Konfigurationsbeispiel für DNA Spaces Captive Portal mit AireOS-Controller

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Netzwerkdiagramm Konfigurationen Verbinden des WLC mit Cisco DNA Spaces Erstellung der SSID auf DNA-Spaces ACL-Konfiguration auf dem Controller Captive Portal ohne RADIUS-Server auf DNA-Spaces Captive Portal mit RADIUS-Server auf DNA-Spaces Portal zu DNA Spaces erstellen Konfigurieren der Captive Portal-Regeln für DNA-Bereiche Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Sie Captive Portals mithilfe von Cisco DNA Spaces mit einem AireOS-Controller konfigurieren.

Beitrag von Andres Silva Cisco TAC Engineer.

Voraussetzungen

Anforderungen

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

- Zugriff auf die Wireless Controller über eine Kommandozeile oder eine grafische Benutzeroberfläche
- Cisco DNS-Räume

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen: • 5520 Wireless LAN Controller Version 8.10.112.0

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Verbinden des WLC mit Cisco DNA Spaces

Der Controller muss über eine der verfügbaren Konfigurationen, Direct Connect, über den DNA Spaces Connector oder über CMX Tethering mit DNA Spaces verbunden werden.

In diesem Beispiel wird die Option "Direct Connect" verwendet, obwohl Captive-Portale für alle Setups auf die gleiche Weise konfiguriert sind.

Um den Controller mit Cisco DNA Spaces zu verbinden, muss er über HTTPS auf die Cisco DNA Spaces-Cloud zugreifen können. Weitere Informationen zum Verbinden des Controllers mit DNA Spaces finden Sie unter diesem Link: <u>DNA Spaces Direct Connect-Konfigurationsbeispiel</u>

Erstellung der SSID auf DNA-Spaces

Schritt 1: Klicken Sie auf Captive Portals im Armaturenbrett von DNA Spaces:



Schritt 2: Öffnen Sie das Captive Portal-Menü, indem Sie auf das Symbol mit drei Zeilen in der oberen linken Ecke der Seite klicken und dann auf **SSIDs** klicken:

	0 a https://dwapers.in/op/radius/	- 0 6
Cisco DNA Spac	es	C tarte
🛛 Partal		
27 Caption Particl Bullet		ImperiConfigure 550
♀ \$50%	564	
A the Measure		

Schritt 3: Klicken Sie auf **Import/Configure SSID**, wählen Sie **CUWN (CMX/WLC)** als Typ "Wireless Network" aus, und geben Sie den SSID-Namen ein:



ACL-Konfiguration auf dem Controller

Eine Vorauthentifizierungs-ACL ist erforderlich, da es sich um eine Webauthentifizierungs-SSID handelt. Sobald das Wireless-Gerät eine Verbindung mit der SSID herstellt und eine IP-Adresse empfängt, wechselt der Richtlinienmanager-Status des Geräts in den Status **Webauth_Reqd,** und die ACL wird auf die Client-Sitzung angewendet, um die Ressourcen zu beschränken, die das Gerät erreichen kann.

Schritt 1: Navigieren Sie zu **Security > Access Control Lists > Access Control Lists,** klicken Sie auf **New** und konfigurieren Sie die Regeln, um die Kommunikation zwischen den Wireless-Clients zu DNA Spaces wie folgt zuzulassen. Ersetzen Sie die IP-Adressen durch die IP-Adressen, die von DNA Spaces für das verwendete Konto angegeben wurden:

Gene	Israi									
Access	List Name	e DNASpeo	m-ACL							
Deny	Counters	۰								
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	34.235.248.212 /	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	٠
r	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	٠

Hinweis: Um die IP-Adressen der DNA-Spaces abzurufen, die in der ACL zugelassen werden sollen, klicken Sie auf die Option **Manuell konfigurieren** aus der SSID, die in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** unter dem ACL-Konfigurationsabschnitt erstellt wurde.

