DNA-ruimtes Captive Portal met AireOS Controller Configuration Voorbeeld

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Configureren **Netwerkdiagram** Configuraties Sluit de WLC aan op Cisco DNA-ruimtes De SSID op DNA-ruimtes maken ACL-configuratie op de controller Captive Portal zonder RADIUS-server op DNA-ruimtes Captive Portal met RADIUS Server op DNA-ruimtes Maak het portaal op DNA-ruimtes Configureer de Captive Portal Rules voor DNA-ruimtes Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u interactieve portalen kunt configureren met behulp van Cisco DNA Spaces met een AireOS-controller.

Bijgedragen door Andres Silva Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de draadloze controllers via Command Line Interface (CLI) of Graphic User Interface (GUI)
- Cisco DNA-ruimtes

Gebruikte componenten

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

• 5520 draadloze LAN-controller versie 8.10.12.0

Configureren

Netwerkdiagram



Configuraties

Sluit de WLC aan op Cisco DNA-ruimtes

De controller moet worden aangesloten op DNA-ruimtes met behulp van een van de beschikbare instellingen, Direct Connect, via DNA Spaces Connector of met CMX Tethering.

In dit voorbeeld is de Direct Connect optie in gebruik, hoewel captive portals op dezelfde manier zijn geconfigureerd voor alle instellingen.

Om de controller te verbinden met Cisco DNA Spaces moet het in staat zijn om de Cisco DNA Spaces-cloud via HTTPS te bereiken. Voor meer informatie over het aansluiten van de controller op DNA-ruimtes, zie deze link: <u>DNA-ruimtes Direct Connect Configuration Voorbeeld</u>

De SSID op DNA-ruimtes maken

Stap 1. Klik op Captive Portals in het dashboard van DNA Spaces:



Stap 2. Open het menu van het toegangsportaal door op het pictogram van drie lijnen linksboven op de pagina te klikken en klik op **SSID's:**

8 - 0 e	C & http://dwapeter.ik/conference/conf	- 0 6 1
Cisco DNA Spi	2005	C 1998
[] Partal		
IF Capital Partal Rule	•	Impart/Configure 1580
♥ 590x	250%	
Al Amports		
A User Management		

Stap 3. Klik op **SSID importeren/configureren**, selecteer **CUWN (CMX/WLC)** als het type "Draadloos netwerk" en voer de naam van de SSID in:

E Cisco DNA Spaces		C 54/30
Class Mervill \$500a		Input/Carligue 180
	SSID Configuration Yes/twote statust are Class Morall (SOK-yet, Select Jobor to per sorted	

ACL-configuratie op de controller

Een pre-authenticatie ACL is vereist als dit een web verificatie SSID is, en zodra het draadloze apparaat verbinding maakt met de SSID en een IP-adres ontvangt, de staat van de beleidsmanager van het apparaat verplaatst naar de staat **Webauth_Reqd** en de ACL wordt toegepast op de client sessie om de bronnen te beperken die het apparaat kan bereiken.

Stap 1. Navigeer naar **Security > Access Control Lists > Access Control Lists**, klik op **New** en configureer de regels om communicatie tussen de draadloze clients mogelijk te maken naar DNA-ruimtes als volgt. Vervang de IP-adressen door de door DNA Spaces opgegeven adressen voor de account in gebruik:

Gene	eral									
Acces	s List Name	DNASpece	n-ACL							
Deny	Counters	0								
Seq	Action	Source IP/Hask	Destination IP/Mask	Protocol	Source Port	Deat Port	OSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	34.235.248.212 /	TCP	Any	HTTPS	Any	Any	0	٠
2	Permit	34.235.249.212 /	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	
1	Permit	0.0.0.0 /	52.55.235.39 / 255.255.255.255	Any.	Any	Any	Any	Any	0	٠
A.	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	

Opmerking: Om de IP-adressen van DNA-ruimtes in de ACL toe te staan, klikt u op de optie **Handmatig configureren** uit de SSID die is gemaakt in stap 3 van de sectie **De SSID op DNA-ruimtes maken** onder de sectie ACL-configuratie.

