

# Configureer de 9800 WLC en Aruba ClearPass - Guest Access en FlexConnect

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Traffic Flow voor CWA Guest Enterprise Implementatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Draadloze gasttoegang tot C9800-parameters configureren](#)

[C9800 - AAA-configuratie voor gasten](#)

[C9800 - Redirectie-ACL configureren](#)

[C9800 - WLAN-profielconfiguratie voor gasten](#)

[C9800 - definitie van gastenbeleidsprofiel](#)

[C9800 - Beleidsmarkering](#)

[C9800 - Profiel voor AP Join](#)

[C9800 - Flex profiel](#)

[C9800 - Sitetag](#)

[C9800 - RF-profiel](#)

[C9800 - Tags toewijzen aan AP](#)

[Aruba CPPM-instantie configureren](#)

[Eerste configuratie van Aruba ClearPass-server](#)

[Licenties aanvragen](#)

[Server Hostname](#)

[HTTP-servercertificaat \(CPPM Web Server Certificate\) genereren](#)

[C9800 WLC definiëren als netwerkapparaat](#)

[Pagina en CoA Timers](#)

[ClearPass - Gastconfiguratie CWA](#)

[ClearPass-metagegevens over endpoints: Allow-Guest-Internet](#)

[Configuratie van handhavingsbeleid voor ClearPass opnieuw verifiëren](#)

[Configuratie van ClearPass Guest Portal Redirect-handhavingsprofiel](#)

[Configuratie van ClearPass-metagegevens-handhavingsprofiel](#)

[Configuratie van beleid voor internettoegang via ClearPass voor gasten](#)

[Configuratie van ClearPass Guest Post-AUP handhavingsbeleid](#)

[Serviceconfiguratie voor ClearPass MAB-verificatie](#)

[Configuratie van ClearPass-webauth-services](#)

[ClearPass - Web Login](#)

[Verificatie - Guest CWA-autorisatie](#)

[Bijlage](#)

## Inleiding

Dit document beschrijft de integratie van Catalyst 9800 draadloze LAN-controller (WLC) met Aruba ClearPass om Guest Wireless Service Set Identifier (SSID) te leveren die gebruik maakt van Central Web Verification (CWA) voor draadloze clients in een Flexconnect-modus van access point (AP) implementatie.

De draadloze verificatie van de gast wordt ondersteund door Guest Portal met een anonieme pagina voor acceptabel gebruikersbeleid (AUP), gehost op Aruba Clearpass in een veilig gedemilitariseerde zone (DMZ) segment.

## Voorwaarden

Deze handleiding gaat ervan uit dat deze componenten zijn geconfigureerd en geverifieerd:

- Alle relevante componenten worden gesynchroniseerd met Network Time Protocol (NTP) en geverifieerd om de juiste tijd te hebben (vereist voor certificaatvalidatie)
- Operationele DNS-server (vereist voor gastverkeersstromen, validatie van certificaatherroeping (CRL))
- Operationele DHCP-server
- Een optionele certificaatautoriteit (CA) (vereist om het door CPPM gehoste Guest Portal te ondertekenen)
- Catalyst 9800 WLC
- Aruba ClearPass Server (vereist platformlicentie, toegangslicentie, on-board licentie)
- ESXi van VMware

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- C9800 implementatie- en nieuw configuratiemodel
- Flexconnect-switching op C980
- 9800 CWA-verificatie (zie <https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213920-central-web-authentication-cwa-on-cata.html>)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst C9800-L-C switch die 17.3.4c draait
- Cisco Catalyst C9130AX switch
- Aruba ClearPass, 6-8-0-109592 en 6.8-3 patch
- MS Windows-server Active Directory (GP geconfigureerd voor automatische op machine gebaseerde certificaatuitgifte aan beheerde endpoints)DHCP-server met optie 43 en optie 60DNS-serverNTP-server om alle componenten te synchroniserenCA

De informatie in dit document is gebaseerd op de apparaten in een specifieke

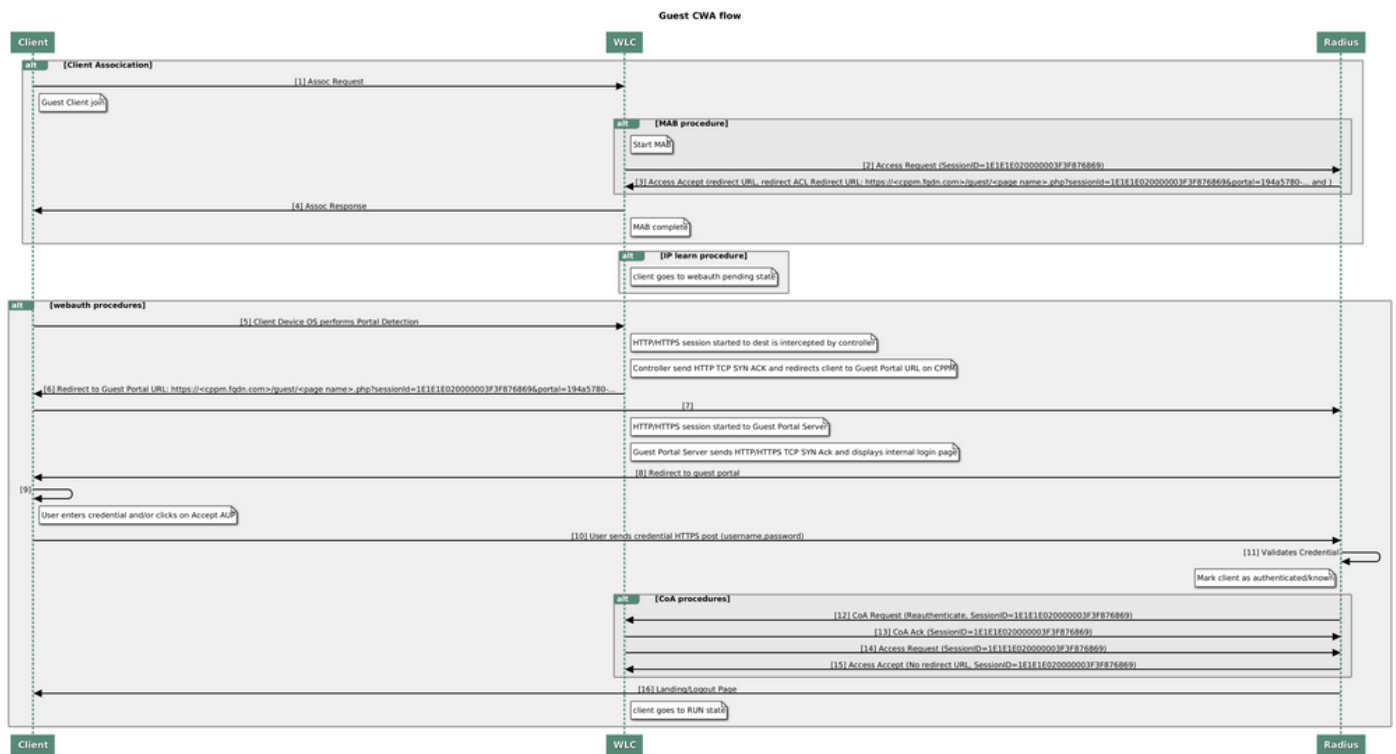
laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

In het diagram worden de details van de WiFi-toegangsuitwisselingen van de gast weergegeven voordat de gast-gebruiker op het netwerk is toegestaan:

1. De gastgebruiker werkt in een extern kantoor samen met de Guest Wifi.
2. Het eerste RADIUS-toegangsverzoek wordt door C9800 naar de RADIUS-server geproxied.
3. De server kijkt omhoog het bijgeleverde gast MAC-adres in de lokale MAC Endpoint Database. Als het mac-adres niet wordt gevonden, reageert de server met een MAC-verificatie-omzeilingsprofiel (MAB). Deze RADIUS-respons omvat:
  - URL-toegangscontrolelijst voor omleiding (ACL)
  - URL-omleiding
4. De client gaat door het IP Learn-proces waar het een IP-adres krijgt toegewezen.
5. C9800 brengt de gastclient (geïdentificeerd door zijn MAC-adres) over naar de 'Web Auth Pending'-status.
6. Het meeste moderne apparaat OS in samenwerking met gast WLAN's voert een soort captive portal detectie uit. Het exacte detectiemechanisme is afhankelijk van de specifieke implementatie van het besturingssysteem. Het client-OS opent een pop-up (pseudo-browser) dialoogvenster met een pagina die door C9800 is omgeleid naar de gast-portal-URL die wordt gehost door de RADIUS-server die wordt geleverd als deel van de RADIUS Access-Accept-respons.
7. Gastgebruiker accepteert de voorwaarden op de gepresenteerde pop-up ClearPass stelt een vlag voor het client-MAC-adres in zijn Endpoint Database (DB) om aan te geven dat de client een verificatie heeft voltooid en een RADIUS-wijziging van autorisatie (CoA) initieert, door de selectie van een interface op basis van de routingstabel (als er meerdere interfaces aanwezig zijn op ClearPass).
8. WLC overgaat Gastclient naar 'Run' staat en de gebruiker krijgt toegang tot het internet zonder verdere omleidingen.

**Opmerking:** Raadpleeg voor Cisco 9800 Foreign, Anker Wireless Controller state flow diagram met RADIUS en extern gehoste Guest Portal de sectie van de bijlage in dit artikel.



Statusdiagram van Guest Central Web Verification (CWA)

## Traffic Flow voor CWA Guest Enterprise Implementatie

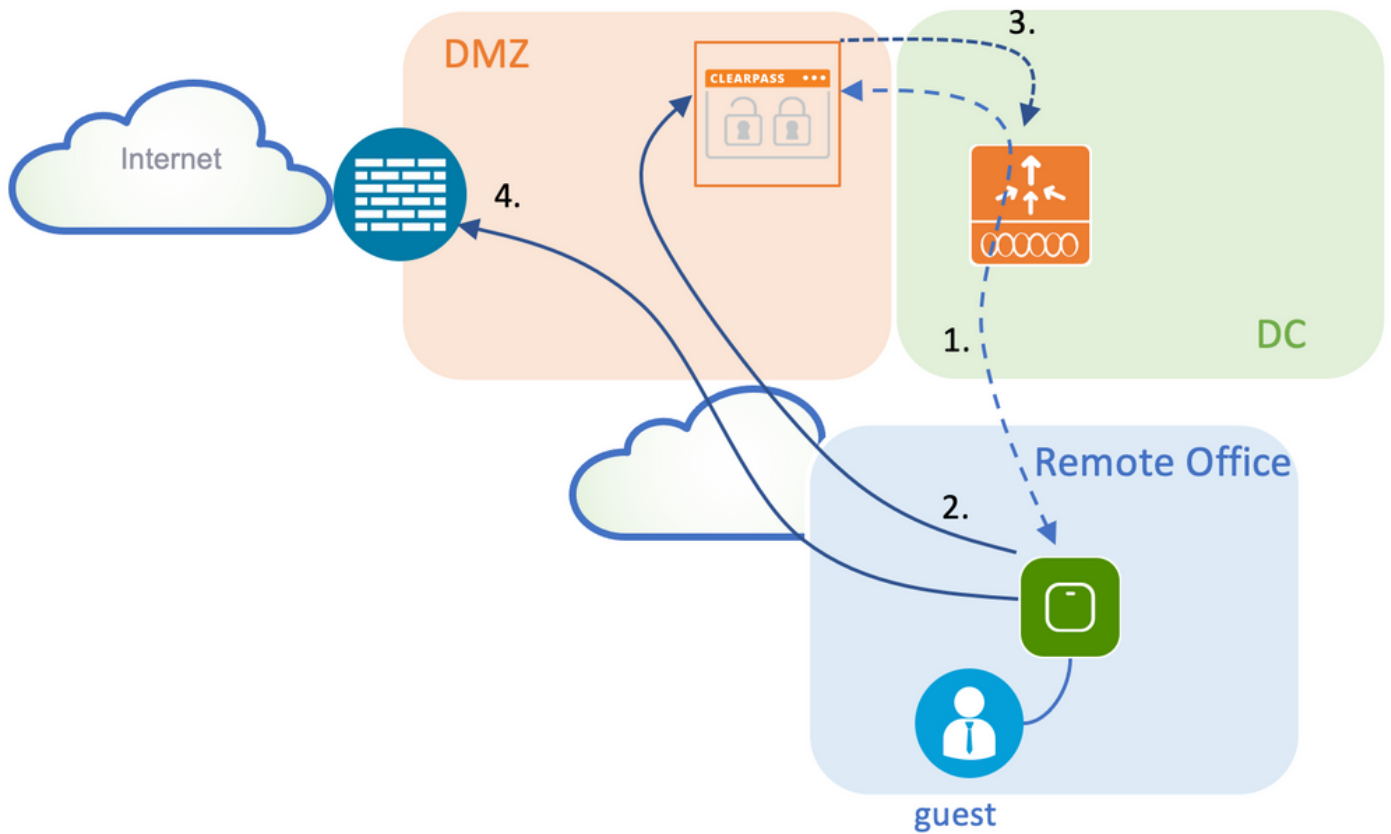
In een typische bedrijfsplaatsing met meerdere bijkantoren, wordt elk bijkantoor opgericht om veilige, gesegmenteerde toegang tot gasten door een Gastenportaal te verlenen zodra de gast EULA goedkeurt.

In dit configuratievoorbeeld wordt 9800 CWA gebruikt voor gasttoegang via integratie in een afzonderlijke ClearPass-instantie die exclusief wordt ingezet voor gastgebruikers in de beveiligde DMZ van het netwerk.

De gasten moeten akkoord gaan met de voorwaarden die worden uiteengezet in het pop-upportaal voor webtoestemming dat wordt aangeboden door de DMZ ClearPass-server. Dit configuratievoorbeeld richt zich op de Anonymous Guest Access methode (dat wil zeggen dat er geen gebruikersnaam/wachtwoord voor de gast nodig is om te verifiëren naar Guest Portal).

