Configura autenticazione Web centrale su SD-Access

Sommario

Introduzione

Questo documento descrive una guida dettagliata alla configurazione di CWA (Central Web Authentication) e delinea le procedure di verifica per tutti i componenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Catalyst 9800 Wireless Controller Architecture
- Autenticazione, autorizzazione e accounting (AAA)

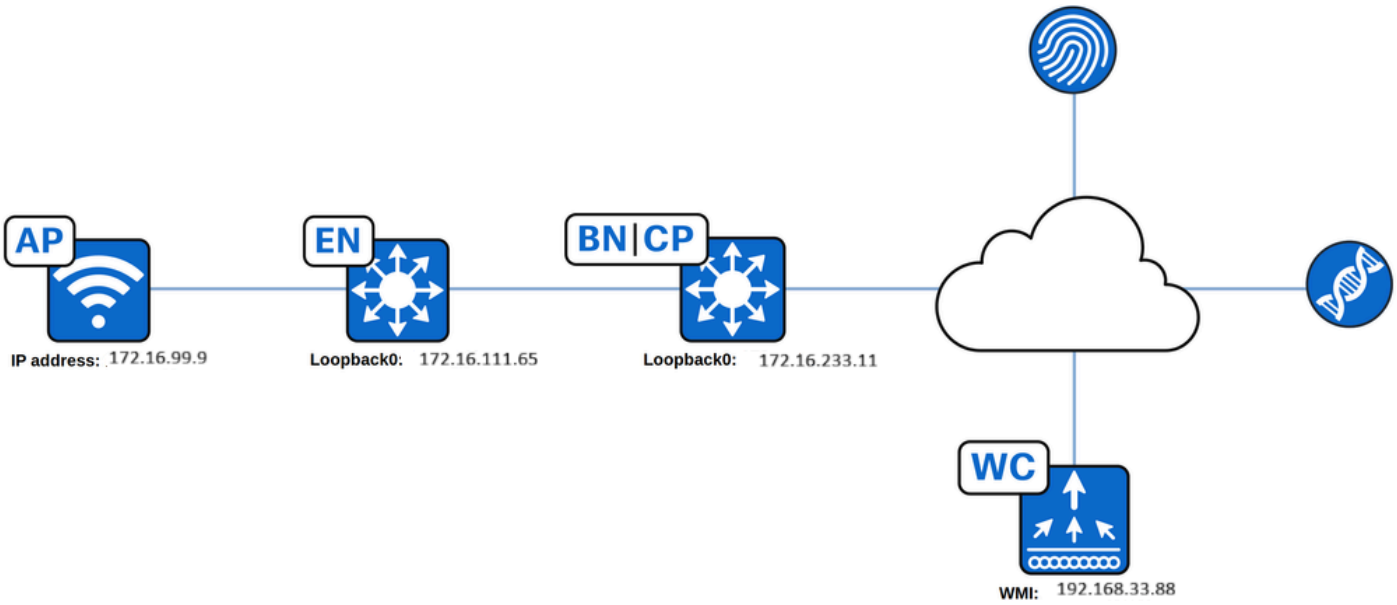
Componenti usati

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

- Cisco Wireless LAN Controller (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - Versione 2.3.7.7
- Cisco Identity Services Engine (ISE) - Versione 3.0.0.458
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- SDA Border Node/Control Plane - C9500-48P, Cisco IOS® XE17.12.05
- Cisco Access Point - C9130AXI-A, versione 17.9.5.47

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.

Topologia



Panoramica

Central Web Authentication (CWA) utilizza un SSID di tipo guest per reindirizzare il browser Web dell'utente a un portale in cattività ospitato da Cisco ISE, utilizzando un ACL di reindirizzamento configurato. Il portale captive consente all'utente di registrarsi e autenticarsi e, dopo l'autenticazione, il controller WLC (Wireless LAN Controller) applica l'autorizzazione appropriata per concedere l'accesso completo alla rete. In questa guida vengono fornite istruzioni dettagliate per la configurazione di CWA con Cisco Catalyst Center.

Configurazione di CWA su Cisco Catalyst Center

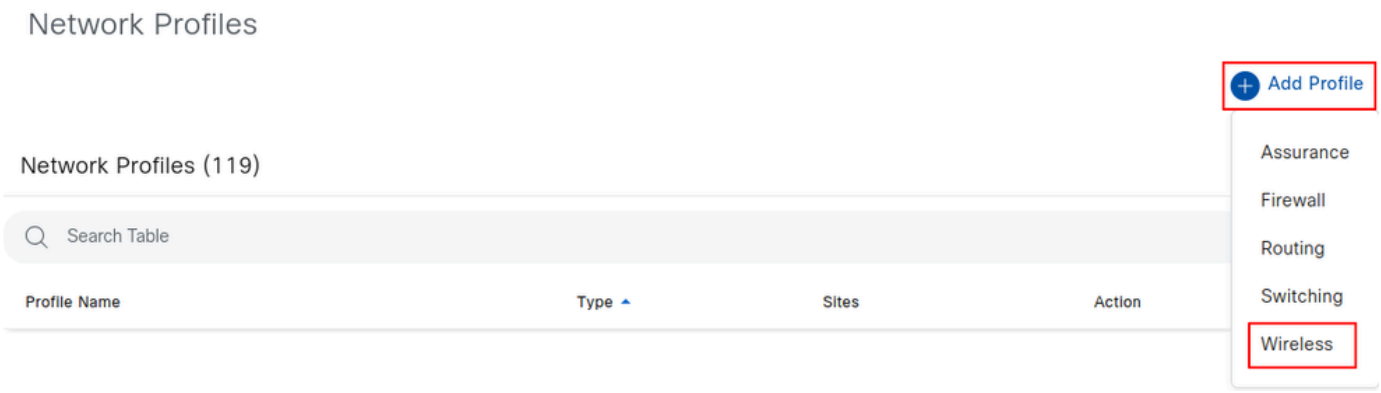
Creazione del profilo di rete

Un profilo di rete consente di configurare le impostazioni che possono essere applicate a un sito specifico. I profili di rete possono essere creati per diversi elementi in Cisco Catalyst Center, tra cui:

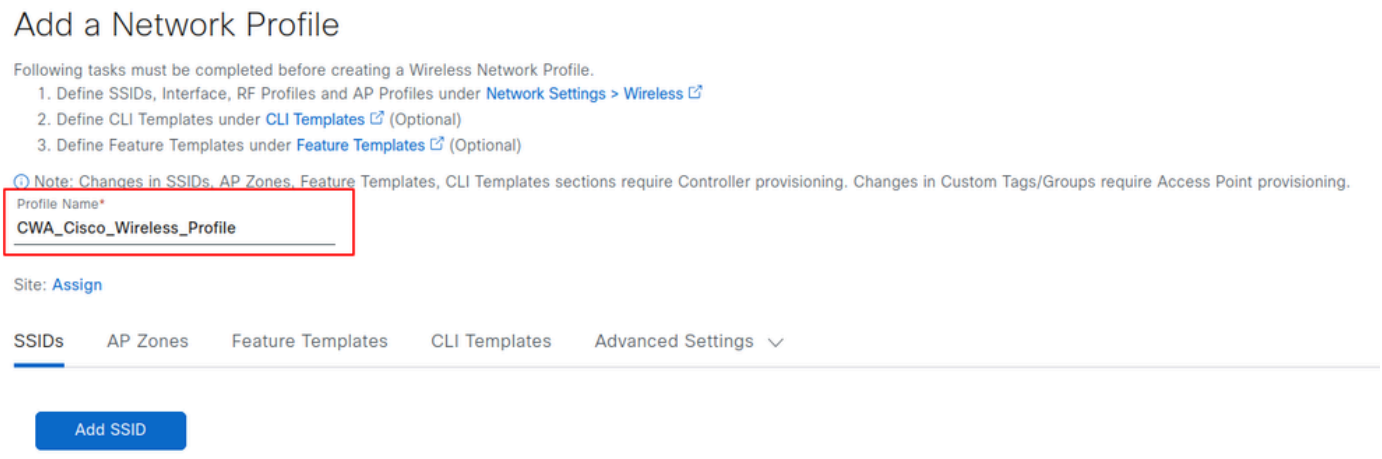
- Garanzia
- Firewall
- Routing
- Switching
- Appliance di telemetria
- Wireless

Per CWA è necessario configurare un profilo wireless.

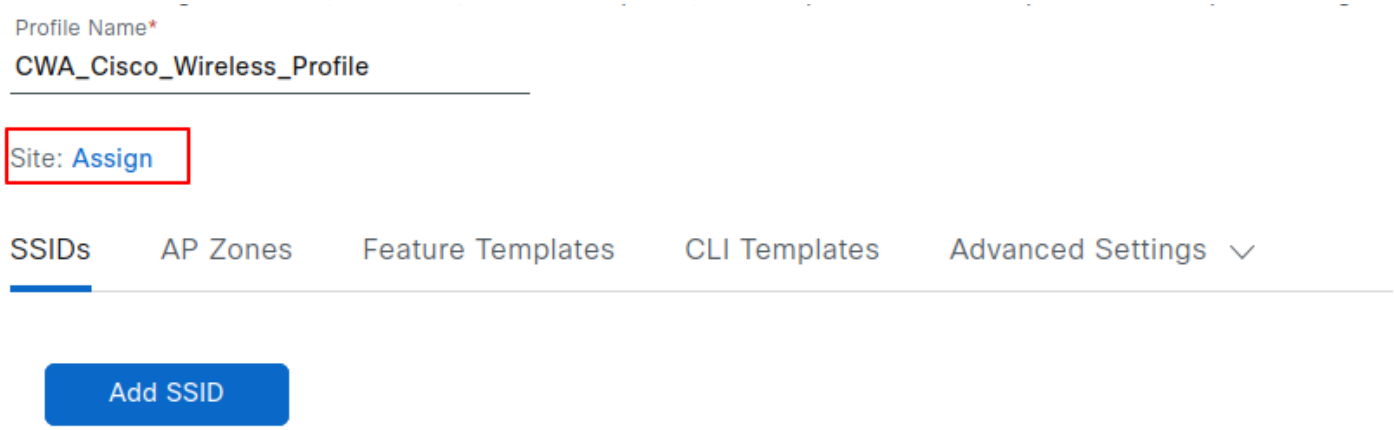
Per configurare un profilo wireless, passare a Progettazione > Profili di rete, fare clic su Aggiungi profilo e selezionare Wireless.



Assegnare al profilo il nome desiderato. In questo esempio, il profilo wireless è denominato CWA_Cisco_Wireless_Profile. È possibile aggiungere qualsiasi SSID esistente al profilo selezionando Aggiungi SSID. La creazione di SSID è illustrata nella sezione successiva.

