Esempio di configurazione di DNA Spaces Captive Portal con il controller AireOS

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione
Esempio di rete
Configurazioni
Connetti il WLC a Cisco DNA Spaces
Crea il SSID in DNA Spaces
Configurazione ACL sul controller
Portale vincolato senza server RADIUS su spazi DNA
Portale vincolato con server RADIUS su spazi DNA
Crea il portale in DNA Spaces
Configura le regole del portale vincolato in Spazi DNA
Verifica
Risoluzione dei problemi

Introduzione

In questo documento viene descritto come configurare i portali vincolati utilizzando Cisco DNA Spaces con un controller AireOS.

Contributo di Andres Silva Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso ai controller wireless tramite interfaccia a riga di comando (CLI) o interfaccia grafica utente (GUI)
- Cisco DNA Spaces

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

• 5520 Wireless LAN Controller versione 8.10.12.0

Configurazione

Esempio di rete



e configurare le regole per consentire la comunicazione tra i client wireless a DNA Spaces come indicato di seguito. Sostituire gli indirizzi IP con quelli forniti da DNA Spaces per l'account in uso:

Geni	eral									
Acces	s List Name	DNASpace	s-ACL							
Deny	Counters	0								
Seq	Action	Source IP/Mask	Destination IP/Heek	Protocol	Source Port	Dest Port	OSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	34.235.248.212 / 255.255.255.255	TOP	Any	HTTPS	Any	Any	0	
2	Permit	34.235.248.212 / 255.255.255.255	0.0.0.0 /	TOP	HTTPS	Any	Any	Arry	0	
1	Permit	0.0.0.0 /	52.55.235.39 / 255.255.255.255	Any	Any	Any	Any	Any	0	
4	Permit	52.55.235.39 / 255.255.255.255	0.0.0.0 /	TCP	HTTPS	Any	Any	Any	0	

Nota: per ottenere gli indirizzi IP degli spazi DNA da consentire nell'ACL, fare clic sull'opzione Configura manualmente dall'SSID creato nel passaggio 3 della sezione Creazione dell'SSID sugli spazi DNA nella sezione di configurazione dell'ACL.

SSID può essere configurato per l'utilizzo di un server RADIUS o senza di esso. Se la durata della sessione, il limite della larghezza di banda o il provisioning completo di Internet sono configurati nella sezione Azioni della configurazione della regola del portale captive, è necessario configurare il SSID con un server RADIUS. In caso contrario, non è necessario utilizzare il server RADIUS. Tutti i tipi di portali su DNA Spaces sono supportati in entrambe le configurazioni.

Portale vincolato senza server RADIUS su spazi DNA

Configurazione SSID sul controller

Passaggio 1. Selezionare WLAN > WLAN. Creare una nuova WLAN. Configurare il nome del profilo e l'SSID. Verificare che il nome SSID sia uguale a quello configurato nel passaggio 3 della sezione Creazione del SSID in Spazi DNA.

oliolo cisco	MONITOR.	mana c	CONTROLLER	WINELESS	SECURITY	MANAGEMENT	COMMANDS	10,7	TEOBACK			
WLANs	WLANs											
* WLANs WLANs	Current Filter: None [Change Filter] (Cean Filter)									8	Ge	
> Advanced	O 1644 10	Tape	Profile Nam	-	WLA	N 5510	Ade	nin Status	Security Policie			
	01	WEAR	AND		.400		6na	blend	[WPA20]Auth(PSP	Q)	T	

Passaggio 2. Configurare la protezione di livello 2. Passare alla scheda Sicurezza > Layer 2 nella scheda Configurazione WLAN e selezionare Nessuno dal menu a discesa Protezione di Layer 2. Assicurarsi che il filtro MAC sia disattivato.