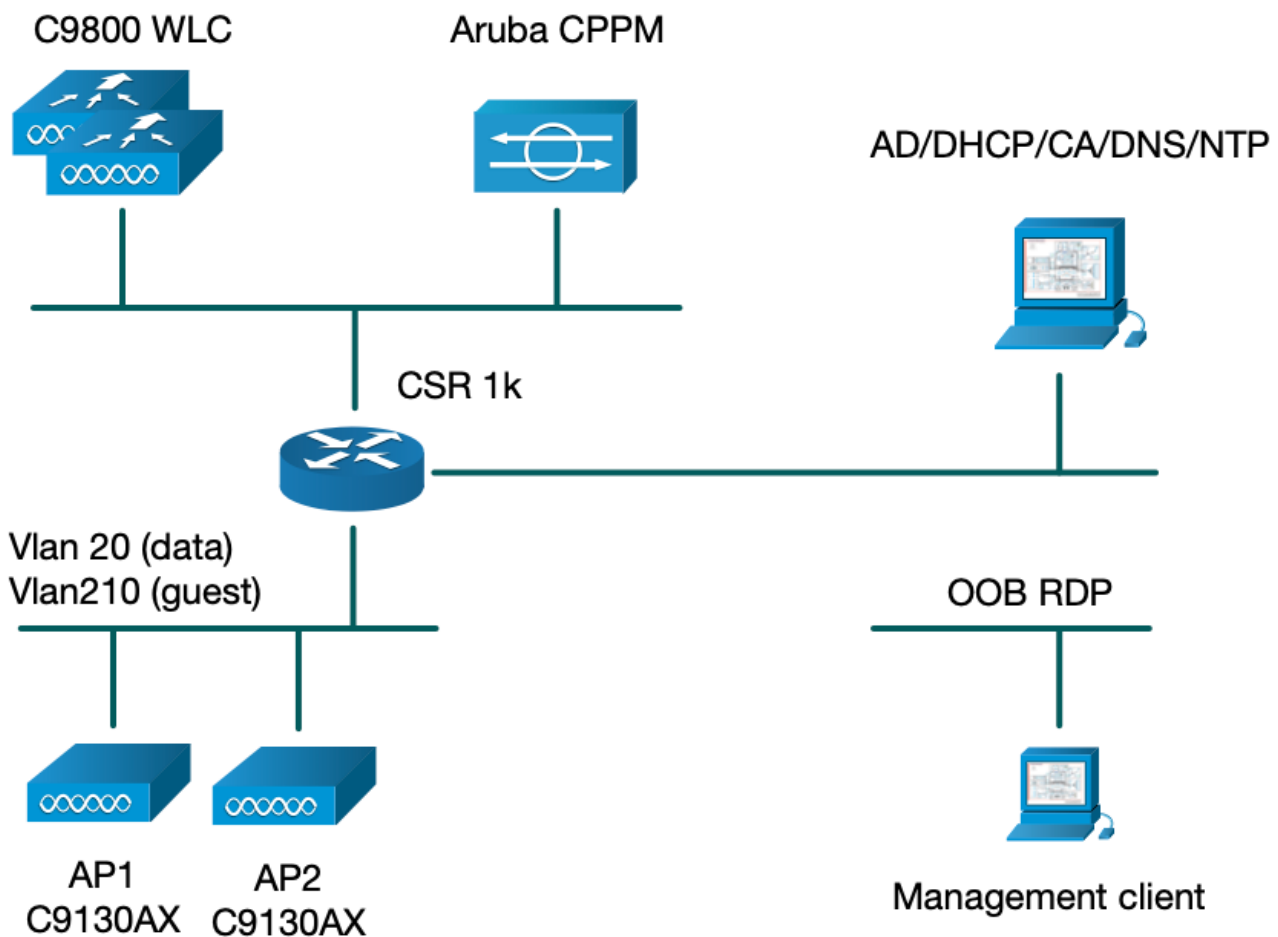
De verkeersstroom die bij deze implementatie hoort, wordt in het beeld weergegeven:

1. RADIUS - MAB-fase
2. Gastclient-URL omleiden naar Gastenportaal
3. Nadat de gast EULA op het Gastenportaal heeft aanvaard, wordt RADIUS CoA Reauthenticate afgegeven van CPPM tot 9800 WLC
4. De gast heeft toegang tot internet



## Netwerkdigram

**Opmerking:** Voor de proefdemo-doeleinden wordt een enkele/gecombineerde Aruba CPPM Server-stantie gebruikt om zowel de functies van de Guest als Corp SSID Network Access Server (NAS) te bedienen.



## Configureren

In dit configuratievoorbeeld wordt een nieuw configuratiemodel op C9800 gebruikt om de benodigde profielen en tags te maken voor dot1x Corporate Access en CWA guest Access naar de enterprise branch. De resulterende configuratie wordt in dit beeld samengevat:

**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-CPM
- 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

## Draadloze gasttoegang tot C9800-parameters configureren

### C9800 - AAA-configuratie voor gasten

**Opmerking:** Over Cisco bug-id [CSCvh03827](#), zorg ervoor dat de gedefinieerde verificatie-, autorisatie- en accounting (AAA) servers niet taakverdeling hebben, omdat het mechanisme afhankelijk is van SessionID-persistentie in WLC om RADIUS-uitwisselingen te wissen.

Stap 1. Voeg de Aruba ClearPass DMZ-server(s) toe aan de 9800 WLC-configuratie en maak een lijst met verificatiemethoden. Navigeer naar **Configuratie > Beveiliging > AAA > servers/groepen > RADIUS > servers > +Add** en voer de RADIUS-serverinformatie in.

## 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* <span style="font-size: small;">(i)</span>	<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

↶ Cancel

📄 Apply to Device

Stap 2. Definieer AAA-servergroep voor gasten en wijs de server die in Stap 1 is geconfigureerd toe aan deze servergroep. Navigeer naar **Configuratie > Beveiliging > AAA > servers/groepen > RADIUS > Groepen > +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



↶ Cancel

📄 Apply to Device



Stap 3. Definieer een lijst met autorisatiemethoden voor gasttoegang en wijs de servergroep toe die in Stap 2 is gemaakt. Navigeer naar **Configuratie > Beveiliging > AAA > AAA-methodelijst > Autorisatie > +Add**. Kies **Type netwerk** en vervolgens **AAA-servergroep** geconfigureerd in stap 2.

Quick Setup: AAA Authorization ✕

Method List Name\*

Type\*  ⓘ

Group Type  ⓘ

Fallback to local

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AAA\_Radius\_CPPM

Stap 4. Maak een lijst met accounting methoden voor gasttoegang en wijs de servergroep toe die in Stap 2 is gemaakt. Ga naar **Configuration > Security > AAA > AAA Method List > Accounting > +Add**. Kies **Type Identity** in het vervolgkeuzemenu en **AAA-servergroep** ingesteld in stap 2.

Quick Setup: AAA Accounting ✕

Method List Name\*

Type\*  ⓘ

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- AAA\_Radius\_CPPM

De omleiding ACL bepaalt welk verkeer moet worden omgeleid naar de Gastenportal vs toegestaan om te passeren zonder omleiding. Hier impliceert de ACL omleiding omleiding of omleiding door, terwijl de vergunning impliceert omleiding naar de portal. Voor elke verkeersklasse moet u rekening houden met de richting van het verkeer wanneer u Access Control Entries (ACE's) maakt en ACE's maakt die zowel aan het in- als uitgaand verkeer voldoen.

Navigeer naar **Configuration > Security > ACL** en definieer een nieuwe ACL met de naam **CAPTIVE\_PORTAL\_REDIRECT**. Configureer de ACL met deze ACE's:

- ACE1: Staat bidirectioneel verkeer van het Bericht van Internet Control Protocol (ICMP) toe om omleiding te mijden en wordt hoofdzakelijk gebruikt om bereikbaarheid te verifiëren.
- ACE10, ACE30: Maakt bidirectionele DNS-verkeersstroom naar DNS-server 10.0.10.4 mogelijk en kan niet worden omgeleid naar het portal. Een DNS raadpleging en onderschepping voor reactie zijn nodig om de gaststroom teweeg te brengen.
- ACE70, ACE80, ACE110, ACE120: Laat HTTP en HTTPS toegang tot het gast captive portal voor de gebruiker worden gepresenteerd met het portal.
- ACE-nr. 150: Al HTTP-verkeer (UDP-poort 80) wordt omgeleid.

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 - WLAN-profielconfiguratie voor gasten

Stap 1. Navigeer naar **Configuratie > Tags & profielen > Draadloos > +Add**. Maak een nieuw SSID Profile WP\_Guest, met de uitzending van SSID 'Guest' dat gastclients associëren met.

## 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		

Onder hetzelfde dialoogvenster **WLAN toevoegen**, navigeer naar het tabblad **Security > Layer 2**.

- Layer 2 Security Mode: None

- MAC-filtering: Ingeschakeld

- Vergunningslijst: AAA\_Authz\_CPPM vanuit het uitrolmenu (geconfigureerd onder Stap 3. als onderdeel van AAA-configuratie)

## 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"/>		

C9800 - definitie van gastenbeleidsprofiel

Op C9800 WLC GUI, navigeer naar **Configuration > Tags & profielen > Policy > +Add.**

Name: PP\_Gast

Status: Ingeschakeld

Centrale switching: Uitgeschakeld

Centrale verificatie: Ingeschakeld

Centrale DHCP: Uitgeschakeld

Centrale vereniging: Uitgeschakeld

### 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*	<input type="text" value="PP_Guest"/>	<b>WLAN Switching Policy</b>	
Description	<input type="text" value="Policy Profile for Guest"/>	Central Switching	<input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED	Central Association	<input type="checkbox"/> DISABLED
<b>CTS Policy</b>		Flex NAT/PAT	<input type="checkbox"/> DISABLED
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

## 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

Navigeer naar het tabblad **Toegangsbeleid** in hetzelfde dialoogvenster **Beleidsprofiel toevoegen**.

