Configuración de la Autenticación Web Central en SD-Access

Contenido

Introducción

Este documento describe una guía paso a paso para configurar la Autenticación web central (CWA) y describe los procedimientos de verificación en todos los componentes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Catalyst Center
- Cisco Identity Services Engine (ISE)
- Arquitectura del controlador inalámbrico Catalyst 9800
- Autenticación, autorización y administración (AAA)

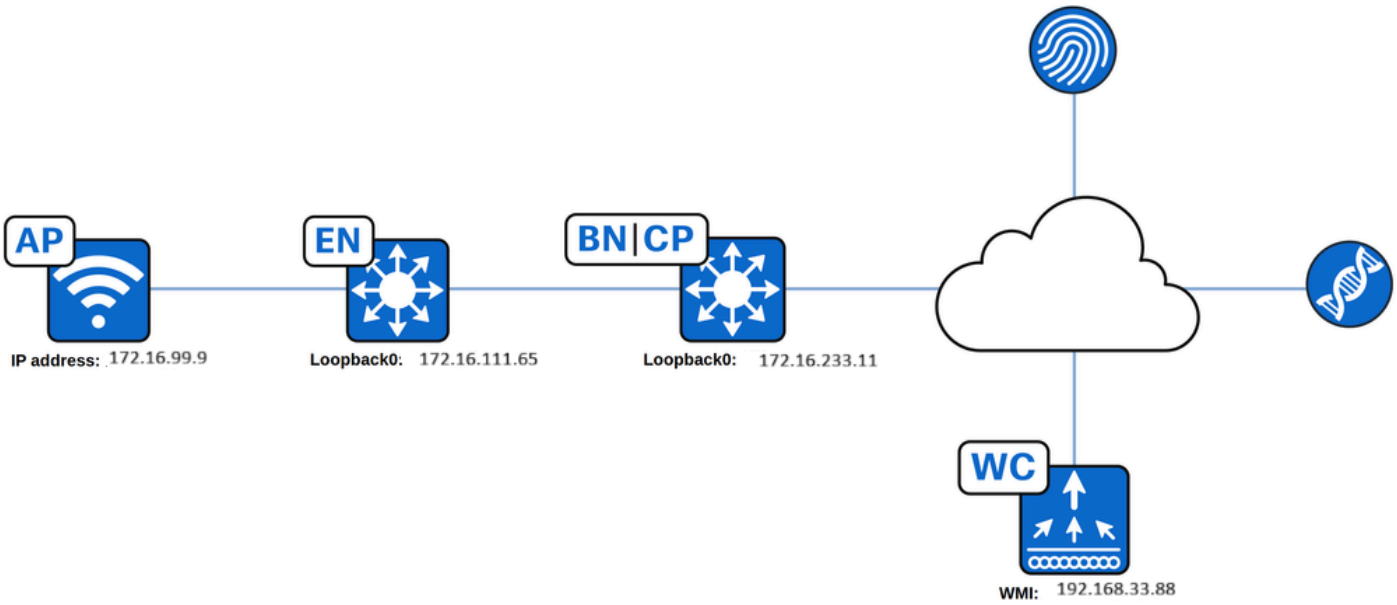
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Wireless LAN Controller (WLC): C9800-CL, Cisco IOS® XE 17.12.04
- Cisco Catalyst Center, versión 2.3.7.7
- Cisco Identity Services Engine (ISE), versión 3.0.0.458
- Nodo perimetral SDA: C9300-48P, Cisco IOS® XE 17.12.05
- Nodo fronterizo SDA/Plano de control: C9500-48P, Cisco IOS® XE17.12.05
- Punto de acceso Cisco - C9130AXI-A, versión 17.9.5.47

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Topología



Overview

La autenticación web central (CWA) utiliza un SSID de tipo invitado para redirigir el navegador web del usuario a un portal cautivo alojado por Cisco ISE, mediante una ACL de redirección configurada. El portal cautivo permite que el usuario se registre y autentique, y después de una autenticación correcta, el controlador de LAN inalámbrica (WLC) aplica la autorización adecuada para conceder acceso completo a la red. Esta guía proporciona instrucciones paso a paso para configurar CWA mediante Cisco Catalyst Center.

Configuración de CWA en Cisco Catalyst Center

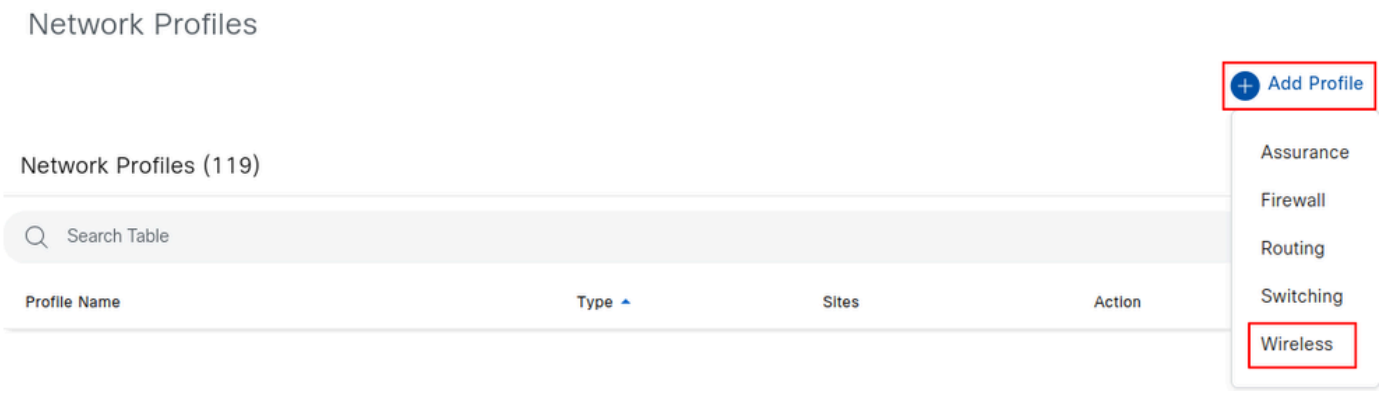
Creación del perfil de red

Un perfil de red permite la configuración de opciones que se pueden aplicar a un sitio específico. Se pueden crear perfiles de red para varios elementos de Cisco Catalyst Center, entre los que se incluyen:

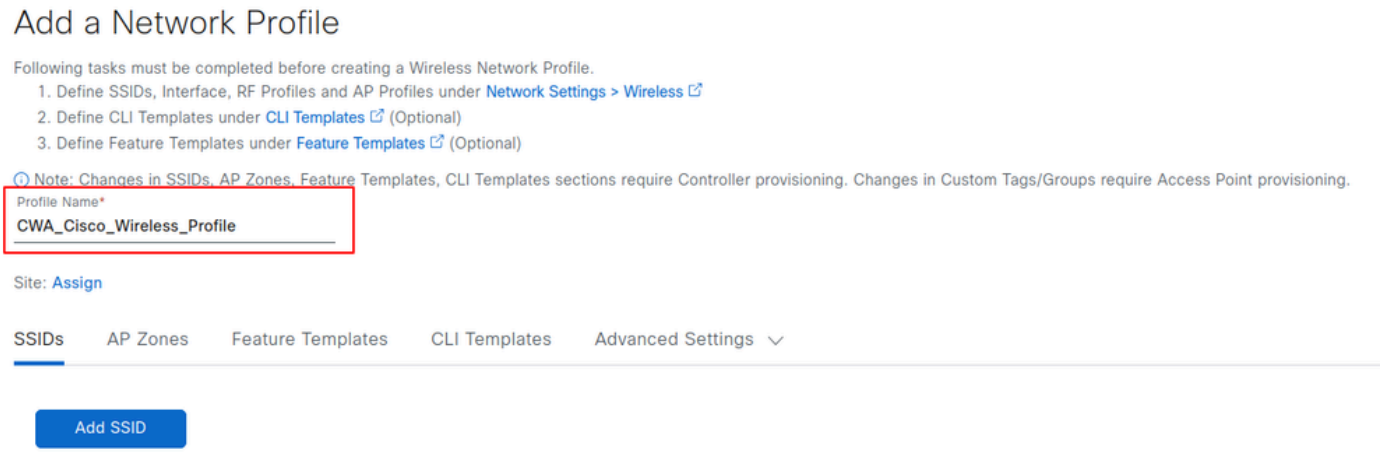
- Garantía
- Firewall
- Ruteo
- Switching
- Dispositivo de telemetría
- Tecnología inalámbrica

Para CWA, se debe configurar un perfil inalámbrico.

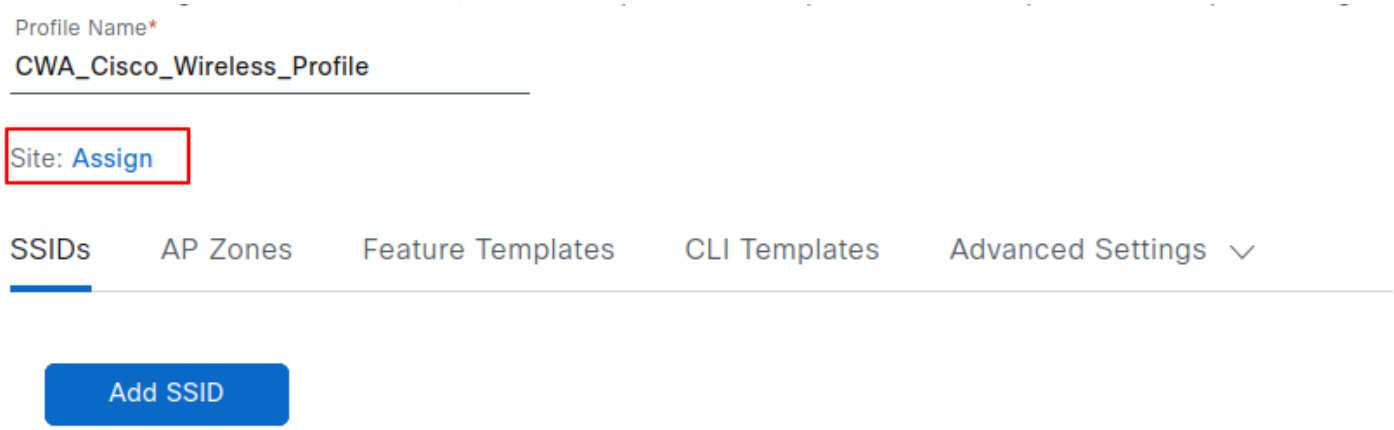
Para configurar un perfil inalámbrico, navegue hasta Diseño > Perfiles de red, haga clic en Agregar perfil y seleccione Inalámbrico.



Asigne al perfil el nombre necesario. En este ejemplo, el perfil inalámbrico se denomina CWA_Cisco_Wireless_Profile. Puede agregar cualquier SSID existente a este perfil seleccionando Add SSID. La creación de SSID se trata en la siguiente sección.

