



ETM[®] (Enterprise Telephony Management) System

v7.1.1

Call Recorder User 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.

© Copyright 1999-2018 SecureLogix Corporation. All Rights Reserved.

This product is protected by one or more of the following patents: US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,718,024 B1, US 6,760,420 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	8
About the ETM [®] System Documentation	8
ETM [®] System User Guides	8
Additional Documentation on the Web	9
Tell Us What You Think	9
Conventions Used in This Guide	9
 Overview of the ETM[®] Call Recorder	 11
Understanding the Call Recorder	11
Recording Capacities	11
Call Recorder Architecture	11
ETM [®] Client and Server	12
Call Recorder Application	12
Recording-Enabled ETM [®] Spans	12
Call Recorder Operation	12
CRC Application	13
Collection Server	13
ETM [®] Web Portal	14
SMDR Extensions	14
Inbound SMDR	15
Transportable Option	15
Obtaining the Call Recorder	15
 Installing and Configuring the Call Recorder	 16
Installation	16
Hardware Installation	16
Call Recorder Software Installation	17
Adding the Call Recorder to an Existing System	17
Installing the Collection Server Software	17
Installing the ETM [®] Web Portal	19
Call Recorder Configuration	20
User Permissions	20
Granting Call Recorder Permission to an Existing User	21
Configuring the CRC	22
Opening the CRC Configuration Dialog Box	22
Naming the CRC	23
Adding a Tool Tip Comment	23
Specifying the Listener Port	24
Enabling Call Recording Volume Warning Thresholds (Optional)	24

Disk Space Reserved for Call Recordings.....	25
Allowing Recording Span Connections to a Dedicated CRC Appliance.....	26
Enabling the CRC to Use a Collection Server	27
Enabling Debug Logging	30
Changing the Heartbeat Interval.....	30
Importing CRC Configuration.....	30
Configuring the Span for Recording.....	31
Opening the Span Configuration Dialog Box	31
Enabling Call Recording on a TDM Span.....	31
Specifying the CRC to Use (TDM)	33
Changing the CRC Port	34
Specifying Which Channels to Record (TDM)	34
Setting the Maximum Individual Recording Length	35
Requesting Inbound SMDR	35
How the Companding Setting Affects TDM Recording Spans	35
Configuring SMDR Extensions	36
Defining SMDR Extensions	36
Importing SMDR Extensions	39
Configuring the Collection Server	39
About the ETM [®] Collection Server Configuration Tool	44
Authorizing CRCs to Connect to the Collection Server	45
Editing a CRC Authorization	46
Deleting a CRC Authorization	46
Setting the Minimum Disk Space Allowed on the Collection Server	46
Automated Collection Server Purging.....	47
Changing the Collection Server Listener Port	48
Setting the Maximum Number of Allowed Cache Connections	48
Specifying the Cache Path.....	48
Specifying the Filter Path	49
Selecting the Filter.....	49
Specifying Post-Filter Processing.....	50
Naming the Collection Server.....	50
Monitoring Expected Call Recording Volume	51
Setting Thresholds for Expected Call Recording Volume.....	51
Configuring an Alert for Threshold Violations	52
Where to Go From Here.....	54

Using the Call Recorder 55

Recording and Accessing Calls.....	55
Recording Calls.....	55
Understanding Recording Policies.....	55
How Call Recorder Policies Interact with Other Policies.....	56
Rule Order	56
About Call Type Changes	56
Policy Transitions	57
When a Span is Added to a Span Group.....	57
Policy Verification.....	57

Fields in a Recording Policy Rule	58
Showing/Hiding the Recording Policies Subtree.....	59
Dirty Policy Indicator	59
No Policy Log for Recording Policies.....	59
Defining and Installing a Recording Policy	60
Creating a New Recording Policy	60
Adding a Rule to a Recording Policy	61
Defining a Recording Policy Rule.....	62
Showing/Hiding the Implied Rule.....	64
Installing a Recording Policy	64
Assigning a Span Group to a Recording Policy	65
Viewing Properties of a Recording Policy	65
Printing a Recording Policy.....	66
Saving a Recording Policy	66
Editing an Installed Recording Policy	67
Saving a Copy of a Policy	68
Renaming a Policy.....	68
Deleting a Recording Policy.....	68
Uninstalling a Recording Policy.....	68
Reverting a Policy to Its Last Saved State.....	69
Using Undo/Redo while Editing a Policy.....	69
Modifying or Deleting Items Contained in Rules.....	69
Hiding Rules.....	69
Disabling Rules	70
Cutting, Copying, and Pasting, Rules.....	70
Deleting Rules	70
Viewing Contents of Directory Entities in Rules	71
Accessing Call Recordings	72
Logging in Via the Web Portal	72
Locating and Listening to Call Recordings	74
Accessing Call Recordings on the Collection Server	78
Data Filtering.....	78
Call Recording Storage Directory Structure	78
Post-Filter Processing	80
Accessing Recorded Calls	81
Viewing Log Files	81

Appendix 83

Maintenance Information	83
Uninstalling the Collection Server Software	83
ETM® Commands for the Call Recorder	83

Index 87

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.

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.

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

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.

Overview of the ETM[®] Call Recorder

Understanding the Call Recorder

The ETM[®] Call Recorder provides policy-based capture of the audio and data content of calls. For example, you can:

- Record all inbound calls for quality assurance and security monitoring.
- Record 911 calls.
- Record calls from/to customer support lines, to provide an audit trail.
- Capture threatening or harassing calls to your staff for investigation.
- Ensure that calls to certain extensions are never recorded.

Since the recording is policy-based, no user intervention is needed to begin recording—recording begins automatically at the start of a call for the lines you specify. You can also define a list of SMDR extensions, such as pharmacy lines, to which calls are never to be recorded, based on Inbound SMDR data*.

** Not available on UTA*

Recording Capacities

The number of available recording “slots” available depends on the application and the hardware on which it is running:

- **2100/3200 TDM Appliance**—Each 8540 Controller Card provides up to 48 recording “slots” among all of the Recording Spans on the Card.
- **1024 CR Appliance**—Up to 24 recording slots.
- **1090 CR Appliance**—Up to 24 (T1) or 30 (E1) recording slots.
- **Inline SIP Application**—Up to 30 recording slots.
- **UTA**—Up to 30 recording slots (.).

Call Recorder Architecture

The Call Recorder architecture consists of the following components:

- **The ETM Server** manages the Recording Spans and the Call Recording Cache (CRC) applications, and provides recordings to the Web Server for access via the Web Portal.

- **The Call Recorder application.** Installed on the ETM Server and accessed via the Performance Manager; used to define, manage, and install Recording Policies; and view Health & Status,.
- **One or more recording-enabled ETM[®] Spans** to transfer calls to a CRC application, where they are recorded in real time. All Span types can be recording-enabled via software.
- **A Call Recording Cache (CRC) application** to which the recording Spans transfer information to be recorded. The CRC application can run on the 1024 and 1090 Appliances, the Unified Trunking Application (UTA) , the SIP application, or a dedicated SecureLogix CRC Server. Note that inline SIP and UTA support only a local CRC; they cannot use a dedicated CRC appliance.
- *(Optional)* **A Collection Server** for offsite storage of call recordings. The Collection Server is a Windows application . See the Minimum System Requirements in the SecureLogix Knowledge Base for supported Windows versions. (**Note:** The Collection Server is optional if the Web Portal is used, but you must have one or the other and can use both.)
- *(Optional)* **The ETM[®] Web Portal** to locate and access call recordings stored on the CRC or Collection Server. (**Note:** The Web Portal is optional if a Collection Server is used, but you must have one or the other and can use both.)

ETM[®] Client and Server

The Performance Manager is used to define and manage Recording Policies and configure and monitor the Recording Spans and CRCs. As with all other Appliance application components in the ETM System, the CRC, and the Recording Spans are represented and configurable through the **Platform Configuration** subtree in the Performance Manager tree pane. If a Collection Server is used, it can also be represented in the tree pane.

The ETM Server pushes Recording Policies and application configuration to the Recording Spans and the CRCs.

Call Recorder Application

The Call Recorder application is installed on the ETM Server and accessed via the Performance Manager; it is used to define, manage, and install Recording Policies. The Call Recorder is separately purchased and is enabled by the Server license.

Recording-Enabled ETM[®] Spans

A recording-enabled Span is an ETM telecom Span on which Call Recorder software is installed, coexisting with other ETM applications such as the Voice Firewall. All Span types can be recording-enabled.

Call Recorder Operation

When a call begins that matches a **Record** Rule in a Call Recording Policy, the Recording Span transmits the call information to the CRC in real time and the CRC records the call as it is received. If a Recording Span cannot connect to a CRC, no recording can occur. If a Recording Span loses

connection to its CRC while recording is in progress, recording ceases and those recordings are discarded.

Calls are recorded and stored on the CRC. Optionally, recordings can be transferred for remote, longer-term storage to a Collection Server running on a Windows computer. Call recordings are accessible remotely, enterprise-wide, via a web-browser interface. To locate and listen to recorded calls, you log in to the ETM Web Portal via a standard web browser and then use a rich set of search tools to locate calls of interest. After locating a call you want to listen to, you can transfer it to your client computer and use Windows Media Player (or another **.wav** file player) to listen to the recorded call. Recordings can also be locally accessed through the Collection Server file system.

When the maximum number of simultaneous recordings is reached for a Card, no new calls on that Card are recorded (regardless of whether they match the Recording Policy) until one of the slots is freed. Recording only begins at the start of a call; ongoing calls are not reevaluated against the Policy when a slot frees.

If the call type of an ongoing call changes, it is reevaluated against Policy; if the type no longer matches any Rule and the call is currently being recorded, a user setting dictates whether recording stops and the call is discarded, or whether recording continues and the call is retained. Recording does not begin for an ongoing call, even if the call type change causes it to match a Rule.

CRC Application

The CRC application stores the call recording WAV files. It uses a circular buffer; older files are overwritten by newer files as space is needed. Files on the CRC can be accessed via the ETM Web Portal.

If a Collection Server is used, after recordings are transferred to the Collection Server, they are deleted from the CRC. Files on the Collection Server can also be accessed via the ETM Web Portal.

Collection Server

The Collection Server is an application that runs on a Windows system, to which one or more CRCs can optionally transmit call recordings for permanent storage, playback, and analysis. See the Minimum System Requirements in the SecureLogix Knowledge Base for supported Windows versions. The Collection Server provides software filters for converting the call recordings into formats for third-party playback and analysis tools, such as Windows Media Player or other privately or commercially available tools. The Collection Server provides a separate configuration GUI and logs, and can optionally be configured to connect to the Management Server. Calls stored on a Collection Server are available either by direct access to the Collection Server computer file system, or via the Web Portal if the Collection Server is configured to connect to the Management Server.

When a Collection Server is used, CRC applications send the audio files and associated call data for the recorded calls at user-defined intervals to the Collection Server for storage.

The Collection Server opens a listener port to wait for new connection requests from CRC Applications. When a request is received, the Collection Server determines whether the current number of active connections is less than the maximum number allowed. If not, the connection is refused. If a connection is available, the Collection Server then checks its **Allowed CRC IP List** to see if the IP address of the CRC making the request is allowed. If it is not, the request is refused and the result is logged. If the IP address is allowed, the connection is accepted.

If the connection is allowed, the CRC sends one or more sets of call records. For each call, the CRC first sends a message containing the call parameter data. From this data, the Collection Server can derive the name of the data and audio files and decide into which subdirectory the files should be placed. Next, the CRC sends a series of messages containing the call recording itself, which is followed by a message indicating that all data has been sent.

The following call parameters are included in the in the call data file sent from the CRC to the Collection Server:

- WAV file name
- Call direction
- Call initiation time
- Call connect time
- Call end time
- Call types
- Source phone number
- Destination phone number
- Call Recording Policy name
- Call Recording Policy rule number
- Call Priority
- WAV file size
- Answer offset
- Recording span MAC address
- CRC MAC address
- Recording span number
- Companding method (A law or Mu law)
- Call initiation time GMT offset
- Call connect time GMT offset
- Call end time GMT offset
- Call flags
- Source phone number flags
- Destination phone number flags

ETM® Web Portal

The ETM Web Portal is the web interface used to access, locate, and listen to call recordings stored on the CRC or Collection Server.

SMDR Extensions

(Not available on UTA) Certain internal extensions may exist to which you never want to record calls, or for which you want to mark recordings as sensitive. For example, for privacy reasons, you may want to prevent recording of inbound calls on pharmacy lines. To ensure that calls to these pharmacy extensions are not recorded when you use a “record all calls” Call Recording Policy; you can define a list of *SMDR Extensions* and specify how call recordings for these extensions are to be handled: deleted, saved,

or saved and marked as sensitive. You then enable Inbound SMDR on channels that are to observe the **SMDR Extensions** list. SMDR Extensions are defined per Switch. Up to 1000 entries can be defined per Switch (ranges are supported and count as one entry).

SMDR Extension processing is only available for inbound calls.

SMDR Extension processing occurs after the call ends and SMDR is received. Calls are not made available via the Web Portal nor transferred to the Collection Server (if one is used) until after SMDR extension processing occurs.

For details about SMDR Extensions and the available handling options, see “Configuring SMDR Extensions” on page 36.

Inbound SMDR

Inbound SMDR is used only for SMDR Extension processing and to populate the destination address in the call data stored on the CRC, not for Policy processing. You enable/disable Inbound SMDR per channel on a TDM Span or overall for a SIP Span.

SMDR Extensions can only be identified on channels for which Inbound SMDR is enabled. Optionally, you can also specify that calls only be recorded when SMDR is matched. If SMDR cannot be resolved to determine whether the call involved a SMDR extension, the recording is discarded. Channels for which Inbound SMDR is not enabled ignore the **SMDR Extensions** list.

For details about SMDR Extensions and the available handling options, see “Configuring SMDR Extensions” on page 36.

Transportable Option

The Call Recorder is also available in a transportable option. The transportable system is self-contained and preinstalled with all of the Call Recorder components. Unlike the fixed system, which is installed inline with the telecom trunks between the CO and the CPE, the transportable system uses custom tap version of the transition module and is installed as a tap on the line between the CO and CPE. Contact your SecureLogix representative for details.

Obtaining the Call Recorder

The ETM[®] Call Recorder is purchased and licensed separately from the rest of the ETM System. Contact your SecureLogix Sales Representative for information.

Installing and Configuring the Call Recorder

Installation

As described in the previous chapter, various configurations are available for the Call Recorder:

- Recording Span(s) using a local CRC on the same Card.
 - To install this configuration, simply license the ETM Server for Call Recording. Then continue with the next chapter, “Configuring the Call Recorder.”
- Recording Span(s) on one or more Cards using a remote, dedicated CRC Server.
 - To install this configuration, license the ETM Server for Call Recording, and install and configure a CRC Server. Then continue with the next chapter, “Configuring the Call Recorder.”
- Either of the above with an optional Collection Server for permanent storage.
 - In addition to the steps above, install and configure the Collection Server application.

Hardware Installation

The Call Recorder is supported on all ETM Appliance application types. The 2100/3200 Cards and the 1024/1090 Appliances used for Call Recording are physically identical to non-Recording-enabled ETM hardware. Call Recording is enabled via a Server license and then Appliance configuration.

As previously described, a dedicated CRC Server can be used for remote call recording storage with TDM appliances.. A dedicated CRC can accept call recordings from up to 32 Recording Spans on up to 8 Cards, and up to 120 simultaneous calls. When this capacity is exceeded, Diagnostic Logs are generated and excess recordings-in-progress may be dropped.

If you have not already done so, install and configure the Appliances, Cards, and their Spans as described in the *ETM® System Installation Guide*. Then continue with these instructions to complete Call-Recorder specific configuration.

Call Recorder Software Installation

The Call Recording software includes:

- An ETM Server component, which is license-enabled and requires no separate installation other than placing the Call Recording Server license file in the ETM Server installation directory.
- Appliance software, which is included in the Appliance software package that you download to the Card(s) when you install or upgrade to this version. See the *ETM® System Installation Guide* for instructions for installing Card software.
- Optionally, Collection Server software installed on a Windows system. See the Minimum system Requirements for supported versions of Windows.*
- Optionally, the ETM Web Portal, a browser-based interface for locating and accessing call recordings. *

Note: You must have either the Collection Server or ETM Web Portal installed, and can use both.

If you purchased Call Recording with your initial ETM System purchase, the correct license file was installed during initial system installation. If you are adding Call Recording to an existing system, see the instructions below for adding the license file.

Adding the Call Recorder to an Existing System

If you are adding the Call Recorder to an existing system, enable the Call Recorder on the ETM Server as follows:

1. Copy the license file you received from Customer Support to the ETM Server installation directory.
2. Restart the ETM Server for the new license to take effect. The Call Recorder features are now enabled and ready to be configured.

Installing the Collection Server Software

The Collection Server runs as a service on a Windows system that has a sufficiently large storage capacity dedicated to call recording storage and LAN/WAN access to the CRCs. See the Minimum System Requirements for supported versions of Windows.

IMPORTANT INFORMATION : A Windows 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 Collection Server Application

1. Insert the ETM System product CD into the CD-ROM drive.
2. Navigate to the **Collection Server** directory, and then double-click **Setup.exe**. The **ETM Collection Server Setup Wizard** appears.
3. Click **Next**. The **Select Installation Folder** dialog box appears.
 - a. The **Folder** box displays the default installation path. To specify a different path, type it in the box or click **Browse** to select the path.
 - b. To verify available hard drive space, click **Disk Cost**. The **Collection Server Disk Space** dialog displays the disk space available on each drive.
 - c. By default, the Collection Server is only installed for the logged in user. To make the Collection Server available to everyone who logs in to the computer, click **Everyone**.
4. Click **Next**. The **Confirm Installation** dialog box appears.
5. Click **Next** to start the installation.
6. When the installation is complete, click **Close** to exit. The **ETM Collection Server Configuration Tool** icon appears on the desktop and a shortcut is added to the **Start** menu under the **SecureLogix** folder. By default, the ETM Collection Server service is configured to start automatically on reboot.

Tip If you are upgrading from a previous version of the Collection Server, you must uninstall that version using the Windows **Add/Remove Programs** feature before running the installer.

***Installing the
ETM[®] Web Portal***

See the *ETM[®] System Installation Guide*. The ETM Web Portal can also be used to view and schedule Usage Manager Reports.

Call Recorder Configuration

Continue by configuring the Call Recorder, as explained in the following procedures. Configuration includes:

- Granting user permissions for the Call Recorder.
- Configuring the **Recording** tab settings for the Recording Spans.
- Configuring the CRCs.
- Configuring the Collection Server (if used).
- Defining the list of SMDR Extensions (if used).
- Enabling Inbound SMDR, if used for SMDR Extension processing.

User Permissions

When the Call Recorder is licensed, the default **admin** account (if present) is automatically granted the Call Recorder permission. No other user accounts are automatically granted this permission. An ETM System administrator with **Manage Users** permission must explicitly grant permission for the Call Recorder to any other authorized users. If the default **admin** account has been removed, no user accounts are automatically granted the Call Recorder permission.

As with other types of ETM Policies, two user permissions govern the Call Recorder:

- **View & Reinstall Recording Policies**—Only users with this permission can see the **Recording Policies** subtree in the Performance Manager tree pane and access Call Recordings via the Web Portal. They can also view any Call Recorder Policy and reinstall Call Recorder Policies that are already installed (for example, when Listings used in the Policy change). They cannot edit Policies unless they also have the **Full Control** permission.
- **Full Control**—Users with this permission can see, edit, delete, install, and uninstall Recording Policies.

