# Configurar o ACS 5.2 para autenticação baseada em porta com um LAP

# Contents

Introduction **Prerequisites Requirements** Componentes Utilizados Conventions Informações de Apoio Configurar Diagrama de Rede **Hipóteses Configuration Steps Configurar LAP** Configurar o switch **Configurar servidor RADIUS** Configurar recursos de rede Configurar usuários Definir Elementos da Política Aplicar políticas de acesso Verificar Troubleshoot Informações Relacionadas

## **Introduction**

Este documento descreve como configurar um Lightweight Access Point (LAP) como um solicitante 802.1x para autenticar em um servidor RADIUS, como um Access Control Server (ACS) 5.2.

# **Prerequisites**

### **Requirements**

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Ter conhecimento básico da controladora Wireless LAN (WLC) e dos LAPs.
- Ter conhecimento funcional do servidor AAA.
- Ter conhecimento completo das redes wireless e das questões de segurança wireless.

#### **Componentes Utilizados**

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

- WLC Cisco 5508 com firmware versão 7.0.220.0
- LAP Cisco 3502 Series
- Cisco Secure ACS que executa a versão 5.2
- Switch Cisco Série 3560

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.

#### **Conventions**

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

## Informações de Apoio

Os LAPs têm certificados X.509 instalados de fábrica - assinados por uma chave privada - que são gravados no dispositivo no momento da fabricação. Os LAPs usam esse certificado para autenticar com a WLC no processo de junção. Esse método descreve outra maneira de autenticar LAPs. Com o software WLC, você pode configurar a autenticação 802.1x entre um ponto de acesso (AP) Cisco Aironet e um switch Cisco. Nesse caso, o AP atua como o solicitante 802.1x e é autenticado pelo switch em um servidor RADIUS (ACS) que usa EAP-FAST com fornecimento de PAC anônimo. Depois de configurado 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:



Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP do servidor ACS (RADIUS) é 192.168.150.24.
- O endereço da interface do gerenciador de AP e gerenciamento do WLC é 192.168.75.44.
- O endereço dos servidores DHCP é 192.168.150.25.
- O LAP é colocado na VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

#### **Hipóteses**

- Os switches são configurados para todas as VLANs de Camada 3.
- O servidor DHCP recebe um escopo DHCP.
- Existe conectividade de Camada 3 entre todos os dispositivos na rede.
- O LAP já está unido à WLC.
- Cada VLAN tem uma máscara /24.
- O ACS 5.2 tem um certificado autoassinado instalado.

# **Configuration Steps**

Esta configuração é dividida em três categorias:

- 1. Configure o LAP.
- 2. Configure o switch.
- 3. Configure o servidor RADIUS.

#### **Configurar LAP**

Suposições:

O LAP já está registrado na WLC usando a opção 43, DNS ou o IP da interface de gerenciamento da WLC configurado estaticamente.

Conclua estes passos:

1. Vá para Wireless > Access Points > All APs para verificar o registro do LAP na



 Você pode configurar as credenciais 802.1x (ou seja, nome de usuário/senha) para todos os LAPs de duas maneiras: GlobalmentePara um LAP já associado, você pode definir as credenciais globalmente de modo que cada LAP que se une à WLC herde essas credenciais.