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

Passaggio 3. Configurare la protezione di livello 3. Passare alla scheda Sicurezza > Livello 3 nella scheda Configurazione WLAN, configurare Criteri Web come metodo di sicurezza di Livello 3, abilitare PassThrough, configurare l'ACL di preautenticazione, abilitare la sostituzione della configurazione globale impostando il tipo di autenticazione Web come esterno, configurare l'URL di reindirizzamento.

altalu cisco	HONITOR WEARS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP REDBACK
WLANS	WLANs > Edit 'AireOS-DNASpaces'
• WLANs BLANs • Advanced	General Security QoS Policy-Mapping Advanced
	Captive Network Assistant Bugess None Authentication Passifirmugh Conditional Web Redirect Splach Page Web-Redirect On MAC Pilter failure ¹
	Presubentization AOL IPv6 DAASpacee-AOL () IPv6 None () WebAuth Rex IPv6 Ad None () Rex IPv6 Ad None (

Nota: per ottenere l'URL di reindirizzamento, fare clic sull'opzione Configura manualmente, dall'SSID creato nel passaggio 3 della sezione Creazione dell'SSID su Spazi DNA, nella



Portale vincolato con server RADIUS su spazi DNA

Nota: il server RADIUS DNA Spaces supporta solo l'autenticazione PAP proveniente dal controller.

Configurazione dei server RADIUS sul controller

Passaggio 1. Selezionare Sicurezza > AAA > RADIUS > Autenticazione, fare clic su Nuovo e immettere le informazioni sul server RADIUS. Cisco DNA Spaces funge da server RADIUS per l'autenticazione degli utenti e può rispondere su due indirizzi IP. Configurare entrambi i server RADIUS:

alialia cisco	BONLOR	20.476	CONTROLL	n waaraa	SECURITY	REALGENERT	COMMINDS	ныл	STERMON		
Security	RADIUS	Authentic	ation Ser	vers							
ALA Constal Constal Authonication Accounting Authonication Authonication Authonication Authonication Constal Constal Constal Constal	Auth Ca Use ABS MAC De Framed	led Station 10 Key Wrap Imitar HTy	тын	P MAC Address 1 besigned for F3P3 yghen	ison B i conterners and	requires a key with	r compliant MAD	toti serve	0		
Downloaded AVP + 1ACRCE+	Natavark Usar	Managamat	Tunnel R Preny	Server Index B	orver Address()	(p=4/1p=6)		Port	(Place	Admin Status	1
LOAP		0	0	1. 34	201.041.005			1812	Disable	d Crabled	
HAC Filtering	8	•	0	2 2	128.1.95			1812	Disable	d Cratied	

Nota: per ottenere l'indirizzo IP e la chiave privata RADIUS per i server primario e secondario, fare clic sull'opzione Configura manualmente dal SSID creato nel passaggio 3 della sezione Creazione del SSID in Spazi DNA e passare alla sezione Configurazione server RADIUS.

Passaggio 2. Configurare il server RADIUS di accounting. Selezionare Sicurezza > AAA > RADIUS > Accounting e fare clic su Nuovo. Configurare gli stessi server RADIUS:

alialia cisco	BONITOR	WLANS (ONTROLL	R WORLESS	SECURITY NEW	KIEMENT (COMMUNICS	нци	EEEOBACK		
Security	RADIUS	Accountin	g Server								
• AAA Coneral • RADUS Authentication Accounting	Acct Cell MAC Dell AP Event	ed Station 10 1 Imiter Is Accounting	Not S	yatam MAC Addre yghen C Eneble							
Fallback DVG	Network Over	Managaman	Tunnel Prexy	Server Index	Server Address(Spv4	(Tavel)		Port	IP544	Admin Status	1
Downloaded AVP	8	0	0	1	34.197.546.105			146.3	Disabled	Enabled	0
 TACACS+ LOAP 	۵	0	0	2	34.228.1.95			1413	Disabled	Enabled	٥

Configurazione SSID sul controller

Importante: prima di iniziare con la configurazione SSID, verificare che Autenticazione Web Radius sia impostata su "PAP" in Controller > Generale.