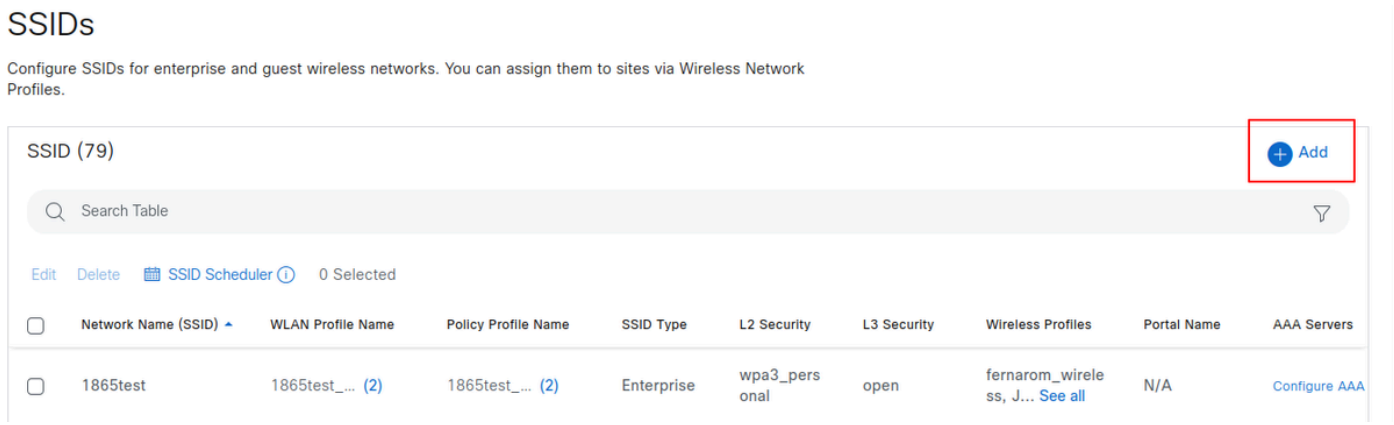


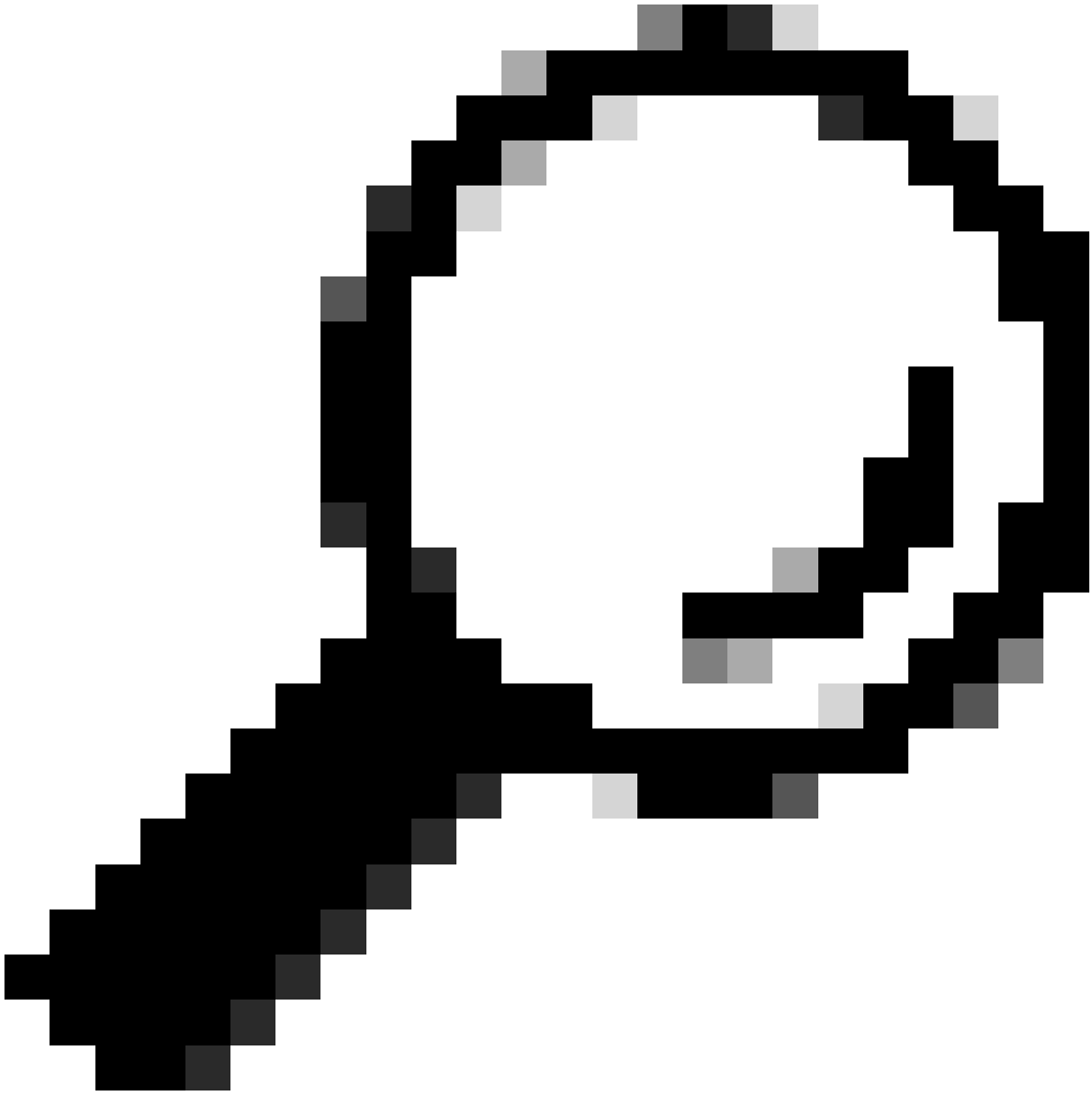
Selezionare Assegna per scegliere il sito a cui applicare il profilo, quindi selezionare il sito desiderato. Dopo aver selezionato i siti, fare clic su Salva.



Creare l'SSID

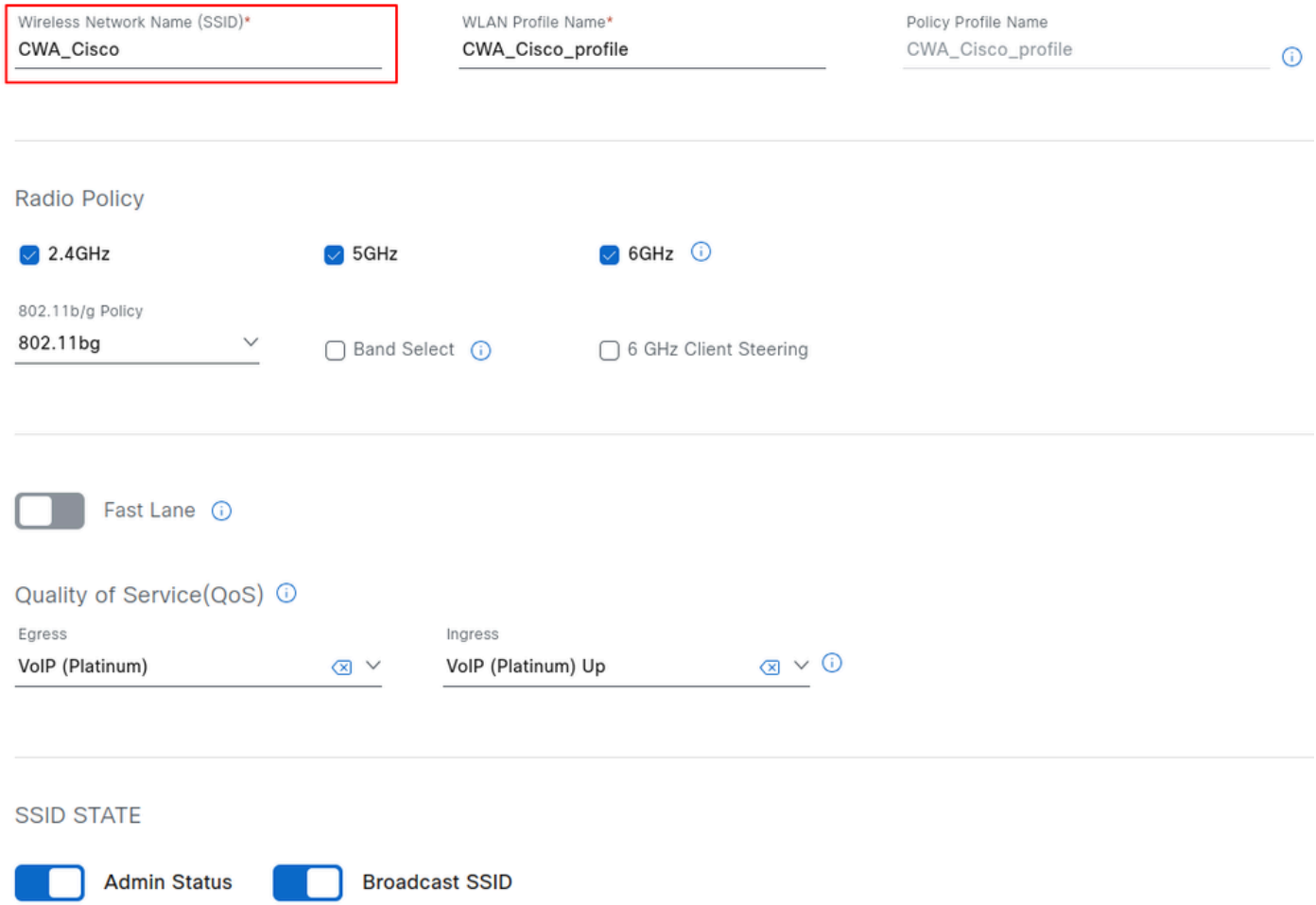
Selezionare Progettazione > Impostazioni di rete > Wireless > SSID e fare clic su Aggiungi.



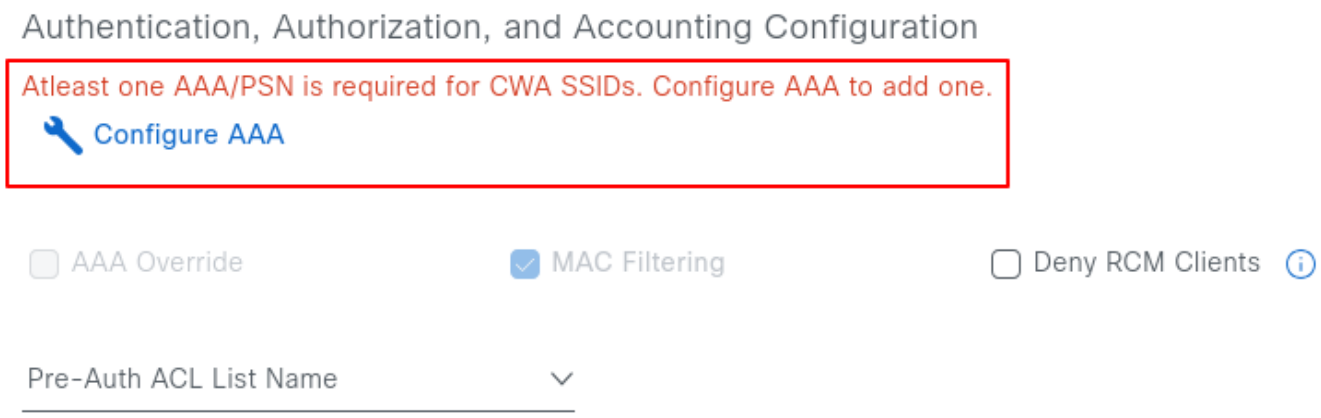


Suggerimento: Quando si crea un SSID per CWA, è essenziale selezionare il tipo Guest. Questa selezione aggiunge un comando al profilo dei criteri wireless del SSID sul WLC - il comando nac - che consente di utilizzare il CoA per la riautenticazione dopo la registrazione dell'utente sul portale captive. Senza questa configurazione, gli utenti possono sperimentare un ciclo infinito di registrazione e reindirizzamento ripetuto al portale.

Dopo aver selezionato Aggiungi, procedere con il flusso di lavoro di configurazione SSID. Nella prima pagina configurare il nome SSID, è inoltre possibile selezionare la banda dei criteri radio e definire lo stato SSID, inclusi lo stato amministrativo e le impostazioni di trasmissione. Per questa guida alla configurazione, il nome dell'SSID è CWA_Cisco.



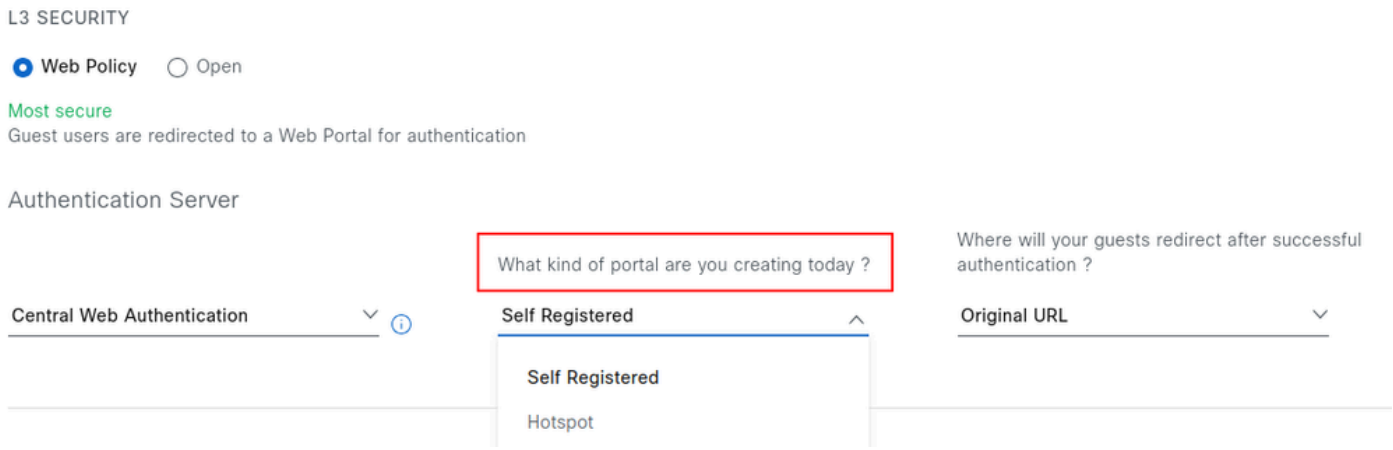
Dopo aver immesso il nome SSID, vengono generati automaticamente il nome del profilo WLAN e il nome del profilo dei criteri. Selezionare Avanti per continuare.
È necessario configurare almeno un AAA/PSN per gli SSID CWA. Se non è stato configurato alcun indirizzo, selezionare Configure AAA e scegliere l'indirizzo IP PSN dall'elenco a discesa.