- RADIUS-profilering: Ingeschakeld

- VLAN/VLAN-groep: 210 (dat wil zeggen dat VLAN 210 het lokale VLAN van het gast is op elke locatie van de tak)

**Opmerking:** Guest VLAN voor Flex moet niet worden gedefinieerd op de 9800 WLC onder VLAN's, in het VLAN/VLAN-groepstype VLAN-nummer.

Bekende fout: Cisco bug-id [CSCvn48234](#) zorgt ervoor dat SSID niet wordt uitgezonden als dezelfde Flex guest VLAN wordt gedefinieerd onder WLC en in het Flex 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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

#### WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name

#### VLAN

VLAN/VLAN Group

Multicast VLAN

#### WLAN ACL

IPv4 ACL

IPv6 ACL

#### URL Filters

Pre Auth

Post Auth

↶ Cancel

📄 Apply to Device

In hetzelfde dialoogvenster **Beleidsprofiel toevoegen** gaat u naar het tabblad **Geavanceerd**.

- AAA negeren toestaan: Ingeschakeld

- Staat NAC: Ingeschakeld

- NAC-type: STRAAL

- Boekhoudkundige lijst: AAA\_Accounting\_CPPM (gedefinieerd in stap 4. als deel van AAA-configuratie)

⚠ 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

**Opmerking:** De 'Network Admission Control (NAC) State - Enable' is vereist om C9800 WLC in staat te stellen RADIUS CoA-berichten te accepteren.

## C9800 - Beleidsmarkering

Op C9800 GUI, navigeer naar **Configuration > Tags & profielen > Tags > Beleid > +Add**.

-Name: PT\_CAN01

-Beschrijving: Policy Tag voor CAN01 Branch Site

In hetzelfde dialoogvenster **Add Policy Tag**, onder **WLAN-POLICY MAPS**, klikt u op **+Add**, en wijst u het eerder gemaakte WLAN-profiel toe aan het beleidsprofiel:

- WLAN-profiel: WP\_Guest

- Beleidsprofiel: PP\_Gast

### Add Policy Tag ✕

Name\*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
0 items per page <span>No items to display</span>	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

---

➤ RLAN-POLICY Maps: 0

## C9800 - Profiel voor AP Join

Op C9800 WLC GUI, navigeer naar **Configuration > Tags & profielen > AP Join > +Add**.

-Name: Branch\_AP\_Profile

- NTP-server: 10.0.10.4 (raadpleeg het diagram van de laboratoriumtopologie). Dit is de NTP-server die door AP's in Branch wordt gebruikt om te synchroniseren.



## Add AP Join Profile

<b>General</b>	Client	CAPWAP	AP	Management	Security	ICap	QoS
Name*	Branch_AP_Profile		<b>OfficeExtend AP Configuration</b>				
Description	Branch AP Join Profile		Local Access	<input checked="" type="checkbox"/>			
LED State	<input checked="" type="checkbox"/>		Link Encryption	<input checked="" type="checkbox"/>			
LAG Mode	<input type="checkbox"/>		Rogue Detection	<input type="checkbox"/>			
NTP Server	10.0.10.4						
GAS AP Rate Limit	<input type="checkbox"/>						
Apphost	<input type="checkbox"/>						
<input type="button" value="Cancel"/>		<input type="button" value="Apply to Device"/>					

## C9800 - Flex profiel

De profielen en tags zijn modulair en kunnen worden hergebruikt voor meerdere sites.

In het geval van FlexConnect-implementatie kunt u hetzelfde flex-profiel opnieuw gebruiken als dezelfde VLAN-ID's worden gebruikt bij alle vestigingen.

Stap 1. Ga op een C9800 WLC GUI naar **Configuration > Tags & profielen > Flex > +Add**.

-Name: FV-tak

- Native VLAN-id: 10 (alleen vereist als u een niet-standaard VLAN hebt waar u een AP-beheerinterface wilt hebben)

## Add Flex Profile

<b>General</b>	Local Authentication	Policy ACL	VLAN	Umbrella	
Name*	FP_Branch		Fallback Radio Shut	<input type="checkbox"/>	
Description	Branch Flex Profile		Flex Resilient	<input type="checkbox"/>	
Native VLAN ID	10		ARP Caching	<input checked="" type="checkbox"/>	
HTTP Proxy Port	0		Efficient Image Upgrade	<input checked="" type="checkbox"/>	
HTTP-Proxy IP Address	0.0.0.0		OfficeExtend AP	<input type="checkbox"/>	
<b>CTS Policy</b>			Join Minimum Latency	<input type="checkbox"/>	
Inline Tagging	<input type="checkbox"/>		IP Overlap	<input type="checkbox"/>	
SGACL Enforcement	<input type="checkbox"/>		mDNS Flex Profile	<input type="text" value="Search or Select"/>	
CTS Profile Name	default-sxp-profile				
<input type="button" value="Cancel"/>		<input type="button" value="Apply to Device"/>			

Navigeer in hetzelfde dialoogvenster **Flex profiel toevoegen** naar het tabblad **Beleids-ACL** en klik op **+Add**.

- ACL-naam: CAPTIVE\_PORTAL\_REDIRECT

- Central Web Auth: Ingeschakeld

Bij een Flexconnect-implementatie wordt van elke beheerde AP verwacht dat hij de omleiding van de ACL lokaal downloadt, aangezien omleiding plaatsvindt op het toegangspunt en niet op de C9800.

The screenshot shows the 'Add Flex Profile' dialog box with the 'Policy ACL' tab selected. The dialog has tabs for 'General', 'Local Authentication', 'Policy ACL', 'VLAN', and 'Umbrella'. Below the tabs are '+ Add' and 'x Delete' buttons. A table lists ACLs, currently empty. A modal form is open with the following fields: 'ACL Name\*' (Captive\_Portal\_F), 'Central Web Auth' (checked), and 'Pre Auth URL Filter' (Search or Select). 'Save' and 'Cancel' buttons are at the bottom. At the bottom of the dialog are 'Cancel' and 'Apply to Device' buttons.

In hetzelfde dialoogvenster **Flex profiel toevoegen**, navigeer naar het tabblad **VLAN** en klik op **+Add** (zie het diagram van de laboratoriumtopologie).

- VLAN-naam: gast

- VLAN-id: 210

The screenshot shows the 'Add Flex Profile' dialog box with the 'VLAN' tab selected. The dialog has tabs for 'General', 'Local Authentication', 'Policy ACL', 'VLAN', and 'Umbrella'. Below the tabs are '+ Add' and 'x Delete' buttons. A table lists VLANs with columns for 'VLAN Name', 'ID', and 'ACL Name'. One entry is visible: 'data' with ID '2'. A modal form is open with the following fields: 'VLAN Name\*' (guest), 'VLAN Id\*' (210), and 'ACL Name' (Select ACL). 'Save' and 'Cancel' buttons are at the bottom. At the bottom of the dialog are 'Cancel' and 'Apply to Device' buttons.

## C9800 - Sitetag

Op 9800 WLC GUI, navigeer naar **Configuration > Tags & profielen > Tags > Site > Add**.

**Opmerking:** Maak een unieke Site Tag voor elke Remote Site die de twee draadloze SSID's

moet ondersteunen zoals beschreven.

Er is een 1-1 afbeelding tussen een geografische locatie, Site Tag en een Flex Profile configuratie.

