Unified Communications Manager Express长话欺骗预防

目录

简介

本文档提供了配置指南，可用于帮助保护Cisco Communications Manager Express(CME)系统并降低收费欺诈威胁。CME是思科基于路由器的呼叫控制解决方案，为希望实施统一通信的组织提供智能、简单且安全的解决方案。强烈建议您实施本文档中介绍的安全措施，以提供更高级别的安全控制并降低收费欺诈的可能性。

本文档旨在向您介绍思科语音网关和CME上提供的各种安全工具。这些工具可在CME系统上实施，以帮助减轻内部和外部双方的长途电话欺诈威胁。

本文档提供有关如何使用各种收费安全和功能限制工具配置CME系统的说明。本文档还概述了为什

么某些部署中使用某些安全工具。

思科ISR平台的整体固有灵活性允许您在多种不同类型的部署中部署CME。因此，可能需要结合使用本文档中描述的功能来帮助锁定CME。本文档是有关如何在CME上应用安全工具的指南，无法保证内部和外部双方不会发生长途电话欺诈或滥用。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager Express

使用的组件

本文档中的信息基于Cisco Unified Communications Manager Express 4.3和CME 7.0。

注意：Cisco Unified CME 7.0包含与Cisco Unified CME 4.3相同的功能，该功能将重新编号为7.0，以与Cisco Unified Communications版本保持一致。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

概述

本文档介绍CME系统上最常用的安全工具，以帮助降低收费欺诈威胁。本文档中引用的CME安全工具包括收费限制工具和功能限制工具。

收费限制工具

- Direct-inward-dial
- 非工作时间收费限制
- 限制类
- 限制H323/SIP中继访问的访问列表

功能限制工具

- 传输模式
- 传输模式被阻止
- 传输最大长度
- 呼叫转移最大长度
- 无前转本地呼叫

- 无auto-reg-ephone

Cisco Unity Express限制工具

- 安全Cisco Unity Express PSTN访问
- 留言通知限制

呼叫记录

- 呼叫记录以捕获呼叫详细记录(CDR)

内部威胁与外部威胁

本文档讨论来自内部和外部各方的威胁。内部参与方包括驻留在CME系统上的IP电话用户。外部参与方包括外部系统上的用户，这些用户可尝试使用主机CME进行欺骗性呼叫，并将呼叫返回给您的CME系统。