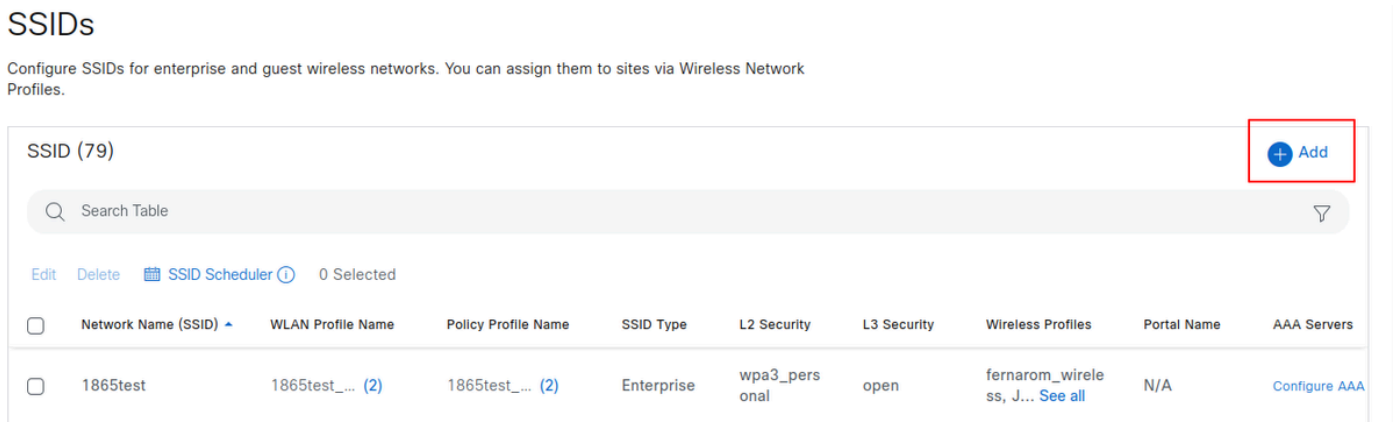


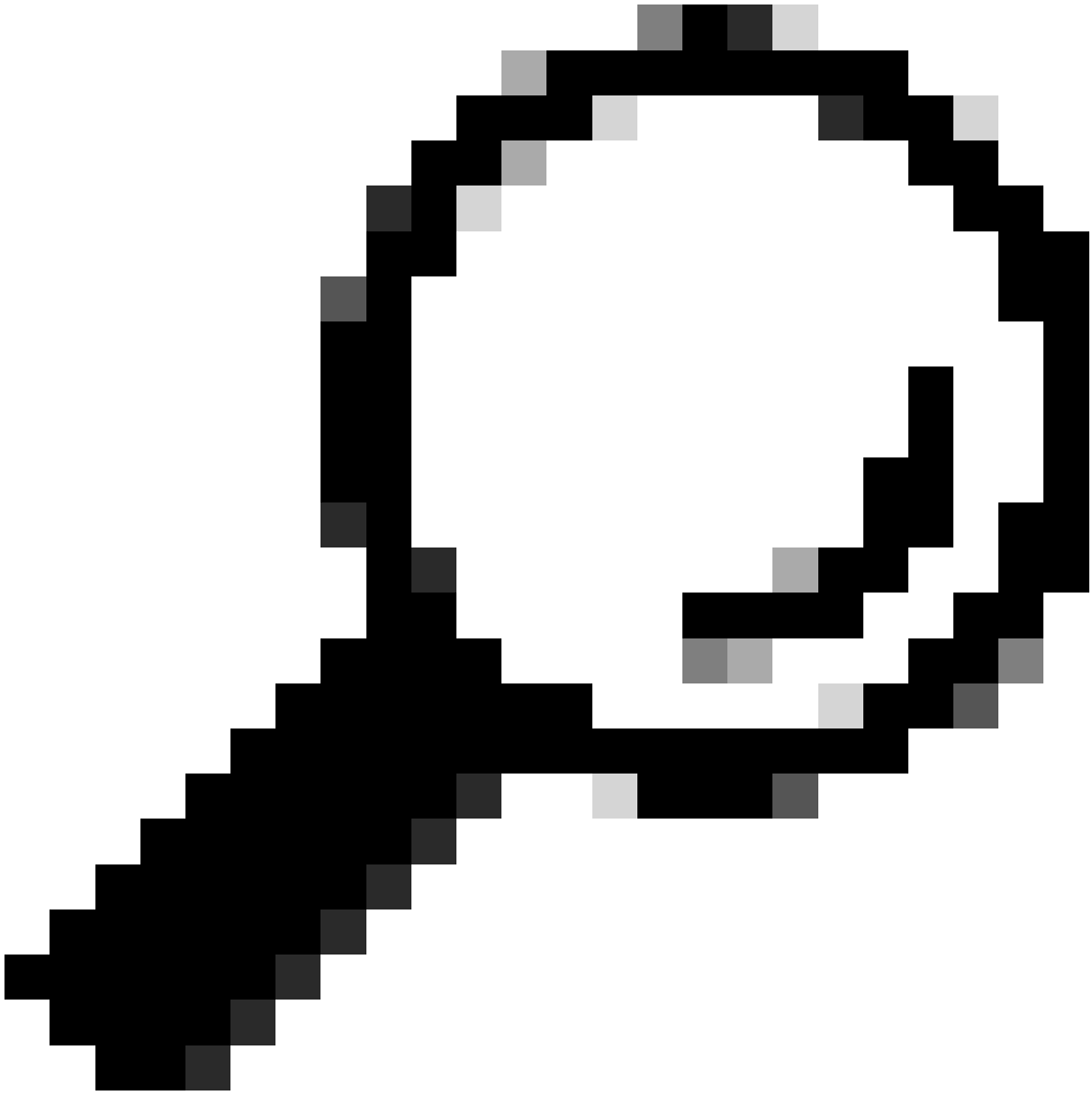
Seleccione Asignar para elegir el sitio en el que se aplicará este perfil y, a continuación, seleccione el sitio deseado. Después de seleccionar los sitios, haga clic en Guardar.



Cree el SSID

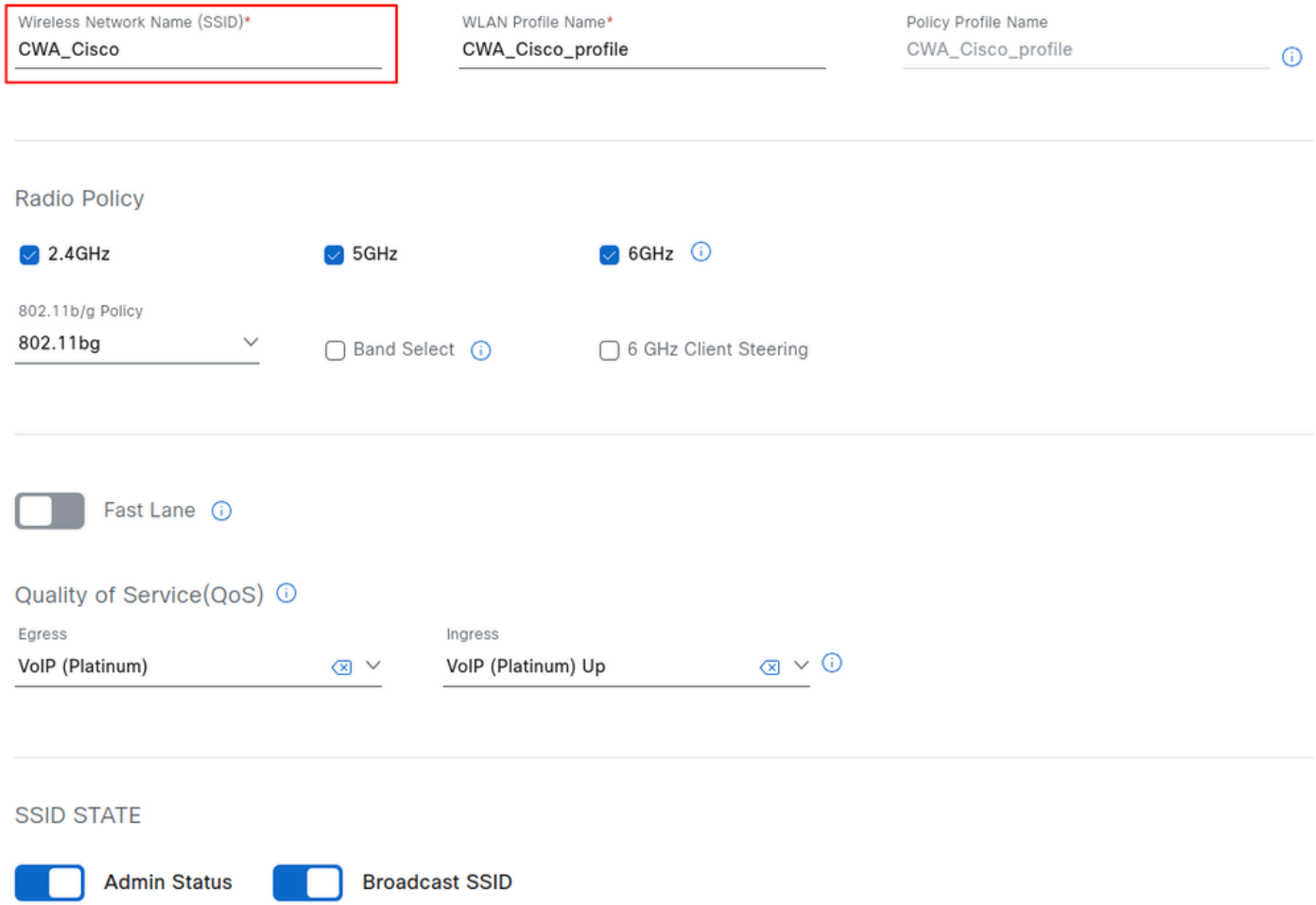
Navegue hasta Diseño > Configuración de red > Inalámbrico > SSIDs y haga clic en Agregar.



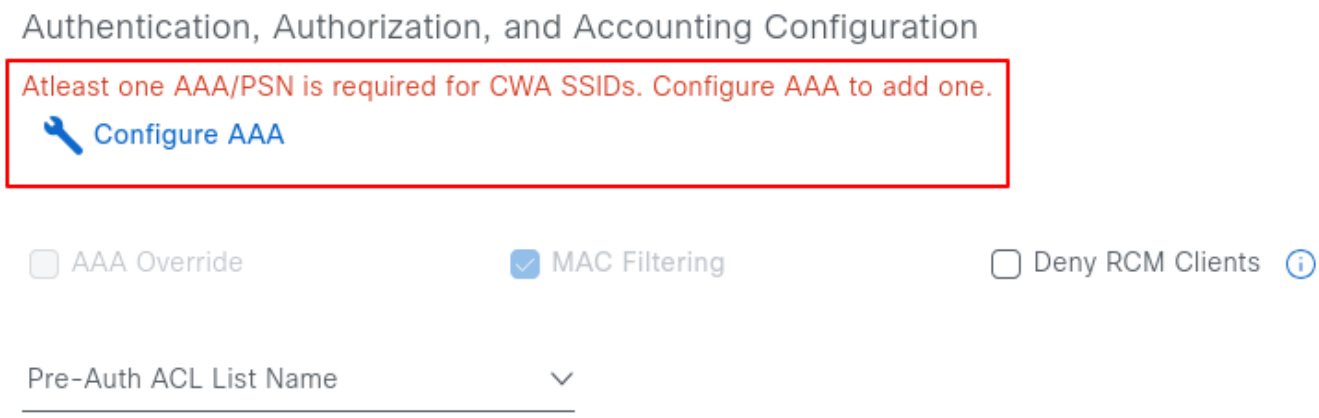


Consejo: Al crear un SSID para CWA, es esencial seleccionar el tipo de invitado. Esta selección agrega un comando al perfil de política inalámbrica del SSID en el WLC - el comando nac - que permite que CoA se utilice para la reautenticación después de que el usuario se registre en el portal cautivo. Sin esta configuración, los usuarios pueden experimentar un bucle infinito de registro y redireccionamiento al portal repetidamente.

Después de seleccionar Add, continúe con el flujo de trabajo de configuración de SSID. En la primera página, configure el nombre SSID, también puede seleccionar la banda de política de radio, y definir el estado SSID, incluyendo el estado administrativo y la configuración de transmisión. Para esta guía de configuración, el SSID se denomina CWA_Cisco.



