Central Web Verification op geconvergeerde toegang en Unified Access WLC's configuratievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren **Topologie 1 Topologie 2 Topologie 3** Voorbeeld **Topologie 1 Configuratievoorbeeld** Configuratie op de ISE Configuratie op de WLC Configuratie-voorbeeld van topologie 2 Configuratie op de ISE Configuratie op de WLC Voorbeeld van configuratie van topologie 3 Configuratie op de ISE Configuratie op de WLC Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u centrale webverificatie kunt configureren op de geconvergeerde draadloze LAN-controller (WLC) en ook tussen de geconvergeerde access WLC en Unified Access WLC (5760 en ook tussen 5760 en 5508).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco WLC 5508, 5760, 3850
- Basiskennis van Identity Services Engine (ISE)
- Basiskennis van draadloze mobiliteit
- Basiskennis van gastverankering

Gebruikte componenten

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

- WLC 5760 die Cisco IOS[®] XE release 3.3.3 ondersteunt
- WLC 5508 Series met Cisco Aironet OS release 7.6
- Switch 3850 waarop Cisco IOS XE release 3.3.3 wordt uitgevoerd
- Cisco ISE-softwarerelease 12.2

Configureren

Opmerking: Gebruik de <u>Command Lookup Tool</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

De stroom omvat deze stappen:

- 1. De gebruiker associeert met de web verificatie Service Set Identifier (SSID), die in feite open+macfiltering en geen Layer 3-beveiliging is.
- 2. De gebruiker opent de browser.
- 3. De WLC wordt omgeleid naar de guest portal.
- 4. De gebruiker verifieert op het portaal.
- 5. De ISE stuurt een RADIUS-wijziging van autorisatie (CoA UDP-poort 1700) om de controller erop te wijzen dat de gebruiker geldig is en drukt uiteindelijk RADIUS-kenmerken zoals de toegangscontrolelijst (ACL) in.

6. De gebruiker wordt gevraagd de oorspronkelijke URL opnieuw te proberen. Cisco maakt gebruik van drie verschillende implementatieinstellingen die alle verschillende scenario's omvatten om Central Web Verification (CWA) te realiseren.

Topologie 1

De 5760 WLC werkt als een standalone WLC en de Access points eindigen op dezelfde 5760 WLC. De clients zijn verbonden met Wireless LAN (WLAN) en zijn geverifieerd op de ISE-kaart.



Topologie 2

Gastverankering tussen de geconvergeerde access WLC met een die fungeert als een Mobility Controller en de andere die fungeert als een Mobility Agent. De Mobility Agent is de Foreign WLC en de Mobility Controller is het anker.



Topologie 3

Gastverankering tussen Cisco Unified WLC 5508 en Converged Access WLC 5760/3850 met een controller die fungeert als een Mobility Controller en een controller die fungeert als een Mobility Agent. De Mobility Agent/Mobility Controller is de Foreign WLC en de 5508 Mobility Controller is het anker.



Opmerking: Er zijn veel implementaties waarbij het Anker de Mobility Controller is en de Foreign WLC de Mobility Agent is die de licentie van een andere Mobility Controller verkrijgt. In dit geval heeft de Foreign WLC slechts één Anchor en dat Anchor is degene die het beleid duwt. Dubbele verankering wordt niet ondersteund en werkt niet omdat niet verwacht wordt dat het op die manier werkt.

Voorbeeld

De WLC 5508 fungeert als anker en de WLC 5760 fungeert als de Mobility Controller voor een 3850 Switch die fungeert als Mobility Agent. Voor Anchor Foreign WLAN is de WLC 5508 het anker voor de 3850 Foreign WLAN. Het is helemaal niet nodig om dat WLAN op de WLC 5760 te configureren. Als u de 3850 Switch naar het 5760 Anker wijst, en dan van deze WLC 5760 naar de WLC 5508 als een dubbel anker, zal het niet werken aangezien dit dubbel anker wordt en het beleid op het 5508 Anker is.

Als u een opstelling hebt die een WLC 5508 als Anchor omvat, een WLC 5760 als de Mobility Controller, en een 3850 Switch als de Mobility Agent en Foreign WLC, dan zal op elk moment het Anker voor de 3850 Switch of de WLC 5760 of de WLC 5508 zijn. Het kan niet tegelijk zijn en het dubbele anker werkt niet.

Topologie 1 Configuratievoorbeeld

Zie <u>Topologie 1</u> voor het netwerkdiagram en een toelichting.

De configuratie is een proces in twee stappen:

- 1. Configuratie op de ISE.
- 2. Configuratie op de WLC.

De WLC 5760 fungeert als een standalone WLC en de gebruikers worden geverifieerd naar de ISE.

Configuratie op de ISE

1. Kies ISE GUI > Administration > Network Resource > Network Devices List > Add om WLC op de ISE toe te voegen als de AAA-client (Verificatie, autorisatie en accounting). Zorg ervoor dat u hetzelfde gedeelde geheim invoert op de WLC dat is toegevoegd aan de RADIUS-server. Opmerking: terwijl u Anchor-Foreign implementeert, moet u gewoon de Foreign WLC toevoegen. Het is niet nodig om de Anker WLC op de ISE toe te voegen als een AAA-client. De zelfde configuratie van ISE wordt gebruikt voor alle andere plaatsingsscenario's in dit document.

Network Devices List > Surbg_5760

Network Devices

	* Name Surbg_5760	
	Description	
1.5		
	* IP Address: 10.105.135.178 / 32	
	Model Name	
	Software Version	
*	* Network Device Group	
	All Locations Set To Default	
	Device Type All Device Types 📀 Set To Default	
L		
✓	✓ Authentication Settings	
	Fachle Authorities Cattings	
	Enable Authentication Settings	
	Protocol RADIUS	
	* Shared Secret	Show
	Enable KeyWrap 🗌 🔅	
	* Key Encryption Key	Show
	* Massage Authoritization Carlo Kaus	
	 Message Authenticator Code Key 	Show
	Key Input Format 💿 ASCII 🔵	HEXADECIMAL
_		
	SNMP Settings	
	Advanced TrustSec Settings	
Si	Save Reset	

2. Kies in de ISE GUI Beleid > Verificatie > MAB > Bewerken om het verificatiebeleid te maken. Het verificatiebeleid accepteert het MAC-adres van de client, dat verwijst naar interne eindpunten. Kies deze selecties in de lijst Opties:Kies Afwijzen in de vervolgkeuzelijst Als de verificatie is mislukt.Kies in de vervolgkeuzelijst Als gebruiker niet gevonden is de optie Doorgaan.Kies in de vervolgkeuzelijst Als het proces is mislukt de optie Drop.Wanneer u met deze opties configureert, gaat de client die mislukt MAC-autorisatie verder met het gastportal.

de de		admin-ise-1-2 admin Logo	it Feedback 0
cisco Identity Services Engine	Home Operations Policy	Administration 🔻	
Authentication S Authorization S Profi	ing 🛛 Posture 🔂 Client Provisioning	🚊 Security Group Access 🛛 🐣 Policy Element	nts
Authentication Policy			
Define the Authentication Policy by selecting the protocols th	at ISE should use to communicate with the network	devices, and the identity sources that it should use	for authentication.
Policy Type O Simple Rule-Based			
🛛 👻 MAB : 1f	Wireless MAB 🔶 All	ow Protocols : Default Network Access	and 🚽
······································			
Default : Use	Internal Endpoints		
	The Discourse Internet Frankrick		
	Identity Source Internal Endpoints		
	If authentication failed Reject		
	If user not found Continue		
	If process failed Drop v		
Dot1X : If Wired_4			and
Wireles	Note: For authentications using PEAP, LEAP, EAP-F/	AST or RADIUS MSCHAP	
Z EAP-FAST : If Ne	It is not possible to continue processing when auth If continue option is selected in these cases, reque	entication fails or user is not found. sts will be rejected.	
- DEAD	a contract of contract of a state of a state of a state		

3. Kies in de ISE GUI **Beleid > Autorisatie > Resultaten > Autorisatieprofielen > Toevoegen**. Vul de gegevens in en klik op **Opslaan** om het autorisatieprofiel te maken. Dit profiel helpt de clients om te worden omgeleid naar de Redirect URL na de MAC-verificatie, waar de clients de gastgebruikersnaam/het wachtwoord invoeren.

uthentication 🧑 Authorization 🧭 P
naries Conditions Results
Its Authentication Authorization Authorization Profiles Downloadable ACLs Downloadable ACLs Downloadable ACLs Downloadable ACLs Client Provisioning Security Group Access

4. Kies vanuit de ISE GUI Beleid > Vergunning > Resultaten > Vergunningsprofielen > Toevoegen om een ander machtigingsprofiel te maken om de gebruikers met de juiste

referenties toegang te verlenen.

