# 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 Netwerkdiagram 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 <u>https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-</u> 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-verificatieomzeilingsprofiel (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 routeringstabel (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 popupportaal 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 Gastenportal

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



# Netwerkdiagram

**Opmerking:** Voor de proefdemo-doeleinden wordt een enkele/gecombineerde Aruba CPPM Server-instantie 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: X000L0000L0000	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
AP MAC: X000KJ000KJ000K	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)
			5GHz Band RF: Typical_Client_Density_rf_5gh
	RF Tag: Branch_RF		2GHz Band RF: Typical_Client_Density_rf_2gh

# Draadloze gasttoegang tot C9800-parameters configureren

C9800 - AAA-configuratie voor gasten

**Opmerking:** Over Cisco bug-id <u>CSCvh03827</u>, 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*	СРРМ		
Server Address*	10.85.54.98	]	
PAC Key			
Кеу Туре	Clear Text 🔻	)	
Key* (i)		]	
Confirm Key*		]	
Auth Port	1812	]	
Acct Port	1813	]	
Server Timeout (seconds)	5	]	
Retry Count	3	]	
Support for CoA			
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 Serve	r Group	>
Name*	AAA_Radius_CPPM	
Group Type	RADIUS	
MAC-Delimiter	none	
MAC-Filtering	none 🔹	
Dead-Time (mins)	5	
Source Interface VLAN ID	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*	AAA_Authz_CPPM						
Type*	network 🔹						
Group Type	group v i						
Fallback to local							
Authenticated							
Available Server Groups	Assigned Server Groups						
radius Idap	> AAA_Radius_CPPM						
tacacs+							
Cancel	Apply to Device						

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 Accounti	ng		×
Method List Name* Type*	AAA_Accounting_CP	PPM	
Available Server Groups	Assigned	d Server Groups	
radius Idap tacacs+	> < >> «	AAA_Radius_CPPM	
Cancel			Apply to Device

#### C9800 - Redirectie-ACL configureren

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.

Sequence 🗸	Action ~	Source vi IP	Source v Wildcard	Destination ~ IP	Destination ~ Wildcard	Protocol 🖂	Source V Port	Destination ~ Port
1	deny	any		site		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

• ACE-nr. 150: AI HTTP-verkeer (UDP-poort 80) wordt omgeleid.

# 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				×
Ge	neral Security	Advanced			
	Profile Name*	WP_Guest	Radio Policy	All	
	SSID*	Guest	Broadcast SSID		
	WLAN ID*	3			
	Status	ENABLED			

Cancel	Apply to Device

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)

Α	dd WLAN					×
	General	Security	Advanced			
	Layer2	Layer3	ААА			
	Layer 2 Sec	urity Mode		None	Lobby Admin Access	
	MAC Filterin	na			Fast Transition	Adaptive Enab 🔻
		.9			Over the DS	
	OWE Transit	tion Mode			Reassociation Timeout	20
	Transition M	lode WLAN II	D*	1-4096		
	Authorizatio	n List*		AAA_Authz_C		
	Cancel	]				Apply to Device

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					×
Gen	Access Policies	QOS and AVC	Mobility	Advanced		
	A Configurir	ng in enabled state will re	esult in loss of co	nnectivity for clients associated with	this profile.	
	Name*	PP_Guest		WLAN Switching Policy		
	Description	Policy Profile for G	iuest	Central Switching	DISABLED	
	Status	ENABLED		Central Authentication	ENABLED	
	Passive Client	DISABLED		Central DHCP	DISABLED	
	Encrypted Traffic Analytics	DISABLED		Central Association	DISABLED	
	CTS Policy			Flex NAT/PAT	DISABLED	
	Inline Tagging					
	SGACL Enforcement					
	Default SGT	2-65519				
C	Cancel				Apply to Dev	rice

Add Polic	y Profile	e						×
		A Configuri	ng in enabled state wil	I result in loss o	f conr	nectivity for clients associated with t	his profile.	
General	Acces	s Policies	QOS and AVC	Mobility	Ad	vanced		
Name*	r		PP_Guest			WLAN Switching Policy		
Descri	ption		Profile for Branch	Guest		Central Switching	DISABLED	
Status			DISABLED			Central Authentication	ENABLED	
Passive	e Client		DISABLED			Central DHCP	DISABLED	
Encryp	ted Traffic	c Analytics	DISABLED			Central Association	DISABLED	
CTS F	Policy					Flex NAT/PAT	DISABLED	
Inline T	lagging							
SGACL	Enforcer	ment						
Default	t SGT		2-65519					
Cance	1						Apply to De	evice

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 <u>CSCvn48234</u> zorgt ervoor dat SSID niet wordt uitgezonden als dezelfde Flex guest VLAN wordt gedefinieerd onder WLC en in het Flex Profile.

