Padronize a autenticação de AP com fio 802.1X com IBNS 2.0 e modelos de interface

Contents

Introdução

Este documento descreve a configuração 802.1X usando modelos de interface IBNS 2.0.

Instrução do problema

O uso do IEEE 802.1X para segurança de porta é uma prática recomendada comum. Além de melhorar a segurança da rede, ele também simplifica as implantações de switch permitindo uma configuração de porta de acesso padronizada em toda a rede.

Este guia descreve como uma configuração de porta de switch única e padronizada pode ser

usada para dispositivos finais e pontos de acesso (APs) da Cisco. Enquanto cada porta de switch opera inicialmente como uma porta de acesso padrão e executa a autenticação IEEE 802.1X, um AP autenticado pode exigir um modo operacional diferente dependendo do seu cenário de implantação.

Em particular, os APs que operam no modo de switching local FlexConnect devem operar em uma porta de tronco, pois o tráfego do cliente de vários SSIDs é ligado localmente. Como resultado, a interface do switch deve fazer a transição dinâmica de uma porta de acesso para uma porta de tronco após a autenticação bem-sucedida.

As portas de acesso que conectam dispositivos de infraestrutura em vez de dispositivos finais simples frequentemente exigem configurações de interface que diferem do comportamento da porta de acesso padrão.

Consequentemente, a configuração da interface do switch deve ser modificada dinamicamente durante o processo de autenticação. Ao longo dos anos, várias abordagens foram usadas para alcançar esse comportamento, incluindo Auto SmartPorts e miniaplicativos Embedded Event Manager (EEM). Atualmente, a solução recomendada é o IBNS 2.0 [1] em combinação com modelos de interface, que fornece um método escalável e consistente para alterar dinamicamente a configuração da interface após a autenticação bem-sucedida.

Abordagem

Para que uma configuração funcione, deve haver vários componentes configurados corretamente, a saber:

- Servidor Radius (Identity Service Engine)
- Switch
- Controlador de ponto de acesso / LAN sem fio

Como existem documentações existentes (consulte as referências no final), nos concentramos em um cenário específico neste documento e referenciamos a documentação existente como material de apoio.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controladora de LAN sem fio (WLC) e APs leves (LAP)
- 802.1x em switches Cisco e ISE
- Protocolo de autenticação extensível (EAP)
- Serviço de Usuário de Discagem de Autenticação Remota (RADIUS)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

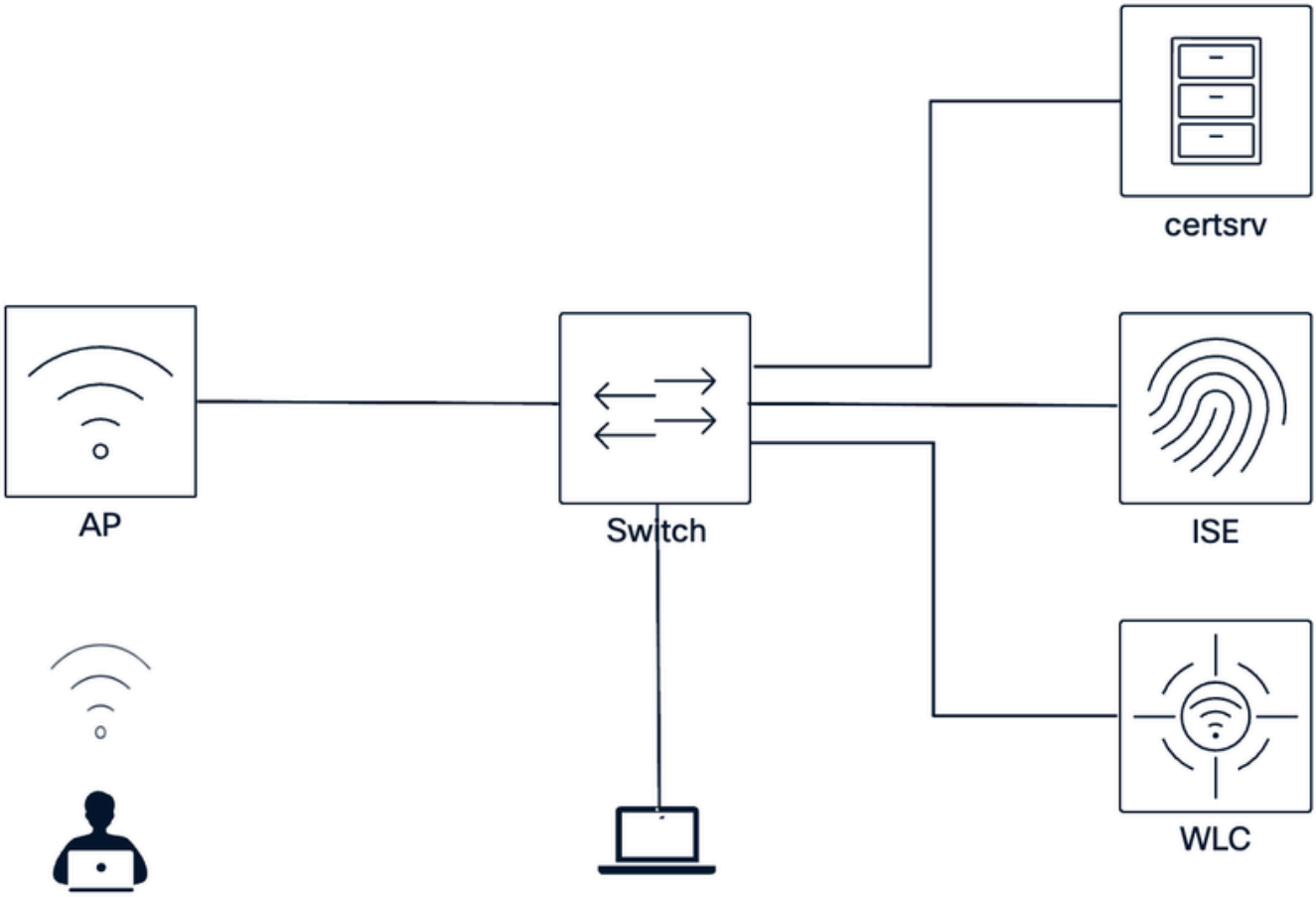
- Cisco C9350 - IOS XE 26.1.1a
- WLC Cisco C9800-40 - IOS XE 26.1.1
- Patch 1 do ISE versão 3.5
- AP CW917x, CW916x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

A configuração também está documentada em netascode.cisco.com modelos de dados para switching e ISE para replicar a configuração facilmente.

