SecureLogix®
We see your voice®

ETM® (Enterprise Telephony Management) System

v7.1.1

Caller ID Authentication (CIDA) User Guide

DOC-CID-711-0924208

About SecureLogix

SecureLogix, a Gartner designated "Cool Vendor" is the leader in enterprise voice/UC policy enforcement and ROI intelligence. SecureLogix 7th generation solutions enable customers to save money through securing and optimizing IP Telephony and legacy voice networks, allowing cost efficient and confident migration to SIP Trunking and Unified Communications. SecureLogix solutions are currently protecting and managing over three-and-a-half million enterprise phone lines.

The highly patented SecureLogix® ETM® System helps to secure, optimize and simplify the management of complex enterprise voice/UC networks through enterprise-wide voice network intelligence and unified policy enforcement. Available as an appliance-based solution or deployed via a software-only model running on the Cisco Enterprise router family, the ETM System enables a hard-dollar ROI payback in less than 12 months by securing the enterprise from attack, fraud, data leakage, financial losses and service abuse over TDM and VoIP (SIP) enterprise phone lines, while optimizing voice service and infrastructure expenses.

For more information about SecureLogix and its products and services, visit us on the Web at *www.securelogix.com* and *www.voipsecurityblog.com*.

Corporate Headquarters:
SecureLogix Corporation
13750 San Pedro, Suite 820
San Antonio, Texas 78232
Telephone: 210-402-9669 (non-sales)
Fax: 210-402-6996
Email: *info@securelogix.com*
Website: *http://www.securelogix.com*

Sales:
Telephone: 1-800-817-4837 (North America)
Email: *sales@securelogix.com*

Customer Support:
Telephone: 1-877-SLC-4HELP
Email: *support@securelogix.com*
Web Page: *http://support.securelogix.com*

Training:
Telephone: 210-402-9669
Email: *training@securelogix.com*
Web Page: *http://training.securelogix.com*

Documentation:
Email: *docs@securelogix.com*
Web Page: *http://support.securelogix.com*

IMPORTANT NOTICE:

This manual and the software and/or Products described in it are furnished under license with SecureLogix Corporation ("SecureLogix") and may be used only in accordance with the terms of such license.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without prior written permission of SecureLogix.

The content of this manual is subject to change without notice. SecureLogix assumes no responsibility or liability for any errors or inaccuracies that may be contained herein or to correct the same.

ETM, We See Your Voice, SecureLogix, and the SecureLogix Emblem are registered trademarks or registered trademarks and registered service marks of SecureLogix Corporation in the U.S.A. and other countries. PolicyGuru is a registered trademark of SecureLogix Corporation in the U.S.A. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

This product is protected by one or more of the following patents: US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,718,024 B1, US 6,760,420 B2, US 6,760,421 B2, US 6,879,671 B1, US 7,133,511 B2, US 7,231,027 B2, US 7,440,558 B2, US 8,150,013 B2, CA 2,354,149, DE 1,415,459 B1, FR 1,415,459 B1, and GB 1,415,459 B1. U.S. Patents Pending.

ETM is used herein as shorthand notation to refer to the ETM® System.

This product includes:

Data Encryption Standard software developed by Eric Young (eay@mincom.oz.au),

Style Report software owned and licensed exclusively by InetSoft Technology Corp.

Software developed by The Apache Software Foundation (http://www.apache.org/)

Linux kernel software developed by Linus Torvalds and others; and Busy Box software developed by Bruce Perens and others. Distributed pursuant to the General Public License (GPL). See the Open Source Code directory on the ETM software CD for related copyrights, licenses, and source code.

GNU C Library software; Distributed pursuant to the Library General Public License (LGPL). See the Open Source Code directory on the ETM software CD for related copyrights, licenses, and source code.

Customer Support
for Your ETM® System

1-877-SLC-4HELP
(1-877-752-4435)
support@securelogix.com
http://support.securelogix.com

SecureLogix Corporation offers telephone, email, and web-based support. For details on warranty information and support contracts, see our web site at

http://support.securelogix.com

Contents

Preface

About the ETM® System Documentation

The complete documentation for the ETM® System consists of a set of user guides in PDF format and in-depth, context-sensitive online Help. The electronic PDFs are available from the **SecureLogix** directory on the **Start** menu (Windows systems), the **Documentation** folder in the ETM System installation directory (all systems), and the root of the ETM Software installation CD.

ETM® System User Guides

The following set of guides is provided for the ETM® System:

ETM® System User Guide—Explains ETM System Concepts and provides task-oriented instructions for using the ETM System, including a Quick Start.

ETM® System Installation Guides—Provide task-oriented installation and configuration instructions and explanations for technicians performing system setup. This set of guides includes a primary system installation guide and separate guides for the Unified Trunk Application (UTA), SRE-V, and inline SIP application installation, and for database preparation.

Voice Firewall User Guide—Provides an overview of the Voice Firewall, examples of and instructions for creating and managing Firewall Policies, and instructions for viewing results of Policy monitoring and enforcement.

Voice IPS User Guide—Provides an overview of the Voice IPS (Intrusion Prevention System), examples of and instructions for creating and managing IPS Policies, and instructions for viewing results of Policy monitoring and enforcement.