De SSID kan worden geconfigureerd om een RADIUS-server te gebruiken of zonder de SID. Als die sessieduur, bandbreedterimiet of naadloos provisioninginternet is geconfigureerd in de sectie **Acties** van de configuratie Captive Portal Rule, moet de SSID worden geconfigureerd met een RADIUS-server, anders is het niet nodig om de RADIUS-server te gebruiken. Alle soorten portals op DNA-ruimtes worden op beide configuraties ondersteund.

Captive Portal zonder RADIUS-server op DNA-ruimtes

SSID-configuratie op de controller

Stap 1. Navigeren naar WLAN's > WLAN's. Maak een nieuw WLAN. Configureer de profielnaam en de SSID. Zorg ervoor dat de SSID-naam hetzelfde is als de naam die is ingesteld in stap 3 van de sectie **De SSID op DNA-ruimtes maken**.

cisco	HONETON HLANS CONTROLLER WE	ELESS SECURITY PRAVAGEMENT	COMMANDS HELP PEEDBACK	
WLANs	WLANs			
* WLANA WLANA	Carrent Pillers None (Chargo	e Filter) (Dear: Filter)	Cruida Nova 📑 😽	
+ Advanced	WLAN ID Type Profile Name	WAN SED	Admin Status Security Policies	
	OIL WAN JOD	.440	Brastel (MPR2)(Auth(PRC))	

Stap 2. Layer 2-beveiliging configureren. Navigeer naar het tabblad **Security > Layer 2** in het tabblad WLAN-configuratie en selecteer als **Geen** in het vervolgkeuzemenu van Layer 2 Security. Zorg ervoor dat MAC Filtering is uitgeschakeld.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security f None
	OWE Transition Mode
	Fast Transition Adaptive
	Over the DS C Reassociation Timeout 20 Seconds

Stap 3. Layer 3-beveiliging configureren. Navigeer naar het tabblad Security > Layer 3 in het tabblad WLAN-configuratie, vorm Web **Policy als de Layer 3-beveiligingsmethode, Passthrough inschakelen, configureer de voorverificatie-ACL, Override Global Config inschakelen** zoals het **Web Auth Type** als **Extern is ingesteld,** en stel de Redirect URL in.

cisco	NOVITOR WARM CONTROLLER WORKLESS SECURITY HANNGEMENT COMMANDS HELP REEDENCK
CISCO WLANs * WLANs #UANs # Advanced	NOVITOR NEXAL CONTROLLER WELCHEN BECURENT PRIVATE COMPANED HELP FEEDMACK WELANIS > Edit 'AlireOS-DNASpaces' General Security QS Paticy-Mapping Advanced Lager 3 Security Web Patry Ref Patry Captive Nutron's Assistant Bayes None Captive Nutron's Assistant Bayes On MACTRS Edit Operationally None Captive Nutron's Assistant Bayes Operationally None Authoritation Operationally None Presentionally Operationally None Presentionally Presentionally None Presentionally Presentionally None Presentionally Presentionally Presentionally Presentionally Presentionally Presentionally </th

Opmerking: om de URL te verplaatsen, klikt u op de optie **Handmatig configureren**, van de SSID die is gemaakt in stap 3 van de sectie **De SSID maken op DNA-ruimtes**, onder de sectie SSID configuratie.

Captive Portal met RADIUS Server op DNA-ruimtes

Opmerking: DNA Spaces RADIUS-server ondersteunt alleen PAP-verificatie die van de controller komt.

