SecureLogix®
We see your voice®

ETM® (Enterprise Telephony Management) System

v9.0.2

User Guide

DOC-UG-902-08172022

About SecureLogix

For over 20 years, SecureLogix has profiled, tracked, and defended customers against the schemes and threats plaguing unified communications networks. We’ve developed patented technology and assembled the most skilled team in the industry to monitor and protect some of the world's largest and most complex contact centers and voice networks.

We're not the largest IT vendor; we're the one with the start-up agility and decades of unrivaled enterprise experience. The one that is there when you need us, with superhero level support.

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

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

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

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

IMPORTANT NOTICE:

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.

This product is protected by one or more of the following patents:
US 11,349,987 B2 and US 11,356,551 B2. U.S. Patent Pending.

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

This product includes:

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

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

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

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

Technical Support
for Your ETM® System

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

https://support.securelogix.com

Contents

Preface 11

ETM® System Concepts 13

Getting Started 45

Objects 65

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 media.

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) and SIP Proxy 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.

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 the ETM System Management Server, Applications, and Appliances.

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

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

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

https://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.

ETM® System Concepts

Introduction

Traditional data and voice network security procedures and technologies do not effectively address the primary vulnerabilities plaguing voice networks: voice fraud, including toll fraud and social engineering attacks; threatening calls, such as bomb threats; voice service abuse, such as theft of long-distance service and unauthorized ISP calls; and unauthorized modems and non-secure authorized modems that produce an unmonitored “back door” into the data network. Most of these threats exist whether the voice network is TDM, Voice-over-IP (VoIP), or hybrid. Additionally, the migration to VoIP introduces an additional set of vulnerabilities alongside these existing ones.

The vast majority of enterprises maintain a presence on the Internet in order to conduct business and provide Internet access for work-related activities. To secure the connection from the Internet and protect internal networks, enterprises deploy a variety of security measures, including firewalls, VPNs, intrusion detection/prevention, anti-virus, and content monitoring. When properly deployed and configured, these products help to protect the internal IP network from attacks originating from the enterprise’s Internet connection. However, none of these Internet-related security technologies protects the internal IP data network from attacks through back-door connections from the voice network created by unauthorized or non-secure modems and poorly configured voice systems. Nor do they protect against malicious activity targeting the voice network itself, such as voice fraud, harassing and threatening calls, and toll service theft or abuse.

The best solution to all of these voice network threats lies in applying security concepts from the IP network to the voice network—specifically, the deployment of expandable, Policy-based security applications on the enterprise voice network. This solution supports transparent voice security and management, providing unified visibility and security while simplifying the transition to Voice over IP (VoIP) for voice managers.

The ETM System provides this solution. The centrally managed ETM Appliances support multiple voice-network security applications including a Voice Firewall, Voice Intrusion Prevention System (IPS), call monitoring and alerting, and call content recording. This approach provides the voice network with the same security protections that have been present on IP data networks for many years. Additionally, the ETM System includes monitoring applications that support usage, utilization , and cost reporting.

Supported Transport Types

The ETM System protects the following circuit types:: T1 (CAS, SS7, and PRI); E1 (PRI and CAS); analog (North American and European); SIP; and with the ETM Unified Trunking Application (UTA), other VoIP protocols (except MGCP) supported by the Cisco ISR and ASR families of routers. On TDM circuits, the ETM System also performs call type detection, which provides a level of control and accuracy that PBX configuration cannot provide, since PBXs do not detect call type.

Seamless Security and Monitoring

The ETM System allows you to seamlessly secure and monitor all of your voice traffic, supporting the migration from a legacy PBX to a VoIP network.

With the ETM System, you can:

- Have visibility and control of the voice network through Policy-based resource access limits, calling pattern thresholds, usage monitoring, CDR reporting, and Call Accounting features, and QoS measurements
- Harden your voice network security by limiting access to protected resources, tracking suspect calling patterns, and alerting for fraudulent or malicious access attempts.
- Define Rule-based Voice IPS Policies to detect and protect against anomalous call patterns that could indicate toll fraud or other intrusion attempts.
- View real-time call activity and manually terminate suspect calls.
- View real-time voice network health and status.
- Receive real-time notification of security or availability events.
- Centrally monitor and manage diverse, geographically dispersed telecommunications resources via a distributed, scalable, client/server architecture.
- Generate reports of call data from a centralized relational database that stores ETM System data across the enterprise, for accurate resource utilization tracking, departmental billback, and cost accounting.
- Monitor QoS parameters for VoIP using real time data and historical reports.

Unprecedented Telecom Network Security

Traditional data and voice network security procedures and technologies do not effectively address the primary vulnerabilities plaguing voice networks: voice fraud, including toll fraud and social engineering attacks; threatening calls, such as bomb threats; voice service abuse, such as theft of long-distance service and unauthorized ISP calls; and unauthorized modems and non-secure authorized modems that produce an unmonitored “back door” into the data network. Most of these threats exist whether the voice network is TDM, VoIP, or hybrid. Additionally, the migration to VoIP introduces an additional set of vulnerabilities alongside these existing ones.

The vast majority of enterprises maintain a presence on the Internet in order to conduct business and provide Internet access for work-related activities. To secure the connection from the Internet and protect internal networks, enterprises deploy a variety of security measures, including firewalls, VPNs, intrusion detection/prevention, anti-virus, and content monitoring. When properly deployed and configured, these products help to protect the internal IP network from attacks originating from the enterprise’s Internet connection. However, none of these Internet-related security technologies protects the internal IP data network from attacks through back-door connections from the voice network created by unauthorized or non-secure modems and poorly configured voice systems. Nor do they protect against malicious activity targeting the voice network itself, such as voice fraud, harassing and threatening calls, and toll service theft or abuse.

Attackers can also use war-dialing techniques to find unauthorized and insecure modems, which are present in nearly every enterprise. These can then be used to bypass the perimeter-focused data network security technologies. Once attackers have access to an internal system, they can exploit it and move to other systems in the network.

Migration to a VoIP network introduces additional vulnerabilities. It is less secure than the circuit-switched voice network (and less secure than other IP services) due to issues such as reliance on real-time packet delivery, complex protocols, insecure implementations due to a rush-to-market approach by vendors, and a weak common methodology for authentication and admission control. Vulnerabilities on the VoIP network can be exploited to launch Telephony Denial of Service (TDoS) attacks on voice networks, and protocol attacks using malformed signaling (both intentional and unintentional). These vulnerabilities also provide the means to commit toll fraud, voice eavesdropping, QoS abuse, and IP phone attacks.

The ETM System provides the tools and visibility you need to solve the many security and management issues associated with voice services delivered over the increasingly complex hybrid TDM and VoIP networks.

Visibility and Control

Besides providing unprecedented security for the data network, the ETM System provides complete visibility into and control of telecommunications resource usage. The ETM System can immediately alert specified personnel and optionally terminate offending calls in response to unauthorized telecom network access attempts, usage violations, anomalous VoIP signaling, telco events, and call pattern accumulations in excess of a set threshold. Email, SNMP traps, syslog alerts, and real-time alert messages in the ETM Client GUI are all available notification methods.

All of the data for each call, including the call type, is stored in Call Logs in the ETM database. This enables you to use the ETM System's Usage Manager reporting feature to generate reports that provide the information you need for accurate telecommunications accounting.

This visibility into your telecom network provides the following benefits:

- Identifies over- and underutilized resources to enable you to size your resources for maximum efficiency and reduce telecommunications costs.
- Enables you to attribute telephone usage to individual extensions (for example, international calls).
- Provides a tool to prevent misuse of resources such as toll fraud (for example, using a dedicated fax line to place international calls).
- Provides call-accounting visibility for IP trunks that may otherwise be unmonitored.
- Provides a tool for comparison and ROI calculations when using a toll-bypass VoIP network for toll cost reductions.

Remote, Enterprise-Wide Management

For large enterprises with geographically separated offices, a LAN, WAN, or the Internet can interconnect the separate components of the ETM System. This distributed, scalable architecture allows for remote, centrally managed, enterprise-wide visibility into telecommunications usage and status, enforcement of corporate telephony security and usage Policies, and real-time notification in specified instances of security or usage violations or telco alarms.

Remote, centralized management enables leveraging of personnel expertise, with fewer security and telecommunications personnel required to manage dispersed telecommunications resources. Larger enterprises with dispersed telecommunications resources can monitor all of those resources, both remote and local, simultaneously from a single ETM System Console.

Each communication link between components of the ETM System is protected through Triple DES (3DES) encryption. Communication between the Management Server and Client can also be encrypted with AES. The UTA Appliance and SIP Proxy can also use AES encryption for communication with the Management Server.

Real-Time Telco Health and Status Alarms

The ETM System provides real-time visibility into issues that can impact availability of your telecommunications network. Visual alarms in the Performance Manager tree pane alert you to telco alarms at a glance. You can also configure the ETM System to generate automatic notifications for a variety of telecommunications events that impact availability, such as loss of a PRI D-channel, excess bipolar violations, or T1 alarms. For each configurable event, you can configure the ETM System to send an email notification to the appropriate personnel, generate an SNMP trap or syslog event, and/or display and sound a real-time alert at the ETM System Console. This capability provides telecom personnel with a proactive tool for managing the telecommunications infrastructure, while lessening dependence on the service provider for real-time information.

Both IPv4 and IPv6 Supported

To support migration from IPv4 to IPv6, the ETM System supports IPv6 extended address spacing throughout the system. The ETM System supports hybrid IP networks.

Overview of the ETM® System

The ETM System consists of both hardware and software components.

Hardware:

- **ETM® Communication Appliances** are switch/media independent hardware and software devices that are installed either physically or logically inline (depending on the application type) on your TDM, analog, and SIP/VoIP trunking to continuously monitor, secure, log, and control all inbound and outbound voice traffic in real time. Each Communication Appliance provides one or more span interfaces (called *Spans* in the ETM System). Several versions of the ETM Communication Appliance are available to suit different sizes of enterprises and circuit types. All Appliances can be remotely managed and upgraded.

  Note: The UTA and SIP Proxy applications can also be virtualized.

- **ETM® Call Recording Cache (CRC) Appliance** that supports Call Recording storage, which can also be remotely managed.

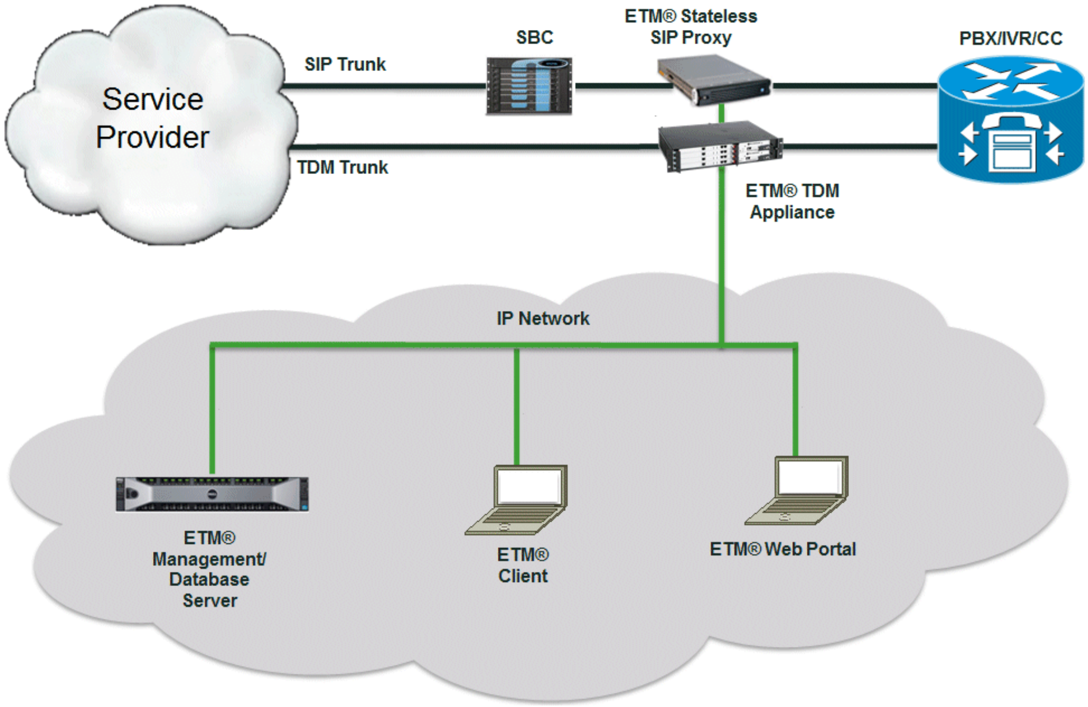
Software—A distributed, scalable Client/Server architecture consisting of:

- **ETM Client Applications and Tools**. These include the:
  - **ETM System Console**, the "launch pad" for the ETM System applications, from which you log in to the ETM System, launch each of the ETM Client Applications, manage the ETM Server and users, set system viewing preferences, and view system-wide status and alerts.
  - **Usage Manager**, an application from which you generate reports of ETM System activity, Policy processing, telecom cost accounting, and resource utilization.
  - **Directory Manager**, a client tool from which you manage the phone numbers and URIs used in the ETM System.
  - **Performance Manager**, an application that provides the dashboard from which you manage and monitor your ETM Appliances, view real-time monitoring and Policy processing, view system diagnostics, and use the ETM Rules-Based Policy Applications, which include:
    - **Call Recorder**
    - **Voice Firewall**
    - **Voice Intrusion Prevention System (IPS)**
  - **ETM Web Portal**, a web application from which you can access Call Recorder recordings.
- **ETM Server Applications and Relational Database**. These include:
  - **ETM Management Server**, the background processing engine that controls all access to and aspects of the ETM System. You log in to the ETM Server via the ETM System Console. The Server receives data from the Appliances, pushes configuration and Policies to them, generates Track (alerting) messages, and controls access to the system.

- **ETM Database**, a relational database that serves as a central data repository for most of the data captured by the ETM System. This includes call and Policy processing data, diagnostic logs, and system settings and configuration. The ETM Server maintains an active connection to the Database at all times. If this connection is lost, the Server enters Standby Mode until the connection is restored.
- **ETM Report Server**, which retrieves Usage Manager data from the database when you generate a report.

ETM® System Illustration

The illustration below depicts an example ETM System deployment on a hybrid network.



Spans

In the ETM System, a *Span* is defined as the interface between the ETM Appliance and the telecommunications network.

Analog Span—Interfaces with 12 or 24 analog lines.

E1 Span—Interfaces with a circuit carrying 30 digital channels using CAS, PRI, or SS7 signaling.

T1 Span—Interfaces with a circuit carrying 24 digital channels using CAS, PRI, or SS7 signaling.

SIP Proxy Span—A pair of IN/OUT Ethernet NIC interfaces, which provide the "tap" point for the ETM Appliance to monitor SIP traffic.

UTA Span—The interface to the Unified Trunking Application (UTA), which is integrated with an API in the IOS of a Cisco ISR or ASR to provide ETM Application functionality for all voice traffic on that router, both TDM and VoIP.

Call Type Detection

Call-type detection on TDM calls provides a level of control and accuracy unique to the ETM System. On SIP Spans, the call type is determined by the codec used.

Policies can prescribe specific actions based on the call type. For example, you can implement a Firewall Policy to terminate modem calls from or to specific numbers, send email notifications of voice calls on fax lines, and add an entry to the **Policy Log** for each unanswered call to your call center. And since all of the call monitoring data for each call, including the call type, is stored in the **Call Log**s in the ETM Database, you can use the Usage Manager to generate reports that provide the information you need for accurate telecommunications accounting.

Call Types Reported by the ETM® System

The table below defines each of the call types reported by the ETM System. All of these call types can be used in Policy Rules. The appropriate call type(s) for a Policy Rule depend on the Span type on which the Policy is to be installed. **Note**: For any call type that applies to UTA, it is reported as received from the API.

Call Type	Definition
Busy	On TDM Spans, busy signal detected (typically on an unanswered call). On SIP Spans, message received indicating a busy line. ***Note:*** Sometimes a message is played on busy lines instead of a busy signal, offering auto-redial when the line is free. In this case, the call type is identified as **Unanswered** or **Undetermined** rather than **Busy**, depending on the signaling on the trunk.
Data Call	(*Applies to PRI, SS7, and SIP*) Determined via specific D-channel or SS7 messaging, denotes a specific type of data call that may use more than one channel. Videoconferencing is a typical example. For SIP, a data codec was used.
Fax	Fax calls. Reported when distinct fax handshake messages are detected on the line. For SIP, indicates a fax codec was used.
Modem	(*Does not apply to SIP or UTA*) Modem calls. Reported when distinct modem handshake messages are detected on the line. See also *Modem Energy*.
Modem Energy	(*Does not apply to SIP or UTA*) Calls for which a type of energy characteristic of modems is detected (in-band call audio with the characteristics of modulated modem data) but that do not present a standard modem handshake. For example, very old modem protocols and non-standards-based data transmission devices lack a standard modem handshake. These calls are reported as Modem Energy. See also *Modem*.
STU	(*Does not apply to SIP or UTA*) Secure Telephone Unit III (STU-III) calls. Reported when distinct STU handshake messages are detected on the line.
Unanswered	The calling party hung up after the call was dialed, but before the call was answered.
Undetermined	A distinct call type has not been detected. This can occur in the following situations: • The calling number hung up after the call was answered but before the call type was determined. These may occur, for example, when a voice mail system answers the call, but the caller decides not to leave a voice mail message and hangs up. • Silent or indistinguishable calls are reported in the Call Monitor as **Undetermined** until one of the following occurs: - A distinct call type is detected. - When **Call Type Timeout** is reached, the call defaults to **Voice**. • For SIP, this call type is set if the codec in use has a type of **Unknown**, or if multiple codecs are negotiated, but no media packets are detected. • If an **Undetermined** call ends before it is answered, it is logged as **Unanswered**.

Call Types, continued

Call Type	Definition
Video	*(Only reported on SIP Spans*) A video codec was used.
Voice	Voice calls. On TDM Spans, reported when voice energy is detected on the line, or when answered calls identified as **Undetermined** reach **Call Type Timeout**. On SIP Spans, reported when a voice codec is used.

Continuous Call Type Monitoring

Continuous call type monitoring is an important function of each Span in the ETM Platform. Because the call type detection is continuous, the Span detects and reports any change in call type on TDM Spans throughout the duration of a call. For example, if someone makes a voice call and then manually initiates a fax transmission during that same call, both of those call types are logged and reported. Any time the call type changes during a call, the call is again compared to the installed Policies.

VoIP codec selection and SIP messaging are similarly monitored and recorded throughout the call. However, in certain scenarios on VoIP, an intermediate determination of **Busy** is discarded and replaced with the terminal state of the call. For example, if a call reaches a busy endpoint but is then redirected to a voicemail system on a different network resource, the call type associated with the codec used to reach the voicemail system is reported instead of the interim **Busy** state.

How the ETM® System Determines Called/Calling Numbers

How the ETM System determines source (calling) or destination (called) phone number depends on the services provided by the CO and PBX, the Span type, and the trunk configuration. For example, destination digits are typically available in call data for both inbound and outbound calls, and source numbers may be available on the line for inbound calls as Caller ID, Automatic Number Identification (ANI), or Calling Party Number (CPN). However, the source phone number may not be available in call data for outbound calls on T1 or analog lines; in this case, Station Message Detail Recording (SMDR) or Call Detail Recording (CDR) data from the PBX can be used to determine the source of the call. For dedicated lines, a Channel Map is provided to identify the associated phone numbers. On VoIP circuits, the Call Type is determined by the codec used.

The ETM System is configured during installation to suit the telecommunications environment at your location. Configuration settings for each monitored channel on each Span specify what numbers are expected to be available on the line (such as Caller ID or CPN) and what numbers are to be used for call accounting and Policy enforcement (for example, extensions obtained from SMDR data). In addition, *Dialing Plans* installed on each Span provide information used to recognize and classify phone numbers.

Dialing Plans

Each ETM Span uses a local and world *Dialing Plan* to process calls against ETM System Policy Rules and to accurately classify calls for call accounting. Local Dialing Plans are specific to the Appliance locale; world Dialing Plans are specific to the country in which the Appliance is located. These Dialing Plans provide necessary information that the Span uses to recognize, normalize, and classify various types of phone numbers. Dialing plans accomplish the following:

- Provide information that the Span uses to convert the dialed digits in call data into numbers containing a country code, area code, and phone number. These are called *normalized* numbers. By normalizing called and calling numbers, the Dialing Plan enables the Span to accurately match calls from all trunk types and dialing environments against Voice Firewall and IPS Policy Rules.
- Specifies which area codes and exchanges are local and long distance for the Appliance locale, enabling the ETM System to classify calls and source and destination numbers for telecommunications auditing.
- Specifies Emergency and Information phone numbers.

By default, Spans have default local and world Dialing Plans installed that enable the ETM System to process calls. The world Dialing Plan is unlikely to require changes; however, various local Dialing Plan sections must be customized for the specific Appliance locale to ensure proper number recognition (for example, if DID is in use) and call classification (for example, local vs. long distance), and to provide labels used to identify Service Types used in Voice IPS policies and for call accounting.

Outbound SMDR and Call Monitoring

On the telco network side of a PBX where the Appliance is typically installed, the source extension for an outgoing call may not be present on the line, particularly on T1 lines. However, Spans can use SMDR or CDR information available from a PBX to obtain station-side extensions and other call data. Several outbound SMDR settings are available to suit different types of trunks. For example, if CPN is available on PRI trunks, SMDR is not needed to identify the source for Policy processing, but you may want to augment the data in the database; on T1 trunks, however, you may need to obtain the source number for Policy processing from SMDR.

The following outbound SMDR settings are available:

- **Off**—The Span does not request SMDR data from the Server. The source number in signaling is used if available; if not, the value in the Extension map is used, if available; otherwise, no source is available. The call data available during the call is used to populate the database.
- **On**—The Span requests and waits for SMDR data from the Server. The source number collected from signaling, if any, is not used, but the source number collected from SMDR is used for Policy processing and is inserted into the database.
- **Augment**—The Span performs Policy processing with the source number in the signaling if it is present, but requests and waits for the source number from SMDR if necessary. If the source number is collected from the signaling, it is used to populate the database; the source number collected from SMDR is only inserted into the database if no source was received in the signaling. Any non-signaling fields (Access Code, SMDR1, SMDR2, etc.) available in SMDR are inserted into the database.
- **Replace**—The Span performs Policy processing with the source number in the signaling if it is present, but requests and waits for the source number from SMDR if necessary. The source number collected by the Span from signaling is used for policy processing, but after the call ends, the value received from the signaling is replaced in the database with the source number collected from SMDR. Any non-signaling fields (Access Code, SMDR1, SMDR2, etc.) available in SMDR are inserted into the database.

To enable the ETM System to use SMDR from the PBX, one ETM Appliance Card is physically connected to the PBX SMDR serial port and configured during installation as the *SMDR Provider* for all of the Spans being monitored at that PBX. The SMDR Provider Card passes SMDR data to the ETM Server, which reconciles call logs with the SMDR/CDR data and distributes extension information to the appropriate Spans for call progress logging and Policy enforcement.

Since the PBX does not typically transmit SMDR data until after the call ends, Firewall Policy Rules cannot enforce call termination based on source number for calls that require SMDR data. However, on these types of lines, you can install policies that prescribe security logging, email, and/or SNMP notification of key personnel when a Rule fires.

Inbound SMDR and Call Recording

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.

See the *ETM® System Call Recorder User Guide* for more details. Unlike outbound SMDR, inbound SMDR is only used for Call Recorder SMDR Extension processing. It is not used in Policy enforcement.

Remote Appliance Software Upgrades

The ETM Appliances are designed to be remotely upgraded as software updates become available, using a convenient dialog box in the Performance Manager. All Appliance software is fully upgradeable, including the operating system and application software, boot software, DSP software (if applicable), and Field Programmable Gate Array (FPGA)/Programmable Logic Device (PLD) firmware (if applicable).

Appliance Security

The ETM System employs various security features to secure Appliance Cards and their Spans from unauthorized access:

- To change Card or Span configuration, ETM System users must have the appropriate permission settings on their user accounts. All configuration changes are logged, indicating which configuration item was modified by which user.
- Access to the Cards/Spans in an Appliance is only allowed for authorized users. To log in to a Card via the Console port on the Appliance, a valid username and password are required. User access and access attempts are recorded in the **Diagnostic Log**.
- When accessing a Span via the Console port or Telnet, authorized users must know a separate "enable" password to make changes to configuration settings.

- Each Card in an Appliance can be placed into one of three security modes (low, medium, or high), which limit the manner in which security and network settings can be changed and determine whether Telnet/SSH is allowed.
- You can enable and disable availability of the Telnet server on the Card, and Telnet/SSH connections are only accepted from authorized IP addresses. By default, no access is allowed. Also, three successive failed Telnet attempts disconnect the Telnet port. Six failed attempts within ten minutes shut down the Card's Telnet server for sixty real minutes.
- Besides optional Telnet/SSH, the only other forms of TCP/IP communication with the Card are through a configurable port the Card uses to connect to the Server. A single port is used to simplify operation through enterprise IP firewalls.
- The ETM System supports a FIPS-compliant mode. The Appliance software is FIPS 140-2 and Common Criteria EAL 2+ certified. In accordance with the FIPS 140-2 Security Policy guidance, the Card uses only 3DES for communication to the ETM Management Server. The UTA Appliance and SIP Proxy can also use AES encryption for communication with the Management Server.

To connect to the ETM Server, the Card must know the ETM Server IP address, port, and DES key, and the Card's IP address must be listed in the ETM Server's **Authorized Cards** list. The Card always initiates the connection to the Server and validates that connection with a Triple DES encrypted message sequence, eliminating the possibility of a rogue “Server” connecting to a Card and thereby potentially impacting voice service. Subsequent communication is protected with 3DES encryption (or in the case of UTA/SIP Proxy, AES can be used).

For detailed information about ETM System security, see the *ETM® System Technical Discussion*, available from the SecureLogix website.

Types of ETM® Appliances/ Applications

Several types of ETM Appliances/software-only applications are available to suit the size and complexity of any organization’s phone network.

Communication Appliances

- The **ETM® model 1024**—(1U) Monitors up to 24 international or North American analog lines. Can optionally support Call Recording.
- The **ETM® model 2100**—(1U) Monitors up to four T1 (CAS, PRI, and/or SS7) or E1 (CAS, PRI, and/or SS7) Spans. Can optionally support Call Recording.
- The **ETM® model 3200**— (2U) Monitors up to 16 T1 (CAS, PRI, and/or SS7) Spans; or up to 16 E1 (PRI and/or CAS) Spans. Can optionally support Call Recording.
- The **ETM® SIP or UTA Servers**—(1U or 2U) The SIP Server provide inline SIP trunk monitoring, and UTA integrates with an API in the iOS in a voice-aware Cisco ISR G2 or later or ASR to monitor any combination of circuit types enabled by that router. UTA provides full ETM system functionality without the need to be inline with the voice network but is instead integrated via web services interfaces. Several sizes of SecureLogix Servers are available to suit various sizes of enterprises.

- **Software-only UTA** running on a blade in a Cisco ISR G2 or later or virtualized on COTS hardware that meets minimum system and resource requirements. Identical in functionality to UTA Server above.
- **Software-only SIP Proxy application** virtualized on COTS hardware that meets minimum system and resource requirements. Identical in functionality to SIP Server above.

Application Appliances

- The **ETM® CRC Server**—A third-generation of the CRC Appliance with greater storage capacity. Optional component of the Call Recorder. Accepts and stores call recordings from up to 32 Recording Spans concurrently, with a maximum call volume of 120 simultaneous calls.

Voice Network Circuit Type Support

The ETM System supports the following types of voice circuits and signaling types:

- **VoIP**—The ETM System supports VoIP with both the SIP Proxy Application and UTA.

  The ETM SIP Proxy Applications function as a stateless SIP proxy that supports SIP trunks from the carrier. These Applications are installed logically inline, enabling call termination. The SIP Proxy Application supports the following SIP specifications: RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3311, RFC 3325, RFC 3389, RFC 3550, RFC 3551, RFC 4566.

  UTA supports most VoIP protocols except MGCP (along with TDM) and functions in conjunction with an API embedded in the iOS of a Cisco ISR G2 or later or ASR, without the need to be inline.
- **Analog**—Analog support is available on the ETM 1024 Appliance. Supports loop start, ground start, and reverse battery loop start trunks. Supports FXS and FXO. It is also available on UTA. When used with UTA, the physical connection is governed by the router and transparent to UTA.
- **T1 CAS**—T1 CAS support is provided by either UTA or the ETM 2100 and 3200 digital Appliances.

  When used with UTA, the physical connection is governed by the router and transparent to UTA.

  The digital appliances support Super Frame and Extended Super Frame framing formats. Supports Alternate Mark Inversion and Bipolar 8 Zero Substitution line coding Supports ground start, loop start, wink start, immediate start, and asymmetrical signaling. Supports various cable lengths (line build outs). Supports DTMF and MF digit detection. For fractional T1s, the non-voice channels can be ignored.
- **E1 CAS**—E1 CAS support is provided by either UTA or the ETM 2100 and 3200 digital Appliances.

  When used with UTA, the physical connection is governed by the router and transparent to UTA.

  The digital appliance supports CAS signaling on a 30-channel E1 Span. Supports the CRC4 Multiframe and Non-CRC4 Multiframe framing formats. Supports Alternate Mark Inversion and High Density Bipolar Order 3 line coding. Supports the R1 signaling type only. Supports MF and DTMF digit detection.

- **T1 PRI**—T1 PRI support is available provided by UTA and the ETM 2100 and 3200 digital Appliances.

  When used with UTA, the physical connection is governed by the router and transparent to UTA.

  The digital appliance supports a 24-channel T1 Span using PRI signaling (often referred to as ISDN PRI). Supports the DMS100, ATT 5ESS, ATT 4ESS, and NI-2 variants. Supports Non-Facility Associated Signaling (NFAS). NFAS allows multiple PRI Spans to be controlled from a single D channel. Supports use of backup D channels.

- **E1 PRI**—E1 PRI support is provided by UTA and the ETM 2100 and 3200 digital Appliances.

  When used with UTA, the physical connection is governed by the router and transparent to UTA.

  The digital appliances support a 30-channel E1 Span using European variants of ISDN PRI. Supports the NET5 and QSIG protocol variants. Certification testing was only performed against the NET5 protocol version, as customer demand for the other protocol variants is limited due to the widespread standardization on NET5. Support for DASS2 and DPNSS is also provided.

- **T1/E1 SS7**—Both fully associated and dedicated SS7 signaling are supported by the UTA Application and by the ETM 3200 Appliance.

  When used with UTA, the physical connection is governed by the router and transparent to UTA.

  3200 Appliances support fully associated SS7 Signaling Links, each SS7 Bearer Span provides support for up to two fully associated SS7 signaling links, allowing SS7 signaling links and bearers to be managed on the same Card. For dedicated SS7 Cards, the cPCI Card sets support 1 to 4 ANSI SS7 signaling links carried over a single DS1. The signaling links may be 56Kbps or 64Kbps (but must all be the same). This Card set is only available for the ETM 3200 Appliance. Note that in this configuration, the Card set cannot process bearer Spans, but can communicate signaling information to other Card sets managing the bearer Spans.

For details about the interfaces for each supported circuit type, see the *ETM® System Technical Discussion* available in the SecureLogix Knowledge Base at https://support.securelogix.com.

Local Appliance/ Application Storage

Each Card in an ETM TDM Appliance has a Compact Flash device to store the Card software, Policies, and call log events/authentication database. UTA and SIP Proxy Applications provide local storage on the host platform on which they are running. This allows Spans to execute the installed Policies even if they cannot communicate with the ETM Server. If communication with the Server is interrupted, the Card/Application can store up to a week of call and Policy event information, depending on call load. This information is sent to the ETM Server when communication is reestablished. Call Recording and Firewall Policies continue to be executed, including prescribed Firewall call terminations. However, events are not logged on the ETM Server and real-time tracking events, such as emails, are not generated until communication is reestablished.

See the *ETM® System Installation and Configuration Guide* for Appliance technical specifications.

Breached IPS Rules cannot be recognized until communication is restored. The thresholds continue to be monitored, but no terminations based on breaches can occur until communication is reestablished. See "Voice IPS Policy Processing" in the *Voice IPS User Guide* for more information about IPS Policy processing in the event of a communication disruption.

Extension Masking/Call Redirection

Masking/Redirection Plans enable you to mask calling extensions, which enables the actual calling extension to be available to the ETM System for Policy processing. You can also redirect calls on based on source, destination, and/or direction. For example, you can:

- Redirect harassing inbound calls from known sources to the security department.
- Supply a substitute source number to be transmitted to called destinations.
- Redirect calls to your CEO and other executives for which Caller ID has been blocked to a recorded message that explains such calls are not accepted.

Masking is available for PRI and SIP Proxy applications. Redirection is available for UTA, PRI, and SIP Proxy applications.

On PRI and SIP Proxy applications, you can mask the calling party number by restricting it from being transmitted to the called party, while still allowing it to be sent to the ETM Application for call monitoring. You can mask CPN for all source numbers on all calls on a given Span, or for specific sources and/or destinations..

On PRI, UTA, and SIP Proxy applications, you can also redirect certain calls to other destinations, such as a recorded message.

You can define Masking/Redirection Plan rules for any entity in the ETM Directory (Listings, Groups, Ranges, Filters, and Wildcards), for caller ID restricted calls, and for calls with no source.

See the *ETM® System Administration and Maintenance Guide* for instructions for defining Masking/Redirection Plans and applying them to the applicable Spans.

User Account Permissions

User accounts control access to the ETM System. A comprehensive set of user account permissions enables you to control who is allowed to log in to the ETM System and which ETM System features they can access. See "User Administration" in the *ETM® System Administration and Maintenance Guide* for complete instructions for managing user accounts and details about available permissions.

User Password Security

The ETM System provides a user password security policy that determines:

- Whether user account passwords expire, and if so, how often.
- If passwords are set to expire, whether a warning is presented in advance, and if so, how far in advance, and how many expiration warnings are allowed before the account is disabled.
- Whether new passwords are checked for uniqueness against previous passwords, and if so, with how many they are compared.
- Frequency at which passwords can be changed.
- Minimum length and format for viable passwords.

By default, the user password policy applies to all user accounts on a Management Server; however, you can prevent the passwords on specific accounts from expiring. See "User Password Security" in the *ETM® System Administration and Maintenance Guide* for instructions for setting user password security.

ETM® System Policy Applications

The ETM System provides real-time Policy applications that enable you to define various types of Rule-based Policies to identify, monitor, and control your telecom network usage, access, security, and costs across circuit types. These Policy applications include:

- The **Voice Firewall**, used to monitor and control individual calls according to call criteria you define.
- The **Voice IPS (Intrusion Prevention System)**, used to identify and control calling patterns that might indicate toll fraud, war dialing attempts, misuse of resources, and other undesired events.
- The **Call Recorder**, used to record calls of interest for security and quality control, such as harassing calls or calls to your Customer Support department.

Voice Firewall Policies

Firewall Policies are used to control individual calls according to call criteria you define. A Firewall Policy consists of one or more user-defined Rules to which each monitored call is compared. Each Rule is defined to look for any combination of one or more of the following: source, destination, call direction, type of call, VoIP call attributes, call duration, midcall DTMF digit patterns, and/or specific call times. A call must match all of the parameters in the Rule before it is considered to match the Rule. When all of the parameters of a Rule match, the Rule is said to *fire,* or to have been *triggered* by the call.

Voice IPS Policies

IPS Policies monitor and protect your telecom resources against calling patterns over time, according to criteria you specify and thresholds you set. *Thresholds* can be based on accumulated cost, count, and/or duration of calls that match the other criteria in the Rule.

Rules can be based on any combination of the source, destination, call type, direction, service type, time, termination disposition, midcall DTMF digit patterns, and duration of calls.

For each IPS Policy Rule, you prescribe a time *Interval* during which thresholds are monitored, define a threshold, and dictate an action to occur when this threshold is breached—allow calls when the threshold is breached, allow active calls to continue when the Rule is breached but terminate future calls that match the Rule, or terminate the current calls that match the Rule and prevent future matching calls.

Call Recorder 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. An available *SMDR Extensions* list allows you specify how call recordings for these extensions are to be handled: deleted, saved, or saved and marked as sensitive.

Objects Used in Policies

The calls or call patterns to which a Policy Rule applies and what actions take place when a Rule matches are specified using *Objects*. Two types of Objects are used: *predefined Objects*, which cannot be user-modified; and *managed Objects*, which can be user-defined. Many of these Objects can also be used to filter logs and reports. See "Objects" on page 65 for instructions for defining each of the managed Objects.

Objects that can be used in Policies include:

- Call Types (predefined; all Policies)
- Directory entities (managed; all Policies)
- Tracks (email Tracks managed, others predefined; all Policies)
- Durations (managed; all Policies)
- Times (managed; all Policies)
- Subnets (managed; all Policies)
- Span Groups (managed; all Policies)
- Billing Plans (managed; IPS Policies)
- Intervals (managed, IPS Policies)
- Service Types (managed; IPS Policies)

Limit to the Number of Phone Numbers in Policies

As with any computing platform, the ETM Appliances have a limit to the amount of data that can be held in memory. This translates to a limit to the number of phone numbers that can be included in all of the Policies installed on a given Span (Call Recorder, Voice Firewall, and IPS).

During Policy installation, the ETM Server evaluates the size of the Policy against the available space on each Span in the included Span Groups. If the policy is too large to fit on any one of the Spans, verification fails and the Policy is not installed.

Normally, the existing Policy remains installed during installation of a new Policy of the same type, and calls in progress are processed against the existing Policy until the new Policy is completely downloaded to the Span and ready to immediately assume processing. At that point, the previous Policy is uninstalled and the new Policy seamlessly assumes processing, leaving no gap in Policy enforcement.

However, for large Policies, it is possible that the new Policy will only fit if the existing Policy is first uninstalled to free up the necessary memory it is using. To accommodate this possibility, two installation mode choices are provided:

- **Normal** mode—An evaluation is performed to determine whether the new Policy will fit on all Spans in the assigned Span Groups without first uninstalling the existing Policy. If so, the Policy installs normally. If the existing Policy must be uninstalled from any Span before the new Policy will fit in memory, Policy installation fails and a message is presented onscreen. You can then determine how to proceed: choose Priority mode to allow the current Policy to be uninstalled first and complete the installation, perhaps waiting until an off-peak call time to minimize risk from lack of Policy enforcement during the installation. Or you can modify the Policy to contain fewer objects, if practical, and then repeat Normal installation.

- **Priority** mode—If the existing Policy must be uninstalled from any Span to free up space for installation of the new Policy, this is performed automatically. Calls are processed using the default Policy until installation of the new Policy is complete.

How Many Phone Numbers?

The number of objects that can be used in Policies depends on the ETM Appliance Card model on which you are installing the Policies.

- 1024 Appliance—30,000 phone numbers.
- 8540 Controller Cards in 2100/3200 Appliance, SIP Proxy, and UTA applications—50,000 phone numbers.

Policy Permissions

See "User Administration" in the *ETM® System Administration and Maintenance Guide* for instructions for managing user permissions.

The level of access and control you have for each type of ETM System Policy is governed by several user permissions: **Access Policy Features**, **View & Reinstall <*Policy_type*> Policies**, and **Full Control**.

- Since Policies are managed from within the Performance Manager, you must have **Access Performance Manager** permission to view or edit any type of Policy or the Objects used in them.
- The ability to edit items used in Policies (Intervals, Tracks, Contacts, Billing Plans, Service Types, Times, Durations, and Span Groups) is governed by the **Access Policy Features** user permission, which must be granted before any other Policy permissions can be granted. Users who do not have **Access Policy Features** permission can view lists of and print reports of the items used in Policies, but cannot create or modify them. They cannot see the Policy trees in the Performance Manager tree pane or on the **View** menu.
- For each type of Policy, two options are available: **View & Reinstall <*Policy_type*> Policies**, and **Full Control**.
  - **View & Reinstall <*Policy_type*> Policies** enables you to view the Policy tree for that Policy type, open any Policy of that type, and reinstall Policies of that type that are already installed (for example, to update the Policy on the Span Group when Listings used in the Policy change).
  - To create, edit, delete, or uninstall any Policy, view Policy Logs, or install a Policy other than the one currently installed on a Span Group, you must also have the **Full Control** permission for that Policy type.

Span Groups

Span Groups organize Spans into logical units according to circuit type and Policy needs. Span Groups aid in Span management, much as trunk groups are used for trunk management.

Before you can install Policies on Spans, you must place the Spans into one or more Span Groups. Policies are installed on Span Groups rather than on individual Spans. However, a Span Group can contain only a single Span if appropriate. Only one Policy of each type can be installed on a Span Group.

When you move a Span into an existing Span Group on which user-defined Policies are already installed, the Span automatically receives and begins enforcing those Policies.

IMPORTANT All Spans enforcing the same IPS Policy must be in the same time zone, since IPS Policies apply to time intervals.

One Policy of each type can be installed on a Span Group. The default Policies are installed when no user-defined Policies are installed.

Default Policies

- The default Firewall Policy contains two Implied Rules: the Emergency Rule, which allows and logs calls to numbers in the default Emergency Group; and the Catchall Rule, which allows calls that did not match a prior Rule.
- The default IPS Policy contains no Rules.
- The default Call Recorder Policy contains one Implied Rule: the **Do Not Record** Rule that prevents recording of calls that did not match a prior Rule.

Active-to-Historical Data Transfer

For each ETM Server, the ETM Database stores two sets of call, IPS, and **Diagnostic Log** data: *active* and *historical*. This enables the ETM Database to function as both a transactional and a data warehouse database, and improves performance for reports. The **Policy Log** (used to view recent Policy processing results) retrieves data from the active data area; the Usage Manager (used to generate reports of ETM System data) retrieves data from the historical data area. Once data has been copied to the historical area, it is available for Reports. Once data has been deleted from the active area, it is no longer viewable in the **Policy Log**. By default, the copy frequency is twice as often as the delete frequency. Note that data is never deleted from the active area unless it has been copied to the historical area and is older than the specified delete frequency. By default, data is copied every 6 hours and copied data is deleted every 12 hours. The frequency at which data is transferred from the active to historical area is configurable; the default is every 6 hours from the time the ETM Server is started. See "Changing the Active-to-Historical Transfer Properties" in the *ETM® System Administration and Maintenance Guide* for instructions for modifying these frequencies.

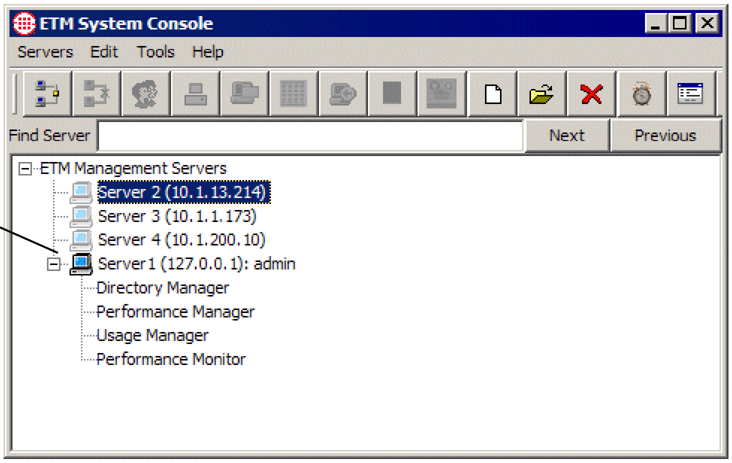
Tour of the ETM® Applications and Licensed Features

The sections below provide an overview of each of the ETM System applications and licensed features.

Tour of the ETM® System Console

The ETM System Console is the launch pad for the ETM System. It is used to:

- Log in to one or more ETM Management Servers.
- Launch the ETM System client tools.
- Manage user accounts.
- Manage ETM Server settings.
- Set viewing preferences.
- Shut down the ETM Server.
- View real-time alerts and status information.



To log in to an ETM Server, right-click it, and then click **Connect**, or click the ETM Server, and then click **Servers** | **Connect**; or click the **Connect to Server** icon.

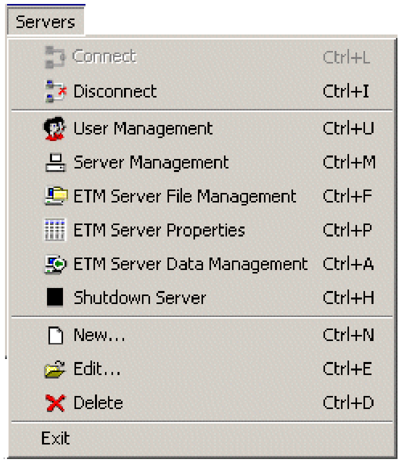
You can log in to multiple ETM Servers at the same time from the ETM System Console to view and modify settings. Each ETM Server provides a separate set of client tools (Performance Manager, Usage Manager, Directory Manager, and Performance Monitor). For example, you open one Performance Manager for ETM Server A and a second Performance Manager for ETM Server B. Real-time alerts for all of the ETM Servers you are logged in to are consolidated in a single **Alert Tool**, launched from the ETM System Console. When you log in, only the tools you have permission to access appear below the ETM Server in the tree.

Multiple users can log in simultaneously to the same ETM Server to monitor activity and modify settings. The Management Server uses *item-level locking* to ensure that only one user modifies configuration of the same item at a time. For example, two users can create contacts at the same time, but they cannot modify the same contact at the same time.

Main Menu

The ETM System Console main menu provides the following set of menus:

- **Servers**—Opens a drop-down menu with the following options:



Connect—Opens the **Login** dialog box so you can log in to the selected ETM Server. Not available unless an ETM Server is selected in the tree.

Disconnect—Logs you out of the selected ETM Server. Not available unless an ETM Server you are logged in to is selected in the tree.

User Management—Opens the **User Administration Tool**, in which you define and manage user accounts.

Server Management—Opens the **Server Administration Tool**, in which you manage ETM Server settings.

