



Cisco Unified Communications Manager Express – Toll Fraud Prevention

Application Note

June 6, 2008
Cisco

Revision History

Revision	Date	Author	Comments
1.0	6/06/2008	Tony Huynh	Initial Draft
2.0	6/14/2008	Maulik Shah	Added SIP Trunking examples
3.0	6/30/2008	Maulik Shah	Minor Edits
4.0	7/18/2008	Tony Huynh	Added Class of Restriction (COR)

Table of Contents

1	Introduction.....	3
1.1	Objective	3
1.2	Scope.....	3
1.3	Audience	3
1.4	Disclaimer.....	3
2	Overview.....	4
2.1	Internal vs External Threats	4
3	Toll Restriction Tools	5
3.1	Direct-inward-dial.....	5
3.2	After-hours Toll Restriction.....	7
3.3	Class of Restriction	8
3.4	Access-list to restrict H.323/SIP Trunks	8
4	Feature Restriction Tools.....	12
4.1	Transfer-Pattern.....	12
4.2	Transfer-Pattern Blocked	13
4.3	Transfer max-length	13
4.4	Call-Forward Max-Length	14
4.5	No forward local-calls.....	14
4.6	Disable auto-registration on CME system	15
5.	CUE Restriction Tools.....	16
5.1	Secure CUE: AA PSTN access.....	16
5.2	CUE Restriction Tables	17
6	Call Logging	18
6.1	Enhanced CDR.....	18
7	References.....	19

1 Introduction

The following document provides a configuration guide that can be used to help secure a Cisco Communications Manager Express (CME) system and mitigate the threat of toll fraud. CME is Cisco's router-based call control solution that provides a smart, simple and secure solution for organizations looking to implement Unified Communications. We highly recommend that Value Added Resellers (VAR)s and Systems Engineers (SE)s implement the security measures described in this application note to provide additional levels of security control and reduce the possibility of toll fraud.

1.1 Objective

The objective of this application note is to educate SEs and VARs on the various security tools available on Cisco Voice Gateways and CME. These tools can and should be implemented on a CME system to help mitigate the threat of toll fraud by both internal and external parties.

1.2 Scope

This application note provides instructions on how to configure a CME system with various toll security and feature restriction tools. The application note also outlines why certain security tools are used in certain deployments.

1.3 Audience

This document is targeted at Cisco SEs and other personnel who assist in pre-sales design of SMB voice solutions.

1.4 Disclaimer

The overall inherent flexibility of Cisco's ISR platforms allows SEs and VARs to deploy CME in many different types of deployments. Thus it may be required to use a combination of the features described in this document to help lock down the CME. This application note serves as a guideline for applying security tools on CME and in no way guarantees that toll-fraud or abuse by both internal and external parties will not occur.

2 Overview

This document covers the most common security tools that can be used on a CME system to help mitigate the threat of toll fraud. The CME security tools referenced in this paper include toll restriction tools and feature restriction tools.

Toll Restriction Tools

- (1) Direct-inward-dial
- (2) After-hours toll restriction
- (3) Class of Restriction (COR)
- (4) Access-list to restrict H323/SIP trunk access

Feature Restriction Tools

- (1) Transfer-pattern
- (2) Transfer-pattern blocked
- (3) Transfer max-length
- (4) Call-forward max-length
- (5) No forward local-calls
- (6) No auto-reg-ephone

CUE Restriction Tools

- (1) Secure CUE PSTN Access
- (2) Message notification restriction

Call Logging

- (1) Call logging to capture call detail records (CDR)s

2.1 Internal vs External Threats

Throughout this document, we will discuss threats from both internal and external parties. Internal parties include IP phone users that reside on a CME system. External parties include users on foreign systems that may try to use the host CME to make fraudulent calls and have the calls charged back to the customer's CME.

