

Configurar o ponto de acesso leve como um solicitante 802.1x

Introduction

Este documento descreve como configurar um Lightweight Access Point (LAP) como um suplicante 802.1x para se autenticar no servidor Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador de LAN sem fio (WLC) e LAP
- 802.1x em switches Cisco
- ISE
- EAP (Extensible Authentication Protocol) - Autenticação flexível via Secure Tunneling (FAST)

Componentes Utilizados

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

- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- ISE 2.0

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. If your network is live, make sure that you understand the potential impact of any command.

Informações de Apoio

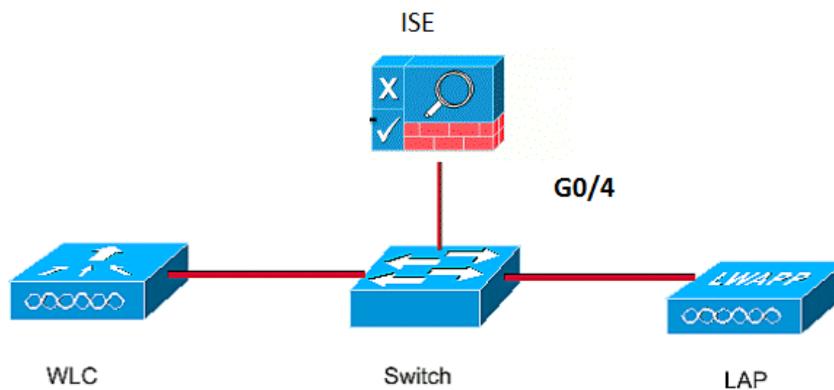
Nessa configuração, o ponto de acesso (AP) atua como o suplicante 802.1x e é autenticado pelo switch em relação ao ISE que usa EAP-FAST com provisionamento de PAC (Protected Access Credentials) anônimo. Quando a porta é configurada para autenticação 802.1x, o switch não permite que nenhum tráfego diferente do 802.1x passe pela porta até que o dispositivo conectado à porta se autentique com êxito. Um AP pode ser autenticado antes de ingressar em uma WLC ou depois de ingressar em uma WLC, caso em que você configura 802.1x no switch depois que o LAP ingressa 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:



Configurações

Este documento usa estes endereços IP:

- O endereço IP do switch é 10.48.39.141
- O endereço IP do servidor ISE é 10.48.39.161
- O endereço IP da WLC é 10.48.39.142

Configurar o LAP

Nesta seção, você recebe as informações para configurar o LAP como um suplicante 802.1x.

1. Se o AP já estiver associado à WLC, vá para a guia Wireless e clique no AP, vá para o campo Credenciais e, no cabeçalho Credenciais do 802.1x, marque a caixa de seleção **Sobrepôr credenciais globais** para definir o nome de usuário e a senha 802.1x para este AP.

Você também pode definir um nome de usuário e uma senha comuns para todos os APs que estão associados à WLC com o menu Configuração global.

2. Se o AP ainda não ingressou em uma WLC, você deve usar o console no LAP para definir as credenciais e usar estes comandos CLI:

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

Configurar o switch

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

```
aaa new-model
!
aaa authentication dot1x default group radius
!
dot1x system-auth-control
!
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123A0C0411045D5679
```