ETM Server File Management—Opens the ETM Server File Management Tool, in which you can remotely access files on the ETM Server and copy files to and from it.

ETM Server Properties—Opens the **ETM Server Properties Tool**, in which you can change various ETM Server properties.

ETM Server Data Management—Opens the **Data Management Tool**, in which you configure items related to city/state data and Directory Import Set imports.

Shutdown Server—Shuts down the ETM Management Server.

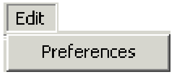
New—Opens a blank **Edit ETM Management Server Definition** dialog box where you can define a new ETM Server for the tree.

Edit—Opens the **Edit ETM Management Server Definition** dialog box showing the information for the selected ETM Server so you can view or change it. Not available unless an ETM Server is selected in the tree.

Delete—Deletes the selected ETM Server definition from the tree. Not available unless an ETM Server is selected.

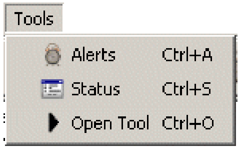
Exit—Logs you out of the ETM Server and closes all client applications.

- **Edit**—Opens a drop-down menu with the following option:



Preferences—Opens the **Preferences** dialog box in which you set display options.

- **Tools**—Opens a drop-down menu with the following options:



Alerts—Opens the **Alert Tool**, which displays real-time alerts from policy processing and system events.

Status—Opens the **Status Tool**, which shows progress and status as configuration is downloaded to appliance components.

Open Tool—Opens the tool(s) selected in the ETM System Console tree. Not available unless one or more tools (Performance Manager, Usage Manager, or Directory Manager) are selected under a Management Server you are logged in to.

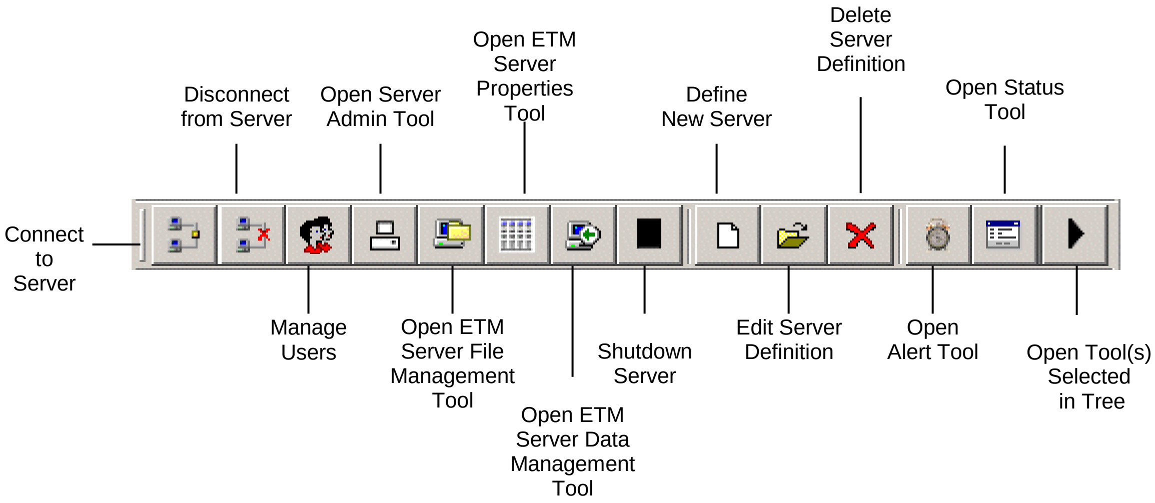
- **Help**—Opens a drop-down menu with the following options:

Help—Opens the online Help file for the ETM System. All of the information in the printed documentation is also provided in the online Help. A keyword search allows you to locate information quickly.

About—Opens the **About** screen for the ETM System Console, which provides the software version identification, the end-user license agreement (EULA), the website address for SecureLogix Customer Support, and trademark and copyright information.

Toolbar

The ETM System Console toolbar provides easy access to the options on the **Server** and **Tools** menus.

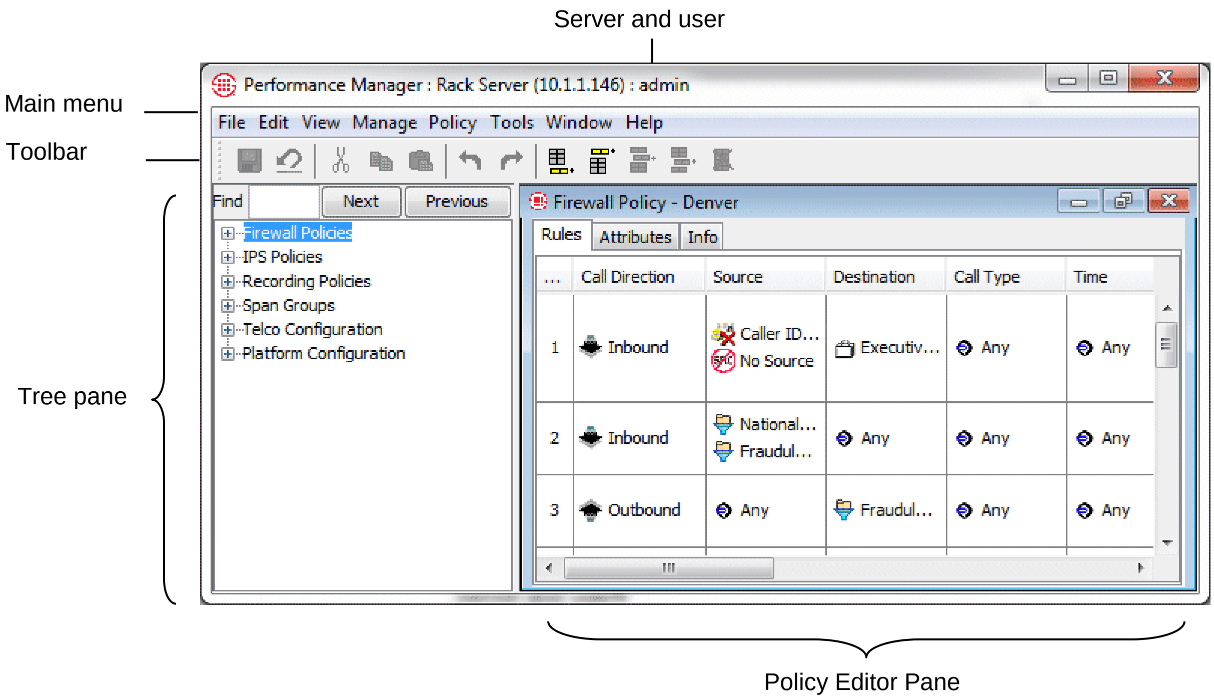


Tour of the Performance Manager

The *Performance Manager* provides the dashboard you use to:

- Monitor voice activity and status.
- Monitor Policy enforcement.
- Administer the ETM Appliances.
- Define and manage ETM System Policies.
- View system and telco diagnostic information.

The following illustration identifies the components of the Performance Manager.



...	Call Direction	Source	Destination	Call Type	Time
1	Inbound	Caller ID... No Source	Executiv...	Any	Any
2	Inbound	National... Fraudul...	Any	Any	Any
3	Outbound	Any	Fraudul...	Any	Any

Tree Pane

The Performance Manager tree pane displays the following items and provides right-click access to configuration and monitoring options for them:

- The **Firewall Policies** subtree is used to define and manage Voice Firewall Policies. It shows all of the Firewall Policies, the Span Group(s) to which they are assigned, and which Span Groups are currently enforcing each Policy.
- The **IPS Policies** subtree is used to define and manage Voice IPS Policies. It shows all of the IPS Policies, the Span Group(s) to which they are assigned, and which Span Groups are currently enforcing each Policy.=
- The **Recording Policies** subtree is used to define and manage Call Recorder Policies. It shows all of the Recording Policies, the Span Group(s) to which they are assigned, and which Span Groups are currently enforcing each Policy.
- The **Span Groups** subtree is used to define and manage Span Groups. It shows all of the defined Span Groups defined and the Spans belonging to each Span Group.

- The **Telco Configuration** subtree is used to configure SMDR, NFAS, SS7 Groups, and Call Recorder SMDR Extensions and to monitor telco status. It shows switches (a logical representation of the PBX) and their associated Spans, NFAS Groups, and SS7 Groups.
- The **Platform Configuration** subtree is used to configure, manage, and monitor status of appliance components. It shows the Appliance(s), Card(s), and Span(s) and how they are associated with one another and provides access to configuration and viewing options.

Real-Time Status Indicators

The tree pane provides real-time status indicators. These indicators appear next to the affected item in the **Span Groups**, **Telco Configuration**, and **Platform Configuration** subtrees, so issues are evident even if one or more subtrees is hidden. If a subordinate item experiences an issue, the indicator appears at each level of the tree, so that the issue is evident even when the tree is rolled up.

Alarm Type	Icon	Color	Meaning
Network	ϟ	Red	At the Span level, indicates the Span has lost network communication with the Server. At a higher level of the tree (such as Card level), indicates that all of the subordinate components have lost communication with the Server.
		Orange	One or more components subordinate to the level where the orange lightning bolt appears has a network error, but not all components are in the same state.
	ϟ CRC	N/A	The Recording Span cannot connect to its Call Recording Cache (CRC).
Telco	🔔	Red	The Span is in telco red alarm. On SIP, no SIP options seen.
		Yellow	The Span is in telco yellow alarm.
		Blue	The Span is in telco blue alarm.
		Orange	One or more Spans subordinate to the level where the orange bell appears are in telco alarm.
	OFF LINE	N/A	The Span is offline (acting as a passive pass-through device).
	Slink!	N/A	The SS7 signaling link time slot is inoperative (down).
	DCH	N/A	The D-channel on the Span is inoperative (down).

Real-Time Status Indicators, continued

Alarm Type	Icon	Color	Meaning
Card Application	FSF	N/A	The Card is in Failsafe mode. (The telco interface is not enabled in Failsafe mode, but the network interface is.)
	⚡	N/A	A Card has lost network communication with the Server, but one or more subordinate Spans are still connected to the Server. This is treated as an application error rather than a network error, because if a Card remains in this state after it has fully initialized, an application error is likely the cause. Note that it is normal for this state to occur briefly when a Card initially connects to the Server or is rebooted.
	LOOP BACK	N/A	The Span is currently in Loopback Test Pass-through Mode.
	⚠	N/A	One or more Cards subordinate to the level where the yellow triangle appears are in an application error state, but not all subordinate Cards are in the same state.
	⊗	N/A	The Signaling Proxy is down..
	SP	N/A	wsapi communication from the UTA appliance to the Router is down; neither are registered..

Main Menu Options

The Performance Manager main menu provides the following menus of options, which are used for all types of ETM System Policies:

Menu	Contains
File	Options for saving, refreshing, and printing Policies, and for closing the Performance Manager.
Edit	Options for working with Policy Rules (adding, cutting, copying, pasting, deleting, undo, redo) and for opening the **Properties** dialog box to set user display preferences for logs and the **Call Monitor**.
View	Options for showing/hiding display elements in the tree pane and in Policies.
Manage	Options for managing Contacts, Times, Tracks, Span Groups, Appliances, Intervals, Service Types, Codecs, Billing Plans, Subnets, Switches, and the list of valid Appliance Card IP addresses allowed to connect to this ETM Server.
Policy	Options for verifying, installing, and uninstalling Policies.
Tools	Option for accessing the **Diagnostic Log**.
Window	Options for arranging the display of open Policies and for selecting which of the open Policies has the focus.
Help	Option for opening the ETM System online Help.

Toolbar Icons

The Performance Manager toolbar provides icons for easy access to many Policy editing tasks. These icons are used with all types of ETM System Policies. When you hover your mouse cursor over an icon, a tool tip appears indicating the icon's purpose. The table below describes each of the available icons.

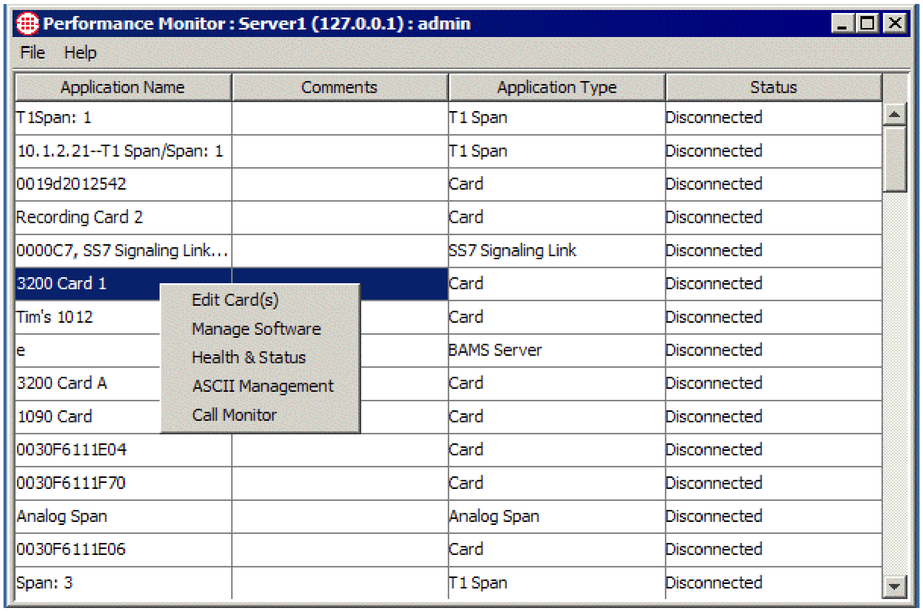
Icon	Purpose
💾	The **Save the Policy** icon saves the open Policy that has the focus. If the Policy is currently installed, saving the Policy also causes it to be downloaded to the Spans.
↺	The **Refresh the Policy** icon discards all unsaved changes and reverts the Policy that has the focus to its last saved state. (A warning message appears for you to confirm.)
✂	The **Cut rule to clipboard** icon removes the selected Policy rule from the display and transfers it to the system data buffer.
⎘	The **Copy rule to clipboard** icon copies the selected Policy rule to the system data buffer.
📋	The **Paste rule from clipboard** icon pastes the contents of the system data buffer (a previously cut or copied rule) into the open Policy that has the focus.
↶	The **Undo** icon causes the last Policy edit to be undone.
↷	The **Redo** icon restores the last Policy edit for which **Undo** was applied.
⊞	The **Add rule to top** icon adds a rule to the top of the list of user-defined Rules.
⊞	The **Add rule to bottom** icon adds a Policy rule to the bottom of the list of user-defined rules.
⊞	The **Add rule before selected** icon adds a Policy rule immediately preceding the selected rule.
⊞	The **Add rule after selected** icon adds a Policy rule immediately following the selected rule.
☒	The **Delete selected rule(s)** icon deletes the selected Policy rule(s).

Policy Editor Pane

Each type of ETM System Policy has its own Policy Editor. The Policy Editors open in the Policy Editor Pane. The options on the main menu and toolbar apply to all types of Policies.

Tour of the Performance Monitor

The **Performance Monitor**, launched from the ETM System Console, provides a dashboard view of the health and status of the Appliances/Spans so issues can be quickly identified without the need to open the Performance Manager. It displays only those platforms experiencing issues. Right-clicking a resource in the Performance Monitor provides a menu of options for further troubleshooting and corrective action.



Application Name	Comments	Application Type	Status
T1Span: 1		T1 Span	Disconnected
10.1.2.21--T1 Span/Span: 1		T1 Span	Disconnected
0019d2012542		Card	Disconnected
Recording Card 2		Card	Disconnected
0000C7, SS7 Signaling Link...		SS7 Signaling Link	Disconnected
3200 Card 1		Card	Disconnected
Tim's 1012		Card	Disconnected
e		BAMS Server	Disconnected
3200 Card A		Card	Disconnected
1090 Card		Card	Disconnected
0030F6111E04		Card	Disconnected
0030F6111F70		Card	Disconnected
Analog Span		Analog Span	Disconnected
0030F6111E06		Card	Disconnected
Span: 3		T1 Span	Disconnected

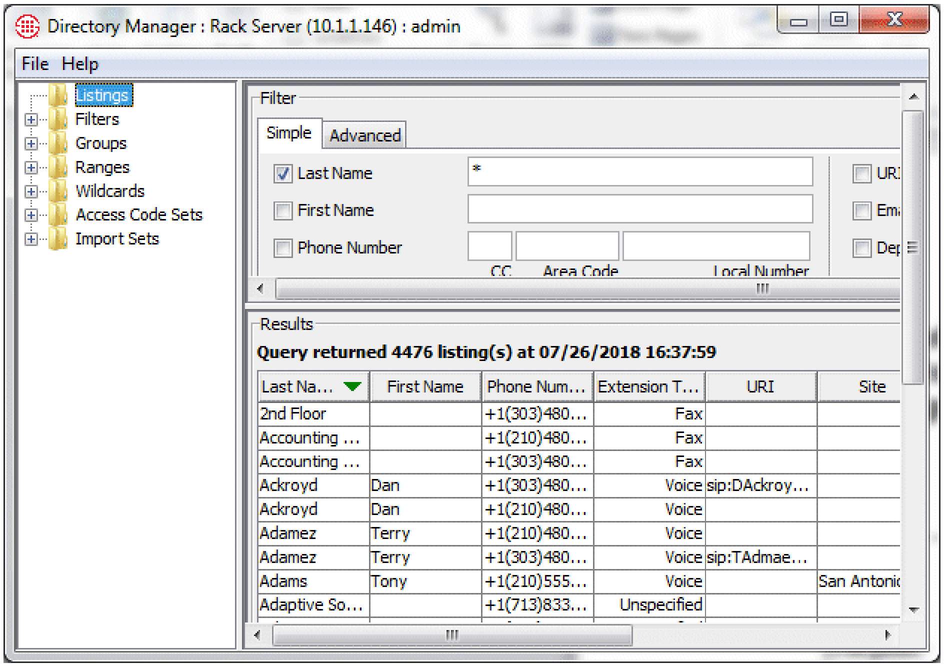
Tour of the Directory Manager

The Directory Manager is used to import and manage phone numbers and their identifying information in the ETM System. The items in the Directory Manager are collectively referred to as *Directory entities*. These entities are used throughout the ETM System in Policies, Reports, and Filters.

Server and user

Main menu

Tree pane. Provides folders for creating and managing each type of Directory entity.



☑ Last Name *

□ First Name

□ Phone Number

□ URI

□ Em

□ Dep

Query returned 4476 listing(s) at 07/26/2018 16:37:59

Last Na...	First Name	Phone Num...	Extension T...	URI	Site
2nd Floor		+1(303)480...	Fax		
Accounting ...		+1(210)480...	Fax		
Accounting ...		+1(303)480...	Fax		
Ackroyd	Dan	+1(303)480...	Voice	sip:DAckroy...	
Ackroyd	Dan	+1(210)480...	Voice		
Adamez	Terry	+1(210)480...	Voice		
Adamez	Terry	+1(303)480...	Voice	sip:TAdmae...	
Adams	Tony	+1(210)555...	Voice		San Antoni
Adaptive So...		+1(713)833...	Unspecified		

Editing pane. Displays and provides editing options for the item selected in the tree pane.

Directory Entities in the Directory Manager

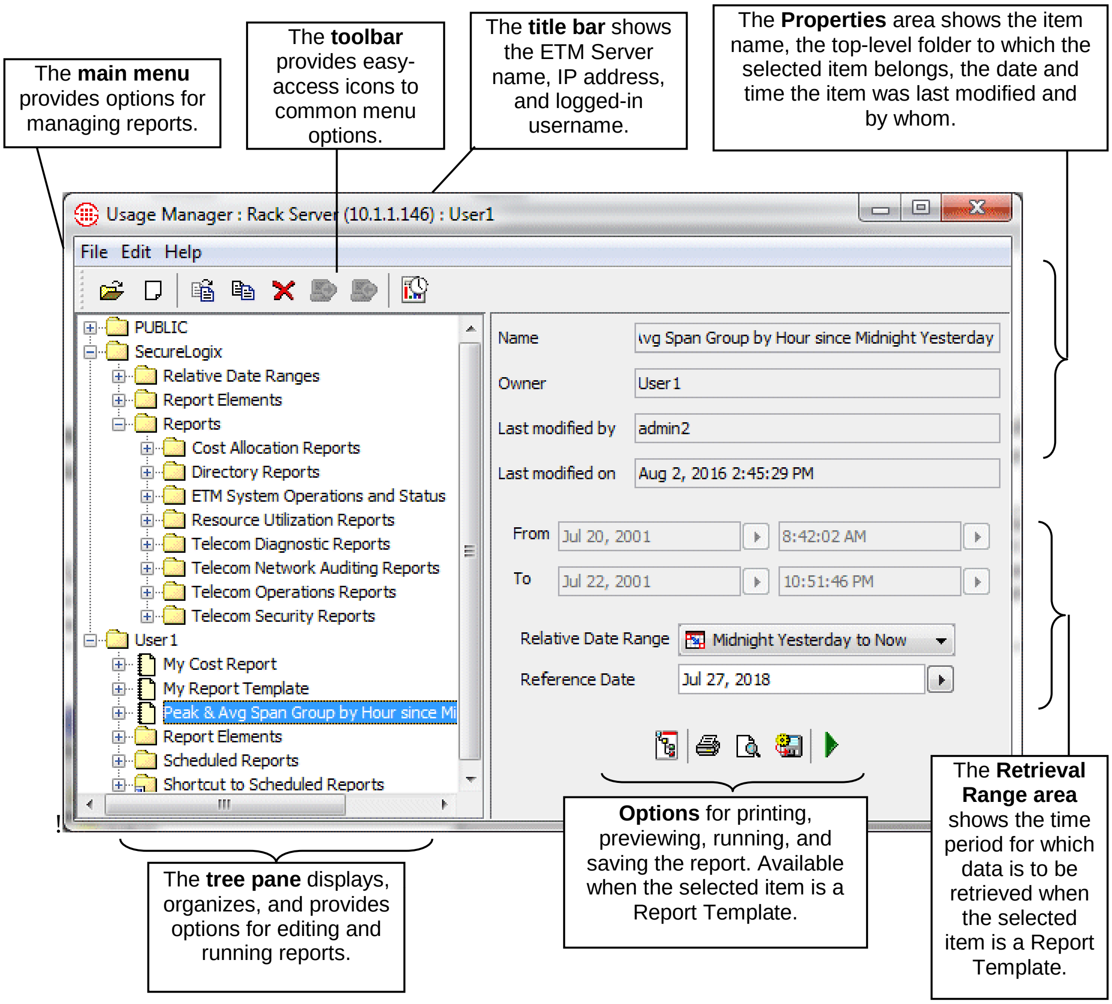
The Directory contains the following types of entries, collectively referred to as *Directory entities*:

- **Listings**, consisting of a single telephone number and its identifying information.
- **Filters**, which define a set of criteria for including Listings. Any Listings in the Directory that match the criteria are dynamically included anywhere the filter is used.
- **Ranges**, consisting of a consecutive series of phone numbers.
- **Groups**, consisting of any combination of Listings, Ranges, Wildcards, Filters, and/or other Groups.
- **Wildcards**. Two different types of Wildcards are available:
  - **Phone Number Wildcards,** which enable you to define Rules or filters to match selected portions of a phone number (country code, country and area code, a portion of the local number) rather than all digits.
  - **URI Wildcards**, which represent any portion of a URI.
- **Import Sets**, which contain a set of Listings imported from a text file or from an LDAP server.
- **Access Code Sets,** which correlate dialing Access Codes obtained from SMDR with Directory Listings.

See "Directory Manager" on page 95 for complete information and instructions for using the Directory Manager.

Tour of the Usage Manager

The Usage Manager GUI provides access to all of the Usage Manager features. The Usage Manager is launched from the ETM System Console after ETM Server login.



The **main menu** provides options for managing reports.

The **toolbar** provides easy-access icons to common menu options.

The **title bar** shows the ETM Server name, IP address, and logged-in username.

The **Properties** area shows the item name, the top-level folder to which the selected item belongs, the date and time the item was last modified and by whom.

Usage Manager : Rack Server (10.1.1.146) : User1

Name: ıvg Span Group by Hour since Midnight Yesterday

Owner: User1

Last modified by: admin2

Last modified on: Aug 2, 2016 2:45:29 PM

From: Jul 20, 2001 8:42:02 AM

To: Jul 22, 2001 10:51:46 PM

Relative Date Range: Midnight Yesterday to Now

Reference Date: Jul 27, 2018

File
Edit
Help
PUBLIC
SecureLogix
Relative Date Ranges
Report Elements
Reports
Cost Allocation Reports
Directory Reports
ETM System Operations and Status
Resource Utilization Reports
Telecom Diagnostic Reports
Telecom Network Auditing Reports
Telecom Operations Reports
Telecom Security Reports
User1
My Cost Report
My Report Template
Peak & Avg Span Group by Hour since Mi
Report Elements
Scheduled Reports
Shortcut to Scheduled Reports

The **tree pane** displays, organizes, and provides options for editing and running reports.

Options for printing, previewing, running, and saving the report. Available when the selected item is a Report Template.

The **Retrieval Range area** shows the time period for which data is to be retrieved when the selected item is a Report Template.

The Usage Manager GUI

The Usage Manager GUI consists of a *tree pane*, an *application pane*, a *toolbar*, a *title bar*, and a *main menu*, as illustrated above.

The Usage Manager tree pane organizes the report components and provides options for generating and editing reports, and viewing saved reports. The item selected in the tree pane appears in the application pane. The tree pane contains the following types of items:

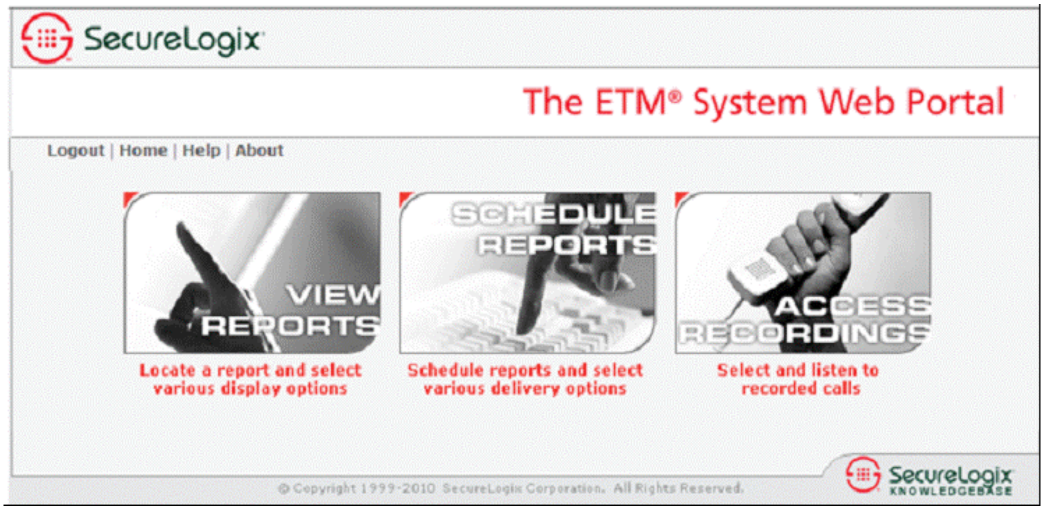
- Report Templates, which define a complete Report.
- Report Elements, which provide the content for Reports.
- Relative Date Ranges, which define the period a Report is to cover.
- Shortcuts to Templates, Elements, Relative Date Ranges, and other folders.
- Folders to organize the items.
- Generated Reports that were saved to the tree.

These items are organized into three top-level folders:

- **PUBLIC** contains items that can be used by anyone allowed to use this Usage Manager. All users can create, edit, and delete items in the **PUBLIC** folder.
- **SecureLogix** contains the predefined Report Templates, Elements, and Date Ranges provided with your system. This folder is read-only—no one can edit or create items in this folder, regardless of user permissions. However, you can run and schedule reports from this folder, including specifying a different Retrieval Range for the current case, and you can copy items from this folder to the **PUBLIC** folder or your user folder, where they become editable.
- ***<user>*** bears your login username and contains items that belong only to your user account. Only you and users with **Full Control** user permission for Usage Manager can see, create, edit, or delete the items in your user folder. Your user folder is empty until you add items to it.

ETM® Web Portal

The ETM® System provides a web-based interface called the Web Portal that enables you to access Call Recorder call recordings.


SecureLogix
The ETM® System Web Portal
Logout | Home | Help | About
VIEW REPORTS
Locate a report and select various display options
SCHEDULE REPORTS
Schedule reports and select various delivery options
ACCESS RECORDINGS
Select and listen to recorded calls
© Copyright 1999-2010 SecureLogix Corporation. All Rights Reserved.
SecureLogix KNOWLEDGEBASE

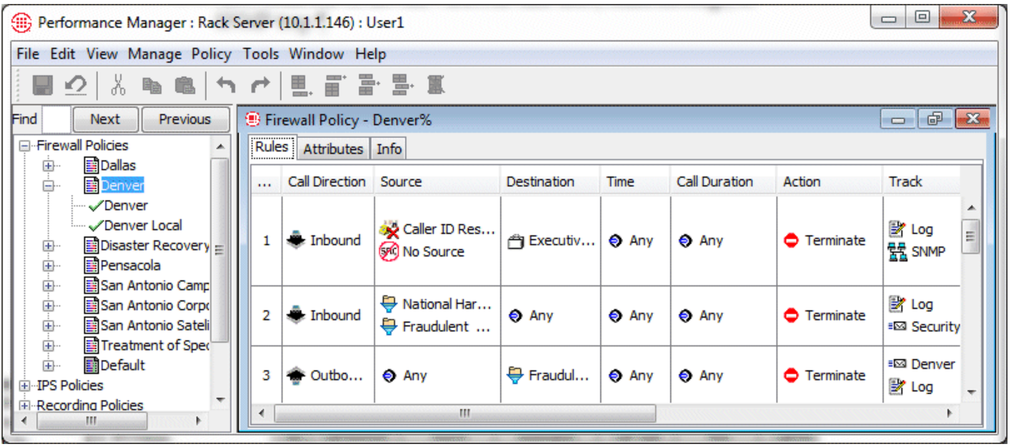
Tour of the Voice Firewall

Voice Firewall Policies allow you accomplish one or more of the following actions for a given call:

- Allow or terminate the call.
- Log the call in the **Policy Log**.
- Alert someone of the call via a real-time alert, email message, syslog alert, or SNMP trap.

A Policy consists of one or more user-defined Rules to which each monitored call is compared. Each Rule is defined to look for a specific source, destination, call direction, type of call, VoIP call attributes, call duration, and/or specific call times. A call must match all of the parameters in the Rule before it is considered to match the Rule. When all of the parameters of a Rule match, the Rule is said to *fire*.

After you define Policies, you install them on the Spans in the ETM® Appliances that are monitoring your voice network. The Spans then automatically enforce the Policy in real time.



...	Call Direction	Source	Destination	Time	Call Duration	Action	Track
1	Inbound	Caller ID Res… No Source	Executiv…	Any	Any	Terminate	Log SNMP
2	Inbound	National Har… Fraudulent …	Any	Any	Any	Terminate	Log Security
3	Outbo…	Any	Fraudul…	Any	Any	Terminate	Denver Log

Firewall Policies subtree. Used to create, open, edit, and manage Firewall Policies.

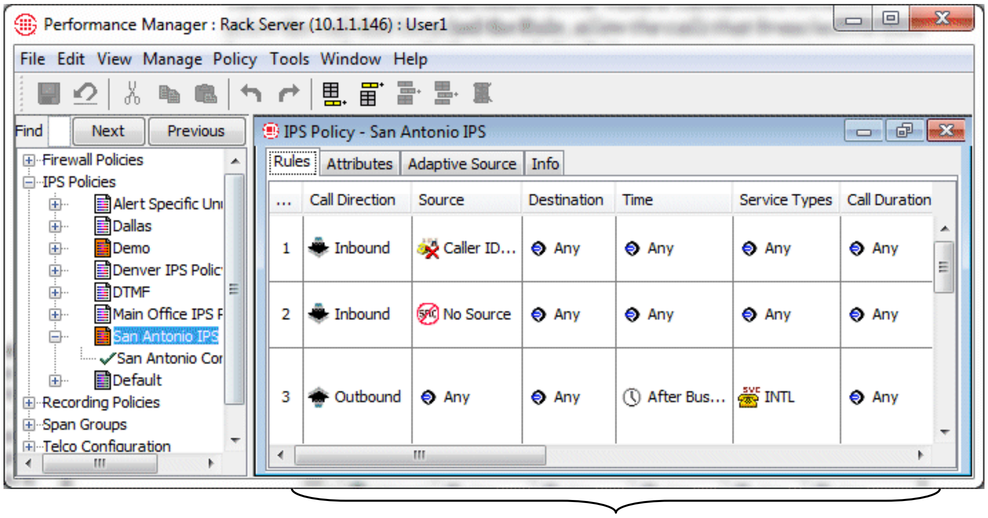
Firewall Policy open in the **Policy Editor**.

See the *Voice Firewall User Guide* for complete instructions for defining and managing Firewall Policies and viewing policy enforcement. For a quick introduction to defining Firewall Policies, see "Voice Firewall Policy Quick Start" on page 56.

Tour of the Voice IPS

Voice Intrusion Prevention System (IPS) Policies enable you to use rule-based Policies to manage usage of your telecom resources and protect your network against potential intrusion attempts, based on calling pattern *Thresholds* over a specified *Interval*. Thresholds can be based on accumulated cost, count, or duration of calls that match the other criteria in the Rule. For each Voice IPS Policy Rule, you prescribe a Threshold and dictate an action to occur when a Threshold is breached: *allow* the call that breached the Rule, *allow the calls that breached the Rule but prevent future calls* that match the Rule, or *terminate ongoing matching calls and prevent future calls* that match the Rule.

After you define Policies, you install them on the Spans in the ETM® Appliances that are monitoring your voice network. The Spans then automatically enforce the Policy in real time.



...	Call Direction	Source	Destination	Time	Service Types	Call Duration
1	Inbound	Caller ID…	Any	Any	Any	Any
2	Inbound	No Source	Any	Any	Any	Any
3	Outbound	Any	Any	After Bus…	INTL	Any

IPS Policies subtree. Used to create, open, edit, and manage IPS Policies.

IPS Policy open in the **Policy Editor**.

Adaptive IPS

An attacker’s calling number may be unknown until after the offense has occurred. The Adaptive IPS feature enables you to configure same-source tracking for IPS Policies, so that suspect patterns of calls from previously unidentified calling numbers can be identified and tracked. Once these numbers are identified, you can evaluate them to determine whether the calls represent an actual threat and take appropriate action on the identified phone numbers: whitelist those that are determined to be authorized and place those that are determined to be suspect in specific IPS, Firewall, and Call Recorder policy rules for further tracking and treatment.

See the *Voice IPS User Guide* for complete instructions for defining and managing IPS Policies and viewing policy enforcement. For a quick introduction to defining IPS Policies, see "IPS Policy Quick Start" on page 59.

Tour of the Call Recorder

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

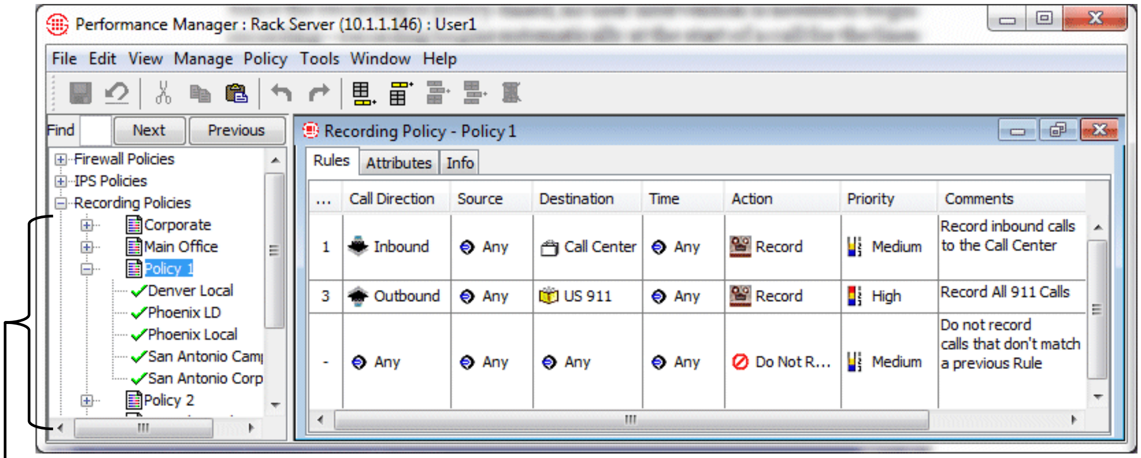
- Record all inbound calls to your call center for quality assurance and security monitoring.
- Record calls from/to customer support lines, to provide an audit trail.
- Capture threatening or harassing calls to your staff for investigation.
- Ensure that calls to protected extensions are never recorded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

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* and specify how call recordings for these extensions are to be handled: deleted, saved, or saved and marked as sensitive.

Calls that match a Rule that specifies **Record** are recorded and stored locally on the Call Recording Cache (CRC) or on an ETM Collection Server, and can be accessible remotely, enterprise-wide, via a web-browser interface called the ETM Web Portal.

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 via the Web Portal, you can transfer it to your client computer and use a **.wav** file playback tool to listen to the recorded call.

You can also locate and listen to calls directly from the Collection Server file system, using **.wav** file playback tools.



...	Call Direction	Source	Destination	Time	Action	Priority	Comments
1	Inbound	Any	Call Center	Any	Record	Medium	Record inbound calls to the Call Center
3	Outbound	Any	US 911	Any	Record	High	Record All 911 Calls
-	Any	Any	Any	Any	Do Not R...	Medium	Do not record calls that don't match a previous Rule

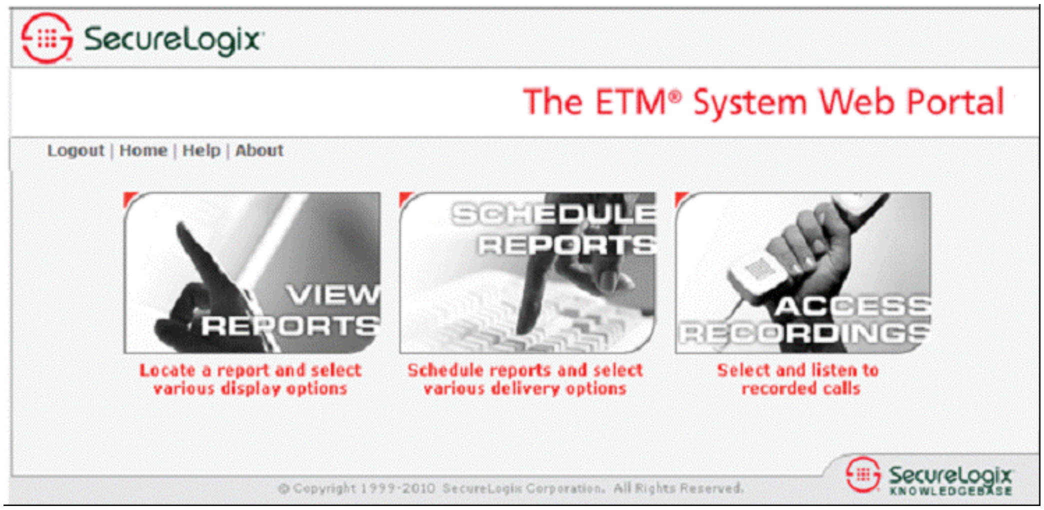
Recording Policies subtree. Used to create, open, edit, and manage Recording Policies.

Recording Policy open in the **Policy Editor** pane.

See the *Call Recorder User Guide* for complete instructions for recording calls and accessing call recordings.

ETM® Web Portal

The ETM Web Portal provides a browser-based interface with a rich set of search tools to locate and listen to call recordings stored on CRCs or the Collection Server. Note that Web Reporting is no longer supported.


SecureLogix
The ETM® System Web Portal
Logout | Home | Help | About
VIEW REPORTS
Locate a report and select various display options
SCHEDULE REPORTS
Schedule reports and select various delivery options
ACCESS RECORDINGS
Select and listen to recorded calls
© Copyright 1999-2010 SecureLogix Corporation. All Rights Reserved.
SecureLogix KNOWLEDGEBASE

Getting Started

Quick Start

This chapter is designed to quickly get you started using the ETM System.

For a quick start to running reports, see "Quick Start" in the *Usage Manager User Guide*.

You will learn how to:

1. Start the Management Server.
2. Log in to the Management Server.
3. Launch the Usage Manager, Performance Manager, Directory Manager, and Performance Monitor.

Starting the ETM® Server

The ETM Management Server usually runs continuously to manage the Appliances. If the ETM Server is not running, use the procedure below to start it. You cannot start the Server from a remote ETM Client.

To start the ETM® Server

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

  ```
  service ETMMS start
  ```

  Windows—Do one of the following:

  - Double-click the **ETM Management Server** icon on the desktop.
  - Click **Start | Programs | SecureLogix | ETM System Software | ETM Management Server**.
  - Start the **ETMManagementService** in the Windows **Services** dialog box.

Logging In to the ETM® Server

Multiple users can log in simultaneously to the same ETM Server to view and modify settings. The ETM Server uses *item-level locking* to ensure that only one user modifies configuration of the same item at a time. For example, two users can create Contacts at the same time, but they cannot modify the same Contact at the same time.

You can log in to multiple ETM Servers simultaneously from a single ETM System Console and easily switch between them to monitor system activity and administer the ETM System.

A client installed on the same computer as the ETM Server is always authorized to connect, whether or not its IP address is listed.

As a security feature, the ETM Server only accepts connections from remote ETM System Console clients whose IP addresses are listed in the Management Server's **Client Hosts** list. One authorized Client IP address is specified during system installation. The ETM System administrator then authorizes other remote clients as needed. For instructions for authorizing other remote clients, see "Authorizing Client Connections" in the *ETM® System Administration and Maintenance Guide*.

To log in to an ETM Server, you must have a user account defined on that Server. For information about defining user accounts, see "User Profiles" in the *ETM® System Administration and Maintenance Guide*. The permissions granted to your user account determine the features you can access and the configuration settings you can modify.

Opening the ETM® System Console

The ETM System Console provides access to all of the other ETM System features. It is used to log in to the ETM Server, launch the ETM Client Tools (Usage Manager, Performance Manager, Directory Manager), view real-time alerts and status, manage user accounts, configure ETM Server settings, and set viewing preferences.

To open the ETM® System Console

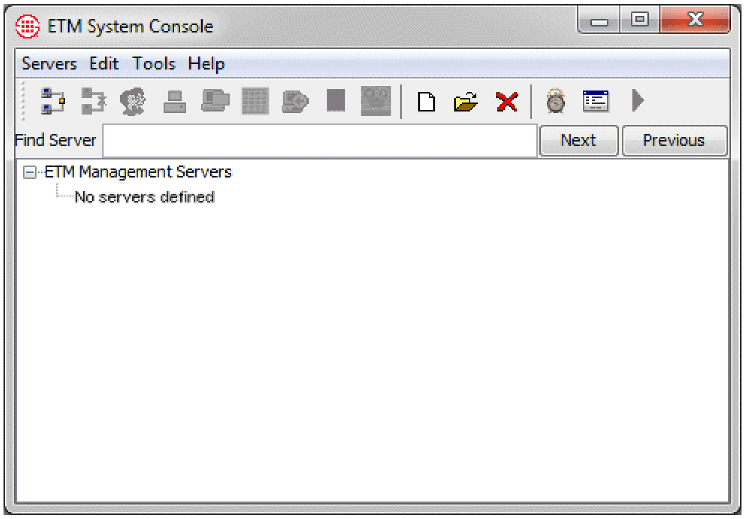
- Linux—Execute the following script, located in the ETM software installation directory:

  ```
  ETMSystemConsole
  ```

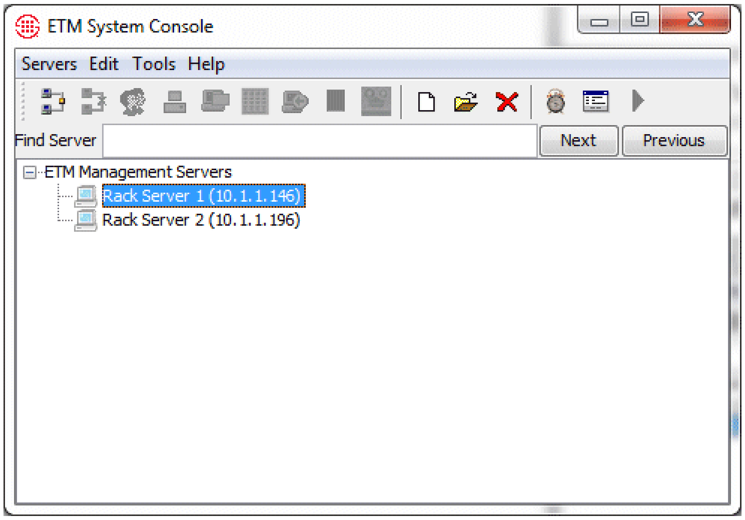
- Windows—
  - Double-click the **ETM System Console** icon on the desktop.
  - Click **Start | Programs | SecureLogix | ETM System Software | ETM System Console**.

The ETM System Console appears.

- If no ETM Servers are defined, the ETM Console appears as shown below. For instructions for defining an ETM Server, see "Defining an ETM® Server Object" on page 48.