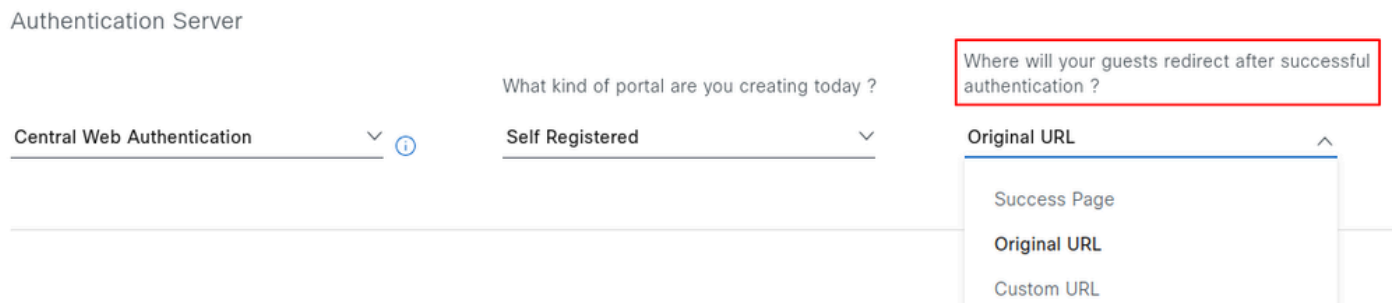
Dopo aver selezionato il server AAA, impostare i parametri di sicurezza di layer 3 e selezionare il tipo di portale: Auto-registrato o hotspot.

Portali ospiti hotspot: Un portale per gli ospiti degli hotspot fornisce l'accesso alla rete senza la necessità di nomi utente e password. In questo caso, gli utenti devono accettare un criterio di utilizzo accettabile per ottenere l'accesso alla rete e ottenere quindi l'accesso a Internet. L'accesso

tramite un portale guest con credenziali richiede che gli utenti guest dispongano di nome utente e password.



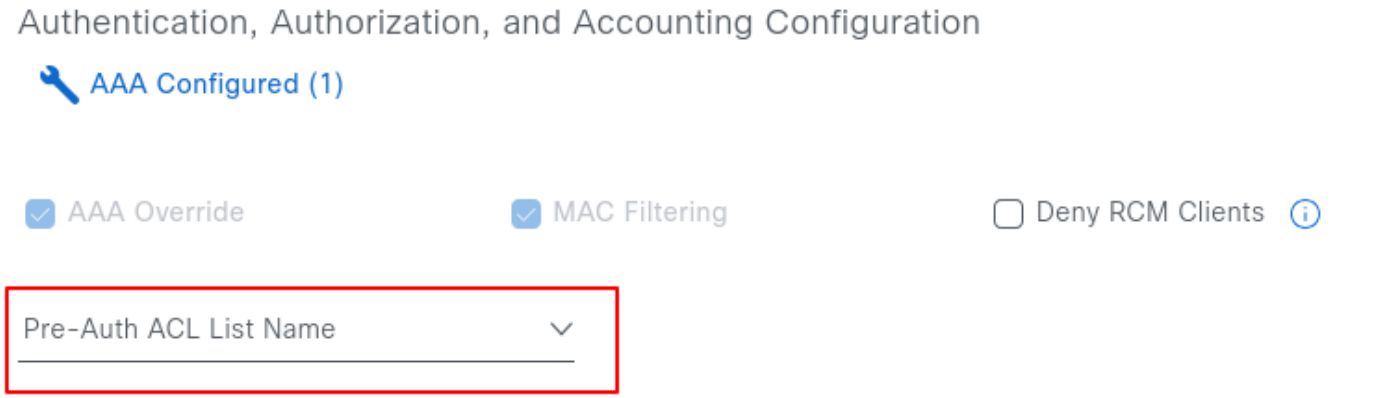
È inoltre possibile configurare l'azione che si verifica dopo la registrazione o l'accettazione del criterio di utilizzo da parte dell'utente. Sono disponibili tre opzioni: Success Page, Original URL, e Custom URL.



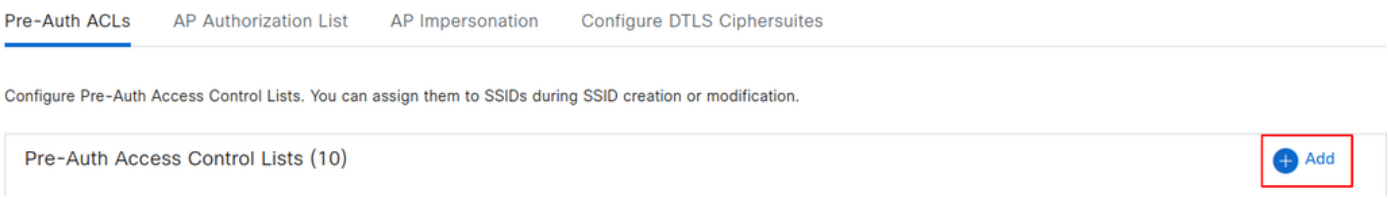
Di seguito viene descritto il comportamento di ciascuna opzione:

Pagina Operazione riuscita: Reindirizza l'utente a una pagina di conferma indicante che l'autenticazione è stata eseguita correttamente.
URL originale: reindirizza l'utente all'URL originale richiesto prima di essere intercettato dal portale vincolato.
URL personalizzato: reindirizza l'utente a un URL personalizzato specificato. Selezionando questa opzione si abilita un campo aggiuntivo per definire l'URL di destinazione

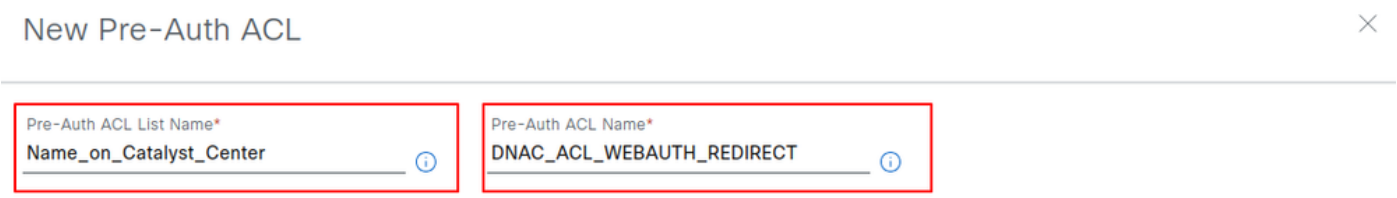
Nella stessa pagina, in Autenticazione, Autorizzazione e Configurazione accounting, è possibile configurare anche un ACL di preautenticazione. Questo ACL consente di aggiungere altre voci per i protocolli oltre agli indirizzi IP DHCP, DNS o PSN, ottenuti dalle impostazioni di rete e aggiunti all'ACL di reindirizzamento durante il provisioning. Questa funzionalità è disponibile in Cisco Catalyst Center versione 2.3.3.x e successive.



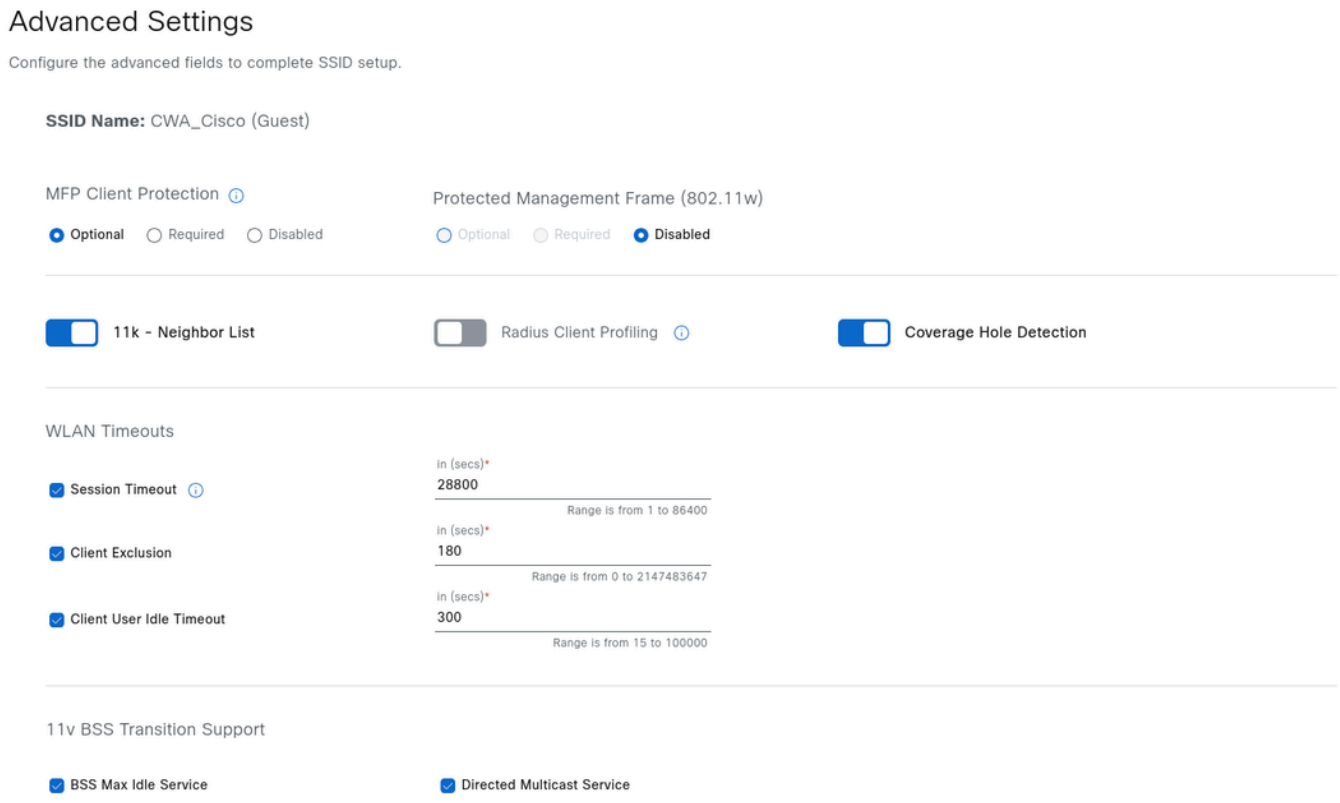
Per configurare un ACL di pre-autenticazione, selezionare Progettazione > Impostazioni di rete > Wireless > Impostazioni di sicurezza, quindi fare clic su Aggiungi.



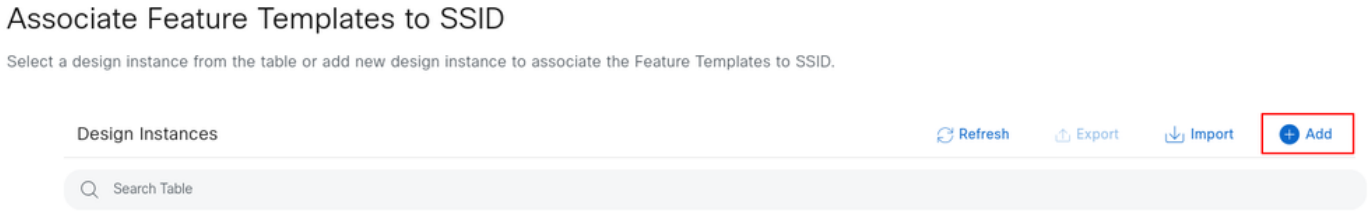
Il primo nome identifica l'ACL nel Catalyst Center, mentre il secondo nome corrisponde al nome ACL sul WLC. Il secondo nome può corrispondere all'ACL di reindirizzamento esistente configurato sul WLC. Come riferimento, Catalyst Center assegna il nome Cisco DNA_ACL_WEBAUTH_REDIRECT al WLC. Le voci dell'ACL di pre-autenticazione vengono aggiunte dopo le voci esistenti.



