Configurer l'authentification Web centrale sur SD-Access

Table des matières

Introduction

Ce document décrit un guide étape par étape pour configurer l'authentification Web centrale (CWA) et décrit les procédures de vérification à travers tous les composants.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Architecture du contrôleur sans fil Catalyst 9800
- Authentification, autorisation et comptabilité (AAA)

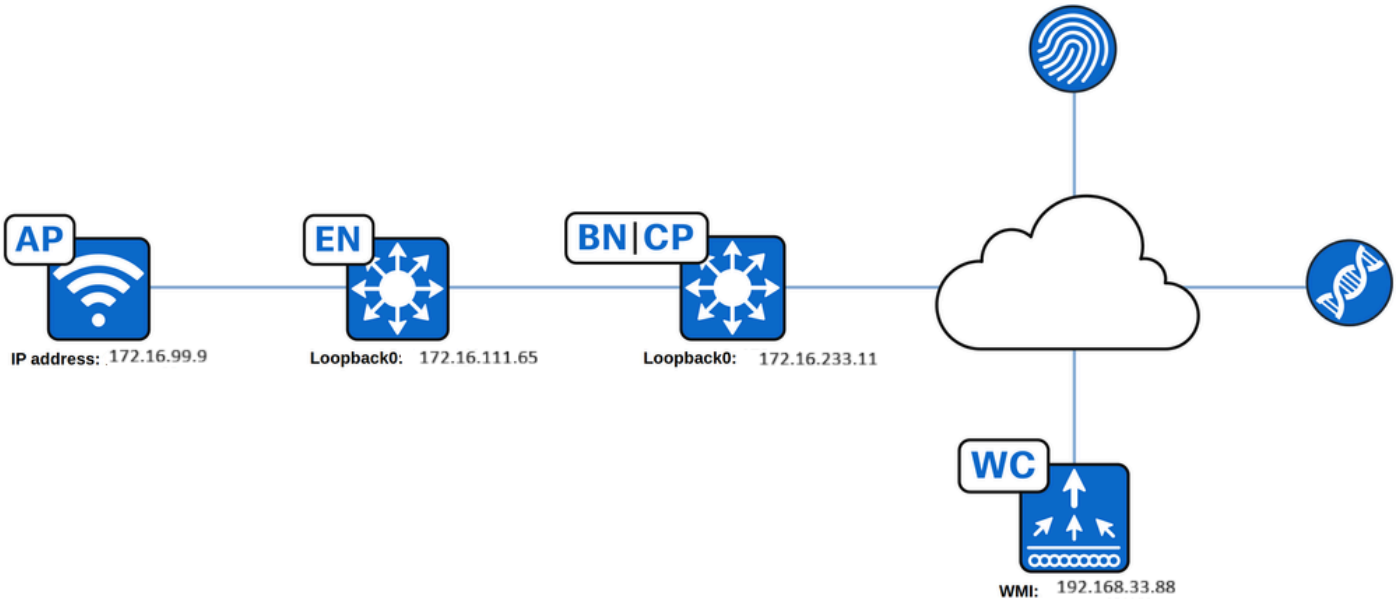
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur LAN sans fil Cisco (WLC) - C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center - Version 2.3.7.7
- Cisco Identity Services Engine (ISE) - Version 3.0.0.458
- Noeud de périphérie SDA - C9300-48P, Cisco IOS® XE 17.12.05
- Plan de contrôle/noeud de périphérie SDA - C9500-48P, Cisco IOS® XE17.12.05
- Point d'accès Cisco - C9130AXI-A, version 17.9.5.47

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie



Aperçu

L'authentification Web centrale (CWA) utilise un SSID de type invité pour rediriger le navigateur Web de l'utilisateur vers un portail captif hébergé par Cisco ISE, à l'aide d'une liste de contrôle d'accès de redirection configurée. Le portail captif permet à l'utilisateur de s'enregistrer et de s'authentifier, et après une authentification réussie, le contrôleur de réseau local sans fil (WLC) applique l'autorisation appropriée pour accorder un accès réseau complet. Ce guide fournit des instructions détaillées sur la configuration de CWA à l'aide de Cisco Catalyst Center.

Configurer CWA sur Cisco Catalyst Center

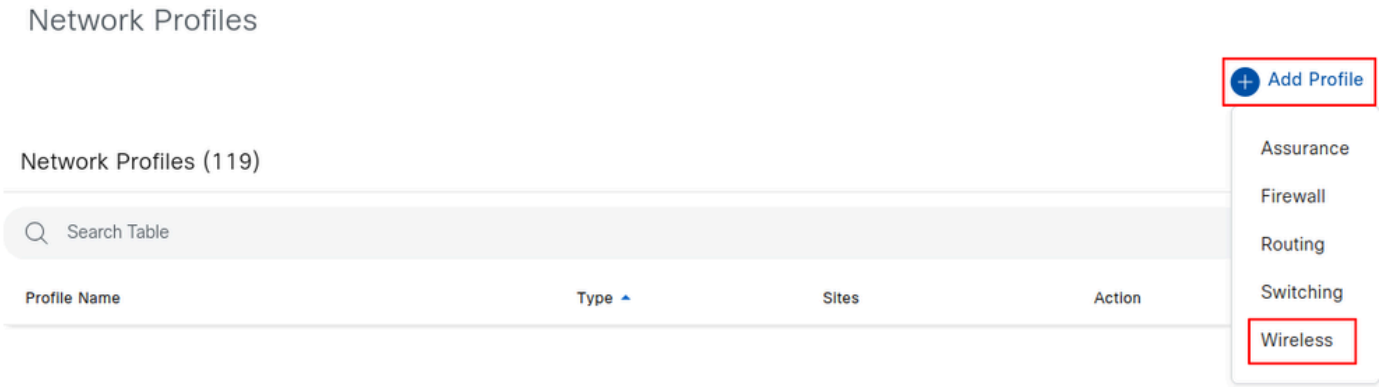
Créer le profil réseau

Un profil réseau permet de configurer des paramètres pouvant être appliqués à un site spécifique. Vous pouvez créer des profils réseau pour divers éléments de Cisco Catalyst Center, notamment :

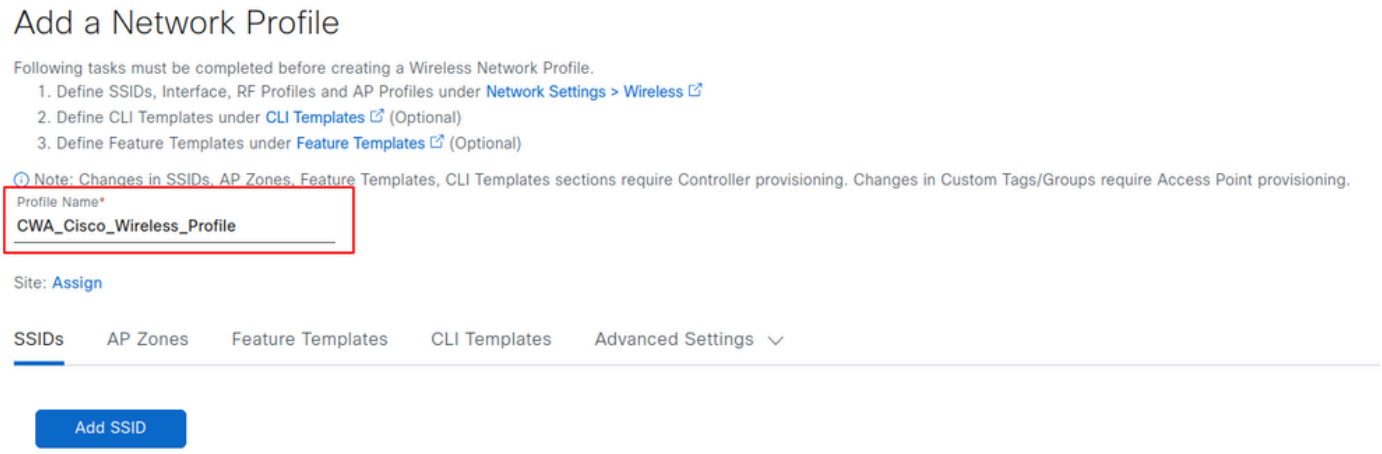
- Assurance
- Pare-Feu
- Routage
- Commutation
- Appareil De Télémétrie
- Sans fil

Pour CWA, un profil sans fil doit être configuré.

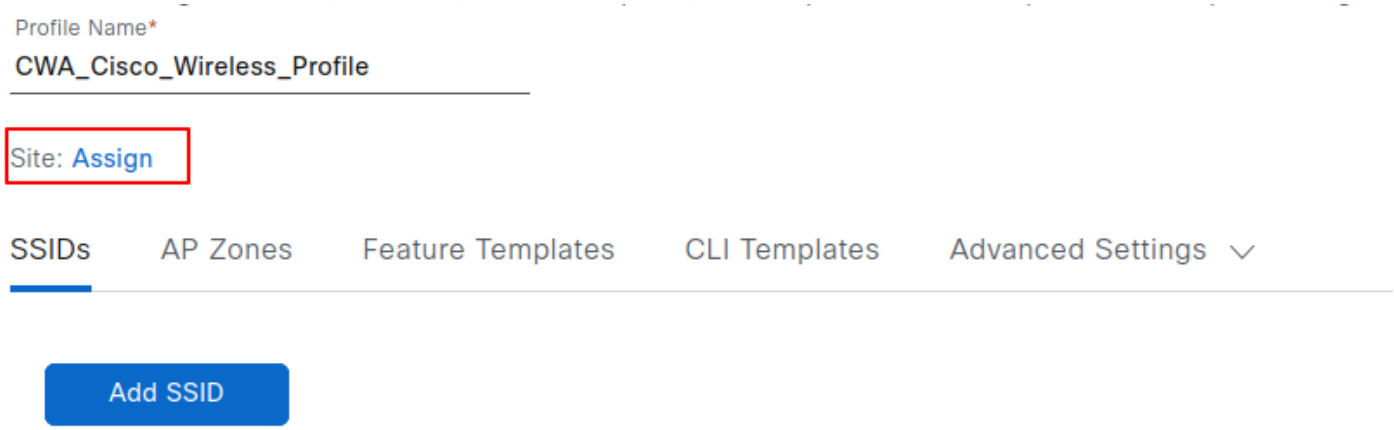
Pour configurer un profil sans fil, accédez à Design > Network Profiles, cliquez sur Add Profile et sélectionnez Wireless.



Nommez le profil comme requis. Dans cet exemple, le profil sans fil est nommé CWA_Cisco_Wireless_Profile. Vous pouvez ajouter des SSID existants à ce profil en sélectionnant Add SSID. La création du SSID est traitée dans la section suivante.

