SecureLogix®
We see your voice®

ETM® (Enterprise Telephony Management) System

v7.1.1

Installation Guide

About SecureLogix

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

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

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

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

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

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

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

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

IMPORTANT NOTICE:

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

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

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

This product includes:

Data Encryption Standard software developed by Eric Young (eay@mincom.oz.au),
© 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 11

Installation Overview 15

Installation Quick Start 19

Step 1: Software Installation 23

Step 2: Hardware Installation 49

Step 3: ETM® System Configuration 61

Appendix A: Appliance Technical Specifications, Connectors, and Pinouts 173

Appendix B: Removing and Replacing TDM Appliance Components187

Appendix C: Span Telco Settings Reference 197

Appendix D: Database Directories and File Names Reference 201

Appendix E: TDM Appliance Status LEDs 203

Index 207

Preface

About the ETM® System Documentation

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

ETM® System User Guides

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

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

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

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

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

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

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

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

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

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

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

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

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

Additional Documentation on the Web

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

http://support.securelogix.com

Tell Us What You Think

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

docs@securelogix.com

Conventions Used in This Guide

The following conventions are used in this guide:

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

  Click **View | Implied Rules**.

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

  Highlight the field and press DELETE.

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

  Press CTRL+ALT+DELETE.

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

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

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

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

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

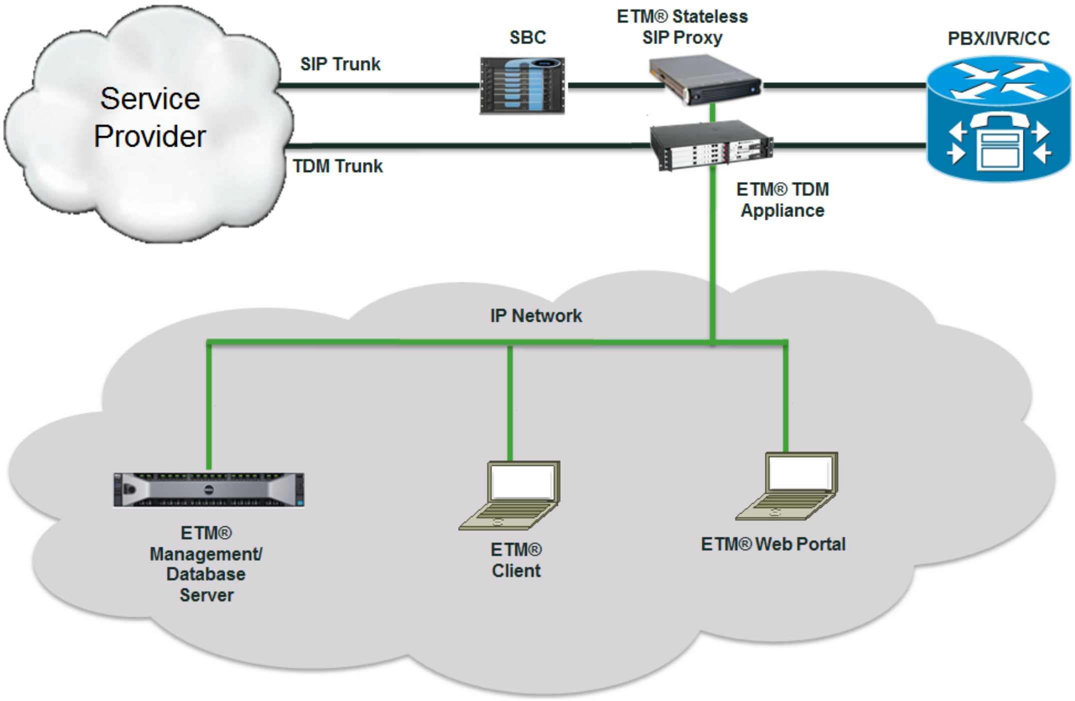
- *Italics* indicate web addresses and names of publications.
- ETM System components and features are capitalized

Installation Overview

Installation Considerations

As with any major telecommunications installation, it is necessary to have a detailed installation plan before actual installation begins. Before you begin installing the ETM® System, take the time to conduct a thorough site survey to identify the details of the telecommunications environment the ETM System is to monitor and the TCP/IP network on which it is to communicate. This approach helps minimize unforeseen complications arising from unique characteristics of a site's phone system or TCP/IP network.

The diagram below illustrates how a completed ETM System installation at a site with both SIP and TDM trunks might look.



This example demonstrates several typical characteristics of an ETM System deployment:

- ETM SIP Appliance location between the SBC and PBX and TDM Appliance adjacent to the PBX
- Dedicated subnet
- Remote ETM System Console on user's desktop computer

Choosing Locations for ETM® System Components

ETM TDM and inline SIP applications and appliances are located inline with your customer-premises telecom equipment to monitor usage and control access to your telecommunications network. UTA appliances or applications are not inline, but still provide all of the ETM System functionality. In a standard deployment, ETM Appliances are typically located on the telephone network side of the PBX, as close as possible to the PBX. Appliances can also be deployed on outside lines that bypass your PBX.

You should install the Management Server and Appliances in a secure location and access to them should be limited. Installing the Management Server and Appliances on a dedicated subnet can provide network security as well as protect Station Message Detail Recording (SMDR) and other transmitted data. Triple DES encryption provides additional security.

Appliance Location

Additional Appliance location considerations include:

- TDM and analog Spans in the 1024, 1090, 2100, and 3200 ETM Appliances should be placed on the trunk side, between the telephone network and the CPE, as close to the CPE as possible.
- ETM Call Recording Cache (CRC) Appliances can be located anywhere that has TCP/IP network connectivity for communication with the Recording Spans, ETM Server, and Collection Server (if used). A low-latency network connection is best, since no recording can occur if the Recording Span cannot connect to the CRC.
- SIP Appliances are installed logically inline on SIP trunks.
- The UTA appliance interfaces directly with the Cisco router using the Cisco Unified Communication(UC) Gateway Services API. UTA is not inline with either signaling or media. Signaling and call information is exchanged through Web Services calls with the iOS API, and the API forks a copy of the media and sends it over a socket connection to the UTA Media Proxy. The API also provides call state, call control functionality, and trunk status to UTA.

Management Server Location

The ETM Management Server should be located in an area with a high level of physical security, such as a server room, and you should maintain good, industry-standard security practices for securing the operating system on the Management Server computer. If you choose not to use DES encryption, it is recommended that the Management Server communicate with its Spans on a dedicated subnet within your LAN so that SMDR and other transmitted data will have a layer of security protection. A dedicated subnet can also be used so that the ETM System network traffic will not have to compete with other network traffic.

Report Server Location

Each ETM Server is associated with a specific Report Server. The Report Server is typically installed on the same computer as the ETM Server, although with proper configuration, it can be installed on a separate computer.

ETM® System Client Location(s)

The ETM System can be managed from the ETM System Client installed on the Management Server host computer and from remote ETM System Clients. If you will be using remote ETM System Clients:

- Ensure that the host computers meet minimum system requirements for the ETM System Client. Minimum system requirements are provided on an insert provided with your ETM System and can also be found on the SecureLogix Knowledge Base at *http://support.securelogix.com*.
- Note the IP addresses or subnet of the ETM Client host computers. The ETM Management Server maintains a list of authorized Clients, which you provide during configuration. Only ETM Clients in this list are allowed to connect. You can authorize ETM Client connections from specific IP addresses or from one or more subnet masks.

Data Network Considerations

The distributed client/server architecture of the ETM System enables centralized control of dispersed telecommunications resources. Each ETM Appliance Card is equipped with an Ethernet 10/100 Base-T network port that accepts an RJ-45 connector. ETM System components communicate via the TCP/IP networking protocol. Both IPv4 and IPv6 are supported.

Types and Amount of IP Data Network Traffic

In an ETM System deployment, IP network traffic exists between:

- **Management Servers and Appliance components, the ETM System Console, and the ETM Database.** Downloading new software to multiple Cards simultaneously can create a short burst of high traffic. Ongoing call events can generate moderate traffic if many Spans are monitored and if call rates are high. SMDR can generate low to moderate traffic depending on the number of lines handled by the PBX and their associated activity.
- **Spans within an NFAS Group**. NFAS Group member Spans communicate signaling information from the NFAS Group member with the primary or backup D channel to other Spans in the same NFAS Group. The traffic level is small to moderate, depending on the level of call activity.
- **Spans within an SS7 Group**. SS7 Bearer-to-SS7 Signaling Link communication generates small to moderate traffic, depending on the level of call activity.

- **Usage Manager and the ETM Database**. The Report Server connects to the ETM Database to gather call data for reports. Traffic is generally low; however, certain reporting activities, such as generating a report with a large volume of call data, can generate significant traffic.
- **Performance Manager and the Management Server**. The Performance Manager connects to the Management Server to monitor operations, download Policies, and view logs. Traffic between the Performance Manager and the Management Server is generally low; however, certain monitoring activities, such as viewing the **Policy Log** or **Call Monitor** during high activity, can generate significant traffic. Downloading Policies and configuration to multiple Cards/Spans simultaneously can generate bursts of high traffic, but these activities are typically infrequent.
- **The ETM Database Maintenance Tool and the ETM Database**. The ETM Database Maintenance Tool connects to the ETM Database to populate and maintain the database. Network traffic is generally low but depends on the amount of data in the database during maintenance and upon the procedure being performed. Importing and exporting data instances can generate high traffic if a large amount of data is present; other tasks create little traffic.

Securing ETM® System IP Data Network Traffic

The ETM System generates a low-to-moderate level of IP data network traffic that could contain sensitive information. The ETM System includes 3DES encryption that secures data transmitted among ETM System components. For additional security and/or if IP data network traffic is a concern at your location, consider the following approach when deploying an ETM System:

- Put ETM Appliances in a subnet separate from your main data network. Placing Appliances in a subnet allows the traffic to be isolated, and enables varying levels of network security to be implemented, depending on your organization's needs. For example, switched routers or hubs can be used to implement basic security measures, while using a dual-homed (2 NIC Cards) machine for the Management Server or isolating the subnet behind an IP firewall implements stronger network security.
- Place the ETM Server, Database, and Database Maintenance Tool within that subnet if possible. Management Server/Card/Database communication contributes to overall network traffic, and may contain sensitive data, such as when SMDR is in use or when DTMF digits are captured throughout call duration.

Installation Quick Start

Understanding the Installation Process

It is strongly recommended that you read *the ETM® System User Guide* and the installation overview chapter of this guide, before beginning your ETM System installation.

This installation guide is designed to walk you through all required procedures in the order in which they are to be performed. Just as an experienced pilot performs preflight procedures before every flight, so you should progress through this guide from start to finish to ensure that all procedures are correctly completed in the proper order, even if you have installed an ETM® System before. Missing or incorrectly performed steps can cause difficult-to-troubleshoot problems that can easily be avoided by following the procedures exactly as written here.

An installation checklist outlining the installation steps is provided below. The remainder of this guide provides detailed instructions for each step.

IMPORTANT If you are upgrading from a previous version of the ETM System, contact SecureLogix Customer Support for important upgrade information before beginning installation.

Installation Process

ETM System installation consists of the following sequence of steps. The checklist below is provided for you to check off each step of the installation as it is completed.

Check	Installation Procedure and Reference Page Number
	Software and Database Installation
	Install the ETM Software: ETM Server, Report Server, Database Maintenance Tool, and ETM System Console. (p. 24)
	License the ETM Server and, if on a separate computer, the Report Server. (p. 30)
	Install, configure, and populate the Oracle DBMS and ETM Database. (p. 32)
	Copy the version-specific Oracle database driver to the ETM Server installation folder. Also copy this file to any remote Report Server installation directory. (p. 32)
	If the Database is installed on a different computer from the ETM Server, install the Oracle Client Tools on the ETM Server computer and copy **tnsnames.ora** and **listener.ora** from the ETM Database computer to the remote ETM Server computer.
	Configure the Management Server with the path to the SQL*Loader database utility. (p. 33)

Installation Procedure and Reference Page Number, continued

Check	Installation Procedure and Reference Page Number
	Configure the ETM applications to communicate through a NAT firewall, if applicable. (p. 42)
	Authorize remote ETM System Console(s) to connect to the Management Server, if applicable. (p. 143)
	Associate the Management Server with its Report Server, if installed on a different computer. (p. 144)
	Appliance Installation and Configuration
	Note: If you are installing ETM SIP Appliances, refer to the *ETM® SIP Appliance Installation and Configuration Guide* for out-of-box configurations instructions. If you are installing UTA, see the *ETM® Unified Trunking Application (UTA) Installation and Configuration Guide* for out of box configuration instructions. Both of these guides can be found in the SecureLogix Knowledge Base. Then return to this guide to complete system configuration through the ETM System Client.
	(*ETM 2100/3200 only*) Install Digital Trunk Interface/Controller Card pairs in the Appliances. (p. 50)
	Install the Appliance(s) in the rack. (p. 50)
	Connect the SMDR cable, if applicable. (p. 51)
	Connect power to the Appliances. (p. 52)
	(*TDM Appliances only*) Using a direct serial connection to each Appliance Card, perform initial network configuration to enable the Card to communicate with the Management Server. (p. 54)
	Change the Management Server's TCP/IP port in the **twms.properties** file if the default of 4313 causes a conflict with another device or service. (p. 59)
	Connect the Ethernet cable(s).
	Authorize Appliance Cards to connect to the Management Server. (p. 68)
	Complete Card configuration. (p. 73)
	Complete Span configuration. (p. 86)
	Define and install location-specific Dialing Plans. (p. 123)
	Configure the ETM System for SMDR (p. 127), Call Recorder SMDR Extensions (p. 135), and NFAS)p.135),, if applicable.)
	Make a cutover plan. (p. 149)
	Connect the telecom cables (*TDM only*) and execute the cutover plan. (p. 150)
	(*TDM Appliances only*) Check line voltage. Contact Customer Support for applicable limits.
	(*TDM Appliances only*) View LEDs to verify Appliance operation. (p. 152)
	View the **Diagnostic Log** for errors. (p. 156)
	View the **Call Monitor** to verify that the Spans are processing calls. (p. 158)

After you have completed all of the procedures listed above:

- Refer to the *ETM® System User Guide* for task-oriented instructions for using the ETM System, with references to the other guides as applicable.
- Refer to the *Voice Firewall User Guide* for instructions for using Voice Firewall Policies.
- Refer to the *Voice IPS User Guide* for instructions for using Voice IPS Policies.
- Refer to the *Call Recorder User Guide* for instructions for recording and accessing calls with the Call Recorder.
- Refer to the *ETM® System Administration and Maintenance Guide* for task-oriented instructions such as configuring user accounts and ETM Management Server settings. monitoring telco status, and managing ETM Appliances.
- Refer to the *Usage Manager User Guide* for instructions for producing reports of telecommunications monitoring and Policy enforcement.
- Refer to the *ETM® System Technical Reference* for system backup information, properties and configuration file settings, Dialing Plan and SMDR information, ETM Commands, error and debug messages, and other technical information.

Step 1: Software Installation

Introduction

This chapter explains how to install the following:

- ETM Management Server
- ETM Database
- ETM Database Maintenance Tool (used to populate, configure, and maintain the ETM Database)
- ETM System Client applications (includes the ETM System Console, Performance Manager, and Directory Manager, and Usage Manager)
- Report Server

Since the ETM System components communicate via TCP/IP, you can install all of the ETM applications on the same computer, or you can install components on separate computers in any combination. Components can also be installed on different supported operating systems. You can also install any number of remote ETM System Clients on user workstations.

See "ETM System Concepts" in the *ETM® System User Guide* for a detailed discussion of each of the applications and the ETM System architecture.

Refer to "Minimum System Requirements" on page 23 and then begin installation by following the instructions in "Install the ETM® Software" on page 24.

Minimum System Requirements

System requirements depend on the number of Spans and the call volume to be monitored. For detailed information about hardware and memory requirements for installation and use of the ETM System, see the SecureLogix Knowledge Base at *http://support.securelogix.com* or contact Customer Support.

Supported Operating Systems

The ETM System applications can be installed and run on supported versions of Linux and Windows. See the SecureLogix Knowledge Base at *http://support.securelogix.com* for supported operating system versions and other detailed information about system requirements, or contact SecureLogix Technical Support Support.

Supported DBMSs

The ETM System supports two versions of the Oracle DBMS on both Windows and Linux. Since support for additional versions of Oracle may be tested after the publication of this guide, see detailed information on the SecureLogix Knowledge Base at *http://support.securelogix.com* or contact Customer Support.

Install the ETM® Software

See the minimum system requirements on the SecureLogix Knowledge Base at *http://support.securelogix.com* or call SecureLogix Customer Support for detailed information about hardware requirements based on the number of phone lines to be monitored.

You can install all of the applications together on a single computer, or you can install the Management Server, ETM System Console (used to login and access the ETM System applications includes the Directory Manager, Performance Manager, and Usage Manager), and Report Server on separate computers. You can install multiple ETM System Consoles on remote workstations.

Software Installation Steps

Software installation consists of the following sequence of steps:

1. Install the ETM Software.
2. License the Management Server and Report Server.
3. Install the Oracle DBMS.
4. Configure the ETM Database.
5. Copy the Oracle database drivers to the ETM Software installation directory.

Begin installation with the applicable operating-system specific software installation procedures:

- "Installing the ETM® Software (Linux)” on page 25.
- "Installing the ETM® Software (Windows)" on page 27.

About Multiple Application Instances

Multiple application instances of the Management Server and Report Server can be installed on a single computer. If you plan to install multiple instances, see "Running Multiple Application Instances on One System" in the *ETM® System Technical Reference* for instructions, and then resume this guide with "License the Management Server and Report Server" on page 30. The procedures below explain typical installation of a single instance.

Installing the ETM® Software (Linux)

The ETM Server and Client can be installed and run on 64-bit Cent OS or Redhat Linux v6.2 or later.

Before you begin

- When you install and configure your Linux platform, allocate space for the ETM applications under **/opt**. ETM RPMs are installed under **/opt** and the installation directory cannot be changed.
- The JVM switch **java.awt.headless=true** is not supported, although most application functions appear to be unimpaired in such a configuration. For a supported configuration and especially to enable the Server to save reports to the tree in Usage Manager, install the **xorg-x11-server-Xvfb** package for RedHat or CentOS.

Installing the ETM Applications

Three installation (RPM) files are included for the Linux ETM Server and Client installation:

- **etm-esc-<version-build>.x86_64.rpm** – ETM System Console only
- **etm-ms-<version-build>.x86_64.rpm** – ETM Management Server only
- **etm-rs-<version-build>.x86_64.rpm** – ETM Report Server only

To Install the ETM® applications on Linux

Execute the following sequence of steps to install each required RPM (not order-dependent):

1. Log in as **root** user.
2. Change to the directory containing the RPM files.
3. Determine whether previous RPMs are installed by typing
   '**rpm –qa |grep –i etm-**'
   - If RPMs exist, remove them by typing
     'rpm –e <rpm_name>' where <rpm_name> is one of
     'etm-esc', 'etm-ms', or 'etm-rs'
4. Install each required RPM by executing the command,
   rpm –ivf <complete_rpm_file_name>

   Files are installed in the **/opt/SecureLogix/ETM** directory with the exception of the Service specific files, which are installed in the **/etc/init.d** directory. The installation directories cannot be changed.

5. From within the ETM directory, execute the **GetSystemID** script by typing '**./GetSystemID**' .If the **GetSystemID** script returns an ID of 00000000, add the system's IP address and host name to the host file **(/etc/hosts**) and then execute the script again. Supply the system ID to SecureLogix Customer Support to obtain a server license file. Place this license file in the **/opt/SecureLogix/ETM** directory.

6. Use **chkconfig** command ('**chkconfig –level 345 <servicename> on'**) or the Services GUI to set the Management Server (**ETMMS**)and Report Server (**ETMRS**)services to start automatically when the system is started.

Java Heap Space settings on a Linux Management Server

The **ETMManagementService.cfg** file contains settings related to the Java Heap space. These settings are as follows:

- **-Xms** = the initial (and minimum) java heap size. **Xms** value cannot exceed **Xmx** value.
- **-Xmx** = the maximum java heap size.
- **PermSize** = initial (and minimum) additional separate heap space to support the **Xmx** value mentioned above. The heap space stores the objects and the **PermSize** space keeps required information about those objects. Therefore, the larger the heap space, the larger the **PermSize** must be.
- **MaxPermSize**=the maximum perm space allocated.

By default, **MaxPermSize** is 32MB for **-client** and 64MB for **-server**. However, if you do not specifically set both **PermSize** and **MaxPermSize**, the overall heap size does not increase unless it is needed. If you set both **PermSize** and **MaxPermSize**, the extra heap space is allocated at server startup and remains allocated.

Continue with "License the Management Server and Report Server" on page 30.

Installing the ETM® Software (Windows)

The default installation path for all of the ETM applications, system files, and documentation is **C:\Program Files\SecureLogix\ETM**.

IMPORTANT INFORMATION for installing on Windows: A feature called User Account Control (UAC) limits application software to standard user privileges and only provides administrator level privileges if authorized by an Administrator-level user. In addition to requiring administrator privileges to perform administrative functions, UAC also introduced File and Registry Virtualization, which causes user-level programs to write data and registry settings to a virtual area for the given user, rather than to a system directory (such as Program Files) or the registry. Various functions, scripts, and installations in the ETM System may be adversely affected.

To prevent issues, do one of the following when installing on one of these operating systems:

- Ensure a user with Administrator privileges installs the ETM System applications and then run the applications as Administrator rather than local user.
- Install the ETM System in a directory that is not a system directory (for example, not in Program Files).
- Disable the UAC feature on your operating system.

To install the ETM® Applications on Windows

1. Insert the installation CD into the CD-ROM drive.
2. Open **My Computer**, double-click the CD drive letter, and then double-click **Software\Installer\setup.exe**. If the Windows installer Service is not yet installed on your system, it is installed from the installation CD. The **InstallShield Wizard Welcome** dialog box appears.
3. Click **Next**. The **License Agreement** dialog box appears.
4. Read the license agreement. If you agree with the terms, click **I accept the terms in the license agreement**, and then click **Next**. You must accept the terms of the license agreement to continue with the installation.
5. The **Customer Information** dialog box appears. In the **User Name** and **Organization** boxes, type your user name and organization, and then click **Next**.
6. The **Destination Folder** dialog box appears. Do one of the following:
   - Click **Next** to install in the default directory.

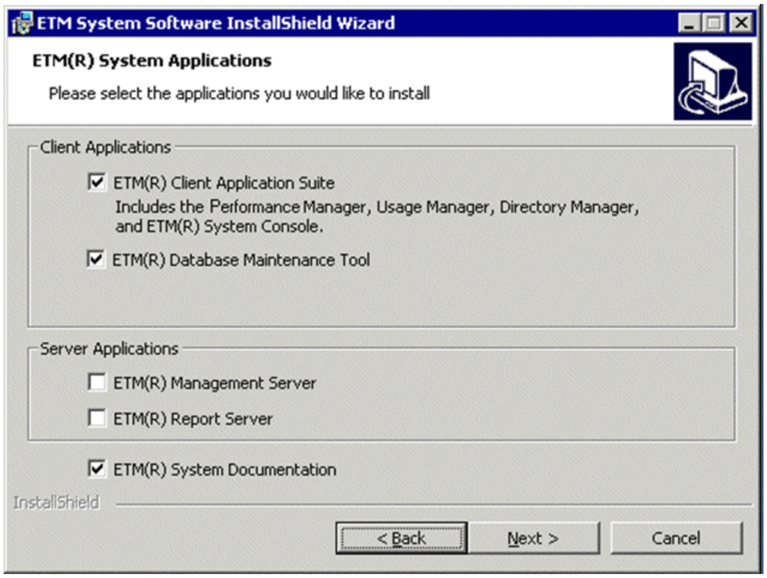
- Click **Change** to specify a different directory. When done, click **Next**.

7. The **Setup Type** dialog box appears. Select one of the following installation types:

- **Typical**. A typical installation includes the ETM Client applications, Database Maintenance Tool, and ETM System documentation; optionally, you can select to install the ETM Management Server, and Report Server.

   a. Click **Typical**, and then click **Next**.

   The **ETM System Applications** dialog box appears.



ETM System Software InstallShield Wizard

ETM(R) System Applications

Please select the applications you would like to install

Client Applications

☑ ETM(R) Client Application Suite
Includes the Performance Manager, Usage Manager, Directory Manager, and ETM(R) System Console.

☑ ETM(R) Database Maintenance Tool

Server Applications

☐ ETM(R) Management Server

☐ ETM(R) Report Server

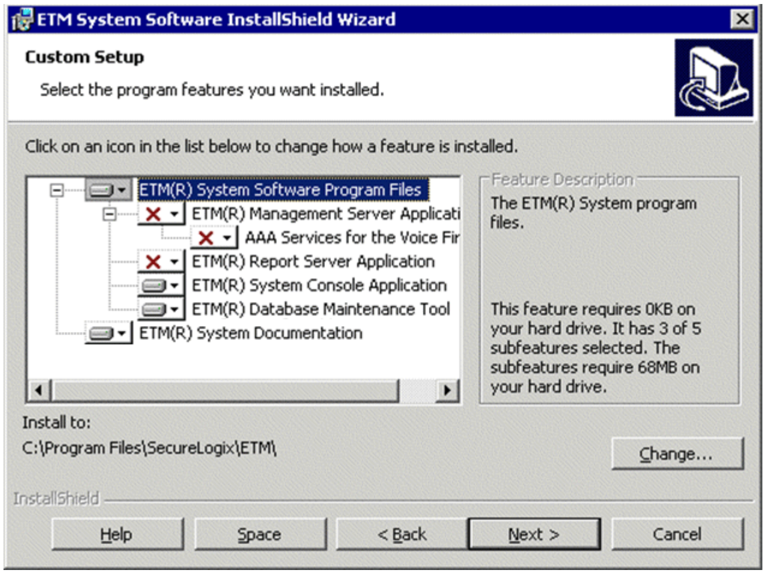
☑ ETM(R) System Documentation

   b. Select the check box for each application that you want to install; clear the check box for each application that you do not want to install.

   c. Click **Next**.

- **Advanced**. Allows customization of which program features will be installed, where they will be installed, and how much hard drive space is available/required for the installation.

   a. Click **Advanced**, and then click **Next**. The **Custom Setup** dialog box appears.



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- ETM(R) System Software Program Files
  - ETM(R) Management Server Applicati
    - AAA Services for the Voice Fir
  - ETM(R) Report Server Application
  - ETM(R) System Console Application
  - ETM(R) Database Maintenance Tool
- ETM(R) System Documentation

Feature Description

The ETM(R) System program files.

This feature requires 0KB on your hard drive. It has 3 of 5 subfeatures selected. The subfeatures require 68MB on your hard drive.

Install to:
C:\Program Files\SecureLogix\ETM\

b. Click the hard drive icon next to the application(s) that you want to install, and then click **This feature will be installed on the local hard drive**.

c. Click the hard drive icon next to the application(s) that you do not want to install, and then click **This feature will not be available**.

***CAUTION*:** If you select **This feature will not be available** for an installed feature, that feature is uninstalled.

d. Optionally, to verify that sufficient space is available in the location that you have specified, click **Space**. The **Disk Space Requirement** dialog box appears and indicates whether disk space is available on the specified volume for the selected features. Click **OK** to return to the **Custom Setup** dialog box.

e. To install in a different location, click **Change**. The **Change Current Destination Folder** dialog box appears. Type a new path, and then click **OK**.

8. Click **Next**. The **System Identification** dialog box appears, displaying the computer's system ID. The System ID is required to obtain a software license. See "License the Management Server and Report Server" on page 30 for information about how to view the system ID and licensing.

9. Click **Next**.

10. **The Ready to install the Program** dialog box appears. Click **Install**.

11. When the **InstallShield Wizard Completed** dialog box appears, click **Finish**.

When installation is complete, application shortcuts appear on your desktop and in the **Start** menu. Note that the ETM Management Service and ETM Report Service are set by default to be manually restarted if the computer is rebooted. If you want them to automatically restart, set them to **Automatic** in the Windows **Services** dialog box. See "Setting the Services to Autostart" in the *ETM® System Technical Reference* for instructions if necessary.

Continue with "License the Management Server and Report Server."

License the Management Server and Report Server

You must obtain a Management Server license before running the ETM Management Server and Report Server. If the Report Server is to be installed on a different computer than the Management Server, a separate license file must be placed in the Report Server installation directory. Without a valid license on its host computer, the Report Server will fail to initialize. Remote ETM System Clients do not require a license.

Obtain a Software License

To obtain the Management Server license

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

Changing the Management Server's TCP/IP Port for Card Connections

The default TCP/IP port on which the Management Server accepts connections from all Cards is 4313. If this port assignment is available on the ETM System host computer, skip this step and continue with "Create and Configure the ETM® Database" on page 32. If this port assignment causes a conflict with another application or device on the Management Server host computer, you can change this value in the **twms.properties** file as described below. You will then configure each Card with the new port number during out-of-the-box Card configuration in "Initial Card Configuration" on page 54.

To change the Management Server TCP/IP port for Card connections

1. On the Management Server computer, open **twms.properties** in a text editor.

   <INSTALL_DIR>\SecureLogix\ETM\twms.properties

2. Locate the lines that read:

   ```
   ## This is the designation of the port which
   ## the Management Server will have open to
   ## receive connections from the Appliances(s)
   Port=4313
   ```

3. Replace **4313** with the value you want to use. On Windows, selecting a value above 5000 is recommended.

Continue with "Create and Configure the ETM® Database" on page 32.

Create and Configure the ETM® Database

Creating and configuring the database consists of the following sequence of tasks:

1. Install a supported DBMS and then run the Perl scripts to configure the ETM Database for use by the ETM Server.
2. Copy the correct database driver to the ETM Server installation directory.
3. (*Does not apply with Oracle 11g XE; the ETM Server must reside on the same computer*.) If the database is on a different computer than the ETM Server, install the Oracle client tools on the ETM Server computer and then copy important database files from the database computer to the ETM Server.
4. Connect to the database with the ETM Database Maintenance Tool and complete database configuration.

Install and Configure the Oracle DBMS and Database

For information about supported Oracle versions, see the *Minimum System and Network Requirements* on the SecureLogix Knowledge Base at **http://support.securelogix.com*.*** Since the procedure for installing and configuring the Oracle DBMS varies according to the operating system on which it is to be installed and the version of Oracle to be used, those instructions are not included in this installation guide. See the SecureLogix Knowledge Base, or contact SecureLogix Customer Support.

The instruction document also describes the Oracle services the ETM System requires, to ensure that an existing installation meets the requirements.

Copy the Oracle Database Driver to the Required Locations

After installing and configuring the database, if you have not already done so, copy the Oracle driver file from **<ORACLE_HOME>\jdbc\lib** in your database installation to each of the following ETM® System installation directories:

- The ETM Server.
- Any remote Report Server.
- Any remote ETM Database Maintenance Tool.

Remote ETM System Consoles do not require the driver file.

By default, the ETM applications are installed at the following path:

Windows

C:\Program Files\SecureLogix\ETM

Linux

/opt/SecureLogix/ETM

Without the correct driver file, the applications are unable to connect to the database. The file is located at the following path on the computer on which you installed Oracle: **<ORACLE_HOME>\jdbc\lib\**

Special Instructions for a Remote ETM® Server Only

(*Does not apply to Oracle 11g XE; the ETM Server must be installed on the same computer as the database*.) If the ETM Server is installed on the same computer as the ETM Database, you do not need to perform this step, because these files are included in the database install. The Oracle Client Tools are used for importing Directory Listings and city/state data files. On a remote ETM Server installation, install the Oracle Client Tools, and then copy **tnsnames.ora** and **listener.ora** from **<ORACLE_HOME>\network\admin** to the same location on the remote Server. These files contain the SID, IP address, port number, and database schema of the ETM Database.

See "Install the Oracle Client Tools" in the ETM System Oracle installation documentation specific to your operating system and version of Oracle, available on the SecureLogix Knowledge base at *http://support.securelogix.com*. (Search on keyword **Oracle**.)

Where to Go From Here

Continue with one of the following:

- If the ETM System components will communicate through a NAT firewall, continue with "Connecting Through a Firewall" on page 42. If not, see the next bullet.
- Continue with "Database Preparation" on page 34.

Database Preparation

The instructions in this section apply to ETM System deployments with a single ETM Server. If multiple server instances and data warehousing are needed for large, dispersed deployments, the system can be configured with an ETM Repository with Managed Databases. For instructions on setting up an ETM Database Repository, see the Knowledge Base article “Setting up a Database Repository with Managed Databases” located at: **http://support.securelogix.com/knowledgebase.htm**

***CAUTION*:** To prevent database conflicts, Repositories, Managed Databases, and Standalone Databases must be assigned to different database schemas.

Using the ETM Database Maintenance Tool to prepare the database consists of the following sequence of procedures:

1. Open the ETM Database Maintenance Tool.
2. Provide database connection information: IP address, port number, database instance name (SID), and database schema.
3. Connect to the database using the username and password you defined for the ETM Server when you ran the Perl script.
4. Create the ETM tables.

   This step is only performed once per database schema; the same tables are used by all ETM Servers using this database schema. It is strongly recommended that you have only one ETM Data Instance per schema.
5. Create a data instance for the ETM Server.

   Each ETM Server uses a specific data instance within the ETM Database, enabling multiple Servers to store data in the same database. When you create this data instance, you also specify the initial password for the default **admin** user account on the ETM Server. Although you can create multiple data instances within a single database schema, it is strongly recommended that you use a separate schema for each ETM Server.
6. Enable the ETM Server to connect to the database by specifying its default data instance.

If you have not already done so, install the ETM software as described in "Install the ETM® Software" on page 24 before continuing with these procedures.

IMPORTANT Ensure that you have copied the correct database driver file for your version of Oracle from the Oracle installation to the ETM Server directory. The driver file is specific to the version of Oracle that you are running and can be found in **<ORACLE_HOME>\jdbc\lib**. If the correct driver is not present in the ETM System installation directory, the ETM Database Maintenance Tool and ETM Server cannot connect to the database. Although the driver file has the same name for several Oracle versions, the file is not actually the same. Be sure to use the one that came with your installation or upgrade.

Opening the ETM® Database Maintenance Tool

The ETM Database Maintenance Tool is used to populate and manage the ETM Database. The ETM Database Maintenance Tool is installed by default with a complete install of the ETM System, or you can install it on a different computer from the Management Server.

To open the ETM Database Maintenance Tool

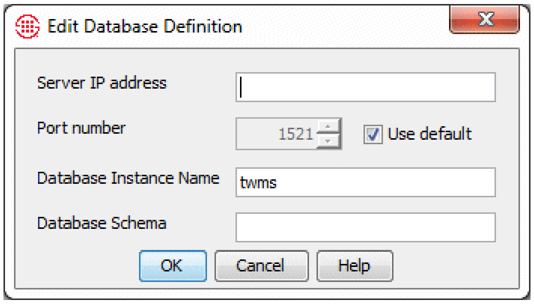
- On the computer on which the ETM Database Maintenance Tool is installed, click **Start | Programs | SecureLogix | ETM System Software | Utilities | ETM Database Maintenance Tool**.

Providing Database Connection Information

The database connection information you provide enables the ETM Database Maintenance Tool to connect to the DBMS for database configuration. In a later procedure, this information is also added to the **twms.properties** file to enable the Management Server to connect to the database.

To create a new Database Object

1. For instructions for opening the ETM Database Maintenance Tool, see "Opening the ETM® Database Maintenance Tool" above. On the main menu of the ETM Database Maintenance tool, click **Standalone Database | New Database**. The **Edit Database Definition** dialog box appears.



Server IP address

Port number 1521 ☑ Use default

Database Instance Name twms

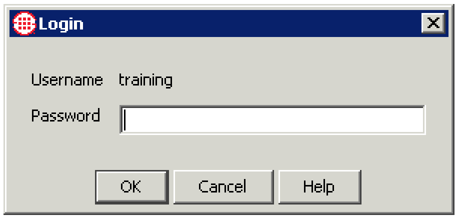
Database Schema

2. In the **Server IP address** box, type the IP address of the computer on which the DBMS is installed.
3. The **Port number** box defaults to 1521. If you are using a port other than the default, clear the **Use default** check box and type or select the correct port number.
4. In the **Database Instance Name** box, type the SID of the database.
5. In the **Database Schema** box, type the username you use to log into the standalone database (username defined for the ETM Server when you ran the Perl script.)
6. Click **OK**.

Connecting to the Database

To connect to the database

1. For instructions for opening the ETM Database Maintenance Tool, see "Opening the ETM® Database Maintenance Tool" above. In the **Standalone Databases** tree of the ETM Database Maintenance Tool, right-click the database, and then click **Connect**. The **Login** dialog box appears.



Login

Username training

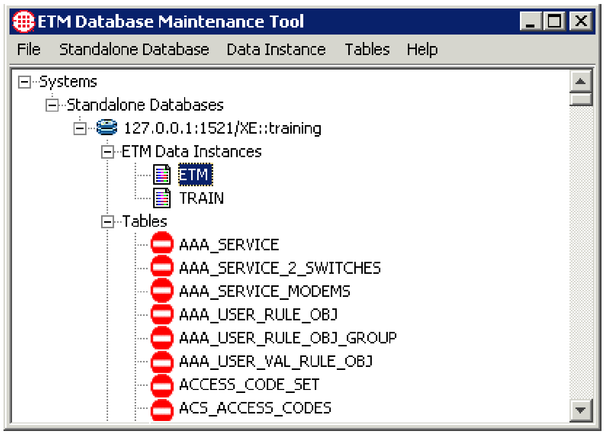
Password

2. In the **Password** box, type the password associated with the specified database username.

You defined the username and password to log in to the database when you ran the database creation script.

3. Click **OK**.

   The ETM Database Maintenance Tool connects to the database. The first time you connect to an unpopulated database, no tables are present. The **Tables** tree shows a list of the expected ETM tables, each with a red oval next to it indicating that the table is missing.



- Systems
  - Standalone Databases
    - 127.0.0.1:1521/XE::training
      - ETM Data Instances
        - ETM
        - TRAIN
      - Tables
        - AAA_SERVICE
        - AAA_SERVICE_2_SWITCHES
        - AAA_SERVICE_MODEMS
        - AAA_USER_RULE_OBJ
        - AAA_USER_RULE_OBJ_GROUP
        - AAA_USER_VAL_RULE_OBJ
        - ACCESS_CODE_SET
        - ACS_ACCESS_CODES

Populating the Database with Tables

This procedure is only performed once per database. After the database is populated with tables, you need only create a new data instance to enable an additional Management Server to use the database. All Management Servers using the database use the same tables. Management Servers are identified in the database by the data instance.

To populate the database with tables

- In the ETM Database Maintenance Tool, while connected to the database, right-click the **Tables** node of the **Standalone Databases** tree, and then click **Create All Tables**. It takes a few minutes for the tables to be created and verified.

When each of the tables has been created and verified, an icon next to each table indicates its status:

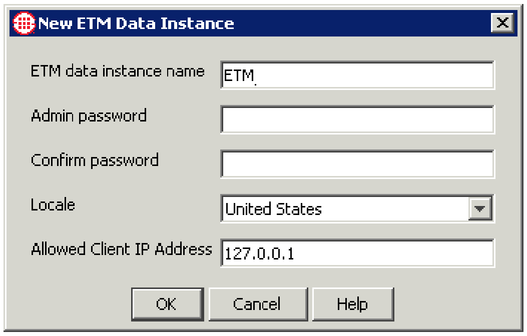
Icon	Meaning
✓	Indicates the table is valid.
⚠	Indicates an error in the table. Right-click the table, and then click **Repair Table** to correct the problem.
⛔	Indicates a missing expected table. Right-click the table, and then click **Create Table** to create the table.
🗎	Indicates views and temporary tables created and managed by the ETM Management Server.

Creating a Data Instance

Each Management Server uses a separate data instance, enabling data from multiple Servers to be stored in the same standalone database. When you create the data instance for a Management Server, you define the password for the default **admin** user account for that Server and you specify the initial IP address from which ETM Client Tool connections are allowed. You use this password to log in to a newly installed Management Server, and you use the ETM System Client at the specified IP address to complete ETM System configuration.

To create a data instance for a Server

1. Connect to the database. (See "Connecting to the Database" on page 36 for instructions, if necessary.)
2. Right-click **ETM Data Instances** and then click. **New Instance**.
3. The **New ETM Data Instance** dialog box appears.



New ETM Data Instance

ETM data instance name: ETM

Admin password:

Confirm password:

Locale: United States

Allowed Client IP Address: 127.0.0.1

4. In the **ETM data instance name** box, type a unique identifier for this data instance.
5. In the **Admin password** and **Confirm password** boxes, type the initial password for the default **admin** user account. When you log in to the Management Server via the ETM Console for the first time, you will use the username **admin** and the password you specify in this

dialog box. (You can change this password in the **User Administration Tool** after you log in to the Management Server.)

6. The **Locale** box causes the ETM data instance to be populated with default values specific to your geographic location. Click the down arrow, and then select your locale from the list of supported locales.
7. The **Allowed Client IP Address** box is used to specify the IP address of the computer from which you will initially log in via the ETM System Console to complete system configuration.
   - If you will perform this initial configuration from a remote Client, type that address here. Only authorized Clients are allowed to connect to the ETM Server. (The client tools installed on the local host are always allowed to connect to the Server, even if you type a remote IP address in this box.)
   - If you will perform initial configuration from the local Client on the ETM Server computer, leave the default localhost address; you can authorize remote Clients through the Client GUI after you log in in a later step.
8. Click **OK**. The data instance is created and its name appears under the **ETM Data Instances** node.

Set the Default Data Instance for the Management Server

When you set a data instance as the default, the ETM Database Maintenance Tool modifies the **twms.properties** file with the information needed to allow the ETM Server to connect to the database. The file sections shown below are modified.

TIP You can encrypt the passwords in this file when you finish configuration. See "Encrypting Values in the twms.properties File" in the *ETM® System Administration and Maintenance Guide* for instructions.

```
#########################################

## The instance name

Instance=<instance_name>

##########################################

## The URL of the database

DatabaseURL=jdbc:oracle:thin:@10.1.1.81:1521:<database_SID>

#################################################

## The user id to log into the database

DatabaseUserid=<etmuserid>

#################################################

## The passphrase to log into the database

DatabasePassphrase=<etmuserpassphrase>
```

Creating a Non-Owner Database User Account (Optional)

The Management Server, by default, connects to the database through the database owner account. The Management Server really only needs to change data—it does not need to drop or create objects.

A non-owner database user account allows the Management Server to connect to the database through an account that has access to modify data only and not to modify the underlying database objects (tables, views, etc.). Therefore, a non-owner account has privileges limited to only the privileges needed for the Management Server to operate.

If you are not using a non-owner database user account, skip this step and continue with "Associating a Data Instance with a Management Server" on page 40.

To associate a non-owner database user with an instance, the non-owner user account must first be created and assigned the required permissions by a database administrator.

TIP Non-owner database user accounts can be set up after installation. If it is not necessary to create a non-owner database user now, skip to "Associating a Data Instance with a Management Server" on page 40.

To create a non-owner database user account

1. Log into SQL*Plus as SYSDBA

2. Create a non-owner user. The following is an example command to create a user. Replace <RUNUSER> with the name of the user and <RUNUSERPASS> with the password.

```
CREATE USER <RUNUSER> PROFILE "DEFAULT" IDENTIFIED
BY <RUNUSERPASS>
   DEFAULT TABLESPACE "ETM"
   TEMPORARY TABLESPACE "TEMP"
   ACCOUNT UNLOCK;
```

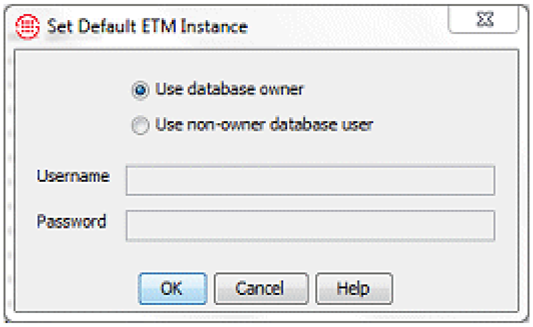
3. Grant privileges to the user account with the following commands as an example. Replace <RUNUSER> with the name of the user.

```
GRANT ALTER SESSION TO <RUNUSER>;
GRANT CREATE PROCEDURE TO <RUNUSER>;
GRANT CREATE SESSION TO <RUNUSER>;
GRANT CREATE <SNAPSHOT_PERM> TO <RUNUSER>;
GRANT CREATE TABLE TO <RUNUSER>;
GRANT CREATE VIEW TO <RUNUSER>;
GRANT UNLIMITED TABLESPACE TO <RUNUSER>;
```

Associating a Data Instance with a Management Server

To associate a Data Instance with a Management Server

1. In the ETM Database Maintenance Tool, while connected to the ETM Standalone Database, right-click the correct data instance, and then click **Set as default**. **The Set Default ETM Instance** dialog box appears.



● Use database owner
○ Use non-owner database user

2. Do one of the following to set the default instance and associate the appropriate login credentials:

   - Select **Use database owner** to set this instance as the default instance and to specify that this instance will use the database owner’s username and password to access the Management Server database, and then click **OK**.

- Select **Use non-owner database user** to specify that this default instance will use a specified user's username and password to access the Management Server. (The non-owner user account must have already been created and assigned the required permissions.) Enter the non-owner database user's **Username** and **Password**, and then click **OK**.

The ETM Database Maintenance Tool updates the **twms.properties** file on its computer with all of the information the Management Server needs to connect to the database and access the correct data instance.

