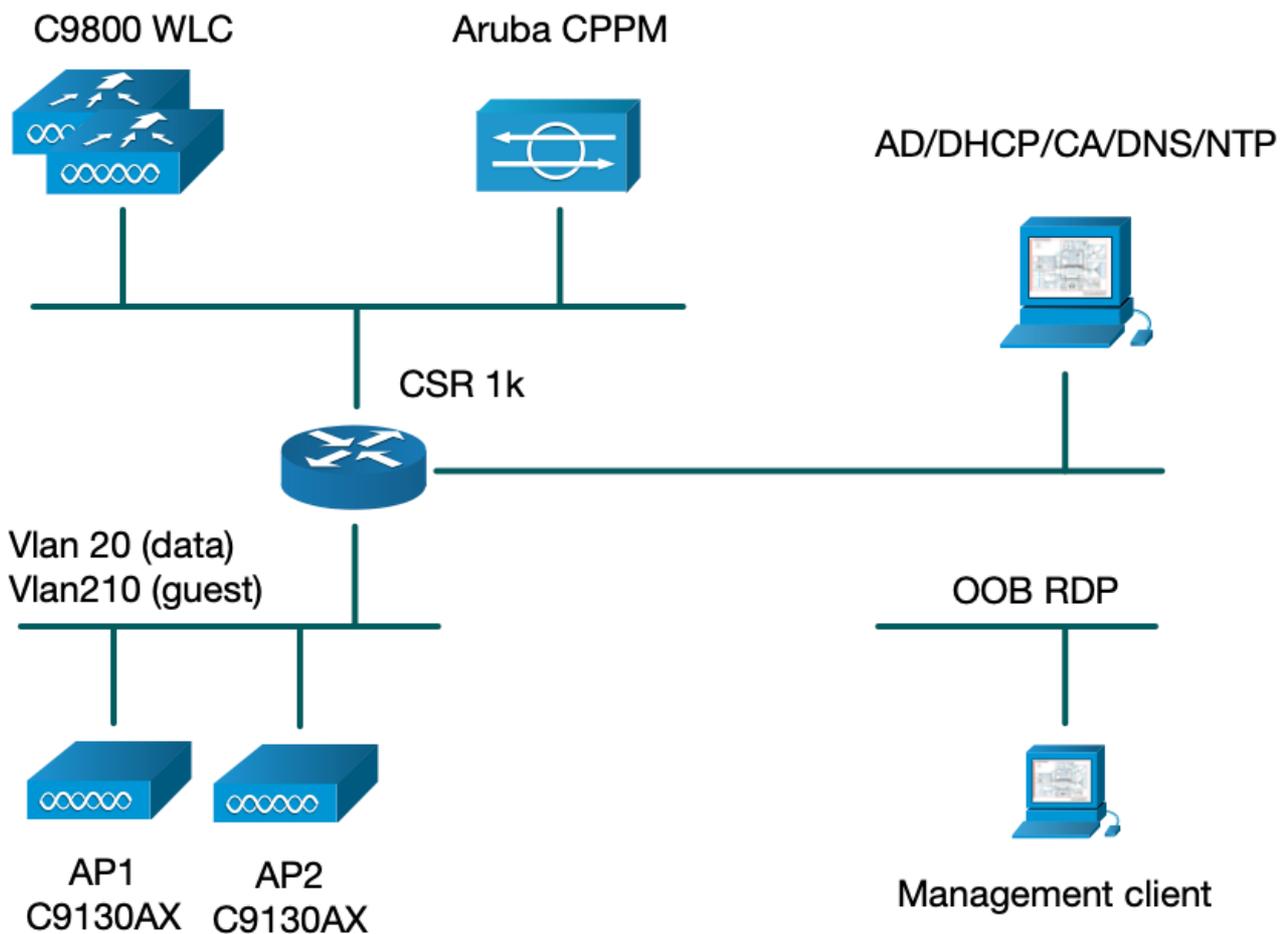
Der Datenverkehrsfluss, der dieser Bereitstellung entspricht, wird im folgenden Image angezeigt:

1. RADIUS - MAB-Phase
2. Gastclient-URL zu Gastportal umleiten
3. Nach der Gastakzeptanz der EULA auf dem Gastportal wird RADIUS CoA Reauthentifizieren von CPPM an 9800 WLC ausgegeben
4. Gastzugriff auf das Internet



Netzwerkdiagramm

Anmerkung: Zu Demonstrationszwecken wird eine einzelne/kombinierte Aruba CPPM Server-Instanz verwendet, um sowohl die Funktionen des Gast- als auch des Unternehmens-SSID-Netzwerkzugriffsservers (NAS) zu bedienen. Eine Best Practice-Implementierung schlägt unabhängige NAS-Instanzen vor.



Konfigurieren

In diesem Konfigurationsbeispiel wird ein neues Konfigurationsmodell auf dem C9800 verwendet, um die erforderlichen Profile und Tags zu erstellen, um dot1x Corporate Access und CWA Guest Access für die Zweigstelle des Unternehmens bereitzustellen. Die resultierende Konfiguration ist in diesem Bild zusammengefasst:

AP
MAC: xxxxx.xxxxx.xxxx

Policy Tag: PT_CAN01

WLAN Profile: WP_Guest
SSID: Guest
Layer 2: Security None
Layer 2: MAC Filtering Enabled
Authz List: AAA_Authz-CPPM

Policy Profile: PP_Guest
Central Switching: Disabled
Central Auth: Enabled
Central DHCP: Disabled
Vlan: guest (21)
AAA Policy: Allow AAA Override Enabled
AAA Policy: NAC State Enabled
AAA Policy: NAC Type RADIUS
AAA Policy Accounting List: Guest_Accounting

Site Tag: ST_CAN01
Enable Local Site: Off

AP Join Profile: MyApProfile
NTP Server: 10.0.10.4

Flex Profile: FP_CAN01
Native Vlan 2
Policy ACL: CAPTIVE_PORTAL_REDIRECT,
ACL CWA: Enabled
VLAN: 21 (Guest)

RF Tag: Branch_RF

5GHz Band RF: Typical_Client_Density_rf_5gh

2GHz Band RF: Typical_Client_Density_rf_2gh

Konfigurieren der C9800-Parameter für den Wireless-Gastzugriff

C9800 - AAA-Konfiguration für Gast

Anmerkung: Informationen zu Cisco Bug-ID [CSCvh03827](https://tools.cisco.com/bugtools/bugsearch/show/CSCvh03827): Stellen Sie sicher, dass die definierten AAA-Server (Authentication, Authorization, and Accounting) keinen Lastenausgleich aufweisen, da der Mechanismus auf der SessionID-Persistenz in WLC- und ClearPass RADIUS-Austauschen beruht.

Schritt 1: Fügen Sie den/die Aruba ClearPass DMZ-Server der 9800 WLC-Konfiguration hinzu, und erstellen Sie eine Liste der Authentifizierungsmethoden. Navigieren Sie zu **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > +Add**, und geben Sie die RADIUS-Serverinformationen ein.

Create AAA Radius Server ✕

Name*	<input type="text" value="CPPM"/>
Server Address*	<input type="text" value="10.85.54.98"/>
PAC Key	<input type="checkbox"/>
Key Type	<input type="text" value="Clear Text"/>
Key* ⓘ	<input type="text" value="....."/>
Confirm Key*	<input type="text" value="....."/>
Auth Port	<input type="text" value="1812"/>
Acct Port	<input type="text" value="1813"/>
Server Timeout (seconds)	<input type="text" value="5"/>
Retry Count	<input type="text" value="3"/>
Support for CoA	<input checked="" type="checkbox"/> ENABLED

Schritt 2: Definieren Sie eine AAA-Servergruppe für Gäste, und weisen Sie den in Schritt 1 konfigurierten Server dieser Servergruppe zu. Navigieren Sie zu **Configuration > Security > AAA > Servers/Groups > RADIUS > Groups > +Add**.

Create AAA Radius Server Group ✕

Name*	<input type="text" value="AAA_Radius_CPPM "/>
Group Type	<input type="text" value="RADIUS"/>
MAC-Delimiter	<input type="text" value="none"/>
MAC-Filtering	<input type="text" value="none"/>
Dead-Time (mins)	<input type="text" value="5"/>
Source Interface VLAN ID	<input type="text" value="1"/>

Available Servers

Assigned Servers



CPPM



Schritt 3: Definieren Sie eine Liste von Autorisierungsmethoden für den Gastzugriff, und ordnen Sie die in Schritt 2 erstellte Servergruppe zu. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung > +Hinzufügen**. Wählen Sie **Network (Netzwerk)** und anschließend **AAA Server Group (AAA-Servergruppe)** aus, die in Schritt 2 konfiguriert wurde.

