Configuring Toll Fraud Prevention

First Published: March 15, 2013

This module describes the Toll Fraud Prevention feature in Cisco Unified Communications Manager Express (Cisco Unified CME).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for Toll Fraud Prevention" section on page 517.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Prerequisites for Configuring Toll Fraud Prevention

- Cisco Unified CME 8.1 or a later version.
- Cisco IOS Release 15.1(2)T.

Information About Toll Fraud Prevention

Cisco Unified CME 8.1 enhances the Toll Fraud Prevention feature to secure the Cisco Unified CME system against potential toll fraud exploitation by unauthorized users. The following are the enhancements to Toll Fraud Prevention in Cisco Unified CME:

- IP Address Trusted Authentication
- Direct Inward Dial for Incoming ISDN Calls
- Disconnecting ISDN Calls With no Matching Dial-peer
- Blocking Two-stage Dialing Service on Analog and Digital FXO Ports

IP Address Trusted Authentication

IP address trusted authentication process blocks unauthorized calls and helps secure the Cisco Unified CME system against potential toll fraud exploitation by unauthorized users. In Cisco Unified CME, **IP address trusted authentication** is enabled by default. When IP address trusted authenticate is enabled, Cisco Unified CME accepts incoming VoIP (SIP/H.323) calls only if the remote IP address of an incoming VoIP call is successfully validated from the system **IP address trusted list**. If the IP address trusted authentication fails, an incoming VoIP call is then disconnected by the application with a user- defined cause code and a new application internal error code 31 message (TOLL_FRAUD_CALL_BLOCK) is logged. For more information, see the, "Configuring IP Address Trusted Authentication for Incoming VoIP Calls" section on page 506.

Cisco Unified CME maintains an **IP address trusted list** to validate the remote IP addresses of incoming VOIP calls. Cisco Unified CME saves an IPv4 session target of VoIP dial-peer to add the trusted IP addresses to **IP address trusted list** automatically.The IPv4 session target is identified as a trusted IP address only if the status of VoIP dial-peer in operation is "UP". Up to 10050 IPv4 addresses can be defined in the trusted IP address list. No duplicate IP addresses are allowed in the trusted IP address list. You can manually add up to 100 trusted IP addresses for incoming VOIP calls. For more information on manually adding trusted IP addresses, see the, "Adding Valid IP Addresses For Incoming VoIP Calls" section on page 508.

A call detail record (CDR) history record is generated when the call is blocked as a result of IP address trusted authentication failure. A new voice Internal Error Code (IEC) is saved to the CDR history record. The voice IEC error messages are logged to syslog if "voice iec syslog" option is enabled. The following is an IEC toll fraud call rejected syslog display:

```
*Aug 14 19:54:32.507: %VOICE_IEC-3-GW: Application Framework Core: Internal Error (Toll
fraud call rejected): IEC=1.1.228.3.31.0 on callID 3 GUID=AE5066C5883E11DE8026A96657501A09
```

The **IP address trusted list** authentication must be suspended when Cisco Unified CME is defined with "gateway" and a VoIP dial-peer with "session-target ras" is in operational UP status. The incoming VOIP call routing is then controlled by the gatekeeper. Table 2-1 shows administration state and operational state in different trigger conditions.

Table 2-1 Administration and Operation States of IP Address Trusted Authentication

Trigger Condition	Administration State	Operation State
When **ip address trusted authenticate** is enabled.	Down	Down
When "gateway" is defined and a VoIP dial-peer with "ras" as a session target is in "UP" operational state	Up	Down
When **ip address trusted authenticate** is enabled and either "gateway" is not defined or no voip dial-peer with "ras" as session target is in "UP" operational state	Up	Up

Note We recommend enabling SIP authentication before enabling Out-of-dialog REFER (OOD-R) to avoid any potential toll fraud threats.

Direct Inward Dial for Incoming ISDN Calls

In Cisco Unified CME 8.1 and later versions the **direct-inward-dial isdn** feature in enabled to prevent the toll fraud for incoming ISDN calls. The called number of an incoming ISDN enbloc dialing call is used to match the outbound dial-peers even if the **direct-inward-dial** option is disabled from a selected inbound plain old telephone service (POTS) dial-peer. If no outbound dial-peer is selected for the outgoing call set up, the incoming ISDN call is disconnected with cause-code "unassigned-number (1)". For more information on direct-inward dial for incoming ISDN calls, see the, "Configuring Direct Inward Dial for Incoming ISDN Calls" section on page 510.