收费限制工具

Direct-inward-dial

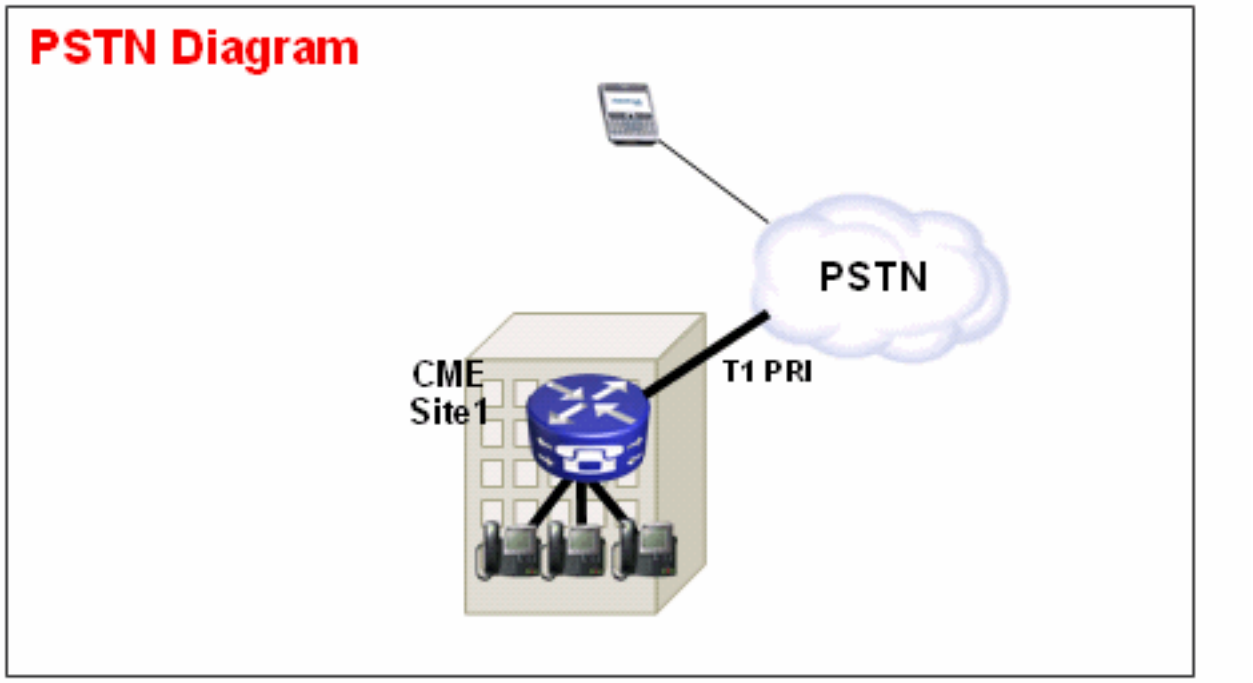
摘要

直接拨入(DID)用于思科语音网关，以便网关在收到来自PBX或CO交换机的数字后处理入站呼叫。启用DID后，思科网关不向主叫方显示辅助拨号音，也不等待从主叫方收集其他数字。它直接将呼叫转发到与入站拨号号码识别服务(DNIS)匹配的目标。 这称为一次拨号。

注意：这是外**部威胁**。

问题陈述

如果在思科网关或CME上未配置直接拨入，则每当呼叫从CO或PBX进入思科网关时，主叫方会听到辅助拨号音。这称为两阶段拨号。一旦PSTN主叫方听到辅助拨号音，他们可以输入数字以接通任何内部分机，或者如果他们知道PSTN访问代码，他们可以拨打长途或国际号码。这会带来问题，因为PSTN呼叫方可以使用CME系统发出出站长途或国际呼叫，并且公司会为这些呼叫付费。



示例 1

在站点1,CME通过T1 PRI中继连接到PSTN。PSTN提供商提**供40855512。**CME站点1的DID范围。因此，所有发往4085551200 - 4085551299的PSTN呼叫都被路由到CME的入站。如果未在系统**上配置直**接拨入，则入站PSTN呼叫者会听到辅助拨号音，必须手动拨打内部分机。更大的问题是，如果主叫方是用户，并且知道系统上的PSTN访问代码(通常为**9**)，则他们可以拨打**9**，然后拨打他们想要拨打的任何目的号码。

解决方案 1

要缓解此威胁，必须配置**直接拨入**。这会导致思科网关将入站呼叫直接转发到与入站DNIS匹配的目标。

配置示例

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

为使DID正常工作，请确保入站呼叫与配置了direct-inward-dial命令的**正确POTS拨号对**等体匹配。在本示例中，T1 PRI连接到端口1/0:23。要匹配正确的入站拨号对等体，请在DID POTS拨号对等体下发出**incoming called-number** 拨号对等体命令。

示例 2

在站点1,CME通过T1 PRI中继连接到PSTN。PSTN提供商提**供40855512..**和**40855513..**CME站点1的DID范围。因此，所有发往4085551200 - 4085551299和4085551300 - 4085551399的PSTN呼叫都路由到CME的入站。

配置不正确：

如果配置入站拨号对等体（如本部分的示例配置），则仍有可能发生长途电话欺诈。此入站拨号对等体的问题是，它仅匹配到40852512的入站呼**叫，然后**应用DID服务。如果PSTN呼叫进入

40852513...，则入站pots拨号对等体不匹配，因此DID服务未应用。如果DID的入站拨号对等体不匹配，则使用默认拨号对等体0。默认情况下在拨号对等体 0 上禁用 DID。

