整合通訊管理員Express收費欺詐防範

目錄

簡介

本文提供設定指南，可用於協助保護Cisco Communications Manager Express(CME)系統並降低收費欺詐的威脅。CME是思科基於路由器的呼叫控制解決方案，為希望實施統一通訊的組織提供智慧、簡單且安全的解決方案。強烈建議您實施本文檔中介紹的安全措施，以提供更高級別的安全控制並減少收費欺詐的可能性。

本文的目的是讓您瞭解Cisco語音網關和CME上可用的各種安全工具。這些工具可以在CME系統上實施，以幫助降低內部和外部各方造成的話費欺詐威脅。

本文說明如何使用各種收費安全和功能限制工具配置CME系統。本文檔還概述了為何在某些部署中使用某些安全工具。

思科ISR平台的整體固有靈活性允許您在許多不同型別的部署中部署CME。因此，可能需要使用本文檔中介紹的功能組合來幫助鎖定CME。本文檔為如何在CME上應用安全工具提供指南，並且無法保證不會發生內部和外部交易方的收費欺詐或濫用行為。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco整合通訊管理員Express版本

採用元件

本檔案中的資訊是根據Cisco Unified Communications Manager Express 4.3和CME 7.0。

注意：Cisco Unified CME 7.0包含與Cisco Unified CME 4.3相同的功能，後者將重新編號為7.0以與思科統一通訊版本保持一致。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

概觀

本文檔介紹可在CME系統上使用的最常見安全工具，以幫助降低收費欺詐的威脅。本文檔中引用的CME安全工具包括收費限制工具和功能限制工具。

收費限制工具

- 直接撥入
- 非工作時間收費限制
- 限制類別
- 用於限制H323/SIP中繼訪問的訪問清單

功能限制工具

- Transfer-pattern
- Transfer-pattern blocked
- 傳輸最大長度
- 來電轉駁最大長度
- 沒有轉接本地呼叫
- No auto-reg-ephone

Cisco Unity Express限制工具

- 安全Cisco Unity Express PSTN訪問
- 消息通知限制

通話記錄

- 呼叫記錄以捕獲呼叫詳細記錄(CDR)

內部與外部威脅

本檔案將討論來自內部和外部各方的威脅。內部參與方包括駐留在CME系統上的IP電話使用者。外部方包括外部系統上的使用者，這些使用者可能嘗試使用主機CME進行欺詐性呼叫，並讓呼叫回您的CME系統。