Note that these permissions do not affect Appliance configuration—any user with **Manage Telecommunications Configuration** permission can access and modify Appliance configuration for any type of Appliance, including the Recording Spans and CRCs.

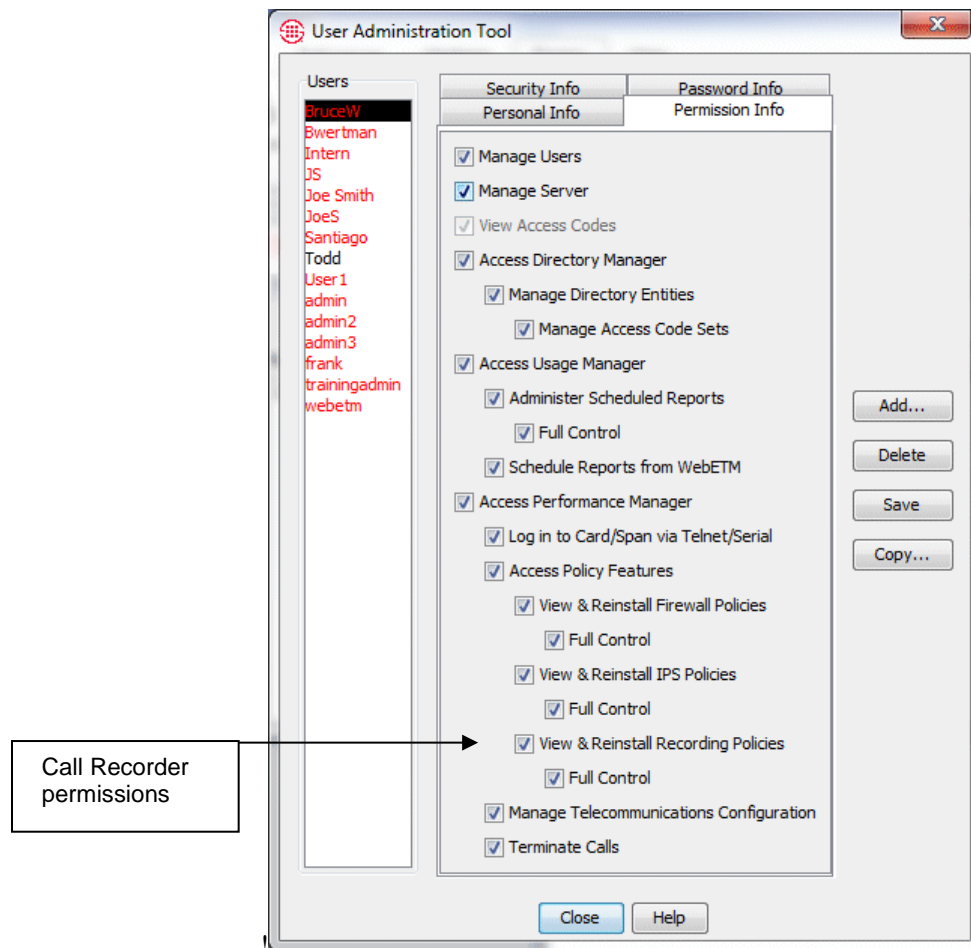
See "User Profiles" in the *ETM® System Administration and Maintenance Guide* for instructions for creating a new user account. The procedure "Granting Call Recorder Permission to an Existing User" on page 21 explains how to grant Call Recorder permissions to an existing account.

Granting Call Recorder Permission to an Existing User

The Call Recorder permissions only appear in the **User Administration Tool** when the Call Recorder is licensed.

To grant Call Recorder permissions to an existing user

1. On the ETM System Console main menu, click **Servers | User Management**. The **User Administration Tool** appears.
2. Click the **Permission Info** tab.




3. In the **Users** list, click the user to whom you want to grant this permission.
4. Select the **View & Reinstall Recording Policies** check box. (**Access Performance Manager** and **Access Policy Features** must be selected before you can grant **View & Reinstall Recording Policies** permission.)

5. If you want this user to be able to define and manage Call Recorder Policies, select the **Full Control** select the check box below the **View & Reinstall Recording Policies** check box.
6. Click **Save**.

Configuring the CRC

CRC configuration provides the settings needed for the CRC to accept call recordings from Recording Spans, specifies whether a Collection Server is used, and if so, provides Collection Server connection information.

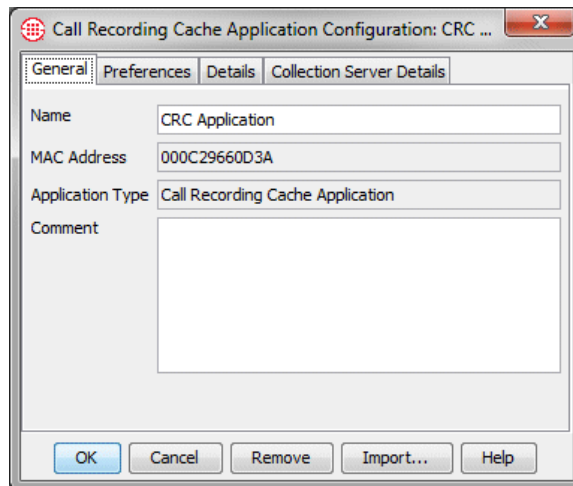
Opening the CRC Configuration Dialog Box

The CRC application appears at the Span level below a Card icon and is identified by the  icon. The instructions below explain how to open the **Call Recording Cache Application Configuration** dialog box to configure a single CRC or the **Multi-Span Configuration** dialog box to configure multiple CRCs with the same settings.

To open the Call Recording Cache Application Configuration dialog box

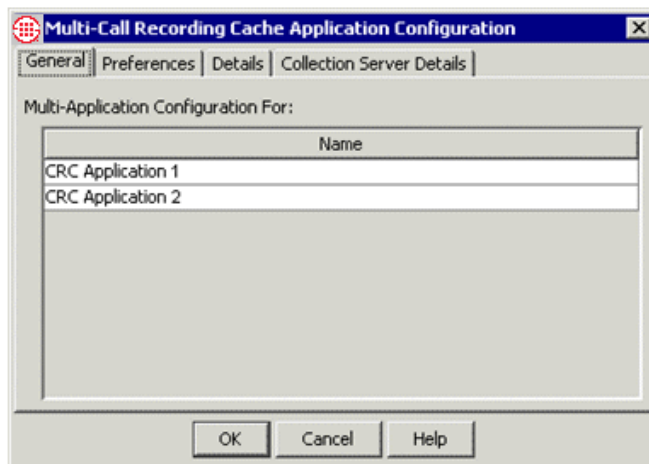
For a single CRC:

- In the Performance Manager tree pane, right-click the CRC and click **Edit Call Recording Cache Application(s)**. The **Call Recording Cache Application Configuration** dialog box appears.



For multiple CRCs:

- Hold down CTRL and then in the Performance Manager tree pane, click each Cache, right-click the selection, and click **Edit Call Recording Cache Application(s)**. The **Multi-Call Recording Cache Configuration** dialog box appears.



Naming the CRC

You must select a single CRC for editing to be able to change the **Name** field.

To name the CRC

- In the **Name** box on the **General** tab of the **Call Recording Cache Configuration** dialog box, type the comment text.

Note: When you have completed CRC configuration, click **OK** to push the configuration to the CRC and close the dialog box. No changes take effect until you click **OK**.

Adding a Tool Tip Comment

You can optionally type a tool tip comment. The comment appears when you hover the mouse cursor over the CRC icon in the Performance Manager tree pane.

To add a tool tip comment

- In the **Comment** box on the **General** tab of the **Call Recording Cache Configuration** dialog box, type the comment text. You can optionally use basic HTML tags to format the tool tip display.

IMPORTANT Since HTML tags are enclosed in angle brackets, use of angle brackets in the **Comment** field has the following limitation: If you want to display a left angle bracket, you must type the following code to denote it: `<`;

In HTML, a typed left angle bracket character is never displayed, a right angle bracket is not displayed if a left angle bracket precedes it anywhere in the text, and any text enclosed in angle brackets is assumed to be a tag and not displayed.

For example, if you type `This is <span_2>` in the **Comment** field, the tool tip displays only `This is`. If you instead type `This`

is `<span_2>`, the tool tip displays This is `<span_2>` as you intended.

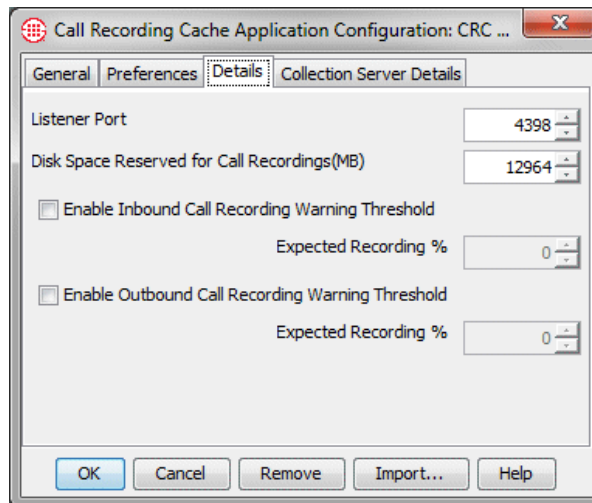
Specifying the Listener Port

The **Listener Port** is the port on which the CRC accepts connections from the Recording Span(s). The default is **4398**. If this CRC is to use a different port for Recording Span connections, specify a different value.

IMPORTANT If you change this value, you must provide the new value to each Recording Span that is to send call recordings to this CRC, or they will be unable to communicate. See "Changing the CRC Port" on page 34 for instructions.

To change the CRC Listener Port

1. In the **Call Recording Cache Application Configuration** dialog box, click the **Details** tab.



2. In the **Listener Port** box, type or select a new value.

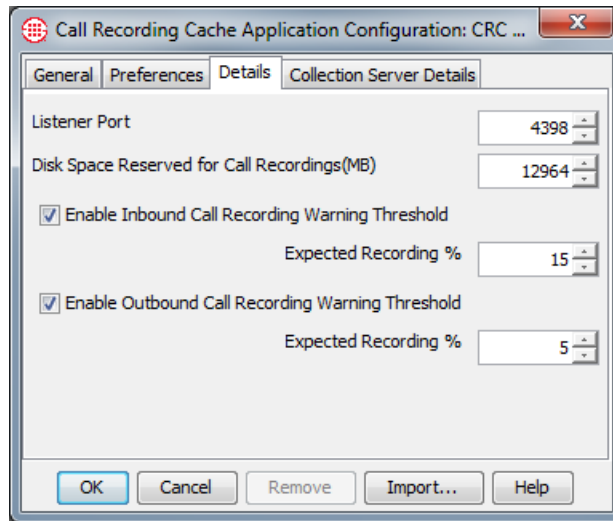
Note: When you have completed CRC configuration, click **OK** to push the configuration to the CRC and close the dialog box. No changes take effect until you click **OK**.

Enabling Call Recording Volume Warning Thresholds (Optional)

You can set thresholds for expected volume of inbound and outbound call recordings as a percentage of call volume, and then configure a System Event to alert you when a threshold is not met. A drop in the expected volume of recorded calls may indicate an error condition resulting in calls not being recorded as expected.

To enable call recording warning thresholds

1. In the **Call Recording Cache Application Configuration** dialog box, click the **Details** tab.



2. Optionally, select **Enable Inbound Call Recording Warning Threshold** and type or select the expected percentage of inbound calls to be recorded. A warning appears in the Diagnostic Log if the percentage of recorded calls falls below this threshold. This can alert you if inbound call recordings are failing, due to faulty configuration or other issues.
3. Optionally, select **Enable Outbound Call Recording Warning Threshold** and type or select the expected percentage of outbound calls to be recorded. A warning appears in the Diagnostic Log if the percentage of recorded calls falls below this threshold. This can alert you if outbound call recordings are failing, due to faulty configuration or other issues.
4. Configure the following System Event to send an alert when a threshold is not met. See “Configuring an Alert for Threshold Violations” on page 52 for instructions for configuring the alert:

Call Recording Threshold Violation—The user-defined threshold of expected call recordings was not met. This can indicate the calls have stopped being recorded due to a Call Recorder issue.

Note: When you have completed CRC configuration, click **OK** to push the configuration to the CRC and close the dialog box. No changes take effect until you click **OK**.

Disk Space Reserved for Call Recordings

Do not change this setting unless instructed to do so by SecureLogix Support personnel.

When the CRC first connects to the Server, the disk space is set by default to the largest amount available for the type of Appliance on which the CRC resides. When this limit is reached, the oldest call recordings are deleted in first-in, first-out priority order (lowest to highest) until enough disk space is freed. That is, all low priority recordings across all dates are deleted first.

Allowing Recording Span Connections to a Dedicated CRC Appliance

To change the disk space reserved for call recordings

1. In the **Call Recording Cache Application Configuration** dialog box, click the **Details** tab.
2. In the **Disk Space Reserved for Call Recordings (MB)** box, type or select the amount of space reserved for recordings. Note that if you supply a value not available on the Appliance type, the Appliance automatically adjusts the value, but the GUI does not reflect the value in use. If this happens, a Diagnostic Log is generated.

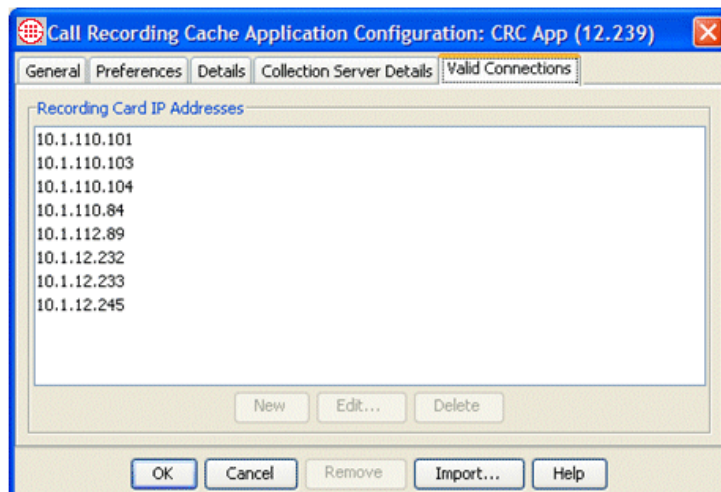
Note: When you have completed CRC configuration, click **OK** to push the configuration to the CRC and close the dialog box. No changes take effect until you click **OK**.

This procedure only applies to dedicated CRC Appliances—CRCs on other Card types only accept connections from their local Spans, which are always authorized. If you are not using a dedicated CRC, skip this procedure. Inline SIP applications and UTA do not support dedicated CRC Appliances.

A dedicated CRC can accept simultaneous connections from up to 32 Spans on up to 8 Cards specified in its list of authorized Recording Spans.

To authorize a Recording Span to connect to a dedicated CRC

1. Right-click the CRC and click **Edit Call Recording Cache Application(s)**.
2. Click the **Valid Connections** tab.



3. Click **New**. The **Recording Card IP Address** dialog box appears.

4. Type the IPv4 or IPv6 address of the Card on which the Recording Span resides, then click **OK**.

Enabling the CRC to Use a Collection Server

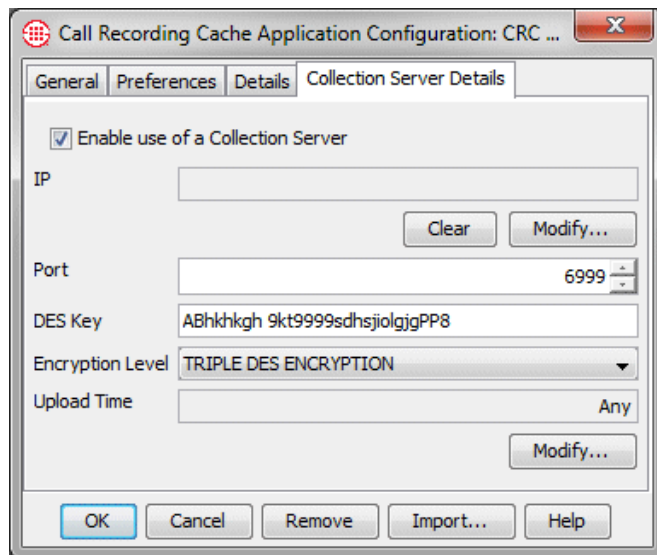
Optionally, the CRC can send call recordings and logs to a Collection Server via TCP/IP. (A Collection Server can receive call recordings from up to 20 CRCs.) The CRC always initiates the connection to the Collection Server.

If a Collection Server is used, use the instructions below to configure the CRC to connect to the Collection Server and to set the upload schedule. If you are not using a Collection Server, skip this procedure.

Note that if you use SMDR Extensions =, call recordings are not transferred to the Collection Server until they are processed against the SMDR Extensions list after the call ends and SMDR data is received.

To enable this CRC to use a Collection Server

1. In the **Call Recording Cache Application Configuration** dialog box, click the **Collection Server Details** tab.

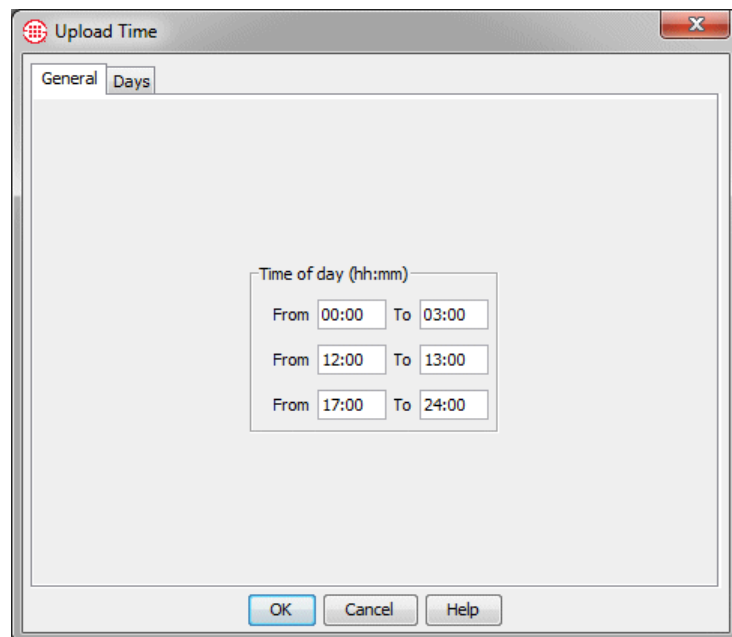


2. Select the **Enable use of a Collection Server** check box.
3. Under the **IP** box, click **Modify**, and then type the IPv4 or IPv6 address of the Collection Server and click **OK**.
4. In the **Port** box, type or select the port on which the Collection Server receives connections from CRCs, if different from the default. The default is **6999**.
5. In the **DES Key** box, type the DES Key used for encrypted communication between the CRCs and the Collection Server. The DES Key must always match between the CRC and the Collection Server; initial communication is always encrypted to validate the connection,

regardless of the **DES Level** setting. If you change the value here, be sure to change it at the Collection Server as well. The same DES key is used by all CRCs connecting to a given Collection Server.

6. In the **DES Level** box, click the down arrow and select the level of encryption: **No Encryption**, **Single DES Encryption**, or **Triple DES Encryption**.
7. **Upload Time** specifies the interval at which call recordings are transferred from the CRC to the Collection Server. Under the **Upload Time** box, click **Modify**.
 - a. The **Upload Time** dialog box appears with the **General** tab selected.