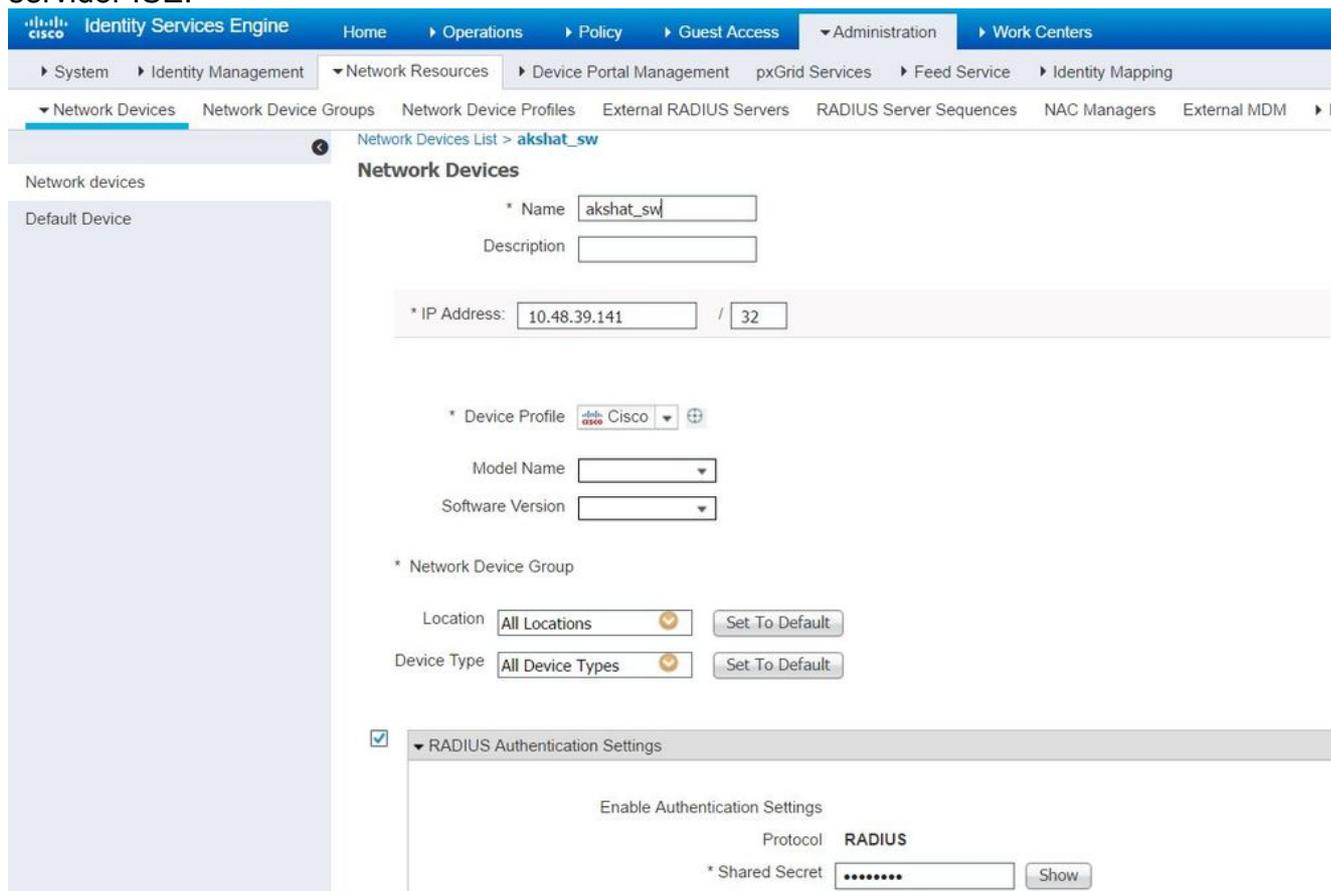
2. Agora, configure a porta do switch AP.

```
interface GigabitEthernet0/4

switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

Configurar o servidor ISE

1. Adicione o switch como um cliente de Autenticação, Autorização e Auditoria (AAA) no servidor ISE.



Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location

Network devices

Default Device

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> GurpWLC1	10.48.39.155/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> GurpWLC2	10.48.39.156/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> akshat_sw	10.48.39.141/32	Cisco	All Locations	All Device Types

2. No ISE, configure a política de autenticação e a política de autorização. Nesse caso, a regra de autenticação padrão que é wired dot.1x é usada, mas é possível personalizá-la de acordo com o requisito.

Identity Services Engine Home Operations Policy Guest Access Administration Work

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MABAllow Protocols	: Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1XAllow Protocols	: Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

Certifique-se de que nos protocolos permitidos de Acesso à Rede Padrão, EAP-FAST seja permitido.

The screenshot shows the configuration for the 'Allow EAP-FAST' policy element. The left sidebar contains a tree view with 'Authentication' expanded. The main configuration area includes the following settings:

- Allow EAP-FAST
- EAP-FAST Inner Methods:
 - Allow EAP-MS-CHAPv2
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-GTC
 - Allow Password Change Retries (Valid Range 0 to 3)
 - Allow EAP-TLS
 - Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
- Use PACs Don't Use PACs
- Tunnel PAC Time To Live: Days
- Proactive PAC update will occur after % of PAC Time To Live has expired
- Allow Anonymous In-Band PAC Provisioning
- Allow Authenticated In-Band PAC Provisioning
 - Server Returns Access Accept After Authenticated Provisioning
 - Accept Client Certificate For Provisioning

3. Quanto à política de autorização (Port_AuthZ), nesse caso, as credenciais de AP foram adicionadas a um grupo de usuários (APs). A condição usada foi "Se o usuário pertencer ao AP do grupo e fizer o dot1x com fio, pressione o Perfil de autorização padrão para acessar." Novamente, isso pode ser personalizado de acordo com o requisito.

The screenshot shows the 'Authorization Policy' configuration page. It includes a header with navigation tabs and a main section titled 'Authorization Policy' with the following text:

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies:

▼ Exceptions (0)