Passaggio 1. Selezionare WLAN > WLAN. Creare una nuova WLAN. Configurare il nome del profilo e l'SSID. Verificare che il nome SSID sia uguale a quello configurato nel passaggio 3 della sezione Creazione del SSID in Spazi DNA.

altalta cisco	MONITOR WLANS O	ONTROLLER WIRELESS SEC	URETY MANAGEMENT	COMMANDS HELP	REDBACK	
WLANs	WLANs					
* WLANs WLANs	Current Filter: Note	[Ohange Filter] (Dear.)	(iter)		Create New	B Ge
> Advanced	O WIAN ID. Type	Profile Name	WLAN \$500	Admin Status	Security Policies	
	C 1 WEAK	,AND	AND	Enubled	(WPA2)(Auth(PSK))	•

Passaggio 2. Configurare la protezione di livello 2. Passare alla scheda Sicurezza > Layer 2 nella scheda di configurazione WLAN. Configurare la sicurezza di layer 2 come Nessuna. Abilitare II Filtro Mac.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs	WLANs > Edit 'AireOS-DNASpaces'
 ₩LANs WLANs Advanced 	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers
	Layer 2 Security A None
	Fast Transition Adaptive I Over the DS I Reassociation Timeout 20

Passaggio 3. Configurare la protezione di livello 3. Passare alla scheda Sicurezza > Livello 3 nella scheda Configurazione WLAN, configurare Criteri Web come metodo di sicurezza di Livello 3, abilitare l'errore del filtro Enable On Mac, configurare l'ACL di preautenticazione, abilitare la sostituzione della configurazione globale impostando il tipo di autenticazione Web come esterno, configurare l'URL di reindirizzamento.

ahaha cisco	HONITOR HEARS CONTROLLER WIRELESS SECURITY HANAGEMENT COMMANDS HELP SEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'
* WLANs	General Security QoS Policy-Happing Advanced
+ Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security Web Policy
	Captive Network Assistant Bypass None
	C Passificaugh
	Conditional Web Redirect
	O On MAC Filter failure ¹⁸
	Presulhentication ACL IPv4 Dhillipecco-ACL 3 IPv6 None 3 WebAuth Flex IPv4 Acl None 3 WebAuth Flex IPv6 Acl None 3
	Redrect URL https://splack.dnaspaces.is/p2/mexeast1
	Strengting Charle Statute
	Overside Guided Canfight () Enable
	Web Auth type Driverue(Re-direct to external server)

Passaggio 4. Configurare i server AAA. Passare alla scheda Sicurezza > Server AAA nella scheda Configurazione WLAN, abilitare Authentication Server e Accounting Server e dal menu a discesa scegliere i due server RADIUS:

cisco	MONITOR W.	ANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	семналоя	неря	FEEDBACK
WLANs	WLANs > Edi	t 'AireOS-DNAS	paces'					
* WLANs WLANs	General	Security QoS	Policy-Map	ping Adv	anced			
	RADUS Services Servic	ervers below to over rers orver Overwrite interfa o ISE Default Settings	ride use of de Ce Enabled Enabled	fault servers (on this WLAN			
		Authentication Serv	ers /	Loosunting Se	rveni	٦		
	Server 1	1P:34.197.146.105,	Port:1812 📴	Enabled IP:34.197.146	6.105, Port:1813	8		
	Server 2	19:34.228.1.95, Per	e:1812 😫	19:34.228.1.9	5, Port:1813	9		
	Server 3	None	0	None		0		
	Server 4	None	0	None				
	Server 5	None	0	None		0		
	Server 6	None	÷.	None		#]		

Passaggio 6. Configurare l'ordine di priorità di autenticazione per gli utenti di autenticazione Web. Selezionare la scheda Security > AAA Servers (Sicurezza > Server AAA) nella scheda WLAN configuration (Configurazione WLAN), quindi impostare RADIUS come prima opzione da ordinare.

alialia cisco	MONITOR MUNN CONTROLLER WIRELESS SECURITY	HANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'	
WLANS WLANS	General Security QoS Policy-Mapping Adva	nced
Advanced	Authentication Survivability	
	Server 1 None	
	Server 3 None 0	
	Local EAP Authentication	
	Authentication priority order for web-auth user	
	Not Used	Order Used For Authentication
		RADIUS Up LOCA, Down

Passaggio 7. Passare alla scheda Advanced (Avanzate) nella scheda WLAN configuration (Configurazione WLAN) e abilitare Allow AAA Override (Consenti sostituzione AAA).