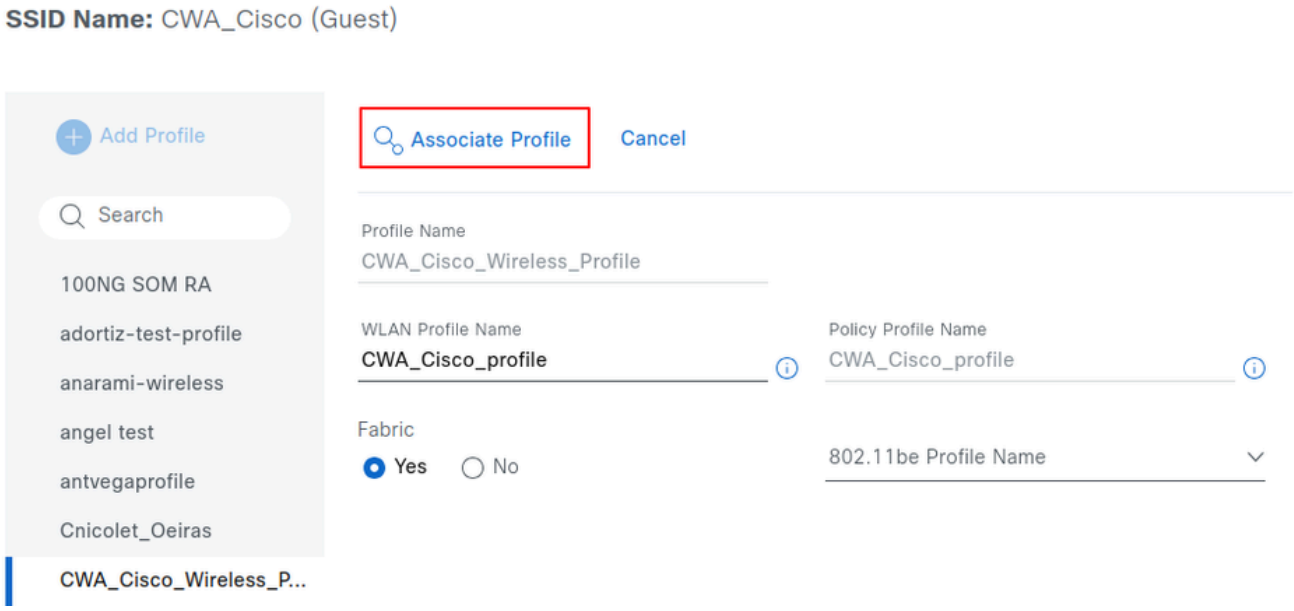
Tornando al flusso di lavoro di creazione dell'SSID, selezionando Avanti vengono visualizzate le impostazioni avanzate, tra cui transizione rapida, timeout della sessione, timeout dell'utente client e limitazione della velocità. Regolate i parametri come richiesto, quindi selezionate Succ (Next) per continuare. Ai fini della presente guida alla configurazione, l'esempio mantiene le impostazioni predefinite.



Dopo aver selezionato Avanti, viene visualizzato un prompt per associare i modelli di funzionalità all'SSID. Se applicabile, selezionare i modelli desiderati facendo clic su Aggiungi e al termine fare clic su Avanti.

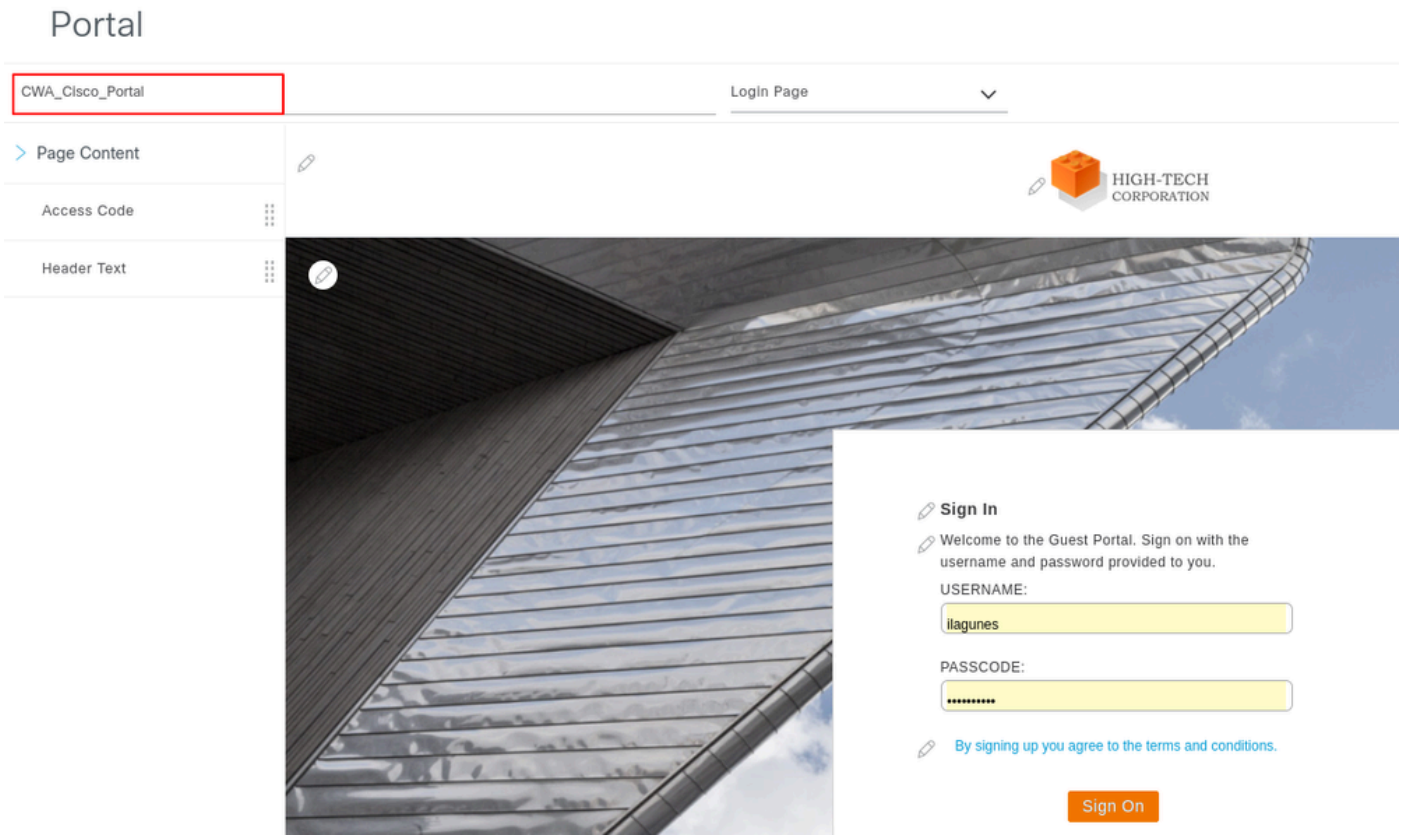


Associare il SSID al profilo wireless creato in precedenza. Per riferimento, vedere la sezione Creazione del profilo di rete wireless. In questa sezione è anche possibile selezionare se il SSID è abilitato o meno per l'infrastruttura. Al termine, fare clic su Associa profilo.

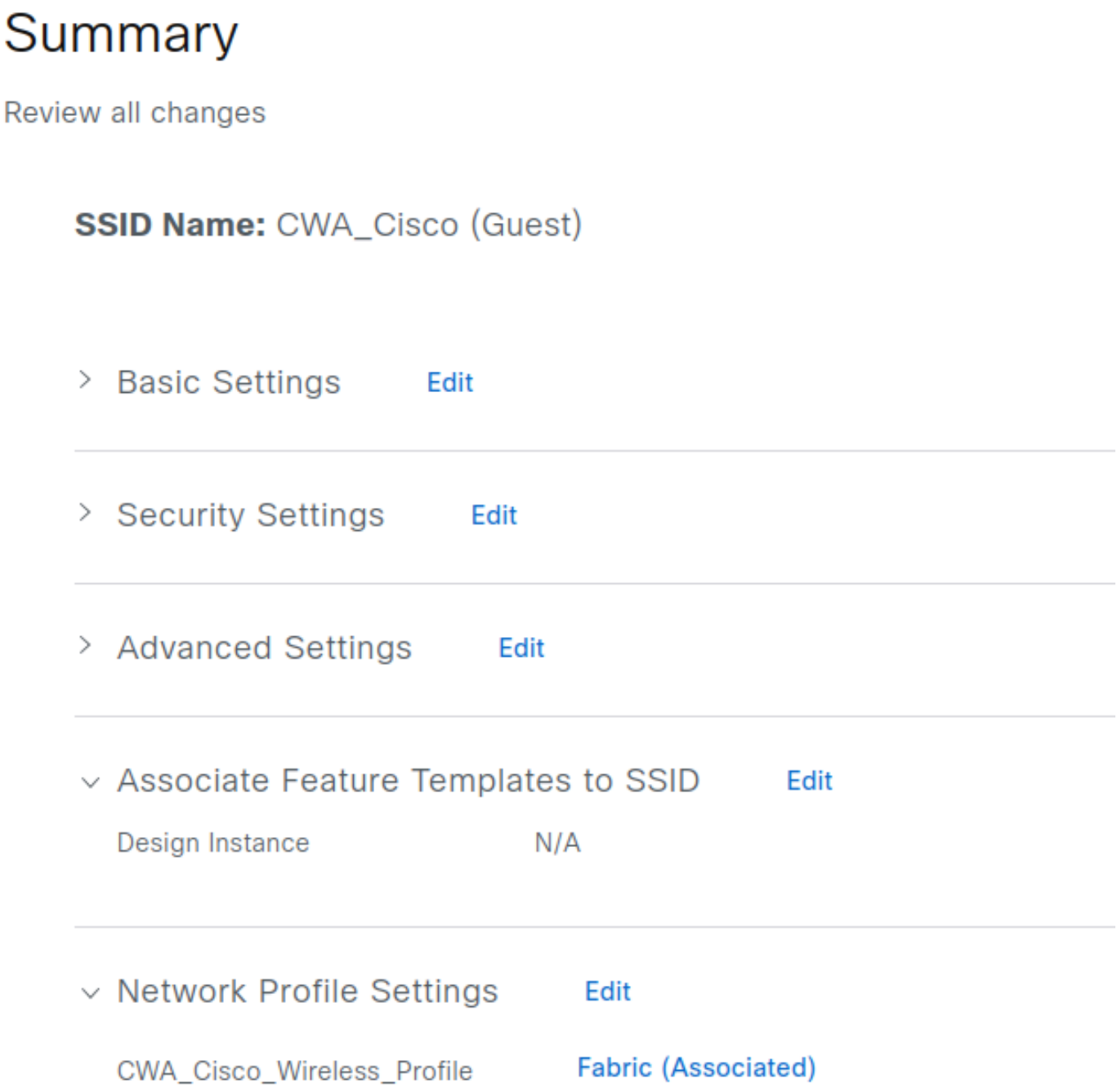


mostra trust point gestione wireless
Una volta associato il profilo all'SSID, fare clic su Avanti per creare e progettare il portale vincolato, per iniziare, fare clic su Crea portale.

Il nome del portale definisce il nome di dominio nell'FQDN e il nome del set di criteri in ISE. Al termine, fare clic su Salva. Il portale rimane modificabile e può essere eliminato se necessario.



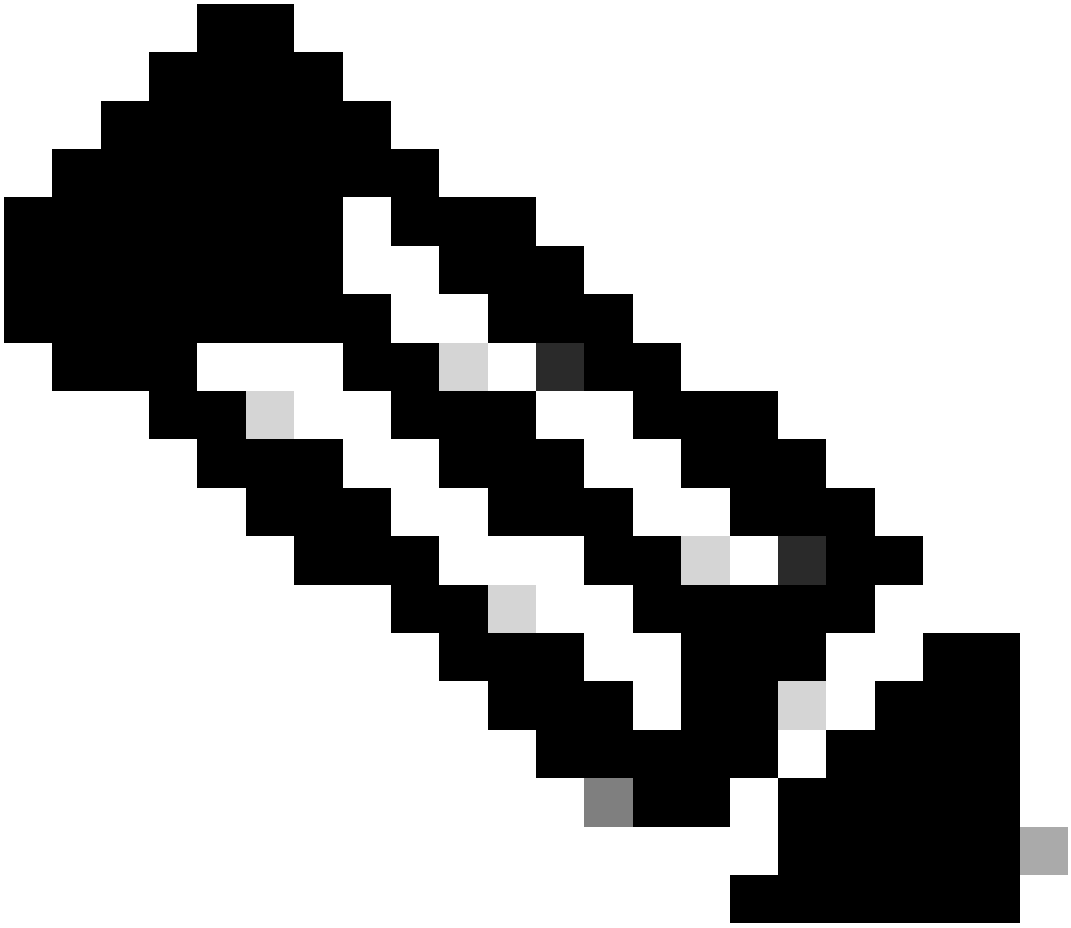
Selezionare Successivo per visualizzare un riepilogo di tutti i parametri di configurazione definiti nei passi precedenti.



