

Release 6.3.0

ETM[®] System

Technical Reference



About SecureLogix Corporation

SecureLogix Corporation enables secure, optimized, and efficiently managed enterprise voice networks. The company's ETM[®] (Enterprise Telephony Management) System hosts a suite of integrated telecom applications that protect critical network resources from telephony-based attack and abuse, and simplify voice network management.

SecureLogix[®] Solutions address real-world problems for real-world voice networks. The flexible ETM System scales to support any voice environment, no matter how large or small. Engineered with full hybrid voice technology, the ETM System supports multi-vendor networks containing any mix of converging VoIP and legacy voice systems.

SecureLogix Solutions are currently securing and managing over two million enterprise phone lines. The company's customers span nearly every industry vertical, from regional banks and hospitals, to the largest military installations and multi-national corporations.

For more information about SecureLogix Corporation and its products and services, visit our website at <http://www.securelogix.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, as well as the software and/or Products described in it, is 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, TeleWatch Secure, TWSA, We See Your Voice, SecureLogix, SecureLogix Corporation, the ETM Emblem, the SecureLogix Emblem and the SecureLogix Diamond Emblem are trademarks and/or service marks or registered trademarks and/or service marks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 1999-2011 SecureLogix Corporation. All Rights Reserved.

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 6,735,291 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, 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),
© Copyright 1995 Eric Young. All Rights Reserved.
(see DESLicense.txt on ETM software CD)

Style Report software owned and licensed exclusively by InetSoft Technology Corp.
© Copyright 1996-2000 InetSoft Technology Corp. All Rights Reserved.

Software developed by The Apache Software Foundation (<http://www.apache.org/>)
© Copyright 2000 The Apache Software Foundation. All Rights Reserved.
(See ApacheLicense.txt on ETM software CD.)

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	9
About the ETM [®] System Documentation	9
ETM [®] System Documentation.....	9
Tell Us What You Think	10
Additional Documentation on the Web	10
Conventions Used in This Guide	10
 Advanced Configuration and Maintenance	 13
About this Section.....	13
Application Properties and Configuration Variables	13
Editing ETM [®] Application Properties and Configuration Files.....	13
Properties and Configuration Files	13
Editing a Properties or Configuration File.....	14
Increasing the Stack Size for the Java Virtual Machine	14
Enabling the ETM [®] Management Service to Write to a Network Drive	15
Setting the Services to Autostart.....	15
Customizing Policy Track Messages	16
Formatting the Access Code Set Distribution Email	17
Changing the Format of Diagnostic Messages	18
Changing the Number of Directory Listings Retrieved per Page	20
Mapping Directory Fields to Default LDAP Attribute Fields.....	20
Limiting the Number of Recorded CDR Records in a Single File	21
Variables in npconfig. properties	21
Variables in twms.properties	21
Using the ETM [®] Database Maintenance Tool	26
Opening the ETM [®] Database Maintenance Tool.....	26
Logging in to the Database	27
Creating a Database Object.....	28
Deleting a Database	29
Disconnecting from a Database	30
Working with Data Instances.....	30
Exporting a Data Instance	30
Importing an Exported Data Instance	32
Setting a Data Instance as the Default	33
Deleting a Data Instance.....	35
Creating a New Data Instance	35
Managing Tables	37
Viewing a Table	37
Attempting to Repair a Table	39

Clearing a Table	39
Deleting a Table	39
Creating a Missing Table.....	40
Running Multiple Application Instances on One System	41
Configuring Multiple Application Instances.....	41
1. Remove the Default Application Instances	41
2. Add Additional Instance(s).....	42
3. Register the Instance(s) with System Startup Facilities.....	42
4. Modify Configuration Files	43
5. Create the Management Server's Data Instance.....	44
6. Enable the Application Instances to Connect to the Database	44
Customizing Database Settings.....	45
Customizing Database Settings in the init.ora file	45
Change the Location of Control Files.....	45
Set Multiblock Read Count Based on Installation Size	45
Set Buffer Size.....	46
Set Shared Pool Size.....	46
For SNP Systems with More Than 1GB RAM.....	46
Automatic Archiving	46
Enable Oracle Trace	47
Specify the Directory to Store Trace and Alert Files.....	47
Enable Resource Management	47
Customizing the Redo Logs, Tablespace, or Rollback Segments	47
Customizing the Redo Logs	47
Adjust the Size of the System Tablespace	47
Adjust the Size of the Rollback Tablespace	48
Temp File and Autoextend	48
Tablespace for Tools	48
Create More Rollback Segments	48

Dialing Plans 49

About Dialing Plans	49
Types of Dialing Plans.....	50
Defining and Installing Dialing Plans	50
Defining Dialing Plans	51
Installing Dialing Plans on a Span.....	51
Dialing Plan Contents	52
Section Header	53
Section Body	53
Dialing Plan Section Header Components	54
cc.....	54
Type.....	54
Name.....	54
Label	54
Call Labels.....	55
Phone Number Labels	56
DSN Codes	57
Compound Labels.....	58

Options.....	59
Defining Dialing Plan Sections	64
CC	64
Classify	64
DDD	65
Default	65
DID	66
Expand	69
NNP	69
NPA	70
Prefix	70
Preprocessed Numbers.....	70
Suffix	70
Special	70
Dialing Plan Processing	71
Phone Number Identification Phase.....	71
Phone Number/Call Classification Phase	73

SMDR Parse Files 75

About SMDR Parse Files	75
Files Already Defined	75
Defining an SMDR Parse File	75
SMDR Parse File Components	76
Section 1: Record Separator	76
Section 2: Call Record	76
Call Record Final Fields	77
Section 3: Access Code Record	79
Access Code Record Final Fields	79
Section 4: Transfer Record	80
Transfer Records Final Fields.....	80
Matching the Dialed Digits String	80
Time Format Syntax	81
Regular Expression Syntax Quick Reference	83
Perl5 Regular Expression Syntax.....	83
Perl5 Extended Regular Expressions	86

ETM[®] System Troubleshooting 87

System Files Used in Troubleshooting.....	87
Management Server Issues	87
ETM [®] Database Issues.....	88
Report Server Issues	88
Client Tool Issues	88
SMDR Issues	88
ETM [®] Appliance Issues.....	89
Call Resolution or Policy Processing Issues	89
Troubleshooting Guide	89
Appliance Status LEDs.....	89
Error and Debug Logs	90

Troubleshooting SMDR Configuration	92
About SMDR Debug Logs	93
Enabling SMDR Debug Logging	93
Reading the SMDR Debug Log.....	94
Logging Appliance Debug Events to a File	95
Symptoms	97
Diagnostic Log Messages	98
System Backup and Recovery Guidelines	99
General Guidelines for Backup Maintenance	99
Complete System Backup	100
ETM Software Installation Directory Contents	100
ETM Software Installation Directory Backup	103
Restoring the ETM Software Installation from a Full Backup	103
Backing Up the Database.....	103
ETM® Commands	105
Using ETM® Commands	105
Important Information about Authority of Server.....	105
Removing a Card from the Tree Pane	106
ETM® Commands Help	106
Logging in to a Card	107
Placing a Digital Span Offline/Inline.....	108
ETM® Command Reference	109
Ports and Services	135

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 Documentation

The following set of guides is provided with your 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 Guide—Provides task-oriented installation and configuration instructions and explanations for technicians performing system setup.

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.

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 and Elements.

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.)

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

Additional Documentation on the Web

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

http://support.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**.

<INSTALL_DIR>\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.

Advanced Configuration and Maintenance

About this Section

This section contains advanced ETM[®] System configuration and maintenance options for experienced technicians. It covers settings that do not normally need to be modified during day-to-day system operation and that should not casually be modified by end users.

Application Properties and Configuration Variables

Several ETM System configuration files contain variables that can be customized by experienced administrators. The **ETM Server Properties Tool**, accessed via the ETM System Console, contains other system properties that can be customized. See the *ETM[®] System Administration and Maintenance Guide* for information about the **ETM Server Properties Tool**.

Editing ETM[®] Application Properties and Configuration Files

You can use a text editor to change variables in some properties and configuration files.

IMPORTANT Only edit the files as recommended in this user guide or by SecureLogix Customer support. Improperly edited files can cause your ETM System to be impaired or inoperable.

Properties and Configuration Files

The following properties and configuration files are located in the ETM Server installation directory. Not all of these files are user-editable.

- **ETMDBMaintTool.cfg—SLCLoader** executable configuration file for the ETM Database Maintenance Tool.
- **ETMManagementService.cfg—ETMManagementService** executable configuration file for the Management Server when launched as a Windows service.

- **ETMManagementServer.cfg**—**ETMManagementServer** executable configuration file for the Management Server on Solaris.
- **ETMReportService.cfg**—**ETMReportService** executable configuration file for the Report Server when launched as a Windows service.
- **ETMReportServer.cfg**—**ETMReportServer** executable configuration file for the Report Server on Solaris.
- **ETMSystemConsole.cfg**—**SLCLoader** executable configuration file for the ETM System Console application.
- **UsageManager.cfg**—**SLCLoader** executable configuration file for the Usage Manager application.
- **DefaultLDAPMappings.properties**—Defines the default mappings of LDAP attribute fields to Directory Manager fields.
- **delivery.properties**—Defines the format of rule-fired messages, diagnostic messages, IPS breach events, and the Access Code Set distribution email.
- **npconfig.properties**—Specifies the format of the numbering plan for country codes and emergency numbers
- **twms.properties**—Defines various parameters used by the Management Server.
- **javax.comm.properties**—Defines the drivers loaded by the Java Communications API standard extension at initialization time. (***Do not edit this file.***)

Editing a Properties or Configuration File

You can use the **ETM Server File Management Tool** to remotely access the properties and configuration files in the ETM System installation directory on the ETM Server computer. See “Managing ETM Server Files from the ETM Client” in the *ETM[®] System Administration Guide* for instructions.

To change a parameter

1. Open the file in a text editor.
2. Add a parameter or edit the value of an existing parameter, and then save the file with the same name in the same location.
3. Restart the affected component for the change to take effect.

Increasing the Stack Size for the Java Virtual Machine

If you experience memory errors while generating reports for large amounts of data, it is recommended that you increase the stack size available to the Java Virtual Machine in the ETM Server, Report Server, standalone Usage Manager, and/or ETM System Console configuration files.

To increase the stack size available to the Java Virtual Machine

1. Stop the application(s) whose configuration file(s) you are modifying (ETM Server, Report Server, ETM System Console, standalone Usage Manager).
2. On the Management Server computer, open the configuration file in a text editor. The file is located at the root of the Management System installation directory.
 - Management Server
 - Solaris—**ETMManagementServer.cfg**
 - Windows—**ETMManagementService.cfg**
 - Report Server
 - Solaris—**ETMReportServer.cfg**
 - Windows—**ETMReportService.cfg**
 - ETM System Console—**ETMSystemConsole.cfg**
 - Standalone Usage Manager—**UsageManager.cfg**
3. Locate the text that reads:
`-Xmx<value>M`
4. By default, 512 MB is allocated for the ETM Server, 400 MB for the ETM System Console, and 200 MB for the Report Server and standalone Usage Manager. Change the number represented by `<value>` to a higher number, such as **600M**, **800M**, etc., depending on system load and available memory.
5. Save the file.
6. Start the application.

Enabling the ETM[®] Management Service to Write to a Network Drive

On Windows operating systems, the ETM Server service runs under the local system account, an account that typically does not have permission to write to a network drive. If you want scheduled reports to be saved to a network drive, you must configure the **ETM Management Service** to run under a user account with permission to write to the network drive. See your IT system administrator or the documentation for your operating system for assistance.

Setting the Services to Autostart

On Windows, the ETM Management Service and ETM Report Service are set by default to be manually restarted if the computer is rebooted . If you want the services to start automatically when the machine is booted, set them to automatic in the Windows **Services** dialog box on the Server host computer.

Customizing Policy Track Messages

The subject and content of **Email** and **Real-Time Alert** Policy Track messages are defined by a file named **delivery.properties**, located in the ETM System installation directory. To modify the Track messages, you can edit this file. The settings in the **delivery.properties** file do not affect System Event Tracks, which are hard-coded into the system.

The **Key to Indexing** at the top of the **delivery.properties** file indicates the data that can be included in the message. These numbers correspond to the numbers within the curly brackets in the Short Descriptions. When the Track message is generated, the actual values in the call data are inserted in the locations designated by these placeholders in the Short Description.

IMPORTANT Be careful not to introduce any trailing spaces following a value in these files; trailing spaces impair parsing and are very difficult to troubleshoot.

You can also change the terminology used for the call direction, type, and disposition by editing the values following the EQUAL SIGN (=) in the terminology key at the bottom of the file.

DO NOT modify the values preceding the EQUAL SIGN.

To change the subject line of Policy messages

1. Open the **delivery.properties** file in a text editor. The file is located at the root of the ETM Server installation directory and is available from the **Global Configuration** section of the **ETM Server File Management Tool**.
2. The subject line is formatted in the file as follows:

Voice Firewall Rules

```
TeleWallRuleFiredShortDesc=\
{7} Call of Type {6} From {2} to {3} fired
Firewall rule {1} of policy {0}: {8}
```

AAA Services Voice Firewall Rules

```
AAARuleFiredShortDesc=\
{7} Call of Type {6} From {2} to {3} fired AAA
Services Firewall rule {1} of policy {0}: {8}
User: {21}
```

Voice IPS Rule Breaches

```
IPSBreachSingleLineFormat = IPS Breach
Occurred. Rule {3} of Policy {2} on Server
{1}: {4}

IPSBreachMultiLineFormat = IPS Breach Occurred.
Rule {3} of Policy {2} on Server {1}\nComment:
{4}
```


3. To modify the subject line, do any of the following:
 - Delete the index placeholders for text that you do not want to include.
 - Edit the text between the bracketed numbers.
 - Add additional text and bracketed numbers that correspond to the key for the type of Rule.

For example, if you do not want the called and calling phone numbers to appear in the subject line of Voice Firewall Track messages, delete the text that is shown underlined and italicized in the example below.

```
{7} Call of Type {6} from {2} to {3} fired
telecom firewall Rule {1} of Policy {0}: {8}
```

The description then appears as follows:

```
{7} Call of Type {6} fired firewall Rule {1} of
Policy {0}: {8}
```

Based on this example, the subject line would appear similar to the following:

```
Allowed Call of Type Modem fired firewall
Rule 8 of Policy MODEM WATCH: Allow and log
all outbound modem calls.
```

4. Save the file.
5. Restart the ETM Server for the change to take effect.

Formatting the Access Code Set Distribution Email

The subject and content of Access Code Set distribution emails are defined by a file named **delivery.properties**, located in the ETM System installation directory.

The Access Code Set distribution email can be formatted in the section that begins:

```
# These items are for formatting the Access
Code Set distribution email
```

To format the Access Code Set distribution email

1. Open the **delivery.properties** file in a text editor. The file is located at the root of the ETM Server installation directory and is available from the **Global Configuration** section of the **ETM Server File Management Tool**.
2. To edit the subject line of the email, edit the text after:
ACSDistribution_Subject=
3. To edit the message body of the email, edit the text after:
ACSDistribution_Body=\

“\n” represents a carriage return.

4. You can add additional text and the bracketed numbers corresponding to the key in **delivery.properties**:
 - {0} = Access Code Set Name
 - {1} = Access Code Set Comments
 - {2} = Access Code
 - {3} = Access Code Modified Date
 - {4} = Directory Listing Last Name
 - {5} = Directory Listing First Name
 - {6} = Formatted Name (Directory Listing First Name and Last Name)
 - {7} = Current Date

For example:

```
Hello, {6}.\n\n\
```

```
    This is an automated message from the ETM
System. On {3,date,MM/dd/yyyy} at
{3,date, hh:mm:ss a}, the following Access
Code was assigned to you: {2}
```

provides a message similar to the following:

```
Hello, John Smith.
```

```
    This is an automated message from the ETM
System. On 08/20/2005 at 12:03:56, the
following Access Code was assigned to you:
2584
```

Changing the Format of Diagnostic Messages

The format of diagnostic messages is specified in the **delivery.properties** file. The file is located at the root of the ETM Server installation directory.

Each of the items that can be inserted into a diagnostic message is listed in the section that begins:

```
# These items are for formatting diagnostic
messages.
```

To change the format of diagnostic messages

1. On the ETM Server computer, open the **delivery.properties** file in a text editor. The file is located at the root of the ETM Server installation directory and is available from the **Global Configuration** section of the **ETM Server File Management Tool**.

2. Locate the following section:

```
singleLineFormat = {0} Reported from: {2}
multiLineFormat = {4,date}: {2} reported {0}
```

3. Do any of the following:
 - Replace the bracketed numbers in the section with the number of the item that you want displayed in diagnostic messages.
 - Add additional text and/or bracketed numbers.

See the **Key to Indexing** section of the file for definitions of the bracketed numbers.

4. Save the file.
5. Restart the ETM Server for the change to take effect.

Changing the Number of Directory Listings Retrieved per Page

By default, 100 listings are retrieved per page when you perform a search for Directory Listings. However, you can specify a different number per page. This setting applies at the ETM System Console level, so the value applies to all connections to any Server from that ETM System Console.

To change the number of listings retrieved per page

1. Open the file **ETMSystemConsole.cfg** in a text editor. The file is located at the root of the ETM System installation directory and is available from the **Global Configuration** section of the **ETM Server File Management Tool**.
2. Locate the line that reads:


```
# Java Switches to supply to the Java Virtual Machine.  
  
Switches=-client -Xmx200M -  
Dsun.java2d.noddraw=true
```
3. At the end of that line, type a space and then type:


```
-DdirTool.QueryResultsLimit=x
```


where x is an integer that defines the number of listings per page.
4. Save the file.
5. Restart the ETM System Console if running.

Mapping Directory Fields to Default LDAP Attribute Fields

The **DefaultLDAPMappings.properties** file maps fields in the Directory Manager to LDAP attributes fields. These mappings provide the default values used when you create a new LDAP Import Set. This file is located at the root of the Management Server installation directory. The file contains the following mappings:

```
LAST_NAME=sn  
FIRST_NAME=givenName  
PHONE_NUM=telephoneNumber  
SITE=l  
DEPT=departmentNumber  
LOCATION=roomNumber  
EMAIL=mail  
MAIL_CODE=postalCode
```

You can map other Directory fields to LDAP attributes fields using the key in the file or change these defaults. For example, you can map the customizable fields USER1, USER2, and USER3 in this file to LDAP attributes fields, and rename them in the **ETM Server Properties Tool** (DirListUser1Label, DirListUser2Label, and DirListUser3Label) to match the LDAP name.

For details about editing the customizable fields, see “Changing User-Defined Directory Listing Field Labels” in the *ETM® System Administration and Maintenance Guide*.

Limiting the Number of Recorded CDR Records in a Single File

When recording SMDR data to a file, the recording mechanism locks the file until the maximum record count is reached (10,000). While the file is locked for writing, the CDR importer cannot import the file. This is intended behavior. However, in low-volume environments, the amount of time the file is locked to reach the max record count may be unacceptable. If a smaller count is needed, add the following command-line switch to the # Java switches to supply to the Java Virtual Machine line in the **ETMManagementService.cfg** file and then restart the Server:

```
-Dsmdr.RecorderRecordsPerFile=<value>
```

Variables in npconfig.properties

The **npconfig.properties** file specifies the format of the numbering plan for country codes and emergency numbers. This file is located at the root of the Management Server installation directory. Do not edit these values unless instructed to do so by SecureLogix Customer Support.

The **npconfig.properties** file contains the following values:

- The classes to be loaded that relate to numbering format.
- The default formatter class if a specific country mapping is not specified below.
- The mapping of specific country codes to a specific formatter.
- The number of emergency numbers in the default emergency group.
- The format of an emergency number.

Variables in twms.properties

The **twms.properties** file provides parameters used by the ETM Server. Certain parameters are present in the **twms.properties** file by default and others can be added depending on your system configuration; therefore, your **twms.properties** file may not contain all of the parameters listed below.

The **twms.properties** file is read by the ETM® System hierarchically. any parameters set in

<INSTALL_DIR>/ps_<INSTANCE_NAME>/twms.properties
will override any value set in
<INSTALL_DIR>/twms.properties.

The **twms.properties** file can be accessed from the **ETM Server File Management Tool**. The global file can be accessed from the **Global Configuration** section; in multi-instance installs, the

instance-specific file can be accessed from the **Instance Configuration** section.

The following parameters can appear in the **twms.properties** file.

- **_TWMSLockPath**—The location and name of the file that is placed on disk as a method of forcing only one Management Server to run at any one time. The default is **ps/#TWLOCK**.
- **ClientEncryptionEnabled**—Specifies the level of encryption between the ETM Server and the client tools. This setting does not affect encryption between any other ETM System components, including Server-to-Card or NFAS communication. The default is 1.

Valid values are:

0 = No encryption
1 = DES encryption
2 = Triple DES encryption

This setting takes affect at Management Server start up, and enables/disables encryption for ALL client connections (not a client-by-client basis). Encryption between the ETM Server and client tools can be resource intensive. This is especially noticeable when the Span state is changing frequently and when the **Call Monitor** is open.

- **ClientPassphrase**—The passphrase the must be in sync between the client tools and the ETM Server. See the file for the default. The passphrases in the twms.properties file can optionally be encrypted. See “Encrypting Values in the twms.properties File” in the *ETM® System Administration Guide* for details.
- **DatabaseNumConnections**—The number of allowed database connections. The default is 10.
- **DatabasePassphrase**—The passphrase to log into the database. The passphrases in the twms.properties file can optionally be encrypted. See “Encrypting Values in the twms.properties File” in the *ETM® System Administration Guide* for details.
- **DatabaseURL**—The URL of the database. The default is **jdbc:oracle:thin:@127.0.0.1:1521:etm**
- **DatabaseUserid**—The user ID to log into the database.
- **DebugFileLocation**—Location where the debug data for SMDR is placed. The default is **ps/debug**.
- **DirectoryRepository**—The folder that contains software packages, dialing plans, error/debug logs, exported instances, and SMDR parse files. The default is **ps/directory**.

- **DispatcherPort**—The port from which a client will connect to initiate a data communication socket with the Management Server. The default is 6991.
- **InitialDatabaseConnectTimeout**—The number of seconds to try to make an initial connection to the database before shutting the Management Server down. During initial connection, the Management Server attempts to connect to the database every 5 seconds until a connection is made or the timeout is reached. The default is 60 seconds.
- **Instance**—The data instance name used by the ETM Server. The default is **etm**.
- **JDBCDriver**—The JDBC Driver class name. The default is `oracle.jdbc.driver.OracleDriver`.
- **NumberConcurrentReports**—The maximum number of reports the Report Server can run simultaneously. This includes both scheduled and ad hoc reports. The default is 5. *(Applies to the Report Server; edit the file on the Report Server computer, if the Management Server and Report Server are on different computers.)*
- **NumberConcurrentScheduledReports**—The maximum number of scheduled reports the Management Server can run at the same time. This does not affect ad hoc reports. This value should be less than or equal to the **NumberConcurrentReports** value. The default is 1. *(Applies to the Management Server; edit the file on the Management Server computer, if the Report Server and Management Server are on different computers.)*
- **NumHistorizedPolicies**—The number of historized Policies to retain before purging the oldest. The default is 20.
- **Passphrase**—The DES passphrase. The passphrase must be in sync between the appliance and the Management Server, because the negotiation is always encrypted. See the file for the default. The passphrases in the `twms.properties` file can optionally be encrypted. See “Encrypting Values in the `twms.properties` File” in the *ETM® System Administration Guide* for details.
- **PersistTimerMSec**—This is the number of milliseconds between persists of the log data. Increasing this number lessens the amount of disk access by the ETM System, but increases the amount of time for logs to be sent to disk and the client tools. The default is 5000.
- **PolicyListingPreloadLimit**—The maximum number of directory listings in an installed Policy to preload at startup of the ETM Server. Larger numbers increase ETM Server startup time, but may reduce the time necessary to open an installed Policy for

editing or installation. An invalid value defaults to 200. The default is 200.