	ing in enabled state will result in loss of connectivity	for clients associated with this profile.	
eneral Access Policies	QOS and AVC Mobility Advanced		
RADIUS Profiling		WLAN ACL	
HTTP TLV Caching		IPv4 ACL Search or Select	
DHCP TLV Caching		IPv6 ACL Search or Select	
WLAN Local Profiling		URL Filters	
Global State of Device Classification	í	Pre Auth Search or Select	
Local Subscriber Policy Name	Search or Select	Post Auth Search or Select 🗸	
VLAN			
VLAN/VLAN Group	210 🔹		
Multicast VLAN	Enter Multicast VLAN		

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

Apply to Device

- AAA negeren toestaan: Ingeschakeld
- Staat NAC: Ingeschakeld
- NAC-type: STRAAL

Cancel

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

#### Add Policy Profile

A Config	uring in enabled state will	l result in loss (	of connectivity for clients associated with this profile.
General Access Policies	QOS and AVC	Mobility	Advanced
WLAN Timeout			Fabric Profile     Search or Select
Session Timeout (sec)	1800		mDNS Service Search or Select
Idle Timeout (sec)	300		Hotspot Server Search or Select 🔻
Idle Threshold (bytes)	0		User Defined (Private) Network
Guest LAN Session Timeout (sec)	60		Status
DHCP			Drop Unicast
			Umbrella
IPv4 DHCP Required DHCP Server IP Address			Umbrella Parameter Map
how more >>>			Flex DHCP Option ENABLED
AAA Policy			DNS Traffic Redirect
Allow AAA Override	<ul> <li>Image: A start of the start of</li></ul>		WLAN Flex Policy
NAC State	<ul> <li>Image: A set of the set of the</li></ul>		VLAN Central Switching
NAC Type	RADIUS	•	Split MAC ACL Search or Select 🔹
Policy Name	default-aaa-policy	× v	Air Time Fairness Policies
Accounting List	AAA_Accounting_(	• • ×	2.4 GHz Policy Search or Select

**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*	PT_CAN01		
Description	Policy Tag for CAN01		
VULAN-POLICY	′ Maps: 0		
+ Add $ imes$ Dele	ete		
WLAN Profile		<ul> <li>Policy Profile</li> </ul>	₩.
	10 🔻 items per page		No items to display
Map WLAN and Pol	icy		
WLAN Profile*	WP_Guest	Policy Profile*	PP_Guest
RLAN-POLICY	Maps: 0		
් Cancel			Apply to Device

## 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 Jo	oin Profile								×
General	Client	CAPWAP	AP	Management	Sec	urity	ICap	QoS	
Name*		Branch	_AP_Prof	ile		Office	Extend A	P Configuratio	on
Descrip	otion	Branch	AP Join	Profile		Local	Access	~	
LED Sta	ate	~				Link Ei	ncryption	~	
LAG M	ode					Rogue	Detection		
NTP Se	erver	10.0.1	0.4						
GAS A	P Rate Limit								
Apphos	st								
Cancel									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 APbeheerinterface wilt hebben)

Add Flex Profile			×
General Local Authentica	ation Policy ACL V	'LAN Umbrella	
Name*	FP_Branch	Fallback Radio Shut	
Description	Branch Flex Profile	Flex Resilient	
Native VLAN ID	10	ARP Caching	
HTTP Proxy Port	0	Efficient Image Upgrade	
HTTP-Proxy IP Address	0.0.0.0	OfficeExtend AP	
CTS Policy		Join Minimum Latency	
Inline Tagging		IP Overlap	
SGACL Enforcement		mDNS Flex Profile	Search or Select
CTS Profile Name	default-sxp-profile x		
Cancel			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.

Add Flex P	rofile		×
General	Local Authentication	Policy ACL VLAN Umbrella	
+ Add	X Delete		
ACL Nan	ne v	Central Web Auth  V Filter  Pre Auth URL  V ACL Name*  CAPTIVE_PORTAL_F V	
H 4	0 ⊳ ⊳ 10 <b>v</b> it	tems per page No items to display Central Web Auth	
		Pre Auth URL Filter Search or Select	
		✓ Save ⊃ Cancel	
Cancel		🗎 Apply to Device	

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

Add Flex Profile		×
General Local Authentication Policy ACL	AN Umbrella	
+ Add × Delete		
VLAN Name v ID v ACL Name	× •	
data 2	VLAN Name* guest	
I → I → I IO → items per page	VLAN Id* 210	
1 - 1 of	1 items ACL Name Select ACL	
	Save	
"D Cancel		ly to Device

## 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 C	A
AP Join Profile	Branch_AP_Profile	•
Flex Profile	FP_Branch	•
Fabric Control Plane Name		•
Enable Local Site		
Cancel		

## 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)



## 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 zeerste 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		

**Opmerking:** Als u de op AP-name 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 × A Rule "BR-CAN01" has this priority. Assigning it to the current rule will swap the priorites. BR\_CAN01 PT\_CAN01 Rule Name\* ×т Policy Tag Name BR-CAN01-.{7} AP name regex\* ST\_CAN01 Site Tag Name ×т YES Active Branch\_RF ×v **RF** Tag Name 1 Priority\* 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)