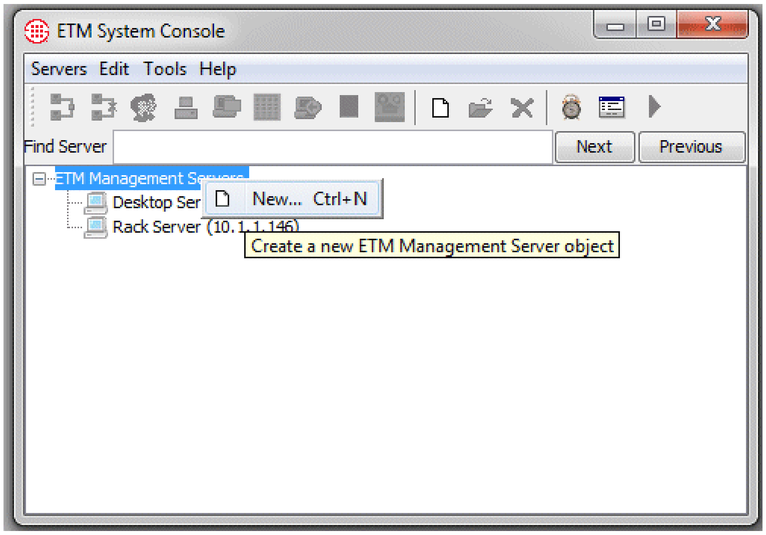
- If one or more ETM Servers have already been defined, the ETM Console appears similar to the following. If the ETM Server you want to log in to appears in the list, continue with "Logging In to the ETM® Server" on page 46. For instructions for defining a ETM Server, see "Defining an ETM® Server Object" on page 48.



Defining an ETM® Server Object

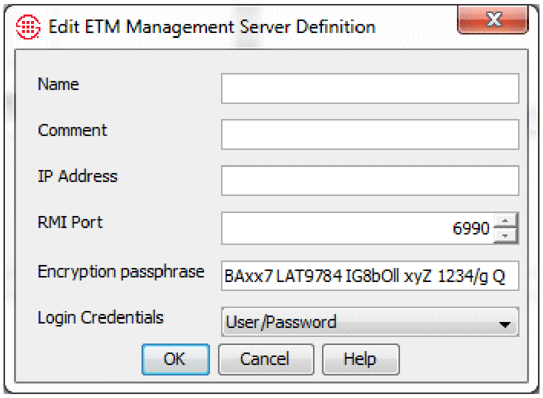
To define an ETM® Server Object

1. In the ETM System Console, right-click **ETM Management Servers** and click **New**.



Create a new ETM Management Server object

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



RMI Port 6990

Encryption passphrase BAxx7 LAT9784 IG8bOll xyZ 1234/g Q

Login Credentials User/Password

3. In the **Name** box, type the name you want to use for this ETM Server. The name can contain up to 265 characters and spaces.

4. In the **Comment** box, type a comment, up to 265 characters and spaces in length.

5. In the **IP Address** box, type the IP address of the computer on which the ETM Server is installed.

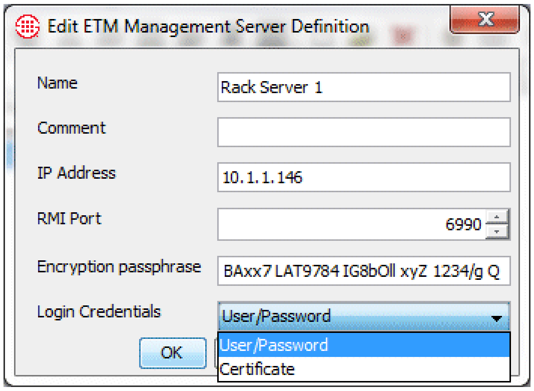
6. The **RMI Port** is the port on which the ETM Server accepts client tool connections. This port is specified in the **twms.properties** file on the ETM Server computer. The default is **6990**.

If your site uses a different RMI port, type or select the correct value. _Do not change this value unless instructed to do so by your ETM System administrator_.

7. The **Encryption passphrase** must match the value specified in the ETM Server's **twms.properties** file, because the initial negotiation is always encrypted to establish the connection. The default automatically appears in the box. If your site uses a different encryption key, type or paste that string here. _Do not change this value unless instructed to do so by your ETM System administrator_.

8. In the **Login Credentials** drop-down box, select one of the following:

   - **User/Password** – To enable username and password login for both default login and LDAP login.
   - **Certificate** – To enable CAC login.



Edit ETM Management Server Definition

Name: Rack Server 1

Comment:

IP Address: 10.1.1.146

RMI Port: 6990

Encryption passphrase: BAxx7 LAT9784 IG8bOll xyZ 1234/g Q

Login Credentials: User/Password

9. Click **OK**.

How to Log In to the ETM® Server

The ETM System provides two methods of logging in to an ETM Server:

- Username/Password login—The user enters their default or LDAP username and password to connect to an ETM Server. See "

To log in to an ETM® Server with username/password” on page 51.

- CAC (Common Access Card) login—The user inserts their card into a CAC reader to connect to an ETM Server. CAC authentication must be enabled. See “To log in to an ETM® Server with a CAC” on page 52.

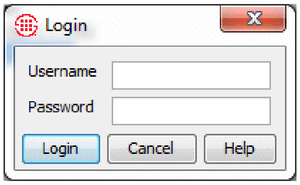
To log in to an ETM® Server with username/password

Tip: If only one ETM Server is defined in the ETM System Console, you can optionally configure the system so that the **Login** dialog box automatically appears when you open the ETM System Console. See "Enabling Single Server Autologin" on page 241 for instructions.

1. In the ETM System Console, click the ETM Server and then click the **Connect** icon. (*If you have only a single server defined and have single-server autologin enabled, skip this step and continue with Step 2*).

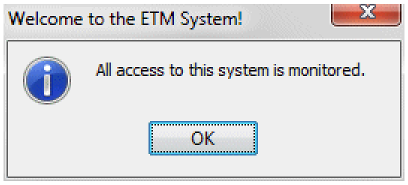
For information on creating user accounts, see “User Profiles" in the *ETM® System Administration Guide*.

2. The **Login** dialog box appears. In the **Username** and **Password** boxes, type your login credentials for the ETM System: the username and password for your user account on this ETM Server, or your LDAP username and password.



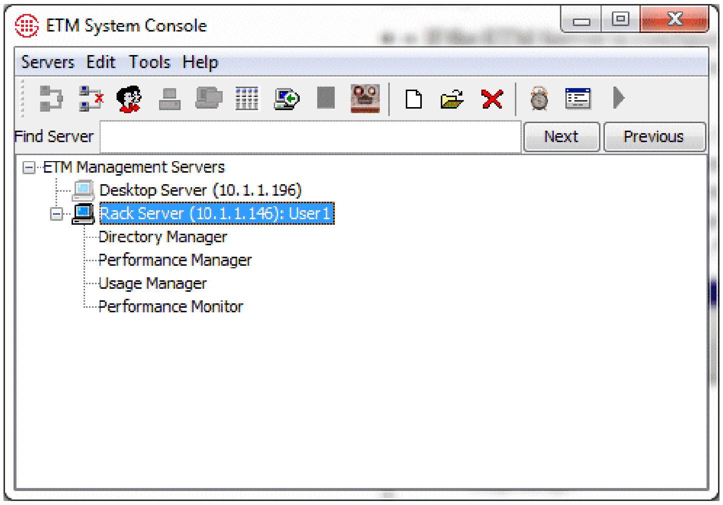
See "Defining a Login Banner" in the *ETM® System Administration and Maintenance Guide* for instructions for defining a Login Banner.

3. Press ENTER or click **Login**.
4. You are logged in to the ETM Server.
   - If the ETM Server is configured with a *Login Banner*, it appears in front of the ETM System Console when you log in. Click **OK** to close the Login Banner.


Welcome to the ETM System!

All access to this system is monitored.

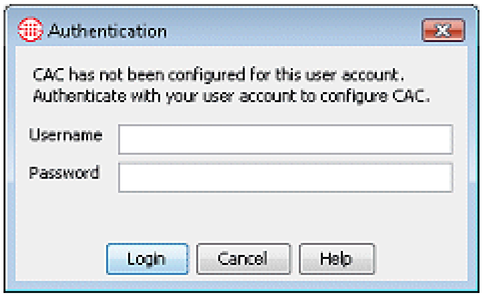
5. The tools your user permissions allow you to access appear below the ETM Server icon in the ETM System Console. For example, if you have permission to access the Directory Manager, the Usage Manager, and the Performance Manager, the display appears similar to the following illustration.



See "Opening Client Tools" on page 55 for instructions for launching the tools.

To log in to an ETM® Server with a CAC

1. Insert your CAC into the card reader. (On many Window systems with CAC, you will have already inserted your CAC in order to log into Windows.)
2. In the ETM System Console, click the ETM Server and then click the **Connect** icon.
3. If this is your first CAC login, the **Authentication** dialog box appears.

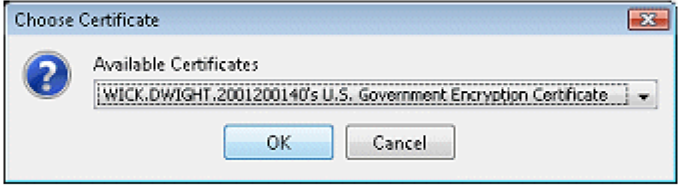


CAC has not been configured for this user account.
Authenticate with your user account to configure CAC.

   a. In the **Username** and **Password** boxes, type your login credentials for the ETM System: the username and password for your user account on this ETM Server.

      b. Press ENTER or click **Login**. Your login information will be validated and with successful login, the ETM System will automatically update your user account with your UID (Unique Identification) and certificate from the card so that the next time you connect to a server connection will be automatic. If you receive an error message and login fails, contact your Help Desk or System Administrator to confirm your login credentials.

6. In the **Choose Certificate** dialog box, select a certificate from the **Available Certificates** drop-down list, and then click **OK.**

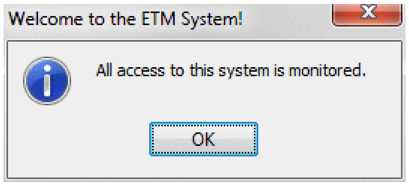


Choose Certificate

Available Certificates: WICK.DWIGHT.2001200140's U.S. Government Encryption Certificate

7. With successful CAC authorization, you are logged in to the ETM Server.

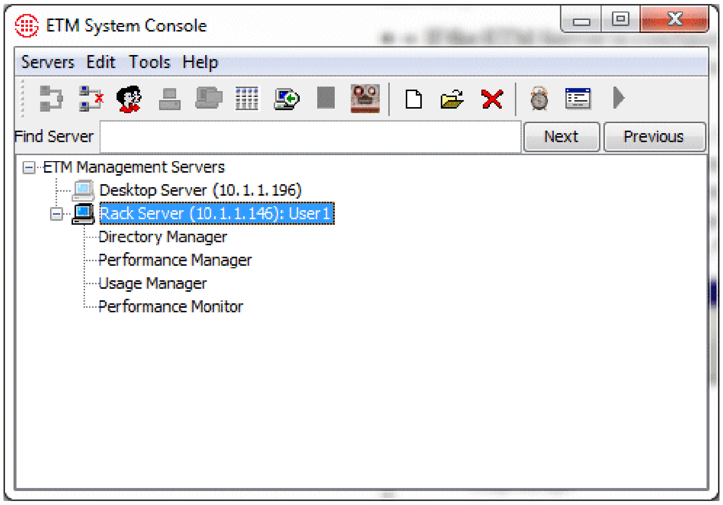
   - If the ETM Server is configured with a *Login Banner*, it appears in front of the ETM System Console when you log in. Click **OK** to close the Login Banner.



Welcome to the ETM System!

All access to this system is monitored.

8. The tools your user permissions allow you to access appear below the ETM Server icon in the ETM System Console. For example, if you have permission to access the Directory Manager, the Usage Manager, the Performance Manager, and the Performance Monitor, the display appears similar to the following screenshot.



4. See "Opening Client Tools" on page 55 for instructions for launching the tools.

How to Simultaneously Log In to Multiple ETM® Servers

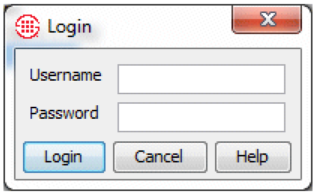
You can log in to multiple ETM Servers at the same time if your user accounts on multiple ETM Servers have identical login credentials, using the procedure below.

If you have different logins on each ETM Server, you simply repeat the single-ETM Server login procedure in "How to Log In to the ETM® Server" on page 49 to log in to each ETM Server.

To simultaneously log in to multiple ETM® Servers

1. In the ETM System Console, hold down CTRL and click each ETM Server to which you want to connect.
2. Right-click the selection and click **Connect**. CAC users are automatically connected to the ETM Servers (If CAC login fails, contact your Help Desk or System Administrator to confirm login credentials. If this is your first CAC login, see “To log in to an ETM® Server with a CAC on page 52.)
3. If you login with a username and password, the ETM Server **Login** dialog box appears. In the **Username** and **Password** boxes, type the username and password for your user account on these ETM Servers, and then click **Login** or press ENTER.

For information on creating user accounts, see “User Profiles" in the *ETM® System Administration and Maintenance Guide*.



How to Log Off of an ETM® Server

To log off of an ETM® Server

- In the ETM System Console, do one of the following:
  - Right-click the ETM Server and click **Disconnect**.
  - Click the ETM Server and click the **Disconnect from Server** icon
  - Click the ETM Server and then click **Servers | Disconnect** on the main menu.

Client tools include:

- The *Performance Manager*.
- The *Directory Manager*.
- The *Usage Manager*.
- *The Performance Monitor* .

Opening Client Tools

The ETM Database Maintenance Tool is accessed via the Windows **Start** menu, not from the ETM System Console. See the *ETM® System Technical Reference* for more information.

To open client tools

- In the ETM System Console, while logged in to the ETM Server, do one of the following:
  - Double-click the client tool you want to open.
  - Click the client tool you want to open, and then click the **Open Selected Tools** icon.
  - Right-click the client tool you want to open, and then click **Open Tool**.
  - To open multiple tools simultaneously, hold down CTRL and click each tool, and then click the **Open Selected Tools** icon.

  You can also configure the system to automatically open specified tools when you log in. See "Setting Client Tools to Autostart upon Login" on page 242 for instructions.

Policy Quick Start

The ETM® System provides several types of Policies, including:

- Voice Firewall Policies.
- Voice IPS Policies.
- Call Recorder Policies.

These Policies have a common look and feel so that once you are familiar with defining one type of Policy, you know much about defining any type of ETM System Policy. All Policies consist of a set of Rules with user-definable fields that you use to specify the criteria for calls that match the Rule. All Policies use the Policy management and editing features provided through the Performance Manager main menu and toolbar. After you define or modify the Policy, you install it on one or more Span Groups to begin enforcement.

Policies can be defined at a central location and then distributed throughout the enterprise, or they can be defined at each location. For Firewall and IPS Policies, the resulting Policy enforcement data is stored in a central database along with all other call data. Call Recorder data is available remotely from the Web Portal or locally from the Collection Server.

See the *Call Recorder User Guide* for instructions for defining and managing Recording Policies.

The sections below introduce IPS and Firewall Policy definition. Separate, detailed guides for defining and managing each type of Policy are also provided in your ETM System documentation set. Although the look and feel is similar for all Policies, the purpose and approach to effective development of each is very different. So is the way in which the ETM System processes each type of Policy. It is important that you refer to the guide for the type of Policy you are developing to familiarize yourself with these concepts.

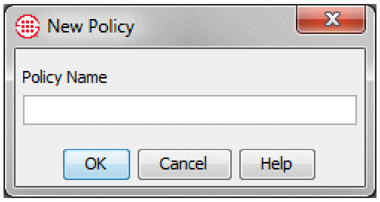
Voice Firewall Policy Quick Start

The instructions below provide a Quick Start for defining a Voice Firewall Policy. For detailed information and instructions, see the *Voice Firewall User Guide*.

To create a Voice Firewall Policy

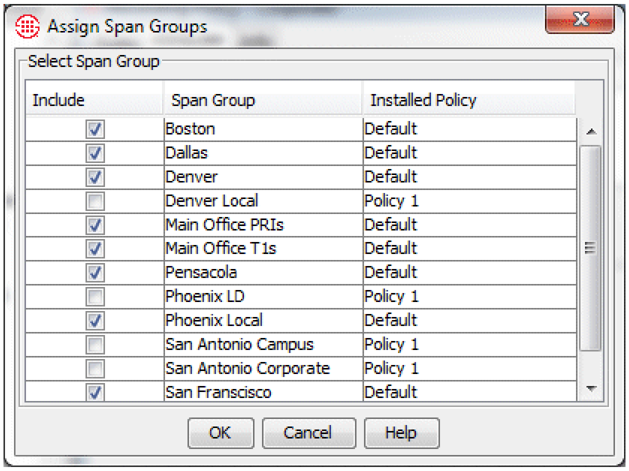
You must have the **Full Control** user permission for Firewall Policies to create them.

1. Open the Performance Manager.
2. In tree pane, right-click **Firewall Policies** and click **New**. The **New Policy** dialog box appears.



3. In the **Policy Name** box, type a name to identify the Policy, and then click **OK**. The **Assign Span Groups** dialog box appears.

See the "Assigning a Span Group to a Policy" in the *Voice Firewall User Guide* instructions for adding Span Groups to an existing Policy.



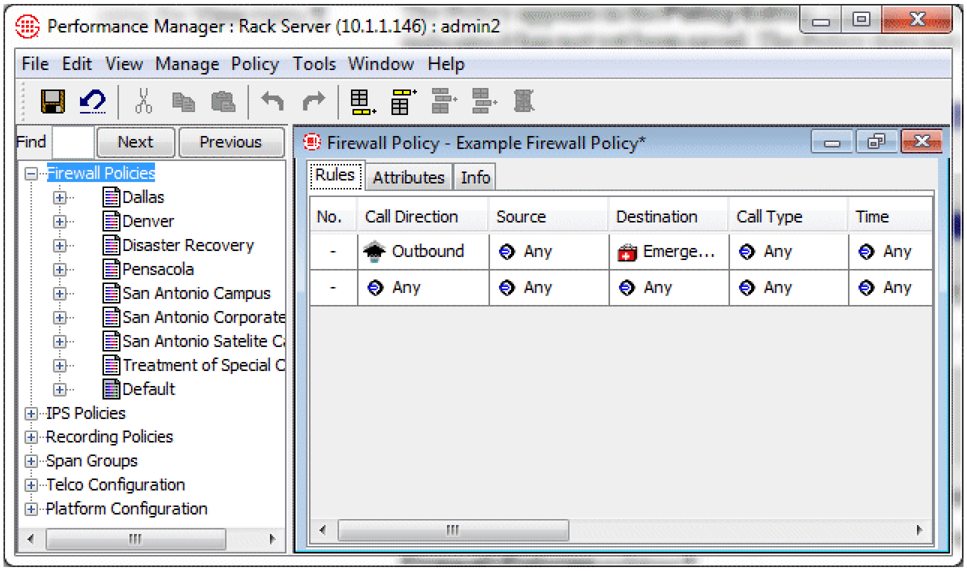
Include	Span Group	Installed Policy
☑	Boston	Default
☑	Dallas	Default
☑	Denver	Default
□	Denver Local	Policy 1
☑	Main Office PRIs	Default
☑	Main Office T1s	Default
☑	Pensacola	Default
□	Phoenix LD	Policy 1
☑	Phoenix Local	Default
□	San Antonio Campus	Policy 1
□	San Antonio Corporate	Policy 1
☑	San Franscisco	Default

The sample Policy below shows the two implied Policy Rules. If these are not visible, you can show them using the **View** menu.

4. All Span Groups on which the default Firewall Policy is currently installed are selected by default. Select each Span Group on which you want to be able to install the Policy and clear the check boxes for Span Groups on which you do not want the Policy installed, and then click **OK**.

- If the Span Group(s) you want to use have not yet been defined, clear any unwanted check boxes and click **OK** to close this dialog box and create the Policy. You can select Span Groups later.

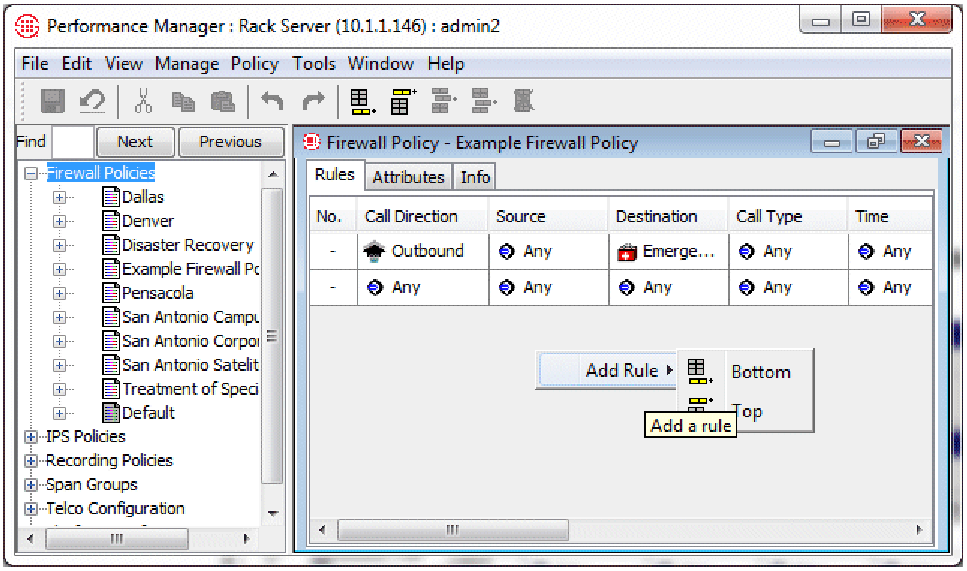
The Policy appears in the **Policy Editor**. The asterisk in the title bar indicates it has not yet been saved. The Policy does not appear in the tree pane until you save it.



No.	Call Direction	Source	Destination	Call Type	Time
-	Outbound	Any	Emerge...	Any	Any
-	Any	Any	Any	Any	Any

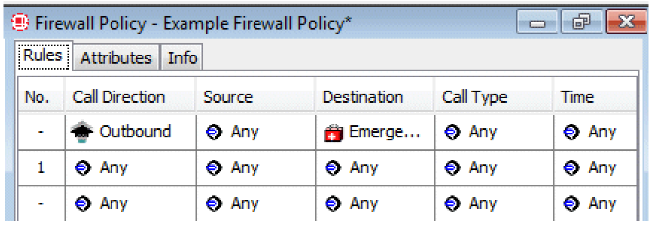
5. Click the **Save** icon, or click **File | Save**. The Policy appears in the **Firewall Policies** subtree.

6. Right-click in the blank area of the Policy and click **Add Rule | Bottom**.



No.	Call Direction	Source	Destination	Call Type	Time
-	Outbound	Any	Emerge...	Any	Any
-	Any	Any	Any	Any	Any

7. A new Rule is added to the Policy with all of the fields at their defaults, as shown below.



No.	Call Direction	Source	Destination	Call Type	Time
-	Outbound	Any	Emerge...	Any	Any
1	Any	Any	Any	Any	Any
-	Any	Any	Any	Any	Any

New blank Rule added. Rules are auto-numbered according to their order in the Policy and identified by this number in logs.

8. To add a value to a field, right-click in the field. A menu of options for that field appears. Select the applicable value. In any field in which you do not want to specify a value, leave the default of **Any**.

   Each Rule has the following fields that determine whether a call matches and what actions occur when one does.

   - **Call Direction**—The direction of the call: **Inbound**, **Outbound**, or **Any**.
   - **Source**—The originator of the call.
   - **Destination**—The destination of the call.
   - **Call Type**—The traffic type(s) to which the Rule applies. You can also *negate* the **Call Type** field so the Rule applies to all call types other than those specified in the field. To negate the field, add one

or more call types, and then right-click in the field and click **Negate**.

- **Time**—The time(s) and day(s) the Rule is in effect. You can also negate the **Time** field so the Rule applies at all times other than those specified in the field. To negate the field, add one or more times, and then right-click in the field and click **Negate**.
- **Call Duration**—The length of the call.
- **Attributes**—Midcall DTMF digit patterns or specific VoIP call attributes, which can include: unknown codec, media timeout, excessive media rate, or signaling anomaly.
- **Action**—Allow or terminate calls that match the Rule.
- **Track**—Notification and logging for calls that match the Rule.
- **Install On**—Which of the Span Groups assigned to the Policy are to enforce the Rule. **Any** means all of the assigned Span Groups are to enforce the Rule, or you can apply the Rule only to some assigned Span Groups and not others.
- **Comment**—Optional notes about the Rule. Very useful for identifying the purpose of the Rule for reference in logs and Reports.

IMPORTANT Rule order is important in Firewall Policies. See the *Voice Firewall User Guide* for a discussion of Policy processing and Rule order.

9. Repeat Steps 6, 7, and 8 for each Rule in the Policy. When you are done, click the **Save** icon.

10. Right-click the Policy in the **Firewall Policies** subtree, point to **Install**, and then click either **Priority Mode** or **Normal Mode**. The Policy is verified and installed on the assigned Span Groups.

    Note: Refer to “Limit to the Number of Phone Numbers in Policies” on page 28 for a discussion of Normal Mode versus Priority Mode.

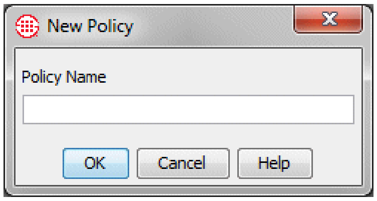
IPS Policy Quick Start

The instructions below provide a Quick Start for defining an IPS Policy. For detailed information and instructions, see the *Voice IPS User Guide*.

To define an IPS Policy

1. In the Performance Manager tree pane, right-click **IPS Policies** and click **New**.

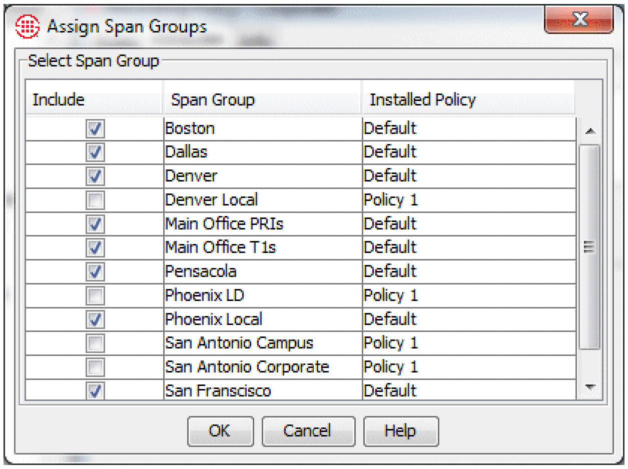
   The **New Policy** dialog box appears.



All Spans in the Span Groups assigned to a given IPS Policy must be in the same time zone, because Intervals are calculated based on the Span’s time zone.

2. In the **Policy Name** box, type the name by which you want to identify this Policy, and then click **OK**.

   The **Assign Span Groups** dialog box appears.



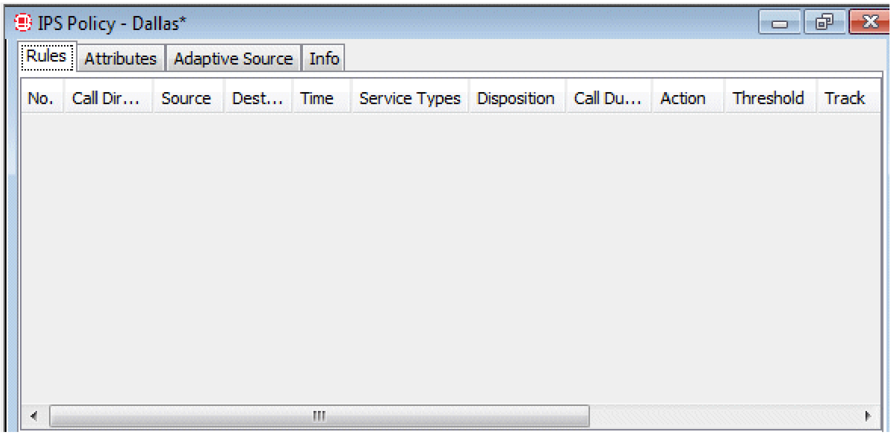
Include	Span Group	Installed Policy
☑	Boston	Default
☑	Dallas	Default
☑	Denver	Default
□	Denver Local	Policy 1
☑	Main Office PRIs	Default
☑	Main Office T1s	Default
☑	Pensacola	Default
□	Phoenix LD	Policy 1
☑	Phoenix Local	Default
□	San Antonio Campus	Policy 1
□	San Antonio Corporate	Policy 1
☑	San Franscisco	Default

3. In the **Include** column, select the check boxes for Span Groups on which you want to install the Policy; clear the check boxes for any Span Groups on which you do not want to install the Policy. By default, all Span Groups on which the default IPS Policy is currently installed are selected. (If no Span Groups are defined, no check boxes appear.)

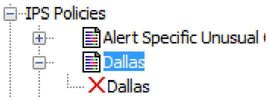
   - If one or more of the Span Groups on which you want to install this Policy are not yet defined, you can add them later using the **Attributes** tab of the **Policy Editor**.

4. Click **OK**.

   The Policy appears in the **Policy Editor**. The asterisk in the title bar indicates it has not yet been saved. New Policies do not appear in the tree pane until they are saved.

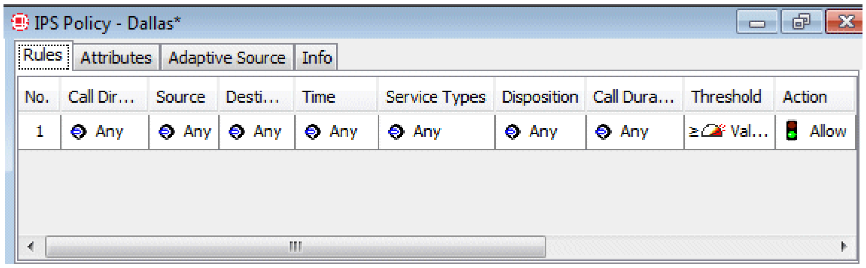


5. On the Performance Manager main menu, click **File | Save**. The new Policy appears in the **IPS Policies** node of the tree pane, and its assigned Span Groups appear under it. The red **X** next to the Span Group name(s) of the assigned Span Groups indicates the Policy is not installed. You'll install it after you define one or more Rules.



IPS Policies
- Alert Specific Unusual
- Dallas
  - ✗ Dallas

6. Add a Rule to the Policy. To add a Rule, right-click in the blank area and click **Add Rule | Bottom**.



IPS Policy - Dallas*

Rules | Attributes | Adaptive Source | Info

No.	Call Dir...	Source	Desti...	Time	Service Types	Disposition	Call Dura...	Threshold	Action
1	Any	Any	Any	Any	Any	Any	Any	≥ Val...	Allow

7. A new Rule is added to the Policy with all of the fields at their defaults. Define the fields as needed. The **Thresholds** field is undefined by default and must be defined before the Policy can be installed. For any field other than **Threshold** in which you do not want to specify a value, leave the default of **Any**.

   To add values to the fields:

   - **Call Direction**—Right-click in the field and click **Inbound** or **Outbound**.
   - **Source**—Right-click in the field and click **Add**, and then click the type of source you want to add: Listings, Filters, Groups, Ranges, Wildcards, Subnets, No Source, or Caller ID Restricted calls. You can add multiple sources of different types if needed.
     - If you click Filters, Groups, Ranges, Wildcards, or Subnets, a dialog box appears containing the selected type of Object. Click the items you want to add, and then click **OK**.
     - If you click **Caller ID Restricted** or **No Source**, it is added to the Rule.
     - If you click **Listings**, the **Listing Search** dialog box appears. Search for the Listing(s), and then select them in the **Results** window and click **Add**. See "Searching for a Directory Listing" on page 100 for instructions for using a simple or advanced search to locate Listings.
   - **Destination**—Right-click in the field and click **Add**, and then click the type of destination you want to add: Listings, Filters, Groups, Ranges, Wildcards, or Subnets.

- If you click Filters, Groups, Ranges, Wildcards, or Subnets, a dialog box appears containing the selected type of Object. Click the items you want to add, and then click **OK**.

- If you click **Listings**, the **Listing Search** dialog box appears. Search for the Listing(s), and then select them in the **Results** window and click **Add**. See "Searching for a Directory Listing" on page 100 for instructions for using a simple or advanced search to locate Listings.

- **Call Type**—Right-click in the field and click **Add**. The **Call Types** dialog box appears.
  - Click the call type(s) you want to add, and then click **OK**.
  - To negate the call type field so it applies to all types other than those listed, after adding one or more call types, right-click in the field and click **Negate**.

- **Time**—Right-click in the field and click **Add**. The **Times** dialog box appears.
  - Click the Time you want to add to the Rule, and then click **OK**. See "Times" on page 69 for instructions for defining Times and Time Groups.
  - To negate the Time so that the Rule applies at all Times other than the one specified, after adding a Time, right-click in the field and click **Negate**.

- **Service Types**—Right-click in the field and click **Add**. The **Service Types** dialog box appears.
  - Click one or more Service Types to add to the Rule, and then click **OK**. See "Service Types" on page 80 for instructions for defining Service Types.
  - To negate the Service Type so that the Rule applies to all Service Types other than those specified, after adding a Service Type, right-click in the field and click **Negate**.

- **Dispositions**—Right-click in the field and click **Add**. The **Dispositions** dialog box appears. Click one or more termination dispositions, and then click **OK**.

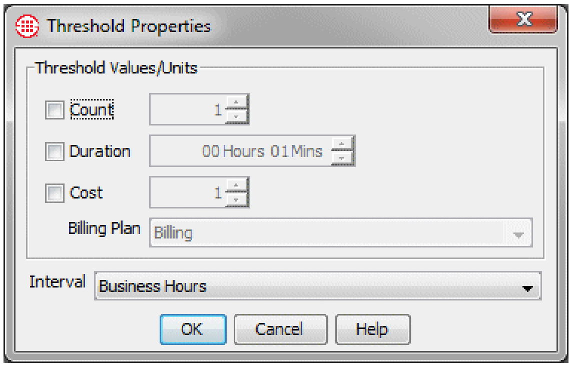
- **Call Duration**—Right-click in the field and click **Add**. The **Durations** dialog box appears. Click a Duration, and then click **OK**. In IPS Policies only, you can add a "less-than" **<** operator to the **Duration** field. The default is "greater than or equal to" **≥**. To apply "less than," right-click in the **Call Duration** field and click **<**. (*Does not apply to Firewall Policies; their* ***Duration*** *field always denotes "greater than or equal to"* **≥**.)

- **Attributes**—Midcall DTMF digit patterns or lack of midcall DTMF digits.

For instructions for defining Durations, see “Durations” on page 73.

- **Threshold**—You must define the **Threshold** field before the Policy can be installed.

  a. Right-click in the field and click **Edit**. The **Threshold Properties** dialog box appears.

  □ Count 1

  □ Duration 00 Hours 01 Mins

  □ Cost 1

  Billing Plan Billing

  Interval Business Hours

  b. In the **Threshold Values/Units** area, select one of the following:

  Count—To set a threshold based on the number of calls that match the Rule, select **Count**, and then type or select a number.

  Duration—To set a threshold based on the cumulative duration of calls that match the Rule, select **Duration**, and then type or select the duration in hours and minutes.

  Cost—To set a threshold for the cost of calls that match the Rule, select **Cost**, and then type the whole dollar limit and select the Billing Plan to use to calculate the cost. See "Billing Plans" on page 83 for instructions for defining Billing Plans.

  c. In the **Interval** box, click the down arrow and select the time Interval over which the accumulations are to be tracked. See "Intervals" on page 74 for instructions for defining Intervals.

  d. Click **OK** to save the changes and close the dialog box.

  e. By default, greater than or equal to **≥** is applied to the Threshold. To specify less than, right-click in the **Threshold** field and click **<**.

- **Comment**—Right-click in the **Comment** field and click **Edit Comment**.

  – The **Edit Comments** dialog box appears. Type optional notes about the Rule. Comments are very useful for identifying the purpose of the Rule for reference in logs and Reports.

8. Repeat steps 6 and 7 for each Rule in the Policy.

9. Click **File | Save**.

10. Right-click the Policy in the **Firewall Policies** subtree, point to **Install**, and then click either **Priority Mode** or **Normal Mode**. The Policy is verified and installed on the assigned Span Groups.

    Note: Refer to “Limit to the Number of Phone Numbers in Policies” on page 28 for a discussion of Normal Mode versus Priority Mode.

Objects

Objects Used in the ETM® System

The ETM System provides various types of *Objects* that are used in Policies, Filters, and Reports. An Object is a "container" that holds a set of information that you can then use as a single unit to perform a task. Examples include Contact Objects, which contain a person's email contact information, and Time Objects, which identify one or more time ranges. *Group Objects* can hold other Objects. For example, a Contact Group Object can hold multiple Contact Objects as a set, such as all telecom managers.

Some of these Objects are predefined and cannot be user-modified, such as Call Types and SNMP Tracks. Other Objects are user-defined with information specific to your organization. User-defined Objects include Contacts, Email Tracks, Times, and others.

Directory entities are discussed separately in "Directory Manager" beginning on page 95.

User-defined Objects "belong" to the Management Server you are logged in to when you define them. After they are defined, Objects are available for reuse throughout the ETM System applications. For example, a Time Object can be inserted into Voice Firewall Policy Rules to specify the time(s) when the Rule is to be enforced, and can also be used to define filters to tailor report content in the Usage Manager.

Some default user-definable Objects are included with the ETM System, such as the **Business Hours** Time. These Objects are used in some predefined Usage Manager Reports. You can modify these Objects to suit your business practices. **Caution** If you delete the default Objects used in predefined Reports, the Reports that use them will no longer be properly defined.

The sections below provide instructions for defining the Policy-related Objects defined in the Performance Manager. You must have the **Access Policy Features** user permission to create or modify these components.

Contacts

Contacts specify email information for people to be notified about various aspects of ETM System operation. Contacts are used in email notification Tracks. For example, you might want your system administrator to be notified when an ETM System security event occurs, such as three failed login attempts or a Telnet login. And you might want your telecom manager to be notified if a telecom-related system event occurs, such as if the D channel on a PRI trunk goes down.

To accomplish this, you define a Contact for each of these people and then use those Contacts to define Email Tracks for your system administrator and your telecom manager. You then use those Tracks in Policies and System Events as needed to generate notifications.

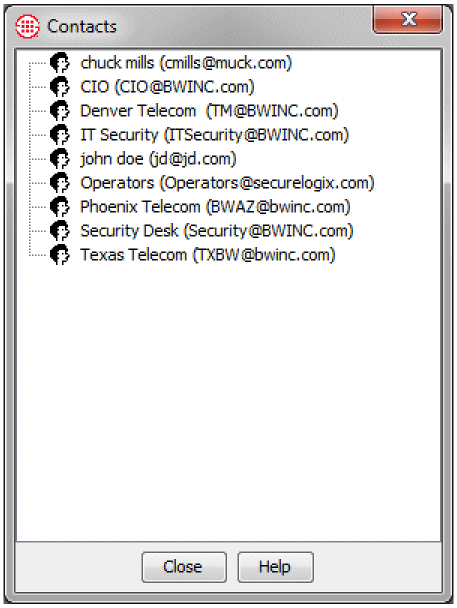
Each Contact specifies a single email address. Multiple Contacts can be grouped into a Contact Group to aid in Contact management.

You must have **Access Policy Features** permission to create or modify Contacts.

Defining a Contact

To define a Contact

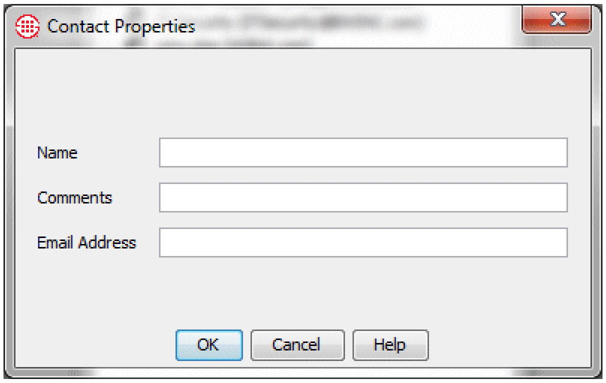
1. On the Performance Manager main menu, click **Manage | Contacts**. The **Contacts** dialog box appears.



chuck mills (cmills@muck.com)
CIO (CIO@BWINC.com)
Denver Telecom (TM@BWINC.com)
IT Security (ITSecurity@BWINC.com)
john doe (jd@jd.com)
Operators (Operators@securelogix.com)
Phoenix Telecom (BWAZ@bwinc.com)
Security Desk (Security@BWINC.com)
Texas Telecom (TXBW@bwinc.com)

2. Right-click in the dialog box and click **New | Contact**.

   The **Contact Properties** dialog box appears.



3. In the **Name** box, type a unique, descriptive name for the new Contact, up to 28 characters and spaces in length. For example, type: `Telco Manager`.

   Note that the name is case-sensitive. That is, "Sysadmin" and "sysadmin" are treated as two unique names.

4. Optionally, in the **Comments** box, type a comment up to 100 characters and spaces in length.
5. In the **Email Address** box, type the email address to which a notification is to be sent.
6. Click **OK**. The new Contact appears in the **Contacts** dialog box.

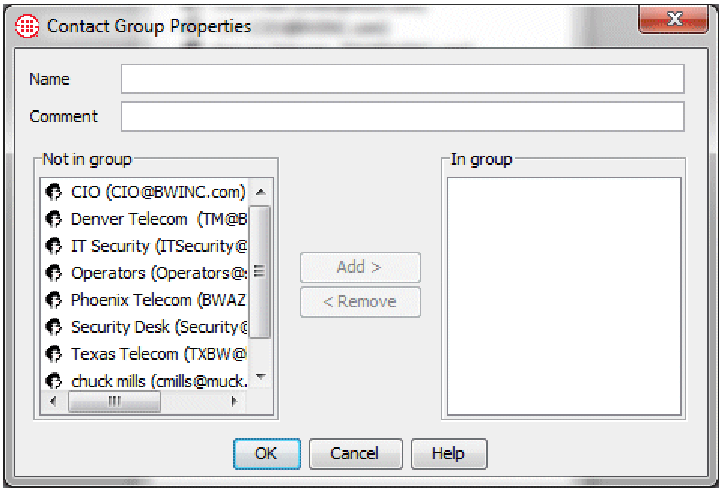
Grouping Contacts

Contact Groups aid in Contact management. Contact Groups work much like email alias groups—you group Contacts with similar interests or functions. This simplifies the task of adding like Contacts to a Track. A Contact Group can be used anywhere an individual Contact is used.

To group Contacts

1. On the Performance Manager main menu, click **Manage | Contacts**. The **Contacts** dialog box appears.
2. Right-click in the dialog box and click **New | Group**.

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



3. In the **Name** box, type a unique, descriptive name for the new Group, up to 28 characters and spaces in length. For example, type: `ETM System Administrators`

   As with most items in the ETM System, the name is case-sensitive.

4. Optionally, in the **Comment** box, type a comment up to 100 characters and spaces in length.

5. In the **Not in group** box, click the name of each Contact you want to add to the Group. To select multiple items, hold down CTRL or SHIFT while clicking.

6. Click **Add** to move the selected name(s) to the **In group** box.

7. Click **OK**. The new Group appears in the **Contacts** dialog box.

Tracks

You must have **Access Policy Features** permission to create or modify Tracks.

A **Track** defines one or more follow-up actions that can be executed in response to a specified event—for example, when a call matches a Voice Firewall Policy Rule or a T1 Span is in telco alarm. Email Tracks can also be used in the Usage Manager to send scheduled reports as attachments. The ETM System provides five types of Tracks. Email Tracks are user-defined. Log, SNMP, Syslog, and real-time alert Tracks are predefined and cannot be user-modified.

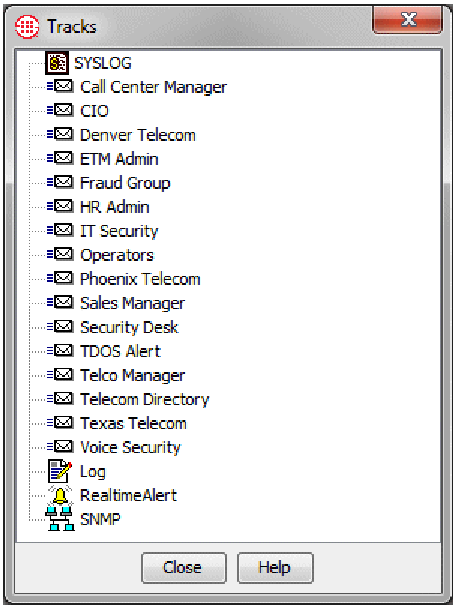
The subject and content of **Email** and **Real-Time Alert** Policy Track messages are defined by a file named **delivery.properties**, located in the ETM® System installation directory. See the *ETM® System Technical Reference* for instructions for modifying this information.

Defining an Email Track

If you need to change information for an email Track, right-click the Track, and then click **Edit**.

To define an Email Track

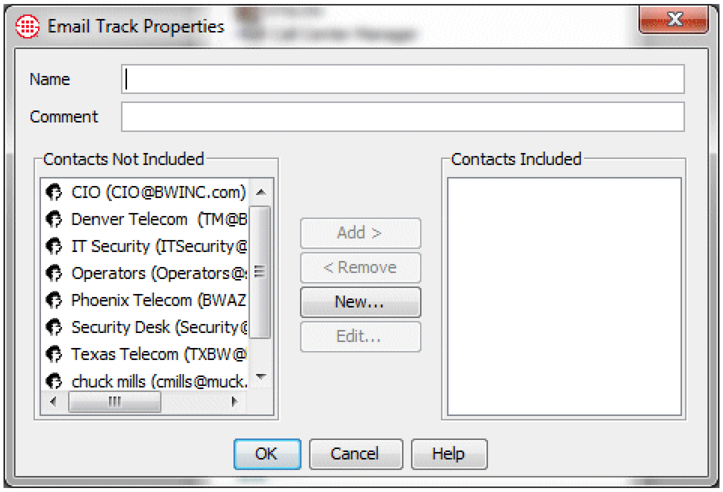
1. On the Performance Manager main menu, click **Manage | Tracks**. The **Tracks** dialog box appears.



