Konfigurieren der zentralen Webauthentifizierung bei SD-Zugriff

Inhalt

Einleitung

Dieses Dokument beschreibt eine schrittweise Anleitung zur Konfiguration der zentralen Webauthentifizierung (CWA) und beschreibt die Verifizierungsverfahren für alle Komponenten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Architektur der Catalyst Wireless Controller 9800
- Authentifizierung, Autorisierung und Abrechnung (AAA)

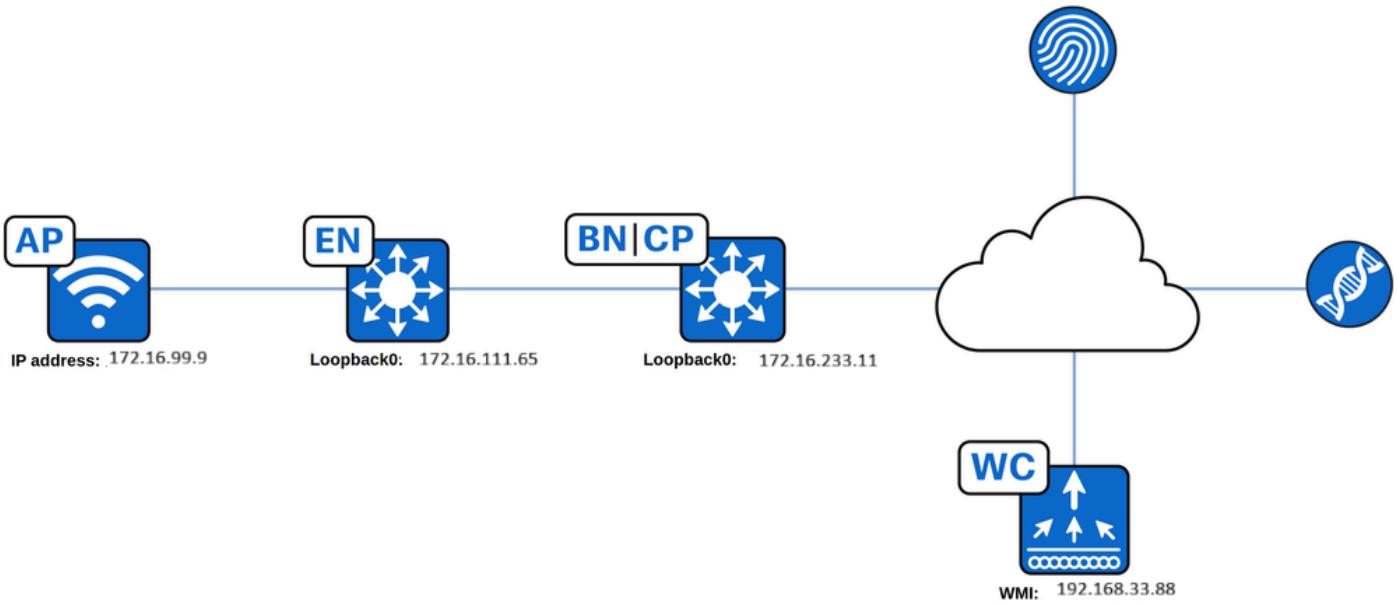
Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Wireless LAN Controller (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
- SDA Edge Node - C9300-48P, Cisco IOS® XE 17.12.05
- SDA-Grenzknoten/Kontrollebene - C9500-48P, Cisco IOS® XE17.12.05
- Cisco Access Point - C9130AXI-A, Version 17.9.5.47

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Topologie



Überblick

Die zentrale Web-Authentifizierung (CWA) verwendet eine Gast-SSID, um den Webbrowser des Benutzers mithilfe einer konfigurierten Umleitungs-ACL an ein Captive Portal umzuleiten, das von der Cisco ISE gehostet wird. Das Captive Portal ermöglicht dem Benutzer die Registrierung und Authentifizierung. Nach der erfolgreichen Authentifizierung erteilt der Wireless LAN Controller (WLC) die entsprechende Berechtigung, um den vollständigen Netzwerkzugriff zu gewähren. Dieses Handbuch enthält detaillierte Anweisungen zur Konfiguration des CWA mit Cisco Catalyst Center.

Konfigurieren von CWA auf Cisco Catalyst Center

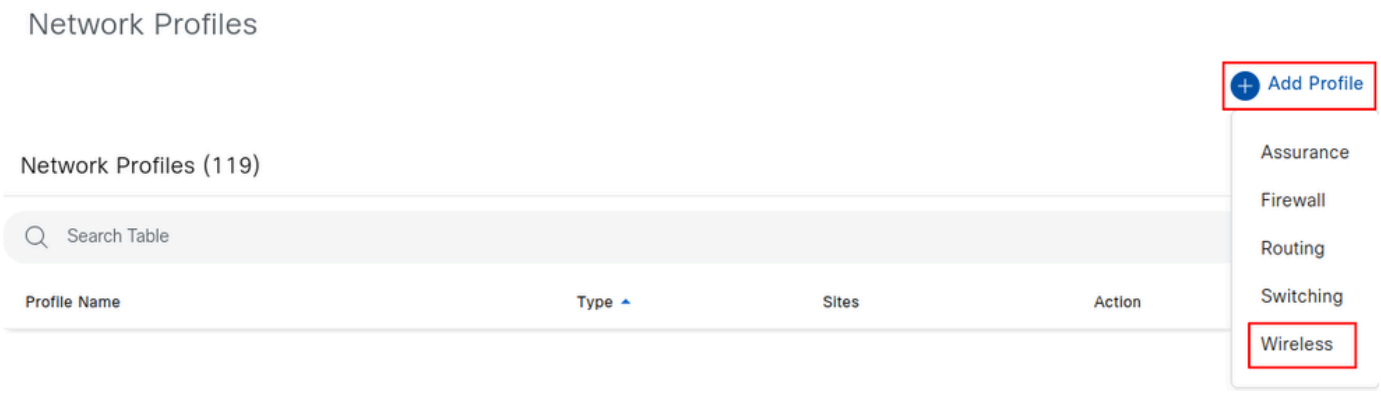
Netzwerkprofil erstellen

Ein Netzwerkprofil ermöglicht die Konfiguration von Einstellungen, die auf einen bestimmten Standort angewendet werden können. Netzwerkprofile können für verschiedene Elemente in Cisco Catalyst Center erstellt werden, darunter:

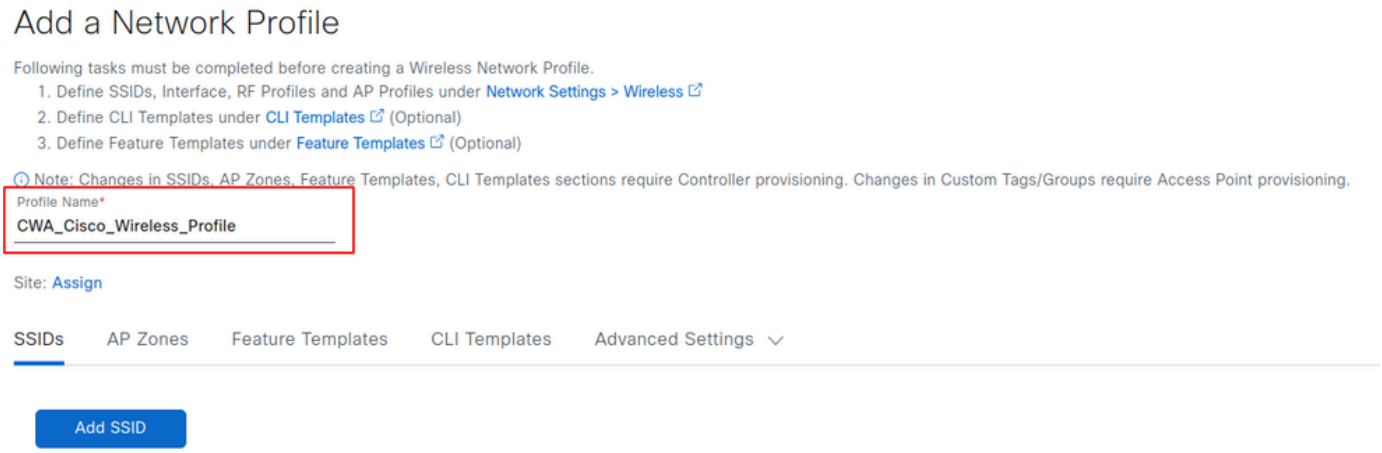
- Sicherheit
- Firewall
- Routing
- Switching
- Telemetriegerät
- Wireless

Für CWA muss ein Wireless-Profil konfiguriert werden.

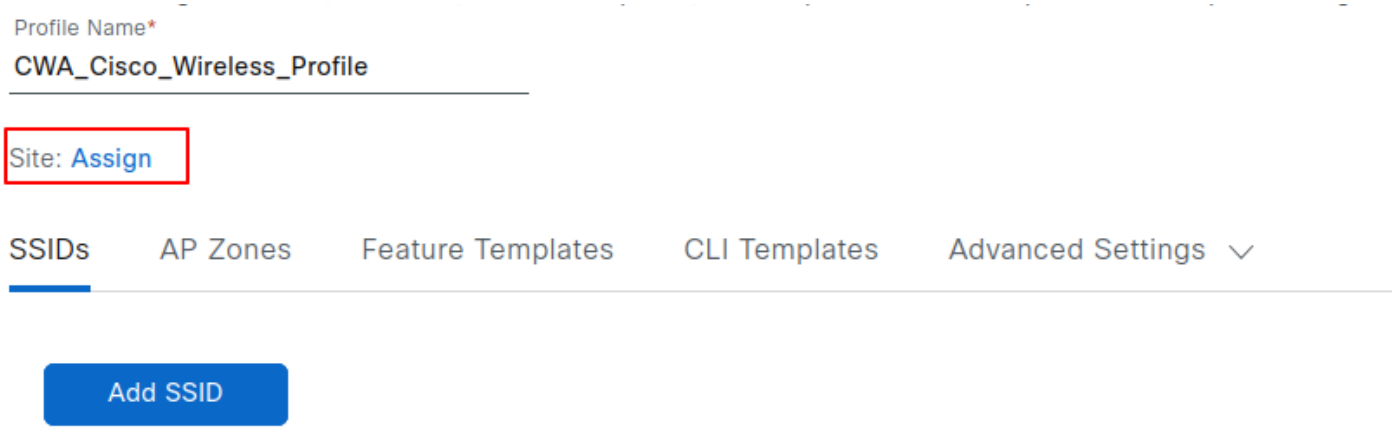
Um ein Drahtlosprofil zu konfigurieren, navigieren Sie zu Design > Network Profiles, klicken Sie auf Add Profile und wählen Sie Wireless aus.



Benennen Sie das Profil nach Bedarf. In diesem Beispiel hat das Drahtlosprofil den Namen CWA_Cisco_Wireless_Profile. Sie können diesem Profil alle vorhandenen SSIDs hinzufügen, indem Sie SSID hinzufügen auswählen. Die SSID-Erstellung wird im nächsten Abschnitt behandelt.