配置示例

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

正确配置

在入站拨号对等体上配置DID服务的正确方法如下例所示：

配置示例

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

有关数字T1/E1语音端口的DID的详细信息，请参阅POTS拨号对等体的DID配置。

注：当在语音端口上使用专用线路自动振铃(PLAR)或在入站拨号对等体上使用服务脚本(如自动总机(AA))时，不需要使用DID。

示例配置 — PLAR

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

示例配置 — 服务脚本

```
dial-peer voice 1 pots
service AA
port 1/0:23
```

非工作时间收费限制

摘要

非工作时间收费限制是CME 4.3/7.0中提供的新安全工具，允许您根据时间和日期配置收费限制策略。您可以配置策略，以便用户在一天中的某些小时或所有时间内，不能对预定义号码进行呼叫。如果配置了7x24非工作时间呼叫阻止策略，它还会限制内部用户可以输入的号码集，以设置全**部呼叫转移**。

注意：这是内部**威胁**。

示例 1

本示例定义了阻止出站呼叫的数字的几种模式。模式1和模式2阻止以“1”和“011”开头的外部号码的呼叫，它们在星期一至星期五的上午7点之前和晚上7点之后、星期六的上午7点之前和下午1点之后以及整个星期日被阻止。模式3每周7天、每天24小时阻止900号码的呼叫。