SYSLOG
Call Center Manager
CIO
Denver Telecom
ETM Admin
Fraud Group
HR Admin
IT Security
Operators
Phoenix Telecom
Sales Manager
Security Desk
TDOS Alert
Telco Manager
Telecom Directory
Texas Telecom
Voice Security
Log
RealtimeAlert
SNMP

2. Right-click in the dialog box, and then click **New Email**. The **Email Track Properties** dialog box appears.

If you need to change information for a Contact, click the Contact in the **Email Track Properties** dialog box, and then click **Edit**.



3. In the **Name** box, type a unique identifier for this Email Track.
4. Optionally, in the **Comment** box, type a comment providing additional information about the Email Track.
5. In the **Contacts Not Included** box, click a Contact, and then click **Add**. All of the Contacts defined on this Server appear in this dialog box. If a Contact you want to add has not yet been defined, you can do that on the fly by clicking **New** in this dialog box. See "Defining a Contact" on page 66 for instructions, if necessary.
6. Click **OK**. The new Email Track appears in the **Tracks** dialog box.

To add multiple Contacts at once, hold down CTRL or SHIFT while clicking.

Before the ETM® System can send email, an email server and an email **Reply-to** address must be specified. See "Specifying an Email Server" in the *ETM® System Administration and Maintenance Guide*, if necessary.

Times

Times are used for the following purposes:

- In ETM® System Policies to specify call days/times at which Rules apply.
- In filters for logs and reports to limit the information to specific days/times.

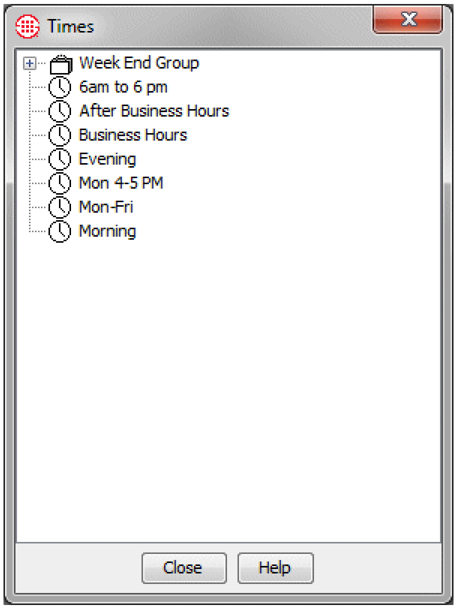
The default **Business Hours** Time defines business hours as 8:00 AM to noon and 1:00 PM to 5:00 PM Monday through Friday. You can edit this Time Object to apply to your business hours, if different, and the change will automatically apply to all report elements and Policies using this component.

Defining a Time

You must have **Access Policy Features** permission to create or modify Times.

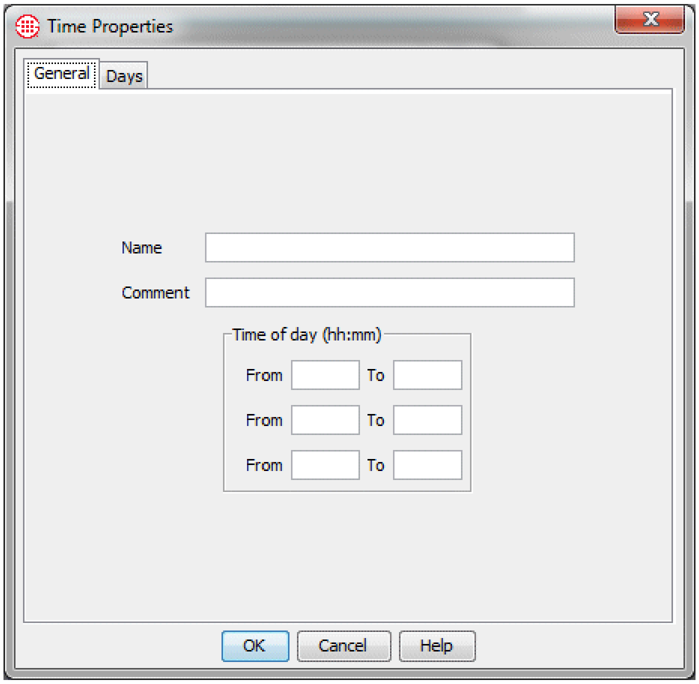
To define a Time

1. On the Performance Manager main menu, click **Manage | Times**. The **Times** dialog box appears.



Week End Group
6am to 6 pm
After Business Hours
Business Hours
Evening
Mon 4-5 PM
Mon-Fri
Morning

Right-click in the white area of the dialog box, and then click **New | Time**. The **Time Properties** dialog box appears.



2. Click the **General** tab.

3. In the **Name** box, type a descriptive identifier for the Time, up to 28 characters and spaces in length.

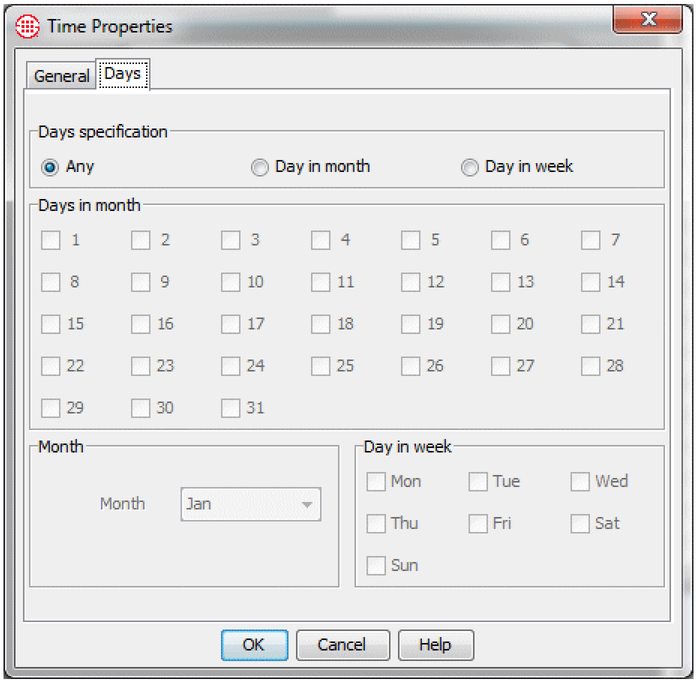
4. Optionally, in the **Comment** box, type a comment up to 100 characters and spaces in length.

5. In the upper-most **From** box in the **Time of day** area, type the start Time, in 24-hour format (*00:00-24:00)*, of the first period. In the adjacent **To** box, type the time this period ends.

   You can specify a maximum of three different start and stop periods. For example, the default **Business Hours** Time specifies 08:00 to 12:00 and 13:00 to 17:00, so that the lunch hour is not included. To create an **Off-Hours** Time, you might specify 17:00 to 24:00, 00:00 to 08:00, and 12:00 to 13:00.

6. Repeat Step 6 for additional periods if needed.

7. Click the **Days** tab.



Time Properties

General | Days

Days specification

● Any ○ Day in month ○ Day in week

Days in month

□ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7
□ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14
□ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21
□ 22 □ 23 □ 24 □ 25 □ 26 □ 27 □ 28
□ 29 □ 30 □ 31

Month

Month: Jan

Day in week

□ Mon □ Tue □ Wed
□ Thu □ Fri □ Sat
□ Sun

By default, the Time applies to all days. Do one of the following:

- If the Time is to apply on all days, click leave the default of **Any** selected and click **OK** to save the changes and close the dialog box.

- If the Times apply only on certain dates in a specific month, select **Day in month** in the **Days specification** area and then:

    a. In the **Month** area, select the appropriate month.

    b. In the **Days in month** area, select as many check boxes as needed to define the days of the month that the Times apply.

- If the Times apply only to specific day(s) of the week, select **Day in week** in the **Days specification** area and then select the check boxes for the day(s) to which it applies.

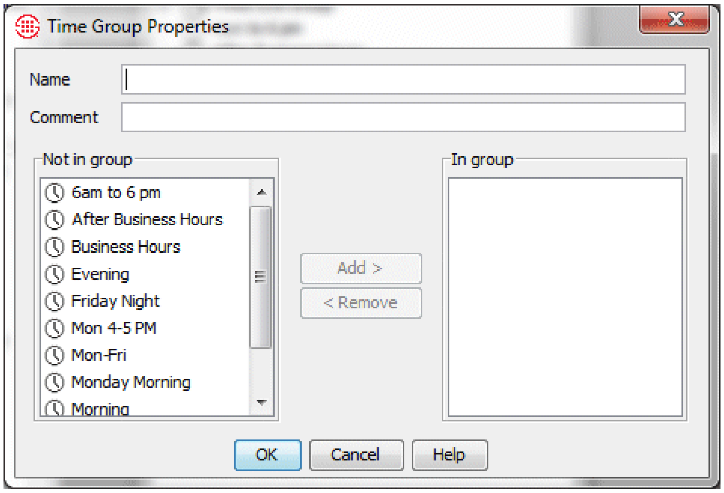
8. Click **OK**. The Time appears in the **Times** dialog box.

Defining a Time Group

To select multiple items, hold down CTRL or SHIFT while clicking.

To define a Time Group

1. On the Performance Manager main menu, click **Manage | Times**. The **Times** dialog box appears.
2. Right-click in the dialog box, and then click **New | Group**. The **Time Group Properties** dialog box appears.



3. In the **Name** box, type a descriptive name for the new Group, up to 28 characters and spaces in length.
4. Optionally, in the **Comment** box, type a comment of up to 100 characters and spaces.
5. In the **Not in group** box, double-click each Time you want to add to the Group. The selected Times move to the **In group** box.
6. Click **OK**. The new Time Group appears in the **Times** dialog box.

Durations

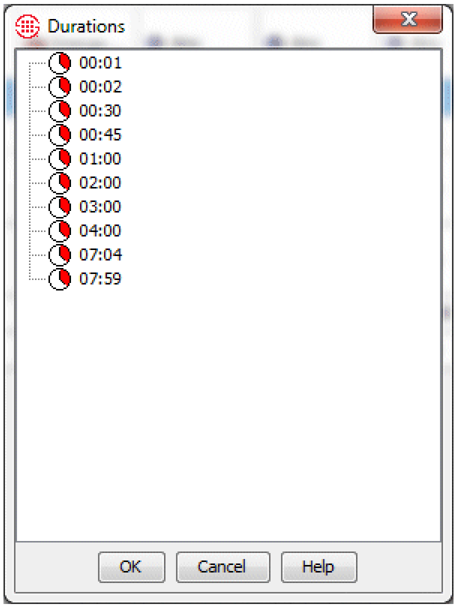
Durations are used in Firewall and IPS Policies to apply Rules based on the length of calls.

Defining a Duration

To define a duration

1. In an open Firewall or IPS Policy, right-click in the **Call Duration** field of the Rule to which you want to apply a Duration and click **Add**.

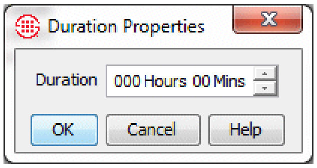
   The **Durations** dialog box appears.



Durations

00:01
00:02
00:30
00:45
01:00
02:00
03:00
04:00
07:04
07:59

2. Right-click in the white area of the dialog box and click **New Duration**. The **Duration Properties** dialog box appears.



Duration Properties

Duration: 000 Hours 00 Mins

3. Type or select the number of hours and/or minutes to represent a call length.
4. Click **OK**. The duration appears in the **Durations** dialog box. Once a duration is added to this dialog box, it is available for use in any Firewall or IPS Policy Rule.
5. Do one of the following:

   - To add the new duration to the Rule and close the **Durations** dialog box, click **OK**.

- To close the **Durations** dialog box without adding any durations to the Rule, click **Cancel**. The durations have already been created and remain in the dialog box; this simply cancels adding one to the Rule. This is useful if you want to define a number of durations at one time for later use in Policies.

Intervals

Intervals define a contiguous range of time. They are used in IPS Policies to define the period over which an IPS threshold is monitored. They are also used in Usage Manager Reports and in time-based filters. The maximum period an Interval can cover is one week. Two types of Intervals are available: Weekly or Daily. You can also partition each Weekly or Daily Interval into Subintervals by hour or by 15 minutes.

- **Week Interval**—A week Interval can be any subset of a week and cannot exceed one week in duration. The time range must be contiguous and the start and end time can be specified to the minute. For example:

  Calendar week: Starts Sunday at 00:00 and ends Saturday at 24:00.

  Workweek: Starts Monday at 00:00 and ends Friday at 24:00.

  Weekend: Starts Friday at 19:00 and ends Monday at 08:00.

  Long Saturday: Starts Friday at 19:00 and ends Saturday 24:00.

- **Day Interval**—The day Interval can be any subset of the days of the week and can be specified to the minute. The days selected do not have to be contiguous, but the time period each day must be contiguous and the same time period apply each day. For example:

  Workdays: 8:00 to 17:00 Monday through Friday.

  Workday Lunchtime: 11:45 to 1:15 Monday through Friday.

  Mon, Weds, and Fri mornings: 08:00 to 12:00 Monday, Wednesday, and Friday.

  Tues/Thurs afternoons: 12:00 to 17:00 Tuesday and Thursday.

- **Subintervals**— Daily and Weekly Intervals can be divided into Hourly or 15-Minute Subintervals:

  - **Hour Subinterval**—.An Hourly Subinterval subdivides the time period in each day of the Interval into 1-hour units of time. Each Hourly Subinterval must start at the top of an hour and last the full hour. For example:

    Weekend hours: Each one-hour period from Friday at 17:00 to Monday at 08:00. (Uses either a Day or Week Interval.)

    Workweek hours: Each one-hour period from 08:00 to 17:00, Monday through Friday. (Uses a Day Interval.)

    Nighttime hours: Each one-hour period from 17:00 to 08:00, Sunday through Saturday. (Uses a Day Interval.)

- **15-Minute Subinterval**—A 15-Minute Subinterval subdivides the time period in each day of the Interval into 15-minute units of time.

Predefined Intervals

A number of predefined Intervals are provided with your ETM® System. These Intervals are used in some predefined Reports and can be used in IPS Policies. You can modify the days and times in the predefined Intervals to suit your business needs. You can also define Intervals from scratch, as described in "Defining an Interval" below. The following predefined Intervals are included:

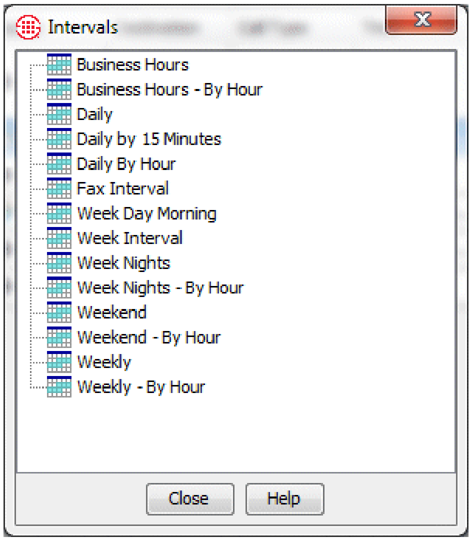
Business Hours	8:00 AM -5:00 PM Mon–Fri
Business Hours, By Hour	Business Hours with hourly subintervals
Daily	12 AM Sun - 12AM Sat-each day
Week Nights	5:00 PM - 8:00 AM M-Th
Week Nights, By Hour	Week Nights with hourly subintervals
Weekend	5:00 PM Friday - 8:00 AM Monday
Weekend, By Hour	Weekend with hourly subintervals
Weekly	12:00 AM Sunday - 12:00 AM Saturday
Weekly, By Hour	Weekly with hourly subintervals

Defining an Interval

To define an Interval

1. On the Performance Manager main menu, click **Manage | Intervals**.

   The **Intervals** dialog box appears.

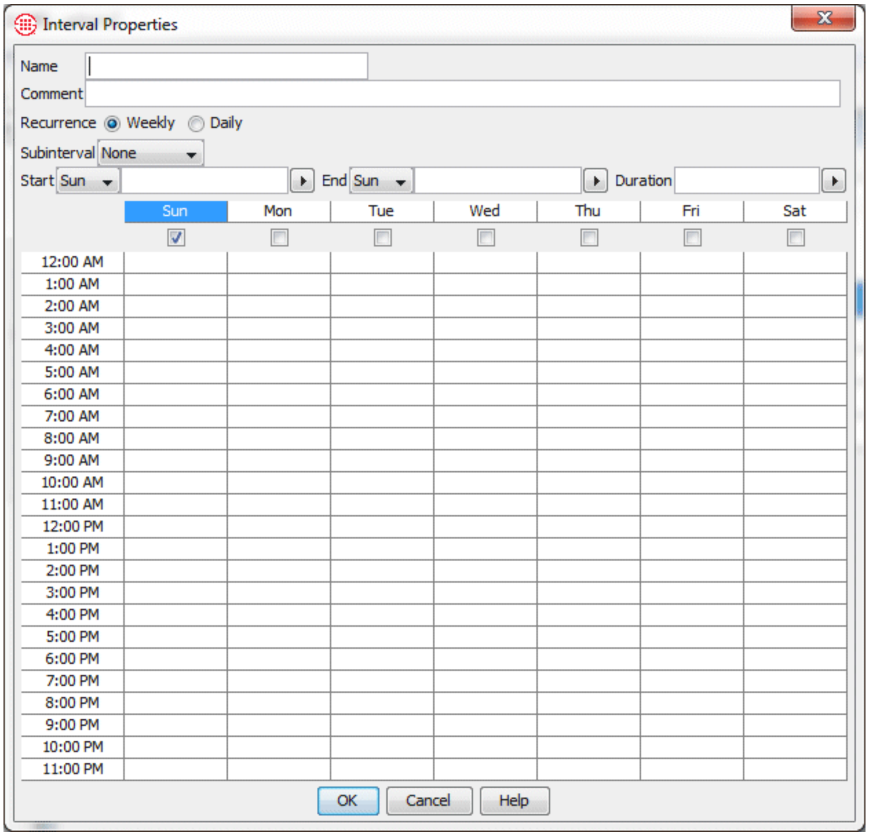


Intervals

- Business Hours
- Business Hours - By Hour
- Daily
- Daily by 15 Minutes
- Daily By Hour
- Fax Interval
- Week Day Morning
- Week Interval
- Week Nights
- Week Nights - By Hour
- Weekend
- Weekend - By Hour
- Weekly
- Weekly - By Hour

2. Right-click in the white area of the dialog box and click **New Interval**.

   The **Interval Properties** dialog box appears.



Interval Properties

Name

Comment

Recurrence ● Weekly ○ Daily

Subinterval None

Start Sun

End Sun

Duration

☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

3. In the **Name** box, type a unique identifier for this Interval.

4. Optionally, in the **Comment** box, type a comment to provide information about the Interval.

5. Do one of the following, according to the type of Interval you are defining:

   Week Interval

   a. In the **Recurrence** area, select **Weekly**.

   b. Select the duration of the Interval in one of the following ways::

      Use the Start and End fields: In the **Start** and **End** boxes, select the day of the week and the time of day on which the Interval is to start and end. The graphic area and the **Duration** box automatically update to match the selected days and times.

      Specify Start day/time and duration: In the **Start** box, select the day of the week and time of day at which the Interval is to start, and then type or select the duration in the **Duration** box. The graphic, **Start**, and **End** boxes automatically update to reflect the selection. Use this approach if you want a full week. For example, to specify Sunday at 12:00 AM to the following Sunday at Midnight, select Sunday 12:00 AM in the **Start** fields and select 168 in the **Duration** field.

Highlight the graphic: In the graphic area, click in the cell for the time and day at which the Interval is to start, and then hold down the left mouse button and drag your cursor to the cell representing the hour and day at which the Interval is to end. The **Start**, **End**, and **Duration** boxes update to reflect the selection. The check box for the day the Interval starts is selected. That is, if you click in the Thursday 2:00 PM cell and drag to Monday at 8:00 AM, the Interval begins on Thursday and ends Monday, so the Thursday check box is selected.

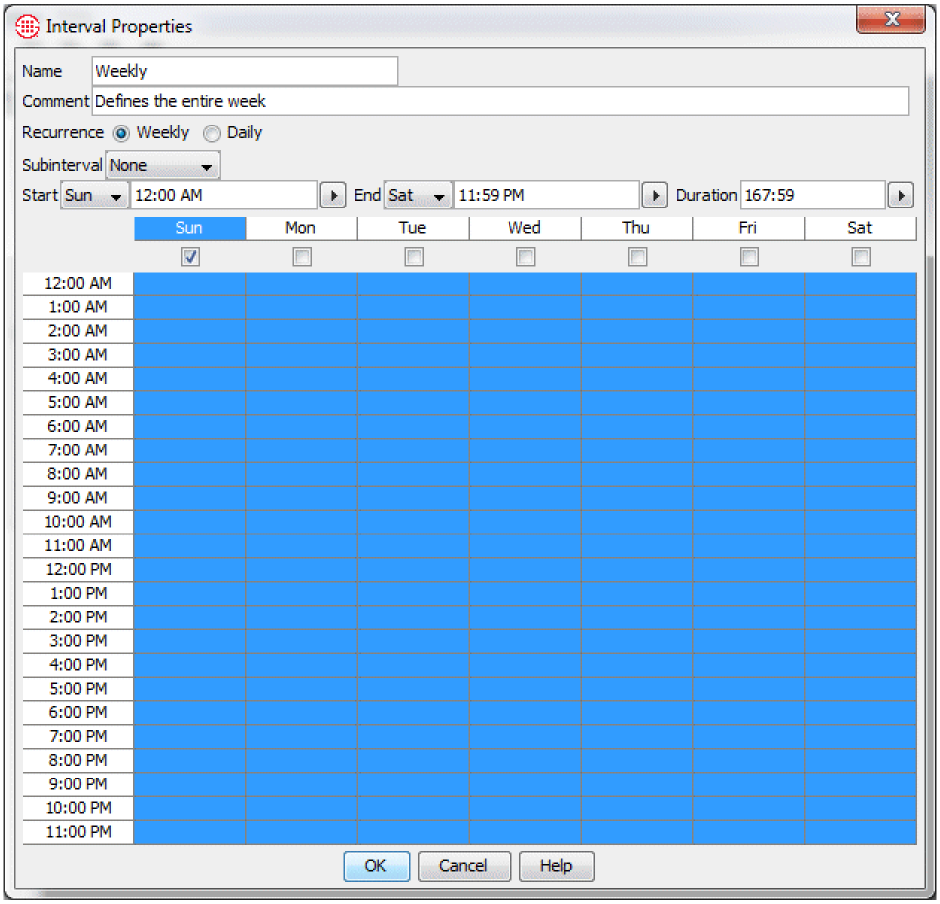
Tip: Check the **Start** and **End** fields to ensure that you have selected the correct time range. You can easily fine-tune the Interval by modifying the **Start** field; the **End** field will automatically update to retain the same span of time.

c. Optionally, specify a Subinterval.

- If you want Hourly Subintervals each day of the time period you selected, click the down-arrow next to **Subinterval** and select **Hourly.** Note that if you have specified the start or end time in minutes rather than the top of an hour, when you select **Hour subinterval**, the start and end times reset to the top of the displayed hour (that is, a start time of 1:45 becomes 1:00). This is because hourly subintervals represent one whole hour from the top of the hour.
- If you want 15-Minute Subintervals each day of the time period you selected, click the down-arrow next to **Subinterval** and select **15-minute**s.

d. Click **OK** to save the Interval. It is available for use in any IPS Policy or Usage Manager Report.

The following illustration shows a Weekly Interval that does not use subintervals—that is, accumulations are reported for the total hours in the Interval. This example is a *calendar week*, meaning it starts Sunday at 00:00 and ends Saturday at 24:00.



Name Weekly

Comment Defines the entire week

Recurrence ● Weekly ○ Daily

Subinterval None

Start Sun 12:00 AM End Sat 11:59 PM Duration 167:59

☑ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Day Interval

a. In the **Recurrence** area, select **Daily**.

b. Select the duration of the Interval in one of the following ways::

Use the Start and End fields: Select the checkbox for the first day the Interval is to apply. In the **Start** and **End** boxes, type or select the time of day on which the Interval is to start and end. The graphic area and the **Duration** box automatically update to match the selected days and times. Then select the checkboxes for the other days on which the Interval applies, if any. The time is automatically applied, since it must be the same on all days.

Specify the Start Day/Time and Duration Select the checkbox for the day of the week on which the Interval is to start, and then type or select the Start Time and the Duration. Then select the checkboxes for the other days on which the Interval applies, if any. The time is automatically applied, since must be the same on all days.

Tip: You can select a contiguous time over multiple days for a Daily Interval by SHIFT-clicking the days of the week headings.

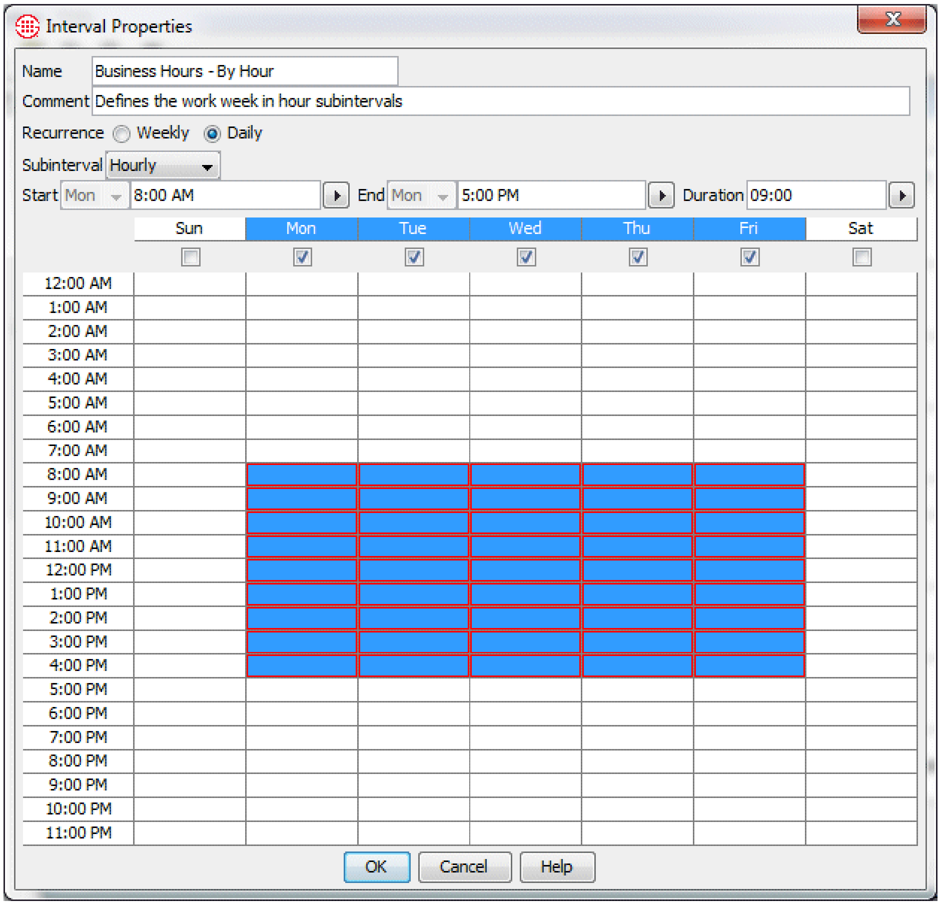
Highlight the graphic: In the graphic area, click in the cell for the time and day at which the Interval is to start, and then hold down the left mouse button and drag your cursor to the cell representing the hour at which the Interval is to end. Then select the checkboxes for the other days on which the Interval applies, if any. The time is automatically applied, since must be the same on all days. The **Start**, **End**, and **Duration** boxes update to reflect the selection.

e. Optionally, specify a Subinterval.

- If you want Hourly Subintervals each day of the time period you selected, click the down-arrow next to **Subinterval** and select **Hourly.** Note that if you have specified the start or end time in minutes rather than the top of an hour, when you select **Hour subinterval**, the start and end times reset to the top of the displayed hour (that is, a start time of 1:45 becomes 1:00). This is because Hourly Subintervals represent one whole hour from the top of the hour.
- If you want 15-Minute Subintervals each day of the time period you selected, click the down-arrow next to **Subinterval** and select **15-minute**s.

c. Click **OK** to save the Interval. It is available for use in any IPS Policy or Usage Manager Report.

The following illustration shows an Interval for Business Hours of 8 AM to 5 PM Monday through Friday using hourly subintervals.



Interval Properties

Name: Business Hours - By Hour

Comment: Defines the work week in hour subintervals

Recurrence ○ Weekly ● Daily

Subinterval: Hourly

Start: Mon 8:00 AM End: Mon 5:00 PM Duration: 09:00

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	□	☑	☑	☑	☑	☑	□
12:00 AM							
1:00 AM							
2:00 AM							
3:00 AM							
4:00 AM							
5:00 AM							
6:00 AM							
7:00 AM							
8:00 AM		🟦	🟦	🟦	🟦	🟦	
9:00 AM		🟦	🟦	🟦	🟦	🟦	
10:00 AM		🟦	🟦	🟦	🟦	🟦	
11:00 AM		🟦	🟦	🟦	🟦	🟦	
12:00 PM		🟦	🟦	🟦	🟦	🟦	
1:00 PM		🟦	🟦	🟦	🟦	🟦	
2:00 PM		🟦	🟦	🟦	🟦	🟦	
3:00 PM		🟦	🟦	🟦	🟦	🟦	
4:00 PM		🟦	🟦	🟦	🟦	🟦	
5:00 PM							
6:00 PM							
7:00 PM							
8:00 PM							
9:00 PM							
10:00 PM							
11:00 PM							

Service Types

Service Types are used to map each Call Label defined in the Spans' Dialing Plans to a class of service such as International, Toll-Free, local, etc. They are used to define Voice IPS Policy Rules that apply to a given service type.

They can also be used for cost accounting. To use them in cost accounting, after you have defined the necessary Service Types, you define one or more *Billing Plans* to associate each Service Type with a cost. These Billing Plans can then be used to run billing reports and to define IPS Policies based on cost. Each label can be used in only a single Service Type, but a Service Type can be used in more than one Billing Plan.

Default Service Types

Default Service Types are defined for several default Call Labels. You can modify these if the Call Labels in your Dialing Plans differ and create your own Service Types as needed.

The table below lists the predefined Service Types.

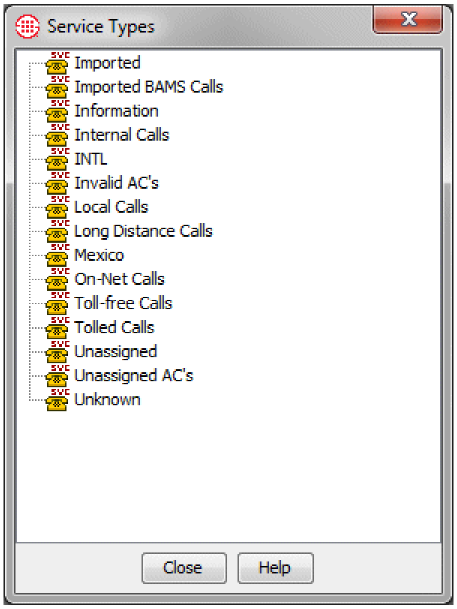
Service Type	**Dialing Plan Call Label**	**Denotes**
Toll-free Calls	FREE	Toll-free calls
Tolled Calls	TOLL	NANP toll calls to numbers in the following area codes: `500, 533, 600, 700, 880..882, 900, 976`
International Calls	INTL	International calls
Long Distance Calls	LD	Long-distance calls
Local Calls	LOC	Local calls
Unknown	UNK	Calls for which the relationship between called and calling number cannot be determined. Occurs when the source for an inbound call or the destination for an outbound call is unavailable.

You may need to adjust your Dialing Plan to ensure that the Call Labels for which you want to define Service Types occur in the Dialing Plan. The Call Labels in use in the Dialing Plans on your Spans can be viewed in the **Call Details** field of logs and reports, or in the Dialing Plan files.

Defining a Service Type

To define a Service Type

1. On the Performance Manager main menu, click **Manage | Service Types**. The **Service Types** dialog box appears.

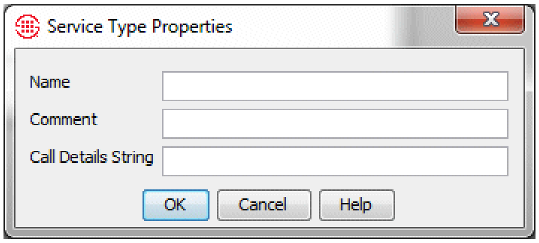


Service Types

Imported
Imported BAMS Calls
Information
Internal Calls
INTL
Invalid AC's
Local Calls
Long Distance Calls
Mexico
On-Net Calls
Toll-free Calls
Tolled Calls
Unassigned
Unassigned AC's
Unknown

2. Right-click in the white area of the dialog box and click **New | Service Type**.

   The **Service Type Properties** dialog box appears.

3. In the **Name** box, type a unique name to identify this Service Type. This name appears in logs, reports, Policies, and the **Service Types** dialog box.

4. In the **Comment** box, optionally type a comment. A comment can consist of up to 255 alphanumeric characters.

5. In the **Call Details String** box, type a string that matches a Call Label exactly as it appears in the **Call Details** field of the Call Log when a call is processed. The string is case-sensitive and can contain up to 20 alphanumeric and special characters except the pipe **|** symbol and single/double quotes.

   - The string in each Service Type Object must be unique, must match the Dialing Plan entry exactly, and is case-sensitive. That is, you cannot define two Service Types for the string **INTL**, and the strings **INTL** and **intl** are treated as unique. If you need different Service Types for different locales, you must first define custom, case-sensitive labels in your Dialing Plans and then define Service Types for each.

   - Some Dialing Plan sections produce an entry such as the following: **LD,CONUS**. A separate Service Type for each of these results is needed if you want to associate a cost with them. The string **LD** will not match a value of **LD,CONUS** in the **Call Details** field, nor will the string **LD,CONUS** match a value of **LD** in the **Call Details** field.

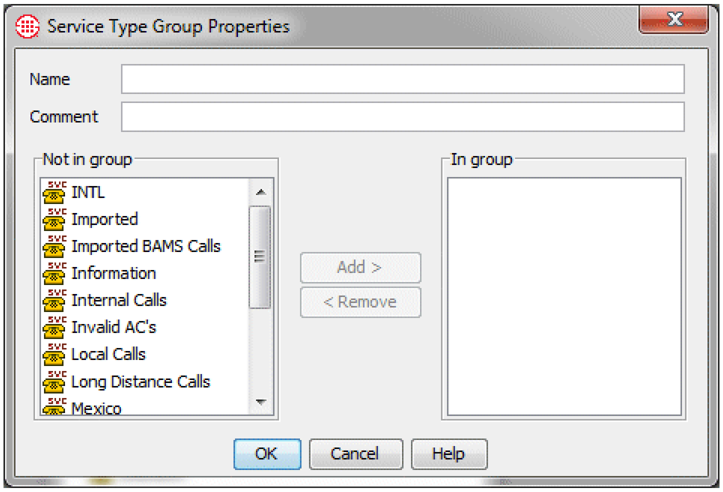
Creating a Service Type Group

Service Type Groups are used to organize Service Types and can be used to apply multiple Service Types to an IPS Rule. Note that only individual Service Types can be used in Billing Plans; Service Type Groups cannot be used in Billing Plan Rules.

To create a Service Type Group

1. Right-click in the Service Types dialog box and click **New | Group**.

2. The **Service Type Group Properties** dialog box appears.



3. In the **Name** box, type an identifier for the Group. Note that the Name is case-sensitive: **Toll-free calls** and **Toll-free Calls** would be created as two distinct Objects.

4. Optionally, in the **Comment** box, type a comment.

5. In the **Not in Group** box, click a Service Type you want to include in the **Group**, and then click **Add**. The Service Type moves to the **In Group** box.

6. Repeat until you have added all the Service Types you want in the Group, and then click **OK**.

Billing Plans

A *Billing Plan* associates Service Types with costs for call accounting. A Billing Plan consists of a set of *Billing Rules*; each Billing Rule associates a specific Service Type with a cost. Within a Billing Plan, each defined Service Type can be associated with a single cost. However, you can create multiple Billing Plans, and a given Service Type can be assigned different rates in different Billing Plans. For example, one rate for LD calls might apply on one set of Spans, while another might apply on a different set of Spans. You can define separate Billing Plans to use when dealing with data from each of these Spans.

You cannot use a Service Type Group in a Billing Rule.

A Billing Rule specifies either a cost per minute or a fixed cost per call that applies to the selected Service Type. If cost per minute is used, rounding criteria and duration method—whether the cost begins to accrue when the call goes off-hook or when it is answered—are also specified. You can define a variety of Billing Plans and Rules to suit your internal call accounting requirements. The **Default Billing Plan** contains predefined Rules for each of the default Service Types in the NANP Dialing Plan, but they do not contain a cost until you edit them to suit your environment.

Important Considerations for Billing Plans

Several important points must be considered when defining and using Billing Plans:

- Only one billing rate can be specified per Service Type and each Service Type must contain a unique string. For example, by default, **INTL** denotes an international call. However, not all international calls have the same billing rate. If you want to create a Billing Plan that addresses multiple international rates, you need to add custom, locale-specific Call Labels to your Dialing Plan and then define Service Types based on them. See the *ETM® System Administration Guide* for instructions for editing and installing Dialing Plans.
- When you define a Billing Rule for a given Service Type, the rate you assign applies at all times of day.
- If the Call Labels in the Dialing Plan are modified, be sure to update your Service Types to reflect the changes, or Billing Plans based on the outdated Call Labels will be invalid.
- Billing plans can be valuable for tracking costs and comparing actual call traffic with the charges assessed by your provider. However, inputs that vary from the actual Billing Plan your provider uses produce results that do not reflect actual charges. Therefore, no guarantee that results are accurate is expressed or implied.

Defining a Billing Plan

Before you begin defining a Billing Plan, be sure you have defined the Service Types to be used in it. Service Types are predefined for the default Call Labels in the default NANP Dialing Plan.

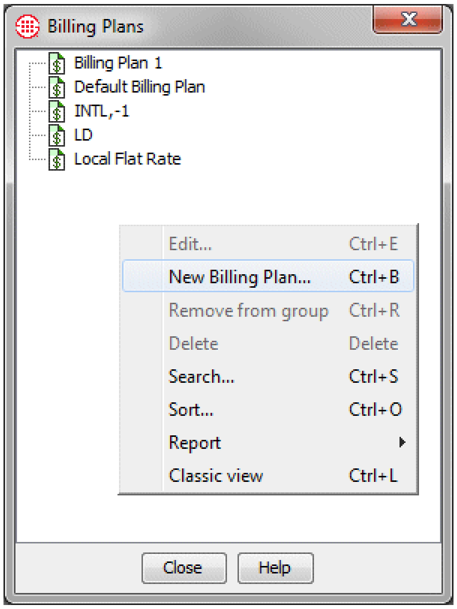
You cannot define Service Types from within the **Billing Plans** dialog box. For instructions for defining Service Types, see "Defining a Service Type" on page 81.

Billing Plans cannot be put into groups, because they can only be used singly.

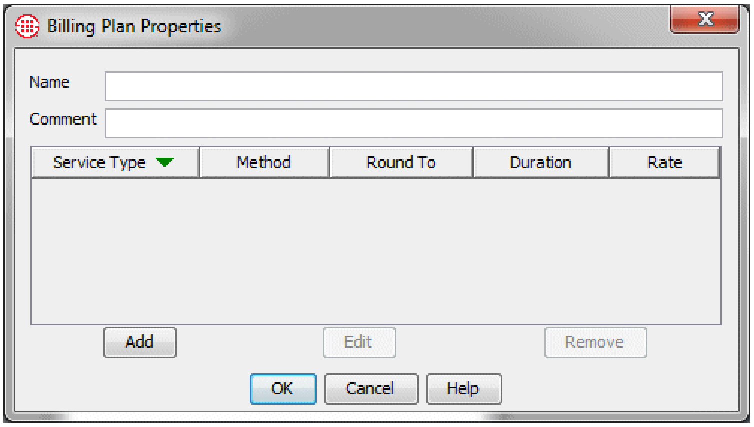
To define a Billing Plan

1. On the Performance Manager main menu, click **Manage | Billing Plans**.

   The **Billing Plans** dialog box appears.



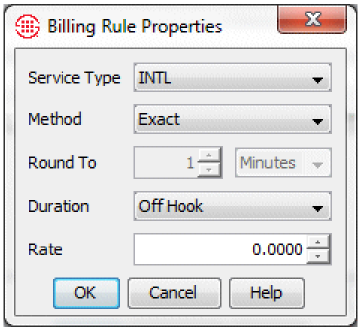
2. Right-click in the white area of the dialog box and click **New Billing Plan**. The **Billing Plan Properties** dialog box appears.



3. In the **Name** box, type a unique identifier for the Billing Plan. Note that the **Name** field is case-sensitive: **Home office** and **Home Office** would be created as two distinct Objects.

4. Optionally, in the **Comment** box, type a comment. A comment can consist of up to 255 alphanumeric characters.

5. Click **Add**. The **Billing Rule Properties** dialog box appears.


Billing Rule Properties

Service Type: INTL

Method: Exact

Round To: 1 Minutes

Duration: Off Hook

Rate: 0.0000

6. In the **Service Type** box, click the down arrow and select the Service Type for the Billing Rule. All of the defined Service Types appear in the drop-down list. For instructions for defining Service Types, see "Defining a Service Type" on page 81.

7. In the **Method** box, choose a method for rounding the cost: **Fixed** means the rate represents the cost per call. **Exact** means no rounding occurs; **Round** results in classic rounding; **Round Up** means the cost is always rounded up to the nearest unit selected in the **Round To** box; **Round Down** means the cost is always rounded down to the nearest unit.

8. (*Not applicable if you selected **Exact** or **Fixed**, since no rounding occurs*) In the **Round To** boxes, specify the rounding unit:

   a. In the first box, type or select a number from 1 to 32767.

   b. In the second box, select the unit to which the cost is to be rounded: **Minutes** or **Seconds**.

   For example, if you want the cost rounded to the nearest 5 seconds, you would select **5** in the first box and **Seconds** in the second box.

9. (*Does not apply if you selected **Fixed***) In the **Duration** box, click the down arrow and select how duration is to be calculated for assigning cost to this Service Type: **Off Hook** means that cost accrues from the time the phone goes off hook; **Answered** means that cost accrues from the time the call is answered.

10. In the **Rate** box, type or select the billing rate for this Service Type. If you selected **Fixed**, this rate applies per call. If you selected any other method, this rate applies per minute.

11. Click **OK**. The Billing Rule appears in the **Billing Plan Properties** dialog box.

12. Repeat steps 5–11 for additional Service Types as needed.

13. When you have added all of the applicable Service Types to the Billing Plan, click **OK**. The Billing Plan appears in the **Billing Plans** dialog box.

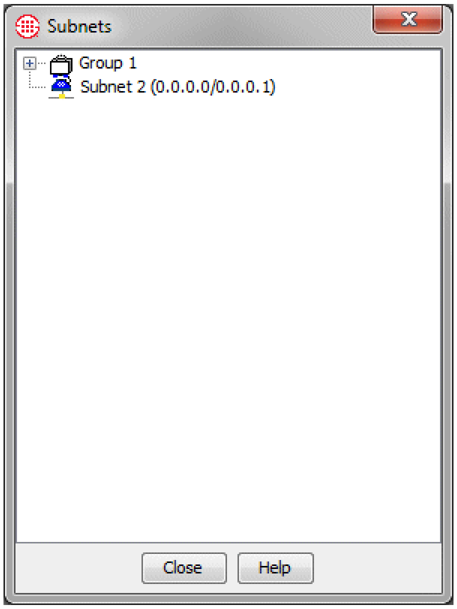
Subnets

A **Subnet**, which consists of an IP address and netmask or prefix length, is used as a "Wildcard" to match multiple IP addresses. For example, the IPv4 subnet (10.1.1.0 / 255.255.255.0) matches any of the internal IP addresses in the 10.1.1.x network. You can use subnets in IPS and Firewall Policies to apply the Rules to all calls in a given subnet.

Defining a Subnet

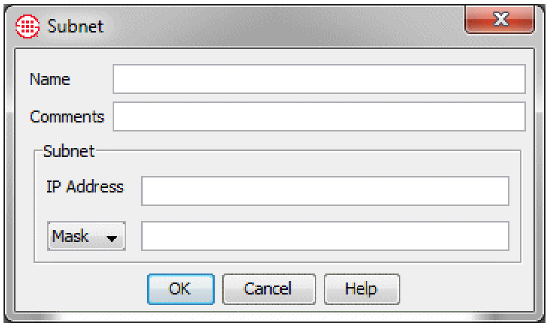
To define a Subnet

1. On the Performance Manager main menu, click **Manage | Subnets**. The **Subnets** dialog box appears.



2. Right-click in the dialog box and click **New.**

   The **Subnet** dialog box appears.



3. In the **Name** box, type a unique identifier.
4. Optionally, in the **Comments** box, type a comment.
5. In the **IP address** box, type the IP address (IPv4 or IPv6)..

6. In the drop-down box, select **Mask** (IPv4 only) or **Prefix**.

   - If you select **Mask**, type the subnet mask.
   - If you select **Prefix**, type the prefix length.

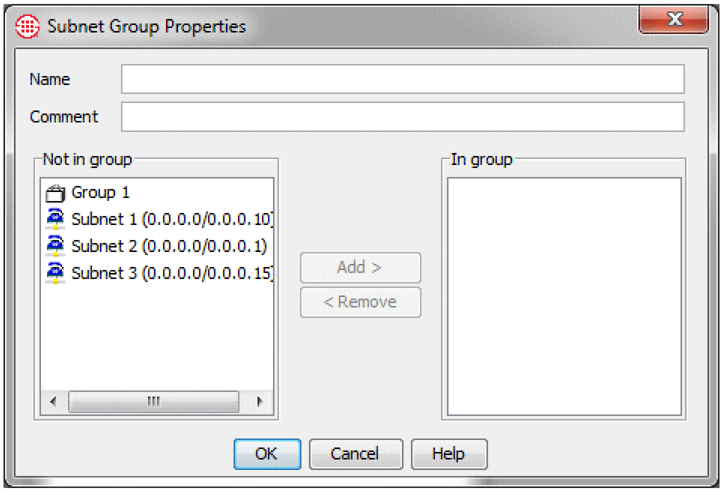
7. Click **OK** to save the changes. The new **Subnet** appears in the **Subnets** dialog box.