收費限制工具

直接撥入

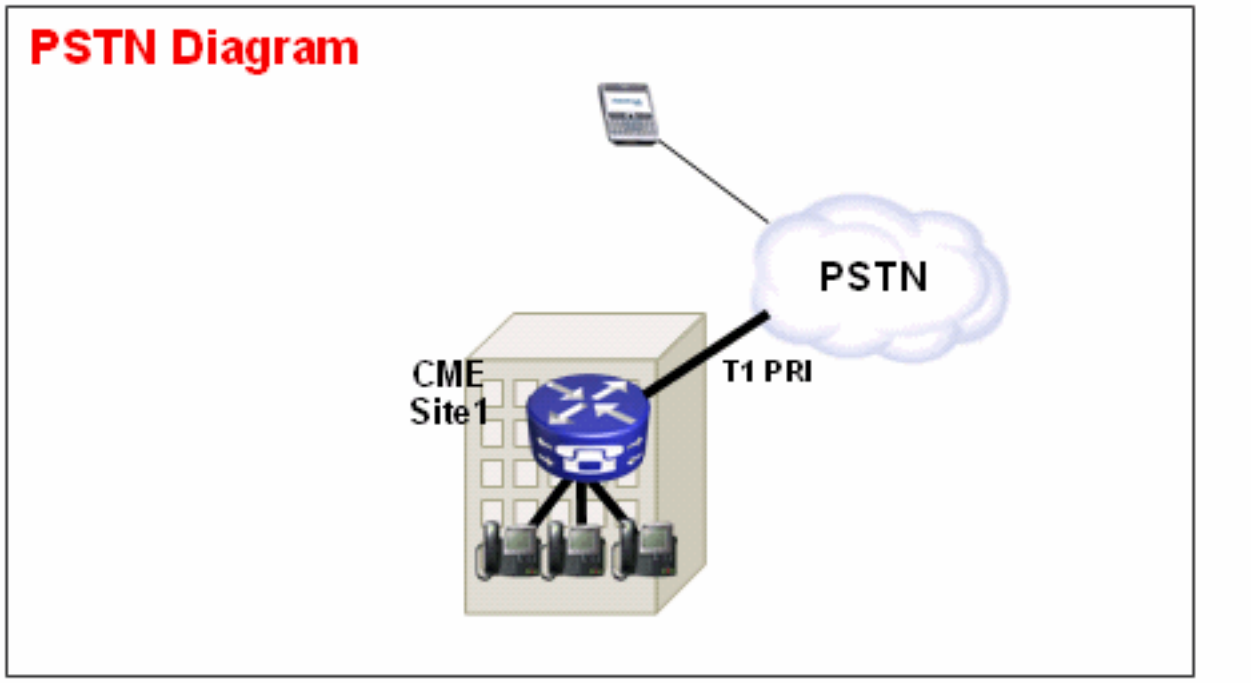
摘要

直接撥入(DID)用於思科語音閘道器，讓閘道在收到來自PBX或CO交換器的位元後處理傳入呼叫。啟用DID時，思科網關不會向呼叫方顯示輔助撥號音，並且不會等待從呼叫方收集其他數字。它會直接將呼叫轉送到與入站撥出號碼識別服務(DNIS)匹配的目標。 這稱為一級撥號。

注意：這是一個外**部威脅**。

問題陳述

如果未在Cisco網關或CME上配置直接撥入，則每當呼叫從CO或PBX進入思科網關時，呼叫者都會聽到輔助撥號音。這稱為兩階段撥號。一旦PSTN呼叫者聽到輔助撥號音，他們可以輸入數字以到達任何內部分機，或者如果他們知道PSTN接入代碼，他們可以撥打長途或國際號碼。這就產生了一個問題，因為PSTN呼叫者可以使用CME系統發出出站長途或國際呼叫，並且公司將收取呼叫費用。



範例 1

在站點1,CME通過T1 PRI中繼連線到PSTN。PSTN提供程式提供**40855512項。**CME站點1的DID範圍。因此，所有目的地為4085551200 - 4085551299的PSTN呼叫都將路由到CME。如果未在系統上配置**直接撥入**，則入站PSTN呼叫方會聽到輔助撥號音，並且必須手動撥打內部分機。更大的問題是，如果呼叫者是濫用者，並且知道系統上的PSTN訪問代碼(通常為9)，他們可以撥打**9**，然後撥打他們想撥的任何目標號碼。

解決方案1

為了緩解這種威脅，您必須配置**直接撥入**。這會導致思科閘道將傳入呼叫直接轉送到與傳入DNIS相符的目的地。

示例配置

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

為使DID正常工作，請確保入站呼叫與配置了**direct-inward-dial**命令的正確POTS撥號對等體匹配。在本示例中，T1 PRI連線到埠1/0:23。為了匹配正確的入站撥號對等體，請在DID POTS撥號對等體下發出**incoming called-number** dial peer命令。

範例 2

在站點1,CME通過T1 PRI中繼連線到PSTN。PSTN提供器提供**40855512..**和**40855513.**CME站點1的DID範圍。因此，發往4085551200 - 4085551299和4085551300 - 4085551399的所有PSTN呼叫都將路由到CME。

配置不正確：

如果您配置入站撥號對等體（如本節的示例配置所示），仍有可能發生收費欺詐。此入站撥號對等體的問題是它只將入站呼叫與**40852512匹配……**，然後應用DID服務。如果PSTN呼叫進入

40852513..，則入站pots撥號對等體不匹配，因此不應用DID服務。如果具有DID的入站撥號對等體不匹配，則使用預設撥號對等體0。撥號對等體0上預設禁用DID。