cisco Identity Services Engine	Home Operations Policy Administration
Identity Services Engine Authentication Authentication Dictionaries Conditions Results Results Image: Service Conditions Image: Service Conditions<	Authorization Profiles > PermitAccess Authorization Profile * Name PermitAccess Description Default Profile with access type as Access-Accept * Access Type ACCESS_ACCEPT Service Template
 Client Provisioning Security Group Access 	 Common Tasks Advanced Attributes Settings Attributes Details Access Type = ACCESS_ACCEPT Save Reset

5. Creëer het autorisatiebeleid. Het autorisatiebeleid 'Guest_Wireless' drukt op de Redirect URL en de Redirect ACL naar de clientsessie. Het profiel dat hier wordt gedrukt is het CWA zoals eerder getoond. Het autorisatiebeleid 'Guest_Wireless-Succes' geeft volledige toegang tot een gastgebruiker die met succes is geverifieerd via het gastportaal. Nadat de gebruiker met succes is geverifieerd op het gastportaal, wordt dynamische autorisatie verzonden door de WLC. Hiermee wordt de sessie van de client opnieuw geverifieerd met het kenmerk 'Network Access:Usecase EQUALS Guest Flow'. Het uiteindelijke autorisatiebeleid ziet er als volgt uit:

Ē	×	Guest_Wireless_Success	if	Guest AND Network Access:UseCase EQUALS Guest Flow	then	PermitAccess	Edit 🔻
1		Guest_Wireless		Wireless_MA8		CWA	Edit 💌

Save Reset

6. Optioneel: In dit geval worden standaard multiportal configuraties gebruikt. Op basis van de vereisten kan hetzelfde worden gewijzigd in de GUI. Kies vanuit de ISE GUI Beheer > Web Portal management > Multi Portal Configurations > DefaultGuestPortal.



De Guest_Portal_sequentie is gemaakt die de Interne, Gast en AD gebruikers mogelijk maakt.

ululu cisco Ide	ntity Services E	ngine	A					au
			Home	Operation	s∣▼	Policy V	Administratio	1 🔻
🔆 System	¹ Identity Man	agement 🔛	Network Resources	🛃 Web I	Portal N	lanagement	Feed S	ervio
Identities	Groups External	Identity Sources	Identity Source Seq	uences	Setting	S		
entity Source Sec	uences List > Guest_Po	ortal_Sequence						
entity Sou	rce Sequence							
Identity So	ource Sequence							
* Name	Ruget Portal Segu	0000						
Description	puest_Portal_Sequ	ence						
Description	A built-in Identity S	sequence for the G	uest Portal					
							11.	
 Certificati 	e Based Authentica	tion						
	olact Cartificate Aut	ontination Profile						
	elect Certificate Aut	ientication Profile						
 Authentic 	ation Search List							
	A set of identity sour	ces that will be acc	cessed in sequence un	til first authe	nticatio	n succeeds		
Available			Selected				_	
Internal E	Endpoints		Internal Users	8				
LUAP_D	5		AD1					
			<				~	
			>>				V	
			~				$\mathbf{\underline{\vee}}$	
	Coarch List Sotting	10						
Select the ac	tion to be performed	if a selected identit	ty store cannot be acce	ssed for aut	hentica	ation		
0.000	and to be performed		,				_	
O Do not	access other stores i	n the sequence an	d set the "Authenticatio	nStatus" att	ribute t	o "ProcessErr	ror"	
Treat as	s if the user was not	found and proceed	to the next store in the	sequence				
Save Re:	set							

7. Kies in de ISE GUI Guest > Multi-Portal Configuration > DefaultGuestPortal. Kies Guest_Portal_Sequence in de vervolgkeuzelijst Identify Store Sequence.



Configuratie op de WLC

- 1. Definieer de ISE Radius-server op de WLC 5760.
- 2. Configureer de RADIUS-server, servergroep en methodelijst met de CLI. dot1x system-auth-control

```
radius server ISE
  address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
   timeout 10
   retransmit 3
   key Cisco123
  aaa group server radius ISE
  server name ISE
  deadtime 10
  aaa authentication dot1x ISE group ISE
  aaa authorization network ISE group ISE
  aaa authorization network MACFILTER group ISE
  aaa accounting identity ISE start-stop group ISE
  !
  aaa server radius dynamic-author
  client 10.106.73.69 server-key Cisco123
  auth-type any
Configureer het WLAN met de CLI.
  wlan CWA_NGWC 10 CWA_NGWC
   aaa-override
  accounting-list ISE
  client vlan VLAN0012
  no exclusionlist
  mac-filtering MACFILTER
  nac
```

```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
session-timeout 1800
no shutdown
```