3. Do one of the following:
   - If the Management Server is installed on the same computer as the ETM Database Maintenance Tool, database preparation is complete.
   - If the Management Server is installed on a different computer from the Database Maintenance Tool, do one of the following:
     - If no previous modifications have been made to the **twms.properties** file on the Management Server computer, copy the **twms.properties** file from the ETM Database Maintenance Tool computer to the Management Server computer.
     - If modifications have previously been made to the **twms.properties** file on the Management Server computer (for example, enabling operation through a firewall or changing the TCP/IP port), either manually edit the applicable sections of the **twms.properties** file on the Management Server computer, or copy the updated database information from the **twms.properties** file on the ETM Database Maintenance Tool computer and paste it over same sections in the **twms.properties** file on the Management Server computer. Perform this step before encrypting passwords in the files, and then encrypt each file separately.

Continue with one of the following:

- If the ETM System components will communicate through a NAT firewall, continue with "Connecting Through a Firewall" on page 42. If not, see the next bullet.
- Continue with "Install the Appliances" on page 49.

Connecting Through a Firewall

If the ETM System client tools will communicate through a firewall or other Network Address Translation (NAT) device, perform the following configuration procedures to enable communication.

Step 1: Gather Required Information

Before you begin configuration, determine the following:

- Select a TCP/IP port above 5000 to use for ETM System client tool connections to the Management Server (TWMSObjectStartPort).
- Select a TCP/IP port above 5000 to use for Usage Manager connections to the Report Server (ReportServerStartPort). If the Report Server and Management Server reside on the same computer, select a different port than that used for the Management Server.
- By default, ports 6990–6993 are assigned to ETM System functions. If any of these ports is in use by another device or application, choose an alternate port.
- By default, port 4313 is assigned in the **twms.properties** file for Management Server/Appliance communication. Ensure no port conflict exists.
- Determine the fully qualified host name of the computer on which the Management Server and the Report Server are installed. (These can be the same or different computers.)
- Determine the internal IP address of the computer on which the Management Server and the Report Server are installed. (These can be the same or different computers.) This is the IP address on the internal network of the computer running the Management Server and Report Server.
- Determine the externally visible IP address of the computer on which the Management Server and Report Server are installed. (These can be the same or different computers.) Consult with the network or firewall administrator for assistance.
  - In some cases, this is the firewall's external (Internet facing) IP address.
  - In other cases, the firewall administrator may dedicate a specific, external (Internet-facing) IP address for the Management Server and Report Server computer(s). If this is the case, use the dedicated external IP address the firewall administrator provides you.

Continue with "Step 2: On the Management Server Computer" below.

Step 2: On the Management Server Computer

The following files must be modified on the Management Server computer:

- The **hosts** file
- The **twms.properties** file
- In some cases (e.g., when the computer is not part of or not logged in to a domain), the Management Server configuration file:

  ETMManagementService.cfg (Windows)

  ETMManagementServer.cfg (Linux)

Edit the hosts File for the Management Server

To edit the Management Server hosts file

1. On the Management Server computer, open the **hosts** file in a text editor.

2. At the end of the file, add a line mapping the Management Server's internal IP address to the fully qualified host name in the following format:

   <ETMServerIPaddress> <ETMServerhostname>

   For example, if the Management Server computer is named "Zephyr" in the domain "topaz.com," you might type

   ```
   192.168.12.9 Zephyr.topaz.com
   ```

Edit the twms.properties File for the Management Server

Note: For a multiple-instance install, you must follow this procedure to edit each of the instance-specific **twms.properties** files.

To edit the twms.properties file for the Management Server

1. On the Management Server computer, open **twms.properties** in a text editor. This file is located at the root of the Management Server installation directory:

   <INSTALL_DIR>\SecureLogix\ETM\twms.properties

2. Locate the line that reads `TWMSObjectStartPort=0` and replace 0 with the port number you selected for the Management Server.
3. Locate the line that reads `TWMSObjectNumPorts=0`. When 0 is specified, anonymous ports are used; when 1 is specified, the port number you specified for TWMSObjectStartPort is used. Replace 0 with 1.
4. Locate the line that reads `DispatcherPort=6991`. This is the default port that ETM client applications connect to when initiating a data communication socket with the Management Server. If this port is in use by another application or device, replace 6991 with the applicable port number.
5. Locate the line that reads `RMIPort=6990`. This is the port number on which the Server accepts connection requests from ETM System client

tools. If this port is in use by another application or device, replace 6990 with the applicable port number.

6. Save the modified file.

Edit the Management Server Configuration File (if applicable)

The RMI server host name for the Management Server must resolve to a fully qualified domain name. The RMI server host name is determined by an entry in the following configuration file, located in the ETM System installation directory:

Windows

ETMManagementService.cfg

Linux

ETMManagementServer.cfg

By default, the following case-sensitive parameter is included in this file to resolve the RMI server host name:

-Djava.rmi.server.useLocalHostName=True

For most computers, this parameter will resolve the fully qualified domain name. However, in some cases, it will resolve to the IP address of the computer instead (typically when the computer is not part of or not logged in to a domain). In this case, replace

-Djava.rmi.server.useLocalHostName=True

with

-Djava.rmi.server.hostname=<*the.hostname.com*>

where ***<the.hostname.com>*** is replaced with either the correct, fully qualified domain name or the IP address for the host.

To determine whether the host name will resolve correctly on Windows

- At a command prompt, type:

  ipconfig /all

  If the Host Name field contains a fully qualified domain name, the host name will resolve correctly. If the Host Name field contains only the host name, and then you must use the -**Djava.rmi.server.hostname** parameter instead.

Step 3: On the Report Server Host Computer

The following files must be modified on the Report Server host computer:

- The hosts file
- The **twms.properties** file
- In some cases, the Report Server configuration file:

  Windows

ETMReportService.cfg

Linux

ETMReportServer.cfg

Edit the hosts File for the Report Server

This step is only required if the ETM Report Server resides on a different computer than the Management Server.

To edit the hosts file

1. On the Report Server computer, open the **hosts** file in a text editor.
2. At the bottom of the file, add a line mapping the Report Server's internal IP address to its fully qualified system name or the hostname, in the following format:

   <ReportServerIPaddress><ReportServerhostname>

   For example, if the Report Server computer is named "Zephyr" in the domain "topaz.com," you might type

   192.168.12.9 Zephyr.topaz.com

Edit the twms.properties File for the Report Server

To enable remote Usage Managers to connect to the Report Server, you must edit the **twms.properties** file on the Report Server computer, whether on the same computer as the Management Server or a different one.

To edit the twms.properties file for the Report Server

1. On the Report Server computer, open **twms.properties** in a text editor. This file is located at the root of the Report Server installation directory:

   <INSTALL_DIR>\SecureLogix\ETM\ twms.properties

2. Locate the line that reads `ReportServerStartPort=0` and replace 0 with the TCP/IP port number you selected.
3. Locate the line that reads `ReportServerNumPorts=0` and replace 0 with 1. When 0 is specified, anonymous ports are used; when 1 is specified, the port number you specified for ReportServerStartPort is used.
4. Locate the line that reads `ReportDispatcherPort=6992`. This is the default TCP port to which the Usage Manager connects when initiating a data communication socket with the Report Server. If this port is in use by another application or device, replace 6992 with the applicable port number.

Edit the Report Server Configuration File

The RMI server host name for the ETM Report Server must resolve to a fully qualified domain name. The RMI server host name is determined by entries in the following configuration file, located in the ETM System installation directory:

Windows

ETMReportService.cfg

Linux

ETMReportServer.cfg

By default, the following parameters are included to resolve the RMI server host name:

-C-Djava.rmi.server.useLocalHostName=True

-J-Djava.rmi.server.useLocalHostName=True

For most computers, these parameters will resolve the fully qualified domain name. However, in some cases, they will resolve to the IP address of the computer instead (typically when the computer is not part of or not logged in to a domain). In this case, replace the parameters

-C-Djava.rmi.server.useLocalHostName=True

-J-Djava.rmi.server.useLocalHostName=True

with

-C-Djava.rmi.server.hostname=<*the.hostname.com*>

-J-Djava.rmi.server.hostname=<*the.hostname.com*>

where <*the.hostname.com*> is replaced with the correct, fully qualified domain name or IP address for the host.

To determine whether the host name will resolve correctly on Windows

- At a command prompt, type:

  ipconfig /all

  If the Host Name field returned contains a fully qualified domain name, the host name will resolve correctly. If the Host Name field contains only the host name, and then you must use the

  -Djava.rmi.server.hostname parameter instead.

Step 4: On the ETM® System Console Host Computer

Edit the hosts file on each ETM System host computer, including the one on the same computer as the Management Server, those on the same local network, and those that are outside of the firewall.

To edit the hosts file

1. On the ETM System Console computer, open the **hosts** file in a text editor.
2. (*Not applicable to local ETM System Consoles running on the Management Server host*) At the end of the file, add a line mapping the Management Server's IP address to its fully qualified host name as follows:
    - If the ETM System Console you are modifying is outside of the Server's firewall, use the Management Server's external IP address.
    - If the ETM System Console you are modifying is inside the Server's firewall, use the Management Server's internal IP address.
3. If the Report Server is on a different computer than the Management Server, add a line mapping the Report Server's IP address to the fully qualified hostname, in the same way as described for the Management Server.
4. Save the modified file.

Step 5: Configure the Firewall

Required modifications vary depending on the firewall in use. Refer to your firewall documentation for information specific to your firewall. General guidelines are provided below.

To enable a remote ETM System Console outside of the firewall to connect to the Management Server behind a firewall, do the following:

- Provide an external IP address that the firewall statically translates to the internal Management Server IP address.
    - To avoid port number conflicts, it is recommended that this external address not be shared or translated for any other device.
    - For added security, it is recommended that you limit the external IP addresses allowed to connect to the Management Server.
- Allow traffic from the remote ETM System Console(s) and Usage Managers to pass through the firewall to the Management Server with a destination port equal to the RMI port (6990 by default), the Dispatcher ports (6991 and 6992 by default), and the RMID port (6993 by default).
- Allow TCP/IP traffic with the destination ports that you selected to pass from the remote ETM System Console to the Management Server. (Do not restrict the source port range; the ETM System Console randomly selects the source port.)

- Allow traffic to port 4313 (or alternate user-defined port) to pass from remote Appliances to the Management Server, if the system is deployed in a distributed architecture.
- Allow Management Server traffic and established sessions to pass out of the firewall to the remote ETM System Console. For many firewalls, outbound traffic is not restricted, so this step may be unnecessary.

Continue with "Install the Appliances" on page 49.

Step 2: Hardware Installation

Install the Appliances

For instructions for installing the UTA and inline SIP applications, see the SecureLogix Knowledgebase at *http:/support.securelogix.com*.

WARNING To ensure equipment and personnel safety, before you begin installing the Appliance(s), read the suggestions and warnings in *ETM® System Safety and Regulatory Information* provided with your Appliances.

Installation of the ETM Appliances consists of the following sequence of steps:

1. (*Applies to ETM 2100 and 3200 Appliances only*.) Install the Controller Card(s) and Digital Trunk Interface(s) in the Appliance chassis.
2. Mount the Appliance chassis in an equipment rack or on the wall.
3. Connect the SMDR cable to the Card that is to be the SMDR provider for the Switch, if SMDR is used.
4. Connect the power cable and power on the Appliance.
5. Use a Console session to configure the Card(s) to connect to the Management Server.
6. (*Not applicable to VoIP, analog, or SS7 Signaling Links*) Change the telco Spans' types, if applicable. All of the Spans in the digital ETM telco Appliances (except the SS7 Signaling Links) are configured for T1 CAS by default.
7. Connect the Ethernet cable.

See "Appendix A: Appliance Technical Specifications, Connectors, and Pinouts" on page 173 for diagrams of each connector on the ETM Appliances.

Install the Digital Trunk Interface/ Controller Card Pairs

(*Applies to ETM 2100 and 3200 Appliances only*.) The Controller Card and Digital Trunk Interface in the ETM 2100 and 3200 Appliances work together as a unit.

IMPORTANT The procedures below apply only to new ETM Appliance installations; if you are removing and replacing configured Cards on an active system, see "Removing and Replacing Cards" on page 188.

CAUTION Do not remove the DSP PMC from the Controller Card unless directed to do so by SecureLogix Customer support.

To install the Digital Trunk Interface/Controller Card pairs

1. At the back of the Appliance chassis, insert the Digital Trunk Interface into the bottom slot. The components on the Card should face up.

   IMPORTANT A Digital Trunk Interface/Controller Card pair must be present in the system slot (the bottom slot) of the ETM 3200 Appliance for proper operation. The Controller Card in this slot serves as the system controller for the unit. The system Controller Card controls communication on the compact Peripheral Component Interconnect (cPCI) backplane, and parks the PCI bus when the bus is idle.

2. Flip the latches inward until you hear them lock.
3. Insert the screws into the latches and hand tighten with a screwdriver to secure the Digital Trunk Interface in the chassis.
4. At the front of the chassis, insert the Controller Card into the slot that corresponds to the Digital Trunk Interface. The components on the Card should face up.
5. Flip the latches inward until you hear them lock.
6. Install the screws into the latches and hand tighten with a screwdriver to secure the Controller Card.
7. In the 3000-series Appliances, repeat steps 1-4 for other Digital Trunk Interface/Controller Card pairs. Cards need not be continuously installed from the bottom up, but a Card set MUST be present in the lowest slot.

Mount the Appliances

The ETM Appliances support front-, mid-, and rear-rack mounting, (and TDM Appliances also support wall mounting), by simply moving the mounting brackets to the appropriate location on the Appliance. Mounting brackets and screws are provided for rack mounting but not for wall mounting. When shipped, the mounting brackets are attached in the front-mounting position.

See "Removing and Replacing TDM Appliance Components" on page 187 for the proper procedures for removing and installing Appliance components, if necessary.

Rack Mounting

The ETM 3200 Appliance uses 2 rack units (RU) of space; all other Appliances use 1 RU.

To mount an Appliance in a rack

1. When shipped, the mounting brackets are attached to the Appliance in the front-mounting position. If you are rear or mid mounting the Appliances, move the brackets to the applicable position on the side of the Appliance.
2. Position the Appliance in a standard 19-inch rack and attach the mounting brackets to the rack rails using the hardware provided.

Wall Mounting

(*TDM Appliances only*) Since wall materials vary, no screws are provided. Use the appropriate type of screw (wood screw, dry wall screw) for the wall on which the Appliance is to be mounted. The brackets provided with the Appliance allow you to wall-mount only 1 Appliance deep; you cannot stack multiple Appliances on the same wall location without special wall-mounting brackets (not provided).

To mount an Appliance on a wall

1. When shipped, the mounting brackets are attached to the Appliance in the front-mounting position. For wall mounting, move the brackets to the appropriate location on the side of the Appliance.
2. Use the appropriate type of screws (not included) to attach the brackets to the wall.

Connect the SMDR Cable to the SMDR Provider Card

For further details about SMDR configuration and the SMDR Provider, see "Configuring a Switch for SMDR" on page 127.

One telco Appliance Card monitoring calls at a given PBX can be connected to the SMDR/CDR port on the PBX to transfer PBX log data to the Management Server. This Card serves as the *SMDR provider* for all of the Spans in all of the Appliances on that PBX. The SMDR cable connects to the **Auxiliary** port on the Controller Card or Appliance, depending on Appliance type:

The **Auxiliary** port accepts an SMDR cable with an RJ-45 connector. On the 2100 and 3200, each Controller Card has an **Auxiliary** port. On the 1024,and 1090, the **Auxiliary** port is on the front of the chassis. The CRC Application Appliances are not telco Appliances and therefore cannot serve as SMDR providers.

To connect the SMDR cable

- Connect a serial cable from the PBX SMDR/CDR port to the **Auxiliary** port on the Appliance or Controller Card that is to serve as the SMDR provider for that Switch. If the SMDR port is currently in use by another device and the PBX does not allow multiple ports for SMDR data, use a Y cable.

Using a Y-Cable for SMDR

See the SecureLogix Knowledge Base located at **http://support.securelogix.com/knowledgebase.htm** for the correct Y-cable pinout. When a Y cable is used to connect an Appliance Card to a PBX SMDR port, the Card assumes that the other device connected to the Y cable (e.g., a computer) is providing the handshake signal to request receive data (the Card does not provide flow control). If the other device is powered off or is not providing the handshake, SMDR data is not sent to the Card.

If the PBX is correctly configured to send SMDR, but the Card does not receive SMDR data when connected to the PBX, verify the following:

- The other device connected to the Y cable is powered on and functioning properly.
- The SMDR Y cable is built correctly.

Connect the Ethernet Cable(s)

Connect the Ethernet cable(s) for Server communication and, if used, VoIP circuits.

When you give the Appliance Card the IP address and port number for the Server during out-of-box configuration, the Card will begin initiating contact with the Server; however, it will be unable to establish a connection until you add its IP address to the Server's list of authorized Card IP addresses via the Performance Manager in a later step.

Connect Power to the Appliance

It is strongly recommended that you connect the Appliance to an uninterruptible power supply. AC versions of all Appliances are available. A DC version of the 3200 Appliance is also available. Use the applicable procedure below to connect power to the Appliance.

WARNING To ensure equipment and personnel safety, before connecting power to the Appliance, refer to the *ETM® System Safety and Regulatory Compliance Information Guide* packaged with your hardware.

⚠ **WARNING** If an Appliance power fault condition occurs, disconnect the Appliance power cord from the rack power supply, not at the Appliance itself.

AC Appliances are supplied with a power cord.

AC Appliances

To connect power to an AC Appliance

1. Connect the receptacle end of the provided power cord to the Appliance.
2. Plug the power cord provided with your Appliance into a 100-240VAC, 50-60Hz power source that is protected by a 15-amp circuit breaker or fuse.
3. Press the Appliance power switch to the **On** position.
4. Observe that the fans are running and that LEDs are illuminated. For information about each of the LEDs on the Appliance(s), see "TDM Appliance LED Descriptions" on page 203.

DC Appliances

The DC version of the ETM 3200 Appliance requires -36VDC to -72VDC at 7.9A. Since customer-premises equipment varies, a wire harness is not provided.

To connect power to a DC Appliance

1. Connect the wire harness to the -48V and RTN terminals at the rear of the Appliance.
2. With power disconnected from the power source, connect the wire harness to a -36 to -72VDC, 7.9A power supply that is protected by a 9.5-amp circuit breaker or fuse.
3. Connect power to the power source. (For example, insert a fuse into the fuse panel position assigned to the Appliance.) The DC Appliance has no power switch.
4. Observe that the fans are running and that LEDs are illuminated. For information about each of the LEDs on the Appliance(s), see "TDM Appliance LED Descriptions" on page 203.

Configure the TDM Card(s) to Connect to the Management Server

To enable TDM Card to establish communication with the Management Server, use a terminal or terminal emulator connected to the **Console** serial port on the Card to provide the Card with site-specific network information. Each Card must be configured separately. HyperTerminal, a standard application on Windows systems, is an example of a terminal emulator that can be used to establish the necessary communication link.

After the Card establishes communication with the Management Server, additional Card and Span configuration is performed in the Performance Manager.

Required Information for Out-of-the-Box Configuration

IMPORTANT All ETM System components except remote ETM System Clients must be assigned static IP addresses. Remote ETM System Clients must have a static IP address unless you allow IP masks.

The following information must be provided during out-of-the box configuration:

- Card IP address, netmask or prefix length, and gateway (if used). A stateless autoconfiguration option allows you to choose either the suggested IPv6 address and prefix length, or type either an IPv6 or IPv4 address manually.
- Management Server IP Address.
- DES Key—This key must always be in sync between the Card and the Management Server, because DES encryption is always used during the initial Card/Server handshake to validate the connection. If this value is wrong, the Server does not accept connection from the Card. For initial connection, you must provide the default DES Key character string, which is defined in the **twms.properties** file located in the ETM System installation directory on the ETM Server computer. You can change the value used by the Cards to a secret key during later configuration via the Performance Manager. You can also optionally encrypt the passphrases in the **twms.properties** file when configuration is complete.

Initial Card Configuration

This procedure is performed for each Card/Appliance.

The **Console** port is at the front of the Appliance/Card and accepts an RJ-45 connector. Adapters are provided with each ETM 2100/3200 chassis and 1000-Series Appliance for connecting an RJ-45 connector to a 9-pin D connector, if necessary.

To configure a Card via direct serial connection

1. Attach an RS-232 serial cable from the **Console** port on the Card to the appropriate serial port on your computer.
2. Start the terminal emulation application (such as HyperTerminal) on your terminal. Configure your terminal using the following serial port settings:

- 115,200 bps
- 8 data bits
- 1 stop bit
- no parity
- no flow control

3. Initiate the session (procedure varies by type of emulation application).

   By default, during the first two minutes of power-on, the Card is in Enable mode and does not require a username/password combination for access. After two minutes or one login session, you must log in with a valid username/password combination. However, you can modify or disable this mode. To change the Enable mode timeout, see "Changing the Enable Mode Timeout" on page 60.

4. At the **Select an installation USERNAME** prompt, type a username and press ENTER.

5. At the **Select an installation PASSWORD** prompt, type a password and press ENTER. This temporary username and password are used only for initial Card configuration and remain on the Card only until communication with the Management Server is established, at which time they are erased. Permanent user accounts are defined at the Management Server using the Performance Manager. A password can be any combination of characters. It must be a minimum of eight characters in length, and must include at least one change of case and one digit.

6. At the **Select an initial ENABLE PASSWORD** prompt, type an Enable password and press ENTER. The Enable password must contain at least 8 characters and must follow the Rules for a good, strong password and include at least one change of case and special character. The Enable password can be a maximum of 50 characters. The Enable password allows you to change Card and Span configuration parameters via the serial port and Telnet. Unlike the temporary installation name and password, the Enable password you supply during out-of-box configuration is sent up to the ETM Server and remains valid unless it is changed via the Performance Manager.

7. At the **Select Card IP address option** prompt, type **1** to accept the suggested IPv6 address and prefix; type **2** to specify either an IPv4 or IPv6 address manually. Press ENTER.

8. Do one of the following:

   - **If you chose option 1:** At the **Select card IPv6 gateway** prompt, type the IPv6 gateway and then press ENTER. See step 9.
   - **If you chose option 2:** At the **Select card IP address** prompt, type the IPv4 or IPv6 address you want to use for the card, and then press ENTER.

9. If you typed an IPv4 address, the **Select Card IP netmask or prefix length** prompt appears.

a. Type either a prefix or the IP netmask (in dot notation) for the network on which this Card is to communicate with the Management Server (or type 0.0.0.0) and press ENTER.

b. At the **Select card IPv4 gateway** prompt, type the gateway IP address for the network on which the Card is to communicate with the Management Server and press ENTER. (If an IP gateway is not used, type: 0.0.0.0)

10. If you typed an IPv6 address, the **Select card IP prefix length prompt** appears.

    a. Type the prefix length and press ENTER.

    b. At the **Select card IPv6 gateway** prompt, type the IPv6 gateway and then press ENTER.

11. At the **Select the Management Server IP** prompt, type the IP address of the Management Server that is to manage this Card.

12. At the **Select the DES secret key/phrase** prompt, press CTRL-P ENTER. This provides the default value as found in the **twms.properties** file. You can change this later to a unique value via the Performance Manager, if needed.

13. At the **Select Card security posture** prompt, type one of the following:

    - **HIGH**—Telnet is disabled and network and security configuration changes are only allowed via the **Console** port.
    - **MED**—Telnet is disabled and security configuration changes are allowed via the Console port or the **ASCII Management Interface**.
    - **LOW**—Telnet is enabled and security configuration changes are allowed via the serial port, the Performance Manager, or Telnet.

The Card security posture only applies to network- and security-related settings. Telecom and Policy configuration is not affected.

    Since you configure security fields via the Performance Manager during installation, it is strongly recommended that you set the security posture to **LOW** or **MED** now. If a security posture of **HIGH** is required by your organization, you can use the Performance Manager to change the setting to **High** once configuration and installation are complete.

14. The configuration settings and the following message appears:

    ```
    Please verify the options are configured
    correctly
    ```

    Review the list of configuration settings for accuracy.

15. At the **Do you want to initialize the Card with these values (y/n)** prompt, do one of the following:

    - To discard displayed values and start over, type: `n`

If you type **n**, the system logs you off without keeping your settings. You can then press any key to begin the configuration process again.

- To accept the displayed values, type: `y`

  If you accept the values, the message **Restarting Card to effect changes** appears while the Card restarts. The Spans restart offline automatically, so that you can configure them with the proper telephony settings before placing them inline. When you complete configuration, be sure to place the Spans inline.

Licensing Additional Spans

(*Not on CRC, SIP, or UTA*) Complete this procedure if more than one Span is to be licensed on the Card; otherwise, skip this step and continue with the next step. Span 1 is licensed by default. To obtain the license key, contact Customer Support at one of the following: **1-877-SLC-4HELP** or **support@securelogix.com**)

You can also provide the Span license via the Performance Manager. However, if you need to change the Span type, you should provide the Span license now.

To license additional Spans

1. After the Card reboots, log in again and enter Enable mode. (Type `Enable`, press ENTER, and then type the Enable password.)
2. At the **ETM:1(r/w)>** prompt, type:

   ```
   LICENSE <key>
   ```

   where <*key*> is the Span License Key provided by SLC Customer Support.
3. Type: `RESTART`

Changing the Span Type

All Digital TDM Spans are shipped as T1 CAS. On 3200, 2100, and 1090 Appliances, you can change the Card rate (T1/E1) and the signaling type (CAS, PRI, or SS7) using the procedure below. If you are installing T1 CAS Spans, skip this step.

IMPORTANT If a new Span has already connected to the Management Server before you change the Span type, the Server refuses connections from the Span after the type is changed. This is because the Management Server is authoritative on most configuration settings and it expects T1 CAS. To remedy this problem, delete the Card from the Performance Manager tree pane. When the Span reconnects, the Management Server accepts the updated configuration.

To change the Span type

1. Log in to the Card and enter Enable mode.
2. At the **ETM:1(r/w)>** prompt, type:

```
RESTART FAILSAFE
```

The Card restarts with all Spans in Fail Safe mode. The **Fail Safe** menu appears.

```
Fail Safe Mode Menu

1 - Enter Fail Safe ETM Shell

2 - Display Configuration Data

3 - Audit Configuration Data

4 - Erase Configuration Data

5 - Restart Appliance

6 - Stop Fail Safe ETM Timer
```

Tip You can also change Span type remotely from the **ASCII Management Interface**. After you type **Restart Failsafe**, you do not see the menu, but wait one minute until the Card reboots into failsafe, indicated by the **Failsafe** icon in the Performance Manager tree pane. You can then execute commands.

3. At the **>** prompt, type:

   ```
   1
   ```

   The **FS(r/w)>** prompt appears.

4. Type:

   ```
   MAINT SPAN TYPE <Span number> <Span type>
   ```

   For example, to set Span 2 to T1 PRI, type:

   ```
   MAINT SPAN TYPE 2 PRI
   ```

5. At the **FS(r/w)>** prompt, type:

   ```
   RESTART
   ```

   The "Fail Safe terminated" message appears and the Card restarts with the new Span settings and returns to the **ETM>** prompt. (You may have to press ENTER for the prompt to appear.)

   The Spans restart offline automatically, so that you can configure them with the proper telephony settings before placing them inline. During Telephony Service Cutover, you will place the Spans inline.

Continue with one of the following:

- If the Management Server is to accept communication from Cards on a TCP/IP port other than 4313, continue with "Changing the Management Server TCP/IP Port" on page 59. If not, see the next bullet.
- If you want to change the Enable mode timeout (for example, to always require a username and password), continue with "Changing the Enable Mode Timeout" on page 60. If not, see the next bullet.
- Out-of-the-box Card configuration is complete. Continue with "Configuring the ETM® System" on page 61.

Changing the Management Server TCP/IP Port

The default TCP/IP port on which the Server accepts connections from all Cards is 4313. If you changed the Management Server port from the default in the **twms.properties** file, you must configure the Card with the new port number.

To specify the Management Server port number (if different from the default)

1. Log in to the Card in **Enable** mode.
2. At the **ETM(r/w)>** prompt, type the following command with the new port number:

   ```
   SERVER PORT <number>
   ```
3. Type: `COMM RESET`

Continue with one of the following:

- If you want to change the **Enable** mode timeout (for example, to always require a username and password), continue with "Changing the Enable Mode Timeout" on page 60. If not, see the next bullet.
- Out-of-the-box Card configuration is complete. Continue with "Configuring the ETM® System" on page 61.

Changing the Enable Mode Timeout

By default, during the first two minutes of power-on, the Card is in Enable mode and does not require a username/password combination for access. After two minutes or one login session, you must login with a valid username/password combination. However, you can change this default to a lesser value, including 0 seconds. If the Enable mode timeout is not changed from the default, you will enter Enable mode on subsequent login sessions.

To change the Enable mode timeout

- At the **ETM(r/w)>** prompt, type:

  ```
  ENABLE LOGIN <value>
  ```

  where <*value*> is the number of seconds for the timeout. For example, to always require a logon to access the Card, type:

  ```
  ENABLE LOGIN 0
  ```

Out-of-the-box Card configuration is complete. Continue with "Configuring the ETM® System" on page 61.

Step 3: ETM® System Configuration

Configuring the ETM® System

If you have completed the procedures in previous chapters, you are ready to configure the ETM® System components. When you have finished the configuration procedures in this chapter, the ETM System will be ready to monitor and protect the voice network.

Overview of Terms

The following terms are used in these instructions:

- An *Appliance* is a chassis that contains one or more *Cards*. In the ETM System, each Appliance is represented by an **Appliance** object in the Performance Manager tree pane. **Appliance** objects group Cards according to the Appliance in which they are contained.
- *Cards* contain one or more interfaces to the telco spans; these interfaces are referred to as *Spans* in the ETM System. They also contain the information that allows connection to the Management Server.
- *Spans* provide the interface that connects the Appliance to a physical span entering a PBX on a customer's premises.
- *Switches* represent the PBX from which the Appliances are monitoring calls. Each PBX is represented by a **Switch** object in the Performance Manager tree pane. Switches are used to configure SMDR, NFAS, and SS7 Groups, and to define SMDR Extensions for Call Recorder.

System Configuration Steps

Configuration of the ETM System consists of the following steps, explained in detail in the procedures that follow:

1. Start the Management Server and connect to it with the ETM System Console that you will use to complete configuration, typically the local one. The Performance Manager is launched from within the ETM System Console.
2. Authorize the Cards in the Appliances to connect to the Management Server.
3. Name each Card and complete network-and security-related Card configuration.
4. Install updated software on the Cards, if necessary.
5. Name each Span and perform telephony-and Policy-related Span configuration.
6. If SMDR, NFAS, and/or SS7 Groups are in use:

    a. Create one or more Switches with which to associate the Span(s) and to configure SMDR processing, SS7 Groups, and/or NFAS.
    b. Move each Span to the Switch with which it is associated.
    c. Configure SMDR, NFAS, and/or SS7 via the switch Object.

7. Configure Management Server settings:
    a. Authorize remote ETM Client connections.
    b. Associate the Report Server with the Management Server.
    c. Specify the path to the Oracle client tools on the Management Server (needed to import Directory Listings and city/state data).

Continue with "Start the Applications and Connect to the Server" below.

Start the Applications and Connect to the Server

Follow the procedures below to start the Management Server, ETM System Console, and Report Server. If connection problems occur or the Server fails to start, see "Troubleshooting System Communication" on page 71.

IMPORTANT If the correct database driver for your version of Oracle is not present in the ETM Server installation directory (and Report Server directory, if installed on a different computer), the ETM Server or Report Server will not start.

Start the Client and Server

Do one of the following:

- If you installed a typical installation with a single instance of the Management Server, see "How to Start the Applications" on page 63.
- If you are running multiple application instances on the same computer, see "How to Start Multiple Application Instances" on page 64.

How to Start the Applications on Windows

To start the applications on Windows

- Management Server—Do one of the following:
  - Double-click the **ETM Management Server** icon on the desktop.
  - Click **Start | Programs | SecureLogix | ETM System Software | ETM Management Server**.
  - Start the **ETMManagementService** in the Windows **Services** dialog box.
- Report Server—Do one of the following:
  - Double-click the Report Server icon on the desktop.
  - Click **Start | Programs | SecureLogix | ETM System Software | ETM Report Server**.
  - Start the ETM Report Service in the **Windows Services** dialog box.
- ETM System Console—Do one of the following:
  - Double-click the **ETM System Console** icon on the desktop.
  - Click **Start | Programs | SecureLogix | ETM System Software | ETM System Console**.
- The Performance Manager, Usage Manager, and Directory Manager are launched from the ETM System Console after you log in to the ETM Server.

Starting, Stopping, and Viewing Status of the Applications on Linux

To start/stop/view status of the ETM® applications on Linux

1. Log in as **root** user.
2. Change to the **/opt/SecureLogix/ETM** directory.
3. Use the following commands:
   - To start the Database Maintenance tool, type:
     ./ETMDBMaintTool
   - To start the ETM System Console, type:
     ./ETMSystemConsole
   - ETM Management Server commands are:
     service ETMMS {start | stop | status}
   - ETM Report Server commands are:
     service ETMRS {start **|** stop **|** status}

Continue with "Define an ETM® Server Object in the ETM® System Console" on page 66.

How to Start Multiple Application Instances

To start a Management Server instance on a multiple-instance installation

Linux

1. Open a terminal window and change to the **<INSTALL_DIR>**.
2. At the prompt type:

   service ETMMS start *<instance_id>*

Windows

- Start each instance using the Control Panel Services Manager.

To start a ETM® Report Server instance on a multiple-instance installation

Linux

1. Open a terminal window and change to the **<INSTALL_DIR>**.
2. At the prompt type:

```
ETMReportServer start<instance_id>
```

Windows

- Start each instance using the Control Panel Services Manager.

To start the ETM® System Console

Starting the ETM® System Console is the same regardless of whether multiple Report Server and Management Server instances are present. The Performance Manager, Usage Manager, and Directory Manager are launched from the ETM System Console after you log in to the Server.

Linux

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

```
ETMSystemConsole
```

Windows

- Do one of the following:
  - Double-click the **ETM System Console** icon on the desktop.
  - Click **Start | Programs | SecureLogix | ETM System Software | ETM System Console**.

Continue with "Define an ETM® Server Object in the ETM® System Console" on page 66.

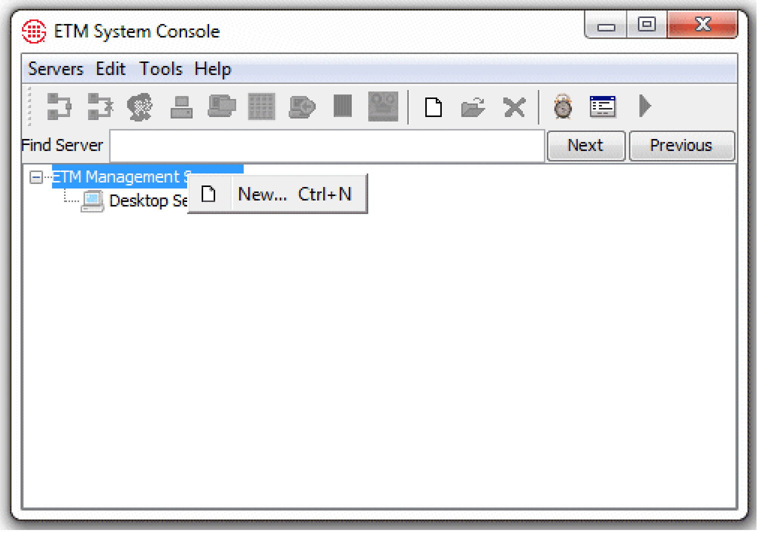
Define an ETM® Server Object in the ETM® System Console

Before you can log in to the ETM Management Server, you must define an ETM Server object in the ETM System Console. Perform this procedure in the ETM System Console on the client computer from which you authorized client connections when you created the data instance, or on the ETM System Console installed on the ETM Server host computer. After you log in the first time, you can authorize connections from other remote ETM Clients.

See "Authorize Remote Client Connections" on page 143 for instructions.

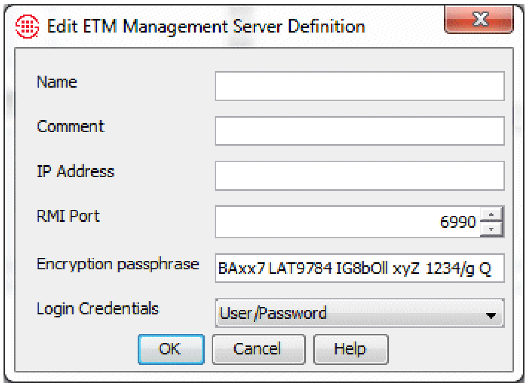
To define an ETM® Management Server object

1. Open the ETM System Console.



2. Right-click **ETM Management Servers**, and then click **New**.

   The **Edit ETM Management Server Definition** dialog box appears.



Name

Comment

IP Address

RMI Port 6990

Encryption passphrase BAxx7 LAT9784 IG8bOll xyZ 1234/g Q

Login Credentials User/Password

   a. In the **Name** box, type a descriptive name for the Management Server. You can use any name you choose.

b. In the **IP Address** box, type the IP address of the Management Server host computer.

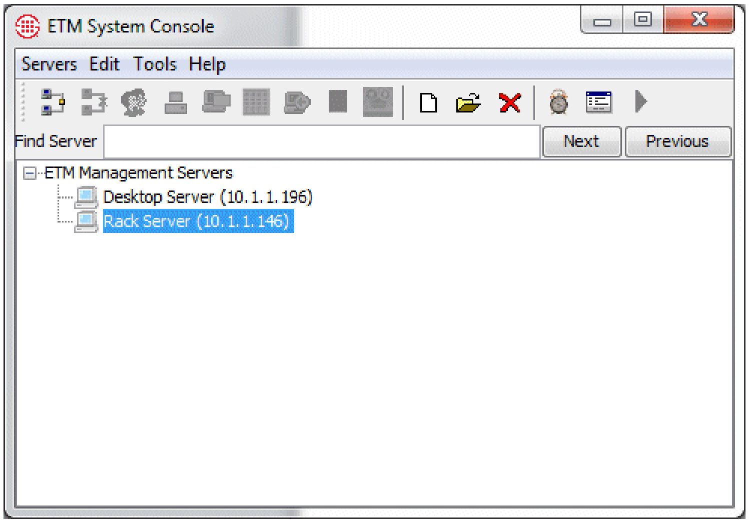
c. In the **RMI Port** box, type the Port number on which the Management Server accepts connection requests from ETM System Consoles, if different from the default of 6990.

d. In the **Encryption passphrase** box, type the DES passphrase. This key must match that of the Management Server, because the initial handshake is encrypted to validate the connection, regardless of whether encryption is licensed or in use.

e. Leave **Login Credentials** set to **User/Password** to complete initial configuration. You can modify this later if you choose to use LDAP or CAC for logins once the system is configured.

f. Click **OK**.

The new Management Server appears in the tree.



3. Repeat for each of the other Servers this ETM System Console will connect to, if any.

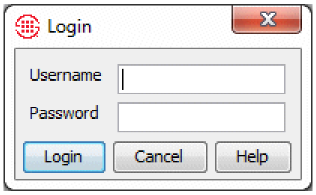
Log in to the ETM® Server

The password for the default **admin** user account on the ETM Server was defined when the data instance for the Management Server was created. Use this account to log in to the ETM Server to configure the system.

If connection problems occur, see "Troubleshooting System Communication" on page 71.

To connect to the Management Server

1. In the ETM System Console, click the Server you want to log in to.
2. On the ETM System Console toolbar, click the **Connect to Server** icon. The **Login** dialog box appears.



3. In the **Username** box, type:

```
admin
```

4. In the **Password** box, type the password defined for the default **admin** user account when the data instance for the ETM Server was created.

5. Click **Login**. The ETM System Console connects to the Server and a list of the ETM Client applications appears in the tree.

   - To open a client application, click it in the tree, and then click the **Open** icon on the toolbar, or double-click the application name.

Continue with "Authorize Cards to Connect to the " on page 68.

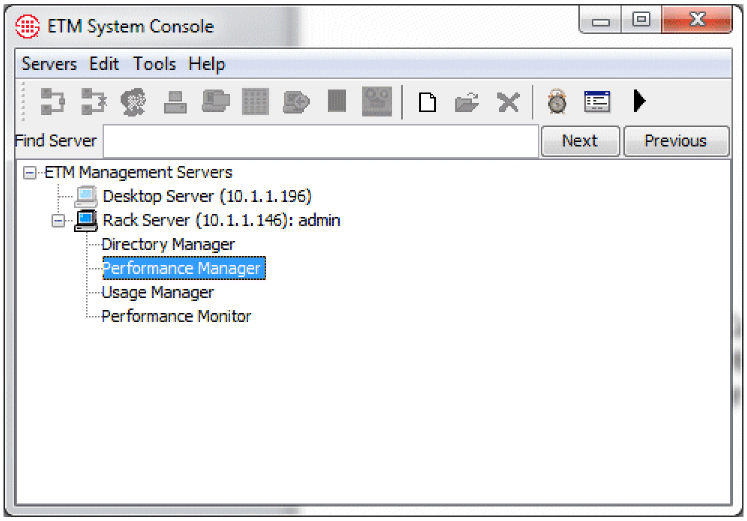
Authorize Cards to Connect to the ETM® Server

Before the ETM Management Server accepts connections from an Appliance Card, you must add the Card's IP address to the Server's **Authorized Cards** list. You can also use a subnet mask or prefix to authorize a range of IP addresses (for example, 10.1.1.0/255.255.255.0 authorizes all Cards with a 10.1.1.x IP address). You configured the Card with network connection information during installation, so the Card is attempting to initiate a connection to the Server. As soon as you add the IP address to the list, the ETM Server accepts connection from the Card and a Card icon appears in the **Platform Configuration** subtree.

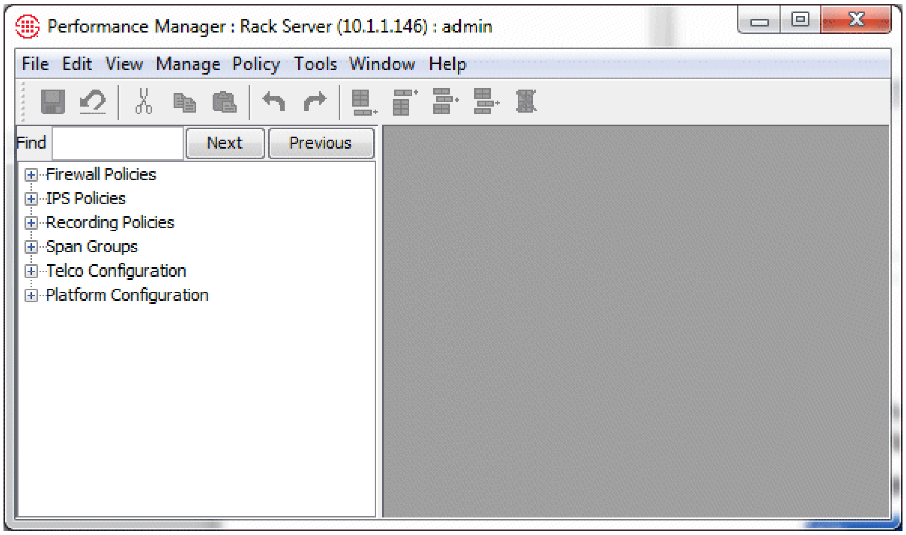
To authorize a Card to connect to the ETM® Server

1. In the ETM System Console, open the Performance Manager.

   - To open a client application, click it in the tree, and then click the **Open** icon ▶ on the toolbar, or double-click the application name.

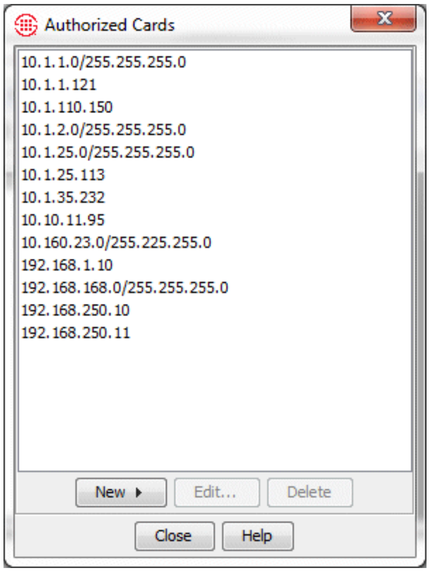


The Performance Manager appears.



2. On the Performance Manager main menu, click **Manage | Authorized Cards**

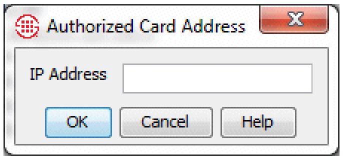
   The **Authorized Cards** dialog box appears.



```
10.1.1.0/255.255.255.0
10.1.1.121
10.1.110.150
10.1.2.0/255.255.255.0
10.1.25.0/255.255.255.0
10.1.25.113
10.1.35.232
10.10.11.95
10.160.23.0/255.225.255.0
192.168.1.10
192.168.168.0/255.255.255.0
192.168.250.10
192.168.250.11
```

If connection problems occur, see "Troubleshooting System Communication" on page 71.

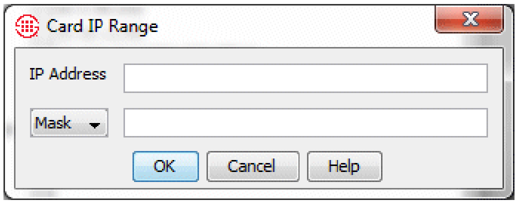
3. To authorize a specific IP address, click **New** and then click **IP Address**. The **Authorized Card Address** dialog box appears.