3 Toll Restriction Tools

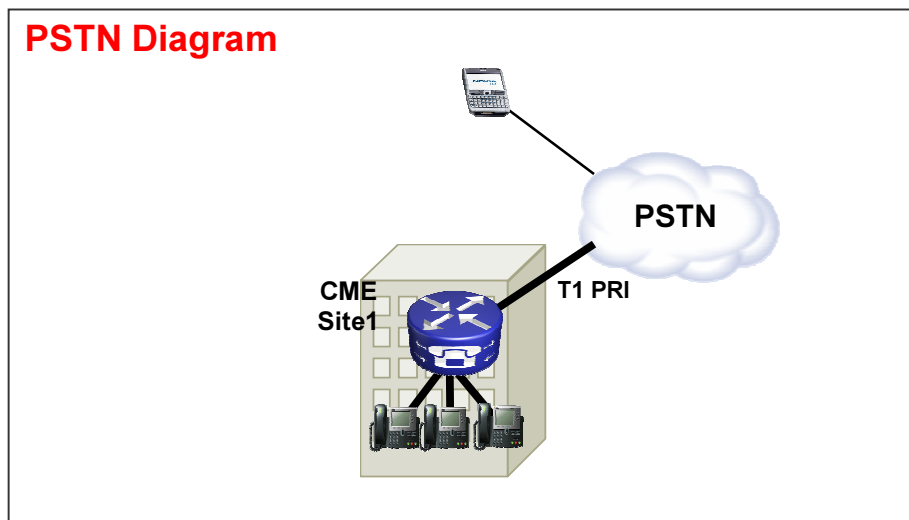
3.1 Direct-inward-dial

3.1.1 Abstract

Direct-inward-dial (DID) is used on Cisco voice gateways to allow the gateway to process an inbound call after it receives digits from the PBX or CO switch. When DID is enabled, the Cisco gateway does not present a secondary dial tone to the caller and does not wait to collect additional digits from the caller. It forwards the call directly to the destination that matches the inbound Dialed Number Identification Service (DNIS) – this is called one-stage dialing. **[External Threat]**

3.1.2 Problem Statement

If direct-inward-dial is **NOT** configured on a Cisco Gateway or CME, whenever a call comes in from the CO or PBX to the Cisco Gateway, the caller will hear secondary dial-tone – this is called two-stage dialing. Once the PSTN caller hears secondary dial-tone, they are able to enter digits to reach any internal extension or if they know the PSTN access code, they can dial long-distance or international numbers. This presents a problem because the PSTN caller can use the CME system to place outbound long-distance or international calls (and the company gets charged for the calls).



3.1.3 Example-1

At site-1, the CME is connected to the PSTN via a T1 PRI trunk. The PSTN provider provides the following DID range for CME site-1: “40855512..”. Thus all PSTN calls destined for 4085551200 – 4085551299 will be routed inbound to the CME. If the CME administrator does **not** configure “**direct-inward-dial**” on the system, an inbound PSTN caller will hear secondary dial-tone and will have to manually dial the internal extension. The bigger problem is that if the caller is an abuser and knows the PSTN access code on

the system, commonly “9”, they can dial “9” followed by any destination-number they wish to reach.

Solution:

To mitigate this threat, the CME administrator should configure “**direct-inward-dial**”. This causes the Cisco gateway to forward the inbound call directly to the destination that matches the inbound DNIS.

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

For DID to work correctly, make sure the incoming call matches the correct POTS dial-peer where the command **direct-inward-dial** is configured – in the above example, the T1 PRI is connected to port 1/0:23. To match the correct inbound dial peer, we recommend using the dial peer command “**incoming called-number .**” under the DID POTS dial peer.

3.1.4 Example-2

At site-1, the CME is connected to the PSTN via a T1 PRI trunk. The PSTN provider provides the following DID ranges for CME site-1: “**40855512..**” and “**40855513..**”. Thus alls PSTN calls destined for 4085551200 – 4085551299 and 4085551300 - 4085551399 will be routed inbound to the CME.