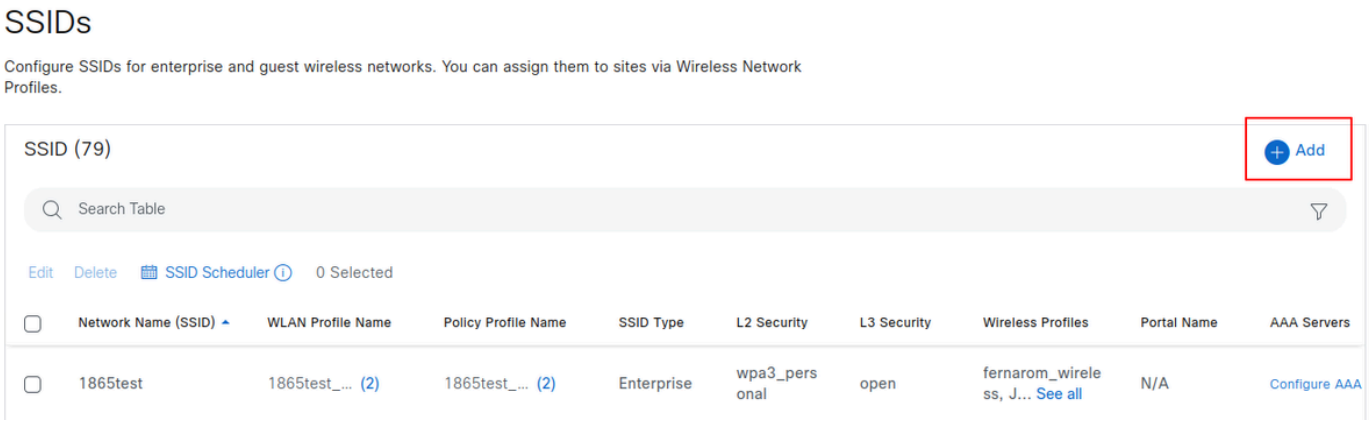


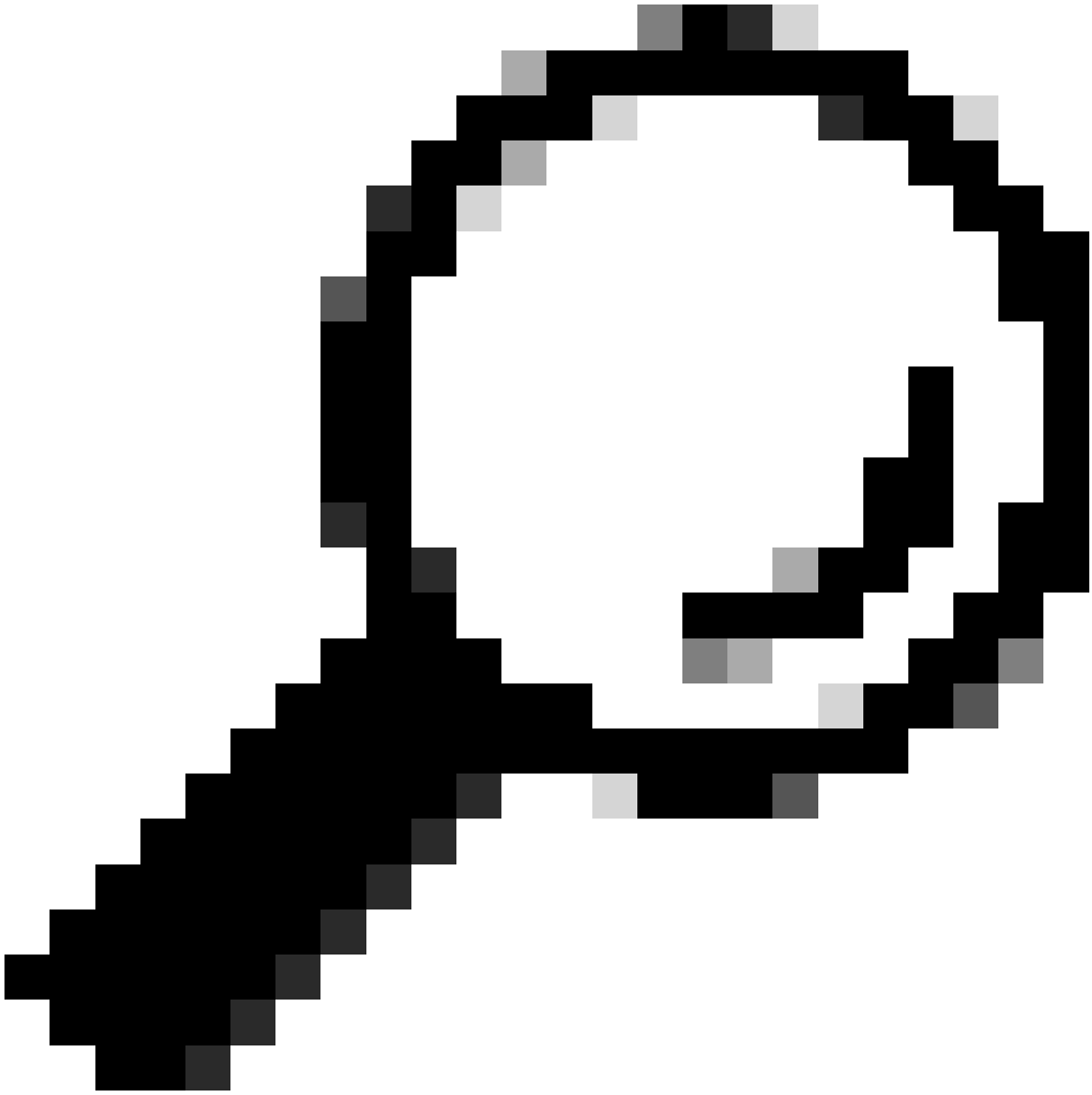
Sélectionnez Affecter pour choisir le site où ce profil doit être appliqué, puis sélectionnez le site souhaité. Après avoir sélectionné les sites, cliquez sur Enregistrer.



Création du SSID

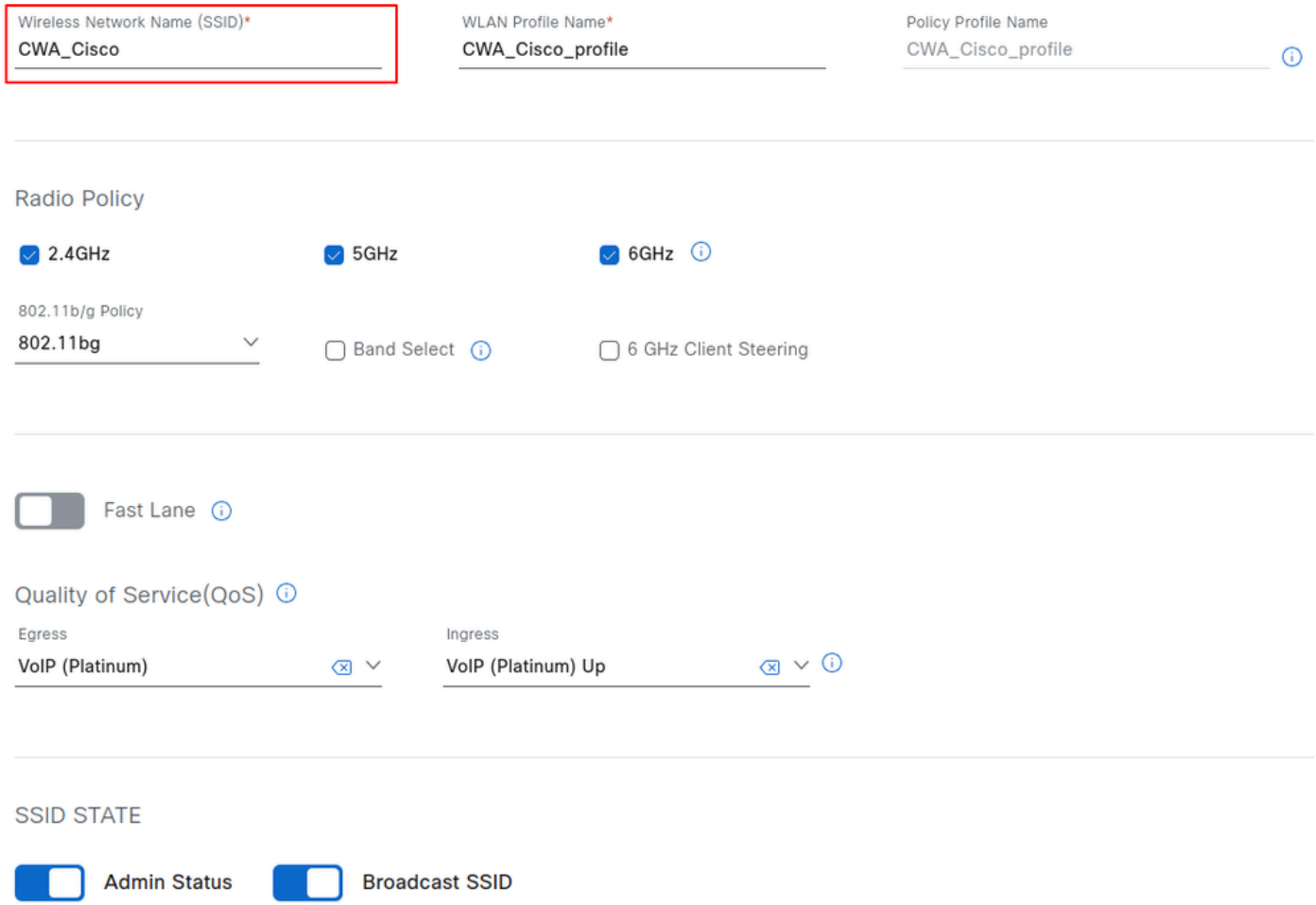
Accédez à Design > Network Settings > Wireless > SSIDs et cliquez sur Add.



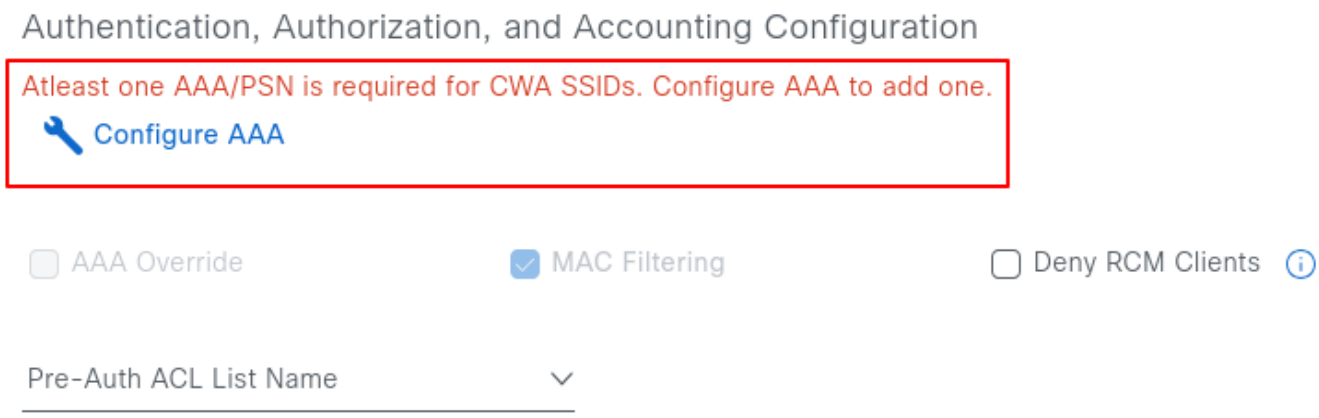


Conseil : Lors de la création d'un SSID pour CWA, il est essentiel de sélectionner le type Guest. Cette sélection ajoute une commande au profil de stratégie sans fil du SSID sur le WLC - la commande nac - qui permet à CoA d'être utilisé pour la réauthentification après que l'utilisateur s'est inscrit sur le portail captif. Sans cette configuration, les utilisateurs peuvent faire l'expérience d'une boucle sans fin d'enregistrement et d'être redirigés vers le portail à plusieurs reprises.

Après avoir sélectionné Add, poursuivez par le workflow de configuration SSID. Sur la première page, configurez le nom SSID, vous pouvez également sélectionner la bande de stratégie radio, et définir l'état SSID, y compris l'état administratif et les paramètres de diffusion. Pour ce guide de configuration, le SSID est nommé CWA_Cisco.



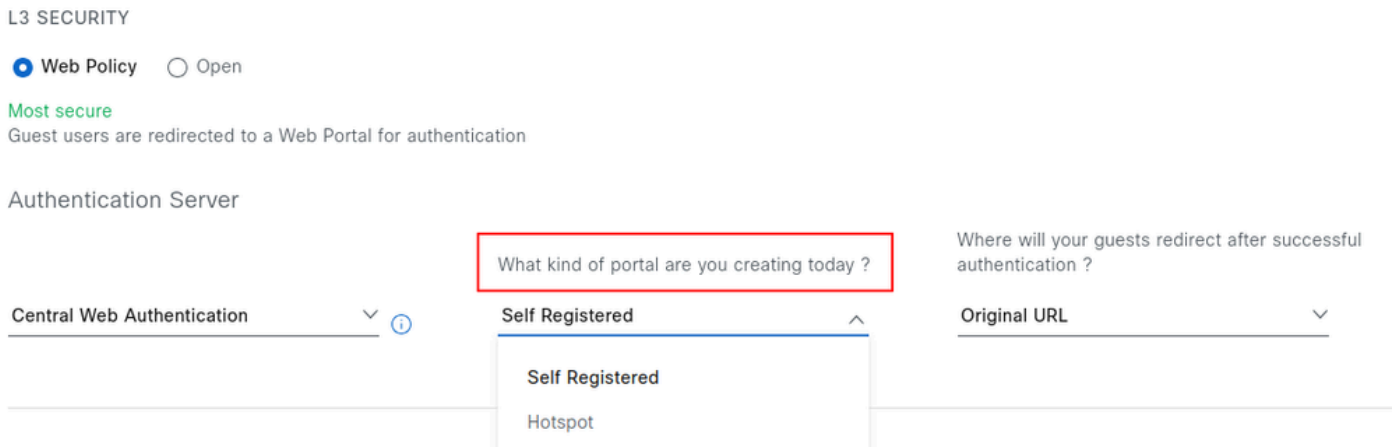
Après avoir saisi le nom SSID, le nom du profil WLAN et le nom du profil de stratégie sont automatiquement générés. Sélectionnez Next pour continuer.
Au moins un AAA/PSN doit être configuré pour les SSID CWA. Si aucun n'est configuré, sélectionnez Configure AAA et choisissez l'adresse IP PSN dans la liste déroulante.



