Configurazione di DNA Spaces Captive Portal con Catalyst 9800 WLC

Sommario

Introduzione

Questo documento descrive come configurare portali vincolati su Cisco DNA Spaces.

Prerequisiti

Questo documento consente ai client su Catalyst 9800 Wireless LAN Controller (C9800 WLC) di utilizzare DNA Spaces come pagina di accesso per l'autenticazione Web esterna.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso tramite interfaccia CLI (Command Line Interface) o GUI (Graphic User Interface) ai controller wireless 9800
- Cisco DNA Spaces

Componenti usati

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

- 9800-L controller versione 16.12.2s

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'autenticazione Web è un semplice metodo di autenticazione di layer 3 che non richiede un'utilità supplicant o client. È possibile eseguire questa operazione

a) Con la pagina interna sul WLC C9800 così com'è o dopo le modifiche

b) Con il bundle di accesso personalizzato caricato su C9800 WLC

c) Pagina di accesso personalizzata ospitata su un server esterno

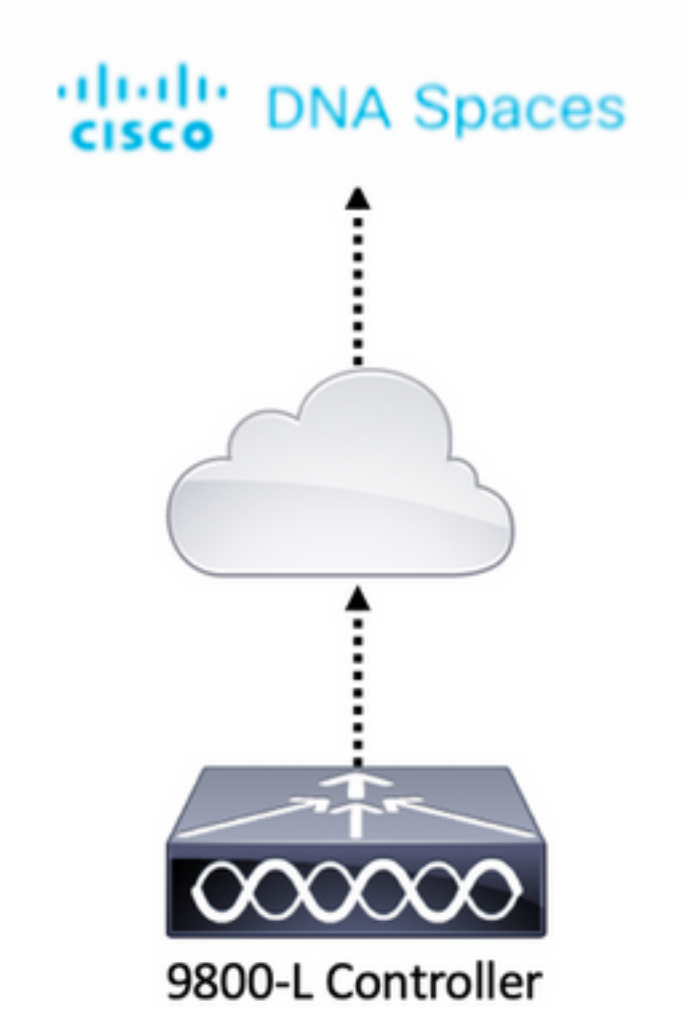
Utilizzare il portale vincolato fornito da DNA Spaces è essenzialmente un modo per implementare l'autenticazione Web esterna per i client su C9800 WLC.

Il processo webauth esterno è descritto in dettaglio all'indirizzo: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html

Sul WLC C9800, l'indirizzo ip virtuale viene definito come mappa dei parametri globali e in genere è 192.0.2.1

Configurazione

Esempio di rete



Collegare il controller 9800 a Cisco DNA Spaces

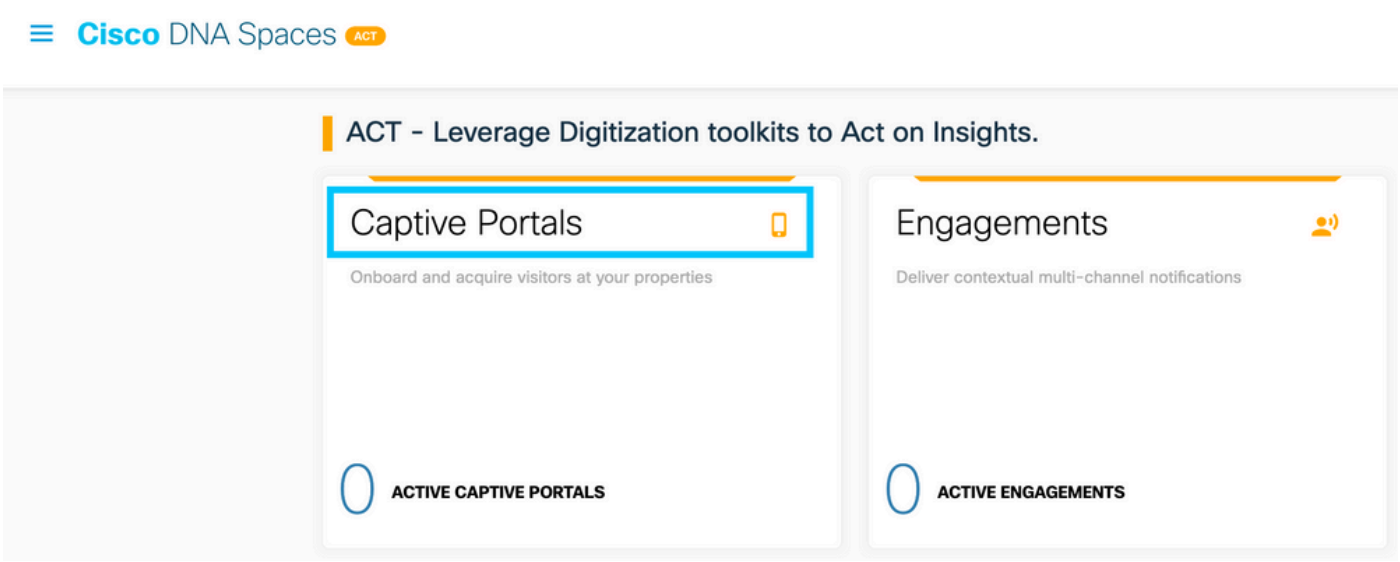
Il controller deve essere collegato a DNA Spaces tramite una delle opzioni disponibili: connessione diretta, connettore DNA Spaces o tethering CMX.

In questo esempio, l'opzione Connessione diretta è in uso, anche se i portali vincolati sono configurati nello stesso modo per tutte le impostazioni.

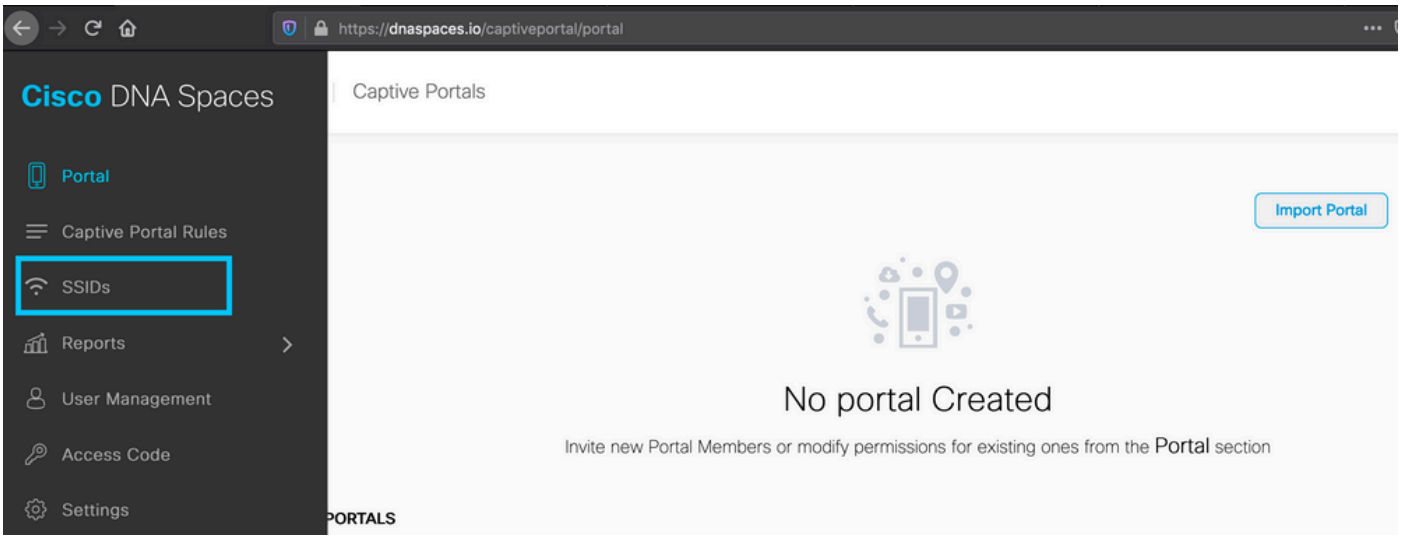
Per connettere il controller a Cisco DNA Spaces, deve essere in grado di raggiungere Cisco DNA Spaces Cloud su HTTPS. Per ulteriori informazioni su come collegare il controller 9800 a DNA Spaces, fare riferimento a questo collegamento: DNA Spaces - 9800 Controller Direct Connect

Crea il SSID in DNA Spaces

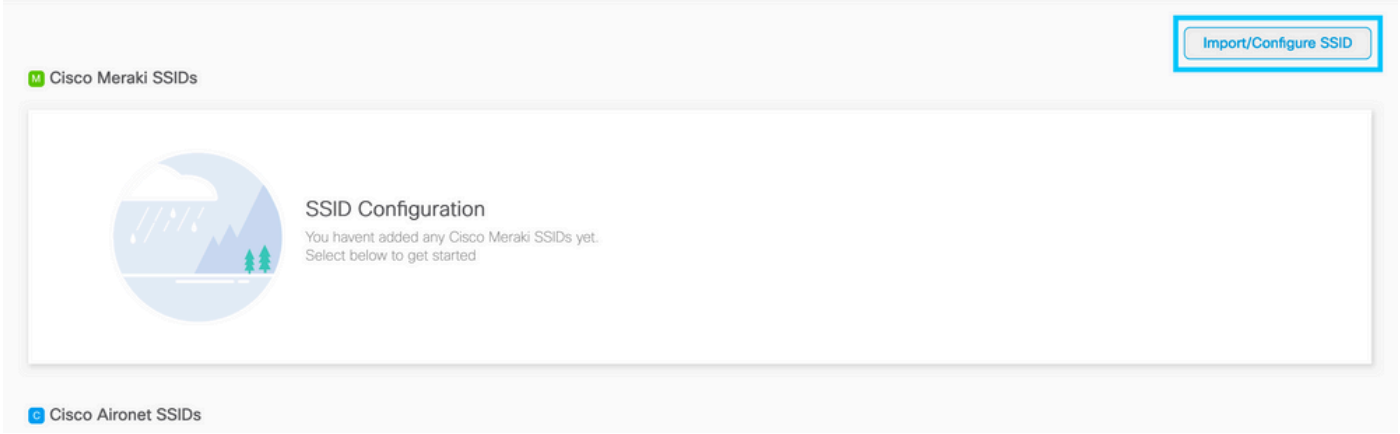
Passaggio 1. Fare clic su **Captive Portals** nel dashboard di DNA Spaces:



Passaggio 2. Aprire il menu specifico del portale vincolato, fare clic sull'icona a tre righe nell'angolo superiore sinistro della pagina e fare clic su **SSID:**



Passaggio 3. Fare clic su **Import/Configure SSID**, Select **CUWN (CMX/WLC)** (Importa/Configura SSID) come tipo "Wireless Network" (Rete wireless) e immettere il nome SSID:



Configurazione di ACL e filtro URL sul controller 9800

Il traffico proveniente da un client wireless non è consentito sulla rete fino al completamento dell'autenticazione. In caso di autenticazione Web, per completarla, un client wireless si connette

a questo SSID, riceve un indirizzo IP e quindi lo stato di gestione dei criteri client viene spostato nello stato **Webauth_reqd**. Poiché il client non è ancora autenticato, tutto il traffico proveniente dall'indirizzo IP del client viene interrotto ad eccezione di DHCP e DNS e HTTP (che viene intercettato e reindirizzato).

Per impostazione predefinita, lo switch 9800 crea ACL di preautenticazione hardcoded quando si configura una WLAN di preautenticazione Web. Questi ACL hardcoded consentono il DHCP, il DNS e il traffico verso il server Web Auth esterno. Tutto il resto viene reindirizzato come qualsiasi traffico http.
Tuttavia, se è necessario consentire l'accesso a uno specifico tipo di traffico non HTTP, è possibile configurare un ACL di preautenticazione. Sarà quindi necessario imitare il contenuto dell'ACL di pre-autenticazione hardcoded esistente (dal passaggio 1 di questa sezione) e aumentarlo in base alle proprie esigenze.

Passaggio 1. Verifica degli ACL hardcoded correnti

Configurazione CLI:

```
Andressi-9800L#show ip access list

Extended IP access list WA-sec-34.235.248.212
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any

Extended IP access list WA-v4-int-34.235.248.212
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212 viene chiamato come tale perché è un ACL o un indirizzo ip del portale con autenticazione Web automatica (WA) "34.235.248.212". Gli ACL di sicurezza hanno definito gli elementi consentiti (su autorizzazione) o eliminati (su negazione)

Wa-v4-int è un ACL di intercettazione, ossia un ACL punt o un ACL di reindirizzamento, che definisce ciò che viene inviato alla CPU per il reindirizzamento (su autorizzazione) o ciò che viene inviato al dataplane (su negazione).

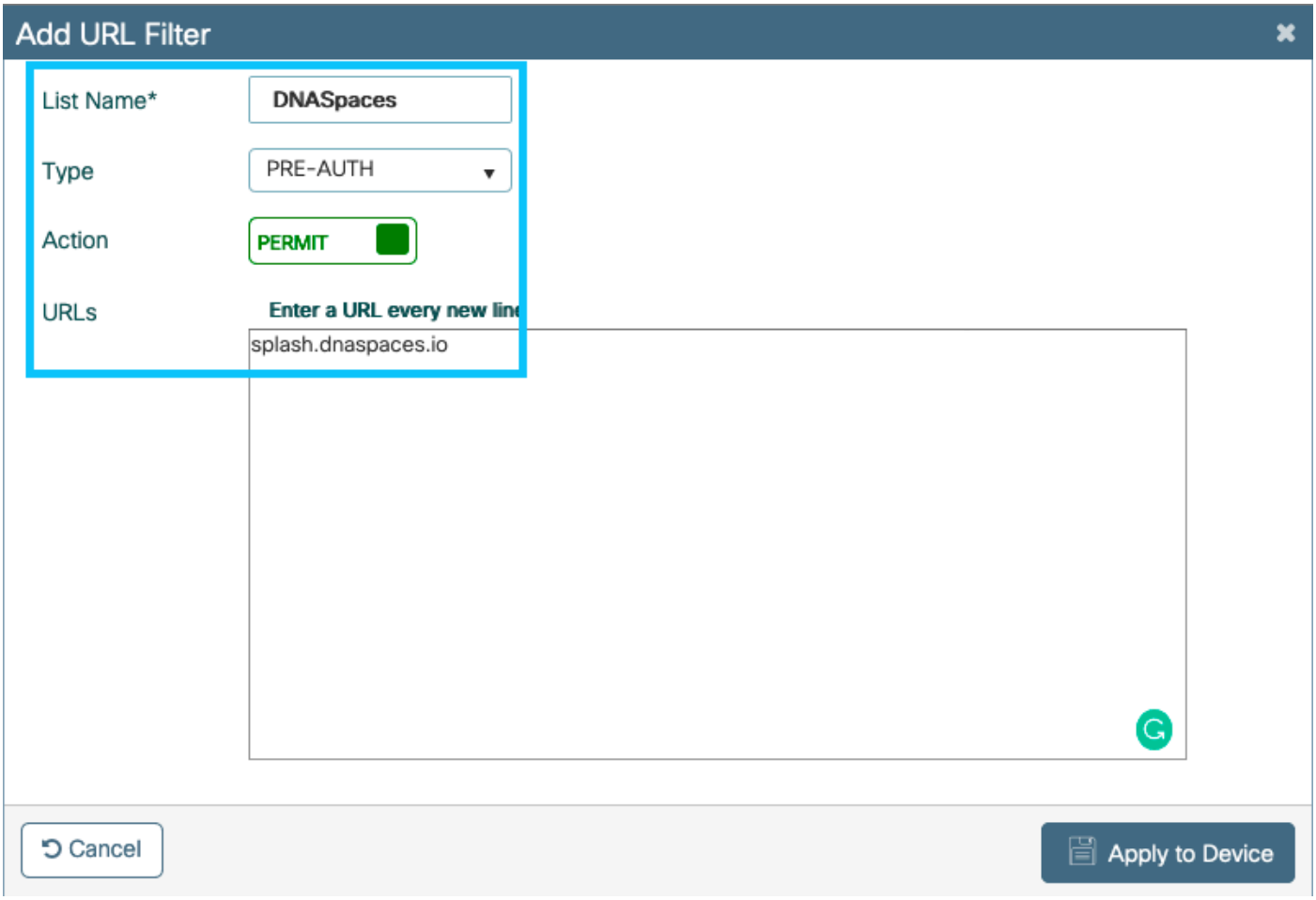
WA-v4-int34.235.248.212 viene applicato per primo sul traffico proveniente dal client e mantiene il traffico HTTP(s) verso il portale DNA Spaces IP 34.235.248.212 sul dataplane (non ancora drop o forward azione, appena consegnato al dataplane). Invia alla CPU (per il reindirizzamento ad eccezione del traffico IP virtuale servito dal server Web) tutto il traffico HTTP(s). Altri tipi di traffico vengono assegnati alla corsia dati.

WA-sec-34.235.248.212 consente il traffico HTTP e HTTPS verso lo spazio DNA IP 34.235.248.212 configurato nella mappa dei parametri di autenticazione Web, nonché il traffico DNS e DHCP e il resto viene eliminato. Il traffico HTTP da intercettare è già stato intercettato prima di raggiungere questo ACL. Pertanto, non è necessario che il traffico venga coperto da questo ACL.

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. Un esempio si trova nella sezione "Quali sono gli indirizzi IP utilizzati da DNA Spaces" alla fine del documento.

DNA Spaces utilizza 2 indirizzi IP e il meccanismo della fase 1 consente di autorizzare un solo indirizzo IP di portale. Per consentire l'accesso in fase di preautenticazione a più risorse HTTP, è necessario utilizzare i filtri URL che causano in modo dinamico dei buchi negli ACL di intercettazione (reindirizzamento) e di sicurezza (preautenticazione) per gli IP correlati al sito Web di cui si immette l'URL nel filtro URL. Le richieste DNS vengono dinamicamente "snooping" affinché il router 9800 possa conoscere l'indirizzo IP di questi URL e aggiungerlo dinamicamente agli ACL.

Passaggio 2. Configurare il filtro URL per consentire il dominio DNA Spaces. Passare a Configurazione > Protezione > Filtri URL, fare clic su **+Aggiungi** e configurare il nome dell'elenco, selezionare **PRE-AUTH** come tipo, azione come **PERMIT** e URL **splash.dnaspaces.io** (o .eu se si utilizza il portale EMEA):



Configurazione CLI:

```
Andressi-9800L(config)#urlfilter list
```

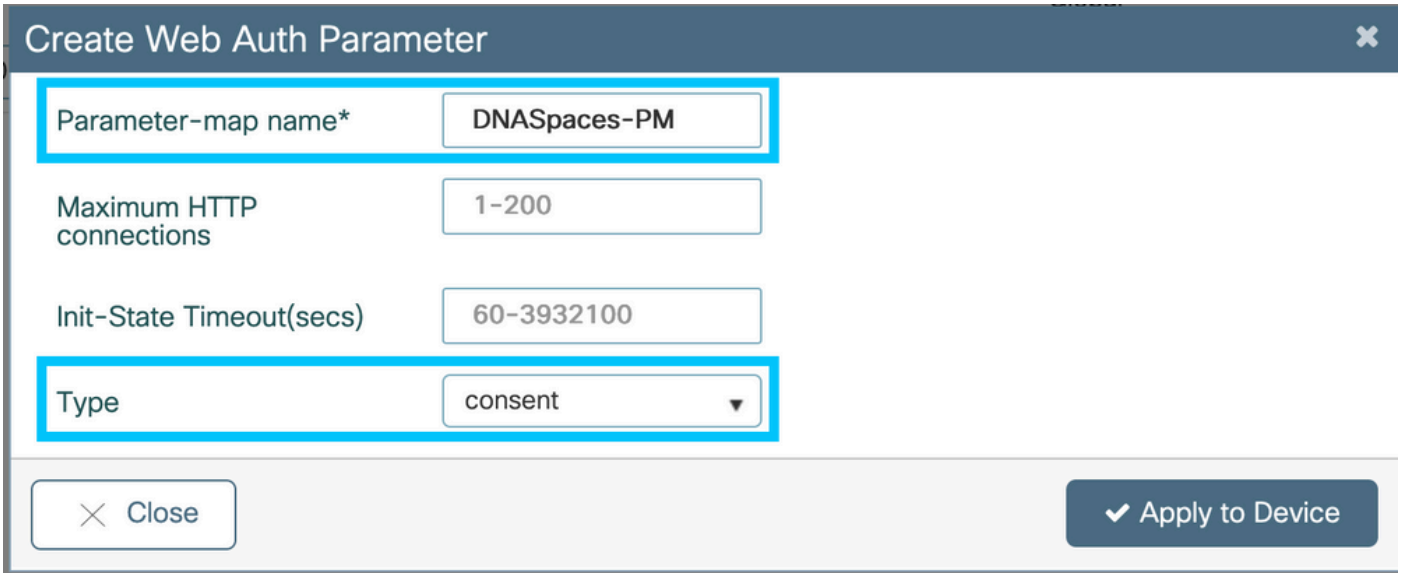
```
Andressi-9800L(config-urlfilter-params)#action permit
Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io
```

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 vincolato, 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.

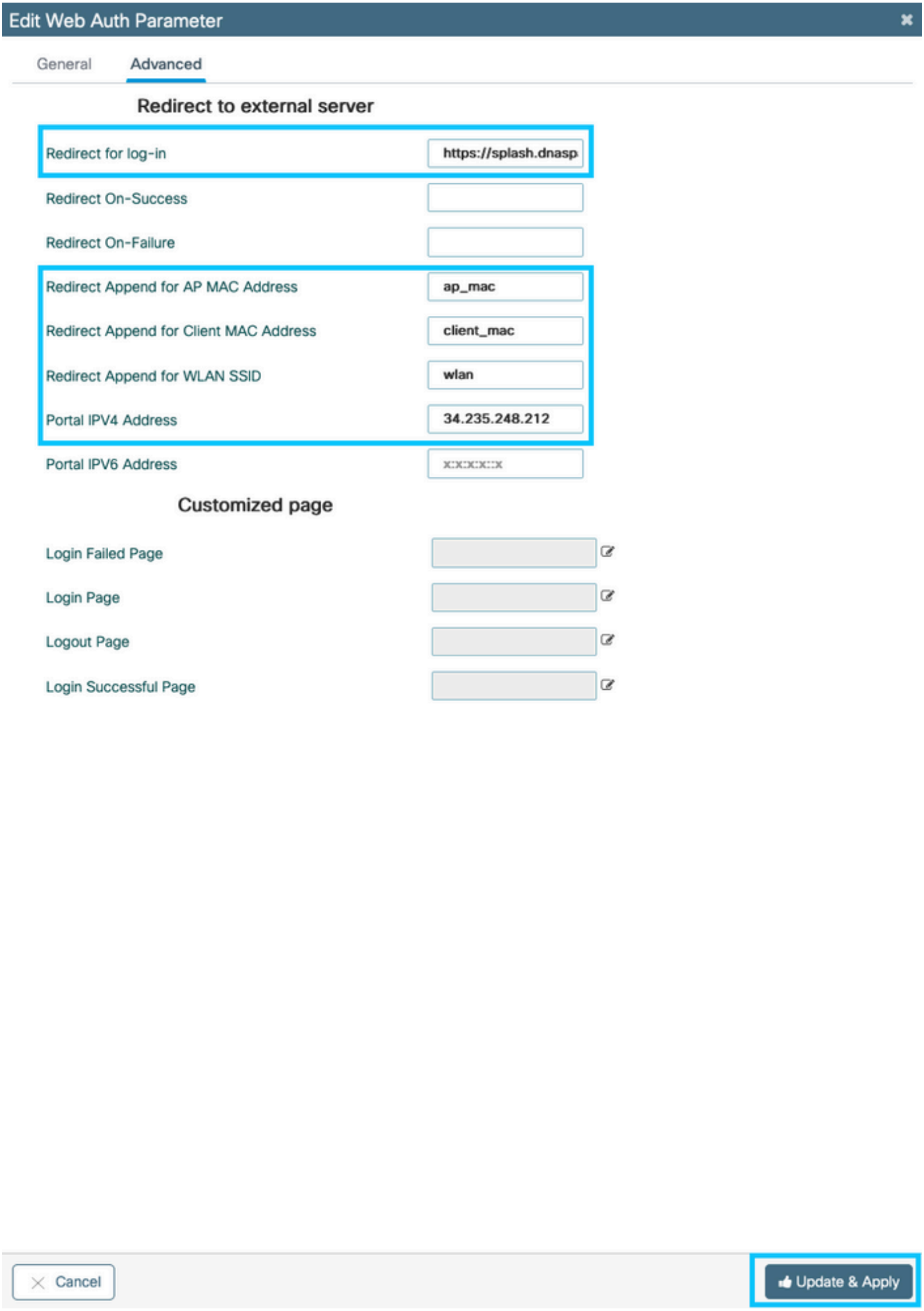
Portale vincolato senza server RADIUS su spazi DNA

Configurazione mappa parametri autenticazione Web sul controller 9800

Passaggio 1. Passare a **Configurazione > Protezione > Autenticazione Web**, quindi fare clic su **+Aggiungi** per creare una nuova mappa dei parametri. Nella finestra che viene visualizzata, configurare il nome della mappa dei parametri e selezionare **Consenso** come tipo:



Passaggio 2. Fare clic sulla mappa dei parametri configurata nel passaggio precedente, passare alla scheda **Avanzate** e immettere il Reindirizzamento per l'URL di accesso, Aggiungi per indirizzo MAC AP, Aggiungi per indirizzo MAC client, Aggiungi per SSID WLAN e indirizzo IPv4 del portale come illustrato Fare clic su **Aggiorna e applica:**


Edit Web Auth Parameter
General
Advanced
Redirect to external server
Redirect for log-in
https://splash.dnasp
Redirect On-Success
Redirect On-Failure
Redirect Append for AP MAC Address
ap_mac
Redirect Append for Client MAC Address
client_mac
Redirect Append for WLAN SSID
wlan
Portal IPV4 Address
34.235.248.212
Portal IPV6 Address
X:X:X:X::X
Customized page
Login Failed Page
Login Page
Logout Page
Login Successful Page
Cancel
Update & Apply

Nota: per ottenere l'URL della pagina iniziale e l'indirizzo di reindirizzamento IPv4, fare clic sull'opzione **Configura manualmente** nella pagina SSID di DNA Spaces. Questo è illustrato nella sezione "Qual è l'URL utilizzato dal portale DNA Spaces?" alla fine del documento

Nota: il portale Cisco DNA Spaces può essere risolto in due indirizzi IP, ma il controller 9800 consente di configurare un solo indirizzo IP, scegliere uno di questi indirizzi IP e configurarlo sulla mappa dei parametri come indirizzo IPv4 del portale.

Nota: assicurarsi che gli indirizzi IPv4 e IPv6 virtuali sono configurati nella mappa dei parametri di autenticazione Web globale. Se l'IPv6 virtuale non è configurato, i client vengono talvolta reindirizzati al portale interno anziché al portale di Spazi DNA configurato. Per questo motivo è necessario configurare sempre un IP virtuale. "192.0.2.1" può essere configurato come Virtual IPv4 e FE80:0:0:0:903A::11E4 come Virtual IPV6. L'utilizzo di IP diversi da quelli non è giustificato per motivi diversi.

Configurazione CLI:

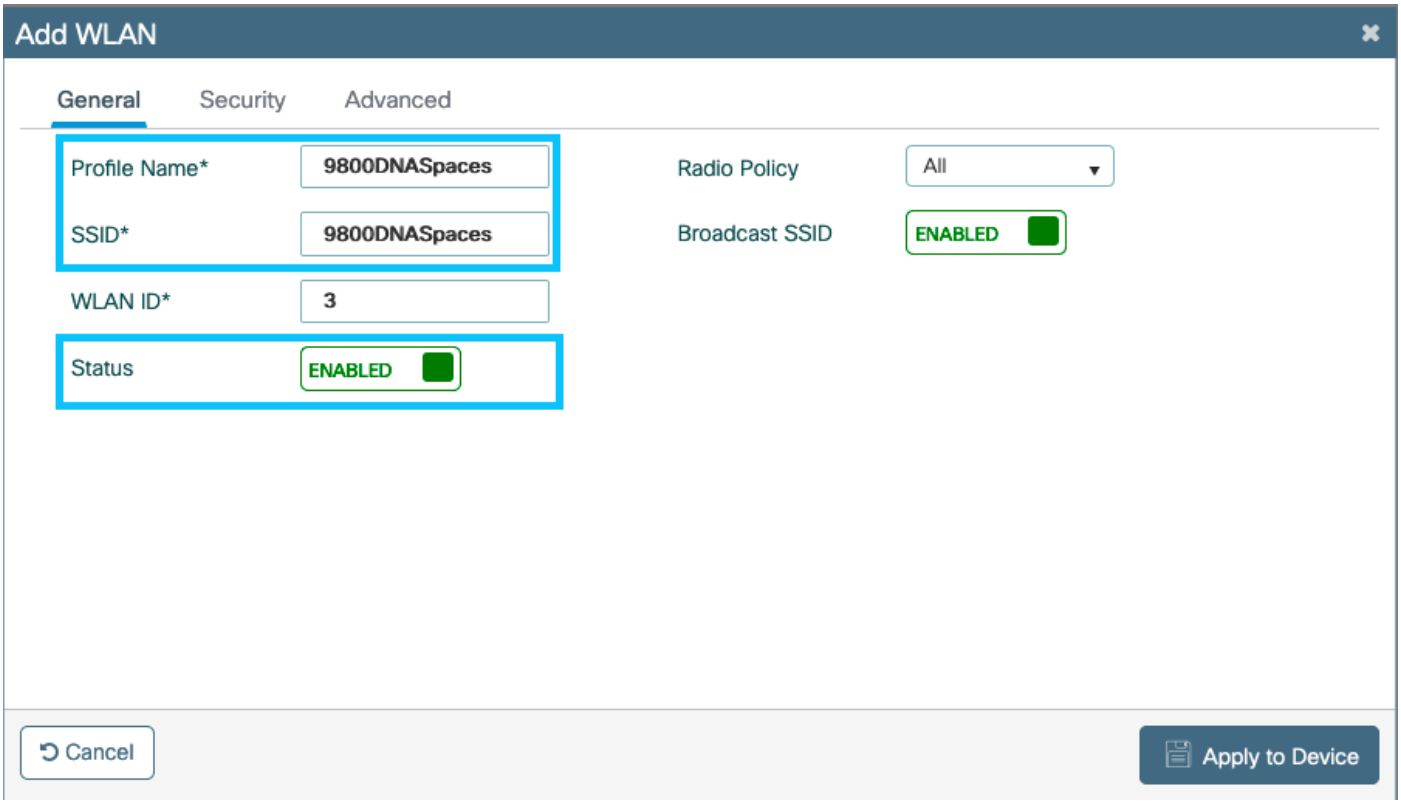
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

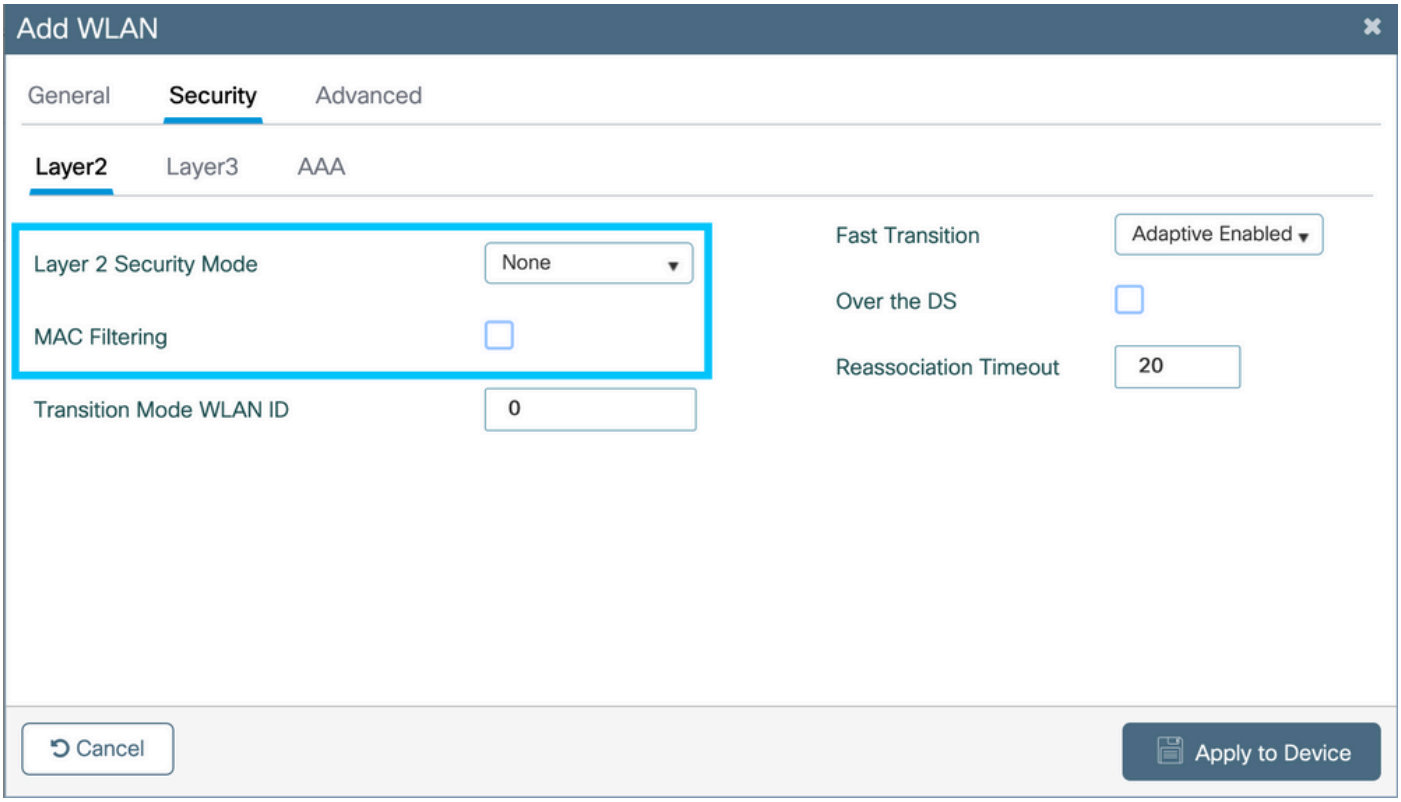
```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

Creare l'SSID sul controller 9800

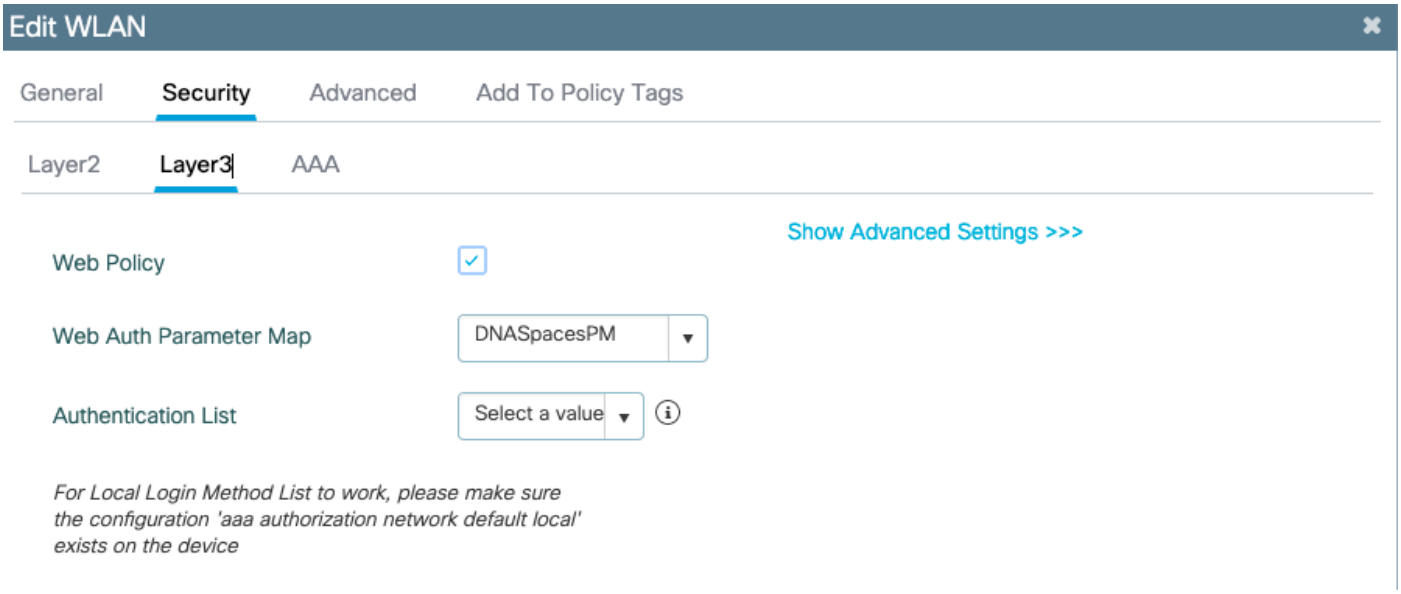
Passaggio 1. Selezionare **Configurazione > Tag e profili > WLAN**, quindi fare clic su **+Aggiungi.** Configurare il nome del profilo, l'SSID e abilitare la WLAN. Verificare che il nome SSID sia uguale al nome configurato nel passaggio 3 della sezione **Creazione del SSID in Spazi DNA.**



Passaggio 2. Passare a **Sicurezza > Layer2.** Impostare la modalità di sicurezza del layer 2 su **None e** verificare che il filtro MAC sia disabilitato.

