Estandarización de la autenticación de PA 802.1X por cable con IBNS 2.0 y plantillas de interfaz

Contenido

Introducción

Este documento describe la configuración de 802.1X mediante plantillas de interfaz IBNS 2.0.

Declaración de problema

El uso de IEEE 802.1X para la seguridad de puertos es una práctica recomendada habitual. Además de mejorar la seguridad de la red, también simplifica las implementaciones de switches al permitir una configuración de puertos de acceso estandarizada en toda la red.

En esta guía se describe cómo se puede utilizar una única configuración de puerto de switch estandarizada tanto para los dispositivos finales como para los puntos de acceso (AP) de Cisco. Mientras que cada puerto de switch funciona inicialmente como un puerto de acceso estándar y realiza la autenticación IEEE 802.1X, un AP autenticado puede requerir un modo operativo diferente dependiendo de su escenario de implementación.

En particular, los AP que funcionan en el modo de conmutación local de FlexConnect deben funcionar en un puerto trunk porque el tráfico del cliente de los SSID múltiples se puentea localmente. Como resultado, la interfaz del switch debe pasar dinámicamente de un puerto de acceso a un puerto trunk después de la autenticación exitosa.

Los puertos de acceso que conectan dispositivos de infraestructura en lugar de dispositivos finales simples a menudo requieren configuraciones de interfaz que difieren del comportamiento predeterminado del puerto de acceso.

Por consiguiente, la configuración de la interfaz del switch debe modificarse dinámicamente durante el proceso de autenticación. A lo largo de los años, se han utilizado varios enfoques para lograr este comportamiento, incluidos los applets Auto SmartPorts y Embedded Event Manager (EEM). Actualmente, la solución recomendada es IBNS 2.0 [1] en combinación con plantillas de interfaz, que proporciona un método escalable y coherente para cambiar dinámicamente la configuración de la interfaz después de una autenticación correcta.

Enfoque

Para una configuración en funcionamiento, debe haber varios componentes configurados correctamente, a saber

- Servidor Radius (Identity Service Engine)
- Switch
- Punto de acceso/Controlador de LAN inalámbrica

Dado que hay documentación existente (véanse las referencias al final), nos centramos en un escenario concreto de este documento y hacemos referencia a la documentación existente como material de apoyo.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de LAN inalámbrica (WLC) y puntos de acceso ligeros (LAP)
- 802.1x en switches Cisco e ISE
- Protocolo de autenticación extensible (EAP)
- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)

Componentes Utilizados

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

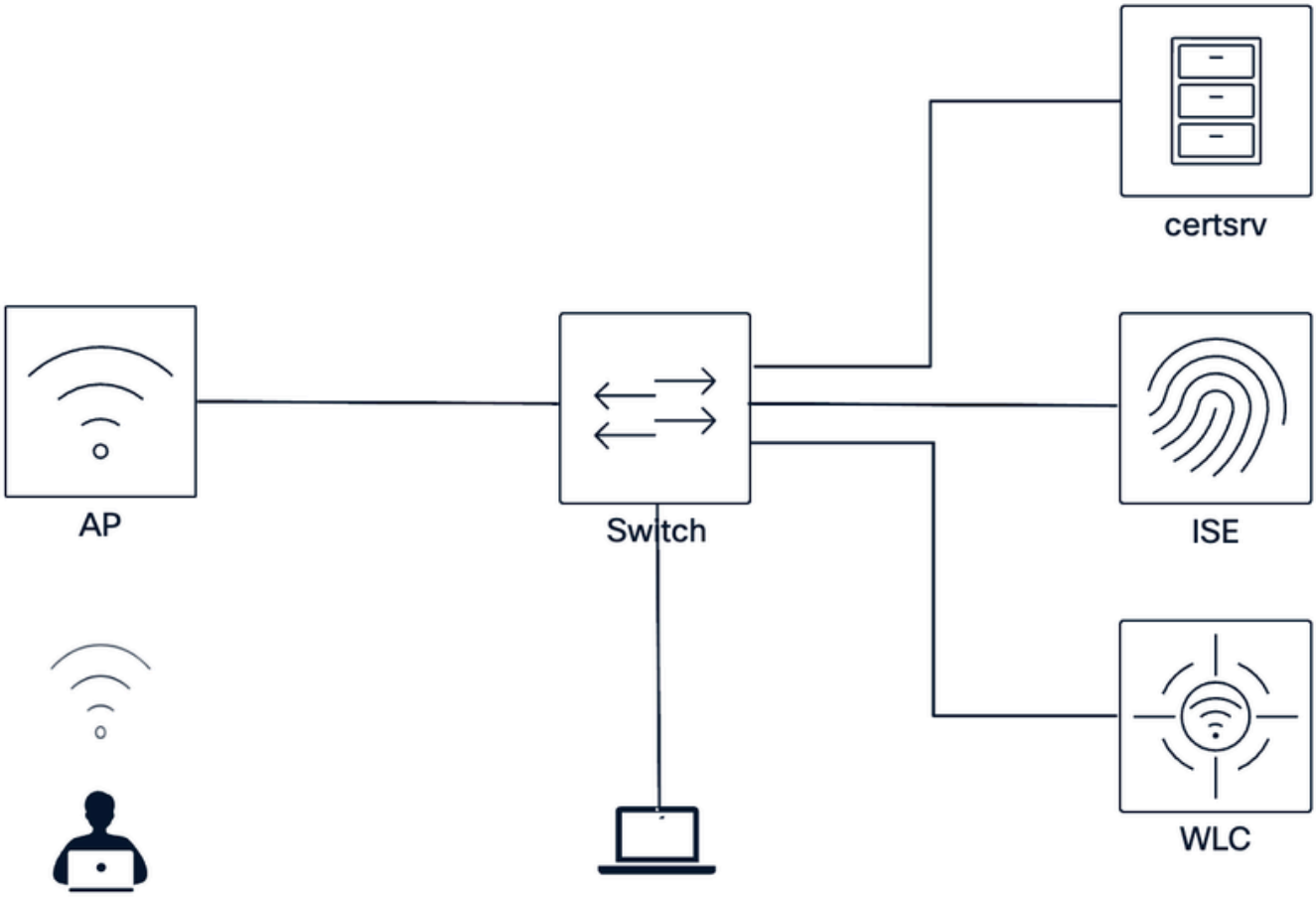
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C9800-40 WLC - IOS XE 26.1.1
- Parche 1 de ISE versión 3.5
- AP CW917x, CW916x

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.

