# Prevenção de fraude na tarifa de chamadas expressas do gerente de comunicações unificadas

## Contents



## Introduction

Este documento fornece um guia de configuração que pode ser usado para otimizar a segurança de um sistema Cisco Communications Manager Express (CME) e reduzir a ameaça de fraudes nas tarifas de ligações. O CME é a solução de controle de chamadas baseada em roteador da Cisco que oferece uma solução inteligente, simples e segura para organizações que desejam implementar as Comunicações Unificadas. É altamente recomendável que você implemente as medidas de segurança descritas neste documento para fornecer níveis adicionais de controle de segurança e reduzir a possibilidade de fraude de pedágio.

O objetivo deste documento é informá-lo sobre as várias ferramentas de segurança disponíveis nos Cisco Voice Gateways e CME. Essas ferramentas podem ser implementadas em um sistema CME para ajudar a reduzir a ameaça de fraude de tarifas por parte de partes internas e externas.

Este documento fornece instruções sobre como configurar um sistema CME com várias ferramentas de segurança tarifada e restrição de recursos. O documento também descreve por que certas ferramentas de segurança são usadas em determinadas implantações.

A flexibilidade inerente geral das plataformas ISR da Cisco permite que você implante o CME em vários tipos diferentes de implantações. Assim, pode ser necessário usar uma combinação dos recursos descritos neste documento para ajudar a bloquear o CME. Este documento serve como diretriz para como aplicar ferramentas de segurança no CME e não garante de forma alguma que a fraude ou o abuso de pedágio por parte de partes internas e externas não ocorrerão.

# Prerequisites

## Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager Express

## Componentes Utilizados

As informações neste documento são baseadas no Cisco Unified Communications Manager Express 4.3 e no CME 7.0.

**Observação:** o Cisco Unified CME 7.0 inclui os mesmos recursos do Cisco Unified CME 4.3, que é renumerado para 7.0 para alinhar com as versões do Cisco Unified Communications.

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 Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Overview

Este documento aborda as ferramentas de segurança mais comuns que podem ser usadas em um sistema CME para ajudar a reduzir a ameaça de fraude de tarifas. As ferramentas de segurança CME mencionadas neste documento incluem ferramentas de restrição de tarifas e ferramentas de restrição de recursos.

### Ferramentas de restrição de tarifas

- Direct-inward-dial

- Restrição de tarifa após o horário
- Classe de restrição
- Lista de acesso para restringir o acesso ao tronco H323/SIP

### Ferramentas de restrição de recurso

- Transfer-pattern
- Padrão de transferência bloqueado
- Transfer max-length
- Call-forward max-length
- Não encaminhar chamadas locais
- Sem autorregistro-ephone

### Ferramentas de restrição do Cisco Unity Express

- Acesso PSTN seguro do Cisco Unity Express
- Restrição de notificação de mensagem

### Registro de chamadas

- Registro de chamadas para capturar registros de detalhes de chamadas (CDRs)

## Ameaças internas versus externas

Este documento discute as ameaças de partes internas e externas. Interessados incluem usuários de telefone IP que residem em um sistema CME. As partes externas incluem usuários em sistemas estrangeiros que podem tentar usar o host CME para fazer chamadas fraudulentas e fazer com que as chamadas sejam cobradas de volta ao seu sistema CME.