Incorrect configuration:

If the CME administrator configures the following inbound dial-peer, the possibility for toll fraud will still occur. The problem with the following inbound dial-peer is that it will only match incoming calls to “**40852512..**” and then apply the DID service. If a PSTN call comes into 40852513.., the inbound pots dial-peer will not match and thus the DID service will not get applied. If an inbound dial-peer with DID is not matched, then default dial-peer 0 will be used. DID is disabled by default on dial-peer 0.

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

Correct configuration:

The correct way to configure DID service on an inbound dial-peer is the following sample config.

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

For more information on DID for digital T1/E1 voice ports, refer to the following link:

http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00801142f8.shtml#did_cfg

NOTE:

The use of DID is **NOT** needed when Private-Line Automatic Ringdown (PLAR) is used on a voice-port or a service script like Auto-Attendant (AA) is used on the inbound dial-peer.

```
Sample config - PLAR:  
voice-port 1/0  
connection-plar 1001
```

```
Sample config – Service script:  
dial-peer voice 1 pots  
service AA  
port 1/0:23
```

3.2 *After-hours Toll Restriction*

3.2.1 *Abstract*

After-hours Toll Restriction is a new security tool available in CME 4.3/7.0 to allow an administrator to configure toll restriction policies based on time and date. The administrator can configure policies so that users are blocked from making calls to predefined numbers during certain hours of the day or all the time. If the 7x24 after-hours call blocking policy is configured, it will also restrict the set of numbers can be entered by an inside user to set “call-forward all”. **[Internal Threat]**

3.2.2 Example 1

The following example defines several patterns of digits for which outgoing calls are blocked. Patterns 1 and 2, which block calls to external numbers that begin with "1" and "011," are blocked on Monday through Friday before 7 a.m. and after 7 p.m., on Saturday before 7 a.m. and after 1 p.m., and all day Sunday. Pattern 3 blocks calls to 900 numbers 7 days a week, 24 hours a day.

```
Sample config:
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 12:00
after-hours day sun 12:00 07:00
```

More information on toll restriction can be found at the following link:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeblock.html#wp1022333

3.3 Class of Restriction

3.3.1 Abstract

If a system administrator wants granular control with respect to configuring toll restriction, the system administrator should use Class of Restriction (COR). For more information, please review the following configuration guide.