uluilu cisco	MONETOR WLAND CON	ROLLER WIRELESS SEC	URETY MINAGEMENT	COMMANDS	HELP (CEDBACK	Saye Configuration   Bing   Legout Belie
Wireless	Global Configuration					Apply
<ul> <li>Access Points Al APs</li> <li>Rodos</li> <li>802.33x/n</li> <li>802.33x/n</li> <li>Clubal Configuration</li> <li>Advanced</li> <li>HalkAP Groups</li> <li>902.31x/n</li> <li>802.31x/n</li> <li>802.31x/n</li> <li>Hedia Streams</li> </ul>	CDP COP State			High Availability AP Heatbest Timest(1-33) [97		
	Ethernet Interface# 0 1 2 3 Redio Slot# 0 1	CDP State		Local Med H-REAP M AR Prime Back-up Back-up Back-up Back-up	le AP fest Heartbeat Timer State lode AP Fast Heartbeat Timer State rry Discovery Timeout(30 to 3800) Primary Controller 3P Address Primary Controller rame Secondary Controller 3P Address Secondary Controller name	Disable      Disable
Country	2 3	2 2		TCP MSS		
+ QeS	Login Credentials			Global TC	P Adjust MSS	
	Username Password			AP Retran	ismit Config Parameters	80 C
	Enable Password			AD Ratin	namit Interval	3
	802.1x Supplicant Cres 902.1x Authentication Unername Password Canfirm Password	dentiols				
	AP Fallover Priority Global AP Failover Priorit	V Disable -				
	AP Image Pre-downlos	id	chann (			
	Interchange Image	Constraint Ba				

IndividualmenteConfigurar perfis 802.1 x por AP. Em nosso exemplo, configuraremos credenciais por AP.Vá para Wireless > All APs e selecione o AP em questão.Adicione o nome de usuário e a senha nos campos Credenciais do solicitante



Observação: as credenciais de login são usadas para Telnet, SSH ou console no AP.

3. Configure a seção Alta disponibilidade e clique em **Aplicar**.

 cisco	MONITOR MUANS CONTROLLER MIRELESS SECURITY MUNUSEMENT COMMANDS HELP EEEDBACK	Saya Configuration   Bing	Logout   Beiro
Wireless	All APs > Details for 3502e	< Bock	Apply
<ul> <li>Access Points All Ars</li> <li>Radios</li> <li>832.11a/n</li> <li>832.11a/n</li> <li>832.11a/n</li> <li>832.11a/n</li> <li>61abel Configuration</li> <li>Advanced</li> <li>Mesh</li> <li>HREAP Groups</li> <li>802.11a/n</li> </ul>	General     Credentials     Interfaces     High Availability     Investory     Advanced       Norme     Resegnment 3P Address       Primary Castrollar     \$556-3     \$192.368.75.44       Secondary Castrollar     S566-3     \$192.368.75.44       AP Failover Priority     Low     *		
▶ Q95			

**Observação:** depois de salvas, essas credenciais são retidas na WLC e o AP é reinicializado. As credenciais são alteradas somente quando o LAP ingressa em uma nova WLC. O LAP assume o nome de usuário e a senha que foram configurados na nova WLC.Se o AP ainda não ingressou em uma WLC, você deve usar o console do LAP para definir as credenciais. Emita este comando CLI no modo de ativação:LAP#Iwapp ap dot1x username <username > password <password> orLAP#capwap ap dot1x username <username > password <password> orLAP#capwap ap dot1x username <username a imagem de recuperação: esse comando está disponível apenas para APs que executam a imagem de recuperação.O nome de usuário e a senha padrão do LAP são cisco e cisco, respectivamente.

#### **Configurar o switch**

O switch atua como um autenticador para o LAP e autentica o LAP em um servidor RADIUS. Se o switch não tiver o software compatível, atualize o switch. Na CLI do switch, execute estes comandos para habilitar a autenticação 802.1x em uma porta do switch:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls gos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

**Observação:** se você tiver outros APs no mesmo switch e não quiser que eles usem 802.1x, poderá deixar a porta não configurada para 802.1x ou emitir este comando:

switch(config-if)authentication port-control force-authorized

O LAP é autenticado com EAP-FAST. Certifique-se de que o servidor RADIUS que você usa suporta este método EAP se você não estiver usando o Cisco ACS 5.2.

A configuração do servidor RADIUS é dividida em quatro etapas:

- 1. Configurar recursos de rede.
- 2. Configurar usuários.
- 3. Definir elementos de política.
- 4. Aplicar políticas de acesso.