4. Type the IPv4 or IPv6 address of the Card.

5. Click **OK**. The IP address appears in the **Authorized Cards** dialog box. When a Card connects, a green icon and the Card name appear in the **Platform Configuration** subtree of the Performance Manager tree pane. The Card name defaults to its MAC address; you will assign a more recognizable name in a later procedure.

6. To authorize a range of IP addresses, click **New** and then click **IP Range**. The **Card IP Range** dialog box appears.



7. In the **IP Address** box, type the IPv4 or IPv6 base address.

8. If you typed an IPv6 address, click the down arrow and select **Prefix**, and then type the prefix length.

9. If you typed an IPv4 address, select **Mask** and type the subnet mask or select **Prefix** and type a prefix length.

10. Click **OK**.
11. Repeat the above steps for all authorized Cards.
12. Click **Close** to save the changes and close the **Authorized Cards** dialog box.
13. Each authorized Card connects to the Management Server and appears in the Performance Manager **Platform Configuration** subtree.

Continue with the following:

- If the ETM Server, Cards, and ETM System Console(s) are communicating, continue with "Completing Card" on page 73. If not, see "Troubleshooting System Communication" below.

Troubleshooting System Communication

If the Management Server, Cards, and/or ETM System Console(s) are not communicating, verify the following:

- IP addresses of the Cards have been entered correctly in the **Card IPs** dialog box. The Management Server must know the IP addresses of the Cards before the Cards are allowed to connect to the Server.
- The DES key entered during Card configuration via the Console port matches the DES key in the **twms.properties** file in the ETM System installation directory. The DES keys must match because initial communication between system components and the Management Server is always encrypted.
- The port numbers in the **twms.properties** files are correct and no conflicts exist with other devices or services.
- The license file **TWLicense.txt** is present in the ETM System installation directory for both the Management Server and the Report Server, if remote.
- If the ETM System components are communicating through a firewall, firewall configuration was completed properly.
- The Oracle database driver file specific to the version of Oracle you are running is present in both the ETM Server directory and any remote Usage Manager or ETM Database Maintenance Tool directories.
- The Oracle database service for the ETM System is running.
- On the Performance Manager main menu, click **Tools | View Diagnostic Logs** to review for error message that may provide insight.

If communication is still not successful, contact SecureLogix Customer Support for telephone or email support at:

- 1-877-SLC-4Help
- *support@securelogix.com*

For more information about SecureLogix Customer Support, see the SecureLogix Customer Support Handbook at **http://support.securelogix.com**/

Completing Card Configuration

For instructions for out-of-box Card configuration to enable a Card to connect to the Server, see "Configure the TDM Card(s) to Connect to the " on page 54.

The procedures below are used to complete Card configuration. The first part of Card configuration was performed via during out-of-box Appliance configuration directly on the Appliance. After the Cards have successfully connected to the ETM Server, Card configuration continues in the Performance Manager. Card configuration settings provide information that enables the Card to communicate on the data network; these settings apply to all of the Spans on the Card. The Card configuration procedure is the same for all and CRCs and Cards regardless of Span type(s) on the Card.

Note that the top-level node of a SIP or UTA Appliance represents the "Card" node, even though they have no physical Cards.

These procedures are organized in the sequence in which they should be completed.

Begin with "Creating an Appliance" below.

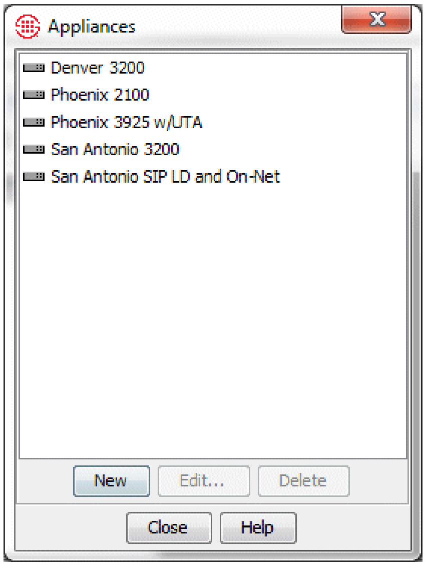
Creating an Appliance

In the **Platform Configuration** subtree, you can organize the Cards according to the Appliance chassis in which they are housed. Although this step is optional, it is recommended for uncluttering and organizing the display. Appliances in the tree pane are an organizational tool only and have no configuration settings. If you do not want to organize the Cards according to their Appliances, proceed to "Single or Multi-Card Configuration?" on page 75.

To define an Appliance

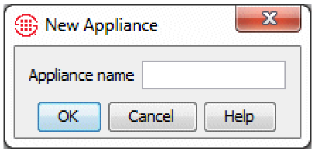
1. In the Performance Manager tree pane, right-click **Platform Configuration**, and then click **Manage Appliances**.

   The **Appliances** dialog box appears.



Denver 3200
Phoenix 2100
Phoenix 3925 w/UTA
San Antonio 3200
San Antonio SIP LD and On-Net

2. Click **New**. The **New Appliance** dialog box appears.



3. Type the label you want to use to identify this Appliance, and then click **OK**. The **Appliance** icon appears in the **Platform Configuration** subtree.

4. Repeat for each Appliance.
5. In the **Appliances** dialog box, click **Close**.

Continue with "Moving Cards to Appliances" on page 74.

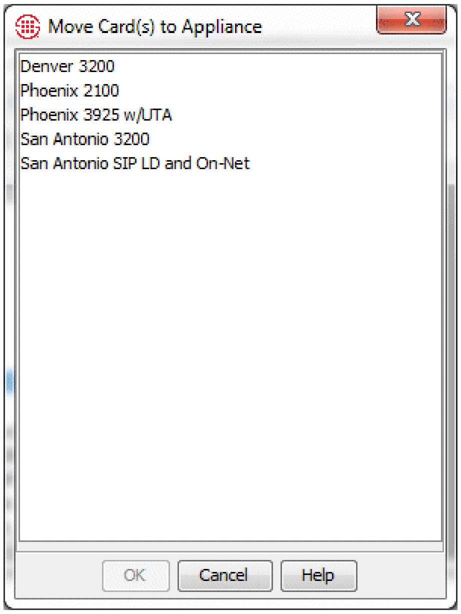
Moving Cards to Appliances

To move a Card to an Appliance

1. In the **Platform Configuration** subtree, right-click the Card, and then click **Move Card**.

   - To move multiple Cards to the same Appliance, hold down CTRL while clicking each Card, right-click the selection, and then click **Move Card(s)**.

   The **Move Card(s) to Appliance** dialog box appears listing all defined Appliances.



Move Card(s) to Appliance

Denver 3200
Phoenix 2100
Phoenix 3925 w/UTA
San Antonio 3200
San Antonio SIP LD and On-Net

2. Click the Appliance to which you want to move the Card(s), and then click **OK**.
3. Repeat for all Cards.
4. Read the discussion of "Single or Multi-Card Configuration?" on page 75, and then continue configuration with "Card Configuration" on page 76.

Single or Multi-Card Configuration?

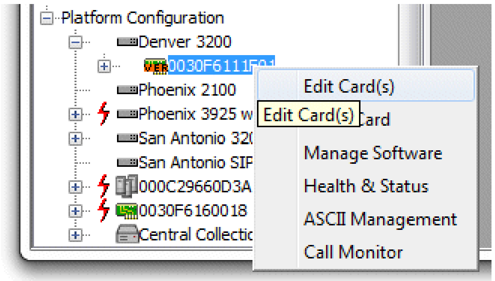
For most Card configuration tasks, you can configure either a single Card or multiple Cards at once, while a few configuration settings are unique to each Card:

- All of the tabs on the **Card Configuration** dialog box and **Multi-Card Configuration** dialog box except the **Card** tab are identical. When multiple Cards in one or more Appliances will have the same settings for these items, you can configure all of them at once using the **Multi-Card Configuration** dialog box.
- The **Card** tab appears only on the (single) **Card Configuration** dialog box and contains Card-specific settings, including the name, IP address, and Span license key (if applicable). These items must be set individually per Card.
- The **General** tab appears only the **Multi-Card Configuration** dialog box and contains the name of each of the selected Cards.

Single Card Configuration

To open the Card Configuration dialog box

- In the **Platform Configuration** subtree, expand the Appliance containing the Card, right-click the **Card** icon, and then click **Edit Card(s).**



Multi-Card Configuration

To open the Multi-Card Configuration dialog box

Select multiple Cards as follows:

- To select multiple adjacent Cards:
  - In the **Platform Configuration** subtree, hold down SHIFT, click the first and last adjacent Card, and then right-click the selection, and then click **Edit Card(s)**.
- To select multiple nonadjacent Cards:
  - In the **Platform Configuration** subtree, hold down CTRL, click each Card, right-click the selection, and then click **Edit Card(s).**

When you select more than one Card to configure at the same time, the **Multi-Card Configuration** dialog box appears. The following buttons appear on the **Multi-Card Configuration** dialog box:

⇐ This button indicates a configuration item is set the same for all selected Cards and the field is editable.

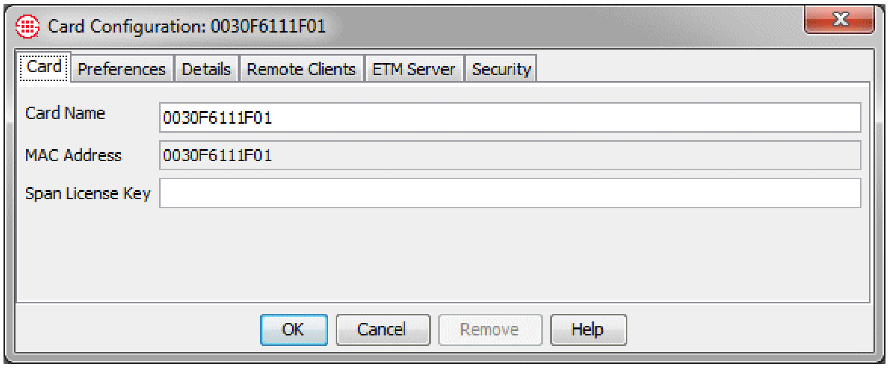
🚫 This button indicates a configuration item is not currently set the same for all selected Cards, and the field is grayed out. If you want to set the item the same for all selected Cards, click the button to enable the field to be edited.

Card Configuration Settings

This procedure assumes single Card configuration, but for the most part, the same procedure applies when configuring multiple Cards. When differences exist, they are pointed out in the procedure. If you want to configure multiple Cards at once, see "Single or Multi-Card Configuration?" on page 75.

To complete Card configuration

1. In the **Platform Configuration** subtree, right-click a Card, and then click **Edit Card(s).** The **Card Configuration** dialog box appears with the **Card** tab selected.



Card Configuration: 0030F6111F01

Card Name: 0030F6111F01

MAC Address: 0030F6111F01

Span License Key:

- The MAC address is a unique hardware identifier specific to this Card; it cannot be modified.

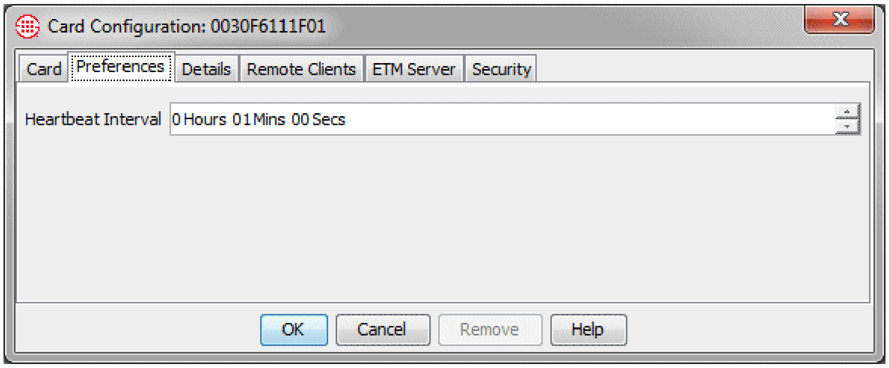
2. In the **Card Name** box, type a unique identifier for the Card. The default is the MAC address. Note that Cards are listed in the tree in ASCII order.

   If you are using the **Multi-Card Configuration** dialog box, the **Card** tab is not available. You must select each Card individually to configure this tab. By default, the Card's MAC address is its name. The name you type here appears in the Performance Manager tree pane for the Card icon. `

3. (*Not applicable to single-Span Cards, including SIP and UTA)* The **Span License Key** box provides the license key that enables multiple Spans on the Card. (Span 1 is licensed by default.). If you need to license additional Spans on the Card and did not do so during out-of-

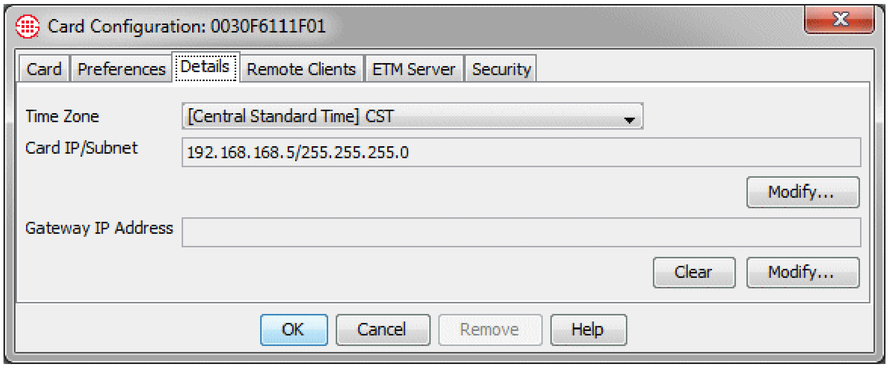
box configuration, type the 16-character Span license that you received from SecureLogix Corporation.

4. The **Preferences** tab sets the heartbeat interval for the Card. It is recommended that you do not change this setting; use the default of 1 minute.



Heartbeat Interval: 0 Hours 01 Mins 00 Secs

5. Click the **Details** tab.



Time Zone: [Central Standard Time] CST

Card IP/Subnet: 192.168.168.5/255.255.255.0

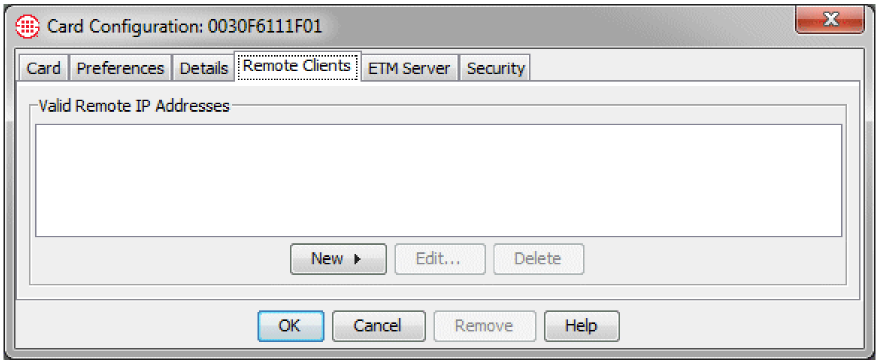
Gateway IP Address:

6. In the **Time Zone** box, click the down arrow and select the correct time zone for the Appliance location. The time zone is set by default to GMT. If the time zone on the Card is not set correctly for the Appliance location, the Management Server cannot correlate calls with SMDR data and monitoring results may be misleading.

7. The **Card IP/Subnet** and **Gateway IP Address** were assigned to the Card during out-of-the-box configuration at the Console port.

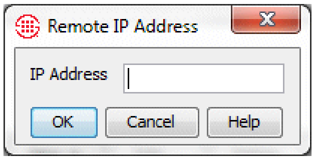
8. Click the **Remote Clients** tab (*optional*).

   The **Remote Clients** tab is used to authorize certain computers as remote clients from which authorized users can access the Card and its Spans via Telnet or SSH to view or change configuration. Telnet or SSH access can be useful, for example, if network problems interrupt communication between the ETM Server and the Cards/Spans. You can authorize up to 64 remote clients. As a security feature, remote client access is only allowed from computers whose IP addresses are listed in this tab. A Card and its Spans only accept Telnet and SSH connections if the Card security posture is set to **LOW**.

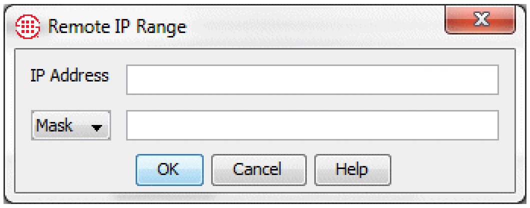


See "Managing Telnet Logins to a Card" in the *ETM® System Administration and Maintenance Guide* and "Logging In to a Span via Telnet" in the *ETM® System Technical Reference* for more information about logging in to a Card or Span via Telnet.

9. To authorize a specific IP address, click **New** and then click **IP Address**. The **Remote IP Address** dialog box appears.

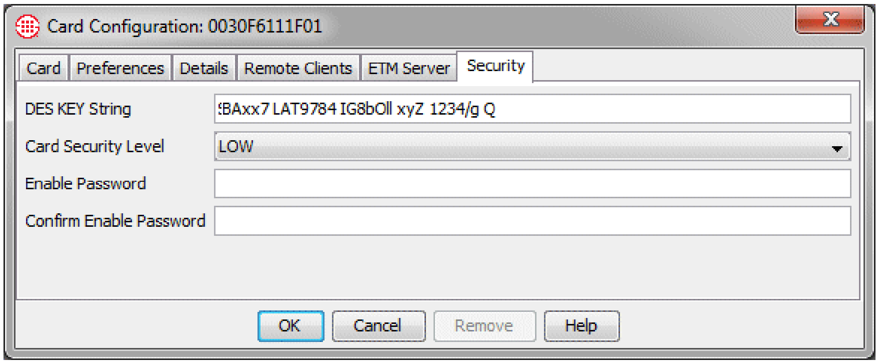


10. Type the IPv4 or IPv6 address of the Card.
11. Click **OK**.
12. To authorize a range of IP addresses, click **New** and then click **IP Range**. The **Remote IP Range** dialog box appears.



13. In the **IP Address** box, type the IPv4 or IPv6 base address.
14. If you typed an IPv6 address, click the down arrow and select **Prefix**, and then type the prefix length.
15. If you typed an IPv4 address, select **Mask** and type the subnet mask or select **Prefix** and type a prefix length.
16. Click **OK**.
17. Repeat the above steps for all authorized remote clients for this Card.
18. The settings on the **ETM Server** tab were configured during initial out-of-box Card configuration. If you need to change these settings, see "Viewing/Changing Network Information for Card/Server Communication" in the *ETM® System Administration and Maintenance Guide*.

19. Click the **Security** tab.



Card Configuration: 0030F6111F01

DES KEY String: :BAxx7 LAT9784 IG8bOll xyZ 1234/g Q

Card Security Level: LOW

Enable Password:

Confirm Enable Password:

a. The Management Server is preconfigured with a default DES key string to enable the ETM Server and Cards to establish communication. Communication between the Cards and the ETM Server is encrypted with 3DES encryption. You can change the DES Key this Card uses to communicate with the Server to a secret key for added security. You can also multiselect Cards and change their DES Keys to the same value.

- In the **DES Key** box, type a new DES Key. The DES Key string must contain 16-50 characters and spaces, and can consist of any combination of letters, digits, and special characters except the "pipe" (|) symbol. The Card always initiates the connection to the Management Server and validates that connection with an encrypted message sequence, eliminating the possibility of a Card connecting to a rogue "Server" and thereby potentially impacting telecommunications service.

b. The **Card Security Level** controls access to the security-related Card settings. In the **Card Security Level** box, click the down arrow and select the appropriate security level:

LOW—Allows you to change security-related Card settings via Telnet, the Performance Manager, or the **Console** port of the Controller Card.

MEDIUM—Allows you to change security-related Card settings via the Performance Manager or the **Console** port of the Controller Card. Telnet is disabled.

HIGH—Allows you to change security-related Card settings only via the **Console** port of the Controller Card. You cannot change security-related settings via the Performance Manager and Telnet is disabled.

Unlike other Card settings, the Card is authoritative on the **Card Security Level** setting, even for established connections. This means that if the value on the Card is different from that on the Server, the Card's value is used and sent to the Server on the next connection. This means that changes of this setting from a command-line are persisted.

The following Card security-related configuration settings are affected by the **Card Security Level** setting.

- Network connection information—netmask, gateway IP address, Management Server IP address, Management Server port.
- Security settings—DES Key, Card security level, Enable password.

IMPORTANT The Server has authority over these settings except when the Card Security Level is set to HIGH. Even when the Card Security Level is HIGH, however, these values are not sent to the Server if they are changed on the Card.

c. You set the Enable password during initial Card configuration at the Appliance. You do not need to type it here unless you are changing it. If you want to change it, type the same password in the **Enable Password** and **Confirm Enable Password** boxes.

20. Click **OK** to save the changes and download them to the Card.

Continue with one of the following:

- If you need to install new software on the Card(s), see "Card Software Installation" on page 80. Perform this procedure only if instructed to do so by SecureLogix installation or support personnel. Otherwise, see the next bullet.
- Continue with “Configuring Telco Spans" on page 86.

Card Software Installation

Since the Appliances are shipped with factory defaults, the latest version of the Appliance software may not be installed. The ETM System installation directory contains the latest software available at release. Additional software updates may be available from the SecureLogix website at *www.support.securelogix.com*. Install the latest software version before continuing configuration. Appliance software is located at the following path:

<INSTALL_DIR>\ps\software_repository\package

Copy the latest version to this directory. You can install software on multiple Cards at once when the Appliances are the same models. Otherwise, you must install software on individual Cards.

Important Information about Installing Card Software

When you download a software package to a Card, it is imperative that you do not reboot or power cycle the Card until the upgrade is complete, or the firmware may become corrupted, rendering the Card inoperable. The Card automatically reboots when the upgrade is complete.

How long a Card upgrade takes varies depending on the size of the package and which firmware devices are being reprogrammed. During a Card upgrade, the compact flash (hard drive) is first reprogrammed; then, depending on the upgrade, the boot flash and one to six other firmware devices may be reprogrammed. The firmware devices are verified against the new code; if different, they are reprogrammed. Verification can take from 20 to 120 seconds per device (depending on the size of the device) and reprogramming can take from 30 to 240 seconds per device.

During reprogramming of the devices, interrupts are ignored, so the Card is very quiet. This is normal and does not indicate a problem. When reprogramming is complete, the Card automatically reboots. This should occur in no more than 15 minutes.

In rare cases, errors do occur that render the Card unresponsive. Should the Card become completely unresponsive, a "watchdog timer" will normally cause the Card to automatically reboot. If it does not and you believe the Card is completely unresponsive, be certain that 15 minutes has elapsed since you began the download. Do not manually power cycle or reboot the Card, and call SecureLogix Technical Support. (On TDM Appliances, connect via the **Console** port if possible prior to contacting Technical Support.) A Last Resort recovery boot is available to recover unresponsive Cards.

Installing Card Software

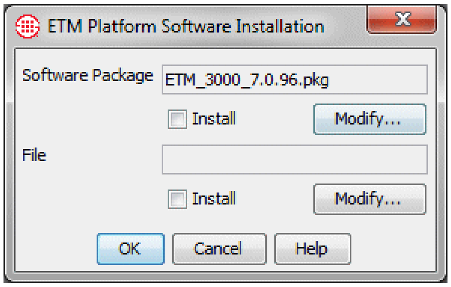
IMPORTANT This procedure applies only to newly installed Cards. If you are upgrading from a previous software version, see the SecureLogix Knowledge Base for upgrade instructions applicable to the installed Card software version instead of using this procedure. Before beginning, ensure that the software to be installed resides in the following directory:

<INSTALL_DIR>\ps\software_repository\package

To install Card software

1. In the **Platform Configuration** subtree, do one of the following:
   - **Single Card**—Right-click the Card, and then click **Manage Software**.
   - **Multiple Cards**—Hold down CTRL, and then click each same-model Card you want to install software on, right-click the selection, and then click **Manage Software**.

   The **ETM Platform Software Installation** dialog box appears.



ETM Platform Software Installation

Software Package: ETM_3000_7.0.96.pkg

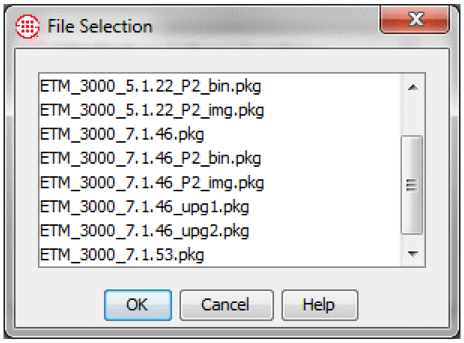
□ Install

File:

□ Install

2. Under the **Software Package** box, click **Modify**.

   The **Software Version Selection** dialog box appears, showing all of the packages on the Server that apply to the selected Card type. For example, if you are selecting software for an ETM 3200 Card, only software packages applicable to 3200 Cards appear.



File Selection

ETM_3000_5.1.22_P2_bin.pkg
ETM_3000_5.1.22_P2_img.pkg
ETM_3000_7.1.46.pkg
ETM_3000_7.1.46_P2_bin.pkg
ETM_3000_7.1.46_P2_img.pkg
ETM_3000_7.1.46_upg1.pkg
ETM_3000_7.1.46_upg2.pkg
ETM_3000_7.1.53.pkg

3. Click the latest software package, for example. **ETM_3000_7.1.53.pkg**, and then click **OK**.

⚠ ***WARNING*** Do not reboot or power cycle the Card during software download, or you may render the Card inoperable. The Card automatically reboots after the software is installed. Observe the **Status Tool** and **Diagnostic Log** during the download. If you believe the Card is completely unresponsive, be certain that 15 minutes has elapsed since you began the download, and then contact SecureLogix Customer Support before you manually power cycle or reboot the Card. A Last Resort recovery boot is available to recover unresponsive Cards.

Additional Steps for SIP and UTA:

- **SIP**—If you are installing software on a SIP Appliance, the procedure above pushed the software to the Call Processor, which then made it available on the Signaling and Media Proxy nodes. Continue with “SIP Appliances Only” on page 83 to activate the new software on the proxy nodes.
- **UTA**— If you are installing software on a UTA Appliance, the procedure above pushed the software to the Call Processor, which then

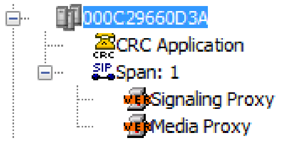
made it available on the Signal Processor and Media Proxy nodes. Continue with “UTA Appliances Only” on page 84 to activate the new software on the proxy nodes.

SIP Appliances Only

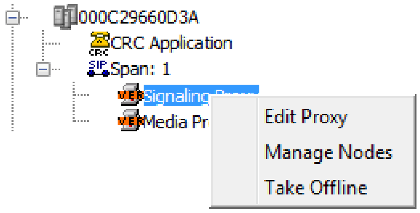
After installing new Appliance software on the SIP Call Processor, you must activate it on each of the proxy nodes for that appliance. If HA is in use, it is recommended that you upgrade one Media Proxy node and one Signaling Proxy node and then isolate all other nodes to force failover to the upgraded nodes. If no issues occur, include the isolated nodes and activate the software on them. If issues do occur, you can include the non-upgraded nodes so processing returns to one of them and isolate the upgraded node until the issues are resolved.

To activate newly installed software on the proxy nodes

1. After pushing the software to the Call Processor , ensure that the installation is complete by viewing the Status Tool before continuing with the steps below. When the installation is complete, a version mismatch indicator appears on the Signaling and Media Proxy icons. Expand the Span node to access the Signaling and Media Proxy nodes.



2. In the Performance Manager tree pane, right-click the Media Proxy and click **Manage Nodes**.



The **Node Manager** appears.

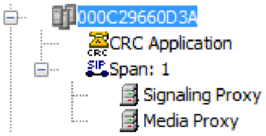
3. Right-click a node and click **Update Software**. The update may take a few minutes to complete.

4. Right-click the Signaling Proxy and click **Manage Nodes**. The **Node Manager** appears.

5. Right-click a node and click **Update Software**. The update may take a few minutes to complete.

6. If HA is in use, isolate the other nodes to force failover to the upgraded node. If no issues occur, include the isolated nodes and repeat the above procedure for each node.

When the update is complete, the version mismatch indicator disappears.

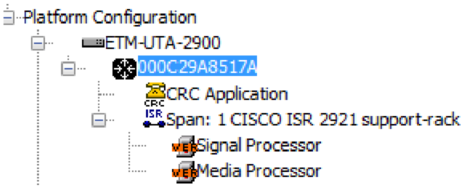


UTA Appliances Only

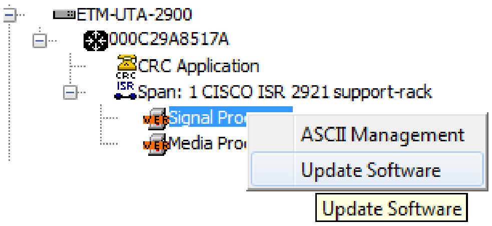
After installing new Appliance software on the UTA Call Processor , you must activate it on each of the UTA nodes for that appliance.

To activate newly installed software on the UTA nodes

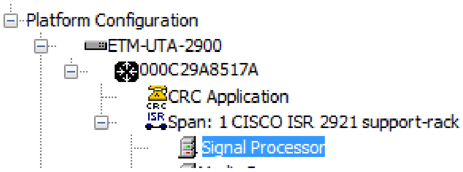
1. Ensure that the software has completed installation on the Call Processor by viewing the Status Tool before continuing with the steps below. When the installation on the Call Processor is complete, a version mismatch indicator appears on the icons for the Media and Signal Processors. Expand the Span icon to access the Media and Signal Processors.



2. Right-click the Signal Processor and click **Update Software**.



The update is complete when the version mismatch indicator disappears from the Signal Processor icon. This may take a few minutes. The status is not shown in the Status Tool.



3. Right-click the Media Processor and click **Update Software**. The update is complete when the version mismatch indicator disappears from the Media Processor icon. This may take a few minutes. The status is not shown in the Status Tool.

Continue with "Configuring Telco Spans" on page 86.

Configuring Telco Spans

Telco Span configuration provides telephony- and Policy-processing information specific to each Span. These instructions do not apply to CRCs. You can configure some Span settings on more than one Span at once, while other configuration settings are only available for individual Spans. If you have more than one Span of the same type, see "Importing Span Configuration" on page 122 to import the settings from one Span to another of the same type.

How These Instructions are Organized

Many Span configuration settings apply to all Span types, while others are specific to certain types of Spans. These instructions are organized per tab on the **Span Configuration** dialog box. Settings that apply to all or most Span types are discussed first, followed by settings specific to certain Span types. The applicable Span type(s) are noted in each procedure, with directions for where to go next at the end of each procedure.

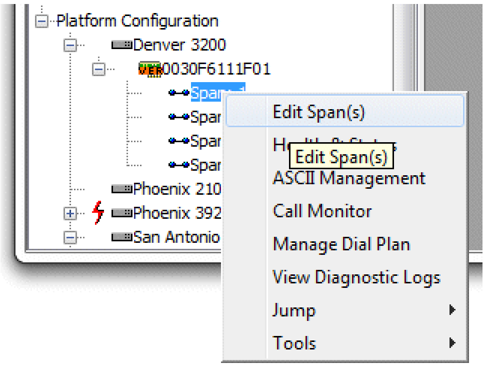
Single or Multi-Span Configuration?

Not all Span configuration items can be set globally; the tabs displayed on the **Multi-Span Configuration** dialog box depend upon the type(s) of the Spans selected. For example, if you select two T1 PRI Spans, the **General**, **Preferences**, **Telephony**, **Global Line Settings**, **PRI**, and **T1 Setup** tabs are displayed. If you select one PRI Span and one non-PRI Span, only the **General**, **Preferences**, **Telephony**, and **Global Line Settings** tabs are displayed, because these are the only values in common between the types of Spans selected..

Single Span Configuration

To open the Span Configuration dialog box

- In the **Platform Configuration** subtree of the Performance Manager tree pane, expand the Card node, right-click the Span, and then click **Edit Span(s)**.



Multi-Span Configuration

When you select more than one Span to configure at the same time, the **Multi-Span Configuration** dialog box appears. The following buttons appear on the **Multi-Span Configuration** dialog box:

⇐ This button indicates a configuration item is set the same for all selected Spans and the field is editable.

🚫 This button indicates a configuration item is not currently set the same for all selected Spans, and the field is grayed out. If you want to set the item the same for all selected Spans, click the button to enable the field to be edited.

To open the Multi-Span Configuration dialog box

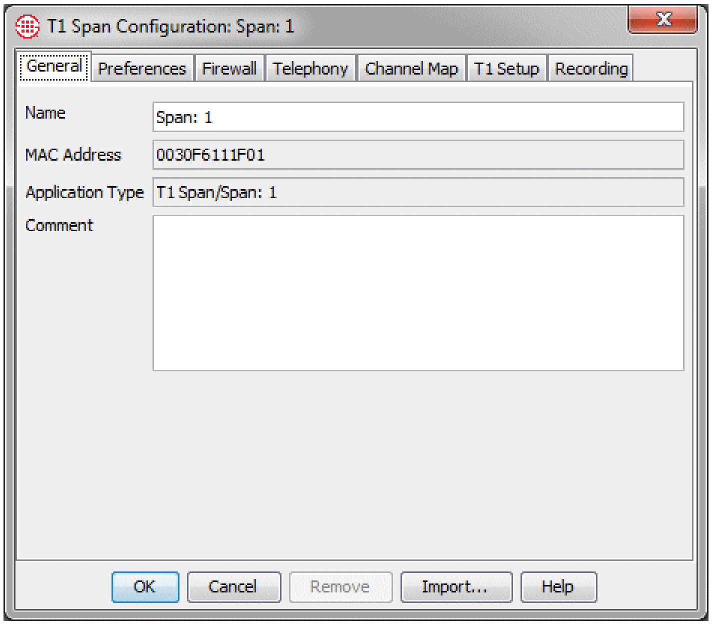
- In the **Platform Configuration** subtree, do one of the following:
  - To configure more than one adjacent Span at once, hold down SHIFT, click the first and last adjacent Span, right-click the selection, and then click **Edit Span(s)**.
  - To configure more than one non-adjacent Span, hold down CTRL, click each Span to be configured, right-click the selection, and then click **Edit Span(s)**.

General Tab

Two of the settings on the **General** tab are user-modifiable: **Name** and **Comment**. By default, all Spans are named **Span:*n***, where ***n*** is the Span's number on the Card (1–4). You should change the name to something unique or the tree display and monitoring results will be confusing. To change the name or comment, you must select only a single Span for editing. On the **Multi-Span Configuration** dialog box, the **General** tab only displays the names of the Spans being configured and is not editable...

To name the Span

1. In the **Span Configuration** dialog box, click the **General** tab.



Name: Span: 1

MAC Address: 0030F6111F01

Application Type: T1 Span/Span: 1

Comment:

- The **MAC Address** is the same as that of the Card.
- The **Application Type** is the type of resource selected and includes the physical number of the Span on the Card.

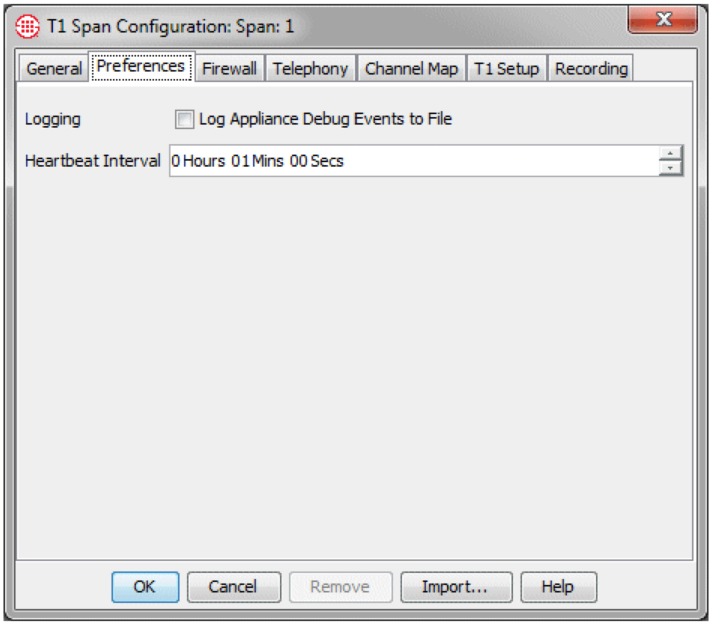
The Spans appear in the tree pane in ASCII order. If you want the Spans to appear in Span order, you must name them appropriately.

2. In the **Name** box, type a name for the Span. You can choose any name that is meaningful to you, such as the circuit ID assigned by the CO or a location/Span-type identifier. The **Name** identifies the Span in the Performance Manager tree pane, call processing results, and reports.
3. Optionally, in the **Comment** field, type a descriptive comment, perhaps identifying the location and type of Span or some other key information. By default, the comment appears as a tool tip when you hover over the Span icon in the Performance Manager tree pane. (You can optionally disable the tool tip in the **ETM Server Properties Tool**. For instructions, see the *ETM® System Administration and Maintenance Guide*.)

Preferences Tab

To configure Span preferences

1. In the **Span Configuration** dialog box, click the **Preferences** tab.



T1 Span Configuration: Span: 1

Logging □ Log Appliance Debug Events to File

Heartbeat Interval 0 Hours 01 Mins 00 Secs

2. In the **Logging** area, select the **Log Appliance Debug Events to File** check box if you want to capture Span-specific debugging information in a file on the hard drive of the Management Server for troubleshooting purposes. Be certain to clear this check box when you no longer need to store this information, to prevent unnecessary use of hard drive space. Debug logging can quickly generate a large file.

   The file is saved in the ETM System installation directory on the Management Server computer at the following path:

   <INSTALL_DIR>/debug/<macaddress_Spannumber_uniqueid>.dbg

3. The **Heartbeat Interval** specifies how often the Span contacts the Management Server. The default heartbeat interval is 60 seconds. It is strongly recommended that you do not change this setting. More frequent heartbeats increase network load and do not increase reliability. However, a shorter heartbeat interval decreases the time until the Management Server becomes aware of a lost connection in some network configurations.

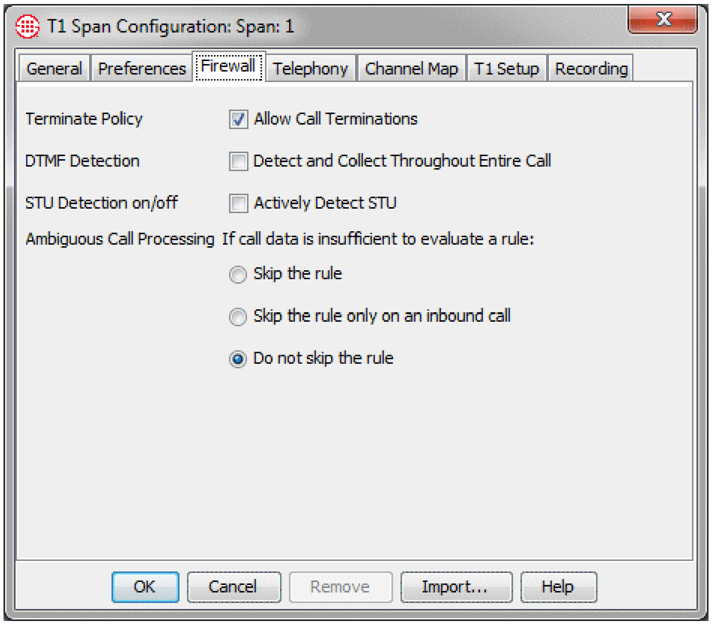
Firewall Tab

The **Firewall** tab provides settings specific to ETM Policy processing.

To set Firewall tab settings

1. In the **Span Configuration** dialog box, click the **Firewall** tab.

The Management Server handles up to 64 DTMF digits.



Terminate Policy ☑ Allow Call Terminations

DTMF Detection □ Detect and Collect Throughout Entire Call

STU Detection on/off □ Actively Detect STU

Ambiguous Call Processing If call data is insufficient to evaluate a rule:

○ Skip the rule

○ Skip the rule only on an inbound call

● Do not skip the rule

2. Select the **Allow Call Terminations** check box to enable calls to be terminated; clear the **Allow Call Terminations** check box to prevent any calls from being terminated on this Span.

   The **Terminate Policy** setting applies to enforcement of terminate Rules in Policies, manual termination via the **Call Monitor**, and terminate commands issued via ETM Commands. If this check box is not selected, no calls can be terminated on this Span, regardless of the setting in a Rule's **Action** field or user permissions. By default, the check box is cleared.

3. The **DTMF Detection** setting applies to all calls on all channels, since DTMF digits are passed once the call is established, even if MF digits are used for signaling.

   - Select the **Detect and Collect Throughout Entire Call** check box to capture all DTMF digits throughout the duration of the call and store them in the Database. If this is selected, interdigit timing is also stored. **IMPORTANT** You can use DTMF digit patterns in Policies without selecting this checkbox to store them in the Database.
   - Clear the **Detect and Collect Throughout Entire Call** check box to capture only digits pertaining to call establishment.

4. (*Not applicable to SIP or UTA Spans*) If STU-IIIs are in use on the selected Span(s), turn STU detection on to enable STUs to be recognized. STU detection is **OFF** by default.

   - To turn STU detection on, in the **STU Detection on/off** area, turn STU detection on by selecting the **Actively Detect STU** check box.

5. (*Not applicable to SIP or UTA Spans*) The **Ambiguous Call Processing** setting determines how calls are to be processed when sufficient call data is not available to evaluate a particular call against a Policy Rule. Select one of the following options:

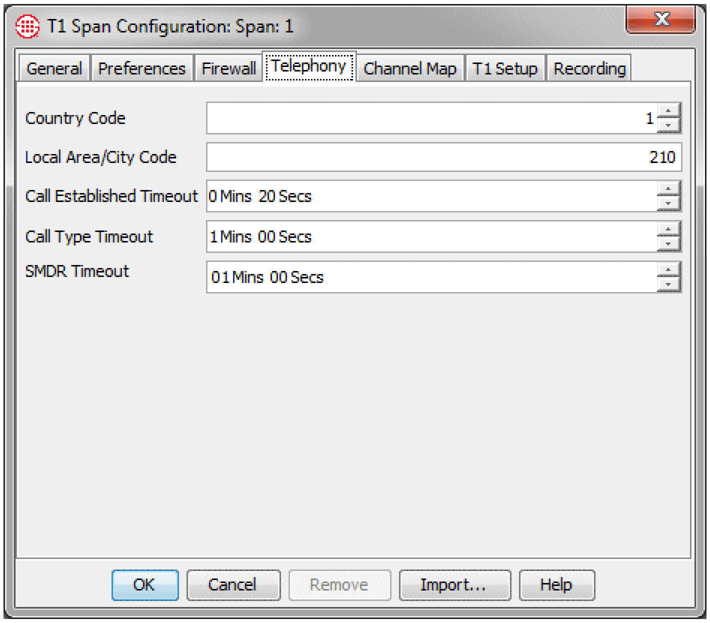
   - **Skip the Rule**—If an ambiguous call is encountered, the Rule is skipped, and processing continues with the next Rule.
   - **Skip the Rule only on an inbound call**—If an ambiguous call is encountered during an inbound call, the Rule is skipped and processing continues with the next Rule in the Policy. When an ambiguous call is encountered during an outbound call, the Policy stops executing and no Tracks (except logging) are executed. Inbound calls are distinguished from outbound calls because call logs from the local PBX (SMDR) can be used to resolve outbound calls that were ambiguous because the source phone number was unavailable during the call. When SMDR data is available to provide the source number, the outbound call is again processed against the Policy and any applicable Tracks are executed.
   - **Do not skip the Rule**—If an ambiguous call is encountered during any call, the Policy stops executing and no Tracks (except logging) are executed. If SMDR is in use, outbound calls that were ambiguous due to missing source number are reprocessed against the Policy when SMDR data is available to provide the source, and any applicable Tracks are executed.

Telephony Tab

(*Does not apply to SS7 signaling links*)

To configure telephony settings

1. In the **Span Configuration** dialog box, click the **Telephony** tab.



Country Code 1

Local Area/City Code 210

Call Established Timeout 0 Mins 20 Secs

Call Type Timeout 1 Mins 00 Secs

SMDR Timeout 01 Mins 00 Secs

2. In the **Country Code** box, type the country code for the country in which the Appliance is located. By default, the country code is set to 1. (U.S., North American Numbering Plan).

3. In the **Local Area Code** box, type the area code where the Appliance is installed. By default, the area code is set to 210 (San Antonio, Texas).

4. (*Not applicable to SIP or UTA Spans*) In the **Call Established Timeout** box, type the length of time after the last digit is dialed until a call is marked as established. The default is 20 seconds, which corresponds with the timeout value of most telephone network switches. If your network differs, adjust this value accordingly. This setting is used for outbound analog and T1 loop start and ground start calls, which do not provide answer supervision.

5. (*Not applicable to SIP or UTA Spans*) In the **Call Type Timeout** box, type the length of time the Span waits after a call is established before first classifying a silent or indistinguishable call as Voice. Call type timeout only applies to calls where lack of activity on the line prevents the Span from determining the call type. Setting this value too low can cause an excessive number of call type changes. The default is 60 seconds.

