

# 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



# DNA Spaces




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:

### General

Access List Name DNAspaces-ACL

Deny Counters 0

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	34.235.248.212 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
2	Permit	34.235.248.212 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0
3	Permit	0.0.0.0 / 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 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

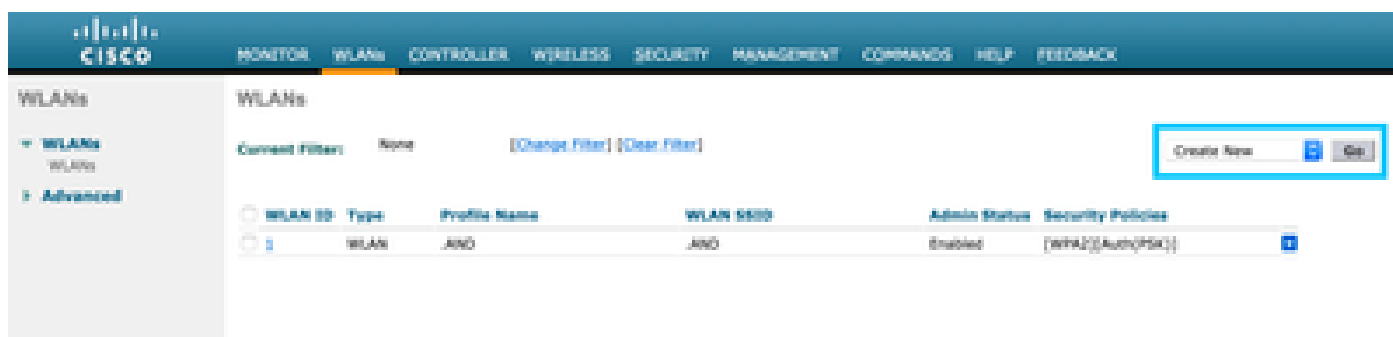
 Nota: per ottenere gli indirizzi IP degli spazi DNA da consentire nell'ACL, fare clic sull'opzione Configura manualmente dall'SSID creato nel passaggio 3 della sezione Creazione dell'SSID sugli spazi DNA nella sezione di configurazione dell'ACL.

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.





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.

The screenshot shows the Cisco WLAN configuration page for 'AireOS-DNASpaces'. The 'Security' tab is active, and the 'Layer 3' sub-tab is selected. The 'Layer 2 Security' dropdown menu is set to 'None'. Below it, 'MAC Filtering' is disabled. The 'Fast Transition' section is expanded, showing 'Fast Transition' set to 'Adaptive', 'Over the DS' checked, and 'Reassociation Timeout' set to 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.

The screenshot shows the Cisco WLAN configuration page for 'AireOS-DNASpaces'. The 'Security' tab is active, and the 'Layer 3' sub-tab is selected. The 'Layer 3 Security' dropdown menu is set to 'Web Policy'. Below it, 'Passthrough' is selected. The 'Preauthentication ACL' is set to 'IPv4' and 'DNASpaces-ACL'. The 'Redirect URL' is set to 'https://splash.dnaspaces.it/02/mxwssst1'. The 'Override Global Config' checkbox is checked and enabled.

 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

 sezione di configurazione SSID.

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

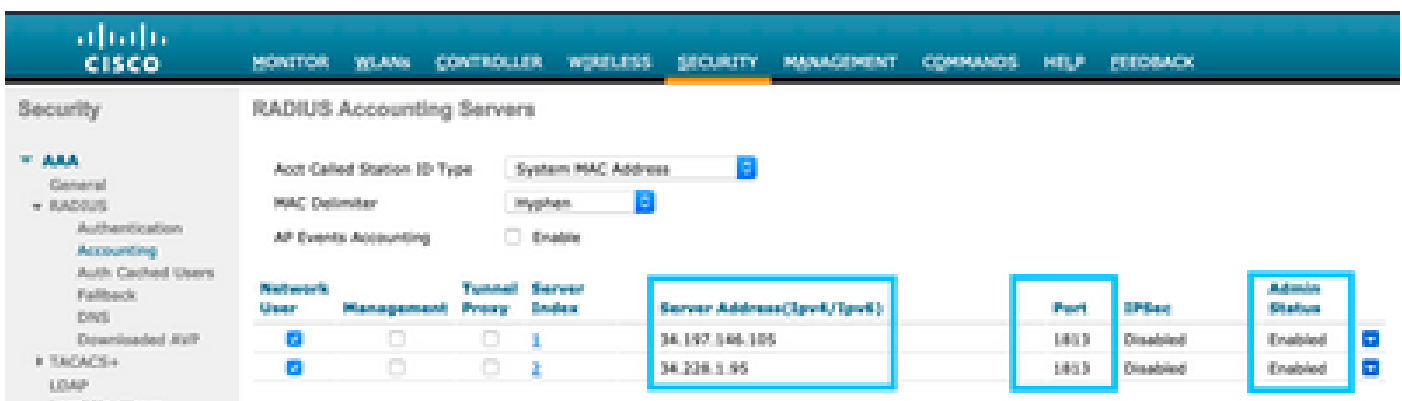
Passaggio 1. Selezionare Sicurezza > AAA > RADIUS > Autenticazione, fare clic su Nuovo e immettere le informazioni sul server RADIUS. Cisco DNA Spaces funge da server RADIUS per l'autenticazione degli utenti e può rispondere su due indirizzi IP. Configurare entrambi i server RADIUS:



Network User	Management	Tunnel Proxy	Server Index	Server Address(IPv4/IPv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	34.197.146.105	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	34.208.1.95	1812	Disabled	Enabled


 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:



Network User	Management	Tunnel Proxy	Server Index	Server Address(IPv4/IPv6)	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	34.197.146.105	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	34.208.1.95	1812	Disabled	Enabled