La configuración también se documenta en netascode.cisco.com modelos de datos para switching e ISE para replicar la configuración fácilmente.

Configuración

Diagrama de la red



Ejemplo de configuración

Para nuestro propósito, nos centramos en un único escenario y proporcionamos fragmentos de configuración y orientación paso a paso. Como existen diferentes variaciones en el camino, las señalamos y hacemos referencia a la documentación existente para este propósito.

Situación descrita en esta guía:

- Punto 1X con cable AP con autenticación EAP-FAST
- Credenciales Dot1X suministradas a través de C9800 WLC
- AP en el modo de switching local de Flex Connect

En este diseño, el puerto de switch utiliza inicialmente una configuración 802.1X de modo cerrado común con repliegue MAB. Durante la primera incorporación, es posible que el punto de acceso aún no tenga credenciales 802.1X, por lo que ISE puede autorizar el punto de acceso a través de MAB con acceso limitado suficiente para alcanzar el WLC o el Catalyst Center. Una vez que se proporcionan las credenciales o los certificados, el AP realiza la autenticación 802.1X por cable. A

continuación, ISE devuelve un resultado de autorización que se aplica a la plantilla de interfaz AP_FLEX_TRUNK y convierte el puerto a la configuración de enlace troncal FlexConnect necesaria.

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

Tabla 1: Variaciones y opciones adicionales en una descripción general

Configuración de AP

Para utilizar la autenticación Dot1x cableada en combinación con su AP, debe desplegar las credenciales y/o los certificados dependiendo del método de autenticación seleccionado a los AP primero.

El suplicante Cisco Catalyst AP Dot1x en general soporta EAP-FAST, EAP-PEAP o EAP-TLS. Además, el MAB también podría ser una opción, especialmente porque los AP necesitan reunir en primer lugar las credenciales o los certificados para poder ejecutar la autenticación de tipo EAP.

- MAB:
  - No se requiere configuración del lado AP
  - La gestión de direcciones MAC de hardware requiere herramientas
  - Se puede suplantar fácilmente
  - Permite la configuración común de puertos

- EAP-FAST:
  - Basado en nombre de usuario/contraseña
  - Fácil de implementar
  - Requiere aprovisionamiento de PAC en banda anónimo habilitado en ISE

- EAP-PEAP:
  - Basado en nombre de usuario/contraseña
  - Requiere certificados para la validación del servidor
  - La renovación del certificado debe planificarse en consecuencia

- EAP-TLS:
  - Basado en certificados
  - La renovación del certificado debe planificarse en consecuencia

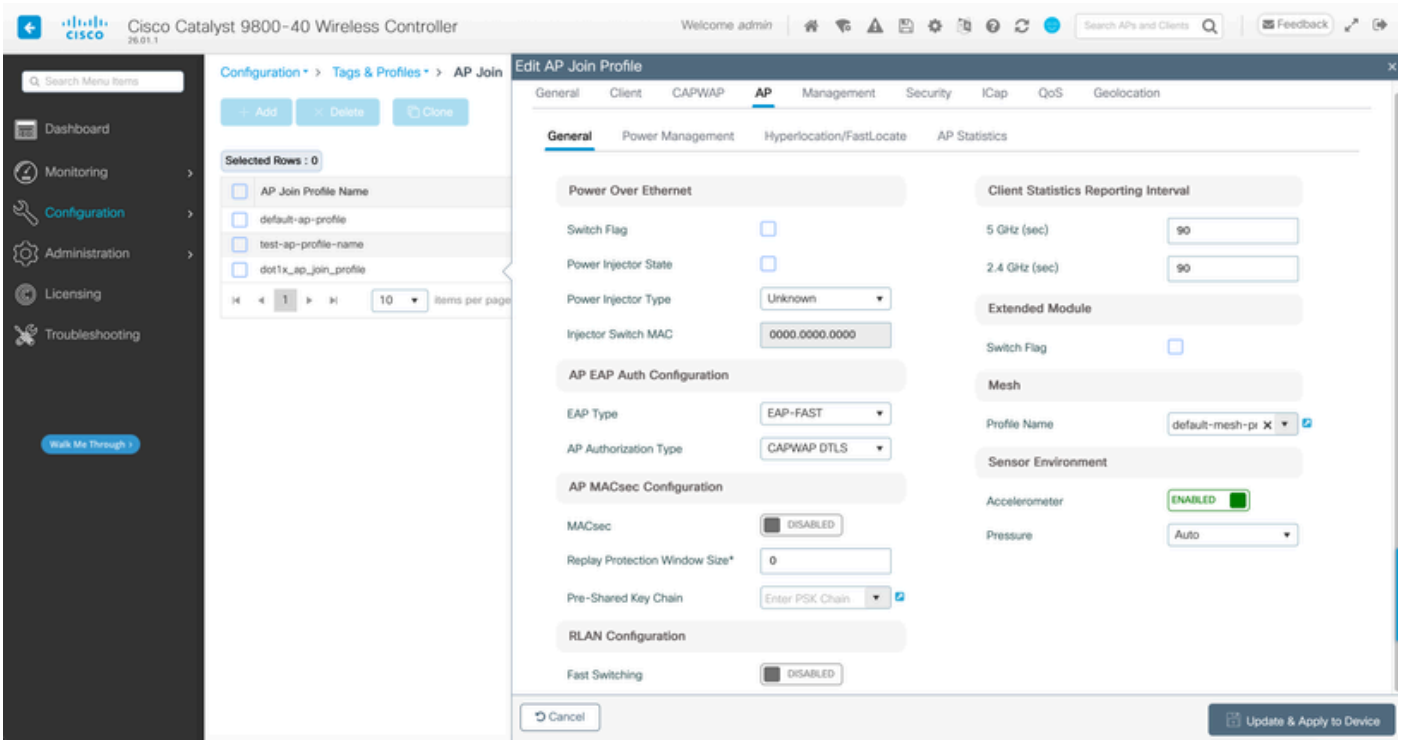
Para configurar el suplicante Dot1X cableado AP, hay dos enfoques para esto, ya sea a través del controlador de LAN inalámbrica o el centro de Catalyst que se describen aquí. Antes de entrar en estos detalles, debe seleccionar previamente el tipo de autenticación que va a utilizar.