Confermare i dettagli di configurazione, quindi selezionare Salva per applicare le modifiche.

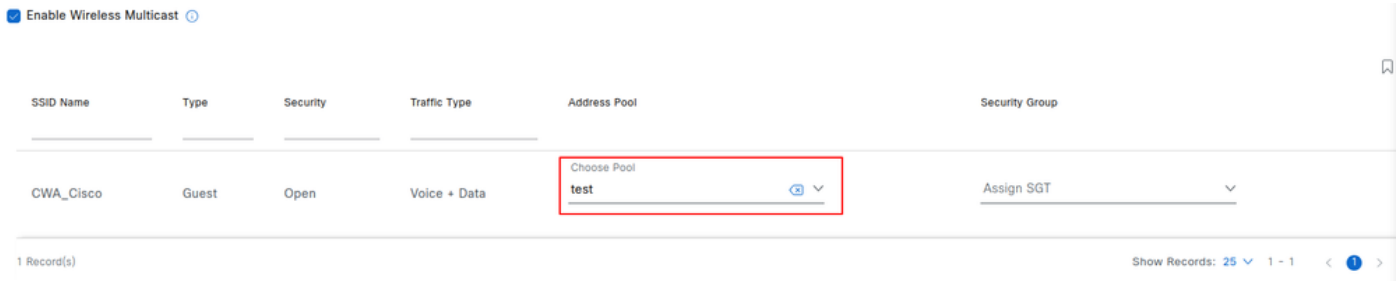
Provisioning fabric

Dopo aver associato il profilo di rete wireless al sito dell'infrastruttura, l'SSID viene visualizzato in Provisioning > Siti dell'infrastruttura > (sito) > SSID wireless.

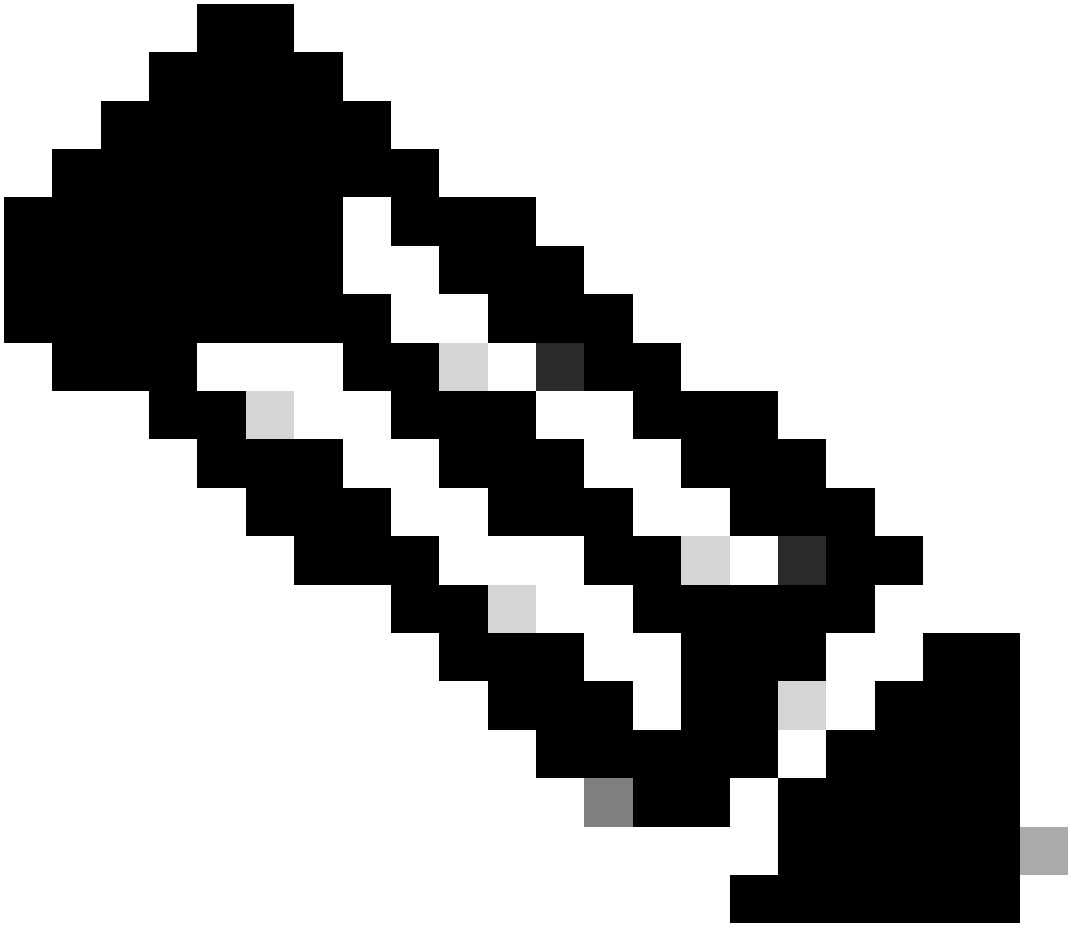


Nota: È necessario eseguire il provisioning del controller LAN wireless del sito per visualizzare gli SSID in SSID wireless

Scegliere il pool SSID, associare facoltativamente un tag del gruppo di sicurezza e fare clic su Distribuisci. L'SSID viene trasmesso dai punti di accesso solo se è stato assegnato un pool.



Sui controller AireOS e Catalyst 9800, eseguire nuovamente il provisioning del controller LAN wireless dopo eventuali modifiche della configurazione SSID in Impostazioni di rete.



Nota: Se al SSID non è assegnato alcun pool, è probabile che gli AP non lo trasmettano. L'SSID viene trasmesso solo dopo l'assegnazione di un pool. Una volta assegnato il pool, non è necessario effettuare nuovamente il provisioning del controller.

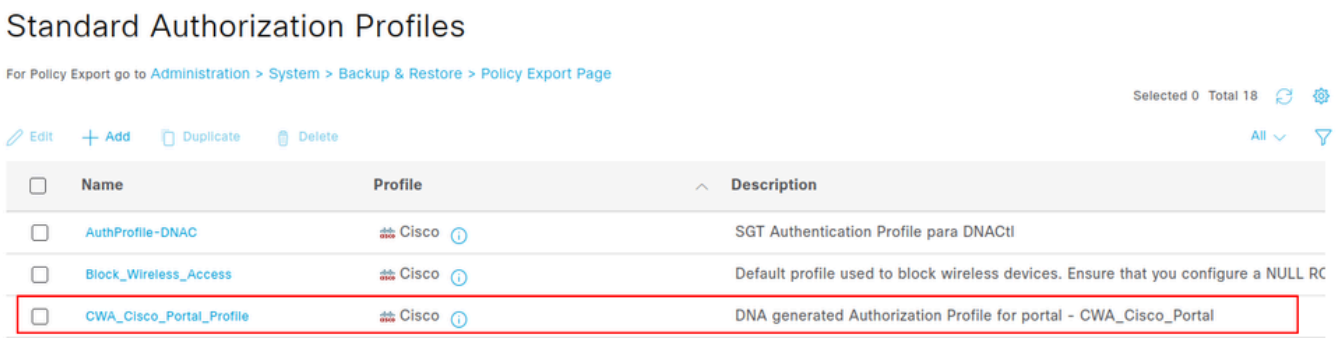
Revisione della configurazione fornita a Cisco ISE

In questa sezione viene esaminata la configurazione fornita dal Catalyst Center a Cisco ISE.

Profilo di autorizzazione

Parte della configurazione di Cisco ISE in cui Catalyst Center esegue il provisioning è un profilo di autorizzazione. Questo profilo definisce il risultato assegnato a un client in base ai suoi parametri e può includere impostazioni specifiche come l'assegnazione della VLAN, gli ACL o i reindirizzamenti dell'URL.
Per visualizzare il profilo di autorizzazione in ISE, selezionare Policy > Policy Elements > Results (Policy > Elementi criteri > Risultati). Se il nome del portale è CWA_Cisco_Portal, il nome del profilo è CWA_Cisco_Portal_Profile. Nel campo Description (Descrizione) viene visualizzato il

testo: Profilo di autorizzazione generato da DNA per il portale - CWA_Cisco_Portal.



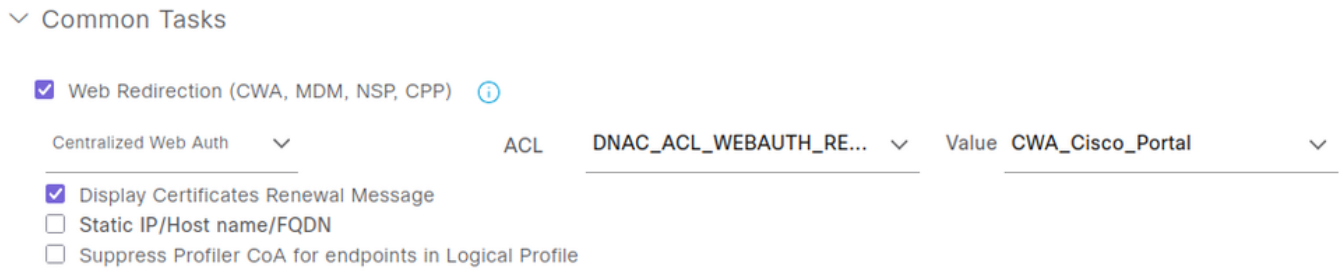
Per visualizzare gli attributi inviati al controller LAN wireless dal profilo di autorizzazione, fare clic sul nome del profilo di autorizzazione e consultare la sezione Attività comuni.
Questo profilo di autorizzazione fornisce l'ACL di reindirizzamento e l'URL di reindirizzamento.

L'attributo di reindirizzamento Web include due parametri:

1. Nome ACL: impostato su Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Valore: fa riferimento al nome del portale vincolato, in questo esempio CWA_Cisco_Portal.

L'opzione Visualizza messaggio di rinnovo certificati consente di utilizzare il portale per il rinnovo dei certificati attualmente utilizzati dall'endpoint.

In Visualizza messaggio di rinnovo certificati è disponibile un'opzione aggiuntiva, Nome host/FQDN statico. Questa funzionalità consente il recapito dell'indirizzo IP del portale anziché del relativo FQDN, utile quando il portale vincolato non viene caricato a causa dell'impossibilità di raggiungere il server DNS.

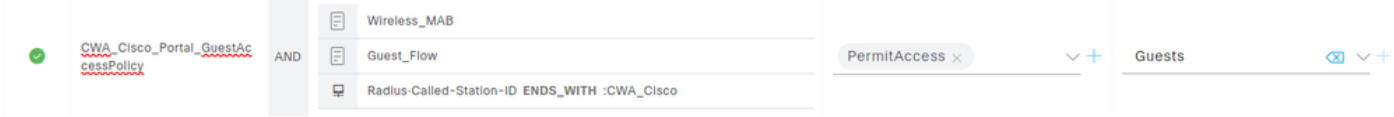


Set di criteri

Selezionare Criterio > Set di criteri > Predefinito > Criterio di autorizzazione per visualizzare i due set di criteri creati per il portale denominato CWA_Cisco_Portal. Tali set di criteri sono:

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

Il criterio CWA_Cisco_Portal_GuestAccessPolicy viene applicato quando il client ha già completato il processo di autenticazione Web, tramite registrazione automatica o tramite il portale dell'hotspot.

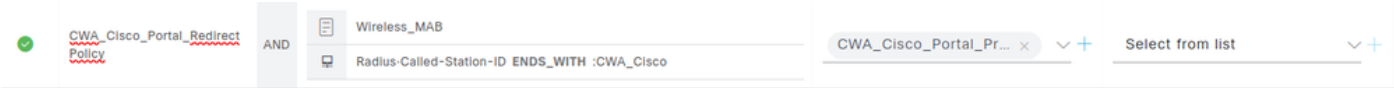


Questo set di criteri soddisfa tre criteri:

- Wireless_MAB: utilizzato quando Cisco ISE riceve una richiesta di autenticazione MAC Authentication Bypass (MAB) da un controller LAN wireless.
- Flusso_guest: Fa riferimento al controllo da parte di ISE dell'indirizzo MAC dell'endpoint rispetto al gruppo di identità GuestEndpoints. Se l'indirizzo MAC dell'endpoint non è presente in questo gruppo, il criterio non verrà applicato.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-ID è un attributo RADIUS in ISE che memorizza l'indirizzo MAC del bridge o del punto di accesso in formato ASCII e aggiunge il SSID a cui si accede, separato da un punto e virgola (:). Nell'esempio, CWA_Cisco rappresenta il nome dell'SSID.