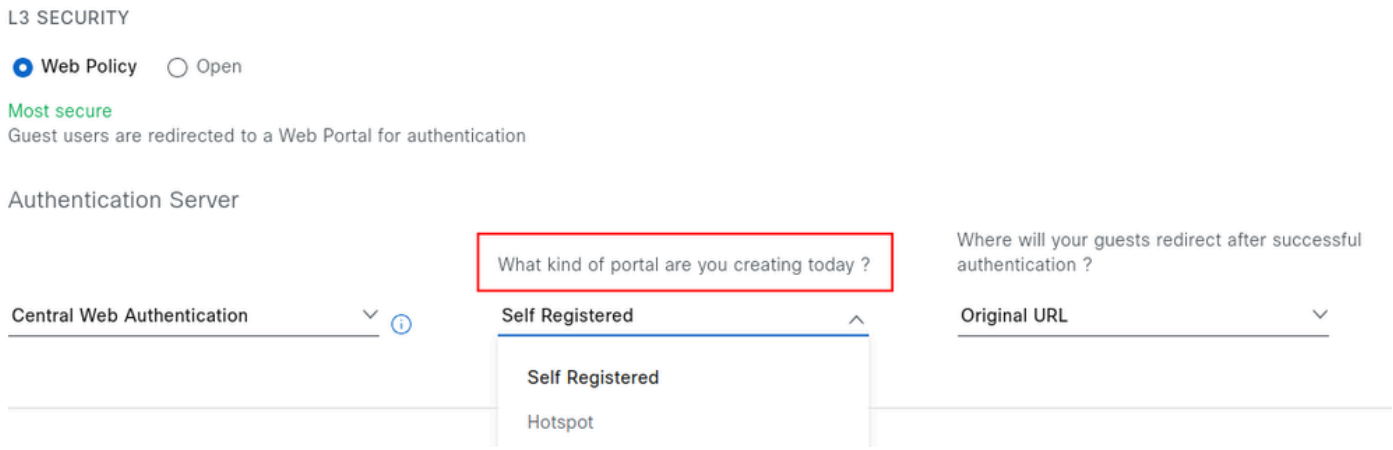
Después de introducir el nombre SSID, el nombre del perfil WLAN y el nombre del perfil de política se generan automáticamente. Seleccione Siguiente para continuar.
Se debe configurar al menos un AAA/PSN para los CWA SSID. Si no se configura ninguna, seleccione Configure AAA y elija la dirección IP PSN en la lista desplegable.



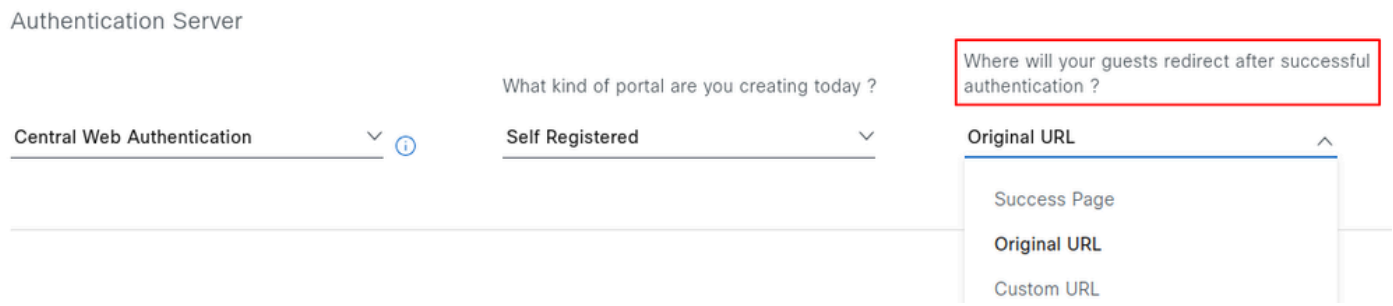
Después de seleccionar el servidor AAA, establezca los parámetros de seguridad de Capa 3 y seleccione el tipo de portal: Registrado automáticamente o zona Wi-Fi pública.

Portales de invitados: Un portal de invitados de zona Wi-Fi proporciona acceso a la red a los invitados sin necesidad de nombres de usuario y contraseñas. En este caso, los usuarios deben aceptar una política de uso aceptable (AUP) para obtener acceso a la red, lo que conduce a un

acceso a Internet posterior. El acceso a través de un portal de invitados con credenciales requiere que los invitados tengan un nombre de usuario y una contraseña.



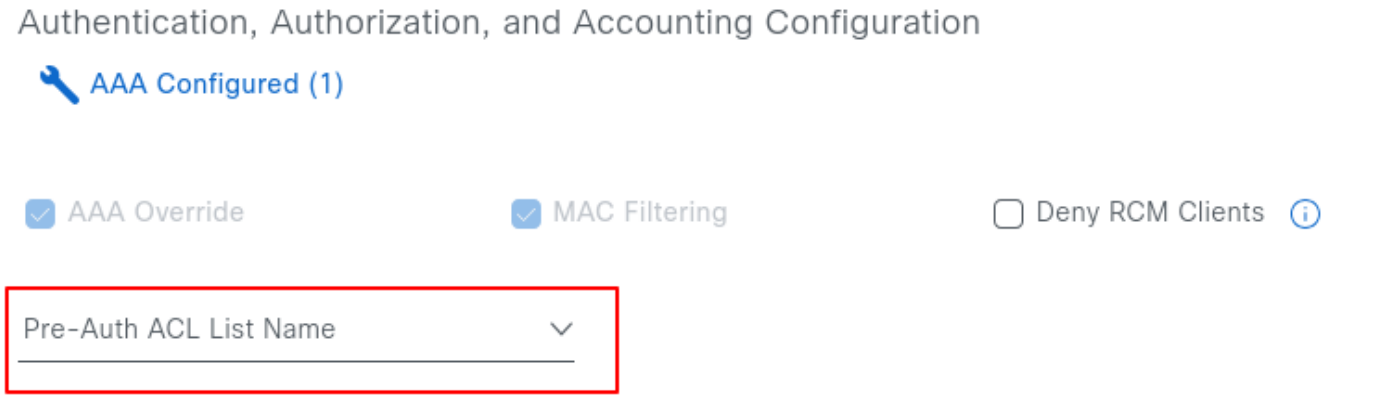
También se puede configurar la acción que se produce después de que el usuario registre o acepte la directiva de uso. Hay tres opciones disponibles: Página de éxito, URL original y URL personalizado.



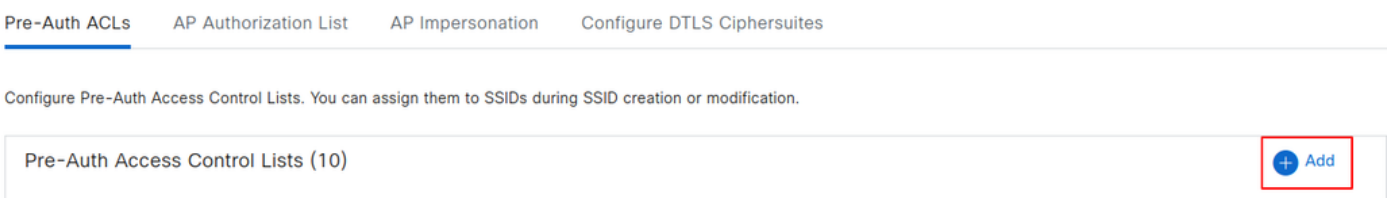
A continuación se describe el comportamiento de cada opción:

Página de éxito: Redirige al usuario a una página de confirmación que indica que la autenticación se ha realizado correctamente.
URL original: redirige al usuario a la URL original solicitada antes de ser interceptada por el portal cautivo.
URL personalizado: redirige al usuario a una URL personalizada especificada. Al seleccionar esta opción, se habilita un campo adicional para definir la dirección URL de destino

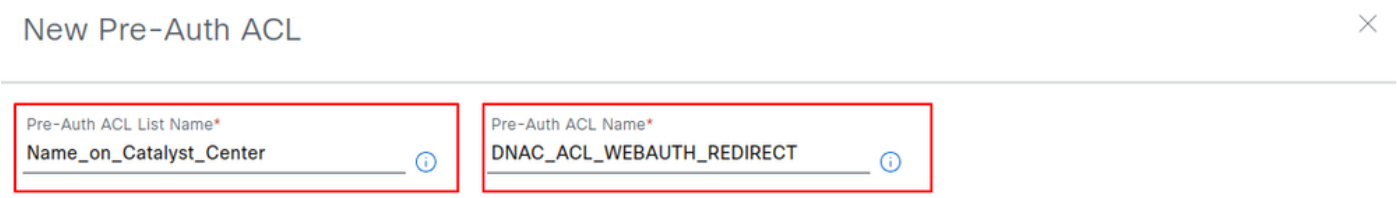
En la misma página, en Autenticación, Autorización y Configuración de Contabilización, también se puede configurar una ACL Pre-auth. Esta ACL permite agregar entradas adicionales para protocolos más allá de las direcciones IP DHCP, DNS o PSN, que se obtienen de la configuración de red y se agregan a la ACL de redirección durante el aprovisionamiento. Esta función está disponible en Cisco Catalyst Center versión 2.3.3.x y posteriores.



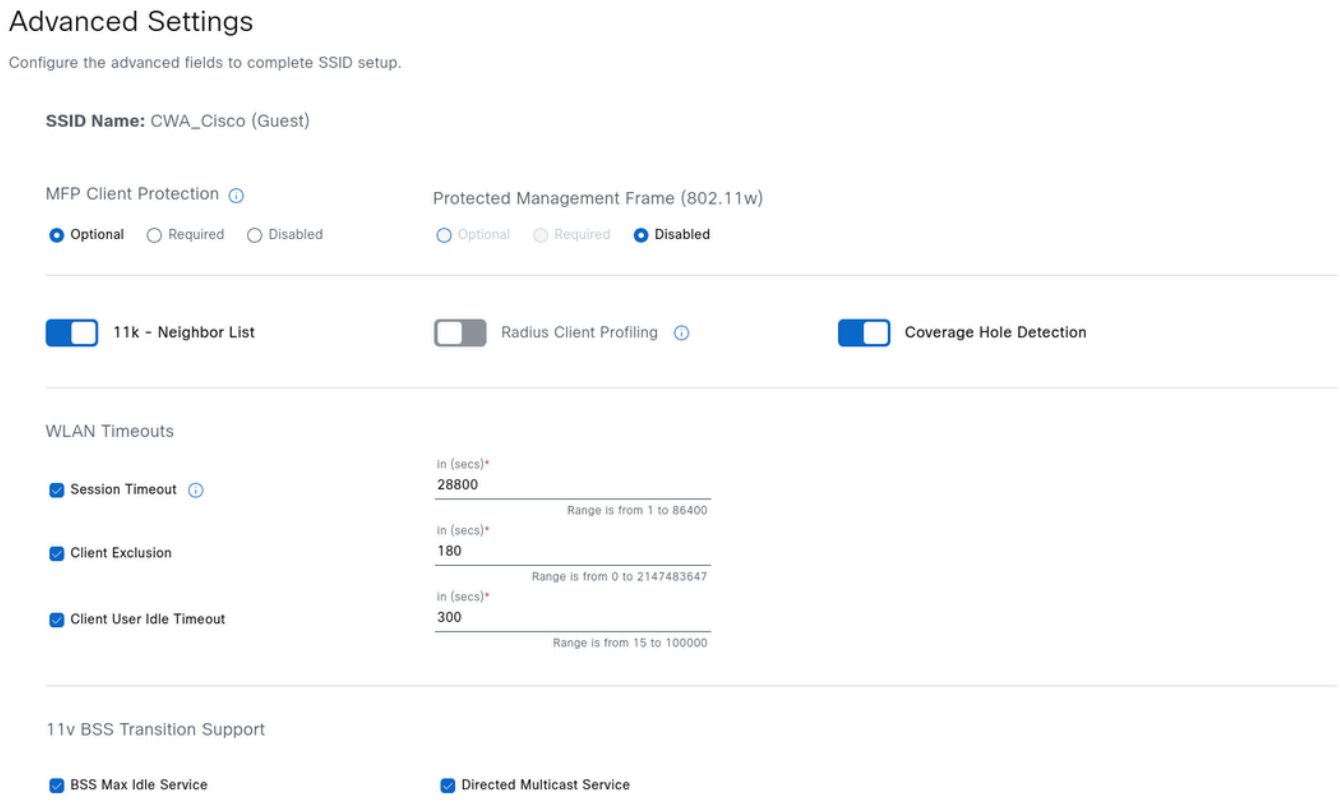
Para configurar una ACL Pre-Auth, navegue hasta Diseño > Configuración de red > Inalámbrico > Configuración de seguridad, y haga clic en Agregar.