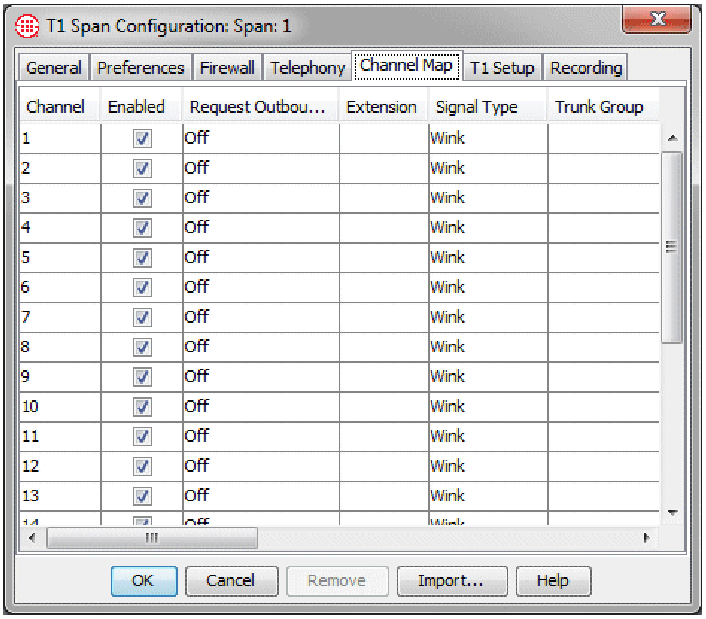
6. (*Not applicable to SIP or UTA Spans*) If SMDR is in use, in the **SMDR Timeout Period** box, type the length of time the Span is to wait for an SMDR result from the Management Server after a call ends. The default is 1 minute.

Channel Map Tab

(*Does not apply to SIP or UTA Spans or SS7 signaling links*) If you are configuring more than one Span at once, the **Channel Map** tab is not available; you can configure some of these settings on the **Global Line Settings** tab (see "Global Line Settings Tab" on page 99 for instructions). The **Channel Map** tab of the **Span Configuration** dialog box contains telecom settings that must be correctly defined to enable the ETM® System to monitor call traffic. Improper settings degrade or prohibit proper signal traffic, cause false signal activity, or impair Policy execution. See "At-a-Glance Reference Table to TDM Span Telco Settings" on page 197 for reference on these settings.

To configure the Channel Map

1. In the **Span Configuration** dialog box, click the **Channel Map** tab.



Channel	Enabled	Request Outbou...	Extension	Signal Type	Trunk Group
1	☑	Off		Wink	
2	☑	Off		Wink	
3	☑	Off		Wink	
4	☑	Off		Wink	
5	☑	Off		Wink	
6	☑	Off		Wink	
7	☑	Off		Wink	
8	☑	Off		Wink	
9	☑	Off		Wink	
10	☑	Off		Wink	
11	☑	Off		Wink	
12	☑	Off		Wink	
13	☑	Off		Wink	
14	☑	Off		Wink	

2. Monitoring is enabled on all channels by default. This is indicated by the check mark in the **Enable** column.

   - Clear the checkbox for each channel you do not want the ETM System to monitor.
   - To clear multiple adjacent channels, click the first cell to be cleared, hold down SHIFT, and then click the last cell to be cleared.

3. (*Only applies if SMDR is in use, and only applies to outbound calls*) By default, **Request Outbound SMDR** is **Off**.

   a. In the **Request Outbound SMDR** column, select each channel for which you want the Span to request outbound SMDR data from the Server. To set all channels on the Span to the same value, click the first cell in the **Request SMDR** column, hold down SHIFT, and then click the last cell in the column.

   b. Click one of the following:

   - **Off**—The Span does not request outbound SMDR data from the Server. The source number in signaling is used if available; if not, the value in the Extension map is used, if available; otherwise, no source is available. The call data available during the call is used to populate the database.

   - **On**—The Span requests and waits for outbound SMDR data from the Server. The source number collected from signaling, if any, is not used, but the source number collected from SMDR is used for Policy processing and is inserted into the database.

   - **Augment**—The Span performs Policy processing with the source number in the signaling if it is present, but requests and waits for the outbound source number from SMDR if necessary. If the source number is collected from the signaling, it is used to populate the database; the source number collected from SMDR is only inserted into the database if no source was received in the signaling. Any non-signaling fields (Access Code, SMDR1, SMDR2, etc.) available in SMDR are inserted into the database.

   - **Replace**—The Span performs Policy processing with the source number in the signaling if it is present, but requests and waits for the outbound source number from SMDR if necessary. The source number collected by the Span from signaling is used for policy processing, but after the call ends, the value received from the signaling is replaced in the database with the source number collected from SMDR. Any non-signaling fields (Access Code, SMDR1, SMDR2, etc.) available in SMDR are inserted into the database.

4. (*Applies only to recording Spans. Not applicable to UTA*) Inbound SMDR can be used to identify the called extension for recorded calls, to ensure that recordings of calls to Protected Extensions are not retained. You specify per channel whether Inbound SMDR is to be requested. Protected Extension processing only applies to channels on which Inbound SMDR is enabled. Inbound SMDR is only used for Protected Extension processing; it is not used for Policy processing.

   See the *Call Recorder User Guide* for instructions for configuring Protected Extensions.

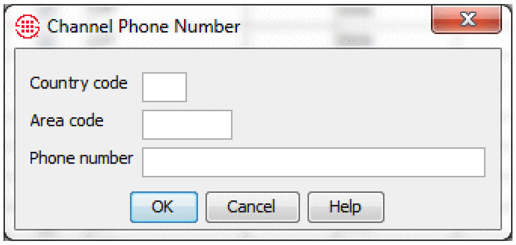
   - In the **Request Inbound SMDR** column, select each recording-enabled channel on which Inbound SMDR is to be used.

You can clear all extensions for multiple Spans by selecting **Clear all Extensions** on the **Global Line Settings** tab.

5. *(Optional)* In the **Extension** column, for each enabled channel, do one of the following:

   - To modify one channel, double-click the **Extension** cell.
   - To assign the same extension to all channels, click the first **Extension** cell, hold down SHIFT, and then double-click the last cell.

     The **Channel Phone Number** dialog box appears.

     Channel Phone Number

     Country code

     Area code

     Phone number

     a. Type the country code, area code, and phone number of the dedicated line number, main switchboard number, or some other recognizable, unique number associated with the channel. For readability, the digits typed in the **Phone number** box can be separated by a space, period, or hyphen.

     b. Click **OK**.

     IMPORTANT The **Extension** map is used to provide the Span with a default source number for outgoing calls or a default destination number for incoming calls only if this information is unavailable from call data or SMDR. If either source or destination is unavailable, the Span may be unable to determine whether a call matches a given Rule, and the call would then be ambiguous.

     If SMDR is available and requested on a given channel, the **Extension** map is ignored for outgoing calls and only SMDR data is used. In this case, the **Extension** map is used only if the Span did not receive the destination number in the dialed digits or call data.

6. In the **Signal Type** column, for each enabled channel, click the down arrow and select the correct signaling in use on the channel.

   CAUTION If **Signal Type** is set incorrectly, the Span will not be able to evaluate Policy Rules against calls or terminate calls.

   - To specify the same signal type for all channels (or an adjoining group of channels), click the first **Signal Type** cell, hold down SHIFT, and then click the last cell, and then click the down arrow in the last selected cell and select the signaling type.

     The following signal types are supported:

     – WINK (T1 CAS)

- GROUND (T1 CAS, Analog)
- LOOP (T1 CAS, Analog)
- IMMEDIATE (T1 CAS, Analog)
- ISDN PRI (E1 and T1 PRI)
- WINK IN/IMMEDIATE OUT (T1 CAS)
- IMMEDIATE IN /WINK OUT (T1 CAS)
- R1 (E1 CAS)

7. *(Optional)* In the **Trunk Group** column, click a cell and type the trunk group for the channel. A trunk group entry can contain a maximum of 20 characters.

   - To specify the same trunk group for an adjoining group of channels, click the first **Trunk Group** cell, hold down SHIFT, and then click the last cell, and then type the trunk group. When you click anywhere else on the dialog box, the trunk group is applied to all of the cells you had selected.

8. The **Caller ID** field indicates whether Caller ID is enabled on a channel and should be used to determine calling numbers. If a Caller ID option is not selected, Caller ID is not used, even if it is available on the line. Note that if you specify Caller ID for a channel on which Caller ID is not actually available, error messages appear in the **Caller ID** field of the call log.

   If Caller ID is available in the call data, in the **Caller ID** column, click the drop-down box and select the type of Caller ID for each enabled channel. The default is **None**. The following options are available:

   Bellcore—US, Canada, South Korea

   UK BT—British Telecom users in the UK

   ETSI—UK, Germany, Italy

   NTT—Japan

   DTMF—UK analog lines that send a polarity reversal and the DTMF caller ID prior to the first ring (ETS 300 659-1).

To place the same value in a contiguous set of fields, click the first field, hold down SHIFT, click the last field, and then click the down arrow in the last field and select an option.

9. In the **Tone Type** column, for each enabled channel, click the down arrow and select the correct tone type to match the telephone network. Tone type specifies the digit tones used for call setup and teardown with ANI, DNIS, ADDR, and DID numbering formats. The ETM System default is **DTMF**.

   - To set the same tone type for an adjoining group of channels, click the first **Tone Type** cell, hold down SHIFT, and then click the down arrow in the last cell, and then select the tone type. All selected cells are populated.

DTMF—Dual-tone, multi-frequency, for touch-tone phones and dial pulse lines.

MF—Multi-frequency, for signaling and dial pulse digits within the telephone network.

Outgoing Numbering Format, Incoming Numbering Format, and Tone Type must be set per Span; they cannot be set globally.

10. For each enabled channel, click the **Outgoing Numbering Format** cell, and then type the applicable tokens (up to 40 characters). Outgoing numbering format specifies the format of the MF or DTMF digits that the PBX sends to the telephone network during address/destination transmission. The Outgoing Numbering Format consists of a user-defined string of tokens. The default is **ADDR**.

    The table below lists valid Outgoing Numbering Format tokens. Note that multiple tokens can be specified in a cell; separate tokens with a space (for example, KP ADDR ST).

Token	Meaning
ADDR	Variable-length destination number
ADDR-n	n-digit destination number (1-33)
KP	MF KP DIGIT
ST	MF ST digit
#	DTMF # digit
*	DTMF * digit

- To set the same outgoing numbering format for an adjoining group of channels, click the first **Outgoing Numbering Format** cell, hold down SHIFT, and then click the last cell, and then type the string. When you click anywhere else in the **Channel Map**, the cells that you had selected are populated.

11. For each enabled channel, click the **Incoming Numbering Format** cell, and then type the applicable tokens (up to 40 characters). Incoming numbering format specifies the format of the MF or DTMF digits received from the telephone network during call setup for ANI, DNIS, and DID calls. The default is **ADDR**.

    Incoming numbering format must match the format on the channel and must correspond correctly to the tone type; otherwise, the ETM System Dialing Plan is unable to process call data.

    If DID/DNIS lines are used, the Incoming Numbering Format must specify DID/DNIS to enable the Dialing Plan to correctly convert the extensions for Policy enforcement and the DID section of the Dialing Plan must be correctly configured. For more information about Dialing Plans, see “Defining Dialing Plans" in the *ETM® System Technical Reference*.

Format Precedence must be set individually per Span; it cannot be set globally

The table below lists the valid Incoming Numbering Format tokens. Note that multiple tokens can be specified in a cell; separate tokens with a space (for example, KP ADDR ST).

Token	Meaning
ADDR	Variable-length destination number
ADDR-n	n-digit destination number
ANI	Variable-length ANI
ANI-n	n -digit ANI (1-33)
DID	Variable-length DID
DID-n	n-digit DID (1-33)
DNIS	Variable-length DNIS
DNIS-n	n-digit DNIS (1-33)
KP	MF KP DIGIT
ST	MF ST digit
#	DTMF # digit
*	DTMF * digit

For more information about Dialing Plans, see "Defining Dialing Plans" in the *ETM® System Technical Reference*.

- To set the same incoming numbering format for an adjoining group of channels, click the first **Incoming Numbering Format** cell, hold down SHIFT, and then click the last cell, and then type the string. Press ENTER to populate the selected cells.

12. For each enabled channel, click the **Format Precedence** cell and type the applicable token. For incoming calls, format precedence determines the priority for selecting which numbering format to use as the destination number for telecommunications auditing and Policy enforcement if similar data values are present in the signaling string.

    If DID/DNIS lines are used, the **Format Precedence** must specify DID/DNIS to enable the Dialing Plan to correctly convert the extensions for Policy enforcement and the DID section of the Dialing Plan must be correctly configured.

    The table below lists valid Format Precedence tokens.

Token	Meaning
ADDR	Destination number (address)
DID	Direct Inward Dialing
DNIS	Dialed Number Identification Service

- To set the same format precedence for an adjoining group of channels, click the first **Format Precedence** cell, hold down

SHIFT, click the last cell, and then type the string. Press ENTER to populate the selected cells.

13. (*SS7 Bearer Spans only*) Each channel on an ISUP bearer trunk has an associated Circuit Identification Code (CIC), ranging from 0 to 16383, and is unique for each LPC/RPC pair.

    - In the **CIC** field, type 0 for the first channel.
        - Alternately, you can right click in the **CIC** field, and then select **Increment Down** to automatically number the CICs for the other channels incrementally.
        - If you are configuring fully associated SS7 Signaling Links on a Bearer Span, **Increment Down** skips the signaling channels.

14. (*Digital Spans only*) The **Companding** column specifies for each channel whether to use A-Law or Mu-Law media formats. This enables you to set the Span to match the companding format in use in your locale, if needed. By default, all channels on E1 Spans are set to A-Law companding, while all channels on T1 Spans are set to Mu-Law.

    To change the setting:

    - For a single channel, click in the **Companding** field for that channel, and then click the down arrow and select the option.
    - For multiple adjacent channels, click in the first **Companding** field, hold down SHIFT, and then click in the last **Companding** field, click the down arrow in that field, and select the option.

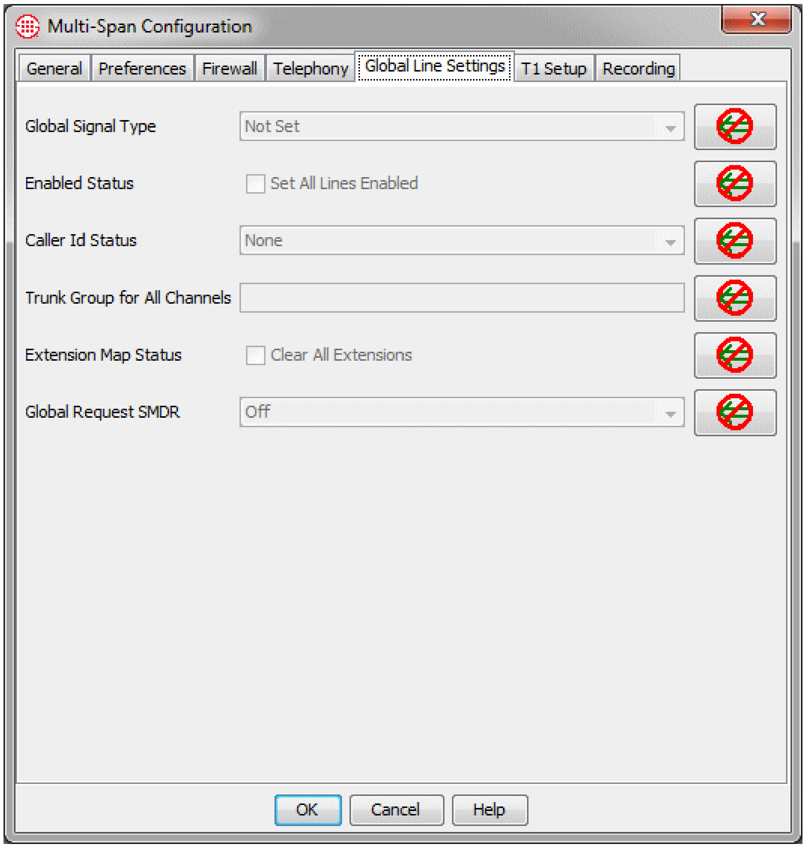
Global Line Settings Tab

The **Global Line Settings** tab is available only on the **Multi-Span Configuration** dialog box. The **Global Line Settings** tab allows you to configure some of the **Channel Map** tab settings for a group of selected Spans at the same time.

Format Precedence, Outgoing Numbering Format, Incoming Numbering Format, and Tone Type must be set per Span; they cannot be set globally.

To configure Global Line Settings

1. In the **Multi-Span Configuration** dialog box, click the **Global Line Settings** tab.
2. For each setting you want to be the same for all selected Spans, click the 🚫 icon to enable the field to be edited.



Global Signal Type: Not Set

Enabled Status: □ Set All Lines Enabled

Caller Id Status: None

Trunk Group for All Channels:

Extension Map Status: □ Clear All Extensions

Global Request SMDR: Off

3. Do any of the following, as appropriate to the selected Spans:

   - In the **Global Signal Type** box, click the down arrow to set the signal type for all selected Spans.

   - In the **Enabled Status** area, select **Set All Lines Enabled** to enable all channels on all selected Spans.

   - In the **Caller ID Status** area, click the down arrow to select the same Caller ID option for on all channels on all selected Spans. Available options are: **None**, **Bellcore** (US, Canada, South Korea), **UK BT** (British Telecom users in the UK), **ETSI** (UK, Germany, Italy), **NTT** (Japan), and **DTMF** (UK).

   - In the **Trunk Group For All Channels** box, type a Trunk Group name to apply to all channels on all selected Spans.

   - In the **Extension Map Status** area, select the **Clear All Extensions** box to clear all extensions from the **Extension** column of the **Channel Map** tab on all channels on all selected Spans.

   - In the **Global Request SMDR** area, click the down arrow to select the same outbound SMDR option (**Off**, **On**, **Replace**,

Augment) for all channels on all selected Spans. (See "Channel Map Tab" on page 93 for a description of each option.)

Continue with one of the following:

- Complete Span-type specific configuration for the types of Spans you are installing:
  - “E1-Specific Span Settings” on page 101.
  - “T1-Specific Span Settings” on page 104.
  - “PRI-Specific Span Settings” on page 107.
  - “SIP-Specific Span Settings” on page 110.
  - “UTA-Specific Span Settings” on page 115.
  - “SS7 Signaling Link-Specific Span Settings” on page 119.
  - More Spans of the same type: “Importing Span Configuration” on page 122.
- If all Span settings have been supplied, continue with “Installing Dialing Plans” on page 123.

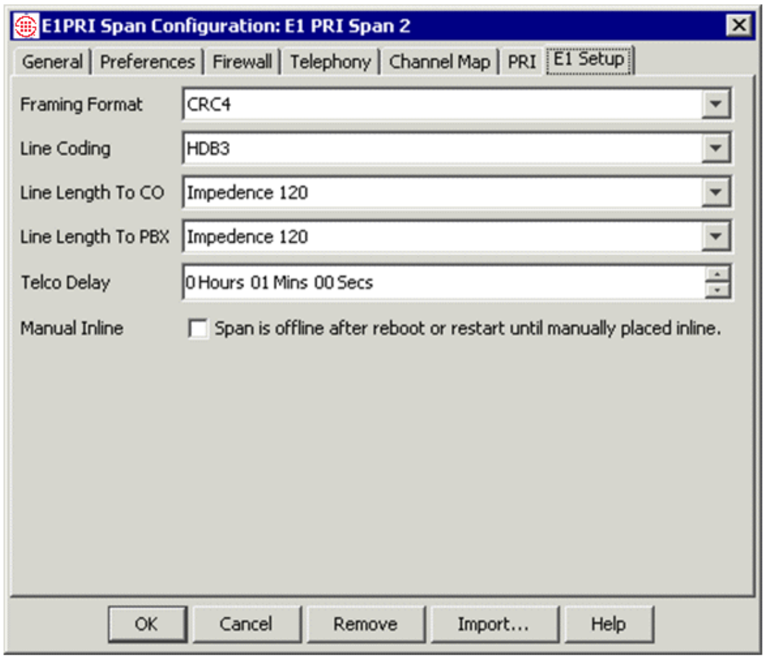
E1-Specific Span Settings

E1-specific Span settings apply to both E1 CAS and E1 PRI Spans.

IMPORTANT All Spans on a Card must use the same clock source. Segregate Spans with different clock sources onto different Cards.

To configure E1 settings

1. In the **E1 PRI Span Configuration** dialog box, click the **E1 Setup** tab.



Framing Format: CRC4

Line Coding: HDB3

Line Length To CO: Impedence 120

Line Length To PBX: Impedence 120

Telco Delay: 0 Hours 01 Mins 00 Secs

Manual Inline: □ Span is offline after reboot or restart until manually placed inline.

2. In the **Framing Format** box, click the down arrow and select one of the following to match the setting at your PBX:

   Basic—Basic/standard frame

   CRC4—Multiframe with Cyclic Redundancy Check 4

   Non-CRC4—Multiframe with no cyclic redundancy check

3. In the **Line Coding** box, click the down arrow and select one of the following to match the settings at your PBX:

   HDB3—High Density Bipolar 3

   AMI—Alternate Mark Inversion

4. In the **Line Length to CO** box, no configuration is necessary; it is set by default to **Impedence 120**.

5. In the **Line Length to PBX** box, no configuration is necessary; it is set by default to **Impedence 120**.

For information about assigning Tracks to System Events, see "System Events" in the *ETM® System Administration Guide*.

6. In the **Telco Delay** box, type or select the time (hours, minutes, and seconds) before notification that the trunk is down is sent to the **Diagnostic Log** (at which time any specified System Event Tracks are executed, such as email alerts). The default is 1 minute.

7. The **Manual Inline** check box controls whether the Span automatically goes inline after it is rebooted or restarted.

   - Select the check box to cause the Span to come up offline whenever it is rebooted or restarted. To place the Span inline after a reboot or restart, execute the ETM Command `SPAN INLINE` from the **ASCII Management Interface**.

- Clear the check box if the Span is to automatically go inline after it is rebooted or restarted.

8. Do one of the following:

    - If you are configuring E1 PRI Spans, continue with “PRI-Specific Span Settings” on page 107.
    - E1 CAS Span configuration is complete. Click **OK** to save the settings and close the dialog box. A message appears asking if you want to download the settings to the Span. Click **Yes**.

Continue with one of the following:

- Complete Span-type specific configuration for the types of Spans you are installing:
    - “T1-Specific Span Settings” on page 104.
    - “PRI-Specific Span Settings” on page 107.
    - “SIP-Specific Span Settings” on page 110.
    - “UTA-Specific Span Settings” on page 115.
    - “SS7 Signaling Link-Specific Span Settings” on page 119.
    - More Spans of the same type: “Importing Span Configuration” on page 122.
- If all Span settings have been supplied, continue with “Installing Dialing Plans” on page 123.

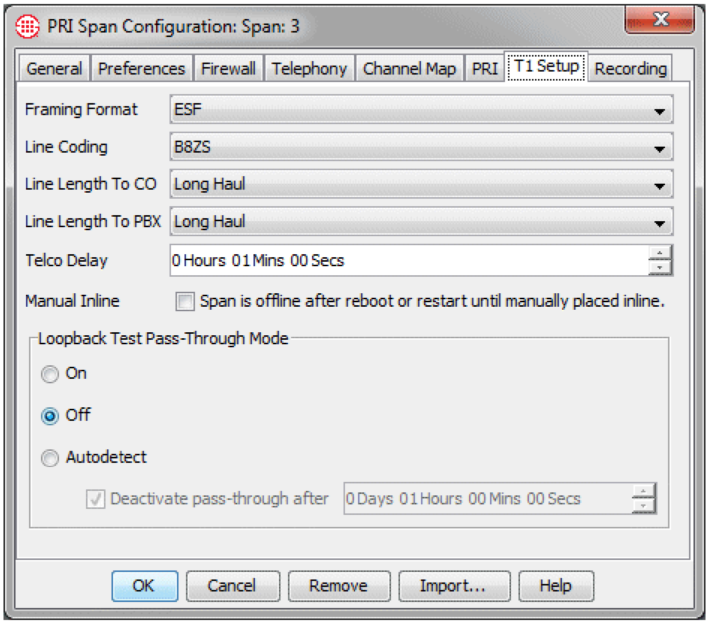
T1-Specific Span Settings

T1-specific Span settings apply to T1 PRI, T1 CAS, T1 SS7 bearer, and T1 SS7 signaling link Spans.

IMPORTANT All Spans on a Card must use the same clock source. Segregate Spans with different clock sources onto different Cards.

To configure T1 settings

1. On the **T1 Span Configuration** dialog box, click the **T1 Setup** tab.



Framing Format: ESF

Line Coding: B8ZS

Line Length To CO: Long Haul

Line Length To PBX: Long Haul

Telco Delay: 0 Hours 01 Mins 00 Secs

Manual Inline: □ Span is offline after reboot or restart until manually placed inline.

Loopback Test Pass-Through Mode

○ On

● Off

○ Autodetect

☑ Deactivate pass-through after 0 Days 01 Hours 00 Mins 00 Secs

2. In the **Framing Format** box, click the down arrow and select the correct option to match the Span. Framing Format must be set to the carrier's setting to ensure proper signal synchronization.

   SF—Super Frame

   ESF—Extended Super Frame

3. In the **Line Coding** box, click the down arrow and select the correct option to match the Span:

   AMI—Alternate Mark Inversion

   B8ZS—Bipolar 8 Zero Substitution

4. **Line length to CO** specifies the distance from the Appliance to the first piece of telephone network equipment. This setting must correspond to the settings at the telephone network and may not necessarily match the actual distance. Click the down arrow and select the option that matches the setting at the telephone network.

5. **Line length to PBX** specifies the distance from the Appliance to the PBX. This setting must correspond to the settings at the telephone network and may not necessarily match the actual distance.

   - In the **Line Length to PBX** box, click the down arrow and select the option that matches the setting at the telephone network.

For information about assigning Tracks to System Events, see "System Events" in the *ETM[®] System Administration Guide*.

6. In the **Telco Delay** box, type or select the time (hours, minutes, and seconds) before notification that the trunk is down is sent to the **Diagnostic Log** (at which time any specified System Event Tracks are executed, such as email alerts). The default is 1 minute.

7. The **Manual Inline** check box controls whether the Span automatically goes inline after it is rebooted or restarted.

   - Select the check box to cause the Span to come up offline whenever it is rebooted or restarted. To place the Span inline after a reboot or restart, execute the ETM Command `SPAN INLINE` from the **ASCII Management Interface**.

   - Clear the check box if the Span is to automatically go inline after a reboot or restart.

You can also turn pass-through mode on and off via ETM Commands. T1 LOOPBACK MODE ON places the Span into pass-through mode; T1 LOOPBACK MODE OFF takes the Span out of pass-through mode.

8. The ETM System supports user-enabled Pass-Through based on received Inband Line and ESF Data Link Loop-Up/Loop-Down codes. The Span activates/deactivates Pass-Through within 5 seconds of detecting the Loop-Up/Loop-Down codes. On T1 CAS Spans, place the Span offline before setting pass-through mode to **On**. For normal operation, use **Off** or **Autodetect**. Note that when auto-detect is used on T1 CAS lines, ghost calls or other errors may occur on either side of the test.

   a. In the **Loopback Test Pass-Through Mode** area, select one of the following:

      - **Off**—(Default) The telephony data is transmitted through the Span parsed and monitored and Policy is enforced.

      - **Autodetect**—When a Loop-Up code is detected, the Span activates Pass-Through. When a Loop-Down code is detected, the Span deactivates Pass-Through. When **Autodetect** is selected, you can also specify a timeout value from 0 seconds up to 1 day. (1 hour is the default; 0 indicates never timeout.)

      Only set the Loopback Test Pass-Through mode to On when you are planning to begin a test, not for normal operation. When Loopback Test Pass-Through Mode is on, no Policy enforcement or call monitoring occurs, D-channel re-establishment and error count threshold checking/logging is disabled, and on T1 CAS lines, call traffic may be impaired. An error count value of 0 is sent to the Management Server.

b. The **Deactivate pass-through after** box is available only if **Autodetect** is selected. If the **Deactivate pass-through after** box is selected, specify the time (days, hours, minutes, and seconds) to turn off Loopback Test Pass-Through Mode if the Loop-Down code is not detected. The default is 1 hour.

9. Do one of the following:

   - If you are configuring PRI Spans, continue with "PRI-Specific Span Settings" on page 107.
   - If you are configuring SS7 signaling links, continue with "SS7 Signaling Link-Specific Span Settings" on page 119.
   - If you are configuring T1 CAS or SS7 bearer Spans, Span configuration is complete. Click **OK** to save the settings and close the dialog box. A message appears asking if you want to download the settings to the Span. Click **Yes**.

Continue with one of the following:

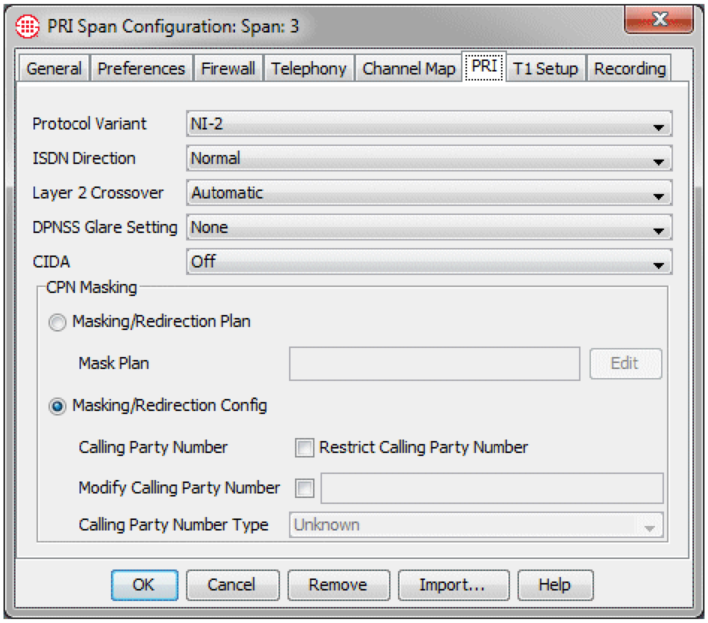
- Complete Span-type specific configuration for the types of Spans you are installing:
  - "PRI-Specific Span Settings" on page 107.
  - "SS7 Signaling Link-Specific Span Settings" on page 119.
  - "SIP-Specific Span Settings" on page 110.
  - "UTA-Specific Span Settings" on page 115.
  - More Spans of the same type: "Importing Span Configuration" on page 122.
- If all Span settings have been supplied, continue with "Installing Dialing Plans" on page 123.

PRI-specific settings apply to both T1 PRI and E1 PRI Spans.

PRI-Specific Span Settings

To configure PRI-specific settings

1. In the **Span Configuration** dialog box, click the **PRI** tab.



PRI Span Configuration: Span: 3

Protocol Variant: NI-2

ISDN Direction: Normal

Layer 2 Crossover: Automatic

DPNSS Glare Setting: None

CIDA: Off

CPN Masking

○ Masking/Redirection Plan

Mask Plan

● Masking/Redirection Config

Calling Party Number □ Restrict Calling Party Number

Modify Calling Party Number □

Calling Party Number Type: Unknown

2. In the **Protocol Variant** box, click the down arrow, and then click the applicable variant type.

   - The following protocol variants are supported on E1:
     - EuroISDN
     - DASS2
     - DPNSS (If you select DPNSS, select the applicable glare setting in the **DPNSS Glare Setting** box.)
     - QSIG (Use the **ISDN Direction** box to indicate whether the PBX on this side of the link is the Master or the Slave.)
   - The following protocol variants are supported on T1:
     - NI-2
     - 4ESS
     - 5ESS
     - DMS100

3. *(Not applicable for DASS2 or DPNSS; leave the default.)* In the **ISDN Direction** box, click the down arrow, and then specify the user/network relationship for ISDN messages: **Normal** or **Reverse**.

- **Normal** is usually used when the ETM Appliance is installed between the telephone network and the PBX. In typical non-tie-trunk installations, Appliances are installed close to the PBX that acts as the User side of the trunk. This is the most common configuration.
- When ETM Spans are installed on a tie trunk between two PBXs, a Span installed with respect to the PBX acting as the Network side must be set to **Reverse**, while a Span installed with respect to the PBX acting as the User side must be set to **Normal** for the D-Channel to function properly. For tie trunks using QSIG, select **Normal** if the local PBX (the one connected to the PBX port of the Span) functions as the QSIG Slave; select **Reverse** if the local PBX functions as the QSIG Master.

4. The **Layer 2 Crossover** setting is used for debugging PRI issues to allow logical insertion/isolation from layer 2 and 3 on PRI Spans. Only change this setting if instructed to do so by SecureLogix Support personnel. To change the value, in the **Layer 2 Crossover** box, click the down arrow and select an option. Valid values are **ON**, **OFF**, and **AUTOMATIC**. (**AUTOMATIC** is not supported for DASS2 protocol variant.)

5. The **DPNSS Glare Setting** applies only if you selected DPNSS as the protocol variant. If you selected any other protocol variant, leave the default of **None** selected. If you selected DPNSS as the protocol variant, select one of the following:

   - **PBX X** if the local PBX (the one to which the PBX port of the Span is connected) is in control when glare occurs.
   - **PBX Y** if the local PBX is not in control when glare occurs.

6. The **CPN Masking** area is used to prevent the actual Calling Party Number (CPN) from being transmitted to the CO and to redirect calls. The ability of the Span to enforce Policy is enhanced when it receives calling party numbers from the PBX. These options enable you to instruct the Span to remove or replace the calling party number so that it is not sent to the telephone network, or you can mask all calls on the Span. Select one of the following:

For instructions for defining extension masking plans, see "Extension Masking/Call Redirection" in the *ETM® System Administration and Maintenance Guide*.

   – **Masking Plan**—Extension masking plans enable you to mask calling extensions and redirect calls on PRI lines, based on call criteria such as source, destination, and direction. If a masking plan is to be used, select this option and then click **Edit** to open the **Masking Plans** dialog box in which you define/edit/select the Masking Plan you want to use.

   – **Masking Config**—Select if you want to mask the source number only on all outgoing calls on the Span. Do the following to replace the actual Calling Party Number with a substitute digit string:

a. Select the **Restrict Calling Party Number** check box, and then type the substitute number in the **Modify Calling Party Number** box. You can also leave the text box blank, if desired, to transmit a null value.

b. In the **Calling Party Number Type** box, click the down arrow, and then select the TON for the number you specified in the **Modify Calling Party Number** box: **National**, **International**, **Subscriber**, or **Unknown**.

7. PRI Span configuration is complete. Click **OK** to save the settings and close the dialog box. A message appears asking whether you want to download the settings to the Span.

8. Click **Yes**.

Continue with one of the following:

- Complete Span-type specific configuration for other types of Spans you are installing:
  - “SS7 Signaling Link-Specific Span Settings” on page 119.
  - More Spans of the same type: “Importing Span Configuration” on page 122.
  - “SIP-Specific Span Settings” on page 110.
  - “UTA-Specific Span Settings” on page 115.
- If all Span settings have been supplied, continue with “Installing Dialing Plans” on page 123.

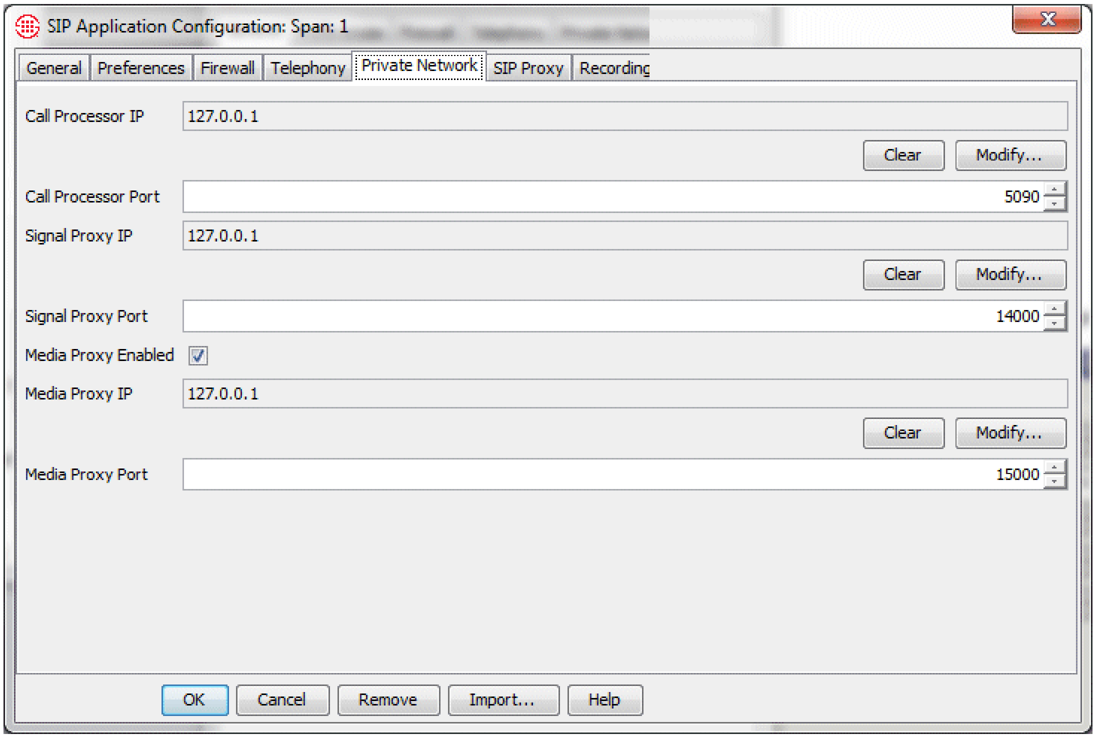
SIP-Specific Span Settings

To complete SIP Application-specific settings

Configure the settings on each of the tabs described below.

Private Network Tab

The **Private Network** tab is used to specify the IP address and port of the Call Processor, Signaling Proxy, and Media Proxy components of this SIP Appliance.



Call Processor IP 127.0.0.1

Call Processor Port 5090

Signal Proxy IP 127.0.0.1

Signal Proxy Port 14000

Media Proxy Enabled ☑

Media Proxy IP 127.0.0.1

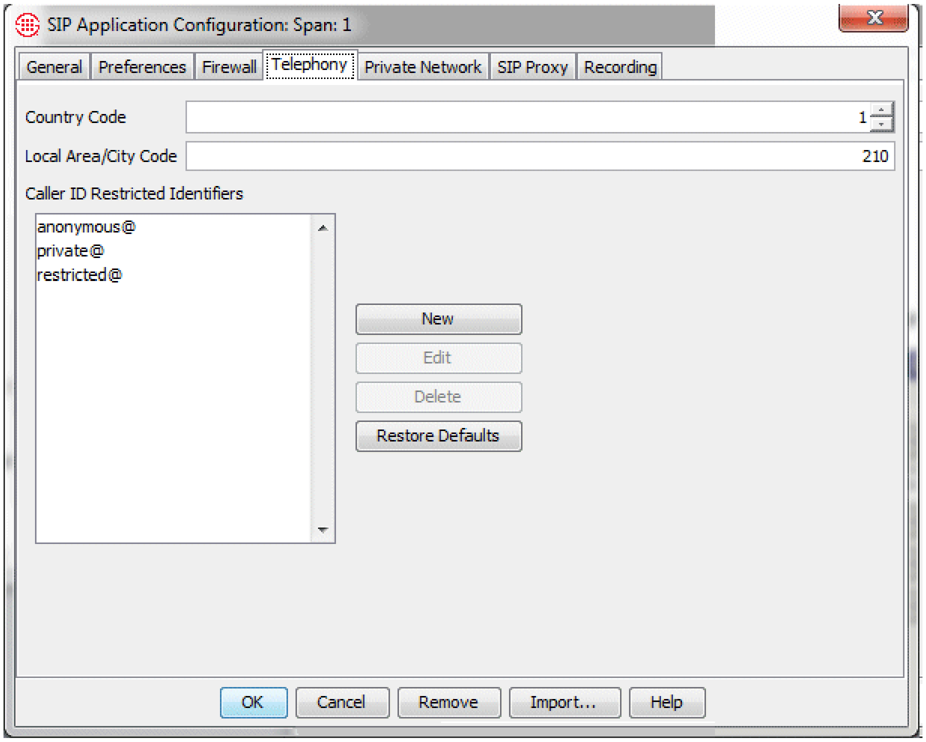
Media Proxy Port 15000

- **Call Processor IP**--Click **Modify** and then type the new IP address.
- **Call Processor Port**--Specifies the port on which the Management Server communicates with the Call Processor.
- **Signal Proxy IP**--Click **Modify** and type the IP address of the Signaling Proxy.
- **Signal Proxy Port**-Specifies the port on which the Call Processor communicates with the Signaling Proxy.
- **Media Proxy Enabled**--Select this check box if media processing is used on this Appliance.
- **Media Proxy IP**--Click **Modify** and type the IP address of the Media Proxy associated with this Appliance.

- **Media Proxy Port**--Specifies the port on which the Call Processor communicates with the Media Proxy.

Telephony Tab

The **Telephony** tab is used to specify the country code and area code for the locale where the Appliance is installed and to define caller ID restricted identifiers.



SIP Application Configuration: Span: 1

Country Code: 1

Local Area/City Code: 210

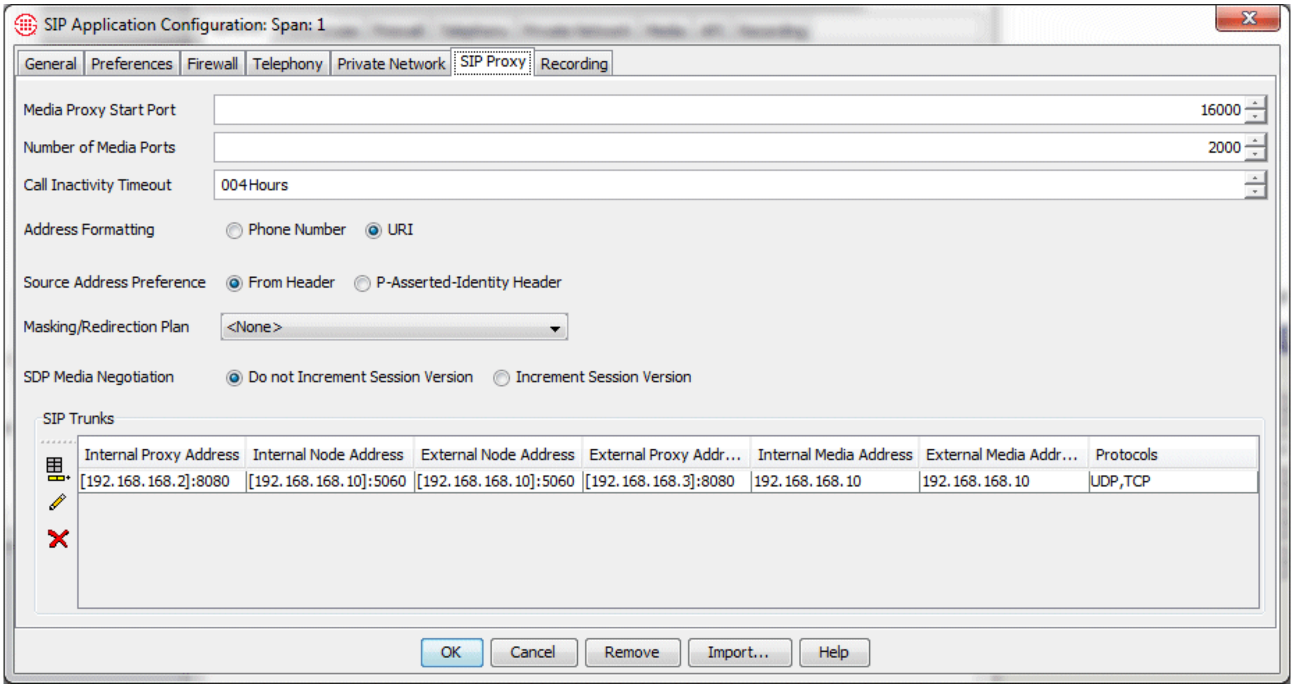
Caller ID Restricted Identifiers

anonymous@
private@
restricted@

- **Country Code**--Type the Country Code for the Appliance locale.
- **Local Area/City Code**--Type the area/city code for the Appliance locale.
- **Caller ID Restricted Identifiers**—For each Caller ID Restricted Identifier, click **New**, type the string, and then click **OK**.

SIP Proxy Tab

The **SIP Proxy** tab is used to identify the SIP trunks monitored by this Appliance.



Media Proxy Start Port: 16000

Number of Media Ports: 2000

Call Inactivity Timeout: 004Hours

Address Formatting: ○ Phone Number ● URI

Source Address Preference: ● From Header ○ P-Asserted-Identity Header

Masking/Redirection Plan: <None>

SDP Media Negotiation: ● Do not Increment Session Version ○ Increment Session Version

SIP Trunks

Internal Proxy Address	Internal Node Address	External Node Address	External Proxy Addr...	Internal Media Address	External Media Addr...	Protocols
[192.168.168.2]:8080	[192.168.168.10]:5060	[192.168.168.10]:5060	[192.168.168.3]:8080	192.168.168.10	192.168.168.10	UDP,TCP

- **Media Proxy Start Port**--(*Only if Media Proxy is enabled on the **Private Network** tab.*)The start port for communicating with the Media Proxy.

- **Number of Media Ports**--The number of ports reserved for media, beginning at the start port.

- **Call Inactivity Timeout**--The length of time before a call with no media is disconnected.

- **Address Formatting: Phone Number** or **URI**--Select whether to log URI information as URIs or as formatted Phone Numbers, when the user part of a URI can be formatted as a Phone Number.