Configuratie RADIUS-servers op de controller

Stap 1. Navigeer naar **Security > AAA > RADIUS > Verificatie**, klik op **New** en voer de RADIUSserverinformatie in. Cisco DNA Spaces fungeert als de RADIUS-server voor gebruikersverificatie en kan reageren op twee IP-adressen. Beide RADIUS-servers configureren:

cisco	BONITOR	NO.	CONTROLL	en wyneuer	S SECURITY H	UNAGEMENT	сонников	ни	BEDBACK		
Security	RADIUS	Authentic	ation Ser	vers							
Ceneral	Auth Ca	And Station 10	Tipe ()	IP MAC Address	\$910 🔒						
 Authentication 	Une Add	Key Wrap	0.0	Designed for F3	S customers and rea	ins a key way	- compliant AADO	US serve	r1		
Accounting	MAC DV	imitar	- 0	Typhan.	8						
Falbeck DAS	Pramed	мти	8	300							
Downloaded AVP	Nativork		Tunnel	Server				_			
+ UACACE+	User	Manageme	d. Preny	Dodex 1	berver Address(Upv	A/Tgreft)		Part	1P9ec	Admin Status	
LOAP				1 1	44.197.146.005			1812	Disabled	Enabled	
Local Met Users				2 2	14.228.1.95			1812	Disabled	Enabled	

Opmerking: om het IP-adres en de geheime sleutel van RADIUS voor zowel primaire als secundaire servers te verkrijgen, klikt u op de optie **Handmatig configureren** van de SSID die is gemaakt in stap 3 van de sectie **De SSID op DNA-ruimtes maken** en naar de sectie **RADIUS Server Configuration** navigeren.

Stap 2. Configureer de RADIUS-server voor accounting. Navigeer naar **Security > AAA > RADIUS > Accounting** en klik op **New**. Configureer de twee RADIUS-servers als volgt:

cisco	HONELON	WLANS C	OATTROLL	en wyneles	IS SECURITY H	WAGEHENT	соннилоз	10,2	REDBACK		
Security	RADIUS	Accounting	Server	15							
General General ALCOUS Authentication Accounting	Aust Cal MAC De AP Exer	led Station 10 T Imiter Its Accounting		lystem MAC Add typhen Eneble	Pana 🖪						
Pallback	Network Unar	Management	Tunnel Presy	Server Index	Server Address()	(pv4/1pv6)	F	Port	IPSec	Admin Statue	1
Downloaded #17				1	34.197.146.105			1813	Orabled	Enabled	
+ TREACE+ LOAP				2	34.228.1.95		L	1813	Oxabled	Enabled	

SSID-configuratie op de controller

Belangrijk: Alvorens met de configuratie van SSID te beginnen, zorg ervoor dat de **Verificatie** van de Radius van het Web aan "PAP"onder Controlemechanisme > Algemeen wordt geplaatst.

Stap 1. Navigeren naar WLAN's > WLAN's. Maak een nieuw WLAN. Configureer de profielnaam en de SSID. Zorg ervoor dat de SSID-naam hetzelfde is als de naam die is ingesteld in stap 3 van de sectie **De SSID op DNA-ruimtes maken**.

cisco	HORETOR, MLANS	CONTROLLER WORDLESS	SECURITY PRANOCHENT	COMMANDS HELP	PTEDBACK	
WLANs	WLANs					
WLANs WLANS	Correct Filters Nor	e (Canpe filter)	Craste Now	8 (94)		
> Advanced	WLAN DD Type	Profile Name	WLAN SED	Admin Status	Security Policies	
	I WAN	.440	.440	Brabled	[MPA2][Autr(P9K]]	

Stap 2. Layer 2-beveiliging configureren. Navigeer naar het tabblad **Security > Layer 2** in het tabblad WLAN-configuratie. Layer 2-beveiliging als **geen** configureren. Schakel Mac-filtering in.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 4 None C MAC Filtering 2 C
	OWE Transition Mode
	Fast Transition Adaptive Over the DS Image: Comparison of the second se

Stap 3. Layer 3-beveiliging configureren. Navigeer naar het tabblad Security > Layer 3 in het tabblad WLAN-configuratie, configureer Web **Policy als de Layer 3-beveiligingsmethode**, **Inschakelen op fouten in Mac-filter, configureer de voorverificatie-ACL, Override Global Config inschakelen** zoals het **Web Auth Type** als **Extern is**, configureer de Redirect URL.