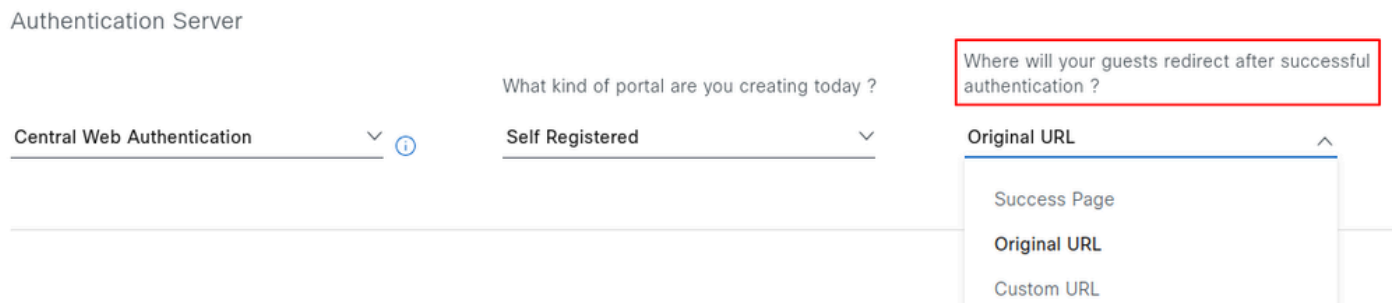
Après avoir sélectionné le serveur AAA, définissez les paramètres de sécurité de couche 3 et sélectionnez le type de portail : Auto-enregistré ou Hotspot.

Portails invités Hotspot : Un portail invité de point d'accès sans fil fournit un accès réseau aux invités sans avoir besoin de noms d'utilisateur et de mots de passe. Ici, les utilisateurs doivent accepter une politique d'utilisation acceptable (AUP) pour obtenir l'accès au réseau, menant à

l'accès Internet suivant. L'accès via un portail d'invité accrédité nécessite que les invités aient un nom d'utilisateur et un mot de passe.



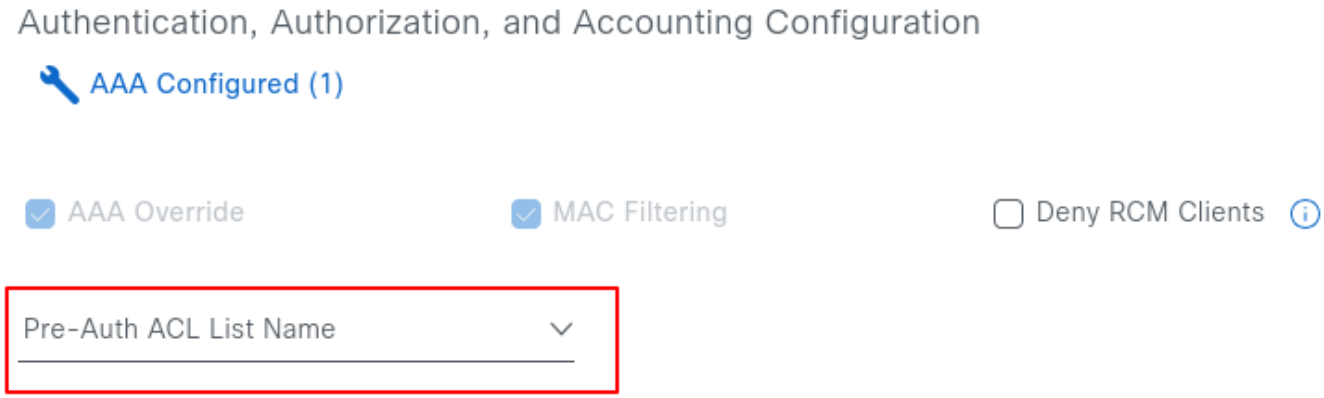
L'action qui se produit après l'enregistrement ou l'acceptation de la stratégie d'utilisation par l'utilisateur peut également être configurée. Trois options sont disponibles : Page de réussite, URL d'origine et URL personnalisée.



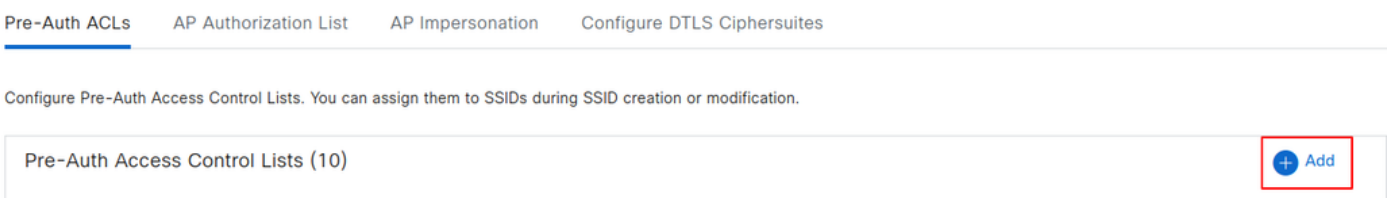
Le comportement de chaque option est décrit ci-dessous :

Page Success : Redirige l'utilisateur vers une page de confirmation indiquant que l'authentification a réussi.
Original URL : redirige l'utilisateur vers l'URL d'origine demandée avant d'être intercepté par le portail captif.
Custom URL : redirige l'utilisateur vers une URL personnalisée spécifiée. La sélection de cette option active un champ supplémentaire pour définir l'URL de destination

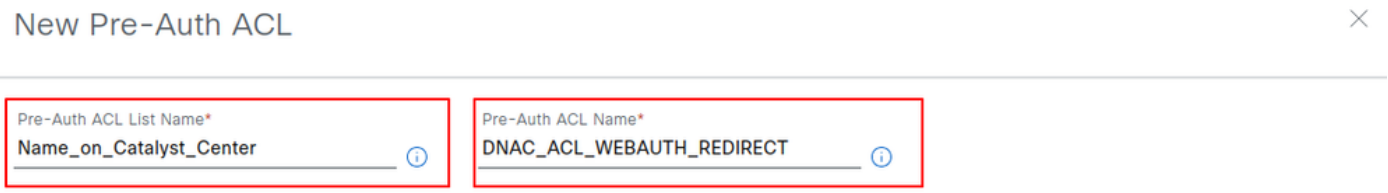
Sur la même page, sous Authentication, Authorization, and Accounting Configuration, une liste de contrôle d'accès de pré-auth peut également être configurée. Cette liste de contrôle d'accès permet d'ajouter des entrées supplémentaires pour les protocoles au-delà des adresses IP DHCP, DNS ou PSN, qui sont obtenues à partir des paramètres réseau et ajoutées à la liste de contrôle d'accès de redirection pendant l'approvisionnement. Cette fonctionnalité est disponible dans Cisco Catalyst Center version 2.3.3.x et ultérieures.



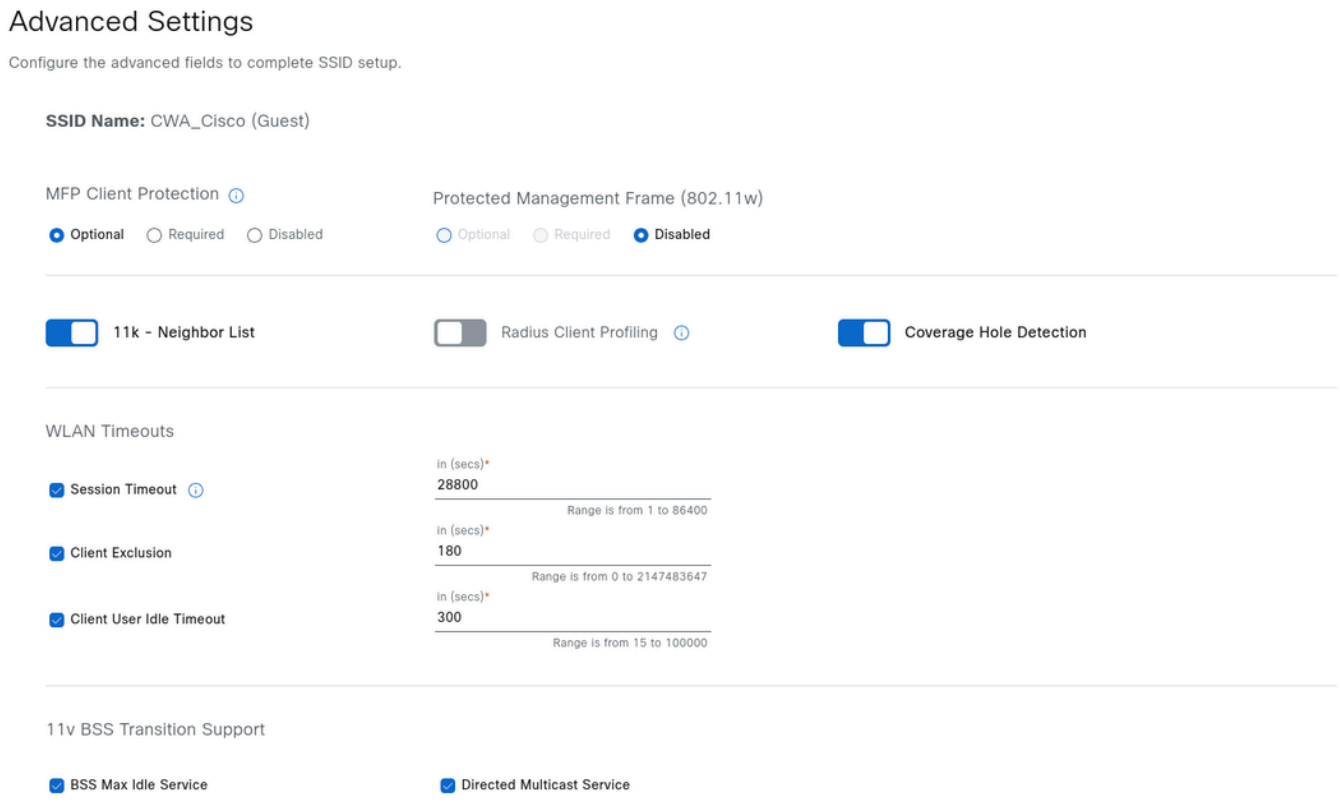
Pour configurer une liste de contrôle d'accès de pré-authentification, accédez à Design > Network Settings > Wireless > Security Settings, puis cliquez sur Add.



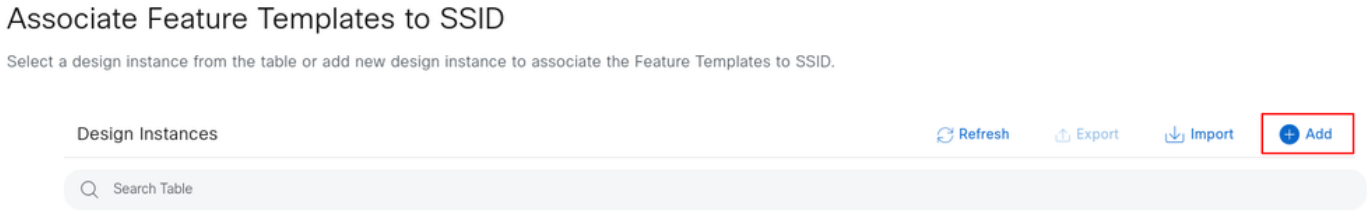
Le premier nom identifie la liste de contrôle d'accès dans Catalyst Center, tandis que le second nom correspond au nom de la liste de contrôle d'accès sur le WLC. Le deuxième nom peut correspondre à la liste de contrôle d'accès de redirection existante configurée sur le WLC. À titre de référence, Catalyst Center attribue le nom Cisco DNA_ACL_WEBAUTH_REDIRECT au WLC. Les entrées de la liste de contrôle d'accès de pré-authentification sont ajoutées après les entrées existantes.