Disconnecting ISDN Calls With no Matching Dial-peer

Cisco Unified CME 8.1 and later versions disconnect unauthorized ISDN calls when no matching inbound voice dial-peer is selected. Cisco Unified CME and voice gateways use the **dial-peer no-match disconnect-cause** command to disconnect an incoming ISDN call when no inbound dial-peer is selected to avoid default POTS dial-peer behavior including two-stage dialing service to handle the incoming ISDN call.

Blocking Two-stage Dialing Service on Analog and Digital FXO Ports

Cisco Unified CME 8.1 and later versions block the two-stage dialing service which is initiated when an Analog or Digital FXO port goes offhook and the private line automatic ringdown (PLAR) connection is not setup from the voice-port. As a result, no outbound dial-peer is selected for an incoming analog or digital FXO call and no dialed digits are collected from an FXO call. Cisco Unified CME and voice gateways disconnect the FXO call with cause-code "unassigned-number (1)". Cisco Unified CME uses the **no secondary dialtone** command by default from FXO voice-port to block the two-stage dialing service on Analog or digital FXO ports. For more information on blocking two-stage dialing service on Analog and Digital FXO port, see Blocking Secondary Dialtone on Analog and Digital FXO Ports, page 512.

How to Configure Toll Fraud Prevention

This section contains the following tasks.

Configuring IP Address Trusted Authentication for Incoming VoIP Calls

Prerequisites

- Cisco Unified CME 8.1 or a later version.

Restrictions

- IP address trusted authentication is skipped if an incoming SIP call is originated from a SIP phone.
- IP address trusted authentication is skipped if an incoming call is an IPv6 call.
- For an incoming VoIP call, IP trusted authentication must be invoked when the IP address trusted authentication is in “UP” operational state.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. ip address trusted authenticate
5. ip-address trusted call-block cause <*code*>
6. end
7. show ip address trusted list

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service voip configuration mode.

Step 4	`ip address trusted authenticate`
	
	Example:
	`Router(conf-voi-serv)# ip address trusted authenticate`
		Enables IP address authentication on incoming H.323 or SIP trunk calls for toll fraud prevention support.
		IP address trusted list authenticate is enabled by default. Use the "**no ip address trusted list authenticate**" command to disable the IP address trusted list authentication.

Step 5	`ip-address trusted call-block cause` *code* **Example:** `Router(conf-voi-serv)#ip address trusted call-block cause` **call-reject**	Issues a cause-code when the incoming call is rejected to the IP address trusted authentication. **Note** If the IP address trusted authentication fails, a call-reject (21) cause-code is issued to disconnect the incoming VoIP call.
Step 6	**end** **Example:** `Router()# end`	Returns to privileged EXEC mode.

Step 7	**show ip address trusted list**
	
	Example:
	`Router# #show ip address trusted list`
	`IP Address Trusted Authentication`
	`Administration State: UP`
	`Operation State: UP`
	
	`IP Address Trusted Call Block Cause:`
	`call-reject (21)`
		Verifies a list of valid IP addresses for incoming H.323 or SIP trunk calls, Call Block cause for rejected incoming calls.

Examples

Router **#show ip address trusted list**

```
IP Address Trusted Authentication
```

```
 Administration State: UP
 Operation State:      UP

IP Address Trusted Call Block Cause: call-reject (21)

VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1

IP Address Trusted List:
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 172.19.245.0 255.255.255.0''
```

Adding Valid IP Addresses For Incoming VoIP Calls

Prerequisites

- Cisco Unified CME 8.1 or a later version.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. ip address trusted list
5. ipv4 *ipv4 address network mask*
6. end
7. show ip address trusted list

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service voip configuration mode.

Step 4	`ip address trusted list`
	
	Example:
	`Router(conf-voi-serv)# ip address trusted list`
	`Router(cfg-iptrust-list)#`
		Enters ip address trusted list mode and allows to manually add additional valid IP addresses.