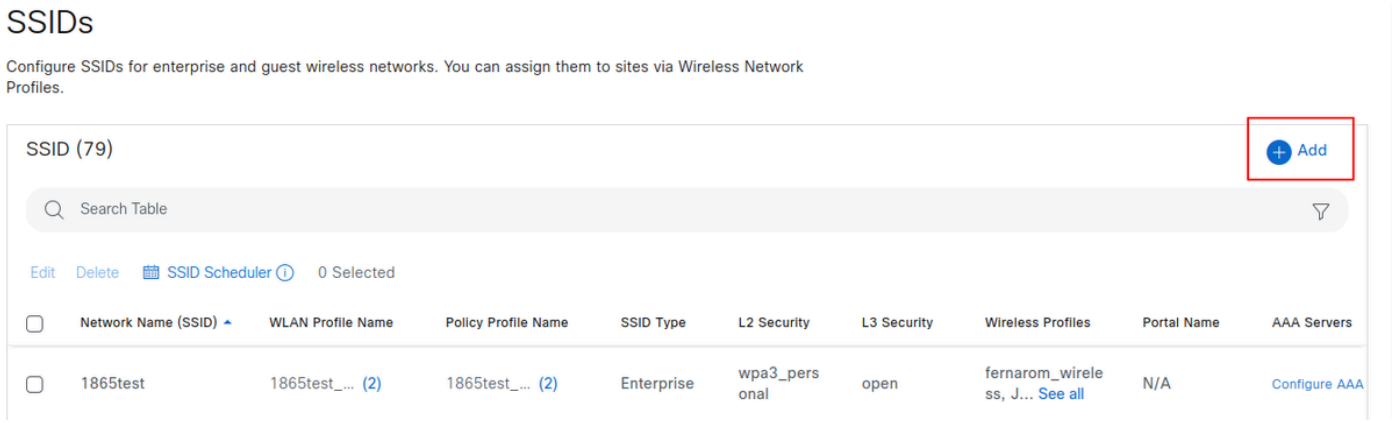


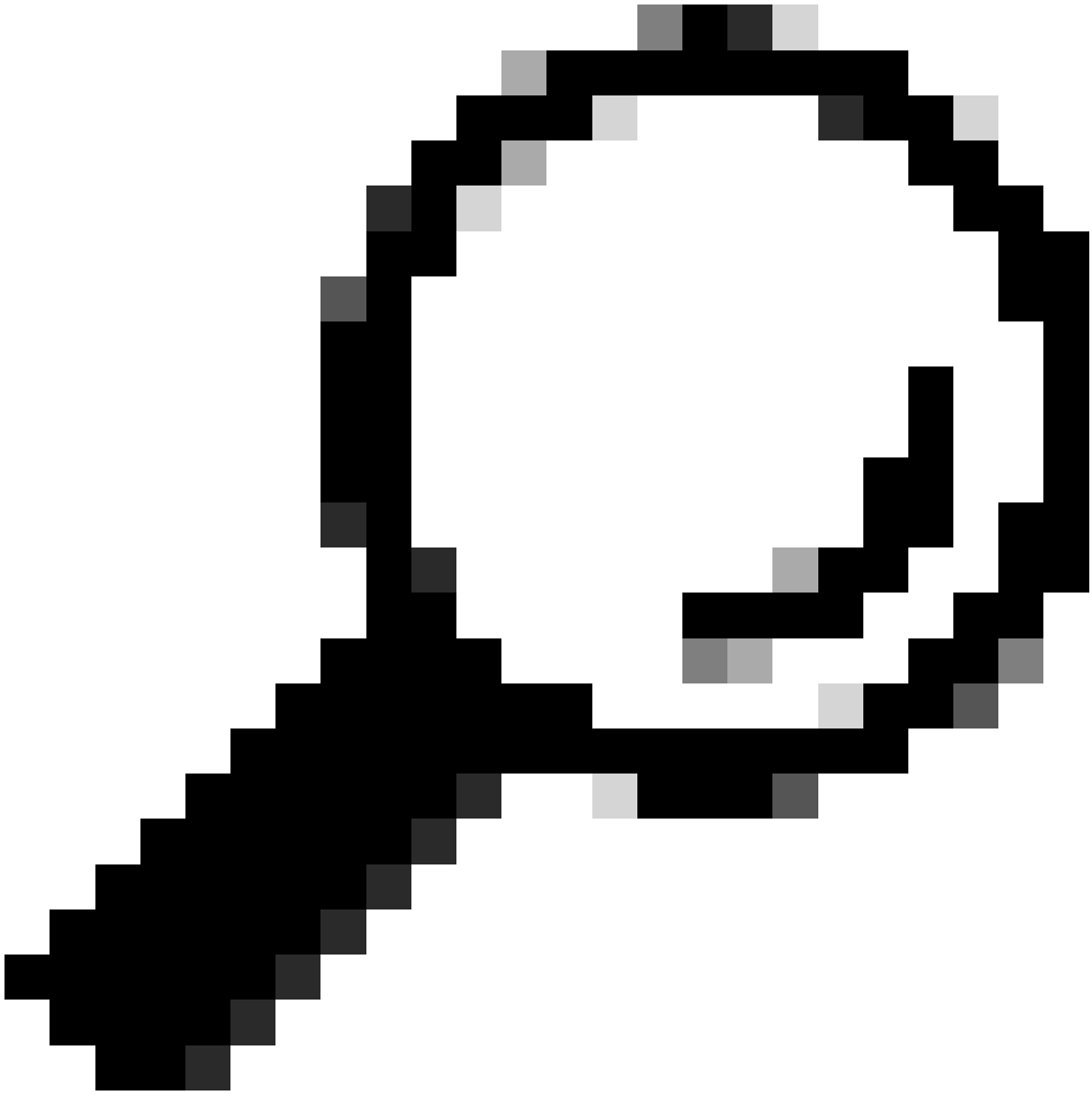
Wählen Sie Zuweisen aus, um den Standort auszuwählen, auf den dieses Profil angewendet werden soll, und wählen Sie dann den gewünschten Standort aus. Nachdem Sie die Websites ausgewählt haben, klicken Sie auf Speichern.



Erstellen der SSID

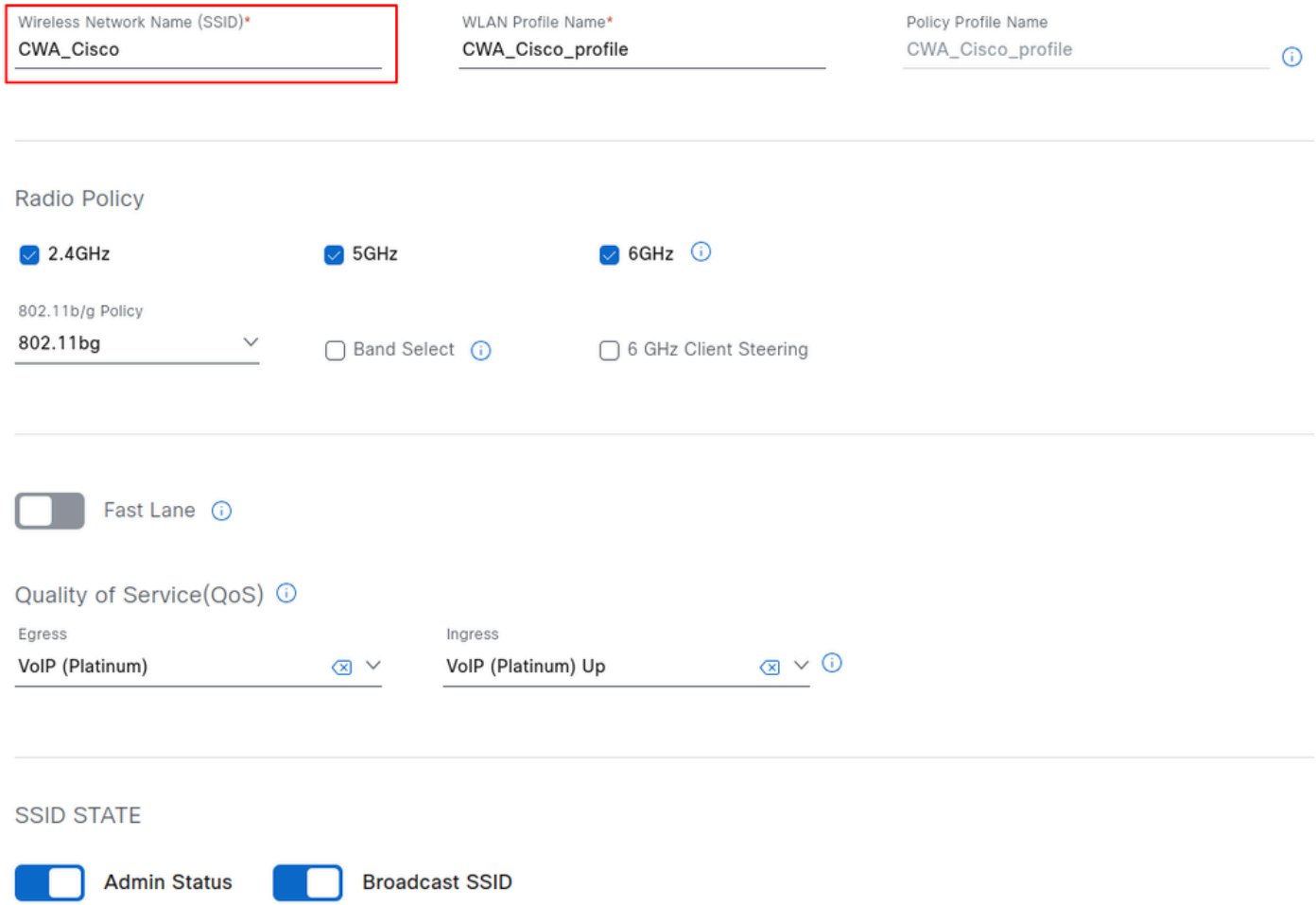
Navigieren Sie zu Design > Network Settings > Wireless > SSIDs, und klicken Sie auf Add.



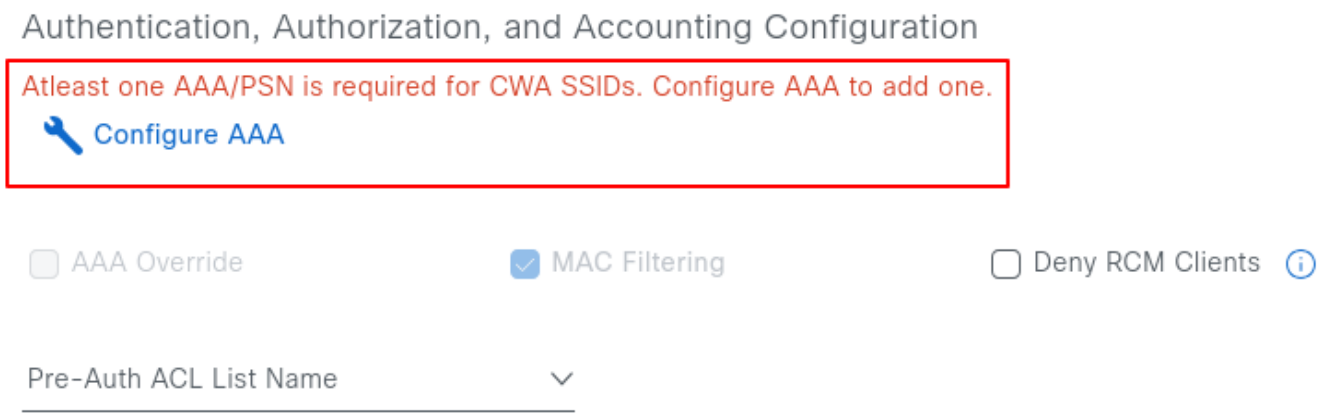


Tipp: Beim Erstellen einer SSID für CWA muss unbedingt der Gasttyp ausgewählt werden. Durch diese Auswahl wird dem Wireless-Richtlinienprofil des SSID auf dem WLC ein Befehl hinzugefügt (der NAC-Befehl), mit dem CoA für die Neuauthentifizierung verwendet werden kann, nachdem sich der Benutzer auf dem Captive Portal registriert hat. Ohne diese Konfiguration können Benutzer eine endlose Schleife der Registrierung erleben und wiederholt auf das Portal umgeleitet werden.

Fahren Sie nach der Auswahl von Add (Hinzufügen) mit dem SSID-Konfigurationsworkflow fort. Auf der ersten Seite können Sie den SSID-Namen konfigurieren. Sie können auch das Radio Policy Band auswählen und den SSID-Status definieren, einschließlich Verwaltungsstatus und Broadcast-Einstellungen. Für diese Konfigurationsanleitung lautet die SSID CWA_Cisco.



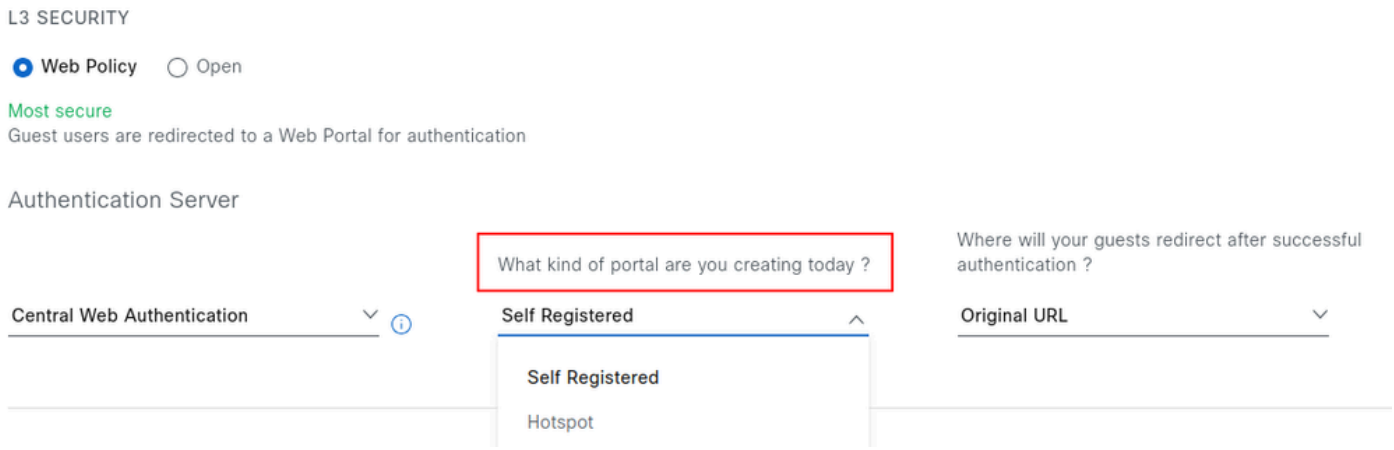
Nach der Eingabe des SSID-Namens werden der WLAN- und der Richtlinienprofilname automatisch generiert. Wählen Sie Weiter, um fortzufahren.
Für CWA-SSIDs muss mindestens ein AAA/PSN konfiguriert werden. Wenn keine konfiguriert ist, wählen Sie Configure AAA und dann die PSN IP address aus der Dropdown-Liste aus.