System	Services Control	Service	Parameters	System Monitori	ng Network	FIPS		
Hostname	:		cppm					
FQDN:			cppm.example.	com				
Policy Man	ager Zone:		default	v)				Manage
Enable Per	formance Monitoring I	Display:	🗹 Enable this	server for perform	ance monitoring	display		
Insight Set	tting:		🗸 Enable Insi	ght 🔽	Enable as Insig	ht Master	Current Master:cppm(10.85.54.98)	
Enable Ing	ress Events Processin	g:	🗌 Enable Ingr	ess Events proces	sing on this serv	er		
Master Ser	ver in Zone:		Primary maste	r v				
Span Port:			None	~				
					IPv4		IPv6	Action
		IP Addr	ess		10.85.54.98			
Managem	ent Port	Subnet	Mask		255.255.255.224	1		Configure
		Default	Gateway		10.85.54.97			
		IP Addr	ess			_		
Data/Exte	ernal Port	Subnet	Mask					Configure
		Default	Gateway					
		Primary			10.85.54.122			
DNS Setti	nas	Second	ary					Configure
Dito Setti	1193	Tertiary						Configure
		DNS Ca	ching		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		8
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:	🗹 EAP 🗹 RadSec 🔽 Database 🔽 Others	
	Update Disable Export Close	e

Stap 2. Maak een aanvraag voor certificaatondertekening aan.

Navigeer naar Beheer > Certificaten > Certificaatopslag > Servercertificaten > Gebruik: HTTPSservercertificaat.

- 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):	Create Certificate Signing Request					
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					

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		8
Certificate Type:	Server Certificate	
Server:	Cppm v	
Usage:	HTTPS Server Certificate	
Upload Method:	Upload Certificate and Use Saved Private Key V	
Certificate File:	Browse No file selected.	
	Import	Cancel

## 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 SNM				
	P Write Settings CLI Setting	s OnConnect Enford	cement Attributes	
ame:	WLC_9800_Branch			
P or Subnet Address:	10.85.54.99 (	e.g., 192.168.1.10 or	192.168.1.1/24 or 19	92.168.1.1-20)
escription:	Cisco 9800 <u>WLC</u> for Branch G	uest <u>Wifi</u>		
ADIUS Shared Secret:		Verify:		
ACACS+ Shared Secret:		Verify:		
endor Name:	Cisco			
nable RADIUS Dynamic Authorization:	✓ Port: 1700			
nable RadSec: [				

# Pagina en CoA Timers

Het is zeer belangrijk om de juiste tijdopnemerwaarden 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'.

Add

Cancel

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 C 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 clientendpoint 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 handhavingsbeleid 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

				010	un uss	I Olicy	Manager	
Dashboard 0	Administrati	ion » Server Manag	er » Server Configuratio	n - cppm				
Monitoring O	Server (	Configuration	- cppm (10.85.	54.98)				
Configuration 0		J		,				
🔐 Administration 📀								
- 🥜 ClearPass Portal								
B Service and Privileges	System	Services Control	Service Parameters	System Monitoring	Network	FIPS		
Server Manager      Server Configuration	Select Servi	ice:	sync network services	<b>v</b>				
- Jog Configuration			Paramete	er Name			Parameter Valu	le
Local Shared Folders     Iconsing	Ingress Ev	ent						
Device Insight	Batch Proce	essing Interval					30	seconds
- Contract Servers	Command	Control						
- J External Accounts	RADIUS Dy	namic Authorizatio	n (DM/CoA) Delay				6	seconds
🖃 🚔 Certificates	Enable SNN	IP Bounce Action					FALSE ~	
Certificate Store	Post Auth							
- Ja Trust List	Number of	request processing	threads				20	threads
Revocation Lists	Lazy handle	er polling frequency	/				5	minutes
Agents and Software Updates	Eager hand	fler polling frequent	-y				30	seconds
	Connection	Timeout					10	seconds
	Palo Alto U	ser Identification T	meout				45	minutes

# 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 Al Guest-Internet = TRUE, sta he op het netwerk. Anders, trigge Redirect en COA: Verifiëren.
2. Gast	Weblogins	Presenteer Anonymous login A pagina. Post-auth ingestelde aangepas attribuut <b>Allow-Guest-Internet</b> TRUE.
3. Beleidsmanager	Service: Web gebaseerde verificatie	Eindpunt bijwerken naar <b>beke</b> r Eigen kenmerk <b>Allow-Guest-In</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.