Die SSID kann für die Verwendung eines RADIUS-Servers oder ohne diesen konfiguriert werden. Wenn die Sitzungsdauer, das Bandbreitenlimit oder die nahtlose Internetbereitstellung im Abschnitt "**Aktionen**" der Captive Portal Rule-Konfiguration konfiguriert ist, muss die SSID mit einem RADIUS-Server konfiguriert werden. Andernfalls muss der RADIUS-Server nicht verwendet werden. Alle Arten von Portalen auf DNA Spaces werden auf beiden Konfigurationen unterstützt.

Captive Portal ohne RADIUS-Server auf DNA-Spaces

SSID-Konfiguration auf dem Controller

Schritt 1: Navigieren Sie zu WLAN > WLANs. Erstellen Sie ein neues WLAN. Konfigurieren des Profilnamens und der SSID Stellen Sie sicher, dass der SSID-Name mit dem in Schritt 3 des Abschnitts Erstellen der SSID auf DNA-Spaces konfigurierten Namen übereinstimmt.

cisco	HONETON	HLANG C	CATROLLER WE	ROLESS SECURITY	PANAGEMENT	COMMANDS	10.7	REDMON		
WLANs	WLANs									
WLANS WLANS	Correct Filter	Connert Pitters None (Change Filter) (Conner Filter)								
+ Advanced	O WLAN SD	Type	Profile Name	w	AN SSOD	Acres	in Matus	Security Polic	ins.	
	01	WUM	JAND	.04	0	trasi	ed	[MM2][AUT/P	5K)]	

Schritt 2: Konfigurieren der Layer-2-Sicherheit Navigieren Sie zur Registerkarte **Security > Layer 2** der Registerkarte WLAN Configuration, und wählen Sie im Dropdown-Menü von Layer 2 Security die Option **None** aus. Stellen Sie sicher, dass die MAC-Filterung deaktiviert ist.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
VILANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security f
	OWE Transition Mode
	Fast Transition Adaptive O
	Over the DS Reassociation Timeout 20 Seconds

Schritt 3: Konfigurieren der Layer-3-Sicherheit Navigieren Sie zur Registerkarte Security > Layer 3 auf der Registerkarte WLAN configuration, konfigurieren Sie Web **Policy als die Sicherheitsmethode Layer 3, aktivieren Sie Passthrough, konfigurieren Sie die ACL für die Vorauthentifizierung, aktivieren Sie Override Global Config,** wenn Sie den **Web Auth Type** als **Extern** festlegen, und konfigurieren Sie die Umleitungs-URL.

uluilu cisco	NOVETON WERNE CONTROLLER WORKLESS SECURITY MANAGEMENT COMMANDS HELP EREDRACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs WLANs	General Security QoS Policy-Mapping Advanced
) Advanced	Lager 3 Security Web Palay Captive Notwork Assistant Bypess None Authoritantian PrestRough Creditional Web Railweit Stephen Page Web Railweit Presummertscolon AG. IPv4 Divelopces-AG. Presummertscolon AG. Presummertscolon AG. Presum

Hinweis: Um die Umleitungs-URL abzurufen, klicken Sie in Schritt 3 des Abschnitts "**Erstellen** der **SSID auf DNA-Spaces**" unter dem SSID-Konfigurationsabschnitt auf die Option "**Manuell konfigurieren**".

Captive Portal mit RADIUS-Server auf DNA-Spaces

Hinweis: Der RADIUS-Server DNA Spaces unterstützt nur die PAP-Authentifizierung, die vom Controller ausgeht.