cisco	MONITOR MUNIC CONTROLLER WIRELESS SECURITY HANAGEMENT COMMANDS HELP (REDMAK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
WLANs WLANs WLANs Advanced	General Security QoS Policy-Happing Advanced Layer 2 Layer 3 AAA Servers Layer 3 Security vectorize Gaption Selecurity Press
	Authentication Peertivrough Canditional Web Redirect Splanh Page Web Redirect On HAC Filter failured
	Prezudhantization ACL IPv4 DhA5pecer ACL I IPv6 None WebAuth Rex IPV4 Ad None I WebAuth Rex IPV4 Ad None II WebAuth Rex IPV4 Ad None II WebAuth Rex IPV4 Ad None II WebAuth Rex IPV4 Ad None III Review III III III IIII IIII IIIIIIIIIIIIII
	Overnide Gisball Config ^{BR}

Stap 4. AAA-servers configureren. Navigeer naar het tabblad **Security > AAA-servers** in het tabblad WLAN-configuratie, **laat verificatieservers** en **accountingservers** toe en kies in het vervolgkeuzemenu de twee RADIUS-servers:

cisco	HONITOR MLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEBAA	×
WLANs	WLANs > Edit 'AireOS-DNASpaces'	
WLANS	General Security QoS Policy-Mapping Advanced	
+ Advanced	Layer 2 Layer 3 AAA Servers	
	RADIUS Servers RADIUS Server Overante Interface Enabled Apply Cisco 19E Default Settings Enabled Authentication Servers Accounting Servers	
	C Enabled C Enabled	
	Server 1 IP:34.197.146.105, Port:1812 DP:34.197.146.105, Port:1813	
	Server 2 19:34.228.1.95, Port:1812 🚦 19:34.228.1.95, Port:1813 🔒	
	Server 3 None O None O	
	Server 4 None 📴 None 📴	
	Server 5 None 0	
	Server 6 None 0	

Stap 6. Configureer de **prioriteitsvolgorde voor verificatie voor webautoregebruikers**. Navigeer naar het tabblad **Security > AAA-servers** in het tabblad WLAN-configuratie en stel RADIUS als eerste in volgorde.

alialia cisco	HONTTOR WLANS CONTROLLER WIRELESS SECURITY HANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
 WLANs WLANs Advanced 	General Security QoS Policy-Happing Advanced EADCUS Authentication Survivability

Stap 7. Navigeer naar het tabblad **Advanced** in het tabblad WLAN-configuratie en schakel **AAA-overbrugging** in.

cisco	HONETON BLANS CONTROLLER WIRELESS SECURITY MANAGEM	ENT COMMUNIS HELP (TEDBACK
WLANs	WLANs > Edit 'AireOS-ONASpaces'	
WLANs MLANS	General Security QuS Policy-Happing Advanced	
Advanced	Allow AAA Override G Enabled	0407
	Coverage Hele Detection 👩 Enabled	DHCP Server Override
	Enable Session Timesut (Jaco)	DISCP Adds. Assignment C Required
	Distance in Contractor	Hanagement Frame Protection (HFP)
	Overlde Interface ACL 3Pv4 None 3 3Pv6 None	MP Cleat Potection f Optional B DTIM Partied (in baseon intervale)
	URLACL None B F2F Blocking Adlen Deated Claret Exclusion 7	802.124/H (1 - 255) 1 802.125/gH (1 - 255) 1
	Timeout Value (sect) Maximum Allowed Clients	NAC State None
	Static P Turneling 44 Enabled W-FI Direct Clerks Policy Directing	Client Load Balancing Client Band Salest

Maak het portaal op DNA-ruimtes

Stap 1. Klik op Captive Portals in het dashboard van DNA Spaces:

ACT - Leverage Digitization toolkits t	o Act on Insights.	
Captive Portals	Engagements	29
Onboard and acquire visitors at your properties	Deliver contextual multi-channel notifications	
	0	