4. Configureer de Redirect ACL's met de CLI. Dit is de url-redirect-acl die ISE teruggeeft als AAA-override samen met de redirect URL voor de guest portal-omleiding. Het is een directe ACL die momenteel op de Unified architectuur wordt gebruikt. Dit is een 'punt'-ACL die een soort omgekeerde ACL is die u normaal gesproken zou gebruiken voor Unified architectuur. U moet de toegang tot DHCP, de DHCP-server, DNS, de DNS-server en de ISE-server blokkeren. Laat alleen www, 443 en 8443 toe indien nodig. Dit ISE-gastenportal maakt gebruik van poort 8443 en de omleiding werkt nog steeds met de hier getoonde ACL. Hier wordt ICMP ingeschakeld, maar op basis van de beveiligingsregels die u kunt weigeren of toestaan.

```
ip access-list extended REDIRECT
deny icmp any any
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

Waarschuwing: wanneer u HTTPS inschakelt, kan dit door de schaalbaarheid tot een aantal hoge CPU-problemen leiden. Schakel deze optie niet in tenzij dit wordt aanbevolen door het Cisco-ontwerpteam.

5. Kies in de GUI van de draadloze controller AAA > RADIUS > Servers. Configureer de RADIUS-server, servergroep en methodelijst in de GUI. Vul alle parameters in en zorg ervoor dat het gedeelde geheim dat hier is geconfigureerd, overeenkomt met het geheim dat op de ISE voor dit apparaat is geconfigureerd. Kies Inschakelen in de vervolgkeuzelijst Ondersteuning voor RFC

3576.

ւլիսիս cisco Wireless Controller	🛆 Home	Monitor 🔻	Configuration •	Administration 🔻	Help	
Security	Radius Servers Radius Servers > Edit					
▼ 🔁 AAA ▼ 🔁 Method Lists	Server Name	Zeizer_ISE				
General Authentication	Server IP Address Shared Secret	10.106.73.69				
Accounting Authorization	Confirm Shared Secret Auth Port (0-65535)	1645]	
Server Groups RADIUS	Acct Port (0-65535) Server Timeout (0-1000) secs	1646				
Fallback	Retry Count (0-100) Support for RFC 3576	3 Enable				

6. Kies in de GUI van de draadloze controller **AAA > Servergroepen > Radius**. Voeg de eerder gemaakte RADIUS-server toe aan de servergroepen.

cisco Wireless Controller	🟡 Hom	e Monitor 🛛 🔻	Configuration •	Administration 💌 Help	
Security	Radius Server Groups Radius Server Groups > Edit				
▼ → AAA ▼ → Method Lists	Ora in Nama	1			
General	MAC-delimiter	n	one 💌		
Accounting	MAC-filtering	n	one 💌	1	
Authorization Server Groups	Dead-time (0-1440) in mir	utes 1	.O		
Ci Radius	Ava	ilable Servers		Assigned Servers	
Ldap	Servers In This Group	5 rosoft_NPS	^		^
▼ Contractive Contraction	136	;	-		Ŧ

7. Kies in de GUI van de draadloze controller **AAA > methodelijsten > Algemeen**. Schakel het aankruisvakje **Dot1x System Auto Control in**. Als u deze optie uitschakelt, werkt AAA niet.

cisco Wireless Controller	☆ Home	Monitor
Security	General	
► AAA ► Method Lists General	Dot1x System Auth Control	Method List

8. Kies in de GUI van de draadloze controller **AAA > methodelijsten > verificatie**. Maak een verificatiemethode voor Type dot1X. Het groepstype is groep. Breng het aan de ISE.

ahaha					
cisco Wireless Controller	🛆 Ho	me Manitar I 🔻	Configuration 🔻	Administration 🔻	Help
Security	Authentication Authentication > Edit				
- CAA					
Method Lists	Method List Name	24	TISE		
General		-			
Authentication	Type	COL	IX .		
Accounting	Graup Type	group			
Authorization	Falback to local	Disabled			
🕶 🔤 Server Groups		Available Server Gr	oups	Assigned Serv	er Groups
Radius		ACS		ISE _	~
Tacacs+	Groups In This Method	ISE Microsoft NPS			
Ldap		victor			
T 🔁 RADILIS			Ŧ		*

9. Kies in de GUI van de draadloze controller **AAA > Methodelijsten > Accounting**. Maak een lijst met accounting methoden voor type-identiteit. Breng het aan de ISE.



10. Kies in de GUI van de draadloze controller **AAA > Methodelijsten > Autorisatie**. Maak een lijst met autorisatiemethoden voor een type netwerk. Breng het aan de ISE.

cisco Wireless Controller	<u>Ω</u> H	ome Monitor 🛛 🔻	Configuration •	Administration 🔻	Help	
Security	Authorization Authorization > Edit					
AAA 🔤 🚽						
✓ Image: The matching of t	Method List Name	-				
Authentication	Туре	net	work			
Accounting	Group Type	group				
Authorization		Available Server G	roups	Assigned Ser	ver Groups	
🕶 📴 Server Groups	Geo and Ito This Mathead	ACS ISE	*		ŕ	~
Radius	Gloups In this Method	Microsoft_NPS	<	>		
Tacacs+		victor	-			-
1 I dan						

11. Optioneel, omdat er ook MAC op de foutondersteuning is. Maak een Autorisatiemethode lijst MACFILTER voor Type netwerk. Breng het aan de ISE.

cisco Wireless Controller	Administration ▼ Help Administration ▼ Help	
Security	Authorization Authorization > Edit	
Method Lists General Authentication Accounting	fethod List Name MACFILTER Type network Group Type group	
Authorization Eaclus Radus Tacacs+ Liden	Available Server Groups Assigned Server Groups ACS ISE Microsoft_NPS victor	

12. Kies WLAN > WLAN's in de GUI van de draadloze controller. Maak een nieuwe configuratie met de hier getoonde parameters.

ahaha		
cisco Wireless Controller	🏠 Home	Monitor 💌 Configuration 💌 Administration 💌 Help
Wireless	WLAN	
	WLAN > Edit General Security	QOS AVC Policy Mapping Advanced
Access Points	Profile Name	CWA_NGWC
> 🪞 802.11a/n/ac	Турв	WLAN
▶ 🧰 802.11b/g/n	SSID	CWA_NGWE
Media Stream	Status	C Enabled
• 🔤 QOS	Security Policies	MAC Filtering (Modifications done under security tab will appear after applying the changes.)
	Radio Policy	AI -
	Interface/Interface Group(G	VLAN0012 🔎
	Broadcast SSID	
	Multicast VLAN Feature	

13. Kies **Beveiliging > Layer 2**. Voer in het veld MAC-filtering **MACFILTER in**.

altalu CISCO - Wireless Controller						
Cisco Anteless controller		M Home	Monitor 🔻	Configuration 🔻	Administra	ation 🔻 Help
Wireless	WLAN					
	WLAN > Edit		_			
* 🗁 WLAN	General	Security	QOS	AVC Policy	Mapping	Advanced
WLANS	l aver 2	Lawar2	AAA Sorvo	r		
Access Points	Coyerz	Layers	AMA 36176	1		
▶ 🚞 802.11a/n/ac	Layer 2 Sec	urity None 💌]			
▶ 🧰 802.11b/g/n	MAC Filterin	0 MACFILT	ER			
🕨 🧮 Media Stream	Fast Transit	ion 🗆				
▶ 🚞 QOS	Over the D	s 🗹				
	Reassociatio	n Timeout 20)			

14. Het is niet nodig om Layer 3 te configureren.

cisco Wireless Controller	
Wireless WLAN WLANs Access Points B02.11a/n/ac B02.11b/g/n Media Stream QOS	WLAN > Edit General Security QOS AVC Policy Mapping Advanced Layer2 Layer3 AAA Server Web Policy

15. Kies **Beveiliging > AAA-server**. Kies **ISE** in de vervolgkeuzelijst Verificatiemethode. Kies **ISE** in de vervolgkeuzelijst Boekhoudmethode.

ahah				
CISCO Wireless Controller	👧 Home	Monitor 🔻	Configuration 🔻	Administration 🔻 Help
Wireless	WLAN			
VLAN	WLAN > Edit: General Security	QOS	AVC Policy	Mapping Advanced
WLANs Access Points	Layer2 Layer3	AAA Serve		
802.11a/n/ac	Authentication Method	8 2	JSE 🔎	
802.11b/g/n	Accounting Method		L <mark>ISE</mark>	
 Media Stream QOS 	Local EAP Authentication			

16. Kies Geavanceerd. Schakel het aanvinkvakje AAA negeren toestaan in. Controleer het aankruisvakje NAC State.

CISCO Wireless Controller	🏠 Home	Monitor I 💌	Configurati	on I 💌 🛛 Administra	ation I 💌 🛛 He	þ
Windess * 📴 WLAN	WLAN WLAN > Edit General Security	Q05	AVC	Policy Mapping	Advanced	
 wLANs Access Points E02.11a/n/ac E02.11b/Q/n Media Stream QOS 	Alow AAA Overide Coverage Hole Detection Session Timeout (secs) Alonet IE Disgnostic Channel P2P Blocking Action Media Stream Multipast-direc Clent Exclusion Max Allowed Clent	200	Arc	DHCP Server IP Ad DHCP Server IP Ad DHCP Address Assis DHCP Option 82 DHCP Option 82 As DHCP Option 82	dress grment require smat sci Mode d Mode	0.0.0.0 d None *
				IPv4 AQL United Interfa	ce ACL configured	

17. Configureer Redirect ACL's op de WLC in de GUI.

Acc ACLs	Access Control Lists ACLs > AEL detail									
Det	ails :									
Nam	Name: REDIRECT									
Тур	Type: IPv4 Extended									
Ad	Add Sequence Remove									
	Seq		Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP	
	3		deny	icmp	any	any		-	-	
	5		deny	udp	any	any	-	eq 67	-	
	6		deny	udp	any	any	-	eq 68	-	
	10		deny	udp	any	any		eq 53	-	
	20		deny	ip	any	10.106.73.69			-	
	30		permit	tep	any	any		eq 80	-	
	40		permit	tep	any	any	-	eq 443	-	

Configuratie-voorbeeld van topologie 2

Zie Topologie 2 voor het netwerkdiagram en de verklaring.

Deze configuratie is ook een proces in twee stappen.

Configuratie op de ISE

De configuratie op de ISE is hetzelfde als voor de Topologie 1-configuratie.

Het is niet nodig om de Anker Controller op de ISE toe te voegen. U hoeft alleen de Foreign WLC op de ISE toe te voegen, de RADIUS-server op de Foreign WLC te definiëren en het autorisatiebeleid onder het WLAN in kaart te brengen. Op het Anker hoeft u alleen maar MAC filtering in te schakelen.

In dit configuratievoorbeeld zijn er twee WLC 5760s die fungeren als Anchor Foreign. Indien u de WLC 5760 als anker wilt gebruiken en de 3850 Switch als Anchor Foreign, dat is de Mobility Agent, aan een andere Mobility Controller dan is dezelfde configuratie correct. Er is echter geen noodzaak om het WLAN te configureren op de tweede Mobility Controller waar de 3850 Switch de licenties van krijgt. Je hoeft alleen maar de 3850 Switch naar de WLC 5760 te wijzen die fungeert als het anker.

Configuratie op de WLC

 Configureer in het vak Vreemd de ISE-server met de lijst AAA-methode voor AAA en wijs het WLAN toe aan een MAC-filterautorisatie. **Opmerking**: het instellen van de omleiding van ACL op zowel Anker en Foreign als ook MAC filtering. dot1x system-auth-control

```
radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
timeout 10
retransmit 3
key Cisco123
aaa group server radius ISE
server name ISE
deadtime 10
aaa authentication dot1x ISE group ISE
aaa authorization network ISE group ISE
aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
1
aaa server radius dynamic-author
client 10.106.73.69 server-key Cisco123
auth-type any
wlan MA-MC 11 MA-MC
 aaa-override
 accounting-list ISE
```

```
client vlan VLAN0012
mac-filtering MACFILTER
mobility anchor 10.105.135.244
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2
ciphers aes
security dot1x authentication-list ISE
session-timeout 1800
no shutdown
```

2. Configureer ACL's met de CLI opnieuw. Dit is de url-redirect-acl die ISE teruggeeft als AAA-override samen met de redirect URL voor de guest portal-omleiding. Het is een directe ACL die momenteel op de Unified architectuur wordt gebruikt. Dit is een 'punt'-ACL die een soort omgekeerde ACL is die u normaal gesproken zou gebruiken voor Unified architectuur. U moet de toegang tot DHCP, de DHCP-server, DNS, de DNS-server en de ISE-server blokkeren. Laat alleen www, 443 en 8443 toe indien nodig. Dit ISE-gastenportal maakt gebruik van poort 8443 en de omleiding werkt nog steeds met de hier getoonde ACL. Hier wordt ICMP ingeschakeld, maar op basis van de beveiligingsregels die u kunt weigeren of toestaan.