ETM® Call Recorder User Guide—Provides an overview of the Call Recorder system, instructions for installing, configuring and using the system, examples of and instructions for creating and managing Call Recorder Policies, and instructions for accessing and managing the recordings.

ETM® System Caller ID Authentication (CIDA) User Guide—Describes installation and use of the ETM System CIDA feature.

SecureLogix® Syslog Alert Tool User Guide—Provides instructions for installing and using the Syslog Alert Tool.

Usage Manager User Guide—Provides task-oriented instructions and tutorials for producing reports of telecommunications accounting and Policy enforcement. Includes an appendix describing each of the predefined Reports.

ETM® System Administration and Maintenance Guide—Provides task-oriented instructions for using the ETM System to monitor telco status and manage ETM System Appliances.

ETM® System Technical Reference—Provides technical information and explanations for system administrators.

ETM® Database Schema—Outlines the schema of the SecureLogix database, to facilitate use of third-party reporting tools.

ETM® Safety and Regulatory Compliance Information—Provides statements regarding safety warnings and cautions; includes statements required for compliance with applicable regulatory and certification authorities. (Provided as a package insert with new Appliance hardware.)

Additional Documentation on the Web

SecureLogix provides corrections and additional documentation for its products via the SecureLogix Knowledge Base online at the following web address:

http://support.securelogix.com/knowledgebase.htm

Tell Us What You Think

We welcome your suggestions or comments on the user guides and the online Help provided with your ETM System. Please send your documentation feedback to the following email address:

docs@securelogix.com

Conventions Used in This Guide

The following conventions are used in this guide:

- Functions that require two or more mouse clicks to open a dialog box or make a selection are written using the pipe symbol. For example:

  Click **View | Implied Rules**.

- Names of keys on the keyboard are uppercase. For example:

  Highlight the field and press DELETE.

- If two or more keys must be pressed at the same time, the PLUS SIGN (+) is used as follows:

  Press CTRL+ALT+DELETE.

- Bold text indicates GUI labels, menu items and options, literal file names, and paths. For example:

  Click **Edit**, and then click **Preferences**.

  C:\Program Files\SecureLogix\ETM\TWLicense.txt

- Keyboard input is indicated by monospaced font. For example:

In the **Name** box, type: `My report tutorial`

- Italics indicate web addresses and names of publications.
- ETM System components and features are capitalized.

Caller ID Authentication (CIDA) Support

Overview of CIDA Support

The ETM System supports Caller ID Authentication through integration with TRUSTID's solution. This licensed feature is particularly valuable in call center environments, and provides four key benefits:

- Decreases call center fraud rates.
- Increases IVR containment rates.
- Speeds the time required to authenticate callers who do reach agents.
- Provides an improved customer experience over other technologies for call authentication.

ETM® System Integration with the TRUSTID™ Solution

The ETM Caller ID Authentication (CIDA) feature is used in conjunction with the TRUSTID Authenticator™.

TRUSTID Authenticator is an undetectable, network-based caller authentication service provided primarily to call centers. Before an incoming call is answered, TRUSTID Authenticator determines the authenticity of a calling party's ANI or Caller ID using proprietary and patent-pending real-time telephone network forensics.

To use TRUSTID Authenticator, inbound call information must be captured and sent to the TRUSTID Authenticator web service before answer supervision signaling is sent to the calling device. When the TRUSTID Authenticator completes its forensics, it returns the results to the system that provided the capture and the inbound call routing is then completed. The ETM System integrates with the TRUSTID Authenticator to provide this call data capture and call control.

For specified lines, the ETM Application delays answer supervision of a call and sends the TRUSTID Authenticator the called number, calling number, and ANI information for authentication. The TRUSTID response ("Credentialed" or "Not Credentialed") is returned to the ETM Server which then passes the response to the ETM Appliance to complete the call setup. Call center operators can use this response to determine appropriate handling of the call.

The ETM Server displays the returned result in the Call Monitor and stores it in the database for offline reporting.

The ETM Server can support up to 100 simultaneous CIDA requests. This feature currently supports T1 PRI lines only.

Use of the CIDA feature requires Internet access on the ETM Server host and an account with TRUSTID.

One of the following values is displayed for each call for which an authentication request was made: “Credentialed”, “Not Credentialed”,

Other Data Fields Available from the TRUSTID Authenticator™

In addition to the “Credentialed” or “Not Credentialed” result, the TRUSTID Authenticator provides 79 additional data fields for each call query. While “Credentialed” results are highly reliable, “Not Credentialed” results may need further analysis to determine the reason. Some of the available values include:

- Intentionally Falsified
- International Call Origination
- Pay Phone Origination
- Pre-paid Phone Origination
- Velocity Counter for recurring “Not Credentialed” results (clients can set the duration of monitoring).

These data fields are not currently available through or used by the ETM System, but can be provided by and tailored through your TRUSTID account. Ask your TRUSTID account representative for more information.

Modes of Operation

The ETM CIDA feature provides two modes of operation: Early Audio and Delayed Audio: The applicable mode is configured per D-Channel Span on each T1 PRI on which this feature is used.