Configurazione SSID sul controller

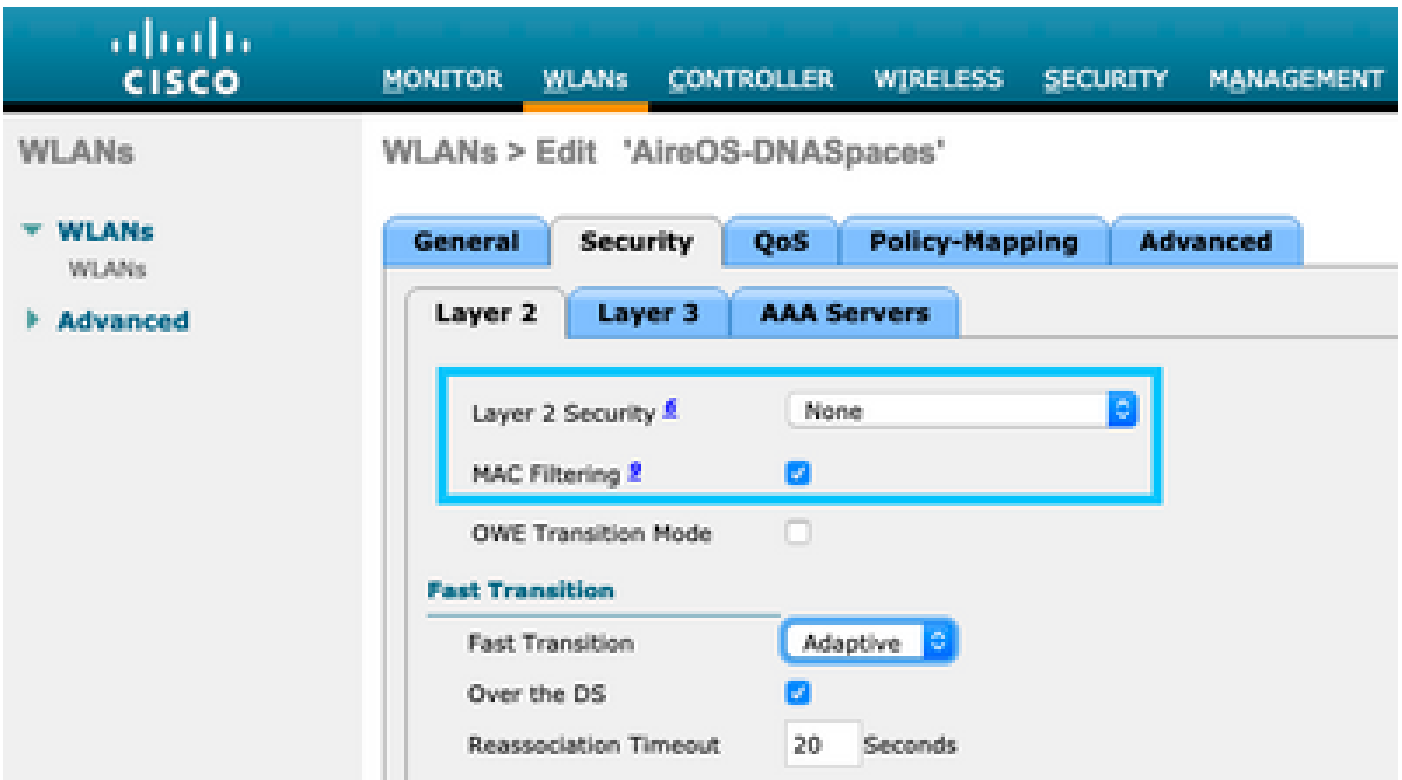
 **Importante:** prima di iniziare con la configurazione SSID, verificare che Autenticazione Web Radius sia impostata su "PAP" in Controller > Generale.

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.



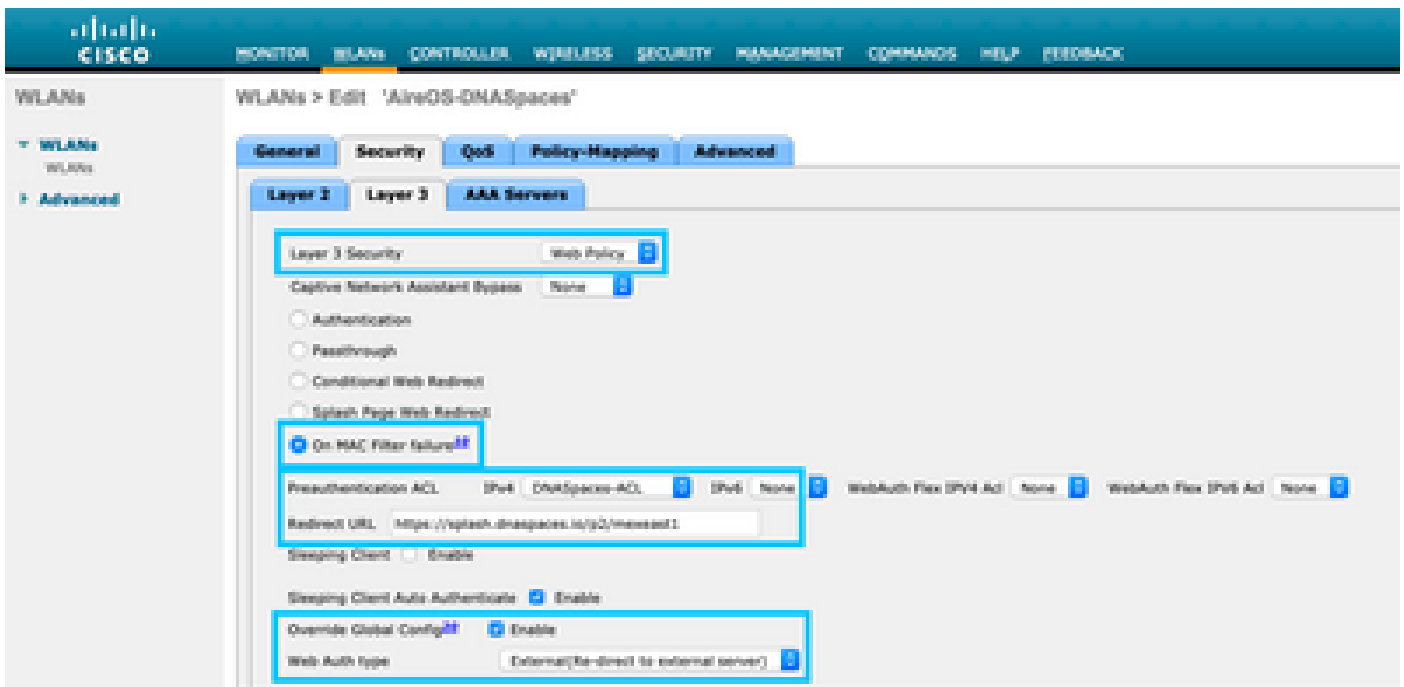
The screenshot shows the Cisco DNA Center interface for configuring WLANs. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows WLANs, with sub-items for WLANs and Advanced. The main content area displays a table of WLANs with columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. A 'Create New' button is highlighted with a red box.

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 Il Filtro Mac.