```
ip access-list extended REDIRECT
deny icmp any any
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

Waarschuwing: wanneer u HTTPS inschakelt, kan dit door de schaalbaarheid tot een aantal hoge CPU-problemen leiden. Schakel deze optie niet in tenzij dit wordt aanbevolen door het Cisco-ontwerpteam.

3. Configureer Mobility op het anker.

wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg **Opmerking**: als u hetzelfde met de 3850-Switch configureert als de Foreign, dan zorg ervoor dat u de Switch peer-groep op de Mobility Controller en vice versa op de Mobility Controller. Configureer vervolgens de bovenstaande CWA-configuraties op de 3850 Switch.

4. Configuratie op het anker. Op het anker, is er geen behoefte om enige configuraties van ISE te vormen. U hebt alleen de WLAN-configuratie nodig.

```
wlan MA-MC 6 MA-MC
aaa-override
client vlan VLAN0012
mac-filtering MACFILTER
mobility anchor
nac
nbsp;no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2
ciphers aes
session-timeout 1800
no shutdown
```

5. Configureer Mobility op het anker. Definieer de andere WLC als het Mobility-lid op deze WLC.

wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg

6. Configureer ACL's met de CLI opnieuw. Dit is de url-redirect-acl die ISE teruggeeft als AAAoverride samen met de redirect URL voor de guest portal-omleiding. Het is een directe ACL die momenteel op de Unified architectuur wordt gebruikt. Dit is een 'punt'-ACL die een soort omgekeerde ACL is die u normaal gesproken zou gebruiken voor Unified architectuur. U moet de toegang tot DHCP, de DHCP-server, DNS, de DNS-server en de ISE-server blokkeren. Laat alleen www, 443 en 8443 toe indien nodig. Dit ISE-gastenportal maakt gebruik van poort 8443 en de omleiding werkt nog steeds met de hier getoonde ACL. Hier wordt ICMP ingeschakeld, maar op basis van de beveiligingsregels die u kunt weigeren of toestaan.

```
ip access-list extended REDIRECT
deny icmp any any
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

Waarschuwing: wanneer u HTTPS inschakelt, kan dit door de schaalbaarheid tot een aantal hoge CPU-problemen leiden. Schakel deze optie niet in tenzij dit wordt aanbevolen door het Cisco-ontwerpteam.

Voorbeeld van configuratie van topologie 3

Zie <u>Topologie 3</u> voor het netwerkdiagram en een toelichting.

Dit is ook een proces in twee stappen.

Configuratie op de ISE

De configuratie op de ISE is hetzelfde als voor de Topology 1 Configuration.

Het is niet nodig om de Anker Controller op de ISE toe te voegen. U hoeft alleen de Foreign WLC op de ISE toe te voegen, de RADIUS-server op de Foreign WLC te definiëren en het autorisatiebeleid onder het WLAN in kaart te brengen. Op het Anker hoeft u alleen maar MAC filtering in te schakelen.

In dit voorbeeld is er een WLC 5508 die fungeert als een Anchor en een WLC 5760 die fungeert als een Foreign WLC. Als u een WLC 5508 wilt gebruiken als anker en een 3850 Switch en Foreign WLC, die een Mobility Agent is, voor een andere Mobility Controller dan is dezelfde configuratie correct. Er is echter geen noodzaak om het WLAN te configureren op de tweede Mobility Controller waar de 3850 Switch de licenties van krijgt. Je hoeft alleen maar de 3850 Switch naar de 5508 WLC te wijzen die fungeert als het anker.

Configuratie op de WLC

- 1. Configureer op de Foreign WLC de ISE-server met de lijst AAA-methode voor AAA en wijs het WLAN aan een MAC-filterautorisatie toe. Dit is niet nodig op het Anker. **Opmerking**: configureer Redirect ACL op zowel Anker als Buitenlandse WLC en ook MAC filtering.
- 2. Kies in de WLC 5508 GUI WLAN's > Nieuw om Anker 5508 te configureren. Vul de details in om het filteren van MAC toe te laten.

راریاری cisco	<u>M</u> ONITOR	<u>W</u> LANs (W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP (
WLANs	WLANs >	Edit '550	8-MA'					
✓ WLANS WLANS	General	Security	y QoS	Policy-Mapp	ing Adva	nced		
▶ Advanced	Profile Type SSID	Name	<mark>5508-MA</mark> WLAN 5508-MA					
	Status Securit	γ Policies	MAC Fil (Modificat	ed tering ions done under	r security tab w	ill appear after ap	pplying the chanç	jes.)
	Radio F Interfa Group(Multica Broadc NAS-IC	Policy ce/Interface G) st Vlan Featur ast SSID	All manager Enable S508-MC	v ment v ed ed				

3. Het is niet noodzakelijk om Layer 2-opties te configureren.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit '5508-MA'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security [©] None -
	MAC Filtering ²
	Fast Transition

4. Het is niet nodig om Layer 3-opties te configureren.

cisco	<u>M</u> ONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	с <u>о</u> м
WLANs	WLANs>	Edit '5	508-MA'				
WLANs WLANs Advanced	General Layer	Secur 2 Lay	rity QoS er 3 AAA Si	Policy-Mapp ervers	ing Adva	anced	
	Laye	r 3 Securit	V Vone	•			

5. AAA-servers moeten worden uitgeschakeld in de Anchor AireOS WLC zodat de CoA kan

worden verwerkt door de buitenlandse NGWC. AAA-servers kunnen alleen worden ingeschakeld in de Anker WLC als er geen RADIUS-servers zijn geconfigureerd onder: Beveiliging > AAA > RADIUS > Verificatie

🔜 IMP Bookmarks 🗍 Cisco Live Australia 2013 📋 Cisco Live 2014 🔒 SURBG Device Access 🗍 Stud								
	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY MANA	AGEMENT C <u>O</u> MMANDS				
WLANs	WLANs > Edit '5508-M	A'						
WLANs WLANs	General Security	QoS Policy-Map	oing Advanced					
Advanced	Layer 2 Layer 3	AAA Servers						
	Radius Servers Enabled Authentication Servers Accounting Servers							
	Server 1	None	▼ None	-				
	Server 2	None	▼ None	-				
	Server 3	None	✓ None	•				
	Server 4	None	▼ None	-				
	Server 5	None	▼ None	-				
	Server 6	None	✓ None	-				

6. Kies WLAN's > WLAN's > Bewerken > Geavanceerd. Schakel het aanvinkvakje AAA negeren toestaan in. Kies Radius NAC in de vervolgkeuzelijst NAC-status.

CISCO	MONITOR <u>W</u> LANS CONT	RDILER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK
.ANs	WLANs > Edit '5508-MA	γ	
WLANS WLANS	General Security	QoS Policy-Mapping Advanced	
Advanced	Allow AAA Override	V Chabled	DHCP
	Coverage Hole Detection	🗹 Enabled	DHCP Server 🔲 Override
	Enable Session Timeout Airconst (E	IBOD Session Timeout (secs)	DHCP Addr. Assignment 🔲 Required
	Diagnostic Channel	Enabled	OEAP
	Override Interface ACL	IBM None w IBM None w	Split Tunnel (Printers) 🛛 🔲 Enabled
	Laver2 Ad	None -	Management Frame Protection (NFP)
	P2P Blocking Action	Disabled v	MFP Client Protection ^g Optional •
		Timeout Value (secs)	DTIM Period (in beacon intervals)
	Maximum Allowed Clients ²	D	802.11a/n (1 - 255) 1
	Static IP Tunneling 📶	Enabled	802.11b/g/n (1 - 295) 1
	Wi-Fi Direct Clients Policy	Disabled •	NAC State Radius NAC -
	Maximum Allowed Clients Per AP Radio	200	Load Dalancing and Dand Select

7. Voeg dit toe als anker voor het WLAN.

E s	*1.33	5500-414	5566-HA	Disabled	MAC filtering	20000
E 12	KLAV.		triater:	Disabled		Accounty Perchants
						802.11s Denigs Maps Basice Odeol spreads Halipet 2.0

8. Nadat het naar lokaal is gericht, zou het dit met Controle en de Weg van Gegevens UP/UP moeten kijken.

											Seve Configure
MONITOR	$\underline{W}LANK$	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDPACK			
Mobility A	Inchora										
WLAN SSE	D -50	S-MA									
Switch IP	Address (Anchor)							Data I	Path	Control Path
local									ц		ор

9. Maak de Redirect ACL op de WLC. Dit ontkent DHCP en DNS. Het maakt HTTP/HTTP's mogelijk.

Access Control Lists > Edit										
Gen	iral	DEDUBERT								
Access List Name REDIREC Deny Counters 0		0 REDIRECT								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	D	
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	D	
3	Permit	0.0.0.0 / 0.0.0.0	10.106.73.69 / 255.255.255.255	Any	Any	Any	Any	Any	D	٠
4	Permit	10.106.73.69 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	D	•

Zo ziet het eruit nadat de ACL is gemaakt.

Security	Access Control Lists					
▶ AAA						
Local EAP	Enable Counters 🔲					
Priority Order	Name	Туре				
Contificato	ACL Provisioning Redirect	IPv4				
P Certificate	REDIRECT	IPv4				
 Access Control Lists 						
Access Control Lists						
CPU Access Control Lists						
FlexConnect ACLs						
Layer2 ACLs						

- 10. Definieer de ISE RADIUS-server op de WLC 5760.
- 11. Configureer de RADIUS-server, servergroep en methodelijst met de CLI. dot1x system-auth-control