O ACS 5.x é um ACS baseado em políticas. Em outras palavras, o ACS 5.x usa um modelo de política baseado em regras em vez do modelo baseado em grupos usado nas versões 4.x.

O modelo de política baseado em regras do ACS 5.x oferece um controle de acesso mais poderoso e flexível em comparação com a abordagem mais antiga baseada em grupos.

No modelo mais antigo baseado em grupos, um grupo define a política porque ela contém e une três tipos de informações:

- Informações de identidade Essas informações podem ser baseadas na associação em grupos AD ou LDAP ou em uma atribuição estática para usuários internos do ACS.
- Outras restrições ou condições restrições de tempo, restrições de dispositivo e assim por diante.
- Permissões VLANs ou níveis de privilégio Cisco IOS®.

O modelo de política do ACS 5.x é baseado em regras do seguinte formato:

Condição If então resultado

Por exemplo, usamos as informações descritas para o modelo baseado em grupo:

Se identidade-condição, restrição-condição então autorização-perfil.

Como resultado, isso nos dá flexibilidade para limitar as condições sob as quais o usuário tem permissão para acessar a rede e também o nível de autorização permitido quando condições específicas são atendidas.

#### Configurar recursos de rede

Nesta seção, configuramos o cliente AAA para o switch no servidor RADIUS.

Este procedimento explica como adicionar o switch como um cliente AAA no servidor RADIUS para que o switch possa passar as credenciais do usuário do LAP para o servidor RADIUS.

Conclua estes passos:

- 1. Na GUI do ACS, clique em Network Resources.
- 2. Clique em Network Device Groups.
- 3. Vá para Location > Create (Local > Criar) na parte

cisco Cisco Secure A	CS			
► 🕀 My Workspace	Network Resources > Network Device Groups > Location			
🔹 🦛 Network Resources	Network Device Groups			
Network Device Groups     Location	Filter: 💌 Match it 💌 Go 💌			
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     All Locations			
Users and Identity Stores				
Policy Elements				
+ 🔂 Access Policies				
• 📄 Monitoring and Reports				
🕨 🎭 System Administration				

inferior.

4. Adicione os campos necessários e clique em

#### Enviar.

cisco Cisco Secure A	CS	
+ 🛞 My Workspace	Network Resources > Network Device Groups > Location > Create	
	Device Group - General All Locations C = Required fields	Select
<ul> <li>Jusers and Identity Stores</li> </ul>		
Operation Policy Elements		
► 🔂 Access Policies		
Monitoring and Reports		
System Administration		

5. A janela é atualizada:

cisco Cisco Secure ACS				
🔸 🦪 My Workspace	Network Resources > Network Device Groups > Location			
🐱 🛵 Network Resources	Network Device Groups			
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: 💽 Match if: 💽 Go 🗢			
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     * <u>All Locations</u>			
B Users and Identity Stores	LAB LAB Devices			
Sp Policy Elements				
Access Policies				
Monitoring and Reports				
🕨 🍇 System Administration				

6. Clique em **Tipo de dispositivo > Criar**.

cisco Cisco Secure A	CS
+ 🚓 My Workspace	Network Resources > Network Device Groups > Device Type > Edit "Device Type:All Device Types:Switches"
Ketwork Resources     Network Device Groups     Location     Device Type     Network Devices and AAA Clients     Default Network Device     External RADIUS Servers	Device Group - General         Ø Name:       Switches         Description:       Switch where LAP is connected         Ø Parent:       All Device Types         Ø = Required fields
Users and Identity Stores	
Policy Elements	
Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	The Weight and the second
🕞 🍇 System Administration	and the summer and the set of the

7. Clique em Submit. Depois de concluída, a janela é

Cisco Secure A     My Workspace     Metwork Resources     Network Device Groups	Network Resources > Network Device Groups > Device Type Network Device Groups Filter
Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Match II:     Match II:

atualizada:

- 8. Vá para Network Resources > Network Devices and AAA Clients.
- 9. Clique em **Criar** e preencha os detalhes como descrito

adu	I.
uqu	••

cisco Cisco Secure A	CS	accadmin SALL-ACSS2 (Primary)
	Network Resources > Network Devices and AUA Clerks > Create  Name: [3500-Betch-LAP] Description: [Switch where LAP is connected Network Device Groups In sources	
Default Network Device External RADIUS Servers • 3 Users and Identity Stores • 9 Policy Elements	Device Type All Device Types Switches  P Address  R Device D Sectors  C D Device Types Switches	Select Authentication Options TXGACB+
C. Access Policies     Si Nontaring and Reports     System Administration	Single IP Address	RADIUS     Recret circa     CoApart 1700
	e -Regardd Salda	C Enable KeyWhap Key Encryption Key Massage Authenticator Code Key Key Input Format C ASCII C HEXADECIMAL

10. Clique em Submit. A janela é atualizada:

cisco Cisco Secure A	cs					acautran	SAUL AC
+ 🔂 Mr Workspace	Network	Resources > Network	Devices and AAA Clients				
<ul> <li>Ap Network Resources</li> </ul>	lietox	ork Devices					Showin
Network Device Groups     Location     Device Tex	Filter	[	💌 Match ift	▼ Go	Ŧ		
Network Devices and AM-Clients		Name +	8P / Mask	NDGLocation	NDG:Device Type	Description	
Detaut Network Device External RADIUS Servera	<u>د</u>	3560-Switch-LAP	192.168.153.10/32	All Locations:LAB	All Device Types:Switches	Switch wittere LAP is connected	
+ 👪 Users and identity Stores							
Policy Elements							
* 💭 Access Policies							
+ 📑 Nonitoring and Reports							
+ 🥂 System Administration							

## Configurar usuários

Nesta seção, você verá como criar um usuário no ACS configurado anteriormente. Você atribuirá o usuário a um grupo chamado "usuários do LAP".

Conclua estes passos:

1. Vá para Users and Identity Stores > Identity Groups >

#### Create.

cisco Cisco Secure A	CS
<ul> <li>My Workspace</li> <li>Network Resources</li> <li>Users and identity Stores</li> <li>Identity Groups</li> <li>Internal Identity Stores</li> <li>External Identity Stores</li> <li>LDAP</li> <li>Active Directory</li> <li>RSA Securit Directory</li> <li>RSA Securit Directory</li> <li>RADIUS Identity Servers</li> <li>Certificate Authorities</li> <li>Certificate Authorities</li> <li>Certificate Sequences</li> </ul>	General Ware: LAP users Description: LAPs authenticating over wired Network Parent All Groups Select Select

2. Clique em Submit.

Cisco Secure ACS					
My Workspace	Users and Identity Stores > Identity Groups				
Network Resources	Identity Groups				
Users and identity Stores  Identity Groups	Filter: Match if. Go 🔫				
<ul> <li>Internal Identity Stores</li> <li>External Identity Stores</li> </ul>	Name      Description				
LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers	All Groups Identity Group Root     LAP users LAPs authenticating over wired Network.				
Certificate Authorities Certificate Authentication Profile Identity Store Sequences					

- 3. Crie o 3502e e atribua-o ao grupo "usuários do LAP".
- 4. Vá para Users and Identity Stores > Identity Groups > Users >



5. Você verá as informações atualizadas:

💮 My Workspace	Users and	Identity Store	es > Internal identity Stor	res > Use	rs	
Network Resources	Interna	al Users				
Users and Identity Stores	Filter:	[	Match if:		Go	Ŧ
Internal Identity Stores	F	Status	User Name	▲ Ide	entity Group	Description
Users			35020	AR	Groups:LAP users	LAP 3502e in vian 253

#### Definir Elementos da Política

Verifique se Permit Access está definido.

cisco Cisco Secure A	ICS
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and identity Stores	Filter 🛛 🔻 Match if 🖉 💽 🐨
<ul> <li>Policy Elements</li> </ul>	
Session Conditions     Authorization and Permissions	Permit Access
<ul> <li>Network Access Authorization Profiles</li> </ul>	
Device Administration     Named Permission Objects	
+ 🔂 Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	
🕨 🦓 System Administration	

#### Aplicar políticas de acesso

Nesta seção, você selecionará EAP-FAST como o método de autenticação usado para LAPs para fazer a autenticação. Em seguida, você criará regras com base nas etapas anteriores.