配置示例

```
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
```

有关长途电话限制的详细信息，请参阅配置呼叫阻止。

限制类

摘要

如果要在配置收费限制时进行精细控制，则必须使用限制类别(COR)。 请参阅限制类：示例。

H.323/SIP中继收费欺诈限制

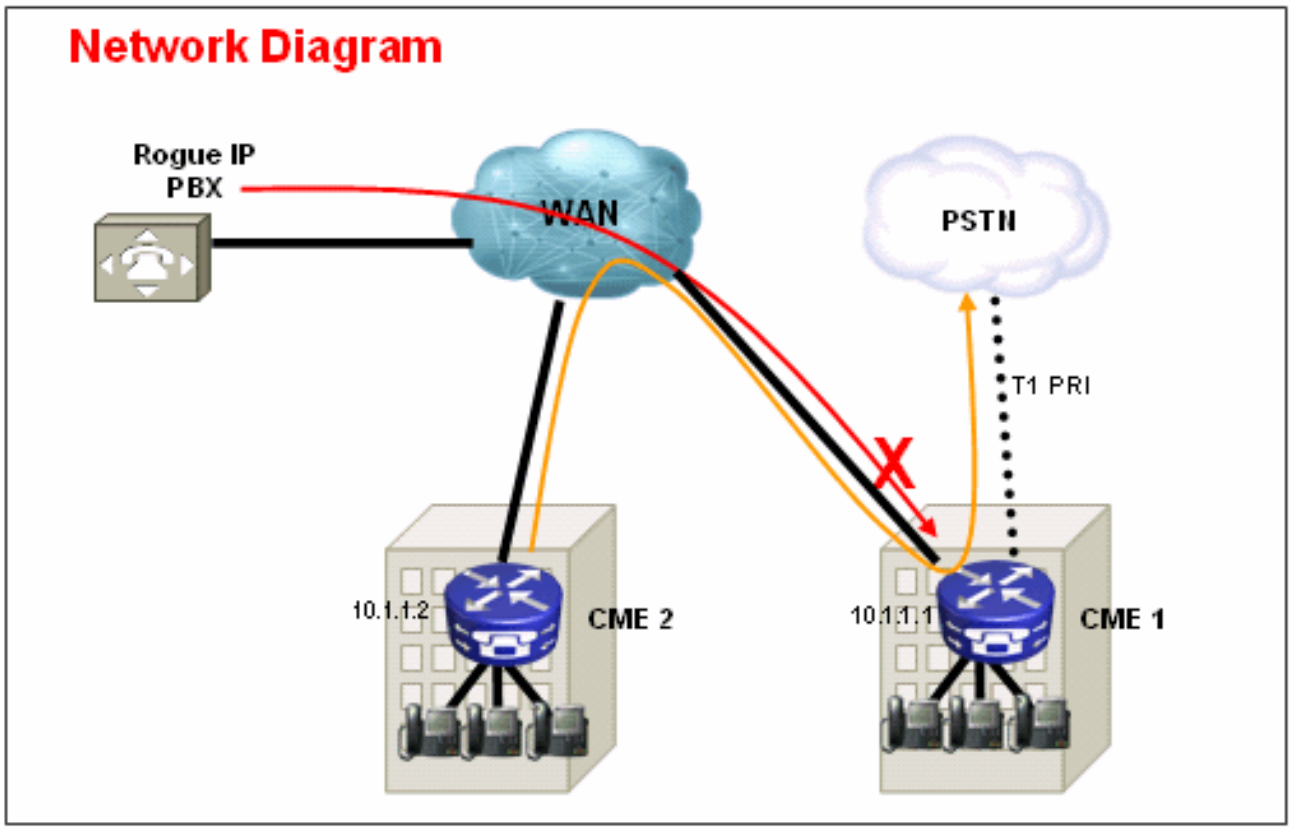
摘要

如果CME系统通过SIP或H.323中继通过WAN连接到其他CME设备，则可以限制对CME的SIP/H.323中继访问，以防止滥用者使用您的系统将呼叫非法中继到PSTN。

注意：这是外**部威胁**。

示例 1

在本例中，CME 1具有PSTN连接。CME 2通过WAN通过H.323中继连接到CME 1。为了保护CME 1，您可以配置访问列表并将其应用于WAN接口的入站流量，从而仅允许来自CME 2的IP流量。这可防止欺诈IP PBX通过CME 1将VOIP呼叫发送到PSTN。



解决方案

不要允许CME 1上的WAN接口接受来自其无法识别的欺诈设备的流量。请注意，访问列表末尾有一个隐式DENY all。如果有更多设备要允许入站IP流量，请务必将设备的IP地址添加到访问列表。