```
radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
timeout 10
retransmit 3
key Cisco123
aaa group server radius ISE
server name ISE
deadtime 10
```

```
aaa authentication dot1x ISE group ISE
   aaa authorization network ISE group ISE
   aaa authorization network MACFILTER group ISE
   aaa accounting identity ISE start-stop group ISE
   !
   aaa server radius dynamic-author
    client 10.106.73.69 server-key Cisco123
    auth-type any
Configureer het WLAN vanuit de CLI.
   wlan 5508-MA 15 5508-MA
    aaa-override
    accounting-list ISE
    client vlan VLAN0012
    mac-filtering MACFILTER
    mobility anchor 10.105.135.151
    nac
    no security wpa
    no security wpa akm dot1x
    no security wpa wpa2
    no security wpa wpa2 ciphers aes
    security dot1x authentication-list ISE
    session-timeout 1800
    shutdown
```

13. Definieer de andere WLC als het Mobility-lid op deze WLC.

wireless mobility group member ip 10.105.135.151public-ip 10.105.135.151 group Mobile-1 Opmerking: Als u hetzelfde met de WLC 3850 configureren als de Foreign, dan zorg ervoor dat u de Switch peer-groep op de Mobility Controller en vice versa op de Mobility Controller. Configureer vervolgens de vorige CWA-configuraties op de WLC 3850.

14. Configureer ACL's met de CLI opnieuw. Dit is de url-redirect-acl die ISE teruggeeft als AAAoverride samen met de redirect URL voor de guest portal-omleiding. Het is een directe ACL die momenteel op de Unified architectuur wordt gebruikt. Dit is een 'punt'-ACL die een soort omgekeerde ACL is die u normaal gesproken zou gebruiken voor Unified architectuur. U moet de toegang tot DHCP, de DHCP-server, DNS, de DNS-server en de ISE-server blokkeren. Laat alleen www, 443 en 8443 toe indien nodig. Dit ISE-gastenportal maakt gebruik van poort 8443 en de omleiding werkt nog steeds met de hier getoonde ACL. Hier wordt ICMP ingeschakeld, maar op basis van de beveiligingsregels die u kunt weigeren of toestaan.

```
ip access-list extended REDIRECT
deny icmp any any
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

Waarschuwing: wanneer u HTTPS inschakelt, kan dit door de schaalbaarheid tot een aantal hoge CPU-problemen leiden. Schakel deze optie niet in tenzij dit wordt aanbevolen door het Cisco-ontwerpteam.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De <u>Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten</u> <u>met</u> **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Sluit de client aan op de ingestelde SSID. Zodra u het IP-adres hebt ontvangen en wanneer de client naar de status Vereiste web gaat, opent u de browser. Voer uw clientreferenties in het portal in.





Na succesvolle verificatie schakelt u het vakje Algemene voorwaarden accepteren in. Klik op Akkoord.



U ontvangt een bevestigingsbericht en kunt nu naar het internet bladeren.



Signed on successfully You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.

Op de ISE ziet de client er als volgt uit:

2014-05-09 05:28:19:334	2	0	shoubeit	00:17:70:27:06:9A	Unknown	Surbg_\$760	PermitAccess	Authorize-Only succeeded	0a498752536c7a1700000117
2014-05-09 05:28:19.298	÷	0		00:17:70:27:86:9A		Surbg_5760		Dynamic Authorization succeeded	0#198752536c7s1700000117
2014-05-09 05:28:19.274	÷	0	shoubeir	00:17:7C:2F:86:9A				Guest Authentication Passed	0x898752536c7s1700000117
2014-05-09 05:19:00.822	2	9	00:17:70:27:86:9	00:17:70:27:86:9A	Unknown	Surbg_\$760	CAA	Authentication succeeded	0s996752536c7s1700000117

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

De <u>Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten</u> <u>met</u> **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.** **Opmerking**: Raadpleeg <u>Belangrijke informatie over debug commando's</u> voordat u **debug** commando's gebruikt.

Op de geconvergeerde access WLC, is het aan te raden om sporen uit te voeren in plaats van debugs. Op Aironet OS 5508 WLC hoeft u alleen maar **debug client <client mac>** in te voeren en **webauth te debug redirect activeren mac <client mac>**.

set trace group-wireless-client level debug set trace group-wireless-secure level debug

set trace group-wireless-client filter mac 0017.7c2f.b69a set trace group-wireless-secure filter mac 0017.7c2f.b69a

Sommige bekende defecten aan Cisco IOS-XE en Aironet OS zijn opgenomen in Cisco bug-id CSCun38344.

Zo ziet de succesvolle CWA-stroom eruit op de sporen:

[05/09/14 13:13:15.951 IST 63d7 8151] 0017.7c2f.b69a Association received from mobile
on AP c8f9.f983.4260
[05/09/14 13:13:15.951 IST 63d8 8151] 0017.7c2f.b69a qos upstream policy is unknown
and downstream policy is unknown

[05/09/14 13:13:15.951 IST 63e0 8151] 0017.7c2f.b69a Applying site-specific IPv6 override for station 0017.7c2f.b69a - vapId 15, site 'default-group', interface 'VLAN0012'

[05/09/14 13:13:15.951 IST 63e1 8151] 0017.7c2f.b69a Applying local bridging Interface Policy for station 0017.7c2f.b69a - vlan 12, interface 'VLAN0012' [05/09/14 13:13:15.951 IST 63e2 8151] 0017.7c2f.b69a **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:15.951 IST 63e3 8151] 0017.7c2f.b69a *** Client State = START instance = 1 instance Name POLICY_PROFILING_80211_ASSOC, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null

[05/09/14 13:13:15.951 IST 63eb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER [05/09/14 13:13:15.951 IST 63ec 8151] 0017.7c2f.b69a AAAS: auth request sent 05/09/14 13:13:15.951 IST 63ed 8151] 0017.7c2f.b69a apfProcessAssocReq (apf_80211.c:6149) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from Idle to AAA Pending

[05/09/14 13:13:15.951 IST 63ee 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1 [05/09/14 13:13:15.951 IST 63ef 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station: (callerId: 20) in 10 seconds [05/09/14 13:13:15.951 IST 63f0 211] Parsed CLID MAC Address = 0:23:124:47:182:154 [05/09/14 13:13:15.951 IST 63f1 211] AAA SRV(00000118): process author req [05/09/14 13:13:15.951 IST 63f2 211] AAA SRV(00000118): Author method=SERVER_GROUP Zubair_ISE [05/09/14 13:13:16.015 IST 63f3 220] AAA SRV(00000118): protocol reply PASS for Authorization [05/09/14 13:13:16.015 IST 63f4 220] AAA SRV(00000118): Return Authorization status=PASS [05/09/14 13:13:16.015 IST 63f5 8151] 0017.7c2f.b69a AAAS: received response, cid=266 [05/09/14 13:13:16.015 IST 63f6 8151] 0017.7c2f.b69a AAAS: deleting context, cid=266 [05/09/14 13:13:16.015 IST 63f7 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet. [05/09/14 13:13:16.015 IST 63f8 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0 [05/09/14 13:13:16.015 IST 63f9 8151] 0017.7c2f.b69a client incoming attribute size are 193 [05/09/14 13:13:16.015 IST 63fa 8151] 0017.7c2f.b69a AAAS: mac filter callback

status=0 uniqueId=280 [05/09/14 13:13:16.015 IST 63fb 8151] 0017.7c2f.b69a AAA Override Url-Redirect 'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa' set [05/09/14 13:13:16.015 IST 63fc 8151] 0017.7c2f.b69a Redirect URL received for client from RADIUS. for redirection. [05/09/14 13:13:16.015 IST 63fd 8151] 0017.7c2f.b69a Setting AAA Override Url-Redirect-Acl 'REDIRECT' [05/09/14 13:13:16.015 IST 63fe 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 'REDIRECT' [05/09/14 13:13:16.015 IST 63ff 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State START [05/09/14 13:13:16.015 IST 6400 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a [05/09/14 13:13:16.015 IST 6401 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station [05/09/14 13:13:16.015 IST 6402 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, gosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 [05/09/14 13:13:16.015 IST 6403 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName: [05/09/14 13:13:16.015 IST 6404 8151] 0017.7c2f.b69a Local Policy: Applying override policy [05/09/14 13:13:16.015 IST 6405 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---[05/09/14 13:13:16.015 IST 6406 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:16.015 IST 6407 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012 [05/09/14 13:13:16.015 IST 6408 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12 [05/09/14 13:13:16.015 IST 6409 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client [05/09/14 13:13:16.015 IST 640a 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC) [05/09/14 13:13:16.015 IST 640b 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile [05/09/14 13:13:16.015 IST 640c 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:16.015 IST 641a 8151] 0017.7c2f.b69a WCDB_ADD: Platform ID allocated successfully ID:259 [05/09/14 13:13:16.015 IST 641b 8151] 0017.7c2f.b69a WCDB_ADD: Adding opt82 len 0 [05/09/14 13:13:16.015 IST 641c 8151] 0017.7c2f.b69a WCDB_ADD: ssid 5508-MA bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0) wlan(ap-group/global) 15/15 client 0 assoc 1 mob=Unassoc(0) radio 0 m_vlan 12 ip 0.0.0.0 src 0x506c800000000f dst 0x0 cid 0x47ad4000000145 glob rsc id 259dhcpsrv 0.0.0