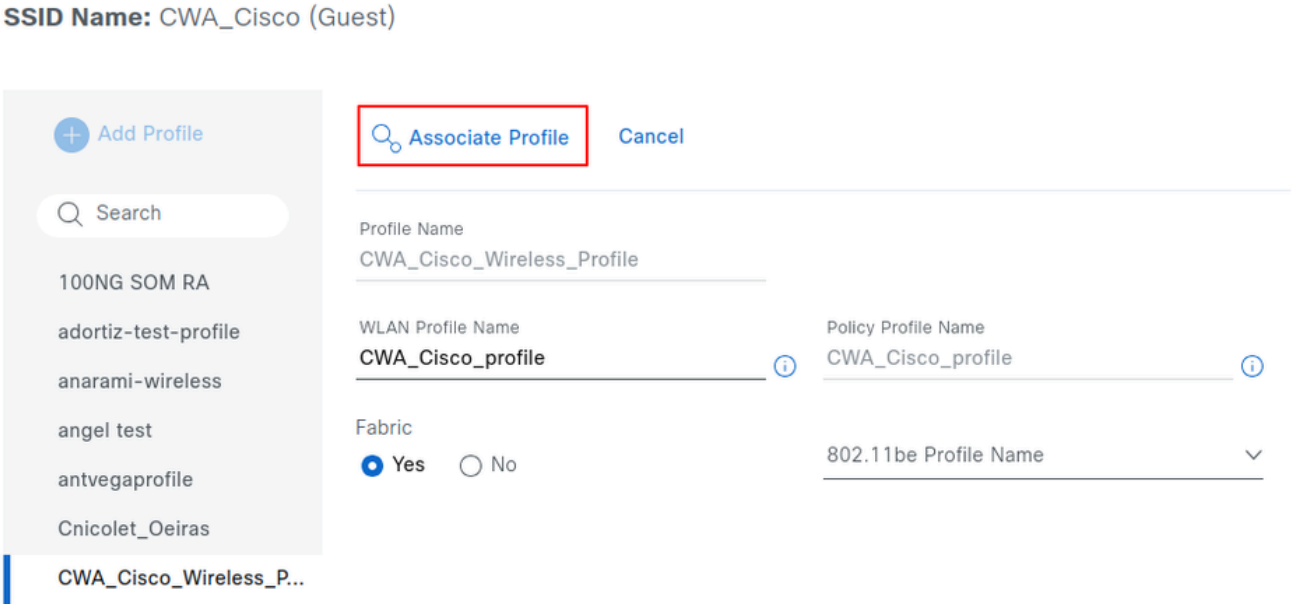
En revenant au workflow de création de SSID, la sélection de Next affiche les paramètres avancés, y compris la transition rapide, le délai d'expiration de la session, le délai d'expiration de l'utilisateur client et la limitation du débit. Ajustez les paramètres selon les besoins, puis sélectionnez Next pour continuer. Pour les besoins de ce guide de configuration, l'exemple conserve les paramètres par défaut.



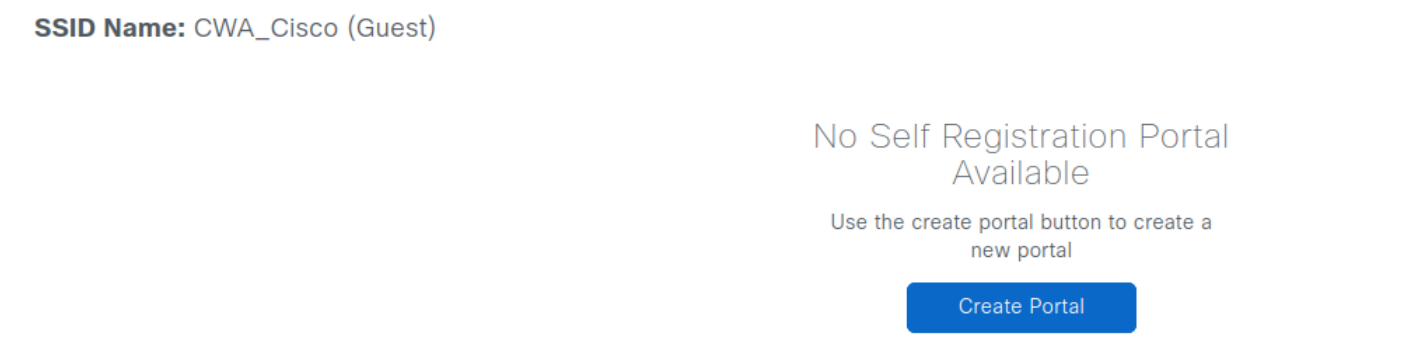
Après avoir sélectionné Next, une invite apparaît pour associer les modèles de fonction au SSID. Le cas échéant, sélectionnez les modèles souhaités en cliquant sur Ajouter, et lorsque vous avez terminé, cliquez sur Suivant.



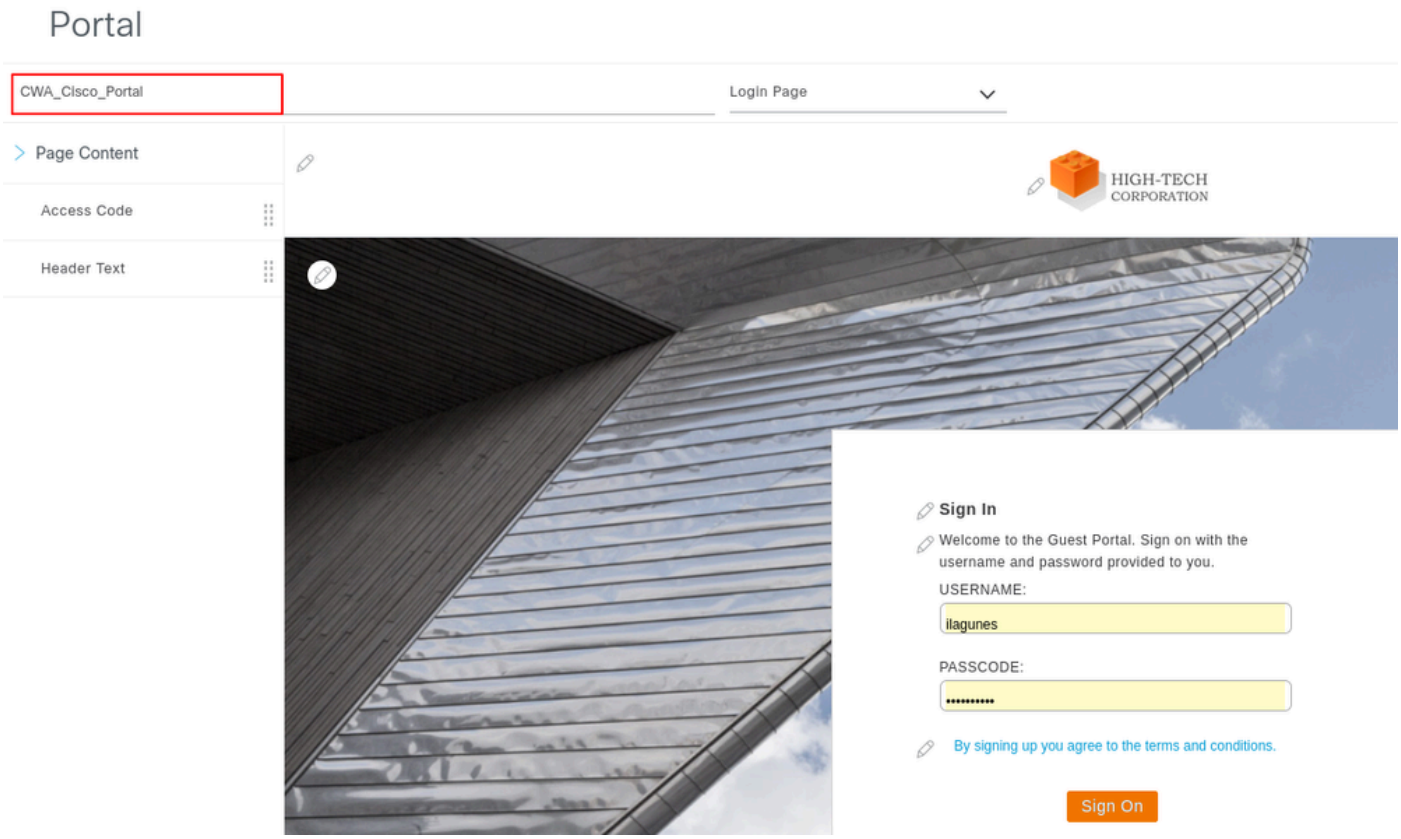
Associez le SSID au profil sans fil précédemment créé. Pour référence, consultez la section Créer le profil de réseau sans fil. Dans cette section, vous pouvez également sélectionner si le SSID est activé ou non par le fabric. Une fois que vous avez terminé, cliquez sur Associer le profil.



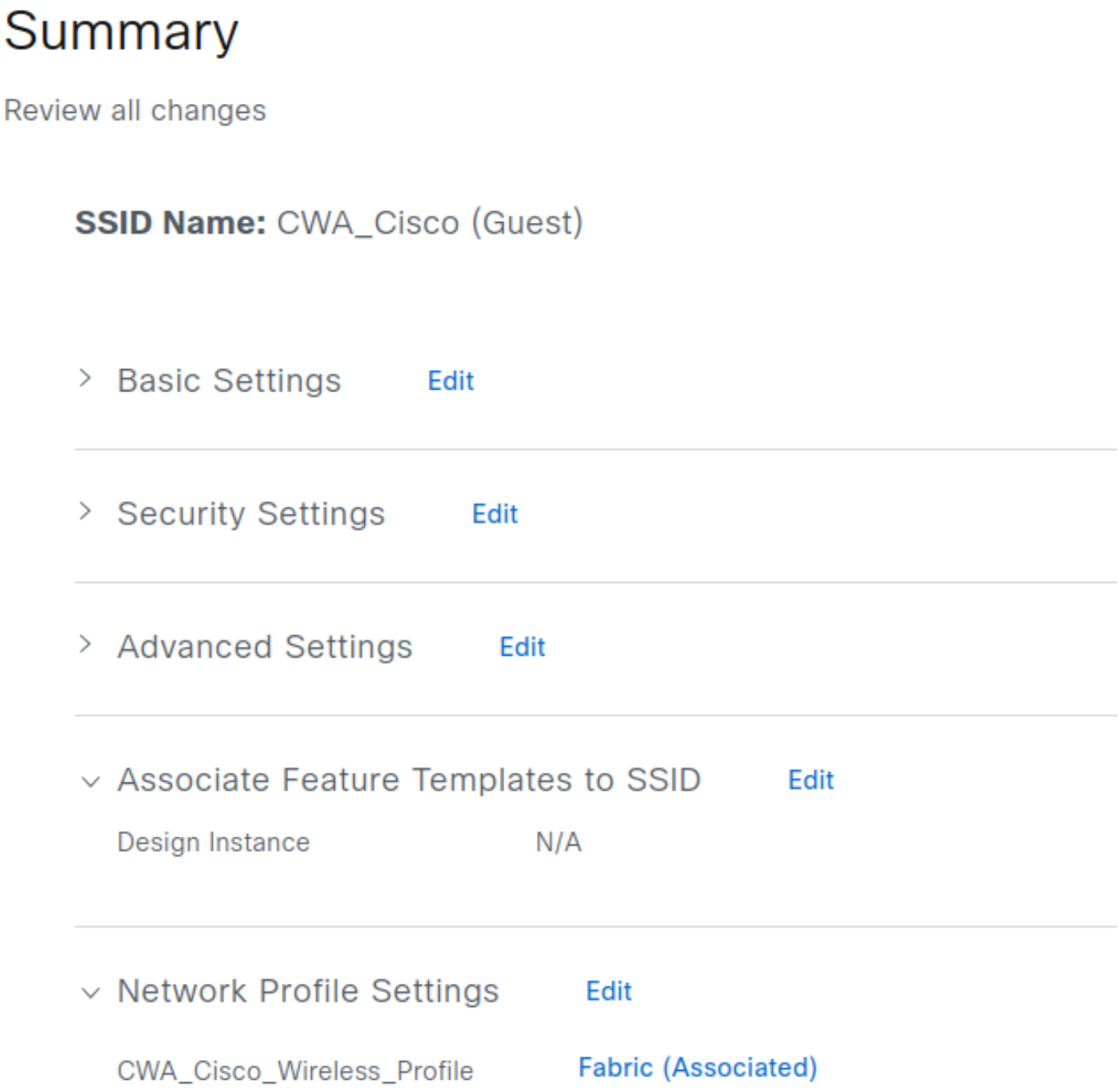
show wireless management trustpoint
Une fois que le profil est associé au SSID, cliquez sur Next pour créer et concevoir le portail captif, pour commencer, cliquez sur Create Portal.



