

Configurar o Access point de pouco peso como um suplicante do 802.1x

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar o REGAÇO](#)

[Configurar o interruptor](#)

[Configurar o server ISE](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como configurar um Access point de pouco peso (REGAÇO) enquanto um suplicante do 802.1x a fim autenticar contra o server do Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador do Wireless LAN (WLC) e REGAÇO
- 802.1x em switch Cisco
- ISE
- Extensible Authentication Protocol (EAP) - Autenticação flexível através do Tunelamento seguro (RÁPIDO)

[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

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

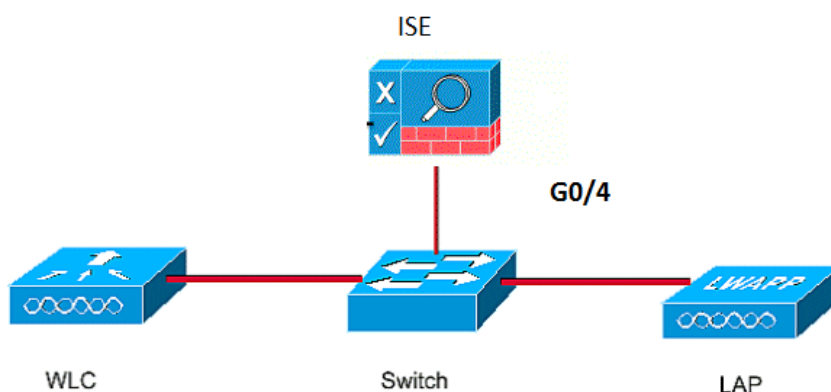
No este setup o Access Point (AP) atua como o suplicante do 802.1x e é autenticado pelo interruptor contra o ISE que usa EAP-FAST com abastecimento protegido anônimo das credenciais do acesso (PAC). Uma vez que a porta é configurada para a autenticação do 802.1x, o interruptor não permite que nenhum tráfego a não ser o tráfego do 802.1x passe através da porta até que o dispositivo conectado à porta autentique com sucesso. Um AP pode ser autenticado ou antes que se junte a um WLC ou depois que se juntou a um WLC, neste caso você configura o 802.1x no interruptor depois que o REGAÇO se junta ao 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

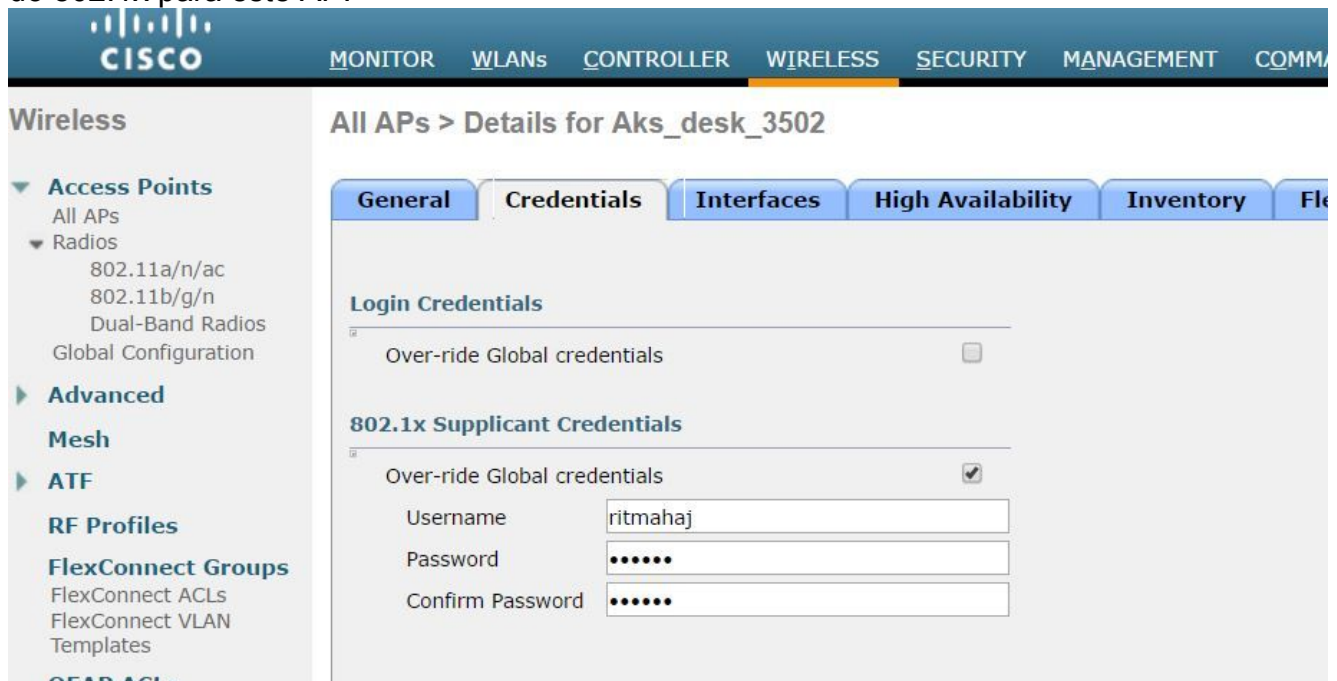
Este documento usa estes endereços IP de Um ou Mais Servidores Cisco ICM NT:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do interruptor é 10.48.39.141
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do server ISE é 10.48.39.161
- O endereço IP de Um ou Mais Servidores Cisco ICM NT do WLC é 10.48.39.142

Configurar o REGAÇO

Nesta seção, você é apresentado com a informação para configurar o REGAÇO como um suplicante do 802.1x.