示例配置

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

正確配置

在入站撥號對等體上配置DID服務的正確方式如下例所示：

示例配置

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

有關數字T1/E1語音埠的DID的詳細資訊，請參閱POTS撥號對等體的DID配置。

注意：在語音埠上使用專用線路自動關註(PLAR)或在入站撥號對等體上使用自動總機(AA)等服務指令碼時，不需要使用**DID**。

示例配置 — PLAR

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

示例配置 — 服務指令碼

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

非工作時間收費限制

摘要

非工作時間收費限制是CME 4.3/7.0中提供的一種新安全工具，允許您根據時間和日期配置收費限制策略。您可以配置策略，這樣使用者在一天中的某些時段或所有時間都不允許呼叫預定義的號碼。如果配置了7x24非工作時間呼叫阻止策略，它還會限制內部使用者可輸入的號碼集，以設定**來電轉駁全部**。

注意：這是內**部威脅**。

範例 1

此示例定義出站呼叫被阻止的多個數字模式。第一模式和第二模式阻止撥打以「1」和「011」開頭的外部號碼，它們在週一到週五的上午7點之前、晚上7點之後、週六的上午7點之前、下午1點之後以及週日全天被遮蔽。Pattern 3每週7天、每天24小時阻止對900號碼的呼叫。