Quick Setup: AAA Authorization ✕

Method List Name*

Type* network (i)

Group Type (i)

Fallback to local

Authenticated

Available Server Groups Assigned Server Groups

radius ldap tacacs+	> < >> <<	AAA_Radius_CPPM	^ ^ v v
---------------------------	--------------------	-----------------	------------------

Schritt 4: Erstellen Sie eine Liste mit den Abrechnungsmethoden für den Gastzugriff, und ordnen Sie die in Schritt 2 erstellte Servergruppe zu. Navigieren Sie zu **Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Abrechnung > +Hinzufügen**. Wählen Sie im Dropdown-Menü **Type Identity (Identitätstyp)** aus, und konfigurieren Sie dann in Schritt 2 die **AAA-Servergruppe**.

Quick Setup: AAA Accounting ✕

Method List Name*

Type* identity (i)

Available Server Groups Assigned Server Groups

radius ldap tacacs+	> < >> <<	AAA_Radius_CPPM	^ ^ v v
---------------------------	--------------------	-----------------	------------------

Die Umleitungs-ACL legt fest, welcher Datenverkehr zum Gastportal umgeleitet werden muss und welcher Datenverkehr ohne Umleitung weitergeleitet werden darf. In diesem Fall impliziert die ACL-Verweigerung eine Umleitung oder Weiterleitung, während "Zulassen" eine Umleitung zum Portal impliziert. Für jede Datenverkehrsklasse muss die Richtung des Datenverkehrs berücksichtigt werden, wenn Sie Zugriffskontrolleinträge (Access Control Entries, ACEs) erstellen und ACEs erstellen, die sowohl Eingangs- als auch Ausgangsdatenverkehr abgleichen.

Navigieren Sie zu **Configuration > Security > ACL**, und definieren Sie eine neue ACL mit dem Namen **CAPTIVE_PORTAL_REDIRECT**. Konfigurieren Sie die ACL mit diesen ACEs:

- ACE1: Umleitung von bidirektionalem ICMP-Datenverkehr (Internet Control Message Protocol), der hauptsächlich zur Überprüfung der Erreichbarkeit verwendet wird
- ACE10, ACE30: Bidirektionaler DNS-Datenverkehrsfluss zum DNS-Server 10.0.10.4 und keine Umleitung zum Portal Eine DNS-Suche und ein Abfangen der Antwort sind erforderlich, um den Gastdatenfluss auszulösen.
- ACE70, ACE80, ACE110, ACE120: Ermöglicht HTTP- und HTTPS-Zugriff auf das Captive Portal des Gasts, damit der Benutzer das Portal erhält.
- ACE150: Der gesamte HTTP-Datenverkehr (UDP-Port 80) wird umgeleitet.

Sequence ▲	Action ▼	Source IP ▼	Source Wildcard ▼	Destination IP ▼	Destination Wildcard ▼	Protocol ▼	Source Port ▼	Destination Port ▼
1	deny	any		any		icmp		
10	deny	any		10.0.10.4		udp		eq domain
30	deny	10.0.10.4		any		udp	eq domain	
70	deny	any		10.85.54.98		tcp		eq 443
80	deny	10.85.54.98		any		tcp	eq 443	
110	deny	any		10.85.54.98		tcp		eq www
120	deny	10.85.54.98		any		tcp	eq www	
150	permit	any		any		tcp		eq www

C9800 - Konfiguration des Gast-WLAN-Profiles

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > Wireless > +Hinzufügen**. Erstellen Sie ein neues SSID-Profil "WP_Guest", und übertragen Sie die SSID "Guest", der die Gastclients zugeordnet sind.

Add WLAN ✕

General Security Advanced

Profile Name*	<input type="text" value="WP_Guest"/>	Radio Policy	<input type="text" value="All"/>
SSID*	<input type="text" value="Guest"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="3"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Cancel

Apply to Device

Navigieren Sie im selben Dialogfeld **WLAN hinzufügen** zur Registerkarte **Sicherheit > Schicht 2**.

- Layer 2-Sicherheitsmodus: None

- MAC-Filterung: Aktiviert

- Autorisierungsliste: AAA_Authz_CPPM aus dem Dropdown-Menü (konfiguriert unter Schritt 3 als Teil der AAA-Konfiguration)

Add WLAN ✕

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="None"/>	Lobby Admin Access	<input type="checkbox"/>
MAC Filtering	<input checked="" type="checkbox"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
OWE Transition Mode	<input checked="" type="checkbox"/>	Over the DS	<input type="checkbox"/>
Transition Mode WLAN ID*	<input type="text" value="1-4096"/>	Reassociation Timeout	<input type="text" value="20"/>
Authorization List*	<input type="text" value="AAA_Authz_C"/>		

Cancel

Apply to Device

Navigieren Sie in der C9800 WLC-GUI zu **Konfiguration > Tags & Profile > Richtlinie > +Hinzufügen**.

Name: PP_Gast

Status: Aktiviert

Zentrales Switching: Deaktiviert

Zentrale Authentifizierung: Aktiviert

Zentrales DHCP: Deaktiviert

Zentralverband: Deaktiviert

Add Policy Profile ✕

General Access Policies QOS and AVC Mobility Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*

Description

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

WLAN Switching Policy

Central Switching DISABLED

Central Authentication **ENABLED**

Central DHCP DISABLED

Central Association DISABLED

Flex NAT/PAT DISABLED

 Cancel

 Apply to Device

Add Policy Profile

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

PP_Guest

Description

Profile for Branch Guest

Status

DISABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Central Association

DISABLED

Flex NAT/PAT

DISABLED

↶ Cancel

📄 Apply to Device

Navigieren Sie zur Registerkarte **Zugriffsrichtlinien** im selben Dialogfeld **Richtlinienprofil** hinzufügen.

- RADIUS-Profilerstellung: Aktiviert

- VLAN/VLAN-Gruppe: 210 (d. h., VLAN 210 ist das lokale Gast-VLAN in jeder Außenstelle)

Anmerkung: Gast-VLAN für Flex muss auf dem 9800 WLC nicht unter VLANs in der VLAN-/VLAN-Gruppentyp-VLAN-Nummer definiert werden.

Bekannter Fehler: Die Cisco Bug-ID [CSCvn48234](#) bewirkt, dass die SSID nicht übertragen wird, wenn dasselbe Flex-Gast-VLAN unter WLC und im Flex-Profil definiert ist.

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

Search or Select ▼

VLAN

VLAN/VLAN Group

210 ▼

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼

IPv6 ACL

Search or Select ▼

URL Filters

Pre Auth

Search or Select ▼

Post Auth

Search or Select ▼

↶ Cancel

📄 Apply to Device

Navigieren Sie im selben Dialogfeld **Richtlinienprofil hinzufügen** zur Registerkarte **Erweitert**.

- AAA-Außerkraftsetzung zulassen: Aktiviert

- NAC-Staat: Aktiviert

- NAC-Typ: RADIUS

- Abrechnungsliste: AAA_Accounting_CPPM (wird in Schritt 4 als Teil der AAA-Konfiguration definiert)

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

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

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>
Guest LAN Session Timeout	<input type="checkbox"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

Show more >>>

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input checked="" type="checkbox"/>
NAC Type	<input type="text" value="RADIUS"/>
Policy Name	<input type="text" value="default-aaa-policy"/>
Accounting List	<input type="text" value="AAA_Accounting_"/>

Fabric Profile

mDNS Service Policy

Hotspot Server

User Defined (Private) Network

Status

Drop Unicast

Umbrella

Umbrella Parameter Map [Clear](#)

Flex DHCP Option for DNS **ENABLED**

DNS Traffic Redirect **IGNORE**

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL

Air Time Fairness Policies

2.4 GHz Policy

Anmerkung: 'Network Admission Control (NAC) State - Enable' ist erforderlich, damit der C9800 WLC RADIUS-CoA-Nachrichten annehmen kann.

C9800 - Richtlinien-Tag

Navigieren Sie in der C9800-Benutzeroberfläche zu **Konfiguration > Tags & Profile > Tags > Policy > +Add**.