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeblock.html#wp1014495

3.4 Access-list to restrict H.323/SIP Trunks

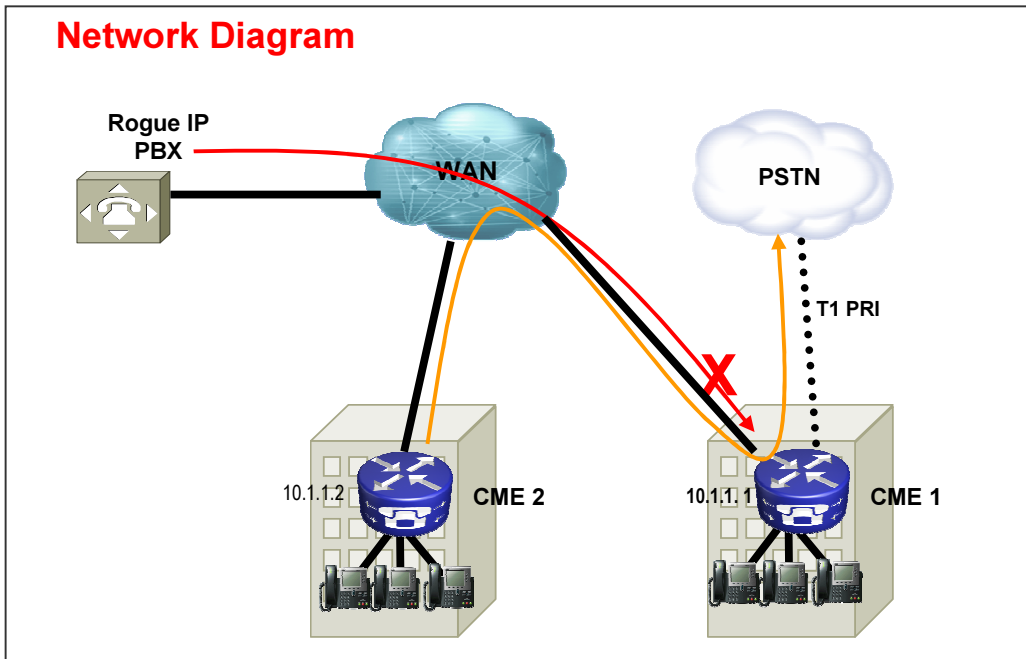
3.4.1 Abstract

In cases where a CME system is connected over a WAN to other CME devices via a SIP or H.323 trunk, the administrator may want to restrict SIP/H.323 trunk access to their CME to prevent abusers from using their system to illegally relay calls to the PSTN.

[External Threat]

3.4.2 Example 1

In the following example, the CME-1 has PSTN connectivity. CME-2 is connected over the WAN to CME-1 via a H.323 trunk. In order to secure the CME-1, the administrator can configure an access-list and apply it inbound on the WAN interface and thus only allow IP traffic from CME-2. This prevents the Rogue IP PBX from sending VOIP calls through CME-1 to the PSTN.



Solution:

Secure the WAN interface on CME-1 from accepting traffic from rogue devices that it does not know about. Please note that there is an implicit DENY all at the end of an access-list. If there are more devices that you wish to allow to inbound IP traffic from, please be sure to add the device's IP address to the access-list.

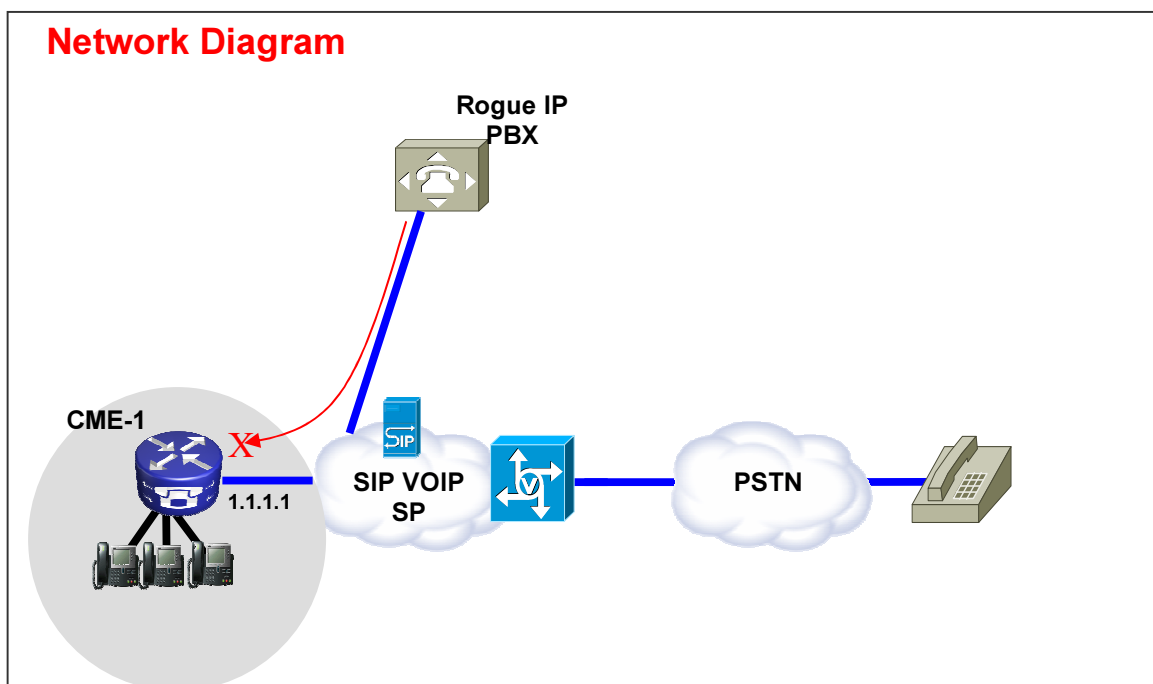
```
Sample config – CME-1:  
interface serial 0/0  
 ip access-group 100 in  
!  
access-list 100 permit ip 10.1.1.2 255.255.255.255 any
```