Defining the **Upload Time** is very similar to defining a Time for a Policy Rule.



- b. In the **Time of day (hh:mm)** area, specify up to 3 different periods, in 24-hour format, when call recordings are to be uploaded. You must specify at least one period. Note that a period cannot span midnight. Use the time range fields chronologically in top to bottom order. Leave unused fields blank. For example, if you want to specify all times, in the first set of **From** and **To** boxes, type 00:00 and 24:00.
 - c. Click the **Days** tab to specify which days calls are to be uploaded during the specified times.

- In the **Days Specification** area, select one of the following:
 - **Any**—Call recordings are uploaded on all days at the times specified on the **General** tab. The other fields on the dialog box are grayed out. Use this option when you want near-real-time streaming of data.

IMPORTANT If SMDR Extensions are used, call recordings are not transferred until after SMDR Extension processing occurs, which happens after the call ends and SMDR data is received. In this case, real-time streaming cannot occur.
 - **Day in Month**—Allows you to specify certain days in a specific month on which call recordings are to be uploaded.
 - a. In the **Days in Month** area, select the days in the month on which call recordings are to be uploaded during the times you set on the **General** tab.
 - b. In the **Month** area, select the **Month**.
 - **Day in week**—Allows you to specify certain days of the week on which call recordings are to be uploaded at the times you set on the **General** tab.
 - In the **Days in Week** area, select each day on which calls are to be uploaded. Note that if you select all days of the week, it has the same result as selecting **Any**.
- d. Click **OK** to save your settings and close the dialog box. The **Upload Times** field updates with a description indicating the days and times specified.

Note: When you have completed CRC configuration, click **OK** to push the configuration to the CRC and close the dialog box. No changes take effect until you click **OK**.

Enabling Debug Logging

As with other Appliance components, debug logging can be used to troubleshoot issues. When enabled, debug events are written to a file on the hard drive of the ETM Server computer. Only enable debug logging if instructed to do so by SecureLogix Support personnel.

To enable debug logging

1. In the **Call Recording Cache Configuration** dialog box, click the **Preferences** tab.
2. Select the **Log Appliance Debug Events to a File** check box.

Clear this check box when debug logging is no longer needed, to avoid unnecessary use of hard drive space. See the *ETM® System Administration and Maintenance Guide* for more information about accessing debug logs.

Note: When you have completed CRC configuration, click **OK** to push the configuration to the CRC and close the dialog box. No changes take effect until you click **OK**.

Changing the Heartbeat Interval

The default heartbeat interval is 1 minute. Do not change this setting unless instructed to do so by SecureLogix Technical Support personnel.

To change the heartbeat interval

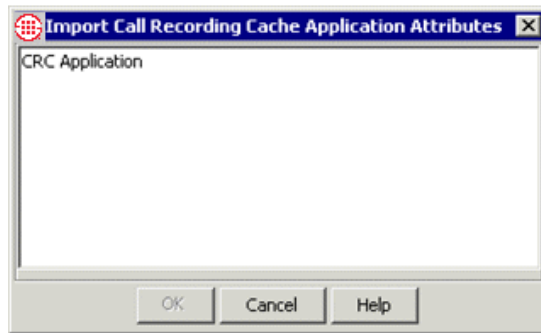
1. In the **Call Recording Cache Application Configuration** dialog box, click the **Preferences** tab.
2. In the **Heartbeat Interval** box, type or select the interval.

Importing CRC Configuration

After you have completed configuration for a CRC, you can import its settings to apply to another CRC for which the settings are to be identical. Settings can only be imported to a single CRC at a time, not globally.

To import CRC settings

1. In the **Platform Configuration** subtree, right-click the CRC into which you want to import settings, and then click **Edit Call Recording Cache Application(s)**.
2. Click **Import**. The **Import Call Recording Cache Application Attributes** dialog box appears.



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

Configuring the Span for Recording

Call Recording is enabled by the Server license. After you install the Call Recording Server license on the ETM Server, the Call Recorder-specific settings become available for each Span. You use these settings to configure recording for the Spans on which calls are to be recorded, as described in the sections below.

If you have not already done so, see “Configuring Spans” in the *ETM® System Installation Guide* for instructions for configuring the telco Spans. Then return to this procedure to perform Call Recorder-specific configuration.

Opening the Span Configuration Dialog Box

To open the Span Configuration dialog box

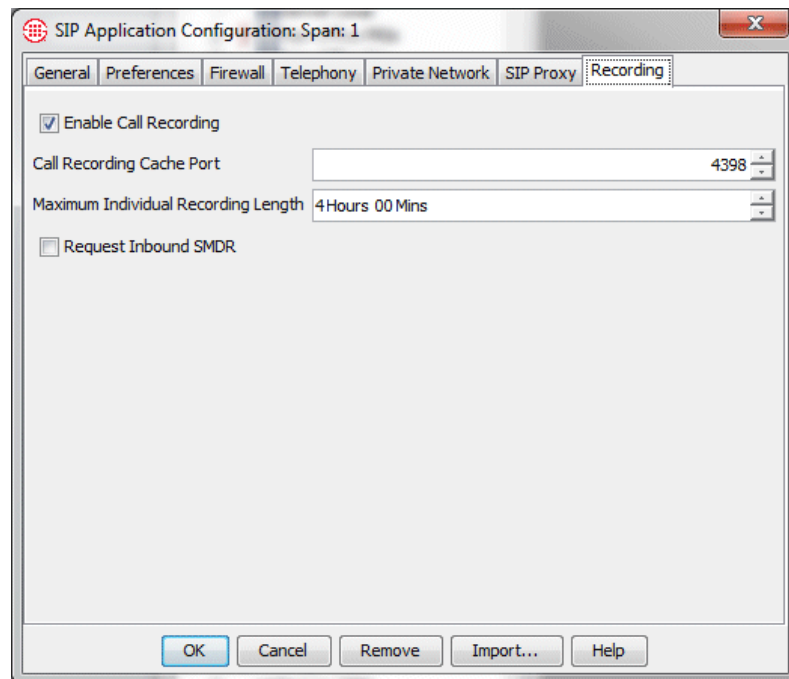
- In the **Telco Configuration** subtree, right-click the Span and click **Edit Span(s)**.

Enabling Call Recording on a TDM Span

To enable Call Recording on a TDM Span

1. Open the **Span Configuration** dialog box and click the **Recording** tab.
2. Select the **Enable Call Recording** check box. Then configure the other settings on this tab as described below, according to the type of Span you are configuring (, SIP, UTA or TDM).

SIP Span Recording Tab



The screenshot shows the 'SIP Application Configuration: Span: 1' window with the 'Recording' tab selected. The window has a title bar with a red 'X' button. Below the title bar is a tabbed interface with tabs for 'General', 'Preferences', 'Firewall', 'Telephony', 'Private Network', 'SIP Proxy', and 'Recording'. The 'Recording' tab is active. Inside the tab, there is a checkbox labeled 'Enable Call Recording' which is checked. Below this is a text field for 'Call Recording Cache Port' with the value '4398'. Below that is a text field for 'Maximum Individual Recording Length' with the value '4 Hours 00 Mins'. At the bottom of the tab is a checkbox labeled 'Request Inbound SMDR' which is unchecked. At the bottom of the window are buttons for 'OK', 'Cancel', 'Remove', 'Import...', and 'Help'.

SIP Application Configuration: Span: 1

General Preferences Firewall Telephony Private Network SIP Proxy Recording

☒ Enable Call Recording

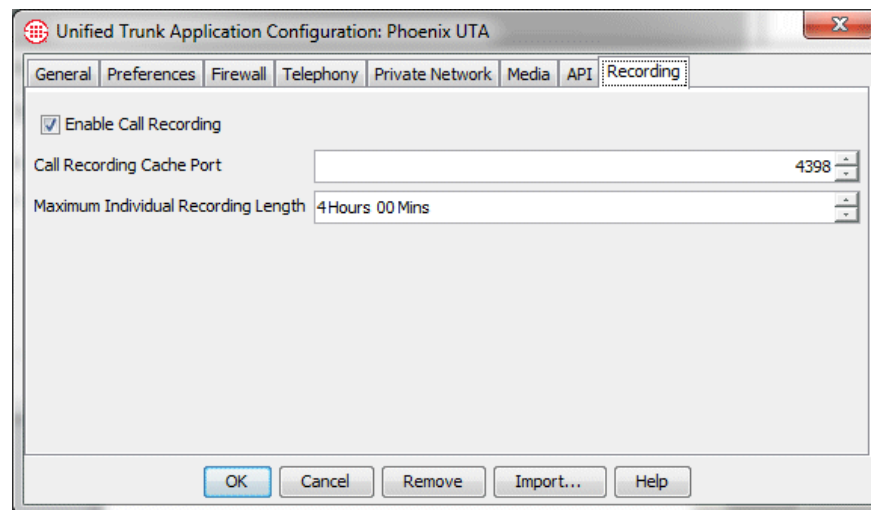
Call Recording Cache Port 4398

Maximum Individual Recording Length 4 Hours 00 Mins

☐ Request Inbound SMDR

OK Cancel Remove Import... Help

UTA Span Recording Tab



The screenshot shows the 'Unified Trunk Application Configuration: Phoenix UTA' window with the 'Recording' tab selected. The window has a title bar with a red 'X' button. Below the title bar is a tabbed interface with tabs for 'General', 'Preferences', 'Firewall', 'Telephony', 'Private Network', 'Media', 'API', and 'Recording'. The 'Recording' tab is active. Inside the tab, there is a checkbox labeled 'Enable Call Recording' which is checked. Below this is a text field for 'Call Recording Cache Port' with the value '4398'. Below that is a text field for 'Maximum Individual Recording Length' with the value '4 Hours 00 Mins'. At the bottom of the window are buttons for 'OK', 'Cancel', 'Remove', 'Import...', and 'Help'.

Unified Trunk Application Configuration: Phoenix UTA

General Preferences Firewall Telephony Private Network Media API Recording

☒ Enable Call Recording

Call Recording Cache Port 4398

Maximum Individual Recording Length 4 Hours 00 Mins

OK Cancel Remove Import... Help

TDM Span Recording Tab

T1 Span Configuration: Span: 1

General Preferences Firewall Telephony Channel Map T1 Setup **Recording**

☒ Enable Call Recording

Call Recording Cache IP Address Modify

Call Recording Cache Port

Maximum Individual Recording Length

Channel Level Recording Details

Channel	Record Inbound	Record Outbound
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>


OK Cancel Remove Import... Help

Specifying the CRC to Use (TDM)

SIP and UTA Spans always use their local CRC. Other Spans can use either their local CRC (the CRC on the same Card as the Span—1024 and 1090 Cards only) or a dedicated CRC Appliance. By default, *localhost* (127.0.0.1) is specified. If the Span is to use its local CRC, skip this procedure. CRCs coresident with telco Spans can accept connections only from their local Spans.

To use a dedicated CRC Appliance, use the procedure below. If a Recording Span cannot connect to a CRC, no recording can occur. If a Recording Span loses connection to its CRC while recording is in progress, recording ceases and those recordings are discarded.

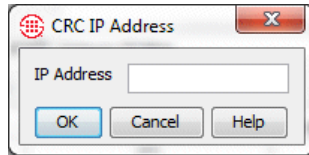
IMPORTANT Be sure to add this Span to the specified CRC's list of authorized Recording Spans so the connection is allowed.

 This icon indicates that a Span is not connected to its CRC.

Note: When you have completed Span configuration, click **OK** to download the changes to the Span(s) and close the dialog box. No changes take effect until you click **OK** to close the dialog box.

To specify a dedicated CRC Appliance on which calls are to be recorded

1. Open the **Span Configuration** dialog box.
2. Click the **Recording** tab.
3. Under the **Call Recording Cache IP Address** box, click **Modify**. The **CRC IP Address** dialog box appears.



4. In the **IP address** box, type the IPv4 or IPv6 address of the CRC where this Span's calls are to be recorded.

Changing the CRC Port

Note: When you have completed Span configuration, click **OK** to download the configuration to the Span and close the dialog box. No changes take effect until you click **OK**.

By default, CRCs accept connections from Recording Spans on port **4398**. If the CRC for this Recording Span uses a different port, change the setting on the Recording Span to correspond to the port set on the CRC or the Recording Span will be unable to connect to the CRC. If the default port is used, skip this procedure and continue with the next procedure.

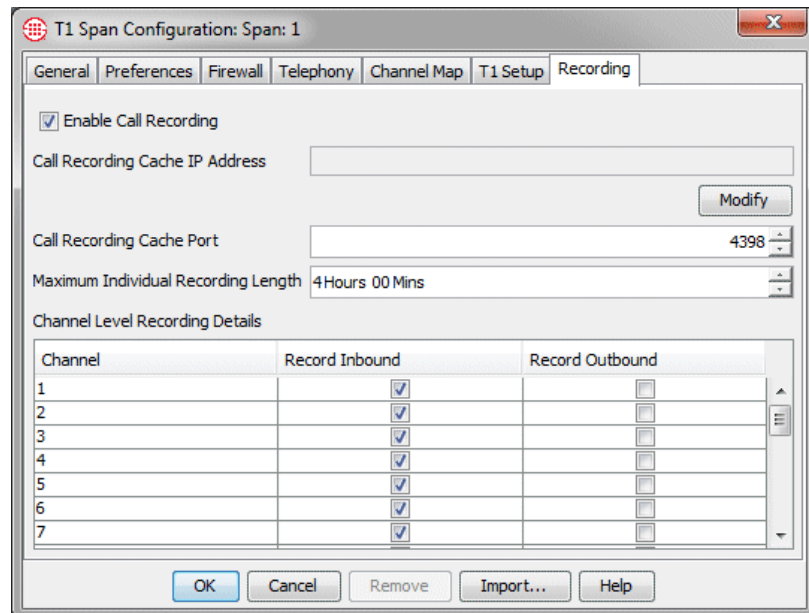
To change the CRC port

1. Open the **Span Configuration** dialog box and click the **Recording** tab.
2. In the **Call Recording Cache Port** box, type or select the port number on which the specified CRC accepts connections from Recording Spans.

Specifying Which Channels to Record (TDM)

To specify which channels to record (not on SIP or UTA)

1. Open the **Span Configuration** dialog box and click the **Recording** tab.



2. The **Channel Level Recording Details** area provides a row for each channel on the selected Span. For each channel:

- To record inbound calls on the channel, select the **Record Inbound** check box. Clear the check box if inbound calls are not to be recorded on this channel.
- To record outbound calls on the channel, select the **Record Outbound** check box. Clear the check box if outbound calls are not to be recorded on this channel.

Setting the Maximum Individual Recording Length

To set the maximum length for an individual call recording

1. Open the **Span Configuration** dialog box and click the **Recording** tab.
2. In the **Maximum Individual Recording Length** box, type or select a value, from 1 minute to 8 hours. The default is 4 hours.

Requesting Inbound SMDR

(*Not on UTA*) On SIP and TDM Spans, inbound SMDR can be used to identify the called extension for recorded calls, to allow special handling for recordings of calls to certain extensions. It can also be used to supply the destination number in the stored call recording data on the CRC.

On SIP Spans, a Span-level setting applies to all calls.

On TDM Spans, you specify per channel whether Inbound SMDR is to be requested. SMDR Extension processing only applies to channels on which Inbound SMDR is enabled. Inbound SMDR is only used for SMDR Extension processing and to supply the destination in the recorded call data; it is not used for Policy processing.

To enable Inbound SMDR

- **SIP Spans:** On the **Recording** tab of the **Span Configuration** dialog box, select **Request Inbound SMDR**.
- **TDM Spans:** On the **Channel Map** tab, in the **Request Inbound SMDR** column, select each recording-enabled channel on which Inbound SMDR is to be used.

See “Configuring SMDR Extensions” on page 36 for an overview and instructions for defining them.

How the Companding Setting Affects TDM Recording Spans

The **Companding** setting on the **Channel Map** tab of TDM Spans tells the Span whether to expect A-law or Mu-law data on a particular channel. For call recording, the Span captures the raw data according to the companding setting and sends the files to the CRC, which optionally sends them to the Collection Server. The filters on the Collection Server convert the A-law or Mu-law data to PCM (linear) for audio files. For data files (fax, modem), the final format is Mu-law, so A-law recording files are converted to Mu-law WAV files.

The companding setting has no bearing on the final WAV file format, but is necessary to make sure the data is captured in the right format on the TDM Recording Span..

Configuring SMDR Extensions

(*Not available on UTA*) SMDR Extensions are internal phone numbers identified by inbound SMDR correlation for which you want to prescribe special 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:

When **Enable SMDR Extension Processing** is selected, SMDR Extension processing occurs before calls are made available via the Web Portal and before they are transferred to the Collection Server, if one is used.

SMDR Extensions are defined per Switch, not per Span. Assign Spans to the Switch containing the applicable SMDR Extensions list.

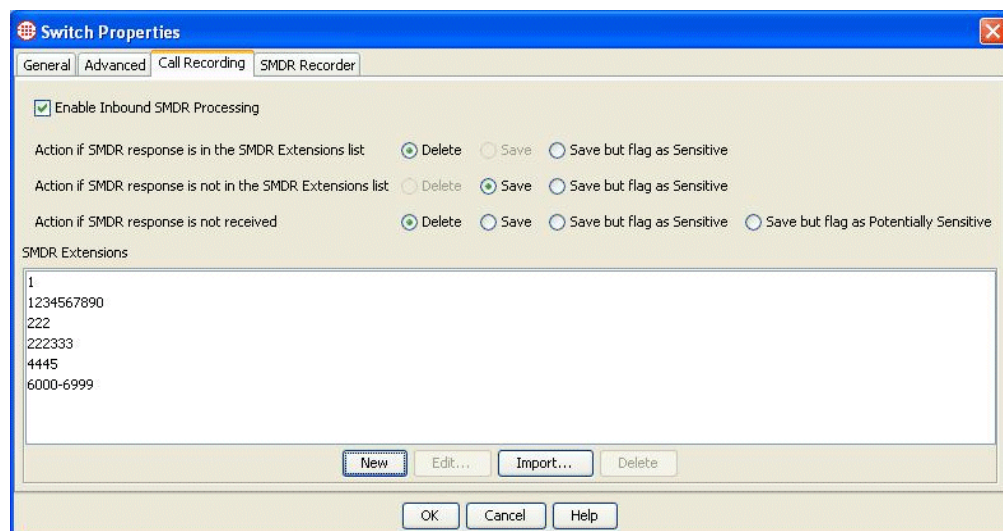
Defining SMDR Extensions

Tip After you have defined a list of SMDR Extensions for one Switch, you can import it into another Switch. See “Importing SMDR Extensions” on page 39 for details.

SMDR Extensions can only be identified on channels for which Inbound SMDR is enabled. Channels for which Inbound SMDR is not enabled cannot use SMDR Extensions and ignore the **Enable SMDR Extension Processing** setting.

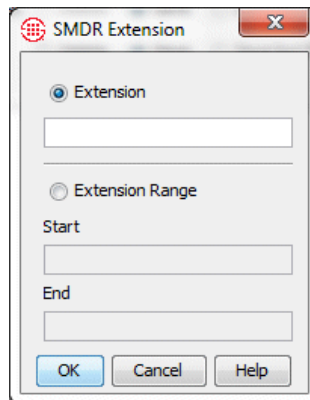
To define SMDR Extensions

1. In the **Telco Configuration** subtree of the Performance Manager, right-click the Switch to which the Recording Spans belong, and then click **Edit Switch**. The **Switch Configuration** dialog box appears.
2. Click the **Call Recorder** tab.