Grouping Subnets

To group Subnets

1. On the Performance Manager main menu, click **Manage | Subnets**. The **Subnets** dialog box appears.

2. Right-click in the dialog box and click **New | Group**. The **Subnet Group Properties** dialog box appears.



3. In the **Name** box, type a name for the Group.

4. Optionally, in the **Comment** box, type a comment.

5. In the **Not in Group** box, double-click each Subnet you want to add to the Group. The selected **Subnets** move to the **In group** box.

   - To remove a Subnet from the Group, double-click it in the **In group** box.

6. Click **OK**.

Attributes

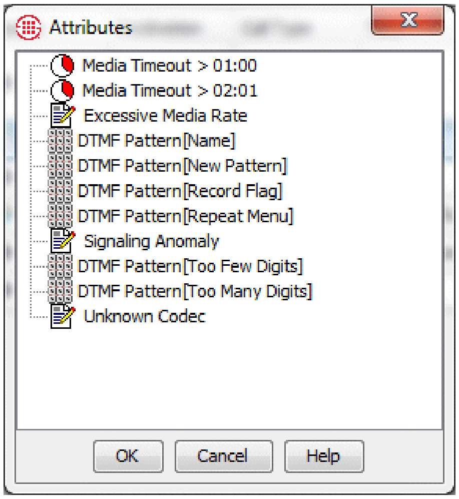
Attributes can be used to apply Firewall and IPS Policy Rules to specific patterns of midcall DTMF digits. They can also be used in Firewall Policies to apply a Rule to detect VoIP call attributes such as an unknown codec or signaling anomaly, or to specify a Media Timeout. Media Timeouts and DTMF digit patterns are user-defined.

Defining DTMF Digit Patterns

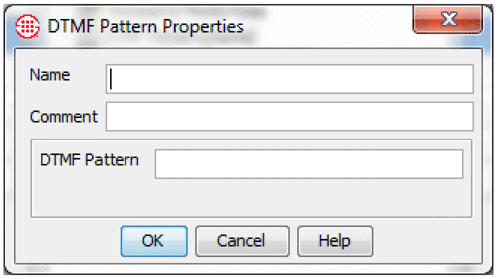
You can use DTMF patterns in Policy Rules without storing midcall DTMF digits in the Database. A separate per-Span configuration setting governs whether they are to be stored.

To define a new pattern:

1. Right-click in the **Attributes** field of a Firewall or IPS Policy Rule and click **Add**. The **Attributes** dialog box appears.


Attributes
Media Timeout > 01:00
Media Timeout > 02:01
Excessive Media Rate
DTMF Pattern[Name]
DTMF Pattern[New Pattern]
DTMF Pattern[Record Flag]
DTMF Pattern[Repeat Menu]
Signaling Anomaly
DTMF Pattern[Too Few Digits]
DTMF Pattern[Too Many Digits]
Unknown Codec
OK
Cancel
Help

2. Right-click in the **Attributes** dialog box and click **New | DTMF Pattern**. The **DTMF Pattern Attributes** dialog box appears.



3. In the **Name** box, type the name for the pattern to identify its purpose in the GUI.

4. In the **Comment** box, type a descriptive comment for the pattern.

5. In the **DTMF Pattern** box, type the pattern to be detected. For example, you might type: `1 8 3 1 8 3`. Regular expressions are supported.

6. Click **OK.** The pattern appears in the dialog box and is selected..

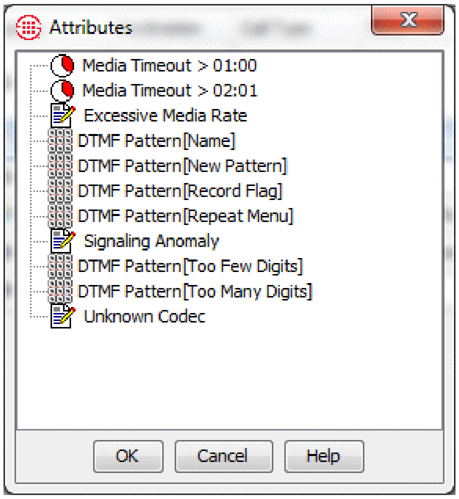
Defining Media Timeouts for VoIP Spans

A VoIP Media Timeout is the amount of time with no media passing through the Span, after which a call is considered to have timed out. The value must be greater than 10 seconds. You can define Firewall Policy Rules to prescribe actions based on Media Timeout values.

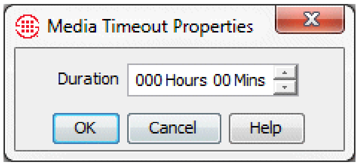
To define a Media Timeout

See the *ETM® System Voice Firewall User Guide* for a description of the other VoIP call attribute values in the **Attributes** dialog box.

1. Right-click in the **Attributes** field of a Firewall Policy Rule and click **Add**. The **Attributes** dialog box appears.


Attributes
Media Timeout > 01:00
Media Timeout > 02:01
Excessive Media Rate
DTMF Pattern[Name]
DTMF Pattern[New Pattern]
DTMF Pattern[Record Flag]
DTMF Pattern[Repeat Menu]
Signaling Anomaly
DTMF Pattern[Too Few Digits]
DTMF Pattern[Too Many Digits]
Unknown Codec
OK
Cancel
Help

2. Right-click in the blank area of the dialog box and click **New Media Timeout**. The **Media Timeout Properties** dialog box appears.



Duration 000 Hours 00 Mins

3. In the **Duration** box, type or select the length of time a call can have no media before it times out. The maximum value is 999 hours, 59 minutes.

4. Click **OK**. The Media Timeout appears in the **Attributes** dialog box.

5. Click **OK**. The newly created Media Timeout is added to the Policy Rule.

Span Groups

Span Groups organize Spans into logical units according to circuit type and Policy needs. Span Groups aid in Span management, much as trunk groups are used for trunk management.

You must have **Access Policy Features** permission to create or modify Span Groups.

Before you can install Policies on Spans, you must place the Spans into one or more Span Groups. Policies are installed on Span Groups rather than on individual Spans. However, a Span Group may contain only a single Span if appropriate. Only one Policy of each type can be installed on a Span Group.

When you move a Span into an existing Span Group on which user-defined Policies are already installed, the Span automatically receives and begins enforcing those Policies as follows:

- The system checks to see whether all installed Policies will fit on the Span. If all policies do not fit, the move fails and a message appears onscreen.
- If all Policies do fit on the Span, a message dialog presents an alert that this operation may result in one or more Policies being uninstalled prior to installing the new Policy, that is; this operation will result in a Priority Mode installation. You have the option to proceed with the move, or cancel the move. If you choose to proceed with the move, Policy installation occurs automatically, and any current Policy may be uninstalled prior to installation of the new Policy.

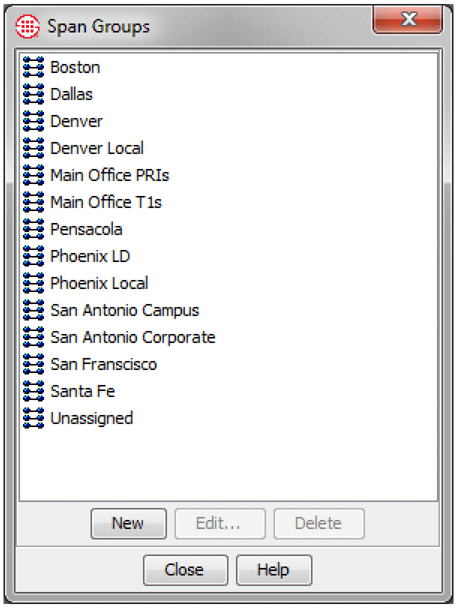
See “Limit to the Number of Phone Numbers in Policies” on page 28 for more information.

IMPORTANT All Spans enforcing the same IPS Policy must be in the same time zone, since IPS Policies apply to time Intervals.

Creating a Span Group

To create a Span Group

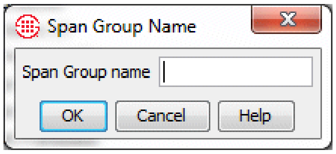
1. In the Performance Manager tree pane, right-click **Span Groups**, and then click **Manage Span Groups**. The **Span Groups** dialog box appears.



- Boston
- Dallas
- Denver
- Denver Local
- Main Office PRIs
- Main Office T1s
- Pensacola
- Phoenix LD
- Phoenix Local
- San Antonio Campus
- San Antonio Corporate
- San Franscisco
- Santa Fe
- Unassigned

The **Unassigned** Span Group contains all Spans that have not yet been specifically assigned to a group. You cannot install Policies on the **Unassigned** Span Group. The default Policies are installed on these Spans.

2. Click **New**. The **Span Group Name** dialog box appears.



3. Type a unique name for the Span Group. For example, you might create a Span Group for all of the PRI Spans at your Houston campus and name it **PRI Spans-Houston**. The name can consist of up to 50 characters and can include any special characters, spaces, digits, and letters.

4. Click **OK**. The Span Group appears in the **Span Groups** dialog box and in the **Span Groups** subtree of the Performance Manager tree pane. The Span Group is empty until you move one or more Spans to it.

Moving a Span to a Span Group

Span Groups appear in the **Span Groups** subtree of the Performance Manager tree pane. Spans that have not yet been assigned to a Span Group appear under the **Unassigned** node. Spans that belong to a Span Group appear beneath that Group.

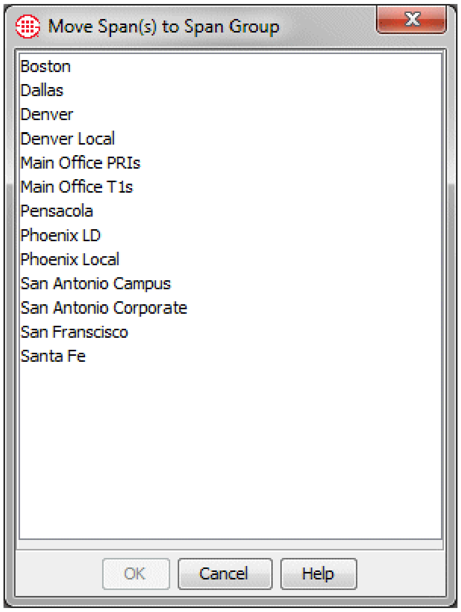
When you move a Span to a Span Group, it automatically receives any user-defined Policies installed on the Span Group. See "Span Groups" on page 91 for more information.

To move one or more Spans to a Span Group

1. In the **Span Groups** subtree of the Performance Manager tree pane, do one of the following to select the Span(s) to move:
   - Right-click a Span, and then click **Move Span(s)**.
   - Hold down CTRL or SHIFT while selecting multiple Spans you want to move to the same Span Group, and then right-click the selection and click **Move Span(s)**

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

IMPORTANT All Spans in a Span Group assigned to an IPS Policy must be in the same time zone. An error message appears if you try to move Spans in a different time zone to a Span Group with an installed IPS Policy, and the Spans are not moved.



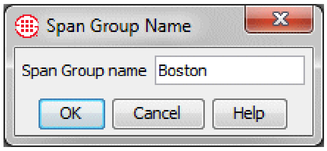
Boston
Dallas
Denver
Denver Local
Main Office PRIs
Main Office T1s
Pensacola
Phoenix LD
Phoenix Local
San Antonio Campus
San Antonio Corporate
San Franscisco
Santa Fe

2. Click the Span Group to which you want to move the Span(s), and then click **OK**.

Renaming a Span Group

To rename a Span Group

1. In the **Span Groups** subtree of the Performance Manager tree pane, right-click the Span Group and click **Edit Span Group Name**. The **Span Group Name** dialog box appears.



Span Group name Boston

!

2. In the **Span Group name** box, type the new name, and then click **OK**. The name can consist of up to 50 characters and can include any special characters, spaces, digits, and letters.

Deleting a Span Group

You cannot delete a Span Group that contains Spans. You must first move the Spans to a different Span Group. You can move them to the **Unassigned** Group or a user-defined Group.

To delete a Span Group

1. Do one of the following:

    - On the Performance Manager main menu, click **Manage | Span Groups**.

    - In the Performance Manager tree pane, right-click the **Span Groups** subtree and click **Manage Span Groups**.

    The **Span Groups** dialog box appears.

2. Click the Span Group you want to delete and click **Delete**. If delete does not become available when you click the Span Group, the Span Group still contains Spans. Note that you cannot delete the **Unassigned** Span Group.

Directory Manager

Understanding the Directory Manager

The Directory Manager is used to import and manage phone numbers in the ETM® System.

The Directory contains the following types of entries, collectively referred to as *Directory entities*:

- **Listings**, consisting of a single telephone number and its identifying information.
- **Filters**, which define a set of criteria for including Listings. Any Listings in the Directory that match the criteria are dynamically included anywhere the filter is used.
- **Ranges**, consisting of a consecutive series of phone numbers.
- **Groups**, consisting of any combination of Listings, Ranges, Wildcards, Filters, and/or other Groups.
- **Wildcards**. Two different types of Wildcards are available:
  - **Phone Number Wildcards,** which enable you to define Rules or filters to match selected portions of a phone number (country code, country and area code, Wildcards in the local number) rather than all digits.
  - **URI Wildcards**, which represent any portion of a URI.
- **Import Sets**, which contain a set of Listings imported from a text file or from an LDAP server.
- **Access Code Sets,** which correlate dialing Access Codes obtained from SMDR with Directory Listings.

Directory Listings

See "Import Sets" on page 155 for detailed information about creating, managing, and importing Listings into Import Sets.

A Directory Listing represents a single network user and the individual phone number, URI(s), and identifying information associated with that person or device. You can manually create Directory Listings, or you can import them from a text file or LDAP source into an *Import Set*. The Directory Manager can accommodate up to 1,000,000 Listings.

All Listings belong to an Import Set. Manually created Listings belong to the **Manual Set**, while imported Listings belong to the Import Set into which they were imported.

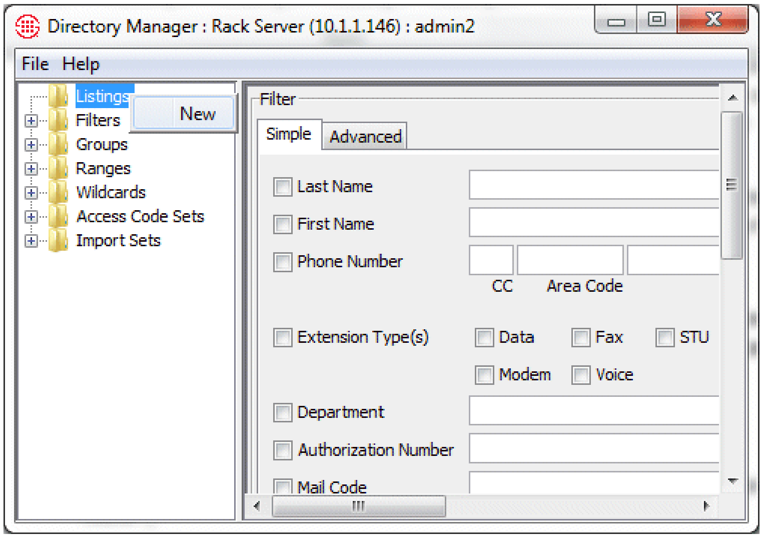
Defining a Manual Directory Listing

The procedure below explains how to manually define a Listing. See "Import Sets" on page 155 for instructions for importing Listings from a text file or an LDAP source.

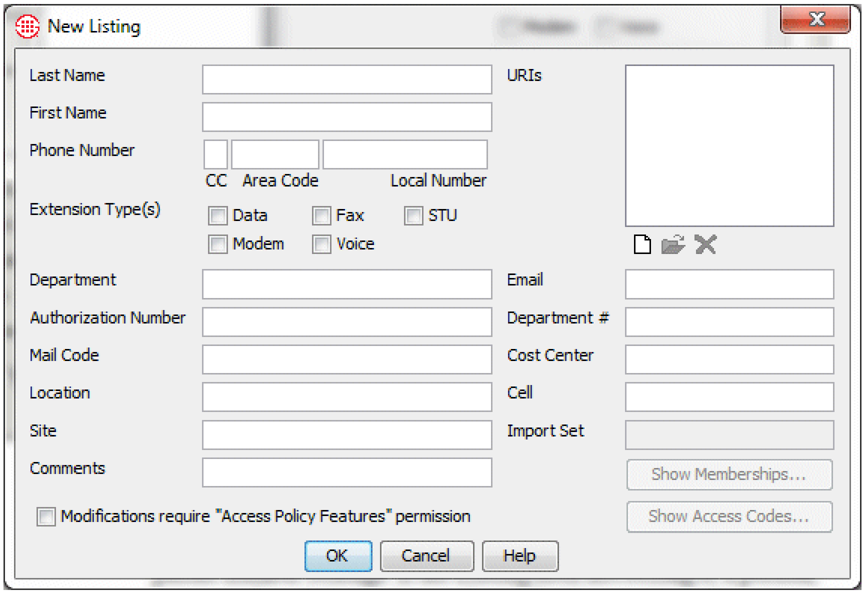
To define a manual Directory Listing

Tip See "Assigning Access Codes to Listings" on page 151 for instructions for associating an Access Code with a Listing.

1. In the Directory Manager tree pane, right-click **Listings** and then click **New**.



2. The **New Listing** dialog box appears.



3. The **Last Name** and **Local Number** fields are required. All other fields are optional. Define the fields as follows:

   - **Last Name**—Type the last name of the person to whom this phone number belongs. If the Listing does not belong to a person, type any descriptive string, such as `9th Floor Fax`.

   - **First Name**—(Optional) Type the first name of the person to whom this phone number belongs. If the Listing does not belong to a person, you can type any descriptive string or leave it blank.

   - **Phone Number**—Type the phone number.

     - **If the phone number is fully qualified**: A fully qualified number consists of a country code, area code, and subscriber number.

       a. In the **Country Code** field, type the 1-to-3-digit country code.

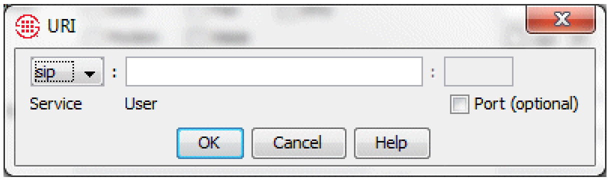
       b. In the **Area Code** field, type the 1-to-8-digit area code.

       c. In the **Local Number** field, type the 1-to-36-digit subscriber number.

     - **If the phone number is a special number**: Special numbers are those that do not have an associated country code and area code when seen by the Appliance, such as **911** (for example, **311** is a special number in San Antonio, Texas, that is used to dial City Public Service). For proper processing, special numbers must be defined as such in the Dialing Plan.

       - In the **Local Number** field, type the digit string for the special number.

- **Department**—(Optional) The department in which the person works. The **Department** field can contain up to 100 characters and spaces, including letters, digits, and special characters.
- **Authorization Number**—(Optional) A PIN or any other character string to be associated with this Listing, such as an employee ID. The **Authorization Number** field can contain up to 100 characters and spaces, including letters, digits, and special characters.
- **Mail Code**—(Optional) Manual routing code, if used, or any other identifier you want to supply. The **Mail Code** field can contain up to 100 characters and spaces, including letters, digits, and special characters.
- **Location**—(Optional) The physical location of the extension. The **Location** field can contain up to 100 characters and spaces, including letters, digits, and special characters.
- **Comments**—(Optional) Type a comment of up to 255 characters and spaces. The comment can contain any combination of letters, digits, spaces, and special characters except commas.
- **Extension Type(s)**—(Optional) Select the types of calls allowed on this extension: Data, Fax, Modem, STU, and/or Voice.
- **Site**—(Optional) The **Site** field can contain up to 100 characters and spaces, including letters, digits, and special characters.
- **URIs**—(Optional) You can define up to five URIs associated with this Listing. To define a URI, click the **New** icon under the **URIs** box. The **URI** dialog box appears.



Define the fields to match the URI you are denoting:

a. In the **Service** box, select either **SIP** or **H.323**.

b. In the **User** box, type the user for this **URI**.

c. In the **Domain** box, type the host string, either a fully qualified domain name (e.g., **securelogix.com**) or a numeric IPv4 address.

d. (*Optional*) If you are certain that your VoIP calls include a port number, select the **Port (optional)** check box; in the **Port** box, type the port number where requests are sent. Typically, the Span does not specify a port. If this is the case in your environment, leave the **Port** check box cleared.

e. Click **OK**.

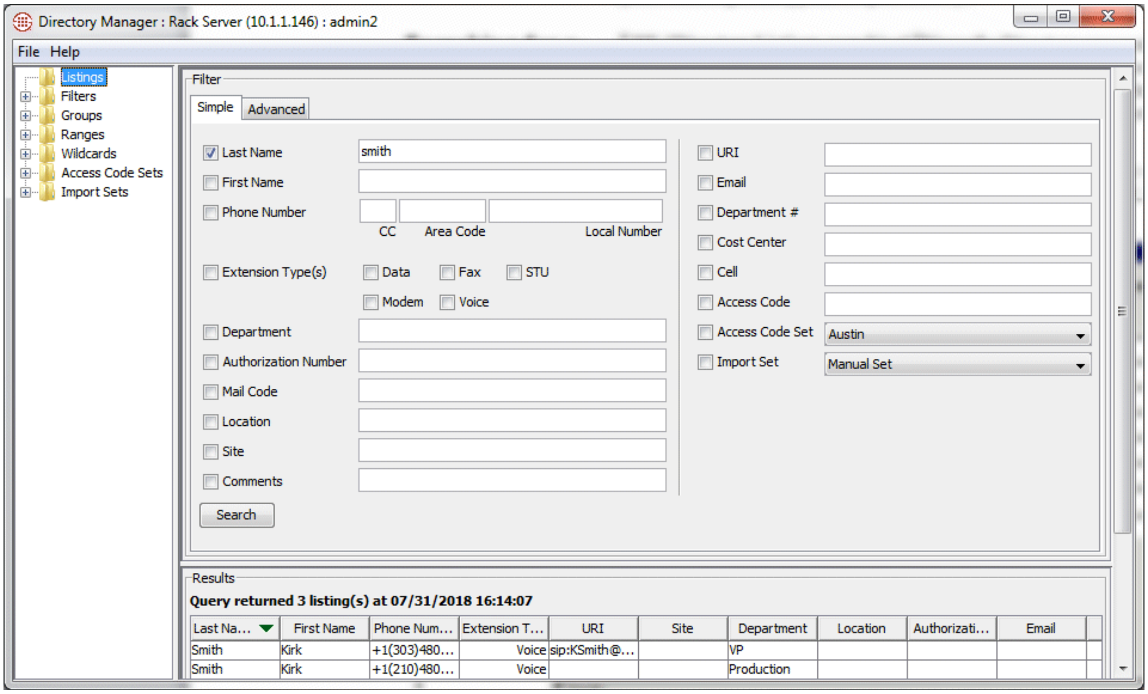
- **Email**—(Optional) Type the person's email address. The **Email** field can contain up to 100 characters.
- **Custom 1, 2, and 3**—(Optional) User-definable fields. These fields can be named to suit your organization and can contain any type of data your organization wants to include in Listings. If the three fields below **Email** in your GUI bear different labels, they have already been renamed. For instructions for modifying these labels, see "Changing User-Defined Directory Listing Field Labels" in the *ETM® System Administration and Maintenance Guide*.
- **Import Set**—Not an editable field. Manually defined Listings belong to the Manual Set of Listings.
- **Modifications Require "Access Policy Features " permission**—Select this check box to restrict editing of this Listing to users with **Access Policy Features** permission.

4. Click **OK**. If an existing Listing in the Manual Set has the same phone number as the one you type, a prompt appears to confirm that this is intentional. Manually defined Listings are not compared for uniqueness against Listings in other Import Sets.

Searching for a Directory Listing

Since the Directory can contain up to 1,000,000 Listings, you cannot browse through the Listings in the **Listings** node as you can with the contents of the other Directory nodes. Instead, to locate a specific Listing or set of Listings in the Directory, you use the **Listing Search** dialog box, as shown below.

You can perform a simple search or an advanced search. Advanced search criteria can also be saved as Directory Filters, which can be used in Policies, report filters, and Listing searches.



☑ Last Name: smith
□ First Name
□ Phone Number
□ Extension Type(s) □ Data □ Fax □ STU □ Modem □ Voice
□ Department
□ Authorization Number
□ Mail Code
□ Location
□ Site
□ Comments
□ URI
□ Email
□ Department #
□ Cost Center
□ Cell
□ Access Code
□ Access Code Set: Austin
□ Import Set: Manual Set

Query returned 3 listing(s) at 07/31/2018 16:14:07

Last Na...	First Name	Phone Num...	Extension T...	URI	Site	Department	Location	Authorizati...	Email
Smith	Kirk	+1(303)480...	Voice	sip:KSmith@...		VP			
Smith	Kirk	+1(210)480...	Voice			Production			

Simple Search

The fields labeled Custom 1, 2, and 3 in this illustration and text are user-definable and bear whatever labels your system administrator has assigned to them. See the *ETM*® *System Administration and Maintenance Guide* for instructions for changing these labels.

You can use one or any combination of the following fields to locate Listings: Last Name, First Name, Phone Number, Extension Type(s), Department, Authorization Number, Mail Code, Location, Site, Comments, URI, Email, Custom 1, Custom 2, Custom 3, Access Code, Access Code Set, and Import Set.

You can use asterisks as Wildcards in any text field to denote unknown or unimportant information. For example, in the illustration above, the **Country Code** and **Local Number** fields contain asterisks, while the **Area Code** and **Last Name** are specified. Therefore, all Listings containing that Area Code and the Last Name *Smith* match the filter. If the **Country Code** and **Local Number** field had been left blank, only Listings in which those fields were actually blank would match.

You can also use asterisks to denote parts of words or numbers. For example, typing `John*` in the **Last Name** field would return all Listings containing a last name beginning with *John* (Johnson, Johnston, Johns, etc.). In the same way, typing `*securelogix.com` in the **Email** field returns all Listings containing an email address ending with *securelogix.com*. Or, to search for all Listings in the 561 exchange, you could type `561*` in the **Local Number** field.

You can browse all of the Listings using a Wildcard search in the **Last Name** field, but depending on the number of Listings in the Directory, this may not be reasonable and you may want to more narrowly tailor your search.

To perform a simple search

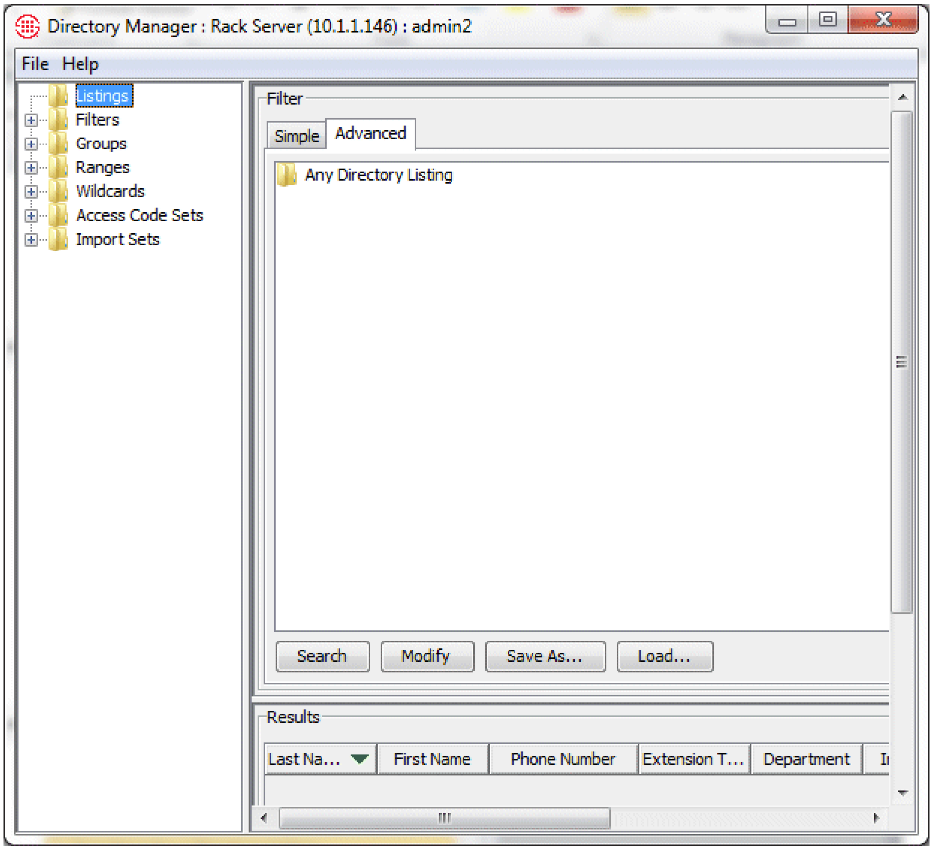
1. In the tree pane, click **Listings**. The **Listing Search** dialog box appears in the application pane.
2. Type or select the information that retrieved Listings are to contain. Refer to the explanatory text at the beginning of this topic for more information.
3. Click **Search**. The results appear in the **Results** area. Only Listings that contain all of the specified criteria are returned. Searches are not case sensitive—**SMITH** and **smith** would both match the last name *Smith*.
4. Do any of the following:
   - By default, results are returned in batches of 100. If more than 100 results are returned, use the **First Page**, **Next Page**, **Prev Page**, and **Last Page** buttons to navigate among the results.
     - You can change the number of Listings returned per page via a parameter in the **ETMSystemConsole.cfg** file. See the *ETM® System Administration and Maintenance Guide* for instructions.
   - To create a new Listing, click **New**.
   - To view or edit a retrieved Listing, click the Listing and click **Edit**.
   - To view the Groups and Filters to which a Listing belongs, click the Listing and click **Edit** to open the **Listing** dialog box, and then click **View Memberships**.
   - To view the Access Codes with which the Listing is associated, click the Listing and click **Edit** to open the **Listing** dialog box, and then click **Show Access Codes**.
   - To print a retrieved Listing, click the Listing and click **Print**.
   - To delete a retrieved Listing from the database, click **Delete**.

Advanced Search

When you define advanced search criteria to locate Listings, you can also save those criteria as a Directory Filter to use later to locate Listings in the Directory, add Listings to Policy Rules, filter log displays, and define reports.

To perform an advanced search

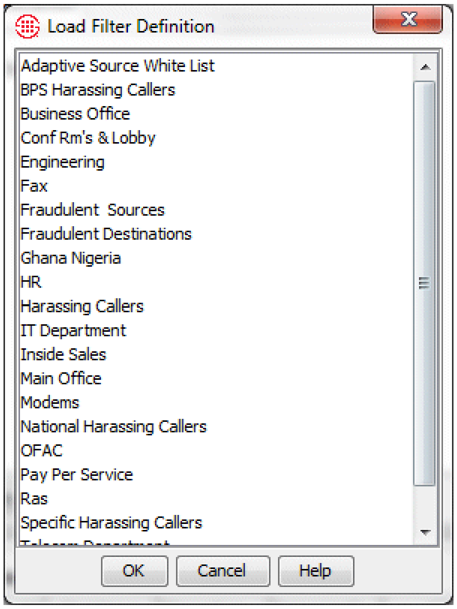
1. In the **Listing Search Filter** dialog box, click the **Advanced** tab.



2. Do one of the following:

   - To reuse search criteria you have already defined and saved:

     a. Click **Load**. The **Load Filter Definition** dialog box appears.


Load Filter Definition

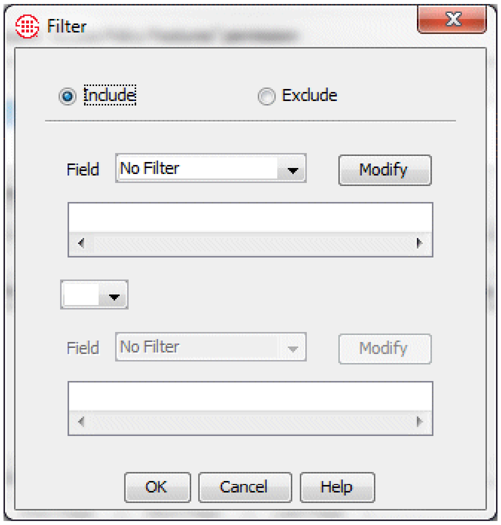
Adaptive Source White List
BPS Harassing Callers
Business Office
Conf Rm's & Lobby
Engineering
Fax
Fraudulent Sources
Fraudulent Destinations
Ghana Nigeria
HR
Harassing Callers
IT Department
Inside Sales
Main Office
Modems
National Harassing Callers
OFAC
Pay Per Service
Ras
Specific Harassing Callers
Telecom Department

b. Click the filter definition you want to use, and then click **OK**.

c. The filter criteria appear in the **Advanced** tab. You can load multiple saved searches at once. You can also use a combination of loaded filters and newly defined criteria to specify the Listings to which the filter applies. See the bullet below for instructions for adding new criteria.

d. When you have specified all the search criteria, click **Search**. The Listings that match appear in the **Results** box.

- To define a new set of search criteria, click **Modify**. The **Filter** dialog box appears.


Filter

● Include ○ Exclude

Field: No Filter

Field: No Filter

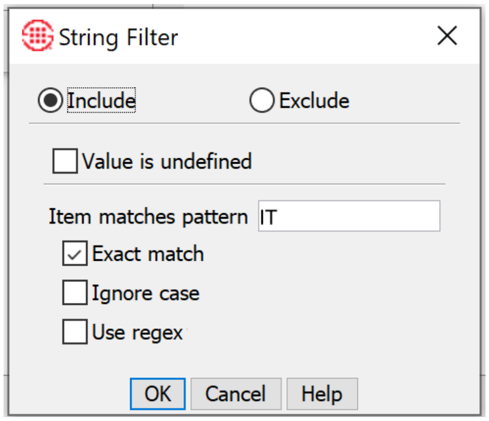
a. To define the filter to exclude Listings that meet the criteria, select **Exclude**; to define the filter to include all Listings that meet the criteria, select **Include**.

b. In the **Field** box, click the down arrow. All of the fields in a Directory Listing appear as options.

c. Select the field to which you want to apply a filter. The filter dialog box for the selected field appears.

For example, suppose you want to include only Listings in the IT department. Select **Department**. The **String Filter** dialog box appears. Select **Include**, Type **IT** as the pattern to match, and click **OK**. The criteria appear in the **Filter** dialog box, as illustrated below.

Note: If you select **Use regex**, **Exact match** and **Ignore case** are grayed out. Type the regex in the **Item matches pattern** box. Full regex is supported for the Directory Manager. See “String Filter” on page 220 for additional information.



String Filter

● Include ○ Exclude

□ Value is undefined

Item matches pattern IT

☑ Exact match

□ Ignore case

□ Use regex

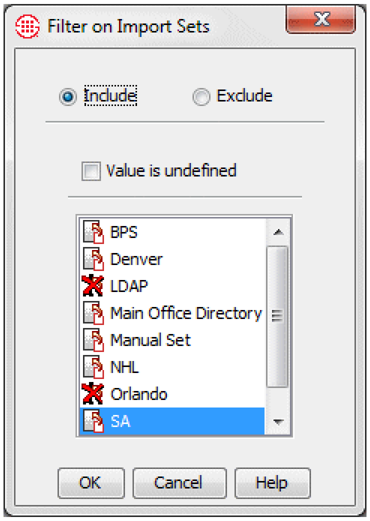
Notice that both the **String Filter** dialog box and the **Filter** dialog box have exclude/include check boxes. These fields work together. For example:

Filter Dialog Box	**String Filter Dialog Box**	**Result**
Include	Include pattern	Includes Listings with the specified string in the selected field..
Include	Exclude Modem	Exclude Listings with the specified string in the selected field.
Exclude	Exclude Modem	Exclude Listings that do not contain the specified string in the selected field..
Exclude	Include Modem	Exclude Listings with the specified string in the selected field.

d. To specify more than one filter criterion, select a logical operator:

- **OR**—Data containing either or both of the specified filter criteria is included.
- **AND**—Only data containing both of the specified filter criteria is included.

e. If you select a logical operator, the second **Field** box becomes editable. Repeat steps a through c to specify the second filter. For example, suppose you also want to specify that the Listings belong to the **SA** Import Set. Select **AND** in the logical operator field, and then select **Import Set** in the second field box. The **Filter on Import Set** dialog box appears.

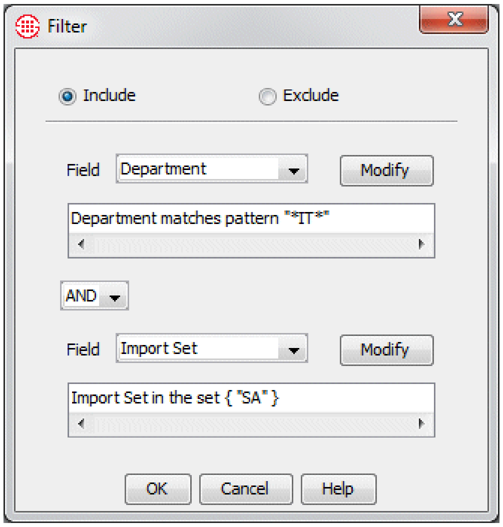

Filter on Import Sets

● Include ○ Exclude

□ Value is undefined

BPS
Denver
LDAP
Main Office Directory
Manual Set
NHL
Orlando
SA

Select the **SA** Import Set, and click **OK**.


Filter

● Include ○ Exclude

Field: Department

Department matches pattern "*IT*"

AND

Field: Import Set

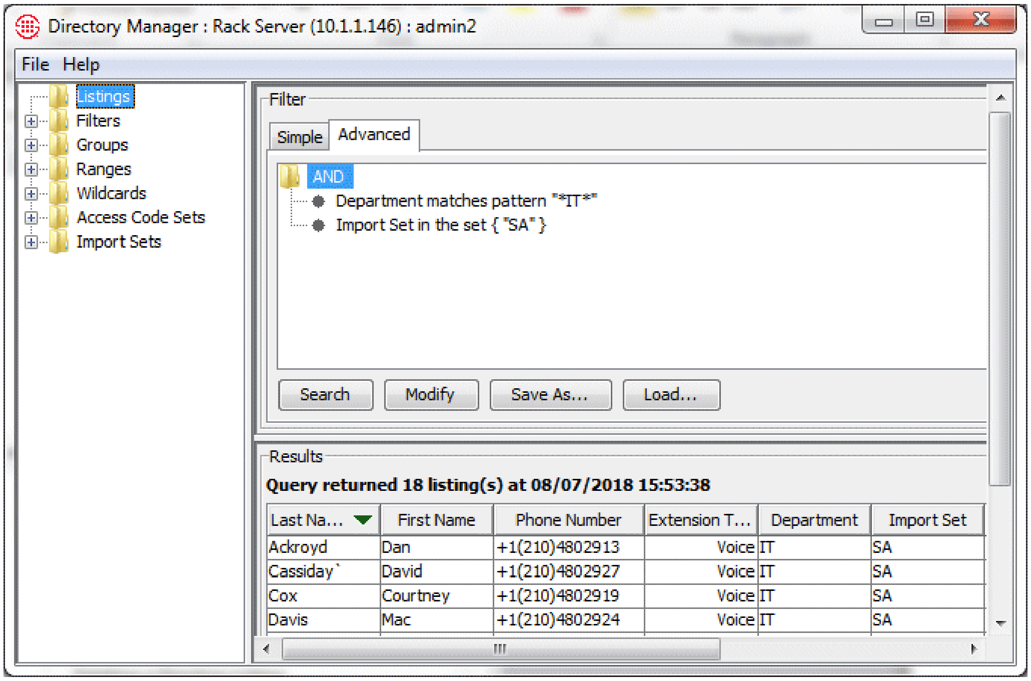
Import Set in the set { "SA" }

Tip You can use a combination of previously defined filters and new criteria. To add a predefined filter to your criteria, click **Load Filter**.

f. To specify additionally filter criteria, you can choose **Sub-filter** in one or both of the **Field** boxes. When you select **Sub-filter**, a second **Filter** dialog box identical to the first appears. Define the subfilter exactly as described above. See "Defining Subfilters" on page 107 for more information, if needed.

g. Click **OK.** The filter criteria appear in the **Advanced** tab..

3. Click **Search**. All of the Listings that match the criteria appear in the **Results** box.



AND
- Department matches pattern "*IT*"
- Import Set in the set { "SA" }

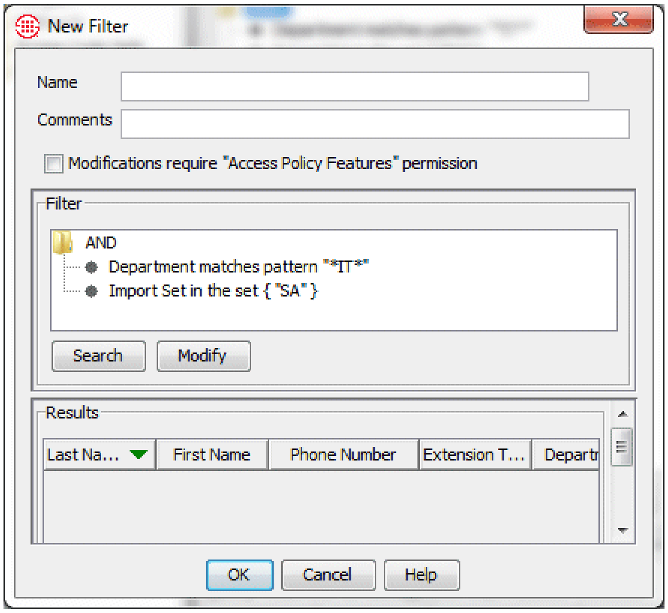
Query returned 18 listing(s) at 08/07/2018 15:53:38

Last Na...	First Name	Phone Number	Extension T...	Department	Import Set
Ackroyd	Dan	+1(210)4802913	Voice	IT	SA
Cassiday`	David	+1(210)4802927	Voice	IT	SA
Cox	Courtney	+1(210)4802919	Voice	IT	SA
Davis	Mac	+1(210)4802924	Voice	IT	SA

- Results are returned in batches of 100. If multiple pages of Listings are returned, click the **First Page**, **Next Page**, **Previous Page**, and **Last Page** buttons to navigate through the results.
  - You can change the number of Listings returned per page via a parameter in the **ETMSystemConsole.cfg** file. See "Changing the Number of Directory Listings Retrieved" in the *ETM*[®] *System Technical Reference* for instructions.
- To view a selected Listing, click the Listing and then click **Edit**.
- To view the Groups and Filters to which a Listing belongs, click the Listing and click **Edit** to open the **Listing** dialog box, and then click **View Memberships**.
- To view the Access Codes for a Listing, click the Listing and click **Edit** to open the **Listing** dialog box, and then click **View Access Codes**.

- To delete a Listing, click the Listing and click **Delete**.
- To print a Listing, click the Listing and click **Print**.
- If you need to change the filter, click **Modify**.

4. To save the search criteria as a Directory Filter, click **Save As**. The **New Filter** dialog box appears showing the specified criteria.



□ Modifications require "Access Policy Features" permission

AND
- Department matches pattern "*IT*"
- Import Set in the set { "SA" }

a. In the **Name** box, type a unique identifier for the Filter.

b. If only users with **Access Policy Features** permission are to be allowed to change this Listing, select the **Modifications require Access Policy Features permission** check box. If anyone who has permission to access the Directory Manager should be able to change this Listing, leave the check box cleared.

c. Click **OK** to save the filter and close the dialog box. The filter appears in the **Filters** node of the Directory Manager tree pane. It can be used in Policies, report filters, and Listing searches.

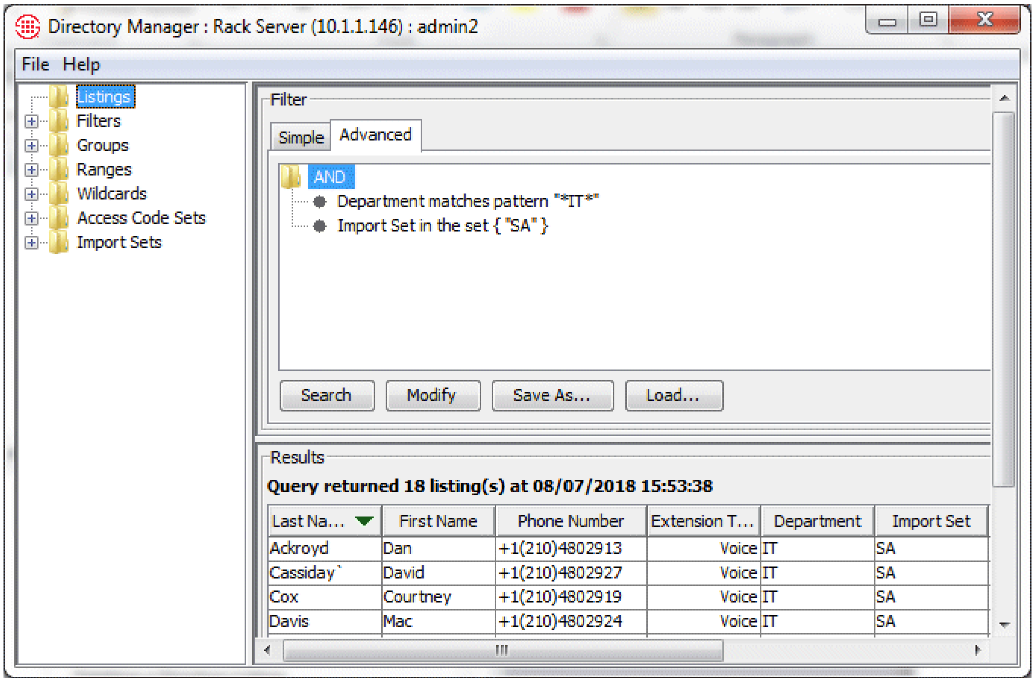
Defining Subfilters

Subfilters enable you to define more narrowly the type of data that matches the filter criteria. For example, perhaps you have 2 sites in San Antonio, Downtown and West, each with an IT department. You would use the following steps to modify the filter in the previous example to add a subfilter by site:

To define a Directory subfilter

1. Refer to “Advanced Search” above on page 102 and use the steps to define a filter. Then you’ll add a subfilter as described here. The image

below shows the filter defined in the previous example. On the **Advanced** tab, click **Modify**.