Configuração

Diagrama de Rede



Configuração de exemplo

Para nosso objetivo, nos concentramos em um único cenário e fornecemos snippets de configuração e orientação passo a passo. Como há diferentes variações ao longo do caminho, nós as indicamos e referenciamos a documentação existente para esse fim.

Cenário abordado neste guia:

- AP com fio Dot1X com autenticação EAP-FAST
- Credenciais Dot1X provisionadas através do C9800 WLC
- AP no modo de switching local do Flex Connect

Neste design, a porta do switch usa inicialmente uma configuração 802.1X de modo fechado comum com fallback de MAB. Durante a primeira integração, o AP potencialmente ainda não tem credenciais 802.1X, portanto o ISE pode autorizar o AP através do MAB com acesso limitado suficiente para acessar o WLC ou o Catalyst Center. Após o provisionamento de credenciais ou certificados, o AP executa a autenticação 802.1X com fio. O ISE retorna um resultado de

autorização que se aplica ao modelo de interface AP_FLEX_TRUNK, convertendo a porta para a configuração de tronco FlexConnect necessária.

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		

Tabela 1: Variações e opções adicionais em uma visão geral

Configuração de AP

Para usar a autenticação Dot1x com fio em combinação com seu AP, você deve primeiro distribuir credenciais e/ou certificados, dependendo do método de autenticação selecionado para os APs.

O suplicante Cisco Catalyst AP Dot1x em geral suporta EAP-FAST, EAP-PEAP ou EAP-TLS. Além disso, o MAB também pode ser uma opção, especialmente porque os APs precisam reunir em primeiro lugar as credenciais ou certificados para poder executar a autenticação do tipo EAP.

- MAB:
  - Nenhuma configuração do lado do AP necessária
  - O gerenciamento de endereços MAC de hardware exige ferramentas
  - Pode ser facilmente falsificado
  - Permite a configuração de porta comum

- EAP-FAST:
  - Baseado em nome de usuário/senha
  - Fácil de implementar
  - Requer fornecimento de PAC anônimo na banda habilitado no ISE

- EAP-PEAP:
  - Baseado em nome de usuário/senha

- Requer certificados para validação do servidor
- A renovação do certificado deve ser planejada de acordo

- EAP-TLS:
  - Baseado em certificado
  - A renovação do certificado deve ser planejada de acordo

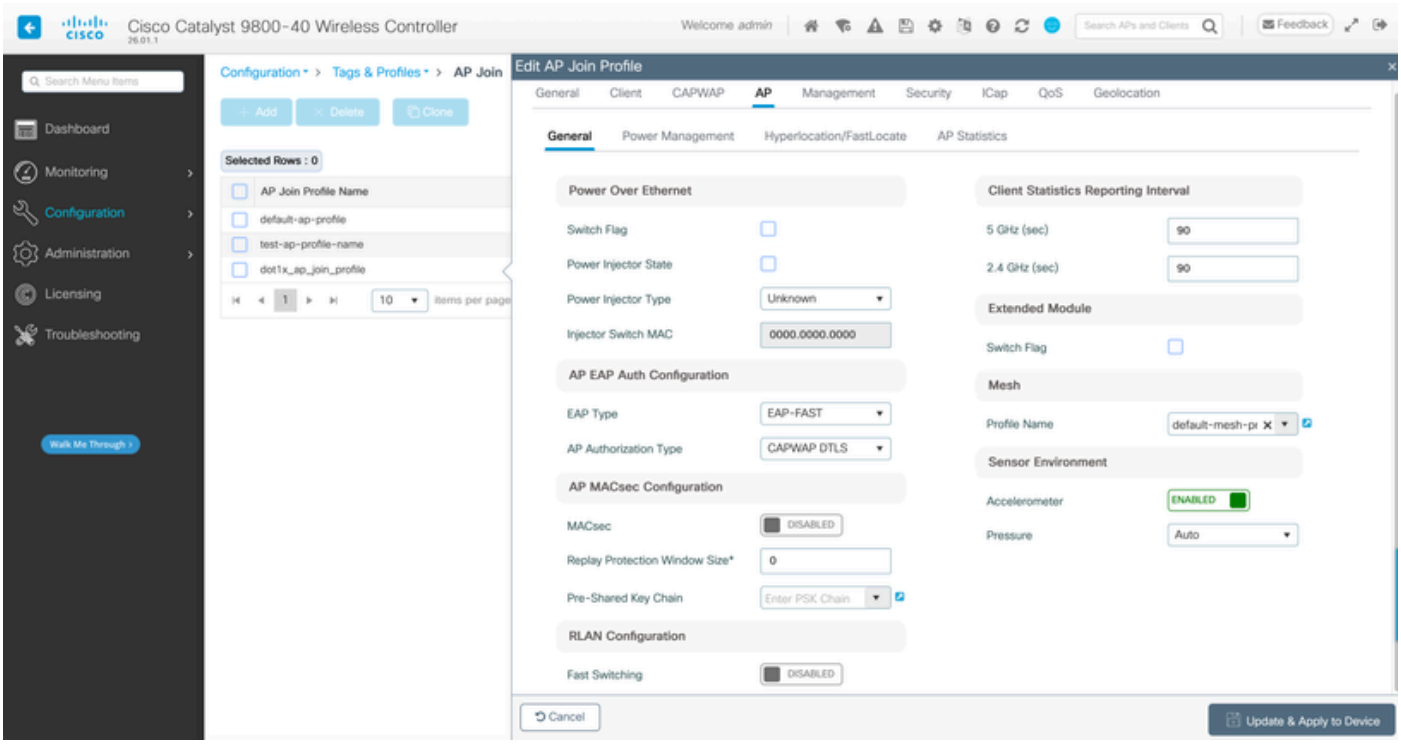
Para configurar o solicitante AP com fio Dot1X, há duas abordagens para isso, através do Wireless LAN Controller ou do Catalyst Center, que são descritas aqui. Antes de entrar nesses detalhes, o tipo de autenticação que você vai usar deve ser selecionado com antecedência.