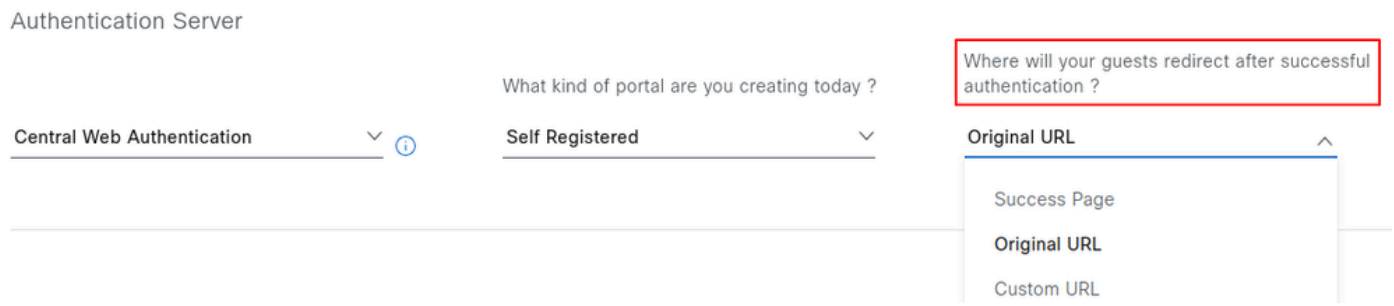
Nachdem Sie den AAA-Server ausgewählt haben, legen Sie die Sicherheitsparameter für Layer 3 fest und wählen Sie den Portaltyp aus: Selbst registriert oder Hotspot.

Hotspot-Gastportale: Ein Hotspot-Gastportal ermöglicht Gästen den Netzwerkzugriff, ohne dass Benutzernamen und Kennwörter erforderlich sind. In diesem Fall müssen die Benutzer eine Richtlinie zur akzeptablen Nutzung akzeptieren, um Zugriff auf das Netzwerk zu erhalten, die zu

einem nachfolgenden Internetzugriff führt. Der Zugriff über ein registriertes Gastportal setzt voraus, dass die Gäste über einen Benutzernamen und ein Kennwort verfügen.



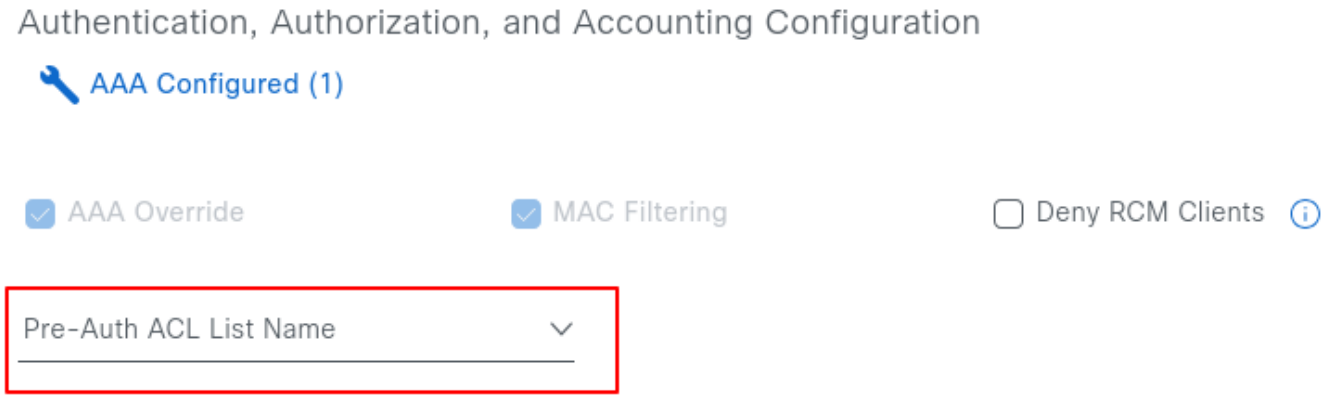
Die Aktion, die ausgeführt wird, nachdem der Benutzer die Nutzungsrichtlinie registriert oder akzeptiert hat, kann ebenfalls konfiguriert werden. Drei Optionen stehen zur Verfügung: Erfolgsseite, ursprüngliche URL und benutzerdefinierte URL.



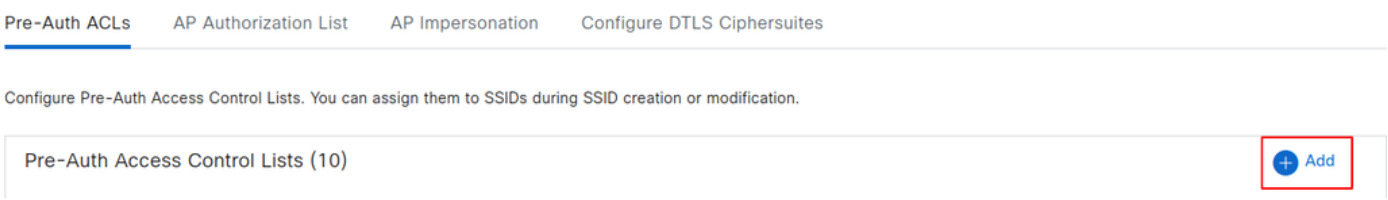
Im Folgenden wird das Verhalten jeder Option beschrieben:

Seite "Erfolg": Leitet den Benutzer zu einer Bestätigungsseite um, die angibt, dass die Authentifizierung erfolgreich war.
Ursprüngliche URL: Leitet den Benutzer zur ursprünglichen URL um, die vor dem Abfangen durch das Captive Portal angefordert wurde.
Benutzerdefinierte URL: Leitet den Benutzer zu einer angegebenen benutzerdefinierten URL um. Durch Auswahl dieser Option wird ein zusätzliches Feld zum Definieren der Ziel-URL aktiviert.

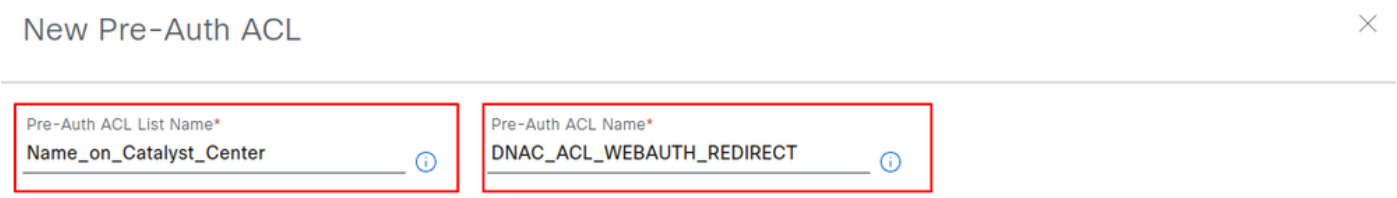
Auf derselben Seite kann unter "Authentication, Authorization, and Accounting Configuration" auch eine Vorabauthentifizierungs-ACL konfiguriert werden. Diese ACL ermöglicht das Hinzufügen zusätzlicher Einträge für Protokolle über DHCP-, DNS- oder PSN-IP-Adressen hinaus, die aus den Netzwerkeinstellungen abgerufen werden und während der Bereitstellung an die Umleitungs-ACL angefügt werden. Diese Funktion steht ab Cisco Catalyst Center Version 2.3.3.x zur Verfügung.



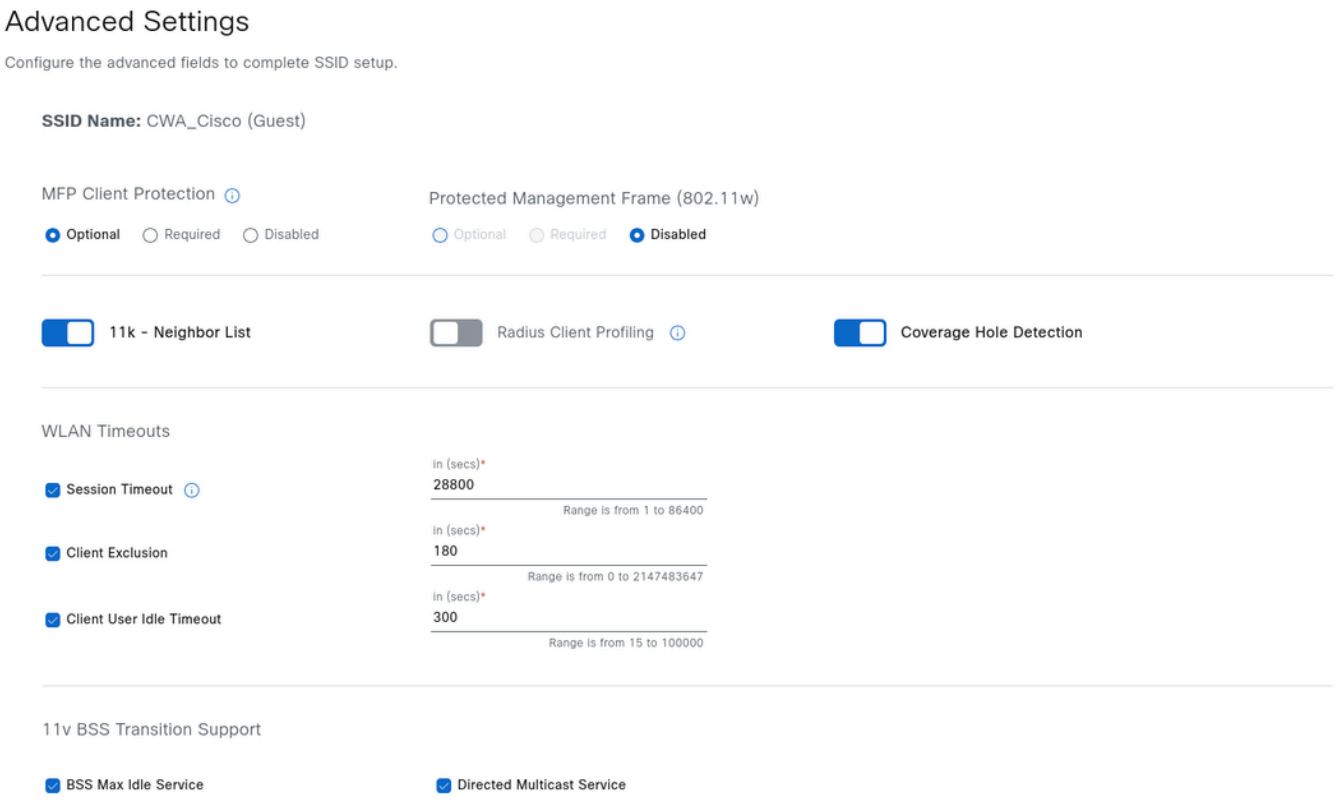
Um eine Pre-Auth ACL zu konfigurieren, navigieren Sie zu Design > Network Settings > Wireless > Security Settings, und klicken Sie auf Add.



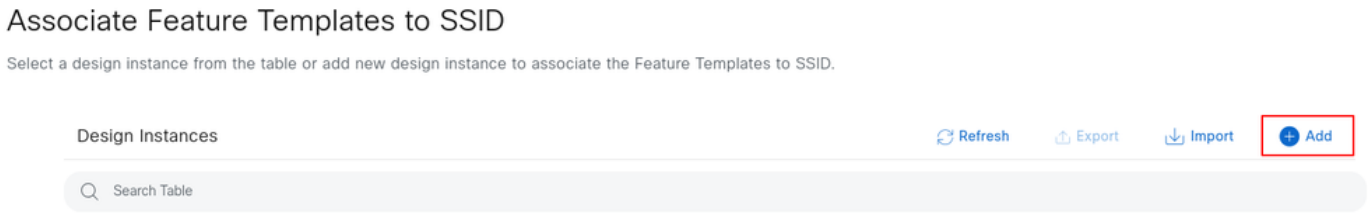
Der erste Name identifiziert die ACL in Catalyst Center, während der zweite Name dem ACL-Namen auf dem WLC entspricht. Der zweite Name kann mit der vorhandenen, auf dem WLC konfigurierten Umleitungs-ACL übereinstimmen. Als Referenz stellt Catalyst Center dem WLC den Namen Cisco DNA_ACL_WEBAUTH_REDIRECT bereit. Einträge aus der Pre-Auth ACL werden nach den vorhandenen Einträgen angehängt.