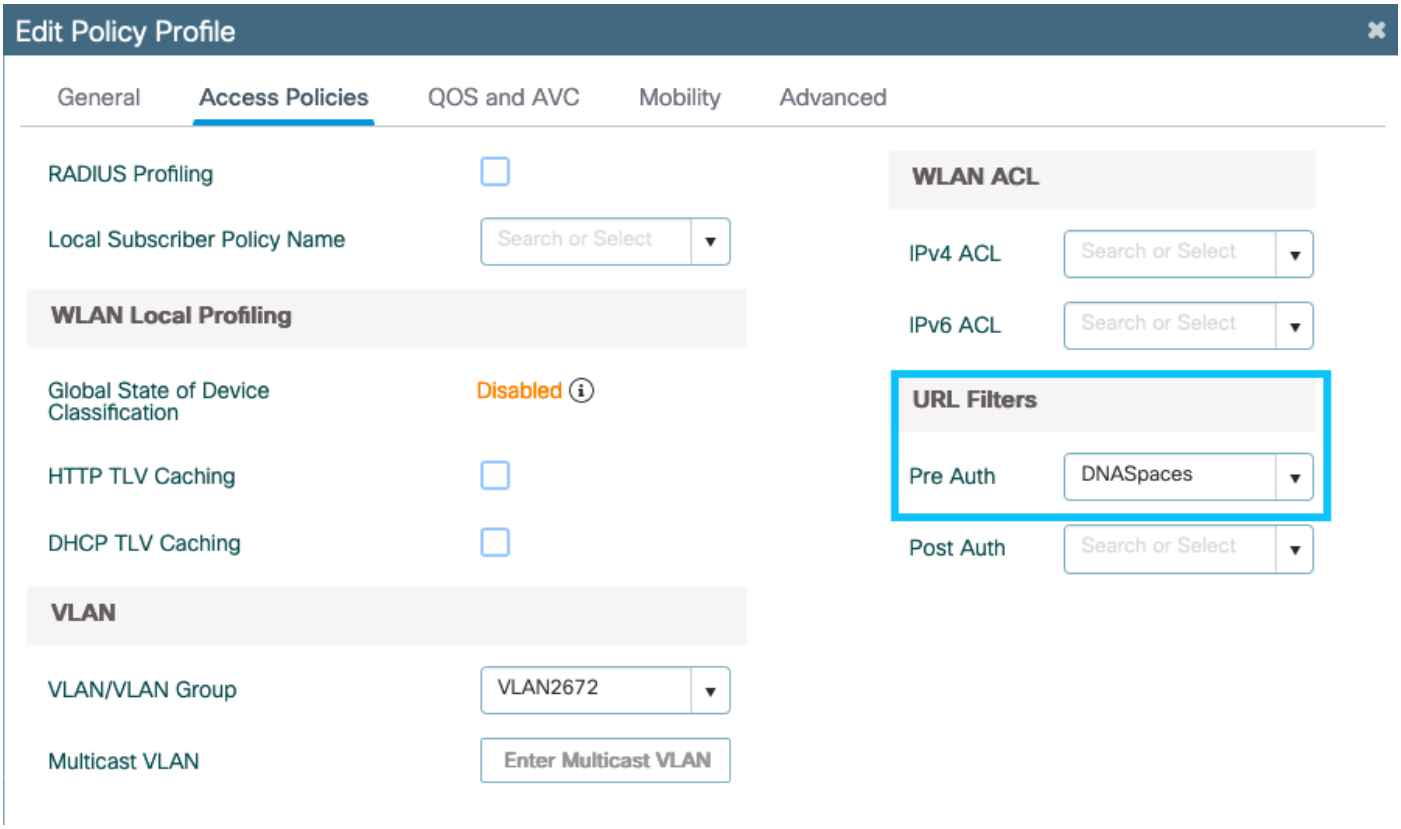


Passaggio 3. Selezionare **Protezione > Layer3.** Abilita criterio Web, configura la mappa dei parametri di autenticazione Web. Fare clic su **Applica alla periferica**.



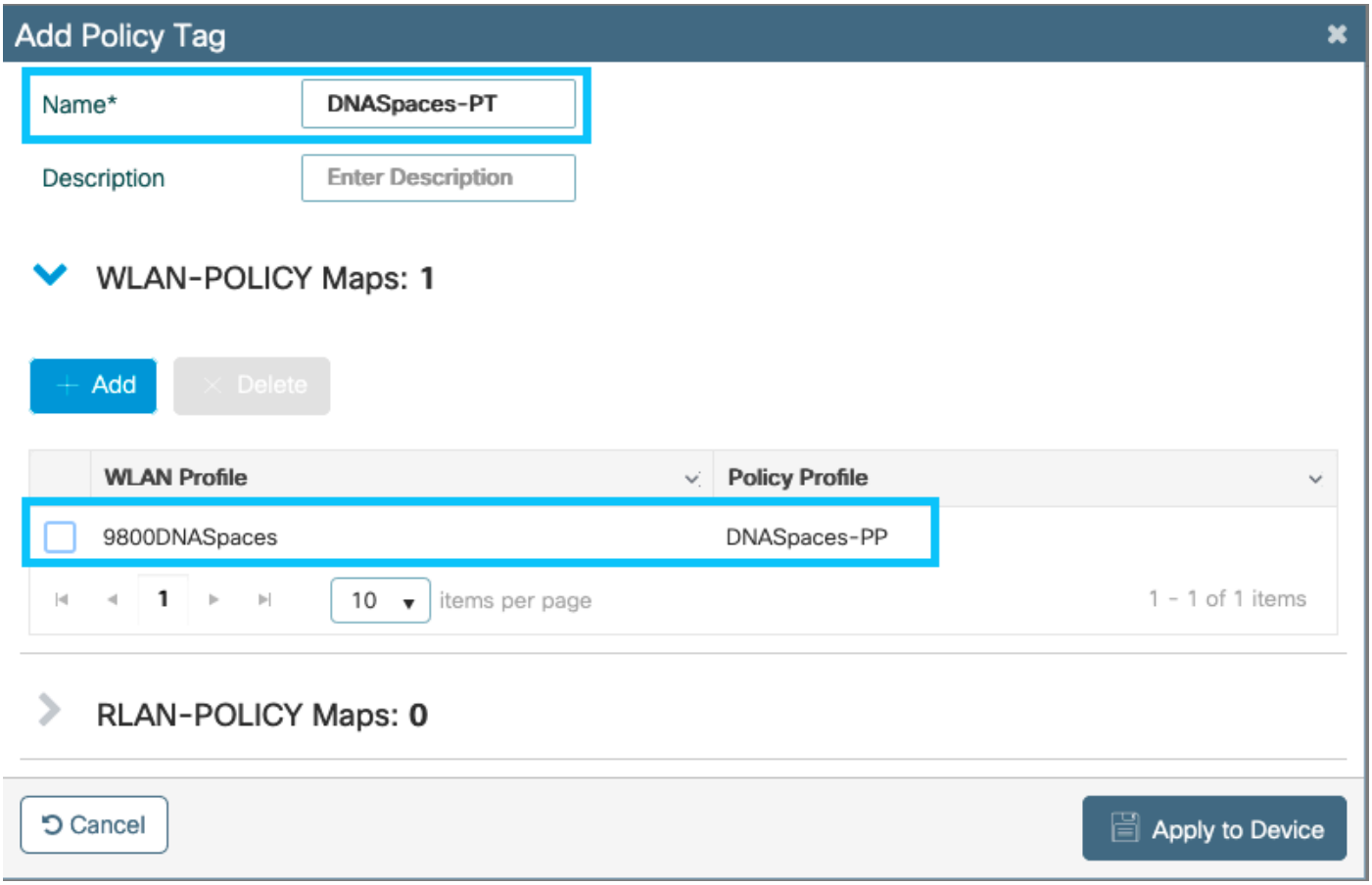
Configurazione del profilo criteri sul controller 9800

Passaggio 1. Passare a **Configurazione > Tag e profili > Criterio** e creare un nuovo Profilo criterio oppure utilizzare il Profilo criterio predefinito. Nella scheda Criteri di accesso configurare la VLAN client e aggiungere il filtro URL.

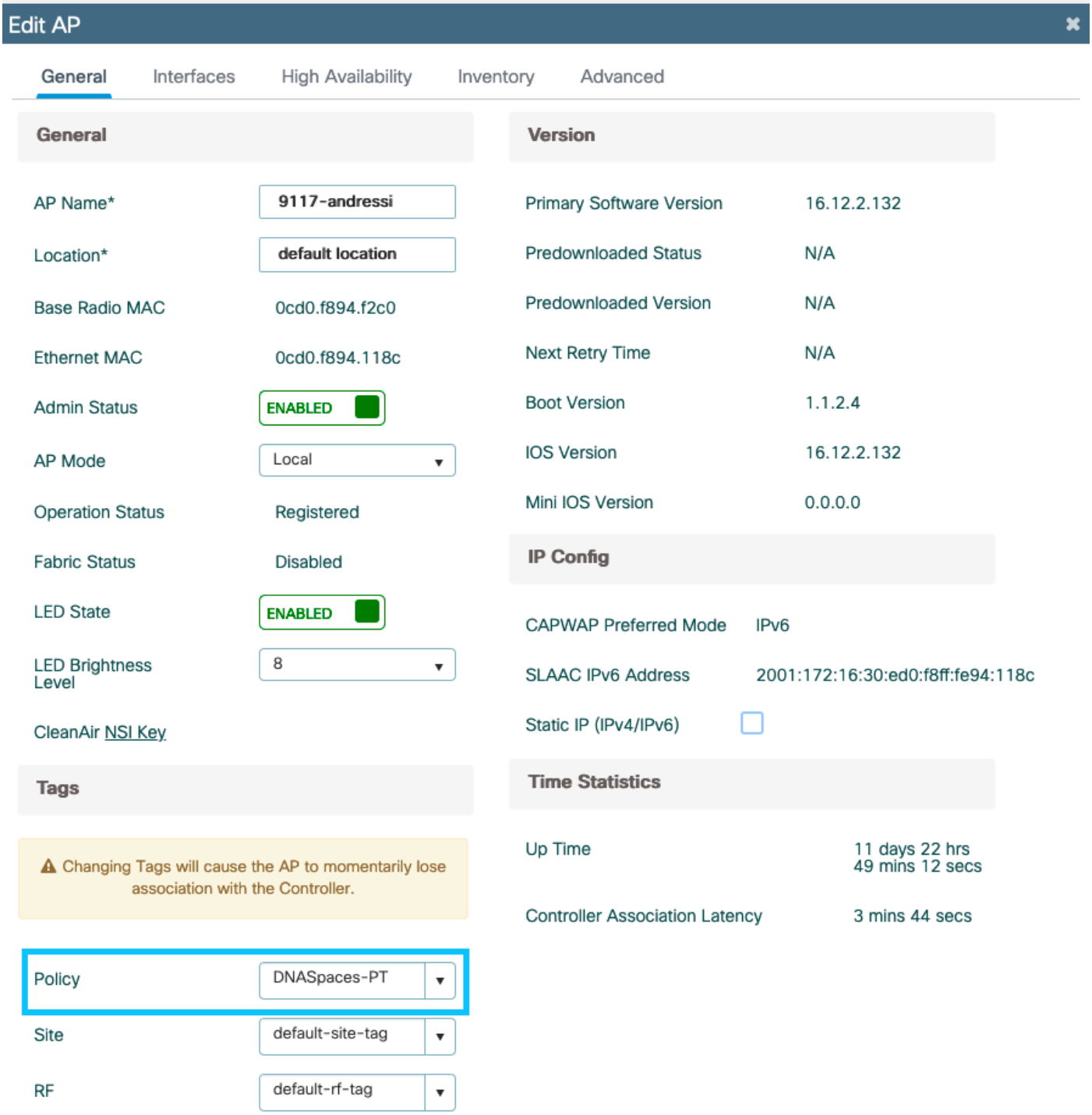


Configura tag criteri sul controller 9800

Passaggio 1. Selezionare **Configurazione > Tag e profili > Criterio.** Creare un nuovo tag criteri o utilizzare il tag criteri predefinito. Mappare la WLAN al Profilo criterio nel Tag criterio.



Passaggio 2. Applicare il tag dei criteri all'access point per trasmettere il SSID. Passare a **Configurazione > Wireless > Access Point,** selezionare l'access point in questione e aggiungere il tag della policy. In questo modo, l'access point riavvia il proprio tunnel CAPWAP e si unisce nuovamente al controller 9800:



Configurazione CLI:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown

Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown

Andressi-9800L(config)#wireless tag policy
```

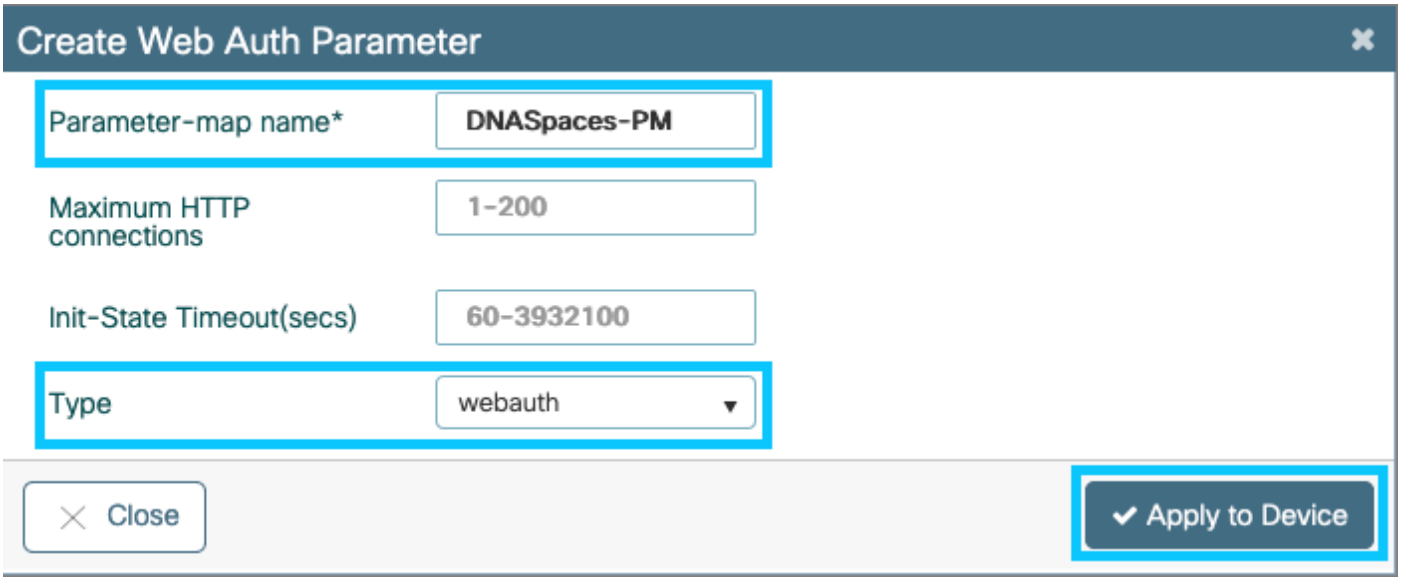
```
Andressi-9800L(config-policy-tag)#wlan
```

Portale vincolato con server RADIUS su spazi DNA

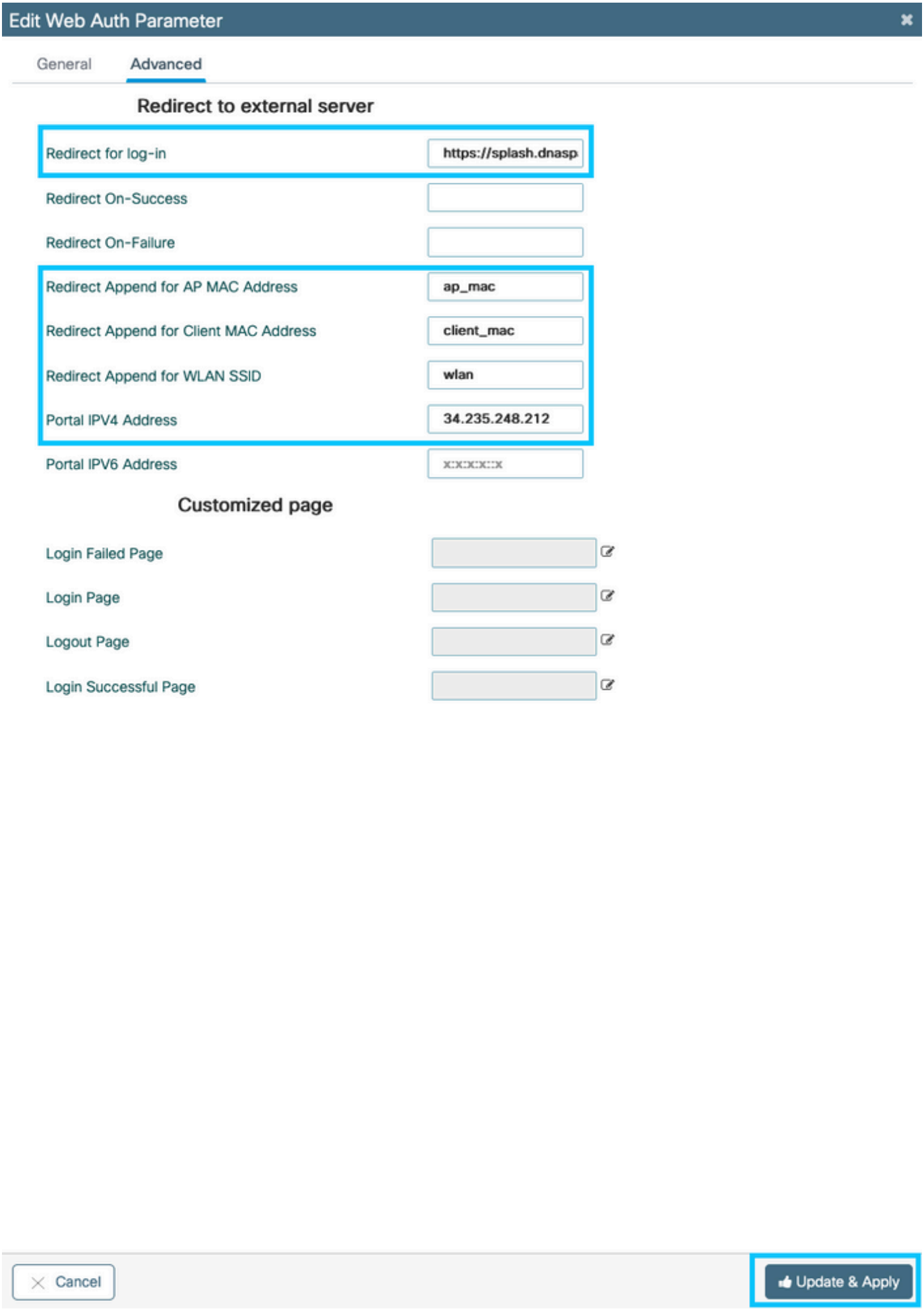
> **Nota**: il server RADIUS DNA Spaces supporta solo l'autenticazione PAP proveniente dal controller.

Configurazione mappa parametri autenticazione Web sul controller 9800

Passaggio 1. Creare una mappa dei parametri di autenticazione Web. Passare a **Configurazione > Protezione > Autenticazione Web**, fare clic su **+Aggiungi**, configurare il nome della mappa dei parametri e selezionare **webauth** come tipo:



Passaggio 2. Fare clic sulla mappa dei parametri configurata nel passaggio 1, fare clic su **Advanced** e immettere il Reindirizzamento per l'accesso, Append for AP MAC Address, Append for Client MAC Address, Append for WLAN SSID e Portal IPv4 Address. Fare clic su **Aggiorna e applica:**


Edit Web Auth Parameter
General
Advanced
Redirect to external server
Redirect for log-in
https://splash.dnasp
Redirect On-Success
Redirect On-Failure
Redirect Append for AP MAC Address
ap_mac
Redirect Append for Client MAC Address
client_mac
Redirect Append for WLAN SSID
wlan
Portal IPV4 Address
34.235.248.212
Portal IPV6 Address
X:X:X:X::X
Customized page
Login Failed Page
Login Page
Logout Page
Login Successful Page
Cancel
Update & Apply

Nota: per ottenere l'URL della pagina iniziale e l'indirizzo di reindirizzamento IPv4, fare clic sull'opzione **Configura manualmente** dall'SSID creato nel passaggio 3 della sezione **Creazione dell'SSID sugli spazi DNA** nella sezione **Creazione degli SSID** nella connessione **diretta WLC Creazione della** sezione rispettivamente della **configurazione dell'elenco di controllo di accesso**.

Nota: il portale Cisco DNA Spaces può essere risolto in due indirizzi IP, ma il controller 9800 consente di configurare un solo indirizzo IP. In questo caso, scegliere uno degli indirizzi IP da configurare nella mappa dei parametri come indirizzo IPv4 del portale.

Nota: Verificare che gli indirizzi IPv4 e IPv6 virtuali siano configurati nella mappa dei parametri di autenticazione Web globale.Se IPv6 virtuale non è configurato, a volte i client vengono reindirizzati al portale interno anziché al portale di Spazi DNA configurato. Per questo motivo è necessario configurare sempre un IP virtuale. "192.0.2.1" può essere configurato come Virtual IPv4 e FE80:0:0:0:903A::11E4 come Virtual IPV6. L'utilizzo di IP diversi da quelli non è giustificato per motivi diversi.

Configurazione CLI:

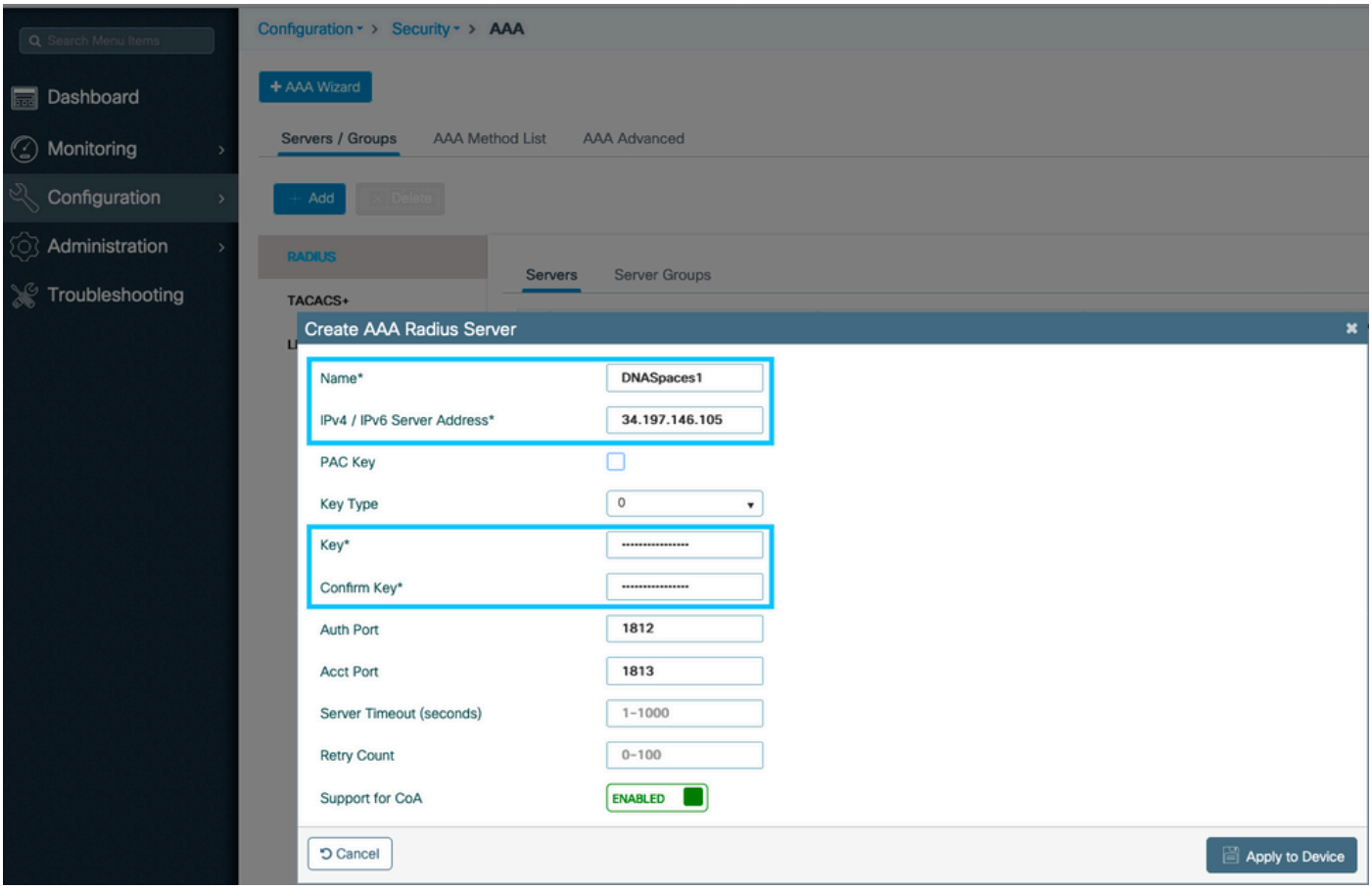
```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

