

## Basic ETM® System Operation/Administration Course Outline

### ETM System v5.2

<b>Day 1</b>
--------------

#### 1) Module 1—Introduction

- a) Introduction to SecureLogix
- b) Welcome to San Antonio
- c) Description of the training lab layout and what materials are provided to each student
- d) Discuss common telephony management issues
- e) Discuss the importance of protecting the voice side of the network
- f) Highlight the advantages that the ETM System provides
- g) What is the basic ETM System architecture and how does it interact with the telco network?
  - i) Appliance models and supported circuit types
  - ii) Supported versions of Oracle
  - iii) Overview of the Call Recorder feature
  - iv) Called/calling numbers and SMDR

#### 2) Module 2—ETM System Overview

- a) How to launch the system components: ETM Management Server, ETM Report Server, ETM System Console, Web Portal
- b) How to log in
  - i) Simultaneous login on multiple ETM Management Servers
  - ii) Item-level locking to prevent multiple users from editing the same content at once
- c) General product overview—The students follow along using their stations
  - i) ETM System Console with the following tools/options:
    - (1) Shutdown Server icon
    - (2) Connect/Disconnect icons
    - (3) ETM Server Properties Tool

- (4) ETM File Management Tool
  - (5) ETM Data Management Tool
  - (6) Status Tool
  - (7) Alert Tool
  - (8) Server Administration Tool
  - (9) Application launch methods
- d) View ETM Management Server installation directory location and structure
- i) ETM System dialing plans
  - ii) ETM System SMDR parse files
  - iii) Error logs
  - iv) ETM System twms.properties file
  - v) ini and package folders
  - vi) Exports
  - vii) Import Sets directory
- e) Exercise 1—Create a User Account

### **3) Module 3—Performance Manager**

- a) Walk through each subtree and explain its purpose
- i) Platform Configuration subtree
    - (1) Discuss the importance of naming conventions for Platform components
    - (2) Call Recording Cache application
    - (3) Span tool tips
    - (4) Downloading firmware to Cards and dialing plans to Spans
    - (5) Health and Status display
  - ii) Telco Configuration subtree
    - (1) Real-time Call Monitor
  - iii) Span Groups sSubtree
    - (1) Define the purpose of Span Groups
    - (2) Call Log

- iv) Policy Subtrees
  - (1) Demonstrate the tools and GUI options commonly used for editing policy
  - (2) Firewall Policy
  - (3) IPS Policies Subtree
  - (4) Call Recorder Policies Subtree
- b) Use the View menu option to customize the tree pane
- c) Describe the objects available under the Manage menu
  - i) AAA Service Users
  - ii) Contacts and Tracks
  - iii) Times
  - iv) Intervals
  - v) Codecs
  - vi) Extension Masking Plans
  - vii) Service Types
  - viii) Billing Plans
  - ix) Subnets
  - x) Authorized Cards list
  - xi) Appliances
  - xii) Span Groups
  - xiii) Switches
- d) Diagnostic Log.
  - i) Demonstrate the Diagnostic Log tool
  - ii) Display the System Events tab located in the Server Administration Tool and explain the correlation between the system events and the diagnostic log
- e) Exercises—Objects used in the upcoming labs:
  - i) Exercise 2—Contacts and Email Tracks (IT Manager, Telco Manager, CIO)
  - ii) Exercise 3—Billing Plan--Edit the default Billing Plan to add costs
  - iii) Exercise 4—Times

- iv) Exercise 5—Intervals
- f) Lab PM1—Basic Platform Configuration

#### 4) Module 4—Directory Manager

- a) Tour of the different Directory Entities:
  - i) Listings
  - ii) Ranges
  - iii) Filters
  - iv) Groups (including the default and the Emergency Group)
  - v) Wildcards
  - vi) Access Code Sets
  - vii) Import Sets
- b) Labs:
  - i) D1—Import listings from a file
  - ii) D2—Define a Listing manually and searching for Listings
  - iii) D3—Create a Directory Range
  - iv) D4—Create a Directory Wildcard
  - v) D5—Create a Directory Filter
  - vi) D6—Add Directory entities to a Group
- c) Extension Masking Plans

<b>Day 2</b>
--------------

\*\*\*\* *Begin with brief review of key concepts from Day 1* \*\*\*\*

#### 5) Module 5—Usage Manager

- a) Explain the components that make up a report
  - i) Templates
  - ii) Elements
  - iii) Date Ranges

- b) Explain the types of report data available: call, resource utilization, cost, diagnostic, directory, IPS
- c) Explain Active-to-Historical data transfer and how it applies to data availability for reports
- d) Explain report generation options: run now, save to tree, preview, save to disk, scheduled reports
- e) Explain how shortcuts work
- f) Demonstrate the Web Portal
- g) Provide custom report examples
- h) CCMI data
- i) Labs R1 through R6

<b>Day 3</b>
--------------

\*\*\*\* *Begin with brief review of key concepts from Days 1 and 2* \*\*\*\*

**6) Module 6—Voice Firewall**

- a) Show a Firewall Policy and explain each field
- b) Show how to make a Rule and add items to each field
- c) Discuss the Implied Rules and how to make/add/edit a new Emergency Group
- d) Explain AAA Services
- e) Discuss how to add/remove Span Groups from a policy
- f) Show how to define a Duration
- g) Discuss the differences between the types of policy rule processing: call reject, call type, and call duration
- h) Discuss the importance of Rule Order
- i) Show and explain the Policy Log. Remind the students about Active-to-Historical data transfer and how it applies to the Policy Log.
- j) Exercise 6—Creating Span Groups
- k) Labs F1, F2, F3, and F4

**7) Module 7—Voice IPS**

- a) Show an IPS Policy and explain how the IPS Policy works
  - i) What are Thresholds and what are the different types
  - ii) How the Duration field in the Policy is different from the Duration setting in the Threshold
  - iii) Polling engine
  - iv) Accumulations counted for length of Interval or subinterval
  - v) When Accumulations for a Rule are reset (maintained for Server restarts)
  - vi) Termination options
  - vii) Reasons for counting Firewall Terminations (ex. If there is a spike in activity, it may indicate your network is under attack)
  - viii) Show and explain the Real-Time Monitor.
  - ix) Show and explain the IPS Policy Log. Remind the students about active-to-historical data transfer.
- b) Labs I1 and I2

**8) Module 8—System Review and Q&A**

**9) Module 9—(Optional) The Call Recorder** This module is only used when class composition warrants. This topic is also described in the SecureLogix Computer Based Training (CBT).

- a) Show a Call Recorder Policy and explain the fields
- b) Describe how Call Recorder Policies differ from the others:
  - i) No Tracks
  - ii) Only define what to record. Implied DO NOT RECORD Rule prevents recording of anything else.
  - iii) No Policy Log for Call Recorder but the call data is still stored in the database like any other monitored call
- c) How calls are processed against Call Recorder policies
  - i) Recording begins at the beginning of a call
  - ii) How call-type changes are handled
  - iii) How Call Recorder Policies interact with other policies

- d) What are Protected Extensions?
- e) How to provide a new announcement file for analog Spans that support announcement
- f) How to access calls on the Web Portal
- g) How to access calls on the Collection Server