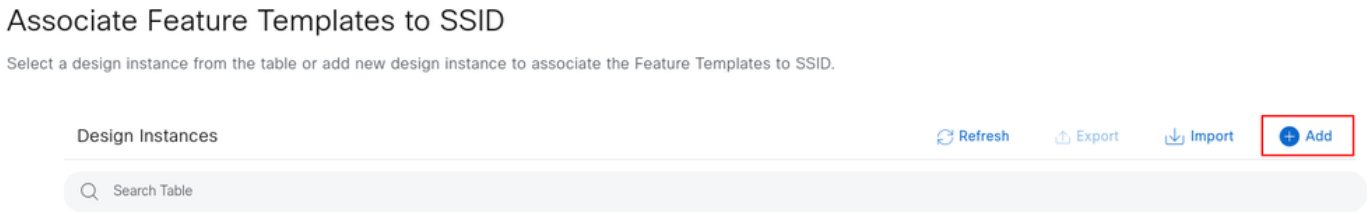
El primer nombre identifica la ACL en el Catalyst Center, mientras que el segundo nombre corresponde al nombre de la ACL en el WLC. El segundo nombre puede coincidir con la ACL de redirección existente configurada en el WLC. Como referencia, Catalyst Center proporciona el nombre Cisco DNA_ACL_WEBAUTH_REDIRECT al WLC. Las entradas de la ACL Pre-Auth se agregan después de las entradas existentes.



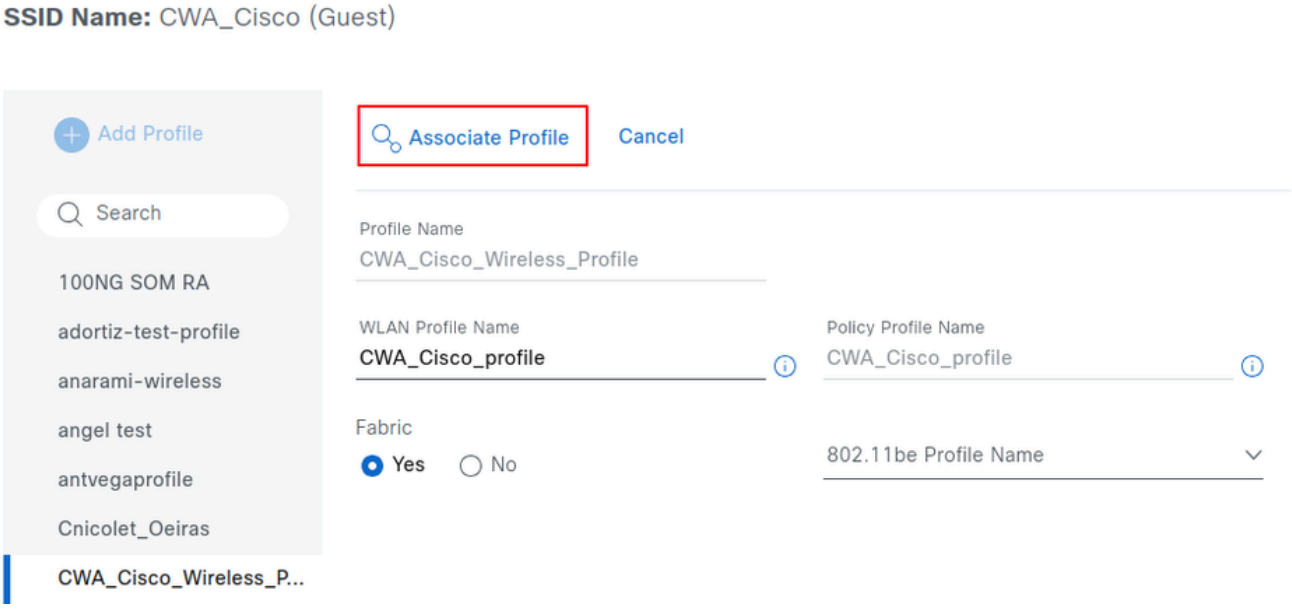
Al volver al flujo de trabajo de creación de SSID, al seleccionar Siguiente se muestran los parámetros avanzados, incluidos la transición rápida, el tiempo de espera de la sesión, el tiempo de espera del usuario cliente y el límite de velocidad. Ajuste los parámetros según sea necesario y, a continuación, seleccione Siguiente para continuar. A efectos de esta guía de configuración, el ejemplo conserva los parámetros predeterminados.



Después de seleccionar Next, aparece un mensaje para asociar cualquier plantilla de función con el SSID. Si procede, seleccione las plantillas que desee haciendo clic en Agregar y, cuando haya terminado, haga clic en Siguiente.

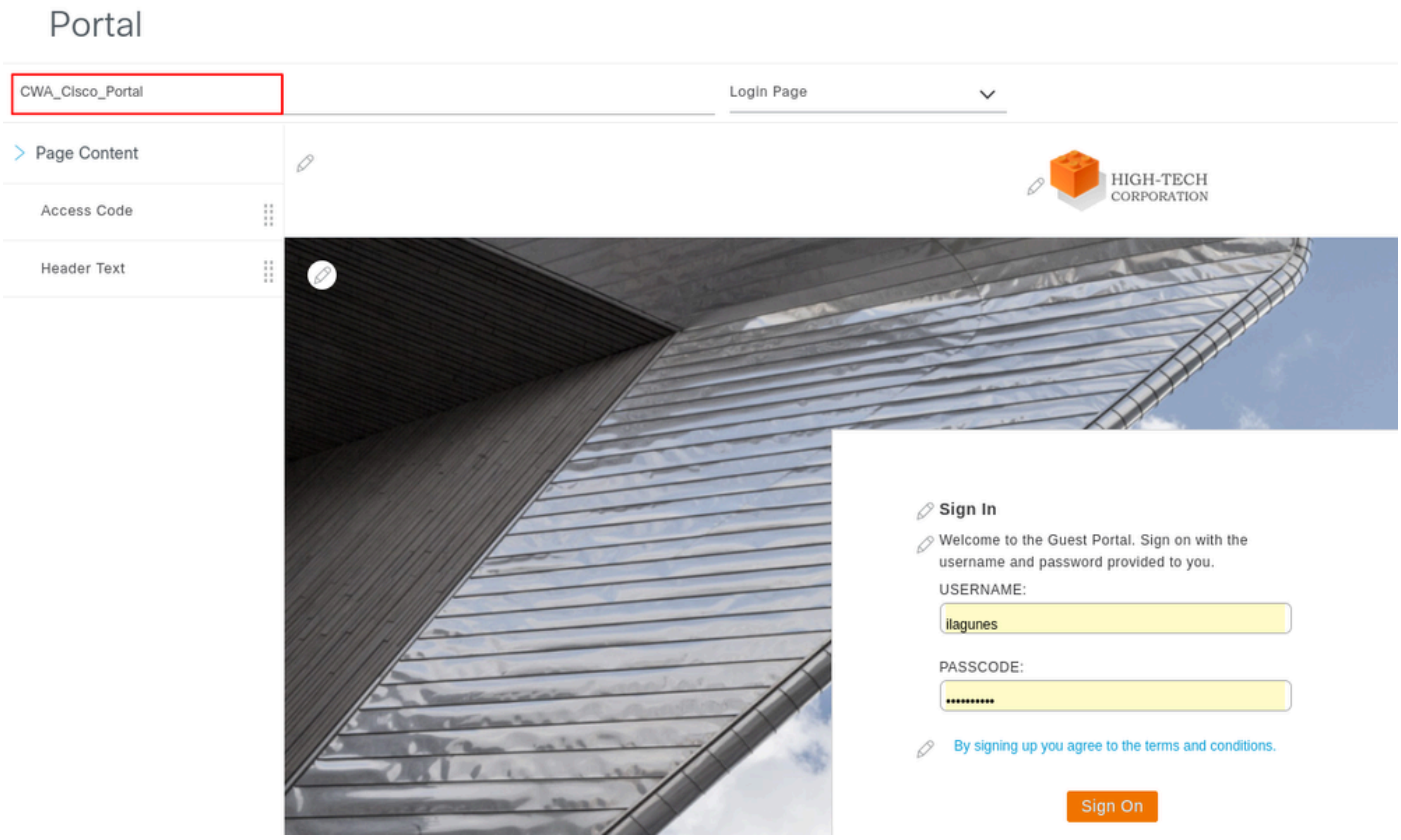


Asocie el SSID al perfil inalámbrico creado anteriormente. Para obtener más información, consulte la sección Creación del perfil de red inalámbrica. En esta sección también puede seleccionar si el SSID está o no habilitado para fabric. Una vez finalizado, haga clic en Asociar perfil.

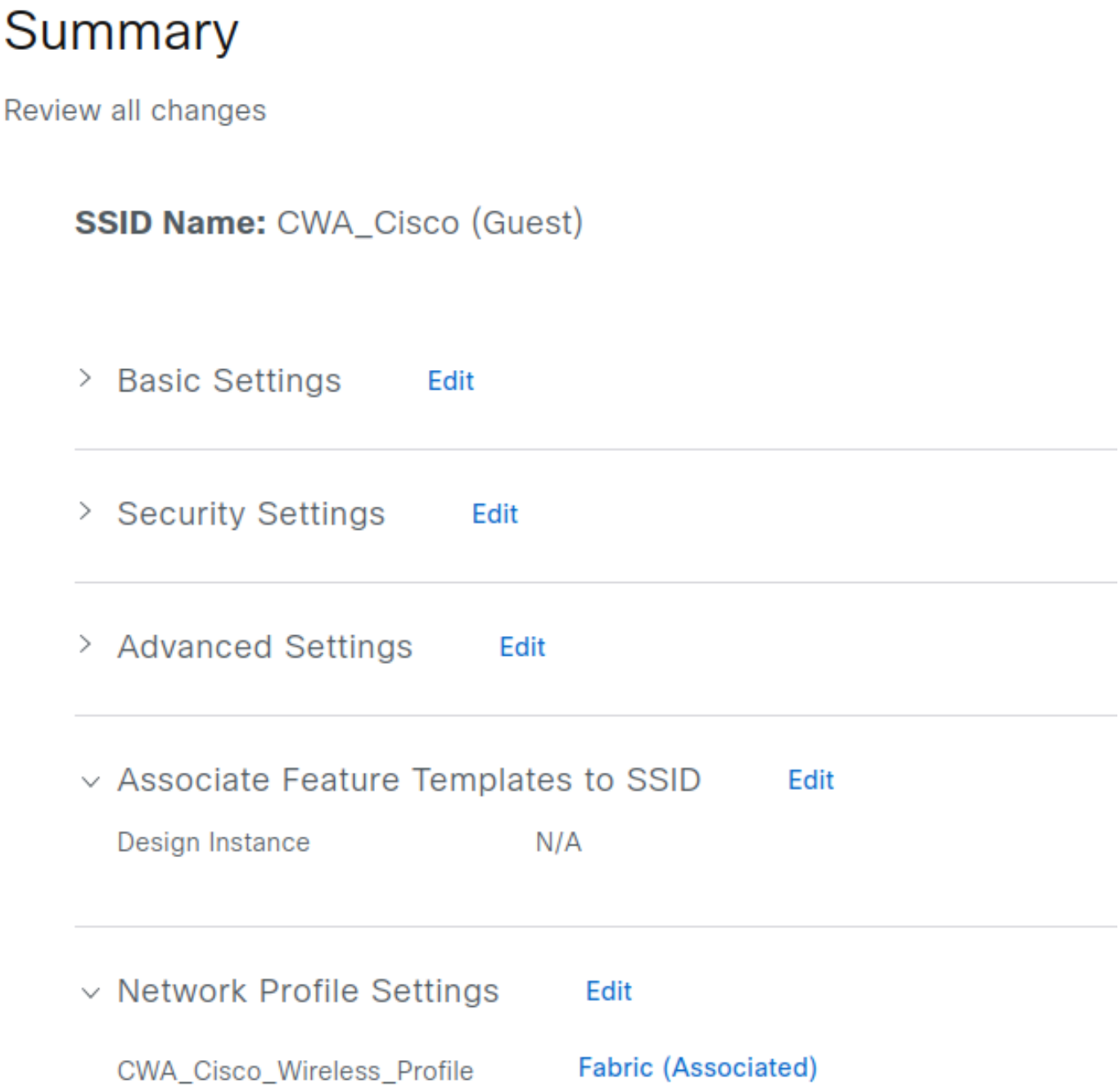


show wireless management trustpoint
Una vez que el perfil esté asociado con el SSID, haga clic en Next para crear y diseñar el portal cautivo; para empezar, haga clic en Create Portal.