Delayed Audio Mode

Delayed Audio Mode provides a mechanism to prevent truncation of the audio announcement from the IVR, which can occur during authentication on some VoIP-based carriers, while minimizing any impact to the caller's user experience.

Normally, when the telephone network is in the "alerting" state (when the caller hears ringback), the caller's network side stops ringing when a "voice" or tones are detected on the line. With most carriers, this happens when the IVR announcement starts. However, with some VoIP-based networks, the IVR announcement may be truncated because the network does not react to the audio from the IVR and continues to play ringback to the caller until the "connect" is completed after TRUSTID authentication. On these networks, ringback and the IVR announcement both play in parallel, with the caller only hearing the ringback. When the connection is completed, the network cuts over the IVR audio; however, by this time the caller has missed hearing a number of seconds' worth of the audio announcement. Delayed Audio Mode prevents this from occurring.

When using Delayed Audio Mode, you can optionally specify redirection destinations for incoming calls based on the authentication results received. For example, if a call center receives a call that is credentialed, it can go to the regular pool of agents as dialed. If the call is not credentialed, it can be redirected to a more senior agent that can take additional authentication steps, such as asking security questions.

IMPORTANT: Redirection is only available for the Delayed Audio Mode of operation.

Early Audio Mode

In Early Audio Mode, the appliance delays answer supervision by holding the CONNECT message that comes from the CPE while waiting for a response from the TRUSTID Authenticator. If the IVR is playing an announcement, the caller typically hears this announcement during this short delay (if the carrier supports this functionality). In other words, the caller's user experience is not affected by the use of CIDA. One known caveat is that the caller-to-IVR audio path is not complete until the "connect" is released to the CO by the appliance. Therefore, while authentication is being performed, the caller typically hears any audio announcement the IVR plays, but no audio or DTMF input from the caller is heard by the IVR.

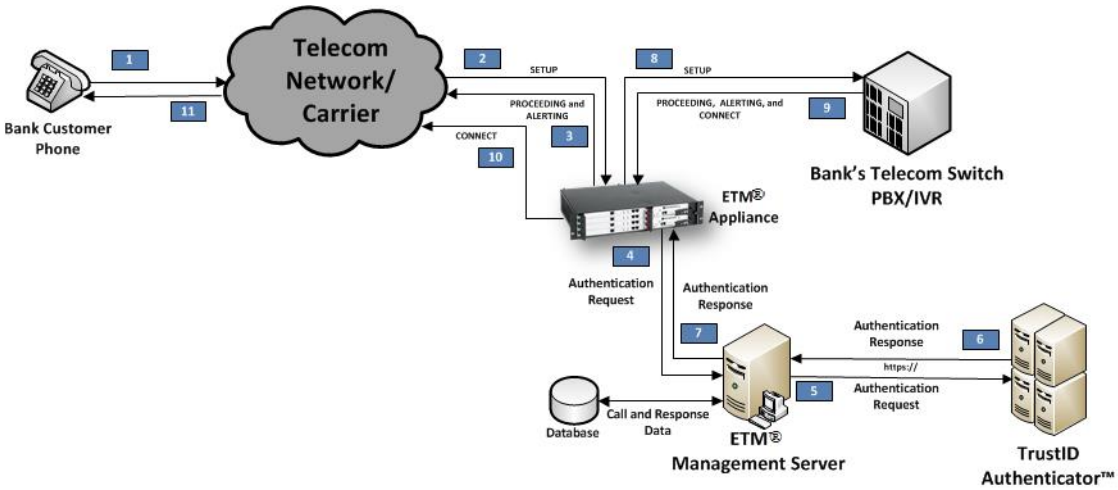
Also, as described above, with some VoIP-based networks, the IVR announcement may be truncated because the network does not react to the audio from the IVR and continues to play ringback to the caller until the "connect" is completed after TRUSTID authentication. On these networks, ringback and the IVR announcement both play in parallel, with the caller

only hearing the ringback. When the connection is completed, the network cuts over the IVR audio; however, by this time the caller has missed hearing a number of seconds' worth of the audio announcement.

If you are concerned about callers hearing clipped announcements, use Delayed Audio Mode instead.

Reference Architecture – Delayed Audio Mode

The following diagram illustrates the general call flow in the Delayed Audio mode of operation. This call flow is described in the following section.



General Call Flow –Delayed Audio Mode

In Delayed Audio Mode, the CIDA call flow proceeds as follows:

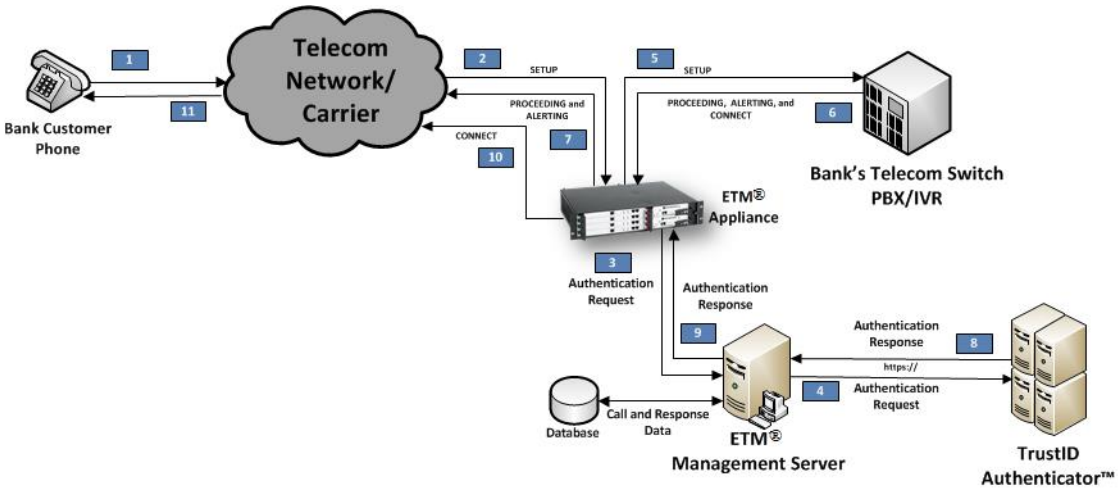
1. Phone device calls the call center's telephone number.
2. Call is routed to the appliance over a T1 PRI line; SETUP message is held.
3. PROCEEDING and ALERTING messages are provided back to the carrier by the appliance.
4. The appliance extracts call information (ANI, etc.) and sends an Authentication Request to the Management Server.
5. The Management Server sends an Authenticator API message to the TRUSTID web service via an HTTPS GET request.
6. The Management Server receives TRUSTID's response to the HTTPS GET request.
7. The Management Server stores the response information in the database and forwards the response to the appliance. Response is received by the appliance. If a response does not arrive within a configurable amount

of time (nominally 10 seconds), the appliance will timeout and continue on to the next step.

8. Appliance initiates call to the Switch by forwarding held SETUP message to the Switch.
9. Switch receives the incoming call SETUP and generates PROCEEDING, ALERTING, and CONNECT messages. Appliance receives PROCEEDING and ALERTING but does not pass the messages to the network.
10. Appliance receives CONNECT and passes the CONNECT to the network, effectively bridging the call.
11. Call proceeds normally.

Reference Architecture – Early Audio Mode

The following diagram illustrates the general call flow in the Early Audio mode of operation. This call flow is described in the following section.



General Call Flow – Early Audio Mode

In Early Audio Mode, the CIDA call flow proceeds as follows:

1. Phone device calls the call center's telephone number.
2. Call is routed to the appliance over a T1 PRI line; SETUP message is received.
3. The appliance extracts call information (ANI, etc.) from the SETUP message and sends an Authentication Request to the Management Server.
4. The Management Server sends an Authenticator API message to the TRUSTID web service via an HTTPS GET request.

5. The SETUP message is held by the appliance for a configurable amount of time and then forwarded to the Switch.

6. PROCEEDING, ALERTING, and CONNECT messages are generated by the Switch.

7. The PROCEEDING and ALERTING messages are forwarded to the carrier. The appliance holds the CONNECT message for a configurable amount of time or until an authentication response is received.

8. The Management Server receives TRUSTID's response to the HTTPS GET request.

9. The Management Server stores the response information in the database and forwards the response to the appliance.

10. The Appliance forwards the held CONNECT message to the carrier. If a response does not arrive within a configurable number of seconds, the appliance will timeout and forward the CONNECT message on timer expiry.

11. Call proceeds normally.

Configuring CIDA

Configuring the CIDA feature consists of the following sequence of steps:

1. License the CIDA feature. An ETM Server license that includes this feature is required.
2. Provide entries in the **twms.properties** file on the ETM Server.
3. Select the mode of operation on the D-Channel Span: Delayed Audio or Early Audio.
4. Define an Authentication Endpoint List (AEL) file and install it on the D-Channel Spans on which the feature is to be used.

Procedures for each step are provided below.

License CIDA

Obtain an ETM Server license that includes the CIDA feature from SecureLogix Customer Support and place it in the ETM Server installation directory, replacing any previous license file. To obtain the license, you must provide the system ID of the ETM Server to Customer Support.

To obtain the Management Server license

1. Contact SecureLogix Corporation Customer Support at one of the following:
   - Telephone: 1-877-752-4435
   - Email: *support@securelogix.com*
2. Provide your System ID to SecureLogix Customer Support and let them know that you purchased the CIDA feature and whether you purchased Call Recorder.
3. SecureLogix provides you with a license file named **TWLicense.txt**. Copy **TWLicense.txt** to the Management Server installation directory. Copy the file to the root of the ETM System Server installation directory, and to the root of the Report Server installation directory, if it is installed on a different computer from the Management Server.