Edi	t Endpoint		8
	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	
Descriptior	1:		//.
Type:		RADIUS_CoA	
Action:		Accept O Reject O Drop	
Device Gro	oup List:		Remove View Details Modify
		Select	<ul> <li></li> </ul>
Straal:IETF		Bel-station-id	%{RADIUS:IETF:Calling-statio
Straal:Cisco	)	Cisco AVPair	abonnee:opdracht=reauthentic
Straal:Cisco	)	Cisco AVPair	%{Straal:Cisco:Cisco- AVPair:abonnee:audit-sessie-i
Straal:Cisco	)	Cisco AVPair	abonnee:reauthenticate-type= 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:			///.
Гуре:		RADIUS	
Action:		💿 Accept 🔘 Reject 🔘 Drop	
Device Group	) List:		Remove
			View Details
			Modify
		Select	$\cdot$

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				
	Туре		Name		Value	
1	. Radius:Cisco		Cisco-AVPair	-	url-redirect-acl=CAPTIVE_PORTAL_REDIRECT	6
2	. Radius:Cisco		Cisco-AVPair	-	url-redirect=https://cppm.example.com/guest/laccept.php?cmd- login&mac=%{Connection:Client-Mac-Address-Hyphen}&switchip=% {Radius:IETF:NAS-IP-Address}	60



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, <u>https://cppm.example.com/guest/iaccept.php</u>
- 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 navigeert.

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.



**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
Descriptior	1:	
Туре:		Post_Authentication
Action:		Accept O Reject O Drop
Device Gro	oup List:	Remove         View Details         Modify

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

Co	Configuration » Enforcement » Profiles » Add Enforcement Profile				
Er	nforcement Pro	files			
Р	Profile Attributes	Summary			
	Туре		Name	Value	
1.	Type Endpoint	•	Name Allow-Guest-Internet	Value = true	•

#### 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

Configuration » Enforcement » Policies » Add

Enforcemer	nt Polici	S	
Enforcement	Rules	ummary	
Name:		NLC Cisco Guest Allow	
Description:		<u>lin</u>	
Enforcement Typ	e:	● RADIUS D TACACS+ ○ WEBAUTH (SNMP/Agent/CLI/CoA) ○ Applicatio	n 🔿 Event
Default Profile:		Cisco_Portal_Redirect ✓ View Details Modify	

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					8
	c	onditions			
Match ALL of the following of	conditions:				
Туре	Name	Operator	Value		
1. Endpoint	<ul> <li>Allow-Guest-Internet</li> </ul>	EQUALS	true	-	<b>D</b> 🕆
2. Click to add					
	Enforce	ement Profiles			
Profile Names:	[RADIUS] [Allow Access Profile]				
	Move Up ↑				
	Move Down ↓				
	Remove				
	Select to Add	~			
1				Court	Connect
				Save	Cancel

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

Configuration » Enforcement » Policies » Add

#### **Enforcement Policies**

Enforcement	Rules	Summary
Name:		Cisco WLC Webauth Enforcement Policy
Description:		
Enforcement Typ	e:	○ RADIUS ○ TACACS+
Default Profile:		[RADIUS_CoA] Cisco_Reauti v View Details 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 followin	ng conditions:			
Туре	Name	Operator	Value	
1. Authentication	Status	EQUALS	User	Ba #
2. Click to add				
		Enforcement Profiles		
Profile Names:	[Post Authentication] [Update Endpoint Known]			
	[Post Authentication] Make-Cisco-Guest-Valid	Move Up ↑		
	[RADIUS_CoA] Cisco_WLC_Guest_COA	Move Down ↓		
		Remove		
	Select to Add			
		•		
				Save Cancel

**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.

Confi	guration » Services » A	Add									
Ser	vices										
Ser	vice Authentication	Authorization	Roles	Enforcement	Profiler	Summary					
Туре	Type: MAC Authentication										
Nam	e:	GuestPortal - Mac A	uth								
Desc	iption:	MAC-based Authen	tication	Service							
Moni	or Mode:	Enable to monito	or networ	k access without	enforcemen	t					
More	Options:	Authorization	Audit E	nd-hosts 🗹 Pro	ile Endpoint	s [ ] Account	ting Proxy				
						Serv	ice Rule				
Match	nes 🔘 ANY or 💿 ALL	of the following co	nditions:								
	Туре		Na	ame			Operator		Value		
1.	Radius:IETF		NA	S-Port-Type			BELONGS_TO		Ethernet (15), Wireless-802.11 (19)	66)	Û
2.	Radius:IETF		Se	rvice-Type			BELONGS_TO		Login-User (1), Call-Check (10)	6 <u>0</u>	8
3.	Connection		CI	ent-Mac-Address			EQUALS		%{Radius:IETF:User-Name}	60	Ť
4.	Radius:Cisco		Ci	sco-AVPair			EQUALS		cisco-wlan-ssid=Guest	6	÷

