

# Configuração RADIUS nos Switches Gerenciados 200/300 Series

## Objetivo

O Serviço de Usuário de Discagem de Autorização Remota (RADIUS - Remote Authorization Dial-In User Service) é um serviço de segurança usado para autenticação de usuários em redes com arquitetura de segurança centralizada. Os Switches Gerenciados 200/300 Series podem atuar como um cliente RADIUS na sua rede e, em conjunto com um servidor RADIUS, você pode estabelecer um sistema centralizado para autenticação de usuários na sua rede. Este artigo explica como configurar um servidor RADIUS e aplicar métodos de autenticação nos Switches Gerenciados da Série 200/300.

## Dispositivos aplicáveis | Versão do software

- Série SF/SG 200 - 1.2.9.x
- Série SF/SG 300 - 1.2.9.x

## Configuração Padrão RADIUS

Esta seção o guia pela configuração padrão de um servidor RADIUS. Esses valores padrão podem ser usados para qualquer servidor RADIUS que você queira adicionar a um switch.

### Passo 1

Faça login no utilitário de configuração da Web e escolha **Security > RADIUS**. A página *RADIUS* é aberta:

## RADIUS

RADIUS Accounting:  Port Based Access Control (802.1X, MAC Based)  
 Management Access  
 Both Port Based Access Control and Management Access  
 None

---

**Use Default Parameters**

IP Version:  Version 6  Version 4

Retries:  (Range: 1 - 10, Default: 3)

Timeout for Reply:  sec. (Range: 1 - 30, Default: 3)

Dead Time:  min. (Range: 0 - 2000, Default: 0)

Key String:  Encrypted   
 Plaintext  (0/128 Characters Used)

RADIUS Table									
<input type="checkbox"/>	Server	Priority	Key String( Encrypted )	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.									
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>									

As imagens neste artigo são de um switch modelo SG300.

## Passo 2

No campo Contabilidade RADIUS, clique em uma das seguintes opções:

- Controle de acesso baseado em porta (802.1x, baseado em MAC) - Para usar o servidor RADIUS para contabilidade de porta 802.1x.
- Acesso de gerenciamento - Para usar o servidor RADIUS para contabilização de login.
- Controle de Acesso Baseado em Porta e Acesso de Gerenciamento - Para usar o servidor RADIUS para 802.1x e contabilidade de login.
- Nenhum - Para não usar o servidor RADIUS para fins de contabilidade.

A Contabilização Radius não está disponível nos switches da série SG200.

## Etapa 3

Na seção Usar Parâmetros Default, no campo Repetições, informe o número de repetições que o switch fez para autenticar o servidor RADIUS.

## Passo 4

No campo Timeout for Reply, insira o tempo em segundos para cada tentativa de autenticação feita no servidor RADIUS.

## Etapa 5

No campo Dead Time (Tempo inativo), insira o tempo em minutos antes que o switch declare um servidor RADIUS sem resposta como inativo e passe para o próximo servidor disponível para tentar a conexão.

## Etapa 6

No campo Sequência de caracteres chave, insira a chave usada para autenticação e criptografia entre o switch e o servidor RADIUS. Essa chave deve corresponder no servidor RADIUS e no switch. Clique em uma das seguintes opções:

- Encrypted - (Criptografado) Se você tiver uma chave criptografada de outro dispositivo, insira a chave.
- Texto sem formatação - se você não tiver uma chave criptografada de outro dispositivo, insira a chave como um texto sem formatação.

## Etapa 7

Clique em **Aplicar** para salvar esses valores padrão e disponibilizá-los para um servidor RADIUS.

## Adicionar/Editar um Servidor RADIUS

Nesta seção, é fornecido um procedimento passo a passo que explica como adicionar ou editar um servidor RADIUS em um 200/300 Series Managed Switches.