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MUNAGEMENT	COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'AireOS-DNASpaces'	
* WLANs WLANs	General Security QoS Policy-Mapping Advanced	
F Advanced	Alex AAA Override 📴 Enabled	Descr.
	Coverage Hole Detection 🖸 Enabled	DHCP Server Override
	Enable Session Timeout (Session Timeout (Seco)	DHCP Addr. Assignment 🔅 Required
	Angolat It	Management Frame Protection (MPP)
	Disprestic Channel M Enstead Override Interface ACL 3Pv4 None 2 1Pv6 None 2 Layer2 Acl None 2	MTP Class Protection # Optional E
	URL ACL None P2P Blocking Action Created Creat Exclusion 7 Created Structured States (Service)	802.114/m (1 - 215) 1 802.119/g/m (1 - 215) 1 844
	Havimum Alowed Clients 8	NRC State None B
	Static IP Turneling M Enabled Wi-N Direct Classics Policy Disabled	Client Load Balancing Client Band Select

Crea il portale in DNA Spaces

Passaggio 1. Fare clic su Captive Portals nel dashboard di DNA Spaces:



Passaggio 2. Fare clic su Crea nuovo, immettere il nome del portale e selezionare i percorsi che possono utilizzare il portale:

		0			
		Portal Information	Authentication	Data Capture	User Agreement
20	ISA, NAME				
	im05-DNASpaces				
1.000					
0	Enable this portal for all locations				
0	Enable this portal for all locations				
	Enable this portal for all locations Location Hierarchy			Select	ed Locations
	Enable this portal for all locations Location Hierarchy MEX-EAST-1			Select	d Locations
	Enable this portal for all locations Location Hierarchy MEX-EAST-1 © SS08-1-CMX			Select	Inclosed X
	Enable this portal for all locations Location Hierarchy MEX-EAST-1			Select	d Locations GracCorrect X
	Enable this portal for all locations Location Hierarchy MEX-EAST-1			Select	d Locations GraceConnect (X)

Passaggio 3. Selezionare il tipo di autenticazione, scegliere se si desidera visualizzare l'acquisizione dei dati e gli accordi utente nella home page del portale e se gli utenti possono scegliere di accettare la ricezione di un messaggio. Fare clic su Avanti:

troat themator	0	a Ins Gates	4 User Aproximity	×
BLUCT HE AUHENNOUND THE Email				
Value, needs subrit her end to access in-menet.		_		
Filmparane a chrun source				
	500	Part 1		

Passaggio 4. Configurare gli elementi di acquisizione dati. Se si desidera acquisire dati dagli utenti, selezionare la casella Abilita acquisizione dati e fare clic su +Aggiungi elemento campo per aggiungere i campi desiderati. Fare clic su Avanti:

	0		-0		×
	Partal Information	Authentication	Data Depters	Use Agreements	
El Enable Cala Capture Rom Fields				Additiate Genere	
🗠 📋 Kinst Name					
A Latiture					



Passaggio 5. Selezionare la casella di controllo Abilita termini e condizioni e fare clic su Salva e configura portale:

	Ø		_0	-0	×
	Portal Information	Automotive	Own Capture	Coast Representation	
This section allows you to enable and configure free	to & Conditions and Privacy policy 3	Merherbs.			
Contractive Terms 1. Conditions					
TUNKE & CORDITION MEEDADE					Qr 1 Digitit
0.9.0.0.2.0.0.0	9.5.8				
8 2 8 6 K K K B B C C	12 B A A A A A 4	$(-++) \in \mathbb{R} = 0$	0.4		
$ \mathrm{Sym} \to \mathrm{Ferm} \to \mathrm{Ferm} \to \mathrm{Sym} \to Sym$	A 0 2 01				
W-P. Serve of Use, Last updated September 17, 20	-0.				
Press Michigana & Constitute Of the (No. 1977)	million with the TERMS OF USE	power your use of the MLFI service.			
Description of the Banvice					
The Dentite provides you will extended access to the or posted using the Dentity to prove that users core	Internet within the providers. We do not, ply with these Wi-P. Torms and/or the lar	an an ordinary practice, prosthery re- s, although it reserves. The right to do t	unite ibe activities of these who us 0.	a the Danote or exercise any addicial control over	r ary naterial tanonified, hould
	0	5an - Pau -	ene & Centigure Pertui		