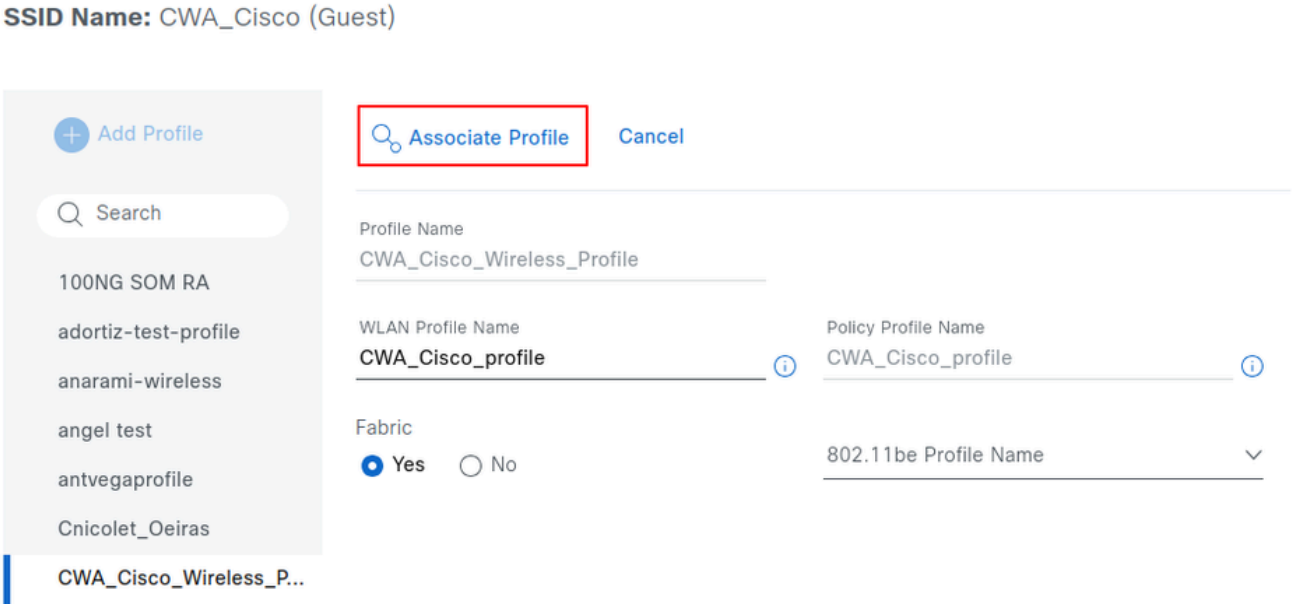
Wenn Sie zum SSID-Erstellungs-Workflow zurückkehren und Weiter auswählen, werden die erweiterten Einstellungen angezeigt, einschließlich schneller Übergänge, Sitzungs-Timeout, Client-Benutzer-Timeout und Ratenbegrenzung. Passen Sie die Parameter nach Bedarf an, und wählen Sie dann Weiter aus, um fortzufahren. Für die Zwecke dieses Konfigurationsleitfadens werden im Beispiel die Standardeinstellungen beibehalten.



Wenn Sie Weiter ausgewählt haben, werden Sie aufgefordert, der SSID Funktionsvorlagen zuzuordnen. Wählen Sie ggf. die gewünschten Vorlagen aus, indem Sie auf Hinzufügen klicken, und klicken Sie abschließend auf Weiter.

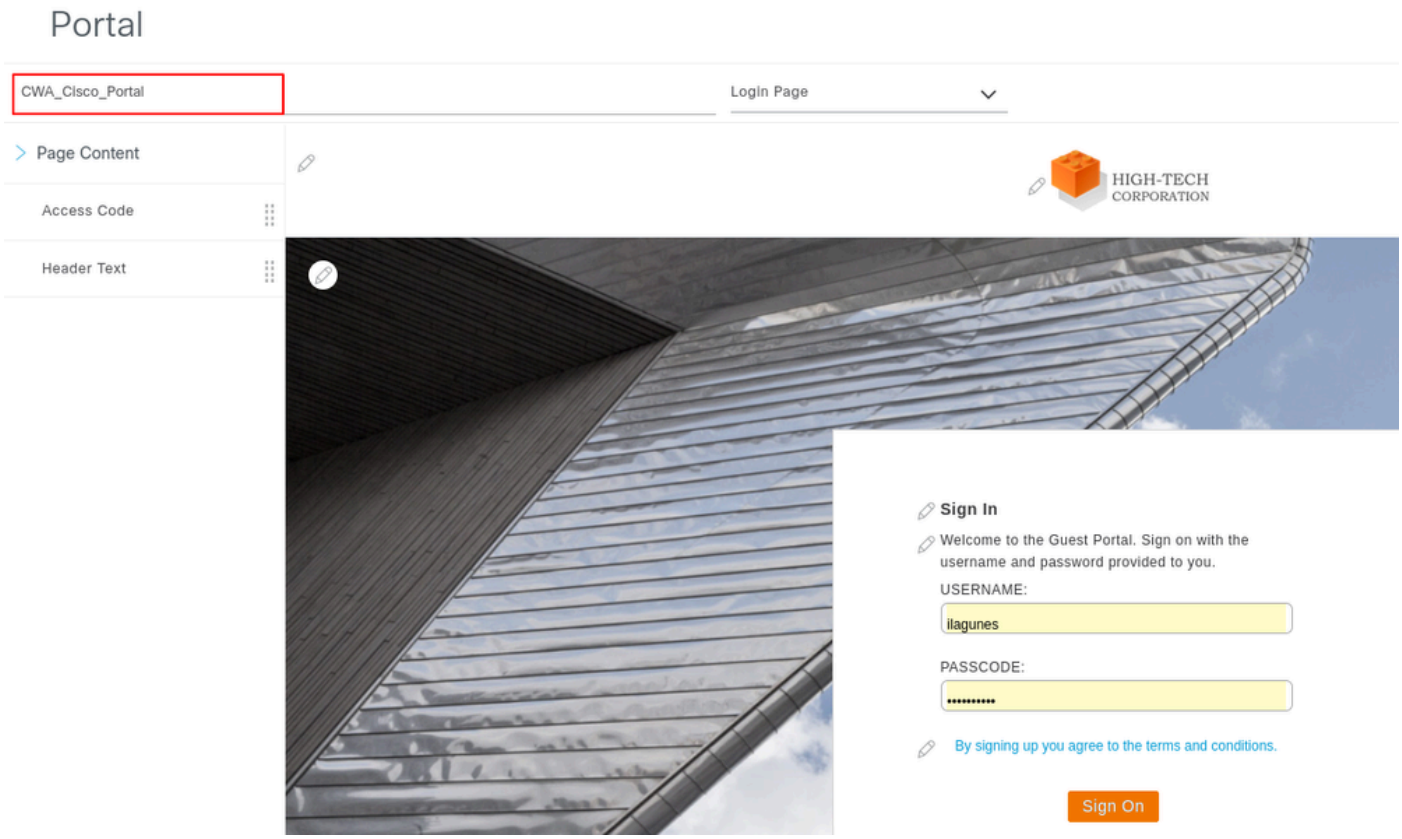


Ordnen Sie die SSID dem zuvor erstellten Wireless-Profil zu. Weitere Informationen finden Sie im Abschnitt Erstellen des Drahtlosnetzwerkprofils. In diesem Abschnitt können Sie auch auswählen, ob die SSID Fabric-aktiviert ist. Wenn Sie fertig sind, klicken Sie auf Profil zuordnen.

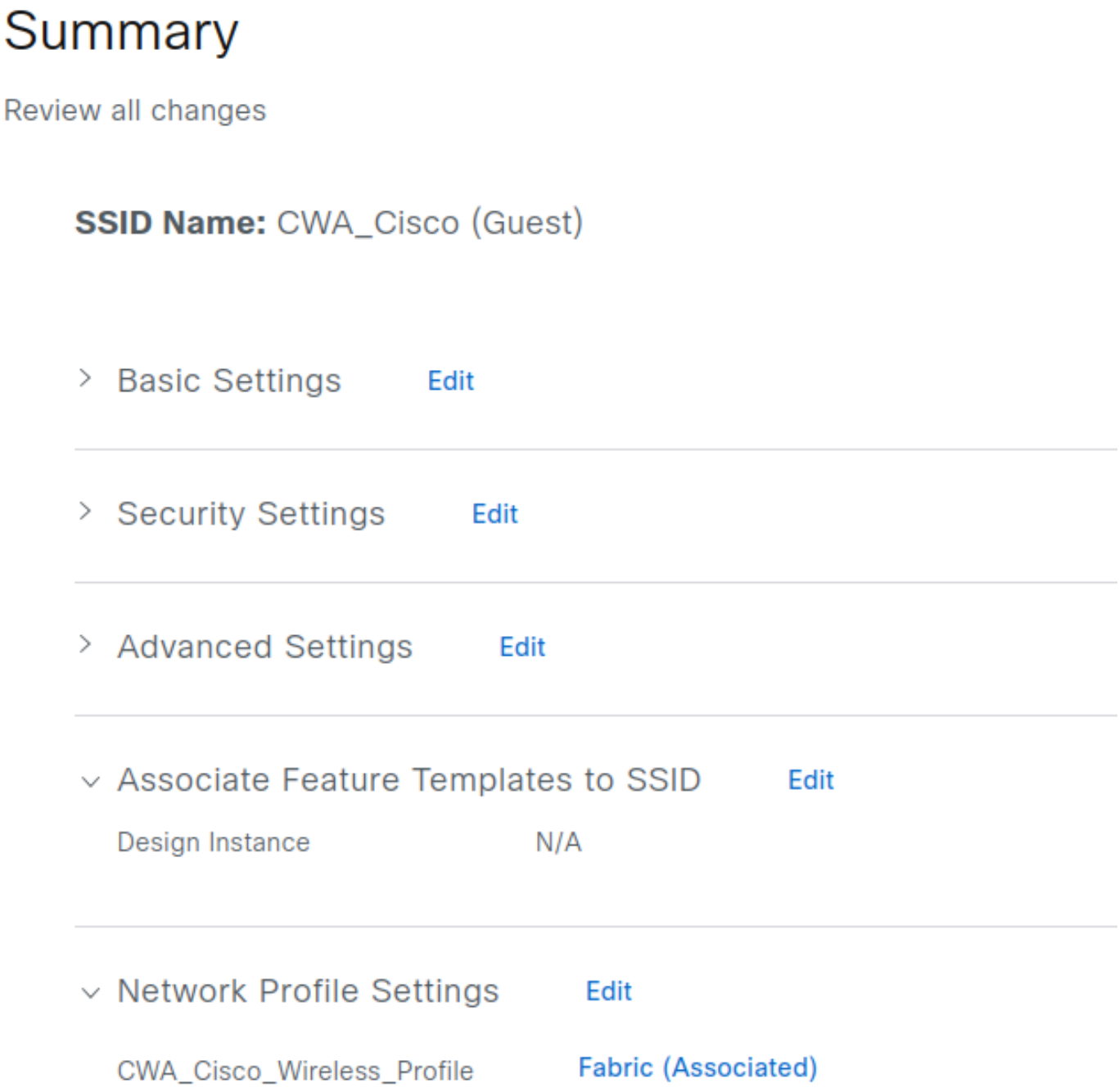


Wireless-Management-Vertrauenspunkt anzeigen
Wenn das Profil mit der SSID verknüpft ist, klicken Sie auf Weiter, um das Captive Portal zu erstellen und zu entwerfen. Klicken Sie zum Starten auf Portal erstellen.

Der Portalname definiert den Domänennamen im FQDN und den Richtliniensatznamen auf der ISE. Klicken Sie abschließend auf Speichern. Das Portal kann bearbeitet und bei Bedarf gelöscht werden.