Konfiguration der RADIUS-Server auf dem Controller

Schritt 1: Navigieren Sie zu Security > AAA > RADIUS > Authentication, klicken Sie auf New, und

geben Sie die RADIUS-Serverinformationen ein. Cisco DNA Spaces fungiert als RADIUS-Server für die Benutzerauthentifizierung und kann auf zwei IP-Adressen antworten. Konfigurieren Sie beide RADIUS-Server:

alialia cisco	BONTOR	WLANS	CONTROLL	en wonen		HANAGEMENT	COMMANDS	нμ	BEDMACK		
Security	RADIUS	Authentik	cation Ser	vers							
• AAA General • RADIUS Authentication Accounting Auth Central Users Fallbock DNS	Auth Ca Una ABS MAC De Pramed	Hed Station 1 5 Key Wrap Ombar MTU	- 100 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	IP MAC Addre Designed for P Typhen 300	ex SSID	requires a key wra	p compliant Madd	US seve	1		
Downloaded AVP + TACACS+	Nativork User	Manageme	Tunnel Presy	Server Index	Berver Address	Ige4/Tge6)		Port	(Pfier	Admin Status	1
LOAP	0	0		1	34.197.346.105			1812	Disabled	Enabled	
Locar Met Users			0	2	34.228.1.95			1812	Disabled	Enabled	

Hinweis: Um die RADIUS-IP-Adresse und den geheimen Schlüssel für den primären und den sekundären Server abzurufen, klicken Sie auf die Option **Manuell konfigurieren** der in Schritt 3 des Abschnitts erstellten SSID. **Erstellen Sie die SSID auf DNA-Spaces,** und navigieren Sie zum Abschnitt "**RADIUS-Serverkonfiguration**".

Schritt 2: Konfigurieren Sie den Accounting-RADIUS-Server. Navigieren Sie zu **Security > AAA > RADIUS > Accounting,** und klicken Sie auf **New**. Beide RADIUS-Server konfigurieren:

cisco	MONETOR	WLANS O	ONTROLL	ER WJAES	LESS SECURITY	нумденент	сочнилос	HELP	TEDMOX		
Security	RADIUS	Accounting	Server	8							
• AAA General • AADOUS Authentication Accounting	Ant Cal MAC De AP Exer	ind Station ID Ty Instar In Accounting		lystem MAC / typhen Enable	Address 📑						
Pailback	Network Unar	Management	Tunnel Praxy	Server Index	Server Addre	m(Ipv4/Ipv6)		Port	1Pliec	Admin Statue	1
Downloaded #17				1	34.197.146.10	5		1813	Otabled	Enabled	
EXCACS+ LDAP				2	34.228.1.95		L	1813	Oxabled	Drabled	•

SSID-Konfiguration auf dem Controller

Wichtig: Bevor Sie mit der SSID-Konfiguration beginnen, stellen Sie sicher, dass **Web Radius Authentication** unter Controller > General (Controller > Allgemein) auf "PAP" gesetzt ist.

Schritt 1: Navigieren Sie zu WLAN > WLANs. Erstellen Sie ein neues WLAN. Konfigurieren des Profilnamens und der SSID Stellen Sie sicher, dass der SSID-Name mit dem in Schritt 3 des Abschnitts Erstellen der SSID auf DNA-Spaces konfigurierten Namen übereinstimmt.

cisco	-	ILANS CO	ONTROLLER WIRELESS	SECURITY PRIMARMENT	COMMANDS HELP	rttobAck				
WLANs	WLANs									
* WLANs WLANS	Correct Filter	arment Pitters None (Change Siter) (Change Siter)								
> Advanced	WLAN D	Type	Profile Name	WLAN SED	Admin Status	Security Policies				
	0 L	WSAN	300	JAND	tratied	[MPR2][Auth(PBR)]	•			

Schritt 2: Konfigurieren der Layer-2-Sicherheit Navigieren Sie auf der Registerkarte für die WLAN-Konfiguration zur Registerkarte **Security > Layer 2**. Konfigurieren Sie die Layer-2-Sicherheit als **None**. Mac-Filterung aktivieren.

alialia 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 💋
	Reassociation Timeout 20 Seconds

Schritt 3: Konfigurieren der Layer-3-Sicherheit Navigieren Sie zur Registerkarte Security > Layer 3 auf der Registerkarte WLAN configuration, konfigurieren Sie Web **Policy als die Layer 3-Sicherheitsmethode, aktivieren Sie bei einem MAC-Filterfehler die ACL für die Vorauthentifizierung, aktivieren Sie Override Global Config,** wenn Sie den **Web Auth Type** als **Extern** festlegen, und konfigurieren Sie die Umleitungs-URL.