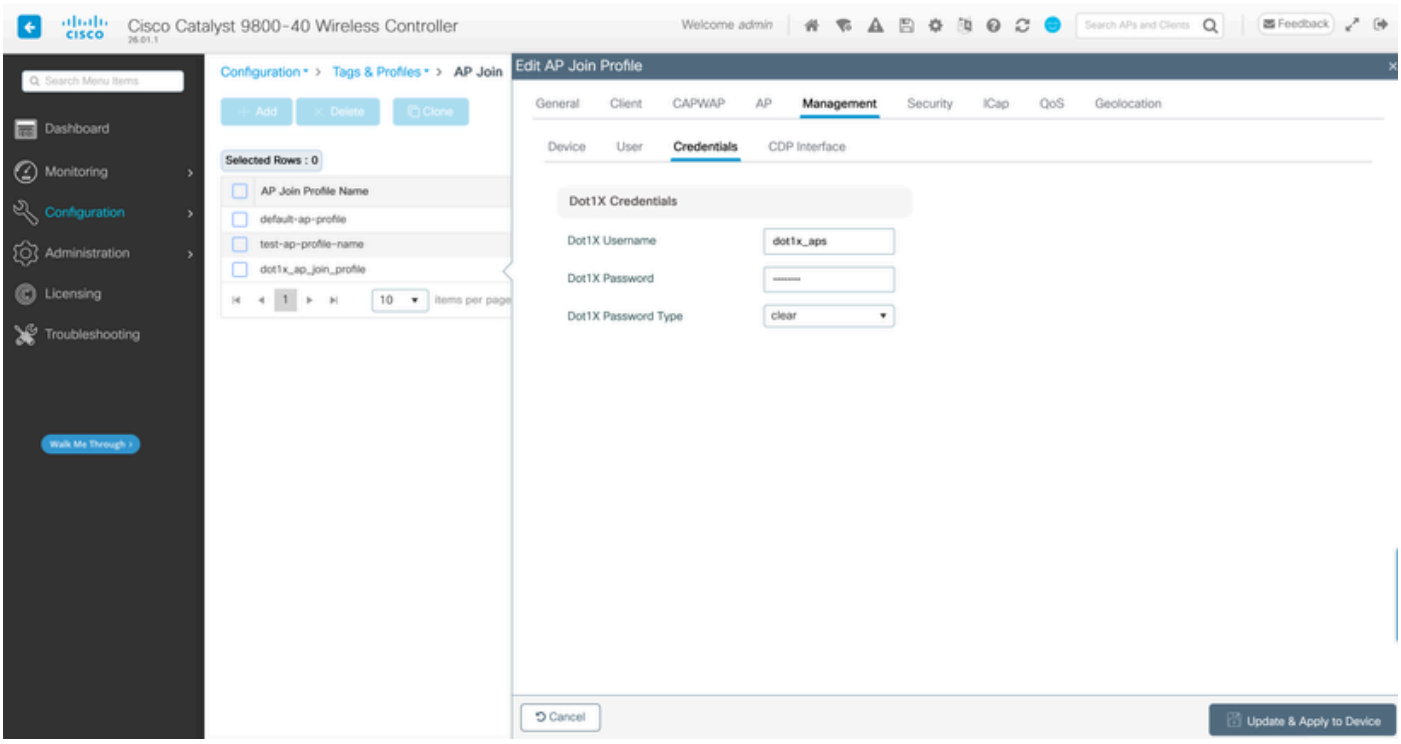
Configuración de punto por cable1X a través del controlador de LAN inalámbrica de Cisco 9800

Si ha seleccionado una autenticación basada en certificados (EAP-PEAP o EAP-TLS [1]), debe decidir como siguiente paso el enfoque sobre cómo planea emitir certificados de PA locales significativos (LSC), ya sea a través de SCEP[2] o EST [3].

Cuando se utiliza EAP-FAST como en nuestro escenario, es suficiente generar un perfil de unión a AP, donde se ingresa el usuario y la contraseña Dot1X, se enlaza ese perfil de unión a una etiqueta de sitio y se asigna a los AP.

Configuración de la interfaz gráfica para el usuario





Configuración de CLI

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

Configuración de la conexión por cable Dot1X a través de Catalyst Center Plug and Play

Para que PnP [4] funcione, Catalyst Center debe integrarse con ISE. Esto es necesario en parte debido a los certificados que se requieren para poder realizar la validación del servidor desde el lado AP para la autenticación EAP con ISE. Para el certificado del lado del dispositivo, los AP consiguen un certificado emitido por la CA del centro de Catalyst que es de forma predeterminada su propio incorporado o si está configurado por una SubCA / SCEP de la CA respectiva.

El proceso de configuración a través de PnP permite el aprovisionamiento de certificados y/o credenciales antes de que el dispositivo se una a los WLC.

Configuración del switch

Además de que la autenticación es un mecanismo de seguridad, también es una manera de estandarizar las configuraciones de los puertos de switch. Por lo tanto, en estas partes se describen los elementos necesarios para lograrlo. Esta es una configuración de ejemplo y debe revisarse y adaptarse a su configuración. En general, esta configuración permite Dot1x y MAB de reserva con el manejo adecuado de los escenarios de radio muerto, reautenticación, etc.