El nombre del portal define el nombre de dominio en el FQDN y el nombre del conjunto de políticas en ISE. Haga clic en Guardar cuando termine. El portal sigue siendo editable y se puede eliminar si es necesario.



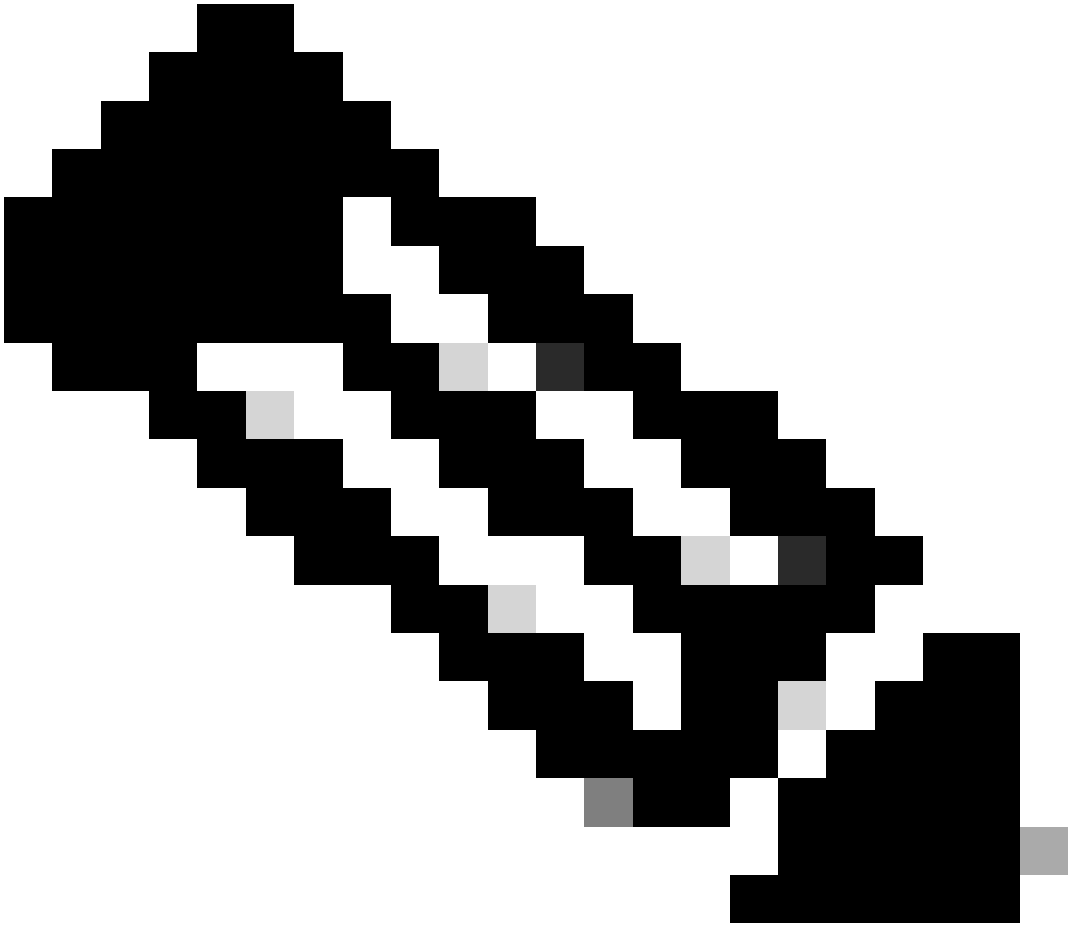
Seleccione Siguiente para mostrar un resumen de todos los parámetros de configuración definidos en los pasos anteriores.



Confirme los detalles de la configuración y, a continuación, seleccione Guardar para aplicar los cambios.

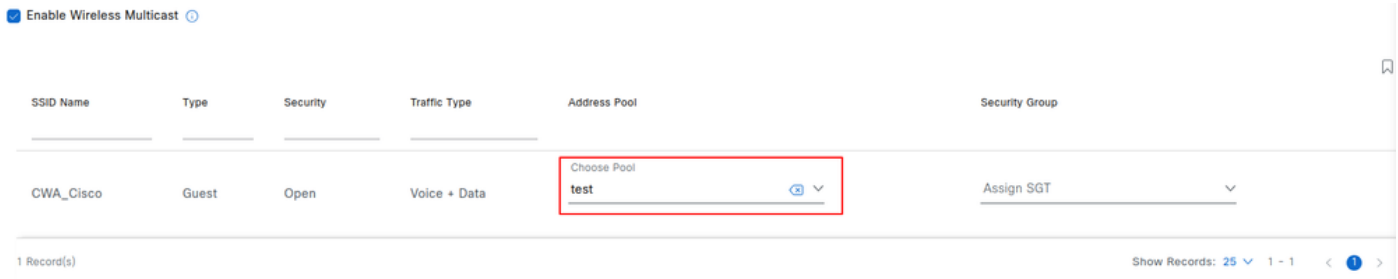
Aprovisionamiento de fabric

Después de asociar el perfil de red inalámbrica con el sitio del fabric, el SSID aparece en Suministro > Sitios del fabric > (Su sitio) > SSID inalámbricos.

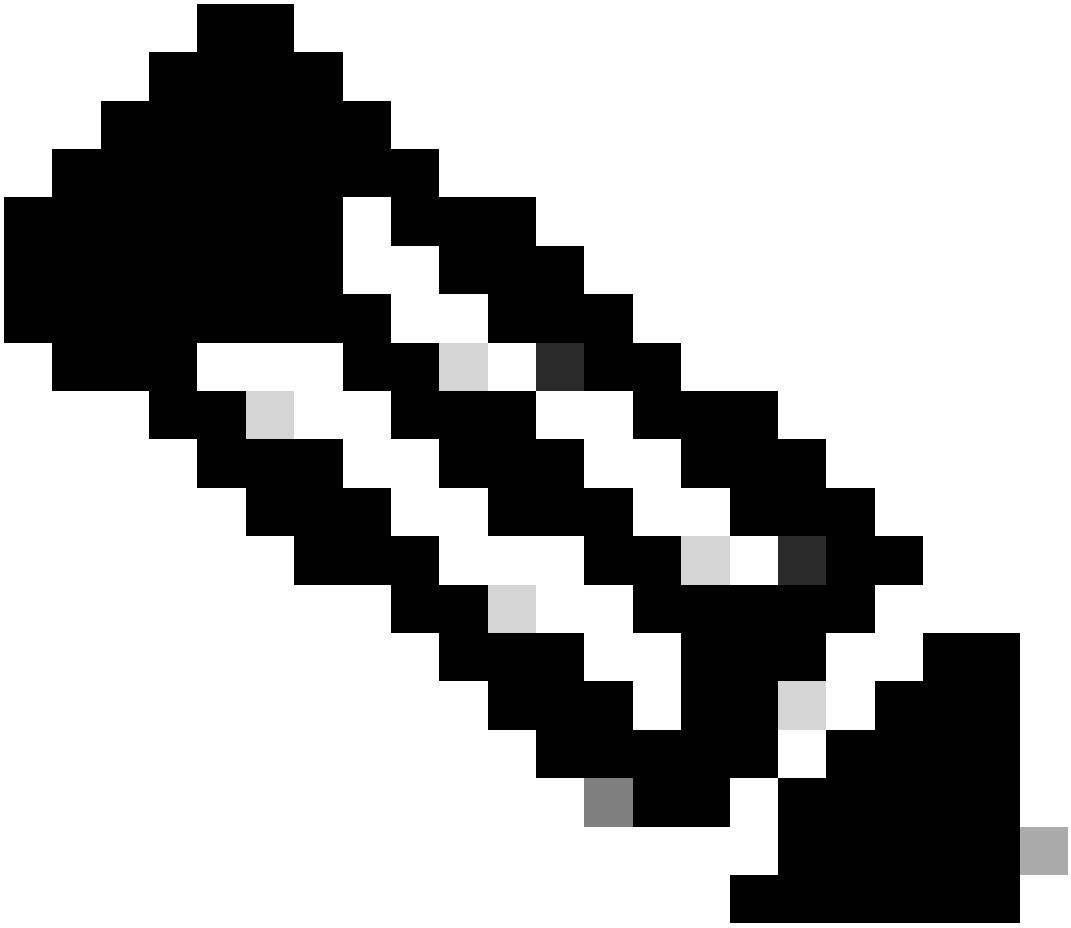


Nota: Debe proporcionar el controlador de LAN inalámbrica para el sitio para que los SSID se muestren en SSID inalámbricos

Elija el conjunto SSID, asocie opcionalmente una etiqueta de grupo de seguridad y haga clic en Implementar. Los puntos de acceso transmiten el SSID solo si se asigna un conjunto.



En los controladores AireOS y Catalyst 9800, vuelva a configurar el controlador de LAN inalámbrica después de cualquier cambio en la configuración SSID en Network Settings.



Nota: Si no se asigna ningún conjunto al SSID, se espera que los AP no lo difundan. El SSID solo se difunde después de asignar un conjunto. Una vez asignado el conjunto, no es necesario volver a aprovisionar el controlador.

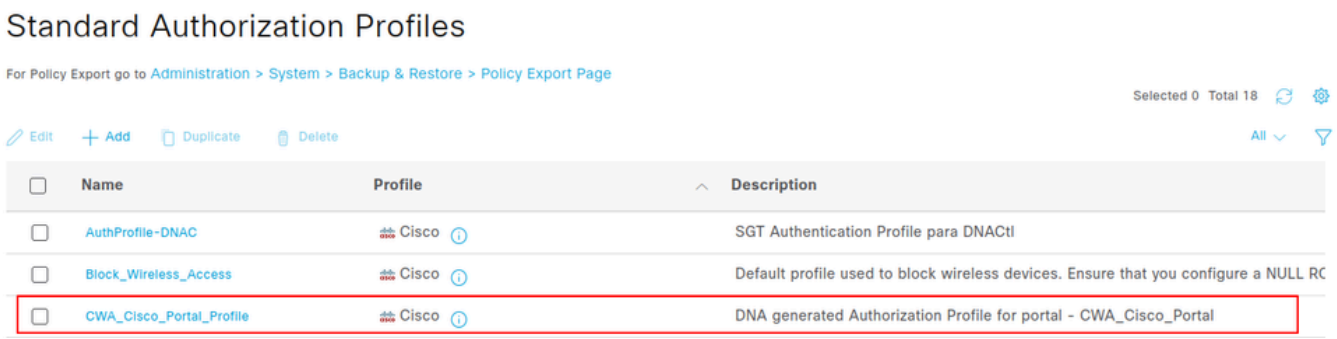
Revisar la configuración aprovisionada para Cisco ISE

En esta sección se examina la configuración proporcionada por Catalyst Center a Cisco ISE.

Perfil de autorización

Parte de la configuración que Catalyst Center proporciona en Cisco ISE es un perfil de autorización. Este perfil define el resultado asignado a un cliente en función de sus parámetros y puede incluir configuraciones específicas como asignación de VLAN, ACL o redireccionamiento de URL.
Para ver el perfil de autorización en ISE, navegue hasta Política > Elementos de política > Resultados. Si el nombre del portal es CWA_Cisco_Portal, el nombre del perfil es CWA_Cisco_Portal_Profile. El campo de descripción muestra el texto: Perfil de autorización

generado por DNA para el portal CWA_Cisco_Portal.



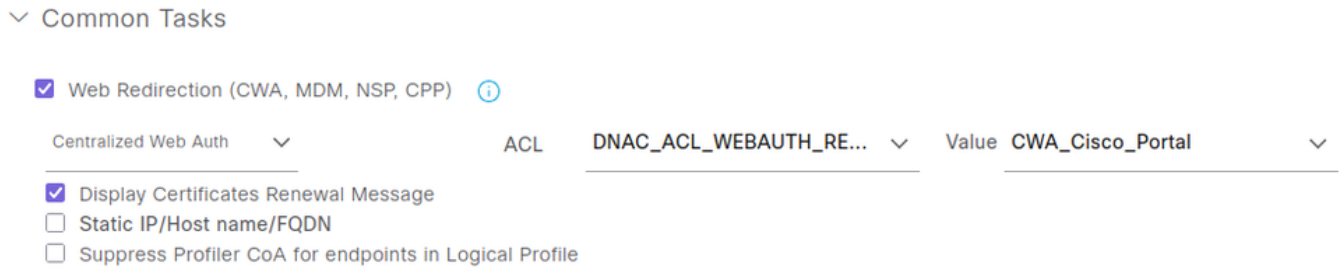
Para ver los atributos enviados al controlador de LAN inalámbrica por este perfil de autorización, haga clic en el nombre del perfil de autorización y consulte la sección Tareas comunes.
Este perfil de autorización proporciona la ACL de redirección y la URL de redirección.