# Ferramentas de restrição de tarifas

## Direct-inward-dial

### Resumo

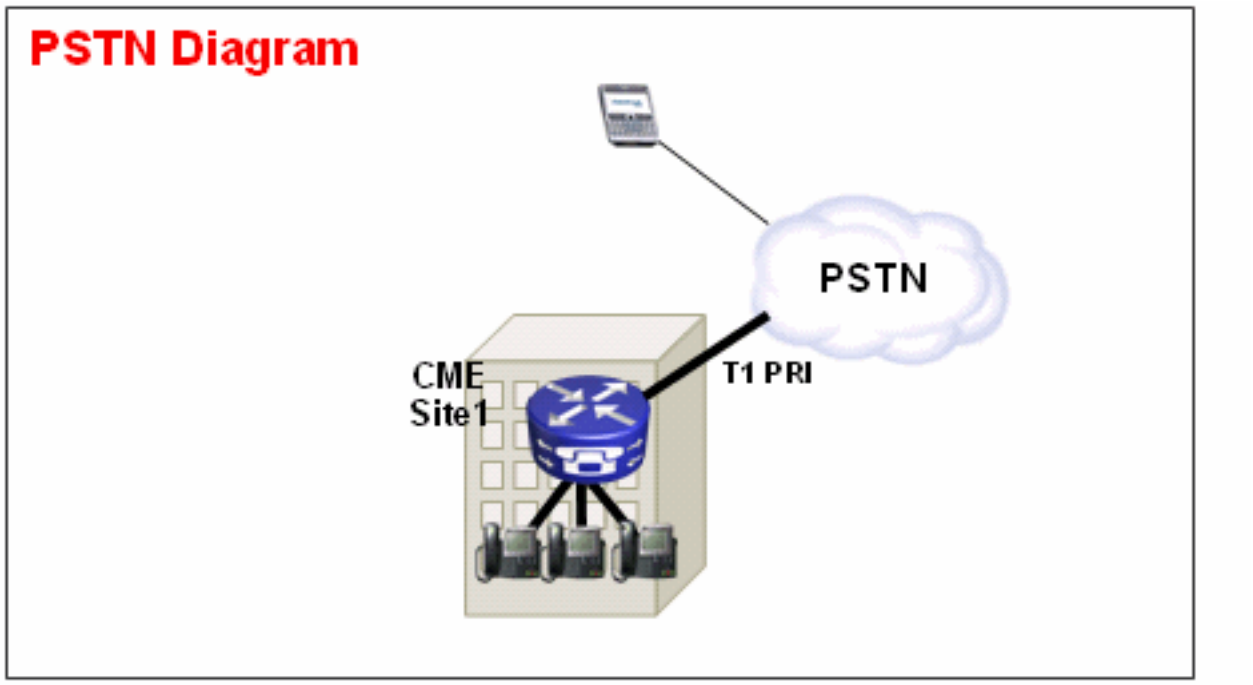
A discagem interna direta (DID) é usada nos gateways de voz da Cisco para permitir que o gateway processe uma chamada de entrada depois de receber dígitos do PBX ou do switch CO. Quando o DID está ativado, o gateway da Cisco não apresenta um tom de discagem secundário para o chamador e não espera para coletar dígitos adicionais do chamador. Encaminha a chamada diretamente para o destino que corresponde ao DNIS (serviço de identificação de número discado) de entrada. Isso é chamado de discagem de um estágio.

**Observação:** essa é uma **ameaça externa**.

### Instrução do problema

Se a discagem interna direta NÃO estiver configurada em um Cisco Gateway ou CME, sempre

que uma chamada for recebida do CO ou PBX para o Cisco Gateway, o chamador ouvirá um tom de discagem secundário. Isso é chamado de discagem em dois estágios. Quando os chamadores PSTN ouvem o tom de discagem secundário, eles podem digitar dígitos para acessar qualquer ramal interno ou, se souberem o código de acesso PSTN, podem discar números de longa distância ou internacionais. Isso apresenta um problema porque o chamador PSTN pode usar o sistema CME para fazer chamadas de saída de longa distância ou internacionais e a empresa é cobrada pelas chamadas.




Exemplo 1

No local 1, o CME é conectado à PSTN através de um tronco T1 PRI. O provedor PSTN fornece o **40855512.** Intervalo DID para o site CME 1. Assim, todas as chamadas PSTN destinadas para 4085551200 - 4085551299 são roteadas de entrada para o CME. Se você não configurar a **discagem interna direta** no sistema, um chamador PSTN de entrada ouvirá um tom de discagem secundário e deverá discar manualmente o ramal interno. O maior problema é que se o chamador for um abusador e souber o código de acesso PSTN no sistema, geralmente **9**, ele poderá discar **9** e então qualquer número de destino que quiser alcançar.

### Solução 1

Para atenuar essa ameaça, você deve configurar a **discagem interna direta**. Isso faz com que o gateway da Cisco encaminhe a chamada de entrada diretamente para o destino que corresponde ao DNIS de entrada.

Configuração de exemplo

```
dial-peer voice 1 pots
port 1/0:23
incoming called-number .
direct-inward-dial
```

Para que o DID funcione corretamente, verifique se a chamada de entrada corresponde ao peer de discagem POTS correto onde o comando **direct-inside-dial** está configurado. Neste exemplo, a PRI T1 está conectada à porta 1/0:23. Para corresponder ao correspondente de discagem de

entrada correto, emita o comando **incoming called-number** no correspondente de discagem DID POTS.

## Exemplo 2

No local 1, o CME é conectado à PSTN através de um tronco T1 PRI. O provedor de PSTN dá o **40855512.** e **40855513...** Intervalos DID para o site CME 1. Assim, todas as chamadas PSTN destinadas para 4085551200 - 4085551299 e 4085551300 - 4085551399 são roteadas de entrada para o CME.

### Configuração incorreta:

Se você configurar um peer de discagem de entrada, como na configuração de exemplo nesta seção, a possibilidade de fraude de pedágio ainda ocorrerá. O problema com esse peer de discagem de entrada é que ele só corresponde chamadas de entrada para **40852512.** e, em seguida, aplica o serviço DID. Se uma chamada PSTN entrar em **40852513..**, o peer de discagem de portas de entrada não corresponde e, portanto, o serviço DID não é aplicado. Se um peer de discagem de entrada com DID não corresponder, o peer de discagem padrão 0 será usado. Por padrão, O DID é desabilitado no peer de discagem 0.