Conclua estes passos:

 Vá para Access Policies > Access Services > Default Network Access > Edit: "Default Network Access".

St. with Manualiana	Access Policies > Access Services > Default Network Access > Edit "Default Network > Edit "De	ault Network Ac
(b) Network Resources		
🚜 Users and Identity Stores	General Allowed Protocols	
Sp. Policy Elements	Name: Default Network Access	
1 Access Policies	Description: Default Network Access Service	-
Access Services II Service Selection Rules	Service Type : Network Access 💌	
Default Device Admin	Policy Structure	
Default Network Access	Identity	

2. Verifique se você habilitou o EAP-FAST e o provisionamento de PAC anônimo em banda.



• 🛃 Access Policies	► E Allow LEAP
Access Services     If Service Selection Rules     O Default Device Admin     O Default Network Access     Idently     Authorization     Ø deleteme     Monitoring and Reports     Ø System Administration	<ul> <li>▼ Allow PEAP</li> <li>PEAP Inner Methods</li> <li>▼ Allow EAP-MS-CHAPv2</li> <li>▼ Allow Password Change Retries: 1</li> <li>▼ Allow EAP-GTC</li> <li>▼ Allow Password Change Retries: 1</li> </ul>
	<ul> <li>Allow EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPv2</li> <li>Allow Password Change Retries: 3</li> <li>Allow EAP-GTC</li> <li>Allow TL3-Renegotiation</li> <li>Use PACs Don't Use PACs</li> <li>Tunnel PAC Time To Live: 90</li> <li>Proactive PAC update will occur after 10</li> <li>% of PAC Time To Live has expired</li> <li>Allow Authenticated In-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticated Provisioning</li> <li>Allow Nachine Authentication</li> <li>Machine PAC Time To Live: 1</li> <li>Weeks </li> <li>Enable Stateless Session Recume</li> <li>Authorization PAC Time To Live: 1</li> <li>Hours </li> </ul>
	Submit Cancel

- 3. Clique em Submit.
- Verifique o grupo Identidade que você selecionou. Neste exemplo, use Internal Users (que foi criado no ACS) e salve as alterações.

cisco Cisco Secure A	CS actadmin SA
	Access Policies > Access Sorvices > Default Network Access > Venity   Single result selection  Reute based result selection  Reute Select  Advanced Options  If authentication failed Reject  If user notifound Reject  If process failed Drop  Note: For authentications using FEAP; LEAP; EAP-PAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected
Identifiating and Reports     System Administration	

5. Vá para Access Policies > Access Services > Default Network Access > Authorization para verificar o perfil de autorização.Você pode personalizar sob quais condições permitirá que um usuário acesse a rede e que perfil (atributos) de autorização você passará depois de autenticado. Essa granularidade está disponível apenas no ACS 5.x. Neste exemplo,

Location, **Device Type**, **Protocol**, Identity Group e EAP Authentication Method estão selecionados.