El atributo de redirección web incluye dos parámetros:

1. Nombre de ACL: Defina en Cisco DNA_ACL_WEBAUTH_REDIRECT.
2. Valor: se refiere al nombre del portal cautivo, en este ejemplo CWA_Cisco_Portal.

La opción Mostrar mensaje de renovación de certificados permite utilizar el portal para renovar los certificados que utiliza actualmente el terminal.

Hay una opción adicional, Static IP/Host Name/FQDN (IP estática/Nombre de host/FQDN), disponible en Display Certificates Renewal Message (Mostrar mensaje de renovación de certificados). Esta característica permite la entrega de la dirección IP del portal en lugar de su FQDN, lo que es útil cuando el portal cautivo no se carga debido a la incapacidad de alcanzar el servidor DNS.

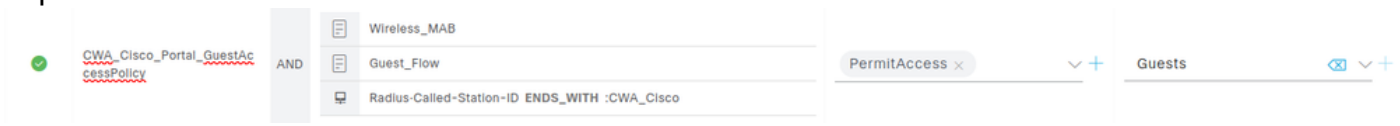


Conjuntos de políticas

Vaya a Policy > Policy Sets > Default > Authorization Policy para ver los dos conjuntos de políticas creados para el portal llamado CWA_Cisco_Portal. Estos conjuntos de políticas son:

- CWA_Cisco_Portal_GuestAccessPolicy
- CWA_Cisco_Portal_RedirectPolicy

La política CWA_Cisco_Portal_GuestAccessPolicy se aplica cuando el cliente ya ha completado el proceso de autenticación web, ya sea a través del autorregistro o a través del portal de zonas Wi-Fi públicas.

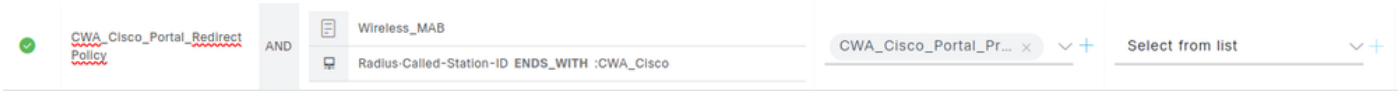


Este conjunto de políticas coincide con tres criterios:

- Wireless_MAB: Se utiliza cuando Cisco ISE recibe una solicitud de autenticación de derivación de autenticación MAC (MAB) de un controlador de LAN inalámbrica.
- Flujo_invitado: Hace referencia a ISE que comprueba la dirección MAC del terminal con el grupo de identidad GuestEndpoints. Si la dirección MAC del terminal no está presente en este grupo, no se aplica la política.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-ID es un atributo RADIUS en ISE que almacena el puente o la dirección MAC del punto de acceso en formato ASCII y agrega el SSID al que se accede, separado por un punto y coma (:). En este ejemplo, CWA_Cisco representa el nombre SSID.

Bajo los perfiles de columna se ve el nombre PermitAccess, se trata de un perfil de autorización reservado que no se puede editar, lo que proporciona acceso completo a la red y también se puede asignar una SGT en la columna Security Groups (Grupos de seguridad), que en este caso es Guest (Invitados).

Se utiliza el perfil PermitAccess. Este es un perfil de autorización reservado que no se puede editar y concede acceso completo a la red. También se puede asignar una SGT en la columna Security Groups; en este caso, el SGT se establece en Invitados.
La siguiente política a revisar es CWA_Cisco_Portal_RedirectPolicy.



Este conjunto de políticas coincide con los dos criterios siguientes:

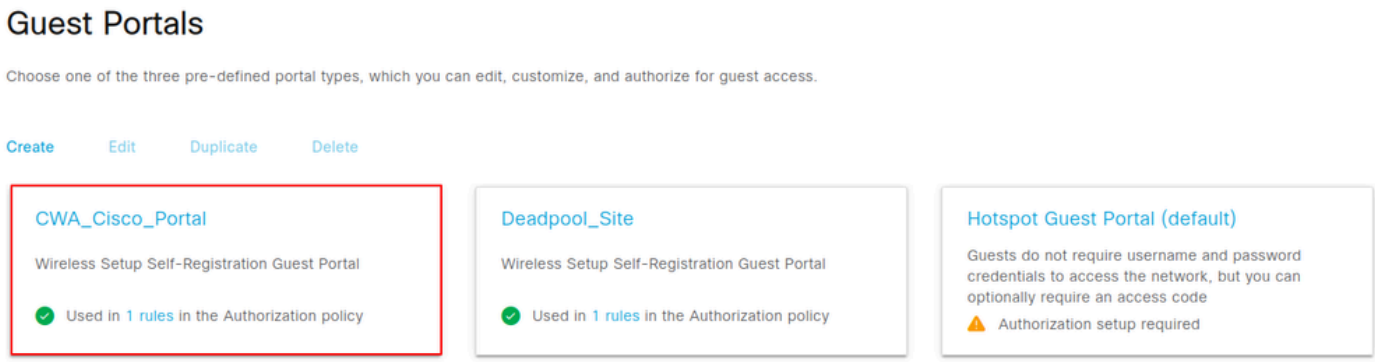
- Wireless_MAB: Se utiliza cuando Cisco ISE recibe una solicitud de autenticación MAB de un controlador de LAN inalámbrica.
- RADIUS Called-Station-ID ENDS_WITH :CWA_Cisco: Called-Station-ID es un atributo RADIUS en ISE que almacena el puente o la dirección MAC del punto de acceso en formato ASCII y agrega el SSID al que se accede, separado por un punto y coma (:). En este ejemplo, :CWA_Cisco representa el nombre SSID.

El orden de estas políticas es fundamental. Si CWA_Cisco_Portal_RedirectPolicy aparece primero en la lista, sólo coincide con la autenticación MAB y el nombre SSID mediante el atributo RADIUS

Called-Station-ID ENDS_WITH :CWA_Training. En esta configuración, incluso si el terminal ya se ha autenticado a través del portal, seguirá coincidiendo con esta política indefinidamente. Como resultado, el acceso completo nunca se concede a través del perfil PermitAccess, y el cliente permanece atascado en un loop continuo de autenticación y redirección al portal.

Configuración del portal de invitados

Vaya a Centros de trabajo > Acceso de invitado > Portales y componentes para ver el portal. El portal de invitados creado aquí utiliza el mismo nombre que en Catalyst Center CWA_Cisco_Portal. Seleccione el nombre del portal que desea utilizar si desea ver detalles adicionales.

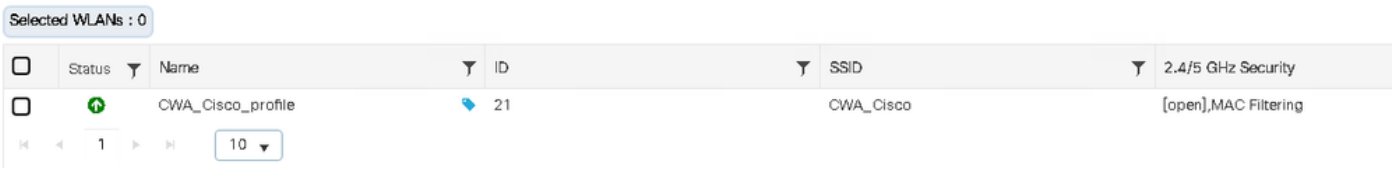


Revise la configuración aprovisionada a el WLC

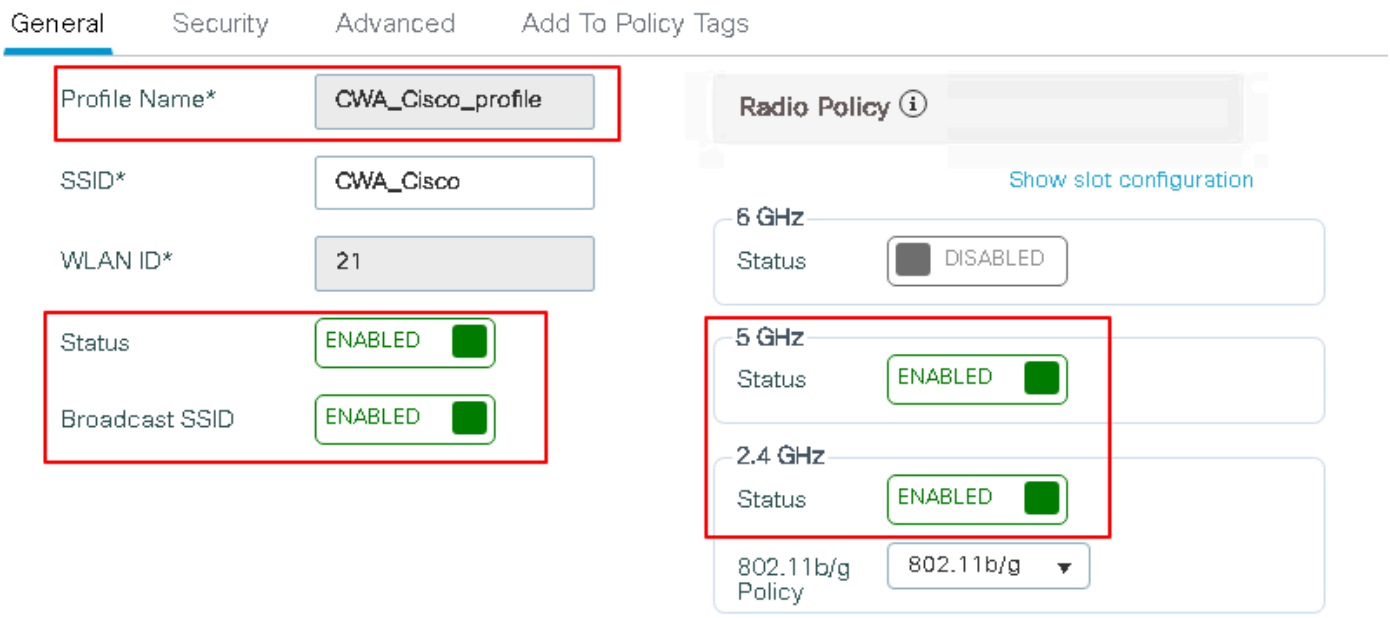
En esta sección se examina la configuración proporcionada por Catalyst Center al controlador de LAN inalámbrica.