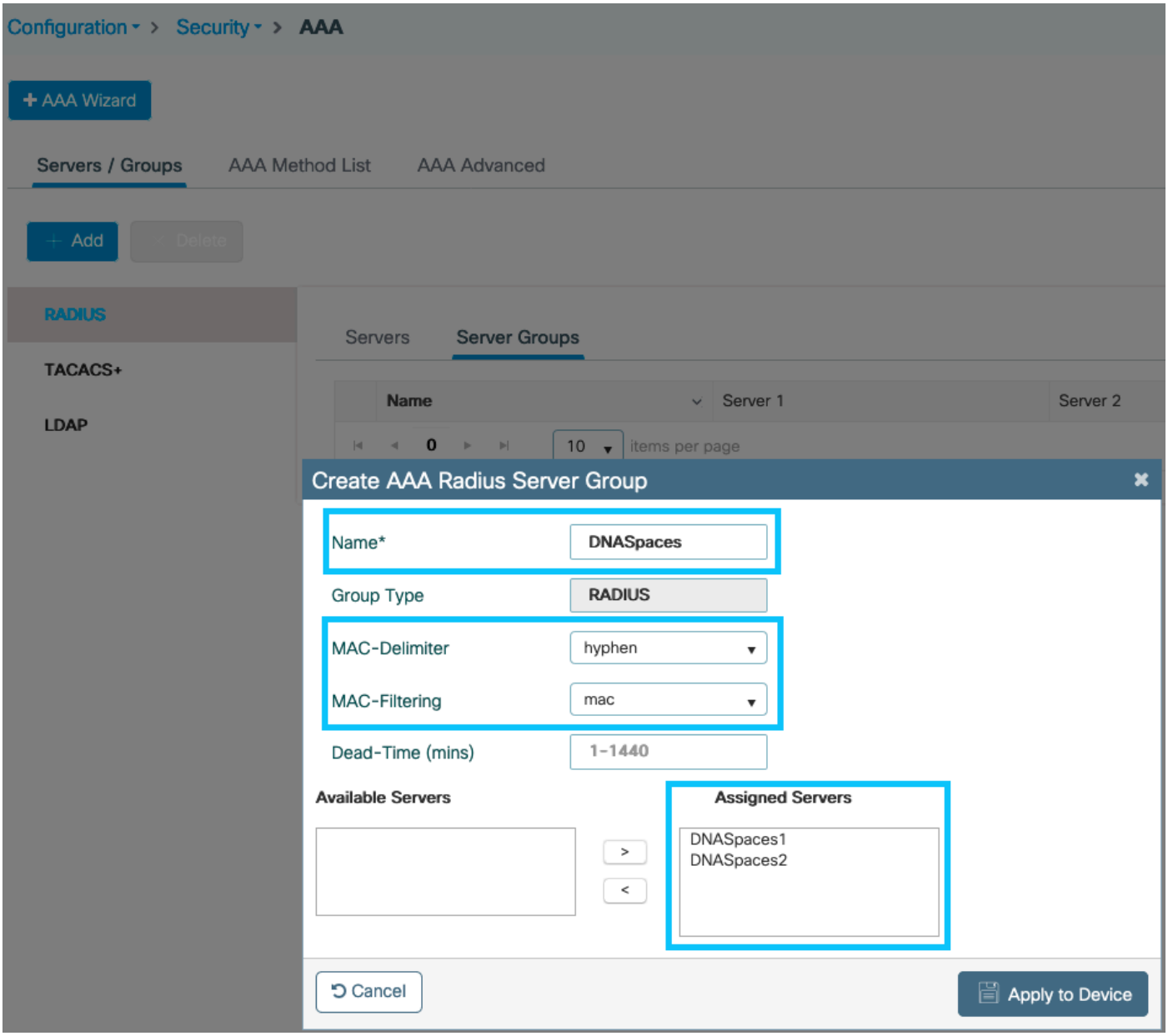
Configurazione dei server RADIUS sul controller 9800

Passaggio 1. Configurare i server RADIUS. Cisco DNA Spaces funge da server RADIUS per l'autenticazione degli utenti e può rispondere su due indirizzi IP. Selezionare **Configuration > Security > AAA**, fare clic su **+Add** e configurare entrambi i server RADIUS:

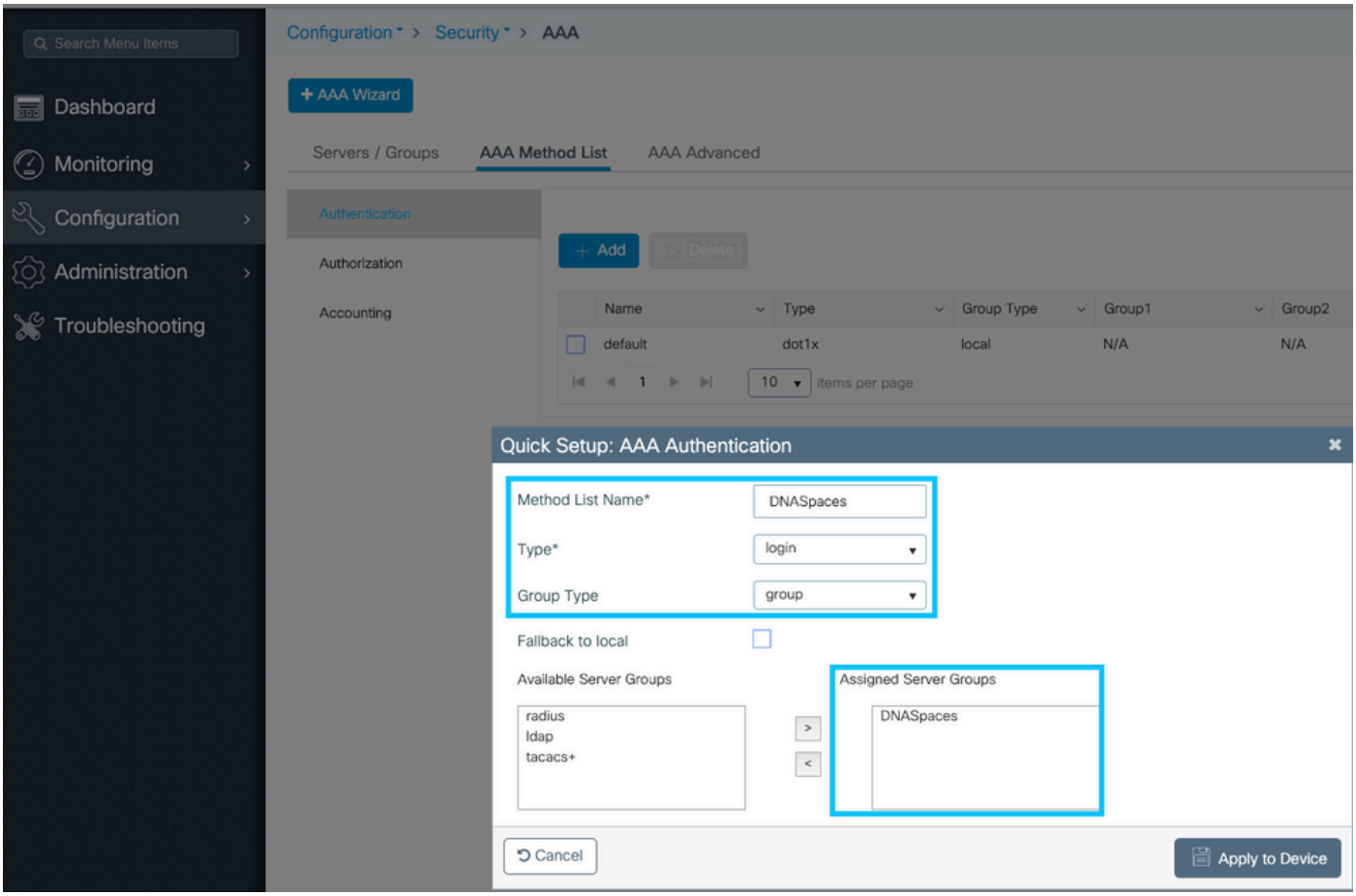


Nota: per ottenere l'indirizzo IP e la chiave privata RADIUS per i server primario e secondario, fare clic sull'opzione **Configura manualmente** dal SSID creato nel passaggio 3 della sezione **Creazione del SSID in Spazi DNA** e passare alla sezione **Configurazione server RADIUS**.

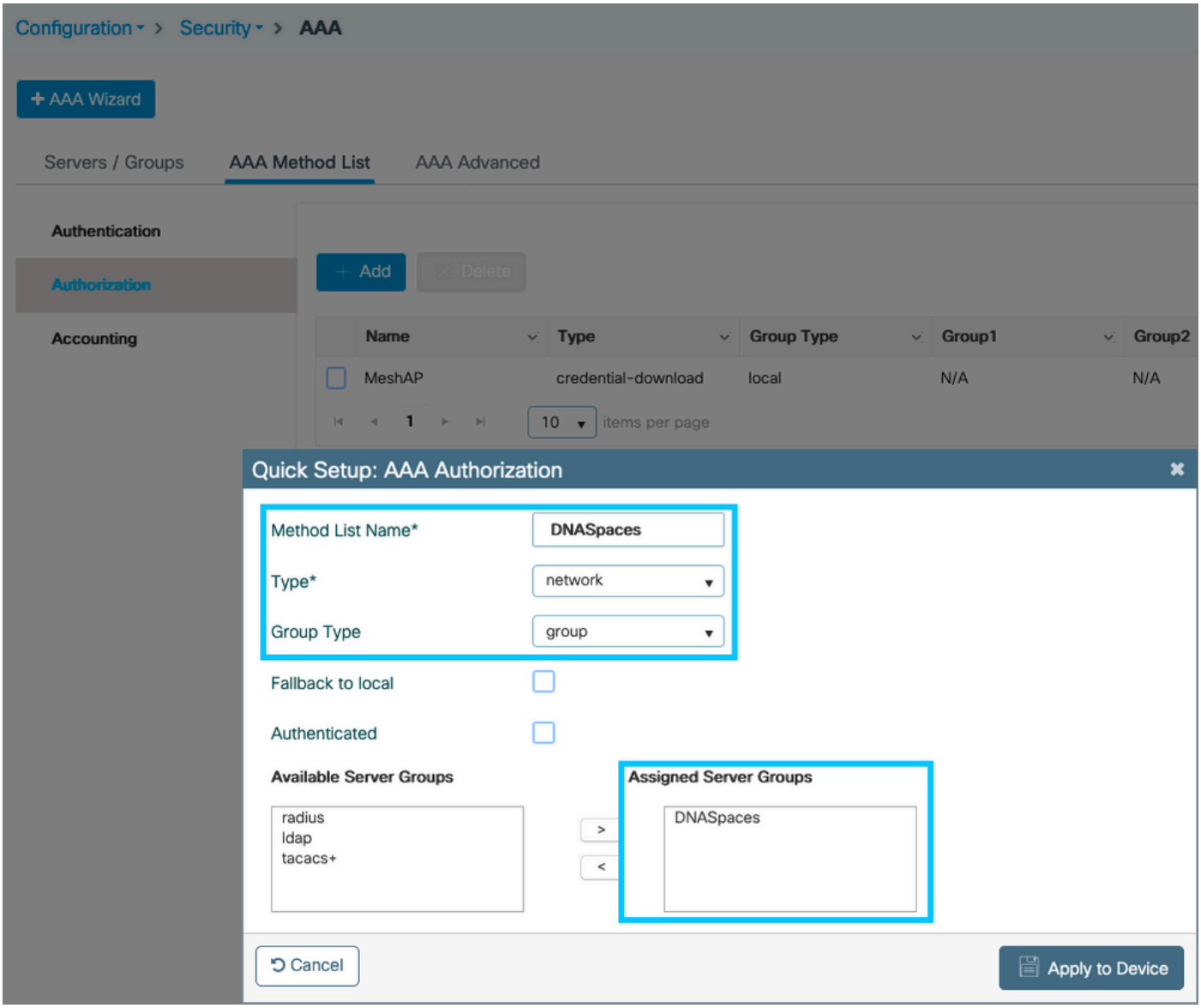
Passaggio 2. Configurare il gruppo di server RADIUS e aggiungere entrambi i server RADIUS. Selezionare **Configurazione > Sicurezza > AAA > Server / Gruppi > RADIUS > Gruppi di server**, fare clic su **+aggiungi,** configurare il nome del gruppo di server, il delimitatore MAC come **trattino,** il filtro MAC come **MAC** e assegnare i due server RADIUS:



Passaggio 3. Configurare un elenco di metodi di autenticazione. Selezionare **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autenticazione,** quindi fare clic su **+aggiungi.** Configurare il nome dell'elenco di metodi, selezionare **login** come tipo e assegnare il gruppo di server:

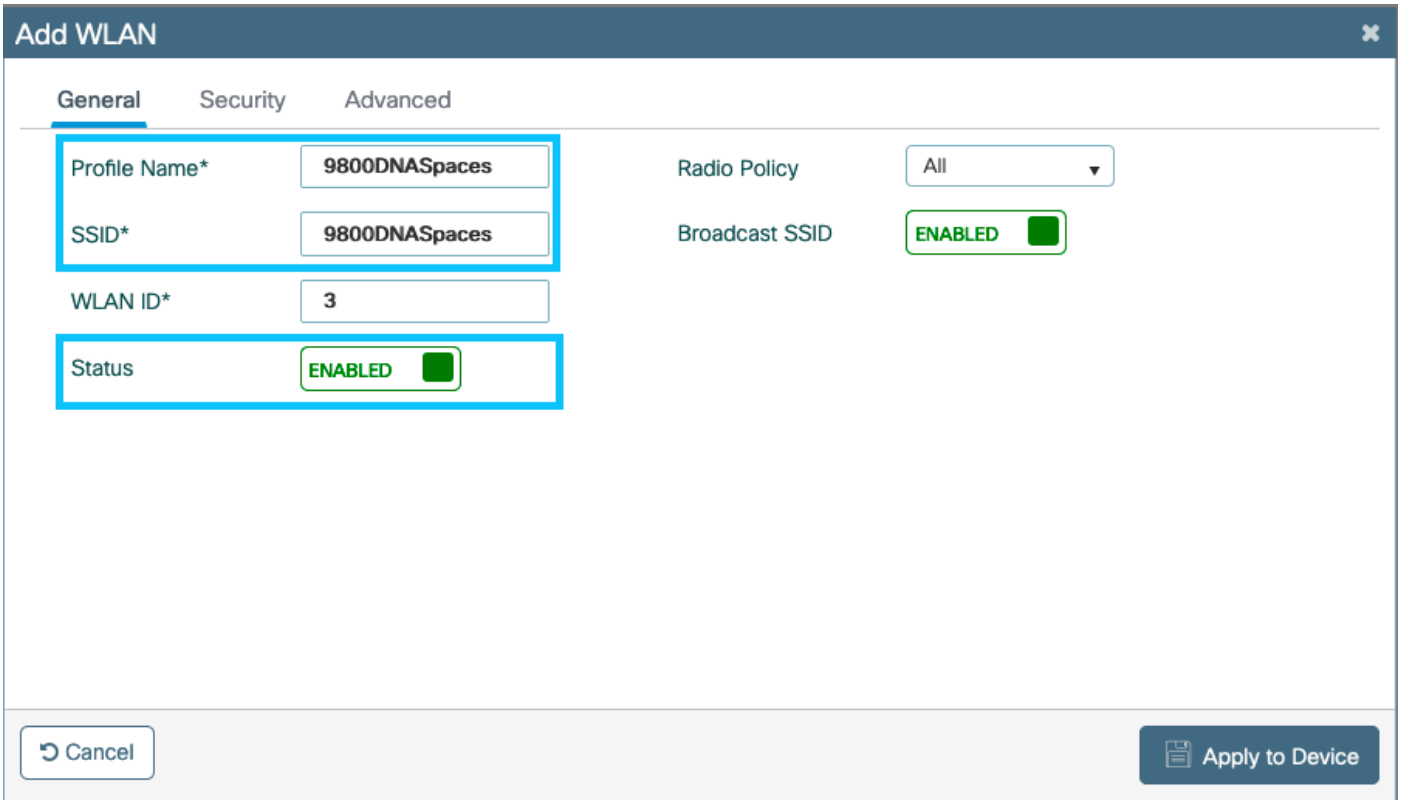


Passaggio 4. Configurare un elenco di metodi di autorizzazione. Selezionare **Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione,** quindi fare clic su **+aggiungi.** Configurare il nome dell'elenco di metodi, selezionare **network** come tipo e assegnare il gruppo di server:

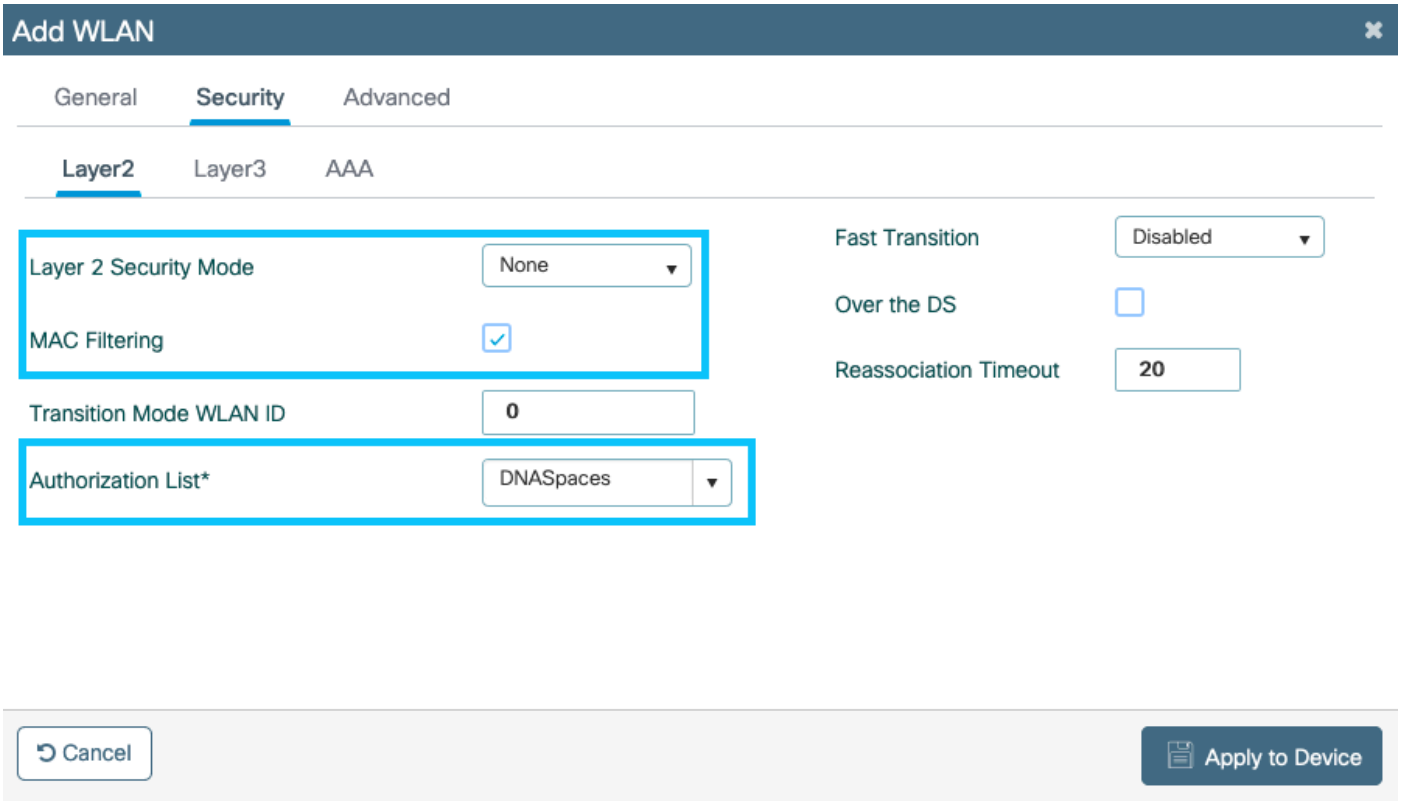


Creare l'SSID sul controller 9800

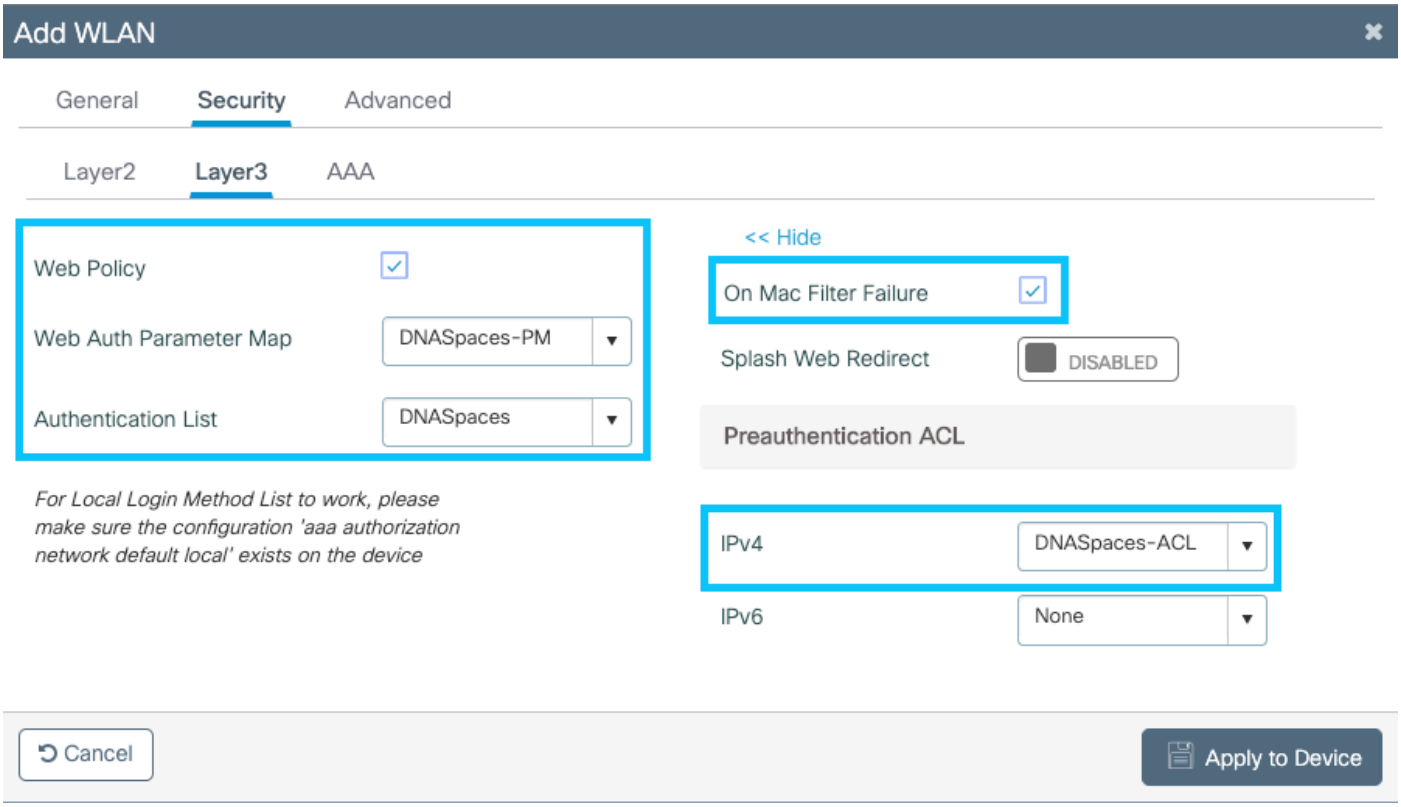
Passaggio 1. Selezionare **Configurazione > Tag e profili > WLAN**, quindi fare clic su **+Aggiungi.** Configurare il nome del profilo, l'SSID e abilitare la WLAN. Verificare che il nome SSID sia uguale al nome configurato nel passaggio 3 della sezione **Creazione del SSID in Spazi DNA.**



Passaggio 2. Passare a **Sicurezza > Layer2.** Impostare la modalità di protezione di layer 2 su **None,** abilitare il filtro MAC e aggiungere l'elenco di autorizzazioni:

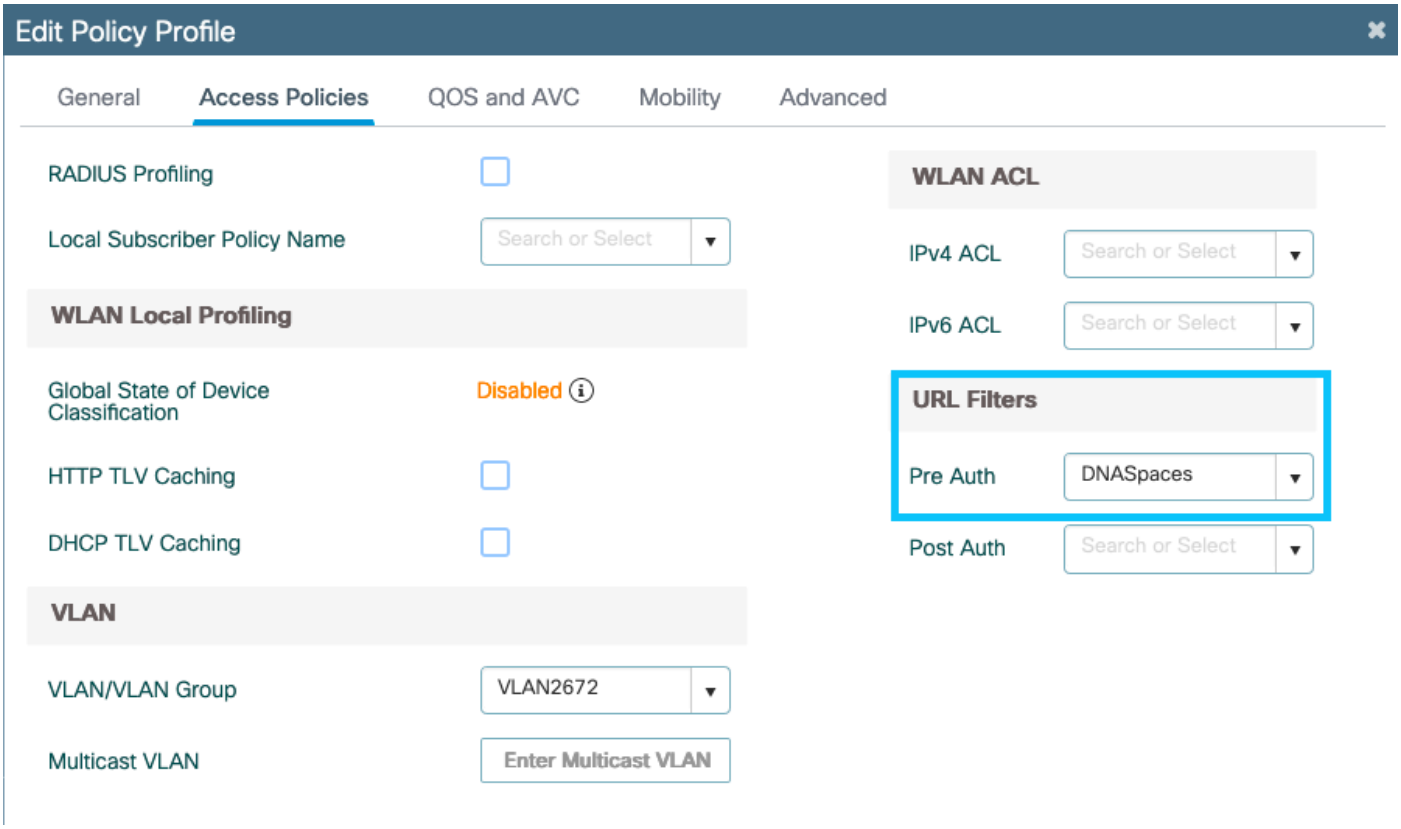


Passaggio 3. Selezionare **Protezione > Layer3.** Abilitare i criteri Web, configurare la mappa dei parametri di autenticazione Web e l'elenco di autenticazione. Abilitare in caso di errore del filtro Mac e aggiungere l'ACL di preautenticazione. Fare clic su **Applica alla periferica**.

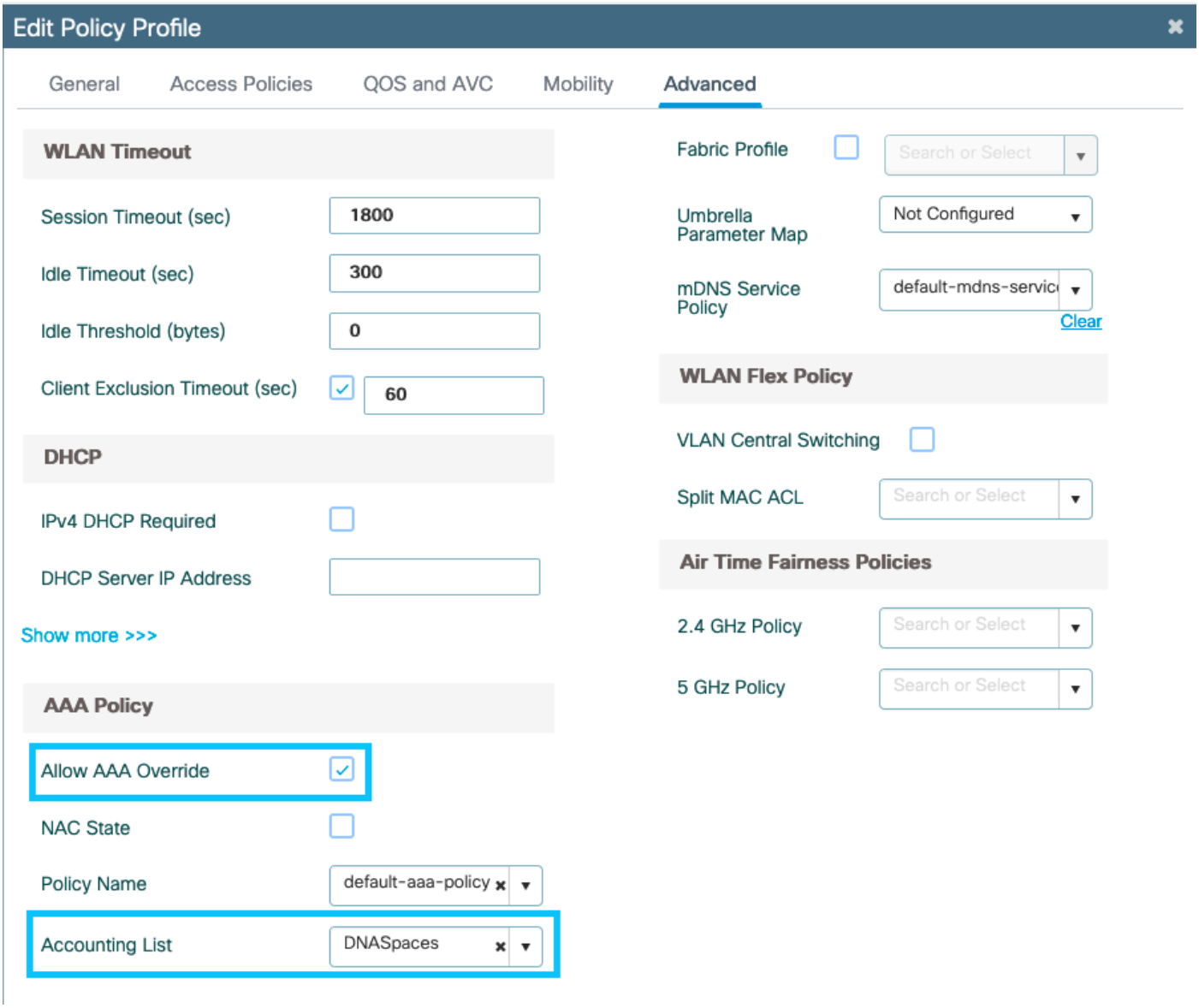


Configurazione del profilo criteri sul controller 9800

Passaggio 1. Passare a **Configurazione > Tag e profili > Criterio** e creare un nuovo Profilo criterio oppure utilizzare il Profilo criterio predefinito. Nella scheda Criteri di accesso configurare la VLAN client e aggiungere il filtro URL.