- **Port**—This is the port number that the Management Server uses to receive connections from the Cards. The default is 4313.
- **RegistryPassphrase**—The passphrase used to encrypt communication to the RMI registry. The passphrase must be in sync between the client and the ETM Server. See the file for the default. The passphrases in the twms.properties file can optionally be encrypted. See “Encrypting Values in the twms.properties File” in the *ETM[®] System Administration Guide* for details.
- **ReportDispatcherPort**—The port from which a client connects to initiate a data communication socket with the Report Server. The default is 6992.
- **ReportServerNumPorts**—Specifies whether Report Server port assignment should be assigned or automatic. If this property is set to zero or is left out, port assignment happens automatically (i.e., anonymous ports are used). Otherwise, it should be set to 1. The default is 0.
- **ReportServerStartPort**—The port by which client tools connect to the Report Server. If this property is set to zero or left out, port assignment happens automatically (i.e., anonymous ports are used). The default is 0.
- **RMIPort**—The port on which the Management Server creates an RMI registry to which the clients connect. The default is 6990. If you change this value, be sure to update the ETM Server connection information for each Client that connects to this Server.
- **RMITime**—The number of milliseconds that the Management Server and Report Server sleep between polling the RMI registry to determine if the registry is still available. If the registry is destroyed, the Management Server and/or the Report Server are unavailable until one of them “wakes up” (if either one is still running) and recreates the registry. The default is 60000 ms.
- **ShutdownDelay**—The number of milliseconds of continuous inactivity to wait before shutting down the Report Server. The default is 60000 ms. (The Report Server automatically restarts at the next report retrieval request.)
- **SoftwareRepository**—Location of the Card software packages. The default is ps/software_repository.
- **SpanConnectivityCheckInterval**—The interval at which Span health is verified. The system event “Extended ETM Application Disconnect Detected” is sent to the **Diagnostic Log** when a Card or Span has been disconnected from the ETM Server in excess of this threshold. The default is 300000 ms. See also **SpanConnectivityCheckState**, below.

- **SpanConnectivityCheckState**—Setting to determine the behavior of the **SpanConnectivityCheckInterval**, above. Valid values are:
 0 = Never Check, never notify (not recommended)
 1 = Check Always, report only once per sensor
 2 = Check Always, report every disconnect, every check.
 The default is 2.
- **StandbyReinitTime**—The number of seconds to wait to auto-reinitialize the ETM Server when it is in standby mode. The default is 60 sec.
- **SystemErrorPersistentStoreLocation**—The location and base name of the System Error file(s). The system adds the current date (yyyyMMdd) to the filename. The default is **ps/errors/SystemError.data**.
- **TWMSObjectNumPorts**—If this property is set to zero or left out, port assignment happens automatically (i.e., anonymous ports are used). Otherwise, this should be set to 1. The default is 0.
- **TWMSObjectStartPort**—The port by which client tools connect to the Management Server. If this property is set to zero or left out, port assignment happens automatically (i.e., anonymous ports are used). Note that port assignment is only necessary when using a firewall to restrict incoming traffic. The default is 0.
- **TWMSPersistentStoreLocation**—The name of the file that stores the Management Server data. The default is **ps/twms/TWMS.data**.

A PDF version of the ETM[®] Database Schema is provided with your ETM Software (on the software CD, in the Documentation directory under the ETM System installation directory, and on Windows, via the **Start** menu shortcut).

Opening the ETM[®] Database Maintenance Tool

Using the ETM[®] Database Maintenance Tool

The ETM Database Maintenance Tool enables you to perform the following tasks:

- Create, delete, import, and export data instances.
- View, repair, clear, create, and delete tables in the database.

The ETM Database Maintenance Tool is typically installed on the Management Server computer, but can also be installed on each computer where a remote ETM System Console is installed. For installation instructions, see “Installing the ETM[®] Software” in the *ETM[®] System Installation Guide*.

To open the ETM Database Maintenance Tool

- Do one of the following:

Windows

- Click **Start | Programs | SecureLogix | ETM System Software | Utilities | ETM Database Maintenance Tool**.

Solaris

- Execute the following script, located in the ETM System installation directory on the computer where the **ETM Database Maintenance Tool** is installed:

ETMDBMaintTool

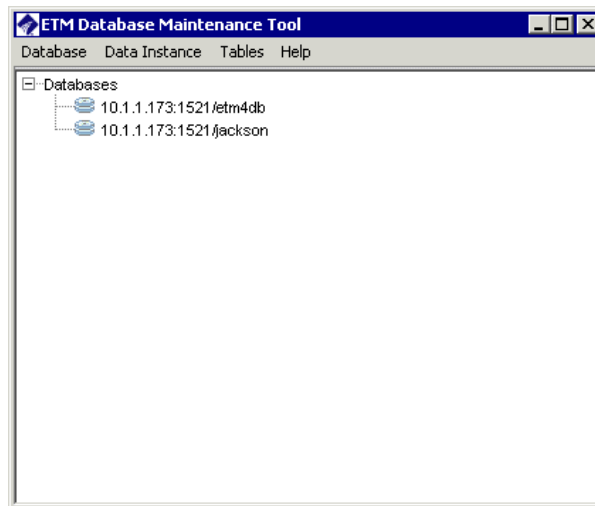
For instructions for creating the ETM Database object, see “Creating a Database Object” on page 28.

Logging in to the Database

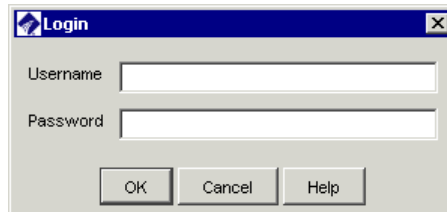
See “Creating a Database Object” on page 28 for instructions for creating a database object.

To log in to the ETM Database

1. Open the ETM Database Maintenance Tool. (See “Opening the ETM® Database Maintenance Tool” on page 26.)








2. In the **Databases** Tree, right-click the database used by this Management Server, and then click **Connect**. The **Login** dialog box appears.



3. In the **Username** box, type the username that authorizes the ETM Database Maintenance Tool to connect to the database. The username is listed in the **twms.properties** file on the line that reads DatabaseUserid.
4. In the **Password** box, type the password associated with the specified username. The password is listed in the **twms.properties** file on the line that reads DatabasePassphrase.
5. Click **OK**.

The ETM Database Maintenance Tool connects to the database and verifies each of the tables in the database.

When verification is complete, an icon appears next to each table, indicating its status:

Icon	Meaning
	Indicates the table is valid.
	Indicates an error in the table. Right-click the table, and then click Repair Table to correct the problem.
	Indicates a missing expected table. Right-click the table, and then click Create Table to create the table.
	Indicates an unknown table. These are typically temporary tables created during database operation, or tables created by DBAs rather than by the ETM System. These do not represent an invalid database state and does not impair system operation. Contact SecureLogix Customer Support before deleting any tables.
	Indicates views and temporary tables created and managed by the ETM Management Server.

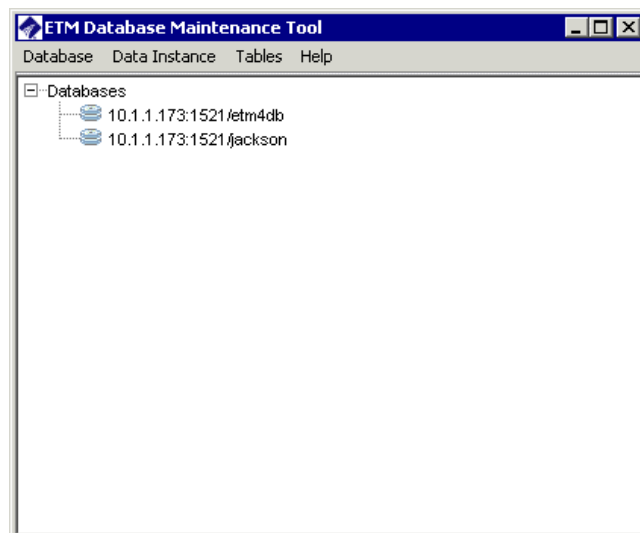
Creating a Database Object

To enable the ETM Database Maintenance Tool to connect to the ETM Database on the DBMS, create a corresponding Database Object that contains the necessary connection information.

To create a new Database Object

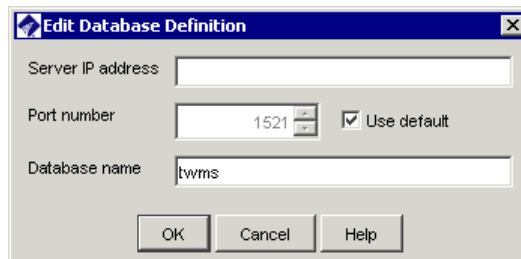
1. Open the ETM Database Maintenance Tool.

The Management Server uses information in its **twms.properties** file to locate and access the database denoted by the Database Object.



2. Click **Database | New**, or right-click **Databases**, and then click **New**.

The **Edit Database Definition** dialog box appears.



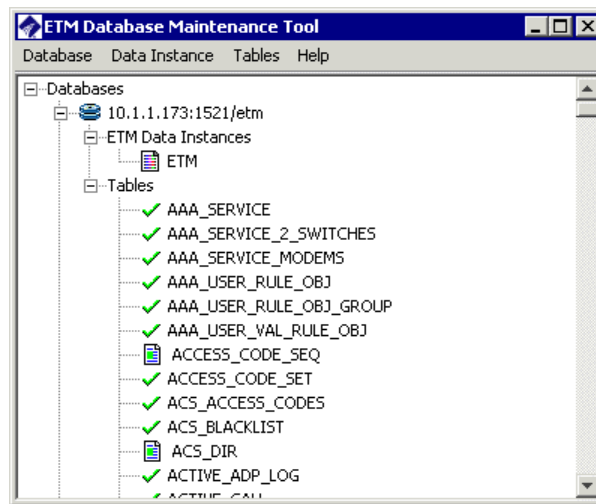
3. Type the following information:

Server IP address—The IP address of the computer on which the DBMS is installed.

Port number—The port on which the DBMS accepts connection requests.

Database name—The name of the database you created on your DBMS.

4. Click **OK**. The database appears in the tree.



Deleting a Database

Deleting a database only deletes the icon that enables the ETM Database Maintenance Tool to connect to the database. It does *not* delete the actual database or any tables, instances, or data.

To delete a database

- In the **Databases** tree, right-click the database, and then click **Delete**.

Disconnecting from a Database

To disconnect from a database

- Right-click the applicable database in the **Databases** tree, and then click **Disconnect**.

Working with Data Instances

Each Management Server stores its data in a data instance within the ETM Database. This enables multiple Servers to store their data in the same database. The data instance that a Server uses is specified in the **twms.properties** file in the Server installation directory. Exports are saved in the following directory:

<INSTALL_DIR>\ps\maint\exports

You can use the ETM Database Maintenance Tool to create, delete, import, and export data instances. |



CAUTION It is recommended that you stop the Management Server while performing any of the data-instance maintenance steps described below.

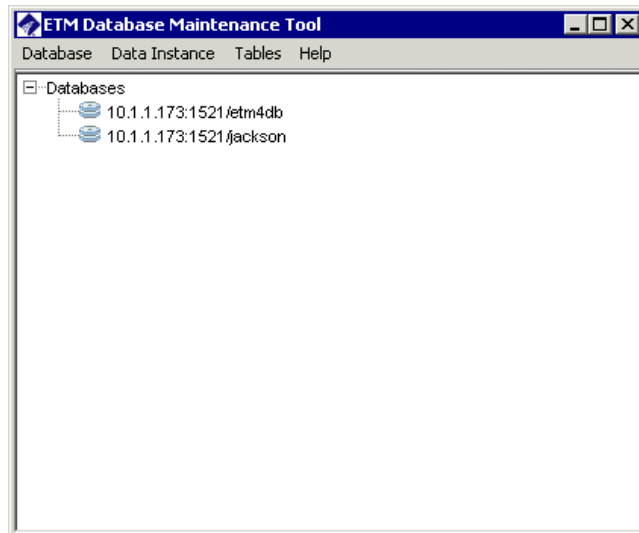
Exporting a Data Instance

The procedure below can be used to export data instances. For example, you might use this procedure if you are preparing to perform upgrade procedures on your DBMS or want to move the ETM Database to a different DBMS. See “Importing an Exported Data Instance” on page 32 for instructions for importing previously exported data instances.

To export a data instance

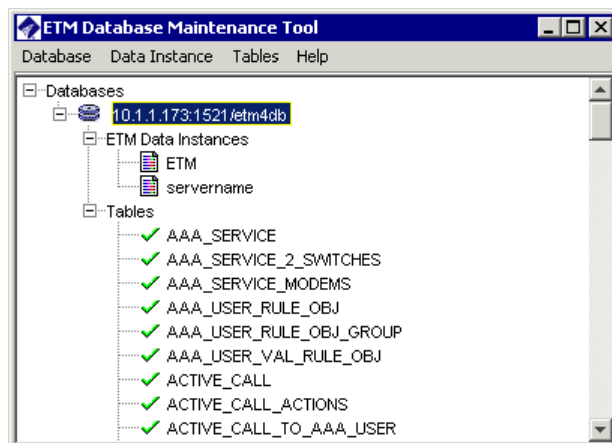
1. Determine where to save the export file. Depending on the amount of data in the data instance, exported instances can be very large (400MB or more) so be sure adequate hard drive space is available.
2. Open the ETM Database Maintenance Tool. (See “Opening the ETM® Database Maintenance Tool” on page 26 for instructions.)

The ETM Database Maintenance Tool appears.

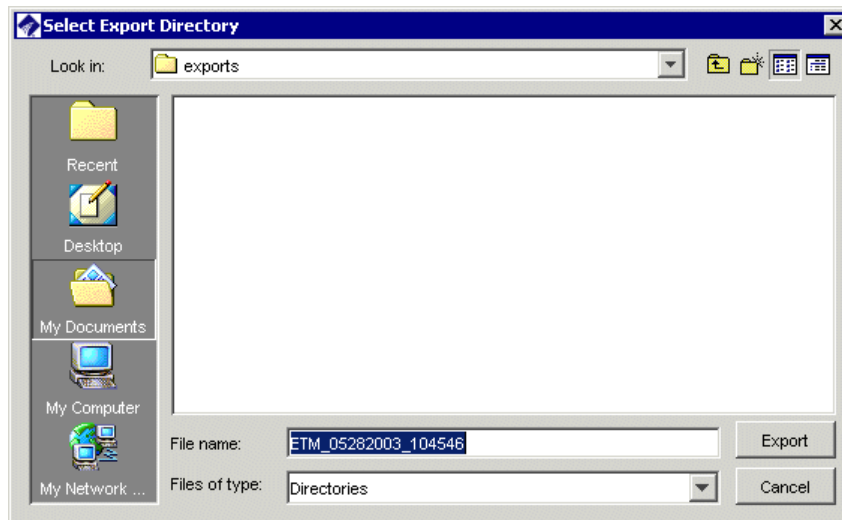


IMPORTANT If the ETM Database Maintenance Tool you are using has not yet been used to connect to the database, the database does not appear in the list. See “Creating a Database Object” on page 28 before continuing with this procedure.

3. Right-click the database that contains the instance you want to export, and then click **Connect**. The database is represented by an icon and the IP address, port, and database name.
4. The **Login** dialog box appears. Type the username and password that the Management Server uses to connect to the database, and then click **OK**. This information can be viewed in the **twms.properties** file on the Management Server computer.
5. The ETM Database Maintenance Tool connects to the database and verifies each of the tables in the database. This may take a few minutes. When verification is complete, a list of all the data instances in the database appears.



6. Right-click the data instance to be exported, and then click **Export Instance**. The **Select Export Directory** dialog box appears.



7. In the **File Name** box, type a file name for the directory that is to contain the exported data instance, or leave the default. The file name defaults to the following format:
instancename_mmddyyyy_hhmmss.
8. By default, exports are saved in the following directory:
<INSTALL_DIR>/ps/maint/exports
 - To select a different directory, next to the **Look in** box, click the down arrow, and then select the applicable directory. Be sure to select a location with adequate available hard drive space.
9. Click **Export**. The export begins and a progress indicator appears.

The time needed to complete the export is directly related to the amount of data in the data instance. A large data instance may take more than 30 minutes to export and may generate a directory containing more than 400 MB of data files.

Importing an Exported Data Instance

You cannot import data into an existing data instance. You must import the data as a new data instance and then set the imported data instance as the default for this Management Server.

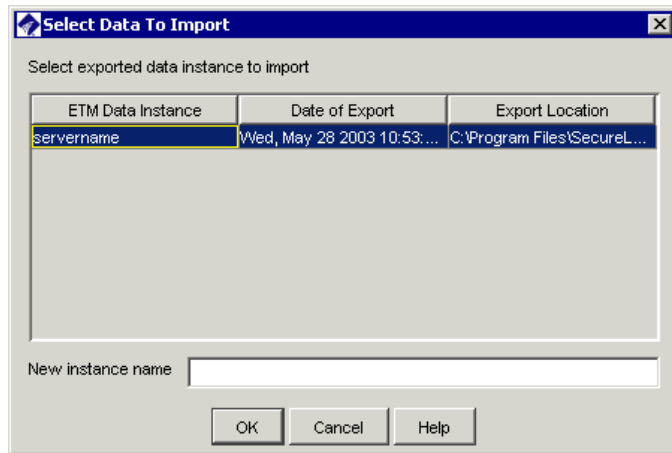
If the data instance that you want to import is stored on a network drive or other storage media, you must copy the exported instance to the **ps\maint\exports** directory of the ETM System installation directory on the client computer.

See also “Exporting a Data Instance” on page 30.

To import a data instance

1. Open the ETM Database Maintenance Tool.
2. Log in to the database. (See “Logging in to the Database” on page 27 for instructions, if necessary.)
3. Right-click **ETM Data Instances**, and then click **Import Instance**.

The **Select Data to Import** dialog box appears, listing the data instances available for import.



4. In the **Select exported data instance to import** area, click the instance to import.
5. In the **New instance name** box, type the name to use for the imported instance. An instance name can contain up to 20 letters and/or digits, but no spaces or special characters.
6. Click **OK**. The data instance is imported into the database and appears under the specified name in the **Data Instances** tree.

Setting a Data Instance as the Default

When you set a data instance as the default, the ETM Database Maintenance Tool modifies the **twms.properties** file with the information needed to associate the Management Server with the data instance. Note that the file on the client computer is modified. If the Management Server is not on the same computer, either copy the **twms.properties** file from the client to the Management Server computer, or manually modify the file.

The following sections of the file (shown here with sample values) specify the database connection information:

```
#####  
## The instance name  
Instance=ETM  
#####  
## The URL of the database  
DatabaseURL=jdbc:oracle:thin:@10.1.1.81:1521:ETM  
#####  
## The user id to log into the database  
DatabaseUserid=etmuser  
#####  
## The passphrase to log into the database  
DatabasePassphrase=etmuser  
#####
```

To associate a data instance with an Management Server

- Do one of the following:
 - If the ETM Database Maintenance Tool is installed on the same computer as the Management Server, while connected to the ETM Database, simply right-click the correct data instance and select **Set as default**.
 - If the ETM Database Maintenance Tool and Management Server are installed on separate computers, you can manually edit the sections of the **twms.properties** file on the Management Server computer, or copy the file from the client to the Management Server.

Deleting a Data Instance



WARNING When you delete a data instance, all of the data corresponding to that instance is permanently removed from the database and cannot be recovered. Contact SecureLogix Customer Support before deleting a data instance.

To delete a data instance

- In the ETM Database Maintenance Tool, while connected to the applicable database, right-click the data instance, and then click **Delete**.

Creating a New Data Instance

Each Management Server uses a separate data instance. This enables data from multiple Servers to be stored in the same database. However, it is strongly recommended that only one data instance be used per database schema.

To create a data instance for a Server

1. On the main menu, click **Data Instance | New Instance**. The **ETM Data Instance Edit** dialog box appears.

If you are using multiple Management Server application instances on the same computer, you must use the **<instance_id>** of the application instance as the data instance name.

2. In the **ETM data instance name** box, type a unique identifier for this data instance.
3. When you create the data instance for a Management Server, you also define the initial password for the default **admin** account for that Server. The **admin** username and password is used to initially log in to a newly installed Management Server. You can change this password in the **User Administration Tool** in the ETM System Console. For instructions, see “Changing the Password for An ETM System Account” in the *ETM® System Administration and Maintenance Guide*.

In the **Admin password** box, type the initial password for the default **admin** user account on the Management Server. When you log in to this Management Server via the ETM System Console, you use the username **admin** and the password you specify in this dialog box.

4. In the **Confirm password** box, type the same password again to confirm it.
5. In the **Locale** box, select the locale where the ETM System is installed. This populates the database with certain locale-specific default values.
6. In the **Allowed Client IP Address** box, type the initial IP address from which ETM Client Tools are allowed to connect to the Management Server that will use this data instance. Client Tools installed on the same computer as the Management Server are always authorized; you do not need to add their IP address. You can authorize other IP addresses via the **Server Administration Tool** in the ETM System Console.
7. Click **OK**. The data instance is created and its name appears under the **ETM Data Instances** node.

Managing Tables

The procedures below explain how to use the ETM Database Maintenance Tool to view, repair, delete, create, and clear ETM Database tables.



WARNING Improper use of the ETM Database Maintenance Tool to manage tables can result in impaired operation of your database or lost data. Contact SecureLogix Customer Support before using the ETM Database Maintenance Tool for any of the table maintenance tasks described below other than viewing tables.

Viewing a Table

To view a table

1. In the ETM Database Maintenance Tool, while connected to the applicable database, double-click a table.

The **Table Properties** dialog box for the selected table appears.

Status	Index	Name	Type	Nullable	DB Index	DB Name	DB Type	DB Null...
✓	1	platform...	char(32)	false	1	PLATFO...	char(32)	false
✓	2	twms_n...	varchar(...	false	2	TWMS_...	varchar(...	false
✓	3	model	integer	false	3	MODEL	decimal(...	false
✓	4	encrypt...	integer	true	4	ENCRYP...	decimal(...	true
✓	5	time_zone	varchar(...	true	5	TIME_Z...	varchar(...	true
✓	6	platform...	varchar(...	true	6	PLATFO...	varchar(...	true
✓	7	netmask	varchar(...	true	7	NETMASK	varchar(...	true

Status	Columns	DB Columns

Primary Key

Primary Key <unnamed> (platform_oid) DB Primary Key ✓ ETM_PLATFORM_PK (PLATFORM_OID)

Close Help

2. The **Description** tab of the **Table Properties** dialog box shows the following information:

- **Columns** area:
 - **Status**—the status of each column:
 - ✓ indicates a valid column.
 - ✗ indicates an invalid column.
 - **Index, Name, and Type**—expected values.

Each row in the **Columns** area represents a column in the Oracle database.

- **DBIndex**, **DBName**, and **DBType**—the corresponding values that actually exist in the database.
 - The **Indices** area shows the indices for the table and their status. (Not all tables have indices; if the table has no index, this area is blank):
 - **Status**—the status of each index:
 - ✓ indicates the index is present.
 - ✗ indicates the index is missing.
 - **Columns**—the expected columns of the index.
 - **DB Columns**—the columns of the index in the database. (If an index is expected but missing, the word <missing> appears.)
 - **Primary Key** area:
 - **Primary Key**—the column expected as the primary key for the table. Not all tables have a primary key; if the table has no primary key, this area is blank.
 - **DB Primary Key**—the status (✓ present or ✗ missing) of the primary key in the table, its value, and its name.
3. The **Data** tab of the **Table Properties** dialog box shows the data stored in the table.