Step 5	**ipv4 {<***ipv4 address***> [<***network mask***>]}**
	
	Example:
	`Router(config)#voice service voip`
	`Router(conf-voi-serv)#ip taddress trusted list`
	`Router(cfg-iptrust-list)#ipv4 172.19.245.1`
	`Router(cfg-iptrust-list)#ipv4 172.19.243.1`
		Allows you to add up to 100 IPv4 addresses in **ip address trusted list**. Duplicate IP addresses are not allowed in the ip address trusted list.
		• (Optional) *network mask*— allows to define a subnet IP address.

Step 6	**end** **Example:** `Router(config-register-pool)# end`	Returns to privileged EXEC mode.
Step 7	**show ip address trusted list** **Example:** `Router# show shared-line`	Displays a list of valid IP addresses for incoming H.323 or SIP trunk calls.

Examples

The following example shows 4 IP addresses configured as trusted IP addresses:

```
Router#show ip address trusted list
IP Address Trusted Authentication
 Administration State: UP
 Operation State:      UP

IP Address Trusted Call Block Cause: call-reject (21)

VoIP Dial-peer IPv4 Session Targets:
Peer Tag        Oper State      Session Target
--------        ----------      --------------
```

```
11              DOWN            ipv4:1.3.45.1
1               UP              ipv4:1.3.45.1

IP Address Trusted List:
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
```

Configuring Direct Inward Dial for Incoming ISDN Calls

To configure Direct Inward Dial for incoming ISDN calls, perform the following steps:

Restrictions

- Direct-inward-dial isdn is not supported for incoming ISDN overlap dialing call.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. *voice service pots*
4. *direct-inward-dial isdn*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	**voice service pots**
	
	Example:
	`Router(config)# voice service pots`
	`Router(conf-voi-serv)#`
		Enters voice service configuration mode with voice telephone-service encapsulation type (pots).

Step 4	***direct-inward-dial*** *isdn* **Example:** `Router(conf-voi-serv)#direct-inward-dial` **isdn**	Enables direct-inward-dial (DID) for incoming ISDN number. The incoming ISDN (enbloc dialing) call is treated as if the digits were received from the DID trunk. The called number is used to select the outgoing dial peer. No dial tone is presented to the caller.
Step 5	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits voice service pots configuration mode.

Examples

```
!
voice service voip
 ip address trusted list
 ipv4 172.19.245.1
 ipv4 172.19.247.1
 ipv4 172.19.243.1
 ipv4 171.19.245.1
 ipv4 171.19.10.1
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 allow-connections sip to sip
 supplementary-service media-renegotiate
 sip
 registrar server expires max 120 min 120
!
!
dial-peer voice 1 voip
 destination-pattern 5511...
 session protocol sipv2
 session target ipv4:1.3.45.1
 incoming called-number 5522...
 direct-inward-dial
 dtmf-relay sip-notify
 codec g711ulaw
!
```

```
dial-peer voice 100 pots
 destination-pattern 91...
 incoming called-number 2...
 forward-digits 4
!
```

Blocking Secondary Dialtone on Analog and Digital FXO Ports

To block secondary dialtone on Analog and Digital FXO port, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. *voice-port*
4. *no secondary dialtone*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice-port** **Example:** `Router(config)#voice-p 2/0/0`	Enters voice-port configuration mode. • Type your Analog or Digital FXO port number.
Step 4	*no secondary dialtone* **Example:** `Router((config-voiceport)# no secondary dialtone`	Blocks the secondary dialtone on Analong and Digital FXO port.
Step 5	**end** **Example:** `Router(conf-voiceport)# exit`	Returns to privileged EXEC mode.
Step 6	**show run** **Example:** `Router# show run | sec voice-port 2/0/0`	Verifies that the secondary dialtone is disabled on the specific voice-port.

Examples

```
Router# conf t
Router(config)#voice-p 2/0/0
Router(config-voiceport)# no secondary dialtone
!
end
```

```
Router# show run | sec voice-port 2/0/0
Foreign Exchange Office 2/0/0 Slot is 2, Sub-unit is 0, Port is 0
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 ...
 Secondary dialtone is disabled
```

Troubleshooting Tips for Toll Fraud Prevention

When incoming VOIP call is rejected by IP address trusted authentication, a specific internal error code (IEC) **1.1.228.3.31.0** is saved to the call history record. You can monitor the failed or rejected calls using the IEC support. Follow these steps to monitor any rejected calls:

Step 1 Use the **show voice iec description** command to find the text description of an IEC code.

```
Router# show voice iec description 1.1.228.3.31.0
    IEC Version: 1
    Entity: 1 (Gateway)
    Category: 228 (User is denied access to this service)
    Subsystem: 3 (Application Framework Core)
    Error: 31 (Toll fraud call rejected)
    Diagnostic Code: 0
```

Step 2 View the IEC statistics information using the **Enable iec statistics** command. The example below shows that 2 calls were rejected due to toll fraud call reject error code.