IMPORTANT: Enable Inbound SMDR on channels that are to observe the **SMDR Extensions** list.

3. Select **Enable SMDR Extension Processing**. This setting applies only to channels on which Inbound SMDR is enabled; it is ignored on channels that do not request Inbound SMDR.
4. Click **New**. The **SMDR Extension** dialog box appears.



5. Do one of the following:
 - Type a single internal extension.
 - Select **Extension Range** and type the starting extension and ending extension.
6. Click **OK**. Note that the entries are compared to the values in raw SMDR data. They are not converted to fully qualified numbers for SMDR Extension processing. (The values in the SMDR data may be converted to fully qualified numbers by the Dialing Plan after the SMDR Extension comparison has occurred, but this information is only stored in the destination field of the call information associated with the recording file. It is not used for Policy or SMDR Extension processing.)
7. Repeat steps 3 and 4 for each SMDR extension or range.

IMPORTANT The handling options are grayed out until you populate the **SMDR Extensions** list.

Note If the handling options are grayed out after you add one or more extensions to the list, a Span that is not upgraded to v7.1.1 or later is assigned to the Switch. Since this Span cannot support the new functionality until it is upgraded, the options are unavailable. If you upgrade all Spans and CRCs, the options become available.

8. Select handling options for these extensions:
 - **Action if SMDR response is in the SMDR Extension list**— If the SMDR response correlates with an entry in the SMDR extensions list:
 - **Delete**—Discard the recording.
 - **Save**—Treat the recording like any other recording.

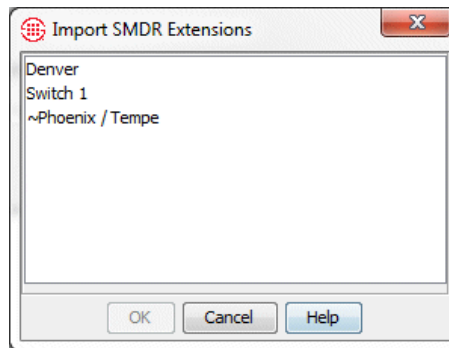
- **Save but flag as Sensitive**—Retain the recording but tag it as Sensitive in the metadata. Sensitive and Potentially Sensitive recordings are stored in a parallel directory structure on the Collection Server where access can be restricted with operating system permissions. Note that these recordings cannot be accessed via the Web Portal.
 - **Action if SMDR response is not in the SMDR Extension list**—If no entry in the SMDR Extensions list correlates with inbound SMDR results::
 - **Delete**—Discard the recording.
 - **Save**—Treat the recording like any other recording.
 - **Save but flag as Sensitive**—Retain the recording but tag it as Sensitive in the metadata. Sensitive and Potentially Sensitive recordings are stored in a parallel directory structure on the Collection Server where access can be restricted with operating system permissions. Note that these recordings cannot be accessed via the Web Portal.
 - **Action if SMDR response is not received**—If an SMDR record is not correlated with the call for any reason:
 - **Delete**—Discard the recording.
 - **Save**—Treat the recording like any other recording.
 - **Save but flag as Sensitive**—Retain the recording but tag it as Sensitive in the metadata. Sensitive and Potentially Sensitive recordings are stored in a parallel directory structure on the Collection Server where access can be restricted with operating system permissions.
 - **Save but flag as Potentially Sensitive**—Since the SMDR was not resolved, it is unknown whether the recording is sensitive or not. This flag denotes this situation. Sensitive and Potentially Sensitive recordings are stored in a parallel directory structure on the Collection Server where access can be restricted with operating system permissions. Note that these recordings cannot be accessed via the Web Portal.
9. When you are done, click **OK**. No changes to any tab are saved until you click **OK**.
 10. A message appears informing you that changes will be downloaded to the device, in this case, the Recording Spans that belong to this Switch. Click **OK**.

Importing SMDR Extensions

You can import the list of SMDR Extensions from one Switch to another.

To import SMDR Extensions

1. In the **Telco Configuration** subtree of the Performance Manager, right-click the Switch into which you want to import **SMDR Extensions** and click **Edit Switch**. The **Switch Configuration** dialog box appears.
2. Click the **Call Recorder** tab.
3. Click **Import**. The **Import SMDR Extensions** dialog box appears.



4. Click the Switch that contains the SMDR Extensions you want to import, and then click **OK**. The list of extensions appears on the **SMDR Extensions** tab.
5. Select the handling options you want for the imported extension. Only the extensions are imported, not the settings. See “Defining SMDR Extensions” on page 36 for a description of the handling options.
6. Click **OK** to save the changes and download the list to the Recording Spans assigned to this Switch. Changes are not saved nor applied until you click **OK**.

Configuring the Collection Server

The Collection Server optionally provides offsite disk storage and conversion of recorded calls into formats compatible with third-party playback and analysis tools. The Collection Server can accept call recordings from up to twenty CRCs simultaneously; however, you can set a lower limit if needed by your network environment.

To use the Sensitive and Potentially Sensitive handling flags with SMDR Extensions, you must use a Collection Server. These flagged recordings are not available from the Web Portal.

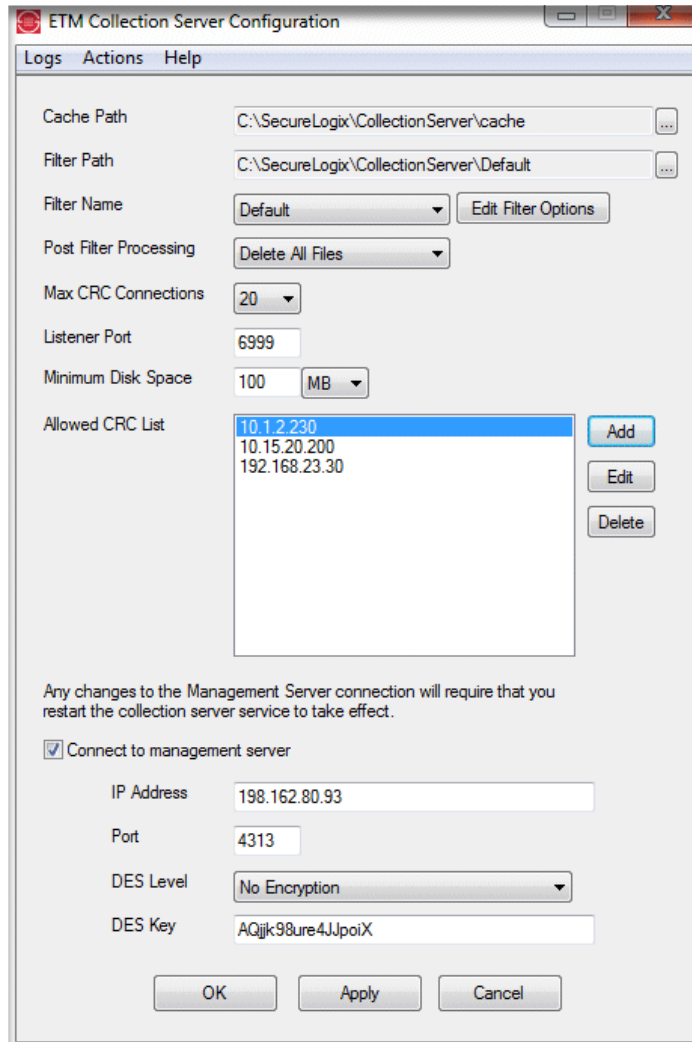
The Collection Server runs as a service on a Windows system that has a sufficiently large storage capacity dedicated to call recording storage and LAN/WAN access to the CRCs. See the Minimum System Requirements for supported versions of Windows.

By default, the Collection Server service starts automatically when the host computer is booted, and runs in the background at all times. You can

start/stop the Collection Server in the same way as any other Windows service.

To configure the Collection Server

1. Open the **Collection Server Configuration Tool** by double-clicking its icon on the desktop of the computer where the Collection Server is running.



2. The **Cache Path** box specifies where files received from the CRCs are stored. The default is:

C:\Program Files\SecureLogix\CollectionServer\cache

- To specify a different cache path, do one of the following:

- Type the complete path to the folder where files received from CRCs are stored to await filter processing.

OR

- Click the **Browse** button to browse for the folder where files received from CRCs are to be stored to await filter processing.

3. The **Filter Path** box specifies where the filtered files are to be stored. Note that changes to the path take effect at the next CRC connection. They do not affect current connections. The default path is:

C:\Program Files\SecureLogix\CollectionServer\Default

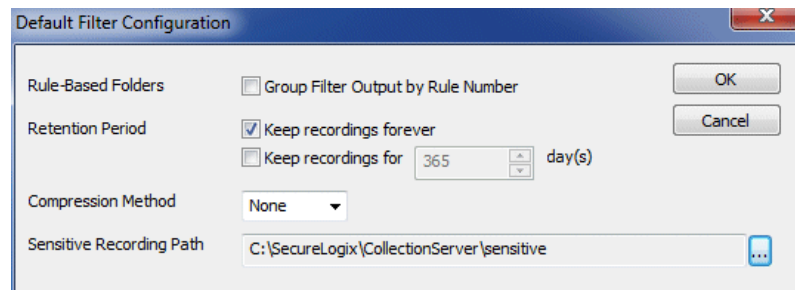
- To specify a different cache path, do one of the following:
 - Type the complete path to the folder where filtered files are stored.

OR

- Click the **Browse** button to browse for the folder where the filtered files are to be stored.

4. The **Filter Name** box specifies the filter to be used to process the files: **Default** or **TSAP**. The default setting is the **Default** filter.

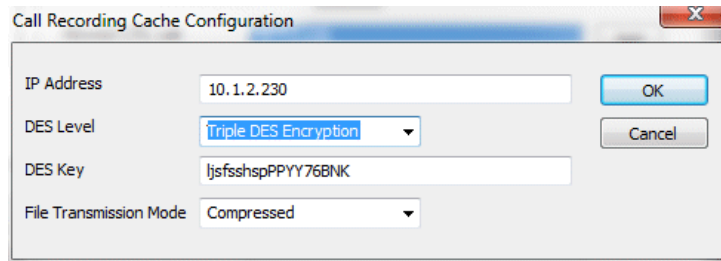
- If you select **Default**, click **Edit Filter Options** and configure any of the following options:



- a. **Group Output By Rule Number**—By default, output is grouped by Policy Name and then by the Date of the recording. If you select **Group Filter Output By Rule Number**, output is grouped by Policy Name, and then by Rule Number, and then the by Date of the recording. This allows the administrator of the Collection Server computer to assign Windows folder access permissions per rule number, to control who has access to different types of recordings, according to the purpose of the rule.
- b. **Retention Period**—If you want recordings to be automatically purged after a certain amount of time, select **Keep recording for *n* days** and then type or select the

number of days, from 1 to 9999. By default, recordings are retained permanently.

- c. **Compression Method**—You can optionally compress the WAV files of voice calls on the Collection Server. To compress the files, select **GSM-FR**. **None** is the default. .
 - d. **Sensitive Recording Path**—Specifies the path where Call Recordings flagged as Sensitive by the SMDR Extension processing are stored. . Click the icon and browse to and select the location.
 - e. Click **OK** to save the filter configuration and close the dialog box.
- To use the TSAP filter, click the down arrow and click **TSAP**.
5. Post-filter file processing determines what is done with the raw call recording data received from the CRCs. Options are to retain all files, retain only error files, or discard all files. See "Post-Filter Processing" on page 80 for more information.
 6. In the **Post-Filter Processing** box, click the down arrow and select an option:
 - **Delete All Files** (the default)
 - **Keep Error Files Only**
 - **Keep All Files**
 7. The default **Max CRC Connections** is 20. To allow fewer, click the down arrow and click a different number.
 8. The Collection Server Listener Port is the port on which the Collection Server accepts connections from authorized CRCs. The default port is 6999. To use a different port:
 - In the **Listener Port** box, type the port number. It is recommended that you choose a port above 5000.
 9. **Minimum Disk Space**—The default is 100 MB. The Collection Server continually monitors the amount of available disk space. When the available disk space falls below a user-configurable threshold, the software generates a warning log message and a warning message appears on the desktop. Until the disk space issue is addressed, no new connections from CRCs are accepted and filtering of raw uploaded files is disabled. Once disk space is freed or the configured threshold is lowered, the Collection Server automatically resumes connection processing and filtering. You can optionally enable automated purging of recordings at a specified interval. Otherwise, be sure to respond promptly to disk space warnings.
 10. Next to the **Allowed CRC List** box, click **Add**. The **Call Recording Cache Configuration** dialog box appears.



11. In the **IP Address** box, type the IP address of the authorized CRC.
12. In the **DES Level** box, click the down arrow and select the level of encryption: **No Encryption**, **Single DES Encryption**, or **Triple DES Encryption**.
13. In the **DES Key** box, type the DES Key used for encrypted communication between the CRC and the Collection Server. The DES Key must always match between the CRC and the Collection Server; initial communication is always encrypted to validate the connection, regardless of whether encryption is specified.
14. In the **File Transmission Mode** box, click the down arrow and select **Compressed** or **Uncompressed** for the communication stream between the CRC and the Collection Server. **Compressed** is recommended for high-volume call recording.
15. Click **OK**. The CRC's IP address appears in the **Allowed CRC List** box.
16. To enable the Collection Server to be searchable via the ETM Web Portal, configure it to connect to the Management Server:
 - a. Select **Connect to Management Server**.
 - b. In the **IP Address** box, type the IP address of the ETM Server.
 - c. In the **Port** box, type the port on which the ETM Server accepts connections from Appliances and Collection Servers.
 - d. In the **DES Level** box, select the level of DES Encryption for communication between the ETM Server and the Collection Server. Options are **None**, **Single DES**, or **Triple DES**.
 - e. In the **DES Key** box, type the DES key for ETM Server/Collection Server communication. This is the Appliance DES key. The DES Key must be in sync between the ETM Server and the Collection Server, because the initial connection is always encrypted to validate the connection.
17. Click **OK** to save the changes and close the tool; click **Apply** to save the changes and leave the tool open.
18. If you made changes to the Server connection information, restart the Collection Server service for the changes to take effect.

About the ETM® Collection Server Configuration Tool

The **ETM® Collection Server Configuration Tool** provides options to configure storage directories, filters, listener port, and maximum connections; specify which CRCs are authorized to send data to the Collection Server; and dictate what to do with the files after processing.

The screenshot shows the 'ETM Collection Server Configuration' window. It has a menu bar with 'Logs', 'Actions', and 'Help'. The main area contains several configuration fields: 'Cache Path' (C:\SecureLogix\CollectionServer\cache), 'Filter Path' (C:\SecureLogix\CollectionServer\Default), 'Filter Name' (Default), 'Post Filter Processing' (Delete All Files), 'Max CRC Connections' (20), 'Listener Port' (6999), 'Minimum Disk Space' (100 MB), and 'Allowed CRC List' (10.1.2.230, 10.15.20.200, 192.168.23.30). There are 'Add', 'Edit', and 'Delete' buttons for the CRC list. At the bottom, there is a section for 'Connect to management server' with fields for 'IP Address' (198.162.80.93), 'Port' (4313), 'DES Level' (No Encryption), and 'DES Key' (AQijk98ure4JjpoiX). The window has 'OK', 'Apply', and 'Cancel' buttons at the bottom.

The Collection Server continually monitors changes to its configuration file; if it detects that the file has changed, the file is re-read and changes are applied immediately. Except for changes to the ETM Server connection information, you do not need to stop the Collection Server to configure it, nor do you need to restart the Collection Server after changing its configuration. Configuration changes are applied seamlessly on a transactional basis.

If you change the ETM Server information, restart the Collection Server service to effect the changes.

To open the ETM[®] Collection Server Configuration Tool

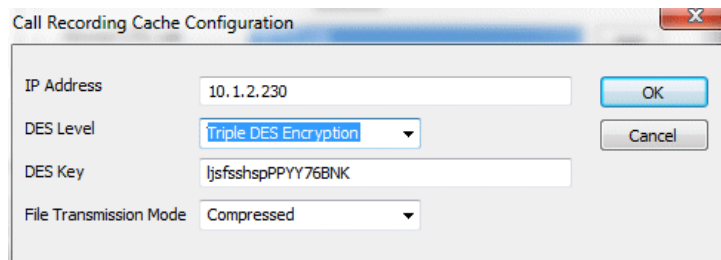
- On the Windows desktop, double-click the **ETM Collection Server Configuration Tool** icon.

Authorizing CRCs to Connect to the Collection Server

The Collection Server can store call recordings from up to 20 CRCs, but only accepts connections from CRCs authorized in the Collection Server's **Allowed CRC List**.

To add CRC to the Allowed CRC List

- Open the **Collection Server Configuration Tool**.
- Next to the **Allowed CRC List** box, click **Add**. The **Call Recording Cache Configuration** dialog box appears.



- In the **IP Address** box, type the IP address of the authorized CRC.
- In the **DES Level** box, click the down arrow and select the level of encryption: **No Encryption**, **Single DES Encryption**, or **Triple DES Encryption**.
- In the **DES Key** box, type the DES Key used for encrypted communication between the CRC and the Collection Server. The DES Key must always match between the CRC and the Collection Server; initial communication is always encrypted to validate the connection, regardless of whether encryption is specified.
- In the **File Transmission Mode** box, click the down arrow and select **Compressed** or **Uncompressed** for the communication stream between the CRC and the Collection Server. **Compressed** is recommended for high-volume call recording.
- Click **OK**. The CRC's IP address appears in the **Allowed CRC List** box.
- Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

Editing a CRC Authorization

To edit a CRC authorization

1. Open the **Collection Server Configuration Tool**.
2. In the **Allowed CRC List** box, click the authorized CRC for which you want to edit information, and then click **Edit**. The **Call Recording Cache Configuration** dialog box appears.
3. Change settings as needed, and then click **OK**. See "Authorizing CRCs to Connect to the Collection Server" on page 45 for details about each field, if necessary.

Deleting a CRC Authorization

If you delete a CRC authorization, the CRC is no longer allowed to connect.

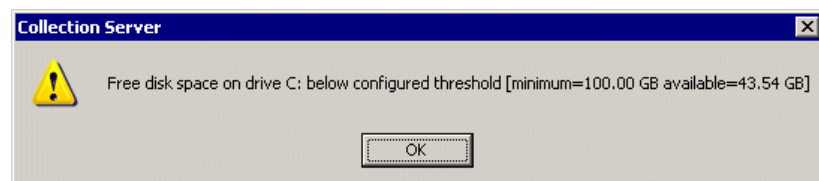
To delete a CRC authorization

1. Open the **Collection Server Configuration Tool**.
2. In the **Allowed CRC List** box, click the CRC for which you want to remove authorization, and then click **Delete**.

Setting the Minimum Disk Space Allowed on the Collection Server

The Collection Server continually monitors the amount of available disk space. When the available disk space falls below a user-configurable threshold, the software generates a warning log message and a warning message appears on the desktop. Until the disk space issue is addressed, no new connections from CRCs are accepted and filtering of raw uploaded files is disabled. Once disk space is freed or the configured threshold is lowered, the Collection Server automatically resumes connection processing and filtering.

IMPORTANT Be sure to regularly monitor disk space, respond promptly to low disk space warnings, and remove recordings to archival media to avoid running out of disk space. Optionally, you can configure automatic purging. This is especially important if you install the Collection Server on your primary partition.



