

# Configurar o solicitante 802.1X para pontos de acesso com o controlador 9800

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configure o LAP como um solicitante 802.1x](#)

[Se O AP Já Estiver Associado À WLC:](#)

[Se O AP Ainda Não Se Uniu A Uma WLC:](#)

[Configurar o switch](#)

[Configurar o servidor ISE](#)

[Verificar](#)

[Verifique o tipo de autenticação](#)

[Verifique 802.1x na porta do switch](#)

[Troubleshoot](#)

## Introduction

Este documento descreve como configurar um ponto de acesso (AP) Cisco como um solicitante 802.1x para ser autorizado em uma porta de switch contra um servidor RADIUS.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador de LAN sem fio (WLC) e LAP (Lightweight Access Point).
- 802.1x em switches Cisco e ISE
- Protocolo de autenticação extensível (EAP)
- Serviço de Usuário de Autenticação Discada Remota (RADIUS)

## Componentes Utilizados

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

- WS-C3560CX, Cisco IOS® XE, 15.2(3r)E2

- C9800-CL-K9, Cisco IOS® XE, 17.6.1
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Nesta configuração, o ponto de acesso (AP) atua como o solicitante 802.1x e é autenticado pelo switch no ISE com o método EAP EAP-FAST.

Depois que a porta é configurada para autenticação 802.1X, o switch não permite que nenhum tráfego diferente de 802.1X passe pela porta até que o dispositivo conectado à porta seja autenticado com êxito.

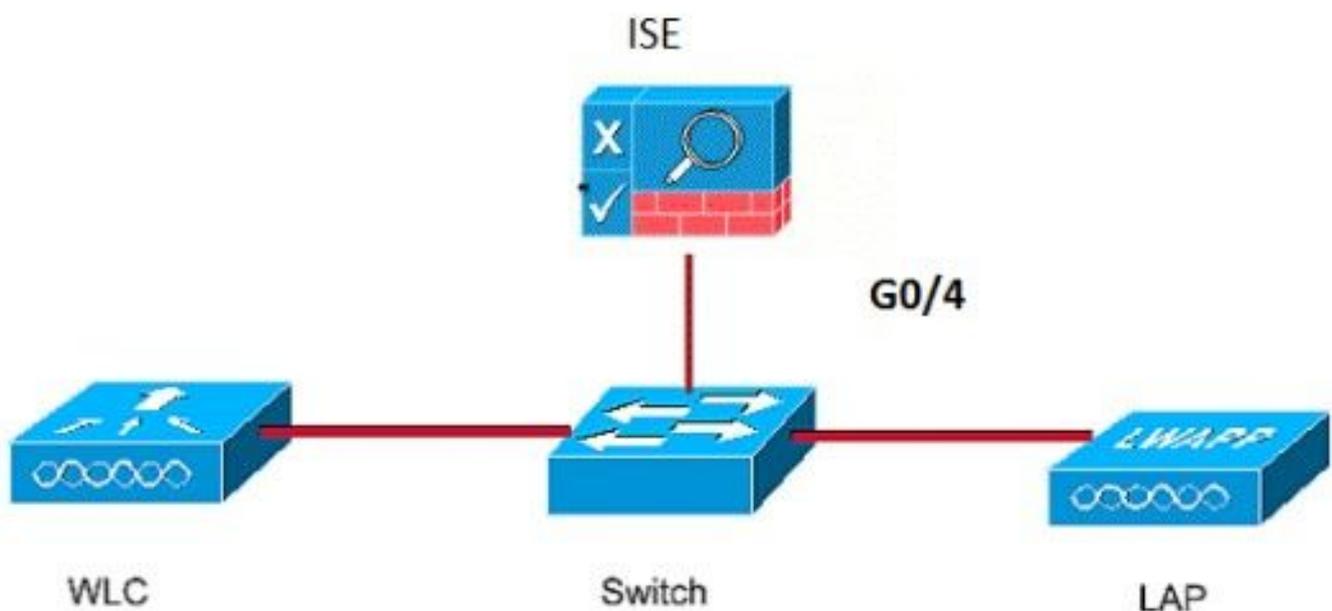
Um AP pode ser autenticado antes de ingressar em uma WLC ou depois de ingressar em uma WLC; nesse caso, você configura 802.1X no switch depois que o LAP ingressar na WLC.

## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

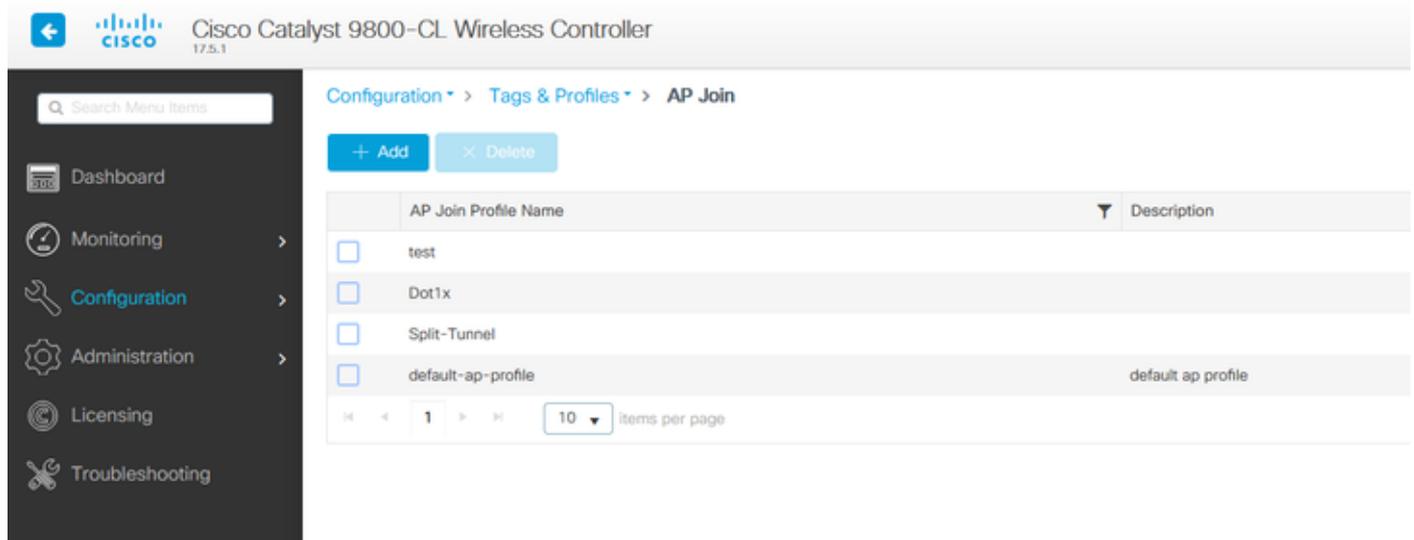


**Configure o LAP como um solicitante 802.1x**

## Se O AP Já Estiver Associado À WLC:

Configurar o tipo de autenticação 802.1x e o tipo de autenticação de AP de LSC (Locally Significant Certificate):

Etapa 1. Navegue até Configuração > **Tags e perfis** > Junção de AP > Na página Perfil de junção de AP, clique em Adicionar para adicionar um novo perfil de junção ou editar um perfil de junção de AP ao clicar no nome.



The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The breadcrumb navigation is Configuration > Tags & Profiles > AP Join. There are '+ Add' and 'X Delete' buttons. A table lists AP Join Profile Names and their descriptions:

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing '1' items per page and a dropdown menu set to '10' items per page.

Etapa 2. Na página AP Join Profile, em **AP > General**, navegue até a seção **AP EAP Auth Configuration**. Na lista suspensa **EAP Type**, escolha o tipo de EAP como EAP-FAST, EAP-TLS ou EAP-PEAP para configurar o tipo de autenticação dot1x.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

**General** Hyperlocation Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

**Client Statistics Reporting Interval**

5 GHz (sec)

2.4 GHz (sec)

**AP EAP Auth Configuration**

EAP Type

AP Authorization Type

- EAP-FAST
- EAP-TLS
- EAP-PEAP

**Extended Module**

Enable

**Mesh**

Profile Name  [Clear](#)

Etapa 3. Na lista suspensa **Tipo de autorização de AP**, escolha o tipo como CAPWAP DTLS + ou CAPWAP DTLS > Clique em **Atualizar e aplicar ao dispositivo**.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

**General** Hyperlocation Packet Capture

**Power Over Ethernet**

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

**Client Statistics Reporting Interval**

5 GHz (sec)

2.4 GHz (sec)

**AP EAP Auth Configuration**

EAP Type

AP Authorization Type

- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

**Extended Module**

Enable

**Mesh**

Profile Name  [Clear](#)

Configure o nome de usuário e a senha do 802.1x:

Etapa 1. Em **Management > Credentials > Enter Dot1x username and password details** > Escolha o tipo de senha 802.1x apropriado > Clique em **Update & Apply to Device**

Edit AP Join Profile ✕

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

**Dot1x Credentials**

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

### Se O AP Ainda Não Se Uniu A Uma WLC:

Você deve usar o console do LAP para definir as credenciais e usar estes comandos CLI: (para SO Cheetah e APs Cisco IOS®)

CLI:

```
LAP# debug capwap console cli  
LAP# capwap ap dot1x username
```

### Para Limpar As Credenciais Dot1x No AP (Se Necessário)

Para APs Cisco IOS®, depois disso, recarregue o AP:

CLI:

```
LAP# clear capwap ap dot1x
```

Para APs Cisco COS, depois disso, recarregue o AP:

CLI:

```
LAP# capwap ap dot1x disable
```

## Configurar o switch

Ative globalmente o dot1x no switch e adicione o servidor ISE ao switch.