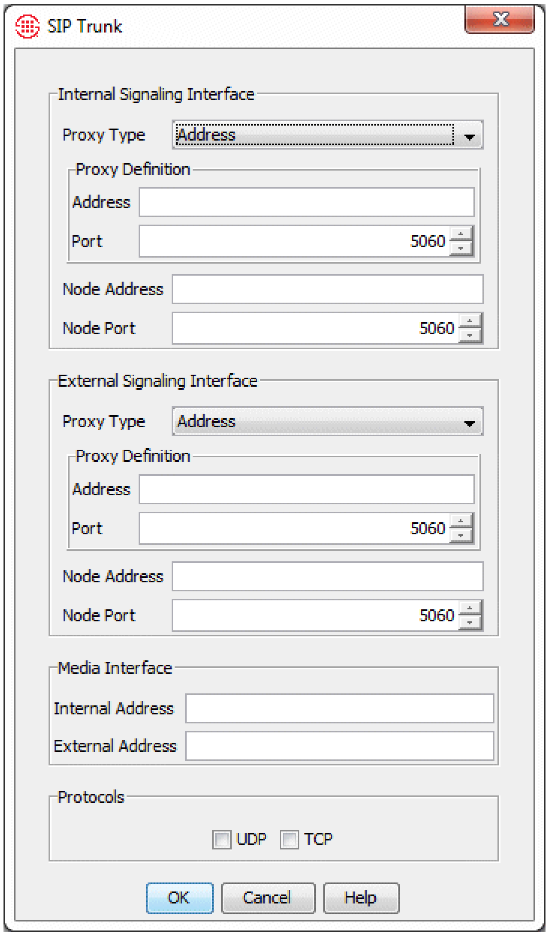
See the *ETM® System Administration Guide* for instructions for defining Masking/Redirection Plans.

- **Source Address Preference: From Header** or **P-Asserted-Identity Header**—Select which is to be preferred when both are present.

- **Masking/Redirection Plan**—Click the down arrow and select the SIP Masking/Redirection Plan this Span is to use.

- **SIP Media Renegotiation**—If the ETM SIP Proxy is installed between Cisco Unified Communications Manager (CallManager) and Cisco CUBE, select **Increment Session Version**. The default is **Do Not Increment Session Version**.

- **SIP Trunks area**—Used to identify the logical SIP trunks monitored by this Appliance. Each Appliance supports up to 4 SIP Trunks. To add a new logical SIP trunk, click the **Add Trunk** icon. The **SIP Trunk** dialog box appears.



SIP Trunk

Internal Signaling Interface

Proxy Type: Address

Proxy Definition

Address:

Port: 5060

Node Address:

Node Port: 5060

External Signaling Interface

Proxy Type: Address

Proxy Definition

Address:

Port: 5060

Node Address:

Node Port: 5060

Media Interface

Internal Address:

External Address:

Protocols

☐ UDP ☐ TCP

To identify a logical SIP trunk, provide the following information:

- **Internal Signaling Interface area**:—Information about the internal proxy (CPE) with which the Appliance will interface:
  - **Proxy Type: Address**, **Domain**, or **SRV Domain**
  - **Proxy Definition** (fields depend on **Proxy Type** selection): **Address** and **Port**, **Domain** and **Port**, or **SRV Domain**.
  - **Node Address and Port**--The internal (CPE side) IP address and port of the Call Processor.
- **External Signaling Interface area**—Information about the external proxy (CO) with which the Appliance will interface:
  - **Proxy Type: Address**, **Domain**, or **SRV Domain.**
  - **Proxy Definition** (fields depend on Proxy Type selection): **Address** and **Port**, **Domain** and **Port**, or **SRV Domain**.

  - **Node Address and Port**--The external (CO side) IP address and port of the SIP Signaling Proxy.

- **Media Interface area:**
  - **Internal Address**--The internal (CPE) side IP address of the media proxy Appliance component.
  - **External Address**--The external (CO) side media proxy IP address.

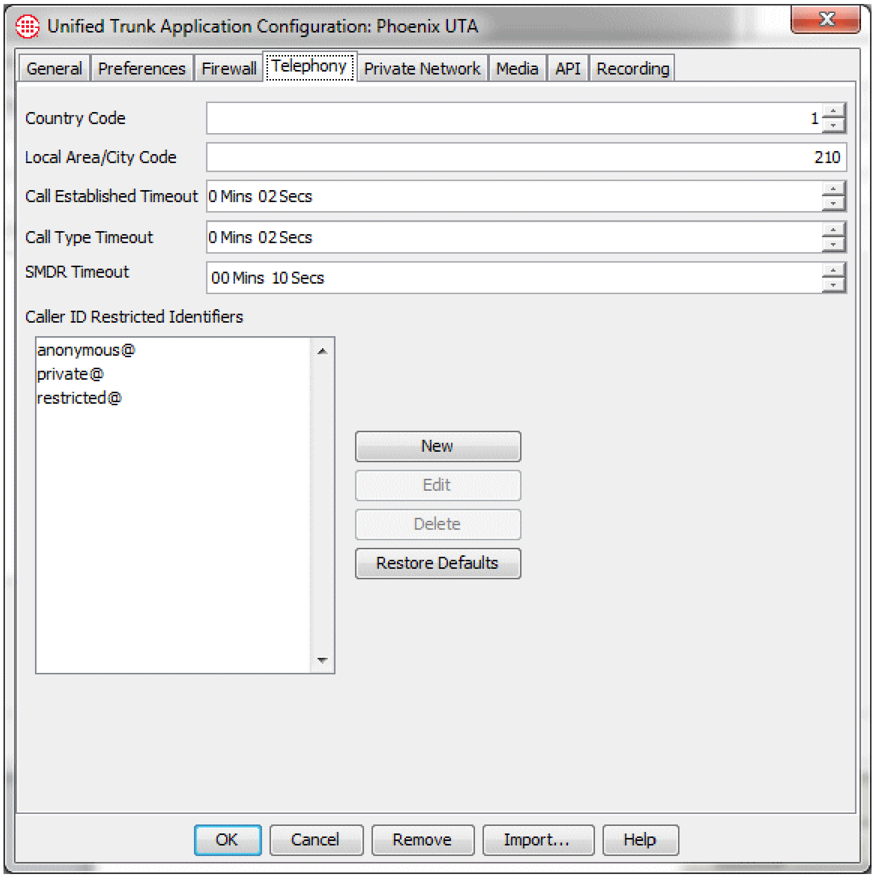
- **Protocols Area:**
  - Specify allowed protocol(s): **UDP** and/or **TCP**.

UTA-Specific Span Settings

Complete UTA Span GUI configuration by configuring the settings on each of the tabs described below.

Telephony Tab

The **Telephony** tab is used to specify the country code and area code for the locale where the Appliance is installed and to define caller ID restricted identifiers.



Country Code 1

Local Area/City Code 210

Call Established Timeout 0 Mins 02 Secs

Call Type Timeout 0 Mins 02 Secs

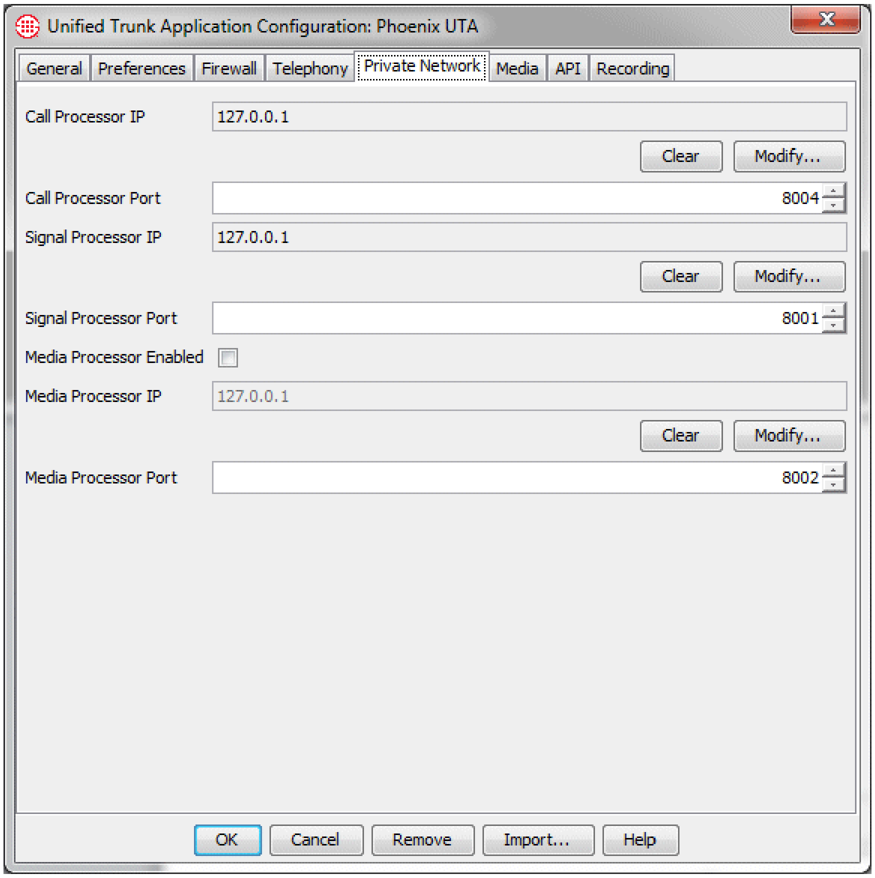
SMDR Timeout 00 Mins 10 Secs

Caller ID Restricted Identifiers

anonymous@
private@
restricted@

Private Network Tab

The **Private Network** tab is used to specify the IP address and port of the Call Processor, Signal Processor, and Media Processor components of this UTA Appliance.



Unified Trunk Application Configuration: Phoenix UTA

Call Processor IP 127.0.0.1

Call Processor Port 8004

Signal Processor IP 127.0.0.1

Signal Processor Port 8001

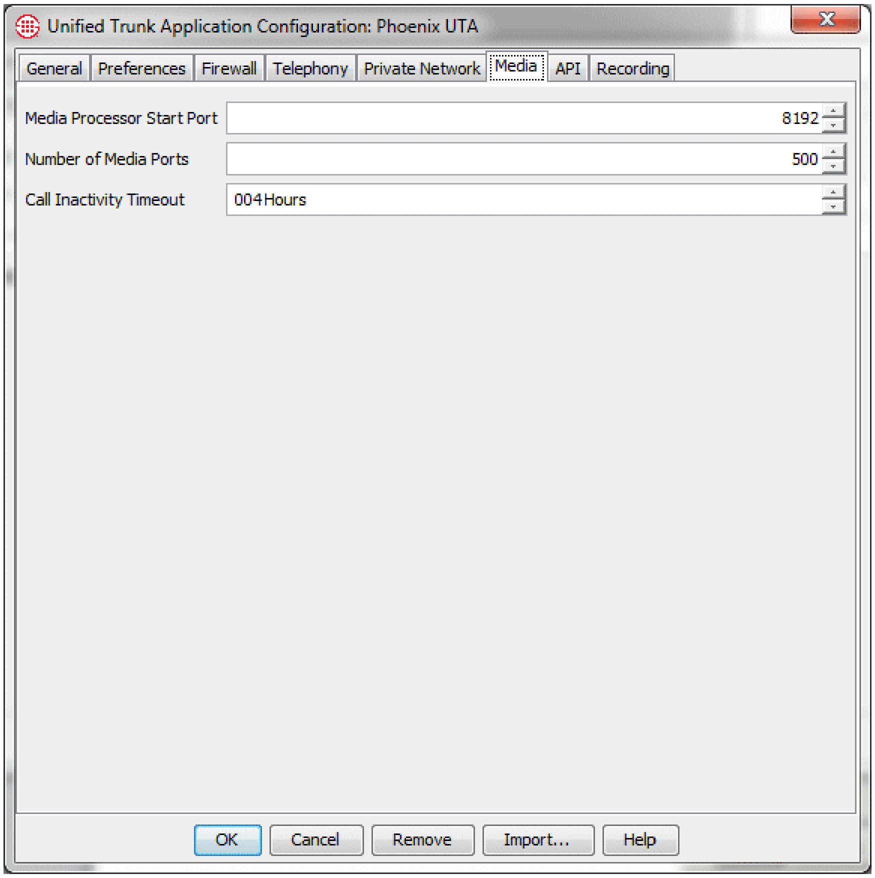
Media Processor Enabled □

Media Processor IP 127.0.0.1

Media Processor Port 8002

- **Call Processor IP**--Click **Modify** and then type the new IP address.
- **Call Processor Port**--Specifies the port on which the Management Server communicates with the Call Processor.
- **Signal Processor IP**--Click **Modify** and type the IP address of the Signal Processor.
- **Signal Processor Port**-Specifies the port on which the Call Processor communicates with the Signal Processor.
- **Media Processor Enabled**--Select this check box if media processing is used on this Appliance.
- **Media Processor IP**--Click **Modify** and type the IP address of the Media Proxy associated with this Appliance.
- **Media Processor Port**--Specifies the port on which the Call Processor communicates with the Media Processor.

Media Tab



Media Processor Start Port 8192

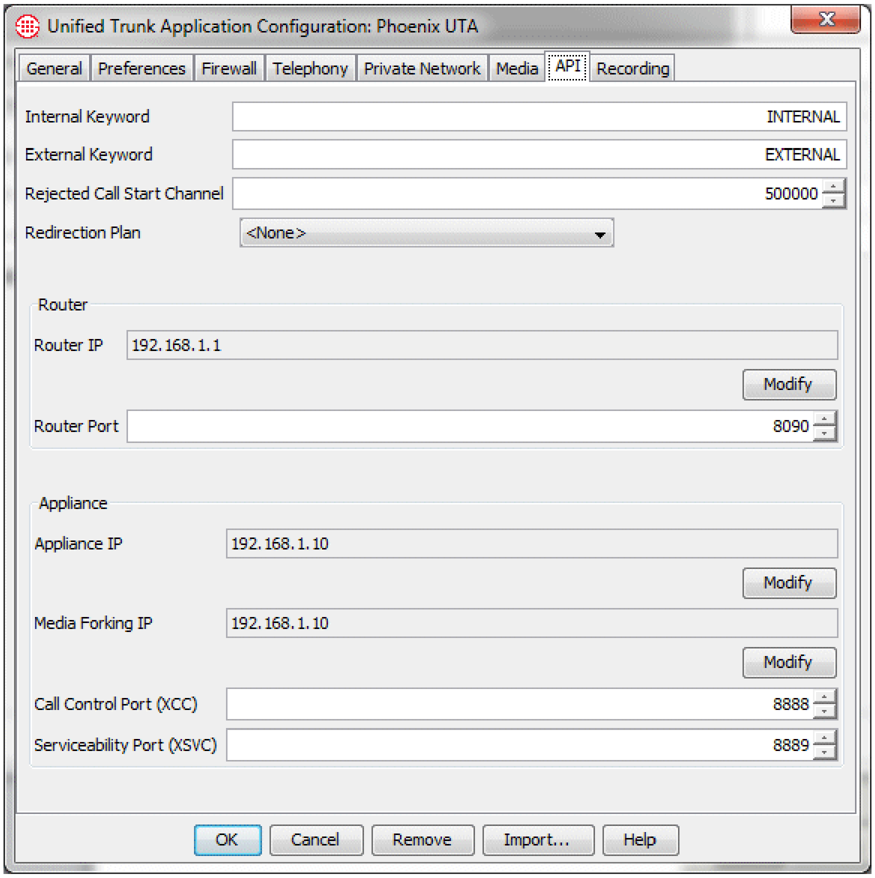
Number of Media Ports 500

Call Inactivity Timeout 004Hours

- **Media Processor Start Port**--(*Only if Media Processor is enabled on the* ***Private Network*** *tab*.)The start port for communicating with the Media Processor.
- **Number of Media Ports**--The number of ports reserved for media, beginning at the start port.
- **Call Inactivity Timeout**--The length of time before a call with no media is disconnected.

API Tab

Important: The values you specify on the **API** tab must match the configuration of the API on the router.



Unified Trunk Application Configuration: Phoenix UTA

Internal Keyword: INTERNAL

External Keyword: EXTERNAL

Rejected Call Start Channel: 500000

Redirection Plan: <None>

Router

Router IP: 192.168.1.1 Modify

Router Port: 8090

Appliance

Appliance IP: 192.168.1.10 Modify

Media Forking IP: 192.168.1.10 Modify

Call Control Port (XCC): 8888

Serviceability Port (XSVC): 8889

- **Internal Keyword** and **External Keyword** —The keywords defined for determining call direction.
- **Rejected Call Start Channel**— The start channel for Reject Terminated calls.
- **Redirection Plan**—Click the down arrow and select the UTA Redirection Plan this Span is to use, if any. See the *ETM$^{®}$ System Administration and Maintenance Guide* for instructions for defining Redirection Plans.
- **Router area**:
  - **Router IP**—The IP address of the router this UTA Appliance is interfacing with.
  - **Router Port**—The router port on which the Appliance interfaces with the router.
- **Appliance area**:
  - **Appliance IP**—The IP address assigned to the UTA Appliance.

- **Media Forking IP**—The UTA Appliance port to which the router is configured to fork media, if enabled.
- **Call Control Port (XCC)**— The port to which the provider/router/XCC is configured to point to the UTA Appliance IP: port .
- **Serviceability Port (XSVC**)— The port to which the status provider/router/XSVC is configured to point to the UTA Appliance IP: port.

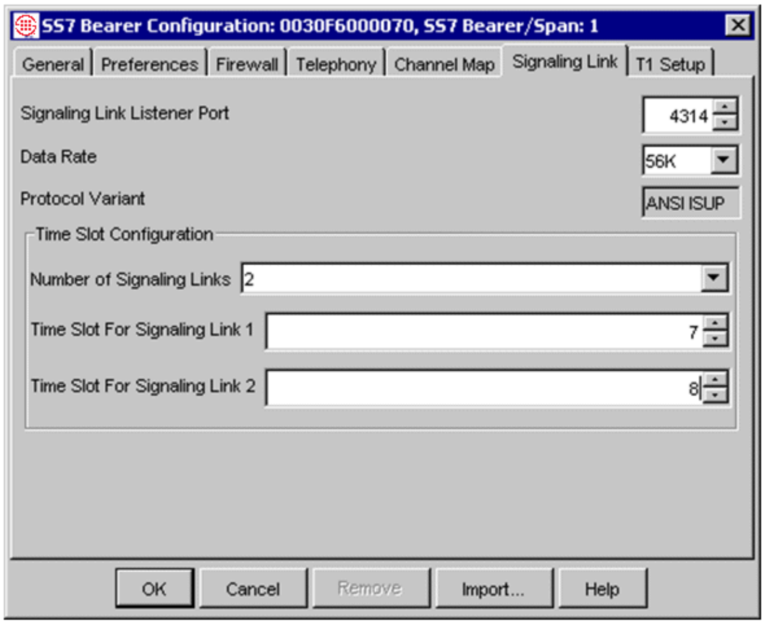
SS7 Signaling Link-Specific Span Settings

SS7 Bearer Spans can be configured to use either fully associated signaling links coresident with the Bearer Spans, or a dedicated SS7 Signaling Link Card. Use the applicable procedure below for your configuration.

Fully Associated Signaling Links

To configure fully associated signaling links:

1. On the **SS7 Bearer Configuration** dialog box, click the **Signaling Link** tab.



SS7 Bearer Configuration: 0030F6000070, SS7 Bearer/Span: 1

Signaling Link Listener Port: 4314

Data Rate: 56K

Protocol Variant: ANSI ISUP

Time Slot Configuration

Number of Signaling Links: 2

Time Slot For Signaling Link 1: 7

Time Slot For Signaling Link 2: 8

2. The **Signaling Link Listener Port** is automatically assigned during out-of-box configuration, by Span number as follows:
   - Span 1: Port 4314
   - Span 2: Port 4315
   - Span 3: Port 4316

- Span 4: Port 4317

To change the port number, in the **Signaling Link Listener Port** box, type or select the port for these signaling links.

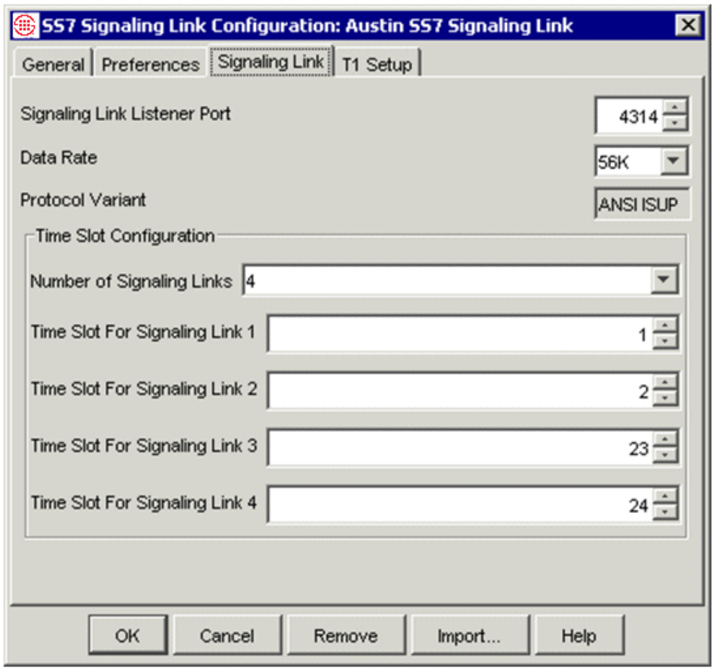
IMPORTANT Each Span on a Card must have a unique Signaling Link Listener Port. If duplicate port assignments are used, port conflicts occur. The following Diagnostic Log message indicates a Signaling Link port conflict: "Unable to bind APP SS7 server to port *n*."

3. In the **Data Rate** box, click the value that defines the data rate of the Signaling Links. Allowed values are 56K/s and 64K/s.
4. The **Protocol Variant** defines the format of SS7 messaging. Options are ANSI ISUP and ETSI ISUP.
5. Up to two SS7 Signaling Links can be defined for each Bearer Span. In the **Number of Signaling Links** box, type or select the number of Signaling Links.
6. **Time Slot Configuration** defines the timeslots associated with each link. Each timeslot correlates to a channel; allowed values are 1-24 on T1 and 1-30 on E1. In each of the **Time Slot For Link #*n*** boxes, type or select the time slot associated with the Signaling Link data channel.
7. Fully associated SS7 signaling link configuration is complete. Click **OK** to save the settings and close the dialog box. A message appears asking whether you want to download the settings to the Span.
8. Click **Yes**.

Dedicated SS7 Signaling Link Cards

If you have dedicated Signaling Link Cards

1. In the **SS7 Signaling Link Configuration** dialog box, click the **Signaling Link** tab.



SS7 Signaling Link Configuration: Austin SS7 Signaling Link

Signaling Link Listener Port: 4314

Data Rate: 56K

Protocol Variant: ANSI ISUP

Time Slot Configuration

Number of Signaling Links: 4

Time Slot For Signaling Link 1: 1

Time Slot For Signaling Link 2: 2

Time Slot For Signaling Link 3: 23

Time Slot For Signaling Link 4: 24

2. In the **Signaling Link Listener Port** box, type or select the port used by this Signaling Link. This port is used by the SS7 Bearer Spans to create network connections to the Signaling Link Cards. Each Signaling Link Card defines its own port value.
3. In the **Data Rate** box, click the value that defines the data rate of the Signaling Links. Allowed values are 56K/s and 64K/s.
4. The **Protocol Variant** defines the format of SS7 messaging. Options are ANSI ISUP and ETSI ISUP.
5. Up to 4 SS7 Signaling Links can be defined for each Signaling Link Card. In the **Number of Signaling Links** box, type or select the number of Signaling Links.
6. **Time Slot Configuration** defines the timeslots associated with each link. Each timeslot correlates to a channel; allowed values are 1-24 on T1 and 1-30 on E1. In each of the **Time Slot For Link #*n*** boxes, type or select the time slot associated with the Signaling Link data channel.
7. Dedicated SS7 signaling link configuration is complete. Click **OK** to save the settings and close the dialog box. A message appears asking whether you want to download the settings to the Span.
8. Click **Yes**.

Continue with one of the following:

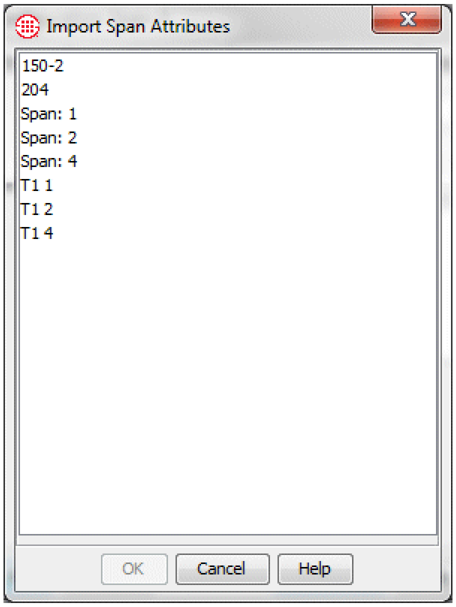
- See "Importing Span Configuration" below if you want to apply configuration settings of one Span to another Span of the same type. Otherwise, see the next bullet.
- Continue with "Installing Dialing Plans" on page 123.

Importing Span Configuration

After you have completed configuration for a Span, you can import its settings to apply to another Span of the same type. Settings can only be imported to a single Span at a time, not globally.

To import Span settings

1. In the **Platform Configuration** subtree, right-click the Span into which you want to import settings, and then click **Edit Span(s)**.
2. Click **Import**. The **Import Span Attributes** dialog box appears. Only Spans of the same type appear as import choices.



3. Click the Span whose attributes you want to apply to the selected Span, and then click **OK**. The **Configuration** dialog box is populated with the settings that you imported.
4. Click the **General** tab and assign a **Span ID** to the Span if you have not yet done so.
5. Click **OK** to accept the configuration.

For each Span you are configuring, continue with "Installing Dialing Plans" on page 123.

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 Numbering Plan (LNP) specific to the Appliance locale and a World Numbering Plan (WNP) specific to the country where the Appliance is located.

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.

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).

SS7 Signaling Links do not require a Dialing Plan.

See "About Dialing Plans" in the *ETM® System Technical Reference* for a detailed explanation of the components of each Dialing Plan file and instructions for modifying each section.

Defining Dialing Plans

To define a Dialing Plan

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

   <INSTALL_DIR>\ps\software_repository\ini\

   Define the appropriate sections according to your Appliance locale. See "About Dialing Plans" in the *ETM® System Technical Reference*, available from the **SecureLogix** directory on the **Start** menu (Windows systems) or the ETM System installation directory (all systems), 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.

   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 123 for instructions.

Installing Dialing Plans on a Span

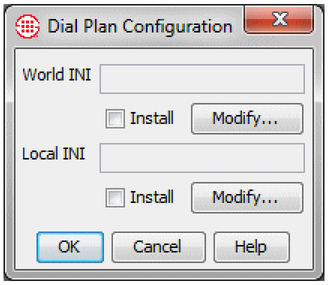
Each Span uses both an LNP and a WNP file.

To install the Dialing Plans on one or more Spans

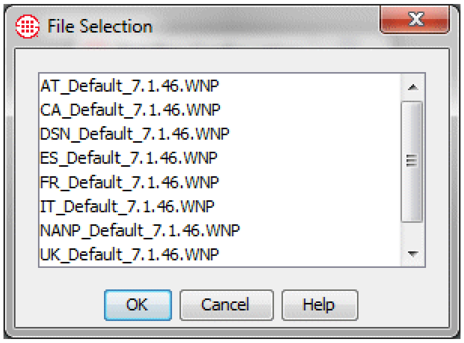
1. In the Performance Manager tree pane, do one of the following:

   - 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. Under the **World INI** box, click **Modify**. The **File Selection** dialog box appears. Only **.WNP** files in the **ps\software_repository\ini** directory in the ETM Server installation directory appear.



AT_Default_7.1.46.WNP
CA_Default_7.1.46.WNP
DSN_Default_7.1.46.WNP
ES_Default_7.1.46.WNP
FR_Default_7.1.46.WNP
IT_Default_7.1.46.WNP
NANP_Default_7.1.46.WNP
UK_Default_7.1.46.WNP

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

3. Click the **.WNP** file that represents the World Numbering Plan for this Appliance locale, and then click **OK**.

4. Under the **Local INI** box, click **Modify**. The **File Selection** dialog box appears. Only **.LNP** files in the **ps\software_repository\ini** directory in the ETM Server installation directory appear.

5. Click the **.LNP** file that represents the Local Numbering Plan for this Appliance locale, and then click **OK**.

6. 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 call processing.

Continue with one of the following:

- If SMDR, NFAS, SS7, or Call Recording are in use, continue with “Configuring Switches” on page 125. Otherwise, see the next bullet.
- Continue with "Performing Telephony Service Cutover" on page 149.

Configuring Switches

Switches are used to organize Spans according to the PBX to which they belong and to configure SMDR, NFAS, SS7 Groups, and Call Recording Protected Extensions. Switches are configured in the **Telco Configuration** subtree in the Performance Manager tree pane.

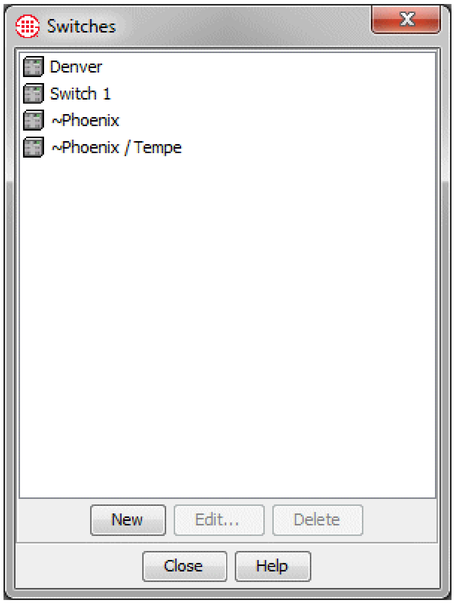
Configuration consists of the following sequence of steps:

1. Create a Switch to represent the PBX. The Switch contains the SMDR configuration fields and enables NFAS and SS7 Group definition.
2. Move all Spans that are to use the SMDR data, Access Codes, SMDR Extensions, NFAS, and/or SS7 groups to the Switch.
3. Do one or more of the following, depending on Span type:
   - Configure the Switch with SMDR settings specific to the PBX in use, including the associated Access Code Set and list of SMDR Extensions.
   - Define NFAS Groups.
   - Define SS7 Groups.

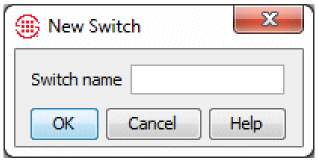
Creating a Switch

To create a Switch

1. Right-click the **Telco Configuration** subtree, and then click **Manage Switches**. The **Switches** dialog box appears.



2. Click **New**. The **New Switch** dialog box appears.



3. Type the name by which you want to identify this Switch and then click **OK**. For example, type: `Meridian`.
4. The Switch appears in the **Telco Configuration** subtree.
5. On the **Switches** dialog box, click **Close**.

Continue with "Moving a Span to a Switch" below.

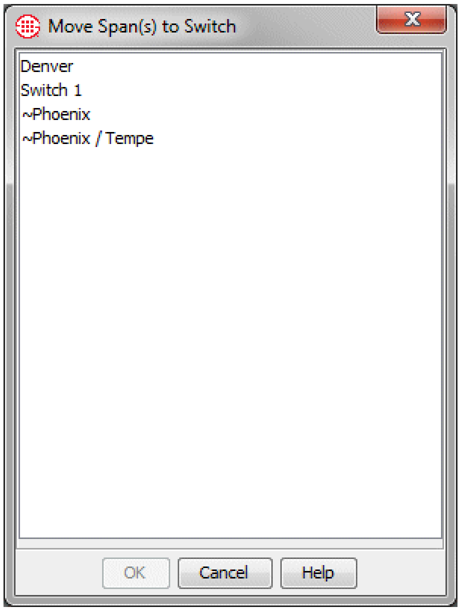
Moving a Span to a Switch

IMPORTANT To select the SMDR Provider, you must first move Span 1 of the SMDR Provider Card to the switch.

To move a Span to a Switch

1. In the **Telco Configuration** subtree, right-click the Span, point to **Move Spans**, and then click **To Switch**.
   - To move multiple Spans at once, hold down CTRL or SHIFT while selecting the Spans, and then right-click the selection.

   The **Move Span(s) to Switch** dialog box appears.



2. Click the Switch to which the Span is to be moved, and then click **OK**.

   The Span appears in the **Switch** node of the **Telco Configuration** subtree.

Continue with one of the following:

- If SMDR is used on this Switch, see "Configuring a Switch for SMDR" below. Otherwise, see the next bullet.
- If NFAS is used on this switch, see "Defining NFAS Groups" on page 135. Otherwise, see the next bullet.
- To configure SS7 Groups, see "Defining SS7 Groups" on page 138. Otherwise, see the next bullet.
- Continue with "Configuring Management Server Settings" on page 143.

Configuring a Switch for SMDR

SMDR can be used to extract call data from the call logs sent by the PBX. Several options for using SMDR data are available, depending on the type of circuits being monitored, whether outbound source numbers are present on the line, and whether Call Recording Protected Extensions are used, and whether you are using the Station-Side CDR reporting feature.

Outbound SMDR for Monitored Channels

Several SMDR options are available to obtain outbound source: When the outbound source data is not available on the line, you can set outbound SMDR use to **ON**, and it will be used for policy processing after the call ends. If the outbound source is available on the line, you can set SMDR use to **Augment**, to use the real-time data for policy processing and then augment the call record in the database with additional call information, such as access codes, when the call ends. Or you can use the real-time call information for policy processing but replace the data in the database with the SMDR data after the call ends, by using the **Replace** setting.

To use outbound SMDR for monitored calls, one of the Cards in one of the Appliances is physically connected to the SMDR port on the PBX during hardware installation. This Card, called the *SMDR Provider*, transmits the SMDR data from the Switch to the Server, where it is available to all of the Spans associated with the Switch.

Inbound SMDR for Call Recorder SMDR Extensions

(*Does not apply to UTA*) If you have purchased the Call Recorder application, inbound destination numbers can be extracted from SMDR for use with Call Recording SMDR Extension processing, using a separate **Inbound SMDR** setting. SMDR Extensions are internal phone numbers identified by inbound SMDR correlation for which you want to prescribe special Call Recorder treatment . For example, you can use SMDR Extensions to define a whitelist of extensions to which calls are never to be recorded, or a blacklist of extensions to which calls are always to be recorded. Recordings can also be marked as sensitive based on this list, for example, for HIPAA-protected calls. Unlike outbound SMDR, inbound SMDR is <u>not</u> used for Policy processing. Inbound SMDR is either **On** or **Off**.

Recording SMDR for Station-side CDR Reporting

If you are using the Station-side CDR feature, an Appliance Card can be configured to record raw SMDR for processing into the ETM Database for reporting. See “Station-Side CDR Importing for Reporting” in the *ETM® System Administration Guide* for details, including configuration instructions.

CDR Parse Files

The specific format of SMDR/CDR data differs widely between PBXs. To successfully correlate SMDR data with calls, the ETM Server requires an *SMDR parse file* specific to the SMDR format in use. SecureLogix Corporation has defined SMDR parse files for a number of formats. These files are located in the ETM Server installation directory at **<INSTALL_DIR>\ps\software_repository\smdr**. If the correct SMDR parse file for the format used is not available, see "Defining an SMDR Parse File" in the *ETM® System Technical Reference* for detailed instructions for defining a new file.

Extracting Access Codes

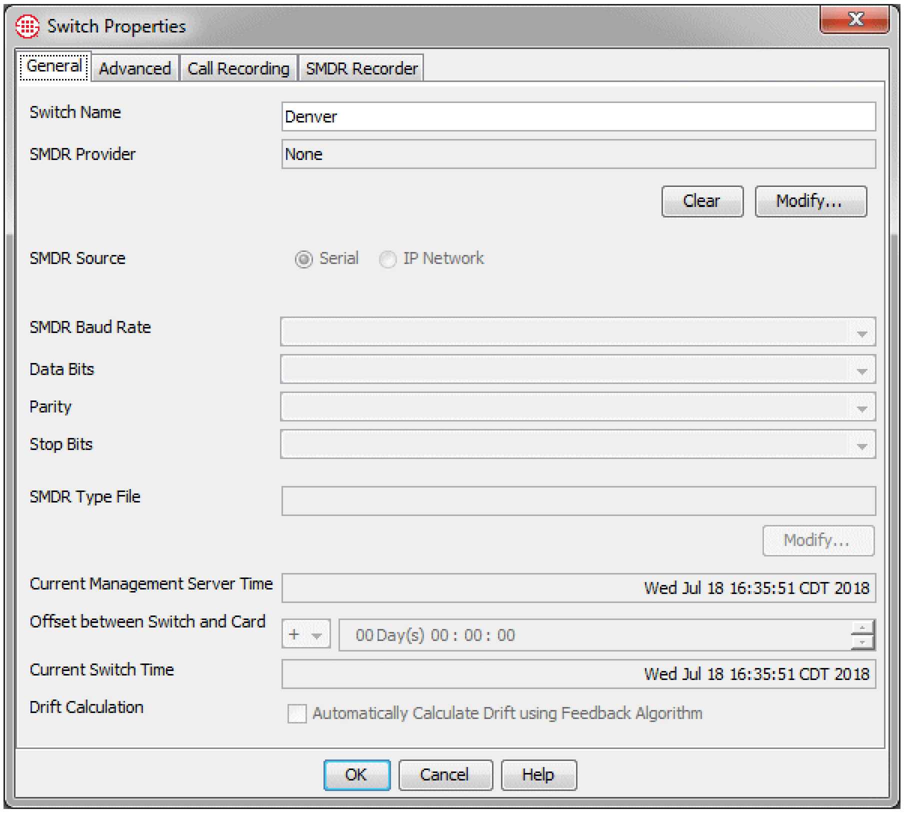
Access codes can also be extracted from SMDR and correlated with listings in the ETM Directory. Before you can modify the **Associated Access Code Set** in the **Switch Properties** dialog box, you must define an Access Code Set in the Directory Manager. See “Access Code Sets” in the *ETM® System User Guide* for instructions for defining an Access Code Set.

Supplying SMDR Processing Information

Note: SIP Spans only can use IP SMDR. UTA Spans do not use SMDR

To supply SMDR processing information

1. In the **Telco Configuration** subtree, right-click the Switch, and then click **Edit Switch**. The **Switch Properties** dialog box appears.



Switch Properties

General | Advanced | Call Recording | SMDR Recorder

Switch Name: Denver

SMDR Provider: None

SMDR Source: ● Serial ○ IP Network

SMDR Baud Rate:

Data Bits:

Parity:

Stop Bits:

SMDR Type File:

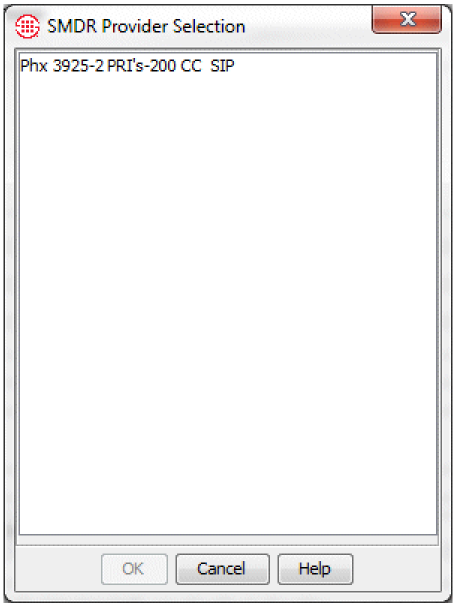
Current Management Server Time: Wed Jul 18 16:35:51 CDT 2018

Offset between Switch and Card: + 00 Day(s) 00 : 00 : 00

Current Switch Time: Wed Jul 18 16:35:51 CDT 2018

Drift Calculation: □ Automatically Calculate Drift using Feedback Algorithm

2. Under the **SMDR Provider** box, click **Modify**. The **SMDR Provider Selection** dialog box appears.



SMDR Provider Selection

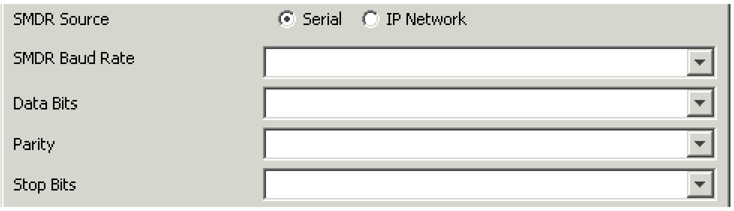
Phx 3925-2 PRI's-200 CC SIP

IMPORTANT Span 1 of the SMDR Provider Card must be moved to the Switch before you can select the SMDR Provider.

- Click the Card that is physically connected to the SMDR port on the PBX, and then click **OK**.

3. Select the type of SMDR source: **Serial** or **IP Network**.

- **For Serial SMDR:**



SMDR Source ● Serial ○ IP Network

SMDR Baud Rate

Data Bits

Parity

Stop Bits

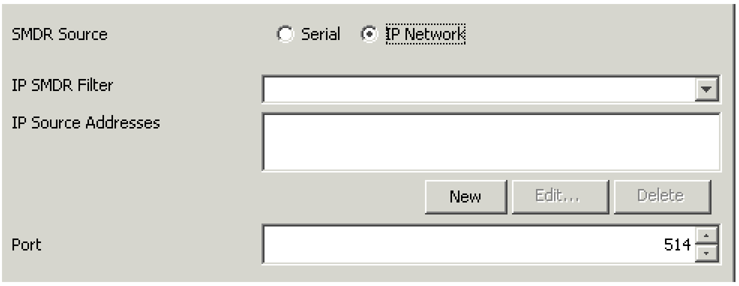
a. In the **SMDR Baud Rate** box, click the down arrow and select the bps that matches that of the PBX SMDR serial port. Options are **300**, **1200**, **2400**, **4800**, **9600**, **19.2k**, **38.4k**, and **57.6k**, and **115.2k**.

b. In the **Data Bits** box, click the down arrow and select value that matches the corresponding settings on the PBX SMDR serial port:
7 or **8**.

c. In the **Parity** box, click the down arrow and select value that matches the corresponding settings on the PBX SMDR serial port: Even, Odd, Mark, or None. (MARK parity only works with 7-bit data; it does not work with 8-bit data).

d. In the **Stop Bits** box, click the down arrow and select value that matches the corresponding settings on the PBX SMDR serial port:
1 or **2**.

- **For IP Network SMDR:**



SMDR Source ○ Serial ● IP Network

IP SMDR Filter

IP Source Addresses

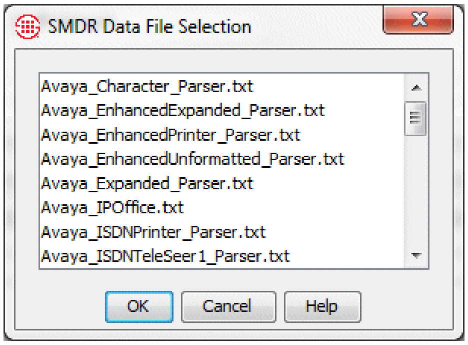
Port 514

a. In the **IP SMDR Filter** box, click the down arrow and click one of the following: **Syslog**, **Unfiltered (UDP)**, or **Unfiltered (TCP/IP)**.

b. In the **IP Source Addresses** box, you specify the IP address of the host sending the SMDR. Click **New**, and then type the IP address of the SMDR source. Optionally, repeat to specify a backup source, if your network is configured with one.

c. In the **Port** box, type or select the port on which the Card receives IP SMDR.

4. Under the **SMDR Type** box, click **Modify**. The **SMDR Data File Selection** dialog box appears.



Avaya_Character_Parser.txt
Avaya_EnhancedExpanded_Parser.txt
Avaya_EnhancedPrinter_Parser.txt
Avaya_EnhancedUnformatted_Parser.txt
Avaya_Expanded_Parser.txt
Avaya_IPOffice.txt
Avaya_ISDNPrinter_Parser.txt
Avaya_ISDNTeleSeer1_Parser.txt

a. All of the SMDR data definition files in the **<INSTALL_DIR>\ps\software_repository\smdr** folder on the ETM Server appear in this dialog box. Click the SMDR parse file that applies to the format in use.

b. Click **OK**.

5. In the **Offset between PBX and Card** box:

a. Click the down arrow and indicate whether the PBX time is later (+) or earlier (-) than that of the SMDR Provider Card. The time on the Card is equal to the time on the ETM Server, plus or minus any time zone difference.

b. Type the correct quantities next to the units of time (days, hours, minutes, and seconds) to indicate by how much the PBX time differs from the SMDR Provider Card time.

See "SMDR Extension Conversion Example" on page 134.

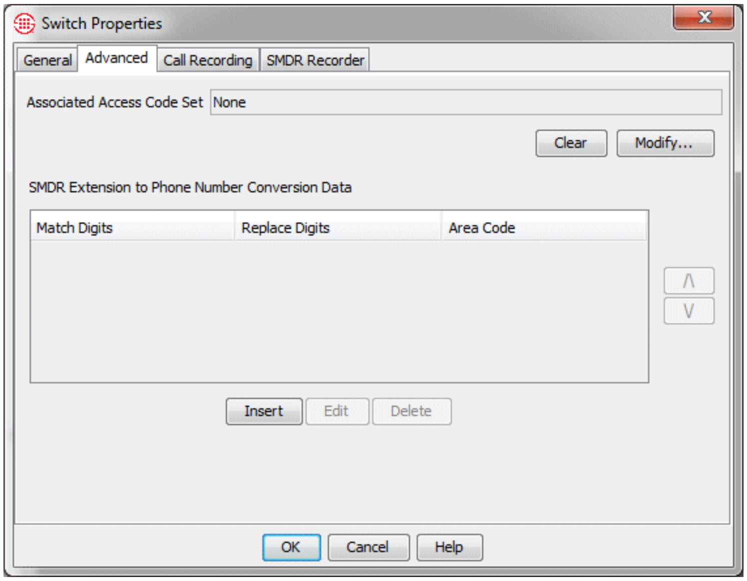
6. In the **Drift Calculation** area, select the **Automatically Calculate Drift Using Feedback Algorithm** box to enable the Server to automatically adjust the offset time to account for drift. To accomplish this, the Server correlates the SMDR requests with the SMDR data and automatically computes what the offset should be. Otherwise, it is highly likely that excessive drift over time will impair the Server's ability to resolve SMDR requests.