PLA...	TVV...	MO...	ENC...	TIM...	PLA...	NET...	GA...	PAS...	ENA...	SEC...	SER...	SER...	SPA...
0102...	ETM	1	2	Ame...	10.1 ...	255...	10.1 ...	Secu...	Ena...	0	10.1 ...	4313	
0102...	ETM	1	2	Ame...	10.1 ...	255...	10.1 ...	Secu...	9F1 ...	0	10.1 ...	4313	
0202...	serv...	1	2	Ame...	10.1 ...	255...	10.1 ...	Secu...	9F1 ...	0	10.1 ...	4313	
0202...	serv...	1	2	Ame...	10.1 ...	255...	10.1 ...	Secu...	Ena...	0	10.1 ...	4313	
0102...	ETM	3	2	CST	10.1 ...	255...	10.1 ...	Secu...	9F1 ...	0	10.1 ...	4313	
0202...	serv...	3	2	CST	10.1 ...	255...	10.1 ...	Secu...	9F1 ...	0	10.1 ...	4313	
0202...	serv...	8	2	GMT	10.1 ...	255...	10.1 ...	Secu...	Ena...	0	10.1 ...	4313	
0202...	serv...	0	2	CST	10.1 ...	255...	10.1 ...	Secu...	9F1 ...	0	10.1 ...	4313	
0202...	serv...	4	2	CST	10.1 ...	255...	10.1 ...	Secu...	Ena...	0	10.1 ...	4313	4B85...

Attempting to Repair a Table

The ETM Database Maintenance Tool provides a **Repair Table** feature that attempts to repair simple errors in a table.



WARNING This feature is provided for troubleshooting by SecureLogix Support personnel. Contact SecureLogix Customer Support before attempting to repair any tables.

To repair a table

- Right-click the table, and then click **Repair Table**. The ETM Database Maintenance Tool makes a backup copy of the affected table and names it **<table_name>_tmp**, and then creates a new table with the correct structure with the original table name. The ETM Database Maintenance Tool then attempts to copy the data from **<table_name>_tmp** into the new, correct table. If the repair succeeds, **<table_name>_tmp** is deleted and a green check mark appears next to the table name. If the data cannot be successfully copied to the new table, **<table_name>_tmp** is not deleted, and the **Repair Table** operation fails. SecureLogix Customer Support can assist you with additional troubleshooting.

Clearing a Table



WARNING Clearing a table permanently deletes the data in the table, and may impair or prevent operation of your database. Do not clear any tables unless instructed to do so by SecureLogix Customer Support.

To clear a table

- In the **Tables** node of the ETM Database Maintenance Tool, right-click the table, and then click **Clear Table**.

Deleting a Table



WARNING Deleting a table removes the table and all of its data from the database, and may impair or prevent operation of your database. Do not delete any tables unless instructed to do so by SecureLogix Customer Support.

To delete a table

- In the **Tables** node of the ETM Database Maintenance Tool, right-click the table, and then click **Delete Table**.

Creating a Missing Table

Tables are unlikely to ever be missing.



WARNING Contact SecureLogix Customer Support before using the **Create Table** feature on a database that contains data.

To create a missing table

- Right-click the table, and then click **Create Table**.

Running Multiple Application Instances on One System

The ETM System supports multiple instances of the Report Server and the Management Server on a single computer. To use this feature, install a complete installation of the ETM software as you normally would, using the operating system-specific ETM software installers. Then follow the procedures below to configure each additional instance of the Management Server and Report Server. Up to 99 Management Server/Report Server instances can be created on a single computer, depending on system memory and processing power. **IMPORTANT** Use a separate database schema for each ETM Server's data instance. Create the necessary schemas before you begin this procedure.

Configuring Multiple Application Instances

The following steps are performed to configure each additional set of application instances:

1. Remove the default application instance. (Performed only once per computer.)
2. Add an additional instance of both the Management Server and Report Server.
3. Register the instances with the system startup facilities.
4. Modify configuration files.
5. Create the ETM Data Instance in the database.
6. Enable the application instance to connect to the database.

1. Remove the Default Application Instances

By default, the ETM System installers automatically install unnamed instances of the Management Server and Report Server applications. Before configuring the system to run multiple application instances, it is suggested that these unnamed application instances be removed to avoid confusion.

To remove the default application instances

Solaris

- Remove the instances from the S99ETMMS and S99ETMRS system startup scripts as follows:

Open a terminal window and change directories to **/etc/rc3.d**

Using a text editor, edit the system startup scripts and remove the following lines:

```
./ETMManagementServer &  
./ETMReportServer &
```

Windows

- Deregister the instances with the Service Control Manager as follows:

Open a command prompt window and change directories to the ETM System installation directory.

At the prompt, type:

```
AppManager /remove /type:both /id:default
```

2. Add Additional Instance(s)

To add an additional instance of both the Management Server and Report Server

1. Choose a unique identifier for the additional application instance. The identifier can consist of up to 20 upper or lowercase alphanumeric characters (a-z, A-Z, 0-9).
2. Create a data directory for the additional application instance as follows:
 - a. In the ETM System installation directory, create a copy of the **ps_skel** subdirectory.
 - b. Rename the copied subdirectory **ps_<instance_id>**. The folder name is case-sensitive. For example, if your instance is named **Houston**, rename the copied subdirectory **ps_Houston**.

3. Register the Instance(s) with System Startup Facilities

To register the additional instances with the system startup facilities

Solaris

- Edit the system startup script:

Open a terminal window and change directories to /etc/rc3.d

Using a text editor, edit the system startup script and type the following lines at the end of the file:

```
./ETMManagementServer <instance_id> &  
./ETMReportServer <instance_id> &
```

Windows

- Register the additional application instances with the Service Control Manager:

Open a command prompt window and change directories to the ETM System installation directory.

At the prompt, type:

```
AppManager /add /type:both /id:<instance_id>
```

4. Modify Configuration Files

You must also configure the Cards managed by each instance with the applicable Server port during out-of-the-box Card configuration.

IMPORTANT This section describes changing port numbers in the **twms.properties** file. On Windows, all of the port numbers that you specify should be above 5000 to prevent conflicts with other services and applications.

To modify configuration files

1. Open the following file:

```
<INSTALL_DIR>\ps_<instance_id>\twms.properties
```

2. Change the following port values so that they are unique to this application instance:

Port

RMIPort

DispatcherPort

ReportDispatcherPort

3. Modify the paths for the following values to use the newly created **ps_<instance_id>** directory by replacing **<instance_id>** in each path with the actual instance ID.

For example, if your instance ID is **Houston**, change

```
_TWMSLockPath=ps<instance_id>/#TWLOCK
```

to

```
_TWMSLockPath=ps_Houston/#TWLOCK
```

4. Modify the following paths:

_TWMSLockPath

SystemErrorPersistentStoreLocation

CoreFileLocation

TWMSPersistentStoreLocation

DebugFileLocation

DirectoryRepository

5. Edit **<INSTALL_DIR>\ps_<instance_id>\ETMReportService.cfg** so that the RMID_Port value is unique to this application instance.

5. Create the Management Server's Data Instance

To create the Management Server's Data Instance in the database

1. Open the ETM Database Maintenance Tool:

Solaris

Execute the following script, located in the ETM software installation directory: **ETMDBMaintTool**

Windows

Click **Start | Programs | SecureLogix | ETM System Software | Utilities | ETM Database Maintenance Tool**.

2. Log in to the schema you created for this ETM Server instance in the Database.
3. Create a data instance for this application instance, using the **<INSTANCE_ID>** as the name of the instance. The Data Instance must be named **<INSTANCE_ID>** because this value is automatically supplied to the Management Server and Report Server applications during startup. See “Creating a New Data Instance” on page 35 for instructions for creating the instance, if necessary.

6. Enable the Application Instances to Connect to the Database

The default **twms.properties** file in the root of the ETM System installation directory provides global database connection information that all of the Management Server and Report Server instances on this computer use to connect to the database.

To set the default instance

- In the ETM Database Maintenance Tool, right-click any ETM Data Instance, and then click **Set as Default**.

The required information is written to the **twms.properties** file. Although a Data Instance is also written to this file, it is ignored; each application instance uses its own Data Instance. By default, the database connection information in this file is in clear text. If you want the database connection information to be encrypted, see “Encrypting the Passphrases in the twms.properties File” in the *ETM® System Administration and Maintenance Guide*.

Customizing Database Settings

The database creation script, **oracle_install.pl**, creates instance-specific versions of the database templates. You may need to customize certain settings in these files; in some cases, you need to make the changes to these files before their section of the script executes.

For detailed procedures for creating the ETM database, see the instructions specific to your version of Oracle in the SecureLogix Knowledge Base at <http://support.securelogix.com>.

Customizing Database Settings in the init.ora file

Initialization parameters are used to optimize performance, set database defaults and limits, and specify names/locations of files. Many initialization parameters can be fine-tuned to improve database performance; other parameters should never be edited or should only be edited by an experienced Oracle DBA. The file **init.ora** in the directory **<ETM_DB_Directory>\pfile** contains values for your database configuration.

Change the Location of Control Files

Every database has a *control file*, which contains entries that describe the structure of the database, such as its name, the timestamp of its creation, and the names and locations of its data files and redo files. By default, all of the control files are installed in the same directory, which may not be desirable in a multi-disk system.

To change the location of control files

1. Locate the section that reads:

```
control_files = <path>
```
2. Edit the path as needed.

Set Multiblock Read Count Based on Installation Size

To set multiblock read count

1. Locate the section that reads:

```
db_file_multiblock_read_count = 8 # SMALL  
#db_file_multiblock_read_count = 16 # MEDIUM  
#db_file_multiblock_read_count = 32 # LARGE
```
2. Uncomment (delete the # from) the count that your database requires and comment out (add a # to) the other values.

Set Buffer Size

To set the buffer size

1. Locate the section that reads:

```
db_block_buffers = 14648 # RAM = 512 MB
#db_block_buffers = 31744 # 512 MB <= RAM <
2 GB
#db_block_buffers = 49152 # 2 GB <= RAM < 4
GB
#db_block_buffers = 63488 # RAM >= 4 GB
```

2. Uncomment the size that your database requires, and comment out the other values.

Set Shared Pool Size

To set the shared pool size

1. Locate the section that reads:

```
shared_pool_size = 16777216 # RAM = 512 MB
#shared_pool_size = 20971520 # 512 MB <= RAM
< 2 GB
#shared_pool_size = 33554422 # RAM >= 4 GB
```

2. Uncomment the size that your database requires, and comment out the other values.

For SNP Systems with More Than 1GB RAM

If your SNP system has more than 1 GB of RAM

1. Comment out the line that reads:

```
large_pool_size = 614400.
```

2. Uncomment the line that reads:

```
#parallel_automatic_tuning = true
```

Automatic Archiving

If archiving is enabled

1. Uncomment the line that reads:

```
# log_archive_start = true
```

2. Specify the archive directory by uncommenting the lines that read:

```
# log_archive_dest_1 = "location = <path>"
# log_archive_format =
%%ORACLE_ORACLE_SID%%T%TS%S.ARC
```

3. Edit the path, if different.

Enable Oracle Trace

The Oracle Trace reporting utility collects data for specific, predefined events. Oracle Trace is disabled by default. When Oracle Trace is enabled, your database may constantly generate trace data, causing your database to exhibit performance-related problems, such as poor query response time, aborted sessions, and database connection attempts that take a very long time.

To enable Oracle Trace

- Uncomment the line that reads:

```
# oracle_trace_enable = true
```

Specify the Directory to Store Trace and Alert Files

To change the directory to store trace and alert files

1. Locate the line that reads:

```
background_dump_dest = <path>
```
2. Edit the path as necessary.

Enable Resource Management

To enable resource management for the database

- Uncomment the line that reads:

```
# resource_manager_plan = system_plan
```

Customizing the Redo Logs, Tablespace, or Rollback Segments

The values and locations of the redo logs, system tablespace, rollback segments, temp file, and autoextend are specified in **create_db_instancename.sql** in the directory **<ETM_DB_Directory>\create**. These changes need to be made before the database creation scripts are run.

Customizing the Redo Logs

To edit the redo logs

- In the section that begins as follows:

```
REM * Creates the physical database. Feel  
free to customize the redo logs here.
```


Edit the locations and size as needed.

Adjust the Size of the System Tablespace

To edit the tablespace

- In the section that begins as follows:

```
REM*****ALTER SYSTEM TABLESPACE*****
```


Edit the values as needed.

Adjust the Size of the Rollback Tablespace

To edit the tablespace for rollback

- In the section that begins as follows:

```
REM *****TABLESPACE FOR ROLLBACK*****
```

Edit the values as needed.

Temp File and Autoextend

To edit the commands for the temp file and autoextend

- In the section that begins as follows:

```
REM*****TABLESPACE FOR TEMPORARY*****
```

Edit the values as needed.

Tablespace for Tools

To edit the commands for the tablespace for tools

- In the section that begins as follows:

```
REM***** TABLESPACE FOR Tools*****
```

Edit the values as needed.

Create More Rollback Segments

To create more rollback segments

1. Copy the lines that form the CREATE statement, from CREATE to the semicolon (;), as shown below:

```
CREATE PUBLIC ROLLBACK SEGMENT RBS0  
TABLESPACE RBS STORAGE ( INITIAL 64K NEXT  
64K MINEXTENTS 200 MAXEXTENTS 32765 );
```

2. Paste the copied lines once for each additional rollback segment, and then change the SEGMENT name (RBS0, RBS1, etc.).
3. Set the rollback segment online by adding an ALTER ROLLBACK SEGMENT line, following the example of the defaults. For example:

```
ALTER ROLLBACK SEGMENT "RBS4" ONLINE;
```


Dialing Plans

About Dialing Plans

Dialing Plans enable the Span to convert a *calling sequence* into a fully qualified, normalized phone number and provide call classification information. A calling sequence consists of phone number components, an associated IP subnet mask, and/or domain name. Phone number components include a prefix (such as an outside line access code), country code, NNP, NPA (area/city code), extension, and suffix (such as a PIN code).

The Dialing Plan serves the following purposes:

- Specifies the order in which components are expected to occur in a calling sequence, based on the direction of the call.
- Specifies the content and/or length of certain components. For example, if an outside-line access code must be dialed, the digits are specified in the Dialing Plan.
- Converts digits dialed from a specific IP address or domain into a fully qualified phone number.
- Adjusts the calling sequence appropriately if one or more components are missing (for example, prepends the local area code).
- Provides call and phone number classification information. This information is used to classify calls as local, long distance, international, information, toll-free or toll, and so forth. These classification labels can be used to define Service Type objects, which are used in cost accounting reports and Voice IPS Policies. See the *ETM® System User Guide* for instructions for defining Service Type objects, Billing Plans, and Voice IPS Policies.

Incorrectly configured Dialing Plan sections can prevent the ETM System from correctly recognizing phone numbers for Policy processing and cause incorrectly classified calls and unavailable phone numbers in reports.

IMPORTANT The Incoming and Outgoing Numbering Formats must be properly specified in the **Channel Map** tab of the **Span Configuration** dialog box for normalization to succeed. For details, see “Channel Map Tab” in the *ETM® System Installation Guide*.

Types of Dialing Plans

Each Span uses two Dialing Plans to identify and classify the called and calling phone numbers for each call:

- The **World Dialing Plan (WNP)** defines global dialing information that rarely needs to be updated. This includes information related primarily to recognizing and classifying long distance, international, toll, and toll-free calls.
- The **Local Dialing Plan (LNP)** defines dialing information specific to the location where the Appliance is installed. This information must be tailored during installation to suit the local dialing environment and may need to be updated periodically if the dialing environment changes. The LNP provides information that the Span uses to convert the string of digits in a called or calling phone number into the actual, fully qualified phone number.

The Dialing Plan Processor (DPP) on the Card reads in the LNP and WNP when the Card is booted up and when a new Dialing Plan is downloaded to it from the Management Server. Any section type can be used in either the WNP or the LNP; both Dialing Plans are read into memory at the same time and used concurrently in processing. In the default Dialing Plans, however, sections that are unlikely to change are placed in the WNP, while those that are likely to require tailoring for the Appliance locale are placed in the LNP.

Defining and Installing Dialing Plans

IMPORTANT Reliable Policy processing and enforcement does not occur until after the correct Dialing Plans are defined and installed on the Span. Each Span uses a Local Dialing Plan (LNP) specific to the Appliance locale and a World Dialing Plan (WNP) specific to the country where the Appliance is located.

Spans have default Local and World Dialing Plans installed that enable the ETM System to process calls. However, various call classification sections should be customized for the specific Appliance locale to ensure proper call classification (for example, local vs. long distance).

The following default LNP and WNP plans are provided:

- **AT_Default**—Austria
- **CA_Default**—Canada
- **DSN_Default**—Defense Switched Network (used by the U.S. Armed Forces)
- **FR_Default**—France
- **IT_Default**—Italy
- **NANP_Default**—United States
- **UK_Default**—United Kingdom
- **ZA_Default**—South Africa

Defining Dialing Plans

See “Defining Dialing Plan Sections” on page 64 for a detailed description of each type of Dialing Plan Section. Each section in the default Dialing Plans is preceded with an explanatory comments section to aid you in customizing those sections.

To define a Dialing Plan

1. Open the default **.LNP** file or **.WNP** file appropriate for your country in a text editor. Default Dialing Plan files are located in the Management Server installation directory. Dialing Plan files are located in the following directory:

<INSTALL_DIR>\ps\software_repository\ini

Define the appropriate sections according to your Appliance locale. See “Defining Dialing Plans” on page 51 for a detailed explanation of the components of each Dialing Plan file and instructions for modifying each section.

2. Save the file under any identifiable name in the same directory, with an **.LNP** file or **.WNP** extension. This extension must be capitalized in order to be recognized by the Management Server for installation.

IMPORTANT The updated Dialing Plan is not used for call processing until it is installed on the Span.

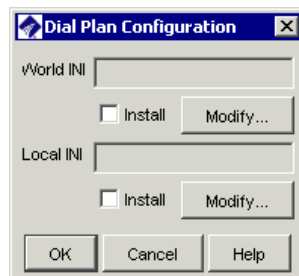
3. Install the Dialing Plan on the Span(s). See “Installing Dialing Plans on a Span” on page 51 for instructions.

Installing Dialing Plans on a Span

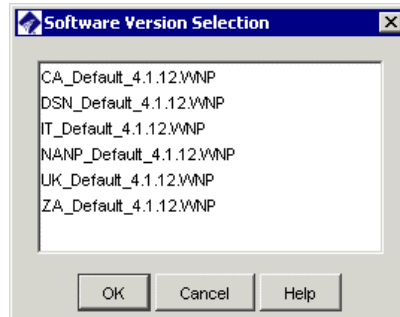
To install the Dialing Plans on one or more Spans

1. In the Performance Manager tree pane, do one of the following:
 - Right-click a Span, and then click **Manage Dial Plan**.
 - Hold down CTRL, click each Span on which you want to install the same Dialing Plan(s), and then right-click the selection, and then click **Manage Dial Plan**.

The **Dial Plan Configuration** dialog box appears.



2. To install the WNP:
 - a. Under the **World INI** box, click **Modify**. The **Software Version Selection** dialog box appears. Only **.WNP** files stored in the **ps\software_repository\ini** directory in the Management Server installation directory appear.



IMPORTANT If a Dialing Plan is modified on the Server, it must be reinstalled on the Span(s) before the changes take effect.

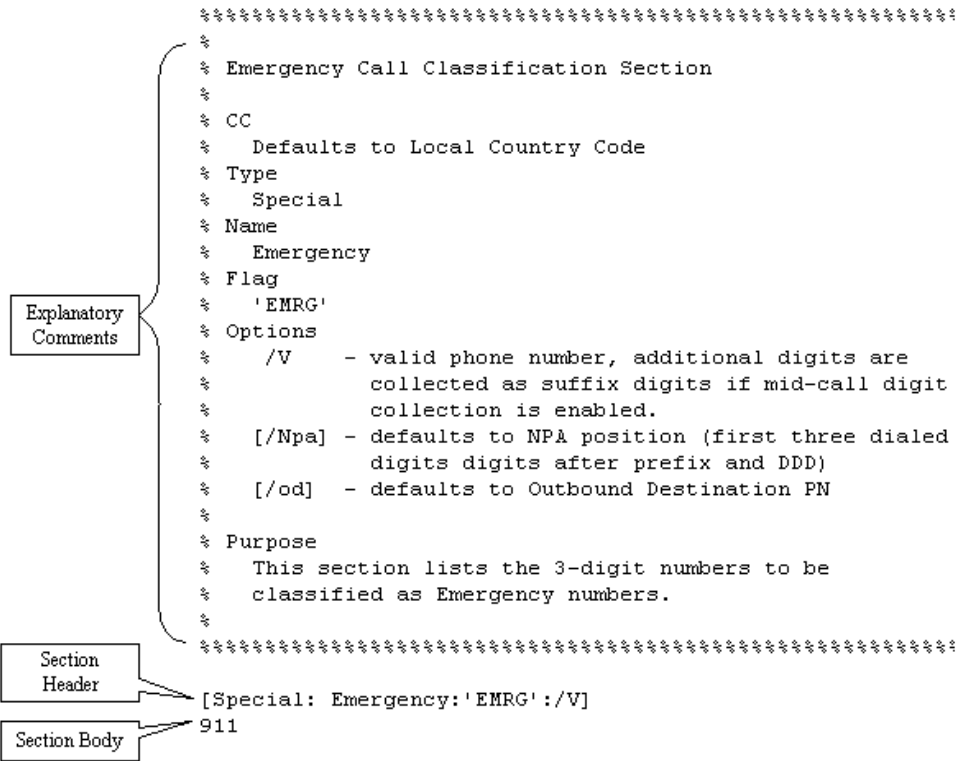
- b. Click the **.WNP** file that represents the Dialing Plan for long distance phone numbers for this Appliance, and then click **OK**.
3. To install the LNP:
 - a. Under the **Local INI** box, click **Modify**. The **Software Version Selection** dialog box appears. Only **.LNP** files stored in the **ps\software_repository\ini** directory in the Management Server installation directory appear.
 - b. Click the **.LNP** file that represents the Dialing Plan for local phone numbers for this Appliance, and then click **OK**.
4. In the **Dial Plan Configuration** dialog box, be sure that **Install** is selected under each box, and then click **OK**.

The Dialing Plan(s) is/are downloaded to the Span(s) and used immediately for new call processing.

Dialing Plan Contents

Dialing Plans consist of a set of sections that represent possible phone number components. Each section consists of a *section header* and *section body*. The default Dialing Plans included with your ETM System contain default sections that represent common situations. Each of these default sections is preceded by a comments area that describes the section.

A default Dialing Plan section is shown below.



Section Header The **Section Header** is enclosed in square brackets on the line above the section body. The fields in the section header are case-sensitive and separated by colons. A section header uses the following general format:

[Country Code:Type:Name:Label:Option]

Only **Type** is required, and the **Option** field does not apply to all types. Each Section Header component is explained in detail in “Dialing Plan Section Header Components” on page 54.

Section Body The **Section Body** provides the values against which the calling sequence is compared. The type of values depends on the section type. “Defining Dialing Plan Sections” on page 64 explains the contents of the Section Body for each Section Type.

The Section Body can contain any of the following:

- Phone Number characters (the digits 0-9, *, #)
- VoIP IP addresses, netmasks, or domain names
- Wildcard characters—**N** or **X** (not case sensitive). **N** or **n** matches any one of the phone number digits 0-9; **X** or **x** matches any one of the phone number characters. For example, **10NNNN** matches any number from 100000 to 109999. Wildcards cannot be used in ranges, CC, NPA, or NNP sections, or DDD sections that use a PRI TON option.
- Range indicator (..). For example, **210..212** represents the numbers 210, 211, and 212. Ranges must be in ascending order.
- A phone number component enclosed in curly brackets (**{ }**), for some sections. For example, **210 {402, 522}** specifies the exchanges 402 and 522 in the 210 area code.