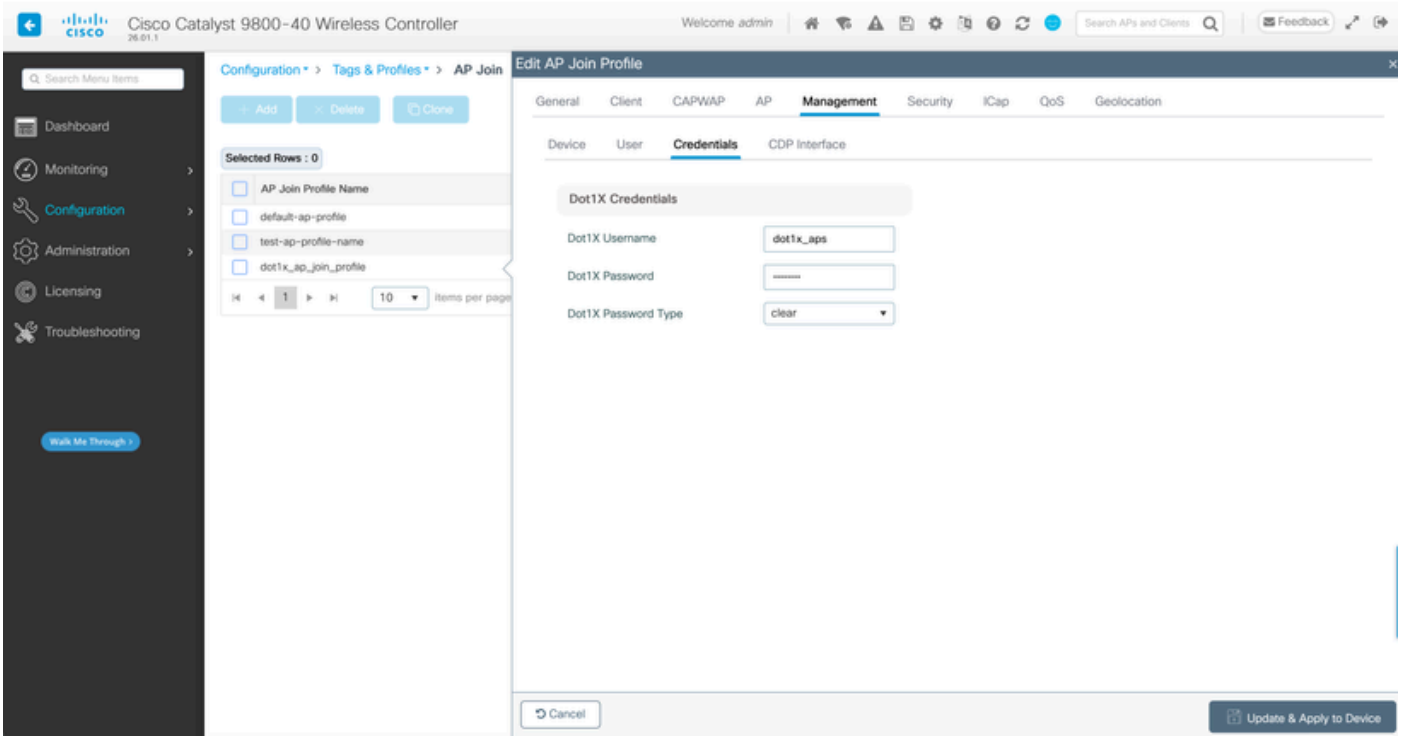
Configuração de Dot1X com fio através do Cisco 9800 Wireless LAN controller

Se você selecionou uma autenticação baseada em certificado (EAP-PEAP ou EAP-TLS [1]), será necessário decidir como próxima etapa a abordagem sobre como você está planejando emitir certificados de AP localmente significativos (LSC), por meio do SCEP [2] ou EST [3]resposta.

Ao usar EAP-FAST como em nosso cenário, é suficiente gerar um perfil de junção de AP, onde você digita o usuário e a senha Dot1X, vincula esse perfil de junção a uma tag de site e o atribui aos APs.

Configuração de GUI





Configuração 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>
```

Configurar Dot1X com fio através do Catalyst Center Plug and Play

Para que o PnP [4] funcione, o Catalyst Center precisa ser integrado ao ISE. Isso é necessário em parte devido aos certificados necessários para poder realizar a validação do servidor do lado do AP para a autenticação EAP com ISE. Para o certificado do lado do dispositivo, os APs recebem um certificado emitido pela CA do Catalyst Center que é por padrão sua própria incorporada ou se configurado por uma SubCA / SCEP da respectiva CA.

O processo de configuração por meio do PnP permite o provisionamento de certificados e/ou credenciais antes de o dispositivo ingressar nas WLCs.

Configuração do Switch

Além de a autenticação ser um mecanismo de segurança, também é uma forma de padronizar as

configurações de switchport. Por conseguinte, estas partes descrevem os elementos necessários para atingir este objetivo. Esta é uma configuração de exemplo e deve ser revisada e adaptada à sua configuração. Em geral, essa configuração permite que o Dot1x e o MAB de recuo lidem adequadamente com cenários Radius inativos, reautenticação e assim por diante.

Atributos globais do raio:

```
!
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>
!
```

Configuração 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>
```

```
!
```

Mapa de classes e modelo de serviço IBNS2.0:

```
!
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 serviço do 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
!
```

Modelos de interface:

```
!
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
!
```

Configuração da interface:

```
!
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
!
```

Obrigatório global:

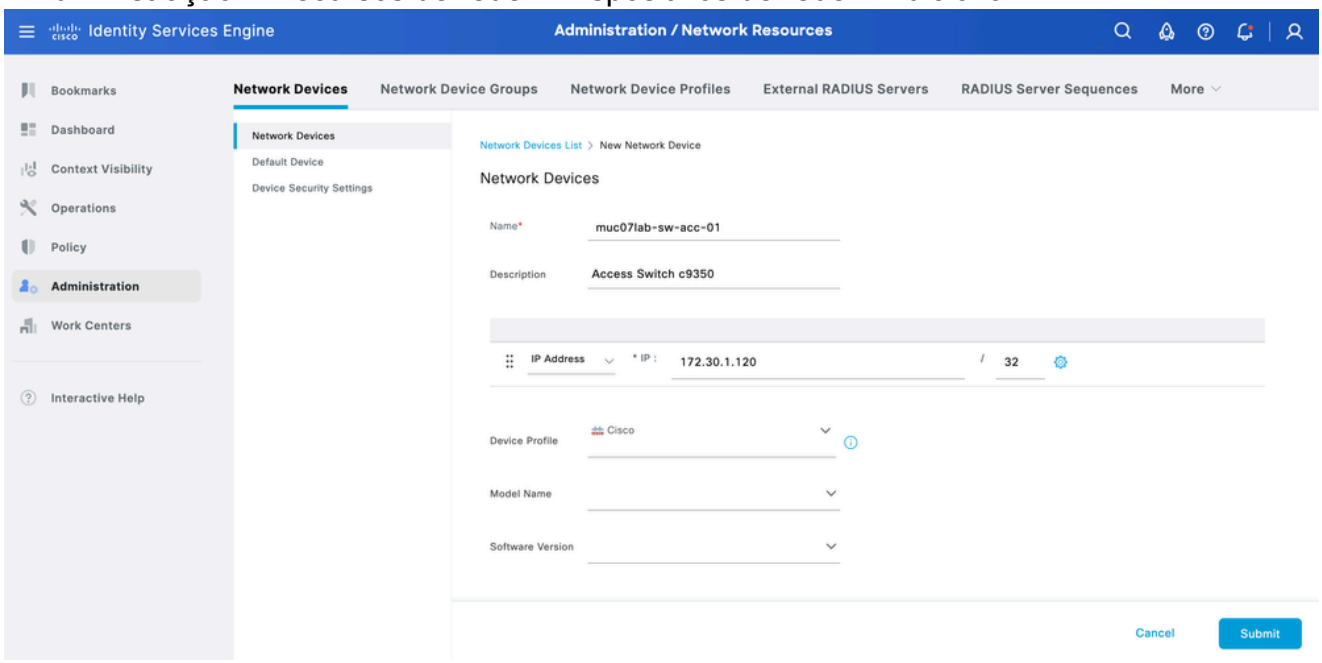
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

Note: Ao usar um CW9178, o AP apresenta dois endereços MAC durante a autenticação. Para evitar que a porta do switch entre no estado err-disabled, a porta deve ser inicialmente configurada para multiauth do modo de host. Após a autenticação 802.1X bem-sucedida, é recomendável alterar dinamicamente a configuração da porta para host-mode multi-host.

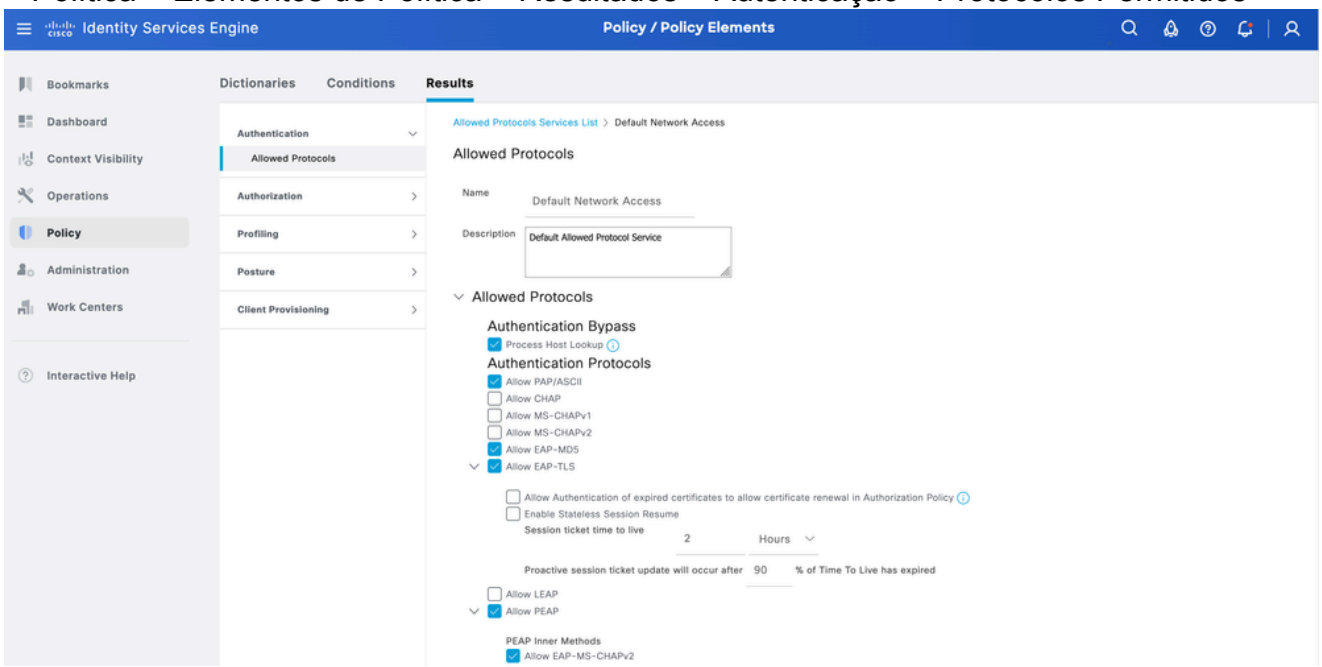
Configuração do Identity Services Engine

Finalmente, o servidor RADIUS também precisa ser configurado para permitir a autenticação. Para Dot1x com fio, há um amplo guia [5], portanto, nos concentramos apenas nas partes relevantes neste caso.