Atributos de radio globales:

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Grupo de servidores Radius:

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
```

```
!
!
aaa group server radius client-radius-group
 server name client-radius-server01
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Configuración AAA:

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

IBNS2.0 Class-map y service-template:

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
```

```
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

Política de servicio de IBNS 2.0:

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
```

```
  10 authenticate using mab priority 20
 70 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
!
```

Plantillas de interfaz:

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

Configuración de la Interfaz:

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Obligatorio global:

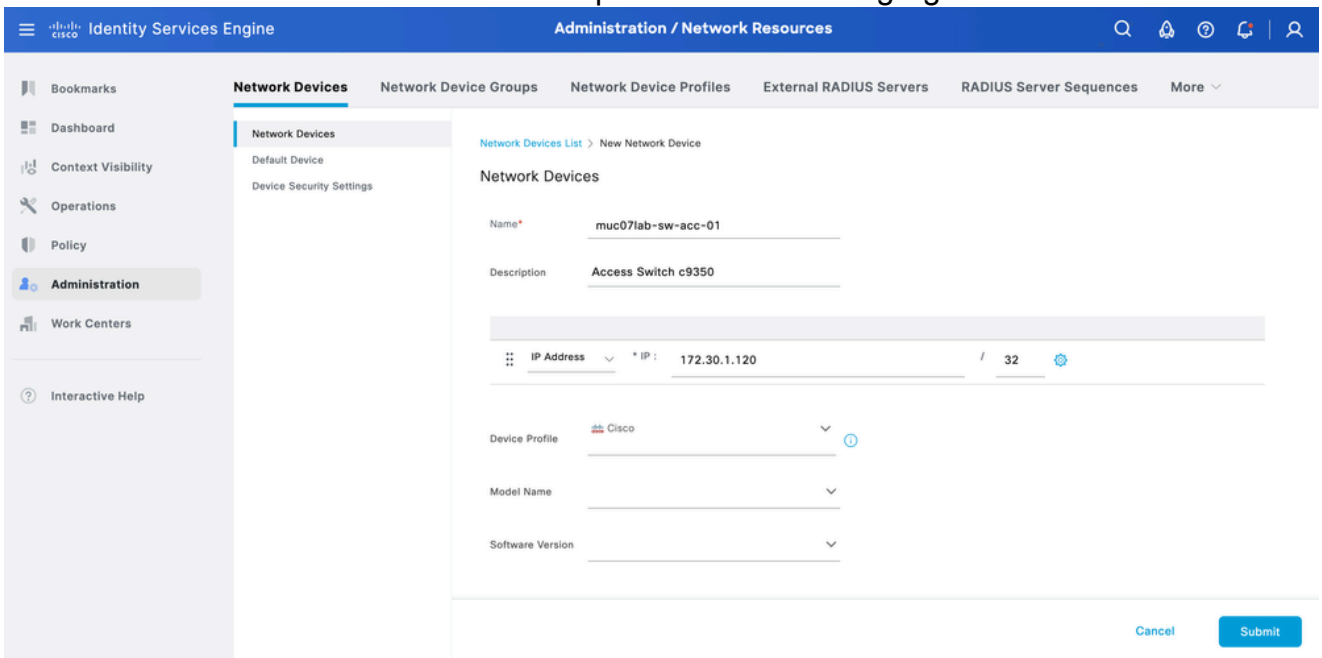
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