Op een flex-verbindingssite moet een flex-verbindingsprofiel zijn gekoppeld. U kunt maximaal 100 access points hebben voor elke flex connect site.

-Name: ST\_CAN01

- Profiel samenvoegen: Branch\_AP\_Profile

- Flex profiel: FV-tak

- Lokale site inschakelen: Uitgeschakeld

### Add Site Tag ✕

Name*	ST_CAN01
Description	Site Tag for Branch CA
AP Join Profile	Branch_AP_Profile ▾
Flex Profile	FP_Branch ▾
Fabric Control Plane Name	▾
Enable Local Site	<input type="checkbox"/>

↶ Cancel Apply to Device

## C9800 - RF-profiel

Op 9800 WLC GUI, navigeer naar **Configuration > Tags & profielen > Tags > RF > Add**.

-Name: Vestigings\_RF

- 5 GHz band radiofrequentie (RF) profiel: Typisch\_client\_dichtheid\_5gh (systeemgedefinieerde optie)

- 2,4 GHz band RF-profiel: Typisch\_client\_dichtheid\_2gh (systeemgedefinieerde optie)

## 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 - Tags toewijzen aan AP

Er zijn twee opties beschikbaar om gedefinieerde tags toe te wijzen aan afzonderlijke AP's in de implementatie:

- AP op naam gebaseerde opdracht, die regex regels die overeenkomen op patronen in het AP Naam veld (**Configureren > Tags & profielen > Tags > AP > Filter**)
- Toewijzing op basis van AP Ethernet MAC-adres (**Configureren > Tags en profielen > Tags > AP > Statisch**)

Bij de implementatie van DNA Center bij de productie wordt het gebruik van DNAC en AP PNP Workflow of een in 9800 beschikbare statische bulk Comma-Separated Values (CSV) uploadmethode ten eerste aanbevolen om handmatige toewijzing per AP te voorkomen. Navigeer naar **Configureren > Tags en profielen > tags > AP > Statisch > Add** (Opmerking over de optie **Upload File**).

- AP MAC-adres: <AP\_ETHERNET\_MAC>
- Policy Tag Name: PT\_CAN01
- Site Tag naam: ST\_CAN01
- RF-labelnaam: Vestigings\_RF

**Opmerking:** Vanaf Cisco IOS®-XE 17.3.4c zijn er maximaal 1000 regex-regels per controllerbeperking. Als het aantal sites in de implementatie dit aantal overschrijdt, moet de statische opdracht per MAC worden uitgevoerd.

## 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

**Opmerking:** Als u de op AP-naam regex-gebaseerde methode voor het toewijzen van tags wilt gebruiken, gaat u naar **Configureren > Tags & profielen > Tags > AP > Filter > Add**.

-Name: BR\_CAN01

- AP naam regex: BR-CAN01-.(7) (Deze regel komt overeen met de naamconventie van de AP die binnen de organisatie is aangenomen. In dit voorbeeld worden de tags toegewezen aan AP's die een veld AP Name hebben dat 'BR\_CAN01-' bevat, gevolgd door zeven tekens.)

-Prioriteit: 1

- Policy Tag Name: PT\_CAN01 (zoals gedefinieerd)

- Site Tag naam: ST\_CAN01

- RF-labelnaam: Vestigings\_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-instantie configureren

Voor productie/best practices gebaseerde Aruba CPPM configuratie, neem contact op met uw

lokale HPE Aruba SE bron.

## Eerste configuratie van Aruba ClearPass-server

Aruba ClearPass wordt geïmplementeerd met het gebruik van de OVF-sjabloon (Open Virtualization Format) op de ESXi <->-server die deze bronnen toewijst:

- Twee gereserveerde virtuele CPU's
- 6 GB RAM
- 80 GB schijf (moet handmatig worden toegevoegd na eerste VM-implementatie voordat de machine wordt ingeschakeld)

## Licenties aanvragen

Platformlicentie toepassen via: **Beheer > Server Manager > Licentie**. Platform-, **access-** en **onboard-licenties** toevoegen.

## Server Hostname

Navigeer naar **Beheer > Serverbeheer > Serverconfiguratie** en kies de nieuwe CPPM-server met voorzieningen.

- Hostname: PPM

- FQDN: cppm.example.com

- Controleer IP-adressering en DNS voor beheerpoorten

Administration » Server Manager » Server Configuration - cppm

Server Configuration - cppm (10.85.54.98)

The screenshot displays the configuration page for a CPPM server. The 'System' tab is active, showing fields for Hostname (cppm) and FQDN (cppm.example.com). Below these are sections for Performance Monitoring, Insight, and Ingress Events. The 'Network' section is expanded to show IPv4 settings for three ports: Management Port, Data/External Port, and DNS Settings. The Management Port is configured with IP 10.85.54.98, Subnet Mask 255.255.255.224, and Default Gateway 10.85.54.97. The DNS Settings section shows a Primary IP of 10.85.54.122. Each network configuration row has a 'Configure' button.

	IPv4	IPv6	Action
<b>Management Port</b>	IP Address	10.85.54.98	<a href="#">Configure</a>
	Subnet Mask	255.255.255.224	
	Default Gateway	10.85.54.97	
<b>Data/External Port</b>	IP Address		<a href="#">Configure</a>
	Subnet Mask		
	Default Gateway		
<b>DNS Settings</b>	Primary	10.85.54.122	<a href="#">Configure</a>
	Secondary		
	Tertiary		
	DNS Caching	Disabled	

HTTP-servercertificaat (CPPM Web Server Certificate) genereren

Dit certificaat wordt gebruikt wanneer de ClearPass Guest Portal-pagina via HTTPS wordt gepresenteerd aan gasten die verbinding maken met de Guest Wifi in Branch.

Stap 1. Upload het CA pub kettingcertificaat.

Navigeer naar **Beheer > Certificaten > Vertrouwenslijst > Toevoegen**.

- Gebruik: Overige inschakelen

### 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

**Update** **Disable** **Export** **Close**

Stap 2. Maak een aanvraag voor certificaatondertekening aan.

Navigeer naar **Beheer > Certificaten > Certificaatopslag > Servercertificaten > Gebruik: HTTPS-servercertificaat**.

- Klik op de **Aanvraag voor certificaatondertekening maken**

- triviale naam: PPM

- Organisatie: **cppm.example.com**

Zorg ervoor dat het SAN-veld wordt ingevuld (er moet een veelvoorkomende naam aanwezig zijn

in het SAN, alsook IP en andere FQDN's, indien nodig). Formaat is 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
<b>Submit</b> <b>Cancel</b>	

Stap 3. Teken in uw CA van keuze de nieuwe CPPM HTTPS Service CSR.

Stap 4. Navigeer naar **certificaatsjabloon > Webserver > Certificaat importeren**.

- Type certificaat: Servercertificaat
- Gebruik: HTTP-servercertificaat
- certificaatbestand: Bladeren en CA-ondertekend CPPM HTTPS-servicecertificaat selecteren

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.
<b>Import</b> <b>Cancel</b>	

C9800 WLC definiëren als netwerkapparaat



Navigeer naar **Configuratie > Netwerk > Apparaten > Toevoegen**.

-Name: WLC\_9800\_Branch

- IP- of subnetadres: 10.85.54.99 (raadpleeg het diagram van de laboratoriumtopologie)

- RADIUS gedeeld Cisco: <WLC RADIUS-wachtwoord>

- Naam leverancier: Cisco-software

- Dynamische autorisatie RADIUS inschakelen: 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**

## Pagina en CoA Timers

Het is zeer belangrijk om de juiste tijdoptimerwaarden door de configuratie te plaatsen. Als timers niet worden afgestemd, zult u waarschijnlijk een cycling Web Portal omleiden met de client niet in 'Run State'.