示例配置

```
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
```

請參閱配置呼叫阻塞以瞭解有關話費限制的詳細資訊。

限制類別

摘要

如果要在配置收費限制時進行精細控制，則必須使用限制等級(COR)。 請參閱限制類別：範例以瞭解詳細資訊。

H.323/SIP中繼收費欺詐限制

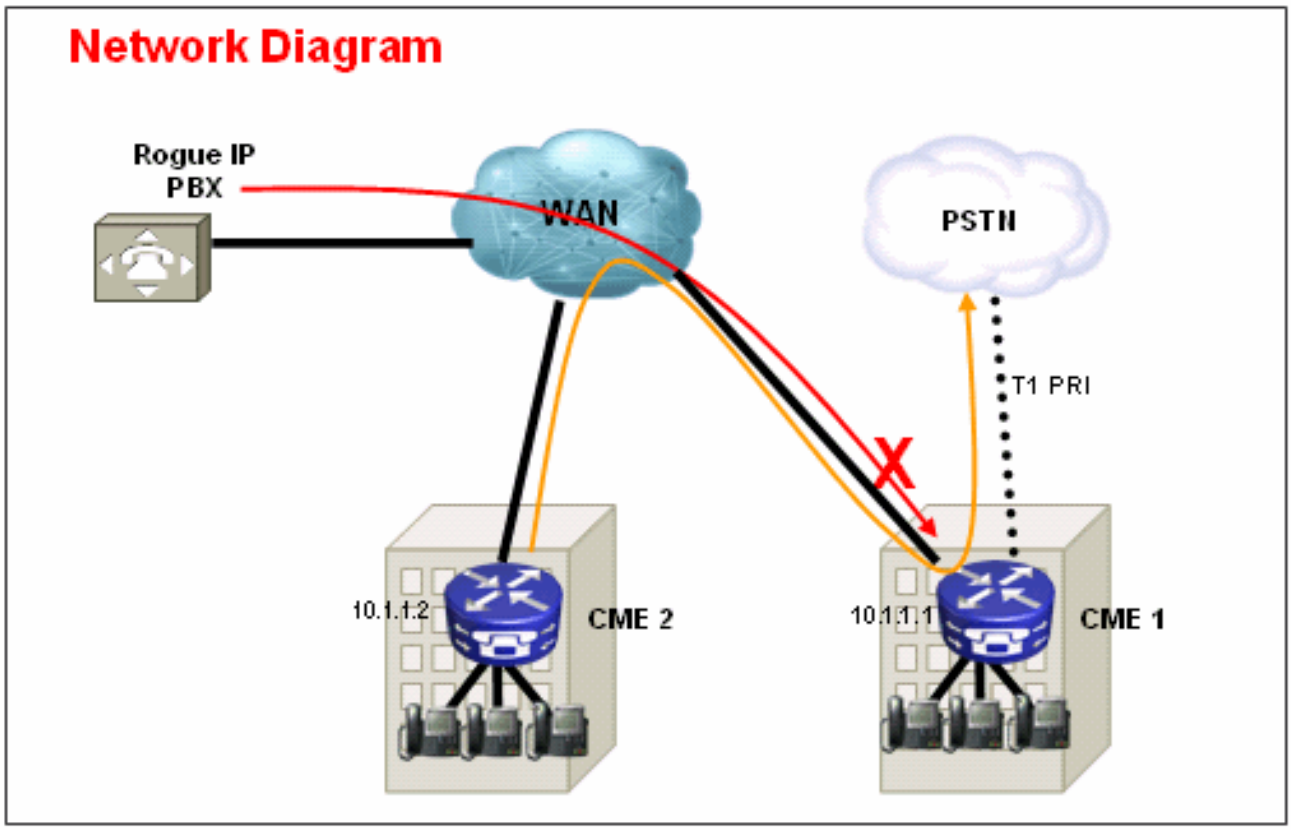
摘要

在CME系統通過WAN通過SIP或H.323中繼連線到其他CME裝置的情況下，您可以限制對CME的SIP/H.323中繼訪問，以防止濫用者使用您的系統非法將呼叫中繼到PSTN。

注意：這是一個外**部威脅**。

範例 1

在本例中，CME 1具有PSTN連線。CME 2通過H.323中繼通過WAN連線到CME 1。為了保護CME 1，您可以配置訪問清單並將其應用於WAN介面上的入站，從而僅允許來自CME 2的IP流量。這可以防止無管理IP PBX通過CME 1向PSTN傳送VOIP呼叫。



解決方案

不允許CME 1上的WAN介面接受來自它無法識別的非法裝置的流量。請注意，存取清單的結尾有隱含的DENY all。如果有更多裝置要允許入站IP流量，請確保將裝置的IP地址新增到訪問清單。