Example:

```
Router# Enable iec statistics
Router(config)#voice statistics type iec
Router#show voice statistics iec since-reboot
Internal Error Code counters
----------------------------
Counters since reboot:
  SUBSYSTEM Application Framework Core [subsystem code 3]
      [errcode  31] Toll fraud call rejected                  2
```

Step 3 Use the **enable IEC syslog** command to verify the syslog message logged when a call with IEC error is released.

Example:

```
Router# Enable iec syslog
Router (config)#voice iec syslog

Feb 11 01:42:57.371: %VOICE_IEC-3-GW: Application Framework Core:
Internal Error (Toll fraud call rejected): IEC=1.1.228.3.31.0 on
callID 288 GUID=DB3F10AC619711DCA7618593A790099E
```

Step 4 Verify the source address of an incoming VOIP call using the **show call history voice last** command.

Example:

```
Router# show call history voice last 1

GENERIC:
SetupTime=3306550 ms
Index=6
...
InternalErrorCode=1.1.228.3.31.0
...
RemoteMediaIPAddress=1.5.14.13
...
```

Step 5 IEC is saved to VSA of Radius Accounting Stop records. Monitor the rejected calls using the external RADIUS server.

Example:

```
Feb 11 01:44:06.527: RADIUS:   Cisco AVpair       [1]   36
"internal-error-code=1.1.228.3.31.0"
```

Step 6 Retrieve the IEC details from cCallHistoryIec MIB object. More information on IEC is available at: ttp://www.cisco.com/en/US/docs/ios/voice/monitor/configuration/guide/vt_voip_err_cds_ps6350_TSD_Products_Configuration_Guide_Chapter.html

Example:

```
getmany 1.5.14.10 cCallHistoryIec
cCallHistoryIec.6.1 = 1.1.228.3.31.0
>getmany 172.19.156.132 cCallHistory
cCallHistorySetupTime.6 = 815385
cCallHistoryPeerAddress.6 = 1300
cCallHistoryPeerSubAddress.6 =
cCallHistoryPeerId.6 = 8000
cCallHistoryPeerIfIndex.6 = 76
cCallHistoryLogicalIfIndex.6 = 0
cCallHistoryDisconnectCause.6 = 15
cCallHistoryDisconnectText.6 = call rejected (21)
cCallHistoryConnectTime.6 = 0
cCallHistoryDisconnectTime.6 = 815387
cCallHistoryCallOrigin.6 = answer(2)
cCallHistoryChargedUnits.6 = 0
cCallHistoryInfoType.6 = speech(2)
cCallHistoryTransmitPackets.6 = 0
cCallHistoryTransmitBytes.6 = 0
cCallHistoryReceivePackets.6 = 0
cCallHistoryReceiveBytes.6 = 0
cCallHistoryReleaseSrc.6 = internalCallControlApp(7)
cCallHistoryIec.6.1 = 1.1.228.3.31.0

>getone 172.19.156.132 cvVoIPCallHistoryRemMediaIPAddr.6
cvVoIPCallHistoryRemMediaIPAddr.6 = 1.5.14.13
```

Additional References

The following sections provide references related to Virtual Route Forwarding.

Related Documents

Related Topic	Document Title
Cisco Unified CME configuration	• *Cisco Unified Communications Manager Express System Administrator Guide* • *Cisco Unified Communications Manager Express Command Reference*
Cisco IOS voice configuration	• *Cisco IOS Voice Configuration Library* • *Cisco IOS Voice Command Reference*
Phone documentation for Cisco Unified CME	• User Documentation for Cisco Unified IP Phones

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Toll Fraud Prevention

Table 2-2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 2-2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 2-2 Feature Information for Virtual Route Forwarding

Feature Name	Cisco Unified CME Version	Feature Information
Toll Fraud Prevention in Cisco Unified CME	8.1	Introduced support for Toll Fraud Prevention feature.