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						
Dashboard 0	Configuration	» Services	» Edit - GuestPort	al - Mac Auth			
Monitoring 0	Services	- Guest	Portal - Mac	Auth			
😤 Configuration 📀	Summary	Service	Authentication	Authorization	Roles	Enforcement	Profiler
—  Service Templates & Wizards —  Services	Authentication	n Methods:	[Allow All MAC A	ОТН]		Moyo Up 1	
Authentication						Move Down ↓ Remove	]
☆ Sources ☆ Identity ☆ Single Sign-On (SSO) ☆ Local Users						View Details Modify	]
- 🎲 Endpoints - 🎲 Static Host Lists - 🎲 Roles - 🎲 Role Mappings	Authentication	n Sources:	[Endpoints Repo [Guest User Rep	sitory] [Local SQL D pository] [Local SQL	B] DB]	Move Up ↑ Move Down ↓	]
<ul> <li></li></ul>	I					Remove View Details Modify	) )
☆ Profiles ⊒-••• Network			Select to Add-			<ul> <li>✓</li> </ul>	J
- Contraction of the second se	Strip Usernam	ne Rules:	Enable to sp	ecify a comma-se	parated li	st of rules to strip	o username prefixes or suffixes

## Kies in hetzelfde dialoogvenster het tabblad Handhaving.

#### - Handhavingsbeleid: WLC Cisco-gastentoekenning

Configuration » Services » Add

#### Services

Service Authentic	ation Roles Enforcemen	t Summary	
Use Cached Results:	Use cached Roles and	Posture attributes from pre	vious sessions
Enforcement Policy:	WLC Cisco Guest Allow	✓ Modify	
			Enforcement Policy Details
Description:	MAB Enforcement Redire	ect	
Default Profile:	Cisco_Portal_Redirect		
Rules Evaluation Algor	thm: first-applicable		
Conditions			Enforcement Pro
1. (Endpoint:Allo	v-Guest-Internet EQUALS tru	e)	[Allow Access Pro

Kies in hetzelfde dialoogvenster het tabblad Handhaving.

Configuration » Services » Add

# Services

Service	Authentication	Authorization	Roles	Enforcemen	Profiler	Summary	
Endpoint Cl	assification:	Select the classifica	ation(s) af	ter which an a	ction must be	e triggered -	
RADIUS Co.	A Action:	Cisco_Reauthentica	te_Sessio	า	View Det	ails Modify	

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

-Name: Guest\_Portal\_Webauth

-Type: Web gebaseerde verificatie

Configuration » Services » Add

# Services

Ser	vice	Authentication	Roles	Enforcement	Summary		
Type:			Web-based	d Authentication		~	
Name	e:		Guest				
Descr	iption:						
Monit	or Moo	le:	🗌 Enable t	o monitor networ	k access with	out enforcement	
More	Optior	IS:	Authorization Posture Compliance				
						S	
Match	ies ()	ANY or 🧿 ALL	of the follo	wing conditions:			
	Туре			Na	ame		
1.	Host			Ch	neckType		
2.	Click	to add					

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

Configurat	on » Services » A	dd					
Service	S						
Service	Authentication	Roles	Enforcement	Summary			
Use Cache	d Results:	Use cach	hed Roles and Po	sture attribute	es from previo	ious sessions	
Enforceme	nt Policy:	Cisco WLC	Webauth Enforce	ment Policy	✓ Modify	1	Add New Enforcement Pol
						Enforcement Policy Detail	i
Description	1:						
Default Pro	ofile:	Cisco_Rea	uthenticate_Ses	sion			
Rules Eval	uation Algorithm:	first-applie	cable				
Con	ditions						Enforcement Profiles
1. (A	uthentication:Stat	us EQUALS	S 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.

aruba	Cle	earPass Guest
🚆 Guest 🛛 0	Home » Configuration » Pages » Forms	
👔 Devices 🔹 📀	Customize Forms	
Configuration	Use this list view to customize the forms within the applic	ation.
- 🃚 Authentication	△ Name	Title
Content Manager	change_expiration Change the expiration time of a single guest account.	Change Expiration
- Public Files	create_multi Create multiple guest accounts.	Create Multiple Guest Accounts
- 🛃 Guest Manager 🖅 🎭 Hotspot Manager	create_multi_result Create multiple accounts results page.	Create Multiple Accounts Results
Pages	Create a single guest account.	Create New Guest Account
	Edit Fields     Constant Fields     Constant Fields     Edit Fields     Edit Fields     Edit Fields	e 🍕 Show Usage 🍇 Translations
Self-Registrations	create_user_receipt Create single guest account receipt.	Create New Guest Account Receipt
- 🏰 Web Logins	🚍 quest edit	

#### 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.

<b>(</b> ) Q	uick Help			Preview Form
A Rank	Field	Туре	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.
E E	dit  🚡 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:	username_auth
Form Display Prope These properties control the	user interface displayed for this field.
Field:	Enable this field When checked, the field will be included as part of the form.
* Rank:	22 Number indicating the relative ordering of user interface fields, which are displayed in order of increasing rank.
* User Interface:	No user interface   Revert  Revert Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Revert  Rev
Form Validation Pro	operties the value of this field is checked.
Field Required:	Field value must be supplied Select this option if the field cannot be omitted or left blank.
Initial Value:	Revert Control of the form is first displayed.
* Validator:	IsValidBool   The function used to validate the contents of a field.
Validator Param:	(None)  V Optional name of field whose value will be supplied as the argument to a validator.
Validator Argument:	
Validation Error:	The error message to display if the field's value fails validation and the validator does not return an error message directly.