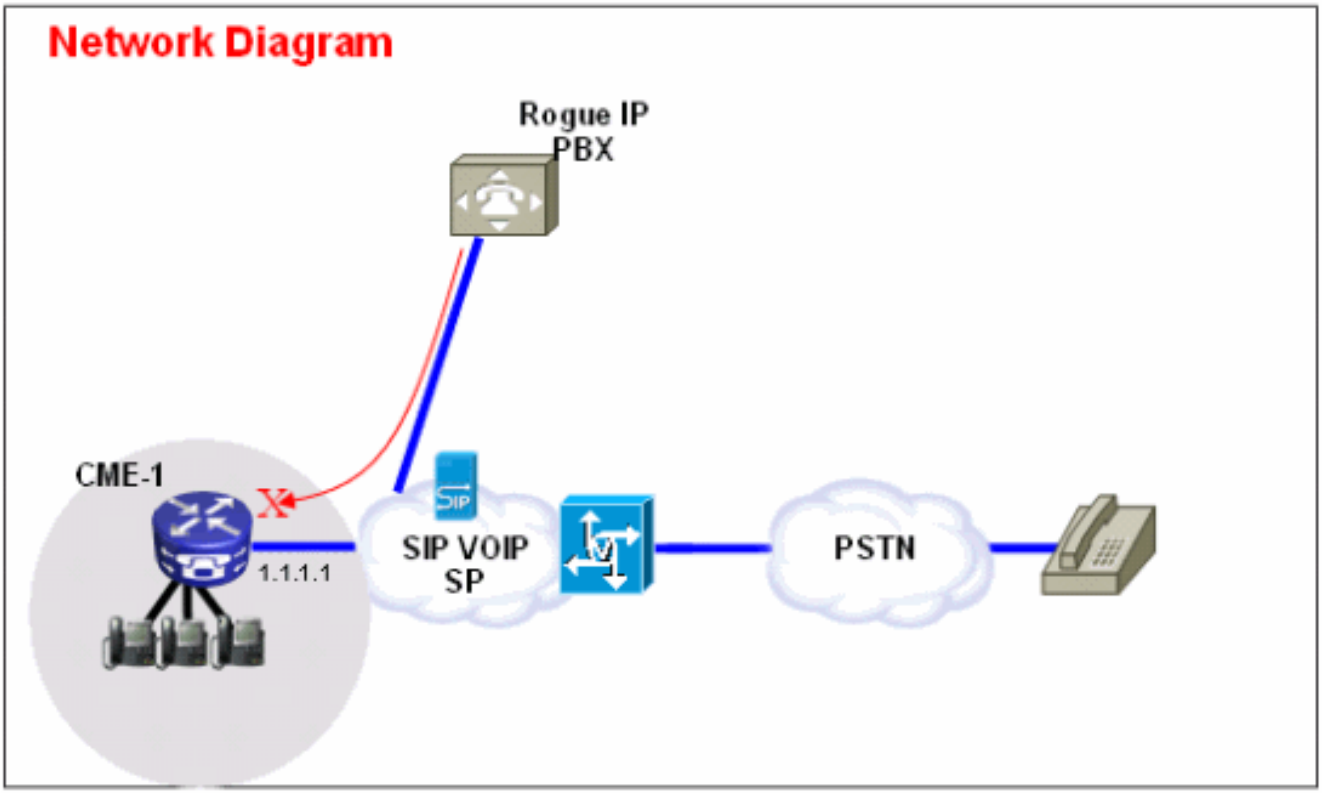
示例配置 — CME 1

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

範例 2

在本示例中，CME 1連線到SIP提供商以進行PSTN連線，其配置示例在Cisco CallManager Express(CME)SIP中繼配置示例中提供。

由於CME 1位於公共網際網路上，因此如果欺詐使用者掃描公有IP地址以獲取H.323(TCP 1720)或SIP（UDP或TCP 5060）信令，並傳送將呼叫從SIP中繼路由回到PSTN的SIP或H.323消息，則可能會發生收費欺詐。在此案例中，最常見的濫用行為是流氓使用者通過SIP或H.323中繼進行多個國際呼叫，並導致CME 1的所有者為這些收費欺詐呼叫付費，有時高達數千美元。



解決方案

為了緩解這種威脅，您可以使用多種解決方案。如果沒有透過CME 1的WAN連結使用任何VOIP訊號（SIP或H.323），必須儘可能使用CME 1上的防火牆技術（存取清單或ACL）加以封鎖。

1. 使用CME 1上的Cisco IOS®防火牆保護WAN介面：這意味著您只允許已知的SIP或H.323流量進入WAN介面。阻止所有其他SIP或H.323流量。這還需要您知道SIP VOIP SP在SIP中繼上用於信令的IP地址。此解決方案假定SP願意提供其網路中使用的所有IP地址或DNS名稱。此外，如果使用DNS名稱，配置要求可訪問可解析這些名稱的DNS伺服器。此外，如果SP在其一端更改了任何地址，則需要在CME 1上更新配置。請注意，除了WAN介面上已經存在的任何ACL條目之外，還需要新增這些行。示例配置 — 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. 確保SIP中繼上的呼叫不會髮夾回出：這意味著CME 1配置僅允許對特定已知PSTN號碼範圍進行呼叫的SIP - SIP髮夾功能，所有其他呼叫將被阻止。您必須為對映到CME 1上的分機或自動總機或語音郵件的SIP中繼上傳入的PSTN號碼配置特定的入站撥號對等體。阻止對非CME 1 PSTN號碼範圍的所有其他號碼呼叫。請注意，這不會影響呼叫轉接/轉接至語音郵件(Cisco Unity Express)，也不會影響從CME 1上的IP電話將所有呼叫轉接至PSTN號碼，因為初始呼叫仍指向CME 1上的分機。示例配置 — 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. 使用轉換規則以阻止特定撥號字串：大多數收費欺詐都涉及國際電話撥號。因此，您可以建立與特定撥號字串匹配的特定入站撥號對等體並阻止對它們的呼叫。大多數CME使用特定訪問代碼（如9）進行撥出，在美國的國際撥號代碼是011。因此，在美國要阻止的最常見的撥號字串是9011 + SIP中繼上該數字之後的任何數字。示例配置 — 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