- 6. Clique em OK e em Save Changes.
- 7. A próxima etapa é criar uma regra. Se nenhuma regra for definida, o LAP terá acesso sem nenhuma condição.
- 8. Clique em **Criar > Regra-1**. Esta regra é para usuários no grupo "usuários LAP".

isco Cisco Secure A	CS					
A My Workspace	Access Pak	des > Access Services > Defail	Network Access > Authoriza	stan		
(b) Network Resources	Standard	Policy Exception Policy				
🔉 🖇 Users and Identity Stores	the Co	en Serure ACS - Morilla Fineire				,
S. Policy Elements	<b>Ca</b> [7					
🕵 Access Policies		192.108.150.24 https://192.	108.150.24/acsadmin/Policy	/inputAction-de		1
Access Senices  Senice Selection Rules  Benice Selection Rules  Benice Admin  Contact Network Access  Identity  Amendation	_1	General Name: Rule-1	Status: Enabled	ht area of the policy rules screen	controls which	
Ø delotemo		poicy condition	its and results are avail	able here for use in policy rules.		
Di Custan Letninistration		Conditions				
A alatan yanakasasan		NDGLocation:	in	All Locations:LAB	Select	
		NDG:Device Type:	in	All Device Types: Switches	Select	
		Protocol:	match	- Radius	Select	
		F Identity Group:	in	All Groups LAP users	Select	
		Eap Authentication Met	hod: ANY-			
		Authorization Profiles: Paemit Access Select Deselect		You may select multiple authorization defined in multiple profiles will use th profile defined.	profiles. Attributes revalue from the first	
	L -	OK Cancel  Estault Fine .1* Duplicate1* Edt	nules defined or no enable Delete An Move to	• ed rule matches.	He	:Ip

9. Clique em **Save Changes**. Se desejar que os usuários que não corresponderem às condições sejam negados, edite a regra padrão para dizer "Negar acesso".

cisco Cisco Secure A	CS SALL 4C 502 (Pr	mery) Lig Dut About Pe
*      * Ny Merispace     *      *      Network Resources	Access Polices > Access Services > Default Retwork Access > Authorization	
<ul> <li>M Users and Identity Stores</li> <li>Policy Elements</li> </ul>	National Princip Access Authorization Policy	
Access Services     Access Services     Service Selection Rules     Ordeut Device Admin     Ordeut Device Admin	Status         NDG Location         NDG Device Type         Protocol         Literally Group         Eap Authentication Method           @         Bule:         In Al LocationsLAB         In All Device Types Switches         match Radius         In All Droups LAP users         +RIT-	Hesuits Hit Authorization Profiles Permit Access 0
Centle Antonine > 21 designe		
By Bystem Administration		
	Ess ruiss defined or no enabled rule matches.	Permit Access
	Create[*] Duglicate[*] Edit Defete A Move10 Y	Custernize Hit Count

10. A última etapa é definir as Regras de Seleção de Serviço. Utilize esta página para configurar uma política simples ou baseada em regras para determinar qual serviço será

aplicado às solicitações recebidas. Por exemplo:

3) Network Resources	-			
1 Loom and Identity Diseas	Single result select	tion 🤗 Rule based result selection		
Contra and identity carres	Service Selection Po	icy		
Sy Policy Elements	Fifter, Status	Natch it Equals V Enabled V Cl	ear Filter   0o   🖛	
Access Policios Erress Renires	E Status	Name Conditions Protocol	Resulta	Hit Count
Default Device Admin	1 🗖 😐	Rule-1 match Radius	Default Network Access	0
O Delauit Network Access Identity Authorization     Ø delateme	2 🗖 🛛	Rule-2 match Tacacs	Default Device Admin	0
Authorization 2 deleteme 3 Monitoring and Reports				

## **Verificar**

Quando 802.1x estiver habilitado na porta do switch, todo o tráfego, exceto o 802.1x, será bloqueado pela porta. O LAP, que já está registrado no WLC, é desassociado. Somente após uma autenticação 802.1x bem-sucedida é que outro tráfego pode passar. O registro bemsucedido do LAP para o WLC depois que o 802.1x é habilitado no switch indica que a autenticação do LAP é bem-sucedida.

