

Configurar o roteador Cisco para autenticação de discagem usando TACACS+

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurações](#)

[Configuração do Microsoft Windows](#)

[Configuração do Microsoft Windows para usuários 1 e 2](#)

[Step-by-Step Instructions](#)

[Configuração do Microsoft Windows para usuário 3](#)

[Verificar](#)

[Troubleshoot](#)

[Router](#)

[Servidor](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar um roteador Cisco para autenticação de discagem com o TACACS+ executado no UNIX. O TACACS+ não oferece tantos recursos quanto o [Cisco Secure ACS para Windows](#) ou [Cisco Secure ACS para UNIX](#) disponível comercialmente.

O software TACACS+ fornecido anteriormente pela Cisco Systems foi descontinuado e não é mais suportado pela Cisco Systems.

Hoje, você pode encontrar muitas versões de freeware TACACS+ disponíveis quando procura "freeware TACACS+" em seu mecanismo de pesquisa de Internet favorito. A Cisco não recomenda especificamente nenhuma implementação de freeware TACACS+ específica.

O Cisco Secure Access Control Server (ACS) está disponível para compra através de canais regulares de vendas e distribuição da Cisco em todo o mundo. O Cisco Secure ACS para Windows inclui todos os componentes necessários para uma instalação independente em uma estação de trabalho Microsoft Windows. O Cisco Secure ACS Solution Engine é fornecido com uma licença de software Cisco Secure ACS pré-instalada. Consulte o [Boletim do Produto Cisco Secure ACS 4.0](#) para obter os números dos produtos. Visite a [página inicial de pedidos da Cisco](#) (somente clientes [registrados](#)) para fazer um pedido.

Note: Você precisa de uma conta CCO com um Contrato de serviço associado para obter a

versão de avaliação de 90 dias para o [Cisco Secure ACS para Windows](#) (somente [registrados](#)).

A configuração do roteador neste documento foi desenvolvida em um roteador que executa o Cisco IOS® Software Release 11.3.3. As versões 12.0.5.T e posteriores do software Cisco IOS usam **tacs+** em vez de **tacacs+**. Declarações como **aaa authentication login default tacacs+ enable** aparecem como **aaa authentication login default group tacacs+ enable**.

Você pode fazer download do freeware TACACS+ e do Guia do usuário por ftp anônimo para ftp-eng.cisco.com no diretório /pub/tacacs.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

[Configurações](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: use a [Command Lookup Tool](#) (somente clientes [registrados](#)) para encontrar informações adicionais sobre os comandos usados neste documento.

Este documento utiliza as seguintes configurações:

- [Configuração do roteador](#)
- [TACACS+ arquivo de configuração no programa gratuito de servidor](#)

Configuração do roteador

```
!  
aaa new-model  
aaa authentication login default tacacs+ enable  
aaa authentication ppp default if-needed tacacs+  
aaa authorization exec default tacacs+ if-authenticated  
aaa authorization commands 1 default tacacs+ if-  
authenticated  
aaa authorization commands 15 default tacacs+ if-  
authenticated  
aaa authorization network default tacacs+  
enable password ww
```

```

!
chat-script default "" at&fls0=1&hl&r2&c1&d2&ble0q2 OK
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
  !--- Challenge Handshake Authentication Protocol !---
  (CHAP/PPP) authentication user. interface Async1 ip
  unnumbered Ethernet0 encapsulation ppp async mode
  dedicated peer default ip address pool async no cdp
  enable ppp authentication chap ! !--- Password
  Authentication Protocol (PAP/PPP) authentication user.
  interface Async2 ip unnumbered Ethernet0 encapsulation
  ppp async mode dedicated peer default ip address pool
  async no cdp enable ppp authentication pap ! !---
  Authentication user with autocommand PPP. interface
  Async3 ip unnumbered Ethernet0 encapsulation ppp async
  mode interactive peer default ip address pool async no
  cdp enable ! ip local pool async 10.6.100.101
  10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
  server timeout 10 tacacs-server key cisco ! line 1
  session-timeout 20 exec-timeout 120 0 autoselect during-
  login script startup default script reset default modem
  Dialin transport input all stopbits 1 rxspeed 115200
  txspeed 115200 flowcontrol hardware ! line 2 session-
  timeout 20 exec-timeout 120 0 autoselect during-login
  script startup default script reset default modem Dialin
  transport input all stopbits 1 rxspeed 115200 txspeed
  115200 flowcontrol hardware ! line 3 session-timeout 20
  exec-timeout 120 0 autoselect during-login autoselect
  ppp script startup default script reset default modem
  Dialin autocommand ppp transport input all stopbits 1
  rxspeed 115200 txspeed 115200 flowcontrol hardware ! end

```

TACACS+ arquivo de configuração no programa gratuito de servidor

```

!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }

```

[Configuração do Microsoft Windows](#)

[Configuração do Microsoft Windows para usuários 1 e 2](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Step-by-Step Instructions

Siga estas etapas.