轉移模式

摘要

預設情況下，自動阻止傳送到除本地SCCP IP電話以外的所有號碼。在配置期間，您可以允許傳輸到非本地號碼。**transfer-pattern**指令用於允許將電話通話從Cisco SCCP IP電話傳輸到Cisco IP電話以外的電話，例如外部PSTN通話或另一個CME系統上的電話。您可以使用**transfer-pattern**來僅限制對內部分機的呼叫，或僅限制對特定區號中PSTN號碼的呼叫。以下示例說明如何使用**transfer-pattern**命令將呼叫限製為不同的號碼。

注意：這是內**部威脅**。

範例 1

僅允許使用者將來電轉駁到408區號。在本示例中，假設為CME配置了目的地模式為9T的撥號對等體。

示例配置

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

Transfer-Pattern Blocked

摘要

在Cisco Unified CME 4.0及更高版本中，您可以阻止單個電話將來電轉駁至全域性允許轉移的號碼。**transfer-pattern blocked**命令會過載**transfer-pattern**命令，並禁止來電轉駁至POTS或VoIP撥號對等體需要到達的任何目的地。其中包括PSTN號碼、其他語音網關和Cisco Unity Express。這可確保當來電轉駁到Cisco Unified CME系統之外時，單個電話不會產生話費費用。可以為單個電話配置來電轉駁阻止，也可以將其配置為應用於一組電話的模板的一部分。

注意：這是內**部威脅**。

範例 1

在此示例配置中，不允許ephone 1使用transfer-pattern（全域性定義）轉接呼叫，而ephone 2可以使用telephony-service下定義的轉接模式轉接呼叫。

示例配置

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

傳輸最大長度

摘要

transfer max-length命令指定在轉接呼叫時，使用者可以撥打的最大位數。**transfer-pattern max-length**會過載**transfer-pattern**命令，強制執行傳輸目的地所允許的最大位數。引數指定呼叫被轉接到的號碼中允許的數字位數。範圍：3到16。預設值：16.

注意：這是內**部威脅**。

範例 1

此配置只允許應用了此ephone模板的電話傳輸到最多四位數的目標。

示例配置

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

來電轉駁最大長度

摘要

若要限制使用IP電話上的CfwdALL軟鍵可輸入的數字位數，請在ephone-dn或ephone-dn-template配置模式下使用**call-forward max-length**命令。若要取消對可輸入數字數的限制，請使用此命令的**no**形式。

注意：這是內**部威脅**。

範例 1

在此示例中，允許目錄分機101對長度為1到4位的任何分機執行呼叫前轉。任何超過四位數的目標呼叫轉發均會失敗。

示例配置

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

或

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

無轉接本地呼叫

摘要

在ephone-dn配置模式下使用**no forward local-calls**命令時，如果ephone-dn繁忙或未應答，則不會轉發對未應用任何前轉本地呼叫的特定ephone-dn的內部呼叫。如果內部呼叫者振鈴此ephone-dn，而ephone-dn正忙，則呼叫者會聽到忙訊號。如果內部呼叫者振鈴此ephone-dn但未響應，則呼叫者會聽到回鈴訊號。即使為ephone-dn啟用了呼叫前轉，也不會轉發內部呼叫。

注意：這是內**部威脅**。

範例 1

在此示例中，分機2222呼叫分機3675並聽到回鈴或忙訊號。如果外部呼叫者到達分機3675並且沒有應答，則該呼叫被轉接到分機4000。

示例配置

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

在CME系統上禁用自動註冊

摘要

在SCCP CME系統上的電話服務下啟用**auto-reg-ephone**後，插入系統的新IP電話將自動註冊，如果將**auto assign**配置為自動分配分機號碼，則新IP電話能夠立即進行呼叫。