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

ruba		ClearPass Guest
Guest 0		Web Login Editor
Onboard 0	* Name:	briter a name for this web login page.
Configuration 0	Page Name:	Works Thife you page same for this with tagin. The web lags will be assessable from "Aparelia".
Authentication Content Heneper		
Private Files	Description:	
Guest Manager	B Magnine Bull	Conversions or descriptive level admost life web legils.           Avaba Webwarka         w)
Hotapet Menager	- Ventor Settings:	Sector a presidente prograf de son en estado de estado en estad
Pages	Legin Method:	and we have a set of the second secon
Torms	Page Redirect	anne mississi tigine regine the carre rec accrete to be avenue, closely non the capity pond nemector preces.
List Views	that see for specifying pa	Constant passed in the initial reduced.
Web Logins	becarity wash-	Release the invest of shoulding in apply to URL parameters parameters proved in the each legic page. The first optime to obtain when URL parameters have tenso modified by the user, for example their NAC address.
- Reb Pages	Login Form	
SHS Services	chosed on theory of a	Anarymeur - De tet repuire a username ar password
Translations	Automotion:	Sider the sufferingsfor repurerail. Roces Cade requires a single code Supername) to be ordered.
		Acts is similar to another both form the set of the time of a log in action in pre-instance exposes, or repurso, Acts is similar to another has been in actionational submetically submetical.
	Auto-Generater	Create a new anonymous assount
		The address we as characterized a second a second meric or regeneration may and meric the second meric (or a). Inter a value for "Weinprince Deer" to use a specific username, or have been to randomly generate a username.
	* Ananymous Users	Ourself in car for a surgement addressing in.
		The presence we are vision when the result. Tender Limit in the number of parals you with in support.
	Prevent CNA:	Enable bypassing the Apple Captive Network Assistant     The Rook Captive Network Assistant (DWC) is the pap-up breven shown when bining a network that has a captive portal.
kéministration é		Note that this option may not work with all vendors, depending on how the captive pertail is implemented.
	Quatom Form:	E' selected, you must supply your own HTHL legit form in the Headler or Foster HTHL areas.
	Curtore Labele:	Overvide the default labels and error messages     Fiseleded, yos will be able to other labels and error messages for the summit legit form.
	* Pro-Auth Check:	Lacal — match a local account v Select how the username and passwort sheald be checked before proceeding to the Md authentication.
	Pro-Auto-Environment	The leaf in discher 2 file constants and assessed linders P <sup>24</sup>
	- comment article	Lauve Mark to use the default (Invalid usersame or password).
	Terma:	Require a Terms and Conditions confirmation If shocked, the user will be forced to accept a Terms and Candilians shocked.
	Terma Label:	The form label for the tarms checkley.
		Lawe Mark to use the default (Yerma ).
	Terris Text)	
		WTML code certaining your Terms and Ecneticons.
		Laws Mark to use the default () accept the via head-"(sea, global name-point, account, terms, of, one, or ()" target-", (Seal"-Searce of one v/or).
	Terma Layout:	Exception tention formations we be a send thank beat.
	Terms Errori	The text to display if the tarres are not accepted.
	Charles and	Leave blank to use the default (In order to leg in, yes must accept the terms and conditions ).  None
	GPTCHC	amongot and command
	Leg to Label I	The form table for the lag in status. Leave black to use the default (Leg In).
	Translations	Skip automatic translation handling
	Default Destination	These needs and pages have transitions available under Comparation + transitions + right Custom block. Select the action of Keep an text as behavior
	Options for controlling t	hs deathnation clients will redirect to after tegin.
	* Default URL:	Entrar the Behaut LML to redirect clients. Means ensure you prepend "Http://" for any external durian.
	Override Destination:	Ports delaut destination for all clients     Ports
	Login Page	
	Options for controlling t	ClearPass Guet Skin v
	- 568	Oncose the skin to use when this web login page is displayed.
	Title:	Record and the rection of the set
		(exa_realization)
		Grad> Grad sular = 'asys'>
		GoWelsene in Daret WirFilGAD Garb
	Header HTML:	Carb Garb Clark series = "black").
		CoOfferenz and Conditions:(/Ao CoOfferenze you evolve the Terms and Conditions in the
		lish below because by observing the tisk how and extenting "Register", you are confirming that you've
		Inset. •
		(tow_text_ide?)(3) apr
		connect a start definer if you are experienting difficulty legging in. N/or(/ne tast)
		a second se
	* Lagin Delayi	and the end of the delay while displaying the legit message.
	Advertising Services	end are then logics pages.
	Advertising	Drable Advertising Services content
	Clead Identity Optimally present quest	ts with warkes dout identity / social login cotions.
	Enabled:	Invable lages with clear lifestity / social network codestant.
	Hulti-Paster Authen Repute a secondary fac	disation So when sub-intesting.
	Provideri	No multifactor authorization v
	metwork Login Acce Certifols access to the Is	dia tadar 198
	Allowed Access:	
		Enter the IP addresses and networks from which lepine are permitted.
	Denied Jaconse	
	0-0-160 PR02880	a true to the determine and reduceds that, are denied large access.
	T Description of	Bend HTTP 404 Net Found states v
	Post-Authentication	Rabel the request of the system in a request that is not preveiled.
	Autors to perform after	a waaanala jee walkeelinatan.
	Health Check	In Angurs a successful Ondeated health check and to accessing the edwark. If selected, the successful be required to case a health check and to accessing the edwark.
	Update Endpoint:	Naik the user's Mic address as a known endpand their details from the endpoint's stributer will also be updated with other details from the user account.
	Advanced	Contamize ethtilates stored with the endpoint
		Visiter_seme   Visiter Seme
	Endpoint Altributes:	en   Wisitor Hemo Visitor None   Visitor Hemo
		Ust of nemalvalue pairs to pass along.