-Name: PT_CAN01

-Beschreibung: Richtlinien-Tag für CAN01-Zweigstelle

Klicken Sie im selben Dialogfeld **Add Policy Tag (Richtlinientag hinzufügen)** unter **WLAN-POLICY MAPS** auf **+Add (Hinzufügen)**, und ordnen Sie das zuvor erstellte WLAN-Profil dem

Richtlinienprofil zu:

- WLAN-Profil: WP_Gast

- Richtlinienprofil: PP_Gast

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
0 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

C9800 - AP-Beitrittsprofil

Navigieren Sie in der C9800 WLC-GUI zu **Konfiguration > Tags & Profile > AP Join > +Add**.

-Name: Außenstellen-AP-Profil

- NTP-Server: 10.0.10.4 (siehe Topologiediagramm der Übungseinheit). Dies ist der NTP-Server, der von den Access Points in der Außenstelle für die Synchronisierung verwendet wird.

General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Name* Description LED State LAG Mode NTP Server GAS AP Rate Limit Apphost

OfficeExtend AP Configuration

Local Access Link Encryption Rogue Detection  Cancel Apply to Device

C9800 - Flex Profile

Die Profile und Tags sind modular und können für mehrere Standorte wiederverwendet werden.

Bei einer FlexConnect-Bereitstellung können Sie dasselbe Flex-Profil wiederverwenden, wenn in allen Zweigstellen dieselben VLAN-IDs verwendet werden.

Schritt 1: Navigieren Sie auf einer C9800 WLC-GUI zu **Configuration > Tags & Profiles > Flex > +Add**.

-Name: FP_Außenstelle

- Native VLAN-ID: 10 (nur erforderlich, wenn Sie über ein natives VLAN verfügen, das nicht der Standardeinstellung entspricht und über eine AP-Verwaltungsschnittstelle verfügen soll)

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

Name* Fallback Radio Shut

Description Flex Resilient

Native VLAN ID ARP Caching

HTTP Proxy Port Efficient Image Upgrade

HTTP-Proxy IP Address OfficeExtend AP

CTS Policy

Inline Tagging Join Minimum Latency

SGACL Enforcement IP Overlap

CTS Profile Name mDNS Flex Profile ▼

Navigieren Sie im selben Dialogfeld **Flex-Profil hinzufügen** zur Registerkarte **Richtlinien-ACL**, und klicken Sie auf **+Hinzufügen**.

- ACL-Name: CAPTIVE_PORTAL_REDIRECT

- Zentrale Webauthentifizierung: Aktiviert

Bei einer Flexconnect-Bereitstellung wird erwartet, dass jeder verwaltete Access Point die Umleitungszugriffskontrollliste lokal herunterlädt, während die Umleitung am Access Point und nicht am C9800 erfolgt.

Add Flex Profile ✕

General Local Authentication Policy ACL VLAN Umbrella

ACL Name	Central Web Auth	Pre Auth URL Filter
◀ ▶ 0 ▶▶ 10 items per page No items to display		

ACL Name* ▼

Central Web Auth

Pre Auth URL Filter ▼

Navigieren Sie im selben Dialogfeld **Add Flex Profile (Flex-Profil hinzufügen)** zur Registerkarte **VLAN**, und klicken Sie auf **+Add** (siehe Topologiediagramm der Übung).

- VLAN-Name: Gast

- VLAN-ID: 210

Add Flex Profile ✕

General Local Authentication Policy ACL **VLAN** Umbrella

+ Add ✕ Delete

VLAN Name	ID	ACL Name
<input type="checkbox"/> data	2	

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

VLAN Name*

VLAN Id*

ACL Name

✓ Save ↶ Cancel

↶ Cancel Apply to Device

C9800 - Site-Tag

Navigieren Sie in der GUI des 9800 WLC zu **Configuration > Tags & Profiles > Tags > Site > Add**.

Anmerkung: Erstellen Sie für jeden Remote-Standort ein eindeutiges Site-Tag, das die beiden Wireless-SSIDs wie beschrieben unterstützt.

Es gibt eine 1-1-Zuordnung zwischen einem geografischen Standort, einer Site-Tag-Nummer und einer Flex Profile-Konfiguration.

Einem Flex Connect-Standort muss ein Flex Connect-Profil zugeordnet sein. Sie können maximal 100 Access Points pro Flex Connect-Standort einrichten.

- Name: ST_CAN01
- Zugangsprofil: Außenstellen-AP-Profil
- Flex Profile: FP_Außenstelle
- Lokalen Standort aktivieren: Deaktiviert

Add Site Tag ✕

Name*

Description

AP Join Profile

Flex Profile

Fabric Control Plane Name

Enable Local Site

↶ Cancel Apply to Device

C9800 - RF-Profil

Navigieren Sie in der GUI des 9800 WLC zu **Configuration > Tags & Profiles > Tags > RF > Add**.

-Name: Zweigstelle_RF

- 5-GHz-Band-Funkfrequenzprofil: Typical_Client_Density_5gh (systemdefinierte Option)

- 2,4-GHz-Band-RF-Profil: Typical_Client_Density_2gh (systemdefinierte Option)

Add RF Tag ✕

Name*	Branch_RF
Description	Typical Branch RF
5 GHz Band RF Profile	Client_Density_rf_5gh ▾
2.4 GHz Band RF Profile	Typical_Client_Densi ▾

↶ Cancel 📄 Apply to Device

C9800 - Zuweisen von Tags zu AP

Es stehen zwei Optionen zur Verfügung, um definierten Tags einzelnen APs in der Bereitstellung zuzuweisen:

- Namensbasierte Zuweisung des Access Points, bei der reguläre Ausdrücke verwendet werden, die mit Mustern im Feld "AP-Name" übereinstimmen (**Konfigurieren > Tags & Profile > Tags > AP > Filter**)

- Adressbasierte Zuweisung von AP-Ethernet-MACs (**Konfigurieren > Tags & Profile > Tags > AP > Statisch**)

In der Produktionsbereitstellung mit DNA Center wird dringend empfohlen, entweder DNAC- und AP PNP-Workflow oder eine statische CSV-Upload-Methode (Comma-Separated Values) zu verwenden, die in 9800 verfügbar ist, um eine manuelle Zuweisung pro AP zu vermeiden. Navigieren Sie zu **Configure > Tags & Profiles > Tags > AP > Static > Add** (Beachten Sie die Option **Upload File**).

- AP-MAC-Adresse: <AP_ETHERNET_MAC>

- Policy-Tag-Name: PT_CAN01

- Site-Tag-Name: ST_CAN01

- RF-Tag-Name: Zweigstelle_RF

Anmerkung: Ab Cisco IOS®-XE 17.3.4c gelten maximal 1.000 reguläre Ausdrücke pro Controller-Begrenzung. Wenn die Anzahl der Standorte in der Bereitstellung diese Anzahl

überschreitet, muss die statische Zuweisung pro MAC genutzt werden.

Associate Tags to AP ✕

AP MAC Address*	aaaa.bbbb.cccc
Policy Tag Name	PT_CAN01
Site Tag Name	ST_CAN01
RF Tag Name	Branch_RF

Cancel

Apply to Device

Anmerkung: Alternativ können Sie zur Verwendung der auf dem AP-Namensregex basierenden Tag-Zuweisungsmethode zu **Configure > Tags & Profiles > Tags > AP > Filter > Add** navigieren.

-Name: BR_CAN01

- AP-Namensregex: BR-CAN01-.(7) (Diese Regel entspricht der AP-Namenskonvention innerhalb der Organisation. In diesem Beispiel werden die Tags APs zugewiesen, die über ein Feld "AP Name" mit dem Zusatz "BR_CAN01-" verfügen, gefolgt von sieben Zeichen.)

-Priorität: 1

- Policy-Tag-Name: PT_CAN01 (wie definiert)

- Site-Tag-Name: ST_CAN01

- RF-Tag-Name: Zweigstelle_RF

Associate Tags to AP ✕

⚠ Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorities.

Rule Name*	BR_CAN01	Policy Tag Name	PT_CAN01	✕	▼
AP name regex*	BR-CAN01-.{7}	Site Tag Name	ST_CAN01	✕	▼
Active	YES	RF Tag Name	Branch_RF	✕	▼
Priority*	1				

Cancel

Apply to Device

Aruba CPPM-Instanz konfigurieren

Wenden Sie sich für produktions-/Best Practices-basierte Aruba CPPM-Konfigurationen an Ihre lokale HPE Aruba SE-Ressource.