注意：這是內**部威脅**。

範例 1

在此配置中，配置了一個新的CME系統，因此您必須手動新增一個ephone，以便該ephone註冊到CME系統並使用該系統進行IP電話呼叫。

解決方案

您可以禁用telephony-service下的**auto-reg-ephone**，以便連線到CME系統的新IP電話不會自動註冊到CME系統。

示例配置

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

範例 2

如果使用SCCP CME並計畫向系統註冊Cisco SIP電話，則必須配置系統，以便SIP終端必須使用使用者名稱和密碼進行身份驗證。為此，只需配置以下內容：

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

請參閱SIP:設定Cisco Unified CME以獲得SIP CME更全面的配置指南。

Cisco Unity Express限制工具

安全Cisco Unity Express:AA PSTN訪問

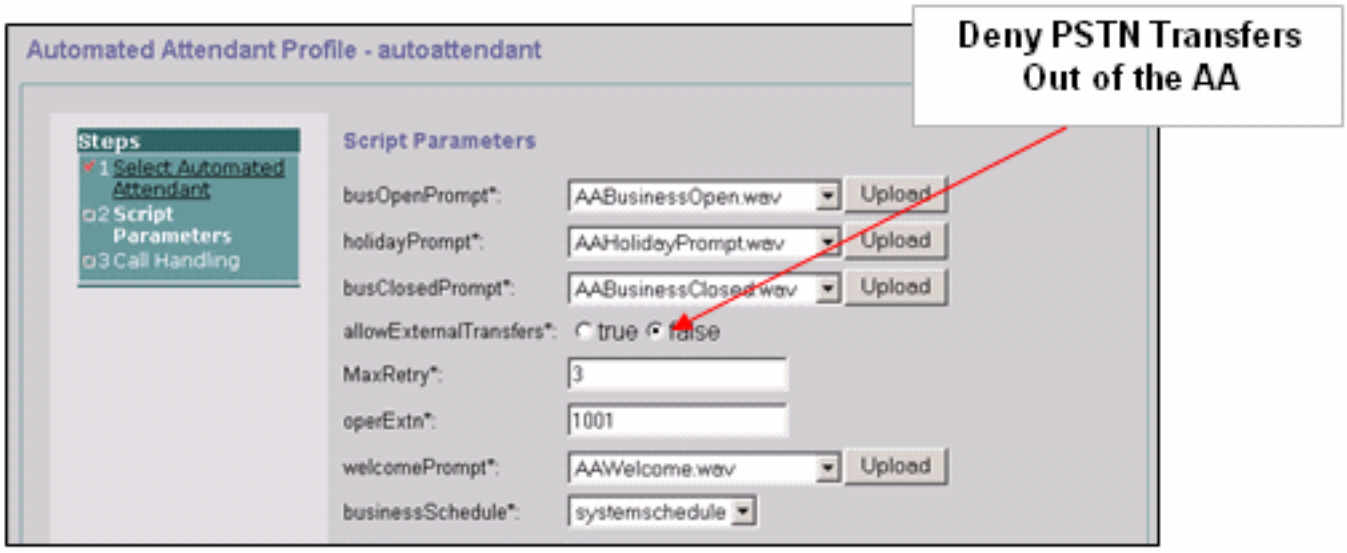
摘要

當您的系統配置為將入站呼叫轉發到Cisco Unity Express上的自動總機(AA)時，可能需要禁用從Cisco Unity Express AA到PSTN的外部傳輸。這不允許外部使用者在到達Cisco Unity Express AA後對外部號碼進行出站撥號。