Schritt 4: Konfigurieren von AAA-Servern Navigieren Sie zur Registerkarte **Security > AAA Servers** (Sicherheit > AAA-Server) auf der Registerkarte WLAN configuration (WLAN-Konfiguration), aktivieren Sie **Authentication Servers** and **Accounting Servers (Authentifizierungsserver** und **Abrechnungsserver)**, und wählen Sie aus dem Dropdown-Menü die beiden RADIUS-Server aus:

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEBBACK
WLANs	WLANs > Edit 'AlreOS-DNASpaces'
* WLANs WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	RADIUS Servers RADIUS Server Dvenerite Interface Enabled Apply Cisco ISE Default Settings Enabled
	C Enabled C Enabled
	Server 1 1P:34.597.146.105, Port: 5852 3 IP:34.597.146.105, Port: 5853
	Server 2 19:34.228.1.05, Port: 1812 3 19:34.228.1.95, Port: 1813
	Server 3 None 9
	Server 4 None 9 None 9
	Server 5 None 0
	Server 6 None 🖯 None

Schritt 6: Konfigurieren Sie die **Reihenfolge der Authentifizierungspriorität für Web-Authentifizierungsbenutzer**. Navigieren Sie zur Registerkarte **Security > AAA Servers** (Sicherheit > AAA-Server) auf der Registerkarte WLAN configuration (WLAN-Konfiguration), und legen Sie RADIUS in der Reihenfolge als Erstes fest.

cisco	HONITOR	MLANS	CONTROLLER	witheress	SECURITY	MANAGEMENT	COMMANDS	HELP	TEEDBACK
WLANs	WLANs > E	Edit 'A	lireOS-DNAS	paces'					
WLANs WLANs Advanced	General RADOUS A Author LDAP Sen Server Server Server Local EAP Local E	Secularity and a secula	rity QoS cation Survivability a S a S a S ticetion entication Enal priority order Used	Policy-Map	th user	Vanced Order L	RADRUS LOCAL LOAP	tication	Up Down

Schritt 7. Navigieren Sie zur Registerkarte **Advanced (Erweitert**) auf der Registerkarte WLAN Configuration (WLAN-Konfiguration), und aktivieren Sie **Allow AAA Override (AAA-Außerkraftsetzung zulassen).**

cisco	MONITOR BLANI CONTROLLER WIRELESS SECURITY MEANSEM	ENT COMMANDS HELP (EEDBACK
VLANs	WLANs > Edit 'AireOS-ONASpaces'	
WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Allow AAA Overvide 🛛 Enabled	DHCP
	Coverage Hele Detection 👩 Enabled	DISCP Server Override
	Enable Session Timeout 20000 Session Timeout (secs) Aironet II: Enabled	DISCP Adds: Assignment C Required Management Frame Protection (MPP)
	Diagneetix Diamed AC (Fielded Override Interface AC), Shut None Shut None	MP Clerk Protection f Optional
	Layar2 Ad None D URL ADL None D P2P Blocking Atline Disabled D Clarit Declarize 2 Disabled 180	802.11a/n (1 - 200) 1 802.104/pin (1 - 200) 1 802.104/pin (1 - 200) 1
	Maximum Allowed Clients 8	NRC State None
	W-Pi Ornett Cherte Palloy Disabled	Client Load Balancing Client Band Select

Portal zu DNA Spaces erstellen

Schritt 1: Klicken Sie auf Captive Portals im Armaturenbrett von DNA Spaces:

ACT - Leverage Digitizatio	on toolkits to Act on Insights.
Captive Portals	D Engagements
Onboard and acquire visitors at your prope	rties Delver contextual multi-channel notifications
1	0

Schritt 2: Klicken Sie auf **Create New (Neu erstellen),** geben Sie den Portalnamen ein, und wählen Sie die Standorte aus, die das Portal verwenden können:

	0			
	Portal Information	Authentication	Data Capture	User Agreeme
PORDUNAME				
AirwOG-ONASpaces				
Enable this portal for all location	ion			
Enable this portal for all local	ions		Talan	
Enable this portal for all local Location Hierarchy	ions		Select	ed Locations
Enable this portal for all local Location Herarchy MEX-EAST-1	ites		Select	decisions
	ions -			dictations
	ions Df			ed Locations devicement X
Cable the portal for all local Location Herarchy MEX-EAST-1 C 9508-1-CMX C 9508-2-Connects S 9520-1-DirectOr	ions or onnect			ed Locations

Schritt 3: Wählen Sie den Authentifizierungstyp aus, und wählen Sie aus, ob Sie Datenerfassung und Benutzervereinbarungen auf der Portal-Startseite anzeigen möchten und ob Benutzer sich anmelden dürfen, um eine Nachricht zu erhalten. Klicken Sie auf **Weiter**:

Paral Hermites	0	a Decision	a Inter Agenetication	×
SELCT THE ACTION OF A CONTRACTOR PART		1		
Union Visitys waiting submit that anality access the improve.				
Display Automication and User Agreements on participante page Allow users to Opt in to monite message				
	-	New York 1		

Schritt 4: Konfigurieren von Datenerfassungselementen Wenn Sie Daten von Benutzern erfassen möchten, aktivieren Sie das Feld **Datenerfassung aktivieren**, und klicken Sie auf **+Feldelement hinzufügen**, um die gewünschten Felder hinzuzufügen. Klicken Sie auf **Weiter**:

	0		-0	•	×
	Paral Internation	Administration	then Captorn	ther Agreements	
E Ender Data Capture					
Form Fields				+ Add Faed Demand	
A Red Name					
A Lathere					
		(See) (Free Next 1		

Schritt 5: Aktivieren Sie die Option **Enable Terms &** Conditions, und klicken Sie auf **Save & Configure Portal**:

	Parial Information	Automicator	Date Capture	the Agreements	
a sector allows you to enable and configur	re Terra & Conditions and Privacy pol-	ty Suprema			
India West Candidan					
IND & CENTRON MESSAGE					Qt 1 (rsp
1 I I S K K K Z Z Z	1 1 1 7 X 1 1 4 4 4 F	(a) =	00c		
Syles - Parent - Part -	1 to 1 1 A D 12 D				
NI Prime of Use, Lost-petited September	27.898				
These Well Terms & Canadiana Of Son (Ne N	W/ Terral spatter with the 107465-07	USE generations at the MAT a	arkica.		
Description of the Danvies					
The Service provides you with minutese access or product value for Service Is attack Fail over	to the Internet within the premises. We do	not, as an artitrary practice, prost	help menter the activities of those to be as	who use the Senice or exercise any adiotal cont	to over any material terranithet, heated

Schritt 6: Bearbeiten Sie das Portal nach Bedarf, und klicken Sie auf Speichern:

Partiel - Abrebil-Olivitances /	/ Parlan./jackas/	Of 1 (2) - Restantion - K ² (Rep
ISBA: (SPOR - Smother sectors to confi Bread Name United Name	ans. Dag, the tensor vector Hestate,	Porte rever C Hose Scene ()
Enal Automization Venue Wep	first Orly 1 Lease chied next	Welsome to Spositions
Vitex Prettyph Vitex	Crear Sutrend	SiGn-UP POR WIRL Complete the form before to connect to internet Complete
Get App Get Manual Proreas & Ofers		(= 1 #)
· Add Markow		
	(term) Content	

Konfigurieren der Captive Portal-Regeln für DNA-Bereiche

Schritt 1: Öffnen Sie das Captive Portal-Menü, und klicken Sie auf Captive Portal Rules:

0	÷ ଫ ✿	Ð	https://dnaspaces.io/captiveportal/tules/captive-portal	
Ci	sco DNA Spaces	5		
۵	Portal			
=	Captive Portal Rules			Created
(ċ	SSIDs			Feb 24, 2020
	Reports			○ 8.02 PM