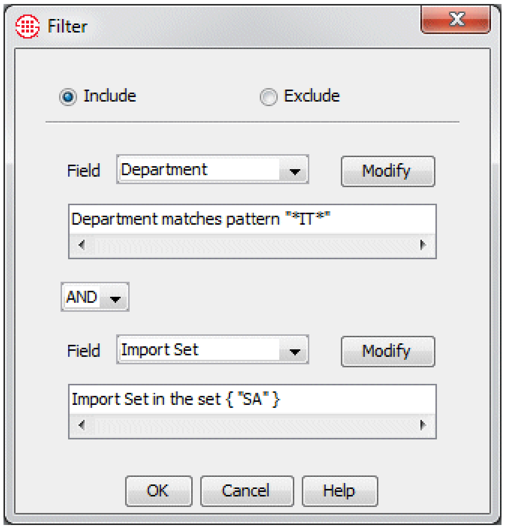


AND
- Department matches pattern "*IT*"
- Import Set in the set { "SA" }

Query returned 18 listing(s) at 08/07/2018 15:53:38

Last Na...	First Name	Phone Number	Extension T...	Department	Import Set
Ackroyd	Dan	+1(210)4802913	Voice	IT	SA
Cassiday`	David	+1(210)4802927	Voice	IT	SA
Cox	Courtney	+1(210)4802919	Voice	IT	SA
Davis	Mac	+1(210)4802924	Voice	IT	SA

2. The **Filter** dialog box appears showing the filter as it is currently defined.



● Include ○ Exclude

Field: Department

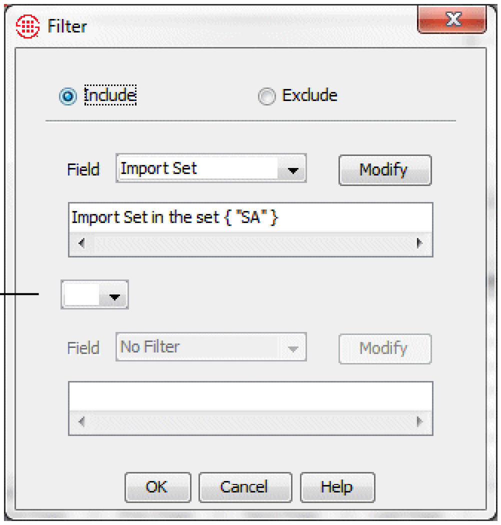
Department matches pattern "*IT*"

AND

Field: Import Set

Import Set in the set { "SA" }

3. In the second **Field** box, click the down arrow and select **Sub-filter**. A second filter box appears showing the current value of the second field.



● Include ○ Exclude

Field: Import Set

Import Set in the set { "SA" }

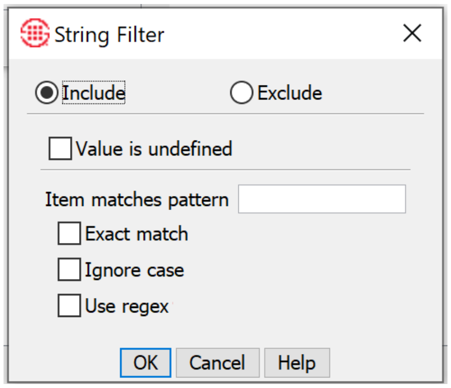
Field: No Filter

Logical Operator box

4. In the **Logical Operator** box, click the down arrow and select **AND**. The second **Field** box becomes editable.

5. In the second **Field** box, click the down arrow and select **Site**. The **String Filter** dialog box appears.

Note: If you select **Use regex**, **Exact match** and **Ignore case** are grayed out. Type the regex in the **Item matches pattern** box. Full regex is supported for the Directory Manager. See “String Filter” on page 220 for additional information.



● Include ○ Exclude

□ Value is undefined

Item matches pattern

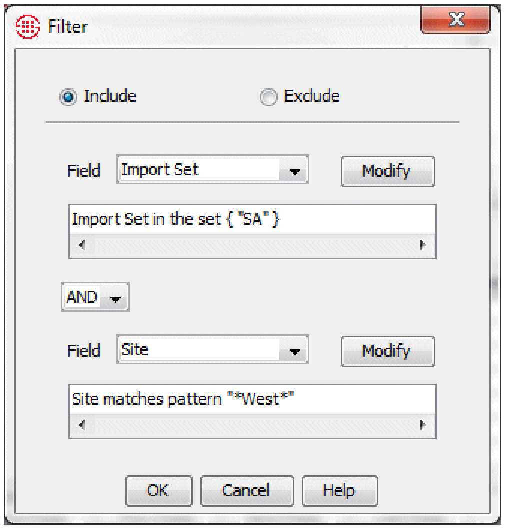
□ Exact match

□ Ignore case

□ Use regex

6. Leave **Include** selected. In **Item matches pattern** box, type `West` and then click **OK**.

7. This **Filter** dialog box now defines the subfilter. Click **OK** to add the subfilter to the filter.



● Include ○ Exclude

Field: Import Set

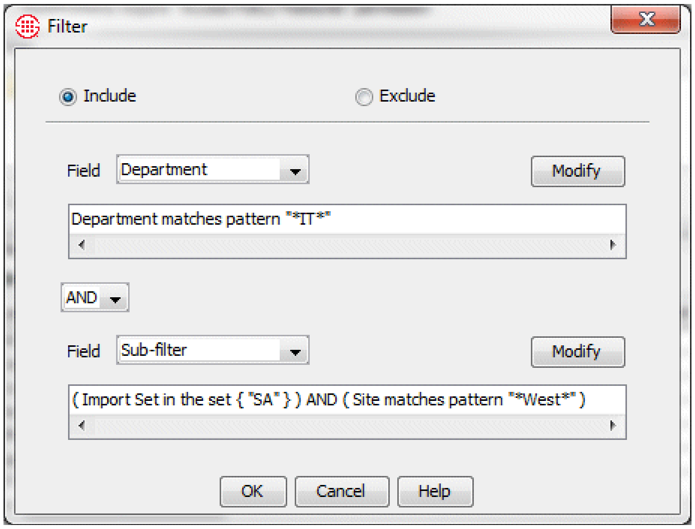
Import Set in the set { "SA" }

AND

Field: Site

Site matches pattern "*West*"

8. The subfilter is added to the filter, as shown below. Click **OK**.



● Include ○ Exclude

Field: Department

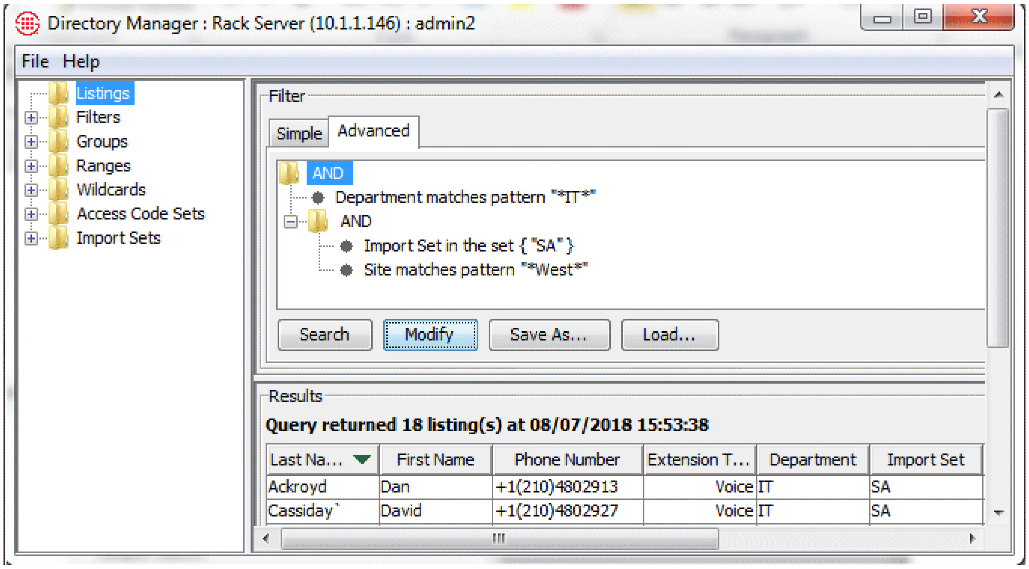
Department matches pattern "*IT*"

AND

Field: Sub-filter

(Import Set in the set { "SA" }) AND (Site matches pattern "*West*")

9. Click **OK** in both **Filter** dialog boxes. The filter appears on the **Advanced** tab of the **Listing Search** dialog box.



```
AND
  Department matches pattern "*IT*"
  AND
    Import Set in the set { "SA" }
    Site matches pattern "*West*"
```

Query returned 18 listing(s) at 08/07/2018 15:53:38

Last Na...	First Name	Phone Number	Extension T...	Department	Import Set
Ackroyd	Dan	+1(210)4802913	Voice	IT	SA
Cassiday`	David	+1(210)4802927	Voice	IT	SA

10. Click **Search**. Note that if you modify existing search criteria, the results are not update until you again click **Search**.

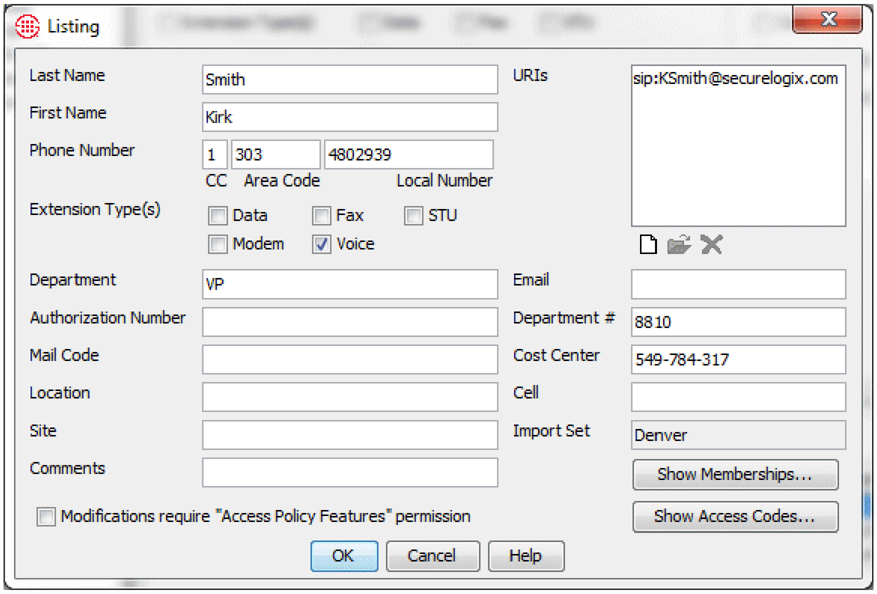
Viewing or Editing a Directory Listing

You can edit both imported and manually created Listings. Be aware that if you manually edit an imported Listing, your changes may be overwritten the next time the Import Set is reconciled, unless you also make the corresponding change to the import source. However, the following manual changes are not affected by import reconciliation:

- The **Modifications require "Access Policy Features " permission** selection is never altered by a reconciliation.
- A null value in the file will not overwrite an actual value in the Listing. For example, if you type a comment in this dialog box but the import file **Comment** field is blank, your comment will remain when reconciliation is performed.

To view or edit a Directory Listing

1. In the Directory Manager, click **Listings** and then search for the Listing you want to view or edit. See "Searching for a Directory Listing" on page 100 for instructions, if necessary.
2. In the **Results** box, click the Listing you want to open, and then click **Edit**. The **Listing** dialog box appears containing the selected Listing.



Listing

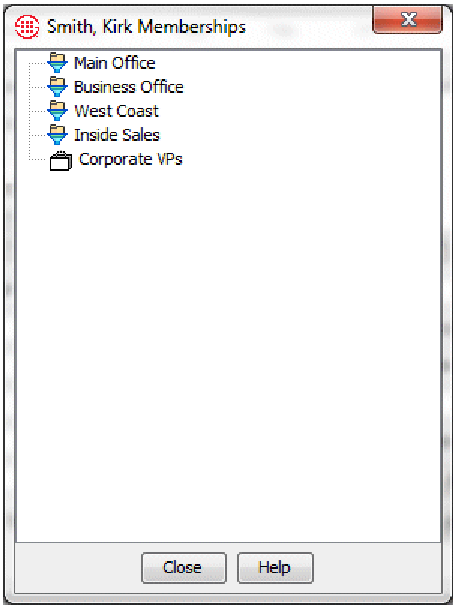
Last Name	Smith	URIs	sip:KSmith@securelogix.com
First Name	Kirk		
Phone Number	1 (CC) 303 (Area Code) 4802939 (Local Number)		
Extension Type(s)	□ Data □ Fax □ STU □ Modem ☑ Voice		
Department	VP	Email	
Authorization Number		Department #	8810
Mail Code		Cost Center	549-784-317
Location		Cell	
Site		Import Set	Denver
Comments			

□ Modifications require "Access Policy Features" permission

3. If you want to edit the Listing, make your changes, and then click **OK**. See "Defining a Manual Directory Listing" on page 96 for a description of the fields, if necessary.

   IMPORTANT The changes do not appear in the **Results** box until you again click **Search**.

4. To view the Groups and Filters of which this Listing is a member, click **Show Memberships**. The **Memberships** dialog box appears.

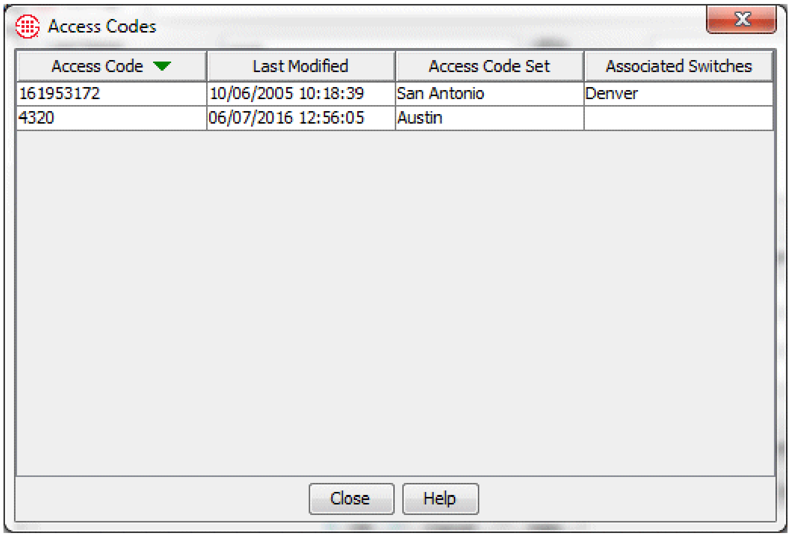


Smith, Kirk Memberships

- Main Office
- Business Office
- West Coast
- Inside Sales
- Corporate VPs

- Click **Close** when you are finished viewing the memberships.

5. To view the Access Codes for this Listing, click **Show Access Codes**. The **Access Codes** dialog box appears.



Access Code ▼	Last Modified	Access Code Set	Associated Switches
161953172	10/06/2005 10:18:39	San Antonio	Denver
4320	06/07/2016 12:56:05	Austin	

- Click **Close** when you are finished viewing the Access Codes.

6. If you made changes to the Listing, click **OK** to save the changes and close the dialog box; click **Cancel** to close the dialog box without saving any changes.

Printing a Directory Listing

To print a Directory Listing

1. In the Directory Manager, click **Listings** and then search for the Listing you want to print. See "Searching for a Directory Listing" on page 100 for instructions, if necessary.
2. In the **Results** box, click the Listing you want to print, and then click **Print**. The **Print Preview** dialog box appears containing the selected Listing.
3. Click the **Printer** icon to print the Listing. The print dialog box for your default printer appears. Print as usual.

Deleting a Directory Listing

Use the procedure below to delete a Listing from the Manual Set. Although you can delete imported Listings, it is recommended that you delete them from the import source. They are then removed from the Directory Manager the next time reconciliation occurs. If you delete an imported Listing from the Directory Manager but do not delete it from the import source, it is recreated in the Directory Manager next time reconciliation is performed.

To delete a Directory Listing

1. In the Directory Manager, click **Listings** and then search for the Listing you want to delete. See "Searching for a Directory Listing" on page 100 for instructions, if necessary.
2. In the **Results** box, click the Listing you want to delete, and then click **Delete**. The **Deletion Confirmation** dialog box appears.
3. Click **Yes**.

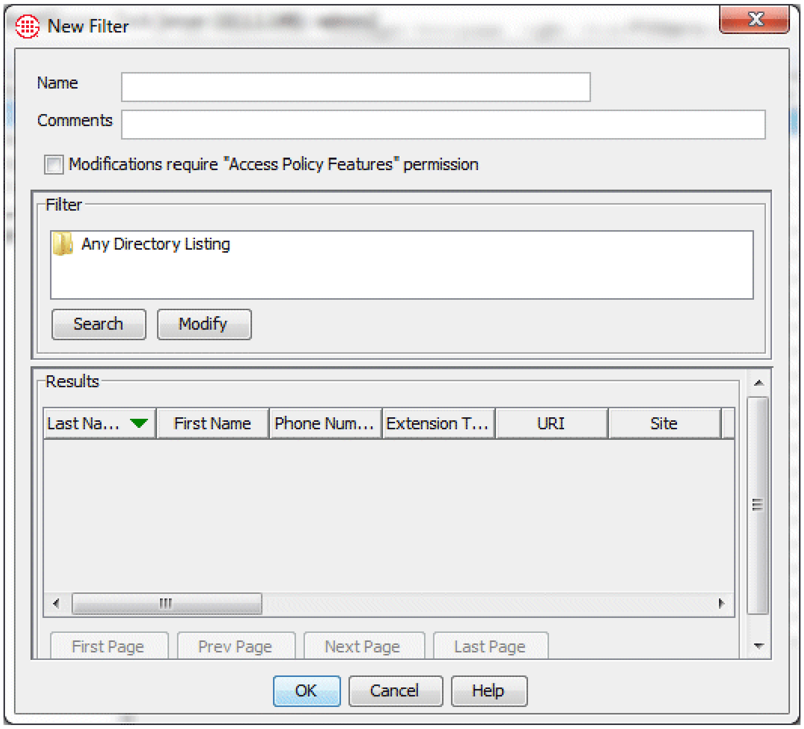
Directory Filters

Directory Filters provide a convenient means to specify and then save a set of search criteria for Listings. You can use these filters in Policies and reports to specify Listings to be included in the same way you would use a single Listing or a Directory Group. This results in all Listings that match the filter criteria automatically being included in the Policy or report. Anytime you add new Listings that match the criteria to the Directory, they are automatically included anywhere the filter is used. For example, if you define a Firewall Policy and use a Directory Filter to specify the source, the Policy applies to any Listings in the Directory that match the criteria. If you later add new Listings that match the criteria, the Policy automatically applies to these new Listings and you will be prompted to reinstall the Policy so the changes take effect on the Span. As with all Directory entities, Directory Filters can be used in Directory Groups.

Defining a Directory Filter

To define a Directory Filter

1. In the Directory Manager tree pane, right-click **Filters** and click **New**. The **New Filter** dialog box appears. Notice that the area where you define the filter criteria is exactly like the **Advanced** tab of the **Listing Search** dialog box, except that you cannot load existing Filters.

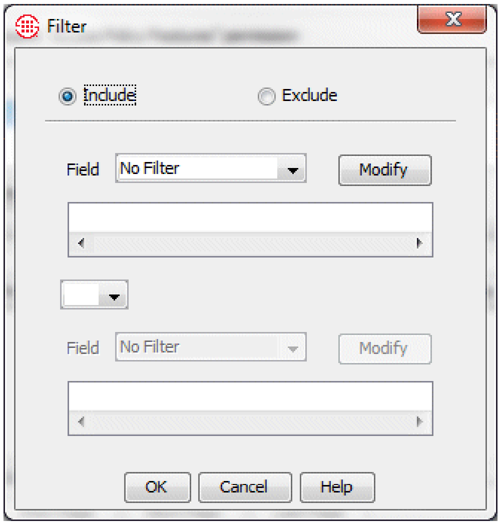


2. In the **Name** box, type a name to identify the Directory Filter.

3. Optionally, in the **Comment** box, type a comment, perhaps to identify the purpose of the filter.

4. If only users with **Access Policy Features** permission are to be allowed to change this Filter, select the **Modifications require Access Policy Features permission** check box. If anyone who has permission to access the Directory Manager should be able to change this Filter, leave the check box cleared.

5. In the **Filter** area, double-click the folder icon. The **Filter** dialog box appears.



Filter

● Include ○ Exclude

Field: No Filter

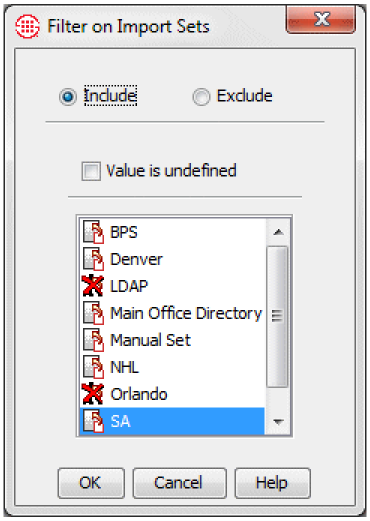
Field: No Filter

6. To define the filter to exclude Listings that meet the criteria, select **Exclude**; to define the filter to include all Listings that meet the criteria, select **Include**.

7. In the **Field** box, click the down arrow. All of the fields in a Directory Listing appear as options.

8. Select the field to which you want to apply a filter. The filter dialog box for the selected field appears.

   For example, suppose you want to limit the filter to include all Listings at your San Antonio Campus, which are in an Import Set named **SA**. Select **Import Set**. The **Filter on Import Set** dialog box appears.



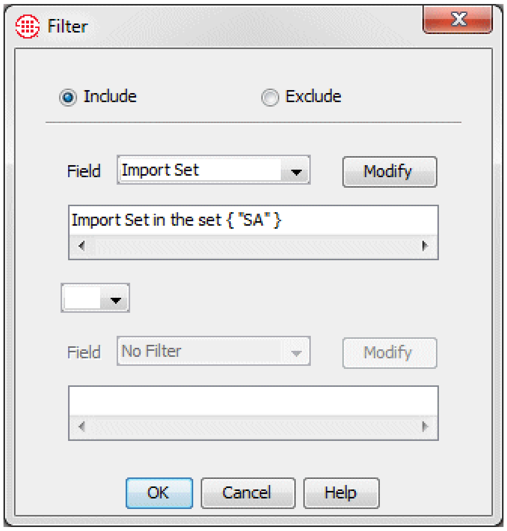
Filter on Import Sets

● Include ○ Exclude

□ Value is undefined

- BPS
- Denver
- LDAP
- Main Office Directory
- Manual Set
- NHL
- Orlando
- SA

Select **Include**, and then click **SA** and click **OK**.



Filter

● Include ○ Exclude

Field: Import Set

Import Set in the set { "SA" }

Field: No Filter

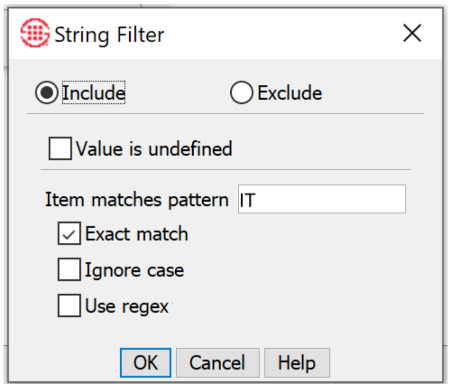
9. To specify more than one filter criterion, select a logical operator:

   OR—Data containing either or both of the specified filter criteria is included.

   AND—Only data containing both of the specified filter criteria is included.

10. If you select a logical operator, the second **Field** box becomes editable. Repeat steps 7 and 8 to specify the second filter. For example, suppose you want also want to specify that the Listings be in the IT department. Select **AND** in the logical operator field, and then select **Department** in the second field box. The **String Filter** dialog box appears.

Note: The filter dialog box that appears varies depending on which field you selected. See "Using Filters in the ETM® System" on page 217 for information about each type of filter.



String Filter

● Include ○ Exclude

□ Value is undefined

Item matches pattern: IT

☑ Exact match

□ Ignore case

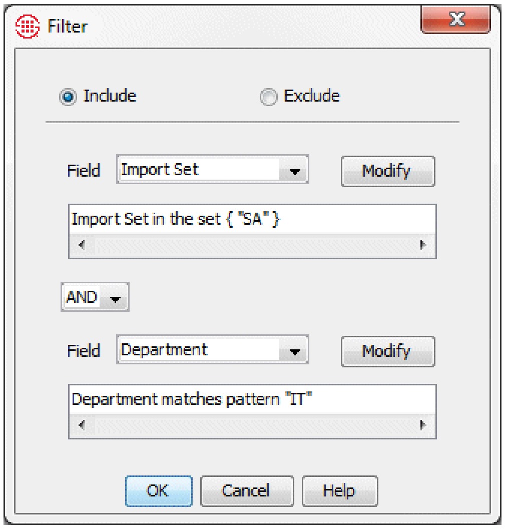
□ Use regex

11. In the **Item matches pattern** box, type `IT`.

12. Optionally, select **Exact match** so that only the exact department name is matched.

    Note: If you select **Use regex**, **Exact match** and **Ignore case** are grayed out. Type the regex in the **Item matches pattern** box. Full regex is supported for the Directory Manager. See “String Filter” on page 220 for additional information.

13. Click **OK**.



Filter

● Include ○ Exclude

Field: Import Set

Import Set in the set { "SA" }

AND

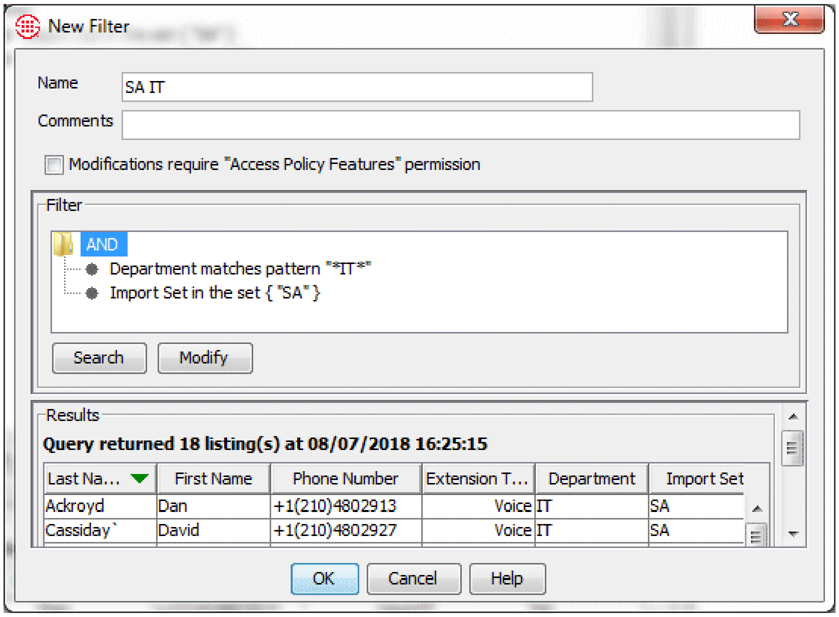
Field: Department

Department matches pattern "IT"

14. To specify additionally filter criteria, you can choose **Sub-filter** in one or both of the **Field** boxes. This is exactly the same procedure as you can use in a Listing search. Refer to “Defining Subfilters” on page 107 for details if necessary.

15. Click **OK** to save the changes and close the dialog box. The filter criteria appear in the **Filter** area of the **New Filter** dialog box.

    - To verify that the Filter retrieves the Listings you intend, click **Search**. The applicable Listings appear in the **Results** area.



New Filter

Name: SA IT

Comments:

☐ Modifications require "Access Policy Features" permission

Filter

AND
- Department matches pattern "*IT*"
- Import Set in the set { "SA" }

Results

Query returned 18 listing(s) at 08/07/2018 16:25:15

Last Na...	First Name	Phone Number	Extension T...	Department	Import Set
Ackroyd	Dan	+1(210)4802913	Voice	IT	SA
Cassiday`	David	+1(210)4802927	Voice	IT	SA

16. If more than 100 results are retrieved, use the **First Page**, **Prev Page**, **Next Page**, and **Last Page** buttons to navigate through the list.

    - If you need to change the filter, click **Modify**.

17. To save the filter and close the dialog box, click **OK**. The filter appears in the **Filters** node of the Directory Manager tree pane.

Viewing a List of all Directory Filters and Their Properties

To view a list of all Directory Filters and their properties

- In the Directory Manager tree pane, click **Filters**. A list of all Filters and their properties appears in the editing pane.

  - To view or edit a Filter, click the Filter in the list and click **Edit**.
  - To delete a Filter, click it and click **Delete**.
  - To print a description of the Filter, click **Print**.
  - To create a new Filter, click **New**.

Printing a Directory Filter

To print a Directory Filter

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

    - Click the **Filters** node. A list of all Directory Filters appears in the editing pane. Click the Filter you want to print.
    - Expand the **Filters** node and click the Filter you want to print. The Filter appears in the editing pane.

2. At the bottom of the editing pane, click **Print**. The **Print Preview** dialog box appears.
3. Click the **Printer** icon. The default print dialog box for your printer appears. Print as usual.

Deleting a Directory Filter

To delete a Directory Filter

1. In the Directory Manager tree pane, do one of the following:
   - Click the **Filters** node. A list of all Directory Filters appears in the editing pane. Click the Filter you want to delete.
   - Expand the **Filters** node and click the Filter you want to delete. The Filter appears in the editing pane.
2. At the bottom of the editing pane, click **Delete**. The **Deletion Confirmation** dialog box appears.
3. Click **Yes**.

Viewing or Editing a Directory Filter

To view or edit a Directory Filter

1. In the Directory Manager tree pane, do one of the following:
   - Click the **Filters** node. A list of all Directory Filters appears in the editing pane. Click the Filter you want to open, and then click **Edit**.
   - Expand the **Filters** node and click the Filter. The Filter appears in the editing pane.
2. For instructions for editing the Filter, see "Defining a Directory Filter" on page 115.

Directory Wildcards

Two types of Directory Wildcards are available: Phone Number Wildcards, which match selected portions of a phone number, rather than all digits; and URI Wildcards, which use pattern matching to match multiple URIs. Both types of wildcards can be used in Policies and report filters.

Phone Number Wildcards

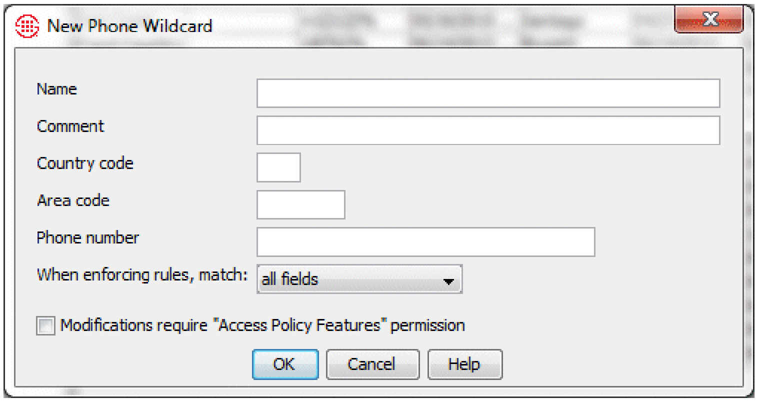
Phone Number Wildcards are used to define Rules or filters to match selected portions of a phone number, rather than all digits. This enables you to represent classes of calls, such as all calls to 800 numbers, rather than just specific phone numbers. You can create Phone Number Wildcards for any of the following:

- **A country code**—The Wildcard matches all phone numbers in that country code.
- **An area code**—The Wildcard matches all phone numbers in that area code within the specified country code.
- **A partial local number (such as an exchange)**—The Wildcard matches all phone numbers containing the specified partial number. A trailing wildcard character % can be used with a partial local number, such as an exchange, to match a range of numbers within a given country and area code. For example, a phone number with **245%** in the phone number field would match any phone number in the 245 exchange within the given country and area code. Only a single % can be used and it must occur at the end of the matching digits.

Defining a Phone Number Wildcard

To define a phone number Wildcard

1. In the Directory Manager tree pane, right-click **Wildcards** and click **Phone Wildcard**. The **New Phone Wildcard** dialog box appears.



When enforcing rules, match: all fields

□ Modifications require "Access Policy Features" permission

2. In the **Name** field, type a descriptive name for the Wildcard. A Wildcard name can contain up to 30 characters.

3. To limit editing of this Wildcard to only users with permission to **Access Policy Features**, select the **Modifications require Access Policy Features permission** check box; if anyone who can access the Directory Manager can change the Wildcard, leave the check box cleared.

4. Optionally, in the **Comment** field, type a comment of up to 255 characters.

5. Do one of the following, depending on the type of Wildcard:

   - To match a partial local number (such as an exchange):

     a. In the **Country code** box, type the dialing access code of the country in which the telephone numbers represented by the Wildcard are located. A country code can be a maximum of three digits.

        The country code is the number that callers *outside* of that country would dial when placing an international call to that number.

     b. In the **Area code** box, type the local area code of the telephone numbers represented by the Wildcard. A North American Numbering Plan (NANP) area code can be a maximum of three digits; other area codes can be a maximum of eight digits.

     c. In the **Phone number** box, type the initial local number digits that you want to match, followed by the **%** Wildcard character. For example, to match all phone numbers in the 810 exchange, type: `810%`

        The **Phone Number** field can contain up to 36 digits. No non-numeric characters or spaces are allowed.

     d. Leave the **When enforcing Rules, match** box set to the default of **all fields**. This means that when this phone number definition is used in a Policy Rule or in a Usage Manager or display filter, the country code, area code, and phone number in the call data must all match those in this Wildcard definition for the Rule to fire or the filter to apply.

   - To match a certain country code:

     a. In the **When enforcing Rules, match** box, select **country code only**. The **Area Code** and **Phone Number** boxes become grayed out.

     b. In the **Country Code** box, type the applicable country code. A country code can be a maximum of three digits.

   - To match a certain area code within a given country code:

a. In the **When enforcing Rules, match** box, select **country and area code**. The **Phone Number** box becomes grayed out.

b. In the **Country Code** box, type the applicable country code.

c. In the **Area Code** box, type the applicable area code.

5. Click **OK**. The Phone Wildcard appears in the tree pane.

URI Wildcards

URI Wildcards use pattern matching to match multiple URIs. In these patterns, you can use alphanumeric characters, symbols, and the following wildcard characters:

? (question mark): matches a single character
***** (asterisk): matches a sequence of zero or more characters.

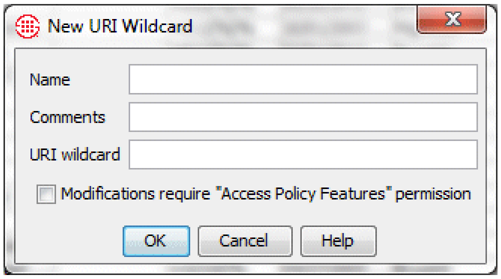
Note that, since these symbols are used as wildcard characters, if you actually want to specify a pattern with a literal question mark or asterisk, you must be escape those characters with a backslash to '\?' or '*' respectively. For example:

URI Wildcard	**Would Match**
b??.smith@sip.securelogix.*	sip:bob.smith@sip.securelogix.com sip:boo.smith@sip.securelogix.edu h323:robot.smith@sip.securelogix.org
b*smith@sip.securelogix.com	sip:beatrice.smith@sip.securelogix.com sip:bob.smith@sip.securelogix.com
joker\?	sip:joker?test@test.org
alan*jones@exam*org	h323:alan*jones@example.org sip:mualan*jones@examination.org
crazy(name){here}@*	sip:crazy(name){here}@test.org sip:not_so_crazy(name){here}@vt.edu
bob_jones@jones.com	sip:bob_jones@jones.com sip:nabob_jones@jones.com.edu

Defining a URI Wildcard

To define a URI Wildcard

1. In the Directory Manager tree pane, right-click **Wildcards** and click **URI Wildcard**. The **New URI Wildcard** dialog box appears.



2. In the **Name** box, type a unique identifier.
3. Optionally, in the **Comment** box, type a comment.
4. In the **URI Wildcard** box, type a pattern denoting the URIs this Wildcard is to match. You can use alphanumeric characters, symbols, and the following wildcard characters:

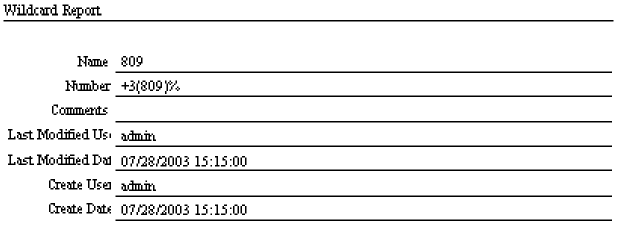
   ? (question mark): matches a single character
   ***** (asterisk): matches a sequence of zero or more characters.

   Note that, since these symbols are used as wildcard characters, if you actually want to specify a pattern with a literal question mark or asterisk, you must escape those characters with a backslash to \? or *, respectively. For example, type `*securelogix.com` to match all URIs in the **securelogix.com** domain; type *10.1.1.1 to match all URIs that contain the string **10.1.1.1**. See "URI Wildcards" on page 123 for more examples of usage.
5. Click **OK** to save the changes. The new **URI Wildcard** appears in the **Wildcards** node of the Directory Manager tree pane.
6. To limit editing of this Wildcard to only users with permission to **Access Policy Features**, select the **Modifications require Access Policy Features permission** check box; if anyone who can access the Directory Manager can change the Wildcard, leave the check box cleared.

Printing a Directory Wildcard

To print a Directory Wildcard

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Wildcards** node.
2. Do one of the following:
   - Right-click the Wildcard and click **Print**.
   - Click the Wildcard, and then click the **Print** button at the bottom of the edit pane.
3. The **Print Preview** dialog box appears showing the Wildcard report. The report includes the following information: Name, Number, the user who last modified it, the date it was last modified, the user who created it, and the date it was created.



Wildcard Report

Name	809
Number	+3(809)%
Comments	
Last Modified Us	admin
Last Modified Dat	07/28/2003 15:15:00
Create Use	admin
Create Date	07/28/2003 15:15:00

4. On the **Print Preview** dialog box toolbar, click the **Print** icon.

Editing a Directory Wildcard

To edit a Directory Wildcard

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Wildcards** node.
2. Click the Wildcard you want to edit. The Wildcard opens in the edit pane.
3. Make changes as desired, and then click **Apply**.
   - To cancel the changes before you click **Apply**, click **Revert**. After you click **Apply**, the changes are committed and cannot be undone.

Deleting a Directory Wildcard

To delete a Directory Wildcard

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Wildcards** node.
2. Do one of the following:
   - Right-click the Wildcard, and then click **Delete**.
   - Click the Wildcard, and then click the **Delete** button at the bottom of the edit pane.

Viewing a List of all Directory Wildcards and Their Properties

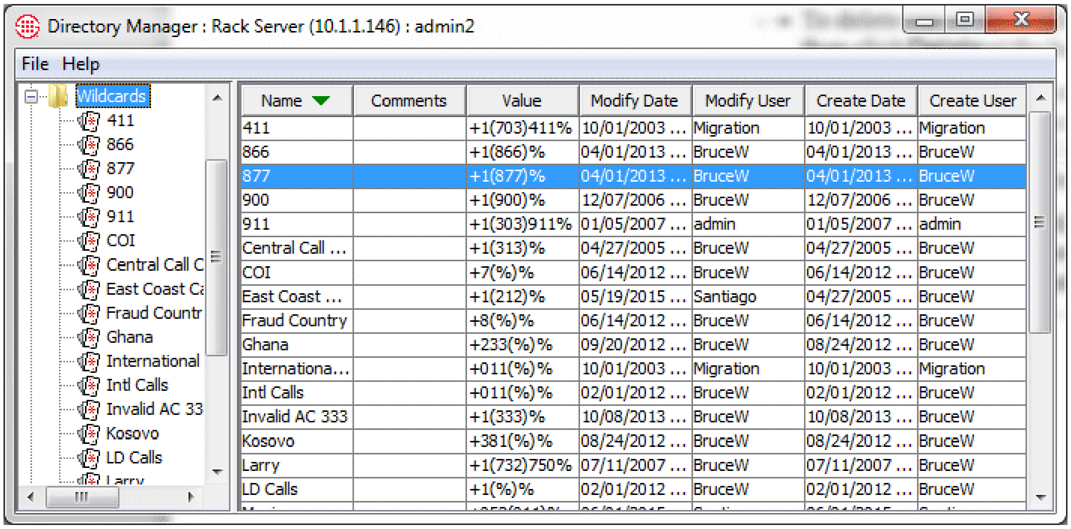
Wildcard properties include: Name, Comment, the value, the date changes were last saved and by whom, and the date created and by whom.

To view a list of all Directory Wildcards and their properties

- In the Directory Manager tree pane, click the **Wildcards** node. The list of all of the Wildcards and their properties appears in the editing pane.
  - To view or edit one of the Wildcards, click the Wildcard in the list, and then click **Edit** at the bottom of the editing pane.
  - To delete one of the Wildcards, click the Wildcard in the list and then click **Delete** at the bottom of the editing pane.
  - To print a report for one of the Wildcards, click the Wildcard in the list and then click **Print** at the bottom of the editing pane. See

"Printing a Directory Wildcard" on page 124 for details about the contents of the Wildcard report.

- To create a new Wildcard, click **New** at the bottom of the editing pane. See "Defining a Phone Number Wildcard" on page 121 or "Defining a URI Wildcard" on page 123 for instructions.



Directory Manager : Rack Server (10.1.1.146) : admin2

Name	Comments	Value	Modify Date	Modify User	Create Date	Create User
411		+1(703)411%	10/01/2003 ...	Migration	10/01/2003 ...	Migration
866		+1(866)%	04/01/2013 ...	BruceW	04/01/2013 ...	BruceW
877		+1(877)%	04/01/2013 ...	BruceW	04/01/2013 ...	BruceW
900		+1(900)%	12/07/2006 ...	BruceW	12/07/2006 ...	BruceW
911		+1(303)911%	01/05/2007 ...	admin	01/05/2007 ...	admin
Central Call ...		+1(313)%	04/27/2005 ...	BruceW	04/27/2005 ...	BruceW
COI		+7(%)%	06/14/2012 ...	BruceW	06/14/2012 ...	BruceW
East Coast ...		+1(212)%	05/19/2015 ...	Santiago	04/27/2005 ...	BruceW
Fraud Country		+8(%)%	06/14/2012 ...	BruceW	06/14/2012 ...	BruceW
Ghana		+233(%)%	09/20/2012 ...	BruceW	08/24/2012 ...	BruceW
Internationa...		+011(%)%	10/01/2003 ...	Migration	10/01/2003 ...	Migration
Intl Calls		+011(%)%	02/01/2012 ...	BruceW	02/01/2012 ...	BruceW
Invalid AC 333		+1(333)%	10/08/2013 ...	BruceW	10/08/2013 ...	BruceW
Kosovo		+381(%)%	08/24/2012 ...	BruceW	08/24/2012 ...	BruceW
Larry		+1(732)750%	07/11/2007 ...	BruceW	07/11/2007 ...	BruceW
LD Calls		+1(%)%	02/01/2012 ...	BruceW	02/01/2012 ...	BruceW

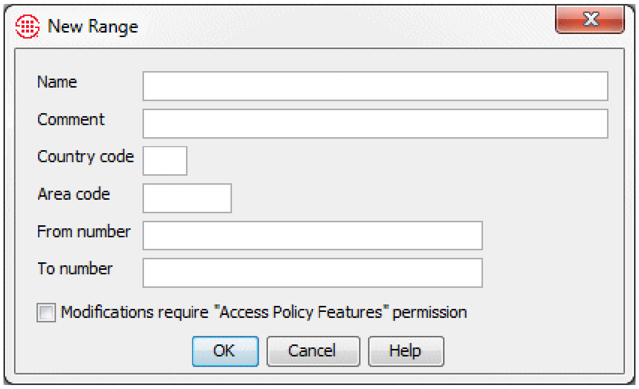
Directory Ranges

A *Directory Range* represents a consecutive series of phone numbers that have the same country code and area code.

Creating a Directory Range

To create a Directory Range

1. In the Directory Manager tree pane, right-click **Ranges** and click **New**. The **New Range** dialog box appears.



New Range

Name	
Comment	
Country code	
Area code	
From number	
To number	

☐ Modifications require "Access Policy Features" permission

2. In the **Name** box, type a unique label for the phone number range. This name identifies the range in the Directory Manager, reports, and

Policies. A name can be any combination of up to 30 characters and spaces.

3. Optionally, in the **Comments** box, type a comment.

4. In the **Country code** box, type the dialing access code of the country in which all of the telephone numbers in the range are located. This is the number that callers outside of the country would dial when placing an international call to any of these numbers. A country code can be a maximum of three digits.