[05/09/14 13:13:16.015 IST 641d 8151] 0017.7c2f.b69a Change state to AUTHCHECK (2) last state START (0)

[05/09/14 13:13:16.015 IST 641e 8151] 0017.7c2f.b69a Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

[05/09/14 13:13:16.015 IST 641f 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 [05/09/14 13:13:16.015 IST 6420 8151] 0017.7c2f.b69a WCDB_LLM: NoRun Prev Mob 0, Curr Mob 0 llmReq 1, return False [05/09/14 13:13:16.015 IST 6421 207] [WCDB] ==Add event: type Regular Wireless client (0017.7c2f.b69a) client id (0x47ad400000145) client index (259) vlan (12) auth_state (ASSOCIATION) mob_state (INIT) [05/09/14 13:13:16.015 IST 6422 207] [WCDB] ===intf src/dst (0x506c80000000f)/(0x0) radio_id (0) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0) [05/09/14 13:13:16.015 IST 6423 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=L2_AUTH(1) vlan 12 radio 0 client_id 0x47ad400000145 mobility=Unassoc(0) src_int 0x506c800000000f dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0 ip_learn_type 0 [05/09/14 13:13:16.015 IST 6424 8151] 0017.7c2f.b69a WCDB_CHANGE: In L2 auth but 12ack waiting lfag not set,so set [05/09/14 13:13:16.015 IST 6425 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00 [05/09/14 13:13:16.016 IST 6426 8151] 0017.7c2f.b69a Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

[05/09/14 13:13:16.016 IST 6434 8151] 0017.7c2f.b69a Sending Assoc Response to station on BSSID c8f9.f983.4260 (status 0) ApVapId 15 Slot 0 [05/09/14 13:13:16.016 IST 6435 8151] 0017.7c2f.b69a apfProcessRadiusAssocResp (apf_80211.c:2316) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from Associated to Associated

[05/09/14 13:13:16.016 IST 6436 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x wireless client [05/09/14 13:13:16.016 IST 6437 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push wireless session for client 47ad4000000145 uid 280 [05/09/14 13:13:16.016 IST 6438 8151] 0017.7c2f.b69a Session Push for wireless client

[05/09/14 13:13:16.016 IST 6439 8151] 0017.7c2f.b69a Session Manager Call Client 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 1 Audit-Session ID 0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:16.016 IST 643a 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session start request from Client[1] for 0017.7c2f.b69a (method: No method, method list: none, aaa id: 0x00000118) - session-push, policy [05/09/14 13:13:16.016 IST 643b 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] - client iif_id: 47AD4000000145, session ID: 0a6987b2536c871300000118 for 0017.7c2f.b69a [05/09/14 13:13:16.016 IST 643c 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of auth-domain for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:16.017 IST 643d 243] ACCESS-CORE-SM-CLIENT-DOT11-ERR: [0017.7c2f.b69a, Ca2] Invalid client authorization notification: NO method [05/09/14 13:13:16.017 IST 643e 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-profile-name for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:16.017 IST 643f 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-name for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:16.017 IST 6440 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-class-tag for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:16.017 IST 6441 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-certainty-metric for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:16.017 IST 6442 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-opaque for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:16.017 IST 6443 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of dc-protocol-map for 0017.7c2f.b69a / 0xFE000110

[05/09/14 13:13:16.017 IST 6444 22] [WCDB] wcdb_ffcp_add_cb: client (0017.7c2f.b69a) client (0x47ad4000000145): FFCP operation (CREATE) return code (0) [05/09/14 13:13:16.017 IST 6445 22] [WCDB] wcdb_send_add_notify_callback_event: Notifying other features about client add [05/09/14 13:13:16.017 IST 6446 22] [WCDB] wcdb_sisf_client_add_notify: Notifying SISF of DEASSOC to DOWN any old entry for 0017.7c2f.b69a [05/09/14 13:13:16.017 IST 6447 22] [WCDB] wcdb sisf client add notify: Notifying SISF of new Association for 0017.7c2f.b69a [05/09/14 13:13:16.017 IST 6448 8151] 0017.7c2f.b69a WCDB SPI response msg handler client code 0 mob state 0 [05/09/14 13:13:16.017 IST 6449 8151] 0017.7c2f.b69a WcdbClientUpdate: L2 Auth ACK from WCDB [05/09/14 13:13:16.017 IST 644a 8151] 0017.7c2f.b69a WCDB_L2ACK: wcdbAckRecvdFlag updated [05/09/14 13:13:16.017 IST 644b 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 [05/09/14 13:13:16.017 IST 644c 8151] 0017.7c2f.b69a WCDB_CHANGE: Suppressing SPI (Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 12 client_id 0x47ad4000000145 mob=Unassoc(0) ackflag 2 dropd 1 [05/09/14 13:13:18.796 IST 644d 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c apfMsSumOverride 447 Returning fail from apfMsSumOverride [05/09/14 13:13:18.802 IST 644e 8151] 0017.7c2f.b69a Applying post-handoff policy for station 0017.7c2f.b69a - valid mask 0x0 [05/09/14 13:13:18.802 IST 644f 8151] 0017.7c2f.b69a QOS Level: -1, DSCP: -1, dotlp: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1 --More--[05/09/14 13:13:18.802 IST 6450 8151] 0017.7c2f.b69a Session: -1, User session: -1, User elapsed -1 Interface: N/A ACL: N/A Qos Pol Down Qos Pol Up [05/09/14 13:13:18.802 IST 6451 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State DHCP_REQD [05/09/14 13:13:18.802 IST 6452 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a [05/09/14 13:13:18.802 IST 6453 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station [05/09/14 13:13:18.802 IST 6454 8151] 0017.7c2f.b69a Override Values: source: 16, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 [05/09/14 13:13:18.802 IST 6455 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName: [05/09/14 13:13:18.802 IST 6456 8151] 0017.7c2f.b69a Local Policy: Applying override policy [05/09/14 13:13:18.802 IST 6457 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---[05/09/14 13:13:18.802 IST 6458 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:18.802 IST 6459 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012 [05/09/14 13:13:18.802 IST 645a 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12 [05/09/14 13:13:18.802 IST 645b 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client [05/09/14 13:13:18.802 IST 645c 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC) [05/09/14 13:13:18.802 IST 645d 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile [05/09/14 13:13:18.802 IST 645e 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and

apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 645f 8151] 0017.7c2f.b69a Local Policy: After Applying Site Override policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:18.802 IST 6460 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile MAC: 0017.7c2f.b69a , source 16 [05/09/14 13:13:18.802 IST 6461 8151] 0017.7c2f.b69a Inserting new RADIUS override into chain for station 0017.7c2f.b69a [05/09/14 13:13:18.802 IST 6462 8151] 0017.7c2f.b69a Override Values: source: 16, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 [05/09/14 13:13:18.802 IST 6463 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName: [05/09/14 13:13:18.802 IST 6464 8151] 0017.7c2f.b69a Local Policy: After ovr check continuation [05/09/14 13:13:18.802 IST 6465 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c apfMsSumOverride 447 Returning fail from apfMsSumOverride [05/09/14 13:13:18.802 IST 6466 8151] 0017.7c2f.b69a Local Policy: Calling applyLocalProfilingPolicyAction from Override2 [05/09/14 13:13:18.802 IST 6467 8151] 0017.7c2f.b69a **** Inside applyLocalProfilingPolicyAction **** [05/09/14 13:13:18.802 IST 6468 8151] 0017.7c2f.b69a *** Client State = DHCP_REQD instance = 2 instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null) [05/09/14 13:13:18.802 IST 6469 8151] 0017.7c2f.b69a Local Profiling Values : isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0, sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,applyPolicyAtRun= 0 [05/09/14 13:13:18.802 IST 646a 8151] 0017.7c2f.b69a ipv4ACL = [], ipv6ACL = [], inQoS = [unknown], outQoS = [unknown] [05/09/14 13:13:18.802 IST 646b 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:18.802 IST 646c 8151] 0017.7c2f.b69a apfMsRunStateInc [05/09/14 13:13:18.802 IST 646d 8151] 0017.7c2f.b69a Session Update for Non-dot1x client [05/09/14 13:13:18.802 IST 646e 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x wireless client [05/09/14 13:13:18.802 IST 646f 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push wireless session for client 47ad4000000145 uid 280 --More--[05/09/14 13:13:18.802 IST 6470 8151] 0017.7c2f.b69a Session Update for Pushed Sessions [05/09/14 13:13:18.802 IST 6471 8151] 0017.7c2f.b69a Session Manager Call Client 47ad4000000145, uid 280, capwap id 506c80000000f,Flag 0 Audit-Session ID 0a6987b2536c871300000118 policy name (null) [05/09/14 13:13:18.802 IST 6472 8151] 0017.7c2f.b69a Change state to RUN (20) last state DHCP_REQD (7) [05/09/14 13:13:18.802 IST 6473 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 [05/09/14 13:13:18.802 IST 6474 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 curr Mob State 3 llReq flag 1 [05/09/14 13:13:18.802 IST 6475 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 currMob State 3 afd action 1 [05/09/14 13:13:18.802 IST 6476 8151] 0017.7c2f.b69a WCDB_LLM: pl handle 259 vlan_id 12 auth RUN(4) mobility 3 client_id 0x47ad4000000145 src_interface 0x506c800000000f

dst_interface 0x75e18000000143 client_type 0 p2p_type 1 bssid c8f9.f983.4260 radio_id 0 wgbid 0000.0000.0000 [05/09/14 13:13:18.802 IST 6477 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 1 ip 0.0.0.0 ip_learn_type 0 [05/09/14 13:13:18.802 IST 6478 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session update from Client[1] for 0017.7c2f.b69a, ID list 0x0000000, policy [05/09/14 13:13:18.802 IST 6479 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 [05/09/14 13:13:18.802 IST 647a 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob State 3 llReg flag 0 [05/09/14 13:13:18.802 IST 647b 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c80000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip 0.0.0.0 ip_learn_type 0 [05/09/14 13:13:18.802 IST 647c 8151] 0017.7c2f.b69a AAAS: creating accounting start record using method list Zubair_ISE, passthroughMode 1 [05/09/14 13:13:18.802 IST 647d 8151] 0017.7c2f.b69a AAAS: initialised accounting start request, uid=280 passthrough=1 [05/09/14 13:13:18.802 IST 647e 8151] 0017.7c2f.b69a AAAS: accounting request sent [05/09/14 13:13:18.803 IST 647f 207] [WCDB] ==Update event: client (0017.7c2f.b69a) client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (L2_AUTH_DONE->RUN) mob_st<truncated> [05/09/14 13:13:18.803 IST 6480 207] [WCDB] ===intf src/dst (0x506c80000000f->0x506c80000000f)/(0x0->0x75e18000000143) radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6 (<truncated> [05/09/14 13:13:18.803 IST 6481 207] [WCDB] Foreign client add. Final llm notified = false [05/09/14 13:13:18.803 IST 6482 207] [WCDB] wcdb_client_mcast_update_notify: No mcast action reqd [05/09/14 13:13:18.803 IST 6483 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0 [05/09/14 13:13:18.803 IST 6484 207] [WCDB] wcdb_client_state_change_notify: update flags = 0x3[05/09/14 13:13:18.803 IST 6485 8151] 0017.7c2f.b69a aaa attribute list length is 79 [05/09/14 13:13:18.803 IST 6486 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a [05/09/14 13:13:18.803 IST 6487 8151] 0017.7c2f.b69a Sending SPI spi_epm_epm_session_create successfull [05/09/14 13:13:18.803 IST 6488 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole ExpForeign !!! [05/09/14 13:13:18.803 IST 6489 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole ExpForeign, updating wcdb not needed [05/09/14 13:13:18.803 IST 648a 8151] 0017.7c2f.b69a Tclas Plumb needed: 0 [05/09/14 13:13:18.803 IST 648b 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF to remove assoc in Foreign [05/09/14 13:13:18.803 IST 648c 207] [WCDB] ==Update event: client (0017.7c2f.b69a) client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN) mob_st<truncated> [05/09/14 13:13:18.803 IST 648d 207] [WCDB] ===intf src/dst (0x506c80000000f->0x506c80000000f)/(0x75e18000000143->0x75e18000000143) radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated> [05/09/14 13:13:18.803 IST 648e 207] [WCDB] wcdb_client_mcast_update_notify: No mcast action reqd [05/09/14 13:13:18.803 IST 648f 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0 [05/09/14 13:13:18.803 IST 6490 207] [WCDB] wcdb_client_state_change_notify: update flags = 0x2[05/09/14 13:13:18.803 IST 6491 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a [05/09/14 13:13:18.803 IST 6492 207] [WCDB] wcdb_sisf_client_update_notify:

Notifying SISF to remove assoc in Foreign [05/09/14 13:13:18.803 IST 6493 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a) client (0x47ad4000000145): FFCP operation (UPDATE) return code (0) [05/09/14 13:13:18.803 IST 6494 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a) client (0x47ad4000000145): FFCP operation (UPDATE) return code (0) [05/09/14 13:13:18.803 IST 6495 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of iif-id for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:18.803 IST 6496 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of audit-session-id for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:18.803 IST 6497 8151] 0017.7c2f.b69a Received session_create_response for client handle 20175213735969093 [05/09/14 13:13:18.803 IST 6498 8151] 0017.7c2f.b69a Received session_create_response with EPM session handle 4261413136 [05/09/14 13:13:18.803 IST 6499 8151] 0017.7c2f.b69a Splash Page redirect client or posture client --More--[05/09/14 13:13:18.803 IST 649a 8151] 0017.7c2f.b69a REDIRECT ACL present in the attribute list [05/09/14 13:13:18.803 IST 649b 8151] 0017.7c2f.b69a Setting AAA Override Url-Redirect-Acl 'REDIRECT' [05/09/14 13:13:18.803 IST 649c 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 'REDIRECT' [05/09/14 13:13:18.803 IST 649d 8151] 0017.7c2f.b69a AAA Override Url-Redirect 'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa' set [05/09/14 13:13:18.803 IST 649e 8151] 0017.7c2f.b69a Wireless Client mobility role is not ExportAnchor/Local. Hence we are not sending request to EPM [05/09/14 13:13:20.445 IST 649f 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 0.0.0.0 ip_learn_type 0 deleted ipv4 0.0.0.0 [05/09/14 13:13:20.446 IST 64a0 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign client (0017.7c2f.b69a) ip addr update received. [05/09/14 13:13:20.446 IST 64a1 207] [WCDB] SISF Update: IPV6 Addr[0] : fe80::6c1a:b253:d711:c7f [05/09/14 13:13:20.446 IST 64a2 207] [WCDB] SISF Update : Binding delete status for V6: = 0[05/09/14 13:13:20.446 IST 64a3 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF to remove assoc in Foreign [05/09/14 13:13:20.448 IST 64a4 8151] 0017.7c2f.b69a MS got the IP, resetting the Reassociation Count 0 for client [05/09/14 13:13:20.448 IST 64a5 8151] 0017.7c2f.b69a AAAS: creating accounting interim record using method list Zubair_ISE, passthroughMode 1 [05/09/14 13:13:20.449 IST 64a6 8151] 0017.7c2f.b69a AAAS: initialised accounting interim request, uid=280 passthrough=1 [05/09/14 13:13:20.449 IST 64a7 8151] 0017.7c2f.b69a AAAS: accounting request sent [05/09/14 13:13:20.449 IST 64a8 8151] 0017.7c2f.b69a Guest User() assigned IP Address (10.105.135.190)[05/09/14 13:13:20.449 IST 64a9 8151] 0017.7c2f.b69a Assigning Address 10.105.135.190 to mobile [05/09/14 13:13:20.449 IST 64aa 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 10.105.135.190 ip_learn_type DHCP deleted ipv4 0.0.0.0 [05/09/14 13:13:20.449 IST 64ab 8151] 0017.7c2f.b69a AAAS: creating accounting interim record using method list Zubair_ISE, passthroughMode 1 [05/09/14 13:13:20.449 IST 64ac 8151] 0017.7c2f.b69a AAAS: initialised accounting interim request, uid=280 passthrough=1 [05/09/14 13:13:20.449 IST 64ad 8151] 0017.7c2f.b69a AAAS: accounting request sent [05/09/14 13:13:20.449 IST 64ae 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20 mmRole ExpForeign !!! [05/09/14 13:13:20.449 IST 64af 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign client (0017.7c2f.b69a) ip addr update received. [05/09/14 13:13:20.449 IST 64b0 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20 mmRole ExpForeign, updating wcdb not needed [05/09/14 13:13:20.449 IST 64b1 8151] 0017.7c2f.b69a Tclas Plumb needed: 0 [05/09/14 13:13:20.449 IST 64b2 207] [WCDB] SISF Update: IPV6 Addr[0] : fe80::6c1a:b253:d711:c7f