Timers om aandacht te besteden aan:

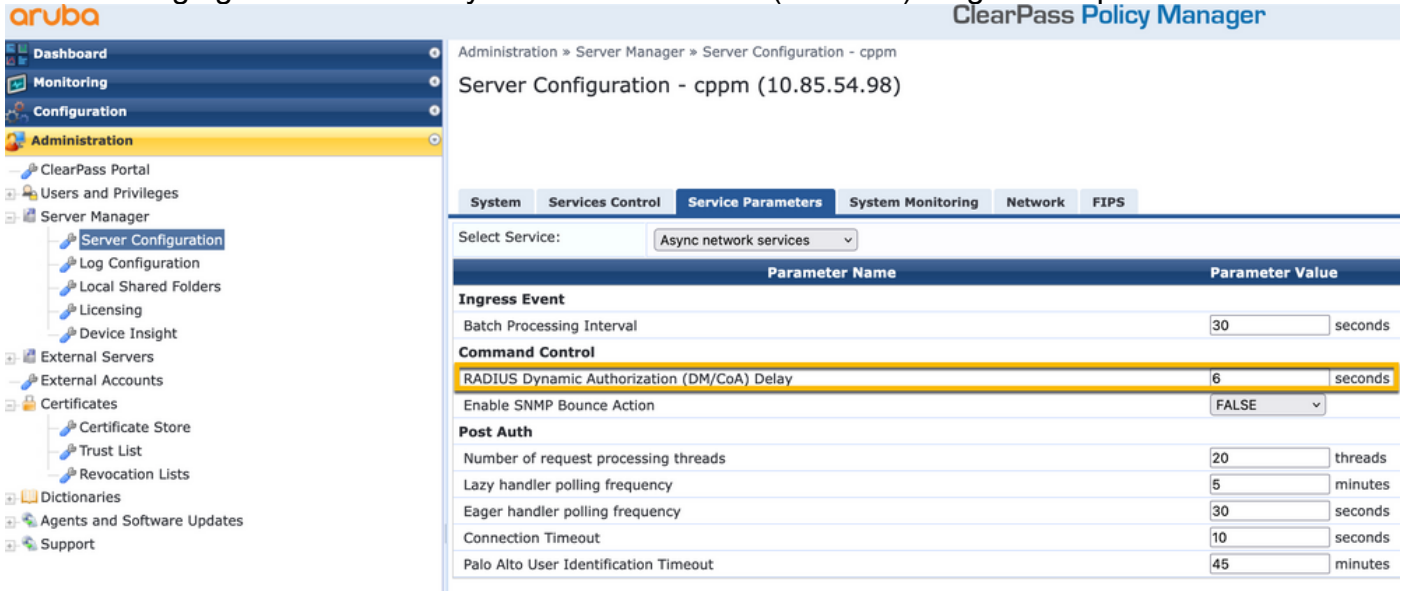
- Portal Web Login timer: Deze timer vertraagt uw omleiden pagina voordat het toegang geeft tot de gast portal pagina om CPPM service te informeren over de overgang van de staat, registreren Endpoint aangepaste attributen 'sta-gast-internet' waarde, en starten van het CoA proces van CPPM naar WLC. Ga naar **Gast > Configuratie > Pagina's > Weblogbestanden**.
  - Kies de naam van het gastenportaal: Lab Anonymous Guest Registration (deze pagina-configuratie voor het gastenportaal is gedetailleerd zoals getoond)
  - Klik op **Bewerken**
  - Inlogvertraging: 6 seconden

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

- ClearPass CoA-vertragingstimer: Dit vertraagt de totstandkoming van CoA-berichten van ClearPass naar WLC. Dit is vereist voor CPPM om met succes de status van het client-endpoint intern te wijzigen voordat CoA-bevestiging (ACK) van WLC terugkomt. De tests van

het laboratorium tonen de sub-milliseconde reactietijden van WLC, en als CPPM niet heeft geëindigd om de eigenschappen van het Endpoint bij te werken, wordt de nieuwe zitting van de RADIUS van WLC aangepast aan het Unauthenticated MAB de handhavingbeleid van de Dienst, en de cliënt wordt gegeven opnieuw opnieuw een opnieuw leiden pagina. Ga naar **CPPM > Beheer > Serverbeheer > Serverconfiguratie** en kies **CPPM Server > Serviceparameters**.

- Vertraging voor RADIUS Dynamic Authorisation (DM/CoA) - ingesteld op 6 seconden



## ClearPass - Gastconfiguratie CWA

ClearPass-side CWA Configuration is samengesteld uit (3) Service points/stappen:

ClearPass-component	Type service	Doel
1. Beleidsmanager	Service: Mac-verificatie	Als een aangepast attribuut <b>Allow-Guest-Internet = TRUE</b> , sta het op het netwerk. Anders, trigger <b>Redirect</b> en <b>COA: Verifiëren</b> . Presenteer Anonymous login A pagina.
2. Gast	Weblogins	Post-auth ingestelde aangepas attribuut <b>Allow-Guest-Internet = TRUE</b> . Eindpunt bijwerken naar <b>bekend</b>
3. Beleidsmanager	Service: Web gebaseerde verificatie	Eigen kenmerk <b>Allow-Guest-Internet</b> instellen = TRUE <b>Cacao: opnieuw authenticeren</b>

## ClearPass-metagegevens over endpoints: Allow-Guest-Internet

Maak een metagegevensattribuut van type Boolean om de Gast Endpoint status te volgen als de client overgangen tussen de 'Webauth Pending' en 'Run' status:

- Nieuwe gasten die verbinding maken met wifi hebben een standaard metadata attribuut ingesteld op **Allow-Guest-Internet=false**. Op basis van deze eigenschap gaat de client auth door de MAB-service

- Gastclient wanneer u op de knop AUP Accept klikt, heeft zijn metagegevenskenmerk bijgewerkt naar Allow-Guest-Internet=true. Volgende MAB gebaseerd op deze eigenschap ingesteld op True verleent niet-omgeleide toegang tot het internet

Navigeer naar ClearPass > Configuration > Endpoints, kies elk eindpunt uit de lijst, klik op het tabblad **Attributen**, voeg **Allow-Guest-Internet toe** met de waarde **false** en **Save**.

**Opmerking:** U kunt hetzelfde eindpunt ook bewerken, en deze eigenschap direct daarna verwijderen - deze stap maakt gewoon een veld in Endpoints metadata DB dat kan worden gebruikt in beleid.

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

### Configuratie van handhavingsbeleid voor ClearPass opnieuw verifiëren

Maak een handhavingsprofiel dat wordt toegewezen aan de gastclient onmiddellijk nadat de client AUP accepteert op de pagina van het gastportaal.

Navigeer naar **ClearPass > Configuration > Profielen > Add**.

- Sjabloon: Dynamische autorisatie RADIUS

-Name: Cisco\_WLC\_Guest\_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:	<div style="display: flex; align-items: center;"> <div style="flex-grow: 1;"> <table border="1" style="width: 100%; height: 40px;"> <tr> <td style="width: 50%;"></td> <td style="width: 50%;"></td> </tr> </table> </div> <div style="margin-left: 10px;"> <div style="margin-bottom: 5px;"><a href="#">Remove</a></div> <div style="margin-bottom: 5px;"><a href="#">View Details</a></div> <div style="margin-bottom: 5px;"><a href="#">Modify</a></div> </div> </div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">--Select--</div>			

Straal:IETF	Bel-station-id	%{RADIUS:IETF:Calling-station-id}
Straal:Cisco	Cisco AVPair	abonnee:opdracht=reauthenticate
Straal:Cisco	Cisco AVPair	%{Straal:Cisco:Cisco- AVPair:abonnee:audit-sessie-id}
Straal:Cisco	Cisco AVPair	abonnee:reauthenticate-type=last type=last

### Configuratie van ClearPass Guest Portal Redirect-handhavingsprofiel

Maak een handhavingsprofiel dat wordt toegepast op Gast tijdens de eerste MAB-fase, wanneer het MAC-adres niet wordt gevonden in de CPPM Endpoint Database met 'Allow-Guest-Internet' ingesteld op **'true'**.