To set the minimum disk space allowed

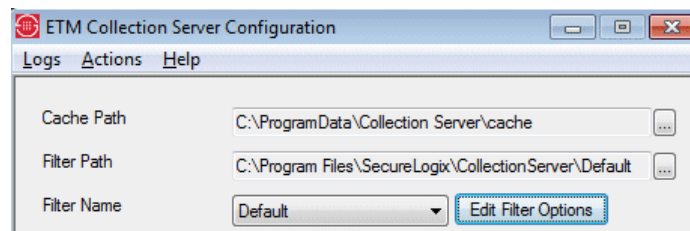
1. Open the **Collection Server Configuration** Tool.
2. In the **Minimum Disk Space** boxes:
 - In the first box, type the size. It is recommended that you specify at least 500 MB free.
 - In the second box, click the down arrow and click the unit of measure: **MB** or **GB**.
3. Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

Automated Collection Server Purging

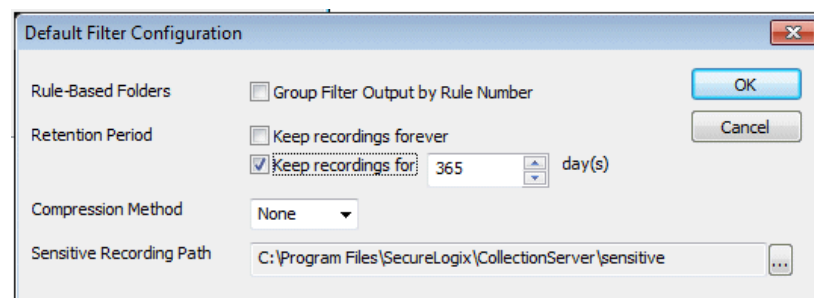
When you use the Default filter, you can enable automatic purging on the Collection Server to avoid running out of configured disk space, which prevents transfer of new calls. Automatic purging is not available for the TSAP filter.

To configure Collection Server purging

1. In the **ETM Collection Server Configuration** tool, with the **Default** filter selected, click **Edit Filter Options**.



2. The **Default Filter Configuration** dialog box appears.



3. Do one of the following:
 - To disable automatic purging and use manual purging, select **Keep recordings forever**.
 - To enable automatic purging, select **Keep recordings for** and specify the number of days of files to keep. The default is **365**. The purger deletes all recordings older than the number of days

specified plus 1 (to account for calls that cross day boundaries). The boundary is a day directory, so if any of the recordings in the directory are too old, the entire directory is deleted.

The purger runs hourly, but when you change the retention period, the purger runs immediately after the change is committed.

NOTE If purging is enabled, but no calls are eligible to be purged and a CRC pushes a call that fills the available space. It won't be able to push another call until you manually free up space, allocate more, or change the retention interval.

Changing the Collection Server Listener Port

The Collection Server Listener Port is the port on which the Collection Server accepts connections from authorized CRCs. The default port is 6999. If you change the port value here, be sure to change it in the configuration for each CRC that uses this Collection Server, or they will be unable to connect. See “Enabling the CRC to Use a Collection Server” on page 27 for instructions, if necessary.

To change the Collection Server Listener Port

1. Open the **Collection Server Configuration Tool**.
2. In the **Listener Port** box, type the port number. It is recommended that you choose a port above 5000.
3. Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

Setting the Maximum Number of Allowed Cache Connections

By default, the Collection Server accepts simultaneous connections from up to twenty CRCs. However, you can reduce this number to suit network conditions at your location.

To set the maximum number of simultaneous CRC connections

1. Open the **Collection Server Configuration Tool**.
2. In the **Max. Cache Connections** box, click the down arrow and select one of the options, from **0** to **20**. If you select **0**, no CRCs are allowed to connect.
3. Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

Specifying the Cache Path

To specify the path at which to store files from CRCs

1. Open the **Collection Server Configuration Tool**.
2. In the **Cache Path** box, do one of the following:
 - Type the complete path to the folder where files received from CRCs are stored to await filter processing.

- Click the **Browse** button to browse for the folder where files received from CRCs are to be stored to await filter processing.
3. Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

Specifying the Filter Path

The filter path specifies where the filtered files are to be stored. Note that changes to the path take effect at the next CRC connection. They do not affect current connections.

To specify the path for the filtered files

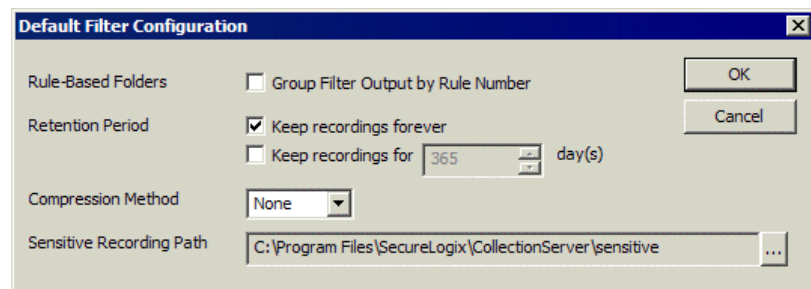
1. Open the **Collection Server Configuration Tool**.
2. In the **Filter Path** box, do one of the following:
 - Type the complete path to the folder where the filtered files are to be stored.
 - Click the **Browse** button to browse for the folder where the filtered files are to be stored.
3. Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

Selecting the Filter

The **Filter Name** box identifies the filter to be used to convert the received data for playback and analysis: **Default** (most common) or **TSAP**

To select a filter

1. Open the **Collection Server Configuration Tool**.
2. In the **Filter Name** box, click the down arrow and select the filter.
 - If you select **Default**, click **Edit Filter Options** and configure any of the following options:



- a. **Group Output By Rule Number**—By default, output is grouped by Policy Name and then by the Date of the recording. If you select **Group Filter Output By Rule Number**, output is grouped by Policy Name, and then by Rule Number, and then the by Date of the recording. This allows the administrator of the Collection Server computer to

assign Windows folder access permissions per rule number, to control who has access to different types of recordings, according to the purpose of the rule.

- b. **Retention Period**—If you want recordings to be automatically purged after a certain amount of time, select **Keep recording for *n* days** and then type or select the number of days, from 1 to 9999. By default, recordings are retained permanently.
- c. **Compression Method**—You can optionally compress the WAV files of voice calls on the Collection Server. To compress the files, select **GSM-FR**. **None** is the default.
- d. **Sensitive Recording Path**—Specifies the path where Call Recordings flagged as Sensitive by the SMDR Extension processing are stored.

Specifying Post-Filter Processing

Post-filter file processing determines what is done with the raw call recording data received from the CRCs. Options are to retain all files, retain only error files, or discard all files. See "Post-Filter Processing" on page 80 for more information.

To specify post-filter processing

1. Open the **Collection Server Configuration Tool**.
2. In the **Post-Filter Processing** box, click the down arrow and select an option:
 - **Delete All Files** (the default)
 - **Keep Error Files Only**
 - **Keep All Files**
3. Click **Apply** to apply the change and leave the GUI open. Click **OK** to apply the change and close the GUI.

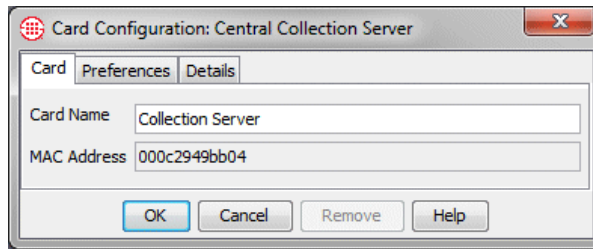
Naming the Collection Server

When the Collection Server connects to the ETM Server, by default it is named "Collection Server." If more than one Collection Server connects, each is named "Collection Server <MAC_Address>". You can optionally provide a user-defined name for the Collection Server to make it easier to identify in the Performance Manager and the Web Portal **Search** box.

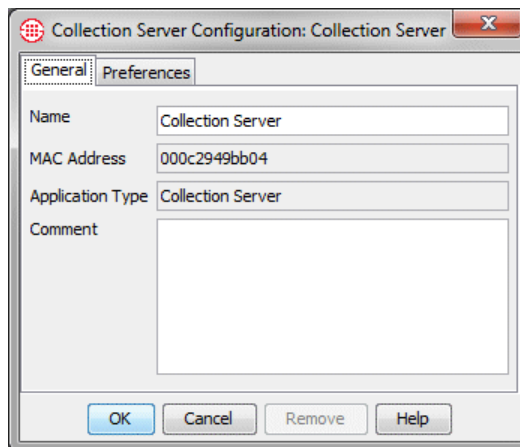
As with all Platform types, the Collection Server is represented in the tree pane by a Card-level icon with a Span-level icon below it, although it has no Cards or Spans.

To name the Collection Server

1. In the Performance Manager tree pane, right-click the Collection Server Card-level icon and click **Edit Cards**.



2. Type a user-defined name for the Collection Server and then click **OK**. For example, you might type : **Collection Server-Dallas**.
3. In the Performance Manager tree pane, Expand the Card node of the Collection Server.
4. Right-click the Collection Server Span-level icon and click **Edit Collection Server Application**.



5. In the **Name** box, type the name to identify this Collection Server. For example, you might type : **Collection Server-Dallas**.
6. Optionally, type a tool tip comment.
7. Click **OK** to save the changes and close the dialog box.

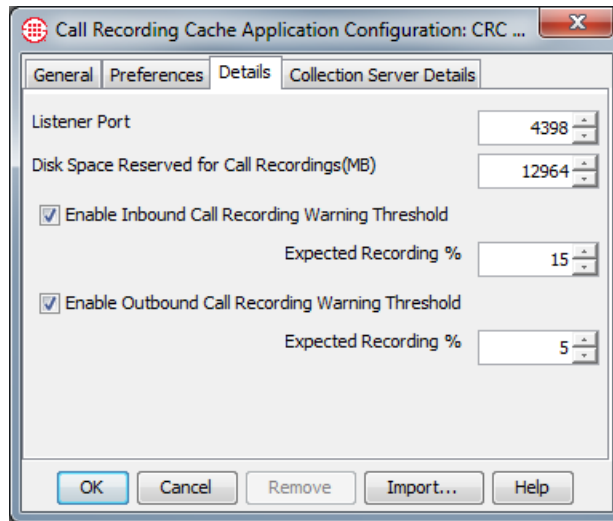
Monitoring Expected Call Recording Volume

Setting Thresholds for Expected Call Recording Volume

You can set thresholds for expected volume of inbound and outbound call recordings as a percentage of call volume, and then configure a System Event to alert you when a threshold is not met. A drop in the expected volume of call recordings may indicate an error condition resulting in calls not being recorded as expected.

To set thresholds

1. In the **Call Recording Cache Application Configuration** dialog box, click the **Details** tab.



2. Select **Enable Inbound Call Recording Warning Threshold** and type or select the expected percentage of inbound calls to be recorded. A warning appears in the Diagnostic Log if the percentage of recorded calls falls below this threshold. This can alert you if inbound call recordings are failing, due to faulty configuration or other issues.
3. Select **Enable Outbound Call Recording Warning Threshold** and type or select the expected percentage of outbound calls to be recorded. A warning appears in the Diagnostic Log if the percentage of recorded calls falls below this threshold. This can alert you if outbound call recordings are failing, due to faulty configuration or other issues.

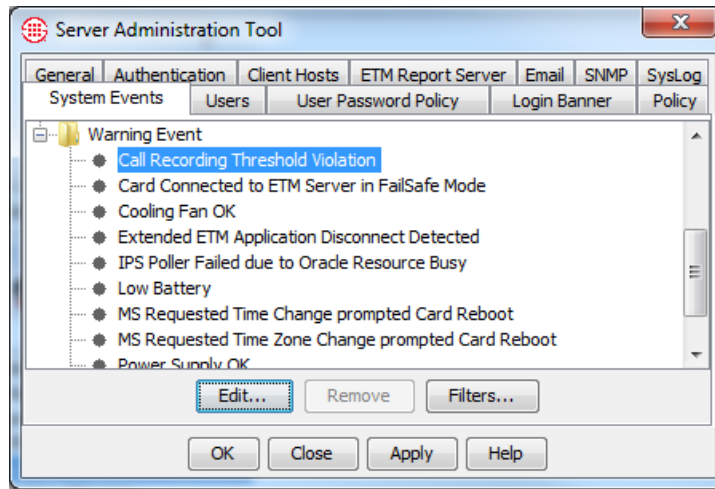
Configuring an Alert for Threshold Violations

Configure the following System Event generate an alert when the threshold is violated:

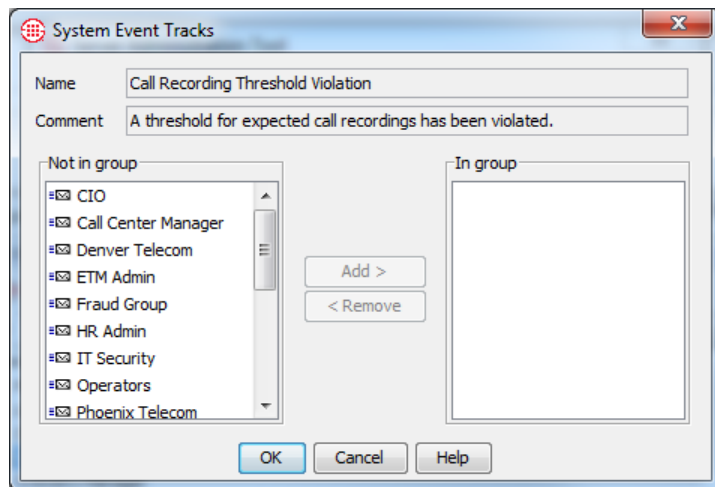
- **Call Recording Threshold Violation**—The user-defined threshold of expected call recordings was not met. This can indicate the calls have stopped being recorded due to a Call Recorder issue.

To configure the alert

1. In the ETM System Console, click the name of the Server and then click the **Server Administration Tool** icon on the toolbar. The **System Administration Tool** appears.
2. Click the **System Events** tab.
3. Click the PLUS SIGN to expand the **Warning Events** node and then click **Call Recording Threshold Violation**.



4. Click **Edit**. The **System Event Tracks** dialog box appears.



5. In the **Not in Group** box, do one of the following:
 - Double-click each Track you want to receive an alert when a threshold is not met. They are added to the **In group** box.
 - Hold down CTRL or SHIFT and select the set of Tracks you want to receive an alert when a threshold is not met, and then click **Add** to add the selected Tracks to the **In group** box.
6. Click **OK**.
7. On the **Server Administration Tool**, click **OK** to save the changes and close the dialog box or **Apply** to save the changes and leave the dialog box open.

Where to Go From Here

The Call Recorder is now ready to use for recording calls. Next, you need to define and install a Recording Policy that specifies which calls you want to record. The next chapter provides detailed instructions for defining and installing a Recording Policy and for accessing completed recordings.

Using the Call Recorder

Recording and Accessing Calls

To record calls, you define and install a Recording Policy on each Call Recording Span. The Recording Policy identifies the calls that are to be recorded, using a set of Rules that specify call attributes of calls to be recorded, such as source, destination, call type, and so on. After you define and install the Policy, no further user intervention is needed to record calls. Calls that match a Record rule in the Policy are automatically recorded.

When a call that is supposed to be recorded ends, the recording is stored on the CRC and available for playback and download via the Web Portal. If no Collection Server is used, the call recording is stored on the CRC until storage constraints cause it to be overwritten, oldest files first (the time varies according to call load).

If a Collection Server is used, the call recording is stored on the CRC only until it is transferred to the Collection Server. Call Recordings on the Collection Server can also be accessed via the Web Portal. They can also be accessed on the Collection Server computer, using third-party play back and analysis tools.

All access to recordings via the Web Portal is logged in the Diagnostic Log.

Recording Calls

To record calls with the Call Recorder, you define and install a *Recording Policy* that specifies which calls are to be recorded. Calls that do not match a Record rule in the Policy are not recorded.

Understanding Recording Policies

A Recording Policy consists of a set of Rules that define specific calls to be recorded. Calls can be identified for recording by any combination of call direction, called and/or calling phone numbers, call time, and call type. Recording begins at the start of a call while Policy processing is performed. Only recordings of calls that match all of the criteria in a Rule throughout the life of the call are retained. As with other Policy types, a call can match more than one Rule if call type changes during the call.

IMPORTANT Calls are only recorded if they match a Rule that specifies **Record**. You can also define rules that specify **Do Not Record**. Every Recording Policy has an Implied Policy Rule that prevents recording of any

calls that never match a recording rule. Additionally, the SMDR Extension list* enables you to define internal extensions to which inbound calls are never to be recorded, based on internal SMDR data.

* SMDR Extensions are not available on UTA.

How Call Recorder Policies Interact with Other Policies

When a call matches both a **Record** Rule in a Recording Policy and a Rule in a Firewall or IPS Policy, the **Action** field of the IPS or Firewall Policy determines the outcome of the call:

- If the Firewall or IPS Rule specifies **Terminate**, the call is terminated, even if recording has already begun. In this case, a message is sent to the **Diagnostic Log** and recording ceases. If the duration of the recorded portion of the call is greater than one second, the recording is retained; if less, it is deleted.
- If the Firewall or IPS Rule specifies **Allow**, recording continues at the same time as the call is processed against the Firewall or IPS Rule.

Rule Order

Rule order is important in Recording Policies when **Do Not Record** rules are used and when a given call would match two Rules. In this case, the call is recorded or not recorded according to the first applicable Rule. If it is recorded and matches two rules, the **Priority** setting of the first matching rule applies. The **Priority** setting governs the order in which calls are transferred from the CRC to the Collection Server, if one is used, and for deleting recordings when disk space limits are reached.

For example, if Rule 1 specifies that calls that are not Voice be recorded and has a priority of **Low**, while Rule 2 specifies that Fax calls be recorded and has a priority of **Medium**, a Fax call matches both Rules. The call will trigger Rule 1 and result in a priority of **Low**.

About Call Type Changes

Each Rule in a Recording Policy can specify one or more call types to which the Rule applies, or it can apply to calls of **Any** type. Recording always begins at the start of the call, while it may take several seconds for call type to be identified. Once determined, if the initial call type does not match any **Record** Rule in the policy, recording stops and the recording file is discarded.

If the call matches a **Record** Rule after call type is determined, recording continues for the duration of the call, as long as the call type continues to be one specified by any **Record** Rule in the Policy.

If the call type changes during the call such that the call no longer matches any **Record** rule, whether recording continues depends on a setting on the **Attributes** tab of the policy:

- **Discard the recording**—(Default) If the call type changes during a call, the call is again processed against the Policy. If, with the new call type, the call matches any **Record** Rule, recording continues. At call end, the highest Priority Rule is reported for the call as a whole, with the final call type shown. However, if the call no longer matches any

Record Rule after the call-type change, recording stops and the recording for that call is discarded. Once recording of a given call stops, it cannot be restarted, even if the call type again changes to a type specified in a **Record** Rule in the Policy. For example, if a Rule specifies Fax and a new fax call begins, the call is recorded. However, if the call type changes to Voice (not specified in any **Record** Rule), recording stops and the recording of that call is discarded or retained according to the setting for the Span. If the call type changes back to Fax, recording does not begin again.

- **Keep the recording**—If the call initially matched a **Record** rule, recording continues if the call type changes and the recording is retained.

Policy Transitions

As with other ETM Policies, when you install a Policy on a Span Group, new calls are processed against the new Policy; calls in progress are not reevaluated against the new Policy. Calls are never reevaluated to start recording of a call in progress, only to stop it.