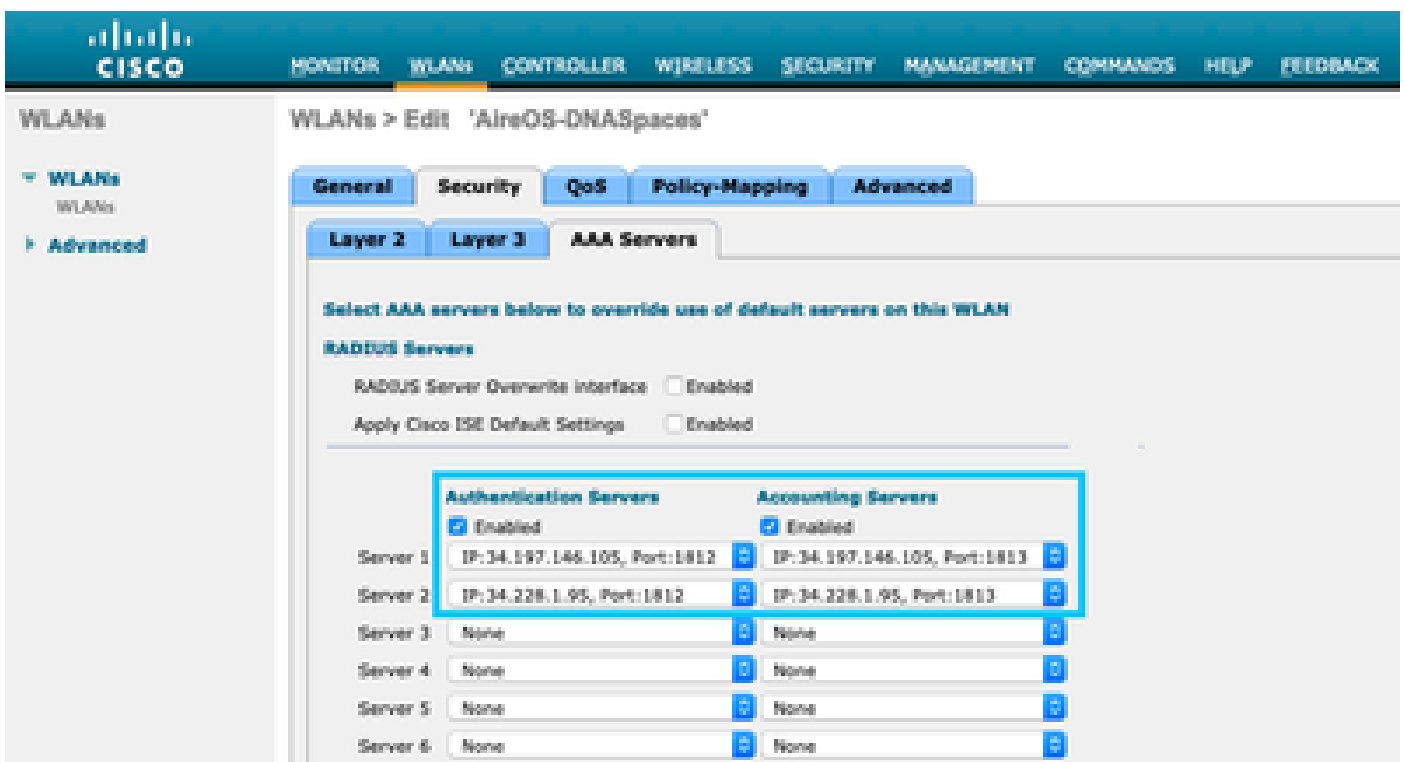


The screenshot shows the Cisco DNA Center interface for configuring the Security > Layer 2 settings for a WLAN. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The left sidebar shows WLANs, with sub-items for WLANs and Advanced. The main content area displays the 'WLANs > Edit 'AireOS-DNASpaces'' configuration page. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'None', and 'MAC Filtering' is checked. The 'Fast Transition' section shows 'Fast Transition' set to 'Adaptive', 'Over the DS' checked, and 'Reassociation Timeout' set to 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 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.