Aruba ClearPass Server - Erstkonfiguration

Aruba ClearPass wird mithilfe der OVF-Vorlage (Open Virtualization Format) auf dem ESXi <> - Server bereitgestellt, der die folgenden Ressourcen zuweist:

- Zwei reservierte virtuelle CPUs
- 6 GB RAM
- 80 GB Festplatte (muss manuell nach der anfänglichen VM-Bereitstellung hinzugefügt werden, bevor der Computer eingeschaltet wird)

Lizenzen beantragen

Wenden Sie die Plattformlizenz an über: **Administration > Server Manager > Licensing (Verwaltung > Server-Manager > Lizenzierung)**. Hinzufügen von **Plattform-, Zugangs- und Onboard-Lizenzen**.

Hostname des Servers

Navigieren Sie zu **Administration > Server Manager > Server Configuration**, und wählen Sie den neu bereitgestellten CPPM-Server aus.

- Hostname: Cppm

- FQDN: cppm.example.com

- Überprüfen der IP-Adressierung und des DNS des Management-Ports

Server Configuration - cppm (10.85.54.98)

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	cppm				
FQDN:	cppm.example.com				
Policy Manager Zone:	default				Manage F
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight <input checked="" type="checkbox"/> Enable as Insight Master Current Master:cppm(10.85.54.98)				
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Master Server in Zone:	Primary master				
Span Port:	-- None --				
		IPv4		IPv6	Action
Management Port	IP Address	10.85.54.98			Configure
	Subnet Mask	255.255.255.224			
	Default Gateway	10.85.54.97			
Data/External Port	IP Address				Configure
	Subnet Mask				
	Default Gateway				
DNS Settings	Primary	10.85.54.122			Configure
	Secondary				
	Tertiary				
	DNS Caching	Disabled			

CPPM-Webserverzertifikat (HTTPS) generieren

Dieses Zertifikat wird verwendet, wenn die Seite des ClearPass-Gastportals über HTTPS für Gastclients angezeigt wird, die eine Verbindung mit dem Gast-Wi-Fi in der Außenstelle herstellen.

Schritt 1: Laden Sie das CA Pub Chain-Zertifikat hoch.

Navigieren Sie zu **Administration > Certificates > Trust List > Add**.

- Verwendung: Andere aktivieren

View Certificate Details	
Subject DN:	
Issuer DN:	
Issue Date/Time:	Dec 23, 2020 16:55:10 EST
Expiry Date/Time:	Dec 24, 2025 17:05:10 EST
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	86452691282006080280068723651711271611
Enabled:	true
Usage:	<input checked="" type="checkbox"/> EAP <input checked="" type="checkbox"/> RadSec <input checked="" type="checkbox"/> Database <input checked="" type="checkbox"/> Others
<input type="button" value="Update"/> <input type="button" value="Disable"/> <input type="button" value="Export"/> <input type="button" value="Close"/>	

Schritt 2: Erstellen einer Zertifikatsignierungsanforderung

Navigieren Sie zu **Administration > Certificates > Certificate Store > Server Certificates > Usage: HTTPS-Serverzertifikat**.

- Klicken Sie auf die **Anforderung zum Erstellen einer Zertifikatssignatur**.
- Allgemeine Bezeichnung: CPPM
- Organisation: **cppm.example.com**

Stellen Sie sicher, dass das SAN-Feld ausgefüllt wird (in SAN sowie IP und anderen FQDNs muss nach Bedarf ein gemeinsamer Name angegeben werden). Format ist DNS: **<fqdn1>,DNS:<fqdn2>,IP<ip1>**.

Create Certificate Signing Request

Common Name (CN):	cppm
Organization (O):	Cisco
Organizational Unit (OU):	Engineering
Location (L):	Toronto
State (ST):	ON
Country (C):	CA
Subject Alternate Name (SAN):	DNS:cppm.example.com
Private Key Password:
Verify Private Key Password:
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512

Submit **Cancel**

Schritt 3: Signieren Sie in der ausgewählten Zertifizierungsstelle die neu generierte CSR für den CPPM HTTPS-Service.

Schritt 4: Navigieren Sie zu **Zertifikatvorlage > Webserver > Zertifikat importieren**.

- Zertifikatstyp: Serverzertifikat

- Verwendung: HTTP-Serverzertifikat

- Zertifikatsdatei: Durchsuchen und CA-signiertes CPPM HTTPS-Service-Zertifikat auswählen

Import Certificate

Certificate Type:	Server Certificate
Server:	cppm
Usage:	HTTPS Server Certificate
Upload Method:	Upload Certificate and Use Saved Private Key
Certificate File:	Browse... No file selected.

Import **Cancel**

Definieren des C9800 WLC als Netzwerkgerät

Navigieren Sie zu **Konfiguration > Netzwerk > Geräte > Hinzufügen**.

-Name: WLC_9800 Zweigstelle

- IP- oder Subnetzadresse: 10.85.54.99 (siehe Topologiediagramm der Übungseinheit)

- RADIUS Shared Cisco: <WLC RADIUS-Kennwort>

- Name des Anbieters: Cisco

- Aktivieren Sie die dynamische RADIUS-Autorisierung: 1700

Device	SNMP Read Settings	SNMP Write Settings	CLI Settings	OnConnect Enforcement	Attributes
Name:	WLC_9800_Branch				
IP or Subnet Address:	10.85.54.99 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)				
Description:	Cisco 9800 WLC for Branch Guest Wifi				
RADIUS Shared Secret:		Verify:	
TACACS+ Shared Secret:			Verify:		
Vendor Name:	Cisco				
Enable RADIUS Dynamic Authorization:	<input checked="" type="checkbox"/> Port: 1700				
Enable RadSec:	<input type="checkbox"/>				

Add **Cancel**

Gastportalseite und CoA-Timer

Es ist sehr wichtig, während der gesamten Konfiguration die richtigen Timer-Werte einzustellen. Wenn die Timer nicht eingestellt sind, werden Sie wahrscheinlich auf eine zyklische Webportal-Umleitung stoßen, bei der sich der Client nicht im Ausführungszustand befindet.

Zeitgeber für:

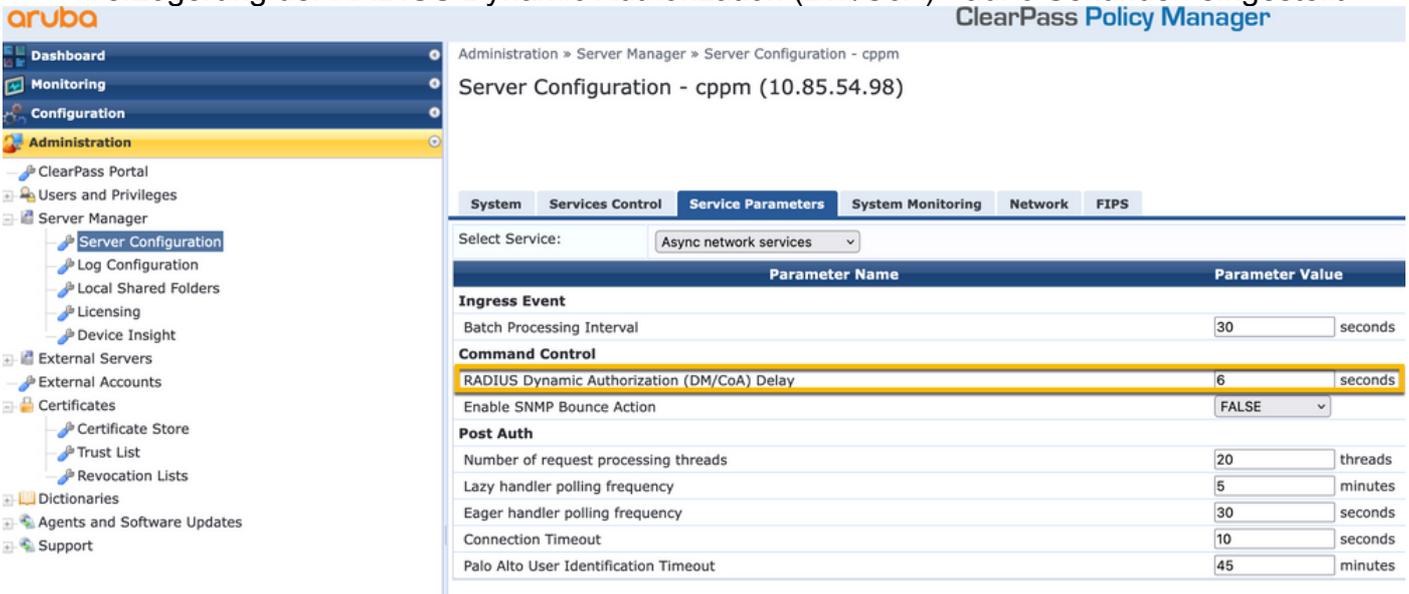
- Portal Web Login timer: Dieser Timer verzögert die Weiterleitungsseite, bevor der Zugriff auf die Gastportalseite möglich ist, um den CPPM-Dienst über den Statusübergang zu informieren, das benutzerdefinierte Endpoint-Attribut "Allow-Guest-Internet" zu registrieren und den CoA-Prozess von CPPM zu WLC auszulösen. Navigieren Sie zu **Gast > Konfiguration > Seiten > Webanmeldungen**.
 - Name des Gastportals auswählen: Registrierung anonymer Gäste im Labor (die Konfiguration dieser Seite für das Gastportal wird wie dargestellt detailliert dargestellt)
 - Klicken Sie auf **Bearbeiten**
 - Anmeldeverzögerung: 6 Sekunden