CLI:

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

Configure a porta do switch AP.

CLI:

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

Se o AP estiver no **modo Flex Connect, switching local**, uma configuração adicional deverá ser feita na interface do switch para permitir vários endereços MAC na porta, já que o tráfego do cliente é liberado no nível do AP:

```
authentication host-mode multi-host
```

**Nota:** Significa que o leitor deve tomar nota. As notas contêm sugestões úteis ou referências a materiais não abordados no documento.

**Observação:** o modo de vários hosts autentica o primeiro endereço MAC e depois permite um número ilimitado de outros endereços MAC. Ative o modo de host nas portas do switch se o AP conectado tiver sido configurado com o modo de switching local. Permite que o tráfego do cliente passe pela porta do switch. Se quiser um caminho de tráfego seguro, habilite dot1x na WLAN para proteger os dados do cliente

## Configurar o servidor ISE

Etapa 1. Adicione o switch como um dispositivo de rede no servidor ISE. Navegue até Administração > Recursos de rede > Dispositivos de rede > Clique em Adicionar > Insira o nome do dispositivo, o endereço IP, habilite as Configurações de autenticação RADIUS, Especifique o valor de segredo compartilhado, porta COA (ou deixe como padrão) > Enviar.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - Network Resources'. The left sidebar has 'Network Devices' highlighted. The main content area is titled 'Network Devices List > New Network Device'. The form contains the following fields and options:

- Name: MySwitch
- Description: (empty)
- IP Address: 10.48.39.100 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Location: All Locations (with 'Set To Default' button)
- IPSEC: Is IPSEC Device (with 'Set To Default' button)
- Device Type: All Device Types (with 'Set To Default' button)
- RADIUS Authentication Settings
  - RADIUS UDP Settings
    - Protocol: RADIUS
    - Shared Secret: (masked) (with 'Show' button)
    - Use Second Shared Secret:  (with 'Show' button)
    - CoA Port: 1700 (with 'Set To Default' button)
  - RADIUS DTLS Settings
    - DTLS Required:  (with 'Show' button)
    - Shared Secret: radius/dtls (with 'Show' button)

Etapa 2. Adicione as credenciais do AP ao ISE. Navegue até Administração > Gerenciamento de identidades > Identidades > Usuários e clique no botão Adicionar para adicionar um usuário. Você precisa inserir aqui as credenciais que você configurou no seu perfil de ingresso AP em seu WLC. Observe que o usuário é colocado no grupo padrão aqui, mas isso pode ser ajustado de acordo com seus requisitos.

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users  
Latest Manual Network Scan Res...

Network Access User

Name dot1x

Status  Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

Login Password ..... Generate Password

Enable Password ..... Generate Password

User Information

Account Options

Account Disable Policy

User Groups

ALL\_ACCOUNTS (default)

Etapa 3. No ISE, configure a **política de autenticação** e a **política de autorização**. Vá para **Policy > Policy Sets** e selecione o conjunto de políticas que deseja configurar e a seta azul à direita. Nesse caso, o conjunto de políticas padrão é usado, mas é possível personalizá-lo de acordo com o requisito.

Cisco ISE Policy - Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	6		

Reset Save

Em seguida, configure a **Authentication Policy** e a **Authorization Policy**. As políticas mostradas aqui são as políticas padrão criadas no servidor ISE, mas podem ser adaptadas e personalizadas de acordo com sua necessidade.

Neste exemplo, a configuração pode ser traduzida em : "Se 802.1X com fio for usado e o usuário for conhecido no servidor ISE, então permitiremos acesso aos usuários para os quais a autenticação foi bem-sucedida". O AP é então autorizado no servidor ISE.

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	⚙️
●	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy (12)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions	
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	+	Select from list	+	6	⚙️
●	Default		DenyAccess x	+	Select from list	+	0	⚙️

Etapa 4. Certifique-se de que nos protocolos permitidos que definem o acesso de rede padrão, EAP-FAST seja permitido. Navegue até Política > Elementos de política > Autenticação > Resultados > Protocolos permitidos > Acesso padrão à rede > Ativar Permitir EAP-TLS > Salvar.