Le nom du portail définit le nom de domaine dans le nom de domaine complet et le nom du jeu de stratégies sur ISE. Cliquez sur Save lorsque vous avez terminé. Le portail reste modifiable et peut être supprimé si nécessaire.



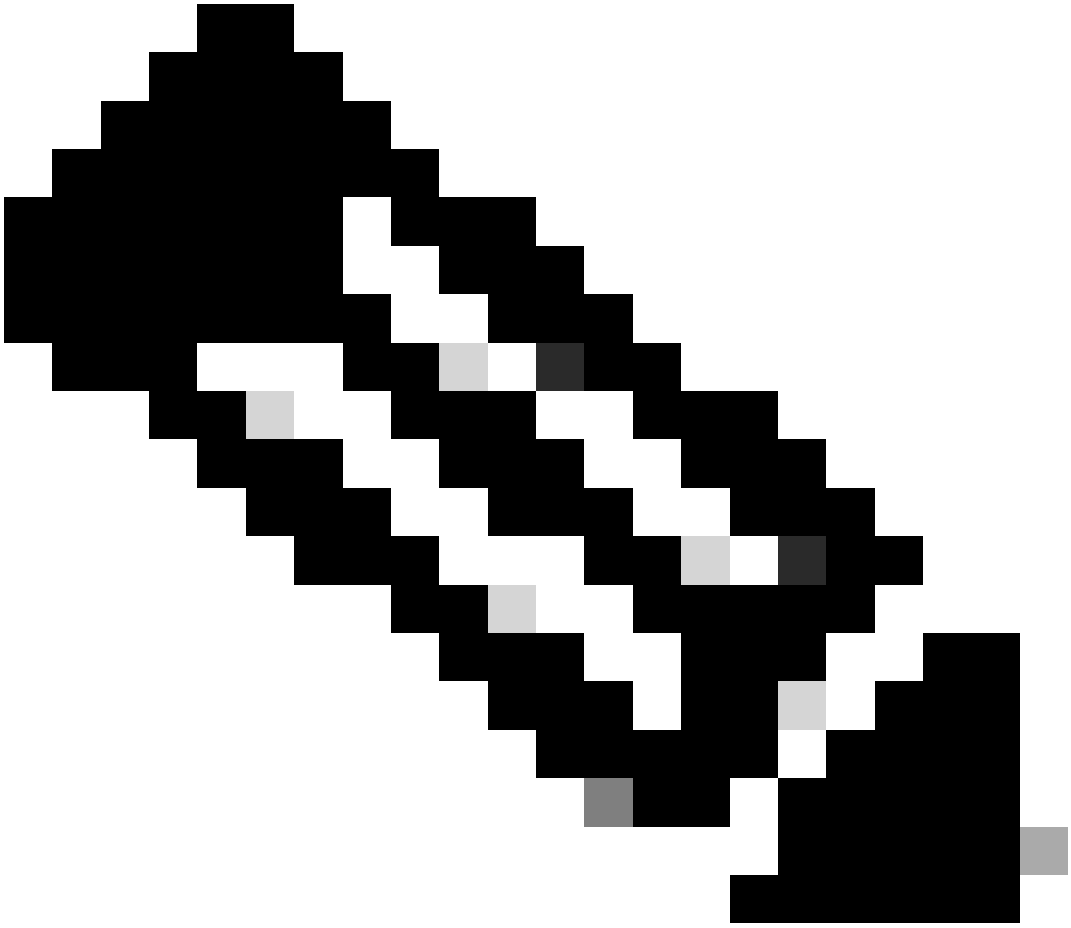
Sélectionnez Next pour afficher un récapitulatif de tous les paramètres de configuration définis lors des étapes précédentes.



Confirmez les détails de la configuration, puis sélectionnez Enregistrer pour appliquer les modifications.

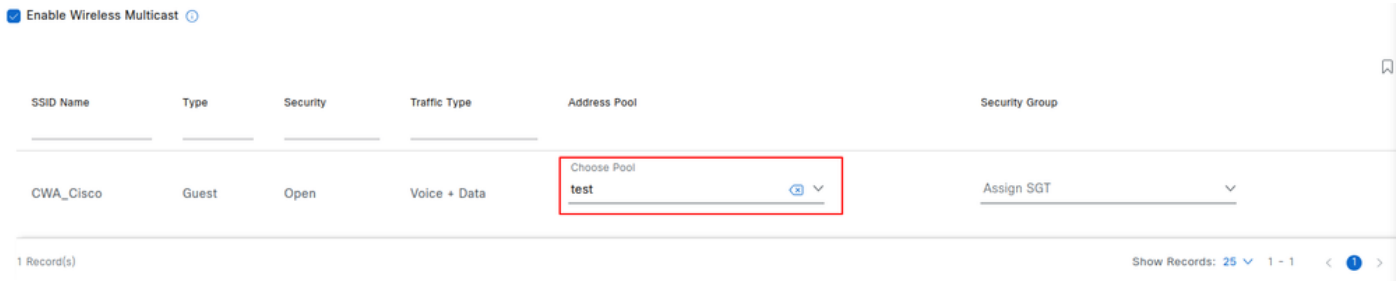
Provisionnement de fabric

Après avoir associé le profil de réseau sans fil au site de fabric, le SSID apparaît sous Provisionnement > Fabric Sites > (Your site) > Wireless SSIDs.

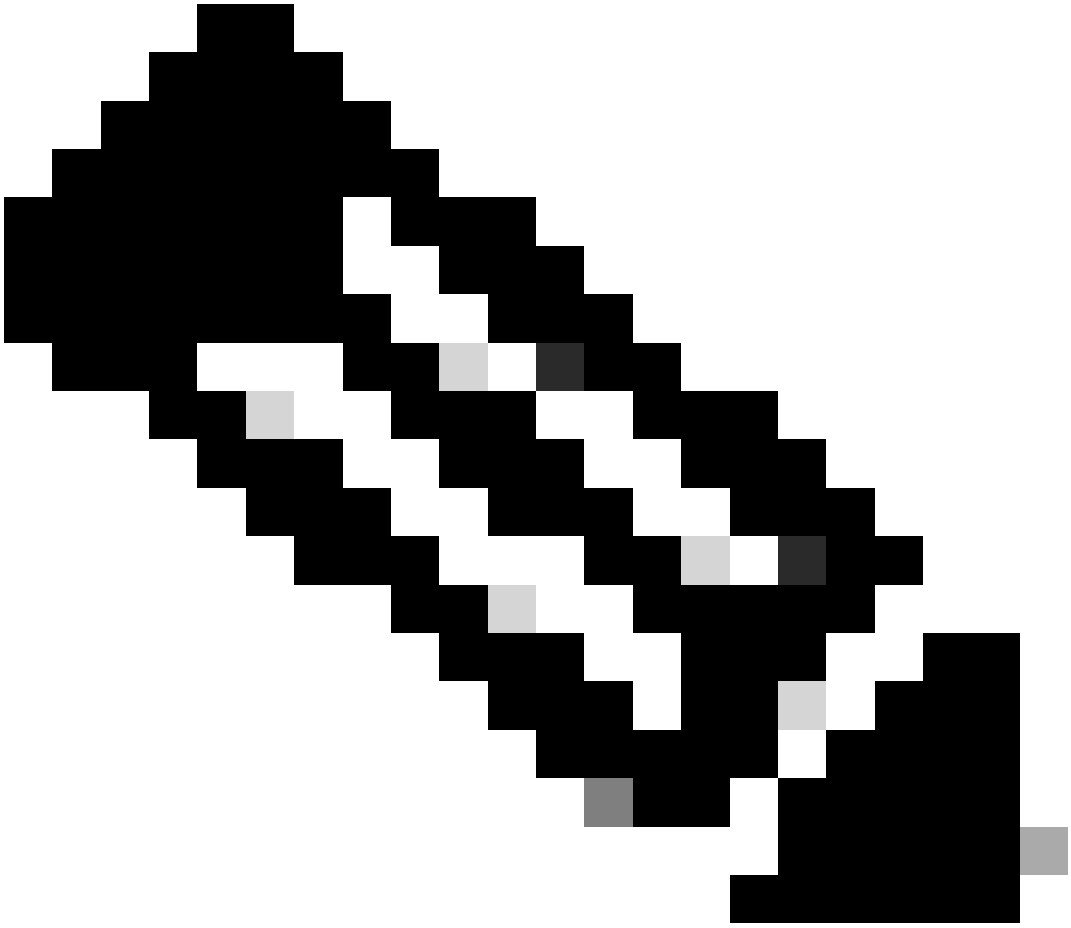


Remarque : Vous devez mettre en service le contrôleur LAN sans fil du site pour que les SSID s'affichent sous Wireless SSID

Choisissez le pool SSID, associez éventuellement une balise de groupe de sécurité, et cliquez sur Déployer. Le SSID est diffusé par les points d'accès uniquement si un pool est attribué.



Sur les contrôleurs AireOS et Catalyst 9800, remettez en service le contrôleur LAN sans fil après toute modification de la configuration SSID dans les paramètres réseau.



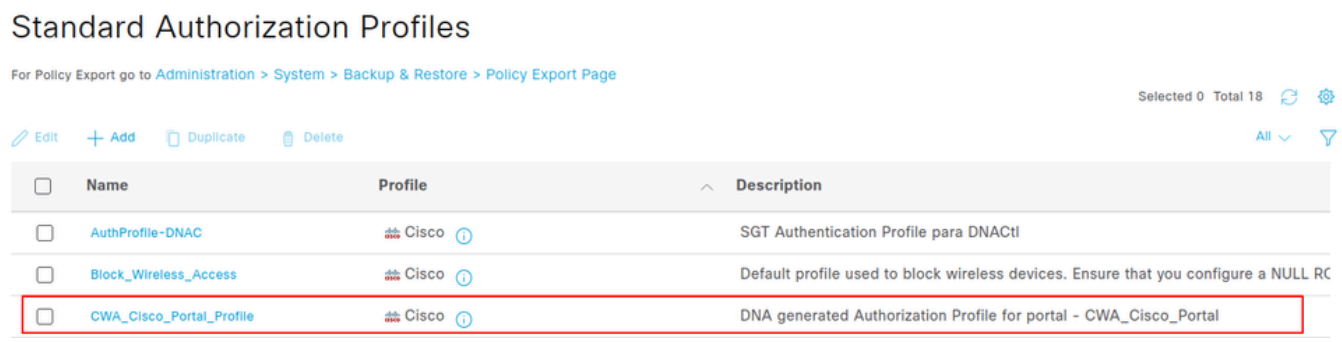
Remarque : Si aucun pool n'est attribué au SSID, il est attendu que les AP ne le diffusent pas. Le SSID est diffusé uniquement après l'attribution d'un pool. Une fois le pool attribué, le contrôleur n'a pas besoin d'être réapprovisionné.

Examiner la configuration fournie à Cisco ISE

Cette section examine la configuration fournie par Catalyst Center à Cisco ISE.

Profil d'autorisation

Un profil d'autorisation fait partie de la configuration que Catalyst Center fournit sur Cisco ISE. Ce profil définit le résultat affecté à un client en fonction de ses paramètres et peut inclure des paramètres spécifiques tels que l'affectation de VLAN, les ACL ou les redirections d'URL.
Pour afficher le profil d'autorisation dans ISE, accédez à Policy > Policy Elements > Results. Si le nom du portail est CWA_Cisco_Portal, le nom du profil est CWA_Cisco_Portal_Profile. Le champ de description affiche le texte : Profil d'autorisation généré par DNA pour le portail - CWA_Cisco_Portal.