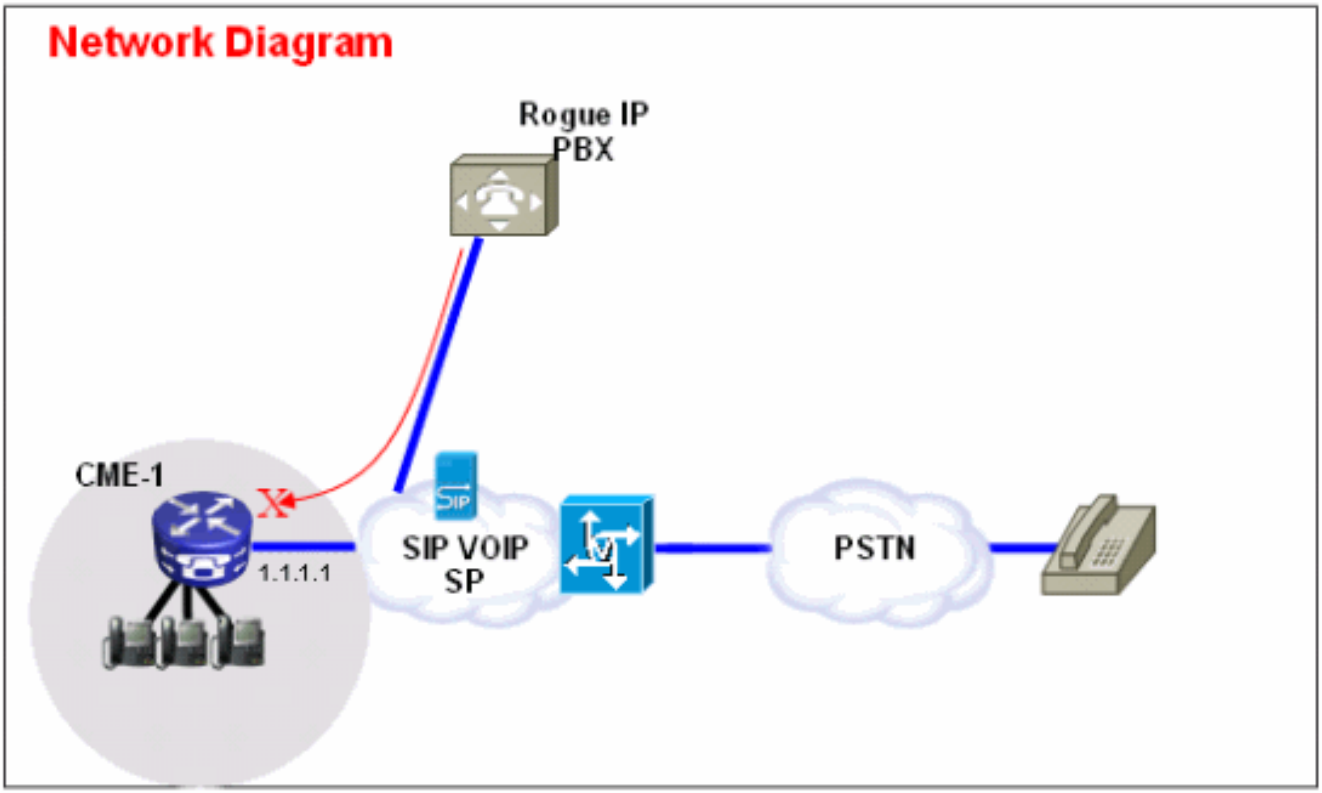
配置示例 — CME 1

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

示例 2

在本示例中，CME 1通过Cisco CallManager Express(CME)SIP中继配置示例中提供的配置示例连接到SIP提供商以实现PSTN连接。

由于CME 1在公共互联网上，因此，如果欺诈用户扫描公有IP地址以查找H.323(TCP 1720)或SIP（UDP或TCP 5060）信令，并发送路由呼叫的SIP或H.323消息，则可能会发生*话费欺诈从SIP中继返回到PSTN*。在这种情况下，最常见的滥用是欺诈用户通过SIP或H.323中继进行多个国际呼叫，并导致CME 1的所有者为这些收费欺诈呼叫支付费用（在某些情况下为数千美元）。



解决方案

为了缓解此威胁，您可以使用多个解决方案。如果任何VOIP信令（SIP或H.323）未通过WAN链路使用到CME 1，则必须尽可能使用CME 1（访问列表或ACL）上的防火墙技术来阻止此流量。