When a Span is Added to a Span Group

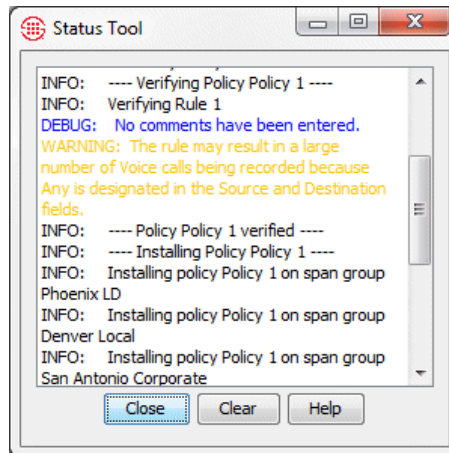
When you move a Span to a new Span Group, the Policy installed on that Span Group is automatically pushed to the added Span. You do not need to reinstall the Policy for it to take effect on the Span.

Policy Verification

When you attempt to install a Policy on a Span Group, it is automatically verified for proper configuration. You can also choose **Verify** from the Policy menu to verify a Policy without installing it. Warning messages point out issues you may want to consider, but still allow the Policy to be installed. Error messages indicate issues that prevent the Policy from being installed.

Recording Policy verification checks for:

- Duplicate Rules. (Generates warning message.)
- Rules without comments in the **Comment** field. (Generates warning message.)
- Rules with **Any** in both the **Source** and **Destination** fields. (Generates warning message.) The volume of calls to be recorded may consistently exceed the recording resources.
- Empty Directory or Time Groups. (Generates error message.) If the Policy contains empty Groups, verification fails and an error message appears describing the configuration problem.



Verification results appear in the **Status Tool**, which is launched from the ETM System Console.

- DEBUG ("No comments have been entered") and INFO ("Verifying Rule 1") messages contain information regarding verification.
- If a WARNING message is generated, the Policy can be installed.
- If an ERROR message appears, verification fails, and the Policy cannot be installed until you correct the error.

Fields in a Recording Policy Rule

Each Recording Policy Rule has the following fields that specify which calls are to be recorded:

No.—A system-generated, sequential number assigned to each user-defined Rule. The Implied Rule, which is always the last Rule in every Policy and prevents recording of any calls that did not match a prior Rule, has a hyphen (-) in this column.

Call Direction—Whether the Rule applies to **Inbound** calls, **Outbound** calls, or **Any** (calls of either direction).

Source—Calling numbers to which the Rule applies. You can specify one or more Directory Listings, Filters, Groups, Ranges, or Wildcards, **Caller ID Restricted**, **No Source**, or **Any** (all calling numbers).

Destination—Called numbers to which the Rule applies. You can specify one or more Directory Listings, Filters, Groups, Ranges, or Wildcards, or **Any** (all called numbers).








Call Type—One or more types of calls to record, such as Voice. You can also negate the **Call Type** field so that the Rule applies to calls of all types other than those in the Rule.

Time—The time(s) at which the Rule applies. You can specify one or more time ranges, or **Any** (the Rule applies at all times). You can also negate the **Time** field so that the Rule applies at all times other than those in the Rule.

Action—Whether calls that match the rule are to be recorded or not. The **Action** field of the Implied Rule is always set to **Do Not Record**, which prevents any calls that do not match a user-defined Rule from being recorded.

Priority—Determines the priority for transferring recorded calls from the CRC to the Collection Server, if one is used, and for deleting recordings when disk space limits are reached. It does *not* affect which calls are recorded. Settings are **Low**, **Medium**, or **High**. The default is **Medium**. If you are not using a Collection Server, it is strongly recommended that you set the priority for all calls the same.

Comments—Provides an area to add information describing the Rule or its purpose.

...	Call Direction	Source	Destination	Call Type	Time	Action	Priority	Comments
1	 Inbound	 Any	 Call Center	 Any	 Any	 Record	 Medium	Record inbound calls to the Call Center

Showing/Hiding the Recording Policies Subtree

To show/hide the Recording Policies subtree

- On the Performance Manager main menu, click **View | Recording Policies Subtree**. This selection works as a toggle to show and hide the subtree. A checkmark appears next to the option when the subtree is visible.

Dirty Policy Indicator

As with Firewall Policies, if Directory Object changes affect an installed Recording Policy, a "dirty policy indicator" appears next to the Policy name in the **Recording Policies** subtree of the Performance Manager tree pane. If you have the Performance Manager open, a message is displayed in the GUI, listing the affected Policies. Only the types of Policies for which your user account has permission are displayed. If you modify Directory Objects, view the **Recording Policies** subtree to verify whether you need to reinstall any Recording Policies to keep the version of the Policy on the Appliance in sync with the copy on the Server, and to effect the Directory change on the Appliance. Remember, no changes to Policies or Directory Objects take effect until you reinstall the Policy on the Span Group.

No Policy Log for Recording Policies

Unlike Firewall and IPS Policies, no **Policy Log** is provided for Recording Policies. This is to ensure that call recordings and all extension-specific data associated with them are protected from access by people without Call Recorder authorization. Therefore, no **Policy Log** option is provided from the Policy right-click menu and no Call Recorder-specific data is included in the call logs in the ETM Database. This means that no Usage Manager Reports specific to Call Recorder call data are available; however, diagnostic information is available in the **Diagnostic Log** and through Diagnostic Reports in the Usage Manager.

When you access the **Call Log** for the Span Group on which the Recording Policy is installed, all calls monitored by that Span Group appear.

Associated Firewall Policy data and IPS Policy terminations appear, but no Call Recording data appears in the **Call Log**.

Defining and Installing a Recording Policy

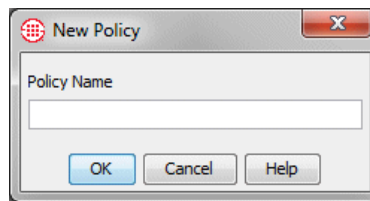
As with all ETM System Policies, Recording Policies are defined using the Policy Editor pane in the Performance Manager. A **Recording Policy** contains the following tabs:

- The **Rules** tab on which you define the Rules of the Policy.
- The **Attributes** tab on which you assign the Span Groups. Since Recording Policies never terminate calls, they have no Emergency Group.
- The **Info** tab on which you can view the properties of the Policy.

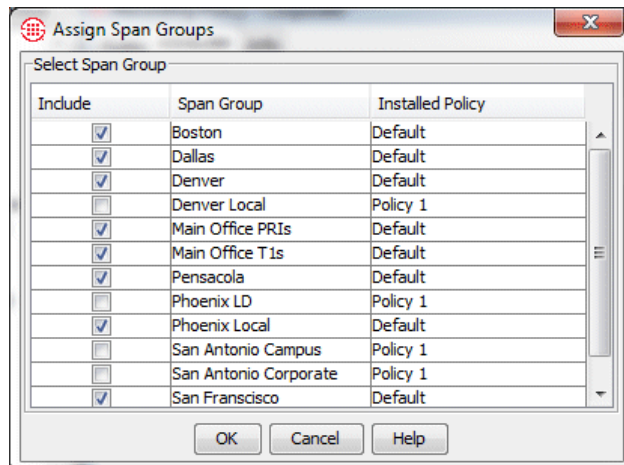
Creating a New Recording Policy

To create a new Recording Policy

1. In the Performance Manager tree pane, right click **Recording Policies**, and then click **New**. The **New Policy** dialog box appears.



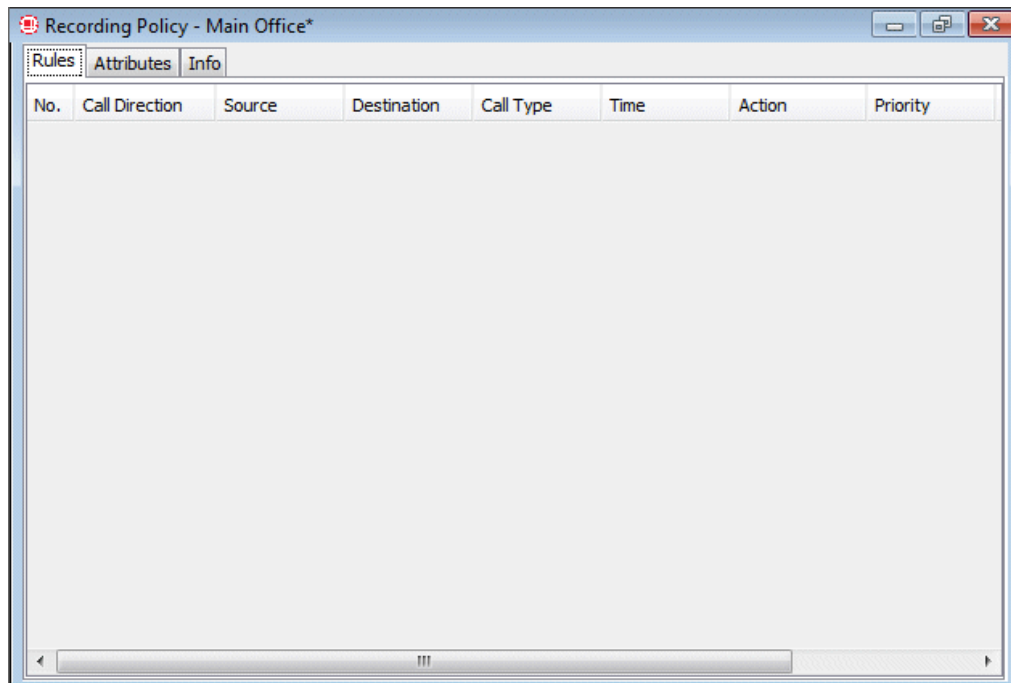
2. In the **Policy Name** box, type a name for the Policy. A Policy name can consist of up to 30 characters and can contain any combination of upper- and lowercase letters, numbers, spaces, periods, and the following special characters: & () + @ ! =.
3. Click **OK**. The **Assign Span Groups** dialog box appears.



4. In the **Include** column, select the checkbox(es) for the Span Group(s) containing the Call Recording Spans on which you want to install the

Policy. Clear the checkbox(es) for any Span Groups on which you do not want to install the Policy. Then click **OK**.

The blank Policy appears in the **Policy Editor**. An asterisk in the title bar indicates that the Policy has unsaved changes. The Policy does not appear in the Performance Manager tree pane until you save it.



5. Click **File | Save**. The Policy appears under the **Recording Policies** subtree in the Performance Manager tree pane.

Adding a Rule to a Recording Policy

See "Rule Order" on page 56 for information about how Rule order affects call recording.

To add a Rule to a Recording Policy

1. Do one of the following:
 - Right-click in the blank area of the Policy
 - Right-click an existing Rule.
2. Point to **Add Rule** and then click one of the following:
 - **Bottom** adds the Rule below any other user-defined Rules as the last user-defined Rule, just above the Implied Rule.
 - **Top** adds the Rule as the first Rule of the Policy.
 - **Before** adds the Rule before the Rule you clicked.
 - **After** adds the Rule after the Rule you clicked.

Defining a Recording Policy Rule

See "Searching for a Directory Listing" in the *ETM® System User Guide* for detailed instructions.

To define a Recording Policy Rule

1. Add a Rule to the Policy. See "Adding a Rule to a Recording Policy" on page 61 for instructions, if necessary.
2. Right-click in each applicable field in turn and select options, as follows:
 - **Direction**—If the Rule applies to calls of either direction, leave the default of **Any**. If it applies only to outbound calls, select **Outbound**. If it applies only to inbound calls, select **Inbound**.
 - **Source**—If the Rule applies to calls from any phone number, leave the default of **Any**. If it applies only to certain calling numbers, right-click in the **Source** field, point to **Add**, and then click one of the following:
 - **Listing(s)**—The **Listings Search** dialog box appears in which you can search for the number(s) that you want to specify in the field. This dialog box is used in many places throughout the ETM System.
 - a. Use the **Simple** or **Advanced** tab to define the search, and then click **Resolve**.
 - b. In the **Results** area, click the phone number(s) to which you want the Rule to apply, click **Add**, and then click **Close**.
 - **Group(s)**—The **Groups** dialog box appears in which you can select one or more Groups to add to the field.
 - **Filter(s)**—The **Filters** dialog box appears in which you can select one or more Filters to add to the field.
 - **Range(s)**—The **Ranges** dialog box appears in which you can select one or more Ranges to add to the field.
 - **Wildcard(s)**—The **Wildcards** dialog box appears in which you can select one or more Wildcards to add to the field.
 - **Caller ID Restricted**—Used to apply the Rule to calls for which the caller has blocked transmission of the Caller ID data. Note that if the phone number is present in the signaling even though CIDR is indicated, both the phone number and CIDR are used for Policy processing. In this case, Rule order determines which takes precedence.
 - **No Source**—Used to apply the Rule to calls for which source is not available on trunks that support the delivery of source information, except for those where it was intentionally blocked (CIDR). To apply a Rule to all calls having no source, specify both **Caller ID Restricted** and **No Source** in the **Source** field of the Rule. .

See also "Requesting Inbound SMDR" on page 35.

- **Destination**—If the Rule applies to calls to any phone number, leave the default of **Any**. If it applies only to certain calling numbers, right-click in the **Destination** field, point to **Add**, and then click one of the Directory Objects as described above.
- **Call Type**—If the Rule applies to calls of any type, leave **Call Type** set to **Any** (the default). If it applies only to calls of one or more specific types, click **Add**, and then select the call type(s).
 - To negate the call type (the Rule applies to calls of any call type other than those specified in the **Call Type** field), right-click the **Call Type** field of the Rule, and then click **Negate**.
- **Time**—If the Rule applies at all times, leave the default of **Any**. If it applies only at certain times or on certain days, click **Add**, and then select the Time definition that applies. See "Times" in the *ETM® System User Guide* for instructions for defining a Time, if necessary.
 - If you want to negate the Time (the Rule applies to calls at any Time other than that specified in the **Time** field), right-click the **Time** field of the Rule, and then click **Negate**.
- **Action**—To record calls that match the criteria, select **Record**. To ensure that calls that match the criteria are not recorded, select **Do Not Record**.
- **Priority**—Priority determines the order in which calls are transferred to the Collection Server, if one is used, and the order in which recordings are deleted if disk space limits are exceeded. The Priority setting does not affect whether calls are recorded—all calls that match a Rule are recorded if a recording slot is available when the call occurs (that is, if fewer than maximum available simultaneous call recordings on the Card are underway). If a Collection Server is not used, it is recommended that you set the priority for all Rules the same. Then they are deleted from oldest to newest when space constraints are reached. Otherwise, CRC disk space constraints will result in purging eventually removing all lower-priority calls, even those that have just been recorded, leaving only higher priority calls, even those that have been on the disk a long time.

When a Collection Server is used, calls are transferred from the CRC to the Collection Server in first-in, first-out order by priority. That is, calls with a Priority of **High** are moved first in the order in which they were recorded, followed by calls with a Priority of **Medium** in the order in which they were recorded, and then calls with a Priority of **Low** in the order in which they were recorded.

The default priority is **Medium**. To increase the priority, click **High**. To reduce the Priority, click **Low**.

- **Comment**—To add an optional comment, perhaps describing the intent of the Rule, click **Edit Comments**, and then type the text in the **Edit Comments** dialog box.
3. On the Performance Manager toolbar, click the **Save** icon to save your changes.

Showing/Hiding the Implied Rule

Every Recording Policy has an Implied Rule that explicitly prevents recording of any calls that did not match a prior Rule. This Implied Rule is always the last Rule in the Policy, although it is not visible if Implied Rules are hidden in the Performance Manager.

To show/hide the Implied Rule

- On the Performance Manager main menu, click **View | Implied Rules**. This selection applies globally to the Policies for all applications you have installed, not just to the current Policy or application. This selection works as a toggle. If a checkmark appears next to **Implied Rules** on the **View** menu, they are visible; if no check mark appears, they are hidden.

Installing a Recording Policy

To install a Recording Policy

- On the Performance Manager main menu, click **Policy | Install** and then click one of the following:
 - **Normal Mode**—Normal installation without uninstalling the existing user-defined Policy, if present. If the Policy will not fit without uninstalling the existing Policy, installation fails and a message is presented.
 - **Priority Mode**—If the new Policy needs the space occupied by the existing user-defined Policy, the existing Policy is uninstalled before the new Policy is installed.

See "Limit to the Number of Phone Numbers in Policies" in the *ETM® System User Guide* for more information.

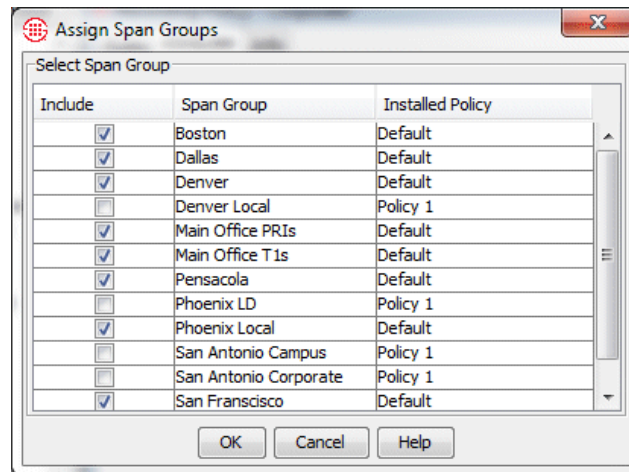
If no object issues are encountered, the Policy is verified and pushed to the Spans in the Span Groups assigned to the Policy. The verification and installation process appears in the **Status Tool**, accessed from the ETM® System Console. See "Policy Verification" on page 57 for details about verification.

If you used Normal Mode and an object issue was encountered, you can either modify the Policy, or choose to install it again using Priority Mode.

When you move a Span to a Span Group, the Recording Policy currently installed on the Span Group is automatically pushed to the Span. As with other Policy types, only one Recording Policy at a time can be enforced on a Span.

Assigning a Span Group to a Recording Policy

When you create a new Policy, the **Assign Span Groups** dialog box appears in which you can assign the Span Groups to enforce the Policy. If you click **OK** without assigning a Span Group, or if you later want to assign one or more other Span Groups, you can do so on the **Attributes** tab of the **Policy Editor**.



To assign a Span Group to a Recording Policy

1. On the **Attributes** tab of the Policy to which you want to assign one or more Span Groups, click **Assign Span Groups**. The **Assign Span Groups** dialog box appears.
2. Select the check box(es) of the Span Group(s) that are to enforce this Policy; clear the check boxes of the Span Groups that are not to enforce this Policy.
3. Click **OK**.

Viewing Properties of a Recording Policy

You can view the properties of a Recording Policy on the **Info** tab of the **Policy Editor**.

The properties of a Policy include the following information:

- **Policy ID**—User-assigned name plus a system-generated number unique to this Policy
- **Created by**—Username of the person who created the Policy.
- **Create Date**—Date the Policy was created.
- **Last Modified By**—Username of the person who last modified the Policy.
- **Modified Date**—Date the Policy was last modified.

Recording Policy - Main Office	
Rules Attributes Info	
Policy ID	Main Office.1532378383390
Created by	admin
Create Date	2018/07/23 15:55:39
Last Modified By	admin
Modified Date	2018/07/23 15:55:39

Printing a Recording Policy

To print a Recording Policy

1. Open the Policy. If you have more than one Policy open, ensure that the Policy that you want to print has the focus.
2. Click **File | Print**, and then select the format:
 - **Print Summary** prints the Policy as it is displayed in the **Policy Editor**, with a summary that includes:
 - Policy ID (generated by the application).
 - Date and time the Policy was created.
 - User name of the creator.
 - Date and time the Policy was last updated (saved).
 - User name of the person who last updated (saved) the Policy.
 - **Print Details** prints the same information as **Print Summary**, plus:
 - Time Groups used in the Policy.
 - Span Group(s) on which the Policy is installed.
3. The **Print Preview** dialog box appears. Click the **Printer** icon.
4. The **Print** dialog box appears. Select a printer, and then click **OK**.
 If you have Adobe Acrobat Distiller or PDF Maker installed on the computer, you can save the Policy in PDF format by choosing the Adobe product as the printer.