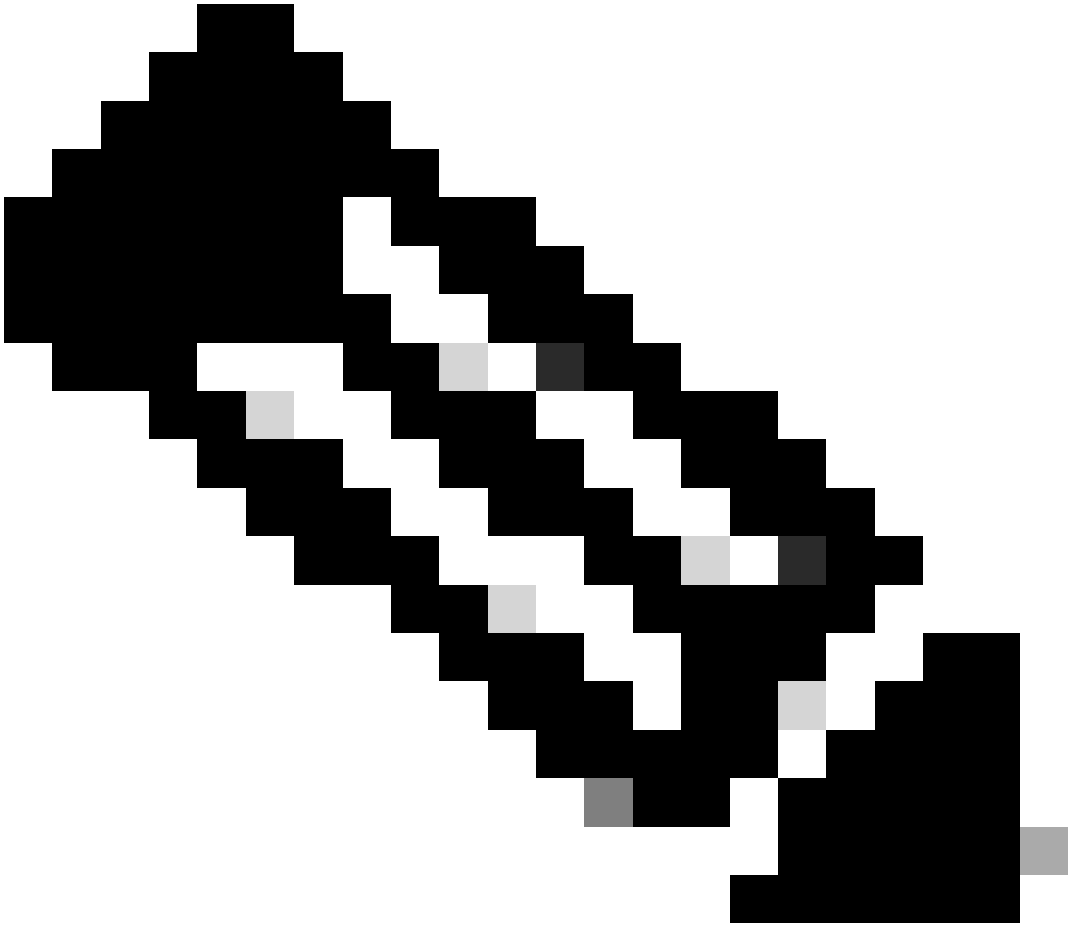
Wählen Sie Weiter, um eine Zusammenfassung aller in den vorherigen Schritten definierten Konfigurationsparameter anzuzeigen.



Bestätigen Sie die Konfigurationsdetails, und wählen Sie dann Speichern, um die Änderungen zu übernehmen.

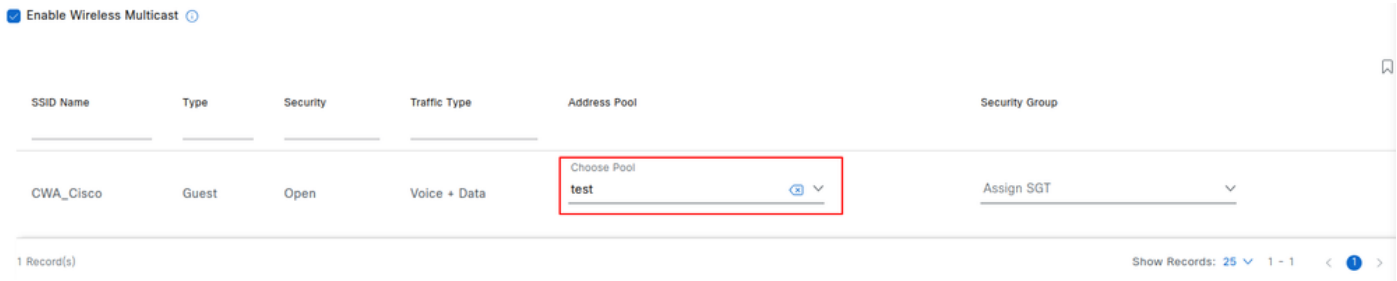
Fabric-Bereitstellung

Nachdem Sie das Profil des Wireless-Netzwerks mit dem Fabric-Standort verknüpft haben, wird der SSID unter Provisioning > Fabric Sites > (Ihr Standort) > Wireless SSIDs (Bereitstellung > Fabric-Standorte > (Ihr Standort) angezeigt.

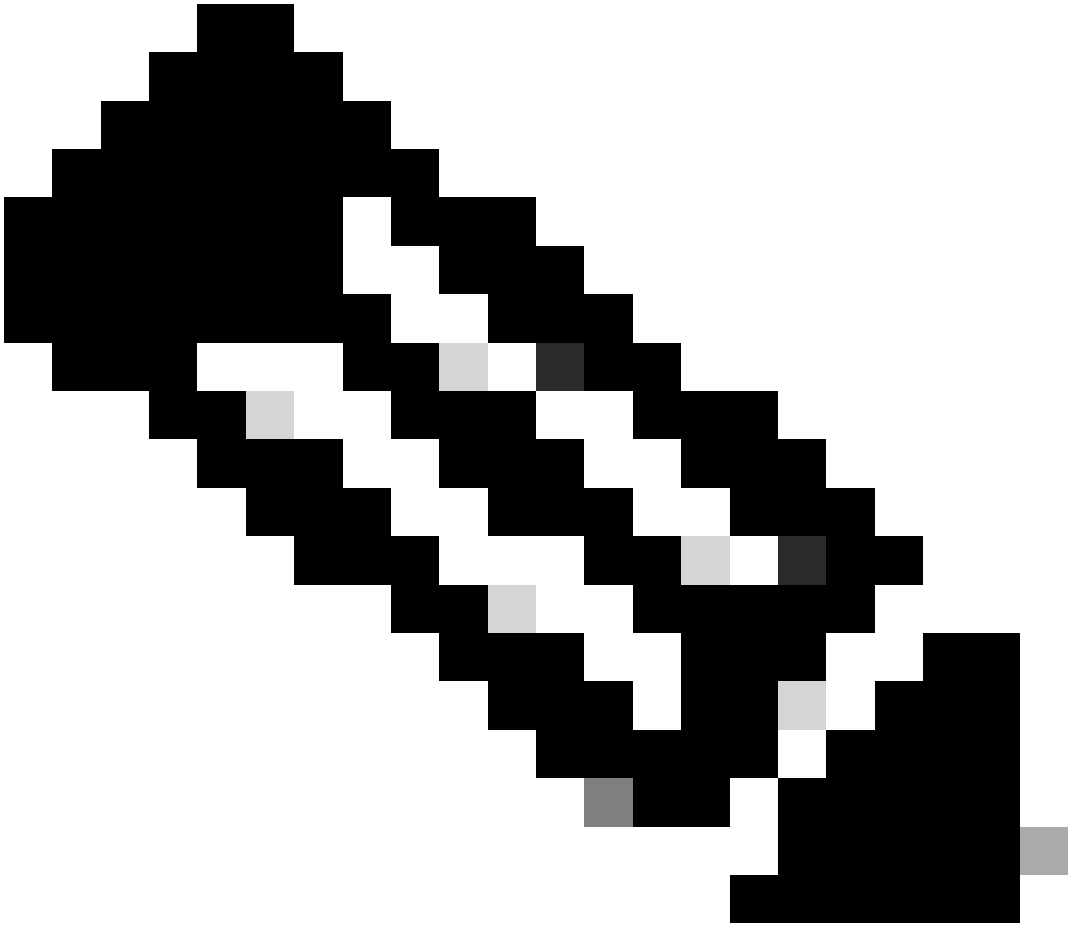


Anmerkung: Sie müssen den Wireless LAN Controller für den Standort bereitstellen, damit die SSIDs unter Wireless SSIDs angezeigt werden.

Wählen Sie den SSID-Pool aus, ordnen Sie optional ein Sicherheitsgruppen-Tag zu, und klicken Sie auf Bereitstellen. Die SSID wird nur dann von Access Points übertragen, wenn ein Pool zugewiesen ist.



Richten Sie den Wireless LAN Controller auf den Controllern AireOS und Catalyst 9800 nach jeder Änderung der SSID-Konfiguration in den Netzwerkeinstellungen erneut ein.



Anmerkung: Wenn der SSID kein Pool zugewiesen ist, wird davon ausgegangen, dass die Access Points diesen Pool nicht übertragen. Die SSID wird erst übertragen, nachdem ein Pool zugewiesen wurde. Nach der Zuweisung des Pools muss der Controller nicht erneut bereitgestellt werden.

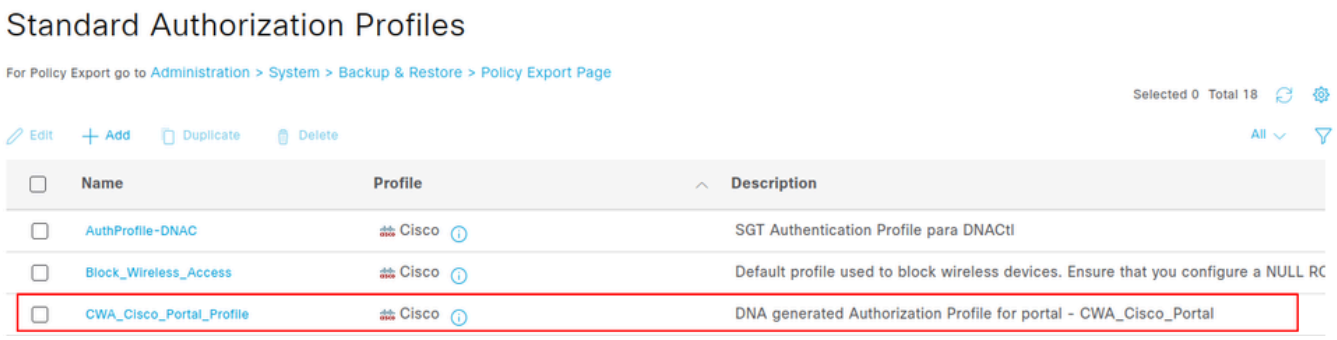
Überprüfen der für die Cisco ISE bereitgestellten Konfiguration

In diesem Abschnitt wird die Konfiguration erläutert, die von Catalyst Center für die Cisco ISE bereitgestellt wird.

Autorisierungsprofil

Teil der Konfiguration, die Catalyst Center auf der Cisco ISE bereitstellt, ist ein Autorisierungsprofil. Dieses Profil definiert das einem Client zugewiesene Ergebnis anhand seiner Parameter und kann spezifische Einstellungen wie VLAN-Zuweisung, ACLs oder URL-Umleitungen enthalten.
Um das Autorisierungsprofil in der ISE anzuzeigen, navigieren Sie zu Richtlinie >

Richtlinienelemente > Ergebnisse. Wenn der Portalname CWA_Cisco_Portal lautet, lautet der Profilname CWA_Cisco_Portal_Profile. Im Beschreibungsfeld wird folgender Text angezeigt: Von DNA generiertes Autorisierungsprofil für das Portal - CWA_Cisco_Portal.



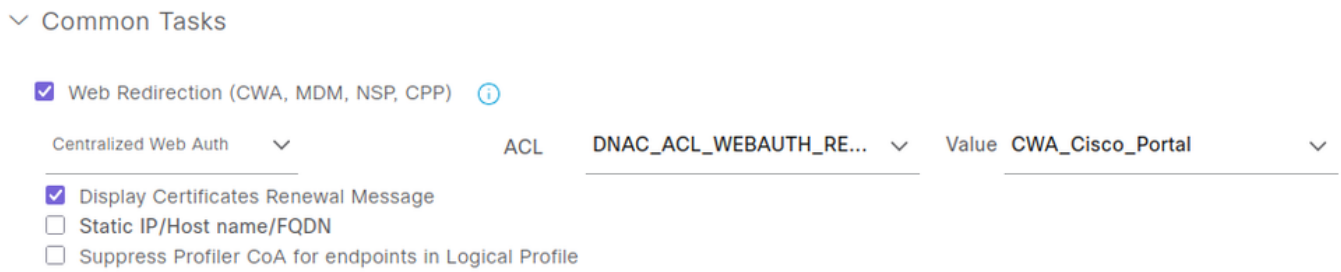
Um die Attribute anzuzeigen, die über dieses Autorisierungsprofil an den Wireless LAN-Controller gesendet wurden, klicken Sie auf den Namen des Autorisierungsprofils, und lesen Sie den Abschnitt Allgemeine Aufgaben.
Dieses Autorisierungsprofil stellt die Umleitungs-ACL und die Umleitungs-URL bereit.

Das Web Redirection-Attribut enthält zwei Parameter:

1. ACL Name (ACL-Name): Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Wert: Bezieht sich auf den Namen des Captive Portals, in diesem Beispiel CWA_Cisco_Portal.

Mit der Option "Zertifizierungserneuerungsmeldung anzeigen" können Sie das Portal für die Verlängerung von Zertifikaten verwenden, die derzeit vom Endpunkt verwendet werden.