* Login Delay: 6
The time in seconds to delay while displaying the login message.

- ClearPass CoA-Verzögerungszeitgeber: Dadurch wird die Generierung von CoA-Nachrichten von ClearPass an den WLC verzögert. Dies ist erforderlich, damit CPPM den Status des Client-Endpunkts intern erfolgreich ändern kann, bevor die CoA-Bestätigung (ACK) vom WLC zurückkommt. Labortests zeigen die Antwortzeiten von WLC in Millisekunden. Wenn CPPM

die Aktualisierung der Endpunktattribute nicht abgeschlossen hat, wird die neue RADIUS-Sitzung von WLC mit der Durchsetzungsrichtlinie für den nicht authentifizierten MAB-Dienst abgeglichen, und der Client erhält erneut eine Umleitungsseite. Navigieren Sie zu **CPPM > Administration > Server Manager > Server Configuration**, und wählen Sie **CPPM Server > Service Parameters**.

- Verzögerung der RADIUS Dynamic Authorization (DM/CoA) - auf 6 Sekunden eingestellt



ClearPass - Gast-CWA-Konfiguration

Die ClearPass-seitige CWA-Konfiguration besteht aus (3) Servicepunkten/Phasen:

ClearPass-Komponente	Servicetyp	Zweck
1. Richtlinien-Manager	Dienst: Mac-Authentifizierung	Wenn das benutzerdefinierte Attribut Allow-Guest-Internet = TRUE lautet, lassen Sie es im Netzwerk zu. Triggern Sie andernfalls Redirect und COA: Erneut authentifizieren . Anonyme Login-AUP-Seite präsentieren.
2. Gast	Web-Anmeldungen	Nach der Authentifizierung legen Sie das benutzerdefinierte Attribut Allow-Guest-Internet = TRUE fest. Legen Sie das benutzerdefinierte Attribut Allow-Guest-Internet = TRUE fest. Legen Sie das benutzerdefinierte Attribut Allow-Guest-Internet = TRUE fest. Kakao: Erneute Authentifizierung
3. Richtlinien-Manager	Dienst: Webbasierte Authentifizierung	

Metadatenattribut für ClearPass-Endpoint: Gast-Internet zulassen

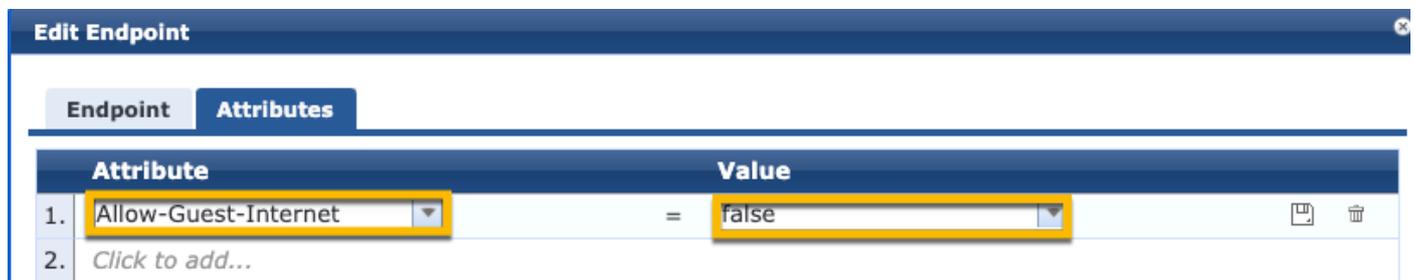
Erstellen Sie ein Metadatenattribut vom Typ Boolean, um den Zustand des Gastendpunkts zu verfolgen, während der Client zwischen dem Zustand 'Webauth Pending' und dem Zustand 'Run' wechselt:

- Für neue Gäste, die eine Wi-Fi-Verbindung herstellen, ist das Metadaten-Standardattribut Allow-Guest-Internet=false festgelegt. Basierend auf diesem Attribut durchläuft die Client-Authentifizierung den MAB-Dienst.

- Wenn Sie auf die Schaltfläche "AUP Accept" (AUP akzeptieren) klicken, wird das Metadatenattribut des Gastclients auf Allow-Guest-Internet=true aktualisiert. Nachfolgende MAB-Datei, die auf diesem Attribut auf True festgelegt ist, ermöglicht den nicht umgeleiteten Zugriff auf das Internet.

Navigieren Sie zu ClearPass > Configuration > Endpoints, wählen Sie einen beliebigen Endpunkt aus der Liste aus, klicken Sie auf die Registerkarte **Attributes**, fügen Sie **Allow-Guest-Internet** mit dem Wert **false** und **Save** hinzu.

Anmerkung: Sie können denselben Endpunkt bearbeiten und dieses Attribut direkt danach löschen. In diesem Schritt wird lediglich ein Feld in der Endpunktmetadaten-Datenbank erstellt, das in Richtlinien verwendet werden kann.



Edit Endpoint	
Attributes	
Attribute	Value
1. Allow-Guest-Internet	= false
2. Click to add...	

Konfiguration der ClearPass-Richtlinie zur erneuten Authentifizierung

Erstellen Sie ein Durchsetzungsprofil, das dem Gast-Client zugewiesen wird, sobald der Client auf der Seite des Gastportals AUP akzeptiert.

Navigieren Sie zu **ClearPass > Configuration > Profiles > Add**.

- Vorlage: RADIUS - dynamische Autorisierung

-Name: Cisco_WLC_Gast_COA

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Dynamic Authorization	
Name:	Cisco_WLC_Guest_COA	
Description:		
Type:	RADIUS_CoA	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="text"/> --Select--	Remove View Details Modify

Radius:IETF	Anrufende Station-ID	%{Radius:IETF:Calling-Station
Radius:Cisco	Cisco AVPair	Subscriber:command=reautheren
Radius:Cisco	Cisco AVPair	%{Radius:Cisco:Cisco-AVPair:Subscriber:Audit-SessiID}
Radius:Cisco	Cisco AVPair	Teilnehmer:reAuthenticate-type=last-type=last

Konfiguration des Durchsetzungsprofils für die ClearPass-Gastportal-Umleitung

Erstellen Sie ein Durchsetzungsprofil, das in der anfänglichen MAB-Phase auf Guest angewendet wird, wenn die MAC-Adresse in der CPPM-Endpunktdatenbank nicht gefunden wird und Allow-Guest-Internet auf "true" festgelegt ist.

Dies veranlasst den 9800 WLC, den Guest Client zur externen Authentifizierung an das CPPM-Gastportal umzuleiten.

Navigieren Sie zu **ClearPass > Enforcement > Profiles > Add**.