Stap 2. Klik op **Nieuw maken**, voer de portalnaam in en selecteer de locaties die de portal kunnen gebruiken:

	0			
	Partal Information	Authentication	Date Depture	User Agreement
PORSAL NA	AR:			
AireCS-	ONASpaces			
C End	ble this portal for all locations			
C End	ble this portal for all locations			
Loca	ble this portal for all locations stice.Hierarchy		Selecte	d Locations
Loca	ble this portal for all locations allon Hieranchy WEX-EAST-1		Selecte	d Locations
Loca	ble this portal for all locations stock Herandhy MEX-EAST-1 9 5906-1-CMX		Selecte	d Locations
Loca	ble this portal for all locations NEOR-Henrarchy VEX-EAST-1 9508-1-CMX 9508-2-Connector		Selecter (sato-)	d Locations desclared x
Loca	ble this portal for all locations ation Hertarchy MEX-EAST-1 9508-1-CMIX 9508-2-Connector 9520-1-DirectConnect		Selecter (1420-1	dilocations descalared at

Stap 3. Selecteer het verificatietype, kies als u gegevensvastlegging en gebruikersovereenkomsten op de portal-startpagina wilt weergeven en als gebruikers mogen inloggen om een bericht te ontvangen. Klik op **Volgende**:

o	-0			×
Penal Internation	Anthropological	Own Captern	ins Agenteen	
18JCT HE ALTHENDOVCK PVH		-		
Enal				
Value native salent for smalles access the mome.		-		
Display Authentication and User Agreements on portal home page				
Allow users to Qut in to receive cheesage				
	500	Page 1		

Stap 4. Configureer de gegevensopnameelementen. Als u gegevens van de gebruikers wilt opnemen, schakelt u het vakje **Enable Data Capture in** en klikt u op **+Add Field Element** om de

gewenste velden toe te voegen. Klik op Volgende:

	0	-0	-0	•	×
	Paral Internation	Adventurior	Data Cagners	the Appendix	
C (
Extrate data Capture				- ANTER	Depart
A Feet Name					
A Latitude					
		See .	Free Name of		

Stap 5. Controleer de **voorwaarden en bepalingen inschakelen** en klik op **Portal opslaan en configureren**:

	Parial Information	Automicators	Date Capiture	the Approximity	
action allows you to enable and configure	herea & Conditions and Privacy put	ty Surveya.			
Inglie Terrisch Canditions					
NO & SEND YON MESSAGE					Qr 1 010
	- 9.0 #				
1.0.6 6 4 2 2 2 2 1	the site of a local sector of the sector of	In the property of the	000		
tyles Porest	10 - 14 B R R				
In Prime of Use, Loss optimest Departure (1)	.899.				
These Wi-F. Terms & Canadiana Of Lines (the Wi-	Variation of the Value of	USE grown your use at the MAT is	phica.		
Description of the Denvice					
The Service provides you with minutese access to in product using the Service to answer that users o	the Internet within the premises. We do	t tot, as an artitrary practice, prover to law, although 1 coverson the light	hely menter the activities of those is do no.	who use the Bernice or eventies any adicital con	trol over any material transmitted, heated

Stap 6. Bewerk het portal zoals nodig, klik op Opslaan:

Partial - AlmeDE-DBM/generes /	n. internat Parlam, juritans /	3 I I I Annacian K ² (90)
PSENCERCOR - Sente a sector to configure Based Name Children Children Children Children D Parethani D Parethani Children Chil	E Pagi the servery reporter mediate ■ Statut from Language (in program in the commission of the comm	Vorsa, remaine C now Scover. (*) Consta Systems Voltome its Sponting Geograde the time bedow its opmant to internal (*) Complete the time bedow its opmant to internal (*)

Configureer de Captive Portal Rules voor DNA-ruimtes

Stap 1. Open het menu van het interactieve portaal en klik op Captive Portal Rules:

⊖ → ♂ ≙	C 🔒 https://dnaspaces.io/captiveportal/in/es/captive-portal	
Cisco DNA Spaces		
D Portal		
E Captive Portal Rules		Created
ି SSIDs	act .	Feb 24, 2020
A Reports	>	© 8:02 PM