Passaggio 6. Modificare il portale come necessario, Fare clic su Salva:



Configura le regole del portale vincolato in Spazi DNA

Passaggio 1. Aprire il menu Captive Portal e fare clic su Captive Portal Rules:



Passaggio 2. Fare clic su + Crea nuova regola. Immettere il nome della regola, scegliere il SSID configurato in precedenza e selezionare le posizioni per cui è disponibile questa regola del

portale:

Create Captue Pontal Bule Institution AmOD-DARIgenies as any or all of the options that apply to your nale below	
When a user is on	Build West
OCATIONS - Where do you want the rule to live?	Sindi Were user is an Will and speeched in Alex
Aic any of the following locations	UNHORNER UDSHITCHS For all Incellance under 1983: 11 OncoOperant
Hills 1 Generalizational X	4,00143
Filter by Ministers Turber by Industry participation of the industry industry industry industry	50-40×43
	ACTON Show Cester Poter

Passaggio 3. Scegliere l'azione del portale vincolato. In questo caso, quando la regola viene trovata, viene visualizzato il portale. Fare clic su Salva e pubblica.

ACTIONS	AURINA
Show Capitie Fund Decade a Pund to be dispused to Decade and the second to the all AireOS-DBADgadess v Second Duration Bandwidth Limit Decade and to be advected at the second and the second at the sec	SOHEDALE ACTION Steles Capitus Rotar ParketRenOS: ONASpectra
Oury Internet Stop years from accounting the Internet	
Taga freez users an Choose - Australia Diseasciala users la choose tega. - + Aust Taga	
Tripper API	
Save & Publish Save	

Verifica

Per confermare lo stato di un client connesso all'SSID, selezionare Monitor > Client, fare clic sull'indirizzo MAC e cercare Policy Manager State:

MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	HANAGEMENT	COMMANDS	HELP	ELEDENCK	
Clients > Detail								< Back
Max Number of Record	s 10 • Ck	ar AVC Stats	J					
General AVC SI	atistics							
					AP radio slot	34	1	
Client Type	Repular				WLAN Profile	•	AireOS-DNASpaces	
Client Tunnel Type	Simple IP				WLAN SSID		AireOS-DNASpaces	
User Name					Status		Associated	
Webauth User Name	None				Association (Þ	1	
Port Number	1				802-11 Auth	entication	Open System	
Interface	management				Reason Code		1	
VLAN ID	20				Status Code		0	
Quarantine VLAN ID	0				CF Pollable		Not Implemented	
CCX Version	Not Supported				CF Poll Requ	est	Not Implemented	
E2E Version	Not Supported				Short Pream	ble	Not Implemented	
Mobility Role	Local				PBCC		Not Implemented	
Hobility Peer IP	N/A				Channel Api	ity	Not Implemented	
Mobility Hove Count	0				Timeout		0	
Policy Manager State	RUN				WEP State		WEP Disable	

Risoluzione dei problemi

Il seguente comando può essere attivato nel controller prima del test per confermare il processo di associazione e autenticazione del client.

<#root>
(5520-Andressi) >
debug client

(5520-Andressi) >

debug web-auth redirect enable mac

Di seguito viene riportato l'output di un tentativo riuscito di identificare ciascuna delle fasi durante il processo di associazione/autenticazione durante la connessione a un SSID senza server RADIUS:

Associazione/autenticazione 802.11:

*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION REQUEST *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 *apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode (1), Resu *apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0 station:34:e1

Autenticazione DHCP e di livello 3:

```
*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
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68 user_agent = A
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to configure
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual IP, us
*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://spl
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now https:/
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is now ht
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now https:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now https://splas
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is <HTML><HEAD><TITLE</pre>
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now https://splash.dn
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now https://splash.dnaspaces.io/p2/me
*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:
*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:
*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
```

Autenticazione di livello 3 completata. Spostare il client nello stato 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 t
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode (0), Res

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result (0), R
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully plumbed mobile

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).