1. 在CME 1上使用Cisco IOS®防火墙保护WAN接口：这意味着您只允许已知SIP或H.323流量进入WAN接口。所有其他SIP或H.323流量都被阻止。这还要求您知道SIP VOIP SP在SIP中继上用于信令的IP地址。此解决方案假设SP愿意提供其网络中使用的所有IP地址或DNS名称。此外，如果使用DNS名称，则配置要求可以解析这些名称的DNS服务器是可访问的。此外，如果SP更改其端的任何地址，则配置需要在CME 1上更新。请注意，除WAN接口上已存在的任何ACL条目外，还需要添加这些行。配置示例 — 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. 确保SIP中继上进入的呼叫不会发夹退出：这意味着CME 1配置仅允许SIP — 呼叫到特定已知PSTN号码范围的SIP发夹，所有其他呼叫都被阻止。您必须为SIP中继上传入的PSTN号码配置特定入站拨号对等体，这些号码映射到CME 1上的分机或自动总机或语音邮件。阻止对不属于CME 1 PSTN号码范围的号码的所有其他呼叫。注意，这不影响呼叫转移/转移到语音邮件(Cisco Unity Express)，并且从CME 1上的IP电话将所有呼叫转移到PSTN号码，因为初始呼叫仍针对CME 1上的分机。配置示例 — 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. 使用转换规则以阻止特定拨号字符串：大多数收费欺诈都涉及国际呼叫拨号。因此，您可以创建与特定拨号字符串匹配并阻止呼叫的特定入站拨号对等体。大多数CME使用特定访问代码（如9）拨出，而美国的国际拨号代码是011。因此，美国最常阻止的拨号字符串是9011 +进入SIP中继后的任意数字。配置示例 — 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
```

功能限制工具

传输模式

摘要

默认情况下，会自动阻止传输到除本地SCCP IP电话上的号码外的所有号码。在配置期间，您可以允许传输到非本地号码。使用**transfer-pattern**命令可允许将电话呼叫从Cisco SCCP IP电话转接到除Cisco IP电话外的电话，如外部PSTN呼叫或另一CME系统上的电话。您可以使用**transfer-pattern**来仅限内部分机的呼叫，或仅限某些区号中的PSTN号码的呼叫。这些示例显示了如**何使用transfer-pattern** 命令将呼叫限制为不同的号码。

注意：这是内部**威胁**。

示例 1

允许用户仅将呼出转接到408区号。在本例中，假设CME配置了目标模式为9T的拨号对等体。

配置示例

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

已阻止传输模式

摘要

在Cisco Unified CME 4.0及更高版本中，您可以阻止单个电话将呼叫转接到全局启用以进行转接的

号码。**transfer-pattern blocked** 命令会绕过**transfer-pattern** 命令，并禁用到需要由POTS或VoIP拨号对等体到达的任何目的地的呼叫转接。这包括PSTN号码、其他语音网关和Cisco Unity Express。这可确保当呼叫在Cisco Unified CME系统外转接时，单个电话不会产生长途电话费。呼叫转移阻止可以配置给单个电话或配置为应用于一组电话的模板的一部分。

注意：这是内部**威胁**。

示例 1