Stap 2. Klik op **+ Nieuwe regel maken**. Voer de regelnaam in, kies de eerder geconfigureerde SSID en selecteer de locaties waar deze poortregel beschikbaar is voor:

When a user is on WHI - and connected to AmCD-CMRQueer -	112 544
	siteO1-Ontiperen
UDO/DOND - Where do you want the rule to find?	NING
Arc any of the following locations + Additionations	Plans care is or NPT and command in the DPAtypeint IODATORI For all teather uniter 1020-1-Development
Hill+Emilleon X	womos
	ID4Dat

Stap 3. Kies de actie van het portaal voor gevangenschap. In dit geval, wanneer de regel wordt geraakt, wordt het portaal getoond. Klik op **Opslaan en publiceren.**

01046	ADDAL
Show Dapties Partal Onuce a Partal to clapaped to Users when they connectify the with	SCHEDALE
AlwOS-DPADpaixs -	ACTON
Interview Duration	Partal AnaOS-OMOpecas
Surdend9-Linit	
Searchearly Previous Internet Descrip produces internet without advanting any suff-artification	
Cerry Internet Stag arms from anomaling the Internet	
Tago these users as Decement - Inscring Deservation - service characteristic	
(*Aathqu)	
C Tigger AT	
Save & Publish	

Verifiëren

Om de status te bevestigen van een client die is aangesloten op de SSID, navigeer naar Monitor >

Clients, klik op het MAC-adres en zoek naar Policy Manager-status:

TTOR WLANS (CONTROLLER	WPIELESS	SECORITY	HANAGEMENT	COMMANDS HELP	ELEDBYCK
nts > Detail						
Number of Record	s 10 * Cle	ar AVC Stats	1			
meral AVC St	atistics					
					AP radio alot 1d	1
lient Type	Regular				WLAN Profile	AireOS-OMASpaces
Dient Tunnel Type	Simple IP				WLAN SSID	AireOS-ONASpeces
iser Name					Status	Associated
lebauth User Name	None				Association 1D	1
ort Number	1				802.11 Authentication	Open System
terface	management				Reason Code	1
LAN ID	20				Status Code	0
acantine VLAN ID	0				CF Pollable	Not Implemented
VX Version	Not Connected				CF Poll Request	Not Implemented
Of Version	Not Supported				Short Preamble	Not Implemented
Andrew Bale	Latel				PBCC	Not Implemented
Ability Peer IP	Local Address				Channel Apility	Not Implemented
4ddress	10.4				Treasul	0
Robility Move Count	0	_				and the second s
Pancy Manager	RUM				wer state	WEP CHEROIR

Problemen oplossen

(5520-Andressi) >debug client

De volgende opdracht kan in de controller worden ingeschakeld voordat wordt getest om het associatie- en verificatieproces van de client te bevestigen.

(5520-Andressi) >debug web-auth redirect enable mac

Dit is de output van een succesvolle poging om elk van de fasen tijdens het vereniging/authentificatieproces te identificeren terwijl het verbinden met een SSID zonder server van de RADIUS:

802.11 koppeling/authenticatie:

*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
DHCP- en Layer 3-verificatie:

*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD *webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in HTTP GET, client mac=34:e1:2d:23:a6:68 *webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68 user_agent = AnyConnect Agent 4.7.04056 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configured Web-Auth type *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, using virtual IP =192.0.2.1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN ID:1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using URL:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio), redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00 *webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"</pre> content="no-cache"><META http-equiv="Pragma" content="</pre> *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34: *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK Location: https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79: dd:d2:00&client_mac=34:e1:2d:23 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-Url:https://splash.dnaspaces.io/p2/mexeast1 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send Layer 3-verificatie gelukt, verplaats de client naar de status RUN:

*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255, URL ACL ID 255, URL ACL ACL ID 255, URL ACL ACL 0)

*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user

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.