-Name: Cisco_Portal_Weiterleitung

-Typ: RADIUS

-Aktion: Akzeptieren

Enforcement Profiles

Profile	Attributes	Summary
Template:	Aruba RADIUS Enforcement	
Name:	Cisco_Portal_Redirect	
Description:		
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:		Remove View Details Modify
	--Select--	

Durchsetzungsprofil für ClearPass-Umleitung

Konfigurieren Sie im selben Dialog auf der Registerkarte **Attribute** zwei Attribute gemäß diesem Bild:

Enforcement Profiles - Cisco_Portal_Redirect

Summary	Profile	Attributes
Type	Name	Value
1. Radius:Cisco	Cisco-AVPair	= url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
2. Radius:Cisco	Cisco-AVPair	= url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=%{Radius:IETF:NAS-IP-Address}

ClearPass-Umleitungsprofilattribute

Das Attribut **url-redirect-acl** wird auf **CAPTIVE-PORTAL-REDIRECT** festgelegt, d. h. auf den Namen der auf C9800 erstellten ACL.

Anmerkung: In der RADIUS-Meldung wird nur der Verweis auf die ACL übergeben, nicht der ACL-Inhalt. Es ist wichtig, dass der Name der auf dem 9800 WLC erstellten ACL genau dem Wert dieses RADIUS-Attributs entspricht, wie dargestellt.

Das **url-redirect**-Attribut besteht aus mehreren Parametern:

- Die Ziel-URL, unter der das Gastportal gehostet wird:
<https://cppm.example.com/guest/iaccept.php>
- **Gast-Client-MAC**, Makro %{Connection:Client-Mac-Address-Hyphen}
- **Authentikator-IP** (9800 WLC löst die Umleitung aus), Makro %{Radius:IETF:NAS-IP-Adresse}
- **cmd-login**-Aktion

Die URL der ClearPass Guest Web-Anmeldeseite wird angezeigt, wenn Sie zu **CPPM > Gast > Konfiguration > Seiten > Web-Anmeldungen > Bearbeiten** navigieren.

In diesem Beispiel wird der Seitenname des Gastportals in CPPM als **iaccept** definiert.

Anmerkung: Die Konfigurationsschritte für die Seite "Guest Portal" werden wie beschrieben ausgeführt.

The screenshot shows the Aruba configuration interface. On the left is a navigation menu with categories: Guest, Devices, Onboard, Configuration (highlighted), Authentication, Content Manager, Guest Manager, Hotspot Manager, Pages (expanded to show Fields, Forms, List Views, Self-Registrations, Web Logins, and Web Pages), and Web Pages. The main content area shows the breadcrumb path: Home » Configuration » Pages » Web Logins. The title is "Web Login (Lab Anonymous Guest Regist)". Below the title is a note: "Use this form to make changes to the Web Login **Lab Anon**". The form contains the following fields: * Name: "Lab Anonymous Guest Registration" (with a hint "Enter a name for this web login page."); Page Name: "iaccept" (with a hint "Enter a page name for this web login. The web login will be accessible from "/guest/"); Description: (empty, with a hint "Comments or descriptive text about the web l"); * Vendor Settings: "Aruba Networks" (with a hint "Select a predefined group of settings suitable").

Anmerkung: Für Cisco Geräte wird normalerweise `audit_session_id` verwendet, was jedoch von anderen Anbietern nicht unterstützt wird.

Konfiguration des Durchsetzungsprofils für ClearPass-Metadaten

Konfigurieren Sie das Durchsetzungsprofil, um das Metadatenattribut des Endpunkts zu aktualisieren, das für die Statusübergangsverfolgung durch CPPM verwendet wird.

Dieses Profil wird auf den Eintrag "Guest Client MAC Address" in der Endpunktdatenbank angewendet und setzt das Argument "**Allow-Guest-Internet**" auf "**true**".

Navigieren Sie zu **ClearPass > Enforcement > Profiles > Add**.

- Vorlage: Durchsetzung der ClearPass-Entitätsaktualisierung

-Typ: Nachauthentifizierung

Enforcement Profiles

Profile	Attributes	Summary
Template:	ClearPass Entity Update Enforcement	
Name:	Make-Cisco-Guest-Valid	
Description:		
Type:	Post_Authentication	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="display: flex; justify-content: flex-end; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Remove</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">View Details</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">Modify</div> </div>	

Im selben Dialog befindet sich die Registerkarte **Attribute**.

-Typ: Endpunkt

-Name: Gast-Internet zulassen

Anmerkung: Damit dieser Name im Dropdown-Menü angezeigt wird, müssen Sie dieses Feld für mindestens einen Endpunkt manuell definieren, wie unter Schritte beschrieben.

-Wert: wahr

Enforcement Profiles

Profile	Attributes	Summary
Type	Name	Value
1. Endpoint	Allow-Guest-Internet	= true
2. <i>Click to add...</i>		

Richtlinienkonfiguration für die Durchsetzungsrichtlinie für den Gastzugriff mit ClearPass

Navigieren Sie zu **ClearPass > Enforcement > Policies > Add**.

-Name: WLC Cisco Gastzugriff

- Durchsetzungstyp: RADIUS

- Standardprofil: Cisco_Portal_Weiterleitung

Enforcement Policies

Enforcement Rules Summary

Name:

Description:

Enforcement Type: RADIUS TACACS+ WEBAUTH (SNMP/Agent/CLI/CoA) Application Event

Default Profile:

Navigieren Sie im selben Dialogfeld zur Registerkarte **Regeln**, und klicken Sie auf **Regel hinzufügen**.

-Typ: Endpunkt

-Name: Gast-Internet zulassen

- Betreiber: GLEICH

- Wert True

- Profilnamen/Hinzuzufügende Auswahl: [RADIUS] [Zugriffsprofil zulassen]

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Endpoint	Allow-Guest-Internet	EQUALS	true
2.	Click to add...		

Enforcement Profiles

Profile Names:

--Select to Add--

Konfiguration der Durchsetzungsrichtlinie für ClearPass-Gastzugriff nach AUP

Navigieren Sie zu **ClearPass > Enforcement > Policies > Add**.

-Name: Cisco WLC-Webauthentifizierungs-Durchsetzungsrichtlinie

- Durchsetzungstyp: WEBAUTH (SNMP/Agent/CLI/CoA)

- Standardprofil: [RADIUS_CoA] Cisco_Reauthentifizierung_Sitzung

Enforcement Policies

Enforcement	Rules	Summary
Name:	Cisco WLC Webauth Enforcement Policy	
Description:		
Enforcement Type:	<input type="radio"/> RADIUS <input type="radio"/> TACACS+ <input checked="" type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	
Default Profile:	[RADIUS_CoA] Cisco_Reauth v	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

Navigieren Sie im selben Dialogfeld zu **Regeln > Hinzufügen**.

- Voraussetzungen: Authentifizierung

-Name: Status

- Betreiber: GLEICH

-Wert: Benutzer

- Profilnamen: <jeweils hinzufügen>:

- [Nach Authentifizierung] [Endpunkt aktualisieren bekannt]

- [Nach der Authentifizierung] [Make-Cisco-Guest-Valid]

- [RADIUS_CoA] [Cisco_WLC_Guest_COA]

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Authentication	Status	EQUALS	User
2.	Click to add...		

Enforcement Profiles

Profile Names:	[Post Authentication] [Update Endpoint Known] [Post Authentication] Make-Cisco-Guest-Valid [RADIUS_CoA] Cisco_WLC_Guest_COA	<input type="button" value="Move Up ↑"/> <input type="button" value="Move Down ↓"/> <input type="button" value="Remove"/>
	<input type="text" value="--Select to Add--"/>	

Anmerkung: Wenn ein Szenario mit einem ständigen Pseudo-Browser-Popup für die Umleitung durch das Gastportal auftritt, ist dies ein Hinweis darauf, dass entweder die CPPM-Timer angepasst werden müssen oder dass die RADIUS-CoA-Nachrichten nicht ordnungsgemäß zwischen CPPM und dem 9800 WLC ausgetauscht werden. Überprüfen Sie diese Standorte.

- Navigieren Sie zu **CPPM > Monitoring > Live Monitoring > Access Tracker**, und stellen Sie sicher, dass der RADIUS-Protokolleintrag RADIUS-CoA-Details enthält.

- Navigieren Sie auf **9800 WLC** zu **Troubleshooting > Packet Capture**, aktivieren Sie pcap auf der

Schnittstelle, an der das Eintreffen der RADIUS CoA-Pakete erwartet wird, und überprüfen Sie, ob RADIUS CoA-Nachrichten vom CPPM empfangen werden.

Konfiguration des ClearPass MAB-Authentifizierungsdiensts

Der Dienst wird auf dem AV-Paar Radius abgeglichen: Cisco | CiscoAVPair | cisco-wlan-ssid

Navigieren Sie zu **ClearPass > Configuration > Services > Add**.