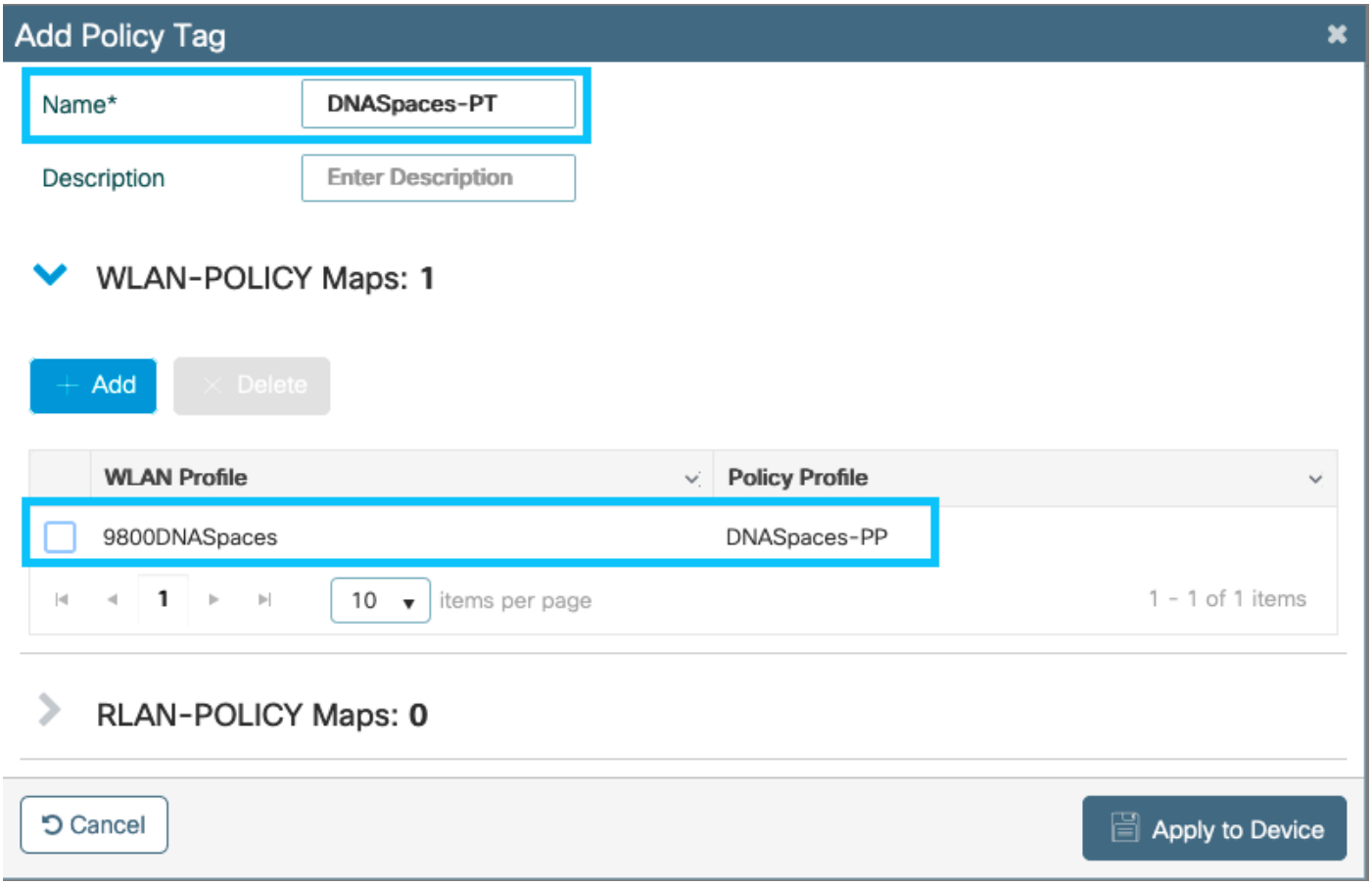


Passaggio 2. Nella scheda Avanzate, abilitare la sostituzione AAA e, se si desidera, configurare l'elenco dei metodi contabili.

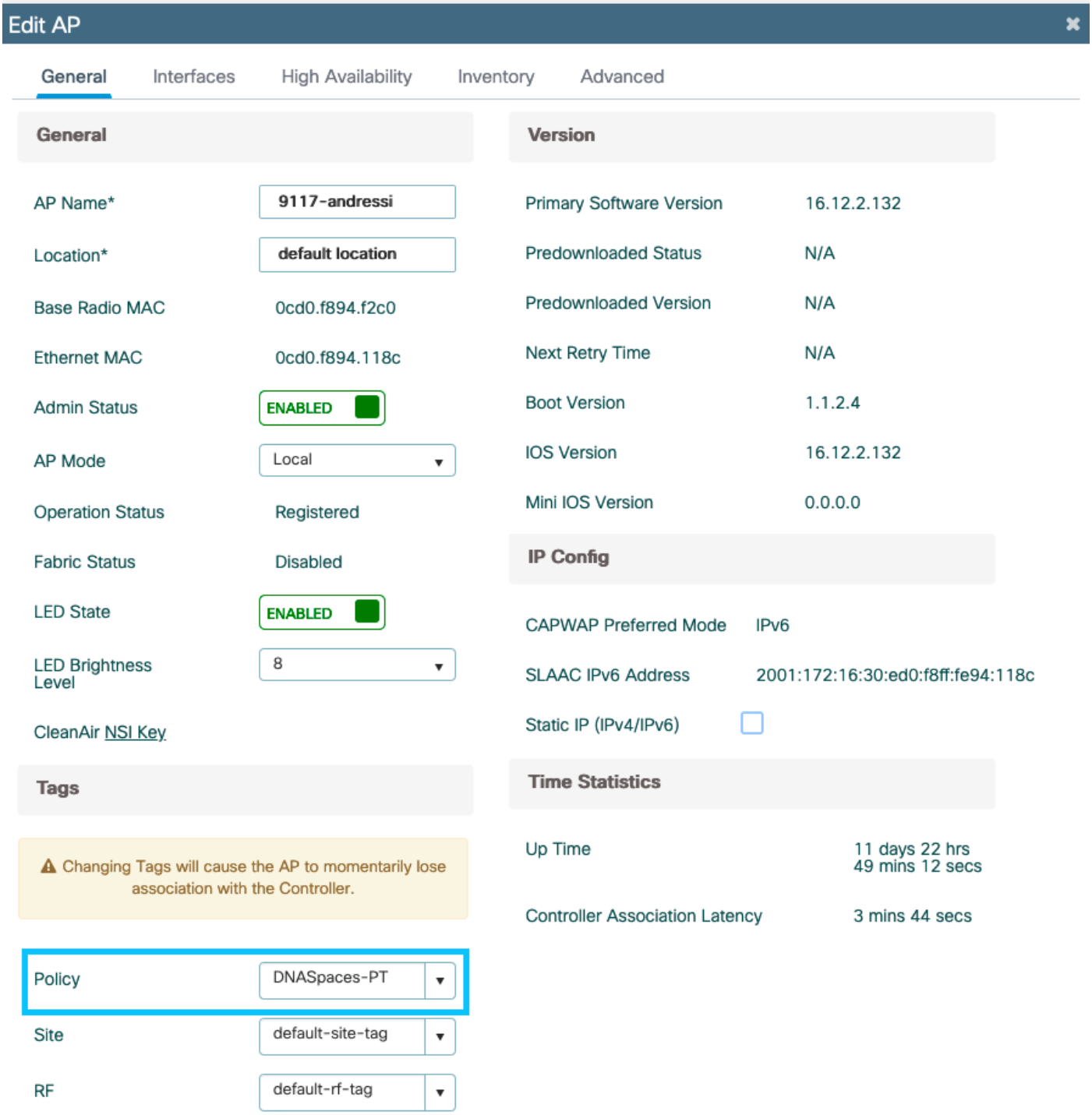


Configura tag criteri sul controller 9800

Passaggio 1. Selezionare **Configurazione > Tag e profili > Criterio.** Creare un nuovo tag criteri o utilizzare il tag criteri predefinito. Mappare la WLAN al Profilo criterio nel Tag criterio.



Passaggio 2. Applicare il tag dei criteri all'access point per trasmettere il SSID. Passare a **Configurazione > Wireless > Access Point,** selezionare l'access point in questione e aggiungere il tag della policy. In questo modo, l'access point riavvia il proprio tunnel CAPWAP e si unisce nuovamente al controller 9800:



Configurazione CLI:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
```

```
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#mac-filtering




Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list




Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown

Andressi-9800L(config)#wireless profile policy




Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list




Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter




Andressi-9800L(config-wireless-policy)#no shutdown

Andressi-9800L(config)#wireless tag policy




Andressi-9800L(config-policy-tag)#wlan
```

Configurare la mappa dei parametri globali

Passaggio non consigliato: eseguire questi comandi per consentire il reindirizzamento HTTPS, ma si noti che il reindirizzamento nel traffico HTTPS del client non è necessario se il sistema operativo del client esegue il rilevamento del portale captive, provoca un maggiore utilizzo della CPU e genera sempre un avviso di certificato. Si consiglia pertanto di evitare di configurarlo, a meno che non sia necessario per un caso di utilizzo molto specifico.

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

> **Nota**: è necessario disporre di un certificato SSL valido per l'IP virtuale installato in Cisco Catalyst serie 9800 Wireless Controller.

Passaggio 1. Copiare un file certificato firmato con estensione .p12 su un server TFTP ed eseguire questo comando per trasferire e installare il certificato nel controller 9800:

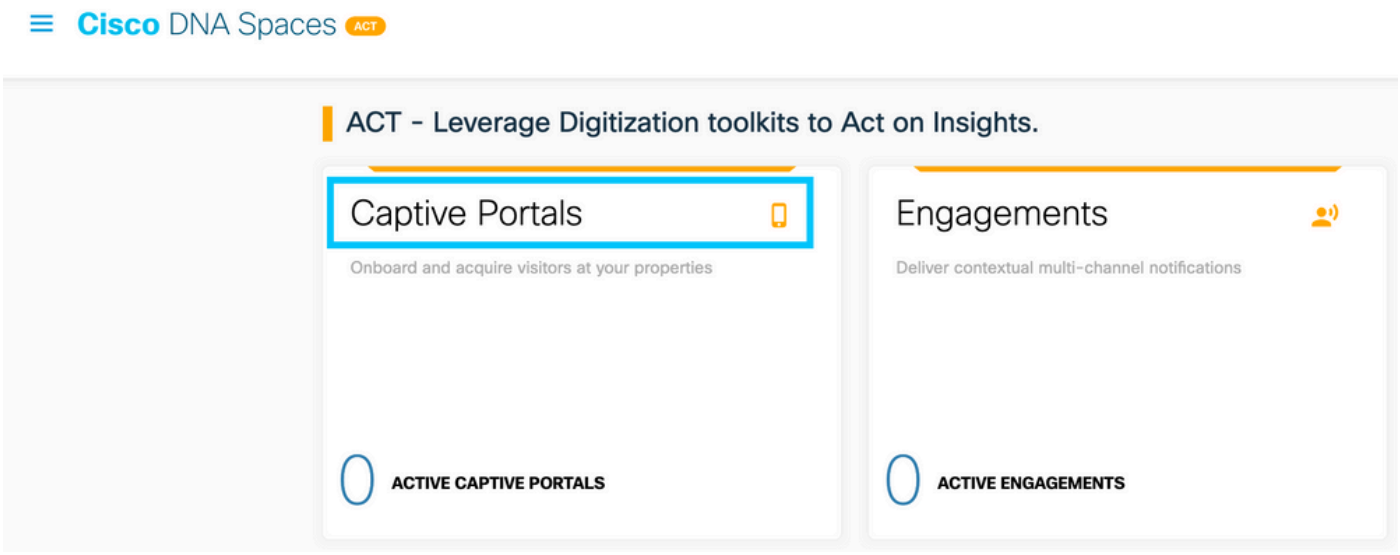
```
Andressi-9800L(config)#crypto pki import
```

Passaggio 2. Per mappare il certificato installato alla mappa dei parametri di autenticazione Web, eseguire i comandi seguenti:

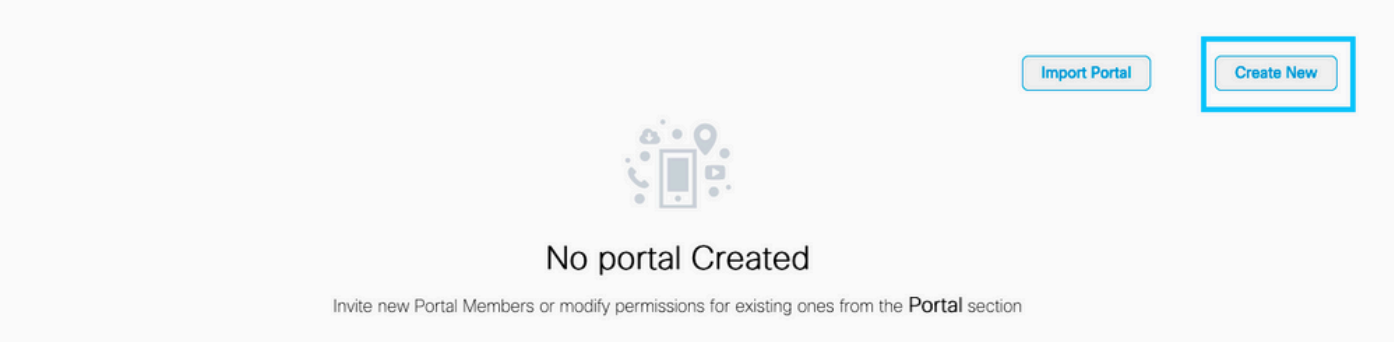
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

Crea il portale in DNA Spaces

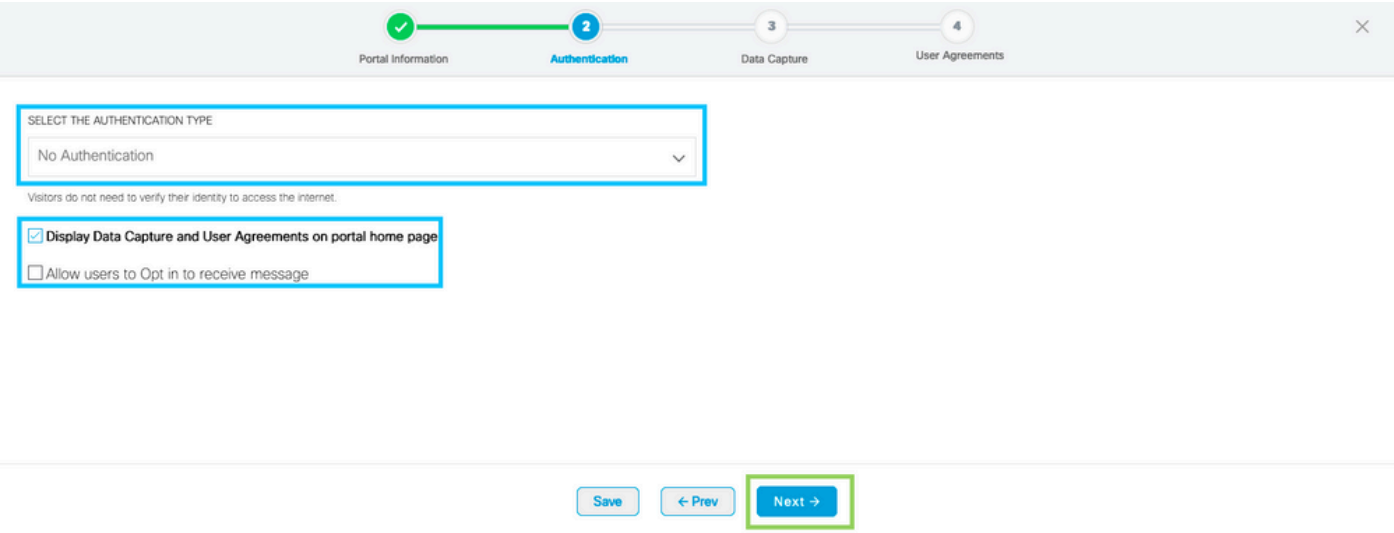
Passaggio 1. Fare clic su **Captive Portals** nel dashboard di DNA Spaces:



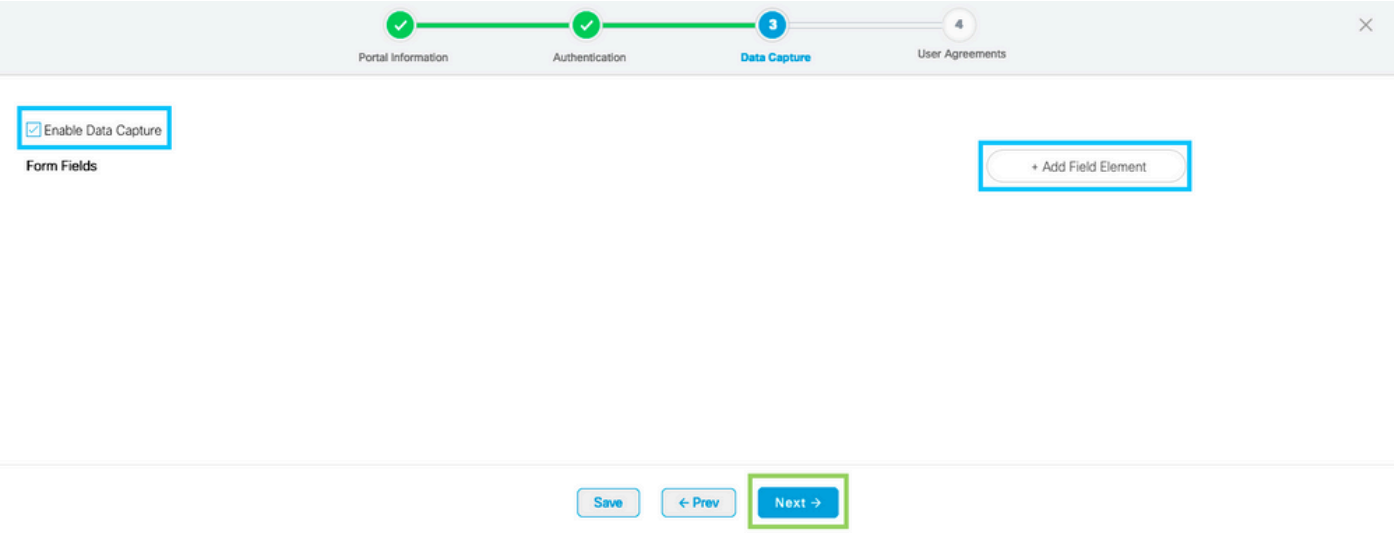
Passaggio 2. Fare clic su **Create New (Crea nuovo),** immettere il nome del portale e selezionare i percorsi che possono utilizzare il portale:



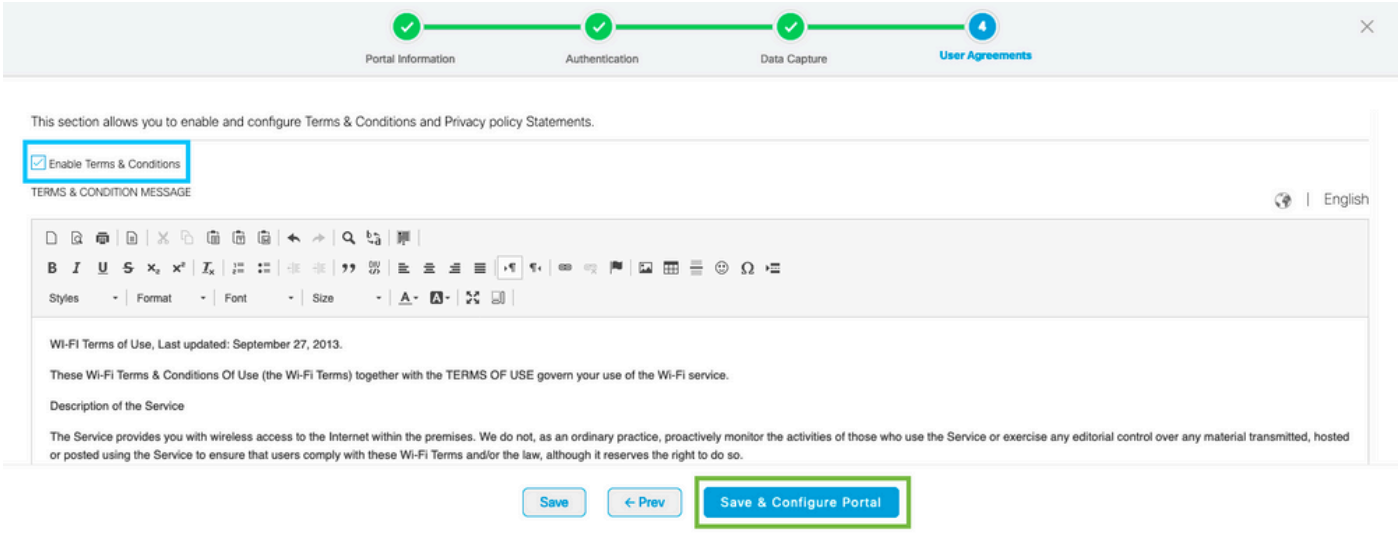
Passaggio 3. Selezionare il tipo di autenticazione, scegliere se si desidera visualizzare l'acquisizione dei dati e gli accordi utente nella home page del portale e se gli utenti possono scegliere di accettare la ricezione di un messaggio. Fare clic su **Avanti**:



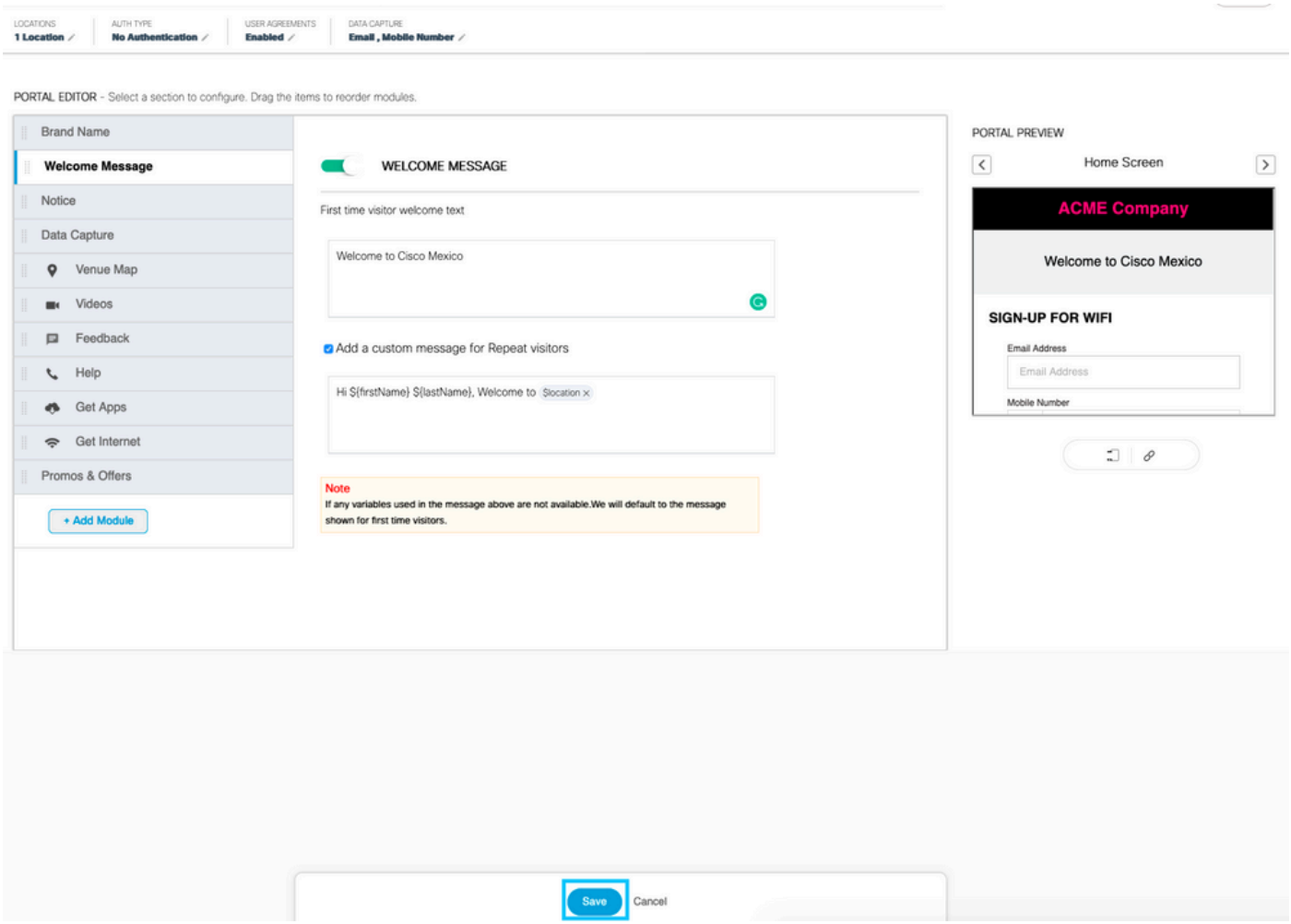
Passaggio 4. Configurare gli elementi di acquisizione dati. Se si desidera acquisire dati dagli utenti, selezionare la casella **Abilita acquisizione dati** e fare clic su **+Aggiungi elemento campo** per aggiungere i campi desiderati. Fare clic su **Avanti**:



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

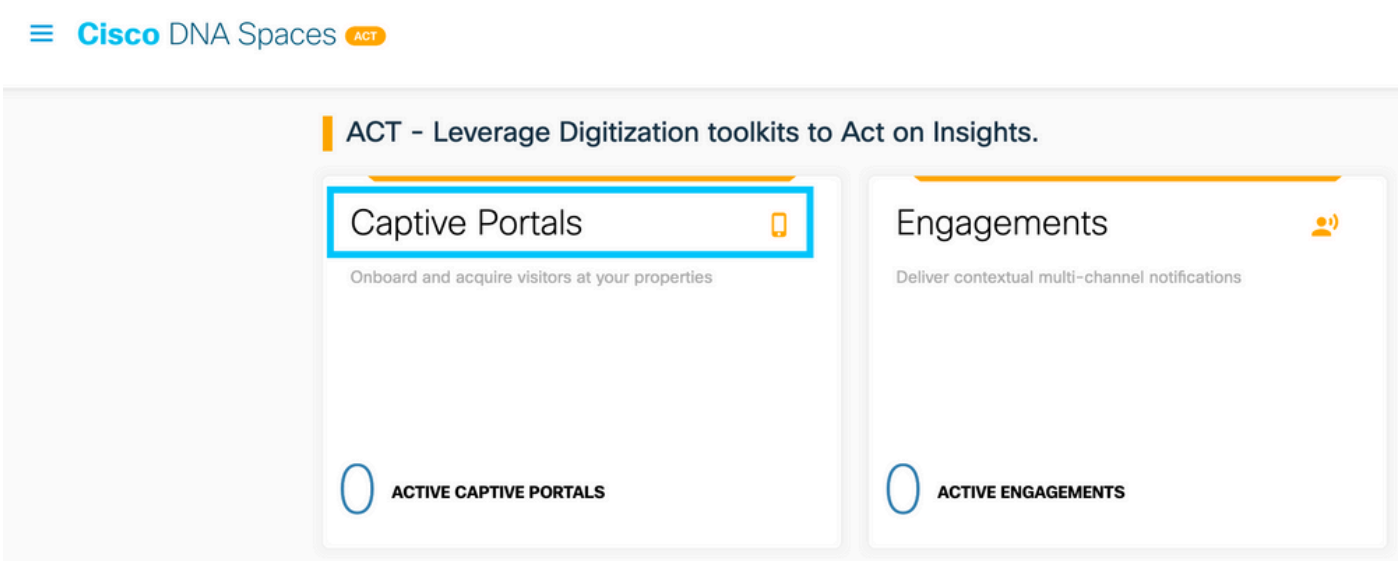


Passaggio 6. Modificare il portale come necessario, Fare clic su **Salva:**

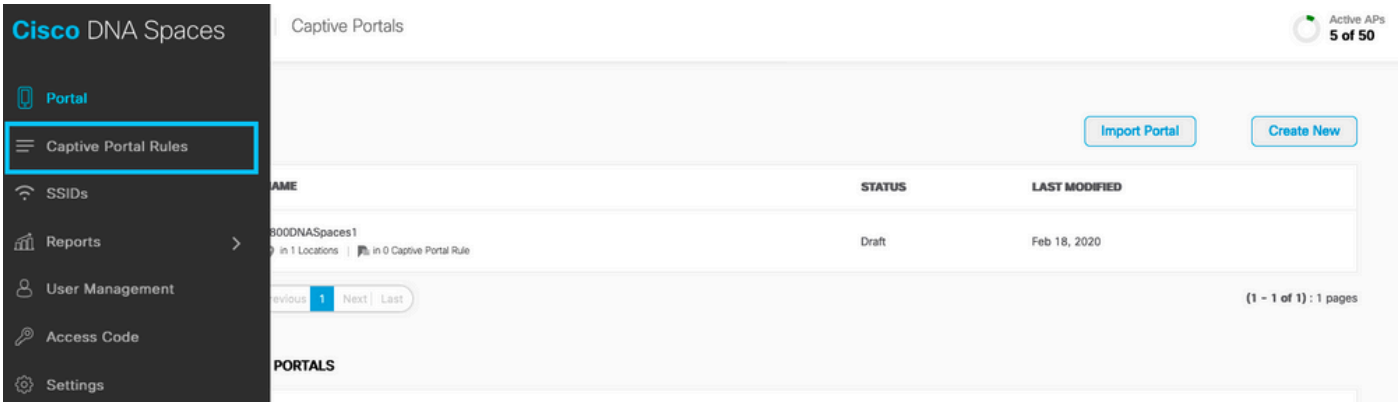


Configura le regole del portale vincolato in Spazi DNA

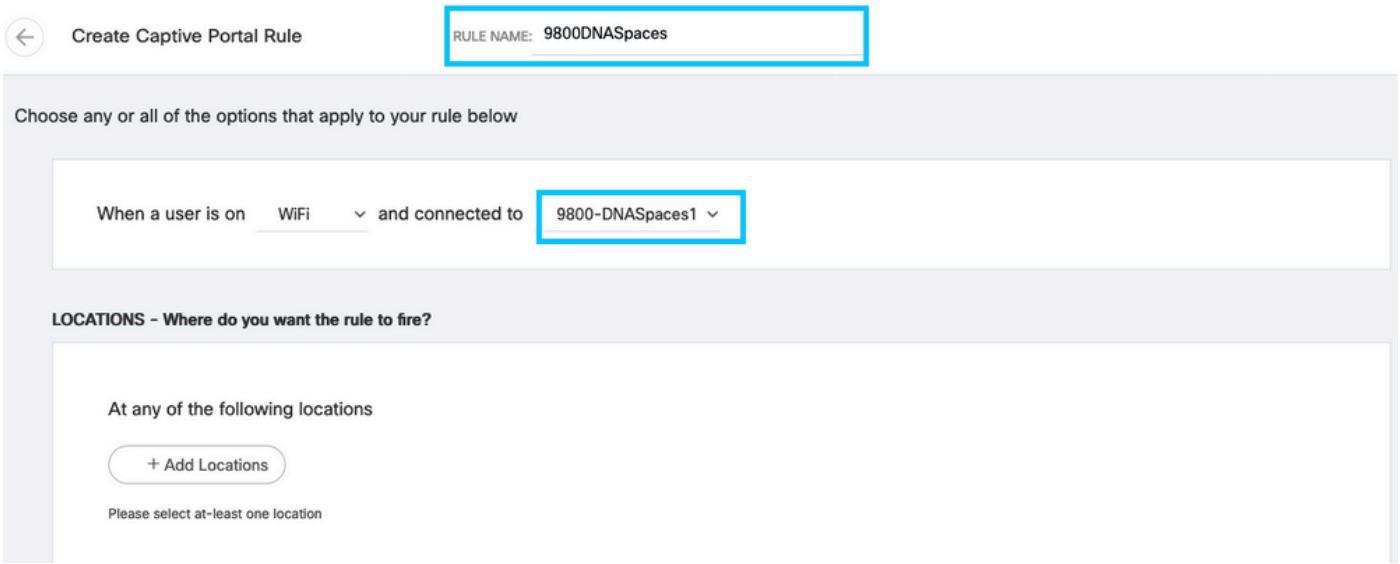
Passaggio 1. Fare clic su **Captive Portals** nel dashboard di DNA Spaces:



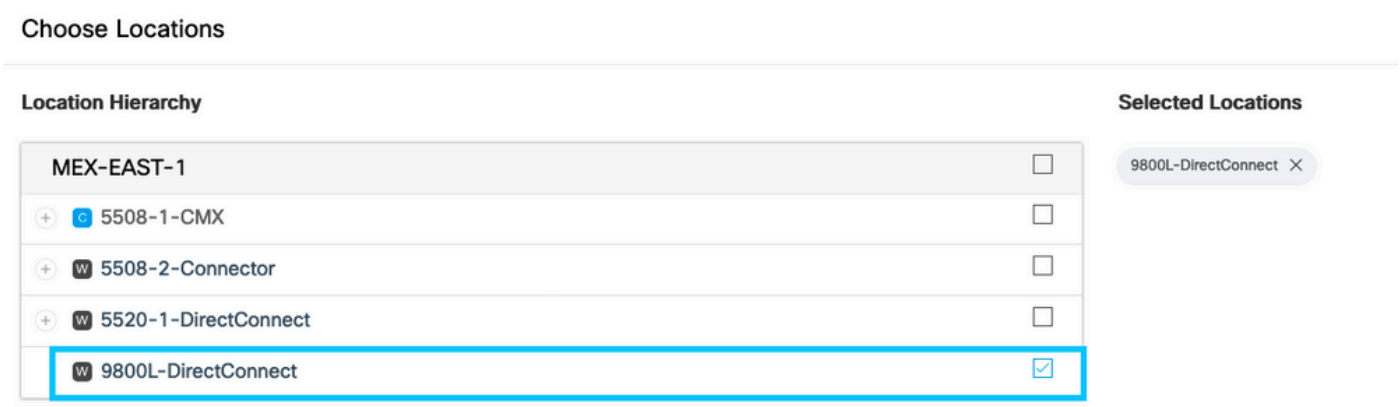
Passaggio 2. Aprire il menu Captive Portal e fare clic su **Captive Portal Rules:**



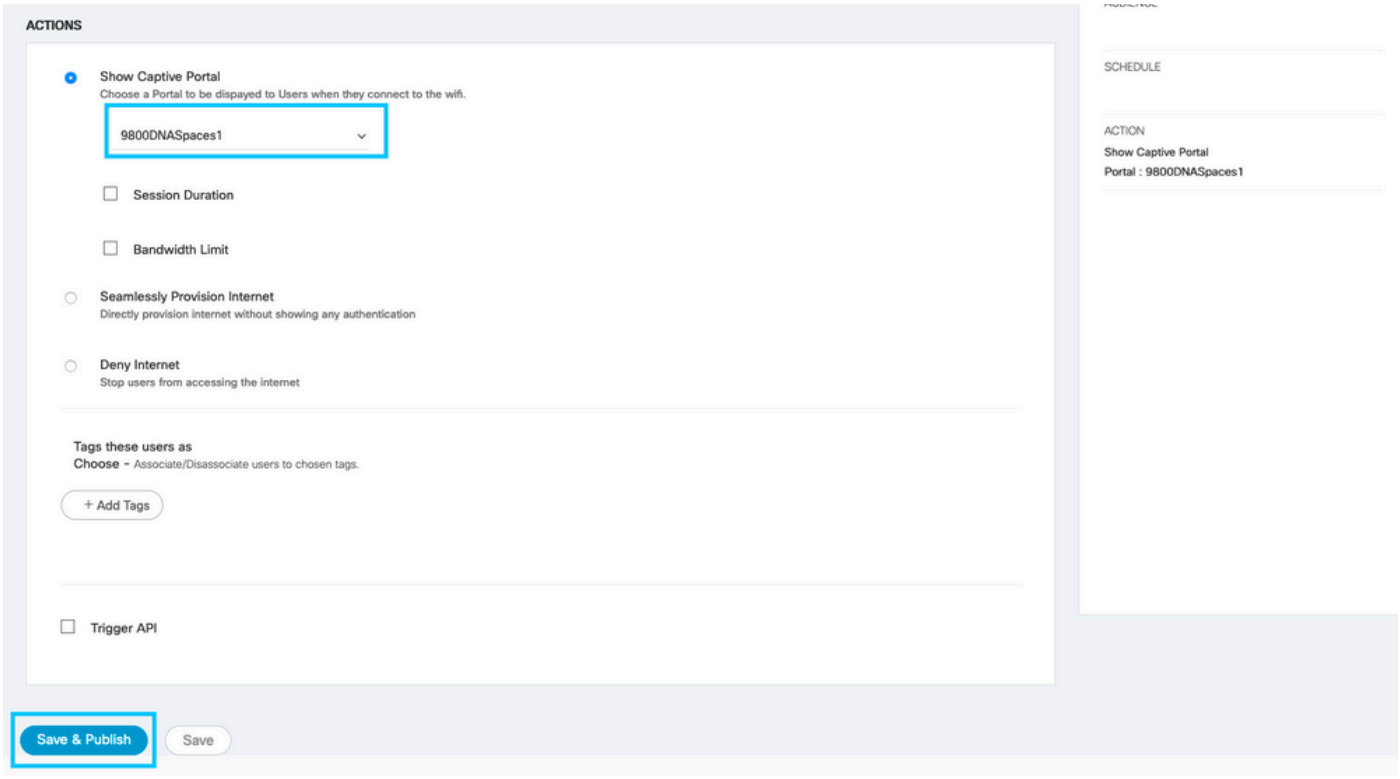
Passaggio 3. Fare clic su **+ Crea nuova regola**. Immettere il nome della regola e scegliere il SSID configurato in precedenza.



Passaggio 4. Selezionare i percorsi in cui il portale è disponibile. Fare clic su **+ Aggiungi percorsi** nella sezione **PERCORSI**. Scegliere quella desiderata dalla gerarchia ubicazioni.



Passaggio 5. Scegliere l'azione del portale vincolato. In questo caso, quando la regola viene trovata, viene visualizzato il portale. Fare clic su **Salva e pubblica.**

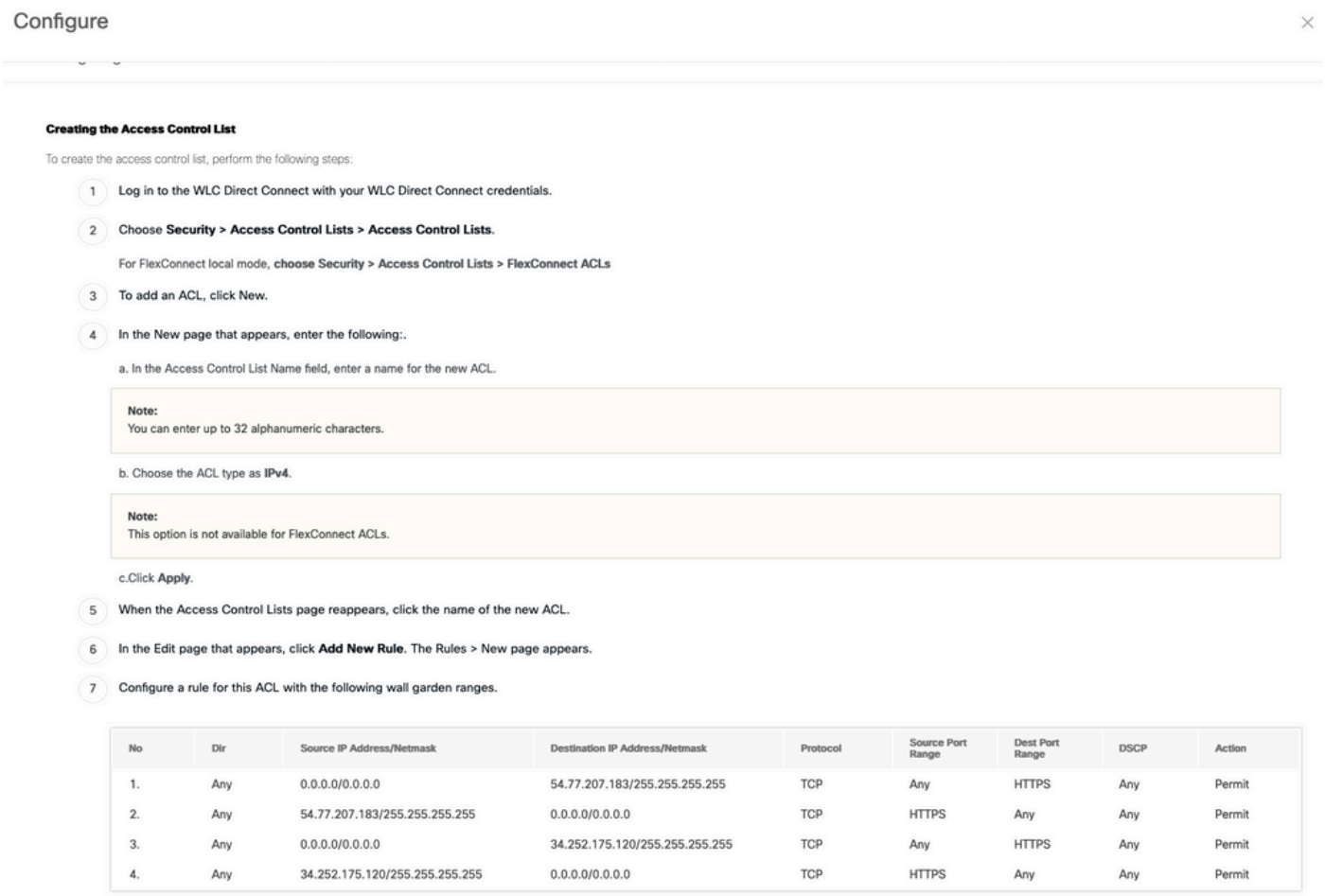


Ottieni informazioni specifiche da DNA Spaces

Quali sono gli indirizzi IP utilizzati da DNA Spaces?

Per verificare gli indirizzi IP utilizzati da DNA Spaces per il portale della propria area, visitare la pagina Captival Portal nella home page di DNA Space. Fare clic su **SSID** nel menu a sinistra, quindi fare clic su **Configure manual** sotto il SSID. Gli indirizzi IP sono menzionati nell'esempio dell'ACL. Questi sono gli indirizzi IP del portale da utilizzare negli ACL e nella mappa dei parametri webauth. DNA Spaces utilizza altri indirizzi IP per la connettività NMSP/cloud complessiva del control plane.

Nella prima sezione del popup che viene visualizzata, il passaggio 7 mostra gli indirizzi IP menzionati nella definizione dell'ACL. Non è necessario seguire queste istruzioni e creare un ACL, è sufficiente prendere nota degli indirizzi IP. Questi sono gli IP utilizzati dal portale nella propria area



Configure

Creating the Access Control List

To create the access control list, perform the following steps:

1. Log in to the WLC Direct Connect with your WLC Direct Connect credentials.
2. Choose **Security > Access Control Lists > Access Control Lists**.

   For FlexConnect local mode, **choose Security > Access Control Lists > FlexConnect ACLs**
3. To add an ACL, click New.
4. In the New page that appears, enter the following:.

   a. In the Access Control List Name field, enter a name for the new ACL.

   Note:
   You can enter up to 32 alphanumeric characters.

   b. Choose the ACL type as **IPv4**.

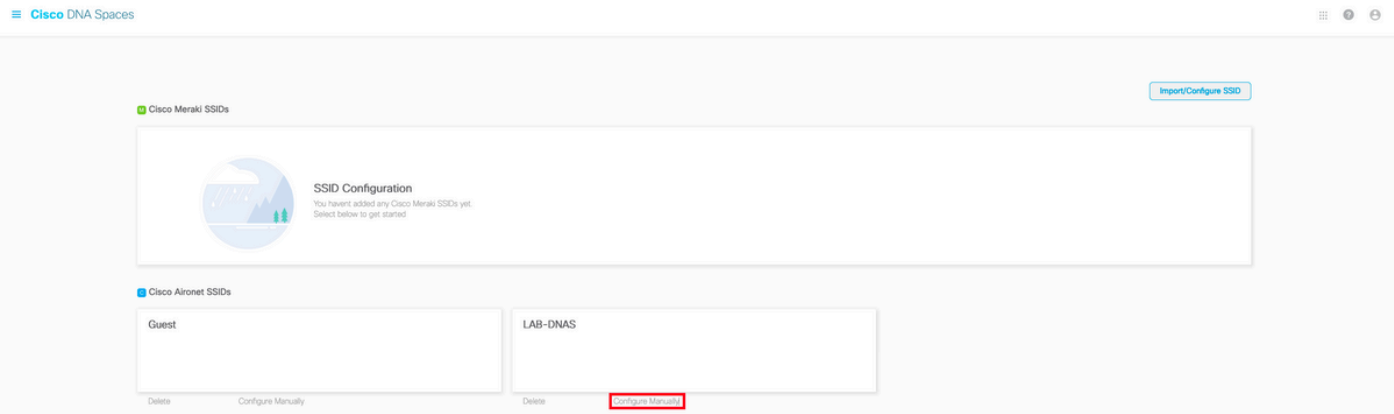
   Note:
   This option is not available for FlexConnect ACLs.

   c.Click **Apply**.
5. When the Access Control Lists page reappears, click the name of the new ACL.
6. In the Edit page that appears, click **Add New Rule**. The Rules > New page appears.
7. Configure a rule for this ACL with the following wall garden ranges.

No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	TCP	Any	HTTPS	Any	Permit
4.	Any	34.252.175.120/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit

Qual è l'URL utilizzato dal portale di accesso di DNA Spaces?

Per verificare quale URL del portale di accesso DNA Spaces utilizza per il portale nella tua regione, vai alla pagina del portale Captival nella home page di DNA Space. Fare clic su **SSID** nel menu a sinistra, quindi fare clic su **Configure manual** sotto il SSID.



Scorrere verso il basso il popup visualizzato e nella seconda sezione, il passo 7 mostra l'URL da configurare nella mappa dei parametri di 9800.

Creating the SSIDs in WLC Direct Connect

To create the SSIDs in the WLC Direct Connect, perform the following steps:

1. In the WLC Direct Connect main window, click the **WLANs** tab.
2. To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
3. In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
4. Click **Apply**.

   The WLAN added appears in the WLANs page.
5. Click the WLAN you have newly created.
6. Choose **Security > Layer 2** , and configure the Layer 2 Security as **None** .
7. In the **Layer 3 tab** , do the following configurations:

   a.From the Layer 3 security drop-down list, choose **Web Policy** .

   b.Choose the **Passthrough** radio button.

   c.In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.

   d.Select the Enable check box for the Sleeping Client.

   e.Select the Enable check box for the Override Global Config.

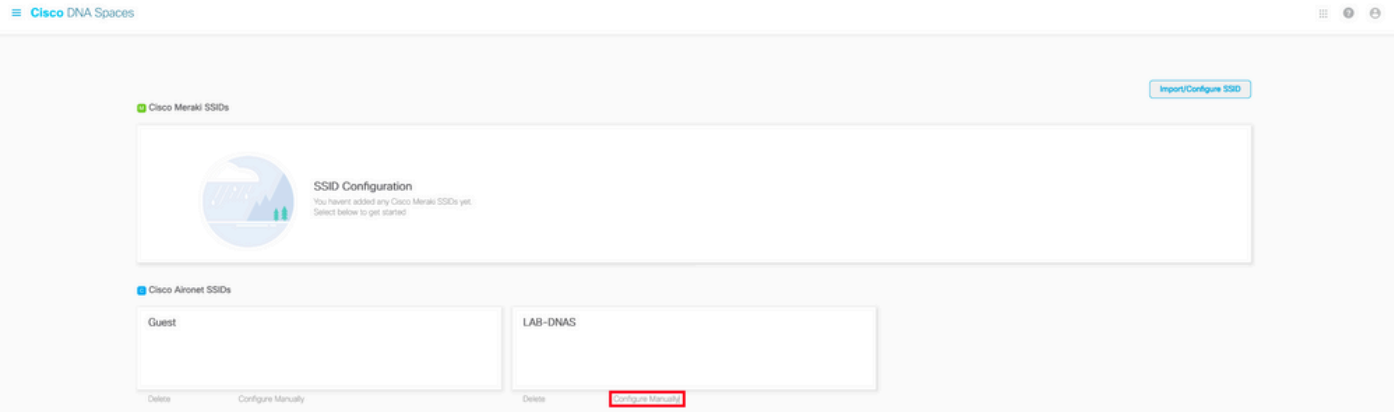
   f.From the Web Auth Type drop-down list, choose **External** .

   g.In the URL field that appears, enter the Cisco DNA Spaces splash URL.

https://splash.dnaspaces.eu/p2/emeabru2

Quali sono i dettagli del server RADIUS per DNA Spaces?

Per scoprire quali sono gli indirizzi IP dei server RADIUS da utilizzare e il segreto condiviso, andare alla pagina Captival Portal nella home page di DNA Space. Fare clic su **SSID** nel menu a sinistra, quindi fare clic su **Configure manual** sotto il SSID.



Nel popup visualizzato, scorrere verso il basso nella terza sezione (RADIUS) e il passaggio 7 fornisce l'indirizzo IP/porta e il segreto condiviso per l'autenticazione radius. La contabilità è facoltativa ed è descritta al passo 12.

7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvUK

8 Choose **Radius > Accounting**.

The Radius Accounting Servers page appears.

9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

10 From the MAC Delimiter drop-down list, choose **Hyphen**.

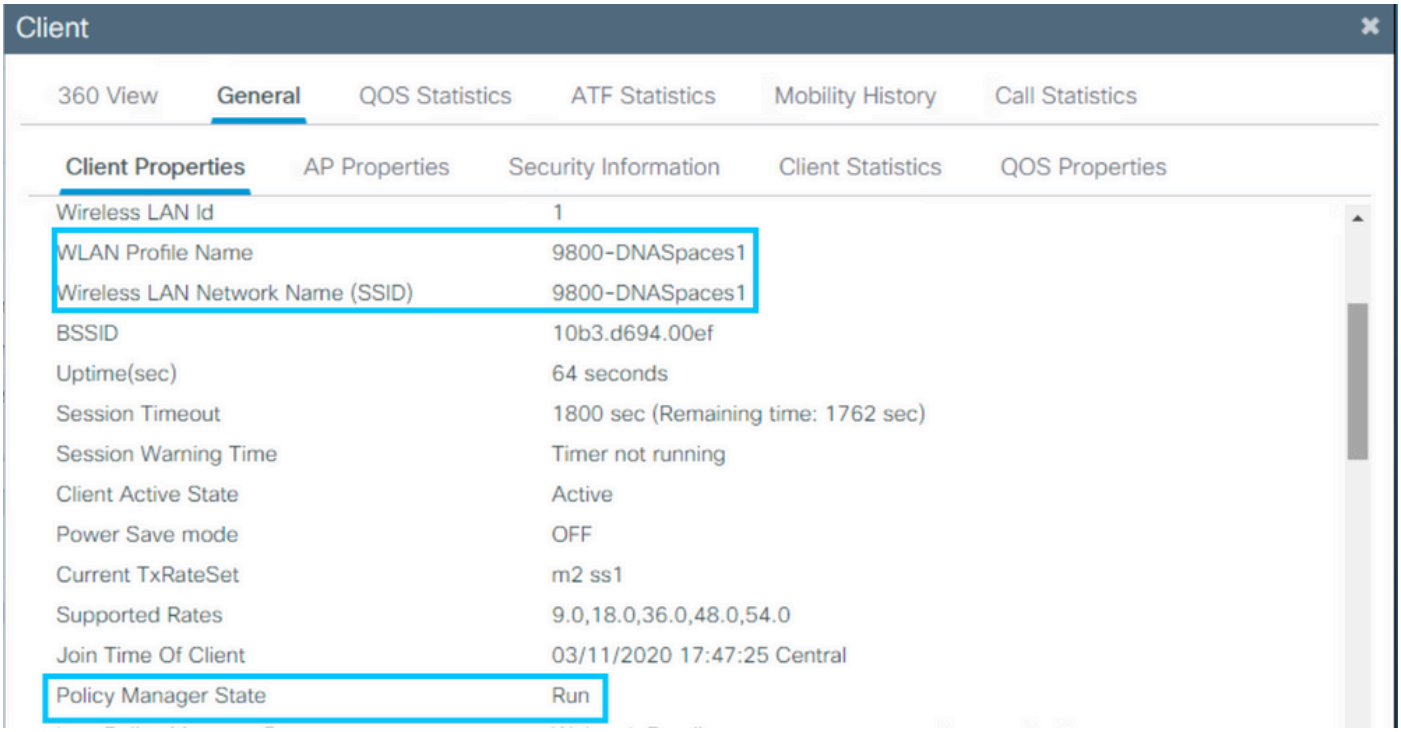
11 Click **New**.

12 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1813
Secret Key: emeab1299E2PqvUK

Verifica

Per confermare lo stato di un client connesso all'SSID, passare a **Monitoraggio > Client**, fare clic sull'indirizzo MAC del dispositivo e cercare Stato di Policy Manager:



Risoluzione dei problemi

Problemi comuni

1. Se per l'interfaccia virtuale sul controller non è configurato alcun indirizzo IP, i client vengono reindirizzati al portale interno anziché al portale di reindirizzamento configurato nella mappa dei parametri.

2. Se i client ricevono un *errore 503* durante il reindirizzamento al portale in Spazi DNA, verificare che il controller sia configurato nella **gerarchia di posizione** in Spazi DNA.

Traccia sempre attiva

WLC 9800 offre funzionalità di traccia ALWAYS-ON. In questo modo, tutti gli errori relativi alla connettività del client, gli avvisi e i messaggi a livello di avviso vengono costantemente registrati ed è possibile visualizzare i registri di un evento imprevisto o di una condizione di errore dopo che si è verificato.

> **Nota**: a seconda del volume di log generati, è possibile tornare indietro di alcune ore a diversi giorni.

Per visualizzare le tracce raccolte per impostazione predefinita dal protocollo 9800 WLC, è possibile connettersi al protocollo 9800 WLC tramite SSH/Telnet e procedere come segue (accertarsi di registrare la sessione su un file di testo).

Passaggio 1. Controllare l'ora corrente del controller in modo da poter tenere traccia dei log nel tempo che intercorre tra il momento in cui si è verificato il problema.