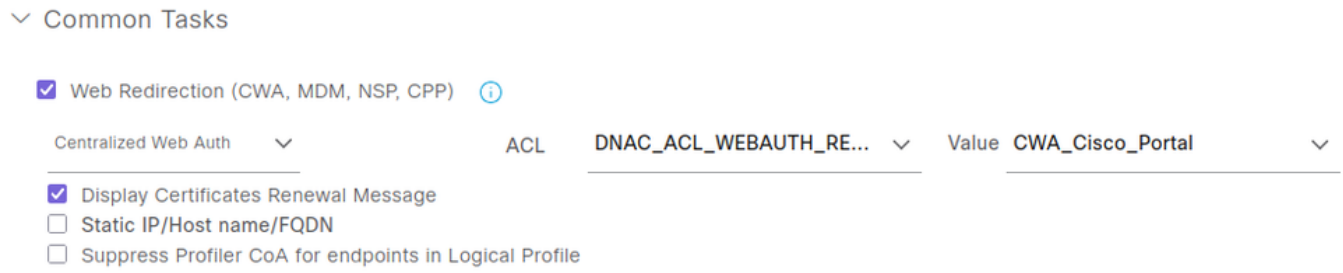
Pour afficher les attributs envoyés au contrôleur de réseau local sans fil par ce profil d'autorisation, cliquez sur le nom du profil d'autorisation et reportez-vous à la section Tâches courantes.
Ce profil d'autorisation fournit la liste de contrôle d'accès Redirect et l'URL Redirect.

L'attribut Redirection Web comprend deux paramètres :

1. ACL Name : défini sur Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Valeur : fait référence au nom du portail captif, dans cet exemple CWA_Cisco_Portal.

L'option Afficher le message de renouvellement des certificats permet d'utiliser le portail pour renouveler les certificats actuellement utilisés par le point de terminaison.

Une option supplémentaire, Static IP/Host Name/FQDN, est disponible sous Display Certificates Renewal Message. Cette fonctionnalité permet de fournir l'adresse IP du portail au lieu de son nom de domaine complet (FQDN), ce qui est utile lorsque le portail captif ne se charge pas en raison de l'impossibilité d'accéder au serveur DNS.

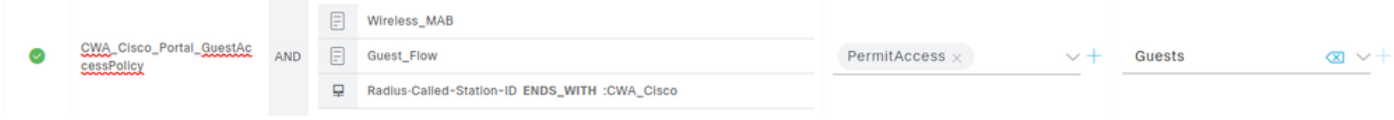


Ensembles de stratégies

Accédez à Policy > Policy Sets > Default > Authorization Policy pour afficher les deux ensembles de stratégies créés pour le portail nommé CWA_Cisco_Portal. Ces ensembles de stratégies sont les suivants :

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

La stratégie CWA_Cisco_Portal_GuestAccessPolicy est appliquée lorsque le client a déjà terminé le processus d'authentification Web, soit par l'auto-inscription, soit par le biais du portail de point d'accès sans fil.

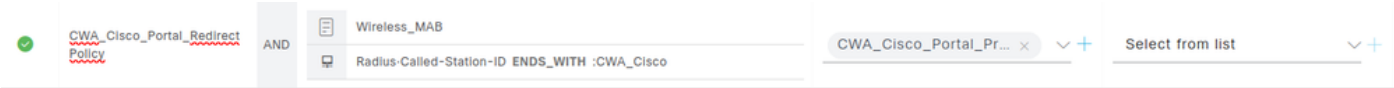


Cet ensemble de stratégies correspond à trois critères :

- Wireless_MAB : utilisé lorsque Cisco ISE reçoit une demande d'authentification MAC Authentication Bypass (MAB) d'un contrôleur LAN sans fil.
- Guest_Flow : Fait référence à la vérification par ISE de l'adresse MAC du point d'extrémité par rapport au groupe d'identité GuestEndpoints. Si l'adresse MAC du point d'extrémité n'est pas présente dans ce groupe, la stratégie n'est pas appliquée.
- RADIUS Called-Station-ID ENDS_WITH : CWA_Cisco : Called-Station-ID est un attribut RADIUS dans ISE qui stocke l'adresse MAC du pont ou du point d'accès au format ASCII et ajoute le SSID auquel on accède, séparé par un point-virgule (:). Dans cet exemple, CWA_Cisco représente le nom SSID.

Sous les profils de colonne que vous voyez le nom PermitAccess, il s'agit d'un profil d'autorisation réservé qui ne peut pas être modifié, qui donne un accès complet au réseau et vous pouvez également attribuer un SGT sous la colonne Groupes de sécurité, qui dans ce cas est Invités.

Le profil PermitAccess est utilisé. Il s'agit d'un profil d'autorisation réservé qui ne peut pas être modifié et qui accorde un accès complet au réseau. Un SGT peut également être attribué dans la colonne Security Groups ; dans ce cas, le SGT est défini sur Invités.
La stratégie suivante à examiner est CWA_Cisco_Portal_RedirectPolicy.



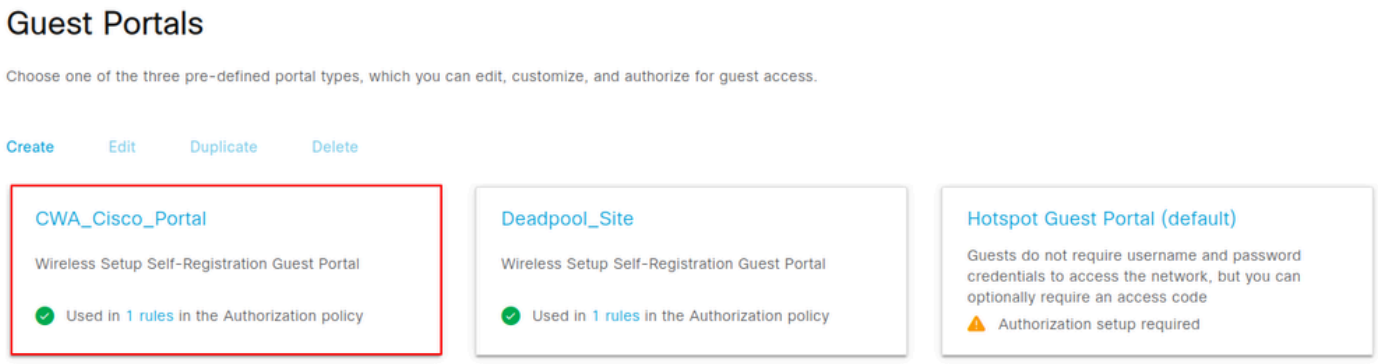
Ce jeu de stratégies correspond aux deux critères suivants :

- Wireless_MAB : utilisé lorsque Cisco ISE reçoit une demande d'authentification MAB d'un contrôleur LAN sans fil.
- RADIUS Called-Station-ID ENDS_WITH : CWA_Cisco : Called-Station-ID est un attribut RADIUS dans ISE qui stocke l'adresse MAC du pont ou du point d'accès au format ASCII et ajoute le SSID auquel on accède, séparé par un point-virgule (:). Dans cet exemple, :CWA_Cisco représente le nom SSID.

L'ordre de ces politiques est essentiel. Si CWA_Cisco_Portal_RedirectPolicy apparaît en premier dans la liste, il correspond uniquement à l'authentification MAB et au nom SSID à l'aide de l'attribut RADIUS Called-Station-ID ENDS_WITH : CWA_Training. Dans cette configuration, même si le point de terminaison a déjà été authentifié via le portail, il continuera à correspondre indéfiniment à cette stratégie. Par conséquent, l'accès complet n'est jamais accordé via le profil PermitAccess, et le client reste coincé dans une boucle continue d'authentification et de redirection vers le portail.

Configuration du portail invité

Accédez à Work Centers > Guest Access > Portals & Components pour afficher le portail. Le portail invité créé ici utilise le même nom que dans Catalyst Center CWA_Cisco_Portal. Sélectionnez le nom du portail vers si vous souhaitez afficher des détails supplémentaires.

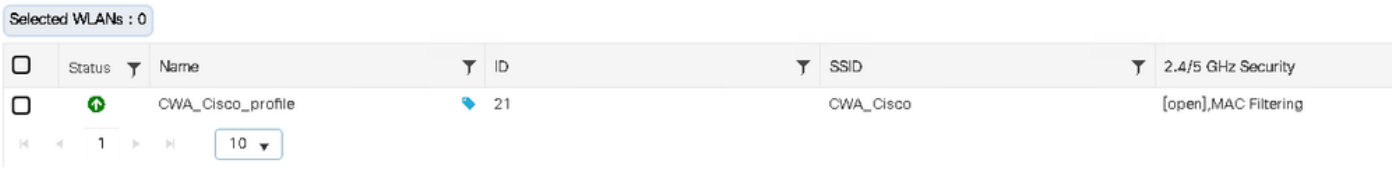


Révisez la configuration provisionnée sur le WLC

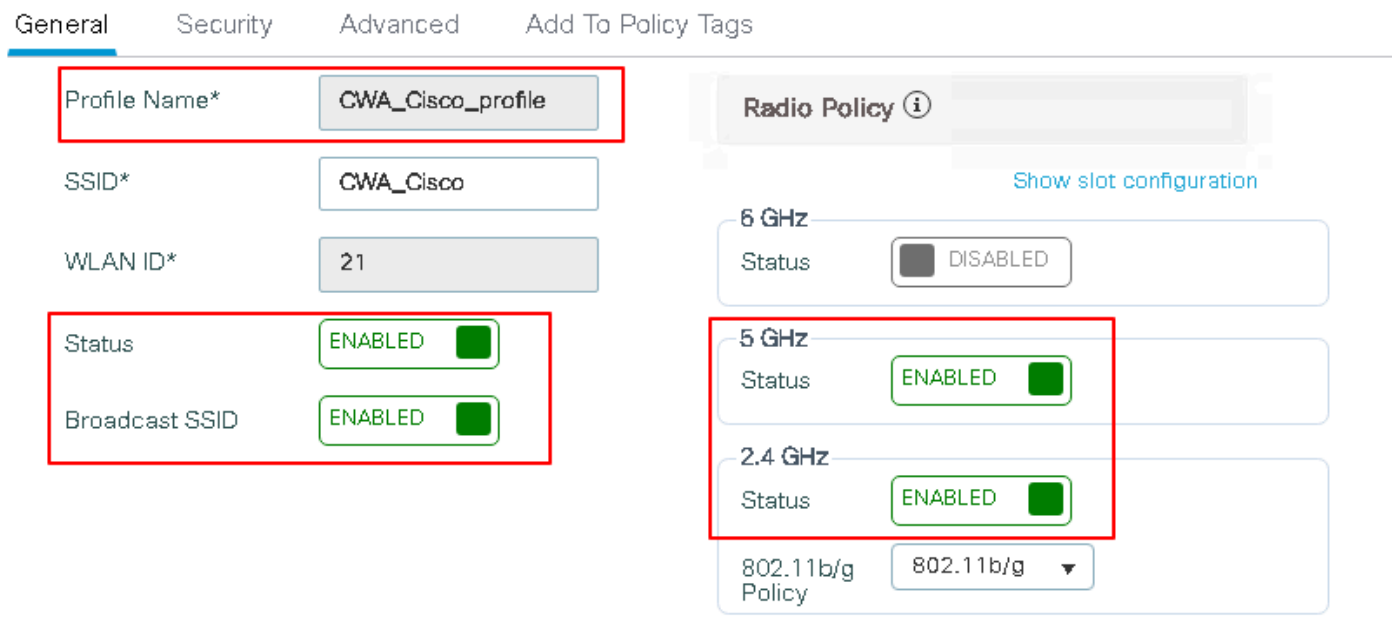
Cette section examine la configuration fournie par Catalyst Center au contrôleur LAN sans fil.

Configuration SSID

Dans l'interface graphique utilisateur du WLC, naviguez vers Configuration > Tags & Profiles > WLANs pour afficher la configuration SSID.