Extracting Access Codes from SMDR

Raw Access Codes can be extracted from SMDR and then correlated with Listings in the ETM Directory. The **Associated Access Code Set** area specifies the Access Code Set containing the Access Codes in use on this Switch. Only one Access Code Set can be correlated with a given Switch. If only one Switch and one Access Code Set are defined, they are assumed to be correlated and you do not have to specify the Access Code Set, but if multiple Access Code Sets or Switches are defined, you must specify the set to use.

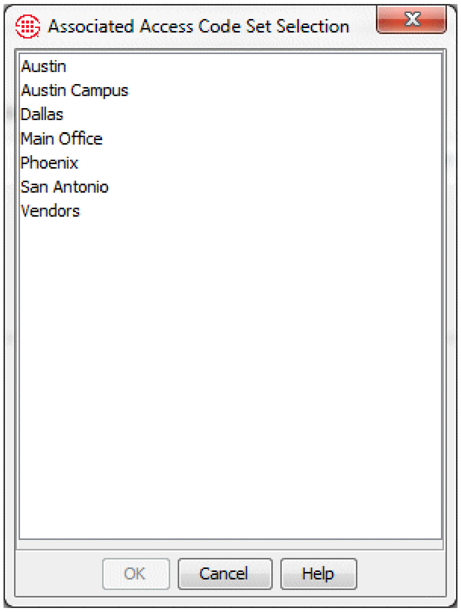
To associate an Access Code Set with the Switch

1. In the **Switch Properties** dialog box, click the **Advanced** tab.



Associated Access Code Set: None

2. In the **Associate Access Code Set** area, click **Modify**. The **Associated Access Code Set Selection** dialog box appears.



Austin
Austin Campus
Dallas
Main Office
Phoenix
San Antonio
Vendors

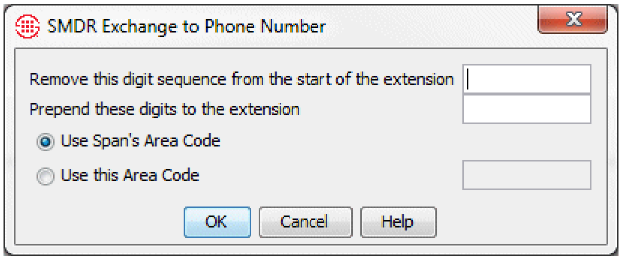
You must define an Access Code Set in the Directory Manager before you can select it here. See the *ETM*® *System User Guide* for instructions for defining an Access Code Set. You can return to this dialog box later to assign the Access Code Set after you complete installation.

3. Click an Access Code Set, and then click **OK**. The selected Access Code Set appears in the **Associated Access Code Set** box.

Converting Internal Extensions from SMDR into Fully Qualified Numbers

The **SMDR Extension to Phone Number Conversion Data** defines how internal extensions obtained from SMDR data are translated into fully qualified phone numbers that accurately represent the originating station. You can specify different conversion algorithms for extensions with different initial digits. See "SMDR Extension Conversion Example" on page 134 for an example of this procedure.

1. In the **Switch Properties** dialog box, click the **Advanced** tab.
2. Below the **SMDR Exchange to Phone Number Conversion Data** box, click **Insert**. The **SMDR Exchange to Phone Number** dialog box appears.



SMDR Exchange to Phone Number

Remove this digit sequence from the start of the extension

Prepend these digits to the extension

● Use Span's Area Code

○ Use this Area Code

3. In the **Remove this digit sequence from the start of the extension** box, type one or more digits to be matched and then removed from the start of the extension.
4. In the **Prepend these digits to the extension** box, type one or more digits to be added to the beginning of the extension after the digits specified in step 3 are removed.
5. Select one of the following to specify the area code that belongs with the extension:
   - If the fully qualified phone number should contain the area code you specified for the Span, select **Use Span's Area Code**.
   - If the fully qualified number should contain a different area code, select **Use this area code**, and then type the correct area code in the text box.
6. Click **OK**. The new conversion Rule appears in the **SMDR Extension to Phone Number Conversion** box.
7. Repeat to add more conversions, if necessary.
8. Extensions are matched and converted in the order in which the conversion Rules appear in this dialog box.
   - To arrange the order of the conversion Rules, click a Rule, and then click the up or down arrow.
   - To remove a conversion Rule, highlight the line, and then click **Delete**.
   - To modify a line, click the line, and then click **Edit**, or double-click the line.

9. Click **OK** to close the **Switch Properties** dialog box and apply the settings. No changes are saved or applied until you click **OK**.

SMDR Extension Conversion Example

See "About SMDR Parse Files" in the *ETM® System Technical Reference* for details about editing the SMDR parse file to extract the dialed digits from the SMDR data.

Suppose the telephone company in San Antonio, Texas, has assigned an organization the following range of phone numbers:

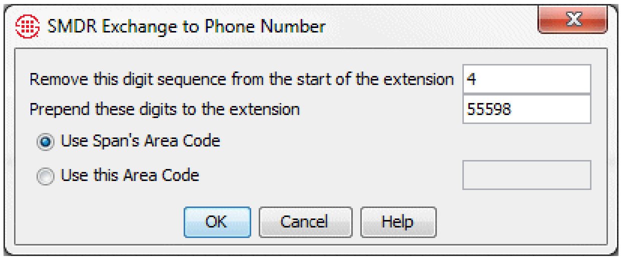
1(210)555-9800 through 1(210)555-9899

Suppose the organization's PBX maps these phone numbers to the following internal extensions (which are the extensions that appear in the SMDR data):

400 through 499

The example procedure below instructs the ETM System to match and remove the 4 from the extension extracted from the SMDR data, add 55598 to the extension, and then add the country code and area/city code to complete the fully qualified phone number:

1. In the **Switch Properties** dialog box, below the **SMDR Extension to Phone Number Conversion Data** box, click **Insert**. The **SMDR Extension to Phone Number** dialog box appears.



SMDR Exchange to Phone Number

Remove this digit sequence from the start of the extension: 4

Prepend these digits to the extension: 55598

● Use Span's Area Code

○ Use this Area Code

2. In the **Remove this digit sequence from the start of the extension** box, type `4`.
3. In the **Prepend these digits to the extension** box, type `55598`.
4. Select **Use Span's area code**, since the extensions are in the same area code as the Span.
5. Click **OK**. The resulting fully qualified numbers to which the Policy Rules are compared are:

   [1](210)555-9800 through [1](210)555-9899.

Continue with one of the following:

- If you are configuring T1 PRI Spans that use NFAS Groups, proceed to "Defining NFAS Groups" on page 135. If not, see the next bullet.
- If SS7 Signaling will be used on this switch, see "Defining SS7 Groups" on page 138. If not, see the next bullet.
- Authorize Management Server connections using the procedures in "Configuring Management Server Settings" on page 143.

SMDR Extensions

(*Not available on UTA*) SMDR Extensions are internal phone numbers identified by inbound SMDR correlation for which you want to prescribe special Call Recorder treatment . For example, you can use SMDR Extensions to define a whitelist of extensions to which calls are never to be recorded, or a blacklist of extensions to which calls are always to be recorded. Recordings can also be marked as sensitive based on this list, for example, for HIPAA-protected calls.

SMDR Extensions only apply to channels on which Inbound SMDR is enabled. When a call completes and SMDR data is received, the inbound destination is compared to the list of SMDR extensions. Several options are provided to define the disposition of the recording when a call matches an SMDR extension, or if for any reason SMDR is not resolved:

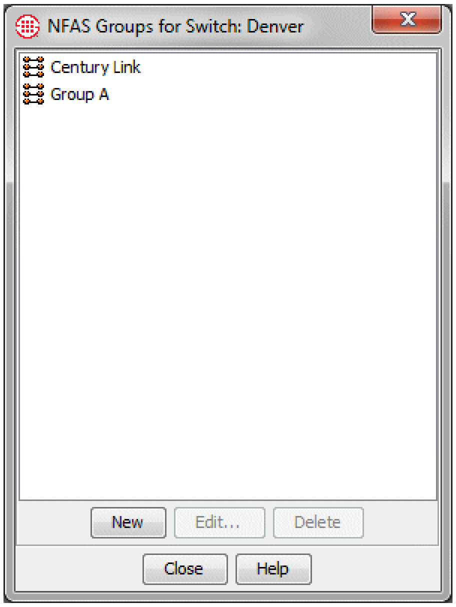
Since the Call Recorder is separately purchased and licensed, its configuration and use instructions are contained in a separate guide. See the *Call Recorder User Guide* for complete configuration instructions, including defining SMDR Extensions.

Defining NFAS Groups

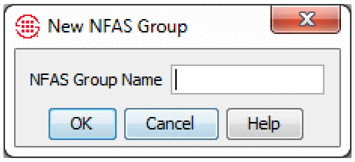
IMPORTANT To prevent the D-Channel from being included in Resource Utilization Reports, disable monitoring of that channel in the **Channel Map** tab of the **Span Configuration** dialog box.

To define an NFAS Group

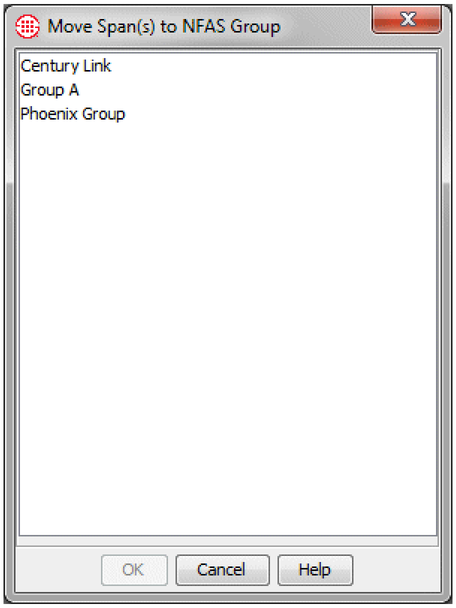
1. In the **Telco Configuration** subtree, right-click the applicable Switch, and then click **Manage NFAS Groups**. The **NFAS Group for Switch** dialog box appears. (If you do not have a switch defined, see "Creating a Switch" on page 125.)



2. Click **New**. The **New NFAS Group** dialog box appears.



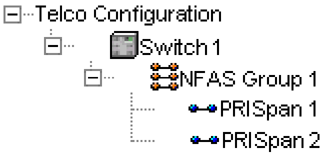
3. In the **NFAS Group Name** box, type the name for the Group, and then click **OK**. The NFAS Group appears in the **NFAS Groups for Switch** dialog box and in the **Telco Configuration** subtree.
4. In the **NFAS Group for Switch** dialog box, click **Close**.
5. In the **Telco Configuration** subtree, hold down CTRL, click each T1 PRI Span that is to be a member of the NFAS Group, right-click the selection, point to **Move Span(s)**, and then click **To NFAS Group**. The **Move Span(s) to NFAS Group** dialog box appears.



Century Link
Group A
Phoenix Group

6. Click the NFAS Group to which these Spans are to belong, and then click **OK**.

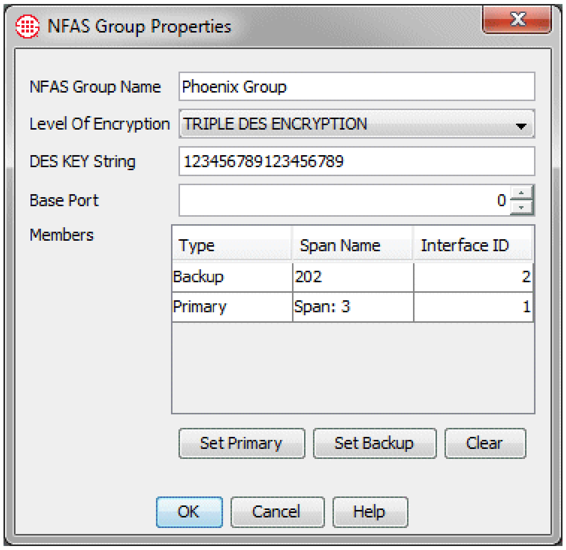
   The Spans move to the selected NFAS Group in the **Telco Configuration** subtree.



- To view the members of the NFAS Group, click the **PLUS SIGN** next to the NFAS Group name.

7. In the **Telco Configuration** subtree, right-click the NFAS Group, and then click **Edit NFAS Group**.

   The **NFAS Group Properties** dialog box appears.



NFAS Group Name: Phoenix Group

Level Of Encryption: TRIPLE DES ENCRYPTION

DES KEY String: 123456789123456789

Base Port: 0

Members

Type	Span Name	Interface ID
Backup	202	2
Primary	Span: 3	1

8. In the **Level of Encryption** box, select the level of encryption for Span-to-Span communication among members of this NFAS Group: **Unencrypted**, **DES Encryption**, or **Triple DES Encryption**. The default is **Unencrypted**. This encryption setting applies only to communication between the members of this NFAS Group.

9. In the **DES Key String** box, type the DES secret key that members of this NFAS Group are to use for encrypted Span-to-Span communication. A DES Key must contain 16-50 characters.

10. In the **Base Port** box, type or select the base TCP/IP port of the port range on which these NFAS Group members are to communicate.

    IMPORTANT Internal system resources reserve up to 8 ports starting at the assigned base TCP/IP port. If two or more Spans on the same Card carry a primary or back up D-channel for different NFAS Groups, **each NFAS Group must use a different base port that is not within the range used by another D-channel, or port contention may occur.** The best practice is to separate all NFAS Group base ports by 10 ports.

11. In the **Members** box, do the following:

    a. Click the Span that carries the Primary D-channel for this NFAS Group, and then click **Set Primary**.

       - To clear the Primary designation, click the Span marked **Primary**, and then click **Clear**.

    b. Click the Span that carries the Backup D-channel for this NFAS Group (if one is provided), and then click **Set Backup**.

- To clear the Backup designation, click the Span marked **Backup**, and then click **Clear**.

c. For each Span listed in the **Members** area, click in the **Interface ID** field and type or select the Interface ID to match the Switch.

12. Click **OK**.
13. Repeat this procedure for additional NFAS Groups, if applicable.

Continue with one of the following:

- If SS7 Signaling is used on this Switch, see "Defining SS7 Groups" on page 138. Otherwise, see the next bullet.
- Authorize Management Server connections using the procedures in "Configuring Management Server Settings" on page 143.

Defining SS7 Groups

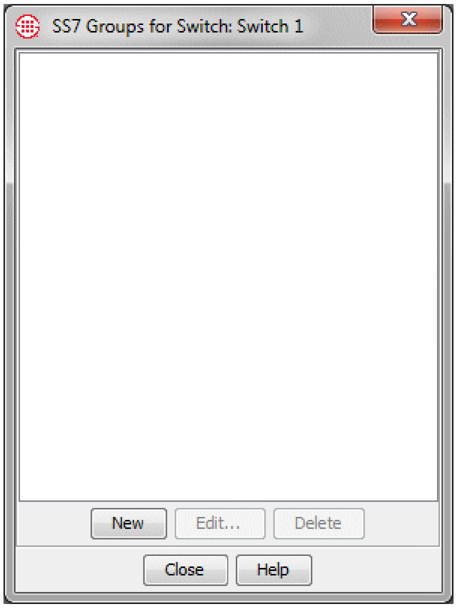
SS7 Groups comprise SS7 Bearer Spans and the SS7 Signaling Links that carry call messaging associated with the SS7 Bearer Spans. Each SS7 Bearer Span can be present in only one SS7 Group; however, SS7 Signaling Links can be present in multiple Groups, because they can be shared by the SS7 Bearer Spans. An SS7 Bearer Span can be associated with up to 16 SS7 Signaling Links.

You must configure the SS7 Signaling Links before you define SS7 Groups. If you have not already done so, complete the procedures in “SS7 Signaling Link-Specific Span Settings” on page 119 before defining the SS7 Group(s).

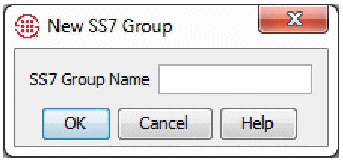
To define an SS7 Group

1. In the **Telco Configuration** subtree, right-click the Switch that represents the PBX to which the SS7 Signaling Links and Bearer Spans are connected, and then click **Manage SS7 Groups**.

   The **SS7 Groups for Switch** dialog box appears.

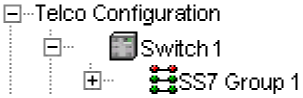


2. Click **New**. The **New SS7 Group** dialog box appears.

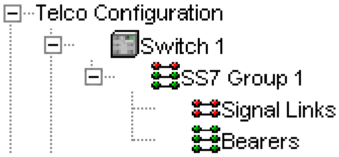


- Type a descriptive name for the Group, and then click **OK**.

The new SS7 Group appears under its switch in the **Telco Configuration** subtree.



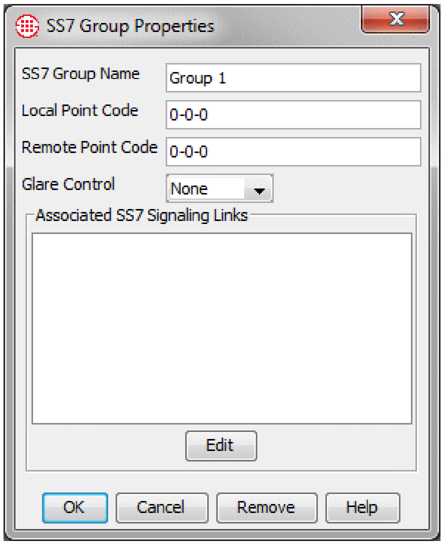
3. Next to the SS7 Group name, click the **PLUS SIGN**.



The SS7 Group contains placeholders for Signaling Links and Bearer Spans.

4. Right-click the SS7 Group, and then click **Edit SS7 Group**. The **SS7 Group Properties** dialog box appears.

CAUTION In the **SS7 Group Properties** dialog box, clicking **Remove** deletes the SS7 Group. If you want to remove Associated SS7 Signaling Links, click **Edit**; and then, in the **Associated SS7 Signaling Links** dialog box, move the Associated SS7 Signaling Links from the **Include** to the **Exclude** box.



SS7 Group Properties

SS7 Group Name: Group 1

Local Point Code: 0-0-0

Remote Point Code: 0-0-0

Glare Control: None

Associated SS7 Signaling Links

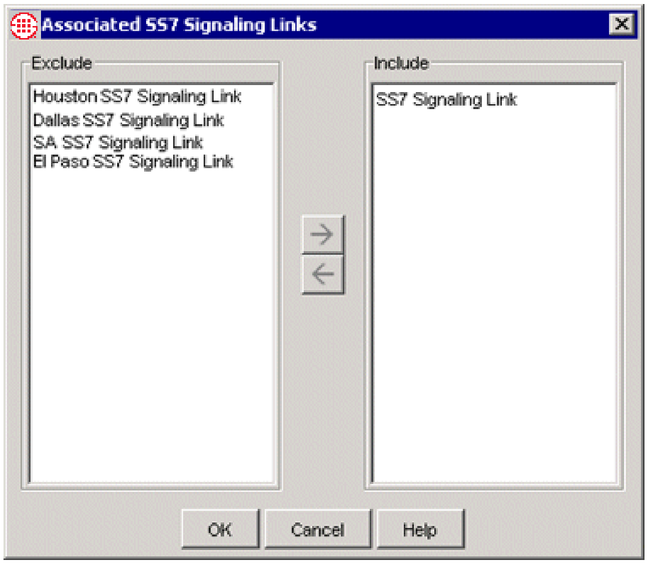
a. The **SS7 Group Name** box contains the name that you gave the Group when you created it. To rename the group, type a different name.

b. In the **Local Point Code** box, type the point code (LPC) of the local Switch or the PBX to which the Bearer Span is connected.

c. In the **Remote Point Code** box, type the point code (RPC) of the remote switch or the CO/IEC switch to which the Bearer trunks are connected.

d. In the **Glare Control** box, click the down arrow, and then click the value used by the local switch. The available values are **None**, **All**, or **Even/Odd**.

e. In the **Associated Signaling Links** box, click **Edit**. The **Associated SS7 Signaling Links** dialog box appears.



Exclude: Houston SS7 Signaling Link, Dallas SS7 Signaling Link, SA SS7 Signaling Link, El Paso SS7 Signaling Link

Include: SS7 Signaling Link

1) In the **Exclude** box, double-click the Signaling Link(s) associated with the Bearer Spans in this SS7 Group, or click it and then click the right-facing arrow. The Signaling Link(s) move to the **Include** box.

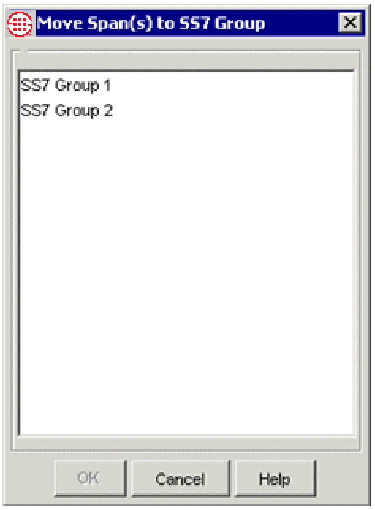
2) Click **OK**.

The Signaling Link(s) appear in the **Associated SS7 Signaling Links** box of the **SS7 Group Properties** dialog box.

f. Click **OK**.

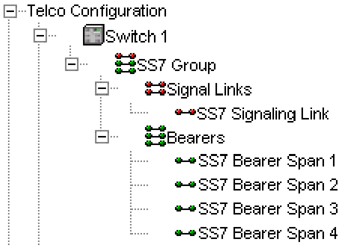
14. In the **Telco Configuration** subtree, hold down CTRL, click each SS7 Bearer Span that is to be a member of the SS7 Group, right-click the selection, point to **Move Span(s)**, and then click **To SS7 Group**.

The **Move Span(s) to SS7 Group** dialog box appears.



SS7 Group 1
SS7 Group 2

15. Click the SS7 Group to which these Spans are to belong, and then click **OK**. In the **Telco Configuration** subtree, the Spans move to the selected SS7 Group.



Continue with:

- "Configuring Management Server Settings" on page 143.

Configuring Management Server Settings

All access to ETM System components is controlled by the ETM Management Server, commonly referred to as the ETM Server. The ETM Server is a background processing engine that controls the ETM Appliances and integrates the ETM System components with your data network. As a security feature, connections from remote client applications (those installed on a computer other than the one on which the ETM Server is installed) must be authorized on the ETM Server computer.

Authorize Remote Client Connections

Authorized ETM System Clients are those whose IP addresses appear in the Client Hosts list for the Server. You can also use a mask (i.e., 10.1.1.255) to authorize a group of IP addresses. The local ETM System Client installed on the ETM Server host computer is authorized by default. Remote Client Hosts may have external IP addresses.

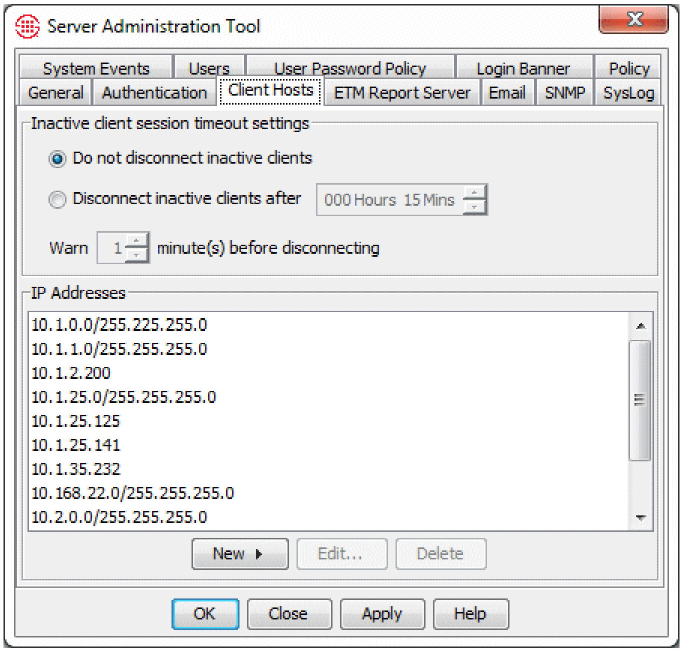
Note: You can also configure an idle Client session timeout on this tab. See the *ETM® System Administration and Maintenance Guide* for instructions.

To authorize a remote ETM® System Console to connect to an ETM® Server

1. In the ETM System Console, click the Server for which you are authorizing remote ETM System Consoles.

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

3. Click the **Client Hosts** tab.



Inactive client session timeout settings

● Do not disconnect inactive clients

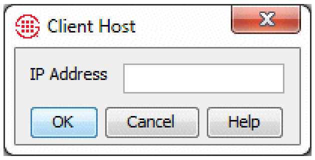
○ Disconnect inactive clients after 000 Hours 15 Mins

Warn 1 minute(s) before disconnecting

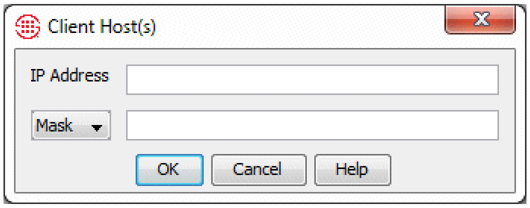
IP Addresses

```
10.1.0.0/255.225.255.0
10.1.1.0/255.255.255.0
10.1.2.200
10.1.25.0/255.255.255.0
10.1.25.125
10.1.25.141
10.1.35.232
10.168.22.0/255.255.255.0
10.2.0.0/255.255.255.0
```

4. To authorize a specific IP address, click **New** and then click **IP Address**. The **Client Host** dialog box appears.



5. Type the IPv4 or IPv6 address of the Client.
6. Click **OK**.
7. To authorize a range of IP addresses, click **New** and then click **IP Range**. The **Client Hosts** dialog box appears.



8. In the **IP Address** box, type the IPv4 or IPv6 base address.
9. If you typed an IPv6 address, click the down arrow and select **Prefix**, and then type the prefix length.
10. If you typed an IPv4 address, select **Mask** and type the subnet mask or select **Prefix** and type a prefix length.
11. Click **OK**.
12. Repeat the above steps for all authorized Clients.
13. On the **Server Administration Tool**, click **OK** to save your changes and close the dialog box or **Apply** to save changes and leave the dialog box open for more configuration settings.

Continue with one of the following:

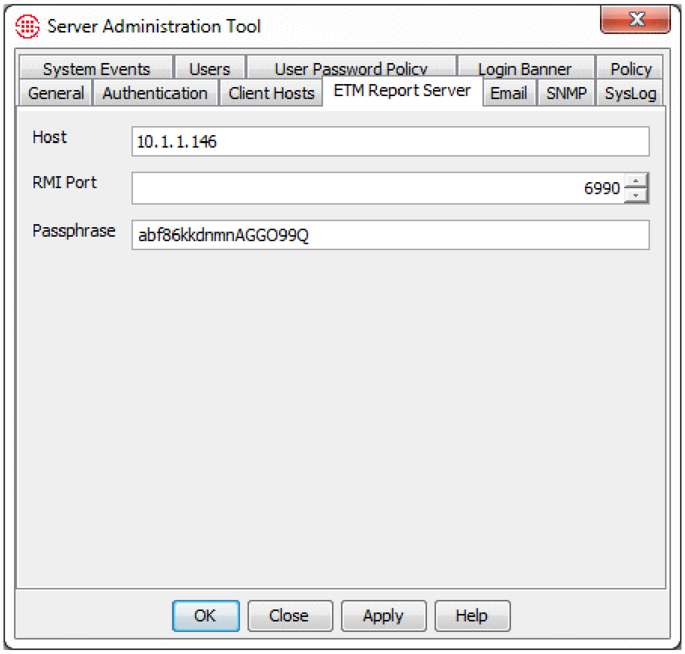
- If the Report Server is installed on a different computer from the Management Server or if you have installed multiple instances of the Report Server and Management Server, see "Associate a Report Server with the ETM® Server" below for configuration instructions. If not, see the next bullet.
- Configure the Management Server with the path to the Oracle client tools, used to import listings and city/state data from external files. See “Specify the Path to the Oracle Client Tools” on page 146.

Associate a Report Server with the ETM® Server

Each ETM Server is associated with a specific Report Server. By default, the Management Server is associated with the Report Server installed on the same computer, if one is installed. To associate the ETM Server with a different Report Server, or if you have installed multiple instances of the ETM Server and Report Server on the same computer, use the following procedure.

To associate a Report Server with the ETM® Server

1. In the ETM System Console, click the Server with which you are associating a Report Server.
2. On the ETM System Console main menu, click **Servers | Server Management**. The **Server Administration Tool** appears.
3. Click the **ETM Report Server** tab.



Host 10.1.1.146

RMI Port 6990

Passphrase abf86kkdnmnAGGO99Q

4. In the **Host** box, type the fully qualified host name or IP address of the computer on which the Report Server is installed.
5. In the **RMI Port** box, type or select the correct RMI port established for the Report Server, if different from the default of 6990. This value is set in the **twms.properties** file on the Report Server computer.
6. In the **Passphrase** box, type the DES key for encrypted communication between the Report Server and the Management Server. This key must always be in sync between the ETM Server and Report Server, because the initial negotiation is always encrypted to establish the connection. The DES Key to use is specified in the **twms.properties** file on the Report Server computer.

Continue with the following:

- Configure the ETM Server to import Directory Listings from an external file or LDAP source and to import the city/state data file that enables Usage Manager reports to provide locale information. See “Specify the Path to the Oracle Client Tools” on page 146.

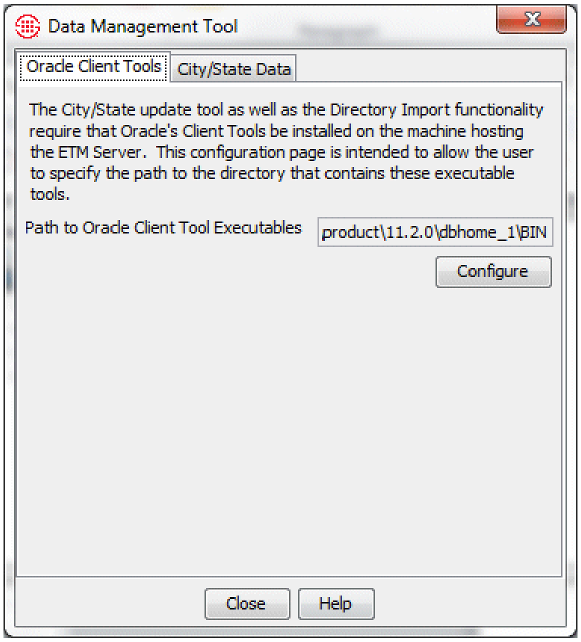
Specify the Path to the Oracle Client Tools

IMPORTANT If the ETM Server is installed on a separate computer from the database, the Oracle client tools must be installed on the ETM Server host computer. This was one of the steps in the procedure for configuring the database. If they were not installed, see "Special Instructions for a Remote ETM® Server Only" on page 33.

The ETM Server uses the Oracle client tools to import Directory Listings and city/state data. Before you can import these items, you must configure the ETM Server with the path to the Oracle client tools.

To specify the path to the Oracle client tools

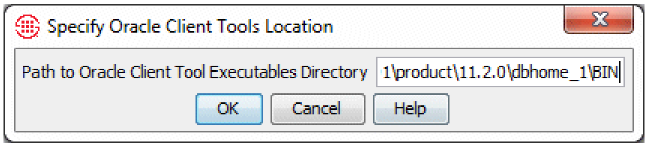
1. In the ETM System Console, click the name of the Server, and then click **Servers | ETM Server Data Management**. The **Data Management Tool** appears.



The City/State update tool as well as the Directory Import functionality require that Oracle's Client Tools be installed on the machine hosting the ETM Server. This configuration page is intended to allow the user to specify the path to the directory that contains these executable tools.

Path to Oracle Client Tool Executables: product\11.2.0\dbhome_1\BIN

2. On the **Oracle Client Tools** tab, click **Configure**. The **Specify Oracle Client Tools Location** dialog box appears.



Path to Oracle Client Tool Executables Directory: 1\product\11.2.0\dbhome_1\BIN

3. In the **Path to Oracle Client Tools Executables Directory** box, type the file path where the Oracle client tool executables reside on the ETM Server host computer. The default location is: **<ORACLE_HOME>\bin**.

   For example, type:

   C:\oracle\ora92\bin\

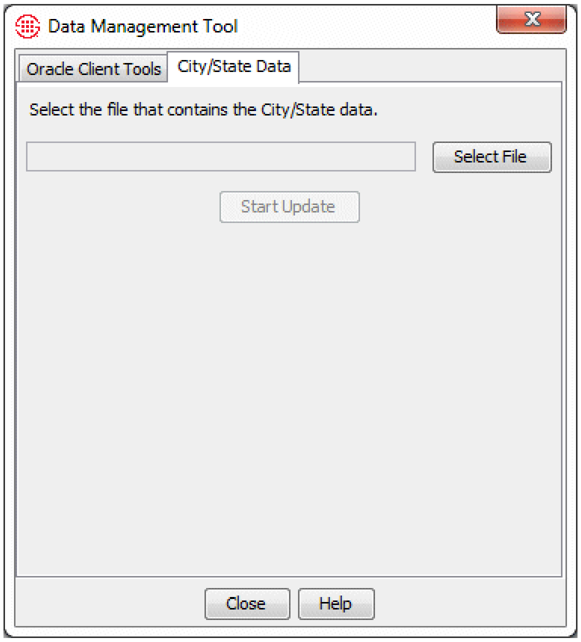
4. Click **OK**.

Importing the City/State Data

At the time this version of the ETM System was released, it contained the latest city/state data. However, this information is updated regularly and must be reimported to remain current. Updated city/state data (CCMI) files are available periodically on the SecureLogix website or by contacting SecureLogix Technical Support. It is recommended that you regularly import updates as they are available (typically monthly).

To import city/state data

1. In the ETM System Console, click the Server name.
2. On the main menu, click **Servers | ETM Server Data Management**. The **Data Management Tool** appears.



Select the file that contains the City/State data.

3. Click the **City/State Data** tab.
4. Click **Select File** to browse for the file, and then click **OK**. The default location, defined in **DataFileLocation** in the **ETM Server Properties Tool**, is **<ETM_install_dir>/ps/data**.
5. Click **Start Update.**

Configuring the Call Recorder

The Call Recorder is separately purchased and licensed. Complete instructions for configuring the ETM Call Recorder components are provided in the *Call Recorder User Guide*. Refer to those instructions to complete Call Recorder configuration. You can do that now and then return to these instructions, or complete the instructions in this guide and then refer to the *Call Recorder User Guide* to complete Call Recorder configuration.

Where to Go From Here

Congratulations!

If you have completed the sequence of procedures described in the preceding sections, the ETM System is installed and configured. You are ready to perform telephony service cutover to place the ETM Appliances inline with your telecommunications system so they can begin monitoring calls.

Continue with "Performing Telephony Service Cutover" on page 149.

Step 4: Telephony Service Cutover

Performing Telephony Service Cutover

Telephony service cutover consists of integrating the ETM® System into the customer-premise equipment (CPE) telecommunications system and then allowing the ETM Appliances to take control of call traffic.

It is highly recommended that you develop a detailed telephony service cutover plan to ensure minimal impact on call traffic during service cutover.

Follow the procedures in this chapter to:

1. Create a telephony service cutover plan.
2. Connect the telco cables and VoIP network cables to the ports on the ETM Appliances.
3. Finalize telephony service cutover.
4. Verify system operation.

IMPORTANT As with any telephony equipment, it is important that the phone circuits be wired correctly when connected to the ETM Appliance, or calls may not be properly recognized. It is particularly important when using Ground Start on the 1024 analog Appliance that tip/ring be properly connected. See "Appendix A: Appliance Technical Specifications, Connectors, and Pinouts" for pinouts of each connector.

Begin with "Creating a Telephony Service Cutover Plan" below.

Creating a Telephony Service Cutover Plan

The following are suggestions for developing a telephony service cutover plan:

- Create a diagram of the circuits to be monitored by the ETM System.
- Create a phone number cross-reference checklist to follow while performing the service cutover, if applicable. For example, if you are performing an analog cutover, create a spreadsheet with columns for Cutover Complete and Punchdown Block IDC Phone Number.
- Determine the time of day when call traffic is minimal and schedule the service cutover for that time.

- Determine how traffic can be rerouted during service cutover for certain blocks. Can hunt groups be used? Can the lines be put into maintenance mode?
- Create a list of numbers to call before service cutover to verify that wiring is correctly installed.
- Create a list of numbers to call after service cutover to verify that Span settings are configured correctly.

Suggested TDM Cutover Plan

The following general cutover plan is suggested to avoid adverse impact to the telephony network if wiring or configuration problems occur.

1. Ask the onsite telco personnel to place the first circuit out of service.
2. With the Appliance powered on, make the telco connection for the first Span. See "Connecting the Telco Cable(s)" on page 150 for instructions for connecting the telco cables to the Appliance telco ports.
3. Verify wiring, and then cut over the Span.
    - For Analog Spans, the Span is inline when you connect the telco cable to the powered-on Appliance.
    - For digital Spans on any Appliance type, place the Span inline by typing the following series of commands via Console connection, Telnet, or the **ASCII Management Interface** for the Span.

      ```
      SPAN INLINE
      ```

      ```
      RESTART
      ```

      You can select multiple Spans at once to place inline via the **ASCII Management Interface**.
4. Verify Span configuration and operation using the procedure in "Post-Cutover Verification" on page 152.
5. Repeat for each Span.

Connecting the Telco Cable(s)

Pinouts of each telco connector are found in "Appendix A: Appliance Technical Specifications, Connectors, and Pinouts" on page 173.

(TDM Appliances Only) To connect the Appliance telco cable(s)

Depending on your Appliance type, follow your service cutover procedures to do the following:

ETM 1024 Analog Spans

1. Connect the cable from the demarcation point or point of presence to the Appliance port labeled **Network** and the cable from the PBX or station to the port labeled **CPE**.
2. Determine the onhook voltage by issuing the `SHOW POTS` ETM Command while the line is onhook.

You can set the threshold values for a specific channel by specifying the channel number, or type ALL to apply the values to all channels.

3. Determine the offhook voltage by issuing the `SHOW POTS` ETM Command while the line is offhook (in the dialing or talking phase). Depending on the polarity and characteristics of the line, the voltage values may be positive or negative and they may fluctuate slightly.

4. Set the `POTS HOOK THRESH <`*`channel`*`> <`*`lower`*`> <`*`upper`*`>` voltages such that the offhook voltage is bracketed, and the onhook voltage is outside of those thresholds. Use magnitudes (disregard sign) when setting the threshold values.

   For instance, suppose the onhook voltage is -48V and the offhook voltage is -7V. Set the hook threshold values to 4 and 10 (brackets the offhook value, 7, and excludes the onhook value, 48) using the command `POTS HOOK THRESH <`*`channel`*`> 4 10`, followed by the command POLICY CONFIG UPDATE. If the onhook voltage is 10V and the offhook voltage is -15V, set the threshold voltages to 13V and 17V (brackets the offhook value, 15, and excludes the onhook value, 10).

   If the onhook and offhook voltage magnitudes are very close together, contact SecureLogix Customer Support to determine the proper threshold values or other necessary actions.

   Depending on the line characteristics and signaling type, the threshold values may need to be tweaked to properly follow hook state throughout the call. The `POTS DEBUG` ETM Command can be used from the Console port to display the voltage values (to the Console connection or in an Appliance debug log) that are used by the software throughout the life of a call. Determine basic values using the method specified above, and then verify the settings by making various test calls that act in different ways (inbound calls, outbound calls, unanswered calls, calls using pulse digits, and so forth). If any of the calls are not detected properly, the `POTS DEBUG ETM Command` output can be used to determine the voltages reported at various stages of each call. You can then set the threshold values to include or exclude these values as appropriate. If this method still does not resolve the problem, contact SecureLogix Customer Support for assistance in determining the appropriate values.

   IMPORTANT Failure to properly connect tip and ring according to the pinouts for these cables may impair operation. Refer to "Connectors and Pinouts" on page 174 for correct pinouts.

Digital TDM Spans

SS7 Signaling Link Cards only use ports 1 and 2.

- For each Card in the Appliance, connect telco cables to each licensed Span as follows:

  Span 1—Port 1 to CO, Port 2 to PBX.

  Span 2—Port 3 to CO, Port 4 to PBX

  Span 3—Port 5 to CO, Port 6 to PBX

  Span 4—Port 7 to CO, Port 8 to PBX

Placing Digital Spans Inline

Upon initial configuration, digital Spans come up offline so that you can configure telco settings without disrupting your traffic. After Spans are configured and you connect the telco cables, place the Spans inline.

To place the Spans inline

- Type the following series of commands via a Console connection or the **ASCII Management Interface** for the Span.

```
SPAN INLINE
RESTART
```

To open the ASCII Management Interface for one or more Spans

- In the Performance Manager tree pane, right-click the Span, and then click **ASCII Management**. To select multiple Spans, hold down CTRL, click each Span, and then right-click the selection, and then click **ASCII Management**.

Post-Cutover Verification

Follow the applicable instructions below to verify operation after performing cutover.

- "Verifying ETM® 1090/2100/3200 Appliance Operation" on page 153.
- "Verifying ETM® 1024 Appliance Operation" on page 154.

Verifying ETM® 1090/2100/3200 Appliance Operation

To verify that an ETM® 1090/2100/3200 Appliance is operating normally

1. View the front of the Appliance and verify the following LEDs for each Card:

   - **I/F**—Illuminated green, indicating communication between the Controller Card and Digital Trunk Interfaces.
   - **PMC**—Illuminated green, indicating communication between the Controller Card and the DSP Mezzanine Card.
   - **Status**—Illuminated green, indicating that there are no errors.
   - **Error**—Not illuminated, indicating that there are no errors.

   If the **Status** LED is not green and blinking, execute a `SHOW STATUS` command from the **Console** port to determine the cause

2. View the back of the Appliance and verify the following for each Card:

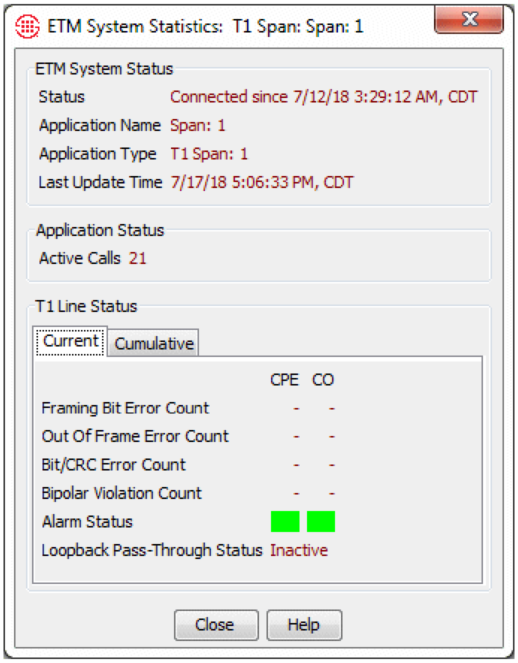
   - **Alarm**—No LEDs are illuminated; no trunks are in alarm.
   - **Online**—All LEDs are illuminated green.

3. View the CSU(s) and PBX and verify that both are free of alarm lights and appear to be operating normally.

4. Follow a comprehensive phone number test list developed by your organization and make calls to verify that lines are working correctly.

5. In the Performance Manager, do the following:

   a. In the **Platform Configuration** subtree, right-click the Span, and then click **Health & Status**. The **ETM System Statistics** dialog box appears. Use this dialog box to view trunk errors, bipolar violations, and alarms. When you first open the dialog box, click **Reset** on the **Cumulative** tab to clear any errors that may have been introduced during cutover. See “Telco Span Health & Status” in the *ETM® System User Guide* for details about each of the fields on this dialog box, which vary according to the type of Span.



ETM System Statistics: T1 Span: Span: 1

ETM System Status

Status	Connected since 7/12/18 3:29:12 AM, CDT
Application Name	Span: 1
Application Type	T1 Span: 1
Last Update Time	7/17/18 5:06:33 PM, CDT

Application Status

Active Calls 21

T1 Line Status

	CPE	CO
Framing Bit Error Count	-	-
Out Of Frame Error Count	-	-
Bit/CRC Error Count	-	-
Bipolar Violation Count	-	-
Alarm Status	🟩	🟩
Loopback Pass-Through Status	Inactive	

b. View the **Diagnostic Log** to verify that no errors are being reported; see "Viewing the Diagnostic Log" on page 156.

c. View the **Call Monitor** to verify that calls are passing through the ETM Appliance; see "Monitoring Calls in Real Time" on page 158.

Verifying ETM® 1024 Appliance Operation

To verify that a 1024 Appliance is operating normally

1. View the front of the Appliance and verify the following LEDs:

   - **I/F**—Illuminated green, indicating communication between the Controller Card and Digital Trunk Interfaces.
   - **PMC**—Illuminated green, indicating communication between the Controller Card and the DSP Mezzanine Card.
   - **Status**—Illuminated green, indicating that there are no errors.
   - **Error**—Not illuminated, indicating that there are no errors.