### Passo 1

Faça login no utilitário de configuração da Web e escolha **Security > RADIUS**. A página *RADIUS* é aberta:

Server	Priority	Key String ( Encrypted )	Timeout for Reply	Authentication Port	Accounting Port	Retries	Dead Time	Usage Type
0 results found.								
Add... Edit... Delete								
Display Sensitive Data As Plaintext								

### Passo 2

Na seção Tabela RADIUS, clique em **Adicionar**. A janela *Add Radius Server* é exibida.

Para editar um servidor Radius atual, clique em **Editar** e edite as propriedades desejadas do servidor RADIUS.

Server Definition:  By IP address  By name

IP Version:  Version 6  Version 4

IPv6 Address Type:  Link Local  Global

Link Local Interface:

Server IP Address/Name:

Priority:  (Range: 0 - 65535)

Key String:  Use Default

### Etapa 3

No campo Definição de servidor, clique em uma das seguintes opções:

- Por nome - Se o servidor RADIUS estiver definido com um nome.
- Por endereço IP - Se o servidor RADIUS for definido com um endereço IP.

### Passo 4

No campo IP Version, clique em **Version 6** ou **Version 4** como o tipo de endereço IP do servidor RADIUS.

### Etapa 5

Se a **Versão 6** for escolhida como o endereço IP no tipo de endereço IPv6, clique em uma das seguintes opções:

- Link Local - Um endereço IPv6 que identifica apenas hosts em um único link de rede.
- Global - Um endereço IPv6 que pode ser acessado de outras redes.

### Etapa 6

Se Link Local for escolhido como o tipo de endereço IPv6, na lista suspensa Link Local Interface, escolha a interface apropriada.

### Etapa 7

No campo Server IP Address/Name (Endereço IP/Nome do servidor), insira o endereço IP ou o nome do servidor RADIUS.

### Passo 8

No campo Priority (Prioridade), insira a prioridade do servidor RADIUS que o switch usará. O servidor com a prioridade mais alta é consultado primeiro no switch. Zero (0) dá a prioridade mais alta.

### Passo 9

No campo Sequência de caracteres chave, clique em uma das seguintes opções:

- Usar padrão - Para usar a chave padrão para autenticação.
- Definido pelo Usuário (Criptografado) - Se disponível, insira a chave criptografada.
- Definido pelo Usuário (Texto sem formatação) - Se não estiver disponível, insira a chave como um texto sem formatação.

### Passo 10

No campo Tempo limite para resposta, clique em uma das seguintes opções:

- Usar Padrão - Para usar o valor padrão.
- Definido pelo usuário - Insira o número em segundos que o switch aguarda por cada tentativa de conexão com o servidor RADIUS.

## Passo 11

No campo Authentication Port (Porta de autenticação), insira a porta UDP que o servidor RADIUS usa para autenticação.

## Etapa 12

No campo Accounting Port (Porta de contabilização), insira a porta UDP que o servidor RADIUS usa para contabilização.

## Passo 13

No campo Novas Tentativas, clique em uma das seguintes opções:

- Usar Padrão - Para usar o valor padrão.
- Definido pelo Usuário - Para usar um valor diferente. Digite o número de tentativas feitas pelo switch antes que uma conexão com o servidor RADIUS seja considerada como tendo ocorrido.

## Passo 14

No campo Tempo inativo, clique em uma das seguintes opções:

- Usar Padrão - Para usar o valor padrão.
- Definido pelo Usuário - Para usar um valor diferente. Digite o tempo em minutos antes que o switch declare um servidor RADIUS sem resposta como inoperante e mude para o próximo servidor disponível para tentar a conexão.

## Etapa 15

No campo Tipo de uso, clique em uma das seguintes opções:

- Login - Autentica os administradores do switch.
- 802.1x - O servidor RADIUS verificará as credenciais de segurança dos usuários que solicitarem acesso à rede com base no esquema 802.1x do Controle de Acesso à Rede (PNAC - Network Access Control) com base na porta.
- Todos - Usa os dois tipos de autenticação.

## Passo 16

Clique em Apply.