Eine weitere Option, Static IP/Host Name/FQDN, ist unter Display Certificates Renewal Message (Zertifizierungserneuerungsnachricht anzeigen) verfügbar. Diese Funktion ermöglicht die Übermittlung der IP-Adresse des Portals anstelle des FQDN. Dies ist nützlich, wenn das Captive Portal aufgrund der Unfähigkeit, den DNS-Server zu erreichen, nicht geladen werden kann.

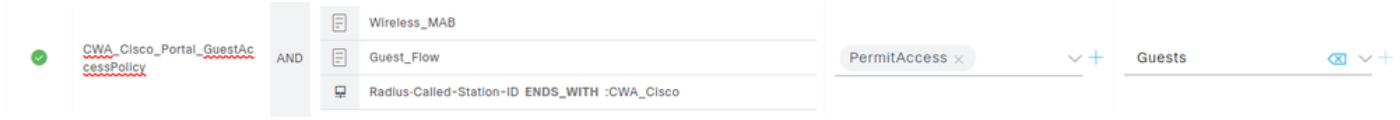


Policy Sets

Navigieren Sie zu Policy > Policy Sets > Default > Authorization Policy, um die beiden für das Portal CWA_Cisco_Portal erstellten Policy Sets anzuzeigen. Diese Policy Sets sind:

- CWA_Cisco_Portal_GastZugangsrichtlinie
- CWA_Cisco_Portal_RedirectPolicy

Die Richtlinie CWA_Cisco_Portal_GuestAccessPolicy wird angewendet, wenn der Client den Webauthentifizierungsprozess bereits abgeschlossen hat, entweder durch Selbstregistrierung oder über das Hotspot-Portal.

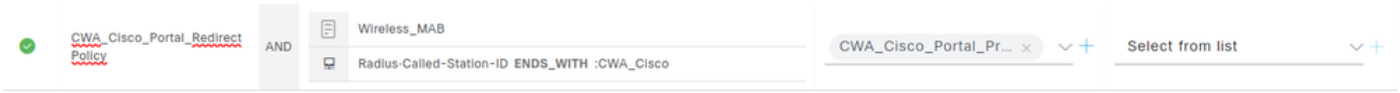


Dieser Richtliniensatz erfüllt drei Kriterien:

- Wireless_MAB: Wird verwendet, wenn die Cisco ISE eine MAC Authentication Bypass (MAB)-Authentifizierungsanforderung von einem Wireless LAN Controller empfängt.
- Gast_Fluss: Verweist auf die ISE-Prüfung der MAC-Adresse des Endpunkts anhand der Identitätsgruppe GuestEndpoints. Wenn die Endpunkt-MAC-Adresse in dieser Gruppe nicht vorhanden ist, wird die Richtlinie nicht angewendet.
- RADIUS Called Station-ID ENDS_WITH :CWA_Cisco: Die Called-Station-ID ist ein RADIUS-Attribut in der ISE, das die Bridge- oder Access Point-MAC-Adresse im ASCII-Format speichert und die SSID anhängt, auf die zugegriffen wird, getrennt durch ein Semikolon (:). In diesem Beispiel stellt CWA_Cisco den SSID-Namen dar.

Unter den Spaltenprofilen sehen Sie den Namen PermitAccess. Dies ist ein reserviertes Autorisierungsprofil, das nicht bearbeitet werden kann, das vollständigen Zugriff auf das Netzwerk bietet, und Sie können auch ein SGT unter der Spalte Security Groups zuweisen, in diesem Fall Guests.

Das PermitAccess-Profil wird verwendet. Hierbei handelt es sich um ein reserviertes Autorisierungsprofil, das nicht bearbeitet werden kann und das vollständigen Zugriff auf das Netzwerk gewährt. Ein SGT kann auch in der Spalte Security Groups (Sicherheitsgruppen) zugewiesen werden. In diesem Fall ist die SGT auf "Gäste" gesetzt.
Die nächste zu überprüfende Richtlinie ist CWA_Cisco_Portal_RedirectPolicy.



Dieser Richtliniensatz erfüllt die folgenden beiden Kriterien:

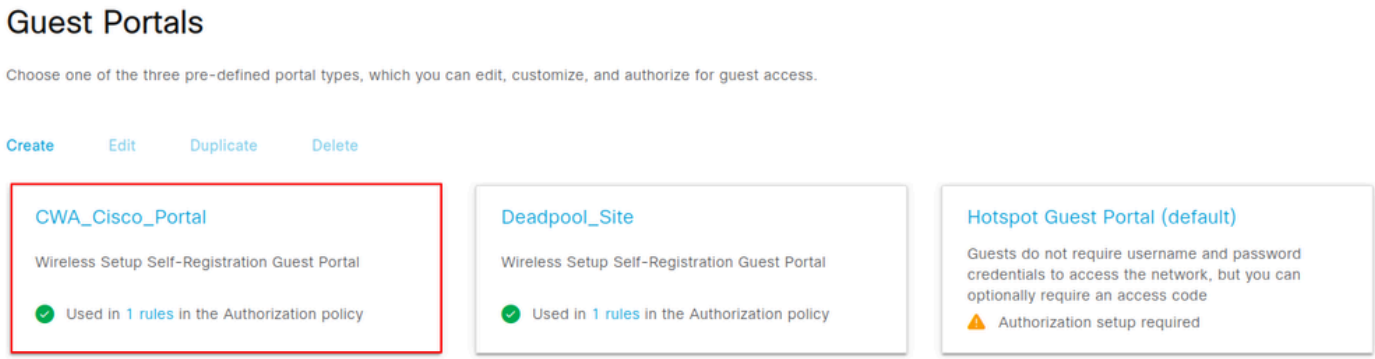
- Wireless_MAB: Wird verwendet, wenn die Cisco ISE eine MAB-Authentifizierungsanforderung von einem Wireless LAN Controller empfängt.
- RADIUS Called Station-ID ENDS_WITH :CWA_Cisco: Die Called-Station-ID ist ein RADIUS-Attribut in der ISE, das die Bridge- oder Access Point-MAC-Adresse im ASCII-Format speichert und die SSID anhängt, auf die zugegriffen wird, getrennt durch ein Semikolon (:). In diesem Beispiel stellt :CWA_Cisco den SSID-Namen dar.

Die Reihenfolge dieser Richtlinien ist von entscheidender Bedeutung. Wenn

CWA_Cisco_Portal_RedirectPolicy in der Liste an erster Stelle steht, werden nur die MAB-Authentifizierung und der SSID-Name mit dem RADIUS-Attribut Called-Station-ID ENDS_WITH :CWA_Training abgeglichen. Selbst wenn sich der Endpunkt in dieser Konfiguration bereits über das Portal authentifiziert hat, wird die Übereinstimmung mit dieser Richtlinie unbegrenzt beibehalten. Daher wird nie über das PermitAccess-Profil vollständiger Zugriff gewährt, und der Client bleibt in einer kontinuierlichen Schleife aus Authentifizierung und Umleitung zum Portal stecken.

Gastportalkonfiguration

Navigieren Sie zu Work Centers > Guest Access > Portals & Components, um das Portal anzuzeigen.
Das hier erstellte Gastportal verwendet den gleichen Namen wie das Catalyst Center CWA_Cisco_Portal. Wählen Sie den Portalnamen für aus, wenn Sie weitere Details anzeigen möchten.

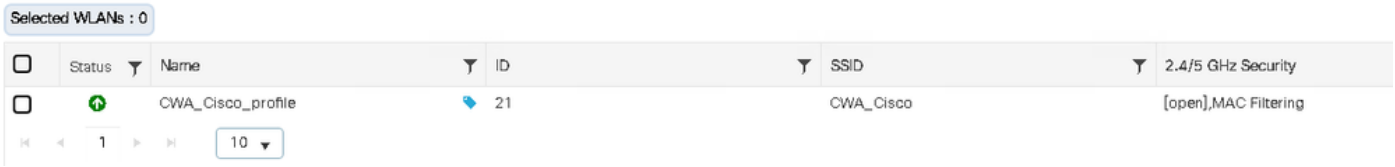


Überprüfen der für den WLC bereitgestellten Konfiguration

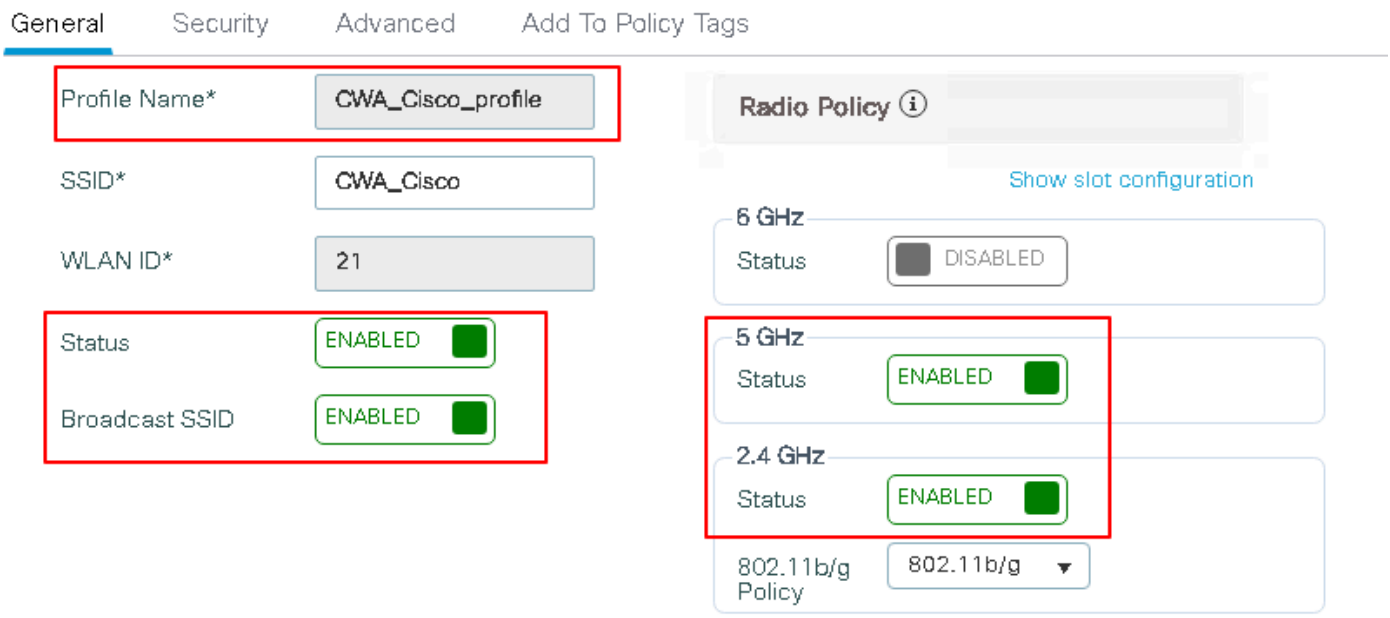
In diesem Abschnitt wird die vom Catalyst Center für den Wireless LAN Controller bereitgestellte Konfiguration beschrieben.

SSID-Konfiguration

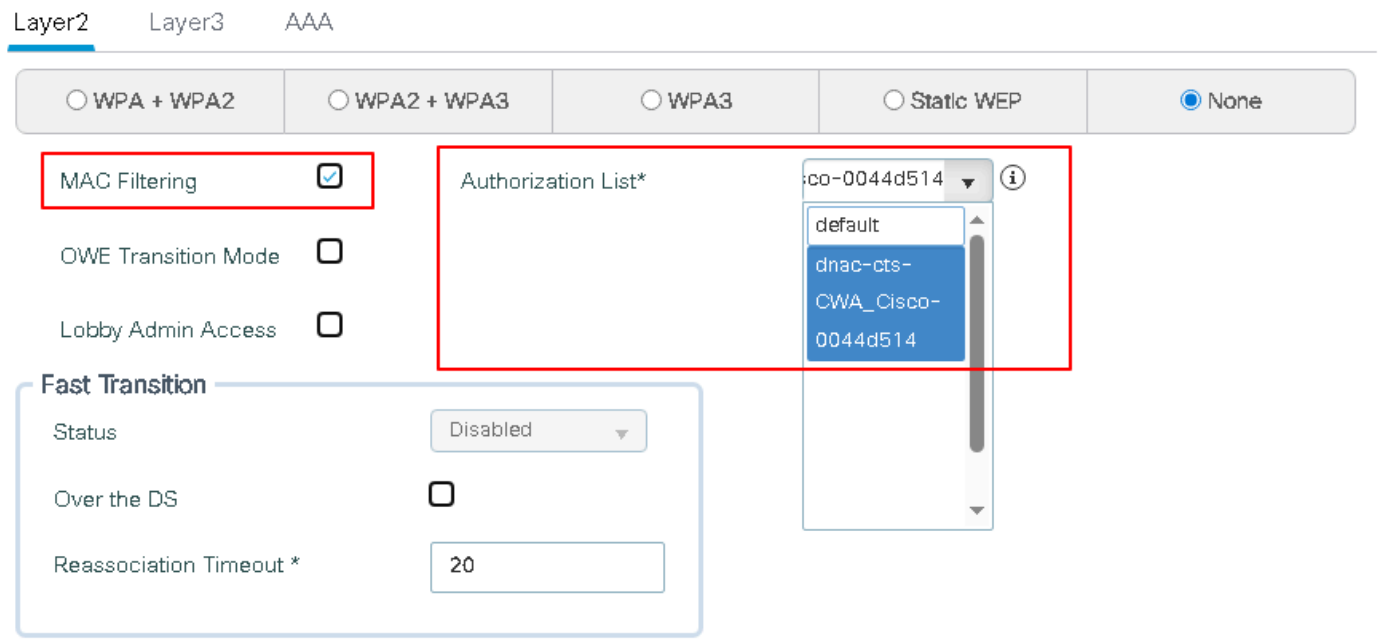
Navigieren Sie in der WLC-GUI zu Configuration > Tags & Profiles > WLANs, um die SSID-Konfiguration anzuzeigen.