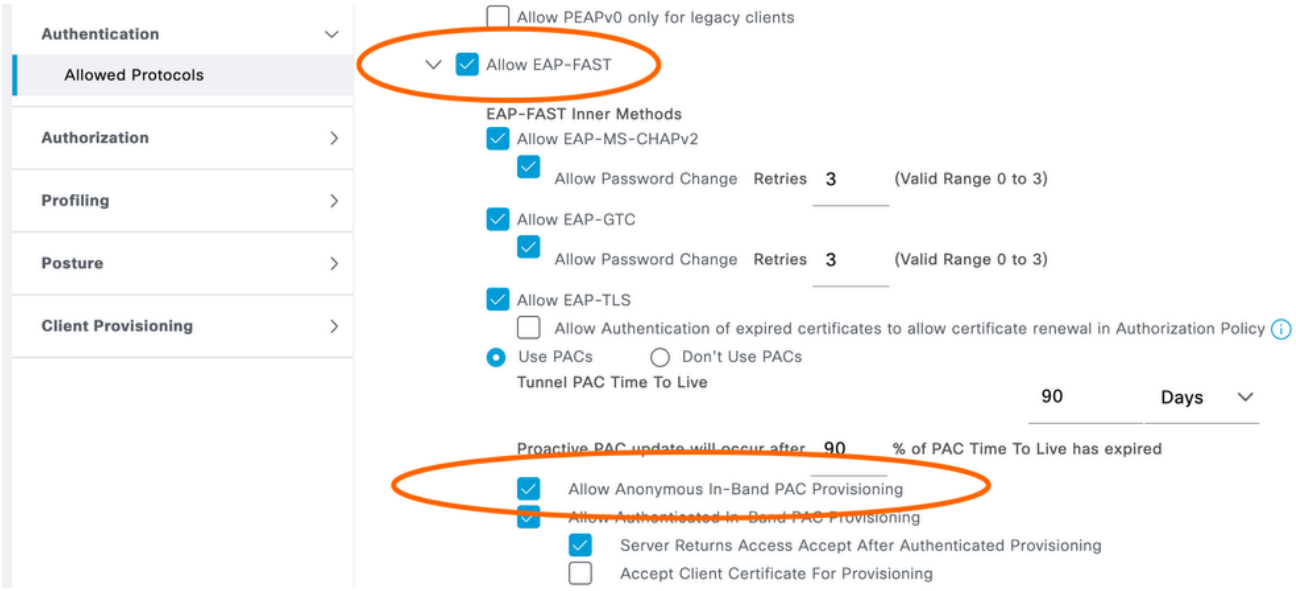
1. Adicione o switch como um dispositivo de acesso à rede:
   > Administração > Recursos de rede > Dispositivos de rede > Adicionar



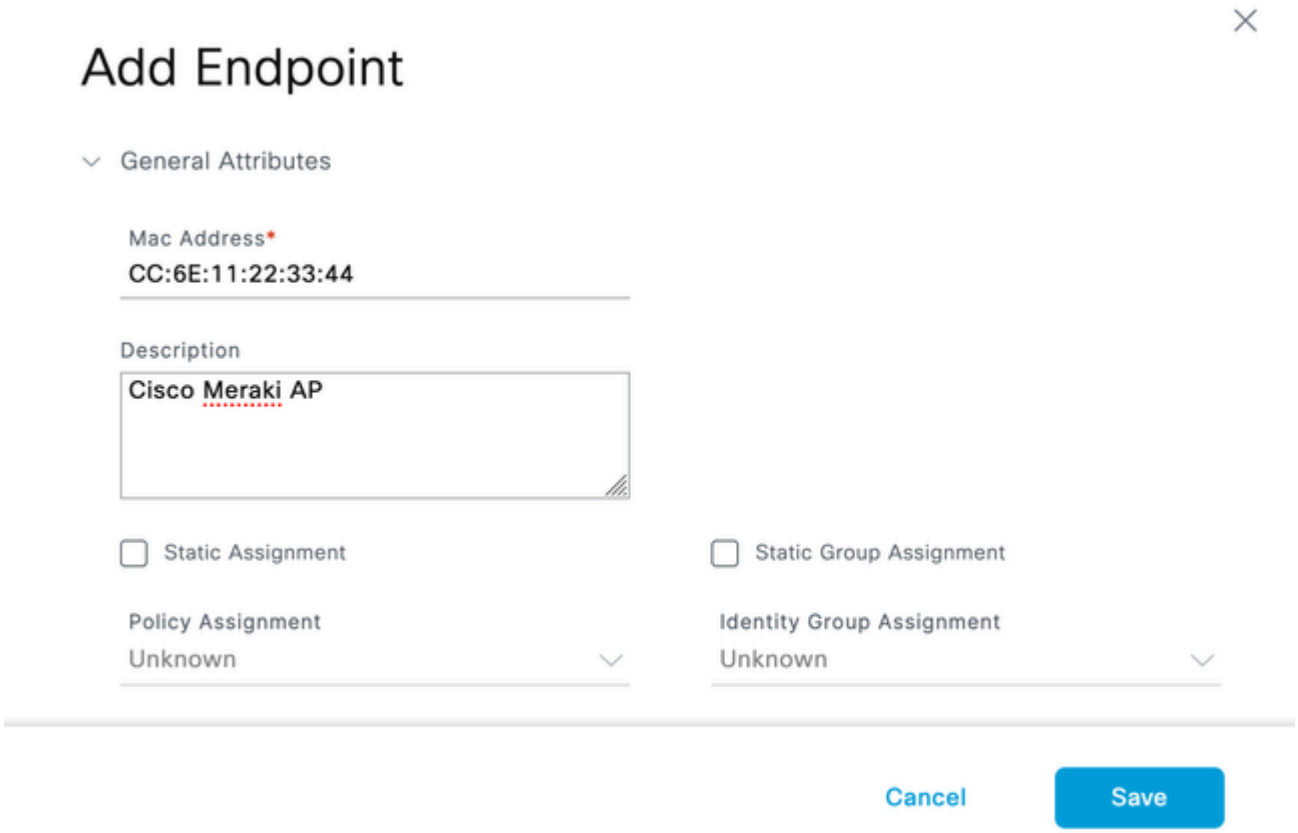
2. Habilite o protocolo EAP que você está usando:
   > Política > Elementos de Política > Resultados > Autenticação > Protocolos Permitidos