Console do AP:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
  192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
  192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface DotllRadiol, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
```

wmmAC status is FALSEged state to CFG \*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to

```
down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
  Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
  down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
  reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radiol, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface DotllRadio0, changed state to
  down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
  keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
  established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.
Logs ACS:
```

 Veja as contagens de ocorrências: Se você estiver verificando os logs dentro de 15 minutos da autenticação, certifique-se de atualizar a contagem de ocorrências. Na mesma página, na parte inferior, você tem uma guia Contagem de ocorrências.

cisco Cisco Secure A	CS											***
+ 🛞 My Workspace	Access	Policies	> Access	Services >	Service Selec	tion R	ules					
+ 🎲 Network Resources	0 s	nole re	sult selec	tion 🖲 R	ule based r	ARUE	election					
Users and Identity Stores	Servi	ce Sek	action Po	licy								
<ul> <li>Policy Elements</li> </ul>	Filter	: Stat	18 -	Match if:	Equals	-	Enabled	-	Clear Filter	Go		
<ul> <li>g. Access Policies</li> <li>Access Services</li> </ul>		-	Status	Name	Protocol		Conditions	_		Service	Results	Hit Count
High Delaut Device Admin	1			Bule-1	match Rad	lus				Default	Network Access	1
<ul> <li>Ø Default Network Access</li> </ul>	2			Rule-2	match Taci	905				Default	Device Admin	0
Identity Authorization > 21 deletame												
+ 📳 Monitoring and Reports												
🕨 🍕 System Administration												

cisco Cisco Secure A	CS			acaadese SAIR.A	CSOT(Primary) List Out	A SILE I			
<ul> <li>Statistics</li> </ul>	Access Policies + Access Carriess + C	Datest Nativort Access + Authorization				12888			
s 160 Network Recourtes	Readard Deline Exception Deline								
Wisers and identity Stores	Statute Porcy: Charles in the								
Policy Elements	NITS NITS ACCUSE AND DRUCK								
- 👗 Access Policies	Filter   Diatus	• Natch if Equals • Enabled	Clear Filter Go V	,					
Access Services     T. Romice Relaction Relact	Name NDGLocation	Condition NDG Dente Type Protocol	8 Identity Group	Esp Authentication Method	Results Authorization Profiles	HE Count			
· O Default Device Admin	Rule-1 In Al Locations LAB	In All Device Types Switches match Radiu	In All Groups LAP users	-AMF-	Permit Access	1			
icenth Americano > 21 deleterre									
<ul> <li>S Nonitoring and Reports</li> </ul>									
» 👫 Dyslem Administration									
	1 If nondes defined or Create , 1 - Duplicato , 1 - E	no esebled rule matches. dt. Dolate A Move to V			Permit Access Customize	• 🗗			

 Clique em Monitoring and Reports e uma nova janela pop-up será exibida. Clique em Authentications -RADIUS -Today. Você também pode clicar em Detalhes para verificar qual regra de seleção de serviço foi aplicada.

_ <b>0</b> 0								Launch Interact	tive Warwar
Showing Page	e 1 of 1			I Geta	lage: Ge				
AAA Protocol > RAD	US Authenticatio	n							
Authentication Status : Date :	Pass or Pail January 25, 2012 (L	ast 30 Ninules   LastH	DAK   LAGE 12 HOME   TO	day i <u>Yesferdar i Last 7 Das</u>	(Last30 Days )				
Generated on January 2	29, 2012 9:15:01 FM	EST							
Rebei	t + Cick for details	9 -House over item	for additional informa	tion					
Logged At	RADUS NAS Status Falure	Details Usemame	MACIP Address	Access Senice	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Gr
Jan 29,12 9:11:12 966	FM 🖌	S 3502#	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-NSCHAP\2)	3590-Switch-LAP	192.168.153.10	GicabtEthemet0/11	

# **Troubleshoot**

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- <u>Cisco Secure Access Control System</u>
- Suporte Técnico e Documentação Cisco Systems

#### 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.

#### 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.