Dialing Plan Section Header Components

Each of the possible components of the section header are described in detail below. Note that all section hHeader components are case sensitive.

cc	<i>(Optional)</i> The cc field specifies the country code to which the section applies. If the cc field is not defined, it defaults to the Span's local country code.
Type	<i>(Required)</i> The section type in the section header indicates what kind of information the section contains. Any section type can be used in either the WNP or the LNP; both Dialing Plans are read into memory at the same time and used concurrently in processing. In the default Dialing Plans, however, sections that are unlikely to change are placed in the WNP, while those that are likely to require tailoring for the Appliance locale are placed in the LNP. A detailed discussion of each type of section is provided in “Defining Dialing Plan Sections” on page 64.
Name	<i>(Optional)</i> The Name field is a user-definable identifier used to identify the section in error or warning messages in the Diagnostic Log . Some sections have default names. If no name is defined for a section, the Diagnostic Log refers to it as “unnamed section.”
Label	<i>(Optional)</i> The Label field provides call and phone number classification information that is useful in reports. Labels can include any character except single (') or double (") quote marks, up to 10 characters per label. Multiple labels can be used per header, up to 60

characters for all labels in the header. Some sections provide default explicit labels; others have implicit labels that are applied if you do not specify a label in the header—when this is the case, it is noted in the comments preceding the section.

Two types of labels are available, described in detail in the following sections:

- **Call labels** classify the call as a whole. These are used in Billing Plans to associate Service Types with costs and in Voice IPS Policies to base Rules on the Service Types of calls. See “Call Labels” on page 55 for more details.
- **Phone number labels** classify a called or calling number. See “Phone Number Labels” on page 56 for details.

To include multiple labels in a header:

- If a call matching a section should have both labels, separate the labels with **&&**. For example, (“LD” & & '101x') applies the call label LD and the phone number label 101x.
- If a call matching the section should have one or the other label, separate the labels with **||**. For example, (“LOC” || “LD”) applies either the call label LOC or the call label LD.

Call Labels

Call labels classify the call as a whole. Enclose call labels in double quotes (i.e., “LOC”). Call labels appear in the **Call Details** field of the **Policy Logs** and Reports. Multiple call labels can be applied to a given call. To specify two call labels for a given section, separate the labels with **&&**, for example, (“LD”&&”INTL”).

On inbound calls, the call label(s) applied is based on the Source number. If Source is unavailable, UNK appears in the **Call Details** field.

- On outbound calls, the call label(s) is based on the Destination number. If Destination is unavailable, UNK appears in the **Call Details** field.
- If no call label is explicitly defined for a call by the matched section(s), the call is labeled “LD” if the NPA of either the inbound source or outbound destination differs from the Span’s local NPA; otherwise, it is labeled “LOC.”
- Call labels for DSN calls are preceded by **DSN**.

Call labels are also used to define Service Types and Billing Plans.

The table below lists the default Call Labels in the NANP dialing plans and describes their meanings.

Call Labels	Meaning
DSN	DSN number
LOC	Local call
LD	Long distance call
FREE	Toll-free numbers (e.g., 1-800 numbers in the U.S.)
INTL	International call
UNK	Unknown relationship between Source and Destination number. Usually caused when inbound source or outbound destination number is unavailable (NOPN appears in the applicable PN label field).

Phone Number Labels

Phone number labels classify a called or calling number. Enclose phone number labels in single quotes (i.e., 'INFO'). The Phone Number Label for the calling number appears in the **Source Details** field of the **Policy Logs** and Reports. The Phone Number Label for the called number appears in the **Destination Details** field of the **Policy Log**.

The tables below list the default Phone Number Labels and describe their meanings.

PN Labels	Meaning
101x	The phone number is a 101x carrier service number (e.g., 1010220+).
800	The phone number represents a toll-free call (e.g., 1-800 in the U.S.).
ACI	(Italy) Road emergency car assistance (e.g. 116)
CLI	(UK only) The phone number is prefixed with a code to suppress calling line identification (CLI).
CLOCK	(UK, Italy) The speaking clock number (such as 4161) .
DID	The phone number was provided by Direct Inward Dialing service.
EMRG	The phone number is an Emergency number (i.e., 911 in the U.S.).
EXP	The phone number has been expanded as dictated by an Expand section in the LNP.
FORESTALE	(Italy) Corpo forestale (State Forestry Corps) (e.g., 1515).

PN Labels	Meaning
GUARDIA	(Italy) Guardia di Finanza (Financial Police) (e.g. 117).
INFO	The phone number is an Information number (i.e., 411 or 555-1212 in the U.S.).
INTLINFO	(UK) International directory enquiry (e.g., 153).
INTLOP	(UK) International directory assistance (e.g., 155).
MAP	The phone number was obtained from the Extension column of the Channel Map tab on the Span Configuration dialog box.
MARE	(Italy) Soccorso in mare (help at sea) (e.g. 1530).
METRO	The phone number is a local number in a foreign numbering plan area (FNPA).
NONEMRG	The phone number is a non-emergency assistance number (e.g., 311 in the U.S.).
NOPN	The phone number is unavailable (for example, a user blocked CPN).
OPER	The phone number was dialed with operator assistance.
PN	The phone number is a normal phone number.
PREP	The phone number is a preprocessed number.
SERV	The phone number is a Service number.
SMDR	The phone number was obtained from SMDR data.
TOLL	The phone number represents a toll call (e.g., 1-900 in the U.S.).
TOLLX	The phone number is a toll exchange number.
VSC	The phone number is prefixed with a vertical service code (*70, etc.).

DSN Codes

If the DSN Dialing Plan is used, any of the following access or route codes may be added to the PN label field:

DSN Access Codes	Meaning
FO	Flash Override
I	Immediate
F	Flash
R	Routine
P	Priority
LTN	Local Telephone Network

DSN Route Codes	Meaning
VDAT	Voice Data
DGD	Data Grade
HOTV	Hot Voice
HOTD	Hot Data
FTS	FTS line type
DDD	DDD line type

Compound Labels

You can also create compound labels by enclosing multiple call and/or phone number labels in parenthesis and separating each label with the logical operator symbols **&&** (meaning AND) or **||** (meaning OR):

- **&&** means calls matching the section receive both labels. For example, you might use the label (“INTL”&&’OPER’) to denote international, operator-assisted calls.
- **||** means calls that match the section receive the first label; calls that do not match receive the second label. For example, you might use the label (“LD”||’LOC”) so that calls that match the section are labeled LD (long distance); those that do not are labeled LOC (local).

Options

(*Optional*) Options are parameters that affect how the information in the section is processed. For example, the option **/fCC** can be used in Prefix and DDD sections to indicate that when a given calling sequence matches the section, the next component is the country code.

Some sections have implicit default options. For example, the DID section type defaults to the **/id** (inbound destination) Call Direction option. Applicable options depend on the section type; not all types have options.

The table below (continued on the following pages) lists and describes valid options and the section type(s) to which each applies.

Note: “Source” is the same as “calling party” and “Destination” is the same as “called party.”

Option Type	Purpose	Option	Effect
Call Direction (Applicable to all section types except Default and DID .)	Indicates the call direction(s) to which the section applies.	/id	Section applies only to inbound destination phone numbers.
		/is	Section applies only to inbound source phone numbers phone numbers.
		/od	Section applies only to outbound destination phone numbers.
		/os	Section applies only to outbound source phone numbers.
		/io	Section applies to both source and destination for both outbound and inbound calls.
Follow (Applicable to Prefix and DDD sections types. /fNUM and /fSUFEX also apply to the NPA section type.)	Indicates the next phone number component expected in a calling sequence that matches the section. If no Follow Option is specified for a Prefix or DDD section, /fNPA is the default; for an NPA section, /fNUM is the default.	/fCC	Country code follows this component.
		/fNPA	NPA follows this component.
		/fNUM	Number follows this component.
		/fSUFEX	Suffix follows this component.

(Options table, continued)

Option Type	Purpose	Option	Effect
Label (Applicable to all section types except Default .)	Indicates how labels in the section header are to be added to the Call and/or PN Label list. If no label option is specified, the label is added to the end of the respective list.	/Acall	Add Call label at end of Call label list.
		/Apn	Add PN label to end of PN label list.
		/AFcall	Add Call label at start of Call label list.
		/AFpn	Add PN label at start of PN label list.
		/Ocall	Overwrite the last Call label of the Call label list.
		/Opn	Overwrite the last PN label of the PN label list.
		/OFcall	Overwrite the first Call label in the Call label list.
		/OFpn	Overwrite the first PN label in the PN label list.
Match (Applicable to the Classify and Special section types.)	Specifies the phone number components to be compared with the section data. If no Match Option is specified, the Special section default is /Npa; the Classify section default is /Npa followed by an optional partial Number match.	/Npa	Only the NPA field is compared.
		/Num	Only the Number field is compared.
		/NN	The NPA and Number fields are compared.
Next (Applicable to the Classify section type only.)	Indicates whether the next Classify section should be examined after a call matches a Classify section. By default, classification stops when a match occurs.	/Next	Proceed to next Classify section, even if a match has occurred.
		/NMNext	Proceed to the next Classify section only if the call does not match the current section.

(Options table, continued)

Option Type	Purpose	Option	Effect
PRI TON (Applicable to Prefix and DDD section types.)	<p><i>Uppercase Options</i>—Used to interpret PRI TON by Spans that receive the specified TON value.</p> <p><i>Lowercase Options</i>—Used by PRI calls that receive a TON value, or other call types in which the DDD value is dialed.</p> <p>If no PRI TON Option is defined and the Span does not receive the component in the call data, that component is not present in the phone number compared against the Policy.</p>	/pcco	For non-PRI calls, indicates the section is to be evaluated if a DDD component was identified in the calling sequence. For PRI calls that receive a TON value, indicates the first entry in the section body represents the PRI Presubscriber Common Carrier Operator code.
		/PCCO	Defines the PRI Presubscriber Common Carrier Operator, used if the DDD component is not in the dialed digits.
		/pi	Entries are matched against the dialed digits of the DDD component as dialed. The first number specified in the list represents the PRI international code, used if the DDD component is not in the dialed digits.
		/PI	Defines the PRI international code, used if the DDD component is not in the dialed digits.
		/pio	Entries are matched against the dialed digits if the DDD component is dialed. The first number specified in the list represents the PRI international operator code, used if the DDD component is not in the dialed digits.
		/PIO	Defines the PRI international operator code, used if the DDD component is not in the dialed digits.
(PRI TON options, continued)		/pn	Entries are matched against the dialed digits if the DDD component is dialed. The first number specified in the list represents the PRI national code, used if the DDD component is not in the dialed digits.
		/PN	Defines the PRI national code, used if the DDD component is not in the dialed digits.

(Options table, continued)

Option Type	Purpose	Option	Effect
		/po	Entries are matched against the dialed digits if the DDD component is dialed. The first number specified in the list represents the PRI operator code, used if the DDD component is not in the dialed digits.
		/PO	Defines the PRI operator code, used if the DDD component is not in the dialed digits.
Required Component (Applicable for Prefix and NNP section types.)	<p><i>Prefix section type</i>—Indicates that the prefix must occur first in the calling sequence. If multiple Prefix sections use the /r option, the prefixes in the dialing sequence must occur in the same order as the prefix sections in the LNP file. If a Prefix section is defined and does not use the /r option, the prefix is treated as optional.</p> <p><i>NNP section type</i>—Indicates that the NNP must occur in the calling sequence. Otherwise, the call is assumed a local number.</p>	/r	One of the listed prefix numbers is required on an outbound call.
Search (Applicable for the Classify section type only.)	Indicates that a calling sequence that has the pattern of a local number (for example, a 7-digit number in the United States) may actually be a number in a foreign NPA (FNPA).	/s	For areas where FNPA long distance numbers can be dialed without the area code, a Classify section using the /s option is used to identify which area code is associated with the specific exchange or partial phone number. The /s causes the section to be searched for a matching area code.
Size (Applicable to NPA section type only.)	<p>Specifies how many digits are in an NPA and/or a phone number.</p> <p>If an NPA size is not specified, the number of digits in the listed NPA is assumed.</p> <p>If a phone number size is not specified (and no Default section defines it), a phone number size is assumed.</p>	/NPA	Defines the number of digits in an NPA.
		/NUM	Defines the number of digits in the subsequent phone number.

(Options table, continued)

Option Type	Purpose	Option	Effect
SMDR	Used for SMDR processing.	/SMDR	Used in conjunction with the PRI TON Options. If a DDD component is matched or inserted by the PRI TON Option, the SMDR Option causes that value to be prepended to the raw destination string. The Management Server uses the raw destination string to reconcile SMDR data with calls.
		/NOSMDR	Causes a prefix digit to be removed from the raw destination. The Management Server uses the raw destination string to reconcile SMDR data with calls.
Valid PN	Used to indicate that the entries of a Prefix , DDD , NPA , or Special section can be accepted as valid phone numbers.	/v	The specified number is a valid phone number alone, but may be followed by additional digits.
		/V	The specified number is a valid phone number, but may be followed by additional digits, which are collected as suffix digits.

Defining Dialing Plan Sections

Each of the possible types of Dialing Plan sections are described below, including when to use them, where they are located by default, and how to define them. Certain types of sections are required in all Dialing Plans, while others depend on the dialing environment. Default sections of each type are included in the default LNP and WNP files. Optional sections are commented out, while those that are required are not. These default sections can be used as templates for customizing the Dialing Plan. The Dialing Plan files provide extensive comments and explanations to assist you. This section elaborates on that information. Refer to “Dialing Plan Section Header Components” on page 54 for a complete description of possible section header components.

Use the procedures below as a reference when customizing the Dialing Plans.

CC

(Predefined) The default WNP contains a **CC** section that is used to recognize and confirm the country code component of a dialing sequence. The **CC** section body consists of a comma-separated list of all possible country codes (no wildcards allowed). The **CC** section is unlikely to require modification.

Classify

Use a **Classify** section to classify calls (for example, as local, long distance, or toll-free) for audit reporting. The difference between “Special” and “Classify” is that a Special number is matched while the number is being received or as the digits are dialed. **Classify** sections are processed after the number has been completely dialed/received and parsed.

A **Classify** section body consists of one of the following:

- A comma-separated list of applicable NPAs. Each NPA can optionally be followed with a list of applicable exchanges or initial portions of the phone numbers, enclosed in curly brackets.
- A comma-separated list of local numbers. In this case, use a /Num Option in the section header.
- A comma-separated list of NPAs and local numbers. In this case, use an /NN Option in the section header.

Unless other options are explicitly specified, the following implicit options apply to **Classify** sections:

- **Match—/NPA** (Only the NPA component is compared, which is the first 3 digits after any Prefix and DDD digits.)
- **Call Direction—/od** (outbound destination).

Classify sections that are unlikely to change (such as toll-free designations) should be placed in the WNP. Those more subject to change (such as Metro exchanges) should be placed in the LNP.

The default Dialing Plans contain several **Classify** sections for common situations that you may need to customize to suit the Appliance locale.

See “Options” on page 59 for a list of options available for Classify sections.

DDD

Use one or more **DDD** (Direct Distance Dialing) sections to identify DDD codes, such as long distance and international dialing access codes, used for outbound calls in the dialing environment. A **DDD** section consists of a comma-separated list of DDD codes. Wildcards are allowed unless a PRI TON option is used. Since DDD codes are specific to the Appliance locale and may be subject to change, place them in the LNP.

Only one value from the DDD section of the Dialing Plan is matched on any given call. For example, a DDD defined as “56” and a call sequence of 565656 will have a DDD of “56” and a PN component (CC, NPA, NUM) that starts with 5656.

The following implicit option applies to **DDD** sections:

- **Call Direction**—**/od** (outbound destination) or **/is** (inbound source).

See “Options” on page 59 for a list of options available for DDD sections.

Default

(Optional) You can define a **Default** section to identify default values for labels and phone number component lengths. The values in **Default** sections are used when a section does not explicitly state a value. If no defaults are specified, the implicit default values are used. A **Default** section can be defined in either the LNP or the WNP.

Default section headers do not use Options.

A **Default** section body consists of one or more entries, each on a separate line, of the form: **<item_name>=“value”;**

Defaults can be set for the following items:

- **DP_Name**—The Dialing Plan name shown in logs.
- **DP_Flag**—Label to be added to all Call labels (for example, “DSN” when the DSN Dialing Plan is used).
- **HNPA_Flag**—Label used for PNs with local NPAs (“LOC”)
- **FNPA_Flag**—Label used for PNs with foreign NPAs (“LD”)

- **URI_Flag**—Label used for Source and Destination values derived from a URI (“URI”)
- **NPA_Length**—Default length of NPA for the CC.
- **NUM_Length**—Default length of local number for the CC.
- **PN_Min_Valid_Length**—Minimum number length.
- **PN_Max_Valid_Length**—Maximum Number length.
- **NPA_Intl_Length**—Default NPA length for INTL PNs.
- **NUM_Intl_Length**—Default Number length for INTL PNs.

DID

Define one or more **DID** (Direct Inward Dialing) sections if inbound destination DID extensions are present in the dialing environment. **DID** sections are used to construct a complete line number from *inbound destination* DID extensions. **DID** sections should be defined in the LNP.

Multiple definitions can be included in one section. If a section contains multiple entries, they are processed in the order in which they appear in the section. If multiple **DID** sections are defined, they are processed in the order they appear in the Dialing Plan files (beginning with the WNP). Four substitution algorithms are provided:

IMPORTANT

Use **DID** sections for Inbound Destination numbers only. In cases where DID-type partial numbers are received for other than Inbound Destination, use an **Expand or Preprocess** section definition instead.

- Use Algorithm 1 when all of the DID extensions are the same length. The algorithm uses the format **1, m, r**.
 - **1** indicates the algorithm number.
 - **m** represents the digits to be matched and replaced from the beginning of the extension. If you want to add digits to the DID extension instead of replacing digits, leave the **m** section empty. In this case, the digits you type for **r** are added to the front of the DID number without replacing any digits. Wildcard characters can be used in the **m** value.
 - **r** represents the digits you want to add to the DID extension, either to replace the digits specified in the **m** section, or in front of the DID extension if you left the **m** field empty.

For example, suppose a typical DID extension in your organization is 22345. To turn this extension into 555-1345 using algorithm 1, you would type the following:

1, 22, 5551

For a more complicated case, suppose you have the following DID ranges associated with the following exchanges:

Exchange 555: DID Range 2000–2099

Exchange 756: DID Range 5800–5999

You would use the following entries to convert the DIDs into local numbers:

1, 20, 55520

1, 58, 75658

1, 59, 75659

- Use Algorithm 2 when DIDs of varying lengths are present and you want to prescribe different actions based on the length of the DID. Algorithm 2 uses the format **2, l, m, r**.
 - **2** indicates the algorithm number.
 - **l** represents the length of the DID extension to be matched.
 - **m** represents the digits to be matched and replaced from the beginning of the extension. If you want to add digits to the DID extension instead of replacing digits, leave the **m** section empty. In this case, the digits you type for **r** are added to the front of the DID number without replacing any digits. Wildcard characters can be used in the **m** value.
 - **r** represents the digits you want to add to the DID extension, either to replace the digits specified in the **m** section, or in front of the DID extension if you left the **m** field empty.

For example, suppose you are in the U.S. and you have some 4-digit extensions and some 3-digit extensions. The 4-digit extensions take exchange 555, and the 3-digit extensions take exchange 399. For the 3-digit extensions, you also need to add an extra digit (in this case, you want to use 1) following the exchange to result in a 7-digit local number. You would use the following entries:

2, 4, , 555

2, 3, , 3991

- Use Algorithm 3 when the DID is of varying lengths and an IP subnet mask or domain are present and you want to prescribe different actions based on the length, IP subnet mask, or domain. Algorithm 3 uses the format: **3, l, m, mIP, r**.
 - **3** indicates the algorithm number.
 - **l** indicates the length of DN, DID, or Call Sequence to be matched.
 - **m** indicates the digit(s) to be matched and replaced.
 - **mIP** indicates the associated IP subnet mask or domain to be matched.
 - **r** indicates the prefix (substitution) string.

For example, the following entry:

3, 4, 20, 190.69.200.37, 51264720

matches any 4-digit number starting with a 20 with an associated IP address of 190.69.200.37, and replaces the 20 with 51264720. So the number 2046 from IP address 190.69.200.37 produces: (512) 647-2046

Matching digits can be empty/"any" and the associated IP can be a mask, domain, or empty/"any". For example:

3, 5, , securelogix.com, 83

matches any 5-digit number from an associated domain securelogix.com (case insensitive) and prefixes 83 to the number. So the number 54321 from securelogix.com produces: 835-4321.

- Use Algorithm 4 when the DID is of varying lengths, contains specific digits or a range of digits, an associated IP subnet mask or domain are to be matched, and you want to add a prefix or suffix and insert digits.

Algorithm 4 uses the format: **4, l, m, mIP, prx, ins, sfx.**

- **4** indicates the algorithm number.
- **l** indicates the length of DN, DID, or Call Sequence to be matched.
- **m** indicates the digit(s) to be matched and replaced.
- **mIP** indicates the associated IP subnet mask or domain to be matched.
- **prx** indicates the prefix string to add.
- **ins** indicates the post-match digits to insert.
- **sfx** indicates the suffix string to add.

Matched digits can be a range. Unlike the previous algorithms, this algorithm does not remove the matched digits. For example:

4, 4, 2000..5599, 190.69.200.37, 210523, , 8887

matches any 4-digit number in the range 2000 to 5999 that has an associated IP address of 190.69.200.37, prepends 210523 to the number and adds 8887 after the number. So the number 3641 from IP address 190.69.200.37 produces: (210) 523-3641.8887.

The length can be empty (“any”); the prefix, insert, or suffix can be “none”; and the associated IP can be a mask, domain or empty (“any”). For example:

4, any, 44, any, 011, none, none

matches any number starting with 44 and prefixes 011 to the number. So the number 44120476583 produces:
011+[44] (1204) 76583.

The insert value can be offset from the beginning of the signaled digits. An offset is designated by an offset value followed by the greater-than symbol > in the insert field. For example:

4, 7, 5621000..5621999, 190.69.200.37,, 3>449, none

matches ESN code 562 with DID range 1000..1999 that has an associated IP address of 190.69.200.37, and inserts exchange number 449 after the 3rd digit of the original number. So the number 5621234 produces: (562) 449-1234.

Expand

Define an **Expand** section if partial DID-type extensions other than inbound destination are present in the dialing environment. An **Expand** section is used to expand these partial non-DID extensions into fully qualified phone numbers.

IMPORTANT Do not use for inbound destination partial extensions; use a **DID** section instead.

Multiple definitions can be included in one section. If a section contains entries of both types of algorithms, they are processed in the order in which they appear in the section. If multiple **Expand** sections are defined, they are processed in the order they appear in the Dialing Plan files (starting from the WNP).

The Expand section does not have a default direction option; it must be explicitly set. If a direction option is not supplied, that section will not be used. The direction options are /od (outbound destination), /is (inbound source), and /os (outbound source).

For example:

[Expand: /od]

The same algorithms used for DID sections are used to define the Expand section. See “DID” on page 66 for a description and examples of the algorithms that can be used in the **Expand** sections.

NNP

Define an **NNP** (National NPA Prefix) section if a prefix is always dialed before the NPA when placing a long-distance, non-international call (for example, 0 in the UK).

NPA

(Required) The default WNP contains an **NPA** (numbering plan area) section used to identify and confirm the NPA phone number component (region/city/area codes) in a calling sequence. The **NPA** section consists of a comma-separated list of all possible NPAs for a given country or numbering plan area. The **NPA** section is placed by default in the WNP, since it is unlikely to change often. Update when new area codes are added to the dialing plan area.