在此示例配置中，ephone 1不允许使用转接模式（全局定义）来转接呼叫，而ephone 2可以使用电话服务下定义的转接模式来转接呼叫。

配置示例

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

传输最大长度

摘要

transfer max-**length**命令指定当呼叫被转接时用户可以拨打的最大位数。transfer-**pattern max-length** over-rides the transfer-pattern**命令并**实施允许用于传输目的地的最大数字。该参数指定呼叫被转接到的号码中允许的位数。范围：3到16。默认值：16.

注意：这是内部**威胁**。

示例 1

此配置仅允许应用此电话模板的电话转接到长度最多为四位的目的地。

配置示例

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

呼叫前转最大长度

摘要

要限制在IP电话上使用CfwdALL软键可输入的位数，请在ephone-dn或ephone-dn-template配置模式下使用**call-forward max-length**命令。要取消对可输入位数的限制，请使用此命令的**no**形式。

注意：这是内部**威胁**。

示例 1

在本例中，允许目录分机101向长度为一到四位的任何分机执行呼叫转移。任何到超过四位数的目的地的呼叫转发都失败。

配置示例

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

或

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

无前转本地呼叫

摘要

当在**ephone-dn配置模式下使用no forward local-calls**命令时，如果ephone-dn忙或未应答，则不会转发到未应用**forward local-calls**的特定ephone-dn的内部呼叫。如果内部主叫方振铃此ephone-dn，且ephone-dn忙，则主叫方听到忙音。如果内部主叫方振铃此ephone-dn，但未应答，则主叫方会听到回铃信号。即使为ephone-dn启用呼叫前转，内部呼叫也不会转接。

注意：这是内部**威胁**。

示例 1

在本例中，分机2222呼叫分机3675并听到回铃或忙音信号。如果外部呼叫者到达分机3675，但没有应答，则呼叫将转接到分机4000。

配置示例

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

禁用CME系统上的自动注册

摘要

当**auto-reg-ephone**在SCCP CME系统的telephony-service下启用时，插入系统的新IP电话将自动注册，如果**auto assign** 配置为自动分配分机号码，则新IP电话可以立即进行呼叫。

注意：这是内部**威胁**。

示例 1

在此配置中，配置了新的CME系统，以便您必须手动添加电话，以便电话注册到CME系统并使用它

进行IP电话呼叫。

解决方案

您可以在**电话服务下**禁用auto-reg-ephone，以便连接到CME系统的新IP电话不会自动注册到CME系统。

配置示例

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

示例 2

如果使用SCCP CME并计划向系统注册思科SIP电话，则必须配置系统，以便SIP终端必须使用用户名和密码进行身份验证。为此，只需配置以下项：