Verificatie - Guest CWA-autorisatie

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

De nieuwe gast gebruiker die verbindt en activeert MAB Service.

### Tabblad Samenvatting:

l

Request Details								
Summary Input O	atput 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							
I ≤ Showing 8 of 1-8 record	ds ► ► Change Status Show Configuration Export Show Logs Close							

Navigeer in hetzelfde dialoogvenster naar het tabblad Invoer.

Request Details								
Summary Input	Output R/	ADIUS CoA						
Username: d43b047a647b		7b						
End-Host Identifier:	d4-3b-04-7a-	-64-7b (Computer / Windows / Windows)						
Access Device IP/Port:	10.85.54.99:7	73120 (WLC_9800_Branch / Cisco)						
RADIUS Request			$\odot$					
Radius:Airespace:Air	respace-Wlan-Ic	d 4						
Radius:Cisco:Cisco-A	VPair	cisco-wlan-ssid=Guest						
Radius:Cisco:Cisco-A	VPair	client-iif-id=1728058392						
Radius:Cisco:Cisco-A	VPair	method=mab						
Radius:Cisco:Cisco-A	VPair	service-type=Call Check						
Radius:Cisco:Cisco-AVPair		vlan-id=21						
Radius:Cisco:Cisco-AVPair		wlan-profile-name=WP_Guest						
Radius:IETF:Called-S	Station-Id	14-16-9d-df-16-20:Guest						
Radius:IETF:Calling-	Station-Id	d4-3b-04-7a-64-7b						
I ◄ 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			
Inforcement	Profiles:	Cisco_Po	rtal_Redirect			
System Postu	re Status:	UNKNOW	N (100)			
Audit Posture Status: UN		UNKNOW	N (100)			
RADIUS Res	oonse					
Radius:Cisc	o:Cisco-AV	'Pair url-re	edirect-acl=CAPTIVE_PORTAL_REDIRECT			
Radius:Cisco:Cisco-AVPair		Pair url-r 04-7	edirect=https://cppm.example.com/guest/iaccept.php?cmd-login&mac=d4-3b- 'a-64-7b&switchip=10.85.54.99			

8

I ≤ Showing 8 of 1-8 records ► ►	Change Status	Show Configuration	Export	Show Logs	Close

# Bijlage

Voor referentiedoeleinden wordt hier een toestandsstroomdiagram weergegeven voor de

interacties van Cisco 9800 Foreign, Anchor Controller met RADIUS Server en extern gehoste Guest Portal.