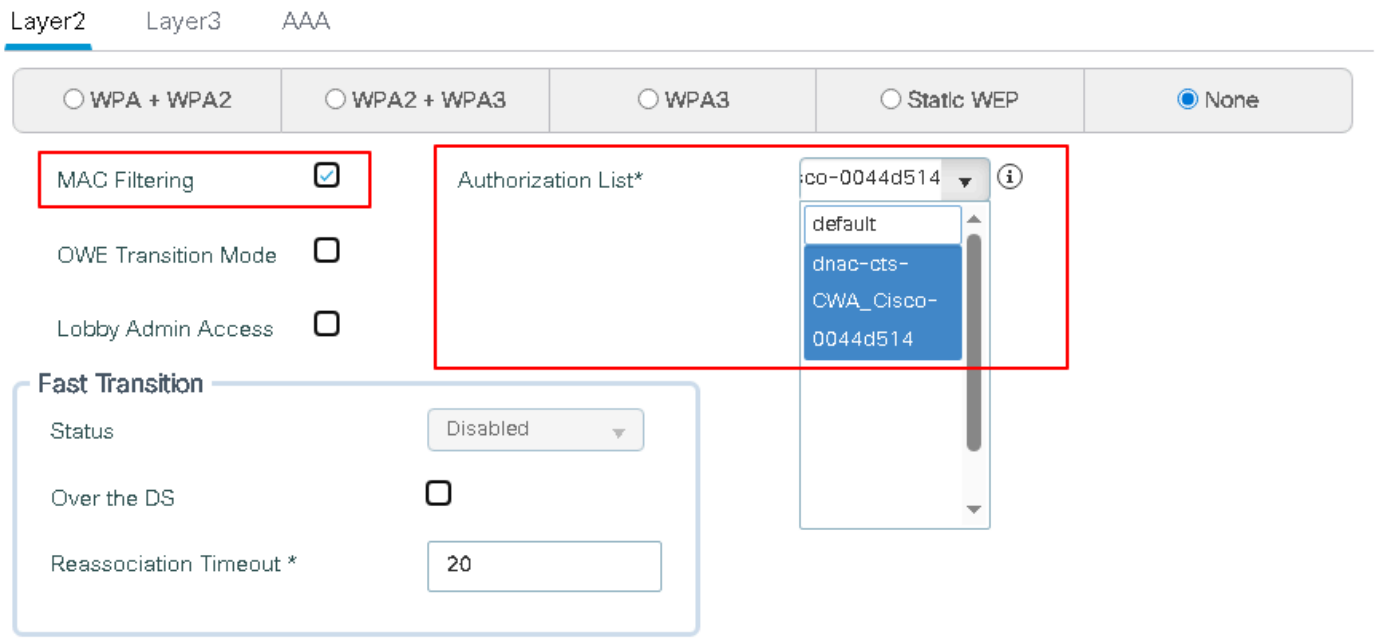


Le SSID CWA_Cisco est nommé CWA_Cisco_profile sur le WLC, avec l'ID 21 et un type de sécurité Open utilisant le filtrage MAC. Double-cliquez sur le SSID pour afficher sa configuration.

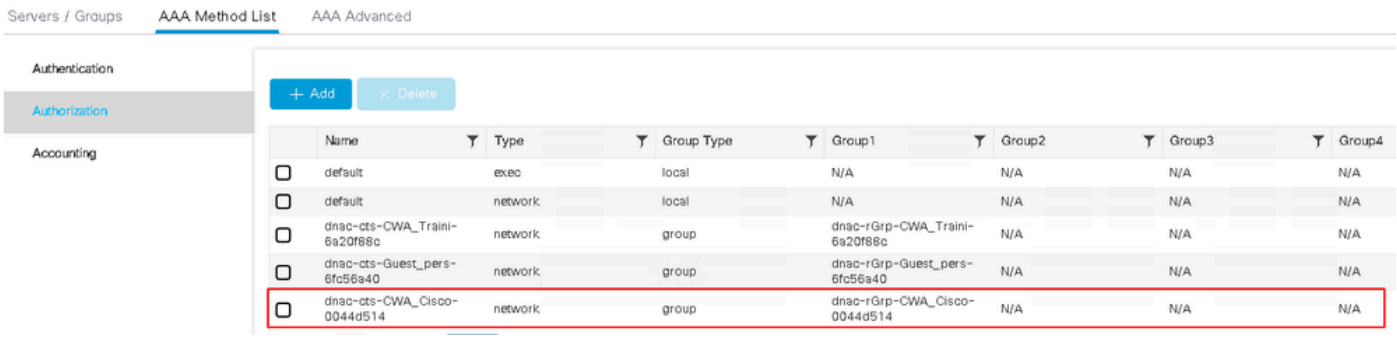


Le SSID est actif et diffuse sur les canaux 5 GHz et 2,4 GHz. Il est associé au profil de stratégie

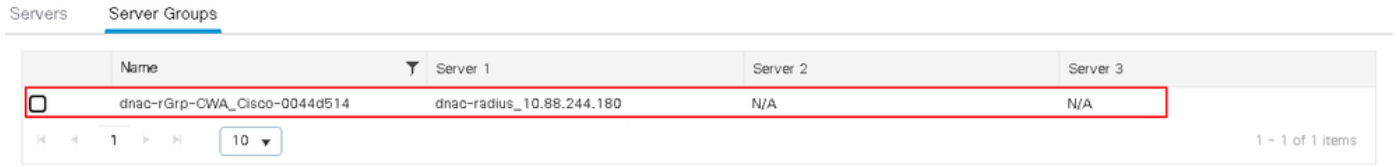
CWA_CIsco_Profile. Cliquez sur l'onglet Security (Sécurité) pour afficher les paramètres.



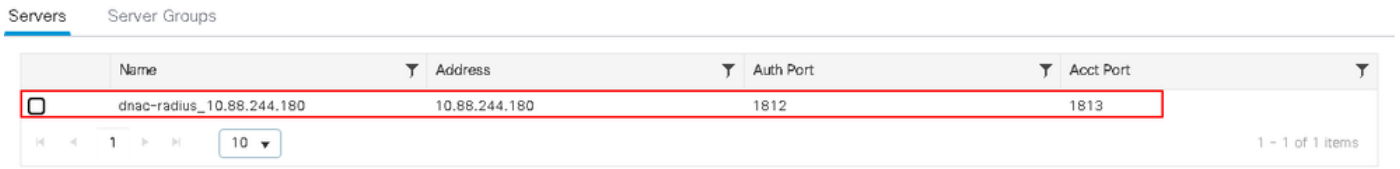
Les paramètres clés incluent la méthode de sécurité de couche 2 (filtrage MAC) et la liste d'autorisation AAA (Cisco DNA-cts-CWA_Cisco-0044d514). Pour vérifier sa configuration, accédez à Configuration > Security > AAA > AAA Method List > Authorization.



La liste des méthodes pointe vers le groupe RADIUS Cisco DNA-Grp-CWA_Cisco-0044d514 dans la colonne Group1. Pour afficher sa configuration, accédez à Configuration > Security > AAA > Server/Groups > Server Groups.



Le groupe de groupes de serveurs Cisco DNA-Grp-CWA_Cisco-0044d514 pointe vers Cisco DNA-radius_10.88.244.180 dans la colonne Server 1. Affichez sa configuration dans l'onglet Serveurs.



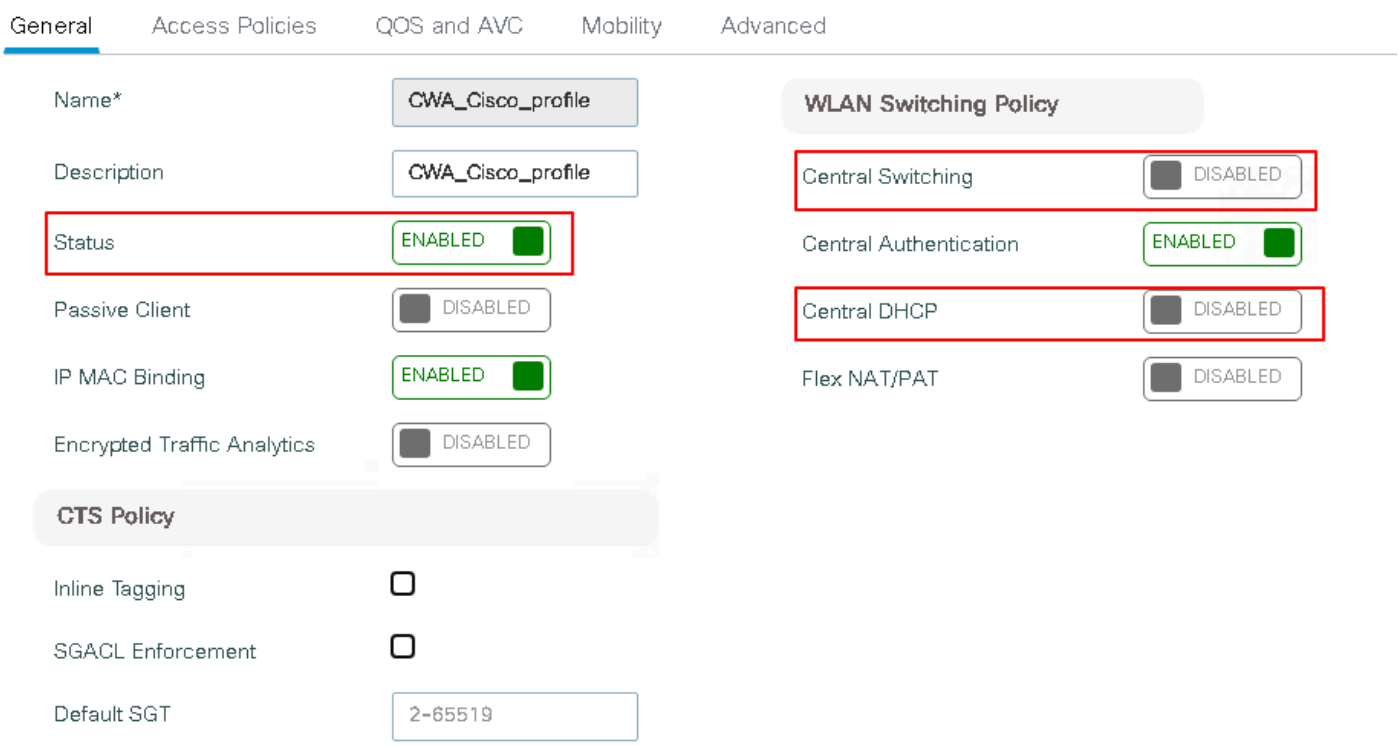
Le serveur Cisco DNA-radius_10.88.244.180 a l'adresse IP 10.88.244.180, cliquez sur son nom pour afficher sa configuration

Une configuration critique est Change of Authorization (CoA), qui fournit un mécanisme permettant de modifier les attributs d'une session d'authentification, d'autorisation et de comptabilité (AAA) après son authentification sur le portail captif. Sans cette fonctionnalité, le point de terminaison reste dans un état d'attente d'authentification Web même après avoir terminé l'enregistrement sur le portail.

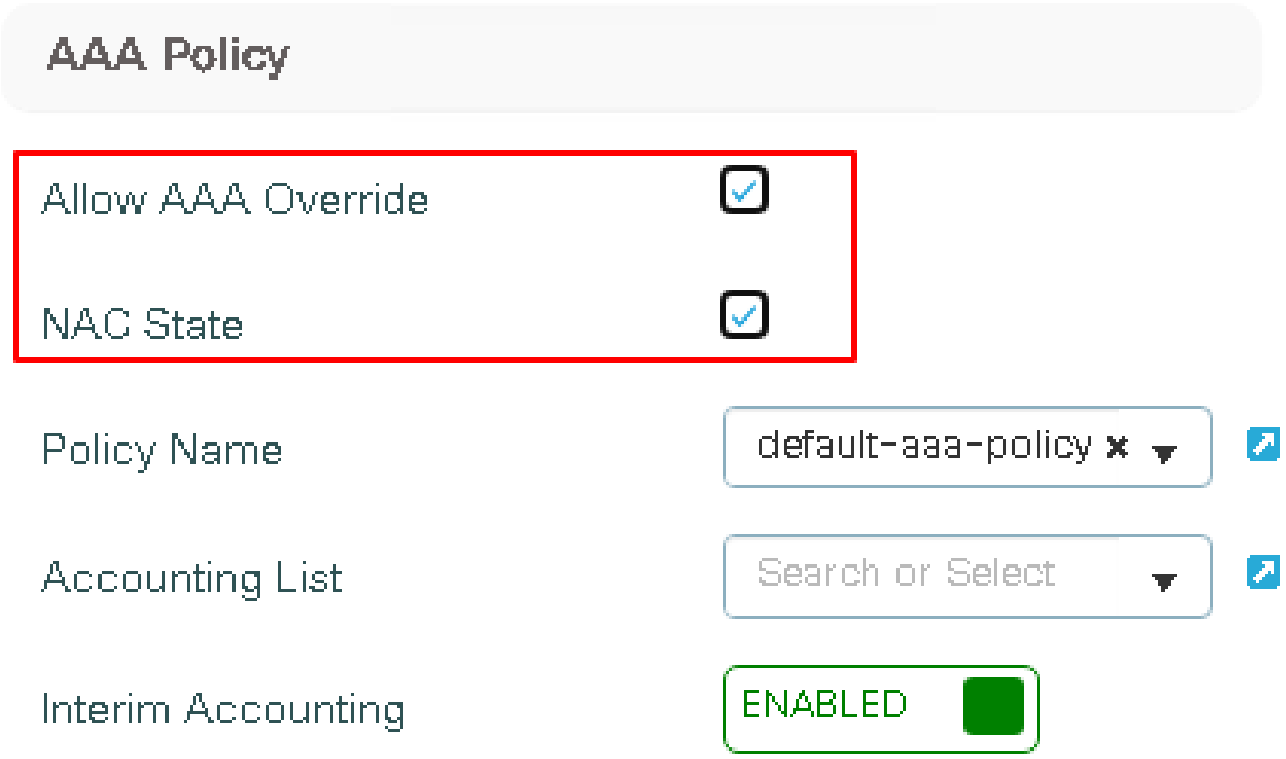
Configuration du profil de stratégie sans fil

Dans le profil de stratégie, les clients peuvent se voir attribuer des paramètres tels que VLAN, ACL, QoS, Mobility Anchor et timers. Pour afficher la configuration du profil de stratégie, accédez à Configuration > Tags & Profiles > Policy.