Prefix

Define a **Prefix** section to identify digits that may occur as the initial digits in a calling sequence (such as an outside line access code, an operator-assistance code, or a prefix character denoting a normalized number in a URI). The section body consists of a comma-separated list of digit strings or ranges.

See “Options” on page 59 for a list of options available for Prefix sections.

Preprocessed Numbers

IMPORTANT Do not use for inbound destinations identified as DID in the **Incoming Numbering Format** and **Format Precedence** settings on the **Channel Map** tab of the **Span Configuration** dialog box; use a **DID** section instead.

Preprocessed numbers are partial phone numbers, such as an extension, that can be expanded into qualified phone numbers (PNs) using the same algorithms described in “DID” on page 66. If preprocessing of a number does not produce a valid phone number, only the dialed digits will be returned for display.

Suffix

Define a **Suffix** section to identify digits or other characters (such as #) that may occur following the extension in a calling sequence to mark the end of the phone number. After prefixes and DDD sections have been examined, any digits following a member of the **Suffix** section are treated as suffix digits.

The **Suffix** section body consists of a comma-separated list of single characters. Only single-character Suffix indicators can be specified. For multiple-digit suffix indicators, only the first digit is recognized.

Special

Define a **Special** section to identify initial digits in a calling sequence that indicate the phone number is not to be normalized, but used as received (for example, emergency access codes such as **911** and service codes such as **1411** for information).

The difference between “Special” and “Classify” is that a **Special** section is matched while the number is being received or as the digits are dialed, while **Classify** sections are processed after the number has been completely dialed/received and parsed. For example, the dialed

sequence 9117654 is classified as an Emergency number by the time the third digit is dialed, since “911” is defined as a Special number in the Dialing Plan. Ensure that the digits that you define as Special numbers are not otherwise valid initial digits in any other calling sequence.

See “Options” on page 59 for a list of options available for **Special** sections.

Dialing Plan Processing

When the Span determines the end of the dialed digits during a call, the Dialing Plan Processor (DPP) in the Span processes the call against its Dialing Plans. The DPP processes each call in two phases:

1. **Phone number identification**, during which the Destination and Source calling sequence are evaluated to identify the complete phone numbers to be used for Policy processing and Usage Manager reporting.
2. **Phone number/call classification**, during which the call is compared to any defined classification sections to determine if any additional call or phone number labels apply to the call. Classify sections are evaluated in the order in which they appear, beginning with the WNP, followed by the LNP.

Phone Number Identification Phase

During the phone number identification phase, the ETM System evaluates the calling sequence against the Dialing Plan to determine the phone number and create a normalized phone number. The Dialing Plan contains various types of sections that represent possible phone number components. Calls are compared with these sections in a specific order, as described below.

Dialing Plans can contain more than one section of a given type; when more than one section of a given type occurs, calls are evaluated against that type of section in the order in which the sections appear in the files.

1. First, special cases are considered:
 - If a PREP section is defined and the call sequence matches the criteria, the sequence is pre-processed (changed) according to the contents of this section.
 - If the calling sequence is a fully qualified, normalized phone number for the locale, processing continues with Phase 2: Classification. For example, in the United States, a normalized phone number is one of the form [CC] (NPA) <exchange>-<extension>.
 - If the calling sequence is marked as an inbound Direct Inward Dialing (DID) extension, the DPP compares the number with any DID sections that are defined in the LNP to see if it

matches those criteria. If so, the number is expanded, and then processing continues as described in 2 below. Whether a calling phone number is marked as a DID is determined by the **Incoming Numbering Format** and **Format Precedence** settings on the **Channel Map** tab of the **Span Configuration** dialog box.

- **Special** sections are compared against the dialed digits as they are being received/dialed.

2. The calling sequence is processed against the Dialing Plan sections in the following order:

- Prefix** sections—**Prefix** sections specify how the beginning digits of the calling sequence are to be treated. A Dialing Plan can contain multiple **Prefix** sections, and more than one **Prefix** section may apply to a given calling sequence. **Prefix** sections may apply only to outbound, only to inbound, or to both call directions. **Prefix** sections can also be marked as required according to call direction; for example, a **Prefix** section can specify that all outbound calls contain a line access code prefix, such as **9**. If they are not marked as required, and then **Prefix** sections indicate digits that may appear at the beginning of the calling sequence. If a calling sequence of the applicable call direction does not match a required **Prefix** section, processing continues normally, but a warning message is sent to the Span debug log.

The calling sequence is matched against **Prefix** sections in the following order:

- Required Prefix**, such as an outside line access code.
 - Optional Prefix**, such as a number used to access a specific long distance provider (i.e., 101xxxx).
- DDD** (Direct Distance Dialing) sections, such as long distance, international, and operator assisted dialing access codes (for example, +1, +0, and +011 in the U.S.).
 - If a previously matched DDD section had the /fCC option, the **CC** (country code) section is evaluated, to determine whether the dialed digits contain a CC. If no CC is present, the Appliance's local CC is used in the normalized number.
 - NNP** (National NPA Prefix) section—In some countries, a required prefix is dialed before the NPA when placing a long distance, non-international call.
 - NPA** (Numbering Plan Area) section—The region/city/area code. The DPP attempts to match the next *n* digits in the calling sequence with the NPA section in the WNP.

The NPA section header can define how many digits an NPA is to contain, and how many digits following the NPA the

A phone number is extracted from a SIP URI only when the URI indicates it contains a phone number via a "tel:" scheme name or equivalent identifier.

If no CC/NPA/NUM lengths are defined, these values default to NANP values.

extension should contain (ranges can be used). If an NPA section does not specify lengths, the default values are used. If no NPA match is found and the calling sequence is the least as long as the specified length for a local number (as defined in the NPA section header, a default section, and so on), the number is assumed to be local to the Appliance location and the local NPA is used in the normalized number.

- f. **Expand**—If none of the previous sections produced a match and the calling sequence is not the right size for a local number, any Expand sections are evaluated. If a match is made, the calling sequence is expanded as defined, and then the expanded number is again processed by the DPP to create a normalized number.
- g. If no match has been found, the calling sequence is invalid and is labeled **NOPN** (no phone number) in **Source Details** or **Destination Details** (depending on direction) column of the **Policy Log**.

Phone Number/Call Classification Phase

After the phone number processing phase is complete and the Destination and Source phone numbers have been identified, Dialing Plan processing continues with the phone number/call classification phase.

During the phone number/call classification phase, Classify sections are evaluated in the order in which they appear, beginning with the WNP, followed by the LNP. Unless a Classify section header has an option that causes evaluation to continue after a match, processing stops when the call matches a Classify section.

- WNP Classify sections provide global type classifications that apply to the call as a whole (for example, international, toll free, toll).
- LNP Classify sections typically provide local, long distance, and metro designations. If no call label is explicitly defined for a call by any matched section(s), the call is labeled “LD” if the NPA of either the inbound source or outbound destination differs from the Span’s local NPA; otherwise, it is labeled “LOC.”

SMDR Parse Files

About SMDR Parse Files

An SMDR parse file is a text file that represents the format of outgoing SMDR records (PBX call logs) so that the ETM[®] System can extract necessary call information from those records. For SMDR parse files to be available for download to the SMDR Provider Card, they must be stored in the **smdr** directory under the ETM Server installation directory. The following sections explain how to define a parse file.

For complete instructions for configuring the ETM System to use SMDR, including installing the correct SMDR parse file on the SMDR Provider Card, see the *ETM[®] System Installation Guide*.

By default, the SMDR correlation algorithm only matches to completed calls.

Files Already Defined

SecureLogix has defined SMDR parse files for formats used by a number of PBX brands, including Avaya, Lucent, Meridian, NEC, Nortel, Northstar, and Rolm. These files are located in the ETM Server installation directory at

<INSTALL_DIR>\ps\software_repository\smdr. Before you attempt to create a custom SMDR data definition file, please contact SecureLogix Customer Support to find out whether a data definition file is already available for your SMDR format. Contact SecureLogix Customer Support at any of the following:

- 1-877-SLC-4HELP
- support@securelogix.com
- <http://support.securelogix.com>

Defining an SMDR Parse File

It is strongly recommended that you use a preexisting SMDR parse file as a template and modify it to fit the needs of the current raw SMDR data. Many SMDR parse files are included in the **smdr** folder.

SMDR parse files are heavily dependent on regular expressions. It is strongly recommended that you have a reference guide for regular expressions as you modify/create the parse files. A brief reference for Perl5 regular expressions is included in this chapter.

Use the following steps, described in detail in this section, to define the SMDR parse file:

1. Capture SMDR data by enabling SMDR debug logging in the **Server Administration Tool** via the ETM System Console.
2. Open an existing SMDR parse file to use as a template.
3. Modify each of the sections or create new sections to match the SMDR data in use. See “SMDR Parse File Components” on page 76 for instructions specific to each section.
4. Save the file with a **.txt** extension in the **smdr** folder on the Management Server computer. If you accepted the installation defaults, this folder is located at the following path:

<INSTALL_DIR>/ps/software_repository/smdr

SMDR Parse File Components

The sections below describe the fields and tokens used to define SMDR parse files to extract call data from inbound and outbound SMDR.

Section 1: Record Separator

The Record Separator indicates how records in the file are separated. It consists of a regular expression enclosed by the following tags:

<RECORD_SEPARATOR>

</RECORD_SEPARATOR>

For single line SMDR data, the easiest delineator to use is ‘**\r\n**’ because this is always how the line ends (even if the raw data seen at the PBX has only ‘**\r**’ or ‘**\n**’ or ‘**^C**’).

If a single call data record spans multiple lines, you should define the final line as the Record Separator. For example, the proprietary Norstar SMDR format uses the following tokens as the Record Separator:

<RECORD_SEPARATOR>

(CALL\sRELEASED\r\n|TRANSFERRED\r\n)

</RECORD_SEPARATOR>

Section 2: Call Record

The Call Record section consists of a series of regular expressions enclosed by the following tags:

<CALL_RECORD>

</CALL_RECORD>

The regular expressions should match the call record produced by the PBX and save the necessary pieces of information.

To create the call record section

1. Print out a number of SMDR records.
2. Highlight the data that represents the fields you need. Refer to the final fields listed for each section type. The point of this step is to determine which pieces of information to save in the regular expressions. For example:
 - For outbound SMDR, highlight **Start Time, Source Extension, Duration, and Dialed Digits**. If **Start Time** is not present, you can use **End Time** and **Duration**.
 - For inbound SMDR, highlight the above fields plus **Direction**.
3. Create a regular expression (or modify an existing one) that matches the raw data you have printed out.

IMPORTANT The expression does NOT have to match the entire data record, but must match from the first saved token to the last. You do not need to write processing code for the fields following the last saved token.
4. To mark a field as one that you want to save, type parentheses () around the fields.

Call Record Final Fields

You must define a number of fields following the Call Record section. Each field is defined on a separate line and enclosed in angle brackets. The sample SMDR definition files included in the ETM Server installation directory demonstrate the syntax of the final fields. Call SecureLogix Customer Support if you have a special case.

The *index* in the final fields refers to the numeric order of the parentheses you have used in the regular expression. For example, if the Start Time call data is represented by the subpattern enclosed within the third set of parentheses, the index is 3; it would use the following final field: <START_TIME_FIELD=3>.

- <TIME_FIELD_FORMAT=*format*>—This specifies the format of the start (or end) time that you have specified to be saved in the Call Record section (for example, **MM/dd/yy HH:mm:ss** or **MM/dd HH:mm**). See “Time Format Syntax” on page 81 for important information about specifying the time format.
- <DURATION_FIELD_FORMAT=*format*>—This is the format of the duration that you have specified to be saved in the Call Record section.
- <STATION_FIELD=*n*>—This is the index (1-based) of where the station/extension field is in relation to the other saved tokens.

- **<DIALED_DIGITS_FIELD=*n*>**—This is the index (1-based) of where the dialed digits field is in relation to the other saved tokens.
- **<START_TIME_FIELD=*n*>**—This is the index (1-based) of where the start time field is in relation to the other saved tokens.
Omit this field if you are using End Time and Duration.
- **<CHANNEL_FIELD=*n*>**—This is the index (1-based) of where the channel field is in relation to the other saved tokens.
- **<END_TIME_FIELD=*n*>**—This is the index (1-based) of where the start time field is in relation to the other saved tokens. **Omit this field if you are using Start Time.**
- **<DURATION_FIELD=*n*>**—This is the index (1-based) of where the duration field is in relation to the other saved tokens.
- **<ACCESS_CODE_FIELD=*n*>**—Used to extract access codes from the SMDR data.
- **Optional: <SMDR_1_FIELD=*n*>, <SMDR_2_FIELD=*n*>, and/or <SMDR_3_FIELD=*n*>**—Provide indexes to up to 3 other saved tokens that you want to appear in the **SMDR #1**, **SMDR #2**, and **SMDR #3** fields in the **Policy Log** and call data store. These fields may be used to extract PIN codes or other call accounting information.
- **Optional: <CORRELATION_FIELD=*n*>**—This is the index (1-based) of where the record identifier is in relation to the other saved tokens. Correlation fields can be used when the call data is distributed among multiple records where the order of the data cannot be implied by a single Call Record definition.
- **Optional: <REQUIRE_ACCESS_CODE_RECORD=*true-false*>**—Denotes whether an Access Code Record must be found and matched before data is used to match against SMDR requests. Valid values are TRUE or FALSE. By default, an Access Code Record is not required (FALSE).

The following fields are only necessary if inbound SMDR is being processed in conjunction with Call Recorder protected extensions.

- **Optional: <DIRECTION_FIELD=*n*>**—This is the index (1-based) of where the call direction is in relation to the other saved tokens.
- **Optional: <INBOUND_DIRECTION_VALUES=*value-list*>**—Denotes the value(s) that specify the record is for an inbound call. Multiple values in *value-list* are separated by commas (,).

- **Optional:** <INBOUND_PARSE_DEFINITIONS=*file-list*>— Specifies the parse file(s) that contain definitions for attempting to parse inbound call records. This is necessary when the inbound record format is significantly different from the outbound record format. Multiple values in *file-list* are separated by commas (.).
- **Optional:** <IMPLIED_CALL_DIRECTION=*direction*>-- Necessary only if Inbound SMDR is being used in conjunction with the Call Recorder. Valid values for *direction* are OUTBOUND or INBOUND.

Section 3: Access Code Record

This section is optional and is defined only if the access code information must be parsed from a separate record from the Call Record. The Access Code Record consists of one or more regular expressions enclosed by the following tags:

```
<ACCESS_CODE_RECORD>
</ACCESS_CODE_RECORD>
```

Access Code Record Final Fields

As with the Call Record definition, you must define a number of fields following the <ACCESS_CODE_RECORD> section.

- <ACR_STATION_FIELD=*n*>—This is the index (1-based) of where the station/extension field is in relation to the other saved tokens.
- <ACR_DIALED_DIGITS_FIELD=*n*>—This is the index (1-based) of where the dialed digits field is in relation to the other saved tokens.
- <ACR_ACCESS_CODE_FIELD=*n*>—Used to extract access codes from the SMDR data.
- **Optional:** <ACR_SMDR_1_FIELD=*n*>, <ACR_SMDR_2_FIELD=*n*>, and/or <ACR_SMDR_3_FIELD=*n*>—Provide indexes to up to 3 other saved tokens that you want to appear in the **SMDR #1**, **SMDR #2**, and **SMDR #3** fields in the **Policy Log** and call data store. These fields may be used to extract PIN codes or other call accounting information.
- **Optional:** <ACR_CORRELATION_FIELD=*n*>--This is the index (1-based) of where the record identifier is in relation to the other saved tokens. Correlation fields can be used to correlate an access code record with the corresponding CALL_RECORD.

Section 4: Transfer Record

The Transfer Record section is optional and is defined only if inbound SMDR is being used for the Call Recorder and protected extensions, and when the transfer information, specifically the transferring and transferred station, comes in a separate record from the Call Record. This section is defined as a set of Regular Expressions enclosed by the following tags:

```
<SUPP_XFER_RECORD>  
</SUPP_XFER_RECORD>
```

Transfer Records Final Fields

As with the Call Record and Access Code definitions, you must define a number of fields following the `<SUPP_XFER_RECORD>` section.

- `<SUPP_XFER_CORRELATION_FIELD=n>`—This is the index (1-based) of where the record identifier is in relation to the other saved tokens. A correlation field is usually a call identifier. Correlation fields can be used to correlate this record with the corresponding Call Record.
- `<SUPP_XFER_ROOT_CORRELATION_FIELD=n>`—This is the index (1-based) of where the record identifier is in relation to the other saved tokens. This is useful when the transferred call generates a new call identifier, but also includes a separate call identifier to the original inbound call.
- `<SUPP_XFER_DEST_FIELD=n>`—This is the index (1-based) of the station/destination to which the call was transferred.

Matching the Dialed Digits String

In some cases, the dialed digits and the SMDR data vary. The SMDR parse file and settings in the **Switch Properties** dialog box provide information to the ETM System to extrapolate SMDR extensions from the raw SMDR data sent by the PBX and to convert those extensions into fully qualified phone numbers for reports and Policy enforcement. You can define two values in the SMDR Parse file that can be used as search and replace values to change the dialed digits string before it is used in the match algorithm.

The dialed digits search and replace fields can be defined anywhere in the SMDR parse file, but are not required.

If the following fields are added to the parse file and the MATCH and SUBSTITUTE values are both found in the SMDR data, the search and replace functions occur.

```
public static final string
DIALED_DIGITS_MATCH_TOKEN =

    "<DIALED_DIGITS_MATCH_PATTERN\\s*=\\s*( ( .
) *?) \\s*>";

public static final string
DIALED_DIGITS_SUBSTITUTE_TOKEN =

    "<DIALED_DIGITS_SUBSTITUTE_PATTERN\\s*=\\
s* ( ( . ) *?) \\s*>";
```

Time Format Syntax

The following table shows examples of time formats:

Format Pattern	Result
"yyyy.MM.dd G 'at' hh:mm:ss z"	1996.07.10 AD at 15:08:56 PDT
"EEE, MMM d, 'yy"	Wed, July 10, '96
"h:mm a"	12:08 PM
"hh 'o'clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:00 PM, PST
"yyyyy.MMMMM.dd GGG hh:mm aaa"	1996.July.10 AD 12:08 PM

The time format is specified using a *time pattern* string. In this pattern, all ASCII letters are reserved as *pattern letters*.

Time pattern letters are defined as the following:

Symbol	Meaning	Presentation	Example
G	era designator	(Text)	AD
y	year	(Number)	1996
M	month in year	(Text & Number)	July & 07
d	day in month	(Number)	10
h	hour in am/pm (1~12)	(Number)	12
H	hour in day (0~23)	(Number)	0
m	minute in hour	(Number)	30
t	tenth of minute (0-9)	(Number)	6
s	second in minute	(Number)	55
S	millisecond	(Number)	978
E	day in week	(Text)	Tuesday
w	week in year	(Number)	27
D	day in year	(Number)	189
F	day of week in month	(Number)	2
W	week in month	(Number)	2
a	am/pm marker	(Text)	PM
k	hour in day (1~24)	(Number)	24
K	hour in am/pm (0~11)	(Number)	0
z	time zone	(Text)	Pacific Standard Time
'	escape for text	(Delimiter)	
"	single quote	(Literal)	'

The count of pattern letters determines the format:

- **(Text)**—4 or more pattern letters, use full form; fewer than 4, use short or abbreviated form, if one exists.
- **(Number)**—the minimum number of digits. Shorter numbers are zero-padded to this amount. Year is handled specially; that is, if the count of 'y' is 2, the year is truncated to 2 digits.
- **(Text & Number)**—3 or more pattern letters, use text; fewer than 3, use number.

Any characters in the pattern that are not in the ranges of ['a'..'z'] and ['A'..'Z'] are treated as quoted text. For instance, characters like ':', '.', ' ', '#', and '@' appear in the resulting time text even if they are not enclosed within single quotes.

A pattern containing any invalid letter results in a thrown exception during formatting or parsing.

Regular Expression Syntax Quick Reference

A *regular expression* uses a sequence of symbols to denote a pattern that serves as a state-machine or mini-program to match specific sequences of characters. The ETM System SMDR parser uses Perl5 regular expressions.

The character set operator [...] works only on ASCII characters (Unicode characters 0 through 255). Otherwise, all Unicode characters should be valid in SMDR parser file regular expressions. The following sections list Perl5 regular and extended regular expression syntax.

Perl5 Regular Expression Syntax

Perl5 regular expression syntax consists of the following:

- Alternatives separated by the “pipe” symbol (|)
- Quantified atoms:

Atom	Meaning
{n, m}	Match at least n but not more than m times.
*	Match 0 or more times.
?	Match 0 or 1 times.
{n,}	Match at least <i>n</i> times.
{n}	Match exactly <i>n</i> times.
+	Match 1 or more times.

By default, a quantified subpattern is *greedy*, meaning it matches as many times as possible without causing the rest of the pattern not to match. To cause the quantifiers to match the minimum number of times possible, without causing the rest of the pattern not to match, add a ? following the quantifier.

For example:

Atom	Meaning
*?	Match 0 or more times
??	Match 0 or 1 times
{n,}?	Match at least n times
{n, m}?	Match at least n but not more than m times
{n}?	Match exactly n times
+?	Match 1 or more times

- Atoms:
 - Regular expression enclosed in parentheses—Matched as subpattern groups and saved for use by certain methods
 - **\$**—(dollar sign) A null token matching the end of a string or line (i.e., the position right before a new line or right after the end of a string)
 - **.**—(period) Matches everything except **\n**
 - **^**—(caret) A null token matching the beginning of a string or line (i.e., the position right after a new line or right before the beginning of a string)
 - Character classes (e.g., [abcd]) and ranges (e.g., [a-z])—Special backslashed characters work within a character class (except for back references and boundaries). Inside a character class, **\b** represents backspace.
 - Special backslashed characters (Any backslashed character not in this list matches itself):

Character	Meaning
\cD	Matches the corresponding control character
\b	Null token matching a word boundary (\w on one side and \W on the other)
\0	Matches null character
\A	Match only at beginning of string
\B	Null token matching a boundary that is not a word boundary
\d	Digit [0-9]
\D	Non-digit [NOT 0-9]
\f	Form feed
\n	New line
\1, \2, \3, etc.	Back reference. Matches whatever the specified parenthesized group matched. If no corresponding group exists, the number is interpreted as an octal representation of a character.
\nn or \nnn	Octal representation of character unless a back reference
\r	Carriage return
\s	Whitespace character [\t\n\r\f]
\S	Non-whitespace character [NOT \t\n\r\f]
\t	Tab
\w	Word character [0-9_a-z_A-Z]
\W	Non-word character [NOT 0-9_a-z_A-Z]

Character	Meaning
\xnn	Hexadecimal representation of character
\Z	Match only at end of string (or before new line at the end)

Perl5 Extended Regular Expressions

Perl5 extended regular expression syntax consists of the following:

Expression	Meaning
(?!regexp)	A zero-width negative lookahead assertion. For example, bay(?!front) matches any occurrence of “bay” not followed by “front”. Since this is a zero-width assertion, x(?!y)z will match xz, for example, because x is followed by a character that is not y (the z) and a z follows the zero-width assertion.
(?#text)	An embedded comment causing text to be ignored.
(?:regexp)	Groups whatever is contained in the regexp but does not cause the group match to be saved.
(?=regexp)	A zero-width positive lookahead assertion. For example, \w+(?=\s) matches a word followed by whitespace, without including whitespace in the MatchResult.
(?imsx)	One or more embedded pattern-match modifiers. <ul style="list-style-type: none">• i enables case insensitivity.• m enables multiline treatment of the input.• s enables single line treatment of the input.• x enables extended whitespace comments.

ETM[®] System Troubleshooting

System Files Used in Troubleshooting

This section lists the files that SecureLogix Customer Support may reference when troubleshooting ETM[®] System problems. The file locations listed here are the defaults.