3.4.3 Example 2

In the following example, the CME-1 is connected to the SIP provider for PSTN connectivity using the sample configuration provided at the note below:

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_configuration_exam ple09186a00808f9666.shtml

Since CME-1 is on the public internet, it is possible that “toll fraud” could occur if a rogue user scans public IP addresses for well known ports for H.323 (TCP 1720) or SIP (UDP or TCP 5060) signaling and sends SIP or H.323 messages which route calls back out the SIP trunk to the PSTN. Most common abuses in this case are the rogue user makes multiple international calls via the SIP or H.323 trunk causing the customer owning CME-1 to pay for these toll fraud calls - in some cases thousands of dollars.



Solution:

To mitigate this threat, the administrator for CME-1 can use multiple solutions. If any VOIP signaling (SIP or H.323) is not being used over the WAN link(s) into CME-1, this should be blocked using the firewall techniques on CME-1 (Access-lists or ACLs) as far as possible.

a. Securing the WAN interface using the IOS firewall on CME-1:

This implies allowing only known SIP or H.323 traffic to come in on the WAN interface – all other SIP or H.323 traffic will be blocked. This also requires that the CME-1 administrator knows the IP addresses that the SIP VOIP SP uses for signaling on the SIP Trunk. This solution assumes that the SP is willing to provide all the IP addresses or DNS names they use in their network. Also, if DNS names are used, the configuration would require that a DNS server that can resolve these names is reachable. Also, if the SP changes any addresses on their end, the configuration

would need to be updated on CME-1. Note that the below lines would need to be added in addition to any ACL entries already present on the WAN interface.

```
Sample config – 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
```

b. Ensuring calls coming in on the SIP trunk do hairpin back out:

This implies that the CME-1 configuration will only allow SIP – SIP hairpin of calls to a specific known PSTN number range, all other calls will be blocked. The CME-1 administrator should configure specific inbound dial-peers for the PSTN numbers coming in on the SIP trunk that are mapped to extensions or auto attendant(s) or voicemail on CME-1. All other calls to numbers that are not part of the CME-1 PSTN number range will be blocked. Note, this will not affect call forwards / transfers to voicemail (CUE) and call forward all to PSTN numbers from IP phones on CME-1 as the initial call is still targeted towards an extension on CME-1.

```
Sample config – 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
```

c. Using translation rules to block specific dial strings:

Most toll frauds involve international call dialing – hence the CME-1 administrator can create a specific inbound dial-peer which matches specific dialed strings and blocks calls to them. Most CMEs use a specific access code (such as 9) to dial out and the international dialing code in the US is 011 – hence the most common dial string to block in the US would be 9011 + any digits after that coming in on the SIP trunk.

```
Sample config – 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
```

4 Feature Restriction Tools

4.1 Transfer-Pattern

4.1.1 Abstract

Transfers to all numbers except those on local SCCP IP phones are automatically blocked by default. During configuration, you can allow transfers to non local numbers. The transfer-pattern command is used to allow the transfer of telephony calls from Cisco SCCP IP phones to phones other than Cisco IP Phones (external PSTN calls or phones on another CME system). You can use the “transfer-pattern” to limit the calls to internal extensions only or perhaps limit calls to PSTN numbers in a certain area code only. The following examples show how transfer-pattern can be used to limit calls to different numbers. **[Internal Threat]**

4.1.2 Example 1

Allow users to transfer calls out to only the 408 area code. In this example, the assumption is that the CME is configured with a dial-peer that has destination-pattern of 9T.

```
Sample config:
telephony-service
transfer-pattern 91408
```