Properties File Entries to Enable CIDA

To enable the CIDA feature after it is licensed; add the following fields to the **twms.properties** file in the ETM System installation directory, provide appropriate values, and then restart the ETM Server.

```
## CIDA
CIDAEnabled=1
CIDAPrimaryURL=https://<URL__OF_PRIMARY_TRUSTID_SERVER>
CIDABackupURL=https://<URL__OF_BACKUP_TRUSTID_SERVER>
CIDAUsername=<TRUSTID_USERNAME>
CIDAPassword=<TRUSTID_PASSWORD>
ConnectionTimeout=<milliseconds_value_post-connection_request_timeout>
ReadTimeout=<milliseconds_value_connection_timeout>
CIDAThreadPoolSize=<NUMBER_OF_SIMULTANEOUS_REQUESTS>
```

NOTES:

- `CIDAThreadPoolSize` defaults to `100`, which should be sufficient for most implementations. No maximum value is enforced, since it is dependent on available system resources.
- `ConnectionTimeout` specifies the amount of time for the ETM Server to connect to the TRUSTID Authenticator before timing out and instructing the appliance to connect the call.
- `ReadTimeOut` specifies the amount of time the ETM Server waits for a response after connecting to the TRUSTID Authenticator before timing out and instructing the appliance to connect the call. Obtain the TRUSTID-specific values from your TRUSTID account representative.

For example:

```
## CIDA
CIDAEnabled=1
CIDAPrimaryURL=https://primary.TRUSTIDinc.com/tid?
CIDABackupURL=https://backup.TRUSTIDinc.com/tid?
CIDAUsername=secureLogixETM
CIDAPassword=N883JHGs0
ConnectionTimeout=5000
ReadTimeout=17000
```

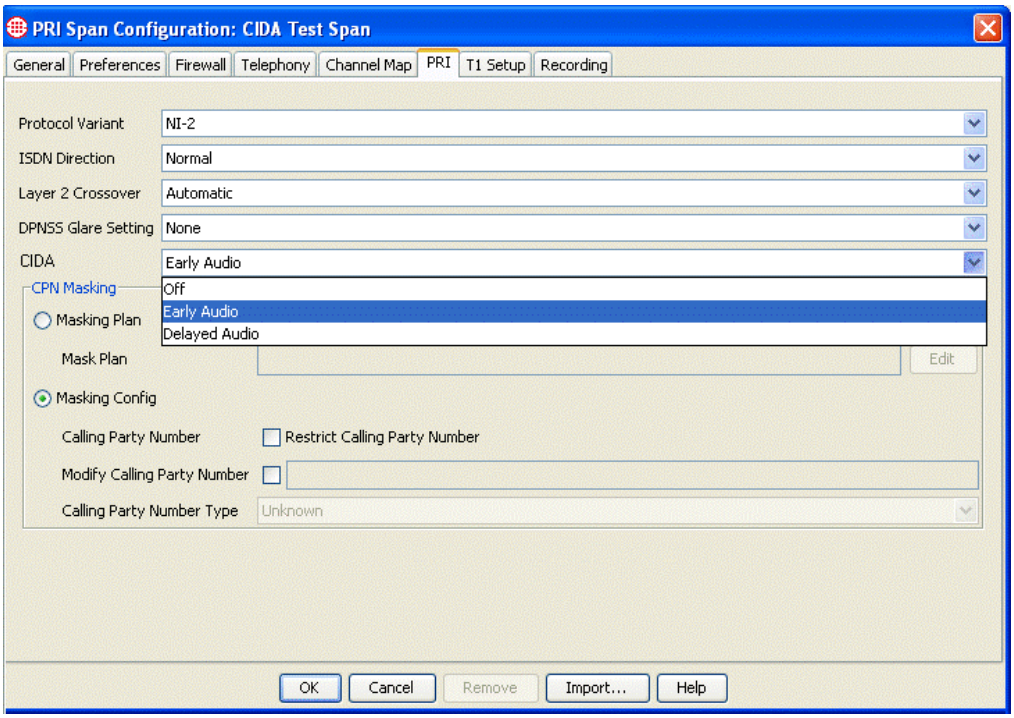
```
CIDAThreadPoolSize=100
```

Setting the Mode of Operation

Two modes of operation are available for the CIDA feature: Delayed Audio and Early Audio. See "Modes of Operation" on page 6 for a description of each mode to determine which mode is appropriate for each appliance that is supporting your implementation of CIDA.

To set the mode of operation

1. In the **Platform Configuration** subtree, right-click the T1 PRI Span containing the D-Channel and select **Edit Span**. The **PRI Span Configuration** dialog box appears.
2. Click the **PRI** tab.



3. In the **CIDA** field, click the down arrow and select **Early Audio** or **Delayed Audio**. The default is **Off**.
4. Click **OK** to save the configuration and download the changes to the Span.

Authentication Endpoint List (AEL)

The Authentication Endpoint List (AEL) is used to define the Inbound Destinations that trigger authentication. When an inbound call is made to a destination in the AEL, the calling party (source) of the call is authenticated using the TRUSTID Authenticator service.

Defining An AEL

The AEL is a text file created with an editor such as Notepad, Notepad++, or WordPad. See below for an example AEL text file. The AEL file resides in the **~/etm/ps/ael** directory.