These sections refer to exporting the **Diagnostic Log** and using ETM Commands. For instructions, see the following topics:

- For information about exporting the **Diagnostic Log**, see “Exporting the **Diagnostic Log** to a CSV File” in the *ETM[®] System Administration and Maintenance Guide*.
- For information about using the ETM Commands, see “ETM[®] Commands” on page 105.
- For information about how to establish a Telnet session and for logging in via the **Console** port, see “Managing Telnet Logins to a Card” in the *ETM[®] System Administration and Maintenance Guide* and “Logging in to a Card” on page 107.

In the sections below, **<INSTALL_DIR>** represents the Management Server installation directory.

Management Server Issues

Information related to the Management Server is found in the following files:

- **<INSTALL_DIR>\server-fatal-<instance_name>.log**
- **<INSTALL_DIR>\ps\errors\SystemError-<year_sequentialnumber><instance_name>.data**
- **<INSTALL_DIR>\ETMManagementService.cfg (Windows) or ETMManagementServer.cfg (Solaris)**
- **<INSTALL_DIR>\twms.properties**
- **Diagnostic Log** (exported CSV file)

ETM® Database Issues

Information related to the ETM Database is found in <ORACLE_HOME> in the following files:

- \admin\database_name\udump\trace_file.trc
- \admin\database_name\bdumb\alert_log.log

Report Server Issues

Information related to the Report Server is found in the following files:

- <INSTALL_DIR>\Report-Fatal-instance_name.log
- <INSTALL_DIR>\ETMReportService.log
- <INSTALL_DIR>\ETMReportService.cfg (Windows) or ETMReportServer.cfg (Solaris)
- <INSTALL_DIR>\ps\errors\SystemError-<year_sequentialnumber><instance_name>.data.
- <INSTALL_DIR>\twms.properties
- **Diagnostic Log** (exported CSV file)

Client Tool Issues

Information related to the ETM Client Tools is saved in the following files:

- <INSTALL_DIR>\esc_client.log
- <INSTALL_DIR>\teleaudit_client\teleaudit_client.log
- <INSTALL_DIR>\ps\maint\maint.log
- **Diagnostic Log** (exported CSV file)

SMDR Issues

Information related to SMDR is found in the following files:

- <INSTALL_DIR>\ps\debug\SMDR_DEBUG.txt
- <INSTALL_DIR>\ps\software_repository\smdr
- **Diagnostic Log** (exported CSV file)

See “Enabling SMDR Debug Logging” in the *ETM® System Administration and Maintenance Guide* for instructions for capturing raw SMDR data. See “SMDR Parse Files” on page 75 for information and instructions for defining SMDR parse files.

ETM[®] Appliance Issues

Information related to the ETM Appliances is found in the following files:

- **Diagnostic Log** (exported CSV file)
- Appliance logs—Capture the logs in one of the following ways:
 - By enabling Appliance Debug Logging on the Span. See “Logging Appliance Debug Events to a File” on page 95.
 - Issuing the following ETM commands via the Console port or Telnet and then copying the output to a text file:

```
WRITE MASK ALL  
  
LOGMASK ALL ALL.
```

Call Resolution or Policy Processing Issues

Information related to call resolution and Policy processing is found in the following files:

- **<INSTALL_DIR>\ps\software_repository\ini\
<LNP_filename>.LNP**
- **<INSTALL_DIR>\ps\software_repository\ini\
<WNP_filename>.WNP**
- **Voice Firewall Policy file installed on the Span**—From a command line, issue the following ETM Commands. Copy the output to a text file.

```
SHOW POLICY FILE  
  
SHOW POLICY STATUS.
```

- **Diagnostic Log** (exported CSV file).

Troubleshooting Guide

Use this reference to assist you with troubleshooting the errors that may occur when running the ETM System.

Appliance Status LEDs

ETM Appliances have LEDs on the front and/or back of the chassis or Card to indicate status of ETM System operation, the TCP/IP network, and the telecommunications connections. The LEDs provide immediate visual notification of errors and warnings. The LEDs indicate whether the Appliance is operating normally and draw attention to conditions related to the Dialing Plan; Policy; ETM Server interface; T1, E1, PRI, and VoIP network status; Fail Safe Mode; and Card temperature issues.

When LEDs indicate error conditions, you can investigate these conditions further by viewing the entries in the **Diagnostic Log** and the **Alert Tool**, viewing the health and status for the Card and/or Span, and by issuing ETM Commands via the **ASCII Management Interface, Console** port, or Telnet.

See the *ETM[®] System Installation and Configuration Guide* for a description of the Appliance LEDs.

For a detailed list of ETM Commands and their uses, see the *ETM[®] System Technical Reference*, available from the **SecureLogix** directory on the **Start** menu (Windows systems) or the ETM System installation directory (all systems), or the online Help.

Error and Debug Logs

Diagnostic Logs, which are stored in the ETM[®] Database and viewable through the Performance Manager, are discussed in the *ETM[®] System Administration and Maintenance Guide*.

Error and debug logs are stored in the Management Server installation directory. Some logs are created by default. Others can be enabled as needed for specific troubleshooting purposes.

For instructions for setting storage limits on error logs, see “Enabling Automatic Purging of Logs” in the *ETM[®] System User Guide*.

The table below describes these logs and identifies their locations.

To view logs

- Open the log file in a text editor.

Log	Description	Location
Error logs: SystemError<yyyymmdd><instance>.data	Created automatically if an error occurs. Contain records of system and user errors.	<INSTALL_DIR>\ps\errors
ErrorData<system-generated_number>.dmp	Contains additional information for debugging system errors and is referenced from the System Error file.	

(Error and debug log descriptions, continued)

Log	Description	Location
Appliance debug logs: <MAC>_<Span#>_<random#>.log	Only created if enabled on the Span Configuration dialog box for troubleshooting system performance issues.	<INSTALL_DIR>\ps\debug See “Logging Appliance Debug Events to a File” on page 95.
SMDR debug log: SMDR_DEBUG.txt	Only created if enabled in the ETM System Administration Tool, used for troubleshooting SMDR resolution issues.	<INSTALL_DIR>\ps\debug See “Troubleshooting SMDR Configuration” on page 92 for instructions for enabling and reading this file.
server-fatal-<servername>.log When the Management Server is restarted, this file is renamed to: server-fatal-<servername>-hhmmddyyyy-<uniqueid>.log where <uniqueid> is simply an incremental number to provide a unique filename.	Created if the Management Server unexpectedly terminates. Useful to Customer Support in determining the cause.	<INSTALL_DIR>
report-fatal<instance_name>.log	Created if the Report Server unexpectedly terminates.	<INSTALL_DIR>
report-fatal<instance>.log When the Report Server is restarted, this file is renamed to: report-fatal-<servername>-hhmmddyyyy-<uniqueid>.log where <uniqueid> is simply an incremental number to provide a unique filename.	(Windows only) Contains information about starting/stopping the Report Server. Useful to Customer Support in identifying issues.	<INSTALL_DIR>
RMIDService.log	(Solaris only) Contains information about starting/stopping the Report Server.	<INSTALL_DIR>
esc_client.log	Contains status and errors related to the processes required to connect/disconnect from the Management Server in the ETM System Console and to open/close the client applications.	<INSTALL_DIR>\esc_client

(Error and debug log descriptions, continued)

Log	Description	Location
SLCLoader.log	Contains information related to launching ETM System Client applications (ETM System Console, standalone Usage Manager, or ETM Database Maintenance Tool) and contains information about the processes required to run the application.	<INSTALL_DIR>
maint.log	Contains information related to the ETM Database Maintenance Tool.	<INSTALL_DIR>\ps\maint
teleaudit_client.log	Contains information about operation of the standalone Usage Manager.	<INSTALL_DIR>\teleaudit_client

Troubleshooting SMDR Configuration

If SMDR is not resolving properly, verify the following:

- The time offset between the Management Server and PBX is correct. You can do this by physically checking the time at the PBX and Management Server or by finding a call in the SMDR debug log that resolved and comparing the start times.
- The SMDR parse file is configured to calculate time correctly. The PBX can transmit SMDR data at start time or an end time/duration combination.
- You are parsing the correct strings. There may be multiple data string formats coming into the Management Server from the PBX.

See the following topics for more information about SMDR:

- For information about configuring SMDR, see “Configuring a Switch for SMDR” in the *ETM® System Installation Guide*.
- For information about enabling and reading the SMDR debug logs, see “Enabling SMDR Debug Logging” on page 93 and “Reading the SMDR Debug Log” on page 94.
- For information about defining and reading SMDR parse files, see “About SMDR Parse Files” on page 75.

About SMDR Debug Logs

SMDR debug logging stores raw SMDR data (PBX call logs). SecureLogix Customer Support can use this information for troubleshooting SMDR resolution issues. Only enable SMDR debug logging if instructed to do so by SecureLogix Customer Support personnel, to avoid using hard drive space unnecessarily. The SMDR debug logging setting does not affect how the ETM System uses SMDR information.

For details about SMDR Parse Files, see “About SMDR Parse Files” on page 75.

Enabling SMDR Debug Logging

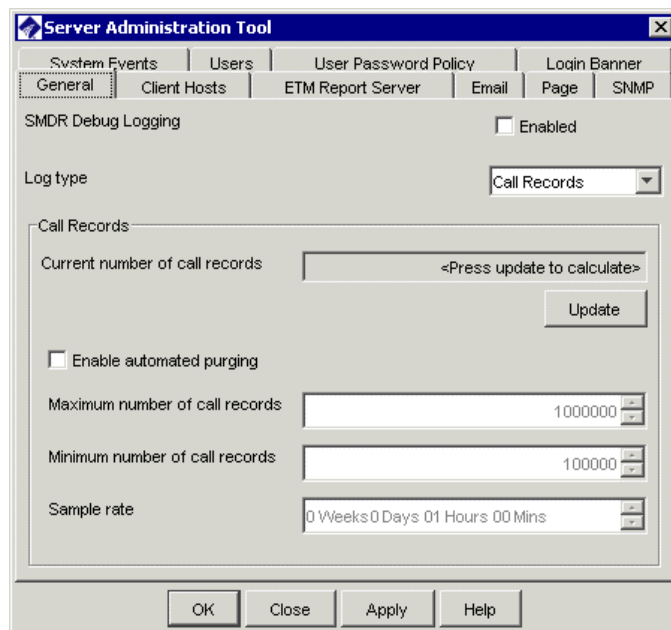
SMDR debug logging stores SMDR data and debugging information in a file named **SMDR_DEBUG.txt**. By default, this file is located at the following path:

<INSTALL_DIR>/ps/debug/SMDR_DEBUG.txt

This information can be used for configuring the ETM System to use SMDR data and for troubleshooting SMDR resolution issues.

To enable/disable SMDR debug logging

1. On the ETM System Console main menu, click **Servers | Server Management**. The **Server Administration Tool** appears.



2. On the **General** tab, in the **SMDR Debugging** area:
 - Select the **Enabled** check box to store SMDR data in a file called **SMDR_DEBUG.txt**.
 - Clear the **Enabled** check box when you no longer need to store the data, to avoid unnecessarily consuming hard drive space.
3. Click **OK** to apply the setting and close the dialog box, or **Apply** to apply the setting and leave the dialog box open.

The **SMDR_DEBUG.txt** file is created and stores SMDR data and debugging information until you disable this setting.

Reading the SMDR Debug Log

The following table provides examples and descriptions of the types of information that can appear in an SMDR debug log.

SMDR Debug Log Entry	Description
SMDR debug logging turned on at: Tue May 20 13:40:59 EDT 2003	SMDR debug log start date and time
SMDRManager::SetNewParser: ps\software_repository\smdr\WSU Parser.txt	Parsing file used
Did not find: <DURATION_FIELD_FORMAT\s*=\s*(.*)*\s*> Did not find: <END_TIME_FIELD\s*=\s*(.*)*\s*> Did not find: <DURATION_FIELD\s*=\s*(.*)*\s*> Did not find: <SMDR_1_FIELD\s*=\s*(.*)*\s*> Did not find: <SMDR_2_FIELD\s*=\s*(.*)*\s*> Did not find: <SMDR_3_FIELD\s*=\s*(.*)*\s*> Did not find: <DIALED_DIGITS_MATCH_PATTERN\s*=\s*(.*)*\s*>	Fields not being used
setPBXTimeParameters set to: 0 autodrift: false	Drift calculation parameters
SMDRGateway Initialization complete.	
Received SMDRRequest:	Call request
Call ID: 0030F609005C 3 10 134118-05202003	Unique key that is assigned by the Span to every call. (Do not confuse with Caller ID.)

SMDR Debug Log entry descriptions, continued

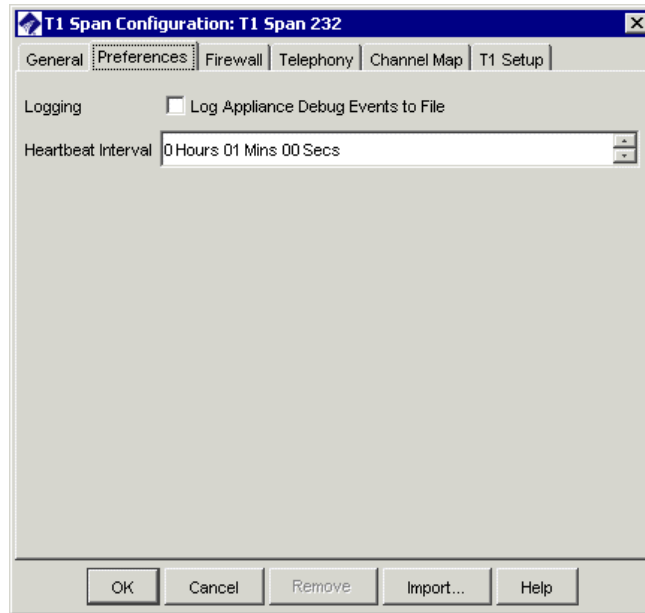
SMDR Debug Log Entry	Description
Dialed Digits: 14196366725	Destination digits dialed
Start Time: Tue May 20 13:41:18 EDT 2003	Time Stamp
Parsed Valid SMDRData: Originating Extension: 4787 Dialed Digits: 3070485 Call Start Time: Tue May 20 14:37:13 EDT 2003 SMDR Raw[01] = null SMDR Raw[11] = null SMDR Raw[21] = null	This message appears if SMDR Data was parsed correctly
Unable to parse Valid SMDR Data from string: 0!KE0700090015501 05201339130520134027 001100070000 00009374260878 0303	This message appears if unable to parse SMDR data
Potential Matching Request Found: SMDRRequest: Call ID: 0030F609005C 1 14 134658-05202003 Dialed Digits: 19373329058 Start Time: Tue May 20 13:46:58 EDT 2003 Current PBXOffset:0 Diff between call starts: 46000 Match Algorithm Returns SUCCESS Found potential match for SMDRData w/Digits: 5811000 Extension after replacement: 031 Raw PhoneString: 5811031 Phone Number: +1(210)5811031	After the request is made and the data is parsed, the ETM Server tries to match the data to the request to get a valid source number. A match returns this type of message.
Failed to find suitable match for SMDR Data: SMDRData: Originating Extension: 8810 Dialed Digits: 19373329058 Call Start Time: Tue May 20 14:44:45 EDT 2003 SMDR Raw[01] = null SMDR Raw[11] = null SMDR Raw[21] = null	No match found returns this type of message.

Logging Appliance Debug Events to a File

SecureLogix Customer Support can use Appliance debug event logs for troubleshooting. Debug logging can quickly generate a large file and greatly increases the amount of network traffic and Appliance load, potentially impacting Appliance performance. Only enable Appliance debug logging if instructed to do so by SecureLogix Customer Support personnel. When no longer needed for troubleshooting, the files can be deleted.

To log Appliance debug events to a file

1. In the Performance Manager tree pane, right-click the Span(s) from which you want to obtain diagnostic information, and then click **Edit Span(s)**. To select multiple Spans, hold down CTRL and select each Span, and then right-click the selection. The **Span Configuration** dialog box appears.
2. Click the **Preferences** tab.



3. In the **Logging** area, select the **Log Appliance Debug Events to File** check box. Clear this check box when you no longer need to store this information, to prevent unnecessary use of hard drive space.

The file is named:

<macaddress_spannumber_uniqueid>.dbg

and is saved on the Management Server host computer at the following path:

<INSTALL_DIR>/ps/debug

Symptoms

The following table describes various symptoms that you may encounter, a description of why the symptom may occur, and recommended solutions.

Symptom	Description/Solution
Memory errors while generating reports for large amounts of data.	<p>Increase the stack size available to the Java Virtual Machine in the Management Server, Report Server, and/or ETM System Console configuration files.</p> <p>For instructions, see “Increasing the Stack Size for the Java Virtual Machine” on page 14.</p>
Calls appear in the Call Monitor of an offline ISDN PRI NFAS member Span.	<p>If the Span is an NFAS Member, the D-channel information of the calls passing through the trunk is still captured by the primary D-channel (if online), and you will continue to see active calls in the Call Monitor. The Call Type for these calls is reported as Voice. This is normal functionality.</p>
A Span transferred from one Server to another cannot connect to the new Server and an error message appears in the Diagnostic Log indicating that the name is already in use.	<p>If you transfer management of a Span from one Management Server to another Server that has a Span with the same name, the like-named Span cannot connect to the new Server.</p> <p>Edit any duplicated Span name before transferring the Spans to the new Server. If you have already transferred a Span with a duplicate name to the new Server, rename the existing Span on the new Server. This allows the transferred Span to connect. After the transferred Span connects, you can then rename the Spans as desired.</p>
You want to change the IP address of an Appliance Card (for example, if your network environment has changed).	<p>The IP address of the Card is assigned during initial configuration. You can change the IP address of a Card in the Card Configuration dialog box or via ETM Commands. If you change a Card’s IP address, be sure to also add the new IP address to the list of authorized Card IPs.</p> <ul style="list-style-type: none"> To change the IP address in the Card Configuration dialog box, see “Changing a Card’s IP Address” in the <i>ETM® System Administration and Maintenance Guide</i>. To add the new IP address to the list of authorized Card IPs, see “Authorizing a Card to Connect to the Management Server” in the <i>ETM® System Administration and Maintenance Guide</i>.
The Management Server or Report Server fails to automatically initialize on reboot or restart.	<p>In the twms.properties file, edit the value for <code>InitialDatabaseConnectTimeout</code> to increase the number of seconds to wait before automatically reinitializing the Management Server when it is in standby mode..</p>
A connect error occurs when attempting to run a Report.	<p>The error, “A(n) connect error occurred. Failed to connect to Report Server at <Report_Server_host>: <RMI_port>. nested exception is java.rmi.NotBoundException: com.securelogix.telecom firewall.management.common reports.ReportServiceIfc...” indicates that the Report Server is not running or the ETM Report Service connection information in the Server Administration Tool is incorrect.</p>

Diagnostic Log Messages

The **Diagnostic Log** displays messages regarding system events, such as configuration changes, telco events, and call-traffic errors. It is recommended that you review this log daily.

For a list and description of the system events in each category, see “About System Events” in the *ETM® System User Guide*.

System Backup and Recovery Guidelines

General Guidelines for Backup Maintenance

Once data is purged, it cannot be recovered by any means other than by restoring from a backup.

This section provides several suggested ETM[®] System backup methods that simplify recovery of system operation and data in cases of hardware failure, natural disaster, or other catastrophic event, or to retain an archive of data purged by the user-configurable purging function. Each section contains guidance on what is to be backed up and how often, enabling your organization to adopt the procedures that best fit your needs.

It is recommended that all backups be saved to a secondary system or to removable media, such as CD-ROM, Zip disk, or AIT (tape).

Maintain a consistent backup routine. Performing this function at the same time daily/weekly/monthly helps to ensure the data that you expect to be available at a time of a system error is there.

Follow the same storage and rotation procedures you use for other critical information assets (e.g., rotate backup tapes, perform full backups on a regular basis, maintain secure offsite storage for backups).

Guidelines are provided for backing up:

- Complete system—Recommended to minimize the amount of time and effort required for reinstallation of the operating system, the ETM Applications, and the database.
- ETM System software installation directory.
- Full database.

Complete System Backup

Methods that you can use to perform a complete system backup include:

- ‘Ghosting’ or mirroring the contents of one drive/partition onto another.
- A hard drive backup utility local to the Management Server computer that offloads information onto removable media, if available.
- Using existing network-based backup system, if available.

An ideal time to obtain this image is at the completion of the ETM System installation and setup process, a point where all configuration and connectivity issues have been resolved and the system is ready to go live.

Additional complete system backups may be necessary as new applications are added/updated (e.g. Management Server upgrade) or as significant changes are made to the operating system (e.g., patches).

ETM Software Installation Directory Contents

The folders and files in the ETM System installation directory are listed and described below.

- **Folders:**
 - **Backup.** This folder is created if you reinstall the application and contains backed up files from previous installations. Not necessary to run the application.
 - **Documentation.** Contains PDF files of the ETM System documentation.
 - **esc_client.** Contains information about users that have logged in to the ETM System Console and past sessions.
 - **JRE.** Java software.
 - **ps.** Contains appliance software packages, error logs, dialing plans, debug information, and SMDR files. The folder is necessary to run the application, but error and log files are not necessary. Should be backed up.
 - **ps_<INSTANCE NAME>.** Present only in multi-instance installations; contains error logs, dialing plans, debug information, and SMDR files . Should be backed up.
 - **ps_skel.** Base ps directory used in multi-instance installations (ps_skel is copied and renamed to ps_<instance name>).
 - **rmid_logs.** Logs for the Report Server.

- **scripts.** Scripts used to create the Oracle database.
- **snmp.** SecureLogix MIB definitions for the ETM System.
- **teleaudit_client.** Contains information about users that have logged in to the standalone Usage Manager and past sessions.
- **Bitmaps for Splash Screens.**
 - ETMDBMaintToolSS.bmp
 - ETMManagementServerSS.bmp
 - ETMSystemConsoleSS.bmp
 - ETMReportServerSS.bmp
 - UsageManagerSS.bmp
- **Configuration Files.** Contain the configuration, paths, and java switches that tell the services how to start. Necessary to run the application. May be modified should be backed up.
 - ETMDBMaintTool.cfg
 - ETMManagementService.cfg
 - ETMSystemConsole.cfg
 - ETMReportService.cfg
 - UsageManager.cfg
- **Executable files.** Files that the ETM applications use to run.
 - activation.jar
 - AppManager.exe
 - comm.jar
 - ETMManagementService.exe
 - jakarta-oro-2.0.jar
 - jhall.jar
 - ldapjdk.jar
 - log4j-1.2.8.jar
 - mail.jar
 - report11_pro.jar
 - report12_pro.jar
 - ServiceController.exe
 - slc-crypt.hmac
 - slc-crypt.jar
 - SLCLoader.exe

- src.jar
- SysID.exe
- ETMReportService.exe
- TeleWall.jar
- twms.dll
- TWMSHelp.jar
- win32com.dll
- Win32Printer.dll
- xercesImpl.jar
- xmlParserAPIs.jar
- **System Log files.** Logs activities of each service; changes each time the services start or fail, depending on the log. Not necessary to run the application. Installation specific.
 - report-fatal-<servername>.log
 - server-fatal-<servername>.log
 - SLCLoader.log
 - ETMReportService.log
 - ETMManagementService.log
 - pp.xml
 - proxy.xml
 - routes.xml
- **Properties files.** Provide the services with specific parameters. May be modified and should be backed up.
 - delivery.properties
 - javax.comm.properties
 - npconfig.properties
 - twms.properties
- **Information files.** Files that indicate whether the AAA application is installed, and provide the system ID, ETM Server license, and application version information.
 - .modules
 - sysid.txt
 - TWLicense.txt
 - Version.txt

- **JDBC driver for Oracle:** JDBC driver that the application uses to connect to Oracle. Needs to match the driver that Oracle is using.
 - **ojdbc14.jar** (10G) or **ojdbc6.jar** (11G). If you update your Oracle installation, update this file with the copy that came with the new version of Oracle.)
- **City/State Data File.** A file that can be imported into the ETM System to provide city/state information in reports.
 - CCMI.slc

ETM Software Installation Directory Backup

Regularly back up your entire ETM Software installation directory (or directories, if you have installed the ETM Applications in a distributed configuration). Store these backups in a secure location to ensure that you can restore your system configuration and other files generated during system operation in the event of hard drive failure or other catastrophic event.