Nota: Cuando se utiliza un CW9178, el AP presenta dos direcciones MAC durante la autenticación. Para evitar que el puerto de switch ingrese al estado err-disabled, el puerto debe configurarse inicialmente para host-mode multi-auth. Después de una autenticación 802.1X exitosa, se recomienda cambiar dinámicamente la configuración del puerto a host-mode multi-host.

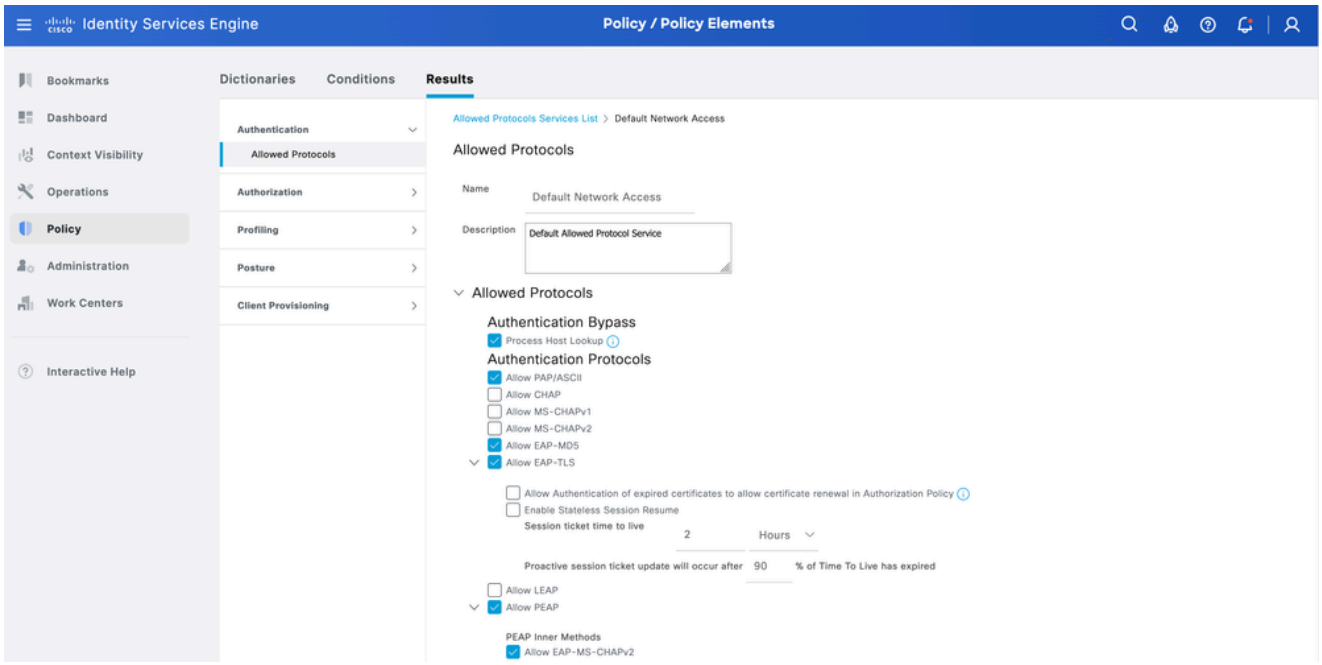
Configuración de Identity Services Engine

Por último, también es necesario configurar el servidor RADIUS para permitir la autenticación. Para los Dot1x cableados hay una extensa guía[5] por lo que nos centramos solo en las partes relevantes en este caso.

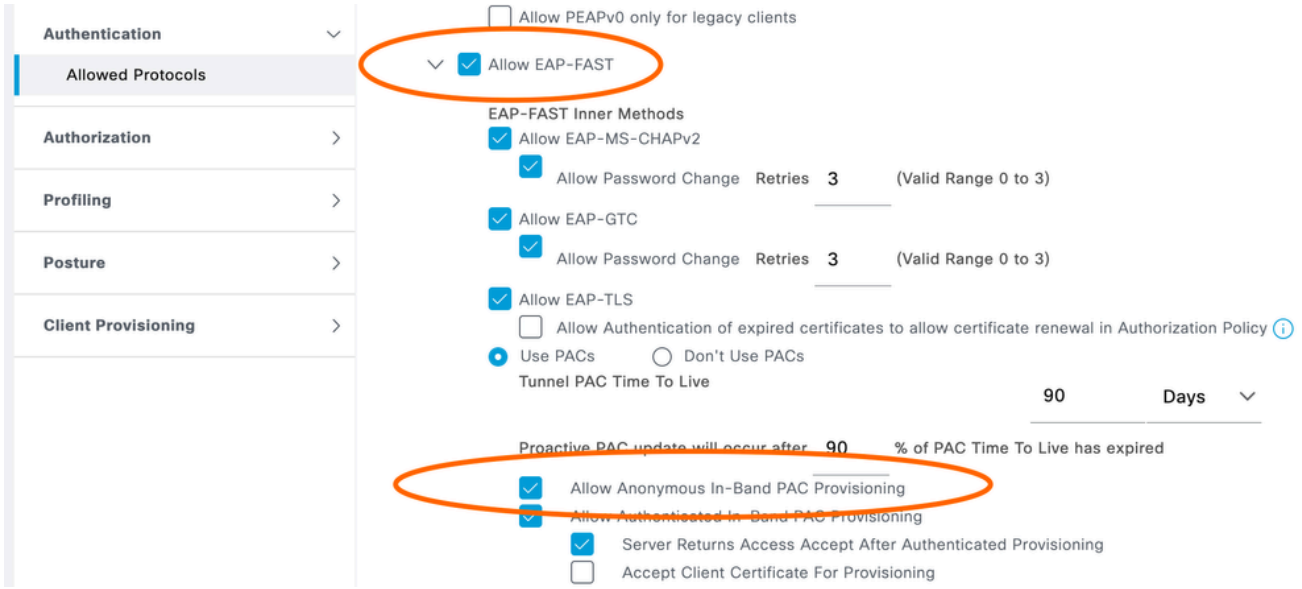
1. Agregue el switch como un dispositivo de acceso a la red:
   > Administración > Recursos de red > Dispositivos de red > Agregar



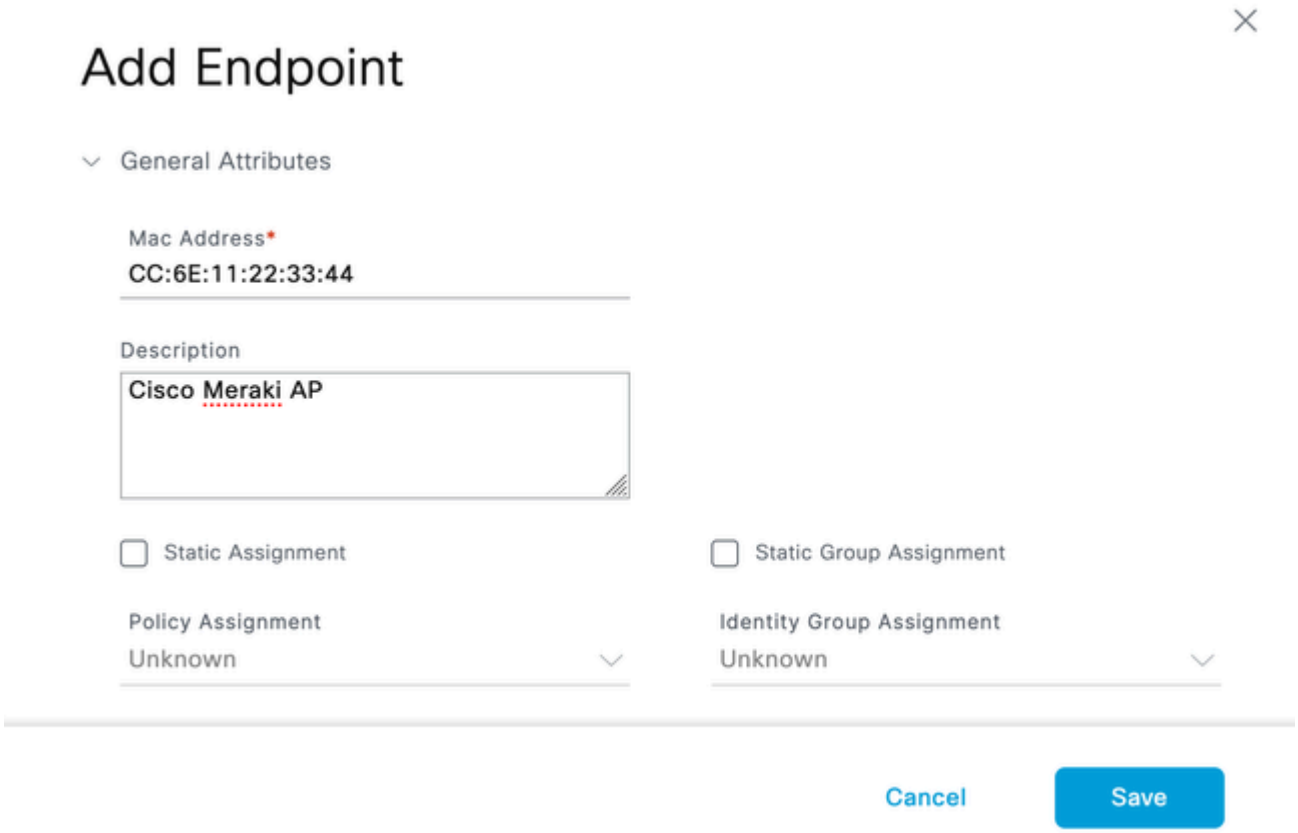
2. Habilite el protocolo EAP que está utilizando:
   > Política > Elementos de política > Resultados > Autenticación > Protocolos permitidos



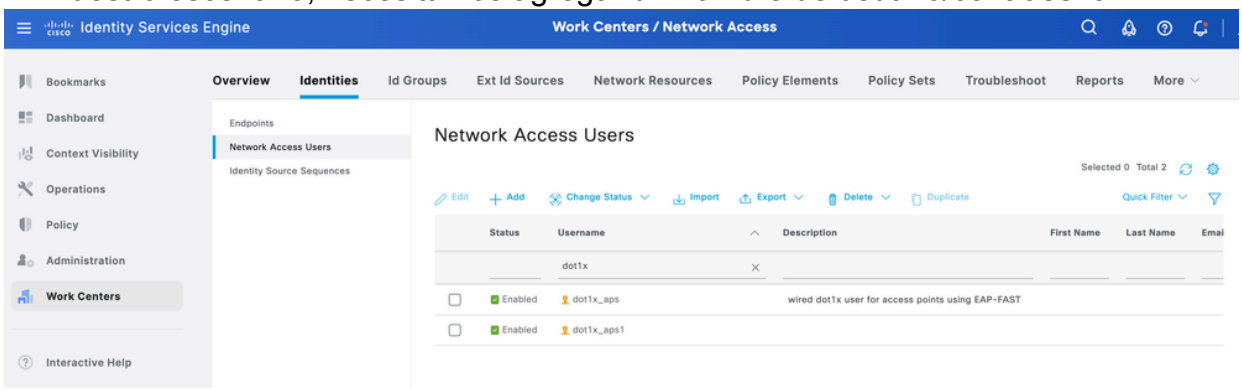
3. Para nuestra situación, ya que estamos utilizando EAP-FAST, tenga en cuenta que se debe habilitar "Anonymous In-band PAC Provisioning" (Aprovisionamiento de PAC en banda anónimo):