Configuración de SSID

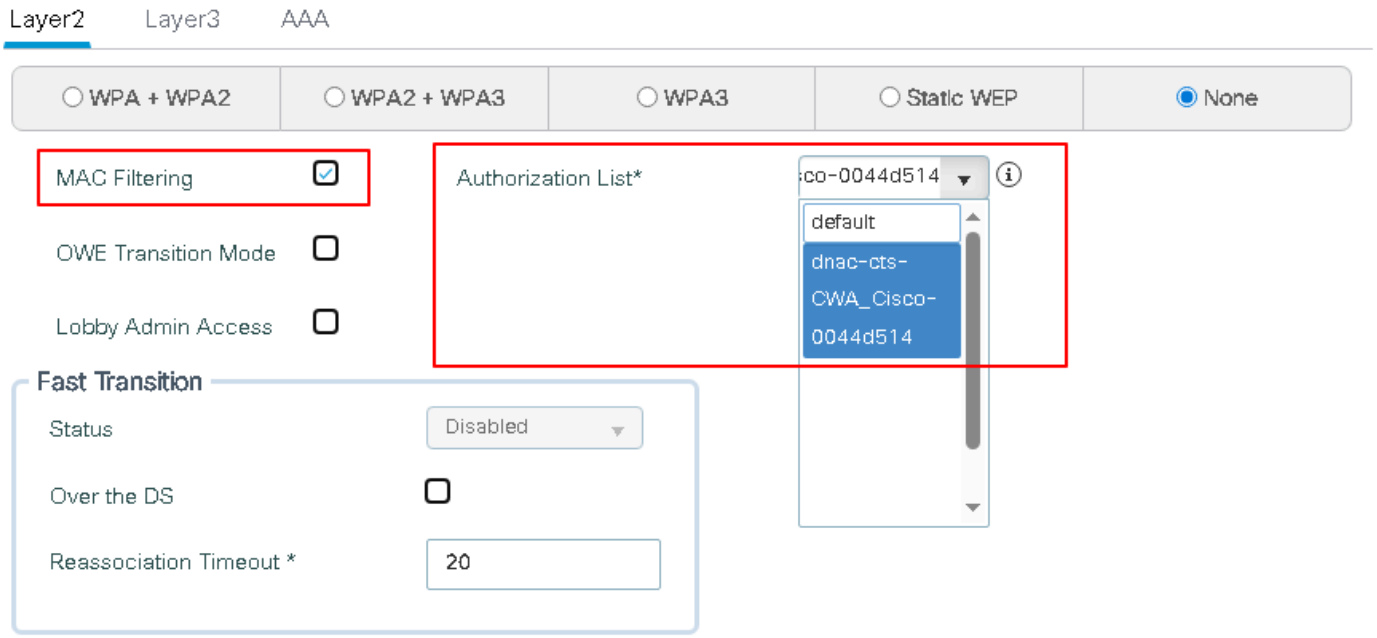
En la GUI del WLC, navegue hasta Configuration > Tags & Profiles > WLANs para ver la configuración SSID.



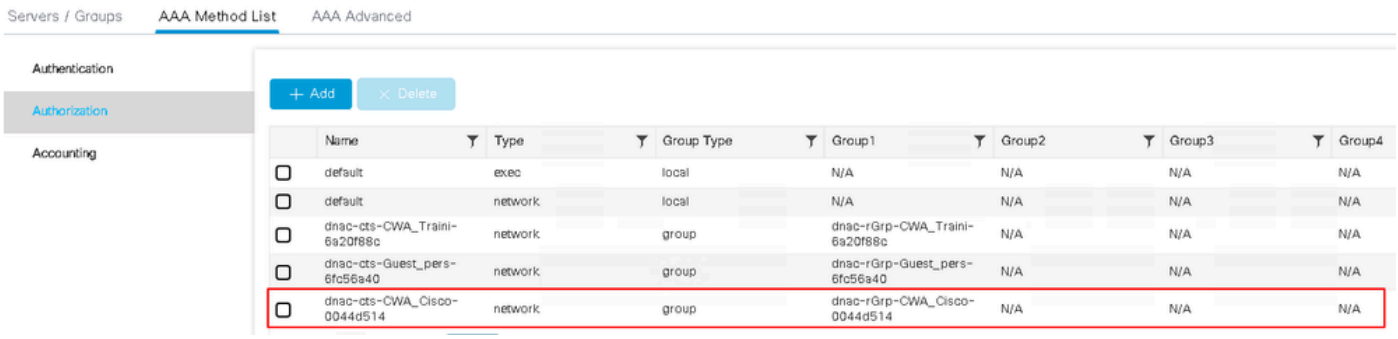
El SSID CWA_Cisco es tiene el nombre CWA_Cisco_profile en el WLC, con ID 21 y un tipo de seguridad Open que utiliza el filtrado de MAC. Haga doble clic en el SSID para ver su configuración.



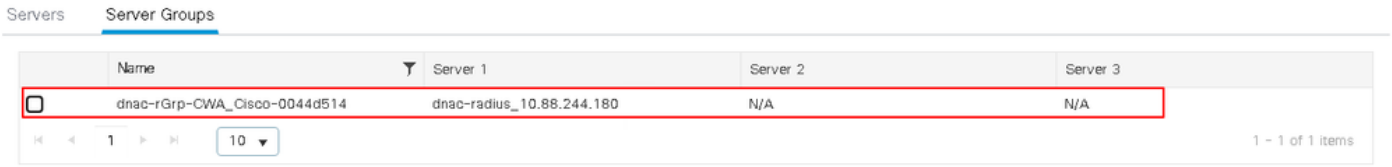
El SSID está ACTIVO y emite en canales de 5 GHz y 2,4 GHz, y está conectado al perfil de política CWA_CIsco_Profile. Haga clic en la pestaña Seguridad para ver la configuración.



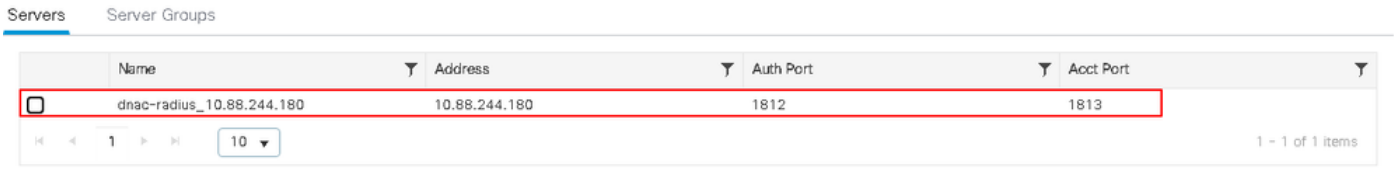
La configuración clave incluye el método de seguridad de capa 2 (filtrado de MAC) y la lista de autorización AAA (Cisco DNA-cts-CWA_Cisco-0044d514). Para revisar su configuración, navegue hasta Configuration > Security > AAA > AAA Method List > Authorization.



La lista de métodos señala al grupo RADIUS Cisco DNA-Grp-CWA_Cisco-0044d514en la columna Group1. Para ver su configuración, navegue hasta Configuration > Security > AAA > Server/Groups > Server Groups .



El grupo de servidores Cisco DNA-Grp-CWA_Cisco-0044d514 señala a Cisco DNA-radius_10.88.244.180 en la columna Servidor 1. Vea su configuración en la pestaña Servidores.



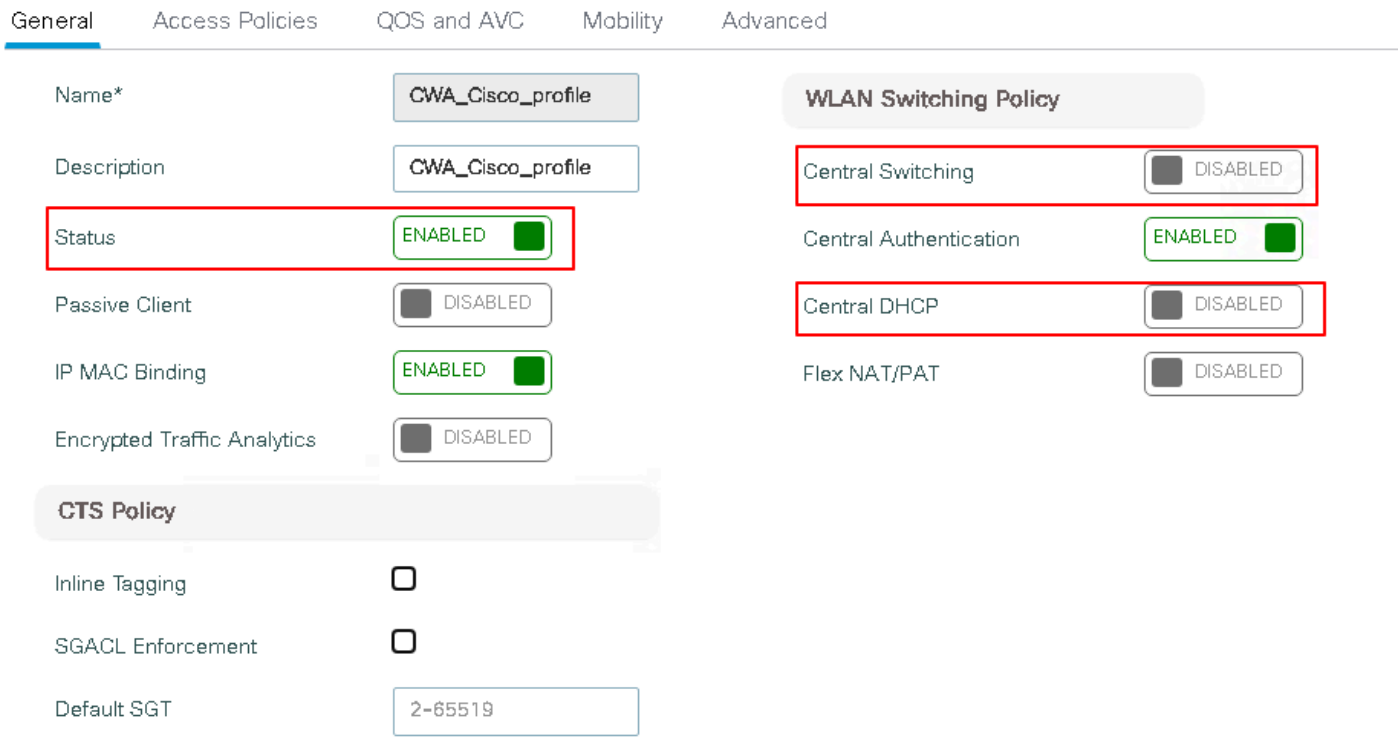
El servidor Cisco DNA-radius_10.88.244.180 tiene la dirección IP 10.88.244.180. Haga clic en su nombre para ver su configuración

Una configuración crítica es el cambio de autorización (CoA), que proporciona un mecanismo para modificar los atributos de una sesión de autenticación, autorización y contabilidad (AAA) después de que se haya autenticado en el portal cautivo. Sin esta función, el terminal permanece en un estado pendiente de web-auth incluso después de completar el registro en el portal.

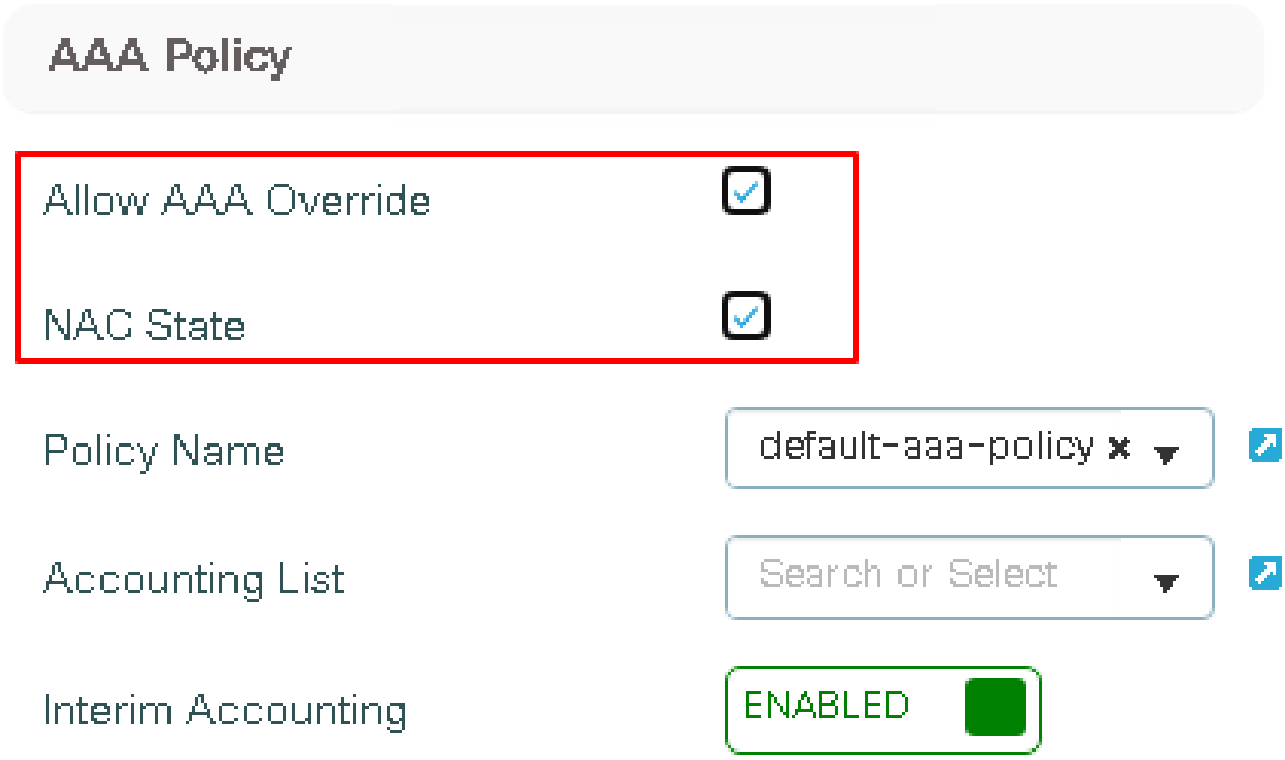
Configuración del perfil de política inalámbrica

Dentro del perfil de política, a los clientes se les pueden asignar configuraciones como VLAN, ACL, QoS, ancla de movilidad y temporizadores. Para ver la configuración del perfil de política, navegue hasta Configuración > Etiquetas y perfiles > Política.