Restoring the ETM Software Installation from a Full Backup

To restore your ETM Software installation from a backup

1. Install the ETM Software as described in “Install the ETM® Software in the *ETM System Installation Guide*. Be sure the installation directory has the same name as the original and does not contain any files from a previous ETM System installation.
2. Copy and paste the backed-up directory over the new installation directory.

IMPORTANT This procedure should only be used in conjunction with a new software installation of the same version in a new directory. If you paste a backup over an existing installation that contains user-modified files, any data saved since the last backup will be lost, and signature file corruption may occur.

Backing Up the Database

The ETM Database stores all call data reported by the ETM Communication Appliances, all configuration settings administered through the Performance Manager, Usage Manager Reports and Elements, and Directory Listings.

It is recommended that you regularly back up the database. Creating a full database backup once or twice each month is especially recommended in locations where the ETM® System is placed in a mission-critical role or where loss of data is not acceptable.

Choosing the method and the frequency of backup depends on the perceived value of the data that could be lost. Contact an Oracle Database Administrator for more information and assistance with backing up your database.

ETM[®] Commands

Using ETM[®] Commands

ETM[®] Commands can be issued to the Spans and Cards in the ETM Appliances via the following command-line interfaces:

- **ASCII Management Interface** in the Performance Manager application.
- Telnet (Telnet is only available if the Card security posture is set to LOW and the client computer is listed in the Telnet Clients list for the Card.)
- A terminal emulator application on a computer that is connected to the **Console** port of the Appliance Card.

Except for passwords, ETM Commands are not case-sensitive; commands are listed in “ETM[®] Command” on page 109 in all upper case for clarity. Variables representing values are italicized within angle brackets. For example, the command to set the area code for a Span is **AREA CODE** *<value>*. For a Span in San Antonio, you type `AREA CODE 210`.

You can type partial commands if the part that you type is unique. For example, for the command **SHOW CONFIG**, you can type `SH CO`.

If you change a configuration item via ETM Commands, the **Diagnostic Log** in the Performance Manager reports the change. The log displays your username and the configuration item that you changed. For example, if you type the ETM Command to stop requesting SMDR on a Span, the log displays:

```
MS user admin has changed config item:
SMDR_QUERY
```

Important Information about Authority of Server

The first time a Card or Span connects to the Management Server, the Server accepts the configuration information from that component.

After Cards and Spans have initially established communication with their owning Management Server, the Server stores a copy of the component's configuration and is authoritative over all configuration settings.

This means that each time the Card or Span connects to the Server, the Server determines whether the component's configuration matches the copy stored on the Server. If they differ, the Server automatically pushes its copy of the configuration settings to the Card or Span.

Since the Server is authoritative, if you change a component's configuration via ETM Commands, the changes are overwritten the next time the component connects to the Server. Changes made via the Performance Manager application are retained.

If it is necessary that the change be pushed from the Appliance component to the Server (such as when you change Span type), use the procedure below to remove the Card icon from the **Platform Configuration** subtree before allowing the Card/Span to reconnect. This deletes the Server's copy of the configuration; the Server then accepts the configuration from the Card when it reconnects.

Removing a Card from the Tree Pane

To remove a Card from the tree pane

1. If the Card and Server are communicating, disrupt communication. To do this, remove the Card IP address from the list of authorized IP addresses, and then reboot the Card.
2. After the red bolt appears, indicating that the Card is not communicating, delete the Card icon from the tree by clicking **Remove** in the **Card Configuration** dialog box.

ETM[®] Commands Help

To view a complete list of commands

- In the **ASCII Management Interface**, at the **Console** port, or when using Telnet, type **HELP**.

To view Span-type-specific commands

- Type **HELP** and the Span type. For example, to view AAA-specific commands, type **HELP AAA**.

To view only the SHOW commands

- Type **HELP SHOW**.

Logging in to a Card

To log in via Telnet to any Card in any Appliance on the network, the **Card Security Level** in the **Card Configuration** dialog box must be set to **Low** and the IP address from which you are using Telnet must be allowed on the **Telnet Clients** tab. You can also log in to a Card via direct serial connection (the Console port) at all security levels.

To log in to a Card

1. Do one of the following:
 - To log in via Telnet, open a command prompt on any computer on the network, and then type:

```
telnet <IP_address_of_Card>
```


For example, type: `telnet 10.1.10.10`
 - To log in via direct serial connection,
 - a. Attach an RS-232 serial cable from the **Console** port to the serial port on your computer.
 - b. Start a session from a terminal emulation application (such as HyperTerminal) on your computer. For serial port settings, see “Serial Port Settings” in the *ETM[®] System Installation Guide*.
 - c. Press any key on your keyboard to activate the screen.
2. At the **USERNAME** prompt, type your username and press ENTER.
3. At the **PASSWORD** prompt, type your password and press ENTER. The ETM> prompt appears.
4. At the **ETM>** prompt, you can view Card and Span configuration using SHOW commands.
 - If you want to change Card and/or Span configuration parameters, place the Card in Enable mode:
 - a. Type ENABLE, and then press ENTER.
 - b. At the **PASSWORD** prompt, type the Enable password and press ENTER.

The **ETM:1(r/w)>** prompt appears indicating that you are in **Enable** mode on Span 1.
 - c. If you want to log in to a different Span, type:

```
SPAN <span_number>
```


where *<span_number>* is the number of the Span. For example, to set the focus to Span 2, type: SPAN 2.

Placing a Digital Span Offline/Inline

Analog Spans cannot be placed offline.

To place a digital Span offline/inline

- From the **ASCII Management Interface**, Telnet, or a serial connection to the Span, type the following command for the action you want to perform: SPAN OFFLINE, SPAN INLINE.
- You can issue the command to multiple Spans at once via the **ASCII Management Interface**. To connect to multiple Spans, hold down SHIFT or CTRL and select multiple Spans, and then right-click the selection and click **ASCII Management**.
- You can also still use the following Span-type-specific commands:

T1 Spans: T1 OFFLINE, T1 INLINE

E1 Spans: E1 OFFLINE, E1 INLINE

ETM[®] Command Reference

This section describes each of the available ETM Commands and on which Card/Span types the Command is valid. Note that you can type any portion of the command that is unique among commands. For example, you can type SH ST for SHOW STATUS.

****HELP COMMAND LIST-TYPES:ALL**

HELP [section]-sections: Network, AAA, Serial, Policy, IPS, Unix, Signaling, Channels, Maint, Sh(ow), ISDN, E1, E1PRI, CRC, SIP

EXIT-close connection

LOGOUT-close connection

DISABLE-disable ENABLE mode (read/write)

ENABLE-prompt for ENABLE mode (read/write) password

ENABLE PASSWORD-set the-ENABLE mode (read/write) password

ENABLE LOGIN secs-set the Power On Root login period (0..120 secs)

CLOCK SET hhmmss-mmddyyyy-set the Appliance time

TIMEZONE zone-set time zone: EST, CST, MST, PST, or GMT

HALT-halt the Appliance in preparation for power off

REBOOT [now]-reboot the Appliance

RESTART [all]-restart the current span or all spans

RESTART SPAN span-restart the specified ETM 3000 span: 1, 2, 3, or 4

RESTART FAILSAFE-stop the spans and switch to FailSafe mode

SECURITY high|med|low-set Appliance security posture

TERMINATE chan|all-terminate call on specified channel

USERNAME name password-define a username

NO USERNAME name-delete a username

LICENSE key-set ETM 3000 license key
SHOW LICENSE-display ETM 3000 license string and licensed features
WRITE MASK mask-specify log events to record (see LOGMASK types below)
LOGMASK type-subtype startRec endRec-set connection log reader mask
Examples: LOGMASK 0xff-0xffff LOGMASK all all LOGMASK none none
LOGMASK tok+tok all-Valid tokens: INFO+CHAN+DEBUG+TELCO+STARTUP+WARN
NO LOGMASK-ERROR+PANIC+SECURITY+CALL+POLICY

****HELP NETWORK-TYPES:ALL**

COMM RESET-close MS, Telnet, and Serial connections and restart
DES KEY key-set Appliance DES secret pass phrase
DES LEVEL level-set Appliance-to-Server level: single, triple, none
HEARTBEAT secs-set span-heartbeat rate to MS in secs
PLATFORM HEARTBEAT secs-set platform heartbeat rate to MS in secs
IP addr-set Appliance IP address
NETMASK mask-set Appliance IP netmask
GATEWAY addr-set Appliance default IP gateway address
SERVER IP addr-set MS IP address
SERVER PORT port-set MS IP port
SERVER COMM on|off span-determines whether specified span connects to MS
TIMEOUT minutes-set serial/Telnet connection timeout 1..120 minutes
TELNET COUNT num-set max num active Telnet connections (0-3)
TELNET ALLOW ADD addr-allow connections from the specified IP or IP mask
TELNET ALLOW DELETE addr-disallow connections from the specified IP or IP mask
NO TELNET addr-remove the IP/IP mask from list of allowed addrs

****HELP AAA -TYPES:AAA**

SHOW AAA CONFIG-display AAA configuration

SHOW AAA NETWORK-display AAA network status

SHOW AAA TOKENS-display AAA tokens

AAA SERVER IP-addr-set the IP address-for the AAA server

AAA SERVER PORT-num-set the listener port for the AAA server

AAA SERVER KEYdes_key-set the DES keyfor the AAA socket comm

AAA SERVER LEVEL level-set the DES level for the AAA socket comm.. Valid levels are: none, single, triple

****HELP SERIAL-TYPES:E1:T1:SS7-TRUNK:ANALOG:PRI**

SMDR QUERY OUT chn|all off|on|augment|replace -Outbound SMDR query type by channel

SMDR QUERY IN chn|all off|on-Inbound SMDR query type by channel

SMDR READER on|off-turn SMDR serial port reader on/off

SMDR DISPLAY on|off-turn SMDR debug displayer on/off

SMDR TIMEOUT secs-max seconds to wait for SMDR query result

SMDR BAUD baud-set SMDR serial port baud rate

SMDR DATABITS num-set SMDR serial port data bits (7 or 8)

SMDR STOPBITS num-set SMDR serial port stop bits (1 or 2)

SMDR PARITY none|odd|even|mark-set SMDR serial port parity

SMDR TYPE-set SMDR source type (SERIAL | IP)

SMDR IP TYPE-set IP SMDR provider type

SMDR IP ADD-add an IP SMDR provider address

SMDR IP DEL-remove IP SMDR provider address

SMDR IP PORT-set the listener port for the IP SMDR provider

SMDR ENCRYPT TYPE-set the encryption type for IP SMDR (NONE | 3DES)

SMDR ENCRYPT PASSWORD-set encryption password for encrypt IP SMDR.

SPAN 1|2|3|4-set CONSOLE serial port focus to span 1-4
FORCE SPAN FOCUS 1|2|3|4-forces CONSOLE serial port focus to span 1-4
CONSOLE BAUD baud-set CONSOLE serial port baud rate
CONSOLE CR on|off-on = use <CR><LF> off = <NEWLINE>
CONSOLE LOCKOUT secs-lockout time for repeated failed logins
CONSOLE TRACE CAPTURE-capture last 8 KB of console output
SHOW CONSOLE TRACE-display captured console output
SHOW SMDR-display SMDR settings
SHOW SMDR QUERY-display SMDR query settings
SHOW SMDR TYPE-display SMDR source (SERIAL|IP)
SHOW SMDR IP TYPE-display IP SMDR provider type
SHOW SMDR IP ADDR-display IP SMDR provider address
SHOW SMDR IP PORT-display the listener port for the IP SMDR provider
SHOW SERIAL-display serial port settings

****HELP SERIAL-TYPES:CRC**

SPAN 1|2|3|4-set CONSOLE serial port focus to span 1-4
FORCE SPAN FOCUS 1|2|3|4-forces CONSOLE serial port focus to span 1-4
CONSOLE BAUD baud-set CONSOLE serial port baud rate
CONSOLE CR on|off-on = use <CR><LF> off = <NEWLINE>
CONSOLE LOCKOUT secs-lockout time for repeated failed logins
CONSOLE TRACE CAPTURE-capture last 8 KB of console output
SHOW CONSOLE TRACE-display captured console output
SHOW SERIAL-display serial port settings

****HELP POLICY-TYPES:E1:T1:SS7-TRUNK:ANALOG:PRI**

AREA CODE-value-set the local area code
COUNTRY CODE value-set the local country code (1=US, 44=UK, etc.)

CHANNEL MAP T1|E1|POTS-monitor first 24|30|12 channels

CHANNEL MAP 0x0ff-monitor first 8 channels

CALLER ID ENCODING ch|all mode-set the caller ID detection mode for channel or all channels. Modes are:

None-detection mode disabled

bellcore-Bellcore signaling mode

etsi ETSI signaling mode

ukbt-UK BT signaling mode

ukDTMF-UK DTMF signaling mode

ntt-Japan NTT signaling mode

EXTENSION channel ext-set the extension of a channel

EXTENSION 1 [1](210)5551212-set the extension of channel [1]= country code (1=US, 44=UK) (210) = area/city code

NO EXTENSION channel|all-clear the extension of channel or all channels

MID CALL DIGITS on|off-determine if digits collected during the call should be reported to the MS

SECOND DIAL TONE on|off-determine if the second dial tone detection on inbound calls is active

POLICY CONFIG UPDATE-utilize updated extension map and timeout values

POLICY ENFORCE on|off-enable or disable policy enforcement

POLICY RESET-reset policy processing state machine

POLICY CALL ESTms-set call established delay

POLICY TYPE DELAY ms-delay until declaring call type: voice, modem, fax

POLICY STU on|off-enable or disable STU-III detection

POLICY AMBIGUOUS SKIP all|inbound|none-specify handling of ambiguous rules

SHOW POLICY FILE-display current security policy

SHOW PLANFILE-display current masking plan

SHOW PLAN-display masking of Calling and Called Numbers

SHOW POLICY STATUS—display policy enforcement, num calls, etc
SHOW EXTENSIONS—display extension map
CALL COUNTER ch|total|all|clear display/clear call progress counters
SHOW CALL COUNTERS—display ALLcall progress counters

****HELP POLICY-TYPES:SIP**

AREA CODE value—set the local area code
COUNTRY CODE value—set the local country code (1=US, 44=UK, etc.)
POLICY ENFORCE on|off—enable or disable policy enforcement
POLICY AMBIGUOUS SKIP all|inbound|none—specify handling of ambiguous rules
SHOW POLICY FILE—display current security policy
SHOW POLICY STATUS—display policy enforcement, num calls, etc
SHOW EXTENSIONS—display extension map

****HELP IPS-TYPES:ALL except CRC**

SHOW IPS POLICY—display IPS policy file contents
SHOW IPS STATUS—display IPS subsystem status
SHOW IPS TERMINATIONS—display IPS rules actively terminating calls

****HELP SIGNALING-TYPES:T1:E1**

SIGNALING TYPE chan|all type

WINK: Wink-Start

IMMEDIATE: Immediate Start

GROUND: Ground-Start

LOOP: Loop-Start

WINK/IMMEDIATE: Wink in/Immediate out

IMMEDIATE/WINK: Immediate in/Wink out

R1—R1 (Q.310 Q.331)

SIGNALING INVERTED yes|no chan—invert A/B bit signaling (E1-CAS only)

SHOW SIGNALING—display signaling type for each channel
 SHOW T1—display T1 parameters, alarms, and statistics
 SHOW T1 COUNTERS—display T1 line statistics
 T1 STATS CLEAR—clear T1 line statistics
 T1 CONFIG UPDATE—use updated T1 line interface configuration
 T1 INLINE|OFFLINE—go inline on reboot or close relays bypassing Appliance
 T1 SPAN CHECK—on|off—turn on|off low level detector of a hung telecom span
 T1 CALL START—ms—min ms of off-hook to signal start of outbound call
 T1 DEBOUNCE A|B—ms—min ms to debounce extraneous A or B bit transitions
 T1 DIGIT ms—min ms of on-hook to signal pulsed digit
 T1 HANGUP ms—min ms of on-hook to hangup
 T1 PULSE ms—max ms of on-hook to signal pulsed digit
 T1 ALERT—ms—max ms of on-hook with no event
 T1 TERMINATE—ms—num ms to forcibly hold on-hook

****HELP SIGNALING—TYPES:PRI**

SIGNALING TYPE chan|all type—PRI —ISDN PRI
 SHOW SIGNALING—display signaling type for each channel
 SHOW T1—display T1 values, alarms, and statistics
 SHOW T1 COUNTERS—display T1 line statistics
 T1 CONFIG UPDATE—utilize updated T1 line interface configuration
 T1 INLINE—set state so Appliance goes inline on reboot
 T1 OFFLINE—close T1 relays bypassing Appliance
 T1 CLOCK—CO|PBX—derive transmit clock from CO or PBX
 T1 FRAMING—SF|ESF—set T1 framing: Super Frame or Extended Super Frame
 T1 LINE CODING AMI|B8ZS—set T1 line encoding
 T1 ERROR THRESHOLD num—minimum num of T1 line errors before TELCO event

T1 TELCO DELAY secs-specify num seconds of alarm before TELCO event
T1 STATS CLEAR-clear T1 statistics
T1 SPAN CHECK-on|off-turn on|off low level detector of a hung telecom span
COMPANDING chan|all mulaw|alaw-set the format for received audio data

****HELP SIGNALING-TYPES:ANALOG**

SIGNALING TYPE chan|all type-

GROUND -Ground Start

LOOP-LoopStart

DID-Reverse Battery Loop Start DID

SHOW SIGNALING-display signaling type for each channel

SHOW POTS-display POTS parameter values

POTS DIALPULSE on|off-specify whether dial pulse is used to/from the CO

POTS CALL START ms-min ms of off-hook to signal start of outbound call

POTS DEBOUNCE HOOK ms-min ms to debounce extraneous hook events

POTS DEBOUNCE POLARITY ms-min ms to debounce extraneous polarity reversal events

POTS DEBOUNCE RING ms-min ms to debounce extraneous ring events

POTS DIGIT ms-min ms of on-hook to signal pulsed digit

POTS HANGUP ms-min ms of on-hook to hangup

POTS PULSE ms-max ms of on-hook to signal pulsed digit

POTS RING ms-max ms of on-hook with no event

POTS TERMINATE TIME-ms-num ms to forcibly hold on-hook

POTS TERMINATE POINT answer|CID|ring-determines when and how loop start and ground start calls are terminated

POTS TERMINATE OVERRIDE on|off-Allow(on)/Disallow(off) a new call during active termination of the previous call on a channel

MAINT VOLTAGE MONITOR chan duration-sample test voltage over given number of seconds

RINGBACK VERIFY on|off-turn on|off phone number validation via dialing plan for ringback events

****HELP SIGNALING-TYPES:ANALOG-**

Analog/POTS settings for Models 1012 and 1024

*****For each of the commands in this section, "chan" can be either "all" or a channel number 1..12**

POTS RING HOLD chan val-ms ring state held active after ring signal ends.
Valid val = 0..510 ms

POTS POLARITY DELAY chan val-ms delay used to debounce polarity reversals.
Valid val = 0..255 ms

POTS CURRENT DELTA chan pcnt-delta (%) for detecting parallel hook state
1-6.25% 2-12.50% 3-18.75% 4-25.00%
5-31.25% 6-37.50% 7-43.75% 8-50.00%

POTS EVENT DELAY chan val-ms delay from event detect to event declared.
Valid val = 0..255 ms

POTS EVENT DELTA chan val-volts minimum delta to declare thresh event.
Valid val = 0..15 volts

POTS UPDATE DELTA chan val-volts difference to update line voltage. Valid
val = 0..15 volts

POTS HOOK THRESH chan lower upper-volts threshold range to declare on
hook/off-hook. Valid val = 0..127 volts

POTS CURRENT BASE chan counts-sets parallel current base value (counts*1.1
mAmps)

POTS DEBUG [+/-]print|log|both|off [[+/-]chn|all] [level 1|2]-hook state
debug msgs

SHOW POTS [raw]-display POTS/Analog parameter values

****HELP E1-TYPES:E1:E1-PRI**

SIGNALING TYPE chan|all PRI-set signaling type, only PRI is currently
valid

SHOW SIGNALING-display signaling type for each channel

SHOW E1-display E1 values, alarms, and statistics

SHOW E1 COUNTERS-display E1 line statistics
 E1 CONFIG UPDATE-utilize updated E1 line interface configuration
 E1 STATS CLEAR-clear E1 statistics
 E1 INLINE-set state so Appliance goes inline on reboot
 E1 OFFLINE-close E1 relays bypassing Appliance
 E1 CLOCK CO|PBX-derive transmit clock from CO or PBX
 E1 FRAMING BASIC|CRC4|NON-CRC4 set E1 framing
 E1 LINE CODING AMI|HDB3-set E1 line encoding
 E1 ERROR THRESHOLD num-minimum num of E1 line errors before TELCO event
 E1 TELCO DELAY secs-specify num seconds of alarm before TELCO event
 E1 SPAN CHECK-on|off-turn on|off low level detector for hung D channel
 E1 LINE LENGTH CO-120-appliance-to-CO-line length impedance in Ohms
 E1 LINE LENGTH PBX 120-appliance-to-PBX line length impedance in Ohms
 COMPANDING chan|all mulaw|alaw-set the format for received audio data

****HELP SIGNALING—TYPES:T1:SS7-SL:SS7-TRUNK**

T1 ERROR THRESHOLD num-minimum num of T1 line errors before TELCO event
 T1 TELCO DELAY secs-specify num seconds of alarm before-TELCO event
 T1 CLOCK CO|PBX-derive transmit clock from CO or PBX
 T1 FRAMING SF|ESF-set T1 framing: Super Frame or Extended Super Frame
 T1 LINE CODING AMI|B8ZSset T1 line encoding
 T1 LINE LENGTH CO-len-Appliance to CO-line length
 T1 LINE LENGTH PBX len-Appliance to PBX line length

Valid line length values:

LH= Long-Haul

DB 7.5= Long-Haul -7.5-db

DB 15.0= Long-Haul -15.0 db

DB 22.5= Long-Haul -22.5 db
TR62411_LH= Long-Haul TR62411
SH_0_110= Short Haul 0..110 feet
TR62411_0_110= Short Haul TR62411
SH_110_220 = Short Haul 110..220 feet
TR62411_110_220 = Short Haul TR62411
SH_220_330 = Short Haul 220..330 feet
TR62411_220_330 = Short Haul TR62411
SH_330_440 = Short Haul 330..440 feet
TR62411_330_440 = Short Haul TR62411
SH_440_550 = Short Haul 440..550 feet
TR62411_440_550 = Short Haul TR62411
SH_550_660 = Short Haul 550..660 feet
TR62411_550_660 = Short Haul TR62411

****HELP SIGNALING-TYPES:PRI**

T1 LINE LENGTH CO length-Appliance to CO line length
T1 LINE LENGTH PBX length-Appliance to PBX line length

Valid line length values:

LH= Long Haul
DB-7.5= Long Haul -7.5-db
DB-15.0= Long Haul -15.0 db
DB-22.5= Long Haul -22.5 db
SH_0_110= Short Haul 0..110 feet
SH_110_220== Short Haul 110..220 feet
SH_220_330== Short Haul 220..330 feet
SH_330_440== Short Haul 330..440 feet