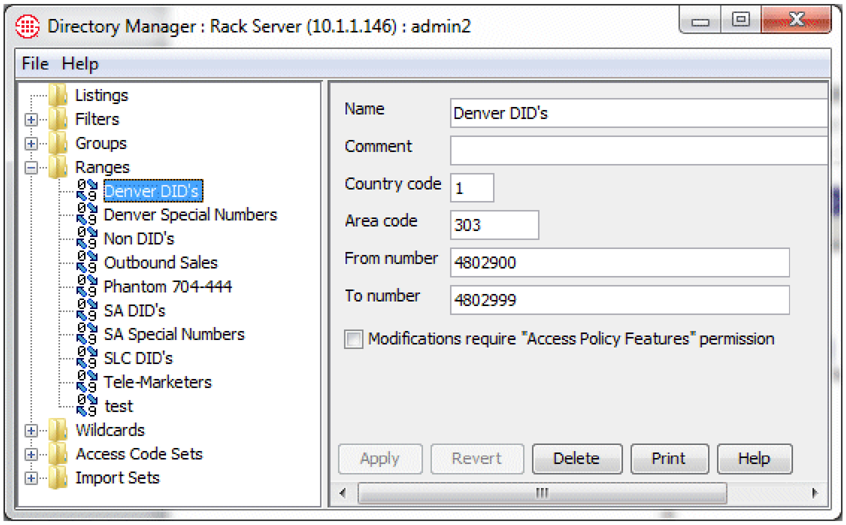
5. In the **Area code** box, type the local area code for this range of telephone numbers. A NANP area code can be a maximum of three digits; other area codes can be a maximum of eight digits.

6. In the **From number** and **To Number** boxes, type the starting and ending telephone numbers in the range. The **From number** and **To Number** can each be a maximum of 36 digits.

   The **To** number must be a greater value than the **From** number.

7. If you want to prevent users who do not have **Access Policy Features** permission from modifying this range, select the **Modifications Require Access Policy Features Permission** check box.

8. Click **OK**. The new phone number range is added to the Directory Manager tree under the **Ranges** node. To view or edit it, simply click it in the tree and it opens in the **Edit** pane.



Directory Manager : Rack Server (10.1.1.146) : admin2

Name: Denver DID's
Comment:
Country code: 1
Area code: 303
From number: 4802900
To number: 4802999
□ Modifications require "Access Policy Features" permission

Editing a Directory Range

To edit a Directory Range

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Ranges** node.

2. Click the Range you want to edit. The Range opens in the editing pane.

3. Edit as desired, and then click **Apply**.
   - To undo your changes before you click **Apply**, click **Revert**. After you click **Apply**, the changes are committed and cannot be undone.

Deleting a Directory Range

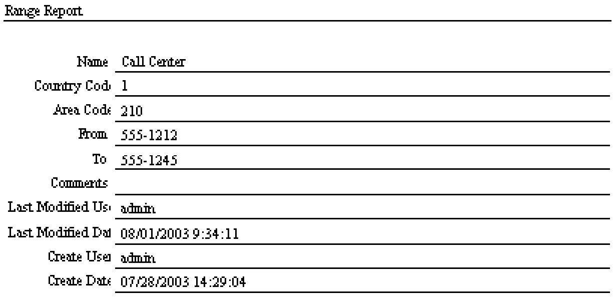
To delete a Directory Range

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Ranges** node.
2. Click the range you want to delete, and then click **Delete**.

Printing a Directory Range

To print a Directory Range

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Ranges** node.
2. Click the Range, and then click **Print**. The **Print Preview** dialog box opens containing the range report. The report includes the following information: Name, Country Code, Area Code, From and To numbers, Comments, Last Modified Date, the user who last modified it, the user who created it, and the date it was created. A sample illustration appears below.



Range Report

Name	Call Center
Country Cod	1
Area Cod	210
From	555-1212
To	555-1245
Comments	
Last Modified Us	admin
Last Modified Da	08/01/2003 9:34:11
Create Use	admin
Create Dat	07/28/2003 14:29:04

3. On the **Print Preview** dialog box toolbar, click the **Print** icon.

Viewing a List of all Directory Ranges and Their Properties

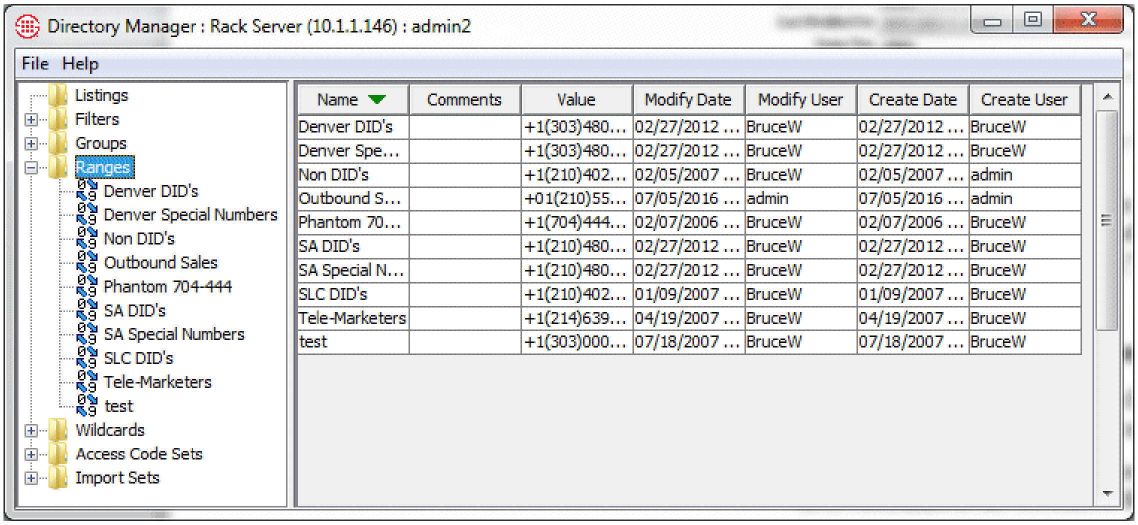
Directory Range properties include: Name, Comment, the value, the date changes were last saved and by whom, and the date created and by whom.

To view a list of all Directory Ranges and their properties

- In the Directory Manager tree pane, click the **Ranges** node. The list of all of the Ranges and their properties appears in the editing pane.
  - To view or edit one of the Ranges, click the range in the list, and then click **Edit** at the bottom of the editing pane.
  - To delete one of the ranges, click the Range in the list and then click **Delete** at the bottom of the editing pane.

- To print a report for one of the Ranges, click the Range in the list and then click **Print** at the bottom of the editing pane. See "Printing a Directory Range" on page 128 for details about the contents of the Range report.

- To create a new Range, click **New** at the bottom of the editing pane. See "Creating a Directory Range" on page 126.



Name	Comments	Value	Modify Date	Modify User	Create Date	Create User
Denver DID's		+1(303)480...	02/27/2012 ...	BruceW	02/27/2012 ...	BruceW
Denver Spe...		+1(303)480...	02/27/2012 ...	BruceW	02/27/2012 ...	BruceW
Non DID's		+1(210)402...	02/05/2007 ...	BruceW	02/05/2007 ...	admin
Outbound S...		+01(210)55...	07/05/2016 ...	admin	07/05/2016 ...	admin
Phantom 70...		+1(704)444...	02/07/2006 ...	BruceW	02/07/2006 ...	BruceW
SA DID's		+1(210)480...	02/27/2012 ...	BruceW	02/27/2012 ...	BruceW
SA Special N...		+1(210)480...	02/27/2012 ...	BruceW	02/27/2012 ...	BruceW
SLC DID's		+1(210)402...	01/09/2007 ...	BruceW	01/09/2007 ...	BruceW
Tele-Marketers		+1(214)639...	04/19/2007 ...	BruceW	04/19/2007 ...	BruceW
test		+1(303)000...	07/18/2007 ...	BruceW	07/18/2007 ...	BruceW

Directory Groups

Directory Groups can contain any combination of Listings, Filters, Ranges, Wildcards, and other Groups. Directory Groups simply provide a convenient organizational tool for using a set of like Directory entities together. For example, you might want to place all of your authorized modems in a Group for use in a Firewall Rule allowing calls from certain numbers to these authorized modems. Note that the members of a Group can still be used as individual entities as well.

IMPORTANT You cannot add more than 10,000 members to a Directory Group. If you need a set containing more than 10,000 members, use a Directory Filter.

Default Groups

The following default groups are used in certain predefined reports. These Groups are empty until you populate them with phone numbers specific to your organization.

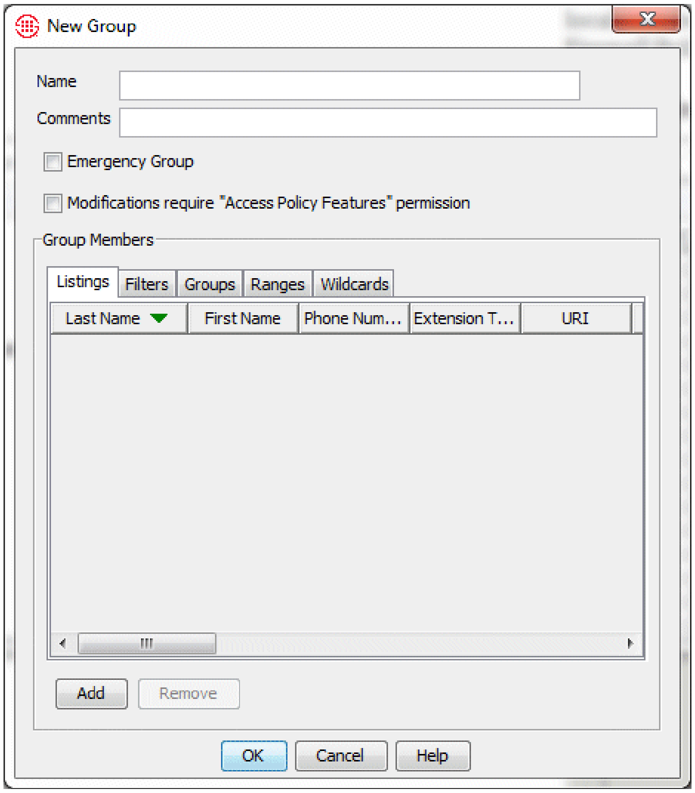
- **Voice Mail**
- **Fax Numbers**
- **Numbers of Interest**
- **ISP Access Numbers**
- **Authorized Modems**

- The default **Emergency Group** is view-only and cannot be edited nor deleted. It contains the national emergency number for the Appliance locale and is present in the implied Emergency Rule that is the first Rule of every Firewall Policy. User-defined Emergency Groups specific to the Appliance locale can be created and added to the Emergency Rule of user-defined Firewall Policies in place of the default Emergency Group.

Creating a Directory Group

To create a Directory Group

1. In the Directory Manager tree pane, right-click **Groups** and click **New**. The **New Group** dialog box appears.



2. In the **Name** box, type the name by which this Group is to be identified in the GUI and reports. A name can be any combination of characters and spaces, with a maximum of 30 characters.
3. Optionally, in the **Comments** box, type a comment.
4. Unless you are specifically defining an Emergency Group, leave the **Emergency Group** check box cleared.
5. If you want to prevent users who do not have **Access Policy Features** permission from modifying this Group, select the

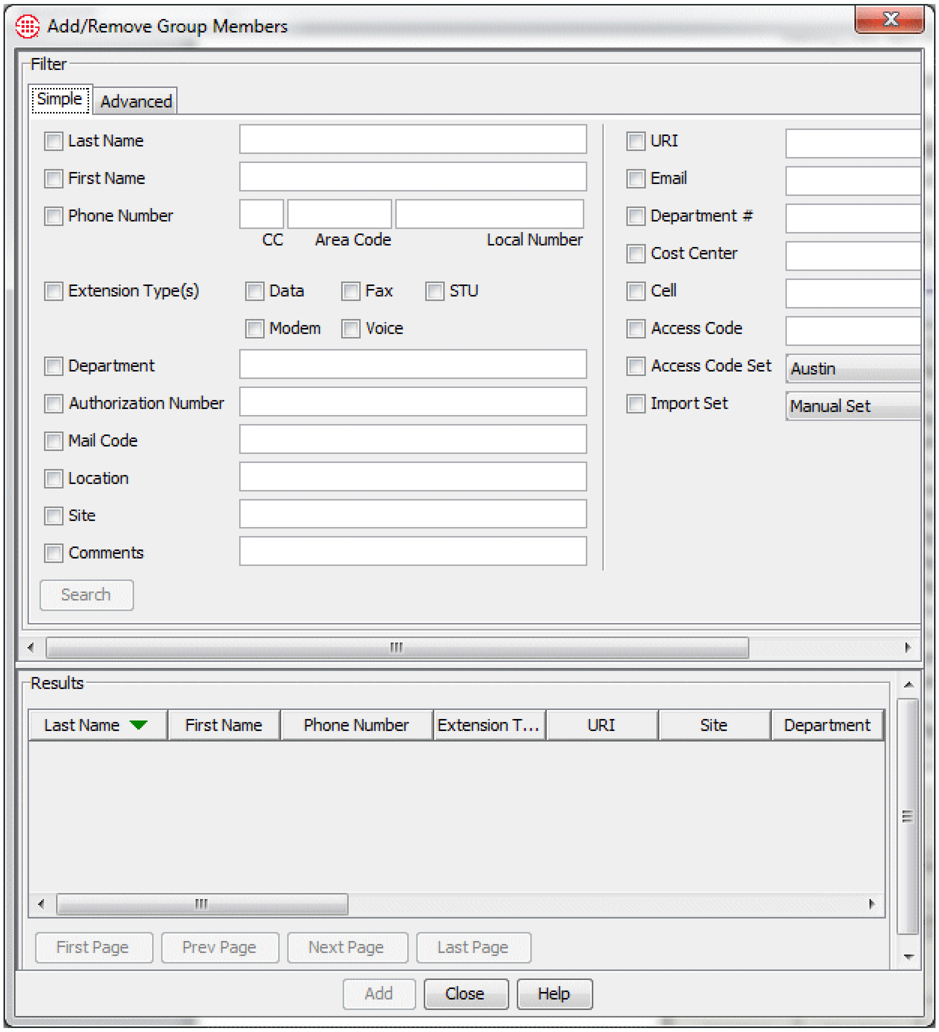
See “Defining a New Emergency Group” on page 136 for information and instructions for Emergency Groups.

Modifications Require Access Policy Features Permission check box.

6. You can add any combination of Listings, Filters, other Groups, Ranges, and Wildcards to a Group. To add each type of Directory entity, do the following:

   - To add one or more Listings to the Group:

     a. On the **Listings** tab, click **Add**. The **Add/Remove Group Members** dialog box appears. Notice that this dialog box is almost identical to the **Listing Search** dialog box and functions identically, except that it provides an **Add** button to add the Listings to the Group.



     b. Define simple or advanced search criteria for the Listings you want to add to the Group, and then click **Search**. See

"Searching for a Directory Listing" on page 100 for detailed instructions, including a description of the search fields and using Wildcards in searches.

c. All of the Listings that match the specified criteria appear in the **Results** box.

   - If multiple pages of Listings are returned, click the **First Page**, **Next Page**, **Previous Page**, and **Last Page** buttons to navigate through the results.

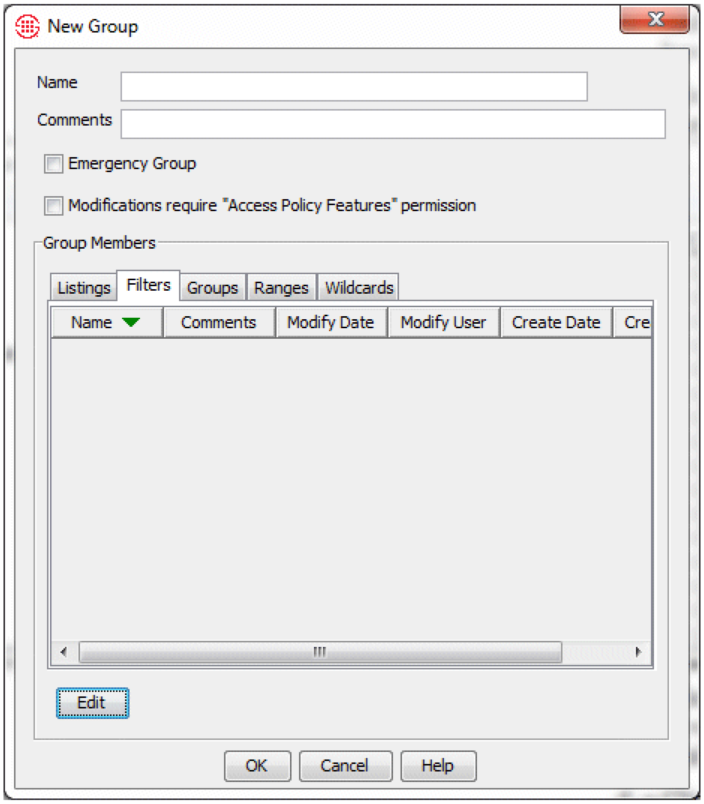
d. Click the Listing(s) you want to add to the Group, and then click **Add**. (To select multiple Listings, hold down CTRL or SHIFT while clicking each Listing.)

e. The Listings are added to the Group. If you want to search for and add additional Listings, repeat this procedure until you have added all of the Listings you want.

f. Click **Close** to return to the **New Group** dialog box. The Listings you added appear on the **Listings** tab.

- To add one or more Directory Filters to the Group:

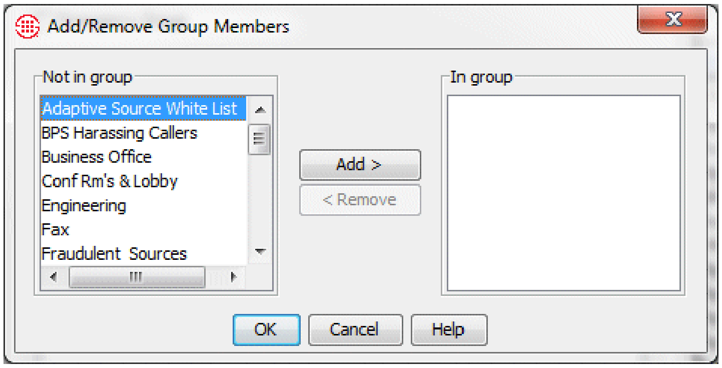
a. Click the **Filters** tab.



□ Emergency Group

□ Modifications require "Access Policy Features" permission

b. Click **Edit**. The **Add/Remove Group Members** dialog box appears. All of the defined Directory Filters appear in the **Not in Group** box.

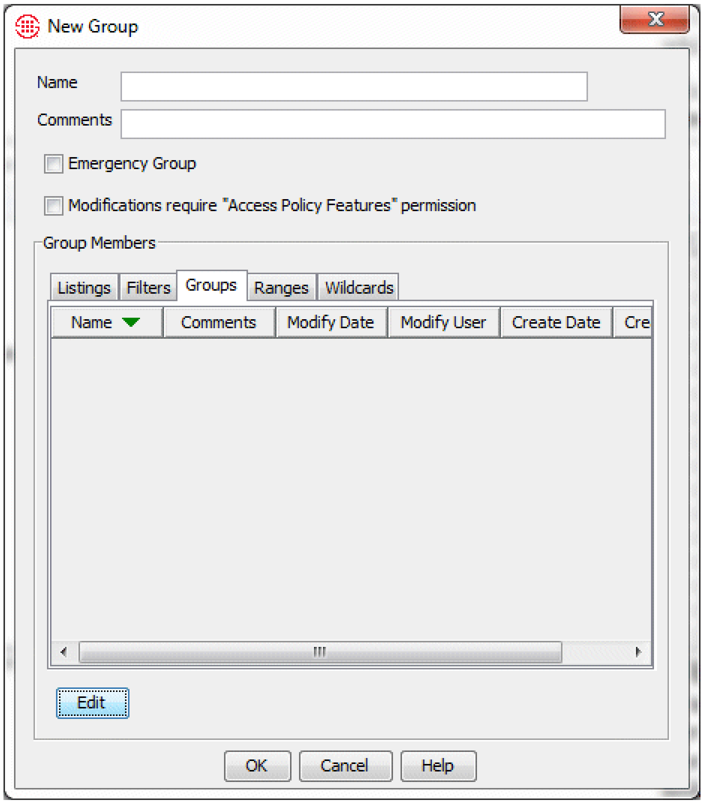


c. Click each filter you want to add to the Group and click **Add**. To select multiple filters at once, hold down CTRL or SHIFT while clicking.

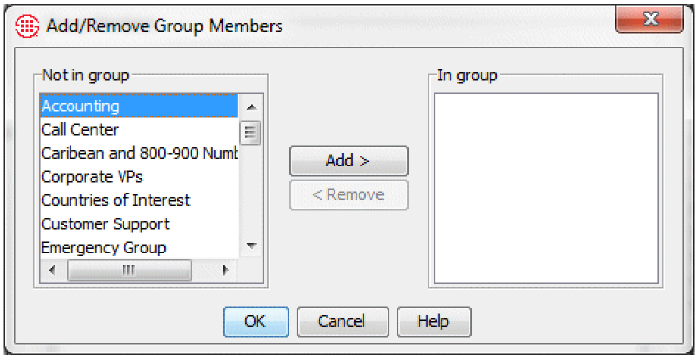
d. Click **OK**. The selected filters appear in the **Filters** tab of the **New Group** dialog box.

- To add one or more other Groups to the Group:

a. Click the **Groups** tab.



b. Click **Edit**. The **Add/Remove Group Members** dialog box appears.



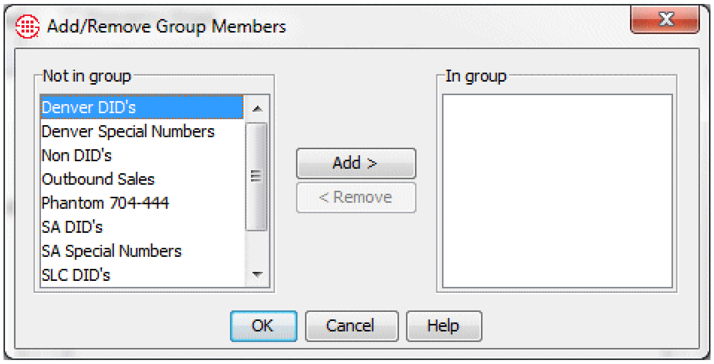
c. In the **Not in Group** box, double-click each Group you want to include. All of the Groups defined on this Management Server appear in this dialog box. Alternatively, you can select one or more Groups and click **Add**. To select multiple items, hold down CTRL or SHIFT while selecting the items.

d. Click **OK**. The Groups appear on the **Group** tab.

- To add one or more Ranges to the Group:

a. Click the **Ranges** tab.

b. Click **Edit**. The **Add/Remove Group Members** dialog box appears. All of the defined Directory Ranges appear in the **Not in Group** box.



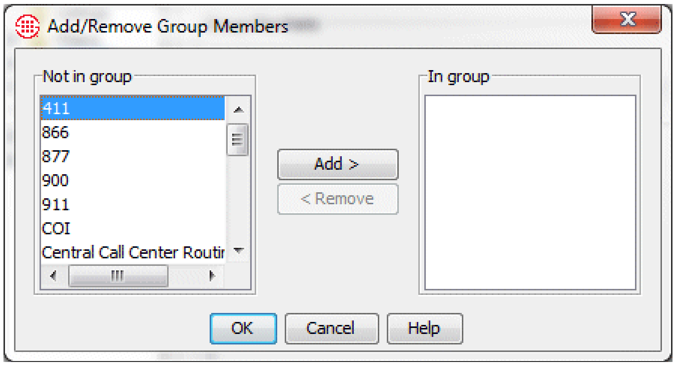
c. In the **Not in Group** box, double-click each range you want to include in the Group. The selected ranges move to the **In Group** box.

d. Click **OK**. The selected ranges appear on the **Ranges** tab.

- To add one or more Wildcards to the Group:

a. Click the **Wildcards** tab.

b. Click **Edit**. The **Add/Remove Group Members** dialog box appears. All of the defined Directory Wildcards appear in the **Not in Group** box.



c. In the **Not in Group** box, double-click each Wildcard you want to add to the Group.

d. Click **OK**. The selected Wildcards appear on the **Wildcards** tab.

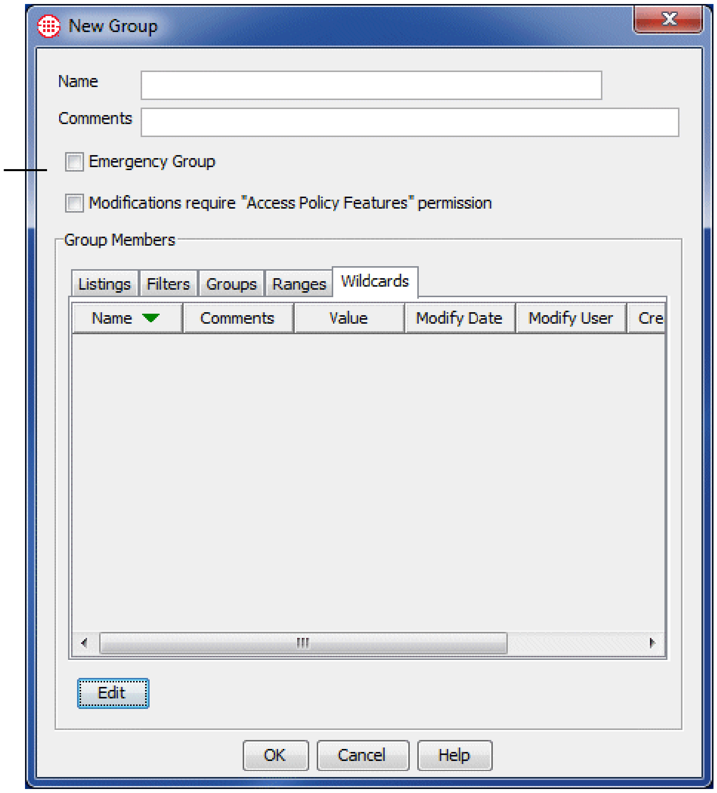
7. Click **OK** to create the Group and close the dialog box.

Defining a New Emergency Group

To define a new Emergency Group specific to the Appliance locale, you create a Directory Group that contains local emergency numbers specified to the Appliance locale, plus the national emergency number (you can simply add the default Emergency Group to your user-defined Emergency Group). When you define the Group, select Emergency Group check box. Emergency Groups are identified by a icon in the Directory Manager tree pane, the **Groups** dialog box, and Policies.

To create an Emergency Group

1. In the Directory Manager tree pane, right-click **Groups** and click **New**. The **New Group** dialog box appears.



Select this check box to denote this group as an Emergency Group

2. Define the Group exactly as you would any other Group, adding any Listings, Groups, Ranges, Filters, and/or Wildcards that contain numbers you want to be treated as emergency numbers.

3. Select the **Emergency Group** check box. Only Groups with this check box selected appear in the **Select Emergency Groups** dialog box (from which you add the Emergency Group to the Policy).

4. Click **OK** to save the Group and close the dialog box.

Editing a Directory Group

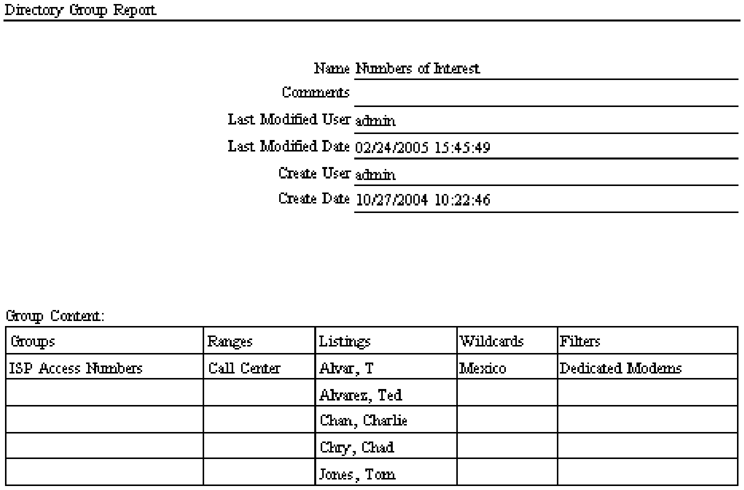
To edit a Directory Group

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Groups** node.
2. Click the Group you want to edit. The Group opens in the editing pane.
3. Make changes as desired.
   - **Listings** tab:
     - To add one or more Listings to the Group, click **Add**.
     - To remove a Listing, click the Listing and click **Remove**.
   - **Filters** tab:
     - To add or remove Filters, click **Edit** at the bottom of the edit pane.
   - **Groups** tab:
     - To add or remove Groups, click **Edit** at the bottom of the edit pane.
   - **Ranges** tab:
     - To add or remove Ranges, click **Edit** at the bottom of the edit pane.
   - **Wildcards** tab:
     - To add or remove Wildcards, click **Edit** at the bottom of the edit pane.
4. Click **Apply**.
   - To discard the changes and revert to the original before you click **Apply**, click **Revert**. After you click **Apply**, the changes are committed and cannot be undone.

Printing a Directory Group

To print a Directory Group

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Groups** node.
2. Do one of the following:
   - Right-click the Group and click **Print**.
   - Click the Group you want to **Print**, and then click the **Print** button at the bottom of the edit pane.
3. The **Print Preview** dialog opens containing the Group report. The report includes the following information: Name, comment, date and time the Group was last modified and by whom, date and time the Group was created and by whom, and a table listing the members of the Group, as shown in the illustration below.



Directory Group Report

Name Numbers of Interest

Comments

Last Modified User admin

Last Modified Date 02/24/2005 15:45:49

Create User admin

Create Date 10/27/2004 10:22:46

Group Content:

Groups	Ranges	Listings	Wildcards	Filters
ISP Access Numbers	Call Center	Alvar, T	Mexico	Dedicated Modems
		Alvarez, Ted		
		Chan, Charlie		
		Chry, Chad		
		Jones, Tom		

4. On the **Print Preview** dialog box toolbar, click the **Print** icon.

Deleting a Directory Group

To delete a Directory Group

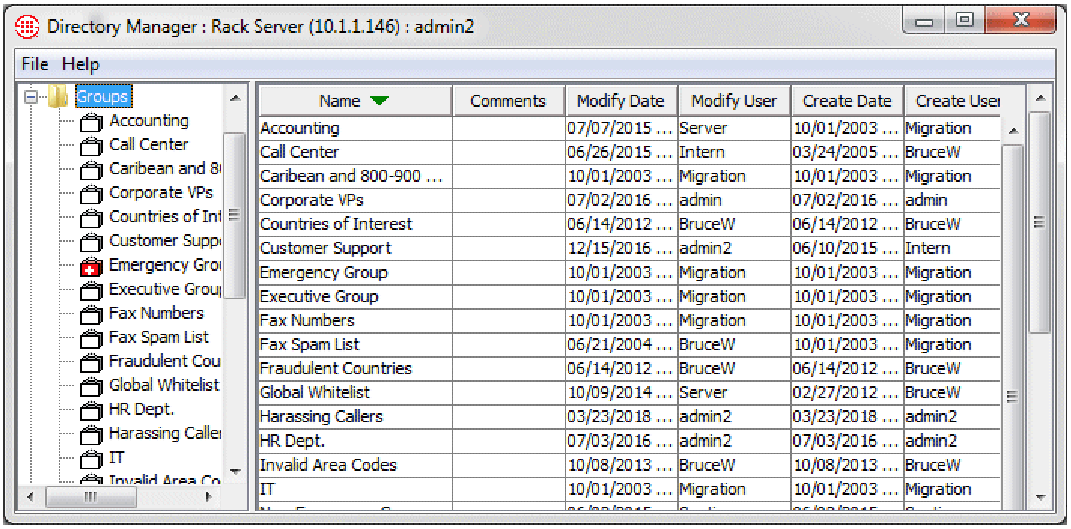
- Do one of the following:
  - In the Directory Manager tree pane, right-click the Group and click **Delete**.
  - In the Directory Manager tree pane, click the Group, and then click **Delete** at the bottom of the editing pane.
  - In the Directory Manager tree pane, click the **Groups** node, and then right-click the Group in the list in the editing pane and click **Delete**.

Viewing a List of All Directory Groups and Their Properties

Directory Group properties include: Name, Comments, the date and time the Group was last modified and by whom, and the date and time the Group was created and by whom.

To view a list of all Groups and their properties

- In the Directory Manager tree pane, click the **Groups** node. The list of all of the Groups and their properties appears in the editing pane.
  - To view or edit one of the Groups, click the Group in the list and then click **Edit** at the bottom of the editing pane.
  - To delete one of the Groups, click the Group in the list and then click **Delete** at the bottom of the editing pane.
  - To print a report for one of the Groups, click the Group in the list and then click **Print** at the bottom of the editing pane. "Printing a Directory Group" on page 138 for details about the contents of the Group report.
  - To create a new Group, click **New** at the bottom of the editing pane. See "Creating a Directory Group" on page 130.



Name	Comments	Modify Date	Modify User	Create Date	Create Use
Accounting		07/07/2015 ...	Server	10/01/2003 ...	Migration
Call Center		06/26/2015 ...	Intern	03/24/2005 ...	BruceW
Caribean and 800-900 ...		10/01/2003 ...	Migration	10/01/2003 ...	Migration
Corporate VPs		07/02/2016 ...	admin	07/02/2016 ...	admin
Countries of Interest		06/14/2012 ...	BruceW	06/14/2012 ...	BruceW
Customer Support		12/15/2016 ...	admin2	06/10/2015 ...	Intern
Emergency Group		10/01/2003 ...	Migration	10/01/2003 ...	Migration
Executive Group		10/01/2003 ...	Migration	10/01/2003 ...	Migration
Fax Numbers		10/01/2003 ...	Migration	10/01/2003 ...	Migration
Fax Spam List		06/21/2004 ...	BruceW	10/01/2003 ...	Migration
Fraudulent Countries		06/14/2012 ...	BruceW	06/14/2012 ...	BruceW
Global Whitelist		10/09/2014 ...	Server	02/27/2012 ...	BruceW
Harassing Callers		03/23/2018 ...	admin2	03/23/2018 ...	admin2
HR Dept.		07/03/2016 ...	admin2	07/03/2016 ...	admin2
Invalid Area Codes		10/08/2013 ...	BruceW	10/08/2013 ...	BruceW
IT		10/01/2003 ...	Migration	10/01/2003 ...	Migration

Access Code Sets

Access Codes extracted from call data can be correlated with ETM Directory Listings in Usage Manager Reports. This allows you to attribute long-distance calls based on the Access Code rather than the phone used to make the call, which gives you a clearer picture of which employee actually made the call. To use Access Codes in reports, your ETM System must be configured to extract Access Codes from SMDR data and you must define one or more Access Code Sets to associate Access Codes with the Listings in the ETM Directory.

See the *ETM® System Technical Reference* for instructions for extracting Access Codes from SMDR.

Besides running reports to correlate Access Codes in call data with Directory Listings, you can use the ETM System to manage your Access Codes. After you define an Access Code Set, you can export a text file of the Access Codes to import into your PBX. Anytime Access Codes change in the ETM System, you can again export the file to update your PBX, and you can easily distribute the Access Codes via email to the people to whom they are assigned with a click of the mouse.

A Diagnostic Log entry is provided anytime an Access Code Set is created or modified.

Two user permissions govern who can see and manage Access Codes.

View Access Codes—Users with this permission can see Access Codes in Reports and Logs. For users without this permission, Access Codes appear as asterisks in Reports and the SMDR Access Code column is not available in Logs.

Manage Access Code Sets—A subpermission of Directory Management, users with this permission can view, modify, and create Access Code Sets. Users without this permission do not see the Access Codes node in the Directory Manager. **View Access Codes** is automatically granted when this permission is granted.

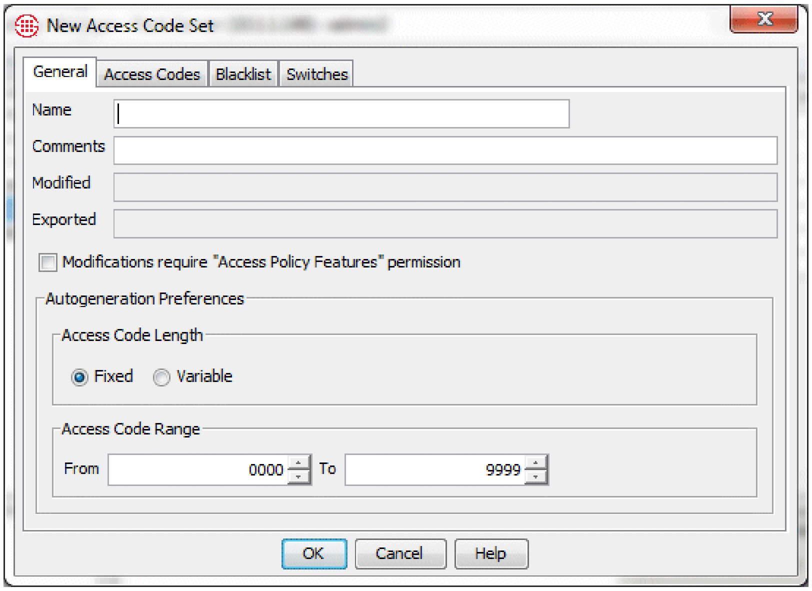
Defining an Access Code Set

An Access Code Set can contain up to 10,000 Listings.

Note You can also create an Access Code Set by importing from a text file. See "Importing Access Codes from a CSV File" on page 147 for instructions.

To define an Access Code Set

1. In the Directory Manager tree pane, right-click **Access Code Sets** and click **New**. The **New Access Code Set** dialog box appears with the **General** tab selected.



Name
Comments
Modified
Exported

□ Modifications require "Access Policy Features" permission

Autogeneration Preferences

Access Code Length

● Fixed ○ Variable

Access Code Range

From 0000 To 9999

2. In the **Name** box, type a unique name for the Access Code Set, up to 30 characters in length.

3. Optionally, in the **Comments** box, type a descriptive comment for the Access Code Set, such as the valid dates, applicability, or the like. The Comment can be included in the automated email used to distribute current access codes to help users to understand the use of their access code.

4. To allow only users who have **Manage Policy Features** permission to edit the Access Code Set, select the **Modifications require "Access Policy Features" permission** check box.

   - To allow all users with **Manage Access Code Sets** permission to edit the Access Code Set, leave the check box cleared.

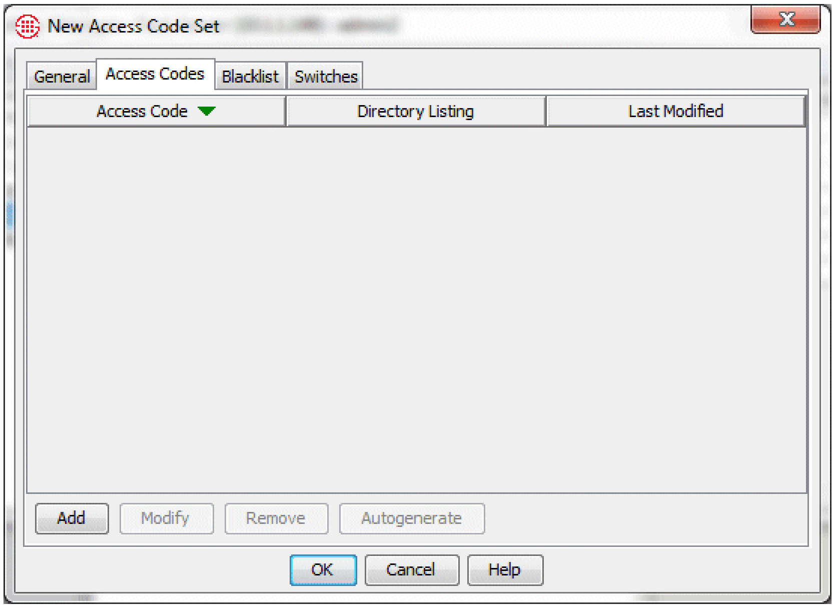
5. In the **Autogeneration Preferences** area:

   a. In the **Access Code Length** area, select one of the following:

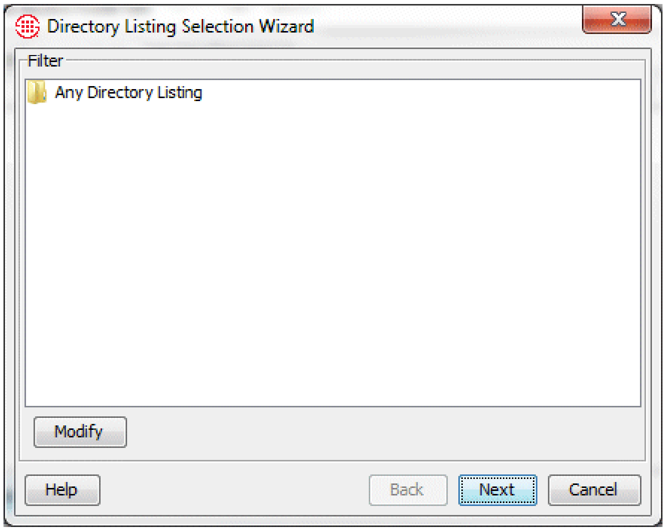
      - **Fixed—**All generated access codes are the same length.
      - **Variable—**Generated access codes vary in length within the range you specify.

   b. In the **Access Code Range** area, type or select the range within which the autogenerated access codes are to fall.

6. Click the **Access Codes** tab.

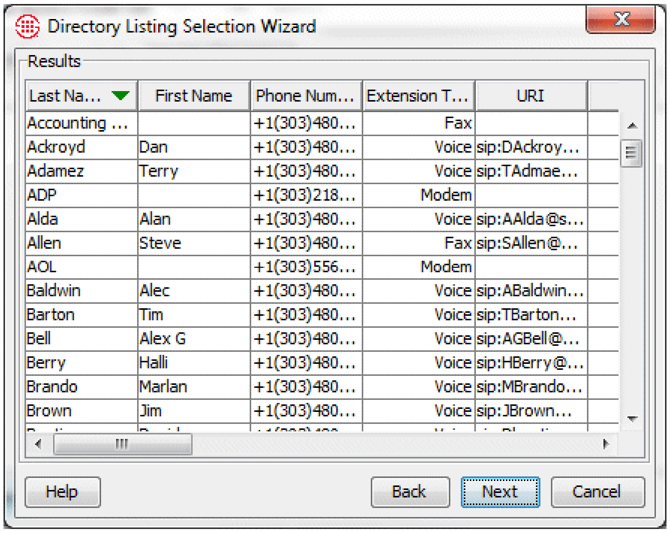


7. Click **Add**. The **Directory Listing Selection Wizard** appears.



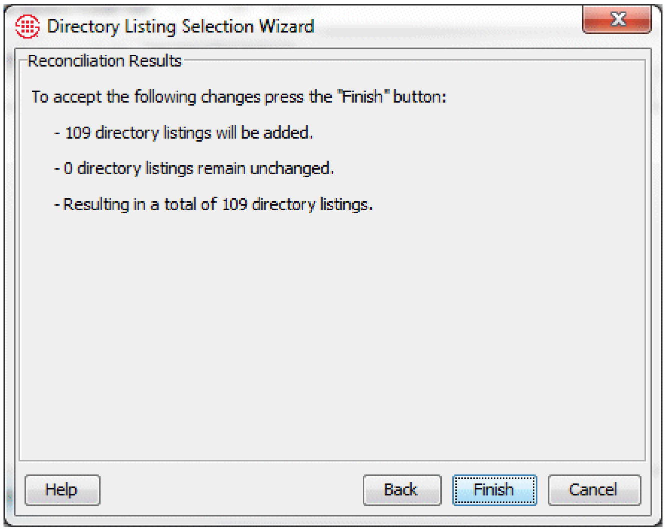
8. Define a Filter to specify which Listings are to belong to this Access Code Set. The Filter works like the **Advanced** tab of a Directory Listing or Report Filter. For instructions for searching for Listings, see "Advanced Search" on page 102.

9. When you have defined the Filter criteria, click **Next**. The Listings that match your search criteria appear. Verify that the results are as expected and then click **Next**.



Last Na...	First Name	Phone Num...	Extension T...	URI
Accounting ...		+1(303)480...	Fax	
Ackroyd	Dan	+1(303)480...	Voice	sip:DAckroy...
Adamez	Terry	+1(303)480...	Voice	sip:TAdmae...
ADP		+1(303)218...	Modem	
Alda	Alan	+1(303)480...	Voice	sip:AAlda@s...
Allen	Steve	+1(303)480...	Fax	sip:SAllen@...
AOL		+1(303)556...	Modem	
Baldwin	Alec	+1(303)480...	Voice	sip:ABaldwin...
Barton	Tim	+1(303)480...	Voice	sip:TBarton...
Bell	Alex G	+1(303)480...	Voice	sip:AGBell@...
Berry	Halli	+1(303)480...	Voice	sip:HBerry@...
Brando	Marlan	+1(303)480...	Voice	sip:MBrando...
Brown	Jim	+1(303)480...	Voice	sip:JBrown...

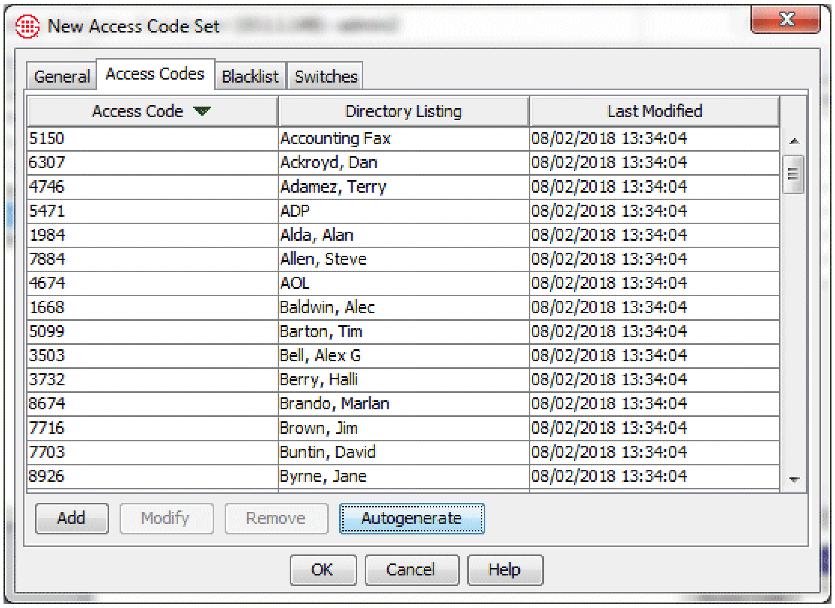
10. The **Reconciliation Results** appear. Since you are creating a new Access Code Set, all specified Listings are simply added to the Group.