   If the **Status** LED is not green and blinking, execute a `SHOW STATUS` command from the **Console** port to determine the cause.

2. Follow a comprehensive phone number test list developed by your organization and make calls to verify that lines are working correctly.

3. In the Performance Manager, do the following:
    a. View the **Diagnostic Log** to verify that no errors are being reported; see "Viewing the Diagnostic Log" on page 156.
    b. View the **Call Monitor** to verify that calls are passing through the ETM Appliance; see "Monitoring Calls in Real Time" on page 158.

Verifying SIP and UTA Span Operation

To verify SIP and UTA Span operation

1. Follow a comprehensive phone number test list developed by your organization and make calls to verify that calls are working correctly.
2. In the Performance Manager, do the following:
    a. View the **Diagnostic Log** to verify that no errors are being reported; see "Viewing the Diagnostic Log" on page 156.
    b. View the **Call Monitor** to verify that calls are passing through the ETM Appliance and call direction is correctly reported; see "Monitoring Calls in Real Time" on page 158.

Bypassing TDM Appliances

Telecommunications degradation or failure can occur if Span configuration settings are incompatible with your telecommunications system. If signals become degraded or if calls are dropped after the telco cables are connected and the Spans placed inline, follow the procedure to allow telecommunications traffic to pass unaffected through the Appliances while you verify Span configuration. Contact SecureLogix Customer Support at 1-877-SLC-4HELP or **support@securelogix.com** for assistance, if necessary.

For instructions for bypassing the SIP Appliances and the SIP/AXP solution, see the SecureLogix Knowledge Base.

IMPORTANT These bypass procedures only affect the telco interface. You can still configure the Appliance from the Performance Manager, because the ETM Server Ethernet interface is unaffected.

To bypass the ETM® Appliances

<u>Analog Spans</u>

Analog Appliances cannot be placed offline while powered on. To bypass an Analog Appliance, install bridge clips at the punchdown block or otherwise wire around the Appliance.

<u>Digital Spans</u>

For each Span, type the following command via the **ASCII Management Interface** via the Performance Manager, the Console port, or Telnet.

```
SPAN OFFLINE
```

- If you are using the **ASCII Management Interface**, you can select and configure multiple Spans simultaneously.
- To bring the Span back inline, type the following series of commands via in the Performance Manager, the **Console** port, or Telnet:

```
SPAN INLINE
RESTART
```

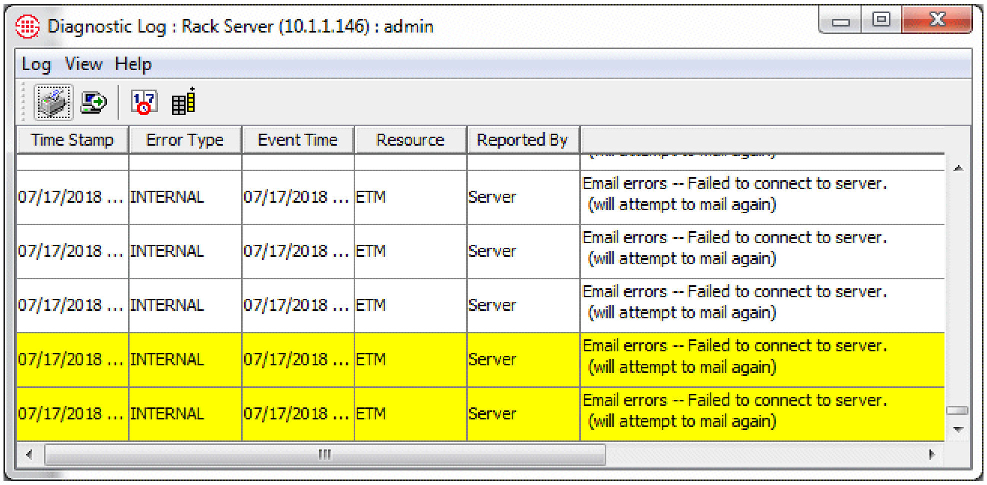
Viewing the Diagnostic Log

After performing telephony service cutover, view the **Diagnostic Log** for evidence of configuration errors or connection problems.

To view the Diagnostic Log

- Do one of the following:
  - On the Performance Manager main menu, click **Tools | View Diagnostic Logs**.
  - To see logs for a specific Span, right-click the Span in the tree, and then click **View Diagnostic Logs**

  The **Diagnostic Log** appears showing diagnostic messages for all resources managed by this Management Server.



Time Stamp	Error Type	Event Time	Resource	Reported By	
07/17/2018 ...	INTERNAL	07/17/2018 ...	ETM	Server	Email errors -- Failed to connect to server. (will attempt to mail again)
07/17/2018 ...	INTERNAL	07/17/2018 ...	ETM	Server	Email errors -- Failed to connect to server. (will attempt to mail again)
07/17/2018 ...	INTERNAL	07/17/2018 ...	ETM	Server	Email errors -- Failed to connect to server. (will attempt to mail again)
07/17/2018 ...	INTERNAL	07/17/2018 ...	ETM	Server	Email errors -- Failed to connect to server. (will attempt to mail again)
07/17/2018 ...	INTERNAL	07/17/2018 ...	ETM	Server	Email errors -- Failed to connect to server. (will attempt to mail again)

Any message reporting a potential configuration error should not be ignored. For example, the message "`Possible configuration error on channel <x>`" indicates potential Span configuration errors for signaling or timing that prevent proper call recognition.

If you select **View Diagnostic Logs** for a specific Span, a filter is applied so that only records for the selected Span appear.

New entries are highlighted in yellow by default. Click **Help** on the **Diagnostic Log** main menu or see "Setting Diagnostic Log Display

Preferences" in the *ETM® System Administration and Maintenance Guide* for information about setting log-display properties, hiding/showing columns, and filtering the display.

The **Diagnostic Log** provides the following information:

Column	Description
Time Stamp	The date and time at which the Server received the message.
Error Type	The type of system event. Types include: **ERROR**—Occurs in response to such events as elevated cabinet temperature or power supply failure. **INFO**—Messages labeled INFO do not represent problems. They provide general information about system operation, such as connection requests from ETM System components. **PANIC**—Occurs in response to such events as Card application or hardware errors. **POLICY**—Events associated with Policies and Dialing Plans. **SECURITY**—Indicates both authorized and unauthorized access, connection, and configuration change events. **START/STOP**—Occurs when a Card or the Server is shut down or initialized. **TELCO**—Provides information about telephony events. Improper Span telecom configuration may cause telco errors. **WARNING**—Occurs in response to such events as lost Card/Server communication, time zone change, or fail-safe mode.
Event Time	The date and time the event occurred.
Resource	The system component that triggered the event (for example, the Management Server or a specific Span managed by that Server).
Reported By	The system component that sent the message to the **Diagnostic Log**. (for example, the Management Server or a hardware component).
Description	The description of the event that triggered the notification.

Monitoring Calls in Real Time

The **Call Monitor** provides a near real-time display of call activity on monitored channels. You can use the **Call Monitor** to verify that call traffic is passing through the Span(s). For details about each column in the **Call Monitor** and for information about setting display properties, see "Call Monitor" in the *ETM® System User Guide*.

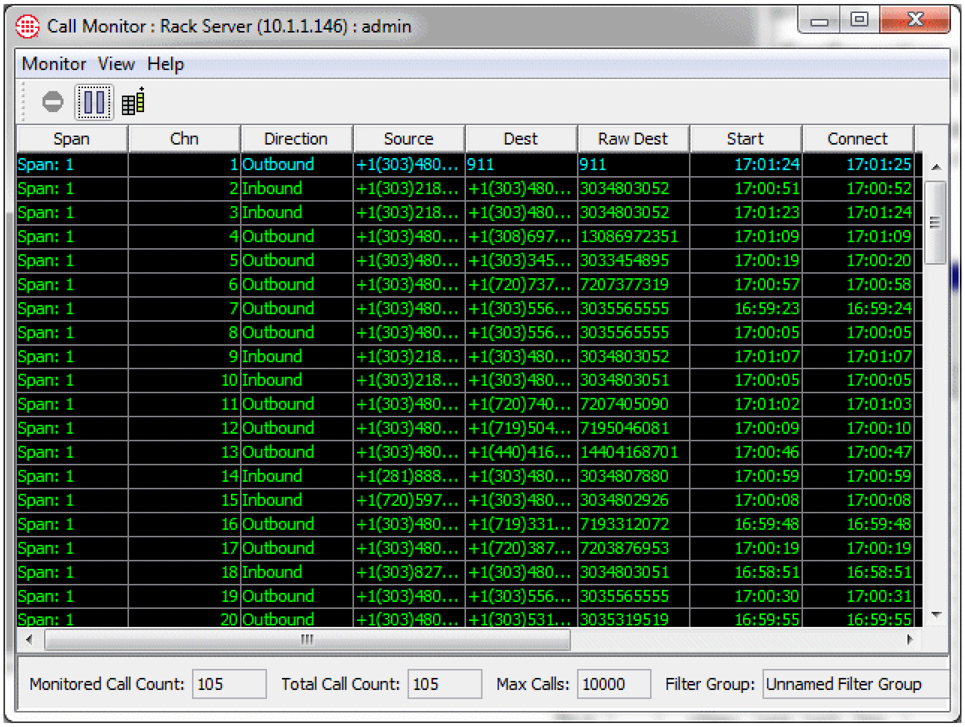
To open the Call Monitor

1. Do one of the following:

    - In the **Telco Configuration** subtree, right-click a switch or one or more Spans, and then click **Call Monitor**.

    - In the **Platform Configuration** subtree, right-click one or more Appliances, Cards, or Spans, and then click **Call Monitor**.

    The **Call Monitor** appears.



Span	Chn	Direction	Source	Dest	Raw Dest	Start	Connect
Span: 1	1	Outbound	+1(303)480...	911	911	17:01:24	17:01:25
Span: 1	2	Inbound	+1(303)218...	+1(303)480...	3034803052	17:00:51	17:00:52
Span: 1	3	Inbound	+1(303)218...	+1(303)480...	3034803052	17:01:23	17:01:24
Span: 1	4	Outbound	+1(303)480...	+1(308)697...	13086972351	17:01:09	17:01:09
Span: 1	5	Outbound	+1(303)480...	+1(303)345...	3033454895	17:00:19	17:00:20
Span: 1	6	Outbound	+1(303)480...	+1(720)737...	7207377319	17:00:57	17:00:58
Span: 1	7	Outbound	+1(303)480...	+1(303)556...	3035565555	16:59:23	16:59:24
Span: 1	8	Outbound	+1(303)480...	+1(303)556...	3035565555	17:00:05	17:00:05
Span: 1	9	Inbound	+1(303)218...	+1(303)480...	3034803052	17:01:07	17:01:07
Span: 1	10	Inbound	+1(303)218...	+1(303)480...	3034803051	17:00:05	17:00:05
Span: 1	11	Outbound	+1(303)480...	+1(720)740...	7207405090	17:01:02	17:01:03
Span: 1	12	Outbound	+1(303)480...	+1(719)504...	7195046081	17:00:09	17:00:10
Span: 1	13	Outbound	+1(303)480...	+1(440)416...	14404168701	17:00:46	17:00:47
Span: 1	14	Inbound	+1(281)888...	+1(303)480...	3034807880	17:00:59	17:00:59
Span: 1	15	Inbound	+1(720)597...	+1(303)480...	3034802926	17:00:08	17:00:08
Span: 1	16	Outbound	+1(303)480...	+1(719)331...	7193312072	16:59:48	16:59:48
Span: 1	17	Outbound	+1(303)480...	+1(720)387...	7203876953	17:00:19	17:00:19
Span: 1	18	Inbound	+1(303)827...	+1(303)480...	3034803051	16:58:51	16:58:51
Span: 1	19	Outbound	+1(303)480...	+1(303)556...	3035565555	17:00:30	17:00:31
Span: 1	20	Outbound	+1(303)480...	+1(303)531...	3035319519	16:59:55	16:59:55

Monitored Call Count: 105 Total Call Count: 105 Max Calls: 10000 Filter Group: Unnamed Filter Group

2. All channels are displayed by default. To view only active channels, click **View | Fixed Row Counts**. The selection acts as a toggle to display all channels or only active channels. A check mark indicates that fixed row counts are shown; no check mark indicates that rows are shown only for active channels.

Where to Go From Here

- If you will use the ETM Web Portal for viewing and scheduling Usage Manager Reports and/or accessing ETM Call Recorder call recordings, see “Installing and Configuring the ETM® Web Portal” on page 161.
- Refer to the *ETM® System User Guide* for an overview of the ETM System, a discussion of key concepts, and general instructions for using the ETM System, including a Quick Start.
- Refer to the *ETM® System Administration and Maintenance Guide* for instructions for defining and managing user accounts, managing the Management Server, and managing the ETM Appliances from the Performance Manager.
- Refer to the *Voice Firewall User Guide* for instructions for defining and using Voice Firewall Policies.
- Refer to the *Voice IPS User Guide* for instructions for defining and using Voice IPS Policies.
- Refer to the *Call Recorder User Guide* for instructions for configuring the Call Recorder and recording calls.
- Refer to the *Usage Manager User Guide* for instructions for producing reports of telecommunications monitoring and Policy enforcement.
- Refer to the *ETM® System Technical Reference* for ETM Database administration, system backup and restoration, ETM Commands, and other technical information not normally a part of day-to-day system operation.

Installing and Configuring the ETM® Web Portal

Web Portal Installation and Configuration

(*Windows only*) You can deploy the ETM Web Portal (which can be used to access call recordings with the optional Call Recorder and can be used to view and schedule Usage Manager Reports) on your existing web server, or you can use the bundled Apache Tomcat web server/Java Servlet Container on Windows.

The ETM Web Portal is a Java Servlet/JavaServer Pages (JSP) Web Application. It is self-contained in a Web Archive (WAR) file called **webetm.war**. The application runs in any Java Servlet Container that follows the Java Servlet/JSP Specifications.

The Apache Software Foundation provides a free Java Servlet Container that also functions as a simple web server—Apache Jakarta Tomcat (also known as Apache Tomcat, or just Tomcat). This application is bundled in the ETM Web Portal Installer. If you do not have an existing web server or do not want to deploy ETM Web Portal on your existing web server, you can use Tomcat. Note that Tomcat is not the same as the Apache HTTP Server.

How you install the ETM Web Portal depends on whether you are planning to use the bundled Tomcat web server or your existing web server. See the applicable section below.

Integrating the Web Portal with an Existing Web Server

To integrate the ETM Web Portal application into an existing web server, do not use the InstallShield Installer. You only require the ETM Web Portal WAR file, **webetm.war**. This file is available on the ETM System Software CD in the following directory:

<CDROOT>\Software\WebETM

Since proper incorporation of a WAR file depends on the web server you use, consult the documentation for your web server and the IT personnel responsible for your web server.

After installation, see “Specifying Management Servers” on page 163.

ETM® Web Portal Log Files

The location of the WebETM log files depends on your installation and web server configuration. Consult your web server administrator. By default, a

logs directory is created in the location from which the application is run. For the bundled installation, Tomcat is run as a service and the log files are placed in **..\WINDOWS\system32\logs** by default. When Tomcat is run this way, the working path can be configured via the Tomcat configuration utility to place the log files in a different location. Tomcat also creates a **\webetm\logs** directory.

Installing Apache Tomcat and the ETM® Web Portal

(*Windows only*) A Windows InstallShield Installer is included on the ETM System Software CD that installs Apache Jakarta Tomcat Version 5.5.9, an embedded JRE required for running Tomcat, and the ETM Web Portal Application. The Tomcat installation is identical to that performed by the standalone Tomcat installation that Apache provides.

By default, Apache Tomcat for the ETM Web Portal is installed at **<WINROOT>\WebETM**, where **<WINROOT>** is the root drive on which the Windows operating system is installed (typically, **C:\**). In the following instructions, the WebETM installation location is referred to as **<INSTALL_DIR>**.

IMPORTANT For the ETM Web Portal application to work correctly with the Java Runtime Environment, Apache Tomcat must be installed into a directory that does not contain spaces. To ensure this, the installer verifies any user-entered install location to ensure that it contains no spaces. If it does, a warning appears and you must enter a different path that contains no spaces to continue the installation.

The installer is located on the Windows ETM System Software CD at **<CDROOT>\Software\WebETM\Installer**.

To install the ETM® Web Portal with Apache Tomcat

1. Run the InstallShield Installer and follow the onscreen prompts.
2. When installation is complete, start the Tomcat Monitor Utility as follows:
   a. Click **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Monitor Tomcat.**
   b. Verify that the **Tomcat Monitor** System Tray icon appears.
3. Start the **Apache Tomcat** Service as follows:
   - Right-click the **Tomcat Monitor** System Tray icon and click **Start Service**.
4. Verify that Tomcat is running correctly by navigating to the Tomcat **Welcome** page as follows:
   - Click **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Welcome**.

See “Accessing the ETM® Web Portal” on page 171 for instructions for logging in.

5. Specify the location of the ETM Management Server(s) with which the Web Portal is to be used, if the Web Portal is installed on a different

host computer from the ETM Server. See "Specifying Management Servers" on page 163 for instructions.

6. Optionally, configure SSL See "Configuring the Web Portal for SSL" on page 166 for instructions.
7. Verify that the ETM Web Portal is running by navigating to the login page on the computer where you installed it:
   - Click **Start | Programs | SecureLogix | ETM Web Reporting | ETM Web Portal**.

Specifying Management Servers

By default, the ETM Web Portal application attempts to connect to a local ETM Management Server (127.0.0.1) using the default client port (6990) and default DES passphrase. If the ETM Management Server is on another host or uses a different port or passphrase, you must edit the configuration to enable the Web Portal to connect. You can also change the Server name displayed in the Server Selection GUI and specify additional Servers.

To edit the configuration

1. Open the following file in a text editor:

   \webetm\WEB-INF\server-defn.xml

   - If you are using Tomcat, this file is located at

<INSTALL_DIR>\jakarta-tomcat-5.5.9\webapps\webetm\WEB-INF\server-defn.xml

   Note that Apache Tomcat must have been started at least once before this file is be available.

   - If you integrated the Web Portal with your existing web server, ask your web server administrator to locate the **webetm** folder. This file is compressed inside the WAR file and the web server extracts it the **WAR** file is executed.

2. Follow the instructions in the file for setting the appropriate configuration.
3. Restart the Tomcat service.

Files and Folders Installed

The following files and folders are created when you install Apache Tomcat for ETM Web Reporting:

- Apache Tomcat—Installed under **<INSTALL_DIR>\jakarta-tomcat-5.5.9.**

  The files and directory structures beneath this directory are essentially that of a normal Tomcat installation, with the exception of the **JRE** and **WebETM** folders (see below).

- The Java Runtime Environment—Version 1.5.0_02-b09 is required to run Tomcat and is installed under **<INSTALL_DIR>\jakarta-tomcat-5.5.9\bin\jre1.5.0_02**.
- WebETM—The ETM Web Reporting Application; installed as a WAR file under **<INSTALL_DIR>\jakarta-tomcat-5.5.9\webapps**.
- SecureLogix Documentation is installed under **<INSTALL_DIR>\Documentation**.

Tomcat Web Server Service

The installer creates a service called **Apache Tomcat** that represents the web server portion of Tomcat. By default, this service is set to autostart at system startup. The service does not start automatically at the end of the installation process. Be sure to start the service before attempting to run Web Reports.

Apache Tomcat Monitor Autostart

The installer installs a registry key that causes the Apache Tomcat Monitor program to automatically start when you log into a desktop session. This mimics the behavior of the normal Apache Tomcat installer. For reference, the registry key is:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ApacheTomcatMonitor

Application Shortcuts

The following shortcuts are created by the installer (the Tomcat specific shortcuts mimic those created by the default Tomcat installer):

- **Start | Programs | SecureLogix | ETM Web Portal | ETM Web Reporting**—Opens a web browser and navigates to the ETM Web Reporting login page of the ETM Web Reporting application when it is running on the local Apache Tomcat service (**http://127.0.0.1/webetm**). This shortcut assumes the HTTP port is the default of 80. If not, edit the file **<INSTALL_DIR>\ETM Web Reporting.url** in a text editor and change the port. Note that if you are running with SSL, you are by default redirected to the SSL port.
- **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Configure Tomcat**—Launches the configuration utility for the **Apache Tomcat** service.

- **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Monitor Tomcat**—Places a monitor utility in the system tray for display the status of the **Apache Tomcat** service. The system tray icon also provides access to startup and shutdown commands and the configuration utility.
- **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Tomcat 5.5 Program Directory**—Opens a Windows Explorer window to the Apache Tomcat 5.5 Program Directory. (**By default C:\WebETM\jakarta-tomcat-5.5.9**).
- **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Tomcat Home Page**—Opens a web browser and navigates to the Apache Tomcat home page at the Apache Software Foundation web site.
- **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Tomcat Manager**—If configured for operation, opens a web browser and navigates to the Tomcat Manager web application running on the local Apache Tomcat service. (See the "Tomcat Manager" section below). This shortcut assumes the HTTP port is the default of 80. If not, edit the file **<INSTALL_DIR>\jakarta-tomcat-5.5.9\bin\Tomcat Manager.url** in a text editor and change the port.
- **Start | Programs | SecureLogix | ETM Web Portal | Apache Tomcat 5.5 | Welcome—**Opens a web browser and navigates to the Apache Tomcat Welcome page running on the local Apache Tomcat service. Useful for testing to see if the local Apache Tomcat is operating correctly. This shortcut assumes the HTTP port is the default of 80. If not, edit the file **<INSTALL_DIR>\jakarta-tomcat-5.5.9\bin\Welcome.url** in a text editor and change the port.
- **Start | Programs | SecureLogix | ETM Web Portal | Documentation | License Agreement**—Displays the SecureLogix Corporation license agreement.
- **Start | Programs | SecureLogix | ETM Web Portal | Documentation | Usage Manager User Guide**—SecureLogix PDF documentation for the Usage Manager, including the ETM Web Portal Reporting application:
- **Start | Programs | SecureLogix | ETM System Software | Documentation | Call Recorder User Guide**—SecureLogix PDF documentation for the Call Recorder, including using the ETM Web to access call recordings.

More about the Web Applications Installed

Web applications are the various applications that can be "served" to users by the Apache Tomcat service. The Apache Tomcat application with the ETM Web Portal installs with four web applications:

- **ROOT**—The root Apache Tomcat web application accessed by navigating to **http://*<hostname or IP address>***/ This is just a

Welcome page that provides links to various things, including the Tomcat documentation mentioned below. (A shortcut is provided on the Start menu of the Tomcat host computer for accessing this URL).

- **tomcat-docs**—The Tomcat documentation. Access the documentation by navigating to **http://<*hostname or IP address*>/** and clicking the **Tomcat Documentation** link. Alternatively, you can access the documentation directly by using the URL: **http://<*hostname or IP address*>/tomcat-docs**
- **manager—**A management application that provides an interface for managing the various web applications running on the Apache Tomcat service. Access the Tomcat Web Application Manager by navigating to **http://<*hostname or IP address*>/** and clicking the **Tomcat Manager** link, or use the Start menu shortcut on the Tomcat host computer. (For details, see "Configuring the Tomcat Web Application Manager" on page 169.)
- **webetm—**The ETM Web Portal application. (A shortcut is provided on the **Start** menu of the Tomcat host computer for accessing this URL).

Configuring the Web Portal for SSL

By default, Apache Tomcat is not configured to provide an SSL connection to the ETM Web Reporting application. The following procedure explains how to enable SSL support for the ETM Web Reporting Application.

Prior to proceeding, it is strongly recommended that you review the "Apache Jakarta Tomcat 5.5 Servlet/JSP Container—SSL Configuration HOW-TO" at:

http://jakarta.apache.org/tomcat/tomcat-5.5-doc/ssl-howto.html

Follow this sequence of steps to configure Apache Tomcat for ETM Web Reports to use SSL:

1. Create a Certificate Keystore.
2. Configure an SSL Port in the Apache Tomcat Configuration.
3. Configure the ETM Web Reporting Application for use over SSL.
4. Restart the Apache Tomcat Service.

To configure SSL support for the ETM Web Portal Application

1. Create a Certificate Keystore as follows:
   a. Open a command prompt window.
   b. Change to the directory **<INSTALL_DIR>\jakarta-tomcat-5.5.9\conf**.
   c. Run the keytool utility using the following command:
   ```
   <INSTALL_DIR>\jakarta-tomcat-5.5.9\bin\
   jre1.5.0_02\bin\keytool.exe -genkey -alias
   tomcat -keyalg RSA -keystore keystore.jks
   ```

TIP When text appears in brackets, you can press ENTER to accept it as the default value.

d. You are prompted for the following information:

```
Enter keystore password:
```

This is the password used to protect the keystore. The default for use with Apache Tomcat is **changeit** but you can type a custom password.

```
What is your first and last name? [Unknown]:
```

Type the "Common Name" (CN) for the issuer, which can be either your name, the server domain name, or an email address. For example, if the server's domain is **SecureLogix.com**, you would type: `SecureLogix.com`

```
What is the name of your organizational
unit? [Unknown]:
```

Enter your organizational unit, if applicable. For example: `Information Technology`

```
What is the name of your organization?
[Unknown]:
```

Enter your organization name. For example: `SecureLogix Corporation`

```
What is the name of your City or Locality?
[Unknown]:
```

Enter the city or locality for the server, if applicable. For example, type: `San Antonio`

```
What is the name of your State or Province?
[Unknown]:
```

Enter the state or province for the server, if applicable. For example: `TX`

```
What is the two-letter country code for this
unit? [Unknown]:
```

Enter the country code for the server. For example: `US`

```
Is CN=SecureLogix.com, OU=Information
Technology, O=SecureLogix Corporation, L=San
Antonio, ST=TX, C=US correct?  [no]:
```

Verify the information and type `yes` to accept.

```
Enter key password for <tomcat>  (RETURN if
same as keystore password):
```

To work correctly, the key password must be the same as the keystore password, so just press ENTER.

2. Configure an SSL Port in the Apache Tomcat Configuration

   a. In a text editor, open the following file:

<INSTALL_DIR>\jakarta-tomcat-5.5.9\conf\server.xml

b. Locate the following section:

Delete this leading comment designator

Type the correct keystore password, if different from the default

Delete this trailing comment designator

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector port="8443"
           maxHttpHeaderSize="8192"
           maxThreads="150"
           minSpareThreads="25"
           maxSpareThreads="75"
           enableLookups="false"
           disableUploadTimeout="true"
           acceptCount="100"
           scheme="https"
           secure="true"
           clientAuth="false"
           sslProtocol="TLS"
           keystoreFile="conf\keystore.jks"
           keystorePass="changeit"
           keystoreType="JKS" />
-->
```

c. Uncomment the **Connector port** section by deleting the leading `<!--` and trailing `-->`.

d. If you specified a custom password when generating the Certificate Keystore, change the text `changeit` to the specified password in the line:

```
keystorePass="changeit"
```

e. Save the changes to the file.

For additional configuration options, refer to the "Apache Jakarta Tomcat 5.5 Servlet/JSP Container - SSL Configuration HOW-TO" at

http://jakarta.apache.org/tomcat/tomcat-5.5-doc/ssl-howto.html

3. To configure Web Reports to operate via SSL:

a. Open the following file in a text editor (*Tomcat must have been started at least once before this file is available)*.

```
<INSTALL_DIR>\jakarta-tomcat-5.5.9\webapps\webetm\WEB-INF\web.xml
```

b. Locate the following section at the end of the file:

```
<user-data-constraint>
    <!--
    To configure WebETM for operation through SSL, change
    the text below from "NONE" to "CONFIDENTIAL"
 -->
 <transport-guarantee>NONE</transport-guarantee>
</user-data-constraint>
```

c. In place of NONE, type CONFIDENTIAL.

d. Save the file.

4. If Tomcat is running, restart it for the change to take effect.

Log File Locations

Log files associated with the Apache Tomcat and ETM Web Reports are stored at the following locations:

- Apache Jakarta Tomcat's log files are created in the following directory:

  <INSTALL_DIR>\jakarta-tomcat-5.5.9\logs

- The ETM Web Reporting Application's log file is created in the following directory by default:

  ..\WINDOWS\system32\logs

Configuring the Tomcat Web Application Manager

The Tomcat Web Application Manager is a web application that comes by default with Apache Tomcat. It displays general server information and lists the web applications currently available and their status. The manager can be used to start, stop, reload, and "undeploy" (delete) the web applications. This tool can be useful for troubleshooting.

You can access the Tomcat Web Application Manager by navigating to the Tomcat **Welcome** page and clicking the **Tomcat Manager** link, or by using the shortcut on the Start menu of the Tomcat host computer.

A username and password are required to access to the Tomcat Manager web application. By default, no user exists to access the application and must be added.

To add a user

1. Open the following file in a text editor:

   <INSTALL_DIR>jakarta-tomcat-5.5.9\conf\tomcat-users.xml

2. Locate the following line:

```
<user username="role1" password="tomcat" roles="role1"/>
```

3. After that line, add the line:

```
<user username="<USERNAME>" password="<PASSWORD>" roles="manager"/>
```

replacing <USERNAME> with the username you are assigning and <PASSWORD> with the password you are assigning. For example:

```
<user username="tomcat-man" password="8&2Rten" roles="manager"/>
```

4. Save the changes to the file.
5. Restart the Apache Tomcat Service.

   Now you can navigate to the Tomcat Manager web application and use the above username and password to access the application.

Additional References

Useful reference information is available at the links listed below.

- Apache Jakarta Tomcat 5.5 Servlet/JSP Container - Documentation Index

  http://jakarta.apache.org/tomcat/tomcat-5.5-doc/index.html

- Apache Jakarta Tomcat 5.5 Servlet/JSP Container - SSL Configuration HOW-TO

http://jakarta.apache.org/tomcat/tomcat-5.5-doc/ssl-howto.html

- Java Runtime Environment 1.5.0 - keytool - Key and Certification Management Tool

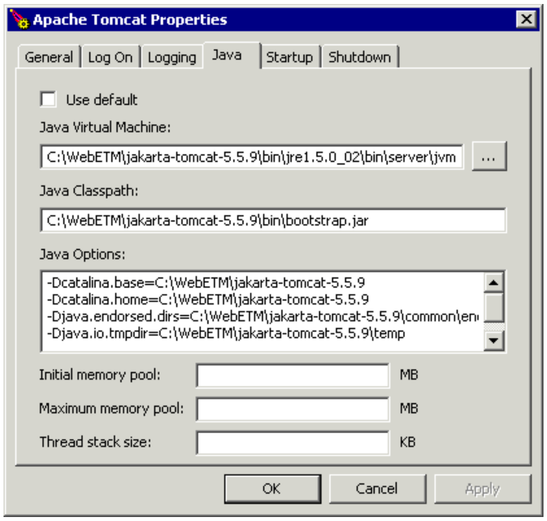
http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html

Increasing the Available Memory Pool for the Web Portal

By default, the Tomcat server allocates a maximum memory pool of 64 MB. In environments where many users are expected to simultaneously access the Web Portal, increase the maximum memory pool to 256 MB or greater to avoid out of memory errors.

To increase the maximum memory pool

1. Stop the Tomcat service, if running.
2. From the **SecureLogix** shortcut on the Windows **Start** menu, point to **ETM Web Portal | Apache Tomcat 5.5 | Configure Tomcat**. The **Apache Tomcat Properties** dialog box appears.
3. Click the **Java** tab.



☐ Use default

Java Virtual Machine: C:\WebETM\jakarta-tomcat-5.5.9\bin\jre1.5.0_02\bin\server\jvm

Java Classpath: C:\WebETM\jakarta-tomcat-5.5.9\bin\bootstrap.jar

Java Options:

```
-Dcatalina.base=C:\WebETM\jakarta-tomcat-5.5.9
-Dcatalina.home=C:\WebETM\jakarta-tomcat-5.5.9
-Djava.endorsed.dirs=C:\WebETM\jakarta-tomcat-5.5.9\common\en
-Djava.io.tmpdir=C:\WebETM\jakarta-tomcat-5.5.9\temp
```

Initial memory pool: MB

Maximum memory pool: MB

Thread stack size: KB

4. In the **Maximum memory pool** box, type a value of 256 or greater.
5. Click **OK**.
6. Restart the Tomcat service.

Accessing the ETM® Web Portal

If the Web Portal is integrated with your existing web server, ask your web server administrator for the URL to access the application.

If you installed the Tomcat implementation, use the following information to access the Web Portal. For convenience, a shortcut is also provided in the **Start** menu of the computer where the Web Portal is installed for accessing the local ETM Web Portal application.

By default, Apache Tomcat serves the application on the default http port: 80. The correct URL to use to access the Web Portal depends on whether you have enabled Anonymous Login:

- If login is required, use the following URL:

  http://<*hostname or IP address*>/webetm

  For example, if Apache Tomcat is running on a host computer with the hostname **www.abc-corp.com**, then the URL would be:

  http://www.abc-corp.com/webetm

- If anonymous login is enabled, use the following URL:

  http://<hostname or IP address/webetm/anonymouslogin

If SSL has been configured, you are automatically redirected from the above address to the secure connection when accessing the ETM Web Portal. To access the SSL connection directly, however, the following URL works for the default SSL port of 8443:

https://<*hostname or IP address*>:8443/webetm

Appendix A: Appliance Technical Specifications, Connectors, and Pinouts

Knowledge Base

See the Knowledge Base for all Tech Spec sheets.

Please see the SecureLogix Knowledge Base for Technical Specifications for all SecureLogix Corporation products.

http://support.securelogix.com/knowledgebase.htm
keyword: **tech spec**

Model 1024 Appliance Specs

Technical Specifications

The following are the technical specifications for the ETM 1024 Appliances.

ETM® 1024 Appliance Technical Specifications	
Processor	
CPU	200 MHz Motorola MPC8241
Bus speed	100 MHz Asynchronous Bus
PCI Bus speed/width	33 MHz/32-bit
DSP	4 x 200 MHz Texas Instruments TMS320VC5510.
Memory	
RAM	64 MB
SRAM (NVRAM)	256 bytes (for configuration parameters).
Interfaces	
Ethernet Data Network Interface:	RJ-45, 10 Mbps or 100Mbps
Console and SMDR/CDR Interfaces	(2) RJ-45 – RS-232C – DCE, Asynchronous up to 115 kbps
Expansion Slots	(2 standard size) PMC daughter-board with front-panel I/O access
Telephony Interface	RJ-21X

ETM® 1024 Appliance Technical Specifications, continued

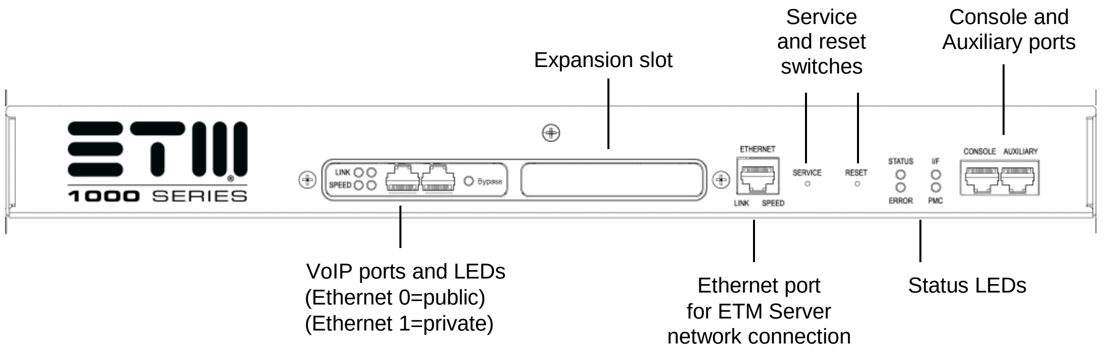
ETM® 1024 Appliance Technical Specifications	
Storage	
Compact Flash	64 MB minimum
Environment	
AC Input	100-240 VAC, 50/60 Hz
Input Current	195 mA
Heat Output	76.5 BTU/hr typical
Fuse	1.6A, 250V
Connection	IEC Connector
Dimensions	1.75” H x 16.9” W x 13” D
Weight	11 lbs
Mounting	Desktop, 19” Rack, or Wall-Mount
Operating Temperature	32 to 104 F (0 to 40 C)
Storage Temperature	-4 to 158 F (-20 C to +70 C)
Telephony Specifications	
Number of Lines	12/24
REN	0.1B
Line Supervision Types	Loop Start, Ground Start, Loop Reverse Battery (for DID only)
Address Signaling Types	DTMF, MF and Pulse Dialing
Signaling Protocols	DID/DNIS, ANI, Caller ID
Line Protection	FCC Part 68 Type A & B (1500V Lightning), Fused Input/Output
Meets or Exceeds the Following Certifications and Approvals	
Telephone Network	FCC Part 68, Industry Canada CS-03, TBR-21, JATE
EMI/EMC	FCC Part 15, ICES-003, EN55022, EN55024, CISPR 22
Safety	CB Scheme (EN/IEC60950), UL /cUL 60950
Marks and Approvals	FCC Part 15, FCC Part 68, JATE, Industry Canada, CE Mark, UL/cUL

Connectors and Pinouts

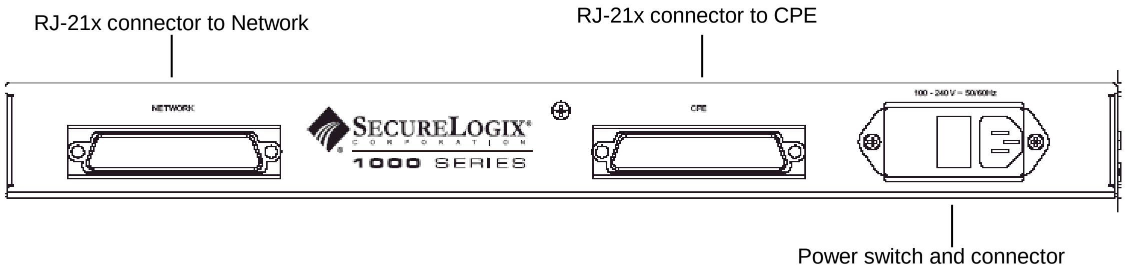
Descriptions and pinouts of the telco connectors on the ETM 1024 Appliances are provided below.

Note: The **Ethernet**, **Console**, and **Auxiliary** port connectors are identical to those on the 3200. The VoIP port connectors (**Ethernet 0** and **Ethernet 1**) are identical to the Management Server Ethernet port.

Front of Chassis

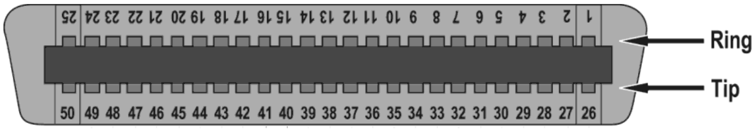

Expansion slot
Service and reset switches
Console and Auxiliary ports
ETM
1000 SERIES
LINK
SPEED
Bypass
ETHERNET
LINK
SPEED
SERVICE
RESET
STATUS
I/F
ERROR
PMC
CONSOLE
AUXILIARY
VoIP ports and LEDs (Ethernet 0=public) (Ethernet 1=private)
Ethernet port for ETM Server network connection
Status LEDs

Back of Chassis



ETM® 1024 Appliance Telephone Network Connector Pinouts

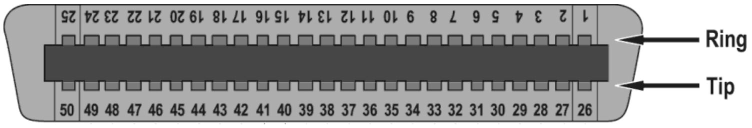
The Network connector on an ETM 1024 Appliance is an RJ-21X connector to connect to the telephone network.



Pin	Wire Color	Description	Pin	Wire Color	Description
1	Blue/White	Ring Channel 1 to Network	26	White/Blue	Tip Channel 1 to Network
2	Orange/White	Ring Channel 2 to Network	27	White/Orange	Tip Channel 2 to Network
3	Green/White	Ring Channel 3 to Network	28	White/Green	Tip Channel 3 to Network
4	Brown/White	Ring Channel 4 to Network	29	White/Brown	Tip Channel 4 to Network
5	Slate/White	Ring Channel 5 to Network	30	White/Slate	Tip Channel 5 to Network
6	Blue/Red	Ring Channel 6 to Network	31	Red/Blue	Tip Channel 6 to Network
7	Orange/Red	Ring Channel 7 to Network	32	Red/Orange	Tip Channel 7 to Network
8	Green/Red	Ring Channel 8 to Network	33	Red/Green	Tip Channel 8 to Network
9	Brown/Red	Ring Channel 9 to Network	34	Red/Brown	Tip Channel 9 to Network
10	Slate/Red	Ring Channel 10 to Network	35	Red/Slate	Tip Channel 10 to Network
11	Blue/Black	Ring Channel 11 to Network	36	Black/Blue	Tip Channel 11 to Network
12	Orange/Black	Ring Channel 12 to Network	37	Black/Orange	Tip Channel 12 to Network
13	Green/Black	Ring Channel 13 to Network	38	Black/Green	Tip Channel 13 to Network
14	Brown/Black	Ring Channel 14 to Network	39	Black/Brown	Tip Channel 14 to Network
15	Slate/Black	Ring Channel 15 to Network	40	Black/Slate	Tip Channel 15 to Network
16	Blue/Yellow	Ring Channel 16 to Network	41	Yellow/Blue	Tip Channel 16 to Network
17	Orange/Yellow	Ring Channel 17 to Network	42	Yellow/Orange	Tip Channel 17 to Network
18	Green/Yellow	Ring Channel 18 to Network	43	Yellow/Green	Tip Channel 18 to Network
19	Brown/Yellow	Ring Channel 19 to Network	44	Yellow/Brown	Tip Channel 19 to Network
20	Slate/Yellow	Ring Channel 20 to Network	45	Yellow/Slate	Tip Channel 20 to Network
21	Blue/Violet	Ring Channel 21 to Network	46	Violet/Blue	Tip Channel 21 to Network
22	Orange/Violet	Ring Channel 22 to Network	47	Violet/Orange	Tip Channel 22 to Network
23	Green/Violet	Ring Channel 23 to Network	48	Violet/Green	Tip Channel 23 to Network
24	Brown/Violet	Ring Channel 24 to Network	49	Violet/Brown	Tip Channel 24 to Network
25	Slate/Violet	Not used	50	Violet/Slate	Not used

ETM® 1024 Appliance CPE Connector Pinout

The CPE connector on an ETM 1024 Appliance is an RJ-21X connector.



Pin	Wire Color	Description	Pin	Wire Color	Description
1	Blue/White	Ring Channel 1 to CPE	26	White/Blue	Tip Channel 1 to CPE
2	Orange/White	Ring Channel 2 to CPE	27	White/Orange	Tip Channel 2 to CPE
3	Green/White	Ring Channel 3 to CPE	28	White/Green	Tip Channel 3 to CPE
4	Brown/White	Ring Channel 4 to CPE	29	White/Brown	Tip Channel 4 to CPE
5	Slate/White	Ring Channel 5 to CPE	30	White/Slate	Tip Channel 5 to CPE
6	Blue/Red	Ring Channel 6 to CPE	31	Red/Blue	Tip Channel 6 to CPE
7	Orange/Red	Ring Channel 7 to CPE	32	Red/Orange	Tip Channel 7 to CPE
8	Green/Red	Ring Channel 8 to CPE	33	Red/Green	Tip Channel 8 to CPE
9	Brown/Red	Ring Channel 9 to CPE	34	Red/Brown	Tip Channel 9 to CPE
10	Slate/Red	Ring Channel 10 to CPE	35	Red/Slate	Tip Channel 10 to CPE
11	Blue/Black	Ring Channel 11 to CPE	36	Black/Blue	Tip Channel 11 to CPE
12	Orange/Black	Ring Channel 12 to CPE	37	Black/Orange	Tip Channel 12 to CPE
13	Green/Black	Ring Channel 13 to CPE	38	Black/Green	Tip Channel 13 to CPE
14	Brown/Black	Ring Channel 14 to CPE	39	Black/Brown	Tip Channel 14 to CPE
15	Slate/Black	Ring Channel 15 to CPE	40	Black/Slate	Tip Channel 15 to CPE
16	Blue/Yellow	Ring Channel 16 to CPE	41	Yellow/Blue	Tip Channel 16 to CPE
17	Orange/Yellow	Ring Channel 17 to CPE	42	Yellow/Orange	Tip Channel 17 to CPE
18	Green/Yellow	Ring Channel 18 to CPE	43	Yellow/Green	Tip Channel 18 to CPE
19	Brown/Yellow	Ring Channel 19 to CPE	44	Yellow/Brown	Tip Channel 19 to CPE
20	Slate/Yellow	Ring Channel 20 to CPE	45	Yellow/Slate	Tip Channel 20 to CPE
21	Blue/Violet	Ring Channel 21 to CPE	46	Violet/Blue	Tip Channel 21 to CPE
22	Orange/Violet	Ring Channel 22 to CPE	47	Violet/Orange	Tip Channel 22 to CPE
23	Green/Violet	Ring Channel 23 to CPE	48	Violet/Green	Tip Channel 23 to CPE
24	Brown/Violet	Ring Channel 24 to CPE	49	Violet/Brown	Tip Channel 24 to CPE
25	Slate/Violet	Not used	50	Violet/Slate	Not used

Model 1090 Appliance

Technical Specifications

The following are the technical specifications for the ETM 1090 Appliances:

ETM® 1090 Appliance Technical Specifications	
Processor	
CPU	200 MHz Motorola MPC8241
Bus speed	100 MHz Asynchronous Bus
PCI Bus speed/width	33 MHz/32-bit
DSP	4 x 200 MHz Texas Instruments TMS320VC5510.
Memory	
RAM	64 MB with ECC
SRAM (NVRAM)	256 bytes (for configuration parameters).
Interfaces	
Ethernet Data Network Interface:	RJ-45, 10 Mbps or 100Mbps
Console and SMDR/CDR Interfaces	(2) RJ-45 – RS-232C – DCE, Asynchronous up to 115 kbps
Expansion Slots	(2 standard size) PMC daughter-board with front-panel I/O access
Telephony Interface	RJ-48C
Storage	
Compact Flash	64 MB minimum
Environment	
AC Input	100-240 VAC, 50/60 Hz
Input Current	195 mA
Heat Output	76.5 BTU/hr typical
Fuse	1.6A, 250V
Connection	IEC Connector
Dimensions	1.75” H x 16.9” W x 13” D
Weight	11 lbs
Mounting	Desktop, 19” Rack, or Wall-Mount
Operating Temperature	32 to 104 F (0 to 40 C)

ETM® 1090 Appliance Technical Specifications, continued

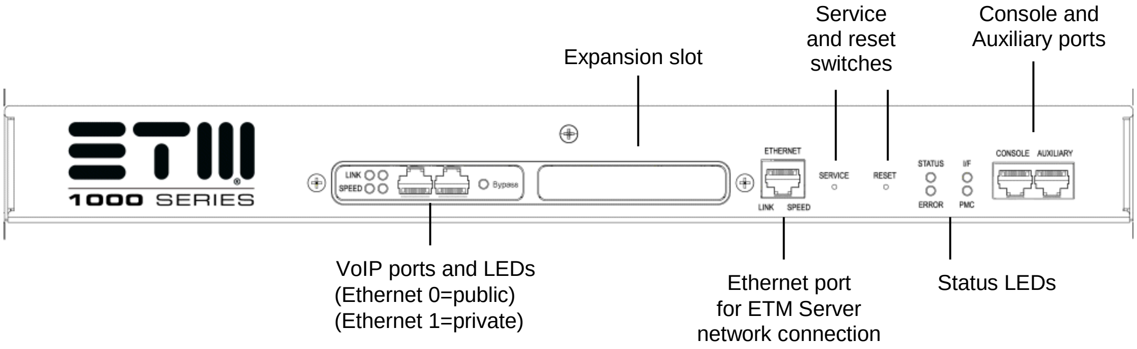
ETM® 1090 Appliance Technical Specifications	
Storage Temperature	-4 to 158 F (-20 C to +70 C)
Telephony Specifications	
Number of Lines	One T1, North American ISDN PRI, or European ISDN PRI Circuit
Line Rate	1.544 or 2.048 Mbps
Line Framing	SF (D4), ESF, CRC 4
Line Code	AMI, B8ZS, HDB3
Input Signal	0 to -36 dB
Line Build Out	T1: Short Haul 0-660ft (110 ft increments), T1: Long Haul 0, -7.5, -15, -22.5 dB, E1: 120 Ohm
Keep Alive	Unframed All Ones (AIS)
Network/CO Activation Alarms	LOS and/or Loss of Frame (Red), RAI (Yellow), AIS (Blue)
Equipment/PBX Activation	LOS and/or Loss of Frame (Red), RAI (Yellow), AIS (Blue)
Reporting	Panel LEDs (Network/CO Red and Yellow, CPE/PBX Red and Yellow), ETM Management Server Diagnostic Messages
Line Supervision Types	Loop Start, Ground Start, Wink Start, Immediate Start, ISDN PRI, R1
Address Signaling Types	DTMF, MF and Pulse Dialing
Signaling Protocols	DID/DNIS, ANI, Caller ID
ISDN Variants	N.A. PRI: NI-2, 4ESS, 5ESS, DMS100 European PRI: NET5, DASS2, DPNSS, QSIG
SS7 Variant	ANSI, ETSI
Other Variants	N.A. PRI: Backup D-Channel and NFAS configurations supported
Line Protection	FCC Part 68 Type A & B (1500V Lightning), Fused Input/Output
Meets or Exceeds the Following Certifications and Approvals	
Telephone Network	FCC Part 68, Industry Canada CS-03, TBR-4, TBR-12, TBR-13
EMI/EMC	FCC Part 15, ICES-003, EN55022, EN55024, CISPR 22
Safety	CB Scheme (EN/IEC60950), UL /cUL 60950
Marks and Approvals	FCC Part 15, FCC Part 68, Industry Canada, CE Mark, UL/cUL
Other Country Approvals	Turkey

ETM® 1090 Appliance Connectors and Pinouts

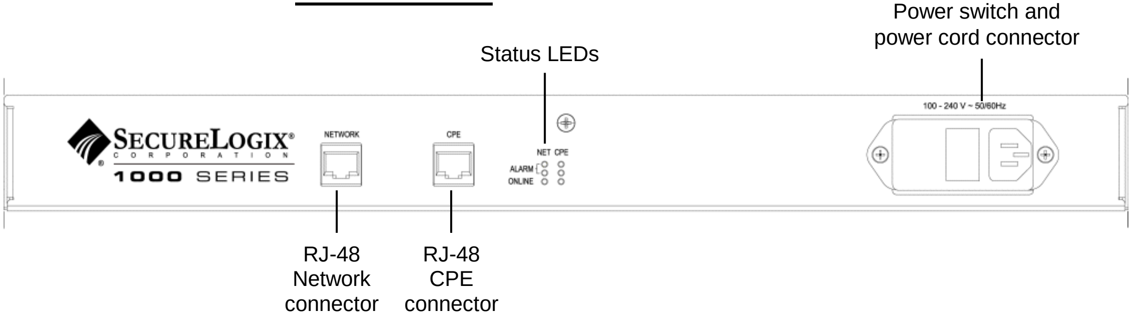
The pinouts on the ETM 1090 Appliance are identical to those in the ETM 2100/3200 Appliances. The VoIP port pinouts are identical to the Ethernet port. The **Network** and **CPE** ports are identical to the **CO** and **PBX** ports on the 2100/3200 Appliances. See "Connector Pinout" on page 185 for descriptions of each connector.

The ETM 1090 Appliance chassis is illustrated below.

Front of chassis


Expansion slot
Service and reset switches
Console and Auxiliary ports
ETM
1000 SERIES
LINK
SPEED
Bypass
ETHERNET
SERVICE
RESET
STATUS
I/F
ERROR
PMC
CONSOLE
AUXILIARY
LINK
SPEED
VoIP ports and LEDs (Ethernet 0=public) (Ethernet 1=private)
Ethernet port for ETM Server network connection
Status LEDs

Rear of chassis



Model 2100 and 3200 Appliances

The ETM 2100 Appliance contains a power supply, a fan unit, and one hot-swappable board set.

The ETM 3200 Appliance contains two hot-swappable power supplies, a removable fan assembly containing 3 cooling fans, and 1-to-4 hot-swappable board sets.

Each board set includes:

- Controller Card, inserted into the front of the Appliance, which includes a PMC "piggy-backed" onto the Controller Card:
- Digital Trunk Interface, inserted into the back of the Appliance.

Technical Specifications

The following are the technical specifications for the ETM 2100 and 3200 Controller Cards:

8540 Controller Card Technical Specifications	
Processor	
CPU	PowerPC, MPC8541, 833 MHz, PowerQUICC-III
DSP	5510, 200 MHz/400 MIPS, v2.2, 1.6V
Memory	
RAM	512 MB with ECC
SRAM (NVRAM)	512K bytes (for configuration parameters).
Interfaces	
Ethernet Data Network Interfaces:	(2) RJ-45, 10/100/1000 Mbps
Console and SMDR/CDR Interfaces	(2) RJ-45 – RS-232C – DCE, Asynchronous up to 115 kbps
Expansion Slots	Unused
Telephony Interface	RJ-48C
Storage	
Compact Flash	8 GB minimum
Environment	
AC Input	100-240 VAC, 50/60 Hz
Input Current (2100)	500mA

8540 Controller Card Technical Specifications, continued

8540 Controller Card Technical Specifications	
Input Current (3200)	1 board set: 650mA, 2 board sets: 950mA, 3 board sets: 1.250A, 4 board sets: 1.550A
Heat Output (2100)	196.2 BTU/hr typical
Heat Output (3200)	1 board set: 255.1 BTU/hr typical, 2 board sets: 372.8 BTU/hr typical, 3 board sets: 490.5 BTU/hr typical, 4 board sets: 608.2 BTU/hr typical
Fuse (AC)	3A, 250V
Connection (AC)	IEC Connector
DC Input (3200 only)	-36 to -72 VDC
DC Input Current	1 board set: 1.100A, 2 board sets: 1.450A, 3 board sets: 2.100A, 4 board sets: 2.750A
DC Heat Output	1 board set: 180.1 BTU/hr typical, 2 board sets: 237.5 BTU/hr typical, 3 board sets: 344.0 BTU/hr typical, 4 board sets: 450.4 BTU/hr typical
Fuse (DC)	8A, 250V
Connection (DC)	screw lug terminals
Power Supply	Dual redundant hot-swappable
Dimensions (2100)	1.75” H x 17.5” W x 12” D
Dimensions (3200)	3.5” H x 17.5” W x 12” D
Weight (2100)	10 lbs.
Weight (3200 AC)	1 board set: 19 lbs, 2 board sets: 20 lbs, 3 board sets: 21 lbs, 4 board sets: 22 lbs
Weight (3200 DC)	1 board set: 19 lbs, 2 board sets: 20 lbs, 3 board sets: 21 lbs, 4 board sets: 22 lbs
Mounting	Desktop, 19” Rack, or Wall-Mount
Operating Temperature	32 to 104 F (0 to 40 C)
Storage Temperature	-4 to 158 F (-20 C to +70 C)
Fans	3 fans on a removable fan tray (3200)
Telephony Specifications	
Number of Lines	Up to 4 (2100) or 16 (3200) T1, North American ISDN PRI, or European ISDN PRI Circuits
Line Rate	1.544 or 2.048 Mbps
Line Framing	SF (D4), ESF, CRC 4
Line Code	AMI, B8ZS, HDB3
Input Signal	0 to -36 dB

8540 Controller Card Technical Specifications, continued

8540 Controller Card Technical Specifications	
Line Build Out	T1: Short Haul 0-660ft (110 ft increments), T1: Long Haul 0, -7.5, -15, -22.5 dB, E1: 120 Ohm
Keep Alive	Unframed All Ones (AIS)
Network/CO Activation Alarms	LOS and/or Loss of Frame (Red), RAI (Yellow), AIS (Blue)
Equipment/PBX Activation	LOS and/or Loss of Frame (Red), RAI (Yellow), AIS (Blue)
Reporting	Panel LEDs (Network/CO Red and Yellow, CPE/PBX Red and Yellow), ETM Management Server Diagnostic Messages
Line Supervision Types	Loop Start, Ground Start, Wink Start, Immediate Start, ISDN PRI, R1
Address Signaling Types	DTMF, MF and Pulse Dialing
Signaling Protocols	DID/DNIS, ANI, Caller ID
ISDN Variants	N.A. PRI: NI-2, 4ESS, 5ESS, DMS100 European PRI: NET5, DASS2, DPNSS, QSIG
SS7 Variant	ANSI, ETSI
Other Variants	N.A. PRI: Backup D-Channel and NFAS configurations supported
Line Protection	FCC Part 68 Type A & B (1500V Lightning), Fused Input/Output
Meets or Exceeds the Following Certifications and Approvals	
Telephone Network	FCC Part 68, Industry Canada CS-03, CTR-4, JATE, MIC
EMI/EMC	FCC Part 15, ICES-003, EN55022, EN55024, CISPR 22
Safety	CB Scheme (EN/IEC60950), UL /cUL 60950
Marks and Approvals	FCC Part 15, FCC Part 68, JATE, Industry Canada, CE Mark, UL/cUL, MIC
Other Country Approvals	Turkey

ETM® 2100 and 3200 Appliance Board Sets

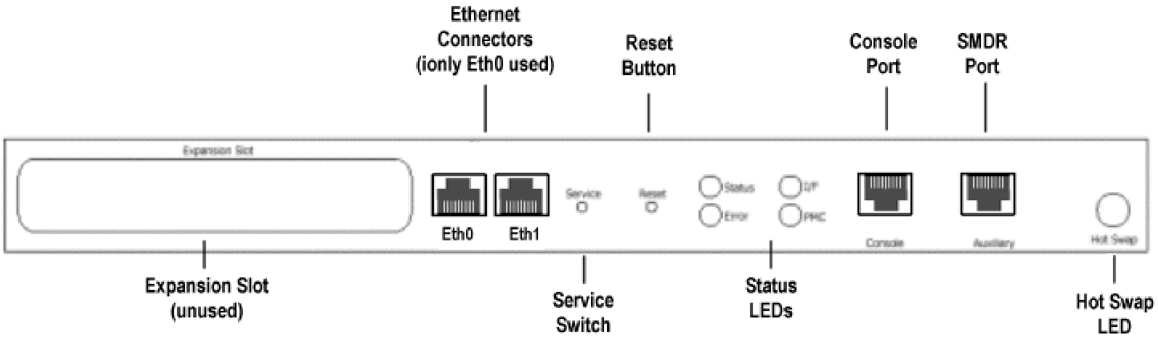
Each four-Span, hot-swappable board set includes:

- Two Ethernet interfaces, RJ-45 10/100/1000 Mbps. Only Eth0 is used.
- Two serial interfaces: RJ-48 Console and Auxiliary ports.
- Eight line interfaces: 4 RJ-48 CO, 4 RJ-48 PBX.
- Diagnostic LEDs.

Controller Card

The Controller Card is accessed from the front of the Appliance. The Controller Card contains the **Ethernet** ports, **Console** and **Auxiliary** serial ports, **Service** and **Reset** buttons, and LEDs that show the status of the system.

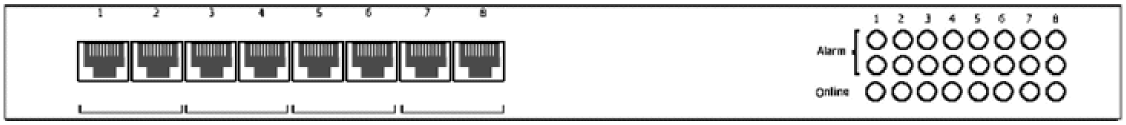
The illustration below shows the access panel of the Controller Card.



Digital Trunk Interface

The Digital Trunk Interface connects to the telephone lines via 8 RJ48 telco connectors, 2 per Span. Eight sets of LEDs that correspond to the numbered telco connectors indicate alarm status and whether each Span is inline.

The illustration below shows the ports and LEDs on the Digital Trunk Interface.

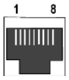


- Pair 1-Port 1 to CO, Port 2 to PBX
- Pair 2-Port 3 to CO, Port 4 to PBX
- Pair 3-Port 5 to CO, Port 6 to PBX
- Pair 4-Port 7 to CO, Port 8 to PBX

ETM® 1090, 2100, and 3200 Appliance Connector Pinouts

Pinouts for each of the connectors on the ETM 1090, 2100, and 3200 Appliances are provided below.

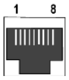
Ethernet Port Pinouts



A standard RJ-45 jack is provided on each 1024 and 1090 Appliance and 3200 and 2100 Controller Card for connection to an Ethernet 10/100/1000 Mbps network.

Pin	Name	Description	Pin	Name	Description
1	Tx +	Transmit +	5	N/C	Not Used
2	Tx -	Transmit -	6	Rx-	Receive -
3	Rx +	Receive +	7	N/C	Not Used
4	N/C	Not Used	8	N/C	Not Used

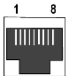
Auxiliary and Console Port Pinout



A standard RJ-45 jack is provided on each 1024 and 1090 Appliance and 3200 and 2100 Controller Card for Console (serial) port and Auxiliary (SMDR/CDR) connection.

Pin	Name	Description	Pin	Name	Description
1	RTS	Request to Send	5	GND	Ground
2	DTR	Data Terminal Ready	6	RXD	Receive Data
3	TXD	Transmit Data	7	DSR	Data Send Ready
4	GND	Ground	8	CTS	Clear to Send

CO Port Pinout



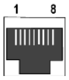
Each Digital Trunk Interface (at the back of the Appliance) has 4 pair of RJ-48 connectors, 1 pair per Span, labeled 1-8, for connection to the telco network. Connectors 1, 3, 5, and 7 connect to the Spans from the CO.

This pinout also applies to the **Network** port on the 1090 Appliance

See “Digital Trunk Interface” on page 184 for information about Span pairs.

Pin	Name	Description	Pin	Name	Description
1	R1	Ring 1 - Receive +	5	T	Tip - Transmit -
2	T1	Tip 1 - Receive -	6	N/C	Not Used
3	N/C	Not Used	7	N/C	Not Used
4	R	Ring - Transmit +	8	N/C	Not Used

PBX Port Pinout



Each Digital Trunk Interface (at the back of the Appliance) has 4 pair of RJ-48 connectors, 1 pair per Span, labeled 1-8, for connection to the telco network. Connectors 2, 4, 6, and 8 connect to the spans from the PBX.

This pinout also applies to the **CPE** port on the 1090 Appliance

See “Digital Trunk Interface” on page 184 for information about Span pairs.

Pin	Name	Description	Pin	Name	Description
1	R1	Ring 1 - Transmit +	5	T	Tip - Receive -
2	T1	Tip 1 - Transmit -	6	N/C	Not Used
3	N/C	Not Used	7	N/C	Not Used
4	R	Ring - Receive +	8	N/C	Not Used

Appendix B: Removing and Replacing TDM Appliance Components

Removing and Replacing TDM Appliance Components

CAUTION 1000-series Appliances contain no user-serviceable parts. Do not open the chassis.

IMPORTANT Before you begin any hardware maintenance, read the suggestions and warnings in the *ETM® System Safety and Regulatory Information*, provided with your Appliances, to ensure equipment and personnel safety.

In the ETM 2100 and 3200 Appliances, the Controller Card and Digital Trunk Interface can be removed and installed without powering off the chassis and without disrupting service to the other Card sets. In the 3200 Appliances, the fan unit and power supplies can also be removed and replaced without powering off the chassis.

⚠ ***WARNING*** The Controller Card supplies power to the Digital Trunk Interface. Do not remove a Digital Trunk Interface from a powered chassis without first removing the Controller Card to which it is connected. Removing a Digital Trunk Interface without first removing the Controller Card can damage both Cards and/or the chassis. Review the following procedures before removing any Cards.

3200 Appliance Card Insertion Order Important

A Controller Card must be present in the system slot (the bottom slot) of the ETM 3200 Appliance for proper operation. The Controller Card in this slot serves as the system controller for the unit. The system Controller Card controls communication on the cPCI backplane, and parks the PCI bus when the bus is idle.

Cards need not be continuously installed from the bottom up, but a Card set MUST be present in the lowest slot. Hot-swapping the system Controller Card disables communication on the cPCI backplane during the time it is removed, but otherwise does not impair operation. Promptly replace the Card.

Basic ESD Precautions

The Cards in the ETM Appliances are designed to be resilient to electrostatic discharge (ESD). In addition, the Cards and enclosures are designed to safely discharge ESD when the Cards are inserted or ejected. However, you should take basic ESD precautions when handling the Cards as described below:

- Use antistatic bags when transporting Cards away from the Appliance.
- Before taking a Card out of a bag or ejecting a Card from an Appliance, ground yourself by touching an unpainted surface on the Appliance or rack.
- Hold the Cards using the black ejector latches. Avoid touching the Card surfaces, components, or connectors when the Cards are out of the Appliance.

If you follow these basic guidelines, it should not be necessary to use grounding straps or mats when removing or installing Appliance Cards.

Removing and Replacing Cards

The Controller Card and Digital Trunk Interface in the ETM 2100 and 3200 Appliances are designed to be removed and replaced without disrupting the operation of other components in the Appliance. The Controller Card and Digital Trunk Interface work together as a unit and require a specific, ordered procedure to remove and install them. See the sections below for the proper procedures for removing and replacing the Cards.

⚠ ***WARNING*** Do not remove the DSP PMC from the Controller Card unless directed to do so by SecureLogix Customer support.

Removing a Controller Card

To remove a Controller Card from the chassis

1. On the Controller Card, at the front of the Appliance, remove the Ethernet and SMDR cables.
2. Press the red button on each of the two black latches on the Card.
3. Wait for the hot-swap LED on the Card to illuminate, indicating that the operating system on the Card has halted.
4. Remove the screws next to the latches on the Card, flip the latches out, away from the Card, and pull the Card from the chassis.

If you are also removing the Digital Trunk Interface, see "Removing a Digital Trunk Interface" on page 189. For instructions for reinstalling the Controller Card, see "Inserting a Controller Card" on page 189.

Removing a Digital Trunk Interface

To remove a Digital Trunk Interface from the chassis

1. Before removing the Digital Trunk Interface, remove the Controller Card as described in "Removing a Controller Card" on page 188.

WARNING Never remove the Digital Trunk Interface from a powered chassis until after you remove the Controller Card.

Never insert the Controller Card back into the chassis until after the Digital Trunk Interface has been replaced. See "Inserting a Digital Trunk Interface" on page 189 for the procedure to reinstall the Digital Trunk Interface.

2. On the Digital Trunk Interface (at the back of the Appliance), remove the screws next to the latches, flip the latches out, away from the Card, and pull the Card from the chassis.

Inserting a Digital Trunk Interface

To install a Digital Trunk Interface

1. Be certain that the corresponding Controller Card is ***not*** inserted.
2. At the back of the Appliance, insert the Digital Trunk Interface. The components on the Card should face up.
3. Flip the latches inward and install the screws to secure the Digital Trunk Interface.
4. After installing the Controller Card as described below, see "Connecting the Telco Cable(s)" on page 150 for instructions for connecting the telco cables, if necessary.

Inserting a Controller Card

This procedure is for reinserting a configured Controller Card that was temporarily removed in order to remove the Digital Trunk Interface. If you are inserting a new Controller Card, see "Replacing a Controller Card" on page 190 for the complete process for replacing and configuring the Controller Card.

To insert a Controller Card

1. Be certain that the corresponding Digital Trunk Interface is present in its slot.
2. At the front of the Appliance, insert the Controller Card into the slot that corresponds to the Digital Trunk Interface. The components on the Card should face up.
3. Flip the latches inward and install the screws to secure the Controller Card.
4. The blue hot-swap LED should go off, indicating that power is applied to the Controller Card.
5. Attach the Ethernet cable.

See "Verifying ETM® 1090/2100/3200 Appliance Operation" on page 153 for instructions for verifying that the Card set is operating normally.

Replacing a Controller Card

The instructions below provide step-by-step procedures for replacing and configuring a Controller Card in an ETM 2100 or 3200 Appliance.

To replace a Controller Card

1. Replace the Card, following correct hot-swap procedures as follows:

   - To remove the Card:

     a. Disconnect the Ethernet cable (and SMDR cable, if applicable).

     b. At the front of the Appliance, press the red button on each of the two black latches on the Controller Card.

     c. Wait for the blue hot-swap LED on the front of the Card to illuminate, indicating that the operating system on the Card has halted.

     d. Remove the screws next to the latches on the Controller Card, flip the latches out, away from the Card, and pull the Controller Card from the chassis.

   - To replace the Card:

     a. Ensure that the corresponding Digital Trunk Interface is present in its slot.

     b. At the front of the Appliance, insert the Controller Card into the slot that corresponds to the Digital Trunk Interface. The components on the Card should face up.

     c. Flip the latches inward and install the screws to secure the Controller Card.

     d. The blue hot-swap LED should go off, indicating that power is applied to the Controller Card.

     e. If you are not changing the Span types on the Card, connect the Ethernet cable (and SMDR cable, if applicable).

See “Changing the Span Type” on page 57 if necessary.

IMPORTANT If you need to change the Span Type of any Span, it is recommended that you DO NOT connect the Ethernet cable until after you complete Steps 3 and 4. Once the Card connects to the Server, the installation username and password are no longer valid, and the Server expects T1 CAS Spans and refuses connection from those whose type has changed. Should this occur, you can use a username and password defined on the Server to complete direct configuration via the serial connection, and then delete the Card icon in the Performance Manager **Platform Configuration** subtree before performing additional configuration. The Spans will then be allowed to connect.

Unless you use the same IP address as the Card you are replacing, you must add this IP address to the Server's valid IP list via the Performance Manager before the Card can connect to the Server. If necessary, see "Authorize Cards to Connect to the " on page 68.

2. Through a serial connection to the new Card, complete the "out-of-the-box" setup procedures as described in “Configure the TDM Card(s) to Connect to the Management Server” on page 54.
3. Connect the Ethernet cable. The new Card connects and creates a new Card icon in the Performance Manager tree pane, identified by the Card's MAC address. The old Card icon remains; you will delete that after completing configuration. Since the old Card is not physically present, it does not matter that the old and new Card icons contain the same Card IP address.
4. You must connect the Ethernet cable before performing this step, since the Card must be communicating with the Server to perform the software download.

   a. In the Performance Manager, expand the **Platform Configuration** subtree, right-click the Card, and then click **Manage Software.** The **ETM Platform Software Installation** dialog box appears.

   b. In the **Software Package** area, click **Modify**. The **Software Version Selection** dialog box appears.

   c. Click the Appliance software package applicable to your Span type, and then click **OK**.

   d. The packages name appears in the **ETM Platform Software Installation** dialog box, and the **Install** check box is selected. Click **OK** to install the software on the Card.

   IMPORTANT When you download a software package to a Card, it is imperative that you do not reboot or power cycle the Card until the upgrade is complete, or the firmware may become corrupted, rendering the Card inoperable. The Card automatically reboots when the upgrade is complete. If you believe the Card has become unresponsive, be certain that 15 minutes have elapsed since you began the download before you manually power cycle or reboot the Card.

You can view the progress of the software download in the **Diagnostic Log** and **Status Display**.

5. In the Performance Manager tree pane, locate the old icon for the Card you replaced.
6. Change the name of this old Card icon so that you can reuse it for the new Card. For example, append **-OLD** to the Card name.
7. Change the name of each Span attached to the old Card icon so that you can reuse these for the new Spans. For example, append **-OLD** to each Span name.
8. Install the correct World and Local Dial Plans for each new Span.

   IMPORTANT Install the correct Dialing Plans before you move the Spans to their Span Groups or calls may be wrongly terminated when the Voice Firewall Policy is installed!

   - To install the Dialing Plans, right-click the Span(s), click **Manage Dial Plan**, and then select and install the correct files.

9. Complete essential Card configuration.
   a. After the new Card connects to the Management Server, right-click the Card icon in the **Platform Configuration** subtree pane, and then click **Edit Card(s)**.
   b. In the **Card Name** box, type the name for the Card.
   c. Click the **Details** tab and select the correct time zone.
10. Configure the newly connected Spans by importing the configuration from the Span icons you renamed in Step 9.
    a. Right-click the first new Span, and then click **Edit Span(s)**.
    b. At the bottom of the **Edit Span(s)** dialog box, click **Import**, click the renamed Span from which you want to import configuration, and then click **OK**.

The Spans appear in the tree pane in ASCII order. If you want the Spans to appear in Span order, you must name them appropriately.

    c. In the **Name** box on the **General** tab, type the name for the Span.
    d. Click **OK**. The configuration is downloaded to the Span and the Span automatically restarts offline. (Spans always restart in the same state unless you type the command for them to change state. For example, if the Span is offline and you simply restart it, it restarts offline. However, if you type the command to place it inline, it goes inline when you restart it.)
    e. Repeat for each Span.
11. Move the Card to the correct Appliance and the Span(s) to the correct switch and Span Group(s). If the Card you replaced was the SMDR Provider, reselect it in the **Edit Switch** dialog box after you move the Span(s) to the correct switch.

    IMPORTANT Moving the Span into the Span Group automatically installs the active Policies for that Span Group.
12. Verify correct operation by comparing all settings to the old Card and Span icons. In particular, you may need to authorize Telnet clients and change the security posture and DES Key.
13. Place each Span inline. To place a Span inline:
    a. In the Performance Manager tree pane, right-click the Span, and then click **ASCII Management**. (You can select multiple Spans and open a multi-select ASCII Management Interface to place multiple Spans inline simultaneously. To do so, hold down CTRL or SHIFT while selecting the Spans, and then right-click the selection).
    b. In the **Enter Command** box, type: `SPAN INLINE`, and then press ENTER.
    c. In the **Enter Command** box, type RESTART.

14. Confirm that each Span is monitoring calls by viewing call activity in the **Call Monitor**. Verify that phone numbers in the **Call Monitor** are correctly displayed. If not, verify that the correct Dialing Plans were installed in Step 10 and that those Dialing Plans are correctly configured.

15. When proper operation has been confirmed, remove the old Card icon from the **Platform Configuration** subtree.

    - To remove the Card icon, right-click the icon, and then click **Edit Card(s)**. In the **Card Configuration** dialog box, click **Remove**.

16. Follow the shipping instructions provided with the new Card to return the old Card to SecureLogix.

Removing and Replacing a Power Supply

In the ETM 3200 Appliance, if one of the power supplies fails, the second power supply can temporarily handle the load while you replace the failed unit. You can also quickly power off a DC Appliance by pulling both power supplies. You can remove and replace a power supply without powering off the chassis.

To remove and replace a power supply

1. Remove the screws securing the failed power supply to the chassis.
2. Flip up the black latch and pull the power supply out from the chassis.
3. Insert the new power supply into the chassis, aligning the power supply connector with the chassis power supply connector.
4. Flip the latch down and insert the screws to secure the power supply to the chassis.
5. Verify that the Power LED on the front of the power supply is illuminated.

Removing/ Replacing the Fan Unit

To view cabinet temperature at any time, right-click a Card in the Performance Manager tree pane, and then click **Health & Status**.

Elevated cabinet temperature can be an indication that a cooling fan has failed. In the ETM 3200 Appliance, the fan unit can be removed and replaced without turning power off to the chassis.

CAUTION If a fan fails, it is important that you replace it as soon as possible, because the power supplies can cause the chassis temperature to rise quickly. A chassis temperature greater than 70 degrees Celsius could damage components.

To remove/replace the fan unit

1. Loosen the thumbscrew(s) on the fan unit and remove the fan unit from the chassis.
2. Install the new fan unit into the chassis, aligning the connector on the unit with the connector in the chassis, and tighten the thumbscrew(s), securing the fan unit to the chassis.

Low-Level Maintenance Mode

Low-level maintenance and troubleshooting tasks, such as recovering from Card software errors or changing the Span type, can be performed in Fail Safe mode. Fail Safe mode may be required, for example, if the power goes off in the middle of downloading a file to the Card and the software becomes corrupted such that the Card does not boot.

Fail Safe mode does not enable the telecommunications interface; therefore, you can work in Fail Safe mode as if the Card were powered off. You cannot make command-line changes to telecommunications parameters while the Card is in Fail Safe mode. For example, an error message appears if you type the SPAN INLINE command at the Fail Safe prompt.

Fail Safe mode provides network support; therefore, if Card configuration parameters are correct and your network is up, Fail Safe mode allows the Card to connect to the Management Server. This means you can use Fail Safe Mode from the **ASCII Management Interface** or from a **Console** port connection.

Entering Fail Safe Mode

If the network connection between the ETM Server and the Card is up, you can enter Fail Safe Mode from either the **ASCII Management Interface** in the Performance Manager or from a **Console** port connection.

Entering Fail Safe Mode from the ASCII Management Interface

To enter Fail Safe Mode from the ASCII Management Interface

1. In the **Platform Configuration** subtree, right-click the Card and click **ASCII Management**. The **ASCII Management Interface** appears.
2. In the **Enter Command** box, type RESTART FAILSAFE. No indication is given in the **ASCII Management Interface** and the Fail Safe menu does not appear, but the Card restarts at the Fail Safe menu. After one minute without input, the Fail Safe timer causes the Card to automatically enter Fail Safe mode and the **Fail Safe** icon appears next to the Card in the tree pane. You can now type commands to the Card.

Entering Fail Safe Mode from a Console Connection

To enter Fail Safe Mode from a Console connection

1. Attach an RS-232 serial cable from the **Console** port to the appropriate serial port on your terminal.
2. Start the terminal emulation application (such as HyperTerminal) on your terminal. Configure your terminal using the following serial port settings:
   - 115,200 bps
   - 8 data bits
   - 1 stop bit
   - no parity
   - no flow control
3. Press any key on your keyboard to activate the screen.
4. Do one of the following:

The Enable password was defined during Card configuration. For details, see "Initial Card Configuration" on page 54.

   - If the **ETM:1(r/w)>** prompt appears, the Card is in Enable mode and you do not need to log in to the Card. The 1 indicates that you are logged in to Span 1; **(r/w)** indicates that you are in Enable mode. Continue with the next step.
   - If the **USERNAME:** prompt appears:
     a. Type a valid username for this Card and press ENTER.
     b. The **PASSWORD:** prompt appears. Type a valid password for this Card and press ENTER.
     c. The **ETM:>** prompt appears.
     d. If you want to change configuration, you must enter Enable mode. To enter Enable mode, at the **ETM:>** prompt, type Enable.
     e. The **PASSWORD:** prompt for Enable mode appears. Type the Enable mode password.

f. The **ETM:1(r/w)>** prompt appears indicating that you are in Enable mode on Span 1.

The **Error** LED on the Controller Card is illuminated red when the Card is in Fail Safe Mode. The Card enters Fail Safe Mode without affecting the other Cards in the Appliance.

5. Enter Fail Safe mode by doing one of the following:
   - If the Card is communicating, at the **ETM:1(r/w)>** prompt, type:

     ```
     RESTART FAILSAFE
     ```

   - If the Card is panicking or otherwise unresponsive: On the Controller Card at the front of the Appliance, press and hold the Reset button, and then use a thin, non-conducting object to push and hold in the **Service** button. When you depress the **Service** button, release the **Reset** button. Continue holding the **Service** button until the **Status** LED illuminates. (If you release the **Service** button before the **Status** LED illuminates, you enter Last Resort boot mode.)
6. The Fail Safe menu appears on your terminal screen. At the **>** prompt, type the number corresponding to the menu item.

   See "Fail Safe Menu Options" on page 196 for a description of each menu option.

Fail Safe Menu Options

To enter Fail Safe Mode, see "Low-Level Maintenance Mode" on page 194.

The Fail Safe menu offers six options. Type the number of the option at the **>** prompt.

1. **Enter Fail Safe ETM Shell**—Displays the **FS(r/w)>** prompt at which you can execute a limited set of ETM Commands; type `Help` to see the available commands.
2. **Display Configuration Data**—Displays configuration items such as IP address of the Card and telecommunications line format.
3. **Audit Configuration Data**—Tests the configuration data integrity and displays the results of the test.
4. **Erase Configuration Data**—Erases Card and Span configuration (in preparation for reconfiguring); a verify prompt appears at which you must type `Y` to continue. (Typing anything other than `Y` returns you to the prompt without erasing configuration.)
5. **Restart Appliance**—Restarts all Spans on the Card.
6. **Stop Fail Safe ETM Timer**—Disables the time to prevent entering Fail Safe ETM Shell upon timeout.

Appendix C: Span Telco Settings Reference

At-a-Glance Reference Table to TDM Span Telco Settings

(*Not applicable to SIP or UTA Spans*) The table below provides an at-a-glance reference to the available TDM telco settings in the **Span Configuration** dialog box, the TDM Span types to which they apply, their purposes, and the possible results if set incorrectly.

Setting	Tab	Span Type	Purpose	Affects
Call Established Timeout	Telephony	Analog, T1 loop start and ground start	Specifies the time after the last digit is dialed before a call is marked as established.	Should be set to match the CO timeout. Affects Policy enforcement and call monitoring.
Caller ID	Channel Map	T1 CAS, Analog	Indicates whether Caller ID is available on the channel for determining source number on inbound calls.	This check box must be selected or Caller ID will not be used, even if it is available.
Enabled	Channel Map	All except SS7	Indicates whether the Span monitors a particular channel.	Call data is recorded and Policies are enforced only on channels selected in this column.
Extension	Channel Map	All except SS7 a	Maps each channel to a default extension, which is only used if source on outbound calls is unavailable from any other means. SMDR and call data always take precedence over the extension map.	Without values in the extension map, call audit data may be incomplete and the Span may be unable to determine whether the call matches Policy Rules.

Span Telco Settings, continued

Setting	Tab	Span Type	Purpose	Affects
Format Precedence	Channel Map	T1 CAS, T1 PRI, SS7	For incoming calls, determines the selection order for using ADDR, DID, or DNIS as the destination number for Voice Firewall Policy enforcement when multiple values are present in the call data.	Affects Policy enforcement.
Framing Format	T1 Setup, E1 Setup	T1 CAS, E1 PRI, T1 PRI	Must be set to the carrier's setting to ensure signal synchronization.	Improper setting causes telco red alarm, with absence of dial tone.
Incoming Numbering Format	Channel Map	T1 CAS, T1 PRI, SS7	Specifies the format for dial pulse, MF, or DTMF digits received by the PBX from the telephone network during address/destination transmission. * On T1 PRI Spans, this field determines whether incoming calls use Direct Inward Dialing (DID) or normal address digit dialing. * On T1 CAS Spans, this field indicates which DTMF or MF strings are present and the order in which they occur.	If DNIS or DID is used, incoming numbering format must specify that format for the Dialing Plan to create normalized numbers. Affects Policy enforcement.
Line Coding	T1 Setup, E1 Setup	T1 CAS, E1 PRI, T1 PRI	For transmission of binary digits.	Setting must identical at the CO, Span, and PBX. Affects D-channel operation and audio quality; can cause telco red alarm with absence of dial tone.
Line Length to CO	T1 Setup, E1 Setup	T1 CAS, E1 PRI, T1 PRI	Specifies the cable length from the Span to the first transmitter/receiver toward the CO.	Degrades signal quality.
Line Length to PBX	T1 Setup, E1 Setup	T1 CAS, E1 PRI, T1 PRI	Specifies the cable length from the Span to the first transmitter/receiver toward the PBX.	Degrades signal quality.

Span Telco Settings, continued

Setting	Tab	Span Type	Purpose	Affects
Loopback Test Pass-Through Mode	T1 Setup	T1 CAS, T1 PRI, SS7	Enables/disables loopback test Pass-Through mode. The Span activates/ deactivates Pass-Through upon detection of the Loop-Up/Loop-Down codes.	Affects Policy enforcement. When the Pass-Through mode is On, telecom data is transmitted without parsing/monitoring through the Span and Policy is not enforced; D-channel re-establishment and error count threshold checking/logging is disabled; Error count value of 0 is sent to the Management Server. When the Pass-Through mode is Off, telecom data is routed through the Span and Policy is enforced. When the Pass-Through mode is set to Autodetect, Pass-Through is activated when a Loop Up code is detected and deactivated when a Loop-Down code is detected. When Autodetect is selected, you can specify a timeout value.
Outgoing Numbering Format	Channel Map	Analog, T1 CAS, SS7	For outgoing calls, specifies the format for dial pulse, MF, or DTMF digits sent by the PBX to the telephone network during address/destination transmission.	Affects Policy enforcement.
Protocol Variant	PRI	T1 PRI, E1 PRI SS7 Signaling	Interprets D-channel messages.	Affects D-channel operation.
Request Outbound SMDR	Channel Map	All except SS7 signaling links	Indicates whether SMDR data should be used on outbound calls to determine the calling number or to augment the call data in the database.	Affects Policy enforcement, call monitoring, and reporting. The **Request Outbound SMDR** column must be configured before SMDR data is used to determine unknown call data for a channel.
Request Inbound SMDR	Channel Map	Recording Spans	Indicates whether SMDR data should be used on inbound calls for Protected Extension processing. Inbound SMDR is NOT used for Policy processing.	Affects Call Recorder Protected Extension processing. The **Request Inbound SMDR** column must be configured before Protected Extensions can be used.

Span Telco Settings, continued

Setting	Tab	Span Type	Purpose	Affects
Signal Type	Channel Map	All except SS7 signaling links	Set to the line interface signaling associated with the monitored circuit.	Improper setting prevents the Span from evaluating calls against Policies or terminating calls.
Tone Type	Channel Map	Analog, T1 CAS	Set to the incoming digit tone type associated with each channel during ANI, DNIS, or DID transmission.	Affects Policy enforcement and logging.
Trunk Group	Channel Map	All except SS7 signaling links	Optional setting for user convenience. Set to match defined trunk groups at the Appliance location.	Optional setting for user convenience.
Companding	Channel Map	All digital Spans except legacy Appliances	Set to match the companding in use on the Span. (Mu-Law or A-Law)	Improper setting prevents the Span from receiving digits; affects Policy enforcement and call monitoring.

Appendix D: Database Directories and File Names Reference

Directories Created by the Database Creation Script

The database creation script creates the following directory structure, in keeping with the Oracle Flexible Architecture specification:

- <ORACLE_BASE>
- <ORACLE_BASE>\admin\<ORACLE_SID> or <ORACLE_HOME>\admin\<ORACLE_SID>, depending on which exists. If both exist, <ORACLE_BASE>\admin\<ORACLE_SID> will be used. This directory is referred to as <ETM_DB_DIRECTORY> in this document.
- <ETM_DB_DIRECTORY>\adhoc
- <ETM_DB_DIRECTORY>\arch
- <ETM_DB_DIRECTORY>\bdump
- <ETM_DB_DIRECTORY>\cdump
- <ETM_DB_DIRECTORY>\create, where all database creation scripts and log files are placed. Refer to this directory to check for errors and to verify the output while running the **oracle_install.pl** script.
- <ETM_DB_DIRECTORY>\exp
- <ETM_DB_DIRECTORY>\pfile, where the init<ORACLE_SID>.ora initialization files are created.
- <ETM_DB_DIRECTORY>\udump contains user log files.
- <ORACLE_DATA>\<ORACLE_SID> contains data files for the database.

Windows Service Name

When installed on Windows, the Windows Service created for the database has a name in the format:

OracleService<ORACLE_SID>

File Names and File Locations

By default, the locations of the data files are the standard locations as specified by the Oracle Flexible Architecture specification. Unless a special requirement is dictated by the installation, it is not necessary to change the file locations. Unless a specific site requires you to conform to a specific naming convention, it is not necessary to change the default file names of the data files.

Value	Description	Default Value(s)s	Default Location
Redo log files	The scripts create three redo log files.	redo01.log, redo02.log, redo03.log	<ORADATA>/<SID>
System data files	The data file for the System tablespace	system01.dbf	<ORADATA>/<SID>
Temp data file	The data file for the Temp tablespace.	temp01.dbf	<ORADATA>/<SID>
RBS data file	The data file for the RBS tablespace.	rbs01.bbf	<ORADATA>/<SID>
ETM data file	The data file for the ETM tablespace.	ETM01.dbf	<ORADATA>/<SID>
Tools data file	The data file for the Tools tablespace.	tools01.dbf	<ORADATA>/<SID>

Appendix E: TDM Appliance Status LEDs

TDM Appliance LED Descriptions

The ETM TDM Appliances have LEDs on the front and/or back of the chassis or Card to indicate status of ETM System operation and the telecommunications connections. The LEDs provide immediate visual notification of errors and warnings. Further investigation of these conditions can be made by viewing the entries in the **Diagnostic Log** and the **Alert Tool**, and by using ETM Commands via the **ASCII Management Interface**, direct serial connection to the Card, or Telnet. The LEDs indicate whether the Appliance is operating normally and draw attention to conditions related to the Dialing Plan, Voice Firewall Policy, Management Server interface, T1 or PRI status, Fail Safe Mode, and Card temperature. 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 using ETM Commands via the **ASCII Management Interface**, **Console** port, or Telnet.

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), the ETM System installation directory (all systems),, or the SecureLogix website.

The sections below describe the meanings of the various LED states on the ETM Appliances.

Telco Appliance LEDs

The table below identifies the types of information, errors, and warnings represented by the LEDs on the ETM 1024, 1090, 2100, and 3200 Appliances.

LED	Location	Status and Meaning
Error	Front	• Off during normal operation with no errors detected and the **Status** LED blinking green. • Red LED indicates: – Card temperature above 70 degrees C – Card in fail safe mode – T1 or PRI Alarms (with Alarm LEDs red or yellow) – Power supply failure – Fan unit failure • Yellow blinking LED can indicate an error in one or more of the following: – Dialing Plan: • File access error • Allocation error • Bad range or entry in file • Range start greater than range end • Unknown file name • Algorithm ID out of range, no match string, or no substitution string (DID) – Policy: • Failed to allocate Policy memory • Invalid file (syntax error)/bad file name • Unable to install default Policy Rules – Management Server interface: • Initially set to indicate Card/Server socket is not established • Loss of Server socket connection – Cabinet/Card temperature above 60 degrees C
Status	Front	• Green and blinking, with **Error** LED off: – Dialing Plan read/parsed successfully – Policy files read/parsed successfully – Server socket connection established – No Telco Alarms – Cabinet temperature below 60 degrees C

LEDs on 1024/1090/2100/3200 Appliances, continued

LED	Location	Status and Meaning
I/F	Front	• Green indicates that the Digital Trunk Interface is operational • Red indicates that the Digital Trunk Interface has an error.
PMC	Front	• Off if the DSP Mezzanine Card is not present. • Green indicates that the DSP Mezzanine Card is operational. • Red indicates that the DSP Mezzanine Card has an error.
Alarm	Rear	• Off during normal operation • Red indicates that the PBX/CO has a red or blue alarm. • Yellow indicates that the PBX/CO has a yellow alarm.
Online	Rear	• Green indicates equipment is inline and able to monitor calls • Off indicates that the equipment is offline.

Index