Configuração de exemplo

```
dial-peer voice 1 pots
incoming called-number 40855512..
direct-inward-dial
```

### Configuração correta

A maneira correta de configurar o serviço DID em um peer de discagem de entrada é mostrada neste exemplo:

Configuração de exemplo

```
dial-peer voice 1 pots
port 1/0:23
incoming called-number .
direct-inward-dial
```

Consulte Configuração DID para Peers de Discagem POTS para obter mais informações sobre DID para portas de voz T1/E1 digitais.

**Observação:** o uso de DID **não** é necessário quando o PLAR (Private-Line Automatic Ringdown) é usado em uma porta de voz ou um script de serviço como o AA (Auto-Attendant, Atendedor automático) é usado no peer de discagem de entrada.

Exemplo de configuração — PLAR

```
voice-port 1/0
connection-plar 1001
```

Exemplo de configuração — Script de serviço

```
dial-peer voice 1 pots
```

```
service AA
port 1/0:23
```

## Restrições de tarifa após o horário

### Resumo

A Restrição de tarifas pós-horário é uma nova ferramenta de segurança disponível no CME 4.3/7.0 que permite configurar políticas de restrição de tarifas com base na hora e na data. Você pode configurar políticas para que os usuários não tenham permissão para fazer chamadas para números predefinidos durante determinadas horas do dia ou durante todo o tempo. Se a política de bloqueio de chamadas pós-horário 7x24 estiver configurada, ela também restringirá o conjunto de números que podem ser inseridos por um usuário interno para definir **call-forward all**.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Este exemplo define vários padrões de dígitos para os quais as chamadas de saída são bloqueadas. Os padrões 1 e 2, que bloqueiam as chamadas para números externos que começam com "1" e "011", são bloqueados de segunda a sexta-feira antes das 7 da manhã e depois das 7 da tarde, no sábado antes das 7 da manhã e depois das 13 da tarde, e no domingo inteiro. O padrão 3 bloqueia chamadas para 900 números 7 dias por semana, 24 horas por dia.

Configuração de exemplo

```
telephony-service
after-hours block pattern 1 91
after-hours block pattern 2 9011
after-hours block pattern 3 91900 7-24
after-hours day mon 19:00 07:00
after-hours day tue 19:00 07:00
after-hours day wed 19:00 07:00
after-hours day thu 19:00 07:00
after-hours day fri 19:00 07:00
after-hours day sat 13:00 07:00
after-hours day sun 12:00 12:00
```

Consulte Configuração do Bloqueio de Chamadas para obter mais informações sobre a restrição de tarifas.

## Classe de restrição

### Resumo

Se você quiser controle granular ao configurar a restrição de tarifas, deverá usar a Classe de Restrição (COR). Consulte a Classe de Restrição: Exemplo para obter mais informações.

## Restrições de fraude de tarifas de troncos H.323 / SIP

### Resumo

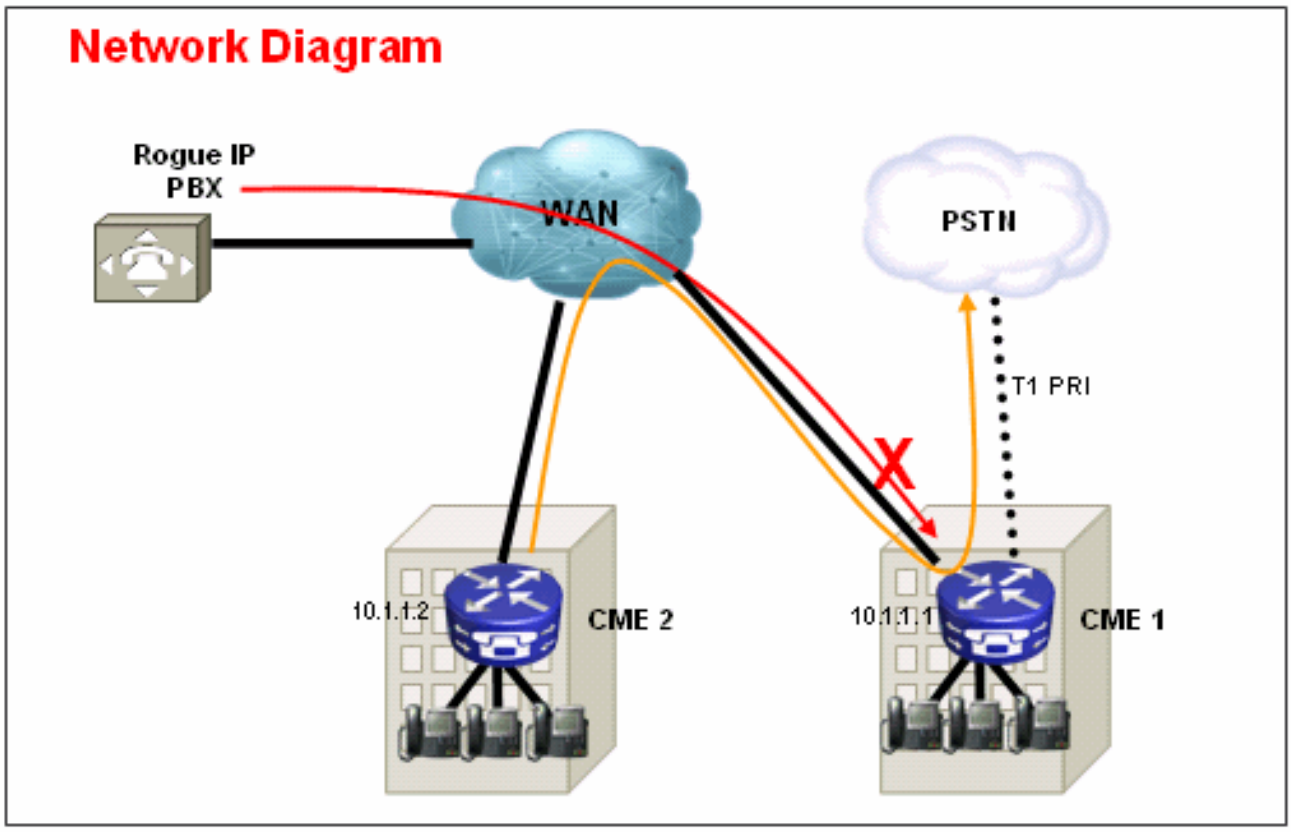
Nos casos em que um sistema CME é conectado por uma WAN a outros dispositivos CME por