Nota: A configuração do PC pode variar um pouco com base na versão do sistema operacional que você usa.

1. Selecione **Iniciar > Programas > Acessórios > Rede dial-up** para abrir a janela Rede dial-up.
2. Escolha **Tornar nova conexão** no menu Conexões e insira um nome para sua conexão.
3. Insira as informações específicas do modem e clique em **Configurar**.
4. Na página Propriedades gerais, selecione a velocidade mais alta do modem, mas não marque a opção **Somente conectar nessa velocidade...** caixa.
5. Na página Propriedades de configuração/conexão, use 8 bits de dados, sem paridade e 1 bit de parada. As preferências de chamada a serem usadas são **Aguardar o tom de discagem antes de discar** e **Cancelar a chamada se não estiver conectada após 200 segundos**.
6. Na página Conexão, clique em **Avançado**. Nas Configurações avançadas de conexão, selecione somente **Controle de fluxo de hardware** e **Tipo de modulação Padrão**. Na página de propriedades Configurar/Opções, nada deve ser marcado, exceto a caixa em Controle de status.
7. Clique em **OK** e em **Avançar**.
8. Digite o número de telefone do destino, clique em **Avançar** novamente e clique em **Concluir**.
9. Quando o ícone de nova conexão for exibido, clique com o botão direito do mouse nele e escolha **Propriedades > Tipo de servidor**.
10. Escolha **PPP:WINDOWS 95, WINDOWS NT 3.5, Internet** e não marque nenhuma opção Avançada.
11. Verifique **TCP/IP** em Allowed Network Protocols (Protocolos de rede permitidos).
12. Em TCP/IP Settings., escolha **Server Assigned IP Address, Server Assigned Name Server Addresses ServerServer** e **Use default gateway em rede remota** e clique em **OK**.
13. Quando o usuário clica duas vezes no ícone para exibir a janela Conectar a para discar, o usuário deve preencher os campos Nome de usuário e Senha e, em seguida, clicar em **Conectar**.

Configuração do Microsoft Windows para usuário 3

A configuração para o usuário 3 (usuário de autenticação com autocomando PPP) é a mesma para os usuários 1 e 2, com as seguintes exceções:

- Na página de propriedades Configurar/Opções (etapa 6), marque a **janela Ativar terminal após discar**.
- Quando o usuário clica duas vezes no ícone para abrir a janela Conectar a para discar (Etapa 13), o usuário não preenche os campos Nome de usuário e Senha. O usuário clica em **Conectar**. Depois que a conexão com o roteador é feita, o usuário digita o nome de usuário e a senha na janela preta exibida. Após a autenticação, o usuário pressiona **Continuar (F7)**.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Router

Consulte [Informações Importantes sobre Comandos de Depuração antes de usar comandos debug](#).

- **terminal monitor**—Exibe a saída do comando **debug** e mensagens de erro do sistema para o terminal e a sessão atuais.
- **debug ppp negotiation** —Exibe os pacotes PPP enviados durante a inicialização do PPP, onde as opções do PPP são negociadas.
- **debug ppp packet** — Exibe os pacotes PPP que são enviados e recebidos. (Este comando mostra cópias parciais da memória de pacote de nível baixo.)
- **debug ppp chap** —Exibe informações sobre se um cliente passa a autenticação (para Cisco IOS Software Releases anteriores a 11.2) .
- **debug aaa authentication** —Exibe informações sobre autenticação, autorização e contabilização (AAA)/TACACS+.
- **debug aaa authorization** — Exibe informações sobre autorização AAA/TACACS+.

Servidor

Observação: isso pressupõe o código do servidor Cisco TACACS+ Freeware.

```
tac_plus_executable -C config.file -d 16  
tail -f /var/tmp/tac_plus.log
```

Informações Relacionadas

- [Página de suporte de TACACS+](#)
- [TACACS+ na Documentação do IOS](#)
- [Cisco Secure Access Control Server](#)
- [Configurando e depurando o CiscoSecure 2.x TACACS+](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)