Saving a Recording Policy

Consider the following when you create a new Policy or make changes to a Policy:

- Save your changes before closing the Policy. If you close a newly created Policy without first saving it, the new Policy is not created. A

message appears when you attempt to close the Policy if you have unsaved changes.

- New Policies do not appear in the **Recording Policies** subtree until they have been saved.
- If you have installed a Policy on a Span Group, and then later make changes and save it, the updated Policy is downloaded to the Span Group; if the Policy is not currently installed, changes are simply saved, not installed.
- Changes do not take effect until you save and install the Policy.

To save a new or modified Policy

- On the main menu, click **File | Save** or, on the toolbar, click the **Save** icon .

Editing an Installed Recording Policy

To edit an installed Recording Policy

1. In the **Recording Policies** subtree, right-click the Policy, and then click **Edit**. The Policy opens in the **Policy Editor**.
2. To modify existing Rules, right-click in the field, and then choose options. See "Defining a Recording Policy Rule" on page 62 for instructions for defining each field.
 - To remove an item from a Rule, do one of the following:
 - If the field contains more than one item, and you are removing only one of the items, right-click the item, and then click **Remove**.
 - If the field contains only one item or you want to remove all items, right-click the field, and then click **Any** or **None** (depending on the field).
3. To add a new Rule, see "Adding a Rule to a Recording Policy" on page 61.
4. When your changes are complete, click the **Save** icon on the Performance Manager toolbar to save your changes and download them to the Spans. The changes do not take effect on the Spans until the Policy is saved and downloaded. To ensure that the copy on the Server and the copy on the Spans always match, you cannot save changes to an installed Policy without downloading it to the Spans.

Saving a Copy of a Policy

Use the following procedure to create a new Policy with all of the attributes of another Policy.

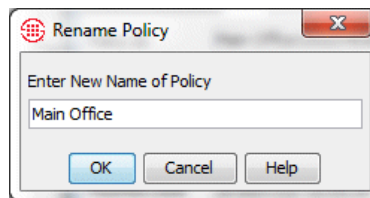
To create a new Policy based on another Policy

1. Open the Policy on which you want to base the new Policy. The Policy appears in the **Policy Editor**.
2. On the main menu, click **File | Save As**. The **New Policy** dialog box appears.
3. Type the name for the new Policy, and then click **OK**. The new Policy appears in the **Policy Editor** and in the **Recording Policies** subtree.
4. Make modifications to the Rules as needed, and then click **File | Save**.

Renaming a Policy

To rename a Policy

1. Right-click the Policy that you want to rename, and then click **Rename**. The **Rename Policy** dialog box appears.



2. In the **Enter New Name of Policy** dialog box, delete the old name, and then type the new name.
3. Click **OK**.

Deleting a Recording Policy

You can delete a Policy that you no longer intend to use. You cannot delete an installed Policy; it must be uninstalled before you can delete it.

If you want to deactivate a Policy without deleting it, see "Uninstalling a Recording Policy" on page 68.

To delete a Policy

1. In the **Recording Policies** subtree, right-click the Policy, and then click **Delete**. A verification message box appears.
2. Click **Yes**. The Policy is deleted from the ETM Database.

Uninstalling a Recording Policy

When you uninstall a Policy from a Span Group, the default Policy is installed on that Span Group. The default Policy contains the Implied Rule only.

To uninstall a Policy

1. In the **Recording Policies** subtree, right-click the Policy, and then click **Uninstall**.

A verification window appears, reminding you that the default Policy will be installed in place of the current Policy.

2. Click **Yes** to continue.

Reverting a Policy to Its Last Saved State

While you are editing a Policy, you can discard all changes since the last save. This is referred to as "refreshing" the Policy.

To refresh a Policy

- Do one of the following:
 - On the Performance Manager main menu, click **File | Refresh**.
 - **-or -**
 - On the Performance Manager toolbar, click the **Refresh** icon.

Using Undo/Redo while Editing a Policy

While editing a Policy, you can use **Undo** and **Redo** to discard or restore your last change.

To discard/restore changes

- To discard your last change, click the **Undo** icon on the Performance Manager toolbar.
- To restore the last change you discarded, click the **Redo** icon on the Performance Manager toolbar.

Modifying or Deleting Items Contained in Rules

If you modify an item that is contained in an installed Policy, the change does not take effect on the Spans unless you reinstall the Policy. For example, if you have specified a Directory Group in an installed Policy, and then later add a Listing to the Group, you must reinstall the Policy.

See "Dirty Policy Indicator" on page 59 for more information about how changes affect installed Policies.

If you modify, delete, or add items in an installed Policy, and then save the Policy, the Policy is automatically reinstalled.

Hiding Rules

If you have numerous Rules, but prefer to only see a few of them, you can hide them. Hidden Rules are still enforced; if you do not want the Rule to be enforced, you can disable it or delete it. See "Disabling Rules" on page 70 and "Deleting Rules" on page 70.

To hide/show a Rule

- Right-click the Rule you want to hide, and then click **Hide Rule**.
- Click the Rule you want to hide, and then, on the Performance Manager main menu, click **View | Hide Rule**.

- To show a hidden Rule, on the Performance Manager main menu, click **View | Show Hidden Rules**.

Disabling Rules

Disabling is useful if you do not want the Rule to fire, yet you do not want to permanently delete it. Disabling is not the same as hiding a Rule—hidden Rules are still enforced, while disabled Rules are not. You can easily reinstate a disabled Rule by enabling it and reinstalling the Policy. A disabled Rule appears dimmed in the **Policy Editor**.

To disable/enable a Rule

- Right-click the Rule you want to disable, and then click **Disable**.
- To enable the Rule, right-click the Rule, and then click **Enable**.

If you disable or enable a Rule in an installed Policy, the Policy must be reinstalled for the changes to take effect.

Cutting, Copying, and Pasting, Rules


To cut and paste or copy and paste a Rule

1. Open the Policy from which to cut or copy the Rule, and, if different, the Policy into which you will paste the Rule.
2. Highlight the Rule you want to move/copy.
3. Do one of the following:
 - To remove the Rule from its current location and transfer it to a new location, on the main menu, click **Edit | Cut**.
 - To create a duplicate of the Rule in a new location, click **Edit | Copy**.
4. Ensure that the Policy into which you want to paste the Rule has the focus, if different, and then do one of the following:
 - To paste the Rule at the bottom of the Policy, click **Edit | Paste | Bottom**.
 - To paste the Rule at the top of the Policy, click **Edit | Paste | Top**.
 - To paste the Rule after the selected Rule, click the Rule, and then click **Edit | Paste | After**.
 - To paste the Rule before the selected Rule, click the Rule, and then click **Edit | Paste | Before**.

Alternatively, you can right-click in the **No** field, and then click **Cut**, **Copy**, or **Paste**.

Deleting Rules

To delete a Rule

- Highlight the Rule(s) that you want to remove, and then click the **Delete** icon .

See also "Hiding Rules" on page 69 and "Disabling Rules" on page 70.

Viewing Contents of Directory Entities in Rules

You cannot edit Directory entities from within a Rule; they can only be edited from within the Directory Manager. However, you can view their contents. See "The Directory Manager" in the *ETM® System User Guide* for instructions for defining and editing Directory Entities.

To view the contents of a Directory entity in the Source or Destination field

- Right-click the item you want to view and click **View**. A read-only copy of the object appears.

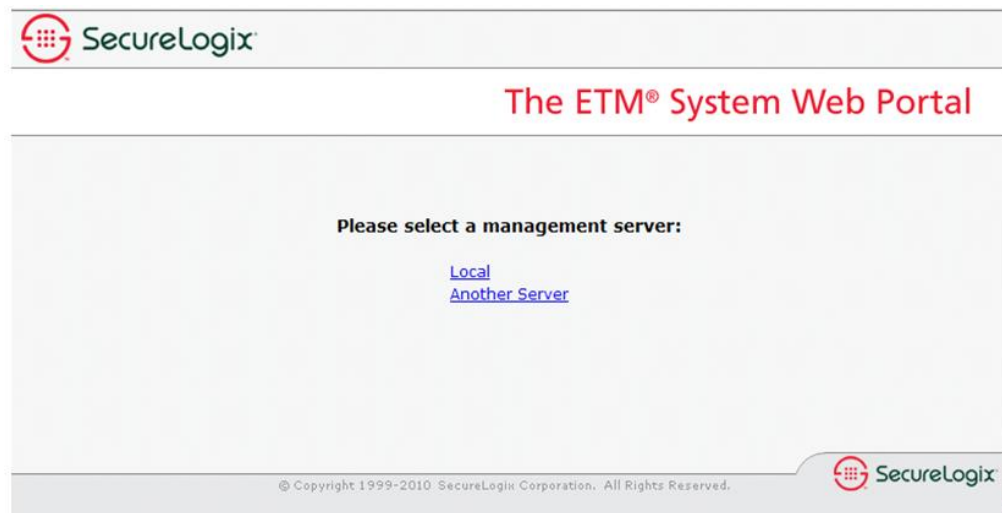
Accessing Call Recordings

You can locate and listen to call recordings from the Web Portal or from the Collection Server, depending on how your system is configured. To access Call Recordings via the Web Portal, you must have the **View & Reinstall Recording Policies** user permission.

Logging in Via the Web Portal

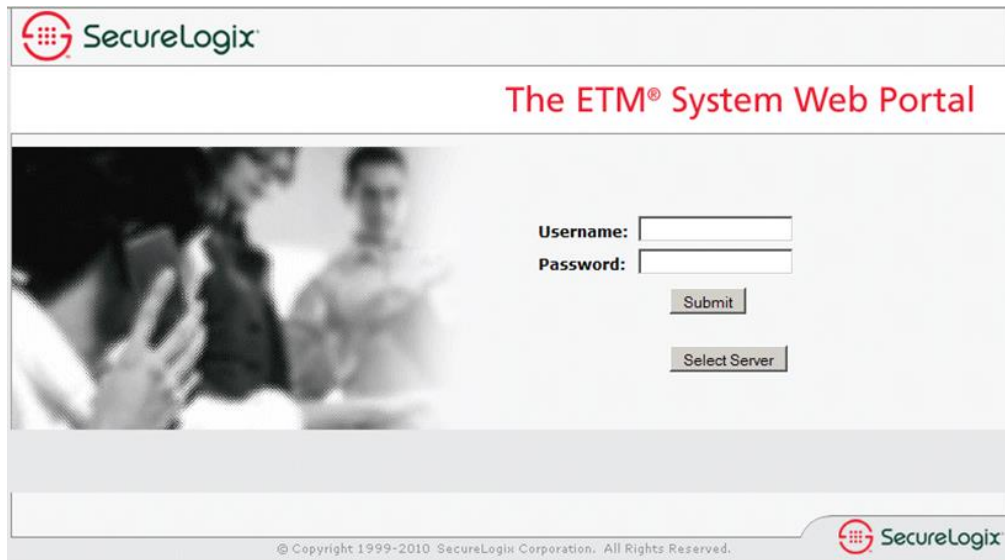
To log in via the Web Portal

1. In Internet Explorer, navigate to the WebETM URL provided by your system administrator.
2. One of the following occurs:
 - If more than one ETM Server is available, the **Server Selection** page appears. Click the ETM Management Server you want to log into.



- If a single ETM Server is available, see the next step.
3. Two login options are available, depending on the configuration at your site.
 - If your Web Portal is configured for anonymous login, the Web Portal logs into the ETM Server. See the next step.
 - If you use your ETM System login to access the Web Portal, the **Login** page appears.

Anonymous login is only available from the **<hostname>/webetm/anonymouslogin** URL



SecureLogix

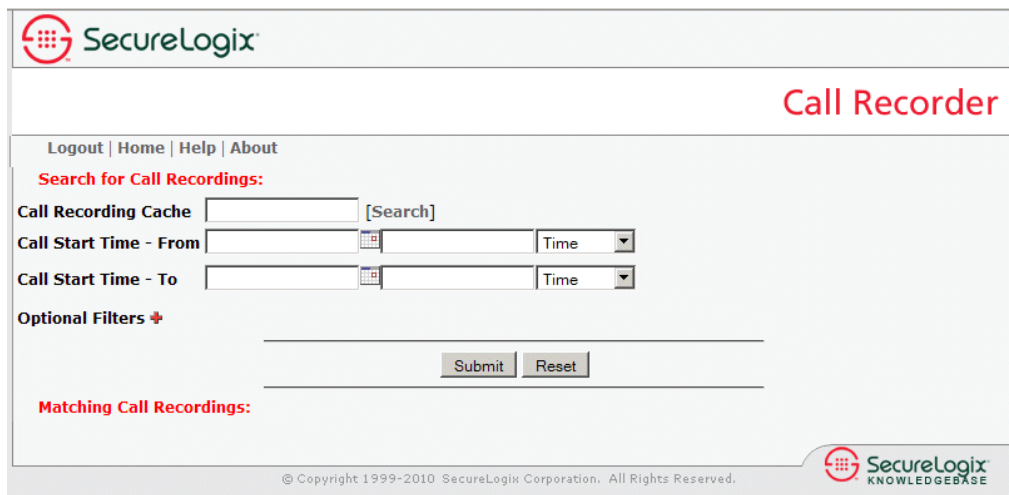
The ETM® System Web Portal

Username:

Password:

© Copyright 1999-2010 SecureLogix Corporation. All Rights Reserved. SecureLogix

4. Type your username and password, and then click **Submit**.
5. The login banner appears, if one is configured. Click **OK**.
6. The page that appears depends on the permissions set on the account you used to access the Web Portal.
 - If you do not have Usage Manager user permission, you are taken directly to the **Call Recording** page.



SecureLogix

Call Recorder

[Logout](#) | [Home](#) | [Help](#) | [About](#)

Search for Call Recordings:

Call Recording Cache [Search]

Call Start Time - From Time

Call Start Time - To Time

Optional Filters

Matching Call Recordings:

© Copyright 1999-2010 SecureLogix Corporation. All Rights Reserved. SecureLogix KNOWLEDGE BASE

- If you have both Call Recording and Usage Manager access permissions, the **Main** page appears. The **Main** page provides options for viewing and scheduling reports and for accessing call recordings.

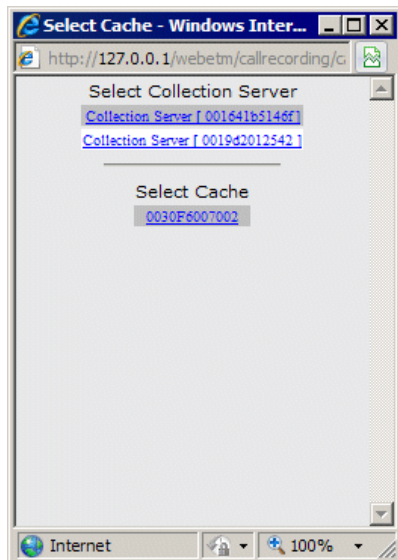
- Click **Access Recordings**. You are taken to the **Call Recording** page.



Locating and Listening to Call Recordings

To locate and listen to recorded calls

1. Log in to the Web Portal. and navigate to the **Call Recording** page.
2. Specify the CRC or Collection Server where the call is stored. Do one of the following:
 - If you know the exact name of the CRC or Collection Server (or enough to uniquely identify it), in the **Call Recording Device** box, type the name of the device. For example, if one CRC is named **MainOfcCRC** and no other CRC or Collection Server names begin with **Main**, you can type just **Main** to access that CRC.
 - If you know part of the name, type it in the **Call Recording Device** box and then click **Search**. The **Select Device** pop-up appears listing potential matches for the search string. Click the correct CRC or Collection Server.



- Leave the box blank and click **Search**. This is treated like the wildcard * and returns all CRCs and Collection Servers. Click the correct device.

The device name appears in the **Call Recording Device** box.

3. Specify the **Call Start Time** range for which you want to access recordings, as follows:
 - a. In the **Call Start Time - From** box, type or select the earliest date for which you want to access calls.
 - b. In the corresponding **Time** box, type or select the earliest call start time you want to see on the specified date.
 - c. In the **Call Start Time - To** box, type or select the latest date for which you want to access calls.
 - d. In the corresponding **Time** box, type or select the latest call start time for which you want to see calls on the specified date.
4. Optionally, you can specify additional filter criteria to narrow the recordings retrieved. To specify optional filters:
 - a. Next to **Optional Filters**, click the **PLUS SIGN**. The **Optional Filters** fields appear.

Search for Call Recordings:

Call Recording Appliance Search

Call Start Time - From ▼

Call Start Time - To ▼

Timezone ▼

Optional Filters ▢

Call Direction ▼

End Time - From Time ▼

End Time - To Time ▼

Duration > ▼ minutes

Wav Size > ▼ kb

Source

Destination

Call Type ▼

Policy

Rule Number

Priority










Span


Call Recording Cache Search

- b. You can specify one or more of the following optional values:
- **Call Direction:** Click the down arrow and select the direction, **Inbound** or **Outbound**.
 - **Duration:** Click the down arrow and select **Less than** or **Greater than**, and then type the number of minutes.
 - **Wav Size:** (*CRC search only; not applicable to Collection Server.*) Click the down arrow and select **Less than** or **Greater than**, and then type the size in kb.
 - **Source:** The calling number. Populate all fields, or you can use % as a wildcard in any field. Any characters after % are ignored, including those in other fields. If you leave a field blank but do not use a wildcard in a preceding field, the filter only matches if the field is actually blank in the data.
 - **Destination:** The called number. Populate all fields, or you can use % as a wildcard in any field. Any characters after % are ignored, including those in other fields. If you leave a field blank but do not use a wildcard in a preceding field, the filter only matches if the field is actually blank in the data.
 - **Call Type:** Click the down arrow and select the call type.
 - **Policy:** Type the name of the Recording Policy used to record the call(s).

- **Rule Number:** Type the number of the Recording Policy rule that caused the call(s) to be recorded.
- **Priority:** Type the priority set in the rule that caused the call(s) to be recorded.
- **Span:** Type the name of the Span that recorded the call(s).
- **Call Recording Cache:** When searching a Collection Server, this field becomes available. Type in the name of the CRC that cached the recording. You can click Search to search for a CRC starting with the provided text, or you can leave the field blank to return results from all available CRCs.

5. Click **Submit**. The calls that match the criteria are found and appear as a list. By default, the list is sorted by **Start Time**. To sort by a different field, click the column heading. Click again to sort in the reverse order.

		Call Direction	Start Time	End Time	Duration	Wav Size	Source	Destination	Call Type	Policy	Rule Number	Priority
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:00:55	417.06 KB		+1(210)5239308	Voice Rec	All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:00:54	413.38 KB		+1(210)5239198	Undetermined	Rec All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:01:01	466.25 KB		+1(210)5239114	Voice Rec	All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:00:56	423.31 KB		+1(210)5239126	Voice Rec	All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:01:01	464.56 KB		+1(210)5239121	Voice Rec	All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:00:58	441.62 KB		+1(210)5239125	Voice Rec	All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:01:01	464.94 KB		+1(210)5239111	Undetermined	Rec All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:01:01	465.19 KB		+1(210)5239118	Voice Rec	All Inbound	1	2
	Preview	Inbound	2/22/06 8:00 AM	2/22/06 8:01 AM	0:01:00	459.88 KB		+1(210)5239119	Voice Rec	All Inbound	1	2

6. To listen to a call recording, click the  icon for the call.

- To preview a recording first to be sure it is the one you want to download, click **Preview** in the call record. A preview contains the first 10 seconds of the call.