meio de um tronco SIP ou H.323, você pode restringir o acesso de tronco SIP/H.323 ao CME para impedir que os usuários não autorizados usem seu sistema para retransmitir chamadas ilegalmente para a PSTN.

**Observação:** essa é uma **ameaça externa**.

[Exemplo 1]

Neste exemplo, o CME 1 tem conectividade PSTN. O CME 2 é conectado através da WAN ao CME 1 através de um tronco H.323. Para proteger o CME 1, você pode configurar uma lista de acesso e aplicá-la na interface da WAN e, portanto, permitir somente o tráfego IP do CME 2. Isso impede que o PABX IP invasor envie chamadas VOIP através do CME 1 para a PSTN.




## Solução

Não permita que a interface WAN no CME 1 aceite o tráfego de dispositivos invasores que não reconhece. Observe que há uma DENY all implícita no final de uma lista de acesso. Se houver mais dispositivos dos quais você deseja permitir o tráfego IP de entrada, não se esqueça de adicionar o endereço IP do dispositivo à lista de acesso.

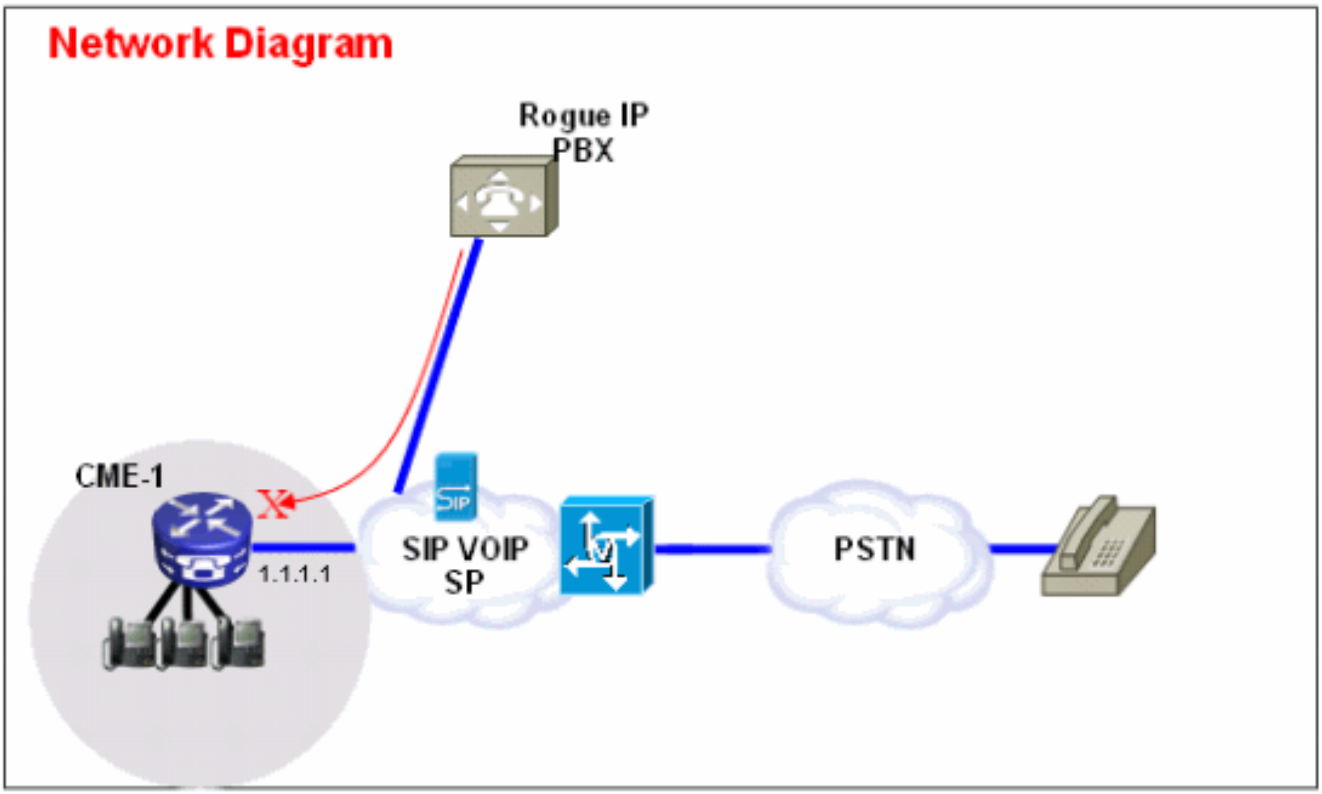
Exemplo de configuração — CME 1

```
interface serial 0/0
  ip access-group 100 in
!
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

[Exemplo 2]

Neste exemplo, o CME 1 está conectado ao provedor SIP para conectividade PSTN com a configuração de exemplo fornecida no Exemplo de Configuração de Entroncamento SIP do Cisco CallManager Express (CME).

Como o CME 1 está na Internet pública, é possível que *fraudes de tarifas* possam ocorrer se um usuário invasor verificar endereços IP públicos em busca de portas conhecidas para sinalização H.323 (TCP 1720) ou SIP (UDP ou TCP 5060) e enviar mensagens SIP ou H.323 que roteiam chamadas de volta do tronco SIP para o PSTN. Os abusos mais comuns nesse caso são que o usuário invasor faz várias chamadas internacionais através do tronco SIP ou H.323 e faz com que o proprietário do CME 1 pague essas chamadas de fraude de pedágio - em alguns casos, milhares de dólares.




## Solução

Para atenuar essa ameaça, você pode usar várias soluções. Se qualquer sinalização de VOIP (SIP ou H.323) não for usada sobre os links de WAN no CME 1, isso deverá ser bloqueado com as técnicas de firewall no CME 1 (Access-lists ou ACLs) o máximo possível.

1. Proteja a interface WAN com o firewall Cisco IOS® no CME 1:Isso significa que você permite que apenas o tráfego SIP ou H.323 conhecido entre na interface da WAN. Todos os outros tráfegos SIP ou H.323 estão bloqueados. Isso também exige que você saiba os endereços IP que o SIP VOIP SP usa para sinalização no Tronco SIP. Essa solução supõe que o SP esteja disposto a fornecer todos os endereços IP ou nomes DNS usados em sua rede. Além disso, se os nomes DNS forem usados, a configuração exigirá que um servidor DNS que possa resolver esses nomes esteja acessível. Além disso, se a controladora alterar qualquer endereço na extremidade, a configuração precisará ser atualizada no CME 1. Observe que essas linhas precisam ser adicionadas além de quaisquer entradas ACL já presentes na interface WAN.Exemplo de configuração — CME 1