An entry in the AEL consists of the following mandatory and optional fields:

Mandatory field:

1. Destination phone number.

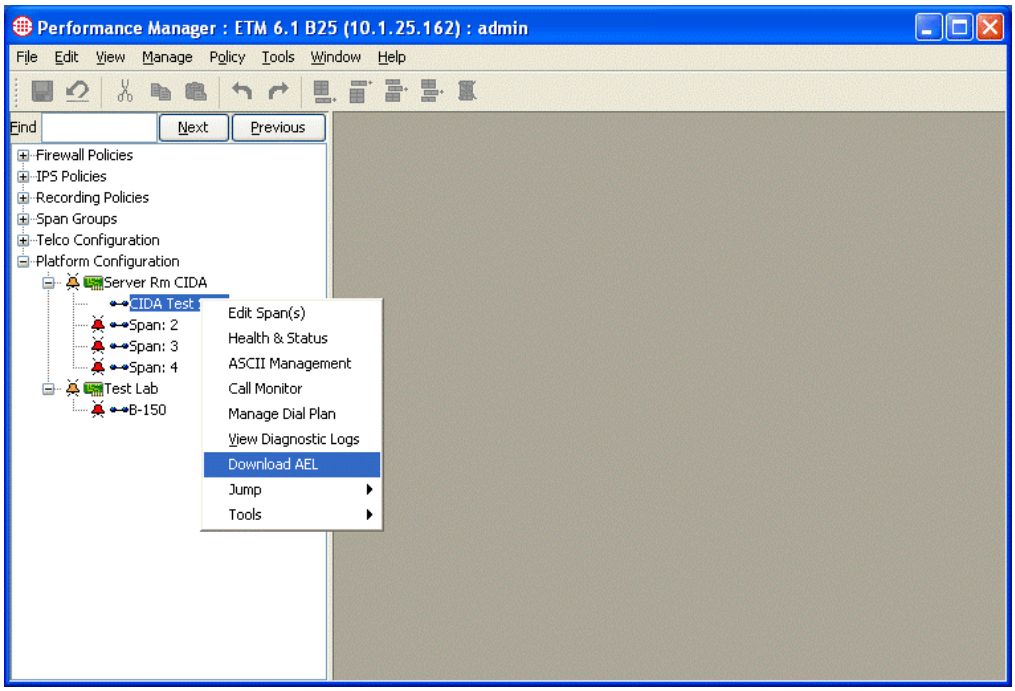
Optional fields:

2. A destination label.
3. (*Delayed Audio Mode only*) An “authenticated” source redirection phone number.
4. (*Delayed Audio Mode only*) A “not authenticated” redirection phone number.
5. (*Delayed Audio Mode only*) An “error” redirection phone number.

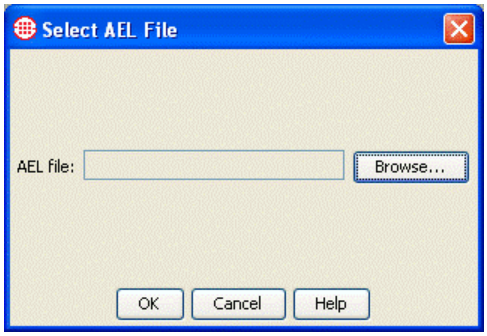
Installing the AEL on the Span

To download the AEL file to the Appliance

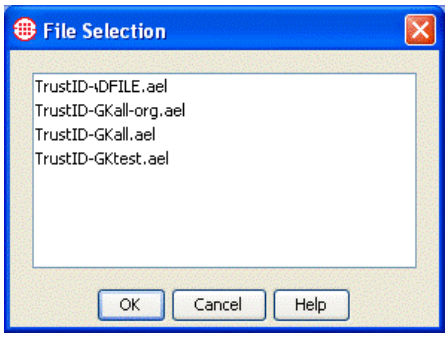
1. In the **Platform Configuration** subtree, right-click the D-Channel Span and click **Download AEL**.



2. The **Select AEL File** dialog box appears.



3. Click **Browse**. The **File Selection** dialog box appears, showing all AEL files in the directory.



4. Select the file that applies to the selected Span and click **OK**.
5. The file is downloaded to the selected Span. The **Status Tool** provides information about the download.

Viewing CIDA Results

CIDA authentication request results can be viewed in the Call Monitor and are stored in the ETM Database for offline reporting. They are not available via the Usage Manager.

Call Monitor

The Call Monitor displays the received authentication results in a CIDA column. One of the following values is displayed for each call for which an authentication request was made: “Credentialed”, “Not Credentialed”, or “Error”. If “Error” is displayed, the **CIDA** field for that call is colored RED.