SH_440_550== Short Haul 440..550 feet
SH_550_660== Short Haul 550..660 feet
TR62411_LH== TR62411 Long Haul
TR62411_0_110== Short Haul TR624110..110 feet
TR62411_110_220== Short Haul TR62411 110..220 feet
TR62411_220_330== Short Haul TR62411 220..330 feet
TR62411_330_440= Short Haul TR62411 330..440 feet
TR62411_440_550= Short Haul TR62411 440..550 feet
TR62411_550_660= Short Haul TR62411 550..660 feet

****HELP SIGNALING—TYPES:T1:PRI:SS7-SL:SS7-TRUNK**

T1 LOOPBACK MODE on|off|automatic-

ON== place span in Pass-Through mode

OFF: deactivate Pass-Through mode

AUTOMATIC: Pass-Through mode becomes active or inactive based on receipt of loopup/loopdown codes

T1 LOOPBACK TIMEOUT seconds-set loopback automatic mode timeout

Valid timeout values:

0: infinite timeout

1: 86400 seconds

****HELP ISDN-TYPES:PRI**

ISDN TYPE type-set configuration: 23+D, 24B, D Primary, D Backup

ISDN TYPE D Primary-set configuration as NFAS D channel server

ISDN TYPE 23+D-set configuration as stand-alone PRI

ISDN TYPE 24B-set configuration as 24 bearer channels

ISDN INTERFACE num-set NFAS interface number, valid values: 0..23

ISDN INTERFACE 0-non NFAS interface number should be set to 0

ISDN PRIMARY id IP span-set interface, span, and IP of primary D channel

ISDN BACKUP-id IP span-set interface, span, and IP of backup-D channel

ISDN BACKUP 6 10.1.1.16 1set backup D channel interface ID to 6, on span 1 at IP address 10.1.1.16

ISDN ADD INTERFACE num ip-set specified interface's IP address

ISDN ADD INTERFACE 1 10.1.1.1

ISDN DEL INTERFACE num-remove specified interface from NFAS table

ISDN MAP-config|plan-set Extension Mapping or Redirection

ISDN PROTOCOL VARIANT type-set msg protocol variant: NI2, 4ESS, 5ESS, DMS100

ISDN PORT num|none-set NFAS TCP port for inter-Appliance communication

ISDN LEVEL level-set NFAS DES encryption level: none, single, triple

ISDN KEYkey-set NFAS DES encryption key

****HELP E1PRI—TYPES:E1-PRI**

ISDN TYPE 30+D-set configuration as stand-alone PRI

ISDN INTERFACE num-set interface number, valid values: 0..23

ISDN INTERFACE 0-interface number often is often set to 0

ISDN PROTOCOL VARIANT typeset protocol variant: NI2, 4ESS, 5ESS, DMS100,

ISDN PROTOCOL VARIANT NI2-EUROISDN, DASS2, DPNSS, QSIG

ISDN CPN RESTRICT on|off-outgoing Calling Party Number delivered to network

ISDN CPN CHANGEon|off-outgoing Calling Party Number modified-to network

ISDN CPN NUMBERnone|numoutgoing 10 digit CPN delivered to network

ISDN CPN NUMBER2105551212

ISDN CPN NUMBERnone-outgoing Calling Party number delivered as blank

ISDN CPN TON-type-outgoing Calling Party Type of Number (TON):

ISDN CPN TON-NATIONAL-UNKNOWN, NATIONAL, INTERNATIONAL, SUBSCRIBER

ISDN DCHANNEL-*chan-channel/timeslot* of D channel (0-31)

ISDN DIRECTION *normal|reverse* set network/user side direction for tie trunks

ISDN CLEAR COUNTERS-reset D channel packet packet counters

ISDN L2 LOGGINGOn|off-include Layer 2 messaging in log or ISDN socket

ISDN L2 CROSSOVER *on|off|automatic*-ON== take appliance logically out-of-line

 OFF== appliance is logically inline, default mode

 AUTOMATIC = appliance automatically toggles between ON and OFF modes based on D channel state

ISDN GLARE *none|X|Y*-set E1 DPNSS glare to PBX X or PBX Y

SHOW ISDN-display ISDN settings

SHOW BLOCKED-display channels with events blocked

ISDN CPN RESTRICT *on|off*-outgoing Calling Party Number delivered to network

ISDN CPN CHANGEOn|off-outgoing Calling Party Number modified to network

ISDN CPN NUMBER *none|num*-outgoing 10 digit CPN delivered to network. Ex:
ISDN CPN NUMBER 2105551212

ISDN CPN NUMBER *none*-outgoing Calling Party number delivered as blank

ISDN CPN TON-type-outgoing Calling Party Type of Number (TON). Valid Values: ISDN CPN TON-NATIONAL-UNKNOWN, NATIONAL, INTERNATIONAL, SUBSCRIBER

ISDN DCHANNEL-*chan-channel/timeslot* of D channel (1-24)

ISDN DIRECTION *normal|reverse*-set network/user side direction for tie trunks

ISDN REJECT CAUSE *cause*-cause value used in rejecting (terminating) inbound calls

ISDN CLEAR COUNTERS-reset D channel packet and NFAS packet counters

ISDN L2 LOGGINGOn|off-include Layer 2 messaging in log or ISDN socket

ISDN L2 CROSSOVER *on|off|automatic*-ON== take appliance logically out-of-line

OFF== appliance is logically inline, default mode

AUTOMATIC = appliance automatically toggles between ON and OFF modes based on D channel state

ISDN GLARE none|X|Y-set E1 DPNSS glare to PBX X or PBX Y

SHOW ISDN-display ISDN settings

SHOW BLOCKED-display channels with events blocked

****HELP CHANNELS-TYPES:T1:SS7-TRUNK:ANALOG**

SHOW CHANNELS-display channel specific values

SHOW COMPANDING-display channel companding: A-law, U-law

SHOW CALL PROGRESS-display DSP call progress settings

TONE TYPE chan|all DTMF|MF-set tone type of signaling digits

DSP DEBUG dsp|ALL OFF|LEVEL1|LEVEL2-set DSP debug level

CALL PROGRESS chan|all na|intl-set DSP call progress (North America/International)

SIGNALING FORMAT IN-chan format-set format of signaling digits to PBX

SIGNALING FORMAT OUT chan format-set format of signaling digits to CO

SIGNALING PRECEDENCE chan format-set signaling types precedence

****HELP CHANNELS-TYPES:PRI**

SHOW CHANNELS-display channel specific values

SHOW COMPANDING-display channel companding: A-law, U-law

SHOW CALL PROGRESS-display DSP call progress settings

TONE TYPE chan|all DTMF|MF-set tone type of signaling digits

DSP DEBUG dsp|ALL OFF|LEVEL1|LEVEL2-set DSP debug level

CALL PROGRESS chan|all na|intl-set DSP call progress (North America/International)

SIGNALING FORMAT IN-chan format-set format of signaling digits to PBX

SIGNALING FORMAT OUT chan format-set format of signaling digits to CO

SIGNALING PRECEDENCE chan format-set signaling types precedence

Valid "format" tokens:

ADDR

DID

DNIS

****HELP CHANNELS-TYPES:SS7-SL:SS7-TRUNK**

SHOW SS7-display SS7 specific values and the current link status

SHOW SS7 CIC-display SS7 CIC/channel assignments on bearer span

SHOW SS7 NET-display SS7 network status

SS7 TONE span-specify the span to provide the termination Reorder Tone

SS7 IP SL_link ip-specify the IP address of a signaling link (1..16) for an associated Signaling Link span. An IP of 0.0.0.0 removes the link.

Example: SS7 IP 1 10.1.1.50

SS7 PORT SL_link port-specify the TCP/IP server port for an associated Signaling Link span. See SS7 IP above. Example: SS7 PORT 1 4314

SS7 LINK link chan-specify the DS0 channel (1-24) to be monitored by the specified logical link.-A channel value of 0 disables the logical link.

Example: SS7 LINK 1 24 -define logical link 1 to monitor DS0 channel 24

****HELP CRC-TYPES:CRC**

RESERVED DISK SPACE length-length (Mbytes) reserved for recording and index files

MAINT EXTERNAL RECORDINGS enable|disable-Enable/Disable recordings from remote spans

RECORDING LISTENER PORT port-set the CRC Recording Listener Port

RECORDING IP ADD ip-set IP Address from which to accept recording requests

RECORDING IP DELETE ip-remove IP Address from which to accept recordings

COLLECTION-SERVER COMMUNICATION enable|disable-Enable/Disable the Collection Server Comms

COLLECTION-SERVER IP ip-Specify IP Address of Collection Server

COLLECTION-SERVER PORT port-Specify Port of Collection Server

COLLECTION-SERVER DES KEY key-Specify Des Key of Collection Server

COLLECTION-SERVER DES LEVEL level-Specify Des Level of Collection Server

DETECTOR INBOUND THRESHOLD-set the inbound call recording detector threshold

DETECTOR OUTBOUND THRESHOLD-set the outbound call recording detector threshold

SHOW CRC STATUS-display Call Recording Cache related status

SHOW CRC CONFIG-display Call Recording Cache Configuration

SHOW CRC CONNECTIONS-display Connected Recording Spans

****HELP SIP-TYPES:SIP:SIP Signal Proxy:SIP Media Proxy**

Call Processor Specific Commands

SHOW SIP CONFIG-display SIP network/HA configuration

SHOW SIP TRUNKS-display SIP trunk configuration

SHOW SIP STATUS-display Signaling/Media Proxy network connection status

SIP PURGECALL chan|all-terminate/purge call on specified channel

NETFILTER enable|disable-turn on/off the IP layer appliance packet firewall

SIP INLINE-place SIP signaling proxy inline

SIP OFFLINE-place SIP signaling proxy offline

Signaling Proxy Specific Commands

NETFILTER enable|disable-turn on/off the IP layer appliance packet firewall

SIP VIA FORCE on|off-configure how SIP messages are routed to next hop

 ON: route SIP packets based on trunk configuration

 OFF: route SIP packets based on received VIA header

SIP VIA TOGGLE on|off-route outgoing message to peer that last sent message (on) or

SIP VIA SHOW-display the force and toggle configuration

SHOW SIP STATUS-display SIP trunk and interface status (up/down)

SHOW SIP TRUNKS-display SIP trunk configuration

SHOW CALLPROC IP-display the private IP address of the Call Processor node

SHOW CALLPROC PORT-display the private IP port of the Call Processor node

SIP TRACE cmd [value]-configure SIP message tracing

Supported 'cmd' tokens:

ON: log incoming and outgoing data to a file

OFF: turn off all logging

UPLOAD: send the log file to the Management Server

CANCEL: abort any file transmission in progress

DEL: delete log files

LEVEL n: set the debug level to n, where n is 1-9

SIZE-nnnn: set the trace log file maximum size, where nnnn is 1-2000 (MB)

FROM MAP **set**|delete|show-configure/show From header mapping

REQUIR **MAP set**|delete|show-configure/show Request URI header mapping

TO MAP **set**|delete|show-configure/show To header mapping

NETFILTER enable|disable-turn on/off the IP layer appliance packet firewall

SIP VIA FORCE on|off-configure how SIP messages are routed to next hop within a DNS/SRV cluster

 ON: route SIP packets based on trunk configuration

 OFF: route SIP packets based on received VIA header

SIP VIA TOGGLE on|off-configure how SIP messages are routed to next hop within a DNS/SRV cluster

 ON: route SIP packet to peer that last sent message to Signaling Proxy

 OFF: route SIP packet to first in-service peer

SIP VIA SHOW-display the force and toggle configuration

SHOW SIP STATUS-display SIP trunk and interface status (up/down)

SIP REJECT SET-configure SIP response code and text for SIP INVITE rejection

SHOW SIP REJECT-display configured SIP response code and text for SIP INVITE rejection

SHOW MP REACTION TIME-display Media Proxy reaction time statistics

Media Proxy Specific Commands

SHOW CALLPROC IP-display the private IP address of the Call Processor node

SHOW CALLPROC PORT-display the private IP port of the Call Processor node

SHOW CHECKPOINT IP-display the private IP address(es) of the Media Proxy nodes

SHOW CHECKPOINT PORT-display the private IP port of the Media Proxy nodes

SHOW MEDIAPROXY IP-display the Media Proxy IP address

SHOW MEDIAPROXY PORT-display the Media Proxy

SHOW SIGPROXY IP-display the Signaling Proxy IP address

SHOW SIGPROXY PORT-display the Signaling Proxy IP port

SHOW SIP TRUNKS-display SIP trunk configuration

NETFILTER enable|disable-turn on/off the IP layer appliance packet firewall

SHOW MEDIAPROXY REC-display active call recording count

****HELP SHOW EVENTS-TYPES:E1:T1:SS7-TRUNK:ANALOG:PRI**

SHOW TRUNK-display status of each channel in the trunk

SHOW EVENTS num mask|all chan-display num events of type mask for channel

SHOW EVENTS 50 AB+DSP+TYPE 2display last 50 AB bit, DSP, and Call Type events

LIU CO-Hook State-0x00000001-MODEM V.21-0x00010000

LIU CPE Hook State-0x00000002-MODEM V.23-0x00020000

LIU Ring State-0x00000004-MODEM Bell 103-0x00040000
MODEM Tone-0x00080000
AB CO-A Bit-0x00000010
AB CO-B Bit-0x00000020-TYPE Modem-0x00100000
AB CPE A Bit-0x00000040-TYPE FAX-0x00200000
AB CPE B Bit-0x00000080-TYPE STU-0x00400000
TYPE Voice-0x00800000
PULSE CO-Hook State-0x00000100-TYPE WideBand-0x01000000
PULSE CPE Hook State-0x00000200-TYPE Busy-0x02000000
PULSE Digit CO-0x00000400-TYPE Unanswered-0x04000000
PULSE Digit CPE-0x00000800-TYPE Undetermined-0x08000000
DSP DTMF Digit-0x00001000-TRANSITION Valid-0x10000000
DSP MF Digit-0x00002000-TRANSITION Invalid-0x20000000
DSP Data Energy-0x00004000
DSP Call Progress-0x00008000

****HELP UNIX-TYPES:ALL**

The following are Unix/DOS style commands which are synonyms for standard ETM commands.

dir-SHOW FLASH dir-display Appliance flash directory
ls-SHOW FLASH dir-display Appliance flash directory
history-SHOW HISTORY-display most recent entered commands
more-MAINT MORE filename-display the specified file
ps-SHOW MEMORY-display Appliance memory utilization
uptimeSHOW STATUS-display general status of Appliance
who-SHOW USERS-display list of active logged on users

Ping and Traceroute

The following commands are available on the 1012, 1024, 1090, and 3000 series appliances:

PING | PING6 ip-sends ECHO_REQUEST to network

TRACEROUTE ip-show packet route

****HELP MAINT COMMANDS-TYPES:ALL**

The following are maintenance commands only to be used when directed by SecureLogix Corp. support personnel. Incorrect use of these command could impair operation of the ETM(R) Appliance.

MAINT CONFIG ERASE key|all-erase specified key from ConfigMgr

MAINT CONFIG RESET spanNum-reset the span's config to the defaults

MAINT DELETE file-delete the specified file

MAINT DOWNLOAD pkg_version-download specified software package from MS

MAINT DSP COUNTERS [chan]-display the number of low level DSP events

MAINT EVENTS mask|all|none-set event socket mask (see SHOW EVENTS above)

MAINT ISDNall|none-set ISDN-socket mask on|off

MAINT LOAD PLD-filename-program the PLD(s)

MAINT LOG SKIP recNum-do not send the specified recNum to the MS

MAINT MANUAL INLINE enable|disable manual intervention required to go inline

MAINT MOREfilename-display the specified file

MAINT CARD TYPE rate type-set card rate (T1/E1) and signaling (CAS,PRI)

MAINT SPAN TYPE num-type-set span type (CAS,PRI,SS7,SS7-SL, OFF)

MAINT TEST LED-cycle the T1/E1 LEDs

MAINT TEST SMDR on|off-use loop back cable and test SMDR reader

MAINT VERIFY filename-verify file contents checksum

****HELP SHOW COMMANDS —TYPES:ALL**

SHOW AAA NETWORK-display AAA network status

SHOW CALL COUNTERS-display call progress counters

SHOW CALL PROGRESS-display dsp call progress settings

SHOW CHANNELS-display channel specific values

SHOW COMPANDING-display channel companding: A-law, U-law

SHOW CONFIG-display summary of Appliance configuration items

SHOW CONSOLE TRACE-display captured console output

SHOW DES-display Appliance DES secret key and configuration

SHOW E1-display E1 parameter values, alarms, and statistics

SHOW E1 COUNTERS-display E1 line statistics

SHOW EXTENSIONS-display extension map

SHOW FEATURES-display Appliance and application minor features

SHOW FLASH dir-display Appliance flash directory

SHOW HELP-display ETM command summary

SHOW HISTORY-display most recent entered commands

SHOW IF-display Appliance network interface

SHOW IP-display Appliance IP address, netmask and IP gateway

SHOW ISDN-display ISDN and NFAS settings

SHOW LICENSE-display ETM 3000 license string and licensed features

SHOW MAC-display Appliance MAC address

SHOW MAP-display current Extension/Redirection Map

SHOW MEMORY-display Appliance memory utilization

SHOW PANIC-display the last fatal error recorded by the Appliance

SHOW POLICY FILE-display current security policy

SHOW POLICY STATUS-display policy enforcement, num calls, etc

SHOW PORT STATUS-display MDI/MDI-X port status

SHOW POTS-display POTS parameter values

SHOW QUEUE-display Appliance queue list
SHOW SERIAL-display serial port settings
SHOW SERVER-display MS IP address, port, and heartbeat
SHOW SIGNALING-display signaling type for each channel
SHOW SMDR-display SMDR serial port and processing settings
SHOW SS7-display SS7 configuration and status values
SHOW SS7 CIC-display SS7 CIC/channel assignments on bearer span
SHOW SS7 NET-display SS7 network status
SHOW STATUS-display general status of Appliance
SHOW T1-display T1 parameter values, alarms, and statistics
SHOW T1 COUNTERS-display T1 line statistics
SHOW TELNET-display status of Telnet and enable/disable IP list
SHOW TIME-display Appliance current time
SHOW TRUNK-display current trunk channel states
SHOW USERS-display list of active logged on users
SHOW USERNAMES-display list of defined usernames
SHOW VERSIONS-display Appliance, DSP, & security policy versions
SHOW VERSIONS ALL-display hardware and firmware version and rev

****HELP SHOW COMMANDS — TYPES:PRI:E1-PRI:SS7-TRUNK:T1**

SHOW IPS POLICY-display IPS policy file contents
SHOW IPS STATUS-display IPS subsystem status
SHOW IPS TERMINATIONS-display IPS rules actively terminating calls

****HELP ANNOUNCE-TYPES:ANALOG**

ANNOUNCE NOTIFY en|dis chn|all-enable or disable announcement on a per channel basis
NOTIFY FILENAME filename-set the notification wav file name

RINGS BEFORE ANSWER default|rings-number of rings to allow before answer

POST RING DELAY default|delay-time (msec) after Ring/before Answer

POST ANSWER DELAY default|delay-time (msec) after Answer/before Notify

POST PICKUP DELAY default|delay-time (msec) after PBX Answer/before ETM Hangup

RINGBACK INTERVAL default|delay-time (msec) between ringbacks

RINGBACK LIMIT default|rings-number of rings to generate before abandoning call

NO ANSWER ACTION default|save|destroy-action to take with recording if no parallel answer

END ON BUSY true|false-abandon call on receipt of busy signal

END ON DIALTONE true|false-abandon call on receipt of dialtone

ANNOUNCE SET enabled|disabled-sets global call announcement state

SHOW ANNOUNCE-displays the call announcement configuration

RING GENERATOR enable|disable-enables/disables use of an external ring generator

****HELP RECORD-TYPES:T1:PRI:ANALOG:E1:E1-PRI:SS7-TRUNK:E1-SS7-TRUNK:J1**

CALL RECORDING enabled|disabled-sets the global call recording state

CACHE IP ip address-sets the IP Address of the Call Recording Cache

CACHE PORT port-sets the listener port of the Call Recording Cache

RECORDING LENGTH default|length-sets the maximum recording length in minutes

RECORD INBOUND en|dis all|chn-sets the channel level inbound recording flags

RECORD OUTBOUND en|dis all|chn-sets the channel level outbound recording flags

RECORD REQUIRE SMDR YES|NO-turn on/off whether or not inbound SMDR is required to save the recording

RECORD PROTECT ADD extension-Add a protected extension

RECORD PROTECT DEL extension-Remove a protected extension

SHOW RECORD CONFIG-displays the span level call recording configuration

SHOW RECORD STATUS-displays the span level call recording status

SHOW RECORD POLICY-displays the call recording policy file

SHOW PROTECTED EXTENSIONS-displays the protected extensions

SHOW DETECTOR STATS-displays the recording detector hourly statistics

Ports and Services

Component	Description	Default Port	Where Configured	Protocol	Encrypted	Serves	Access Restricted to
MS	Appliance Listener Port	4313	twms.properties [Port]	TCP	Yes	TA, CA	Auth. Card IP Addr
MS	RMI Port	6990	twms.properties [RMIPort]	TCP	Yes	PM	Auth. Client IP Addr
MS	Dispatcher Port	6991	twms.properties [DispatcherPort]	TCP	Yes	PM	Auth. Client IP Addr
MS	Client Port	Note 1	twms.properties [TWMSObjectStartPort]	TCP	Yes	PM	Auth. Client IP Addr
RS	Dispatcher Port	6992	twms.properties [ReportDispatcherPort]	TCP	Yes	PM/MS	Auth. Client IP Addr
RS	Usage Manager Client Port	Note 1	twms.properties [ReportServerStartPort]	TCP	Yes	PM/MS	Auth. Client IP Addr
RS	RMI Daemon	6993	ETMReportService.cfg [RMID_Port]	TCP	No	MS	No Restriction (only used internally, not externally accessible)
DBS	TNS Listener Port	1521	listener.ora	TCP	No	MS/RS/DBT	No Restriction
TA	ICMP Ping	N/A	Cannot be configured	ICMP	No	Any host	MS and Telnet Allow IP Addr
TA	Telnet	23 - 26	Can be disabled by editing card security level.	TCP	No	Any host	MS and Telnet Allow IP Addr
TA	PRI NFAS Primary	Note 2	Configured per span when required for NFAS trunk groups	TCP	Yes	TA	NFAS group member IP Addr
TA	PRI NFAS Backup	Note 2	Configured per span when required for NFAS trunk groups	TCP	Yes	TA	NFAS group member IP Addr
TA	SS7 Signaling Link	Note 3	Configured per span when required for NFAS trunk groups	TCP	Yes	TA	SS7 group member IP Addr
CA	CRC Listener	4398	Edit CRC configuration	TCP	No	TA	Auth. Card IP Addr
CS	Listener	6999	Edit Collection Server configuration	TCP	Yes	CA	Auth. CA IP Addr

Note 1 By default, this is an anonymous port, but it can be configured to use a defined port.

Note 2 ISDN PRI NFAS listener ports are configured when needed for telecommunications appliances managing NFAS trunk groups. No default ports exist; each NFAS group is configured with hard port assignments when created.

Note 3 SS7 listener ports are configured when needed for telecommunications appliances managing SS7 trunk groups. No default ports exist; each SS7 group is configured with hard port assignments when created.

MS = ETM Server Application

RS = ETM Report Server Application, which is typically hosted on a common platform with the MS

DBS = Oracle RDBMS Server Application, which is typically hosted on a common platform with the MS

PM = Performance Manager

TA = ETM Telecommunications Appliance ETM 1012, 1024, 1090, 2100, 3200

CA = ETM Call Recording Cache Appliance ETM 1060

CS = ETM Call Recording Collection Server Application