Registerkarte "**Service**":

-Name: GuestPortal - Mac-Authentifizierung

-Typ: MAC-Authentifizierung

- Weitere Optionen: Autorisierung auswählen, Endgeräte profilieren

Zuordnungsregel hinzufügen:

-Typ: RADIUS: Cisco

-Name: Cisco AVPair

- Betreiber: GLEICH

-Wert: cisco-wlan-ssid=Guest (Übereinstimmung mit konfiguriertem Gast-SSID-Namen)

Anmerkung: "Guest" ist der Name der vom 9800 WLC übertragenen Guest-SSID.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement Profiler Summary

Type:

Name:

Description:

Monitor Mode: Enable to monitor network access without enforcement

More Options: Authorization Audit End-hosts Profile Endpoints Accounting Proxy

Service Rule

Matches ANY or ALL of the following conditions:

	Type	Name	Operator	Value		
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)		
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)		
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}		
4.	Radius:Cisco	Cisco-AVPair	EQUALS	cisco-wlan-ssid=Guest		

Wählen Sie im selben Dialogfeld die Registerkarte **Authentifizierung**.

- Authentifizierungsmethoden: [MAC AUTH] entfernen, [Alle MAC AUTH zulassen] hinzufügen

- Authentifizierungsquellen: [Endpunkte-Repository][Lokale SQL-Datenbank], [Gast-Benutzer-Repository][Lokale SQL-Datenbank]

aruba ClearPass Policy Manager

Configuration » Services » Edit - GuestPortal - Mac Auth

Services - GuestPortal - Mac Auth

Summary Service **Authentication** Authorization Roles Enforcement Profiler

Authentication Methods: [Allow All MAC AUTH]

Authentication Sources: [Endpoints Repository] [Local SQL DB] [Guest User Repository] [Local SQL DB]

Strip Username Rules: Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

Wählen Sie im selben Dialogfeld die Registerkarte **Durchsetzung**.

- Durchsetzungsrichtlinie: WLC Cisco Gastzugriff

Configuration » Services » Add

Services

Service Authentication Roles **Enforcement** Summary

Use Cached Results: Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: WLC Cisco Guest Allow **Modify**

Enforcement Policy Details

Description:	MAB Enforcement Redirect
Default Profile:	Cisco_Portal_Redirect
Rules Evaluation Algorithm:	first-applicable

Conditions	Enforcement Profiles
1. (Endpoint:Allow-Guest-Internet EQUALS true)	[Allow Access Profile]

Wählen Sie im selben Dialogfeld die Registerkarte **Durchsetzung**.

Configuration » Services » Add

Services

Service Authentication Authorization Roles Enforcement **Profiler** Summary

Endpoint Classification: Select the classification(s) after which an action must be triggered -

RADIUS CoA Action: Cisco_Reauthenticate_Session **View Details** **Modify**

Konfiguration des ClearPass-Webauthentifizierungsdiensts

Navigieren Sie zu **ClearPass > Enforcement > Policies > Add**.

-Name: Gast_Portal_Webauth

-Typ: Webbasierte Authentifizierung

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Type:	Web-based Authentication			
Name:	Guest			
Description:				
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance			
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name			
1.	Host	CheckType		
2.	Click to add...			

Im selben Dialogfeld wird auf der Registerkarte "Durchsetzung" die Richtlinie: Cisco WLC-Webauthentifizierungs-Durchsetzungsrichtlinie

Configuration » Services » Add

Services

Service	Authentication	Roles	Enforcement	Summary
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	Cisco WLC Webauth Enforcement Policy Modify			Add New Enforcement Poli
Enforcement Policy Details				
Description:				
Default Profile:	Cisco_Reauthenticate_Session			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authentication:Status EQUALS User)	[Update Endpoint Known], Make-Cisco-Guest-Valid, Cisco_Reauthenticate_Session			

ClearPass - Webanmeldung

Verwenden Sie für die Seite "Anonymous AUP Guest Portal" einen einzigen Benutzernamen ohne Kennwortfeld.

Für den verwendeten Benutzernamen müssen die folgenden Felder definiert/festgelegt sein:

Benutzername_Authentifizierung | Benutzername-Authentifizierung: | 1

Um das Feld 'username_auth' für einen Benutzer festzulegen, muss dieses Feld zuerst im Formular 'Benutzer bearbeiten' verfügbar gemacht werden. Navigieren Sie zu **ClearPass > Guest > Configuration > Pages > Forms**, und wählen Sie **create_user** form aus.

The screenshot shows the Aruba ClearPass Guest web interface. The left sidebar contains a navigation menu with 'Forms' highlighted. The main content area shows the breadcrumb 'Home » Configuration » Pages » Forms' and the title 'Customize Forms'. Below this is a list of form templates with columns for 'Name' and 'Title'. The 'create_user' form is selected and highlighted.

Name	Title
change_expiration Change the expiration time of a single guest account.	Change Expiration
create_multi Create multiple guest accounts.	Create Multiple Guest Accounts
create_multi_result Create multiple accounts results page.	Create Multiple Accounts Results
create_user * Create a single guest account.	Create New Guest Account
create_user_receipt Create single guest account receipt.	Create New Guest Account Receipt
guest_edit	

Wählen Sie **visitor_name** (Zeile 20) aus, und klicken Sie auf **Einfügen nach**.

Home » Configuration » Pages » Forms

Customize Form Fields (create_user)

Use this list view to modify the fields of the form **create_user**.

The screenshot shows the 'Customize Form Fields' interface for the 'create_user' form. It features a table with columns for 'Rank', 'Field', 'Type', 'Label', and 'Description'. The 'visitor_name' field (Rank 20) is selected. Below the table are several action buttons, with 'Insert After' highlighted.

Rank	Field	Type	Label	Description
1	enabled	dropdown	Account Status:	Select an option for changing the status of this account.
10	sponsor_name	text	Sponsor's Name:	Name of the person sponsoring this account.
13	sponsor_profile_name	text	Sponsor's Profile:	Profile of the person sponsoring this account.
15	sponsor_email	text	Sponsor's Email:	Email of the person sponsoring this account.
20	visitor_name	text	Guest's Name:	Name of the guest.

Buttons: Edit, Edit Base Field, Remove, **Insert Before**, **Insert After**, Disable Field

Customize Form Field (new)

Use this form to add a new field to the form **create_user**.

Form Field Editor	
* Field Name:	<input type="text" value="username_auth"/> <small>Select the field definition to attach to the form.</small>
Form Display Properties <small>These properties control the user interface displayed for this field.</small>	
Field:	<input checked="" type="checkbox"/> Enable this field <small>When checked, the field will be included as part of the form.</small>
* Rank:	<input type="text" value="22"/> <small>Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.</small>
* User Interface:	<input type="text" value="No user interface"/> <input type="button" value="Revert"/> <small>The kind of user interface element to use when entering or editing this field.</small>
Form Validation Properties <small>These properties control how the value of this field is checked.</small>	
Field Required:	<input type="checkbox"/> Field value must be supplied <small>Select this option if the field cannot be omitted or left blank.</small>
Initial Value:	<input type="text" value="1"/> <input type="button" value="Revert"/> <small>Value to initialize this field with when the form is first displayed.</small>
* Validator:	<input type="text" value="IsValidBool"/> <small>The function used to validate the contents of a field.</small>
Validator Param:	<input type="text" value="(None)"/> <small>Optional name of field whose value will be supplied as the argument to a validator.</small>
Validator Argument:	<input type="text"/> <small>Optional value to supply as the argument to a validator.</small>
Validation Error:	<input type="text"/> <small>The error message to display if the field's value fails validation and the validator does not return an error message directly.</small>

Erstellen Sie nun den Benutzernamen, der hinter der Seite des AUP-Gastportals verwendet werden soll.

Navigieren Sie zu **CPPM > Gast > Gast > Konten verwalten > Erstellen**.

- Gastname: GastWiFi
- Name des Unternehmens: Cisco
- E-Mail-Adresse: guest@example.com
- Benutzername-Authentifizierung: Gastzugriff nur unter Verwendung des Benutzernamens erlauben: Aktiviert
- Kontoaktivierung: Jetzt
- Kontoablauf: Das Konto läuft nicht ab.
- Nutzungsbedingungen: Ich bin der Sponsor: Aktiviert

Create Guest Account

New guest account being created by **admin**.