Appendices

Appendix A: Sample AEL File

```
########################################################################
# Call ID Authentication Endpoint List (CIDA AEL)
#
# File:   Example.ael
#
# Author: Kirk E. Smith
# Date:   07 February 2013
#
########################################################################
#
# Comments start with a '#' (hash mark).
# Blank lines are ignored.
#
# Abbreviations:
# PN    - Phone Number
# CC    - Country Code
# AC    - Area Code or NPA (Numbering Plan Area)
# Exchg - Exchange (for North America, 3 digits)
# Ext   - Extension (for North America, 4 digits)
#
# An entry consists of a phone number and optional destination
#   label, "authenticated" redirection PN, "not authenticated"
#   redirection PN, and/or "error" redirection PN. Entries begin and
#   end with angle brackets (<>) and are comma delimited.
#
# Example:
```

```
#      <dest=[1](210)555-1001, label=MyLabel, auth=[1](210)555-1002,
#       notAuth=[1](210)555-1003, error=[1](210)555-1004>
#
# Phone numbers take the following forms:
#  [CC](NPA)Exchg-Ext
#  [CC](NPA)Exchg.Ext
#
# White space is ignored in phone number.
#
# Label cannot start with a '<', '>' or ',' character.
# Leading or trailing white space is removed from labels.
# Labels are limited to 127 characters.
#
#########################################################################
#
# Corporate line
#
<dest=[1](210)555-2677, label=Corporate>

#
# Auto Insurance Agents
#
<dest=[1](210)555-2468, label=AutoInsurance>
<dest=[1](210)555-2469, label=AutoInsurance>

#
# Home Insurance Agents
#
<dest=[1](210)556-4663, label=HomeInsurance>
<dest=[1](210)555-4664, label=HomeInsurance>

#
# Redirection
#
# normal=Agent Pool  not auth=Senior Agent
```

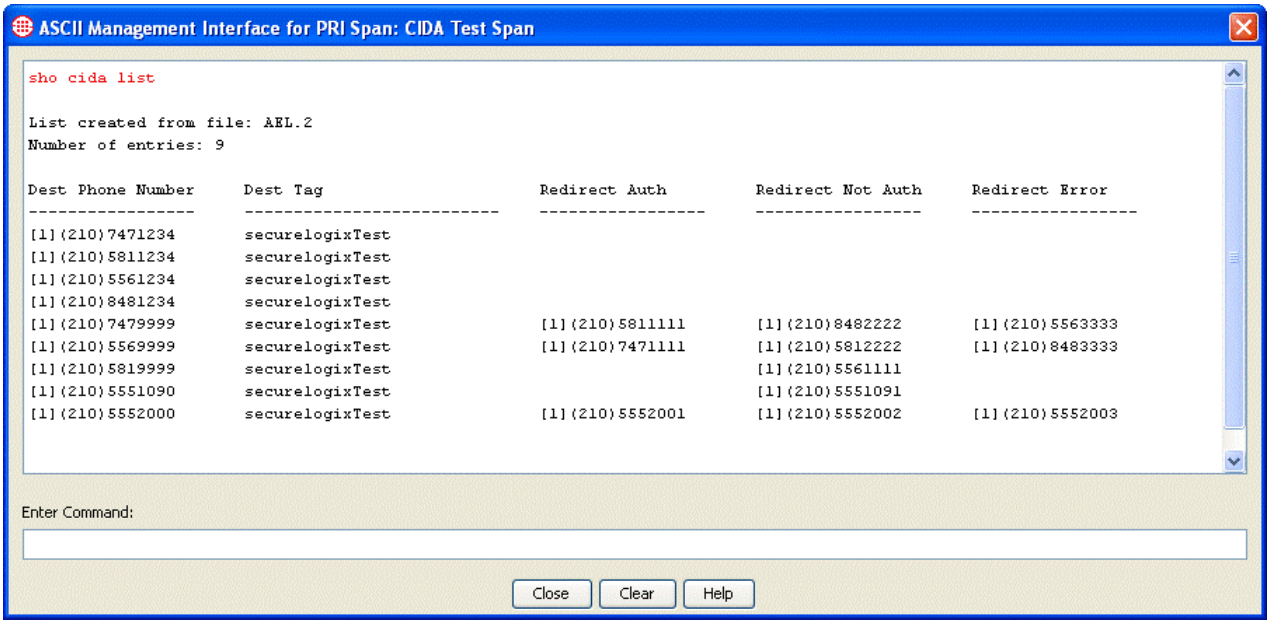
```
<dest=[1](210)555-7665, label=AgentPool, notAuth=[1](210)555-7367>


#
# NOTE: In this example, no calls will route to the 7666 extension.
# auth=Agent Pool  not auth=Senior Agent  error=Special Agent
#
<dest=[1](210)555-7666, label=AgentPool, auth=[1](210)555-7665,
notAuth=[1](210)555-7367, error=[1](210)555-7263>


###############################################################################
#                       end of file example.ael
###############################################################################
```

Show CIDA List Output

Downloading the above example file produces the following ASCII Management window output after issuing a SHOW CIDA LIST command:



Appendix B: CIDA Appliance Commands Reference

The table below provides a summary of the Appliance ETM Commands available for the CIDA feature. A detailed command description follows the table.