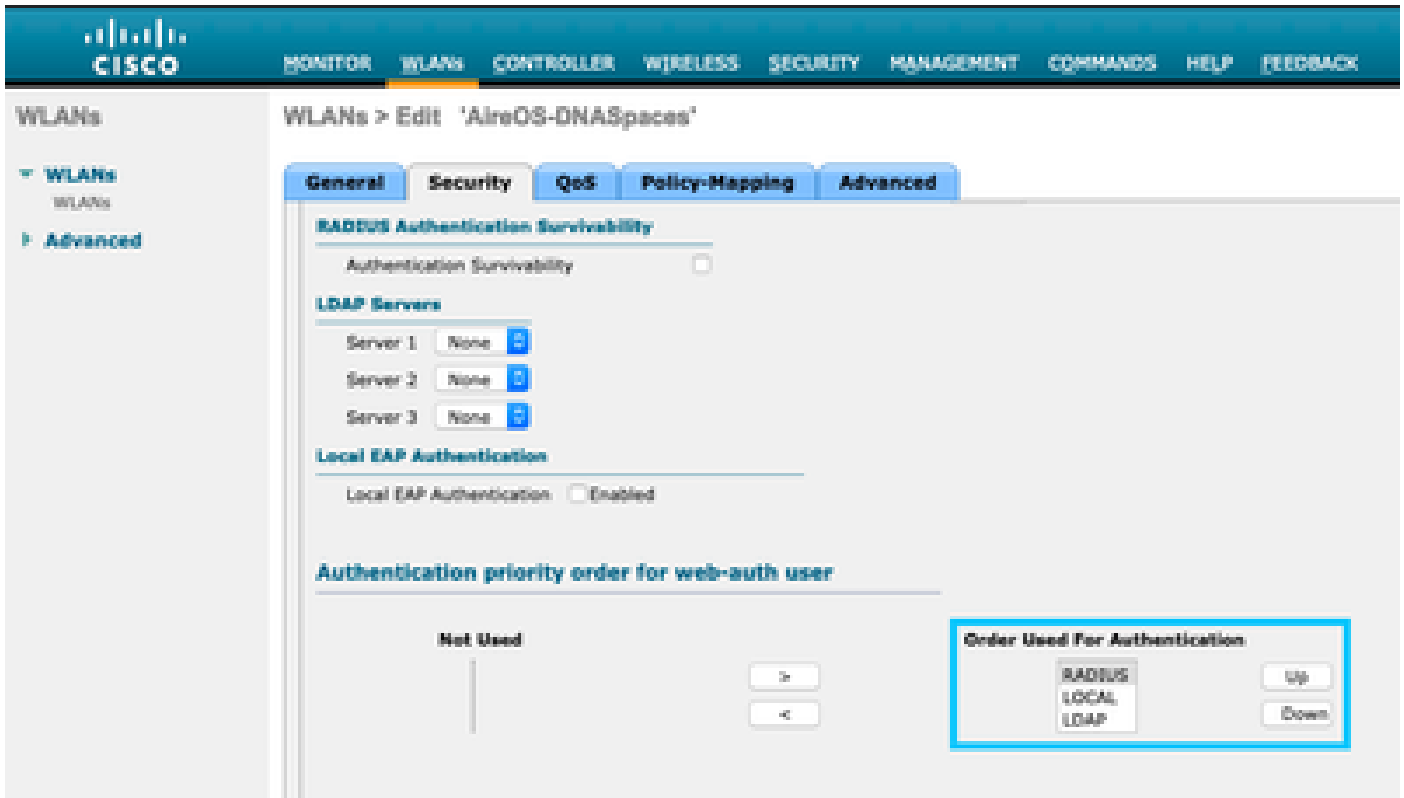


Passaggio 4. Configurare i server AAA. Passare alla scheda Sicurezza > Server AAA nella scheda Configurazione WLAN, abilitare Authentication Server e Accounting Server e dal menu a discesa scegliere i due server RADIUS:

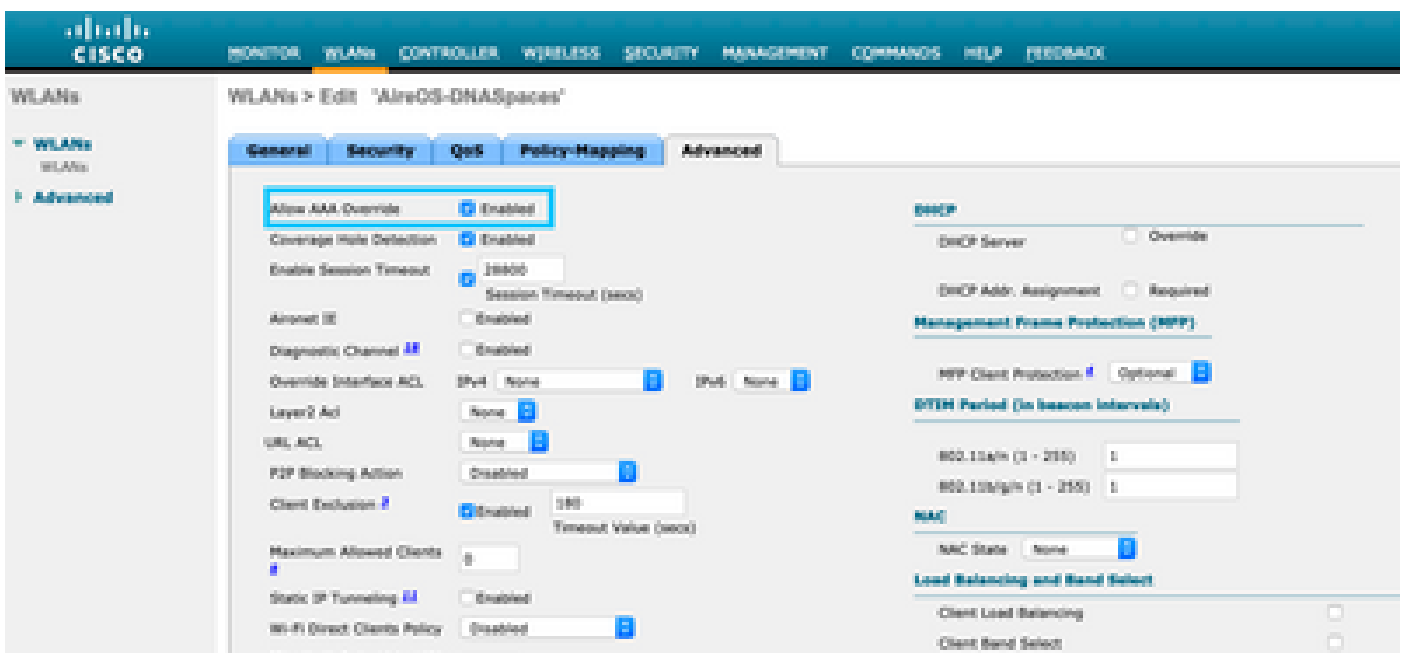


Passaggio 6. Configurare l'ordine di priorità di autenticazione per gli utenti di autenticazione Web. Selezionare la scheda Sicurezza > AAA Servers (Sicurezza > Server AAA) nella scheda WLAN configuration (Configurazione WLAN), quindi impostare RADIUS come prima opzione da ordinare.



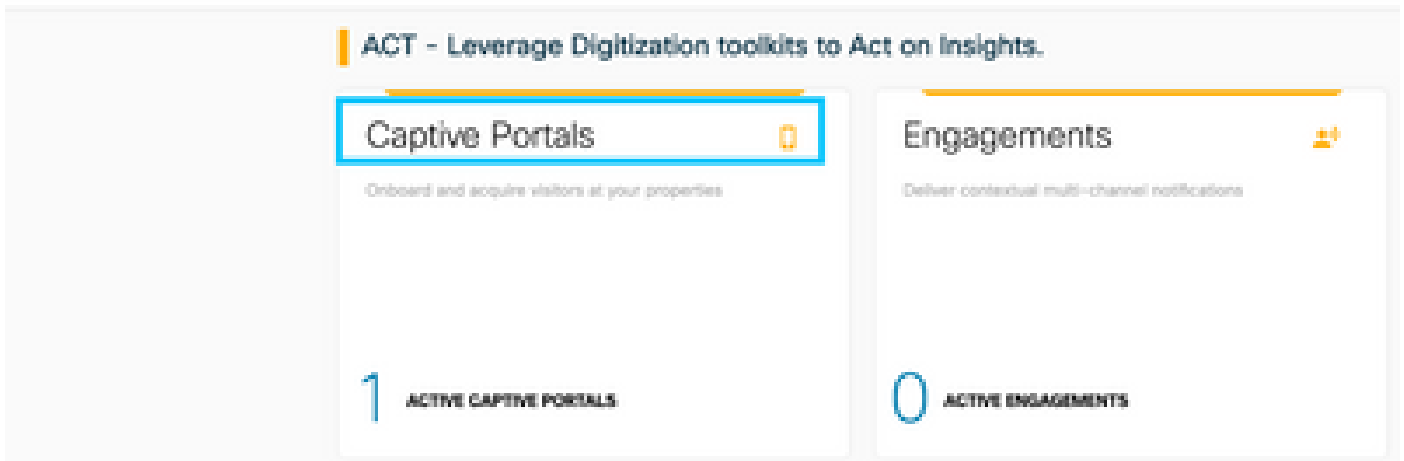


Passaggio 7. Passare alla scheda Advanced (Avanzate) nella scheda WLAN configuration (Configurazione WLAN) e abilitare Allow AAA Override (Consenti sostituzione AAA).