Cisco ISE Policy - Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

- Process Host Lookup

Authentication Protocols

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1
- Allow MS-CHAPv2
- Allow EAP-MD5
- Allow EAP-TLS

Expand  Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

## Verifique o tipo de autenticação

O comando show exibe as informações de autenticação de um perfil de AP:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

Exemplo:

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE   : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

## Verifique 802.1x na porta do switch

O comando show exibe o estado de autenticação de 802.1x na porta do switch:

CLI:

```
Switch# show dot1x all
```

Exemplo de saída:

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout         = 0
SuppTimeout           = 30
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
```

Verifique se a porta foi autenticada ou não

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

Exemplo de saída:

```
Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout         = 0
SuppTimeout           = 30
ReAuthMax              = 2
MaxReq                 = 2
```

TxPeriod = 30

Dot1x Authenticator Client List

```
-----  
EAP Method = FAST  
Supplicant = f4db.e67e.dd16  
Session ID = 0A30279E00000BB7411A6BC4  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE
```

ED

Auth BEND SM State = IDLE

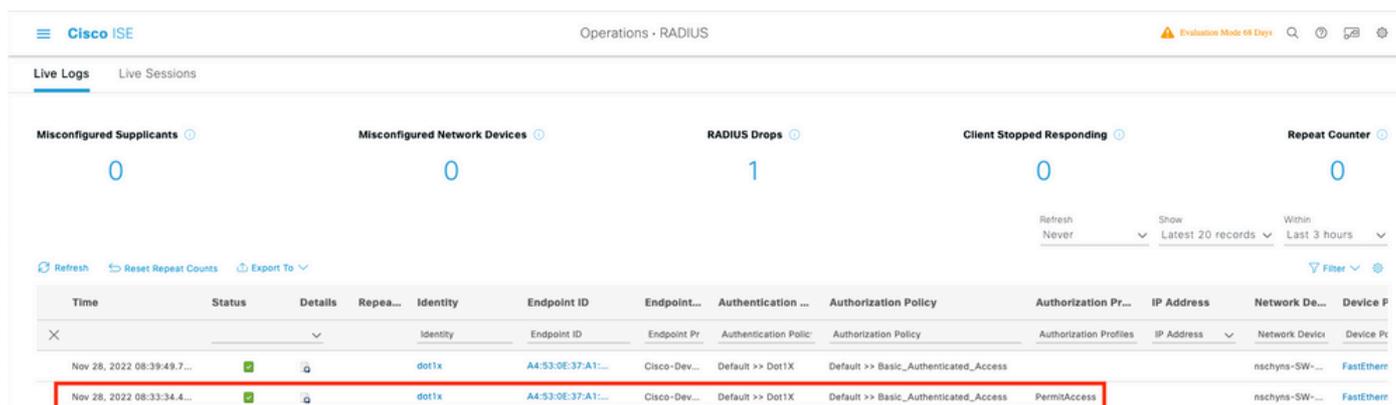
Do CLI:

Switch#show authentication sessions

Exemplo de saída:

```
Interface MAC Address Method Domain Status Fg Session ID  
Gi0/8 f4db.e67e.dd16 dot1x DATA Auth 0A30279E00000BB7411A6BC4
```

No ISE, escolha **Operations > Radius LiveLogs** e confirme se a autenticação foi bem-sucedida e se o perfil de autorização correto foi enviado por push.



The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are several summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (0). Below these cards is a table of Live Logs. The table has columns for Time, Status, Details, Repeated, Identity, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, Authorization Profiles, IP Address, Network Device, and Device Port. A row is highlighted with a red border, showing a successful authentication session on Nov 28, 2022, at 08:33:34.4. The Identity is dot1x, Endpoint ID is A4:53:0E:37:A1:..., and the Authorization Policy is Default >> Basic\_Authenticated\_Access. The Authorization Profiles column shows PermitAccess.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	Success	...		dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	nschyns-SW-...	FastEther		
Nov 28, 2022 08:33:34.4...	Success	...		dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess	nschyns-SW-...	FastEther	

## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

1. Insira o comando **ping** para verificar se o servidor ISE pode ser acessado do switch.
2. Certifique-se de que o switch esteja configurado como um cliente AAA no servidor ISE.
3. Certifique-se de que o segredo compartilhado seja o mesmo entre o switch e o servidor ISE.
4. Verifique se EAP-FAST está habilitado no servidor ISE.
5. Verifique se as credenciais 802.1x estão configuradas para o LAP e se são as mesmas no servidor ISE.

**Observação:** o nome de usuário e a senha fazem distinção entre maiúsculas e minúsculas.

6. Se a autenticação falhar, digite estes comandos no switch: **debug dot1x** e **debug authentication**.

Observe que os pontos de acesso baseados no Cisco IOS (onda 1 do 802.11ac) não suportam as versões 1.1 e 1.2 do TLS. Isso pode causar um problema se o seu servidor ISE ou RADIUS estiver configurado para permitir apenas TLS 1.2 dentro da autenticação 802.1X.

## 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.