[05/09/14 13:13:20.449 IST 64b3 207] [WCDB] SISF Update : Binding delete status for V6: = 0 [05/09/14 13:13:20.449 IST 64b4 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF to remove assoc in Foreign [05/09/14 13:13:20.449 IST 64b5 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay add/update sync of addr for 0017.7c2f.b69a / 0xFE000110 [05/09/14 13:13:49.429 IST 64b6 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session authz update requested cmd 5, mac 0017.7c2f.b69a, attr-list 0x0 for Client[1] [05/09/14 13:13:49.430 IST 64b7 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session authz update request sent to Client[1] [05/09/14 13:13:49.430 IST 64b8 8151] 0017.7c2f.b69a 1XA: Processing update request from dot1x. COA type 5 [05/09/14 13:13:49.430 IST 64b9 8151] 0017.7c2f.b69a AAAS: authorization init, uid=280, context=268 [05/09/14 13:13:49.430 IST 64ba 8151] 0017.7c2f.b69a AAAS: initialised auth request, uinque id=280, context id = 268, context reqHandle 0xfefc172c [05/09/14 13:13:49.430 IST 64bb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER [05/09/14 13:13:49.430 IST 64bc 8151] 0017.7c2f.b69a AAAS: auth request sent [05/09/14 13:13:49.430 IST 64bd 8151] 0017.7c2f.b69a processing COA type 5 was successful [05/09/14 13:13:49.430 IST 64be 8151] 0017.7c2f.b69a processing COA type 5 was successful [05/09/14 13:13:49.430 IST 64bf 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2] Session authz update response received for Client[1] [05/09/14 13:13:49.430 IST 64c0 211] Parsed CLID MAC Address = 0:23:124:47:182:154 [05/09/14 13:13:49.430 IST 64c1 211] AAA SRV(00000118): process author req [05/09/14 13:13:49.430 IST 64c2 211] AAA SRV(00000118): Author method=SERVER GROUP Zubair ISE [05/09/14 13:13:49.430 IST 64c3 211] Parsed CLID MAC Address = 0:23:124:47:182:154 [05/09/14 13:13:49.430 IST 64c4 211] AAA SRV(00000000): process response req [05/09/14 13:13:49.469 IST 64c5 220] AAA SRV(00000118): protocol reply PASS for Authorization [05/09/14 13:13:49.469 IST 64c6 220] AAA SRV(00000118): Return Authorization status=PASS [05/09/14 13:13:49.469 IST 64c7 8151] 0017.7c2f.b69a AAAS: received response, cid=268 [05/09/14 13:13:49.469 IST 64c8 8151] 0017.7c2f.b69a AAAS: deleting context, cid=268 [05/09/14 13:13:49.469 IST 64c9 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet. [05/09/14 13:13:49.469 IST 64ca 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0 [05/09/14 13:13:49.469 IST 64cb 8151] 0017.7c2f.b69a client incoming attribute size are 77 --More--[05/09/14 13:13:49.469 IST 64cc 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 uniqueId=280 [05/09/14 13:13:49.469 IST 64cd 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State RUN [05/09/14 13:13:49.469 IST 64ce 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a [05/09/14 13:13:49.469 IST 64cf 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station [05/09/14 13:13:49.469 IST 64d0 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xfffffffff, sessionTimeout: -1 [05/09/14 13:13:49.469 IST 64d1 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName: [05/09/14 13:13:49.469 IST 64d2 8151] 0017.7c2f.b69a Local Policy: Applying override policy [05/09/14 13:13:49.469 IST 64d3 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---[05/09/14 13:13:49.469 IST 64d4 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64d5 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012

[05/09/14 13:13:49.469 IST 64d6 8151] 0017.7c2f.b69a Local Policy:Setting local bridging

[05/09/14 13:13:49.469 IST 64d7 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client [05/09/14 13:13:49.469 IST 64d8 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC) [05/09/14 13:13:49.469 IST 64d9 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile [05/09/14 13:13:49.469 IST 64da 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:49.469 IST 64db 8151] 0017.7c2f.b69a Local Policy: After Applying Site Override policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:49.469 IST 64dc 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile MAC: 0017.7c2f.b69a , source 2 [05/09/14 13:13:49.469 IST 64dd 8151] 0017.7c2f.b69a Inserting new RADIUS override into chain for station 0017.7c2f.b69a [05/09/14 13:13:49.469 IST 64de 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 [05/09/14 13:13:49.469 IST 64df 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName: [05/09/14 13:13:49.469 IST 64e0 8151] 0017.7c2f.b69a Local Policy: After ovr check continuation [05/09/14 13:13:49.469 IST 64e1 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c apfMsSumOverride 447 Returning fail from apfMsSumOverride [05/09/14 13:13:49.469 IST 64e2 8151] 0017.7c2f.b69a Local Policy: Calling applyLocalProfilingPolicyAction from Override2 [05/09/14 13:13:49.469 IST 64e3 8151] 0017.7c2f.b69a **** Inside applyLocalProfilingPolicyAction **** [05/09/14 13:13:49.469 IST 64e4 8151] 0017.7c2f.b69a *** Client State = RUN instance = 2 instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null) [05/09/14 13:13:49.469 IST 64e5 8151] 0017.7c2f.b69a Local Profiling Values : isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0, sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,applyPolicyAtRun= 0 [05/09/14 13:13:49.469 IST 64e6 8151] 0017.7c2f.b69a ipv4ACL = [],ipv6ACL = [], inQoS = [unknown], outQoS = [unknown] [05/09/14 13:13:49.469 IST 64e7 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800 [05/09/14 13:13:49.469 IST 64e8 8151] 0017.7c2f.b69a In >= L2AUTH_COMPLETE for station 0017.7c2f.b69a [05/09/14 13:13:49.469 IST 64e9 8151] 0017.7c2f.b69a AAAS: creating accounting interim record using method list Zubair_ISE, passthroughMode 1 [05/09/14 13:13:49.469 IST 64ea 8151] 0017.7c2f.b69a AAAS: initialised accounting interim request, uid=280 passthrough=1 [05/09/14 13:13:49.469 IST 64eb 8151] 0017.7c2f.b69a AAAS: accounting request sent [05/09/14 13:13:49.469 IST 64ec 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00 [05/09/14 13:13:49.469 IST 64ed 8151] 0017.7c2f.b69a In SPI call for >= L2AUTH_COMPLETE for station 0017.7c2f.b69a [05/09/14 13:13:49.469 IST 64ee 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 [05/09/14 13:13:49.469 IST 64ef 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob State 3 llReq flag 0 [05/09/14 13:13:49.469 IST 64f0 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip 10.105.135.190 ip_learn_type DHCP --More--[05/09/14 13:13:49.469 IST 64f1 8151] 0017.7c2f.b69a apfMsAssoStateInc [05/09/14 13:13:49.469 IST 64f2 8151] 0017.7c2f.b69a apfPemAddUser2 (apf_policy.c:197)

Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from AAA Pending to Associated

[05/09/14 13:13:49.469 IST 64f3 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1 [05/09/14 13:13:49.469 IST 64f4 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station: (callerId: 49) in 1800 seconds [05/09/14 13:13:49.469 IST 64f5 8151] 0017.7c2f.b69a Ms Timeout = 1800, Session Timeout = 1800

[05/09/14 13:13:49.469 IST 64f6 207] [WCDB] ==Update event: client (0017.7c2f.b69a) client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN) mob_st<truncated> [05/09/14 13:13:49.469 IST 64f7 207] [WCDB] ===intf src/dst (0x506c80000000f->0x506c80000000f)/(0x75e1800000143->0x75e1800000143) radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated> [05/09/14 13:13:49.469 IST 64f8 207] [WCDB] wcdb_client_mcast_update_notify: No mcast action reqd [05/09/14 13:13:49.469 IST 64f9 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client (0017.7c2f.b69a) id 0x47ad400000145 ffcp update with flags=0x0 [05/09/14 13:15:47.411 IST 650a 8151] 0017.7c2f.b69a Acct-interim update sent for station 0017.7c2f.b69a [05/09/14 13:16:38.431 IST 650b 8151] 0017.7c2f.b69a

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.