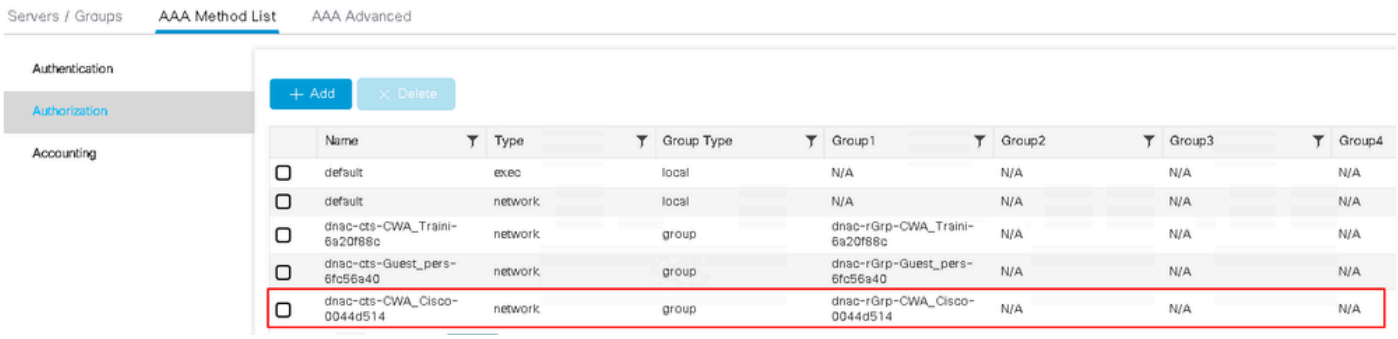
Die SSID "CWA_Cisco" trägt den Namen "CWA_Cisco_profile" auf dem WLC, mit der ID 21 und einem offenen Sicherheitstyp mit MAC-Filterung. Doppelklicken Sie auf die SSID, um deren Konfiguration anzuzeigen.



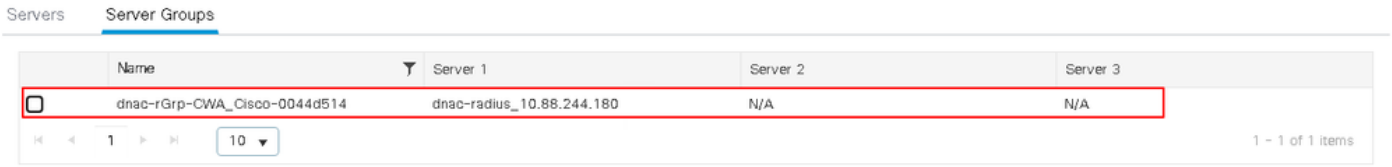
Die SSID ist aktiv und sendet auf 5-GHz- und 2,4-GHz-Kanälen. Sie ist mit dem Richtlinienprofil "CWA_CIsco_Profile" verbunden. Klicken Sie auf die Registerkarte Sicherheit, um die Einstellungen anzuzeigen.



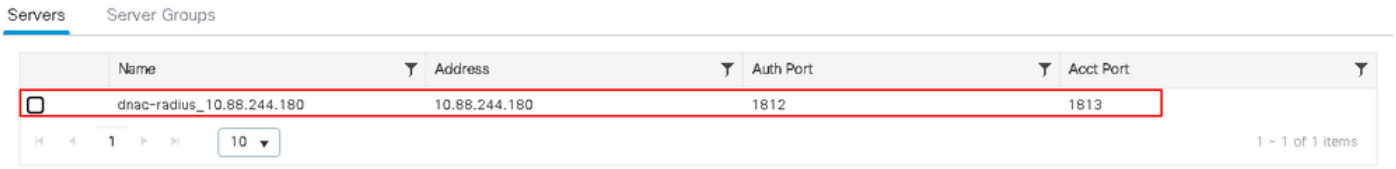
Zu den wichtigsten Einstellungen gehören die Layer-2-Sicherheitsmethode (MAC-Filterung) und die AAA-Autorisierungsliste (Cisco DNA-cts-CWA_Cisco-0044d514). Um die Konfiguration zu überprüfen, navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authorization.



Die Methodenliste verweist auf die RADIUS-Gruppe Cisco DNA-Grp-CWA_Cisco-0044d514in der Spalte Group1. Um die zugehörige Konfiguration anzuzeigen, navigieren Sie zu Configuration > Security > AAA > Server/Groups > Server Groups.



Die Servergruppe Cisco DNA-Grp-CWA_Cisco-0044d514 verweist in der Spalte Server 1 auf Cisco DNA-radius_10.88.244.180. Zeigen Sie seine Konfiguration auf der Registerkarte Server an.



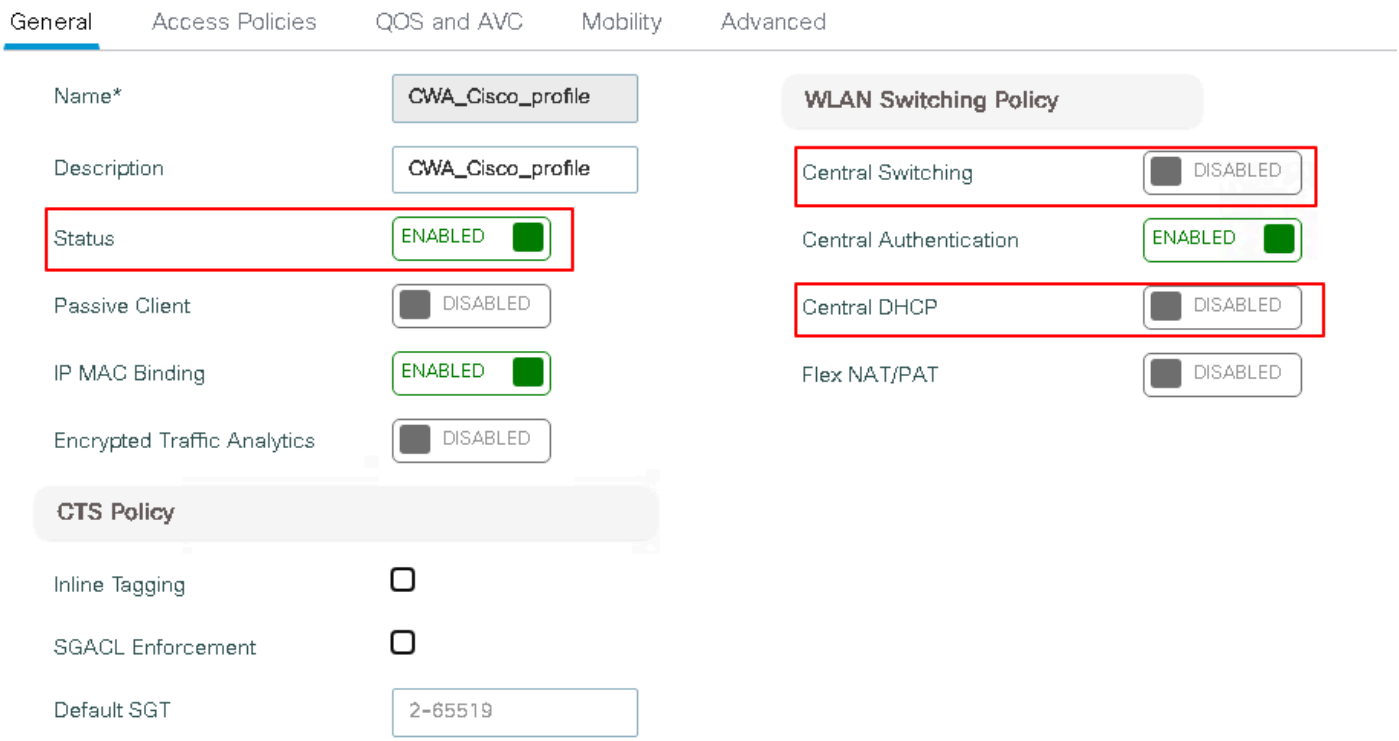
Der Server Cisco DNA-radius_10.88.244.180 hat die IP-Adresse 10.88.244.180, Klicken Sie auf seinen Namen, um die Konfiguration anzuzeigen

Eine wichtige Konfiguration ist die Autorisierungsänderung (CoA), die einen Mechanismus zum Ändern der Attribute einer AAA-Sitzung (Authentication, Authorization, and Accounting) bereitstellt, nachdem diese im Captive Portal authentifiziert wurde. Ohne diese Funktion befindet sich der Endpunkt auch nach Abschluss der Registrierung im Portal weiterhin im ausstehenden Zustand der Webauthentifizierung.

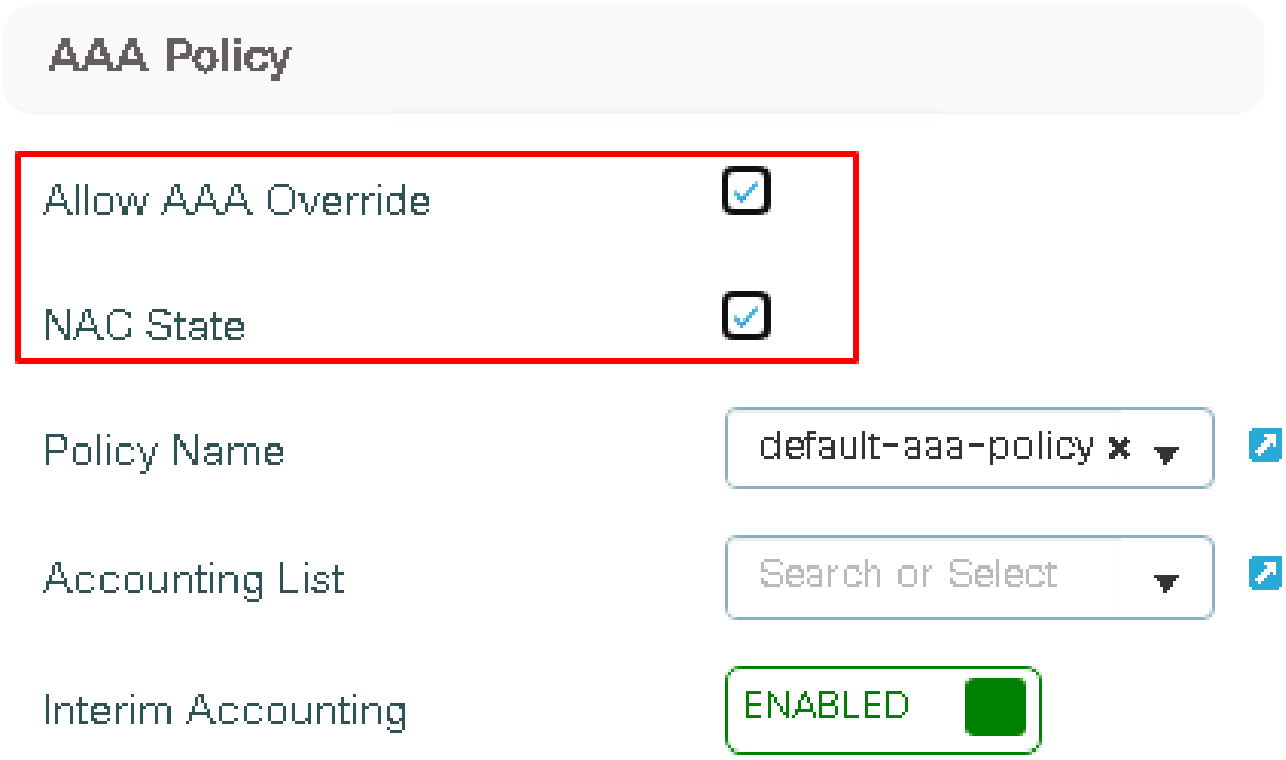
Konfiguration des Wireless-Richtlinienprofils

Innerhalb des Richtlinienprofils können den Clients Einstellungen wie VLAN, ACLs, QoS, Mobility Anchor und Timer zugewiesen werden. Um die Konfiguration für das Richtlinienprofil anzuzeigen, navigieren Sie zu Configuration > Tags & Profiles > Policy.

