# Autenticação com Fio 802.1x em um Catalyst 3550 Series Switch e um Exemplo de Configuração ACS Versão 4.2

#### Contents

Introduction Prerequisites Requirements Componentes Utilizados Configurar Configuração de switches de exemplo Configuração do ACS Verificar Troubleshoot

## Introduction

Este documento fornece um exemplo de configuração básica do IEEE 802.1x com o Cisco Access Control Server (ACS) Versão 4.2 e o protocolo Remote Access Dial In User Service (RADIUS) para autenticação com fio.

## Prerequisites

#### Requirements

A Cisco recomenda:

- Confirme a alcançabilidade de IP entre o ACS e o switch.
- Certifique-se de que as portas 1645 e 1646 do User Datagram Protocol (UDP) estejam abertas entre o ACS e o switch.

#### **Componentes Utilizados**

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

- Cisco Catalyst 3550 Series Switches
- Cisco Secure ACS versão 4.2

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.

## Configurar

#### Configuração de switches de exemplo

1. Para definir o servidor RADIUS e a chave pré-compartilhada, insira este comando:

Switch(config)# radius-server host 192.168.1.3 key cisco123

2. Para habilitar a funcionalidade 802.1x, insira este comando:

Switch(config)# dot1x system-auth-control

 Para habilitar globalmente a autenticação e a autorização AAA (Authentication, Authorization, and Accounting) e RADIUS, insira estes comandos:
 **Observação**: isso será necessário se você precisar passar atributos do servidor RADIUS; caso contrário, você poderá ignorá-los.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
awitch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

#### Configuração do ACS

Para adicionar o switch como um cliente AAA no ACS, navegue para Network Configuration
 > Add entry AAA client e insira estas informações:

Endereço IP: *<IP>*Segredo compartilhado: *<key>*Autenticar usando: Radius (Cisco IOS<sup>®</sup>/PIX 6.0)

sco		* You can use the wildcard asteriak (*) for an	
	AAA Client Hostname	switch	octet in the IP address. For example, if you yant every AAA dient in your 192.168.13.1 Class
User Setap Group	AAA Client IP Address	192.168.1.2	C network to be represented by a single AAA client entry, enter 192,160,13.* in the AAA Client IP Address box.
Sw1ap Diarad/Profile Components	Free cherry in Phaness	4	You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.160.13.12
Network Cenfliguration	Shared Secret cisco123		and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.
Confliguration	RADIUS Key Wrap	(Beck to Top)	
Interface Configuration	Key Encryption Key		Shared Secret
Administration Casteol	Message Authenticator Code Key		The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA client and ACS. The shared secret must be configured in the AAA client and
External Uper Databases	Key Input Format	ASCII      Hexadecimal	ACS identically, including case sensitivity.
Pastate			[Beck to Top]
alidation	Authenticate Using	RADIUS (Cisco IOS/PIX 6.0) ·	Network Device Group
ebrook Access whiles	Single Connect TACACS+ AAA	From the list, click the name of the Network Device Group (NDG) to which this AAA client belance.	
Activity	Log Update/Watchdog Packets	Note: To enable NDGs, click Interface	
Online Documentation	Log RADIUS Tunneling Packets	Configuration: Advanced Options: Network Device Groups.	
	Replace RADIUS Port info with Username from this AAA Client		[Back to Top]
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client		RADIUS Key Wrap

 Para configurar a autenticação, navegue até System Configuration > Global Authentication Setup e verifique se a caixa de seleção Allow MS-CHAP Version 2 Authentication está marcada:

cisco	System Configuration [EAP-ILS session timeout (minutes): 120	<b>a</b> 1
Group Setup Setup Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition Composition	Select one of the following options for setting username during authentication:	Use this page to specify settings for various authentication protocols.    EAP Conferentian  EAP-FAST
Spten Endigeration Interface Configuration	LEAP Allow LEAP (For Aironet only)	EAP Configuration EAP is a flexible request-response protocol for arbitrary authentication information (SPC 2264). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "extendication" types.
Castral Defermal Uper Defeterer	EAP-MD5 Ø Allow EAP-MD5	Täisk to Taol PEAP
Tablan Tablan	AP EAP request timeout (seconds): 20	PEAP is the outer layer protocol for the secure tunnel.
Prefilez	MS-CHAP Configuration	Note: FEAP is a certificate-based authentication protocol. FEAP authentication can occur only after you have completed the required steps on the AES Certificate Setup page. Allow EAP-NECKAPV2 — Use to enable EAP-MECKAPV2 within HS FEAP authentication. Enable this protocol for any repositiony that supports ME-CMAPV2, such as Microsoft AD, and the ACS Internal
donamentation	Allow MS-CHAP Version 1 Authentication Allow MS-CHAP Version 2 Authentication	Database.  Allow EAP-CTC - Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.

 Para configurar um usuário, clique em User Setup no menu e conclua estas etapas: Insira as informações de usuário: Network-Admin *<username>*.Clique em Add/Edit.Insira o nome real: Network-Admin *<nome descritivo>*.Adicione uma Descrição: *<sua escolha>*.Selecione a opção Password Authentication: ACS Internal Database.Insira a senha: ...... *<password>*.Confirme a senha: *<password>*.Clique em Submit.

allada	User Setup	
CISCO	User: Network-Admin (New User)	Caliback     Chert IP Address Assignment     Advanced Settings
Getap	Count Disabled	Hetwork Access Restrictions     Hax Sensions     Uneque Quotas
StaredProfile	Supplementary User Info	Account Onebia     Dentita ACLa     Advanced TACACS+ Settings     TACACS+ Control
Network Configuration System Configuration	Real Name Description	IdCAC51: Enable Parameter     IdCAC51: Contexand Parameter     IdCAC51: Shell Command Authorization     Command Authorization for Network Device Hanagement Applications     ToCAC51: Unknown Services     IETE RADIUS Attributes     RADIUS Attributes     RADIUS Attributes
Advinistration Central	User Setup ?	Ime Round Alternate Group     Account Disabled Status
Di External User Dutabacec	Password Authentication: ACS Internal Database	Select the Account Disabled check box to disable this account; dear the check box to enable the account.
Network Access Post lec	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)	Deleting a Ucername
Activity	Password •••••	The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, did. Baktor, Users action to confirm users action, did. Off
Conumentation	Password ******	[Back to Too]
	Separate (CHAP/MS-CHAP/ARAP)	Supplementary User Info
	Decement	Ture the socilizable information in any supplemental user information boxes that annear

## Verificar

A <u>ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns</u> <u>comandos de exibição.</u>. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Insira estes comandos para confirmar se sua configuração funciona corretamente:

- show dot1x
- show dot1x summary
- show dot1x interface
- show authentication sessions interface <interface>
- show authentication interface <interface>

Switch(config)# show dot1x

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

Switch(config)# show dot1x summary

```
Interface PAE Client Status
```

Fa0/4 AUTH

Switch(config)# show dot1x interface fa0/4 detail

Dot1x Info for FastEthernet0/4

```
PAE = AUTHENTICATOR

PortControl = FORCE_AUTHORIZED

ControlDirection = Both

HostMode = SINGLE_HOST

QuietPeriod = 5

ServerTimeout = 0

SuppTimeout = 30

ReAuthMax = 2

MaxReq = 2

TxPeriod = 10
```

# Troubleshoot

Esta seção fornece comandos de depuração que você pode usar para solucionar problemas de configuração.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

- debug dot1x all
- debug authentication all
- debug radius (fornece as informações de radius no nível de depuração)
- debug aaa authentication (debug for authentication)
- debug aaa authorization (debug para autorização)

#### 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.