4.2 Transfer-Pattern Blocked

4.2.1 Abstract

In Cisco Unified CME 4.0 and later versions, you can prevent individual phones from transferring calls to numbers that are globally enabled for transfer. The “transfer-pattern blocked” command over-rides transfer-pattern and disables call transfer to any destination that needs to be reached by a POTS or VoIP dial-peer. This includes PSTN numbers, other voice gateways and Cisco Unity Express (CUE). This ensures that individual phones do not incur toll charges by transferring calls outside the Cisco Unified CME system. Call transfer blocking can be configured for individual phones or configured as part of a template that is applied to a set of phones. **[Internal Threat]**

4.2.2 Example 1

In the following sample configuration, ephone 1 is not allowed to use transfer-pattern (defined globally) to transfer calls, while ephone 2 can use the transfer-pattern defined under telephony-service to transfer calls.

```
Sample config:
ephone-template 1
transfer-pattern blocked
!
ephone 1
ephone-template 1
!
ephone 2
!
```

4.3 Transfer max-length

4.3.1 Abstract

The transfer max-length command specifies the maximum number of digits the user can dial when transferring a call. Transfer-pattern max-length over-rides transfer-pattern and enforces maximum digits allowed for transfer destination. The argument specifies the

number of digits allowed in a number to which a call is being transferred. Range: 3 to 16. Default: 16. **[Internal Threat]**

4.3.2 Example 1

The following configuration only allows phones that have this ephone-template applied to transfer to destinations that are a maximum of 4 digits long.

```
Sample config:  
ephone-template 1  
transfer max-length 4
```

4.4 Call-Forward Max-Length

4.4.1 Abstract

To restrict the number of digits that can be entered using the CfdwALL soft key on an IP phone, use the **call-forward max-length** command in ephone-dn or ephone-dn-template configuration mode. To remove a restriction on the number of digits that can be entered, use the **no** form of this command. **[Internal Threat]**

4.4.2 Example 1

In the following example, directory extension 101 is allowed to perform a call-forward to any extension that is 1-4 digits in length. Any call-forwards to destinations longer than 4 digits long will fail.

```
Sample config:  
ephone-dn 1 dual-line  
number 101  
call-forward max-length 4  
  
or  
  
ephone-dn-template 1  
call-forward max-length 4
```

4.5 No forward local-calls

4.5.1 Abstract

When the “**no forward local-calls**” command is used in ephone-dn configuration mode, internal calls to a particular ephone-dn (with “no forward local-calls” applied) are not forwarded if the ephone-dn is busy or does not answer. If an internal caller rings this ephone-dn and the ephone-dn is busy, the caller hears a busy signal. If an internal caller rings this ephone-dn and it does not answer, the caller hears a ringback signal. The

internal call is not forwarded even if call forwarding is enabled for the ephone-dn.

[Internal Threat]

4.5.2 Example 1

In the following example, extension 2222 calls extension 3675 and hears ringback or a busy signal. If an external caller reaches extension 3675 and there is no answer, the call is forwarded to extension 4000.

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

4.6 Disable auto-registration on CME system

4.6.1 Abstract

When “auto-reg-ephone” is enabled underneath telephony-service on a SCCP CME system, new IP phones that are plugged into the system are auto registered and if “auto assign” is configured to automatically assign extension numbers, then a new IP phone will be able to make calls immediately. **[Internal Threat]**

4.6.2 Example 1

In this configuration, a new CME system is configured so that an administrator has to manually add an ephone in order for the ephone to register to the CME system and use it to make IP telephony calls.

Solution:

Disable “auto-reg-ephone” underneath telephony-service so that new IP phones connected to a CME system will not auto register to the CME system.

```
Sample config:  
telephony-service  
no auto-reg-ephone
```

4.6.3 Example 2

If the customer is using SCCP CME and planning to register Cisco SIP phones to the system, the administrator should configure the system so that the SIP endpoints have to authenticate using a username and password. To do so, simply configure the following:

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

For a more comprehensive configuration guide for SIP CME, please refer to the following:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cm esystem.html#wp1025405

5. CUE Restriction Tools

5.1 Secure CUE: AA PSTN access

5.1.1 Abstract

When a customer's system is configured so that inbound calls are forwarded to auto-attendant (AA) on CUE, it may be necessary to disable external transfer to the PSTN from CUE AA. This prevents external users from dialing outbound to external numbers after they reach CUE AA. **[External Threat]**

Solution:

Disable the “**allowExternalTransfers**” option on the CUE GUI.