[+ Create a New Rule](#)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

The screenshot shows the 'Identity Groups' configuration page. The left sidebar shows a tree view with 'User Identity Groups' selected. The main configuration area is titled 'User Identity Groups > APs' and includes the following fields:

- * Name:
- Description:
- Buttons: Save, Reset

User Identity Groups > APs

Identity Group

* Name:

Description:

Save Reset

Member Users

Users

Selected 0 | Total 1

+ Add - Delete

Show:

Status	Email	Username	First Name	Last Name
<input type="checkbox"/> <input checked="" type="checkbox"/> Enabled		ritmahaj		

Verificar

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

Quando o 802.1x é ativado na porta do switch, todo o tráfego, exceto o 802.1x, é bloqueado pela porta. O LAP, que se já estiver registrado na WLC, é desassociado. Somente após uma autenticação 802.1x bem-sucedida é permitido que outro tráfego passe. O registro bem-sucedido do LAP para a WLC depois que o 802.1x é ativado no switch indica que a autenticação do LAP é bem-sucedida. Você também pode usar esses métodos para verificar se o LAP foi autenticado.

1. No switch, insira um dos comandos **show** para verificar se a porta foi autenticada ou não.

```
akshat_sw#show dot1x interface g0/4
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
akshat_sw#show dot1x interface g0/4 details
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
Dot1x Authenticator Client List
-----
```

```
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
```

```
akshat_sw#show authentication sessions
```

```
Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. No ISE, escolha **Operations > Radius Livelogs** e verifique se a autenticação foi bem-sucedida e se o perfil de autorização correto foi enviado.

Time	Status	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-03-09 10:32:28.956	All		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess
2017-03-09 10:31:29.227	All		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess

Troubleshoot

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

1. Insira o comando **ping** para verificar se o servidor ISE está acessível no switch.
2. Verifique se o switch está configurado como um cliente AAA no servidor ISE.
3. Verifique se o segredo compartilhado é o mesmo entre o switch e o servidor ACS.
4. Verifique se o EAP-FAST está ativado no servidor ISE.
5. Verifique se as credenciais 802.1x estão configuradas para o LAP e são as mesmas no servidor ISE. **Note:** O nome de usuário e a senha diferenciam maiúsculas e minúsculas.
6. Se a autenticação falhar, insira estes comandos no switch: **debug dot1x** e **debug authentication**.