The 10 second default can be changed to a different value. Contact SecureLogix Customer Support for instructions.

Because they are usually much shorter than the complete recording, previews generally take much less time to download than a complete call recording.

7. The **Downloading** status pop-up appears while the call recording is being transferred from the CRC to the web client computer. It shows the total size of the recording in kb and the amount transferred so far.

- To cancel the transfer before it completes, click **Cancel Download**.



8. When the download is complete, the **.wav** file player configured for the browser computer, such as Windows Media Player, launches and plays the recording.

Accessing Call Recordings on the Collection Server

To access call recordings on the Collection Server, you use third-party playback and analysis tools. For example, if you use the default filter, you can use Windows Media Player to listen to the calls.

Data Filtering

The Collection Server runs a filter to convert each recorded call's audio file and call data from its received format to a final format that can be used with third-party playback and analysis tools. To provide a simple means to correlate a call recording with the Policy that caused it to be recorded, the Policy name in the call record is used as the directory name for the folder where the filtered data is stored.

The data filter runs as a separate thread that "wakes up" at specific intervals and scans the call record cache directories for received files. If files are present, the filter first parses the call data file to retrieve all of the call parameter data from it. The filter then converts audio files into stereo PCM format and data files into mono Mu-law format and saves the files in the filter directory for the type of filter you specified: Default or TSAP.

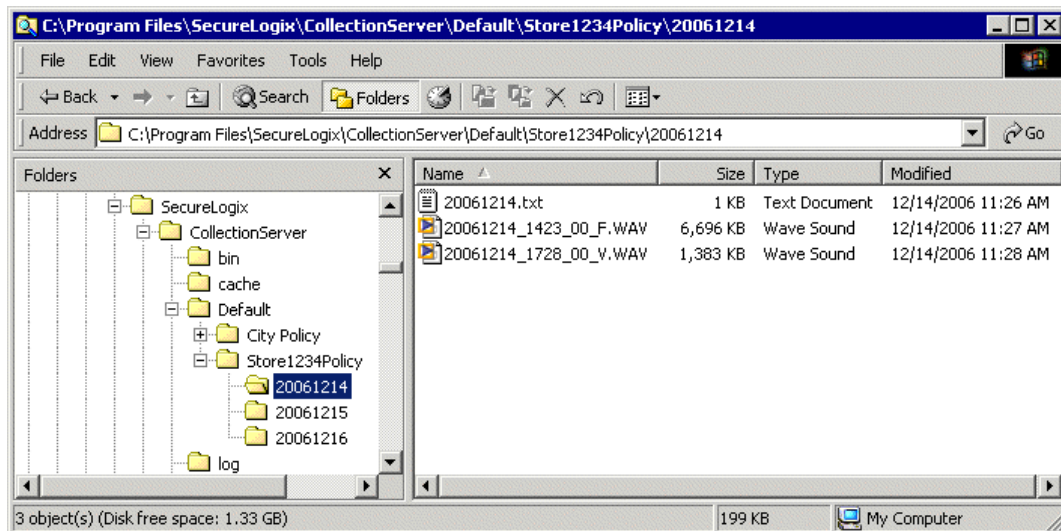
Call Recording Storage Directory Structure

Call recordings are stored in a directory structure in which the top level bears the name of the Recording Policy:

- By default, output is grouped by Policy Name and then date. The Policy folder contains a folder for each day on which calls are recorded, in which the WAV files and a call details file are stored.
- If **Group Filter Output by Rule Number** is selected in the Collection Server configuration, output is grouped by Policy Name, and then Rule Number, and then the date of the recording. This allows the administrator of the Collection Server computer to assign Windows folder access permissions per rule number, to control who has access to different types of recordings, according to the purpose of the rule.

Sensitive and Potentially Sensitive recordings are stored in a separate but identical directory structure under the Sensitive Recording Path. This allows the administrator of the Collection Server computer to assign Windows folder access permissions per rule number, to control who has access to sensitive recordings.

An illustration of the default directory structure appears below.



Each call is captured in a single WAV file. To listen to the call recording, open the WAV file in a tool such as Windows Media Player. The naming convention for the WAV files is as follows:

yyyymmdd_hhmmss_nn_<call type>.wav, where *nn* is an incrementor used if the time stamp is not unique. The *nn* incrementor starts at 00. The call types encountered during the call are each listed, with underscores delimiting multiple values (such as V_ME_V). Call type values are:

- F = fax
- V = voice
- M = modem
- ME = modem energy
- ST = STU
- DC = data call
- B = busy
- UA = unanswered
- UD = undetermined

Details for all calls on the given day (default) or given day for the specified rule (if Rule-Based filtering is enabled) are consolidated into a single, comma-delimited call-details text file. The first line of the call details file is a header line containing comma-delimited labels for each field. Each call record is appended on a new line at the end of the file. To view call details, open the file in a text editor or spreadsheet tool such as Microsoft Excel. For each call, the call details file provides the following information:

- MAC address of the Card on which the call was recorded.

- MAC address of the CRC from which the raw data was received.
- Source and destination phone numbers.
- Call direction.
- Call start time.
- Call connect time.
- Call connect time GMT offset.
- Call end time.
- Call end time GMT offset.
- Call duration.
- Recording Policy name, Rule fired, and Priority rating.
- Call types during the length of the call.
- Name of the associated WAV file that contains the recording.
- Call Attributes (Sensitive or Potentially Sensitive attribute used in the Sensitive Recording directory structure only)

Post-Filter Processing

Once the filter has completed processing the files for a call, the Collection Server either deletes the received files or keeps them, depending on its **Post Filter Processing** setting, described below:

- If the configuration is set to keep all files, then files that were successfully processed are moved to the **processed** subdirectory in the **cache** directory, while those for which system or application errors prevented processing are moved to the **error** subdirectory.
- If only the error files are to be kept, then successfully processed files are deleted and those for which system or application errors prevented processing are moved to the **error** subdirectory.
- If the configuration is set to delete all files, then all raw files are deleted.

To conserve disk space, it is recommended that you set **Post-Filter Processing** to either **Delete All Files** (the default) or **Keep Error Files Only**. A log file of filtering activity and results is created and available from the **Logs** menu. See "Viewing Log Files" on page 81 for more information about viewing logs.

Errors that prevent processing include:

Application Errors

- Missing audio file (the actual call recording). The Collection Server receives two files for each recorded call; if the audio file is missing, the call cannot be processed.
- Empty audio file (no call recording).

- The data file containing the call attributes, such as call init time, call end time, source number, destination number, and so forth, could not be parsed because of a format error.
- The name of the Policy that triggered the call recording was not included in the data file. The Policy name is used as the name of the folder in which the call recording is stored.

System Errors

- The top-level directory could not be created.
- One of the subdirectories or files could not be created.
- The WAV file could not be created.

Accessing Recorded Calls

To access call recordings

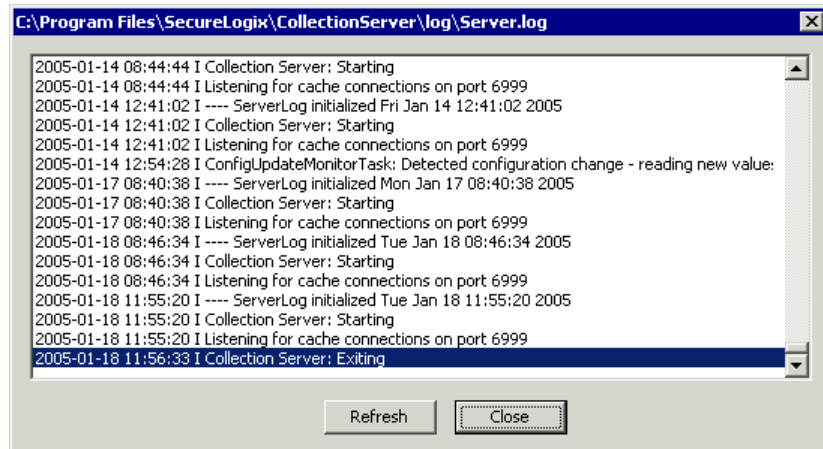
- Browse to the **Default** filter directory. Call recordings are stored in a 3-tiered directory structure. The top-level folder bears the name of the Recording Policy. The Policy folder contains a folder for each day on which calls are recorded, in which the call recording WAV files and a call details file are stored. See “Call Recording Storage Directory Structure” on page 78 for details.
 - Open the WAV files in a tool such as Windows Media Player.
 - Open the call details file in a text editor or a spreadsheet tool such as Microsoft Excel.

Viewing Log Files

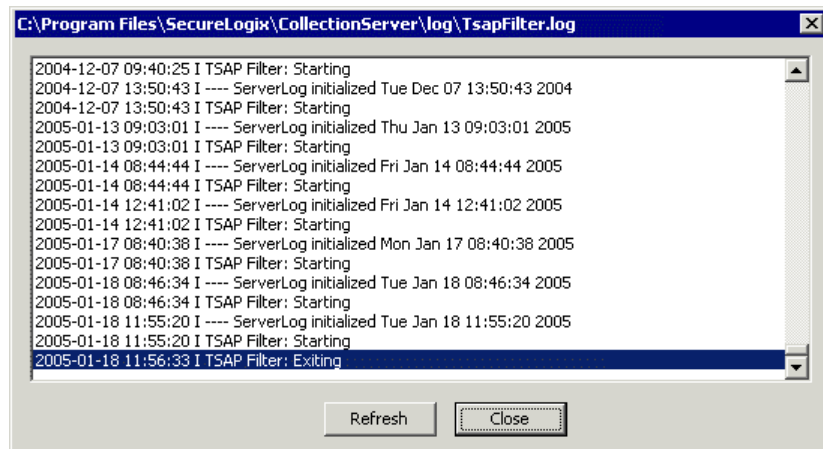
The Collection Server provides logs of Collection Server activity and filter processing.

To view Server/Filter log files

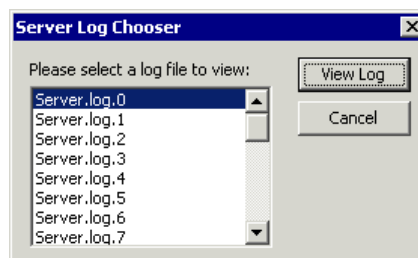
1. Open the **ETM Collection Server Configuration** Tool.
2. On the **ETM Collection Server Configuration** Tool main menu, click **Logs**, and then click one of the following:
 - **View Server Logs**—The log viewer displays the Collection Server logs.



- **View Filter Logs**—Select the type of filter. The log viewer displays the filter logs for the selected filter.



- **View Archive**—From this menu, click **Server Logs** or **Filter Logs**.
 - a. The **Log Chooser** for the selected type of archived log appears. The example below shows server logs.



- b. Click the log you want to view, and then click **View Log**.

Appendix

Maintenance Information

This appendix provides maintenance information for the Call Recorder, including instructions for uninstalling the Collection Server and Call-Recorder-specific ETM Commands.

Uninstalling the Collection Server Software

To uninstall the Collection Server Software

1. Ensure that the Windows Services GUI is closed.
2. Use the **Add/Remove Programs** feature in Windows.

ETM[®] Commands for the Call Recorder

ETM[®] Commands specific to the Call Recorder are listed below. As with other ETM Commands, these commands can be used from a console connection, Telnet, SSH, or the **ASCII Management Interface**. As with other ETM Commands, once the Appliance component has connected to the ETM Server, the Server is authoritative on all configuration items except those noted as Appliance only. Command-line changes to other settings are overwritten when the Appliance component connects to the Server.

Command(s)	Description
CACHE IP ip SHOW RECORD CONFIG	Specifies the IP address of the CRC. RESTART Span for command to take effect.
CACHE PORT port SHOW RECORD CONFIG	Specifies the listener port on the CRC. RESTART Span for command to take effect.
CALL RECORDING enabled disabled SHOW RECORD CONFIG	Global setting for the Span that enables or disables the call recording subsystem. Span RESTART required for command to take effect.
COLLECTION-SERVER COMMUNICATION enabled disabled SHOW CRC CONFIG	Enables/disables uploading of recordings to a Collection Server. RESTART CRC for command to take effect.
COLLECTION-SERVER DES KEY string SHOW CRC CONFIG	The DES key to use when encrypting communication with the Collection Server. Must be between 16-50 characters. RESTART CRC for command to take effect.

Command(s)	Description
COLLECTION-SERVER DES LEVEL none single triple SHOW CRC CONFIG	The DES level to use when encrypting communication with the Collection Server. RESTART CRC for command to take effect.
COLLECTION-SERVER IP ip SHOW CRC CONFIG	The Collection Server IP address. RESTART CRC for command to take effect.
COLLECTION-SERVER PORT number SHOW CRC CONFIG	The Collection Server port. RESTART CRC for command to take effect.
DETECTOR INBOUND THRESHOLD	Set the inbound call recording detector threshold.
DETECTOR OUTBOUND THRESHOLD	Set the outbound call recording detector threshold.
END ON BUSY true false	Abandon call on receipt of busy signal.
END ON DIALTONE true false	Abandon call on receipt of dialtone.
NO LINE channel all	Clear the line identifier of the specified channel or all channels.
RECORDING IP ADD ip RECORDING IP DELETE ip SHOW CRC CONFIG	Adds/removes entries in the list of IP addresses of call recording spans allowed to connect to the CRC. RESTART CRC for command to take effect.
RECORDING LENGTH number default SHOW RECORD CONFIG	The maximum length, in minutes, of any single recording.
RECORDING LISTENER PORT number SHOW CRC CONFIG	The port on which the CRC listens for connections from call recording spans. RESTART CRC for command to take effect.
RECORD INBOUND enable disable chn all 0xffffffff SHOW RECORD CONFIG	Enables/disables recording of inbound calls on a per channel basis.
RECORD OUTBOUND enable disable chn all 0xffffffff SHOW RECORD CONFIG	Enables/disables recording of outbound calls on a per channel basis.
RECORD PROTECT add delete string SHOW PROTECTED EXTENSIONS	Adds/removes members of the list of SMDR extensions.
RECORD SMDRMATCH ACTION [delete save sensitive potentially_sensitive]	Sets the SMDR Extension processing behavior if SMDR is matched.
RECORD SMDRNOTMATCH ACTION [delete save sensitive potentially_sensitive]	Sets the SMDR Extension processing behavior if SMDR is not matched.
RECORD SMDRTIMEOUT ACTION [delete save sensitive potentially_sensitive]	Sets the SMDR Extension processing behavior if SMDR is not received.

Command(s)	Description
RECORD SMDR PROCESSING [yes no]	Enables SMDR Extension processing. This command replaces RECORD REQUIRE SMDR
RESERVED DISK SPACE number SHOW CRC CONFIG	The amount of disk space in MB reserved for storing recordings and associated files.
RING GENERATOR enable disable SHOW RECORD CONFIG	Enables/disables the use of an external ring generator. RESTART Span for command to take effect.
SHOW ANNOUNCE	Display Call Announcement configuration.
SHOW CRC CONFIG	Display Call Recording Cache configuration.
SHOW CRC CONNECTIONS	Display connected Recording Spans.
SHOW CRC STATUS	Display Call Recording Cache related status.
SHOW PROTECTED EXTENSIONS	Displays the list of extensions protected from being recorded.
SHOW RECORD CONFIG	Display SMDR Processing on/off, SMDR match action, SMDR no match action, and SMDR timeout action.
SHOW RECORD POLICY	Display the Call Recorder policy.
SHOW RECORD STATUS	Display Call Recorder status information.

Index

accessing call recordings	72
from Web Portal	72
on Collection Server	81
Action field.....	63
architecture	11
Authorizing Spans for CRC	26
call data collected	14
Call Recorder	
configuration	31
licensing	12
Recording Span	12
software	17
Call Recording Cache.....	22
port	34
call recordings	
accessing.....	72
on Collection Server	78
on Web Portal	74
Call Type field.....	63
Caller ID Restricted.....	62
channels	
enabling recording on	34
Collection Server.....	13
accessing call recordings	78, 81
allowed simultaneous connections	48
allowing connections to	45
application	13
cache path	41, 49
compression.....	42
configuration	40
data filtering	78
deleting authorized CRC	46
directory structure.....	78
errors that prevent filter processing	80
filter	49
filter path	41, 49
filter processing	80
listener port.....	48
log files	81

minimum disk space	46
post-filter processing	42, 50
sensitive recording path	42
software installation.....	17
uninstalling	83
Collection Server Configuration Tool	44
opening	45
Comment field	64
companding	35
configuration	40
Call Recorder.....	31
Collection Server	40
companding	35
CRC	22
importing	30
of CRC to use Collection Server	27
Configurations	16
CRC	
configuration	22
importing	30
configuring to use Collection Server	27
connection lost.....	33
heartbeat interval	30
listener port.....	24
naming	24
port	34
specifying	33
data filtering	78
Debug logging	30
Destination field	63
Direction field	62
Directory entities	
viewing	71
disk space	
Collection Server	46
limit on CRC	26
enabling recording	31
ETM Collection Server Configuration Tool.....	44
ETM Commands	83
ETM Server	12
ETM Web Portal	14
filter	
Collection Server	49
path	41, 49
post-filter processing	42, 50
hardware	16
heartbeat interval	30
Implied Rule	64
inbound SMDR	

and SMDR Extension processing	37
requesting	35
installation	
Call Recorder software	17
Recording Policies	64
licensing	12
limit	
Collection Server disk space.....	46
CRC disk space	26, 59
simultaneous Collection Server connections	39
simultaneous Collection Server connections	14
simultaneous Collection Server connections	48
simultaneous recording	13
listener port	
Collection Server	48
CRC	24
listening to recorded calls	74
log files.....	81
minimum disk space	
Collection Server	46
negation	
Call Type field	63
Time field	63
No Source	62
number of simultaneous calls	13
Performance Manager	
and Call Recorder	12
port	
Collection Server listener	48
CRC	34
Priority field	63
recorded calls	
listening to	74, 78
Recording Card	
installation	16
Recording Policies.....	56
adding a Rule.....	61
and call-type changes	56
and Span Groups	57
creating a new Policy.....	60
defining and installing	60
defining the fields in a Rule.....	62
dirty policy indicator	59
fields in.....	58
hiding subtree	59
installing	64
interaction with other ETM Policies	56
Policy Log	59
Rule order	56

show/hide the Implied Rule	64
transitions	57
verifying	57
Recording Policy	
deleting	68
editing an installed Policy	67
printing	66
refreshing	69
renaming	68
Save as	68
saving	66
undo/redo	69
viewing attributes of	65
recording process	13
Recording Span	31
enabling recording on	31
Rules	
copying	70
deleting	70
disabling	70
hiding	69
modifying	69
simultaneous recordings	11, 13
SMDR	
requesting inbound	35
smdr extensions	
definition	15
SMDr Extensions	
importing	39
SMDR Extensions	
and Upload Time	29
defining	36
Source field	62
Span configuration	
companding setting	35
opening the dialog box	31
Span Group	
assigning	65
Time field	63
transportable option	15
Upload Time	
CRC to Collection Server	28
user permissions	20, 21
verification	57
Web Portal	14
listening to recorded calls	74
logging in via	72