4. Agregar identidades
   > Centros de trabajo > Acceso a la red > Identidades
   a. Para que la operación se realice correctamente, el proceso suele constar de dos pasos. Inicialmente, el AP no tiene credenciales y, por lo tanto, no puede responder a la autenticación EAP. Como resultado, el puerto del switch primero debe autenticar el AP usando MAB. Puede basarse en una política de autorización genérica, una política basada en la ubicación o la definición de perfiles de dispositivos. Independientemente de la política utilizada, la autenticación MAB inicial debe tener éxito para permitir que el AP obtenga sus credenciales, ya sea del WLC vía CAPWAP o de Cisco Catalyst Center a través de Plug and Play (PnP).

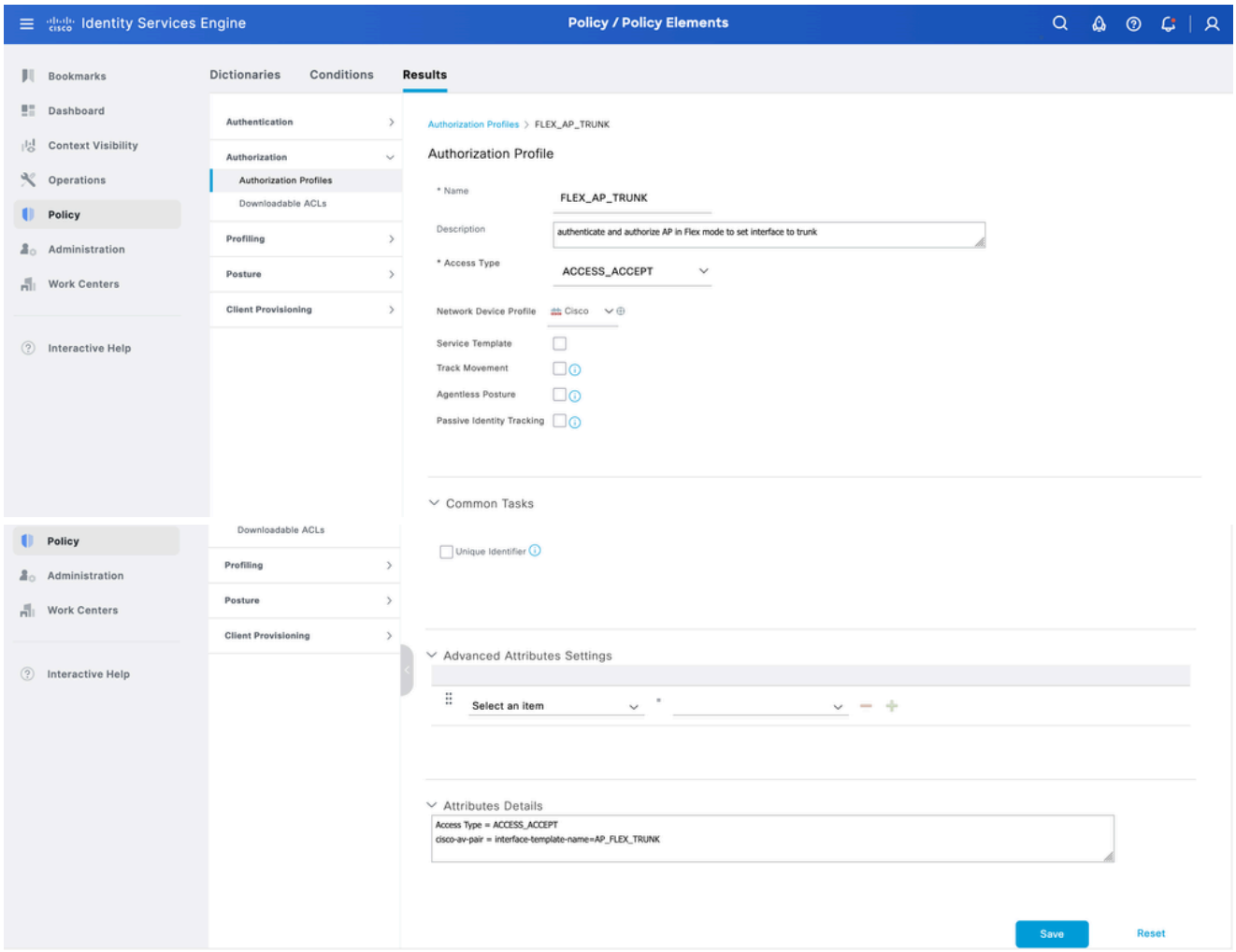


b. Después de que el AP haya reunido las credenciales/certificado, el suplicante Dot1X cableado del AP responde a EAPoL y Dot1X es el método subsiguiente para la autenticación que habilita el AP para el acceso completo.
En nuestro escenario, necesitamos agregar un nombre de usuario/contraseña:

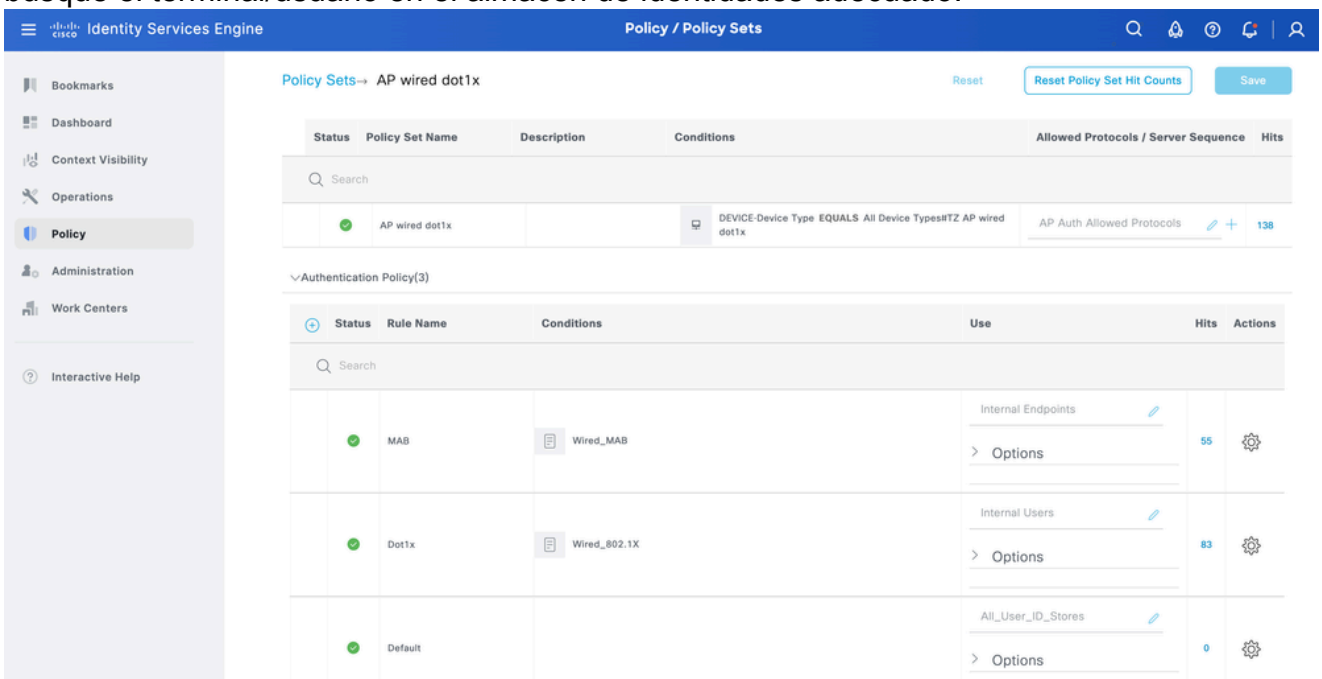