Sotto i profili di colonna viene visualizzato il nome PermitAccess, un profilo di autorizzazione riservato che non può essere modificato, che consente l'accesso completo alla rete e consente inoltre di assegnare un SGT nella colonna Security Groups, che in questo caso è Guests.

Viene utilizzato il profilo PermitAccess. Questo è un profilo di autorizzazione riservato che non può essere modificato e concede l'accesso completo alla rete. Nella colonna Gruppi di sicurezza può anche essere assegnato un SGT; in questo caso, il SGT è impostato su Guests.
Il criterio successivo da esaminare è CWA_Cisco_Portal_RedirectPolicy.



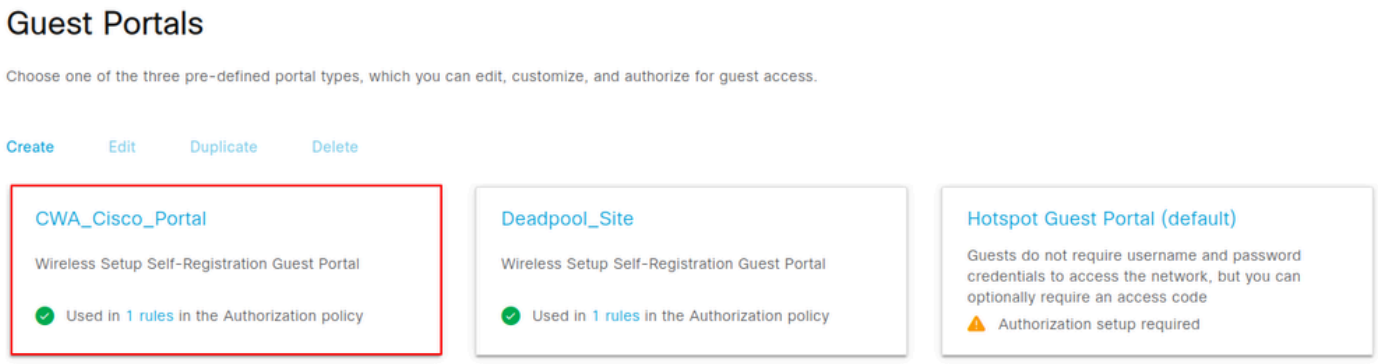
Questo set di criteri soddisfa i due criteri seguenti:

- Wireless_MAB: utilizzato quando Cisco ISE riceve una richiesta di autenticazione MAB da un controller LAN wireless.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-ID è un attributo RADIUS in ISE che memorizza l'indirizzo MAC del bridge o del punto di accesso in formato ASCII e aggiunge il SSID a cui si accede, separato da un punto e virgola (:). In questo esempio, :CWA_Cisco rappresenta il nome SSID.

L'ordine di queste politiche è critico. Se CWA_Cisco_Portal_RedirectPolicy viene visualizzato per primo nell'elenco, corrisponde solo all'autenticazione MAB e al nome SSID utilizzando l'attributo RADIUS Called-Station-ID ENDS_WITH :CWA_Training. In questa configurazione, anche se l'endpoint è già stato autenticato tramite il portale, continuerà a corrispondere a questo criterio per un periodo di tempo indefinito. Di conseguenza, l'accesso completo non viene mai concesso tramite il profilo PermitAccess e il client rimane bloccato in un ciclo continuo di autenticazione e reindirizzamento al portale.

Configurazione portale guest

Passare a Centri di lavoro > Accesso guest > Portali e componenti per visualizzare il portale. Il portale Guest creato in questa pagina utilizza lo stesso nome di Catalyst Center CWA_Cisco_Portal. Selezionare il nome del portale in cui si desidera visualizzare ulteriori dettagli.

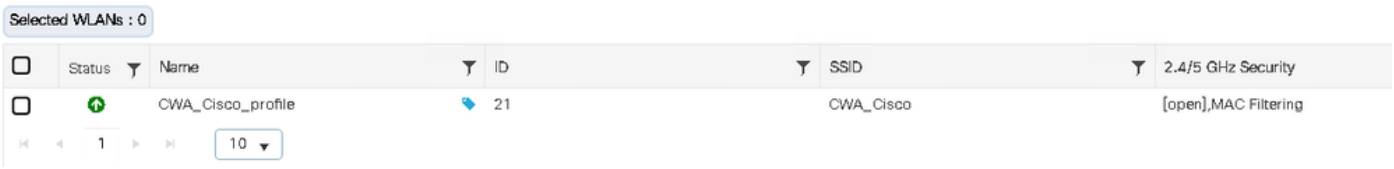


Revisione della configurazione sottoposta a provisioning sul WLC

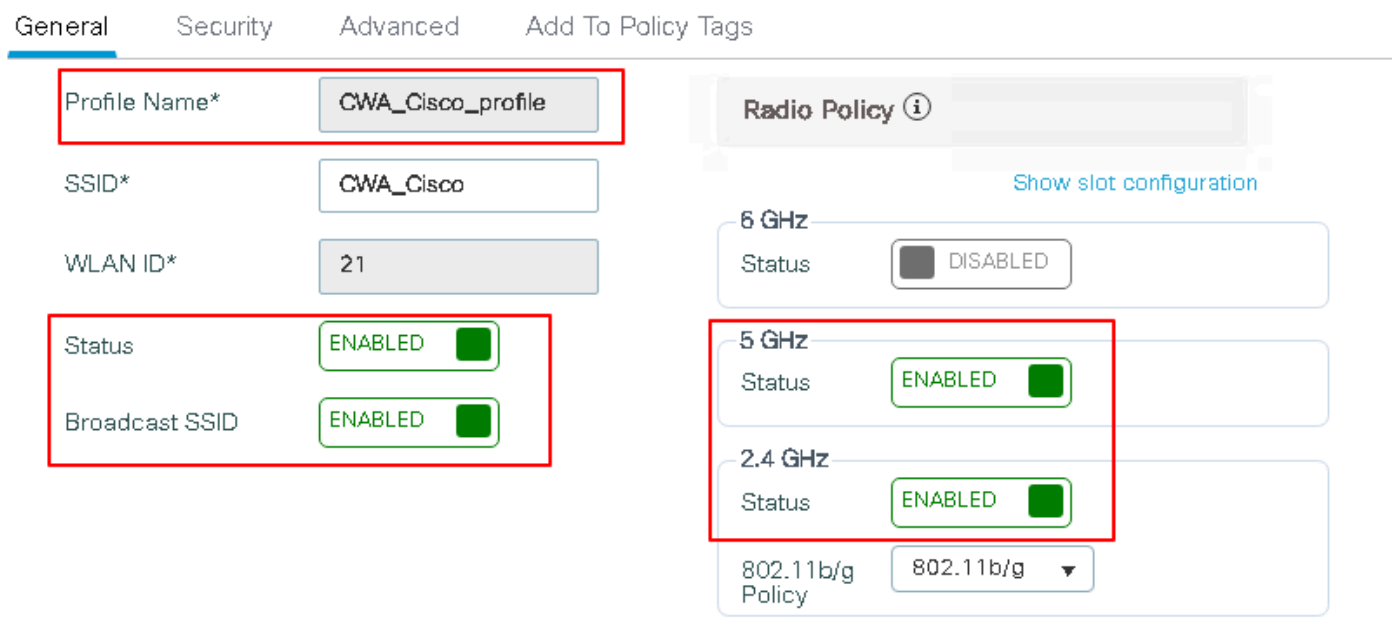
In questa sezione viene esaminata la configurazione del controller LAN wireless fornita dal Catalyst Center.

Configurazione SSID

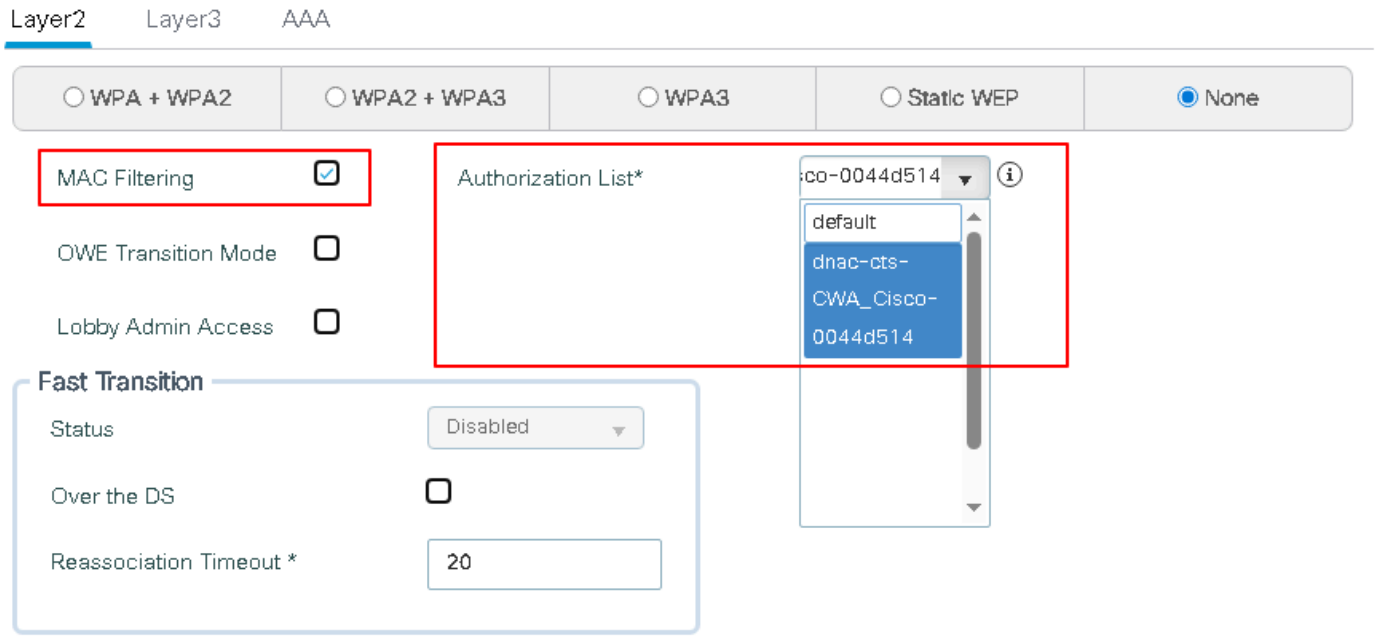
Nell'interfaccia utente del WLC, selezionare Configuration > Tags & Profiles > WLAN (Configurazione > Tag e profili > WLAN) per visualizzare la configurazione SSID.



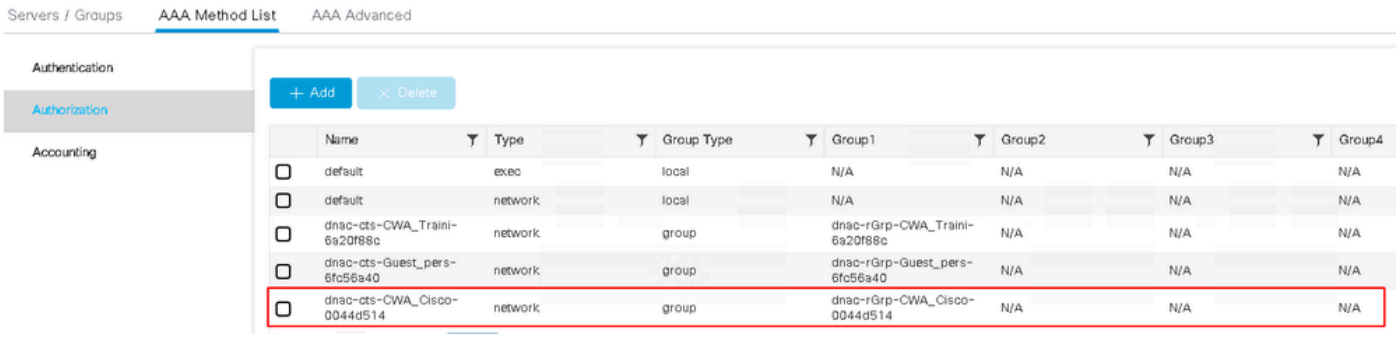
L'SSID CWA_Cisco è denominato CWA_Cisco_profile sul WLC, con ID 21 e un tipo di sicurezza Open che utilizza il filtro MAC. Fare doppio clic sull'SSID per visualizzarne la configurazione.