Cliquez sur le nom de la stratégie pour afficher sa configuration.



L'état de la stratégie est Activé et, comme pour tout SSID de fabric, la commutation centrale et le DHCP central sont désactivés. Cliquez sur l'onglet Avancé, puis accédez à la section Stratégie AAA pour afficher des détails de configuration supplémentaires.



AAA Override et NAC (Network Access Control) peuvent être activés. AAA Override permet au contrôleur d'accepter les attributs renvoyés par le serveur RADIUS, tels que les ACL ou les URL, et d'appliquer ces attributs aux clients. NAC active la modification d'autorisation (CoA) après l'enregistrement du client sur le portail.
Cette configuration peut également être visualisée via l'interface de ligne de commande sur le

WLC.
Pour vérifier le profil de stratégie, le SSID est attaché pour exécuter la commande :

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

WLAN  Profile Name       SSID       Status
------------------------------------------------------------------------------
21

CWA_Cisco_profile

  CWA_Cisco  UP
```

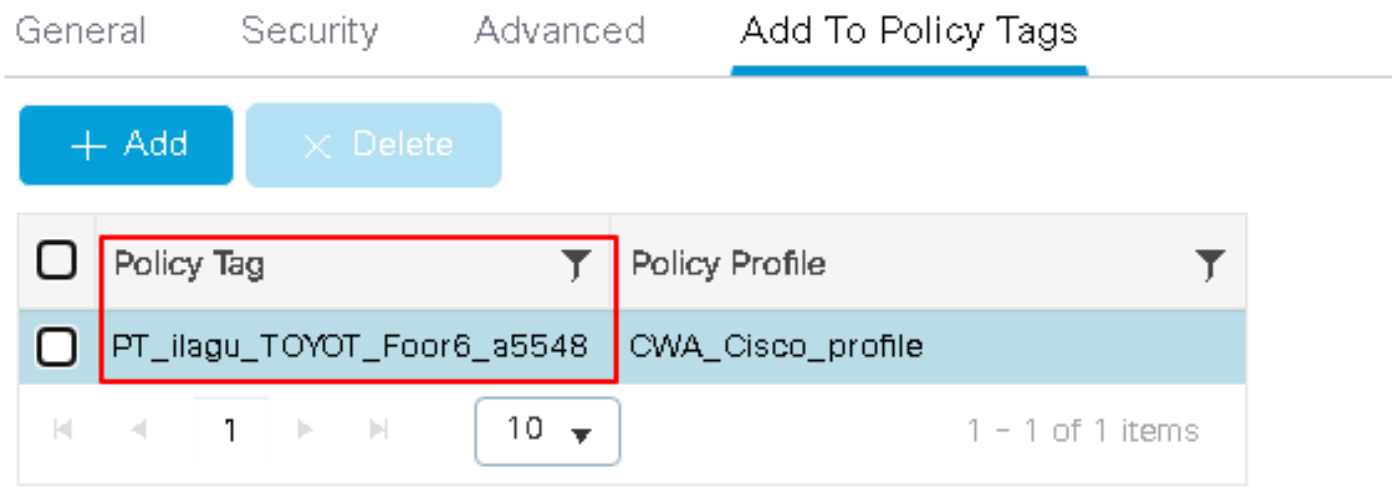
Pour afficher la configuration du profil de stratégie CWA_Cisco_profile, exécutez la commande suivante :

<#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
```

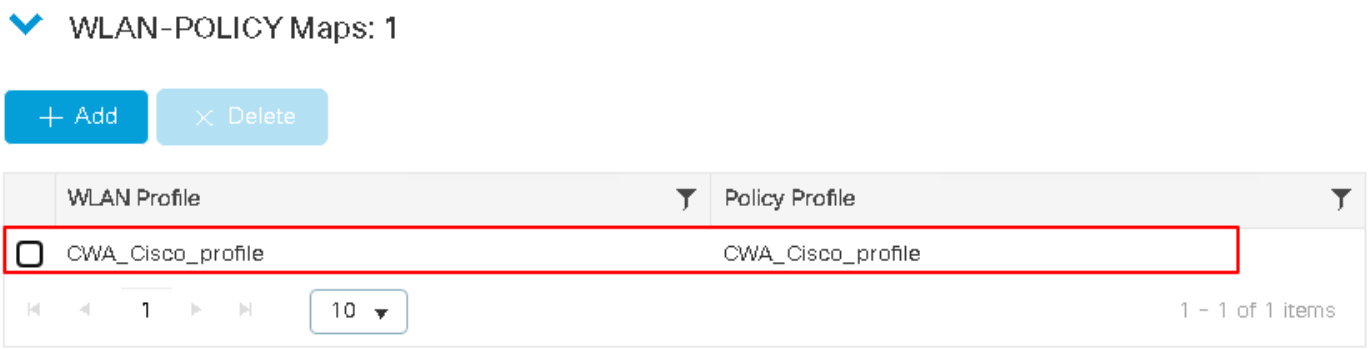
Configuration des balises des politiques

La balise de stratégie est la façon dont vous liez le WLAN avec le profil de stratégie, naviguez vers Configuration > Tags & Profiles > WLANs, cliquez sur le nom WLAN, et naviguez vers Add to Policy Tags pour identifier la balise de stratégie attribuée au SSID.



Pour le SSID CWA_Cisco_profile, la balise de stratégie PT_ilagu_TOYOT_For6_a5548 est utilisée pour vérifier cette configuration. Accédez à Configuration > Tags & Profiles > Tags > Policy.

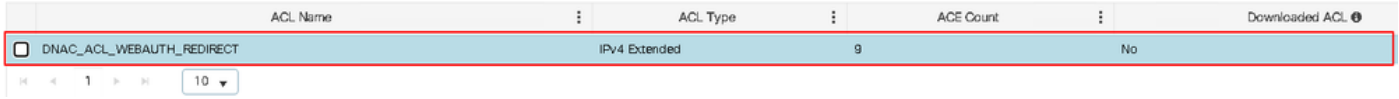
Cliquez sur le nom pour afficher ses détails. La balise de stratégie PT_ilagu_TOYOT_For6_a5548 lie le WLAN CWA_Cisco associé au nom CWA_Cisco_profile sur le WLC (voir la page WLAN pour référence) au profil de stratégie CWA_Cisco_profile.



Le nom WLAN CWA_Cisco_profile fait référence au WLAN CWA_Cisco.

Configuration d'une liste de contrôle d'accès de redirection

Dans CWA, une liste de contrôle d'accès de redirection définit quel trafic est redirigé vers le WLC pour un traitement ultérieur et quel trafic contourne la redirection
Cette configuration est poussée vers le WLC après la création du SSID et la mise en service du WLC à partir de l'inventaire. Pour l'afficher, accédez à Configuration > Security > ACL, Le nom de l'ACL que Catalyst Center utilise pour l'ACL de redirection est Cisco DNA_ACL_WEBAUTH_REDIRECT.



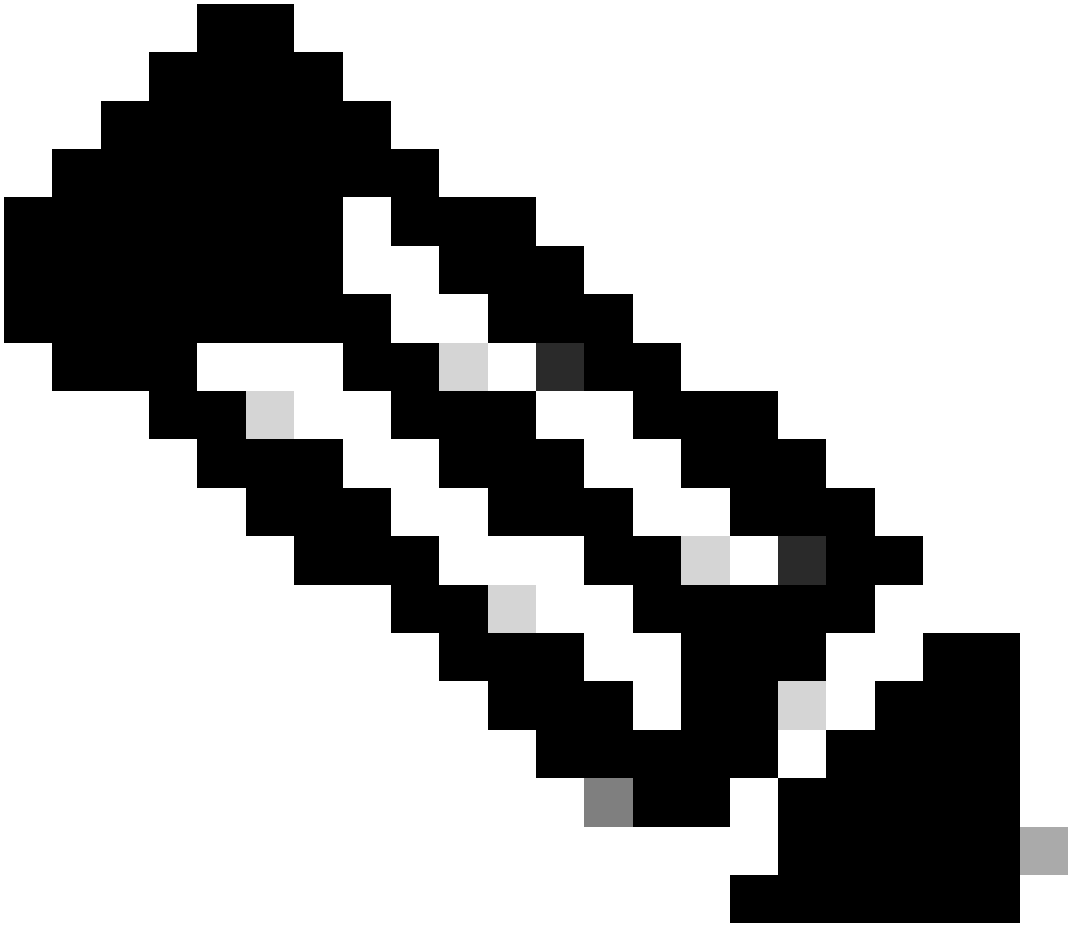
ACL Name	ACL Type	ACE Count	Downloaded ACL
DNAC_ACL_WEBAUTH_REDIRECT	IPv4 Extended	9	No

1 10

Cliquez sur le nom pour afficher sa configuration. Les valeurs sont dérivées des paramètres réseau des paramètres réseau du site sur 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



Remarque : Ces valeurs sont obtenues à partir des paramètres réseau du site configurés dans Catalyst Center, et les valeurs DHCP/DNS proviennent du pool configuré dans le WLAN. L'adresse IP du PSN ISE est référencée dans la configuration AAA dans le workflow SSID.

Pour afficher la liste de contrôle d'accès de redirection sur la CLI WLC, exécutez cette commande :

<#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
```

La liste de contrôle d'accès de redirection peut être appliquée au profil Flex pour être envoyée aux points d'accès. Exécutez cette commande pour confirmer cette configuration

<#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

Redirection ACL sur le point d'accès

Sur le point d'accès, les valeurs permit et deny sont inversées : permit indique le trafic de transfert et deny indique la redirection. Pour examiner la configuration de la liste de contrôle d'accès de redirection sur le point d'accès, exécutez cette commande :

<#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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.