```
interface serial 0/0
  ip access-group 100 in
```

```
!
access-list 100 permit udp host 1.1.1.254 eq 5060 any
!--- 1.1.1.254 is SP SIP proxy access-list 100 permit udp host 1.1.1.254 any eq 5060
access-list 100 permit udp any any range 16384 32767
```

2. Certifique-se de que as chamadas recebidas no tronco SIP **NÃO** façam backout:Isso implica que a configuração do CME 1 permite somente o hairpin SIP - SIP de chamadas para um intervalo de números PSTN conhecido específico, e todas as outras chamadas são bloqueadas. Você deve configurar peers de discagem de entrada específicos para os números PSTN que entram no tronco SIP que são mapeados para ramais, atendimento automático ou correio de voz no CME 1. Todas as outras chamadas para números que não fazem parte do intervalo de números PSTN do CME 1 são bloqueadas. Observe que isso não afeta o encaminhamento de chamadas/transferências para o correio de voz (Cisco Unity Express) e o encaminhamento de chamadas para números PSTN de telefones IP no CME 1, pois a chamada inicial ainda é direcionada para um ramal no CME 1.Exemplo de configuração — CME 1

```
dial-peer voice 1000 voip
  description ** Incoming call to 4085551000 from SIP trunk **
  voice-class codec 1
  voice-class sip dtmf-relay force rtp-nte
  session protocol sipv2
  incoming called-number 4085551000
  dtmf-relay rtp-nte
  no vad
!
dial-peer voice 1001 voip
  permission term
!--- Prevent hairpinning calls back over SIP Trunk. description ** Incoming call from SIP
trunk ** voice-class codec 1 voice-class sip dtmf-relay force rtp-nte session protocol
sipv2 incoming called-number .T
!--- Applies to all other inbound calls. dtmf-relay rtp-nte no vad
```

3. Use regras de tradução para bloquear cadeias de discagem específicas:A maioria das fraudes de pedágio envolve discagem de chamadas internacionais. Como resultado, você pode criar um peer de discagem de entrada específico que corresponda a strings discadas específicas e bloqueie as chamadas para elas. A maioria dos CMEs usa um código de acesso específico, como 9, para discar e o código de discagem internacional nos EUA é 011. Portanto, a string de discagem mais comum a ser bloqueada nos EUA é 9011 + qualquer dígito depois disso aparecer no tronco SIP.Exemplo de configuração — CME 1