Create New Guest Account	
* Guest's Name:	<input type="text" value="GuestWiFi"/> Name of the guest.
* Company Name:	<input type="text" value="Cisco"/> Company name of the guest.
* Email Address:	<input type="text" value="guest@example.com"/> The guest's email address. This will become their username to log into the network.
Username Authentication:	<input checked="" type="checkbox"/> Allow guest access using their username only Guests will require the login screen setup for username-based authentication as well.
Account Activation:	<input type="text" value="Now"/> Select an option for changing the activation time of this account.
Account Expiration:	<input type="text" value="Account will not expire"/> Select an option for changing the expiration time of this account.
* Account Role:	<input type="text" value="[Guest]"/> Role to assign to this account.
Password:	281355
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the terms of use
<input type="button" value="Create"/>	

Web-Anmeldeformular erstellen. Navigieren Sie zu **CPPM > Gast > Konfiguration > Web-Anmeldungen**.

Endpunktattribute im Abschnitt "Nach der Authentifizierung":

Benutzername | Benutzername
Besuchername | Besuchername
cn | Besuchername
Besucher_Telefon | Besuchertelefon
E-Mail | E-Mail
Post | E-Mail
Name des Sponsors | Name des Sponsors
Sponsor-E-Mail | Sponsor-E-Mail
Gast-Internet zulassen | wahr

Navigieren Sie im CPPM zu **Live Monitoring > Access Tracker**.

Der neue Gastbenutzer, der den MAB-Dienst verbindet und auslöst.

Registerkarte "Übersicht":

Request Details

Summary | Input | Output | RADIUS CoA

Login Status:	ACCEPT
Session Identifier:	R0000471a-01-6282a110
Date and Time:	May 16, 2022 15:08:00 EDT
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Username:	d43b047a647b
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)
Access Device Name:	wlc01
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	Guest SSID - GuestPortal - Mac Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository]
Roles:	[Employee], [User Authenticated]
Enforcement Profiles:	Cisco_Portal_Redirect

◀ ◀ Showing 8 of 1-8 records ▶ ▶ **Change Status** **Show Configuration** **Export** **Show Logs** **Close**

Navigieren Sie im selben Dialogfeld zur Registerkarte **Eingabe**.

Request Details

Summary Input Output **RADIUS CoA**

Username:	d43b047a647b
End-Host Identifier:	d4-3b-04-7a-64-7b (Computer / Windows / Windows)
Access Device IP/Port:	10.85.54.99:73120 (WLC_9800_Branch / Cisco)

RADIUS Request

Radius:Airespace:Airespace-Wlan-Id	4
Radius:Cisco:Cisco-AVPair	audit-session-id=6336550A00006227CE452457
Radius:Cisco:Cisco-AVPair	cisco-wlan-ssid=Guest
Radius:Cisco:Cisco-AVPair	client-iif-id=1728058392
Radius:Cisco:Cisco-AVPair	method=mab
Radius:Cisco:Cisco-AVPair	service-type=Call Check
Radius:Cisco:Cisco-AVPair	vlan-id=21
Radius:Cisco:Cisco-AVPair	wlan-profile-name=WP_Guest
Radius:IETF:Called-Station-Id	14-16-9d-df-16-20:Guest
Radius:IETF:Calling-Station-Id	d4-3b-04-7a-64-7b

◀ ◀ Showing 8 of 1-8 records ▶ ▶ **Change Status** **Show Configuration** **Export** **Show Logs** **Close**

Navigieren Sie im selben Dialogfeld zur Registerkarte **Ausgabe**.

Request Details

Summary Input **Output** RADIUS CoA

Enforcement Profiles:	Cisco_Portal_Redirect
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

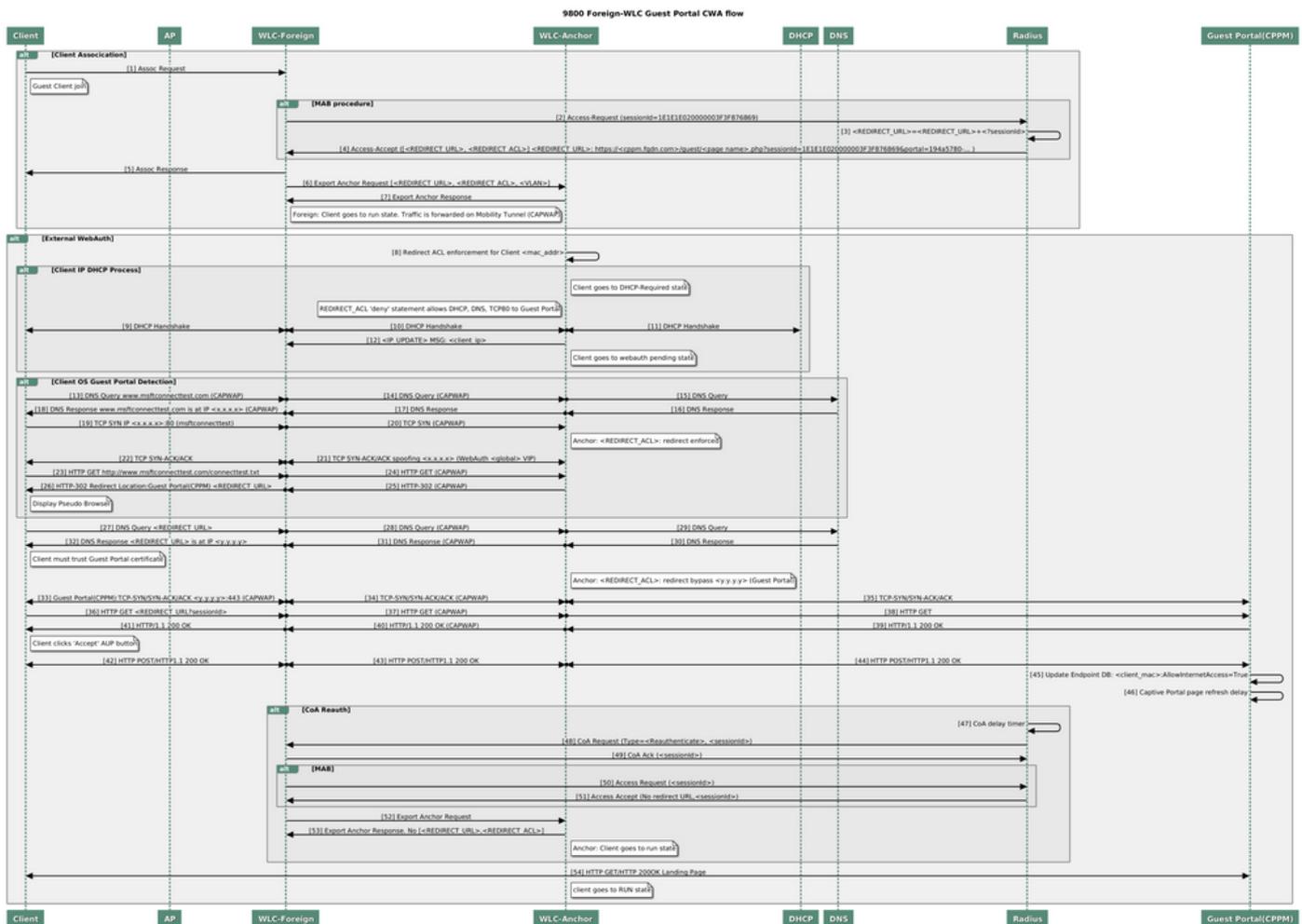
Radius:Cisco:Cisco-AVPair	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT
Radius:Cisco:Cisco-AVPair	url-redirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b-04-7a-64-7b&switchip=10.85.54.99

◀ ◀ Showing 8 of 1-8 records ▶ ▶ **Change Status** **Show Configuration** **Export** **Show Logs** **Close**

Anhang

Zu Referenzzwecken wird hier ein Statusflussdiagramm für Cisco 9800 Foreign, Anchor Controller

Interactions mit RADIUS Server und extern gehostetes Gastportal dargestellt.



Zustandsdiagramm zur Guest Central-Webauthentifizierung mit Anker-WLC

Zugehörige Informationen

- [Cisco 9800 - Best Practices-Leitfaden zur Bereitstellung](#)
- [Catalyst Wireless Controller der Serie 9800 - Konfigurationsmodell](#)
- [FlexConnect auf Catalyst 9800 Wireless Controller verstehen](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

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.