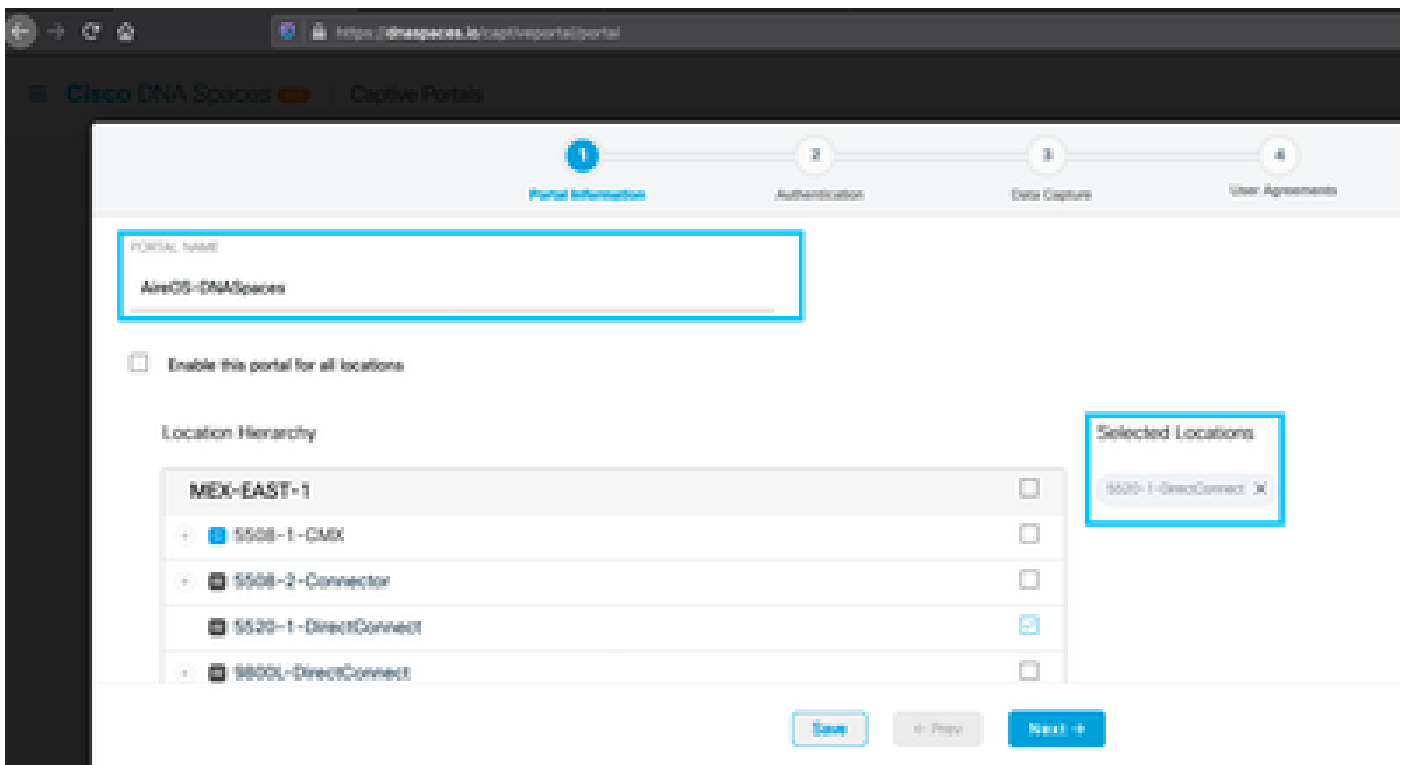


Crea il portale in DNA Spaces

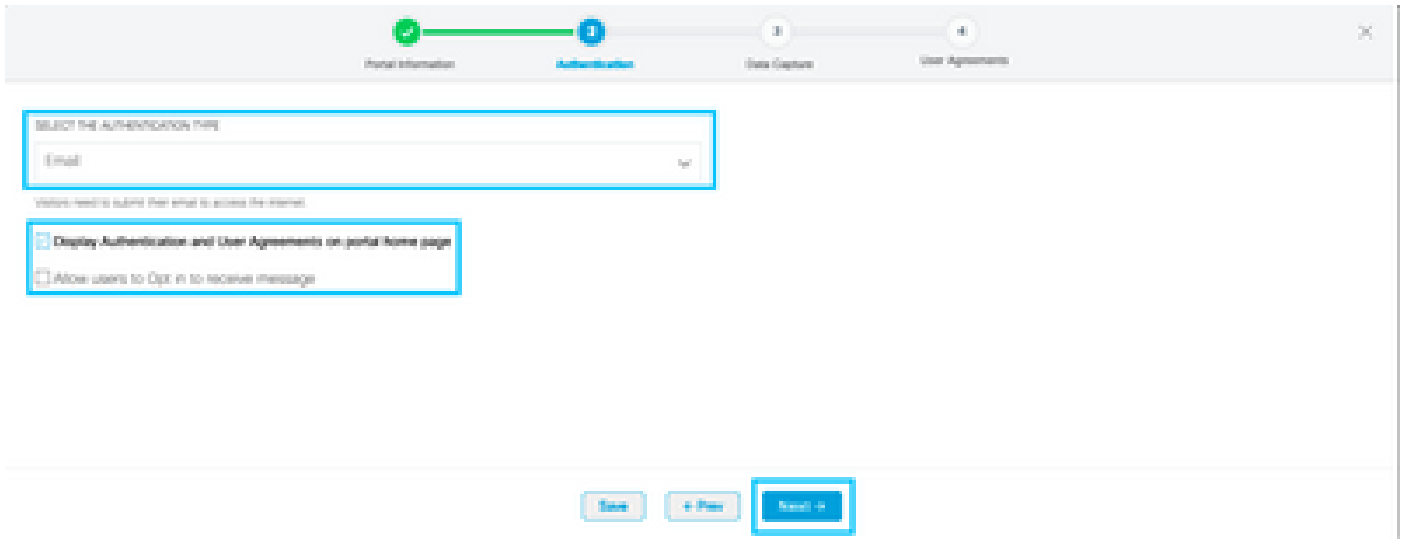
Passaggio 1. Fare clic su Captive Portals nel dashboard di DNA Spaces:



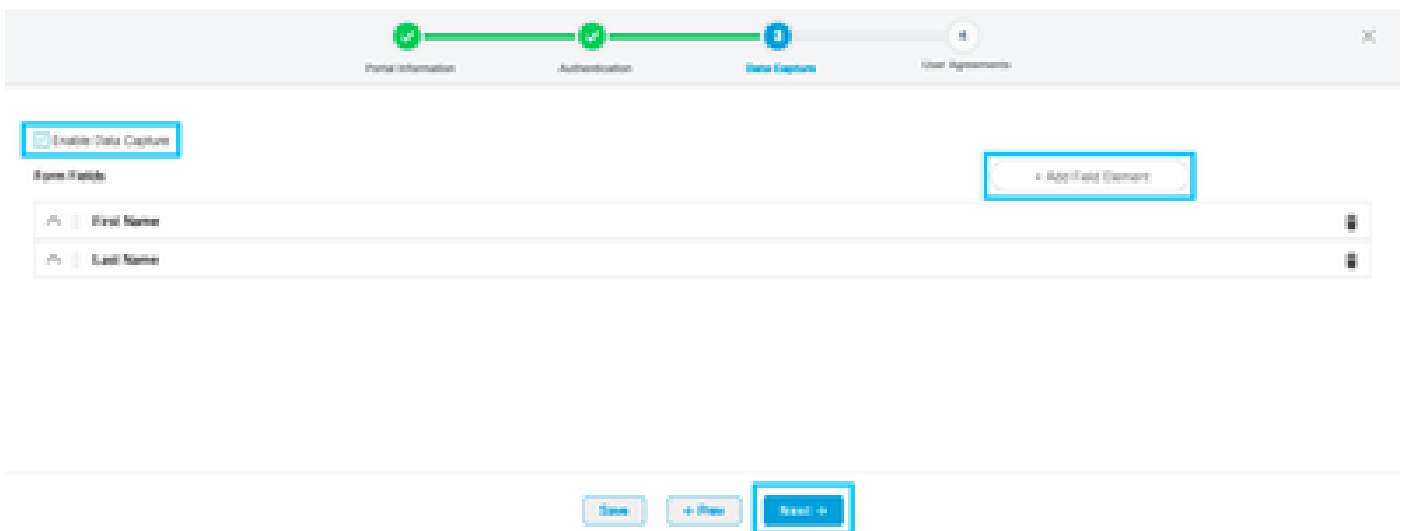
Passaggio 2. Fare clic su Crea nuovo, immettere il nome del portale e selezionare i percorsi che possono utilizzare il portale:



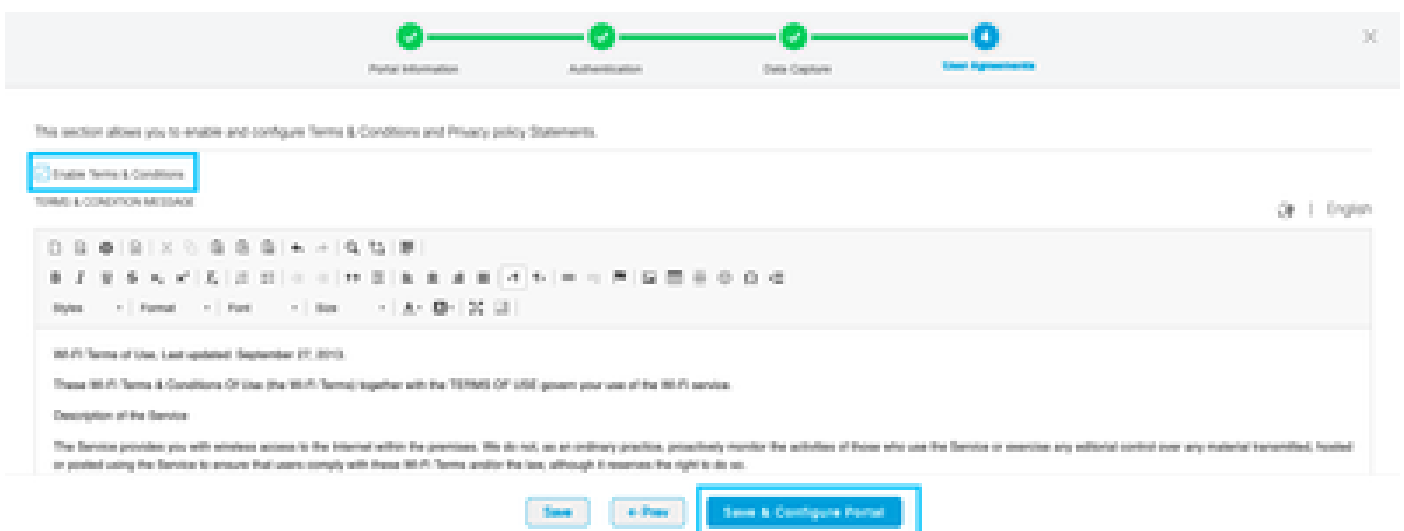
Passaggio 3. Selezionare il tipo di autenticazione, scegliere se si desidera visualizzare l'acquisizione dei dati e gli accordi utente nella home page del portale e se gli utenti possono scegliere di accettare la ricezione di un messaggio. Fare clic su Avanti:



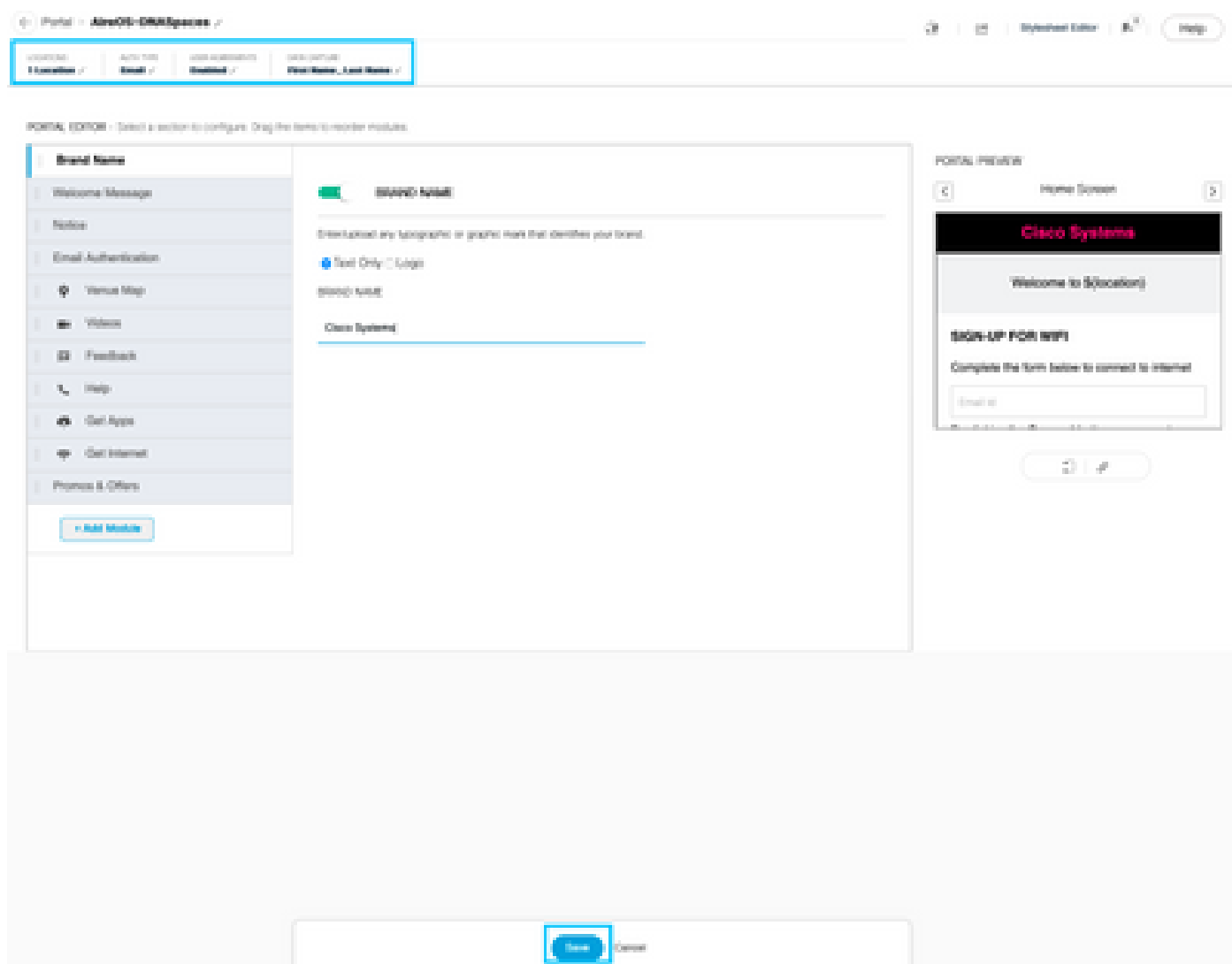
Passaggio 4. Configurare gli elementi di acquisizione dati. Se si desidera acquisire dati dagli utenti, selezionare la casella Abilita acquisizione dati e fare clic su +Aggiungi elemento campo per aggiungere i campi desiderati. Fare clic su Avanti:



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

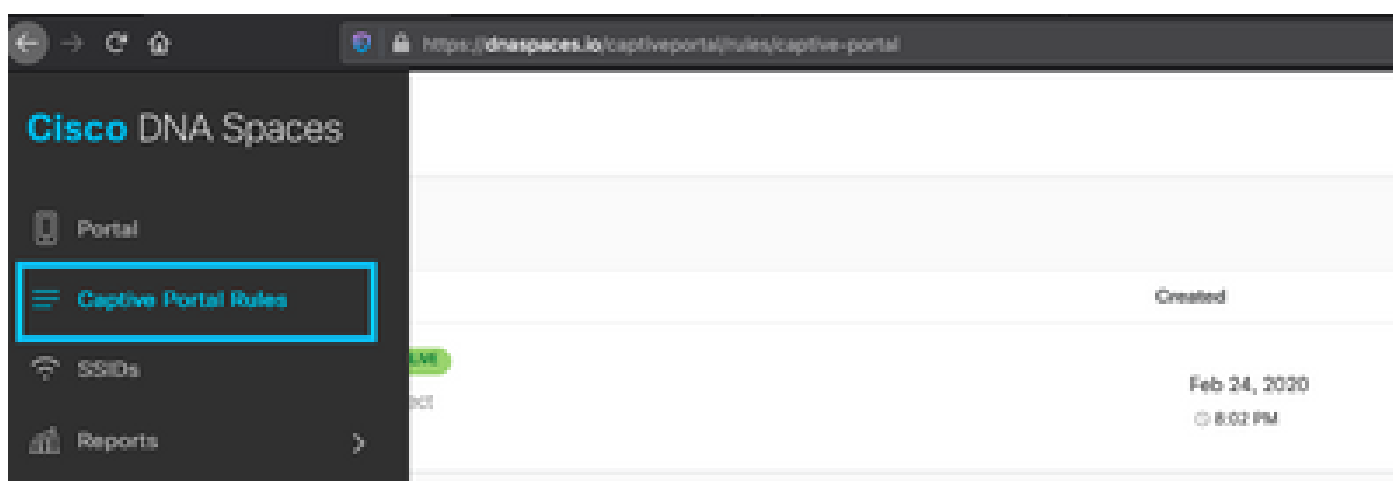


Passaggio 6. Modificare il portale come necessario, Fare clic su Salva:



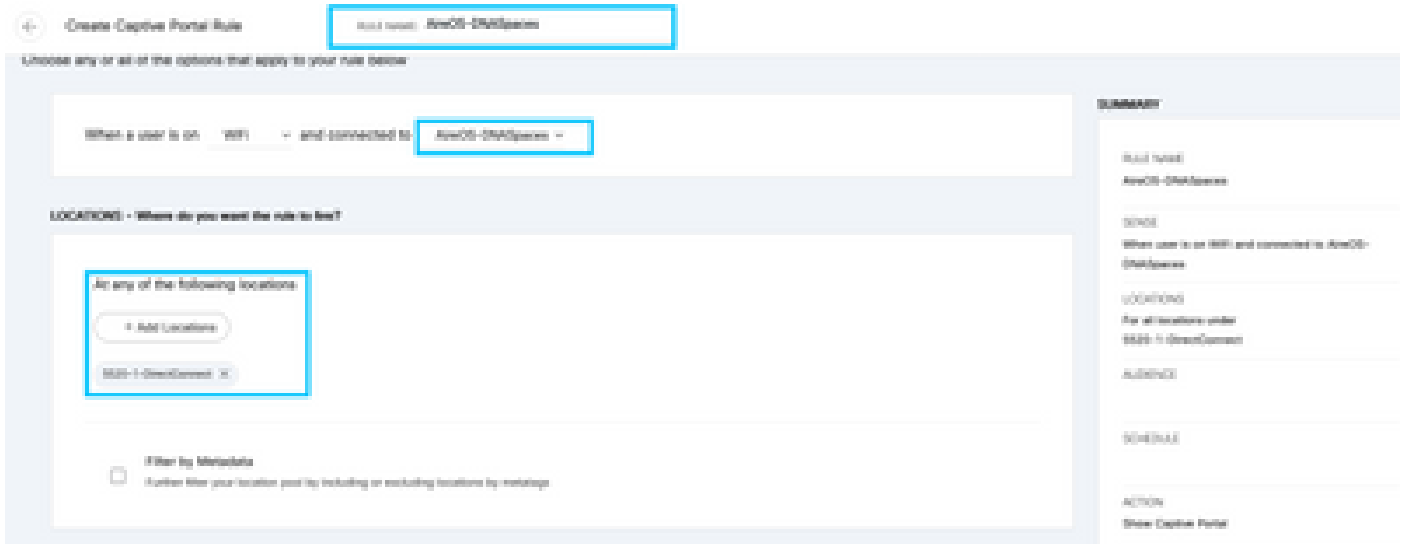
Configura le regole del portale vincolato in Spazi DNA