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

请参阅SIP:设置Cisco Unified CME以获得更全面的SIP CME配置指南。

Cisco Unity Express限制工具

安全Cisco Unity Express:PSTN访问

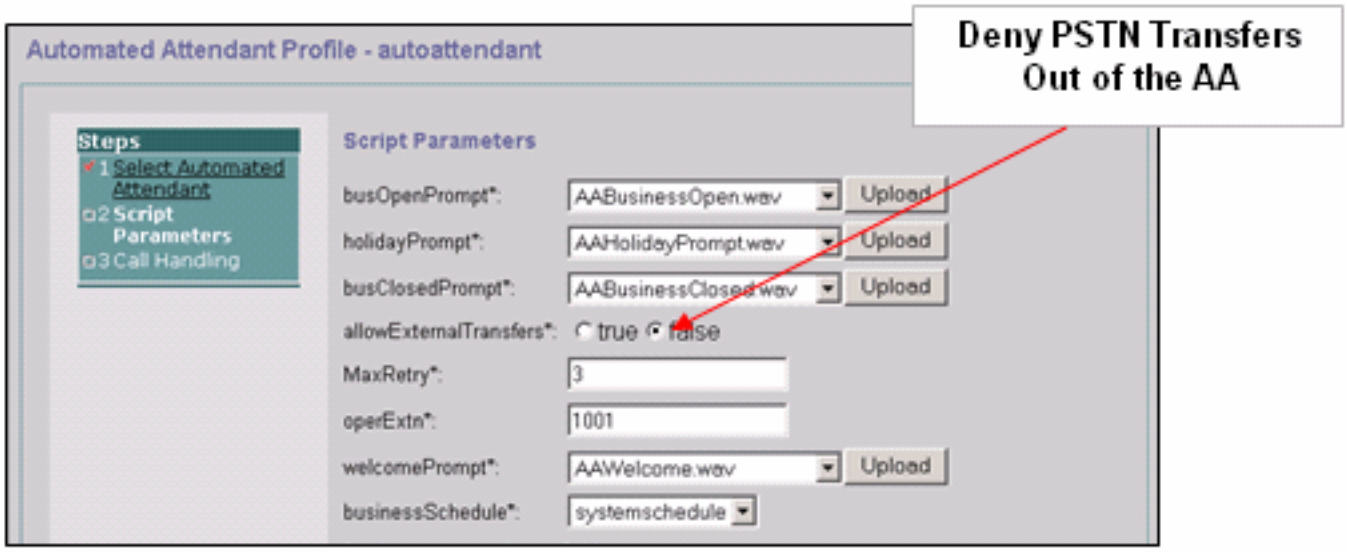
摘要

当您的系统配置为将入站呼叫转发到Cisco Unity Express上的自动总机(AA)时，可能需要禁用从Cisco Unity Express AA到PSTN的外部传输。这不允许外部用户在到达Cisco Unity Express AA后拨打外部号码。

注意：这是外**部威胁。**

注意： 解决方案

注意：在Cisco Unity Express **GUI上**禁用allowExternalTransfers选项。



注意：如果需要从AA进行PSTN访问，请限制脚本认为有效的号码或号码范围。

Cisco Unity Express限制表

摘要

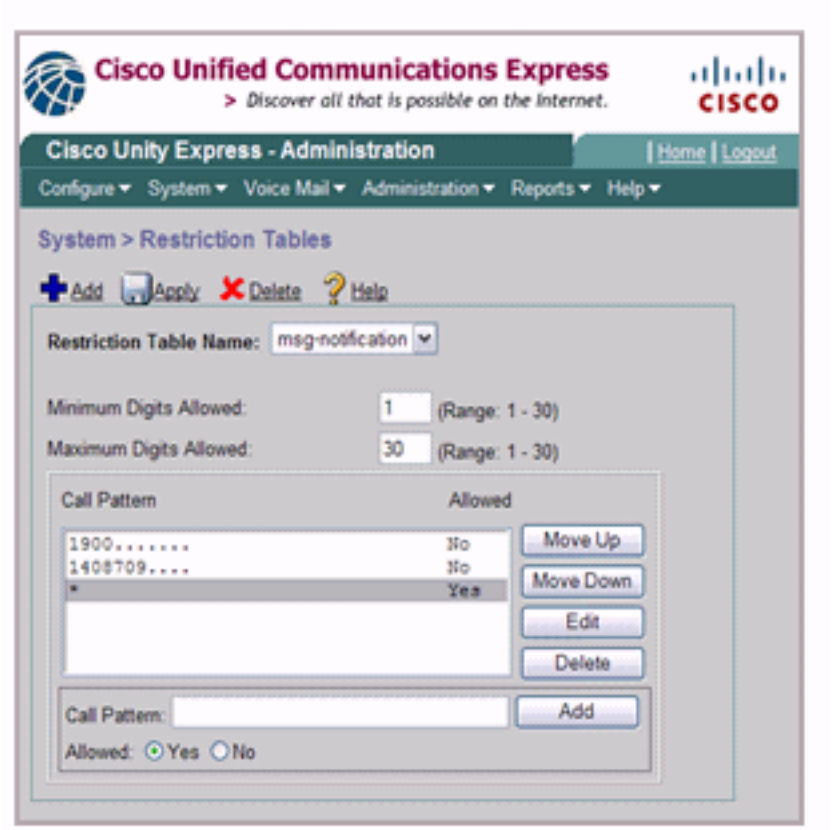
您可以使用Cisco Unity Express限制表来限制在从Cisco Unity Express发出呼出时可以到达的目标。Cisco Unity Express限制表可用于防止长途电话欺诈和恶意使用Cisco Unity Express系统进行出站呼叫。如果使用Cisco Unity Express限制表，可以指定通配符匹配的呼叫模式。使用Cisco Unity Express限制表的应用包括：

- 传真
- 思科Unity Express Live重播
- 留言通知
- 非用户消息传送

注意：这是内部**威胁**。

解决方案

要限制Cisco Unity Express在出站外部呼叫时可以到达的目标模式，请从Cisco Unity Express GUI的**System > Restrictions Tables**中配置**Call Pattern**。



呼叫记录

增强的CDR

您可以配置CME系统以捕获增强的CDR并将CDR记录到路由器闪存或外部FTP服务器。然后，这些记录可用于重新跟踪呼叫，以查看是否发生了内部或外部方的滥用。

Cisco IOS版本12.4(15)XY中CME 4.3/7.0引入的文件记帐功能提供了一种捕获逗号分隔值(.csv)格式的记帐记录并将记录存储到内部闪存或外部FTP服务器中的文件的方法。它扩展了网关记帐支持，包括记录记帐信息的AAA和系统日志机制。

记帐过程收集在思科语音网关上创建的每个呼叫段的记帐数据。您可以将此信息用于后处理活动，例如生成帐单记录和网络分析。思科语音网关以包含思科定义的属性的呼叫详细记录(CDR)形式捕获记帐数据。网关可以将CDR发送到RADIUS服务器、系统日志服务器，并使用新的文件方法，以.csv格式发送到闪存或FTP服务器。

有关增强的CDR功能的详细信息，请参阅CDR示例。

相关信息

- 思科统一通信管理器Express安全最佳实践
- Cisco Communications Manager Express管理员指南
- Cisco Communications Manager Express管理员指南 — 呼叫阻止
- 了解IOS平台上的拨号对等体匹配
- 使用语音转换配置文件进行号码转换
- CME解决方案参考网络设计指南
- 技术支持和文档 - Cisco Systems