Haga clic en el nombre de la política para ver su configuración.



El estado de la política es Activado y como con cualquier SSID de fabric, el switching central y el DHCP central están desactivados. Haga clic en la pestaña Avanzado y navegue hasta la sección Política AAA para ver detalles adicionales de la configuración.



Se pueden habilitar tanto la anulación de AAA como el control de acceso a la red (NAC). AAA Override permite al controlador aceptar los atributos devueltos por el servidor RADIUS, como ACL o URL, y aplicar estos atributos a los clientes. NAC habilita el cambio de autorización (CoA) después de que el cliente se haya registrado en el portal.
Esta configuración también se puede ver a través de la CLI en el WLC.
Para verificar el perfil de política, se adjunta el SSID para ejecutar el comando:

<#root>

```
WLC#show fabric wlan summary


Number of Fabric wlan : 1

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

Para ver la configuración del perfil de política CWA_Cisco_profile, ejecute el comando:

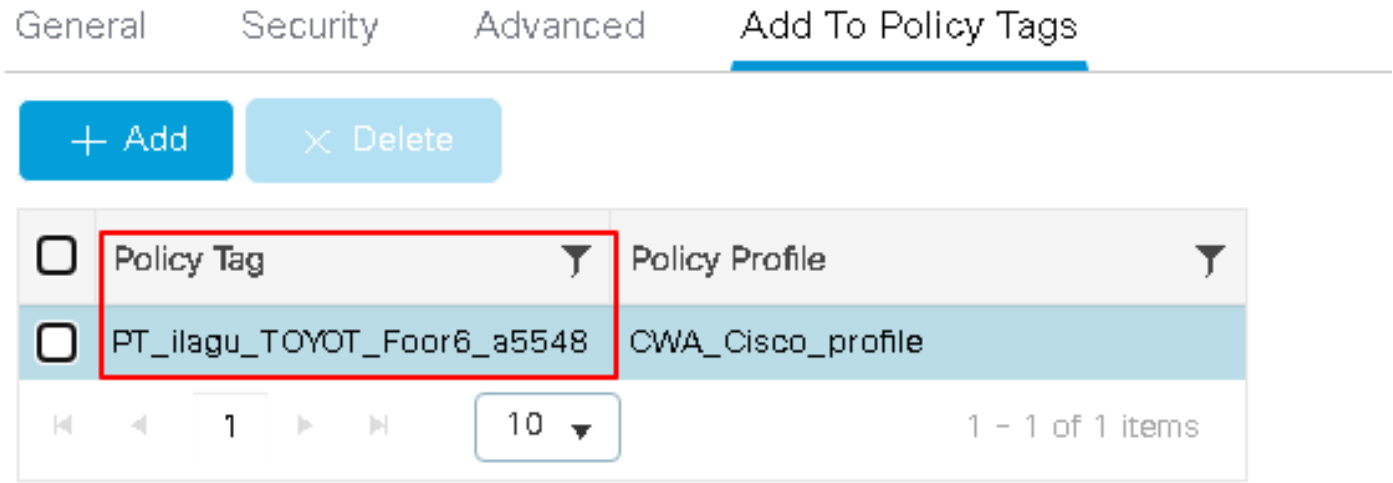
<#root>

```
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
```

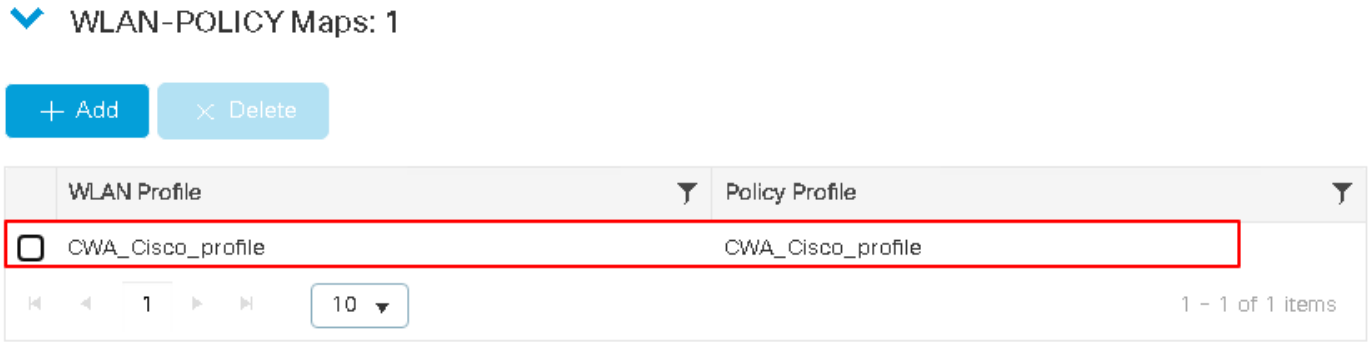
Configuración de etiquetas de políticas

La etiqueta de política es la forma en que vincula la WLAN con el perfil de política, navegue hasta Configuración > Etiquetas y perfiles > WLANs, haga clic en el nombre de WLAN y navegue hasta Agregar a etiquetas de política para identificar la etiqueta de política asignada al SSID.



Para el SSID CWA_Cisco_profile, se utiliza la etiqueta de política PT_ilagu_TOYOT_For6_a5548 para verificar esta configuración; navegue hasta Configuration > Tags & Profiles > Tags > Policy.

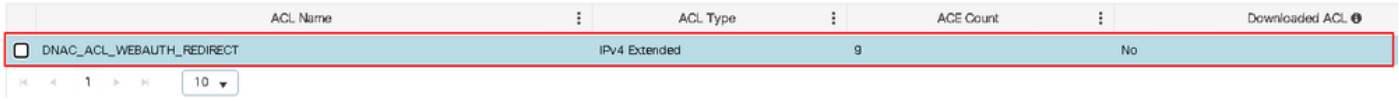
Haga clic en el nombre para ver los detalles. La etiqueta de política PT_ilagu_TOYOT_For6_a5548 enlaza la WLAN CWA_Cisco que está asociada con el nombre CWA_Cisco_profile en el WLC (vea la página de WLANs para referencia) al Perfil de Política CWA_Cisco_profile.



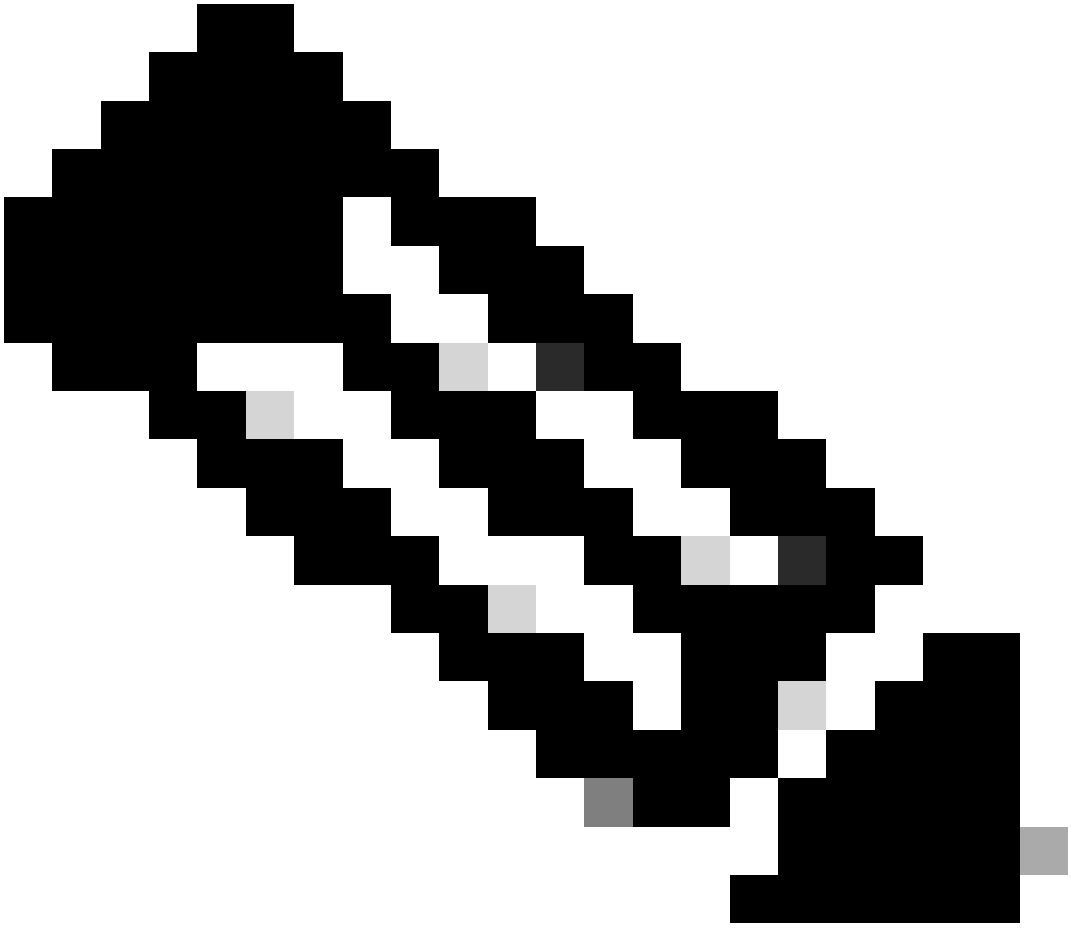
El nombre WLAN CWA_Cisco_profile hace referencia a WLAN CWA_Cisco.

Configuración de ACL de redireccionamiento

En CWA, una Lista de control de acceso de redirección define qué tráfico se redirige al WLC para un procesamiento adicional y qué tráfico omite la redirección
Esta configuración se envía al WLC después de crear el SSID y de aprovisionar el WLC del inventario. Para visualizarla, navegue hasta Configuration > Security >ACL, El nombre de la ACL que Catalyst Center utiliza para la ACL redirigida es Cisco DNA_ACL_WEBAUTH_REDIRECT.



Haga clic en el nombre para ver su configuración. Los valores se derivan de la configuración de red de la configuración de red del sitio en Catalyst Center.



Nota: Estos valores se obtienen de la configuración de red del sitio configurada en Catalyst Center y los valores DHCP/DNS se obtienen del conjunto configurado en la WLAN. En la configuración AAA del flujo de trabajo de SSID se hace referencia a la dirección IP PSN de ISE.

Para ver la ACL de redirección en la CLI del WLC, ejecute este 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
```

La ACL de redirección se puede aplicar al perfil flexible para que se pueda enviar a los puntos de acceso. Ejecute este comando para confirmar esta configuración

<#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
```

Redirección de ACL en el punto de acceso

En el punto de acceso, los valores permit y deny se invierten: permit indica tráfico de reenvío y deny indica redirección. Para revisar la configuración de la ACL de redirección en el AP, ejecute este 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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).