5. Creación del perfil de autorización
El perfil de autorización responde con el par AV necesario. En nuestro caso, como estamos modificando dinámicamente el switchport, la interfaz-plantilla debe configurarse:
> Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización

Nombre: FLEX_AP_TRUNK
Tipo de acceso: ACCESS_ACCEPT
Plantilla de interfaz: AP_FLEX_TRUNK

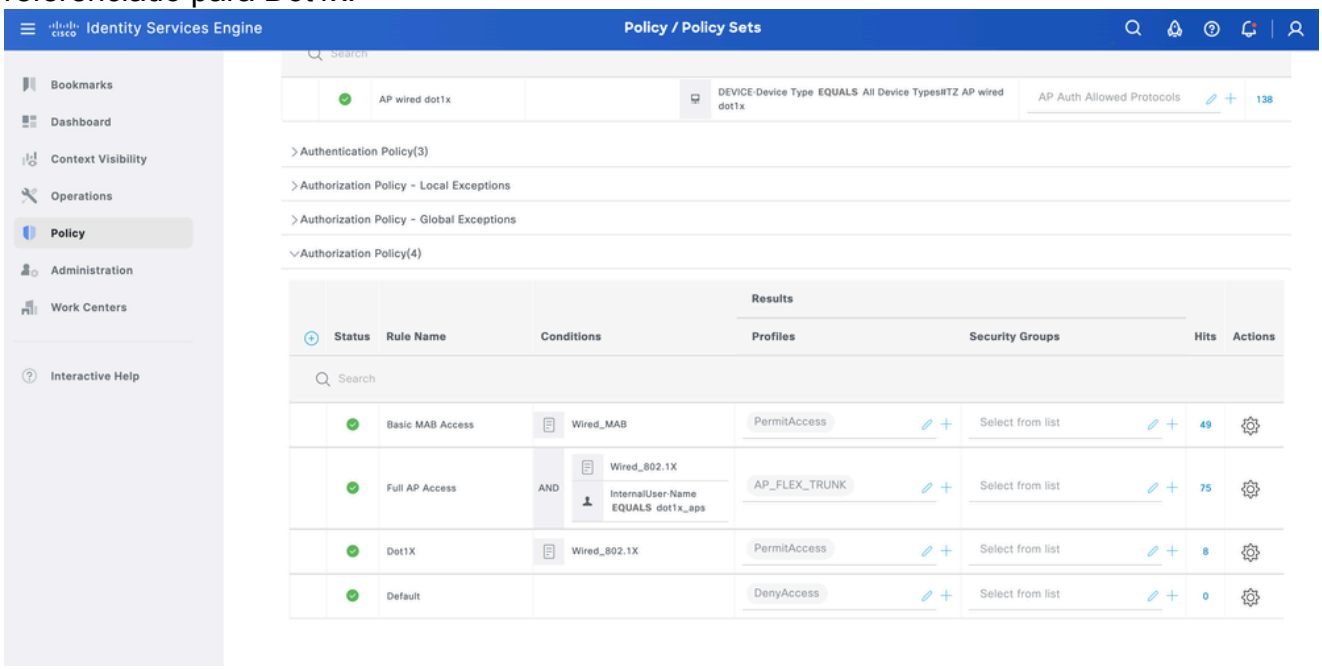


6. Crear directiva de autorización
   Cree una política de autenticación que permita tanto el MAB como el Dot1X cableado y busque el terminal/usuario en el almacén de identidades adecuado.



Ponga un resultado de autorización de acceso limitado, dependiendo de sus necesidades

de MAB, y un acceso de AP completo que incluya el par av-template de interfaz referenciado para Dot1x:



Verificación

Una vez que esta configuración se haya implementado, conecte el AP al switch. Como requisito previo, se espera que la configuración de red predeterminada, en nuestro caso un conjunto DHCP en la VLAN de acceso con la opción 43 que señala al WLC y la comunicación CAPWAP sea posible para el AP al WLC.

Comandos de AP