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 Captive Portal Rule

Rule Name: AireOS-DMZSystem

Choose any or all of the options that apply to your rule below

When a user is on: WiFi and connected to: AireOS-DMZSystem

LOCATIONS - Where do you want the rule to be?

All any of the following locations

+ Add Locations

SSID-1-DMZSystem

Filter by Metadata

Apply filter your location post by including or excluding locations by metadata

SUMMARY

Rule Name: AireOS-DMZSystem

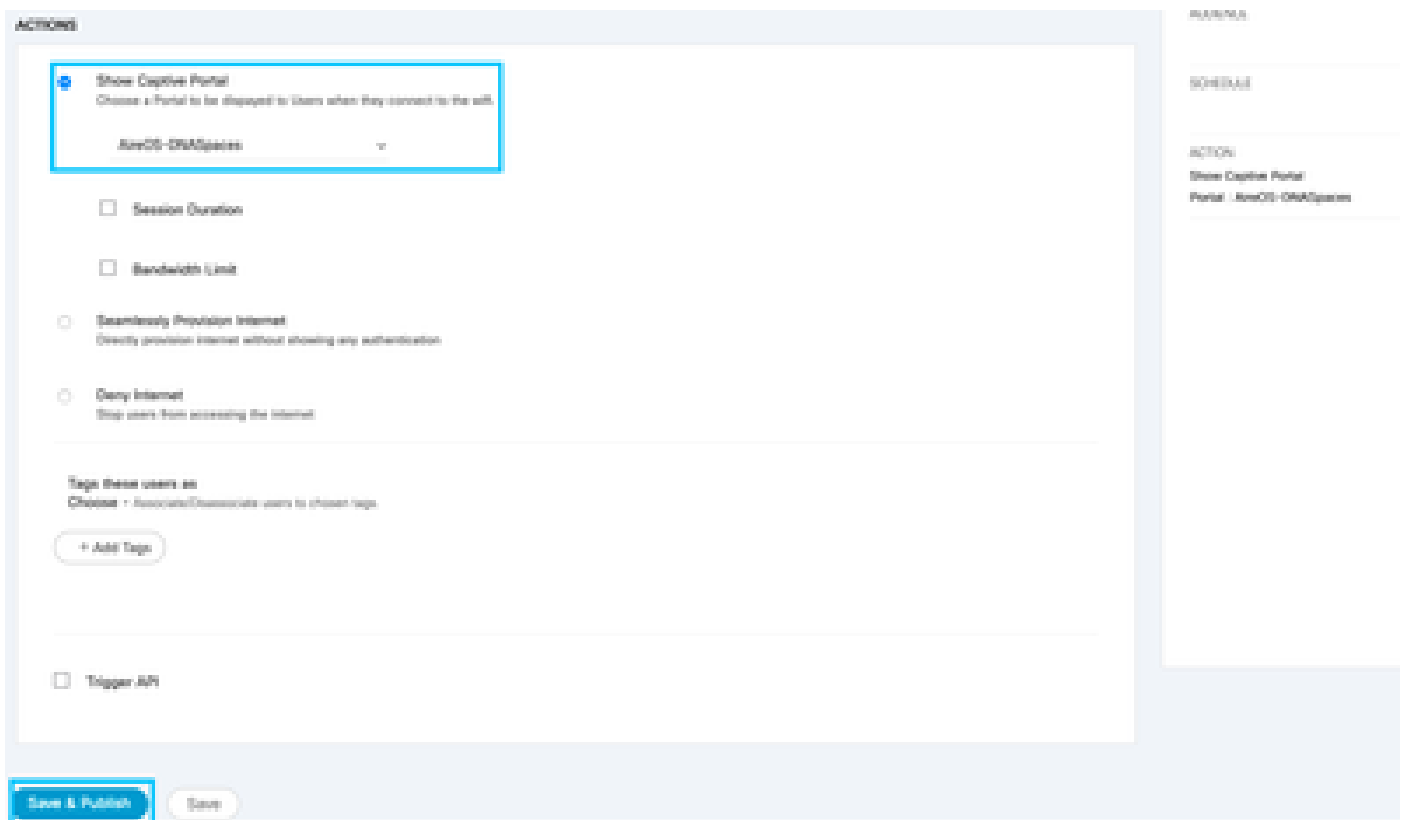
NAME: AireOS-DMZSystem

When user is on: WiFi and connected to: AireOS-DMZSystem

LOCATION(s): All any of the following locations under SSID-1-DMZSystem

ACTION: Show Captive Portal

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

Show Captive Portal

Choose a Portal to be displayed to Users when they connect to the wifi.

AireOS-DMZSystem

Session Duration

Bandwidth Limit

Seamlessly Provision Internet

Directly provision internet without showing any authentication

Deny Internet

Stop users from accessing the internet

Tag these users as

Choose a Resource to associate users to chosen tags

+ Add Tags

Trigger API

Save & Publish

Save

SUMMARY

SCHEDULE

ACTION

Show Captive Portal

Portal: AireOS-DMZSystem

## Verifica

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

Max Number of Records 10 

General		AVC Statistics	
Client Type	Regular	AP radio slot Id	1
Client Tunnel Type	Simple IP	WLAN Profile	AireOS-DNASpaces
User Name		WLAN SSID	AireOS-DNASpaces
Webauth User Name	None	Status	Associated
Port Number	1	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	20	Reason Code	1
Quarantine VLAN ID	0	Status Code	0
CCX Version	Not Supported	CF Pollable	Not Implemented
EDE Version	Not Supported	CF Poll Request	Not Implemented
Mobility Role	Local	Short Preamble	Not Implemented
Mobility Peer IP Address	N/A	RFCC	Not Implemented
Mobility Move Count	0	Channel Agility	Not Implemented
Policy Manager State	EUM	Timeout	0
		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 capability 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
*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), Resu
```

\*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 mobi  
\*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).