1. Se o AP é juntado já ao WLC, vai a aba wireless e clica sobre o AP, vai as credenciais coloca e sob as credenciais do suplicante do 802.1x que dirigem, verifica a caixa de **verificação de credenciais global da ultrapassagem** a fim ajustar o nome de usuário e senha do 802.1x para este AP.



The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMM'. The left sidebar is titled 'Wireless' and contains a tree view with 'Access Points' (All APs, Radios, Dual-Band Radios, Global Configuration), 'Advanced', 'Mesh', 'ATF', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'All APs > Details for Aks_desk_3502' and has tabs for 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', and 'Flex'. The 'Credentials' tab is active, showing 'Login Credentials' and '802.1x Supplicant Credentials'. Under '802.1x Supplicant Credentials', the 'Over-ride Global credentials' checkbox is checked. The 'Username' field contains 'ritmahaj', and the 'Password' and 'Confirm Password' fields are masked with dots.

Você pode igualmente ajustar um nome de usuário e senha comum para todos os AP que são juntados ao WLC com o menu da configuração global.

The screenshot shows the Cisco Wireless configuration interface. The 'Global Configuration' link under 'Dual-Band Radios' is highlighted with a red box. The page displays various configuration sections:

- Ethernet Interface# CDP State:** A table with 5 rows (0-4) and a checked checkbox for each.
- Radio Slot# CDP State:** A table with 3 rows (0-2) and a checked checkbox for each.
- Login Credentials:** Fields for Username, Password, and Enable Password.
- 802.1x Supplicant Credentials:** A checked checkbox for 802.1x Authentication, and fields for Username, Password, and Confirm Password.
- TCP MSS:** A checkbox for Global TCP Adjust MSS (IPV4: 536 - 1363, IPV6: 1220 - 1331).
- AP Retransmit Config Parameters:** Fields for AP Retransmit Count (5) and AP Retransmit Interval (3).
- OEAP Config Parameters:** A checkbox for Disable Local Access.

2. Se o AP não se juntou a um WLC ainda, você deve consolar no REGAÇO a fim ajustar as credenciais e usar estes comandos CLI:

```
LAP#debug capwap console cli
```

```
LAP#capwap ap dot1x username <username> password <password>
```

Configurar o interruptor

1. Permita o dot1x no interruptor globalmente e adicionar o server ISE ao interruptor.

```
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, configurar a porta de 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 server ISE

1. Adicionar o interruptor como um cliente do Authentication, Authorization, and Accounting (AAA) no server ISE.

Identity Services Engine 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

Network Devices List > akshat_sw

Network devices

Default Device

Network Devices

* Name: akshat_sw

Description: []

* IP Address: 10.48.39.141 / 32

* Device Profile: Cisco

Model Name: []

Software Version: []

* Network Device Group

Location: All Locations [Set To Default]

Device Type: All Device Types [Set To Default]

RADIUS Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: [] [Show]

Identity Services Engine 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

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, configurar a política da política de autenticação e da autorização. Neste caso, a regra da autenticação padrão que é dot.1x prendido é usada, mas um pode personalizá-lo conforme a exigência.

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_MAB	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X	Allow 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

Assegure isso nos protocolos permitidos que o acesso de rede padrão, EAP-FAST são permitidos.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

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
 - 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

- Quanto para à política da autorização (Port_AuthZ), as credenciais AP foram adicionadas neste caso a um grupo de usuário (AP). A circunstância usada era “se o usuário pertence ao grupo AP e fazer o dot1x prendido, a seguir empurra o acesso da licença do perfil da autorização do padrão.” Além disso, isto pode ser personalizado conforme a exigência.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authorization Policy

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
✓	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > APs

Identity Group

* Name: APs

Description: Credentials for APs

Save Reset

Member Users

Users Selected 0 | Total 1

+ Add - Delete Show All

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

Verificar

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

Uma vez que o 802.1x é permitido na porta de switch, todo o tráfego a não ser que o tráfego do 802.1x seja obstruído através da porta. O REGAÇO, que se já registrado ao WLC, obtém dissociado. Somente depois que uma autenticação bem sucedida do 802.1x é o outro tráfego permitido passar completamente. O registro bem-sucedido do REGAÇO ao WLC depois que o 802.1x é permitido no interruptor indica que a autenticação do REGAÇO é bem sucedida. Você pode igualmente usar estes métodos a fim verificar se o REGAÇO autenticou.

1. No interruptor, inscreva um dos **comandos show** a fim 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 **operações > raio LiveLogs** e veja que a autenticação é bem sucedida e o perfil correto da autorização está empurrado.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-03-09 10:32:28.956	All		0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess
2017-03-09 10:31:29.227	All		0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

1. Inscreva o **comando ping** a fim verificar se o server ISE é alcançável do interruptor.
2. Certifique-se de que o interruptor está configurado como um cliente de AAA no server ISE.
3. Assegure-se de que o segredo compartilhado seja o mesmo entre o interruptor e o servidor ACS.
4. Verifique se EAP-FAST é permitido no server ISE.
5. Verifique se as credenciais do 802.1x são configuradas para o REGAÇO e são mesmas no server ISE. **Note:** O nome de usuário e senha é diferenciando maiúsculas e minúsculas.
6. Se a autenticação falha, incorpore estes comandos no interruptor: **debugar o dot1x** e o **debug authentication**.