Schritt 2: Klicken Sie auf **+ Neue Regel erstellen**. Geben Sie den Regelnamen ein, wählen Sie die zuvor konfigurierte SSID aus, und wählen Sie die Standorte aus, für die diese Portalregel verfügbar ist:

Oners Captive Portal Rule RELEVANCE And Distances	
is any or an or the options that apply to your rule below	
	SUBMARY .
Aften a user is on VMH - and connected to Awd0-0940paper -	10.1 644
Weiling . When the second back to be ?	atrecht Charlipares
Controlete - Australia de las seras.	50.490
	Altern year is an full frank constraint to function
At any of the following locations	and the second
the any of the content of research	LODANDHE
+ Mellianshina	For all locations under
	1010-1 OnexCorrect
Milt+Emolarme X	and all will be a set of the set
	ID4DAB
The by Reference	
and the set of a second for a second se	87304
	Res Casta Basel

Schritt 3: Wählen Sie die Aktion des Captive Portals aus. In diesem Fall wird das Portal angezeigt, wenn die Regel getroffen wird. Klicken Sie auf **Speichern und veröffentlichen**.

2.110.442	100010
Show Explain Pursel Oncome to horse to be dispuped to Likers when they connectify the will.	504041
Amos-DrApeus v	ACTON INC.
Section Duration	Partal AnaOS-ON/Galeine
Davalations	
Securitary Provident Internet Descrip genetice Internet eliterate internet eliterate	
Deep internet Bog asses from accessing the internet	
Taga these values as Choose - Associate Deservation or to choose tags.	
+ Add Tega	
C THOSE AT	
ave & Publich	

Überprüfung

Um den Status eines mit der SSID verbundenen Clients zu bestätigen, navigieren Sie zu **Monitor > Clients,** klicken Sie auf die MAC-Adresse, und suchen Sie nach Policy Manager State:

MONITOR	MIAN	CONTROLLER	WPELESS	SECORITY	HANAGEMENT	COMMANDS	HELP	EEDBACK	
Clients >	Detail								< Back
Max Numbe	r of Recor	(s 10 * 10k	sar AVC Stats						
General	AVC 5	tatistics							
	-					AP radio als	e 1d	1	
Client T	pe	Regular				WLAN Profil	e	AireOS-ONASpaces	
Client T	annel Type	Simple IP				WLAN SSID		AireOS-ONASpeces	
User Na	me					Status		Associated	
Webeut	h User Name	None				Association	10	1	
Port Nur	nber	1				802.11 Aut	hentication	Open System	
breefeo		management				Reason Cod	le	1	
VLAN ID		30				Status Code	0	0	
Quarant	ine VLAN ID	0				CF Pollable		Not Implemented	
CCX Ver	noie	Not Supported				CF Poil Reg	Jest.	Not Implemented	
E2E Ven	nois	Not Supported				Short Pream	nble	Not Implemented	
Mobility	Role	Local				PBCC		Not Implemented	
Hobility	Peer IP	N/A				Chernel Ag	iky	Not Implemented	
Mobility	Move Count	0				Timeout		0	
Pency H State	arager	RUN				WEP State		WEP Disable	

Fehlerbehebung

Der folgende Befehl kann vor dem Testen im Controller aktiviert werden, um den Zuordnungs- und Authentifizierungsprozess des Clients zu bestätigen.

```
(5520-Andressi) >debug client
```

Dies ist die Ausgabe eines erfolgreichen Versuchs, jede der Phasen während des Assoziierungs-/Authentifizierungsprozesses zu identifizieren, während eine Verbindung zu einer SSID ohne RADIUS-Server hergestellt wird:

802.11-Zuordnung/Authentifizierung:

```
*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- und Layer 3-Authentifizierung:

```
*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-Location: typ2/mexeast1 *webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-Layer-3-Authentifizierung erfolgreich. Verschieben Sie den Client in den RUN-Status:

*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
Action 0)

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.