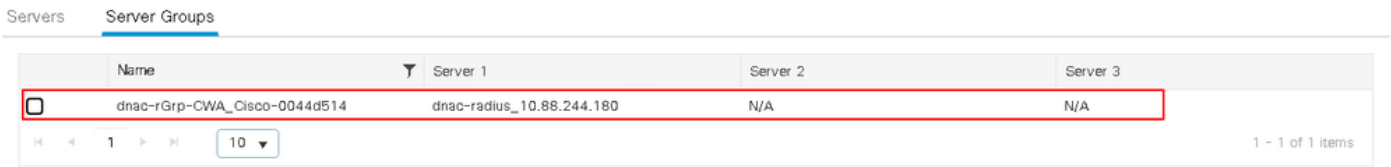
Il SSID è UP e sta trasmettendo su canali a 5 GHz e a 2,4 GHz ed è associato al profilo della policy CWA_Cisco_Profile. Fare clic sulla scheda Protezione per visualizzare le impostazioni.



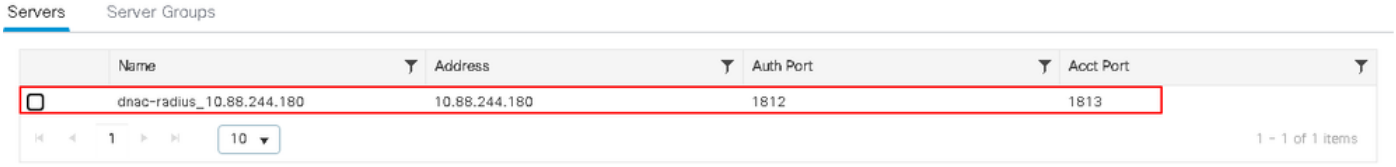
Le impostazioni chiave includono il metodo di sicurezza di layer 2 (filtro MAC) e l'elenco di autorizzazioni AAA (Cisco DNA-cts-CWA_Cisco-0044d514). Per rivedere la configurazione, selezionare Configurazione > Sicurezza > AAA > Elenco metodi AAA > Autorizzazione.



L'elenco dei metodi fa riferimento al gruppo RADIUS Cisco DNA-Grp-CWA_Cisco-0044d514 nella colonna Group1. Per visualizzare la configurazione, selezionare Configurazione > Sicurezza > AAA > Server/Gruppi > Gruppi di server.



Il gruppo di server Cisco DNA-Grp-CWA_Cisco-0044d514 fa riferimento a Cisco DNA-radius_10.88.244.180 nella colonna Server 1. Visualizzarne la configurazione nella scheda Server.



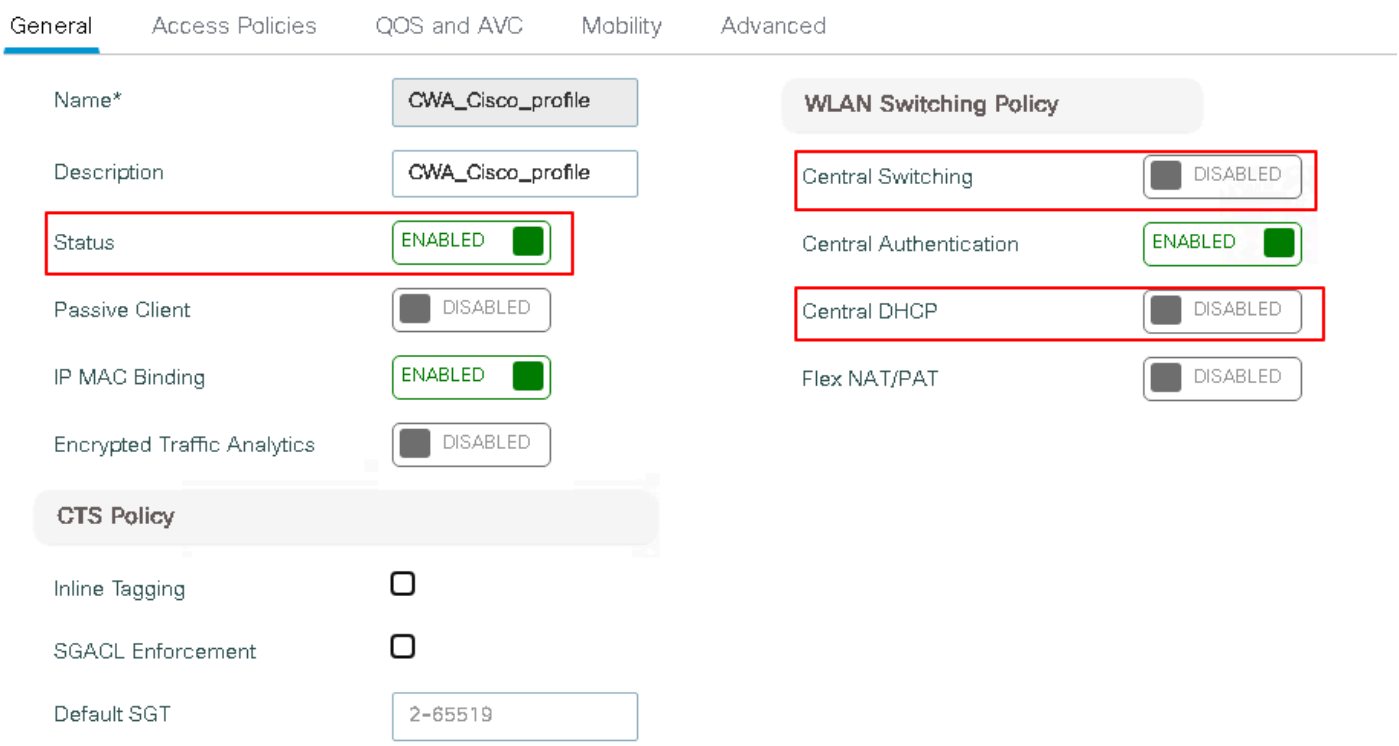
Il server Cisco DNA-radius_10.88.244.180 ha l'indirizzo IP 10.88.244.180. Fare clic sul nome per visualizzarne la configurazione

Una configurazione critica è il processo di modifica dell'autorizzazione (CoA, Change of Authorization), che fornisce un meccanismo per modificare gli attributi di una sessione di autenticazione, autorizzazione e accounting (AAA, Authentication, Authorization, and Accounting) dopo che è stata autenticata sul portale captive. Senza questa funzionalità, l'endpoint rimane nello stato web-auth in sospeso anche dopo il completamento della registrazione sul portale.

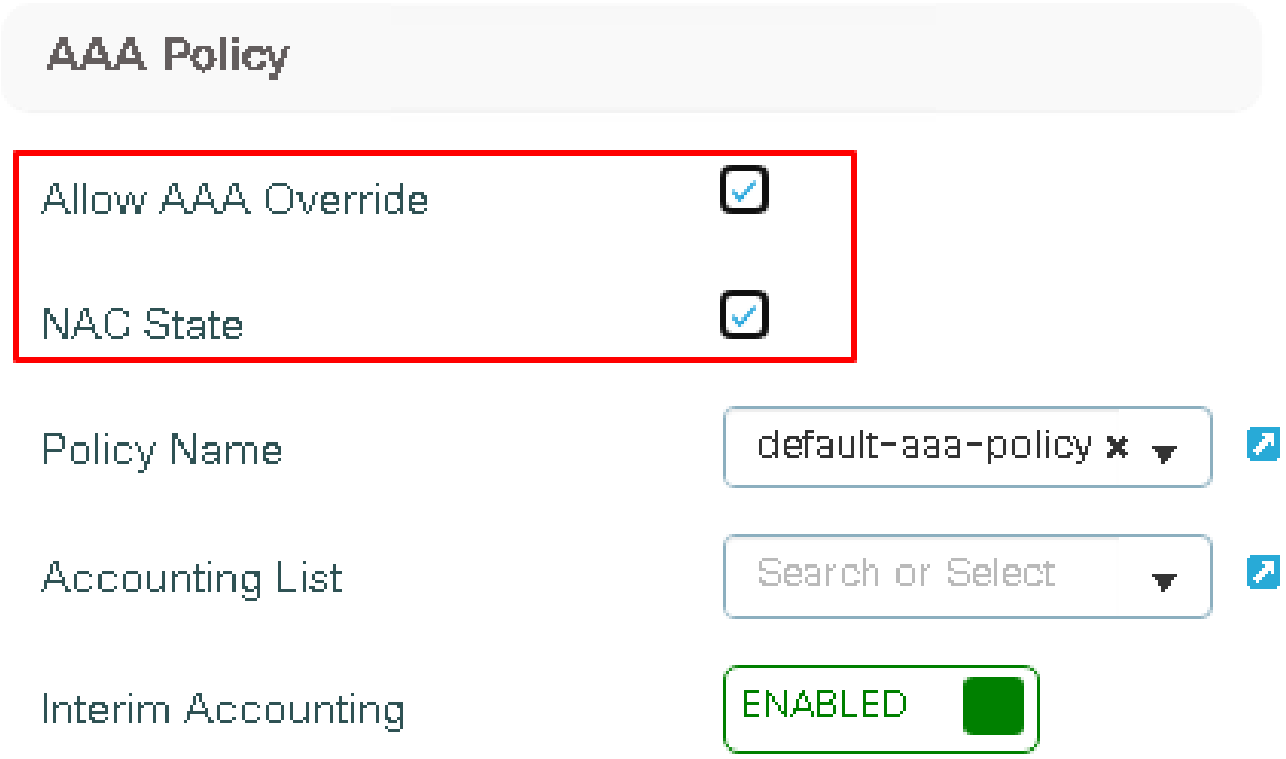
Configurazione profilo criteri wireless

All'interno del Profilo criterio, è possibile assegnare ai client impostazioni quali VLAN, ACL, QoS, Ancoraggio di mobilità e timer. Per visualizzare la configurazione per il profilo dei criteri, passare a Configurazione > Tag e profili > Criteri.

Fare clic sul nome del criterio per visualizzarne la configurazione.



Lo stato del criterio è Abilitato e, come per qualsiasi SSID dell'infrastruttura, la commutazione centrale e il DHCP centrale sono disabilitati. Fare clic sulla scheda Avanzate, quindi passare alla sezione Criteri AAA per visualizzare ulteriori dettagli di configurazione.



È possibile abilitare sia l'override AAA che il controllo dell'accesso alla rete (NAC). L'override AAA consente al controller di accettare gli attributi restituiti dal server RADIUS, ad esempio ACL o URL, e di applicare questi attributi ai client. Il NAC abilita la modifica dell'autorizzazione (CoA) dopo la registrazione del client sul portale.
Questa configurazione può essere visualizzata anche dalla CLI sul WLC.

Per verificare il profilo del criterio, il SSID viene collegato per eseguire il comando:

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21
CWA_Cisco_profile
  CWA_Cisco  UP
```

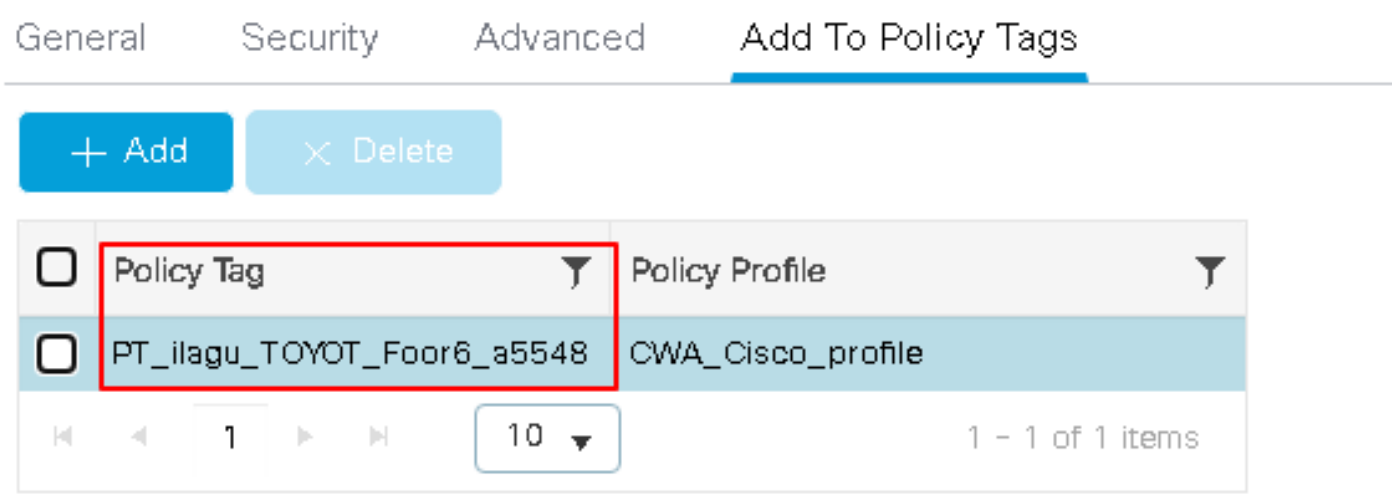
Per visualizzare la configurazione del profilo dei criteri CWA_Cisco_profile, eseguire il comando:

<#root>