	9800 Foreign-WLC Guest Portal CWA flow									
Clie	ant A	P WL	C-For	wilc-A	Inchor	DHCP	DNS	ladius	Guest	Portal(CPPM)
	[Client Assocication]									
	[1] Assoc Reg	west	+							
	Guest Client join									
			100	[MAB procedure]						
				[2]	Access-Request (sessionid+1E1E1E020000003F3F876869)	-		*		
							(3) <redirect_url> = <redirect_url> + &lt;7sessioni</redirect_url></redirect_url>			
			-	[4] Access-Accept [] <redirect url="">, <redirect acl="">] <redirec< td=""><td>T_URL&gt;: https://<copm.fpdn.com>/guest/<page_name>.php?session</page_name></copm.fpdn.com></td><td>vid+1E1E1</td><td>E020000003F3F8768696portal=194a5780)</td><td>-</td><td></td><td></td></redirec<></redirect></redirect>	T_URL>: https:// <copm.fpdn.com>/guest/<page_name>.php?session</page_name></copm.fpdn.com>	vid+1E1E1	E020000003F3F8768696portal=194a5780)	-		
	(5) Assoc Resp	onse	_							
			-	[6] Export Anchor Request [ <redirect url="">, <redirect acl="">, <vlan>]</vlan></redirect></redirect>						
				[7] Export Anchor Response						
				Foreign: Client goes to run state. Traffic is forwarded on Mobility Tunnel (CAPWAP)						
100	(External WebAuth)		-					-		_
				[8] Redirect ACL enforcement for Client <mac_addr></mac_addr>	-					
E ST	[Client IP DHCP Process]		+		•	÷				
			1		Client goes to DHCP-Required state					1
			1							
				REDIRECT_ACL 'deny' statement allows DHCP, DNS, TCP80 to Guest Portal						
	[9] DHCP Hand	shake		[10] DHCP Handshake	[11] DHCP Handshake	+				
			1	[12] <ip_opdate> MSG: <client go<="" td=""><td></td><td></td><td></td><td></td><td></td><td></td></client></ip_opdate>						
			1		Client goes to webauth pending state					
	Client OS Guest Portal Detection	1				-	-			
	[13] DNS Query www.msftconn	ecttest.com (CAPWAP)	+	[14] DNS Query (CAPRIAP)	[15] 0%5 Query	_	•			
	[18] DNS Response www.ms/tconnecttest	com is at IP <x x=""> (CAPWA</x>	P) 🖣	[17] DNS Response	[16] DNS Response	-				
1	[19] TCP STN IP <x.x.x.>:8</x.x.x.>	0 (msftconnecttest)	*	(20) TCP SYN (CAPWAP)						1
					Anchor: «REDIRECT_ACL>: redirect enforced					
	[22] TCP SYN-AC	CRIACK		[21] TCP SYN-ACK/ACK speefing <x.x.x.x> (WebAuth <global> VIP)</global></x.x.x.x>						
	[23] HTTP GET http://www.msftconn	ecttest.com/connecttest.txt	+	[24] HTTP GET (CAPWAP)						
	The HULL HAVE REPARED CONTRACTOR	POPULICIPANI KALDIALCI DALA	+	[2] (1153) (Server)						1
	Display Pseudo Browsel									
-	[27] DNS Query <red< td=""><td>RECT URL&gt;</td><td></td><td>[28] DNS Query (CAPWAP)</td><td>[29] DNS Query</td><td></td><td>•</td><td></td><td></td><td></td></red<>	RECT URL>		[28] DNS Query (CAPWAP)	[29] DNS Query		•			
	[32] DNS Response <redirect< p=""></redirect<>	URL> is at P <y y=""></y>	-++	[31] DNS Response (CAPWAP)	[30] DNS Response	_	-			
	Client must trust Guest Portal certificate		1							1
			1		Anchor: <redirect acl="">: redirect bypass <vvv.vvv> (Guest Porta</vvv.vvv></redirect>	ъ				
	1331 Guest Portal CERE TCE SYNSIN AC	KACK of a strategy of Alward		DALTER-STREET ACKACK (CAPWAR)		-	1351 TOP SYNSTEMACKACK			
	(36) HTTP GET «REDIRECT	r URL?sessionid>	T	[37] HTTP GET (CAPWAP)			[38] HTTP GET			1
	[41] HTTP/1.1 2	99.0K	1	[40] HTTP/1.1 200 OK (CAPWAP)	1		[39] HTTP:1.1.200 OK			1
	Client clicks 'Accept' AUP button									
	[42] HTTP POST/HTTP	P1.1 200 OK		[43] HTTP POST/HTTP1.1 200 OK			[44] HTTP POSTHITTP1.1 200 OK			
			1					[45] Update	Endpoint D8: <client_mac>:AllowInternetAccess=</client_mac>	True
									[46] Captive Portal page refresh o	lelay
			alt	(CoA Reauth)				-		-
							[47] CoA delay tim	-		
					40] CoA Request (Type= <reauthenticate>, <sessionid>)</sessionid></reauthenticate>					
			1		[49] CoA Ack ( <sessionid>)</sessionid>	-		•		
			1	[MA8]						
			H		[30] ACCESS Request (< sessionez>) [51] Access Accest (No reviner) UBL assessmedtr)			*		
			4					7		
			F	[52] Export Archor Request						
			1	AND ADDRESS OF DESIGNATION AND ADDRESS AND ADDRESS	harden fried and have start					
					Percent Coren, goes to run state					
	•				[54] HTTP GET/HTTP 2000K Landing Page			-		+
					client goes to RUN state					
-						-				
Clie	ant A	P WL	C-For	wLC-A	Inchor	DHCP	DNS	Ladius	Guest	Portal(CPPM)

Guest Central Web Verification State Diagram met anker WLC

# Gerelateerde informatie

- Handleiding voor best practices voor Cisco 9800 implementaties
- Inzicht in Catalyst 9800 configuratiemodel voor draadloze controllers
- Begrijp FlexConnect op Catalyst 9800 draadloze controller
- Technische ondersteuning en documentatie Cisco Systems

#### 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.