```
voice translation-rule 1000
 rule 1 reject /^9011/
 rule 2 reject /^91900…….$/
 rule 3 reject /^91976…….$/
!
voice translation-profile BLOCK
translate called 1000
!
dial-peer voice 1000 voip
description ** Incoming call from SIP trunk **
incoming called-number 9011T
call-block translation-profile incoming BLOCK
```

# Ferramentas de restrição de recurso

## Padrão de transferência

### Resumo

As transferências para todos os números, exceto os dos telefones IP SCCP locais, são automaticamente bloqueadas por padrão. Durante a configuração, você pode permitir transferências para números não locais. O comando **transfer-pattern** é usado para permitir a transferência de chamadas telefônicas de telefones IP Cisco SCCP para telefones diferentes de telefones IP Cisco, como chamadas PSTN externas ou telefones em outro sistema CME. Você pode usar o **padrão de transferência** para limitar as chamadas somente a ramais internos ou talvez limitar as chamadas para números PSTN em um determinado código de área. Estes exemplos mostram como o comando **transfer-pattern** pode ser usado para limitar as chamadas a números diferentes.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Permitir que os usuários transfiram chamadas para apenas o código de área 408. Neste exemplo, presume-se que o CME é configurado com um peer de discagem que tem um padrão de destino 9T.

Configuração de exemplo

```
telephony-service
transfer-pattern 91408
```

## Padrão de transferência bloqueado

### Resumo

No Cisco Unified CME 4.0 e versões posteriores, você pode impedir que telefones individuais transfiram chamadas para números globalmente ativados para transferência. O comando **transfer-pattern blocking** substitui o comando **transfer-pattern** e desativa a transferência de chamadas para qualquer destino que precise ser alcançado por um peer de discagem POTS ou VoIP. Isso inclui números PSTN, outros gateways de voz e o Cisco Unity Express. Isso garante que os telefones individuais não sofram tarifas quando as chamadas são transferidas para fora do sistema Cisco Unified CME. O bloqueio de transferência de chamadas pode ser configurado para telefones individuais ou configurado como parte de um modelo aplicado a um conjunto de telefones.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Nesta configuração de exemplo, o ephone 1 não tem permissão para usar o padrão de transferência (definido globalmente) para transferir chamadas, enquanto o ephone 2 pode usar o padrão de transferência definido em serviço de telefonia para transferir chamadas.

Configuração de exemplo

```
ephone-template 1
```

```
transfer-pattern blocked
!
ephone 1
ephone-template 1
!
ephone 2
!
```

## Transfer max-length

### Resumo

O comando **transfer max-length** especifica o número máximo de dígitos que o usuário pode discar quando uma chamada é transferida. O **transfer-pattern max-length** substitui o comando **transfer-pattern** e aplica os dígitos máximos permitidos para o destino de transferência. O argumento especifica o número de dígitos permitidos em um número para o qual uma chamada é transferida. Faixa: 3 a 16. Padrão: 16.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Essa configuração permite apenas telefones que tenham este ephone-template aplicado para transferência para destinos que tenham no máximo quatro dígitos.

Configuração de exemplo

```
ephone-template 1
transfer max-length 4
```

## Comprimento máximo do encaminhamento de chamadas

### Resumo

Para restringir o número de dígitos que podem ser inseridos com a tecla virtual CfwdALL em um telefone IP, use o comando **call-forward max-length** no modo de configuração ephone-dn ou ephone-dn-template. Para remover uma restrição do número de dígitos que podem ser inseridos, use a forma **no** desse comando.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Neste exemplo, a extensão de diretório 101 tem permissão para executar um encaminhamento de chamada para qualquer ramal com um a quatro dígitos. Qualquer encaminhamento de chamada para destinos com mais de quatro dígitos falha.

Configuração de exemplo

```
ephone-dn  1  dual-line
number 101
call-forward max-length 4
```

or

```
ephone-dn-template  1
call-forward max-length 4
```

## Sem Encaminhamento de Chamada Local

### Resumo

Quando o comando **no forward local-calls** é usado no modo de configuração ephone-dn, as chamadas internas para um ephone-dn específico com **nenhuma chamada local de encaminhamento** aplicada não são encaminhadas se o ephone-dn estiver ocupado ou não atender. Se um chamador interno tocar em ephone-dn e ephone-dn estiver ocupado, o chamador ouvirá um sinal de ocupado. Se um chamador interno tocar nesse ephone-dn e ele não atender, o chamador ouvirá um sinal de chamada de volta. A chamada interna não é encaminhada mesmo que o desvio de chamadas esteja ativado para ephone-dn.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Neste exemplo, o ramal 222 chama o ramal 3675 e ouve um sinal de chamada de volta ou de ocupado. Se um chamador externo alcançar o ramal 3675 e não houver resposta, a chamada será encaminhada para o ramal 4000.

Configuração de exemplo