**RADIUS**

RADIUS Accounting:  Port Based Access Control (802.1X, MAC Based)  
 Management Access  
 Both Port Based Access Control and Management Access  
 None

---

**Use Default Parameters**

IP Version:  Version 6  Version 4

Retries:  (Range: 1 - 10, Default: 3)

Timeout for Reply:  sec. (Range: 1 - 30, Default: 3)

Dead Time:  min. (Range: 0 - 2000, Default: 0)

## Etapa 17

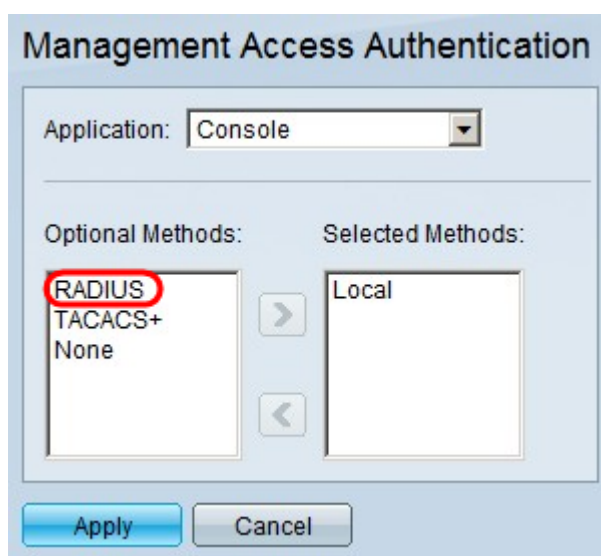
(Opcional) Para excluir um servidor RADIUS, na seção Tabela RADIUS, marque a caixa de seleção do servidor RADIUS que deseja excluir e clique em **Excluir**.

## Autenticação RADIUS

Depois que o servidor RADIUS estiver configurado corretamente, você precisará autenticá-lo no switch. Esta seção explica como autenticar um servidor RADIUS nos Switches Gerenciados 200/300 Series.

### Passo 1

Faça login no utilitário de configuração da Web e escolha **Security > Management Access Authentication**. A página *Autenticação de Acesso de Gerenciamento* é aberta:



Management Access Authentication

Application: Console

Optional Methods: Selected Methods:

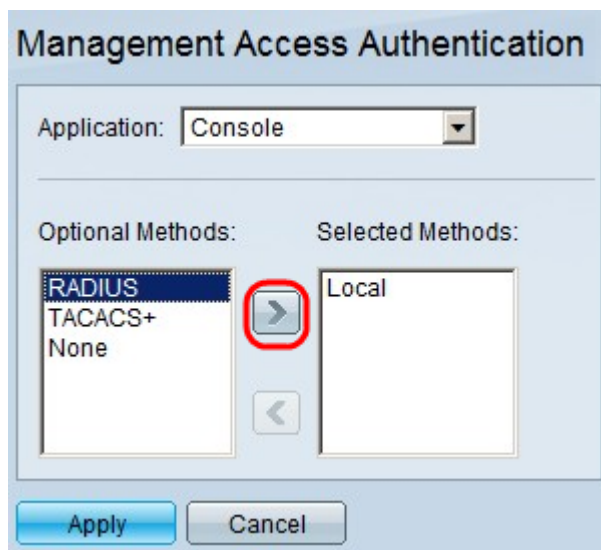
RADIUS  
TACACS+  
None

Local

Apply Cancel

### Passo 2

Na lista Métodos Opcionais, escolha RADIUS.



Management Access Authentication

Application: Console

Optional Methods: Selected Methods:

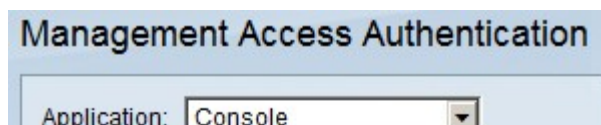
RADIUS  
TACACS+  
None

Local

Apply Cancel

### Etapa 3

Clique no botão >.



Management Access Authentication

Application: Console

## **Passo 4**

Clique em Apply.

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.