Dit zorgt ervoor dat de 9800 WLC de Gastclient naar het CPPM Guest Portal leidt voor externe verificatie.

Navigeer naar **ClearPass > Handhaving > Profielen > Toevoegen**.

-Name: Cisco\_Portal\_Redirect

-Type: STRAAL

-Actie: accepteren

## 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:		<div style="text-align: right;"> <input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> </div>
	--Select--	

ClearPass-handhavingsprofiel voor omleiding

In hetzelfde dialoogvenster configureert u op het tabblad **Kenmerken** twee kenmerken zoals in deze afbeelding:

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-profielkenmerken omleiden

Het kenmerk **url-redirect-acl** is ingesteld op **CAPTIVE-PORTAL-REDIRECT**, de naam van de ACL die is gemaakt op C9800.

**Opmerking:** Alleen de verwijzing naar de ACL wordt doorgegeven in het RADIUS-bericht en niet de ACL-inhoud. Het is belangrijk dat de naam van de ACL die op 9800 WLC is gemaakt, exact overeenkomt met de waarde van dit RADIUS-kenmerk, zoals wordt weergegeven.

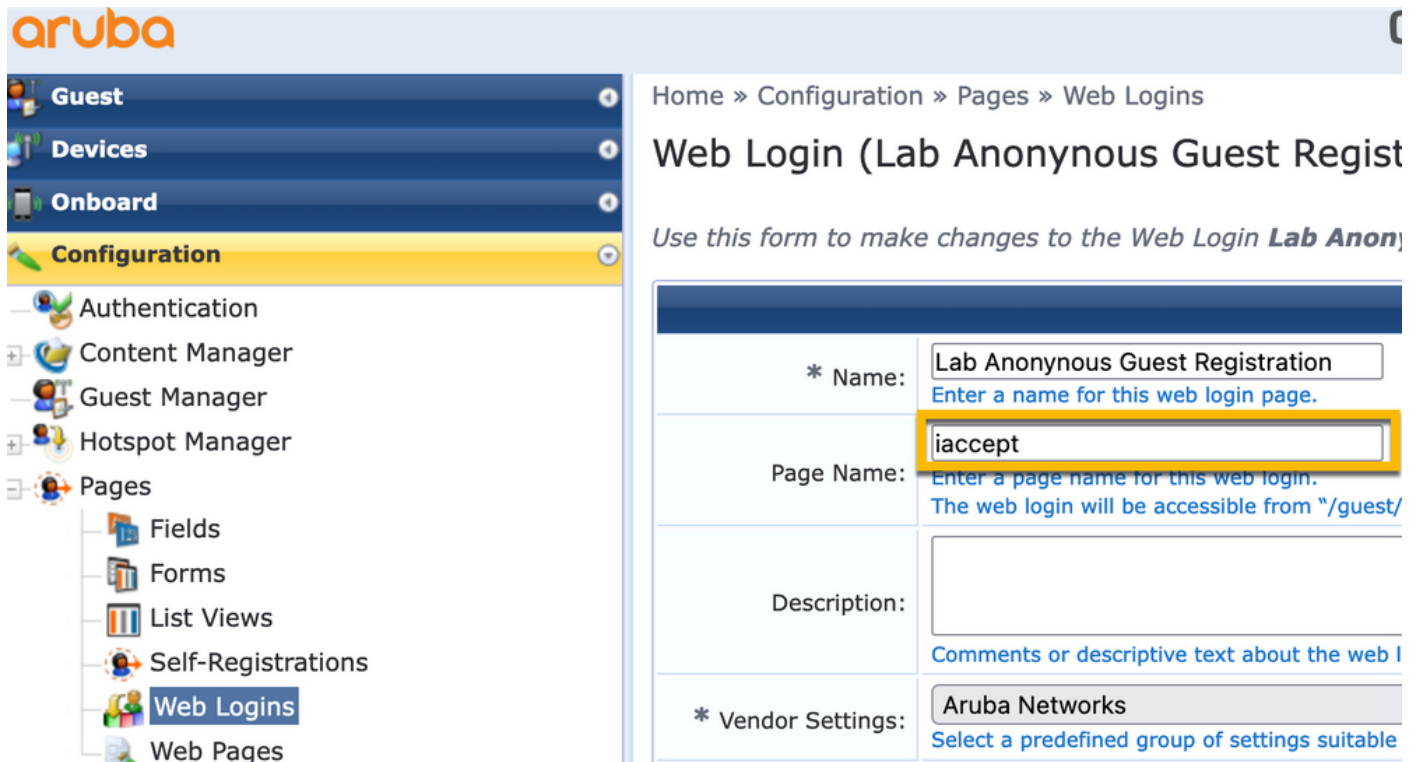
Het kenmerk **url-redirect** bestaat uit verschillende parameters:

- **De doel-URL** waar het Guest Portal wordt gehost, <https://cppm.example.com/guest/iaccept.php>
- **Gastclient-MAC**, macro % {verbinding:client-MAC-adres-koppelteken}
- **Auteur IP** (9800 WLC zorgt voor doorverwijzing), macro %{Straal:IETF:NAS-IP-adres}
- **cmd-login** actie

De URL van de inlogpagina van ClearPass Guest Web wordt weergegeven wanneer u naar **CPPM > Guest > Configuration > Pages > Web Logins > Edit** navigiert.

In dit voorbeeld wordt de naam van de Guest Portal pagina in CPPM gedefinieerd als **acceptabel**.

**Opmerking:** De configuratie stappen voor de Guest Portal pagina zijn zoals beschreven.



The screenshot displays the Aruba configuration interface. On the left, a navigation sidebar lists various management areas: 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 configuration for a Web Login titled 'Web Login (Lab Anonynous Guest Regist...'. The breadcrumb trail is 'Home » Configuration » Pages » Web Logins'. Below the title, there is a note: 'Use this form to make changes to the Web Login **Lab Anonynous Guest Registration**'. The configuration form includes the following fields: '\* Name:' with the value 'Lab Anonynous Guest Registration'; 'Page Name:' with the value 'iaccept' (highlighted in yellow); 'Description:' which is empty; and '\* Vendor Settings:' with the value 'Aruba Networks'. Each field has a small blue link below it providing instructions or context.

**Opmerking:** Voor Cisco-apparaten wordt `audit_sessie_id` normaal gebruikt, maar dat wordt niet ondersteund door andere leveranciers.

### Configuratie van ClearPass-metagegevens-handhavingsprofiel

Configuratie van handhavingsprofiel om Endpoint metagegevenskenmerk dat wordt gebruikt voor stateovergang stapelen door CPPM bij te werken.

Dit profiel wordt toegepast op de Gastclient MAC-adresvermelding in de Endpoint database en stelt het argument '**Allow-Guest-Internet**' in op '**true**'.

Navigeer naar **ClearPass > Handhaving > Profielen > Toevoegen**.

- Sjabloon: Handhaving van ClearPass-entiteiten

-Type: Post\_Verificatie

## 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="display: flex; align-items: center;"> <div style="flex-grow: 1; border: 1px solid #ccc; margin-right: 5px;"></div> <div style="display: flex; flex-direction: column; 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> </div>	

In hetzelfde dialoogvenster vindt u het tabblad **Kenmerken**.

-Type: Endpoint

-Name: Allow-Guest-Internet

**Opmerking:** Om deze naam in het vervolgkeuzemenu te laten verschijnen, moet u dit veld handmatig definiëren voor ten minste één eindpunt zoals beschreven in de stappen.

-Value: echt

## Enforcement Profiles

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

### Configuratie van beleid voor internettoegang via ClearPass voor gasten

Navigeer naar **ClearPass > Handhaving > Beleid > Toevoegen**.