```
WLC#show running-config | section policy CWA_Cisco_profile


wireless profile policy CWA_Cisco_profile
 aaa-override


 no central dhcp


 no central switching


 description CWA_Cisco_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 fabric CWA_Cisco_profile
 http-tlv-caching
 nac


 service-policy input platinum-up
 service-policy output platinum
 no shutdown
```

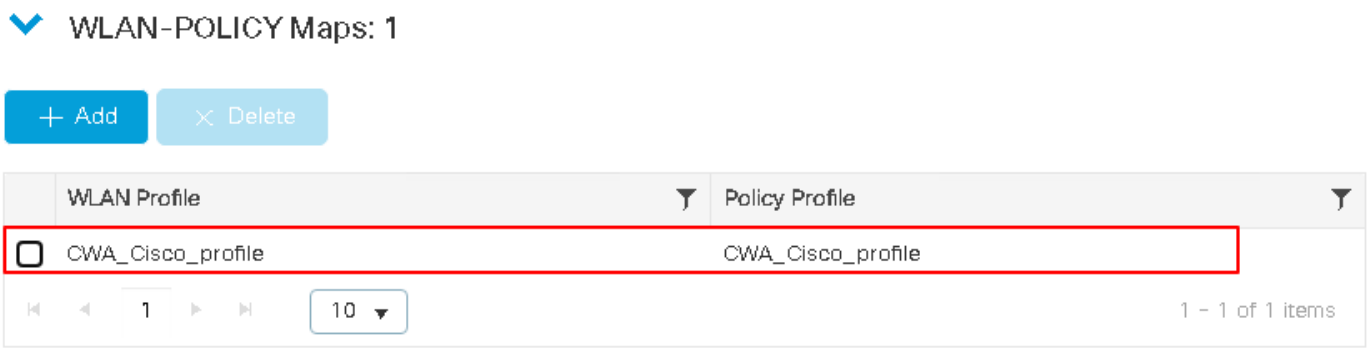
Configurazione del tag di policy

Il tag della policy è il modo in cui si collega la WLAN con il Profilo della policy, si passa a Configurazione > Tag e profili > WLAN, si fa clic sul nome della WLAN e si passa a Aggiungi ai tag della policy per identificare il tag della policy assegnato all'SSID.



Per il SSID CWA_Cisco_profile viene utilizzato il tag di criterio PT_ilagu_TOYOT_For6_a5548 per verificare questa configurazione. Selezionare Configurazione > Tag e profili > Tag > Criterio.

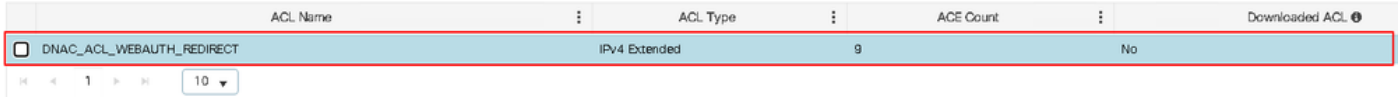
Fare clic sul nome per visualizzarne i dettagli. Il tag di policy PT_ilagu_TOYOT_For6_a5548 collega la WLAN CWA_Cisco associata al nome CWA_Cisco_profile sul WLC (per ulteriori informazioni, vedere la pagina WLAN) al profilo della policy CWA_Cisco_profile.



Il nome della WLAN CWA_Cisco_profile fa riferimento alla WLAN CWA_Cisco.

Configurazione degli ACL di reindirizzamento

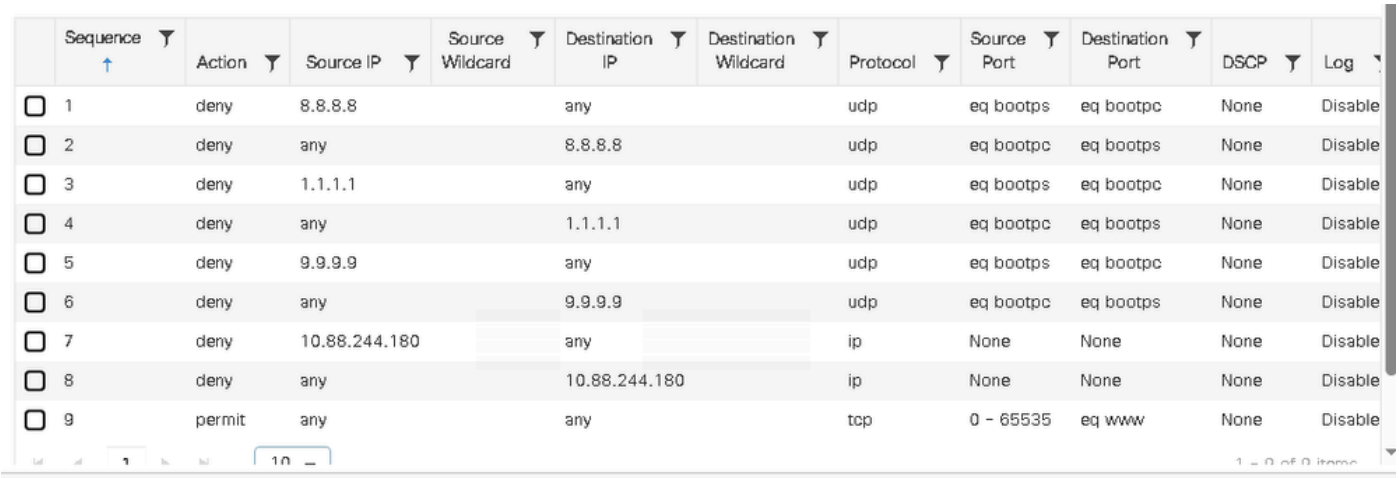
In CWA, un elenco di controllo di accesso con reindirizzamento definisce il traffico reindirizzato al WLC per un'ulteriore elaborazione e il traffico che ignora il reindirizzamento
Questa configurazione viene trasferita sul WLC dopo la creazione dell'SSID e il provisioning del WLC da Inventory. Per visualizzarlo, selezionare Configuration > Security >ACL, il nome dell'ACL usato da Catalyst Center per il reindirizzamento dell'ACL è Cisco DNA_ACL_WEBAUTH_REDIRECT.



ACL Name	ACL Type	ACE Count	Downloaded ACL
DNAC_ACL_WEBAUTH_REDIRECT	IPv4 Extended	9	No

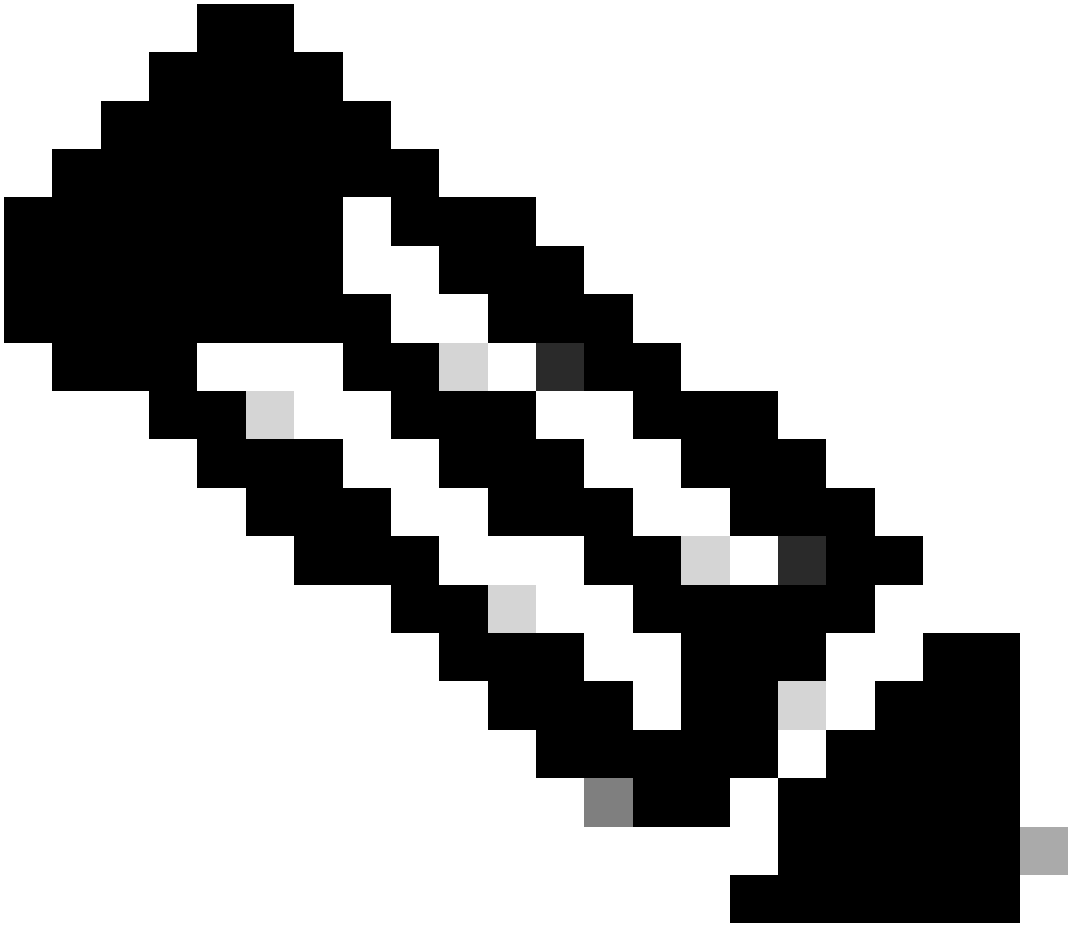
1 10

Fare clic sul nome per visualizzarne la configurazione. I valori derivano dalle impostazioni di rete del sito in Catalyst Center.



Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
1	deny	8.8.8.8		any		udp	eq bootps	eq bootpc	None	Disable
2	deny	any		8.8.8.8		udp	eq bootpc	eq bootps	None	Disable
3	deny	1.1.1.1		any		udp	eq bootps	eq bootpc	None	Disable
4	deny	any		1.1.1.1		udp	eq bootpc	eq bootps	None	Disable
5	deny	9.9.9.9		any		udp	eq bootps	eq bootpc	None	Disable
6	deny	any		9.9.9.9		udp	eq bootpc	eq bootps	None	Disable
7	deny	10.88.244.180		any		ip	None	None	None	Disable
8	deny	any		10.88.244.180		ip	None	None	None	Disable
9	permit	any		any		tcp	0 - 65535	eq www	None	Disable

1 10



Nota: Questi valori vengono ricavati dalle impostazioni di rete del sito configurate in Catalyst Center, mentre i valori DHCP/DNS derivano dal pool configurato nella WLAN. L'indirizzo IP del PSN ISE è referenziato nella configurazione AAA all'interno del flusso di lavoro SSID.

Per visualizzare l'ACL di reindirizzamento sulla CLI del WLC, eseguire questo comando:

<#root>

```
WLC#show ip access-lists Cisco DNA_ACL_WEBAUTH_REDIRECT


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 deny udp host 8.8.8.8 eq bootps any eq bootpc
2 deny udp any eq bootpc host 8.8.8.8 eq bootps
3 deny udp host 1.1.1.1 eq bootps any eq bootpc
4 deny udp any eq bootpc host 1.1.1.1 eq bootps
5 deny udp host 9.9.9.9 eq bootps any eq bootpc
6 deny udp any eq bootpc host 9.9.9.9 eq bootps
7 deny ip host 10.88.244.180 any
8 deny ip any host 10.88.244.180
9 permit tcp any range 0 65535 any eq www
```

L'ACL di reindirizzamento può essere applicato al Flex Profile in modo da essere inviato ai punti di accesso. Eseguire questo comando per confermare la configurazione

<#root>

```
WLC#show running-config | section flex


wireless profile flex default-flex-profile

 acl-policy Cisco DNA_ACL_WEBAUTH_REDIRECT



central-webauth



urlfilter list Cisco DNA_ACL_WEBAUTH_REDIRECT
```

Reindirizzamento dell'ACL sul punto di accesso

Sul punto di accesso, i valori di permesso e rifiuto sono invertiti: allow indica l'inoltro del traffico, mentre deny indica il reindirizzamento. Per rivedere la configurazione dell'ACL di reindirizzamento sull'access point, eseguire questo comando:

<#root>

```
AP#sh ip access-lists


Extended IP access list Cisco DNA_ACL_WEBAUTH_REDIRECT
1 permit udp 8.8.8.8 0.0.0.0 dhcp_server any eq 68
2 permit udp any dhcp_client 8.8.8.8 0.0.0.0 eq 67
3 permit udp 1.1.1.1 0.0.0.0 dhcp_server any eq 68
4 permit udp any dhcp_client 1.1.1.1 0.0.0.0 eq 67
5 permit udp 9.9.9.9 0.0.0.0 dhcp_server any eq 68
6 permit udp any dhcp_client 9.9.9.9 0.0.0.0 eq 67
7 permit ip 10.88.244.180 0.0.0.0 any
8 permit ip any 10.88.244.180 0.0.0.0
9 deny tcp any range 0 65535 any eq 80
```

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).