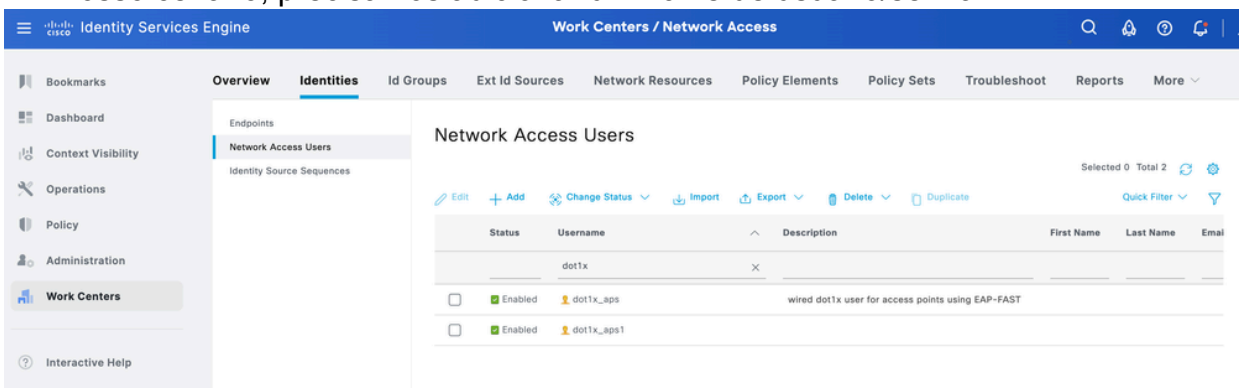
3. Em nosso cenário, como estamos usando EAP-FAST, tenha em mente que o "Provisionamento de PAC anônimo em banda" deve estar ativado:



4. Adicionar Identidades
   > Centros de trabalho > Acesso à rede > Identidades
   a. Para uma operação bem-sucedida, o processo normalmente consiste em duas etapas. Inicialmente, o AP não tem credenciais e, portanto, não pode responder à autenticação EAP. Como resultado, a porta do switch deve primeiro autenticar o AP usando MAB. Isso pode ser baseado em uma política de autorização genérica, uma política baseada em local ou criação de perfil de dispositivo. Independentemente da política usada, a autenticação MAB inicial deve ser bem-sucedida para permitir que o AP obtenha suas credenciais, seja da WLC via CAPWAP ou do Cisco Catalyst Center através de Plug and Play (PnP).

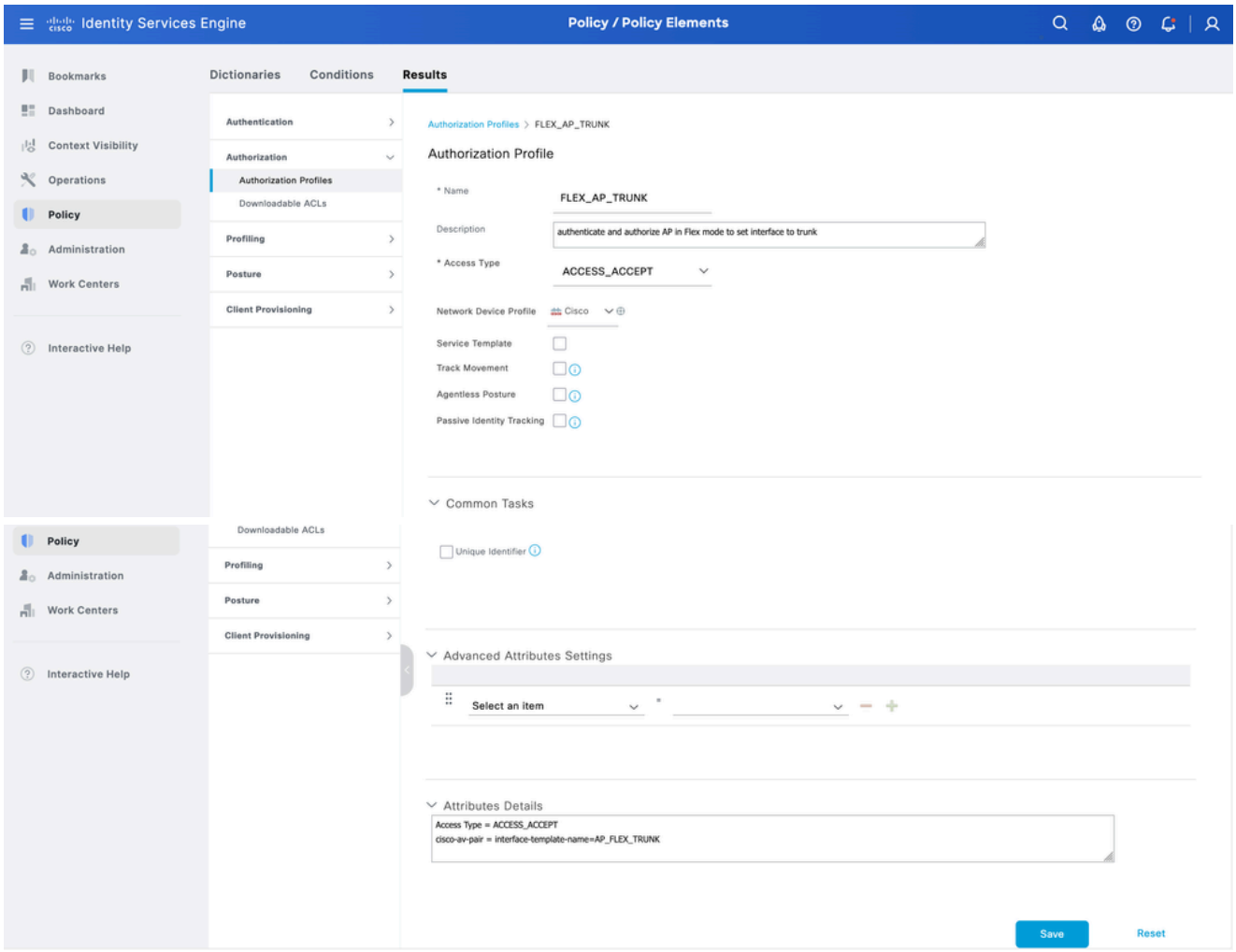


b. Depois que o AP tiver reunido as credenciais/certificado, o solicitante do AP com fio Dot1X responde ao EAPoL e o Dot1X é o método subsequente para autenticação, habilitando o AP para acesso total.
Em nosso cenário, precisamos adicionar um nome de usuário/senha:

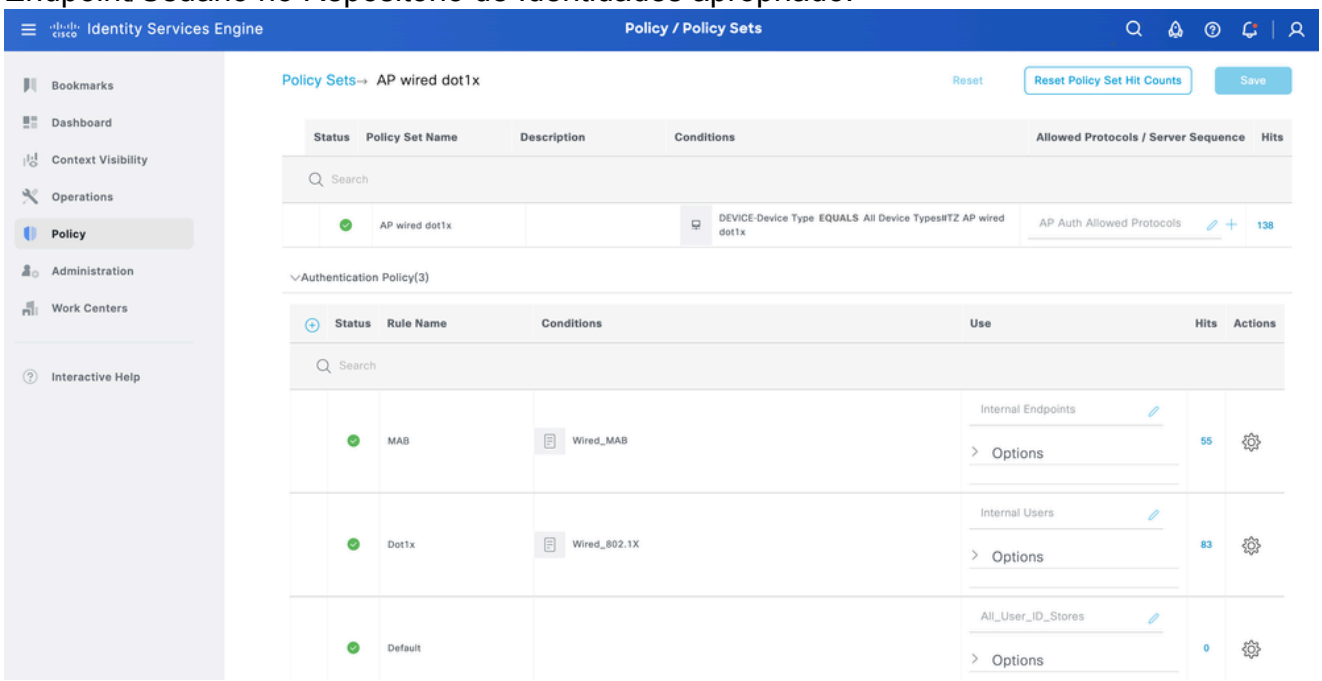


5. Criar perfil de autorização
O perfil de autorização responde com o av-pair necessário. Em nosso caso, como estamos modificando dinamicamente a porta do switch, o modelo de interface precisa ser configurado:
> Política > Elementos de Política > Resultados > Autorização > Perfis de Autorização

Nome: FLEX_AP_TRUNK
Tipo de acesso: ACCESS_ACCEPT
Modelo de interface: AP_FLEX_TRUNK