注意：這是一個外**部威脅**。

附註： 解決方案

注意：在Cisco Unity Express GUI上禁用**allowExternalTransfers選項。**



注意：如果需要從AA進行PSTN訪問，請限制指令碼認為有效的數字或數字範圍。

Cisco Unity Express限製表

摘要

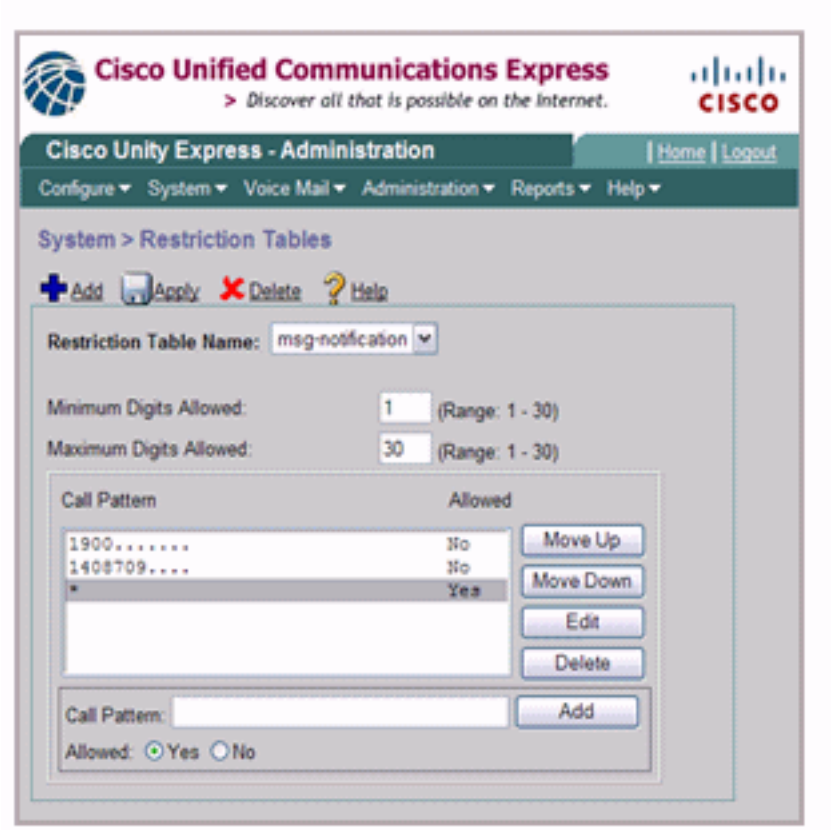
您可以使用Cisco Unity Express限製表來限制從Cisco Unity Express發出呼叫期間可到達的目標。Cisco Unity Express限製表可用於防止收費欺詐和惡意使用Cisco Unity Express系統進行出站呼叫。如果使用Cisco Unity Express限製表，則可以指定呼叫模式進行萬用字元匹配。使用Cisco Unity Express限製表的應用包括：

- 傳真
- Cisco Unity Express Live Replay
- 留言通知
- 非訂戶消息傳送

注意：這是內**部威脅**。

解決方案

為了限制Cisco Unity Express在出站外部呼叫中可到達的目標模式，請從Cisco Unity Express GUI在**System > Restrictions Tables**中配置**Call Pattern**。



通話記錄

增強型CDR

您可以配置CME系統以捕獲增強的CDR，並將CDR記錄到路由器快閃記憶體或外部FTP伺服器。然後，這些記錄可用於跟蹤呼叫，以檢視是否發生了內部或外部方的濫用。

Cisco IOS版本12.4(15)XY中的CME 4.3/7.0引入的檔案記帳功能提供了一種方法，可擷取逗號分隔值(.csv)格式的記帳記錄，並將記錄儲存到內部快閃記憶體中的檔案或外部FTP伺服器中。它擴展了網關記賬支援，還包括記錄記賬資訊的AAA和系統日誌機制。

記帳過程收集在思科語音網關上建立的每個呼叫段的記帳資料。您可以將此資訊用於後期處理活動，如生成帳單記錄並進行網路分析。思科語音網關以包含思科定義的屬性的呼叫詳細記錄(CDR)形式捕獲記帳資料。網關可以將CDR傳送到RADIUS伺服器、系統日誌伺服器，並使用新的檔案方法以.csv格式傳送到快閃記憶體或FTP伺服器。

有關增強型CDR功能的詳細資訊，請參閱CDR示例。

相關資訊

- Cisco Unified Communications Manager Express安全最佳實踐
- Cisco Communications Manager Express管理員指南
- Cisco Communications Manager Express管理員指南 — 呼叫阻塞
- 瞭解IOS平台上的撥號對等體匹配
- 使用語音轉換配置檔案進行號碼轉換
- CME解決方案參考網路設計手冊
- 技術支援與文件 - Cisco Systems