CIDA Appliance Command Summary				
Command	**Value 1**	**Value 2**	**Default**	**Description**
CIDA ALERTING GEN	0-6	0x0000-0xFFFF	2	Generate message with Channel IE
CIDA ALERTING MOD	0-12	0x0000-0xFFFF	0	
CIDA ALERTING TIMEOUT	0-10000	-	0	
CIDA CONNECT EXCLUSIVE	enable disable	-	enable	
CIDA CONNECT TIMEOUT	0-20000	-	10000	
CIDA PROCEEDING GEN	0-6	0x0000-0xFFFF	2	Generate message with Channel IE
CIDA PROCEEDING MOD	0-12	0x0000-0xFFFF	0	
CIDA PROCEEDING TIMEOUT	0-4000	-	0	
CIDA PROGRESS MOD	0-12	0x0000-0xFFFF	0	
CIDA PROGRESS GEN	0-6	0x0000-0xFFFF	0	Do not generate message
CIDA PROGRESS TIMEOUT	0-10000	-	0	
CIDA RELEASE MOD	0xccccpppp	-	0x80908290	
CIDA RESPONSE	0-30000	-	20000	

TIMEOUT				
CIDA SETUP TIMEOUT	0-4000	-	1500	
CIDA SPAN MODE	disable earlyAudio delayedAudio	-	disable	
SHOW CIDA CONFIG	-	-	-	
SHOW CIDA FILE	-	-	-	
SHOW CIDA LIST	-	-	-	

CIDA Common Commands

1) CIDA SPAN MODE

The CIDA Span Mode command sets the mode for CID Authentication for the D-channel span and by association, the bearer channels serviced by the D-channel.

User supplied value for the command is one of the following:

- disable – disables (turns off) CID Authentication for the D-channel span.
- earlyAudio – selects early audio CIDA mode
- delayedAudio – selects delayed audio CIDA mode

See the FDD for an explanation of the CIDA modes and their uses.

DEFAULT: disabled

2) CIDA CONNECT EXCLUSIVE

The CIDA Connect Exclusive command directs the handling of the exclusive channel indication in the SETUP message forwarded to the CPE/PBX/IVR. For SETUP messages that contain a Channel ID IE (indicating the desired channel that the call will occupy), there is a bit (bit 4) in the IE that indicates whether the requested channel is preferred or exclusive. Exclusive in this context means that only the indicated channel is acceptable. The setting of the exclusive bit in the Channel IE of the SETUP message is intended to prevent channel negotiation from taking place between the CPE and the CO. The CIDA subsystem does not

manage the telephony channels. Since the appliance is delaying and/or interrupting call supervision, it will be responding to the CO without knowing the state of the channel within the CPE. By setting the exclusive bit when forwarding the SETUP message to the CPE, the appliance is forcing the CPE to honor that channel or tear down the call due to the resource being busy. If Connect Exclusive is disabled, then the SETUP message Channel ID IE is not modified.

User supplied value for the command is one of the following:

- default – sets the configuration item to its default value
- enable – the exclusive bit will be set in the SETUP Channel ID IE
- disable – the SETUP Channel ID IE will not be modified

DEFAULT: enabled

3) CIDA RESPONSE TIMEOUT

CIDA RESPONSE TIMEOUT default|timeout max milliseconds to wait for auth response
(response may come in after connect)

CIDA CONNECT TIMEOUT default|timeout msecs before initiating connection to CPE
(overdue authentication response)

CIDA RELEASE MOD value Call release messages modifier
0xccccpppp - cause values for release messages where
cccc = hex code for the release cause to CO
pppp = hex code for the release cause to CPE

Early Audio Commands

CIDA SETUP TIMEOUT default|timeout msecs to hold SETUP before forwarding to CPE

CIDA PROCEEDING MOD cmd value Proceeding message modifier

CIDA PROGRESS MOD cmd value Progress message modifier

CIDA ALERT MOD cmd value Alert message modifier
0 - do nothing
1 - gen message (no additional IE's)
2 - gen message with Chn IE
3 - gen message with Chn IE (exclusive)
4 0xnnnn - gen message with progress IE 0xnnnn
5 0xnnnn - gen message with Chn IE + progress IE 0xnnnn
6 0xnnnn - gen message with Chn IE (exclusive) + progress IE 0xnnnn
7 - drop msg (does not cross over msg from CPE to CO)
8 - add message Chn IE
9 - add/set message Chn IE (exclusive)
10 0xnnnn - add/set message progress IE 0xnnnn (a value of 0x0000 removes the IE)
11 0xnnnn - add/set message Chn IE + progress IE 0xnnnn
12 0xnnnn - add/set message Chn IE (exclusive) + progress IE 0xnnnn

Delayed Audio Commands

CIDA PROCEEDING TIMEOUT default|timeout msecs from SETUP before sending PROCEEDING

CIDA PROGRESS TIMEOUT default|timeout msecs from SETUP before sending PROGRESS

CIDA ALERTING TIMEOUT default|timeout msecs from SETUP before sending ALERTING

CIDA PROCEEDING GEN cmd value Proceeding message modifier

CIDA PROGRESS GEN cmd value Progress message modifier

CIDA ALERT GEN cmd value Alert message modifier
where 0 - do nothing
1 - gen message (no additional IE's)
2 - gen message with Chn IE
3 - gen message with Chn IE (exclusive)
4 0xnnnn - gen message with progress IE 0xnnnn
5 0xnnnn - gen message with Chn IE + progress IE 0xnnnn
6 0xnnnn - gen message with Chn IE (exclusive) + progress IE 0xnnnn

Show Commands

SHOW CIDA CONFIG	displays the CID Authentication configuration
SHOW CIDA LIST	displays the CIDA destination PN list
SHOW CIDA FILE	displays the CIDA destination PN list file contents