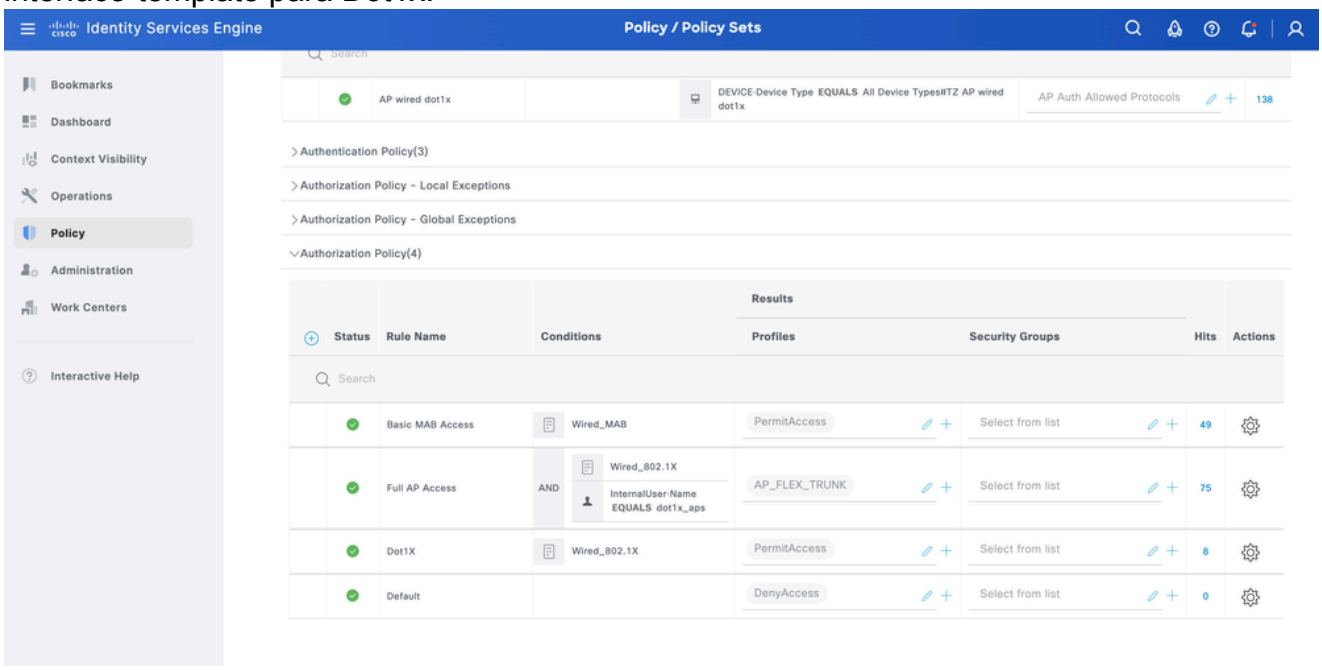


6. Criar Política de Autorização
   Crie uma Política de Autenticação que permita MAB e Dot1X com fio e procure o Endpoint/Usuário no Repositório de Identidades apropriado.



Coloque um Resultado de Autorização de Acesso limitado, dependendo de suas

necessidades para MAB, e um Acesso AP Completo incluindo o av-pair referenciado interface-template para Dot1x:



Verificar

Uma vez que esta configuração foi colocada em vigor, conecte o AP ao switch. Como pré-requisito, espera-se que as configurações de rede padrão, em nosso caso um pool de DHCP na VLAN de acesso com a Opção 43 apontando para a WLC e a comunicação CAPWAP, sejam possíveis para o AP para a WLC.

Comandos AP

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

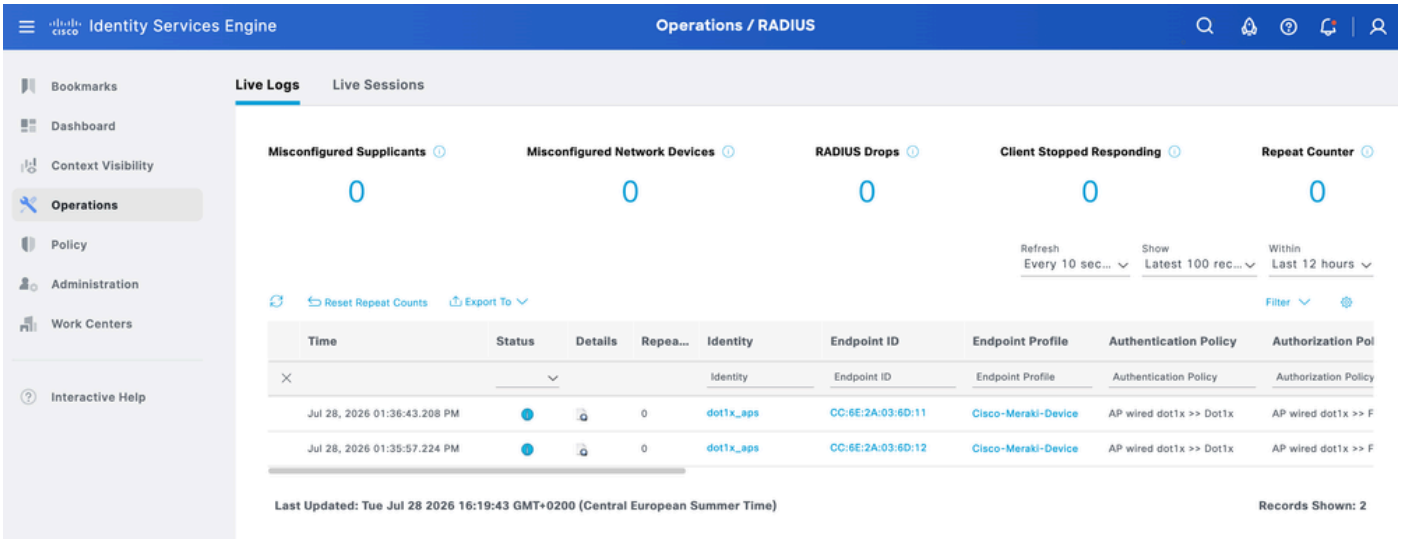
Comandos do switch

```
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

Acrônimo	Expansão
AAA	Autenticação, autorização e contabilidade
AP	Ponto de acesso
AuthC	Autenticação
AuthZ	Autorização
CA	autoridade de certificação
CISP	Protocolo de sinalização de informações do cliente
Ponto1x	IEEE 802.1X
EAP	Protocolo de autenticação extensível
EST	Inscrição em Transporte Seguro
RÁPIDO	Autenticação flexível via encapsulamento seguro
IBNS	Serviços de rede baseados em identidade
ISE	Identity Services Engine
MAB	Desvio de Autenticação MAC

NAD	Dispositivo de acesso à rede
PEAP	Protocolo de autenticação extensível protegido
SCEP	Protocolo de Registro de Certificado Simples
TLS	Segurança da camada de transporte
WLC	Controlador de LAN sem fio

Referências

[1] Configurar 802.1X em APs para PEAP ou EAP-TLS com LSC

[2] Configurar SCEP para Provisionamento de Certificado Localmente Significativo na WLC 9800

[3] Guia de implantação local do Cisco Wireless EST

[4] integração de AP seguro - Uma introdução à segurança de rede aprimorada

[5] Guia de implantação prescritiva do acesso com fio seguro do ISE

[6] seção do Guia de configuração do LSC

[7] Configurar o Solicitante 802.1X para Pontos de Acesso com Controlador 9800

[8] Secure a Flexconnect AP Switchport com Dot1x

[9] Guia de Configuração de Software do Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE 17.18.x - 802.1x

[11] Guia do usuário do Cisco Catalyst Center, versão 3.2.x - Defina as configurações de gerenciamento para um perfil de AP para dispositivos Cisco IOS XE

[12] Utilização do IBNS 2.0 e dos modelos de interface para uma configuração de switchport padrão.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.