-Name: WLC Cisco-gastentoekenning

- Type handhaving: STRAAL

- Standaardprofiel: Cisco\_Portal\_Redirect

## Enforcement Policies

**Enforcement** Rules Summary

Name:

Description:

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

Default Profile:

Navigeer in hetzelfde dialoogvenster naar het tabblad **Regels** en klik op **Regel toevoegen**.

-Type: Endpoint

-Name: Allow-Guest-Internet

- Exploitant: GELIJK

- Value True

- Profielnamen / Selecteer om toe te voegen: [RADIUS] [Toegangsprofiel toestaan]

**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--

## Configuratie van ClearPass Guest Post-AUP handhavingsbeleid

Navigeer naar **ClearPass > Handhaving > Beleid > Toevoegen**.

-Name: Cisco WLC-webauth voor handhavingsbeleid

- Type handhaving: WEBAUTH (SNMP/Agent/CLI/CoA)

- Standaardprofiel: [RADIUS\_CoA] Cisco\_Reauthenticate\_Session



## 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	<input type="button" value="View Details"/> <input type="button" value="Modify"/>

Navigeer in hetzelfde dialoogvenster naar **Regels > Toevoegen**.

-Voorwaarden: Verificatie

-Name: Status

- Exploitant: GELIJK

-Value: Gebruiker

- Profielnamen: <voeg elk toe>:

- [Verificatie achteraf] [Update endpoint bekend]

- [Verificatie achteraf] [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--"/>	

**Opmerking:** Als u een scenario tegenkomt met een continue Guest Portal omleiden pseudo browser pop-up, is het indicatief dat de CPPM Timers aanpassingen vereisen of dat de RADIUS CoA berichten niet goed worden uitgewisseld tussen CPPM en 9800 WLC. Controleer deze sites.

- Navigeren naar **CPPM > Bewaking > Bewaking tijdens bewegend beeld > Access Tracker**, en ervoor zorgen dat het RADIUS-logbestand gegevens van RADIUS CoA bevat.

- Op **9800 WLC**, navigeer naar **Problemen oplossen > Packet Capture**, schakel pcap in op de interface waar de aankomst van RADIUS CoA-pakketten wordt verwacht en controleer of RADIUS

CoA-berichten worden ontvangen van het CPPM.

## Serviceconfiguratie voor ClearPass MAB-verificatie

De service is afgestemd op AV-paarstraal (Attribute Value): Cisco-software | Cisco AVPair | cisco-WLAN

Navigeer naar **ClearPass > Configuration > Services > Add**.

Tabblad **Service**:

-Name: Gastenportal - Mac Auth

-Type: MAC-verificatie

- Meer opties: Selecteer Autorisatie, profiel endpoints

Matchregel toevoegen:

-Type: Straal: Cisco-software

-Name: Cisco AVPair

- Exploitant: GELIJK

-Value: cisco-wlan-ssid=Guest (stem af op de geconfigureerde SSID van uw gast)

**Opmerking:** 'Guest' is de naam van de uitgezonden Guest SSID door 9800 WLC.

Configuration » Services » Add

### Services

Service	Authentication	Authorization	Roles	Enforcement	Profiler	Summary
Type:	MAC Authentication					
Name:	GuestPortal - Mac Auth					
Description:	MAC-based Authentication Service					
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement					
More Options:	<input checked="" type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input checked="" type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy					
Service Rule						
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> 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		

Kies in hetzelfde dialoogvenster het tabblad **Verificatie**.

- Verificatiemethoden: [MAC AUTH] verwijderen, toevoegen [All MAC AUTH toestaan]

- Verificatiebronnen: [Endpoints Repository][Local SQL DB], [Guest User Repository][Local SQL DB]

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

Kies in hetzelfde dialoogvenster het tabblad **Handhaving**.

- Handhavingsbeleid: WLC Cisco-gastentoekenning

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]

Kies in hetzelfde dialoogvenster het tabblad **Handhaving**.

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**

## Configuratie van ClearPass-webauth-services

Navigeer naar **ClearPass > Handhaving > Beleid > Toevoegen**.

-Name: Guest\_Portal\_Webauth

-Type: Web gebaseerde verificatie

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...			

In dezelfde dialoog, onder het tabblad **Handhaving**, het Handhavingsbeleid: Cisco WLC-webauth voor handhavingsbeleid.

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 <a href="#">Modify</a>			<a href="#">Add New Enforcement Poli</a>
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 - Web Login

Gebruik voor de pagina Anonymous AUP Guest Portal één gebruikersnaam zonder wachtwoordveld.

De gebruikersnaam die wordt gebruikt, moet deze velden bevatten:

gebruikersnaam\_adres | Gebruikersverificatie: | 1

Om het 'gebruikersnaam\_auth' veld voor een gebruiker in te stellen, moet dat veld eerst worden weergegeven in het 'bewerken gebruiker' formulier. Navigeer naar **ClearPass > Gast > Configuratie > Pagina's > Formulieren**, en kies **Create\_user** form.

Home » Configuration » Pages » Forms

### Customize Forms

Use this list view to customize the forms within the application.

Name	Title
<b>change_expiration</b> Change the expiration time of a single guest account.	Change Expiration
<b>create_multi</b> Create multiple guest accounts.	Create Multiple Guest Accounts
<b>create_multi_result</b> Create multiple accounts results page.	Create Multiple Accounts Results
<b>create_user *</b> Create a single guest account.	Create New Guest Account
<a href="#">Edit</a> <a href="#">Edit Fields</a> <a href="#">Reset to Defaults</a> <a href="#">Duplicate</a> <a href="#">Show Usage</a> <a href="#">Translations</a>	
<a href="#">Launch</a> <a href="#">Edit Fields</a>	
<b>create_user_receipt</b> Create single guest account receipt.	Create New Guest Account Receipt
<b>guest_edit</b>	

Kies **visitor\_name** (rij 20) en klik op **Insert After**.

Home » Configuration » Pages » Forms

### Customize Form Fields (create\_user)

Use this list view to modify the fields of the form **create\_user**.

Quick Help Preview Form

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	<b>visitor_name</b>	text	Guest's Name:	Name of the guest.

[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>
<b>Form Display Properties</b> <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>
<b>Form Validation Properties</b> <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>

Maak nu de gebruikersnaam om achter de AUP Guest Portal pagina te gebruiken.

Ga naar **CPPM > Gast > Gast > Account beheren > Aanmaken**.

- Naam gast: WiFi
- Bedrijfsnaam: Cisco-software
- E-mailadres: guest@example.com
- Gebruikersverificatie: Geef gasttoegang met alleen het gebruik van hun gebruikersnaam: Ingeschakeld
- Accountactivering: Nu
- Accountverloop: De account is niet verlopen
- Gebruiksvoorwaarden: Ik ben de sponsor: Ingeschakeld

## 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:	<b>281355</b>
Notes:	<input type="text"/>
* Terms of Use:	<input checked="" type="checkbox"/> I am the sponsor of this account and accept the <a href="#">terms of use</a>
<input type="button" value="Create"/>	

Aanmeldingsformulier voor web maken Navigeer naar **CPPM > Gast > Configuratie > Weblogs**.

De Endpoint Attributes in de sectie na de auditie:

username | Gebruikersnaam  
bezoeker\_naam | Naam bezoeker  
kannen | Naam bezoeker  
bezoeker\_telefoon | Telefoon bezoekers  
email | E-mail  
post | E-mail  
sponsor\_name | Naam sponsor  
sponsor\_email | E-mail sponsor  
**Allow-Guest-Internet | waar**





In het CPPM navigeer je naar **Live Monitoring > Access Tracker**.

De nieuwe gast gebruiker die verbindt en activeert MAB Service.

Tabblad **Samenvatting**:

**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**

Navigeer in hetzelfde dialoogvenster naar het tabblad **Invoer**.

**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**

Navigeer in hetzelfde dialoogvenster naar het tabblad **Uitvoer**.

**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**

## Bijlage

Voor referentiedoeleinden wordt hier een toestandsstroomdiagram weergegeven voor de



## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.