```
# show clock
```

Passaggio 2. Raccogliere syslog dal buffer del controller o dal syslog esterno in base alla configurazione del sistema. In questo modo è possibile visualizzare rapidamente lo stato del sistema e gli eventuali errori.

```
# show logging
```

Passaggio 3. Verificare se sono abilitate le condizioni di debug.

```
# show debugging
Cisco IOS-XE Conditional Debug Configs:

Conditional Debug Global State: Stop

Cisco IOS-XE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                            Port
------------------------------------------------------|----------
```

> **Nota**: se viene visualizzata una condizione, significa che le tracce vengono registrate a livello di debug per tutti i processi che soddisfano le condizioni abilitate (indirizzo MAC, indirizzo IP e così via). Ciò aumenta le dimensioni dei log. Pertanto, si consiglia di cancellare tutte le condizioni quando non si effettua attivamente il debug.

Passaggio 4. Se l'indirizzo mac in fase di test non è stato elencato come condizione nel passaggio 3, raccogliere le tracce del livello di avviso always on per l'indirizzo mac specifico.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

Èpossibile visualizzare il contenuto della sessione oppure copiare il file su un server TFTP esterno.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Debug condizionale e traccia Radioactive (RA)

Se le tracce sempre attive non forniscono informazioni sufficienti per determinare il trigger del problema in esame, è possibile abilitare il debug condizionale e acquisire la traccia Radio attiva (RA), che fornisce le tracce dei livelli di debug per tutti i processi che interagiscono con la condizione specificata (in questo caso l'indirizzo MAC del client). Per abilitare il debug condizionale, eseguire la procedura seguente.

Passaggio 1. Accertarsi che non vi siano condizioni di debug abilitate.

```
# clear platform condition all
```

Passaggio 2. Abilitare la condizione di debug per l'indirizzo MAC del client wireless che si desidera

monitorare.

Questi comandi iniziano a monitorare l'indirizzo MAC fornito per 30 minuti (1800 secondi). È possibile aumentare questo tempo fino a 2085978494 secondi.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

> **Nota**: per monitorare più client alla volta, eseguire il comando debug wireless mac <aaa.bbbb.ccc> per ogni indirizzo MAC.

> **Nota**: non si visualizza l'output dell'attività del client nella sessione terminale, in quanto tutto viene memorizzato internamente per essere visualizzato successivamente.

Passaggio 3. Riprodurre il problema o il comportamento che si desidera monitorare.

Passaggio 4. Interrompere i debug se il problema viene riprodotto prima che il tempo di monitoraggio predefinito o configurato sia attivo.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Una volta trascorso il tempo di monitoraggio o interrotto il debug wireless, il controller 9800 WLC genera un file locale con il nome:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Passaggio 5. Recuperare il file dell'attività dell'indirizzo MAC. È possibile copiare la traccia RA .log su un server esterno o visualizzare l'output direttamente sullo schermo.

Controllare il nome del file delle tracce RA

```
# dir bootflash: | inc ra_trace
```

Copiare il file su un server esterno:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
tftp://a.b.c.d/ra-FILENAME.txt
```

Visualizzare il contenuto:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Passaggio 6. Se la causa principale non è ancora ovvia, raccogliere i log interni che offrono una visualizzazione più dettagliata dei log del livello di debug. non è necessario eseguire di nuovo il debug del client. Per ulteriori informazioni, vedere i log di debug già raccolti e archiviati internamente.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }
to-file ra-internal-<FILENAME>.txt
```

> **Nota**: questo output del comando restituisce tracce per tutti i livelli di registrazione per tutti i processi ed è piuttosto voluminoso. Contattare Cisco TAC per analizzare queste tracce.

Èpossibile copiare il file ra-internal-FILENAME.txt su un server esterno o visualizzare l'output direttamente sullo schermo.

Copiare il file su un server esterno:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Visualizzare il contenuto:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Passaggio 7. Rimuovere le condizioni di debug.

```
# clear platform condition all
```

> **Nota**: assicurarsi di rimuovere sempre le condizioni di debug dopo una sessione di risoluzione dei problemi.

Esempio di tentativo riuscito

Questo è l'output di RA_traces per 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:

```
Association received. BSSID 10b3.d694.00ee, WLAN 9800DNASpaces, Slot 1 AP 10b3.d694.00e0,
2802AP-9800L
Received Dot11 association request. Processing started,SSID: 9800DNASpaces1, Policy profile:
DNASpaces-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan
ID: 1RSSI: 0, SNR: 32
Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
dot11 send association response. Sending association response with resp_status_code: 0
dot11 send association response. Sending assoc response of length: 144 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS
Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

Processo di apprendimento IP:

```
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
Client IP learn successful. Method: ARP IP: 10.10.30.42
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
Received ip learn response. method: IPLEARN_METHOD_AR
```

Autenticazione di livello 3:

```
Triggered L3 authentication. status = 0x0, Success
Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
L3 Authentication initiated. LWA
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING


Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
INIT state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src
[10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Microsoft NCSI
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
LOGIN state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src
[10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in
LOGIN state
```

Autenticazione di livello 3 completata. Spostare il client nello stato RUN:

```
[34e1.2d23.a668:capwap_90000005] Received User-Name 34E1.2D23.A668 for client 34e1.2d23.a668
L3 Authentication Successful. ACL:[]
Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entry (34E1.2D23.A668) joined with ssid
(9800DNASpaces) for device with MAC: 34e1.2d23.a668
Managed client RUN state notification: 34e1.2d23.a668
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU
```

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).