```
ephone-dn  25
number 3675
no forward local-calls
call-forward noan 4000 timeout 30
```

## Desative o registro automático no sistema CME

### Resumo

Quando o **autorreg-ephone** é ativado sob o serviço de telefonia em um sistema SCCP CME, os novos telefones IP conectados ao sistema são registrados automaticamente e se a **atribuição automática** é configurada para atribuir automaticamente números de ramal, um novo telefone IP pode fazer chamadas imediatamente.

**Observação:** essa é uma **ameaça interna**.

### Exemplo 1

Nesta configuração, um novo sistema CME é configurado para que você deve adicionar manualmente um telefone para que o telefone se registre no sistema CME e use-o para fazer chamadas de telefonia IP.

**Solução**

Você pode desabilitar o **autoreg-ephone** sob o serviço de telefonia para que os novos telefones IP conectados a um sistema CME não se registrem automaticamente no sistema CME.

Configuração de exemplo

```
telephony-service
no auto-reg-ephone
```

### Exemplo 2

Se você usa o SCCP CME e planeja registrar os telefones SIP da Cisco no sistema, configure o sistema para que os endpoints SIP tenham que se autenticar com um nome de usuário e senha. Para fazer isso, basta configurar:

```
voice register global
 mode cme
 source-address 192.168.10.1 port 5060
 authenticate register
```

Consulte o SIP: Configurando o Cisco Unified CME para obter um guia de configuração mais abrangente para o SIP CME.

## Ferramentas de restrição do Cisco Unity Express

### Cisco Unity Express seguro: acesso PSTN AA

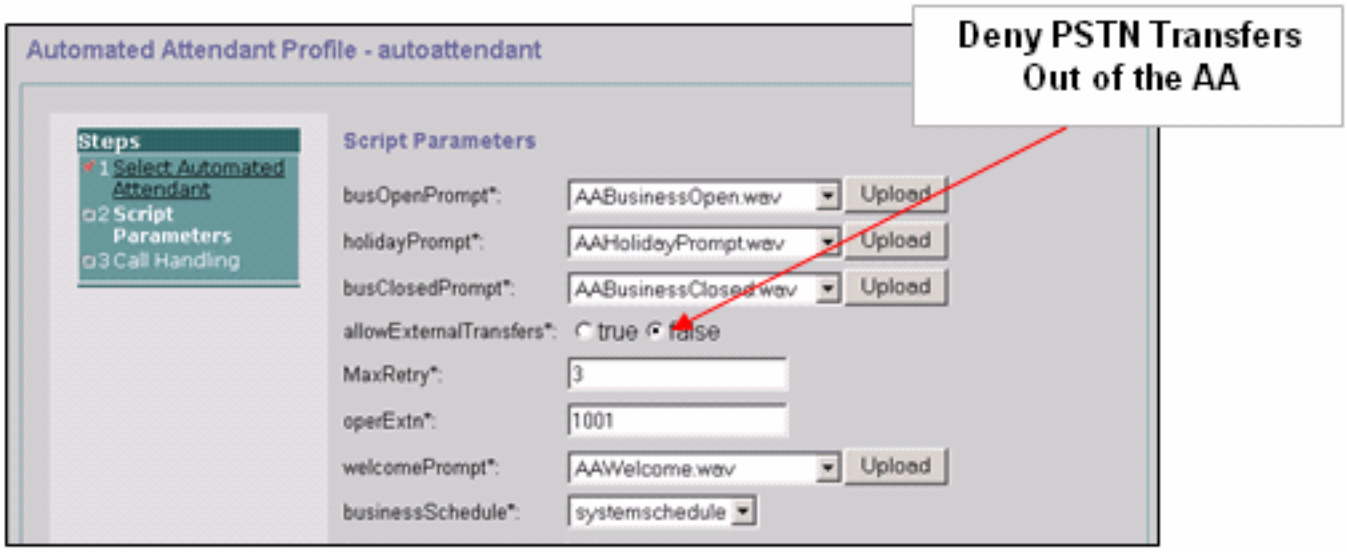
#### Resumo

Quando o sistema está configurado para que as chamadas de entrada sejam encaminhadas para o atendimento automático (AA) no Cisco Unity Express, pode ser necessário desativar a transferência externa para a PSTN do AA do Cisco Unity Express. Isso não permite que usuários externos disquem para números externos depois de acessarem o AA do Cisco Unity Express.

**Observação:** essa é uma **ameaça externa**.

**Note: Solução**

**Observação:** desative a opção **allowExternalTransfers** na GUI do Cisco Unity Express.




**Observação:** se o acesso PSTN do AA for necessário, limite os números ou o intervalo de números considerados válidos pelo script.

## Tabelas de restrições do Cisco Unity Express

### Resumo

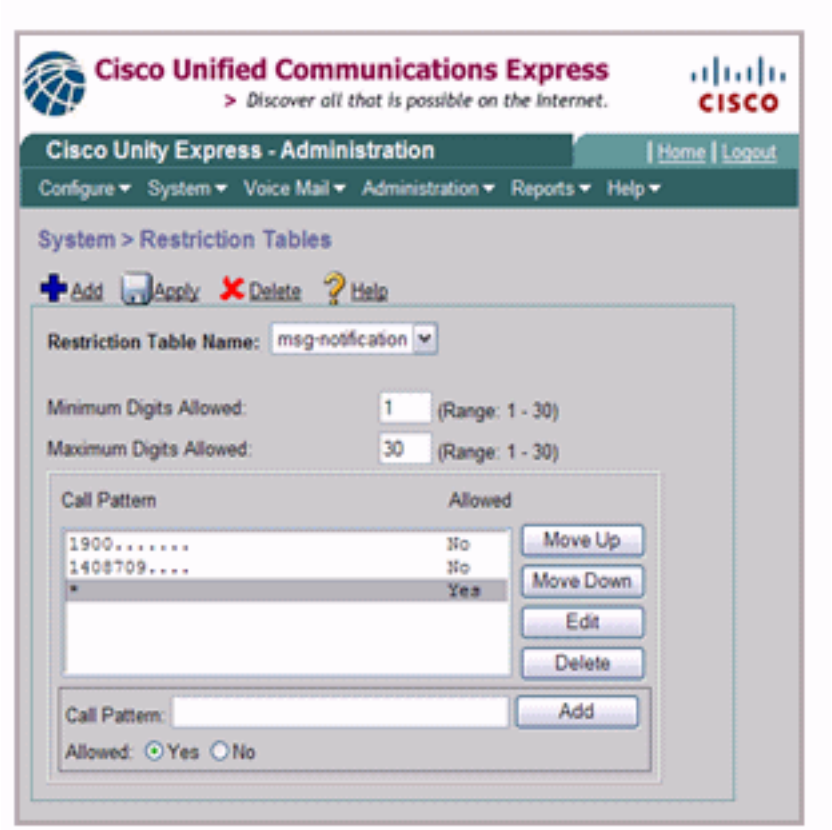