```
show ap authentication status
show crypto
show crypto pki trustpool
```

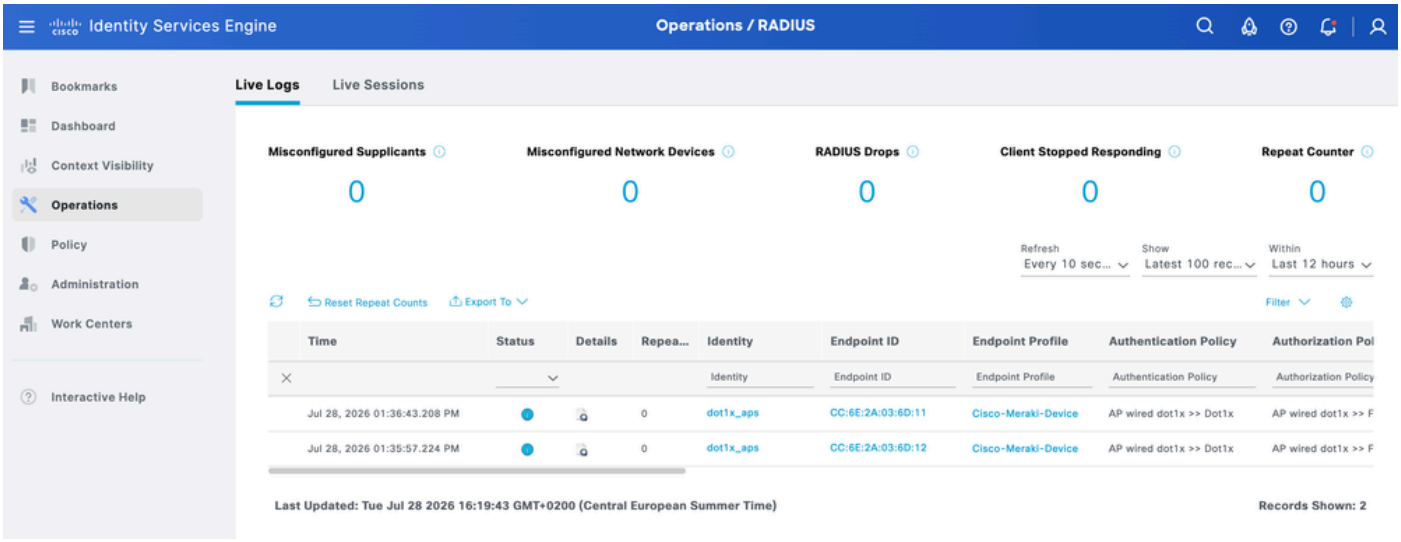
Comandos de switch

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
```

```
Interface MAC Address Method Domain Status Fg Session ID
---------------------------------------------------------------------------------------
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



Lista de siglas

Acrónimo	Expansión
AAA	Autenticación, autorización y contabilidad
AP	punto de acceso
AuthC	autenticación
AuthZ	Autorización
CA	entidad de certificación
CISP	Protocolo de señalización de información del cliente
Punto1x	IEEE 802.1X
EAP	Protocolo de autenticación extensible
EST	Inscripción en transporte seguro
RÁPIDO	Autenticación flexible a través de tunelación segura
IBNS	Servicios de red basados en identidad
ISE	Identity Services Engine
MAB	Omisión de autenticación MAC

Y	Dispositivo de acceso a red
PEAP	Protocolo de autenticación extensible protegido
SCEP	Protocolo de inscripción de certificado simple
TLS	Seguridad de capa de transporte
WLC	Controlador de LAN inalámbrica

Referencias

[1] Configure 802.1X en los AP para PEAP o EAP-TLS con LSC

[2] Configure SCEP para el aprovisionamiento de certificados de importancia local en el WLC 9800

[3] Guía de implementación in situ de Cisco Wireless EST

[4] Incorporación segura de puntos de acceso: una introducción a la seguridad de red mejorada

[5] Guía de implementación prescriptiva de ISE Secure Wired Access

[6] sección Guía de configuración para LSC

[7] Configuración de suplicante 802.1X para puntos de acceso con controlador 9800

[8] Proteja un puerto de switch AP Flexconnect con Dot1x

[9] Guía de configuración del software del controlador inalámbrico Cisco Catalyst serie 9800, Cisco IOS XE 17.18.x - 802.1x

[11] Guía del usuario de Cisco Catalyst Center, versión 3.2.x - Configuración de los ajustes de administración para un perfil de AP para dispositivos Cisco IOS XE

[12] Uso de IBNS 2.0 y plantillas de interfaz para una configuración de switchport predeterminada

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).