Klicken Sie auf den Richtliniennamen, um die Konfiguration anzuzeigen.



Der Richtlinienstatus lautet "Aktiviert", und wie bei jeder Fabric-SSID sind "Zentrales Switching" und "Zentrales DHCP" deaktiviert. Klicken Sie auf die Registerkarte "Erweitert" und navigieren Sie dann zum Abschnitt "AAA-Richtlinie", um weitere Konfigurationsdetails anzuzeigen.



Sowohl AAA Override als auch Network Access Control (NAC) können aktiviert werden. Mit AAA Override kann der Controller vom RADIUS-Server zurückgegebene Attribute wie ACLs oder URLs akzeptieren und diese Attribute auf Clients anwenden. NAC aktiviert die Autorisierungsänderung (Change of Authorization, CoA), nachdem sich der Client im Portal registriert hat.
Diese Konfiguration kann auch über die CLI des WLC angezeigt werden.
Um das Richtlinienprofil zu überprüfen, wird die SSID mit dem folgenden Befehl verbunden:

<#root>

WLC#show fabric wlan summary

```
Number of Fabric wlan : 1

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

CWA_Cisco_profile

```
  CWA_Cisco  UP
```

Führen Sie den folgenden Befehl aus, um die Konfiguration für das Richtlinienprofil "CWA_Cisco_profile" anzuzeigen:

<#root>

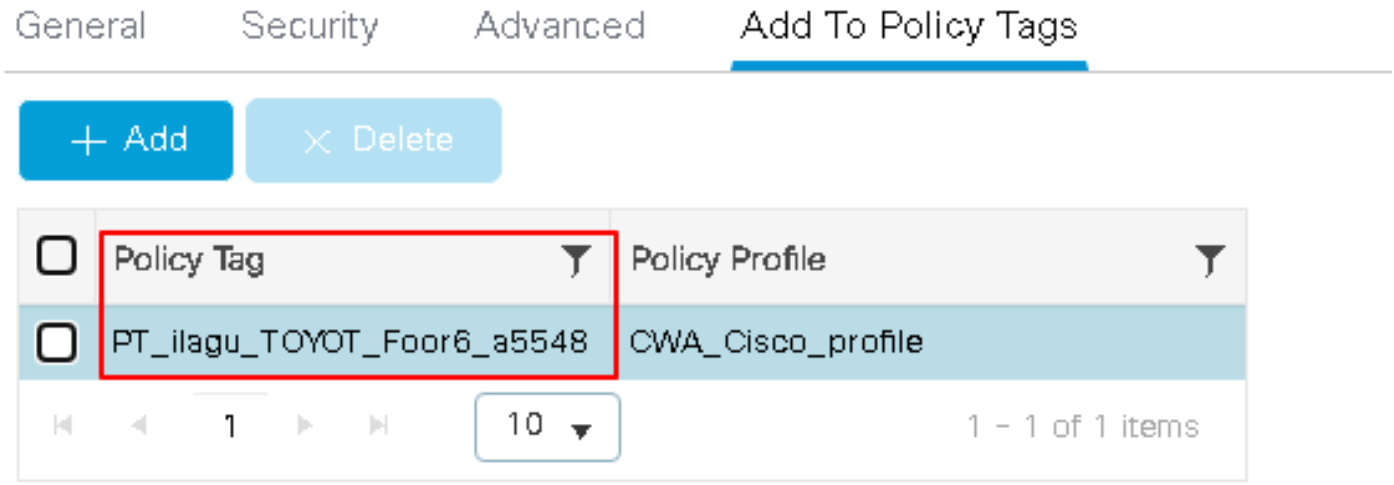
WLC#show running-config | section policy CWA_Cisco_profile

```
wireless profile policy CWA_Cisco_profile
```

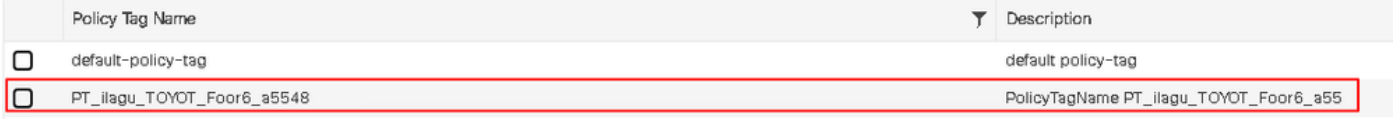
```
aaa-override


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
```

Richtlinien-Tag-Konfiguration

Mit dem Policy-Tag verknüpfen Sie das WLAN mit dem Richtlinienprofil, navigieren zu Konfiguration > Tags & Profile > WLANs, klicken auf den WLAN-Namen und navigieren zu Zu Policy-Tags hinzufügen, um das dem SSID zugewiesene Policy-Tag zu identifizieren.

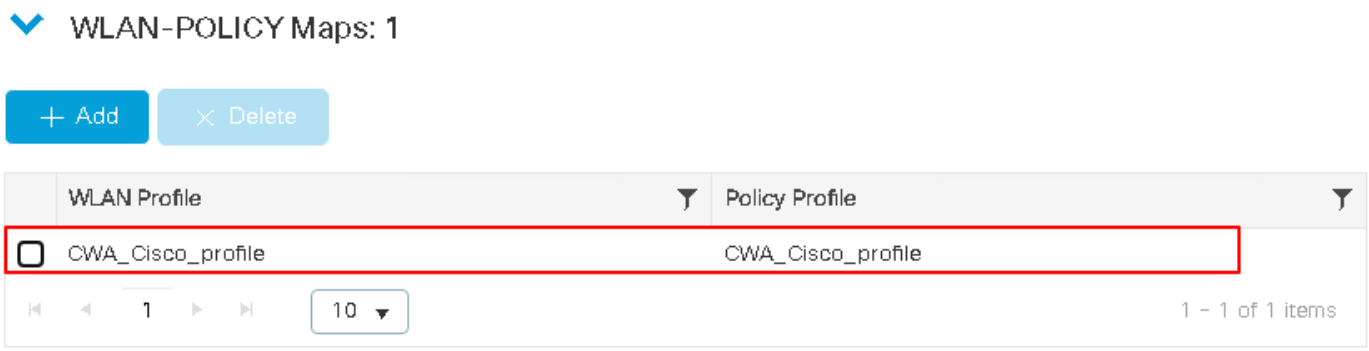


Für die SSID CWA_Cisco_profile wird das Richtlinientag PT_ilagu_TOYOT_For6_a5548 verwendet, um diese Konfiguration zu überprüfen. Navigieren Sie dazu zu Konfiguration > Tags & Profile > Tags > Richtlinie.



Klicken Sie auf den Namen, um die zugehörigen Details anzuzeigen. Das Policy-Tag PT_ilagu_TOYOT_For6_a5548 verbindet das WLAN CWA_Cisco, das dem Namen

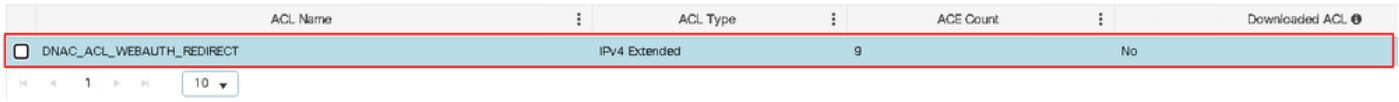
CWA_Cisco_profile auf dem WLC zugeordnet ist (siehe Seite "WLANs"), mit dem Policy Profile CWA_Cisco_profile.



Der WLAN-Name CWA_Cisco_profile verweist auf das WLAN CWA_Cisco.

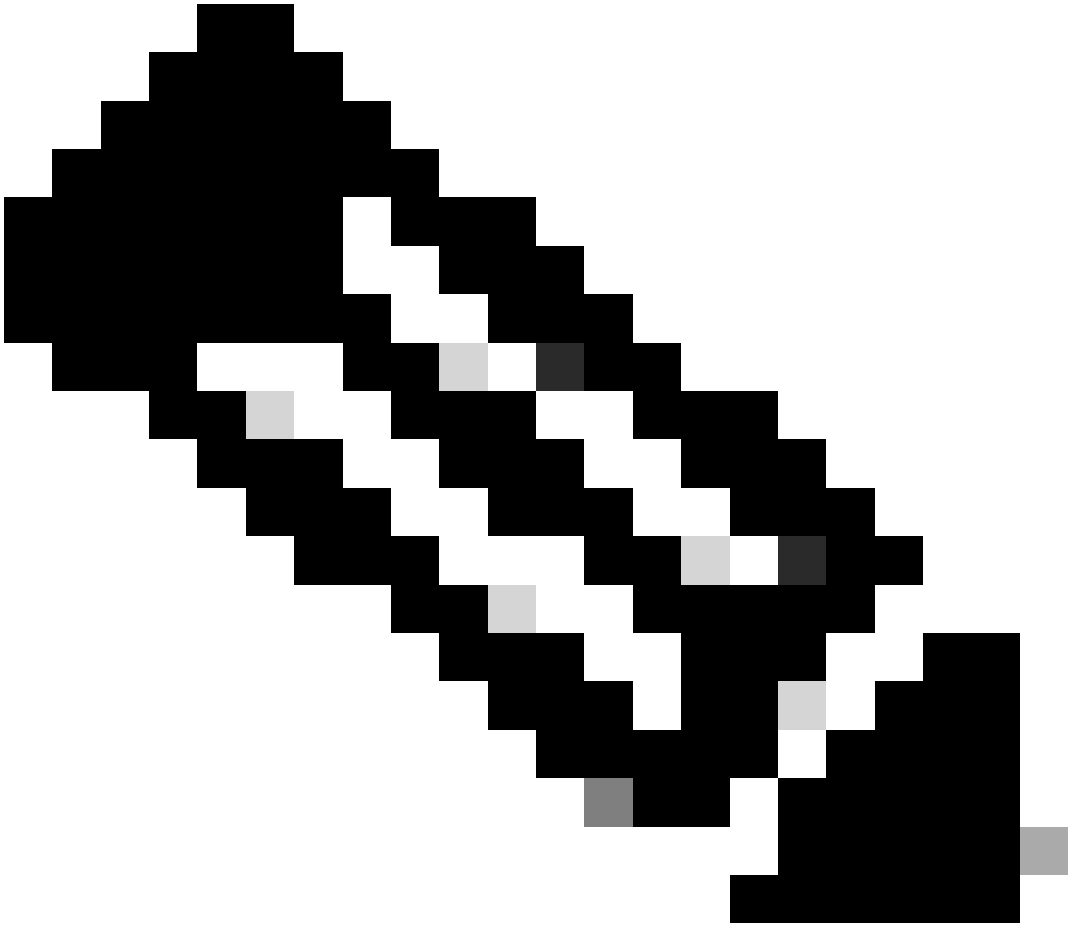
Umleiten der ACL-Konfiguration

In CWA definiert eine Redirect Access Control List (ACL), welcher Datenverkehr zur weiteren Verarbeitung an den WLC umgeleitet wird und welcher Datenverkehr die Umleitung umgeht Diese Konfiguration wird an den WLC weitergeleitet, nachdem die SSID erstellt und der WLC aus dem Bestand bereitgestellt wurde. Um sie anzuzeigen, navigieren Sie zu Configuration > Security >ACL (Konfiguration > Sicherheit >Zugriffskontrollliste). Der Name der Zugriffskontrollliste, die Catalyst Center für die Umleitungszugriffskontrollliste verwendet, lautet Cisco DNA_ACL_WEBAUTH_REDIRECT.



Klicken Sie auf den Namen, um die Konfiguration anzuzeigen. Die Werte werden aus den Netzwerkeinstellungen der Netzwerkeinstellungen des Catalyst Center-Standorts abgeleitet.

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



Anmerkung: Diese Werte stammen aus den Netzwerkeinstellungen des Standorts, die in Catalyst Center konfiguriert wurden, und die DHCP-/DNS-Werte stammen aus dem im WLAN konfigurierten Pool. Auf die ISE-PSN-IP-Adresse wird in der AAA-Konfiguration im SSID-Workflow verwiesen.

Führen Sie den folgenden Befehl aus, um die ACL für die Umleitung in der WLC-CLI anzuzeigen:

<#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
```

Die Umleitungs-ACL kann auf das Flex Profile-System angewendet und an die Access Points gesendet werden. Führen Sie diesen Befehl aus, um diese Konfiguration zu bestätigen.

<#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
```

Umleiten der Zugriffskontrollliste auf dem Access Point

Am Access Point werden die Werte für Zulassen und Ablehnen umgekehrt: permit gibt die Weiterleitung des Datenverkehrs an, deny die Umleitung. Führen Sie den folgenden Befehl aus, um die Konfiguration der Umleitungszugriffskontrollliste auf dem Access Point zu überprüfen:

<#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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.