Automated Attendant Profile - autoattendant

Steps

- 1 Select Automated Attendant
- 2 Script Parameters
- 3 Call Handling

Script Parameters

busOpenPrompt*: AABusinessOpen.wav Upload

holidayPrompt*: AAHolidayPrompt.wav Upload

busClosedPrompt*: AABusinessClosed.wav Upload

allowExternalTransfers*: true false

MaxRetry*: 3

operExtn*: 1001

welcomePrompt*: AAWelcome.wav Upload

businessSchedule*: systemschedule

Deny PSTN Transfers Out of the AA

- If PSTN access from the AA is required, limit the numbers (or range of numbers) that are considered valid by the script

5.2 CUE Restriction Tables

5.2.1 Abstract

A system administrator can use the CUE restriction tables to restrict the destinations that can be reached during an outcall from CUE. The CUE restriction table can be used to prevent toll fraud and malicious use of the CUE system to make outbound calls. Using the CUE restriction table, the administrator can specify call patterns to wild card match. Applications that use the CUE restriction table include: **[Internal Threat]**

1. Fax
2. CUE Live Reply
3. Message Notification
4. Non-Subscriber Message Delivery

Solution:

In order to restrict the destination patterns that can be reached by CUE on an outbound external call, configure the “**Call Pattern**” in the **System > Restrictions Tables** from CUE GUI.

The screenshot shows the Cisco Unity Express Administration interface. The main heading is "System > Restriction Tables". Below this, there are buttons for "Add", "Apply", "Delete", and "Help". The "Restriction Table Name" is set to "msg-notification". The "Minimum Digits Allowed" is 1 and the "Maximum Digits Allowed" is 30. The "Call Pattern" table is as follows:

Call Pattern	Allowed
1900.....	No
1408709....	No
*	Yes

Buttons for "Move Up", "Move Down", "Edit", and "Delete" are visible next to the table rows. At the bottom, there is a "Call Pattern:" input field and an "Add" button. The "Allowed:" section has radio buttons for "Yes" (selected) and "No".

6 Call Logging

6.1 *Enhanced CDR*

An administrator may want to configure the CME system to capture enhanced CDR and log the CDR to the router flash or an external FTP server. These records can then be used to retrace calls to see if abuse by internal or external parties has occurred.

The file accounting feature introduced with CME 4.3/7.0 using Cisco IOS Release 12.4(15)XY provides a method for capturing accounting records in comma separated value (.csv) format and storing the records to a file in internal flash or to an external FTP server. It expands gateway accounting support which also includes the AAA and syslog mechanisms of logging accounting information.

The accounting process collects accounting data for each call leg created on a Cisco voice gateway. You can use this information for post processing activities such as generating billing records and network analysis. Cisco voice gateways capture accounting data in the form of call detail records (CDRs) containing attributes defined by Cisco. The gateway can send CDRs to a RADIUS server, syslog server, and with the new file method, to flash or an FTP server in .csv format.

For more information on the Enhanced CDR capabilities, please refer to the following link:
<http://www.cisco.com/en/US/docs/ios/voice/vsa/feature/guide/itfileac.html>

7 References

1. Cisco Unified Communications Manager Express Security Best Practices
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/security.html
2. Cisco Communications Manager Express Administrators Guide
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/security.html
3. Cisco Communications Manager Express Administrators Guide – Call Blocking
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeblock.html#wp1014495
4. Understanding Dial-Peer Matching on IOS platforms
http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a008010fed1.shtml#topic1
5. Number Translation using Voice Translation Profiles
http://www.cisco.com/en/US/tech/tk652/tk90/technologies_configuration_example09186a00803f818a.shtml#con11
6. CME Solution Reference Network Design Guide
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucme/srnd/design/guide/security.html