Você pode usar as tabelas de restrição do Cisco Unity Express para restringir os destinos que podem ser alcançados durante uma chamada externa do Cisco Unity Express. A tabela de restrições do Cisco Unity Express pode ser usada para evitar fraudes de pedágio e uso mal-intencionado do sistema Cisco Unity Express para fazer chamadas de saída. Se você usar a tabela de restrição do Cisco Unity Express, poderá especificar padrões de chamada para correspondência de curinga. Os aplicativos que usam a tabela de restrição do Cisco Unity Express incluem:

- Fax
- Cisco Unity Express Live Replay
- Notificação de mensagem
- Entrega de mensagem de não-assinante

**Observação:** essa é uma **ameaça interna**.

### Solução

Para restringir os padrões de destino que podem ser alcançados pelo Cisco Unity Express em uma chamada externa de saída, configure o **Padrão de Chamada** no **Sistema > Tabelas de Restrições** da GUI do Cisco Unity Express.




# Registro de chamadas

## CDR avançado

Você pode configurar o sistema CME para capturar CDR avançado e registrar o CDR na memória flash do roteador ou em um servidor FTP externo. Esses registros podem ser usados para rerastrear chamadas para verificar se houve abuso por parte de partes internas ou externas.

O recurso de contabilização de arquivos introduzido com CME 4.3/7.0 no Cisco IOS versão 12.4(15)XY fornece um método para capturar registros de contabilidade no formato de valor separado por vírgulas (.csv) e armazenar os registros em um arquivo na memória flash interna ou em um servidor FTP externo. Ele expande o suporte de contabilidade de gateway, que também inclui os mecanismos AAA e syslog de registro de informações de contabilidade.

O processo contábil coleta dados contábeis para cada trecho de chamada criado em um gateway de voz da Cisco. Você pode usar essas informações para atividades de pós-processamento, como para gerar registros de cobrança e para análise de rede. Os gateways de voz da Cisco capturam dados de contabilidade na forma de registros de detalhes de chamadas (CDRs) que contêm atributos definidos pela Cisco. O gateway pode enviar CDRs para um servidor RADIUS, servidor syslog e, com o novo método de arquivo, para flash ou para um servidor FTP no formato .csv.

Consulte Exemplos de CDR para obter mais informações sobre os recursos de CDR avançado.

# Informações Relacionadas

- Práticas recomendadas de segurança do Cisco Unified Communications Manager Express
- Guia dos administradores do Cisco Communications Manager Express

- Guia do Cisco Communications Manager Express Administrators - Bloqueio de chamadas
- Entendendo a correspondência de peer de discagem em plataformas IOS
- Tradução de números usando perfis de conversão de voz
- Guia de projeto de rede de referência da solução CME
- Suporte Técnico e Documentação - Cisco Systems