To accept the following changes press the "Finish" button:

- 109 directory listings will be added.
- 0 directory listings remain unchanged.
- Resulting in a total of 109 directory listings.

11. Click **Finish**. The Listings appear on the **Access Codes** tab.



Access Code	Directory Listing	Last Modified
5150	Accounting Fax	08/02/2018 13:34:04
6307	Ackroyd, Dan	08/02/2018 13:34:04
4746	Adamez, Terry	08/02/2018 13:34:04
5471	ADP	08/02/2018 13:34:04
1984	Alda, Alan	08/02/2018 13:34:04
7884	Allen, Steve	08/02/2018 13:34:04
4674	AOL	08/02/2018 13:34:04
1668	Baldwin, Alec	08/02/2018 13:34:04
5099	Barton, Tim	08/02/2018 13:34:04
3503	Bell, Alex G	08/02/2018 13:34:04
3732	Berry, Halli	08/02/2018 13:34:04
8674	Brando, Marlan	08/02/2018 13:34:04
7716	Brown, Jim	08/02/2018 13:34:04
7703	Buntin, David	08/02/2018 13:34:04
8926	Byrne, Jane	08/02/2018 13:34:04

12. To add Access Codes to the Listings, do one of the following:

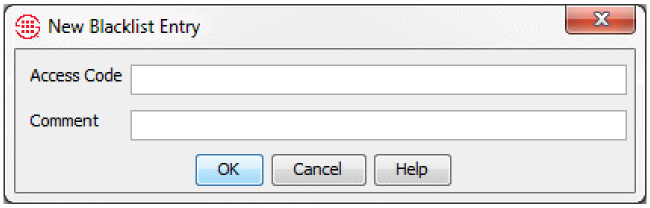
    - Click **Autogenerate**. The **Specify Entries** dialog box appears with **All Entries** selected. Click **OK**. An Access Code is generated for each Listing, according to the constraints you selected in the **Autogeneration Preferences** area on the **General** tab.

    - To manually assign an Access Code to a Listing, click the Listing and then click **Modify**. The **Access Code** dialog box appears. Type the Access Code, and then click **OK**. Repeat for each Listing.

Tip To select multiple Listings, hold down CTRL or SHIFT while clicking.

13. If you want to specify access codes that are never to be used with a Listing in this Access Code Set, click the **Blacklist** tab. If you do not want to blacklist any access codes, skip this step and see the next bullet.

    a. Click **Add**. The **New Blacklist Entry** dialog box appears.



    b. In the **Access Code** box, type the blacklisted access code.

    c. Optionally, in the **Comment** box, type the reason the access code was blacklisted, or any other comment.

    d. Click **OK**.

    e. Repeat for additional blacklisted access codes.

14. The **Switches** tab is used to view the Switch(es) with which this Access Code Set is associated, if more than one Access Code Set is defined on this Server.

    - If only one Access Code Set is defined for this Server, configuration is complete and you do not need to associate the Access Code Set with a Switch; it is assumed to be associated with all Switches on the Server.
    - If more than one Access Code Set is defined, you must associate each Access Code Set with the Switch at which the access codes are used before the Usage Manager can correlate access codes in call data with Listings. This is because the same Access Codes may be used at different Switches but be correlated with different Listings. See "Associating an Access Code Set with a Switch" on page 146 for instructions.

15. Click **OK** to save the Access Code Set and close the dialog box. All Listings must have an assigned Access Code before you can save the Access Code Set. See "Distributing Access Codes via Email" on page 145.

Distributing Access Codes via Email

You can distribute access codes to the email addresses of the Listings to which they belong. If any Listing in the Access Code Set lacks an email address, you are notified and given the option to abort the distribution to first supply the email address, or continue and skip those without email addresses.

To distribute Access Codes via email

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Access Code Sets** node.
2. Right-click the **Access Code Set** you want to distribute, and then click **Distribute**. An Access Code Notification is sent to the email address in each Listing in the set.

   The message below is an example of the default format:

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

Format of the Email Message

The format of the email message is defined in the **delivery.properties** file located in the ETM System installation directory on the ETM Server computer. See "Formatting the Access Code Set Distribution Email" in the *ETM® System Technical Reference* for instructions for modifying the content of the message.

Email Settings for Access Code Distribution

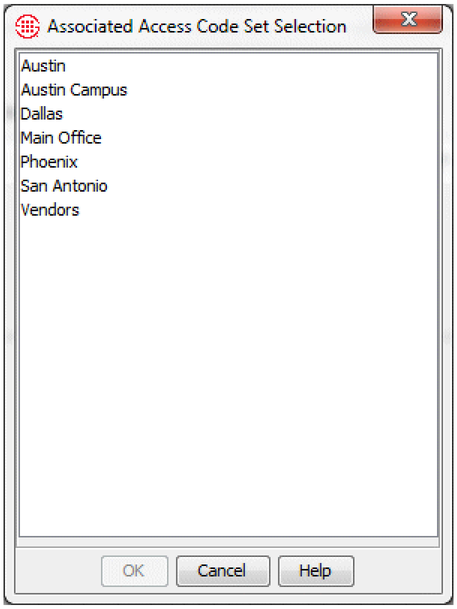
The **ETM Server Properties Tool** provides several properties that govern the number of messages sent at once, pause between batches sent, number of allowable errors during distribution, and the number of threads to be used. See "Access Code Import and Distribution Settings" in the *ETM® System Administration and Maintenance Guide* for details.

Associating an Access Code Set with a Switch

If more than one Access Code Set is defined in the Directory Manager, you must associate each Access Code Set with the Switch at which the access codes are used. This enables the Usage Manager to correlate Listings with the access codes in the call data. If only one Access Code Set is defined, it is assumed to be associated with all Switches on the Server and you do not need to perform this procedure. One Access Code Set can be associated with each Switch. However, multiple Switches can be associated with the same Access Code Set.

To associate an Access Code with a Switch

1. In the Performance Manager tree pane, right-click the Switch to which the Access Code Set applies, and then click **Edit Switch**. The **Switch Properties** dialog box appears.
2. Click the **Advanced** tab.
3. Under the **Associated Access Code Set** box, click **Modify**. The **Associated Access Code Set Selection** dialog box appears.



Austin
Austin Campus
Dallas
Main Office
Phoenix
San Antonio
Vendors

4. Click the Access Code Set associated with this Switch, and then click **OK**. Only one Access Code Set can be associated with a given Switch.
5. Click **OK** to save the changes and close the **Switch Properties** dialog box. A message appears to confirm applying changes. Click **OK**.

Importing Access Codes from a CSV File

If you have an external CSV file of access codes, you can import those access codes to apply to existing Listings, to initially create an Access Code Set. After the set is created, you should use the ETM Directory to maintain the access codes. You cannot update an Access Code Set via import.

Format of the Import File

For successful import, the CSV file must contain one entry per line, separated by commas, and contain the following fields in this order: **Last Name**, **First Name** (*can be null only if it is null in the Listing*), **Access Code**. Any other fields in the file are ignored. The **Last Name** and **First Name** fields can contain up to 50 characters and the **Access Code** field can contain up to 15 digits. Each entry in the file must correlate exactly with the **Last Name** and **First Name** field in an existing Directory Listing, or the entry is skipped during import.

How Importing Works

As mentioned above, each entry in the file must correlate exactly with the **Last Name** and **First Name** field in an existing Directory Listing, or the entry is skipped. If any of the records fails to match a Listing, a list of non-matched file entries is provided at the end of the import.

If an entry in the file matches more than one Directory Listing, a dialog box is provided for you to manually select the Listing to which the access code applies. If duplicate entries exist in the file, they are correlated and imported, but you must resolve the duplication before you can save the Access Code Set. This means you must determine which entry is correct and delete the extraneous entry.

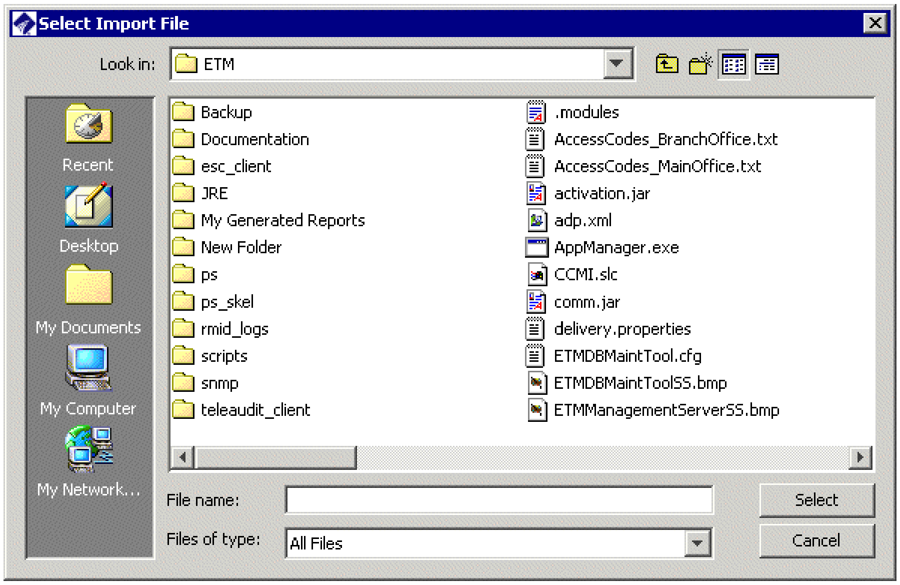
If, during import, the number of unique matched Listings exceeds the maximum of 10,000 allowed entries for an Access Code Set, you are provided the option to either complete the current import with the 10,000 matched Listings and not import the remainder, or abort the import so you can first divide the import file into smaller sets before importing.

The **ETM Server Properties Tool** provides settings that govern the allowable number of errors during an import. See "Access Code Import and Distribution Settings" in the *ETM® System Administration and Maintenance Guide* for instructions for viewing and modifying this threshold.

Importing Access Codes

To import access codes

1. Ensure that Listings exist that correlate with the entries in the import file. See "Format of the Import File" above for details.
2. In the Directory Manager tree pane, right-click **Access Code Sets** and click **Import**. The **Select Import File** dialog box appears.



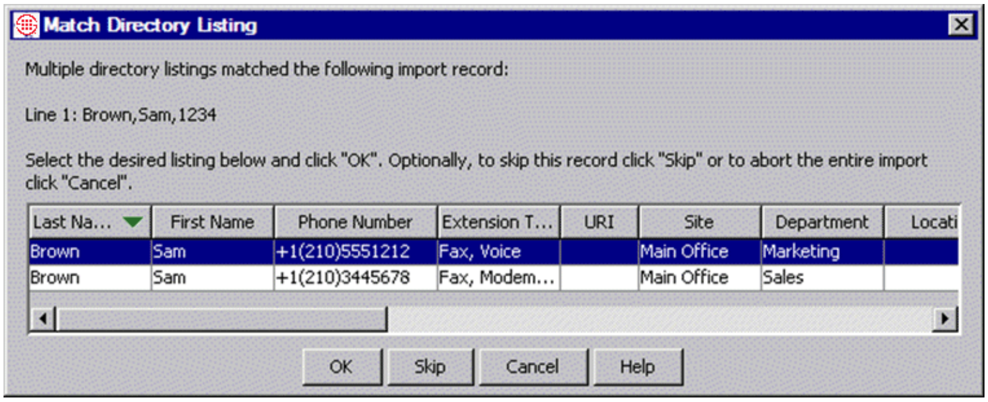
Look in: ETM

File name:

Files of type: All Files

3. Click the file that contains the access codes, and then click **Select**. The entries in the import file are correlated with the Listings in the Directory.

   - If duplicate matches are found, the **Match Directory Listing** dialog box appears.



Multiple directory listings matched the following import record:

Line 1: Brown,Sam,1234

Select the desired listing below and click "OK". Optionally, to skip this record click "Skip" or to abort the entire import click "Cancel".

Last Na...	First Name	Phone Number	Extension T...	URI	Site	Department	Locati
Brown	Sam	+1(210)5551212	Fax, Voice		Main Office	Marketing	
Brown	Sam	+1(210)3445678	Fax, Modem...		Main Office	Sales	

Do one of the following:

- Click the Listing to which you want to assign the Access Code, and then click **OK**.
- Click **Skip** to skip the record in the import file. No access code is assigned to any Listing for that record, but the other records are imported.
- Click **Cancel** to abort the import and correct the duplication before importing. If you click **Cancel**, skip the rest of this procedure; no Access Code Set is created.

4. The **New Access Code Set** dialog box appears, with the Access Codes tab populated with the Listings and their access codes.

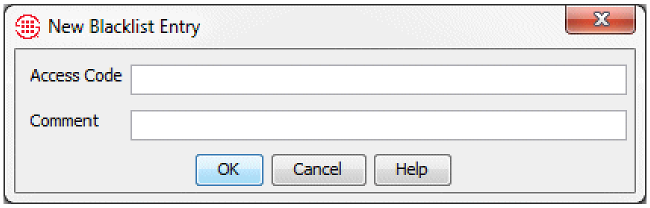
5. In the **Name** box, type a unique name for the Access Code Set.

6. Optionally, in the **Comments** box, type a descriptive comment about the Access Code Set, such as its purpose.

7. Optionally, to allow only users with both the **Access Policy Features** and **Manage Access Code Sets** user permissions to make changes to this Access Code Set, select the **Modifications require "Access Policy Features" permission** check box. To allow all users with **Manage Access Code Sets** permission to modify the Access Code Set, leave the check box cleared.

8. If you want to blacklist any Access Codes for this Access Code Set, click the **Blacklist** tab. If you do not want to blacklist any access codes, skip this step and see the next bullet.

   a. Click **Add**. The **New Blacklist Entry** dialog box appears.

   b. In the **Access Code** box, type the blacklisted access code.

   c. Optionally, in the **Comment** box, type the reason the access code was blacklisted, or any other comment.

   d. Click **OK**.

   e. Repeat for additional blacklisted access codes.

9. The **Switches** tab is used to view the Switch(es) with which this Access Code Set is associated, if more than one Access Code Set is defined on this Server. If only one Access Code Set is defined for this Server, configuration is complete and you do not need to associate the Access Code Set with a Switch; it is assumed to be associated with all Switches on the Server. If more than one Access Code Set is defined, you must associate each Access Code Set with the Switch at which the access codes are used before the Usage Manager can correlate access codes in call data with Listings. This is because the same Access Codes may be used at different Switches but be correlated with different Listings.

10. Click **OK** to save the Access Code Set and close the dialog box.

Exporting an Access Code Set

You can export access codes to a text file so that you can import them into your PBX. When you export the Access Code Set, an ASCII text file is created with a single access code per line.

To export an Access Code Set

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Access Codes** node.
2. Right-click the Access Code Set you want to export, and then click **Export**. The **Select Export File** dialog box appears for you to provide the file name and location to which to export the file. The location defaults to the ETM System installation directory, and the file name for the export file defaults to the name of the Access Code Set with the date and time appended, for example:

   ```
   Branch Office_08152005_142751.txt
   ```

3. Click **Select**. The file is exported.

Viewing a List of all Access Codes Sets and Their Properties

To view a list of Access Code Sets and their properties

- In the Directory Manager tree pane, click **Access Code Sets**.

The right pane updates with a table containing a list of Access Code Sets and their properties. Right-click an entry to access a menu with the following options:

- **New** opens the New Access Code Set dialog box.
- **Edit** opens the selected Access Code Set in the Access Code Set dialog box, where you can view details, add or remove Listings, generate new access codes, and so forth.
- **Delete** permanently deletes the Access Code Set.
- **Print** creates an Access Code Report in the **Print Preview** dialog box. The report contains the properties of the Access Code Set and its contents. Click the **Print** icon on the **Print Preview** dialog box to send the report to your default printer.
- **Distribute** emails the access codes to the email addresses associated with the Listings.
- **Import** enables you to import a CSV file of access codes to create a new Access Code Set.
- **Export** enables you to export the access codes in the selected Access Code Set to a text file for import into a PBX.

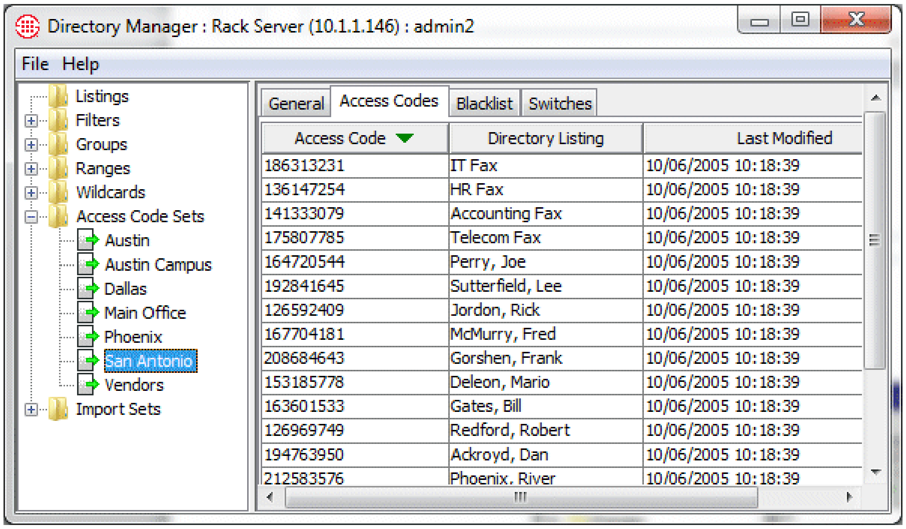
Adding Listings to an Access Code Set

When new Listings are added to the Directory, use the procedure below to associate them with an Access Code Set.

To add Listings to an Access Code Set

1. In the Directory Manager tree pane, click the **PLUS SIGN** next to **Access Code Sets** to expand the node.

2. Click the Access Code Set you want to edit. The Access Code Set opens in the right pane.



Access Code	Directory Listing	Last Modified
186313231	IT Fax	10/06/2005 10:18:39
136147254	HR Fax	10/06/2005 10:18:39
141333079	Accounting Fax	10/06/2005 10:18:39
175807785	Telecom Fax	10/06/2005 10:18:39
164720544	Perry, Joe	10/06/2005 10:18:39
192841645	Sutterfield, Lee	10/06/2005 10:18:39
126592409	Jordon, Rick	10/06/2005 10:18:39
167704181	McMurry, Fred	10/06/2005 10:18:39
208684643	Gorshen, Frank	10/06/2005 10:18:39
153185778	Deleon, Mario	10/06/2005 10:18:39
163601533	Gates, Bill	10/06/2005 10:18:39
126969749	Redford, Robert	10/06/2005 10:18:39
194763950	Ackroyd, Dan	10/06/2005 10:18:39
212583576	Phoenix, River	10/06/2005 10:18:39

3. Click the **Access Codes** tab.

   - To remove a Listing from the set, click the Listing and click **Remove**.

   - To add Listings to the set, click **Add**. The **Directory Listing Selection Wizard** appears, containing the filter criteria last used to add Listings to this set, if any. (If the set was imported from a file, no filter criteria appear.)

     - To retrieve new Listings that match the existing criteria, click **Next**. The matching Listings are retrieved. Click **Next**. A summary of the changes appears. Verify the results are as intended, and then click **Finish**. Any new Listings that match the criteria appear on the **Access Codes** tab.

     - To change the criteria for including Listings, click **Modify** and define the filter criteria. Note that this may result in Listings being removed from the Access Code Set if they no longer match the new criteria.

4. Assign an access code to each new Listing using the procedure in "Assigning Access Codes to Listings" on page 151.

5. Click **Apply** to save your changes. To discard unsaved changes, click **Revert**. Note that if you click **Revert**, all unsaved changes are discarded, not just the last action.

Assigning Access Codes to Listings

To assign new access codes to Listings

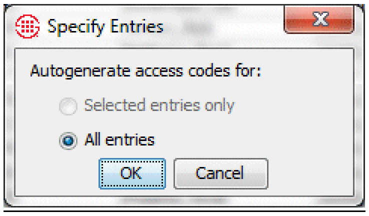
1. In the Directory Manager tree pane, click the **PLUS SIGN** next to **Access Code Sets** to expand the node.

2. Click the Access Code Set that correlates with the Listings to which you want to assign new Access Codes. The Access Code Set opens in the right pane.

3. Do one of the following:

   To autogenerate new codes for all Listings in the set

   a. Click **Autogenerate**. The **Specify Entries** dialog box appears with **All Entries** selected.

   Specify Entries

   Autogenerate access codes for:

   ○ Selected entries only

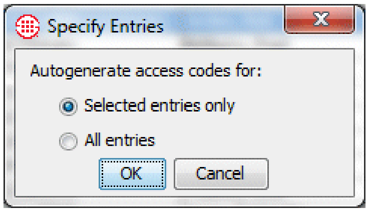
   ● All entries

   b. Click **OK**. A new code is generated for all of the Listings in the set, within the constraints set on the **General** tab. None of the previously assigned codes is reused for the set.

   To autogenerate new codes for selected Listings:

   a. Select the Listings for which you want to generate new codes. To select multiple Listings, hold down SHIFT (contiguous selection) or CTRL (noncontiguous selection) while clicking.

   b. Click **Autogenerate**. The **Specify Entries** dialog box appears with **Selected entries only** selected.

   Specify Entries

   Autogenerate access codes for:

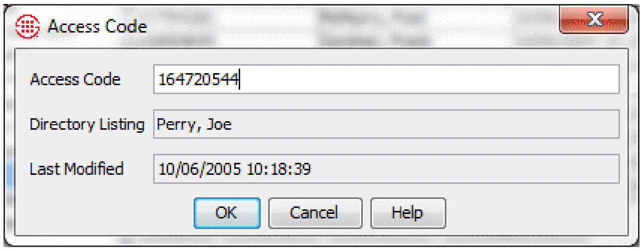
   ● Selected entries only

   ○ All entries

   c. A new code is generated for each selected entry, within the constraints set on the **General** tab. None of the previously assigned codes is reused for the set.

   To manually assign a new code to Listings in the set:

   a. Click a Listing, and then click **Modify**. The **Access Code** dialog box appears.


Access Code

Access Code: 164720544

Directory Listing: Perry, Joe

Last Modified: 10/06/2005 10:18:39

b. Type the new Access Code, and then click **OK**.

c. Repeat for each applicable Listing.

4. Click **Apply** to save your changes. To discard unsaved changes, click **Revert**.

Deleting an Access Code Set

To delete an Access Code Set

1. In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Access Code Sets** node.
2. Right-click the Access Code Set you want to delete and click **Delete**.

Viewing or Editing an Access Code Set

To view or edit an Access Code Set

- In the Directory Manager tree pane, click the **PLUS SIGN** to expand the **Access Code Sets** node. The Access Code Set opens in the right pane. The following options are available:
  - **Add** opens the **Directory Listing Selection Wizard** dialog box.
  - **Remove** removes the Listing(s) selected on the **Access Codes** tab from the Access Code Set. Only available when at least one Listing is selected.
  - **Autogenerate** generates a new access code for each selected Listing or for all Listings in the set, depending on selection.
  - **Apply** saves changes.
  - **Revert** discards all unsaved changes.
  - **Delete** permanently deletes the Access Code Set.
  - **Print** creates an Access Code Report in the **Print Preview** dialog box. The report contains the properties of the Access Code Set and its contents. Click the **Print** icon on the **Print Preview** dialog box to send the report to your default printer.
  - **Distribute** emails the access codes to the email addresses associated with the Listings.
  - **Export** enables you to export the Access Codes in the Access Code Set to a text file for import into a PBX.

Printing an Access Code Set Report

An Access Code Set report provides the following information:

- The name of the Access Code Set.
- The date/time it was created and by whom.
- The date/time it was last modified and by whom.
- The contents of the current filter for matching Directory Listings.
- A list of the Access Codes and their corresponding Listings.
- A list of any blacklisted Access Codes.
- The Switch with which the Access Code Set is associated, if any.

To print an Access Code Set report

Instead of right-clicking, you can click the **Print** button at the bottom of the editing pane after selecting the item to print.

1. Do one of the following:
   - In the **Access Code Sets** node of the Directory Manager tree pane, right-click the Access Code Set and click **Print**.
   - In the Directory Manager tree pane:
     a. Click the **Access Code Sets** node. A table appears in the editing pane listing all of the Access Code Sets.
     b. Right-click the Access Code Set, and then click **Print**.

   The **Print Preview** dialog box appears containing the report
2. Click the **Print** icon. The printer dialog box for your default printer appears. Print as you normally would.

Import Sets

Import Sets enable you to synchronize the phone numbers in your external phone number list or LDAP source with those in the ETM Directory. Two types of Import Sets are available: file-based and LDAP.

- File-based Import Sets allow you to manually import a text file of Listings.
- LDAP Import Sets allow you to schedule recurring imports of phone number Listings from your LDAP server.

File-Based Import Sets

File-based Import Sets are used to import text files of Listings into the ETM System and to easily keep the Listings up-to-date with your external phone number list. When changes occur, you update the text file and then reimport it into the Import Set. Up to 50 Import Sets can be maintained; each Import Set can contain a maximum of 100,000 Listings. Only Listings can be imported. Filters, Groups, Ranges, and Wildcards must be manually created.

Import Set Reconciliation

When you import a text file of Listings into an Import Set, the entries in the file are compared with the Listings in the Import Set in the database. This is called *reconciliation*. After reconciliation completes, any entries in the file that did not match an existing Import Set Listing are added to the Import Set as new Listings. Any Import Set Listings that did not match an entry in the file are deleted from the database.

A copy of the text file you import is created in the Import Sets directory of the ETM Server installation directory. Each Import Set has its own subdirectory. The file is called **reconcile.txt**.

To determine whether the entry in the text file matches an existing Listing in the Import Set, the following reconciliation criteria are applied to each entry in the file in the order shown here:

1. First Name, Last Name, Dept., Phone Number
2. First Name, Last Name, Dept.
3. First Name, Last Name
4. First Name, Dept., Phone Number
5. Phone Number

If an entry in the file matches an Import Set Listing according to any of these criteria, a match is found and any fields in the matched Listing that differ from those in the file entry are updated.

IMPORTANT NOTES

- **Only Listings within the selected Import Set are considered**. Manual Listings and Listings within other Import Sets are not considered when reconciliation is performed.
- **Values are never overwritten with nulls**. That is, if a matching entry in the file has no value in a field for which the existing Listing has a value, the value in the Listing is retained. It is not updated to be null. For example, suppose a given phone number is being reassigned from an individual named Joe Smith to the PBX Maintenance Port. If you change the **Last Name** field in the import file to "PBX Maint Port" but simply delete the value from the **First Name** field, the Listing is updated as `PBX Maint Port, Joe,...`. To avoid this, specify a value in any field that you want to be changed from its current value. In the previous example, you might type `NA` or `Service Tech Access`.
- **By default, duplicate entries in the file are processed**. If you want duplicates to be discarded, see "Discarding Duplicate Entries in an Import File" in the *ETM® System Administration and Maintenance Guide*.

Consider the following examples:

Reconciliation Examples

Existing Listing	Data File Entry	Criteria Matched?	Result
Jones, **Bill**, **1(210)555-9000**, SATX, **Boiler Room Tech**, Main Office, P8406, bill.jones@xyzabc.com, 78240	**Jones**, **Bill**, **1(210)555-9000**, SATX, **Boiler Room Tech**, Basement, P9000, bjones@xyzabc.com, 78240	1	The Listing is updated with the changed email address, authorization number, and location from the file entry.
Doe, **Pat**, 1(210)555-1212, SATX, **Customer Service**, Main Office, P8406, pdoe@xyzabc.com, 78240	**Doe**, **Pat**, 1(214)555-2222, DFW, **Customer Service**, Branch Office, D8406, pdoe@xyzabc.com, 75208	2	The Listing is automatically updated with the new phone number, site, location, and authorization number from the file entry.
Perez, **Sue**, 1(210)555-1212, SATX, Customer Service, Main Office, P8406, pperez@xyzabc.com, 78240	**Perez**, **Sue**, 1(214)555-2222, DFW, Mail Room, West Campus, Q6714, sue.perez@xyzabc.com, 78208	3	All of the fields in the Listing other than First Name and Last Name are updated from the file entry.
Martin, **Jane**, **1(210)555-7000**, SATX, **Engineering**, Main Office, P6784, jmartin@xyzabc.com, 78240	Rogers, **Jane**, **1(210)555-7000**, SATX, **Engineering**, Contract Ofc, Z6784, jrogers@xyzabc.com, 78213	4	All of the fields in the Listing that differ are updated from the file entry.
Gonzales, Jose, **1(210)555-4000**, SATX, Engineering, East Campus, R7496, ggonzales@xyzabc.com, 78201	Campos, Darlene, **1(210)555-4000**, SATX, Mail Room, Main Office, Q5467, dcampos@xyzabc.com, 78240	5	All of the fields other than Phone Number are updated from the file entry
Wilke, Darla, 1(210)555-8721, SATX, Engineering, East Campus, R6784, dwilke@xyzabc.com, 78201	Wilke, Darla, 1(210)555-8721, SATX, Engineering, East Campus, R6784, dwilke@xyzabc.com, 78201 and Mann, Horace, 1(210)555-8721, SATX, Telco Tech, East Campus, R6784, hmann@xyzabc.com, 78201	First entry matches 1, second entry matches 5.	Since the criteria are applied in the order listed above, the Wilke, Darla Listing matches and a new Listing is created for Mann, Horace, with the same phone number as Wilke, Darla. **Note:** By default, duplicate phone numbers in an Import Set are permitted. If you want to disallow duplicate phone numbers, see the *ETM*® *System Technical Reference* for instructions.

Collisions

When two entries in the file potentially match the same Listing, a *collision* is said to occur. When a collision occurs, you are prompted to select which of the similar Import Set Listings, if any, matches the entry in the file. Or, you can specify that the file entry become a new database entry.

Only the reconciliation criteria discussed in "Import Set Reconciliation" on page 155 trigger collisions. Other fields in the Listing are not considered.

Consider the following example:

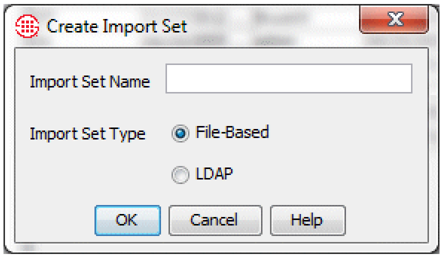
Existing Listing	Potential Matches in File	Result
Jones, **Bill**, **1(210)555-9000**, SATX, Boiler Room Tech, Main Office, P8406, bill.jones@xyzabc.com, 78240	**Jones**, **Bill**, **1(210)555-9000**, SATX, Mailroom, Basement, P9000, bjones@xyzabc.com, 78240 **Jones**, **Bill**, **1(210)555-9000**, SATX, Engineering, Main Office, P9000, bjones@xyzabc.com, 78240	You are prompted to select whether the first entry matches the Listing or should be created as a new Listing. If you determine that it matches the Listing, the Listing is updated to match the entry and the second entry is created as a new Listing.

After reconciliation completes, any entries in the file that did not match an existing Import Set Listing are added as new Listings. Any Import Set Listings that did not match an entry in the file are deleted from the database.

Creating a File-Based Import Set

To create a file-based Import Set

1. In the Directory Manager tree pane, right-click **Import Sets** and click **New**. The **Create Import Set** dialog box appears.



Create Import Set

Import Set Name

Import Set Type ● File-Based ○ LDAP

2. In the **Import Set Type** area, select **File-Based**.
3. Type a name for the Import Set of up to 32 characters. The name can include letters, digits, spaces, and the following special characters: **& ( ) . ! ' + = @**
4. Click **OK**. The Import Set appears in the **Import Sets** node of the Directory Manager tree pane. To import Listings into the Import Set, see "Importing a Text File of Listings" on page 162.

Formatting the File for Import

When you import Listings from a text file into the Directory Manager, the text file must be formatted in a certain way for successful import.

For successful import, each entry in the text file to be imported must be on a separate line, with no blank lines between entries. By default, each entry consists of the following fields in the order listed here, separated by commas. If a field is not required, you can use an empty set of commas to denote that field. Only **Last Name** and **Local Number** are required. See "Changing the Order of Fields/Delimiter" on page 160.

Field	Contents
Last Name	Up to 50 characters and spaces, including letters, digits, and special characters other than double quotes (")
First Name	Up to 50 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.
Country Code	1 to 3 digits.
Area Code	1 to 8 digits.
Local Number	1 to 36 digits. Any punctuation in the number is discarded during import.
Site	Up to 100 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.
Department	Up to 100 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.
Location	Up to 100 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.
Authorization Number	Up to 100 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.
Email Address	Up to 100 characters.
Mail Code	Up to 100 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.
Comment	Up to 255 characters and spaces, including letters, digits, and special characters other than double quotes (") or commas.

Formatting the Import File, continued

<table>
<tr><th>Field</th><th colspan="2">Contents</th></tr>
<tr><td rowspan="7">Extension Type(s)</td><td colspan="2">Type one or more of the following characters in uppercase to indicate the extension type(s): Invalid characters and duplicates are ignored. The order of multiple entries is not important. Do not use commas between multiple entries. For example, to denote Modem and Fax, type `MF` or `FM`.</td></tr>
<tr><td><b>Character</b></td><td><b>Denotes</b></td></tr>
<tr><td>V</td><td>Voice</td></tr>
<tr><td>M</td><td>Modem</td></tr>
<tr><td>D</td><td>Data</td></tr>
<tr><td>F</td><td>Fax</td></tr>
<tr><td>S</td><td>STU-III</td></tr>
<tr><td>Custom1</td><td colspan="2">The first user-defined field in the Listing, labeled Custom1 by default but able to be renamed.</td></tr>
<tr><td>Custom2</td><td colspan="2">The second user-defined field in the Listing, labeled Custom2 by default but able to be renamed.</td></tr>
<tr><td>Custom3</td><td colspan="2">The first user-defined field in the Listing, labeled Custom1 by default but able to be renamed.</td></tr>
<tr><td>URI1</td><td colspan="2">The first URI associated with the Listing.</td></tr>
<tr><td>URI2</td><td colspan="2">The second URI associated with the Listing.</td></tr>
<tr><td>URI3</td><td colspan="2">The third URI associated with the Listing.</td></tr>
<tr><td>URI4</td><td colspan="2">The fourth URI associated with the Listing.</td></tr>
<tr><td>URI5</td><td colspan="2">The fifth URI associated with the Listing.</td></tr>
</table>

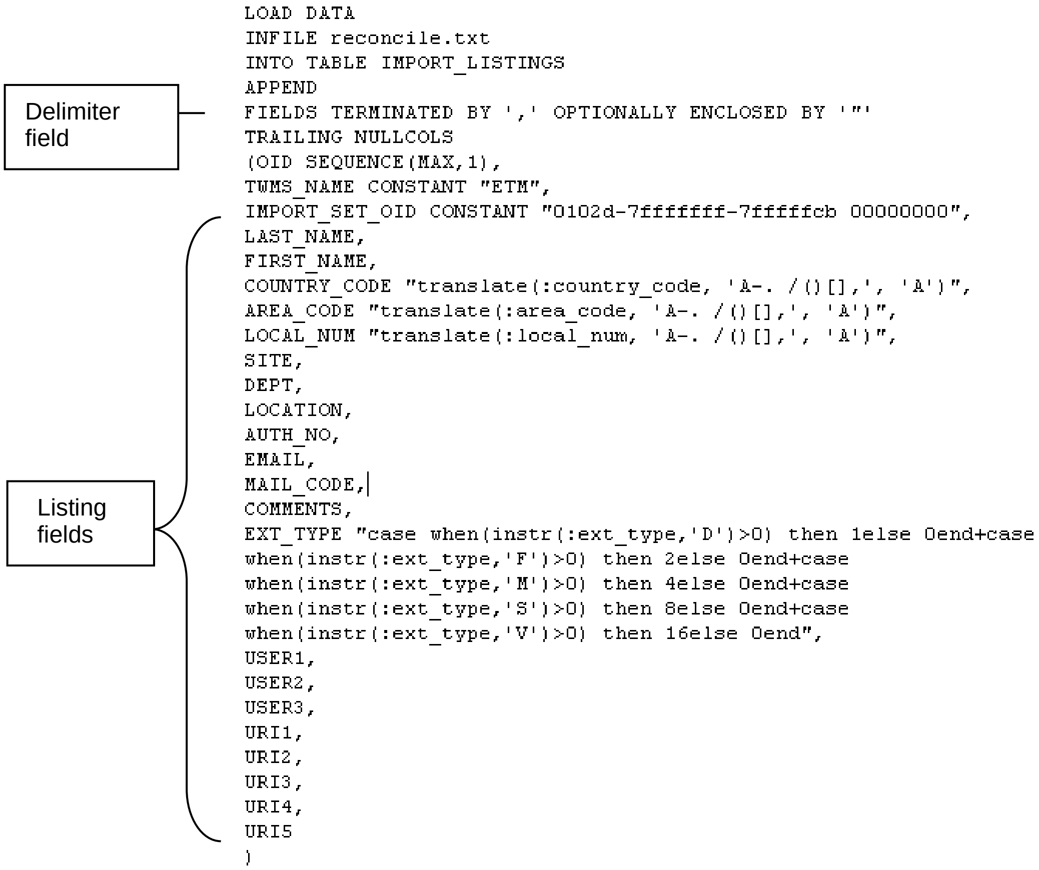
Changing the Order of Fields/Delimiter

The required format for the import text file is determined by a SQL*Loader control file in the ETM$^{®}$ System installation directory. Each Import Set uses its own copy of this file. This copy is created when you create a new Import Set. If the fields in the import file are in a different order from the **reconcile.ctl** file or are delimited by tabs instead of commas, you can edit this file after you create the Import Set but before you import the Listings.

When you create a new Import Set, a system-named Import Set Directory is created in the **ps\Directory\import_sets** directory of the ETM System installation directory—for example, **C:\Program Files\SecureLogix\ETM \ps\Directory\import_sets\0102d-7fffffff-7ffffec 00000002**. A text file in this directory named **import_set_details.txt** identifies the Import Set by the name you gave it in the GUI.

In each Import Set directory, the file **reconcile.ctl** defines the required format for imported file(s). This is the file you edit to change the order of the fields or the delimiter.

When a new Import Set is created, the following is the default format of the **reconcile.ctl** file.



```
LOAD DATA
INFILE reconcile.txt
INTO TABLE IMPORT_LISTINGS
APPEND
FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '"'
TRAILING NULLCOLS
(OID SEQUENCE(MAX,1),
TWMS_NAME CONSTANT "ETM",
IMPORT_SET_OID CONSTANT "0102d-7fffffff-7fffffcb 00000000",
LAST_NAME,
FIRST_NAME,
COUNTRY_CODE "translate(:country_code, 'A-. /()[],', 'A')",
AREA_CODE "translate(:area_code, 'A-. /()[],', 'A')",
LOCAL_NUM "translate(:local_num, 'A-. /()[],', 'A')",
SITE,
DEPT,
LOCATION,
AUTH_NO,
EMAIL,
MAIL_CODE,
COMMENTS,
EXT_TYPE "case when(instr(:ext_type,'D')>0) then 1else 0end+case
when(instr(:ext_type,'F')>0) then 2else 0end+case
when(instr(:ext_type,'M')>0) then 4else 0end+case
when(instr(:ext_type,'S')>0) then 8else 0end+case
when(instr(:ext_type,'V')>0) then 16else 0end",
USER1,
USER2,
USER3,
URI1,
URI2,
URI3,
URI4,
URI5
)
```

The order in which the Listing fields appear in this file is the order in which they must appear in the text file to be imported. The **Delimiter** field specifies the character that separates the fields.

To change the order of the fields and/or the delimiter

1. Open **reconcile.ctl** in a text editor.
2. Arrange the Listing fields in the order that they appear in the text file to be imported.

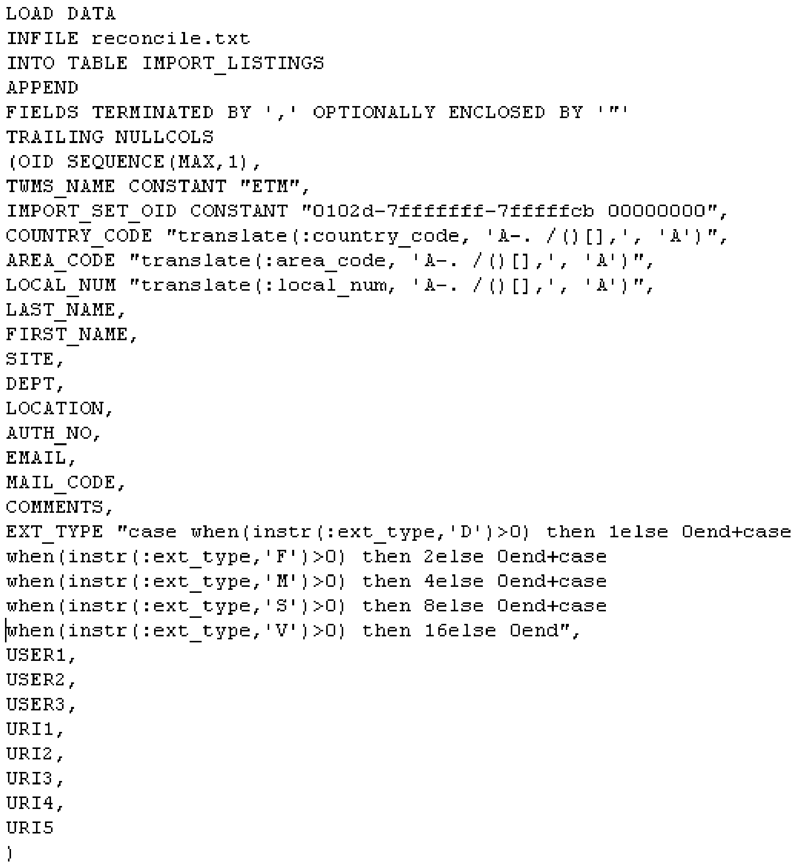
   For example, if the fields in the text file are arranged as follows:

   ```
   COUNTRY_CODE,AREA_CODE,LOCAL_NUM,LAST_NAME,FIRST_NAME
   ,SITE,DEPT,LOCATION,AUTH_NO,EMAIL,MAIL_CODE,COMMENTS,
   EXT_TYPE,USER1,USER2,USER3,URI1,URI2,URI3,URI4,URI5
   ```

   you would arrange the fields as shown in the illustration below.

Making a backup copy of any file you intend to edit is good practice.

IMPORTANT Do not edit any text in the file except the delimiter. Do not rearrange the first nine lines.



Do not rearrange the first 9 lines

```
LOAD DATA
INFILE reconcile.txt
INTO TABLE IMPORT_LISTINGS
APPEND
FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '"'
TRAILING NULLCOLS
(OID SEQUENCE(MAX,1),
TWMS_NAME CONSTANT "ETM",
IMPORT_SET_OID CONSTANT "0102d-7fffffff-7fffffcb 00000000",
COUNTRY_CODE "translate(:country_code, 'A-. /()[],', 'A')",
AREA_CODE "translate(:area_code, 'A-. /()[],', 'A')",
LOCAL_NUM "translate(:local_num, 'A-. /()[],', 'A')",
LAST_NAME,
FIRST_NAME,
SITE,
DEPT,
LOCATION,
AUTH_NO,
EMAIL,
MAIL_CODE,
COMMENTS,
EXT_TYPE "case when(instr(:ext_type,'D')>0) then 1else 0end+case
when(instr(:ext_type,'F')>0) then 2else 0end+case
when(instr(:ext_type,'M')>0) then 4else 0end+case
when(instr(:ext_type,'S')>0) then 8else 0end+case
when(instr(:ext_type,'V')>0) then 16else 0end",
USER1,
USER2,
USER3,
URI1,
URI2,
URI3,
URI4,
URI5
)
```

3. In the line that begins `FIELDS TERMINATED BY`, the comma (**,**) indicates that the text file you will import is a comma-separated values (CSV) file. If the text file you want to import is TAB delimited, replace the comma with: **\t**.
4. Click **Save**.

Importing a Text File of Listings

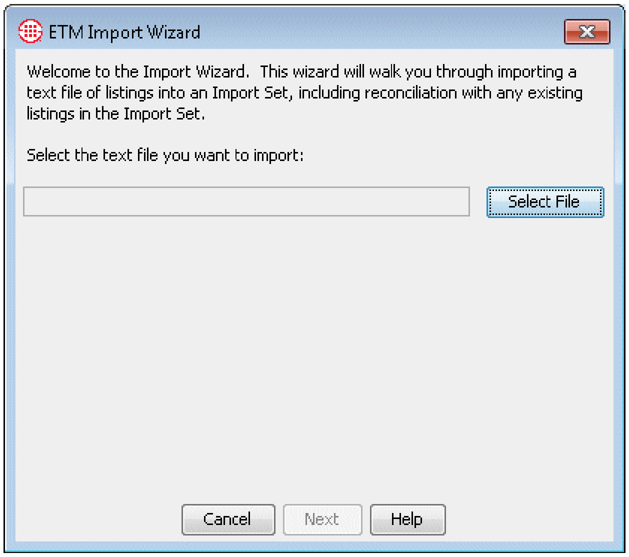
See "Formatting the File for Import" on page 159 for information about how the entries in the text file must be formatted for successful import.

To import Listings from a text file

1. In the Directory Manager tree pane, click the Import Set into which you want to import the Listings.

The **Import Wizard** uses an Oracle utility called **SQL*Loader**, which resides on the Management Server computer. The path to **SQL*Loader** is typically specified during installation. If you receive a **SQL*Loader** error when launching the wizard, see "Configuring the Import Wizard" on page 177.

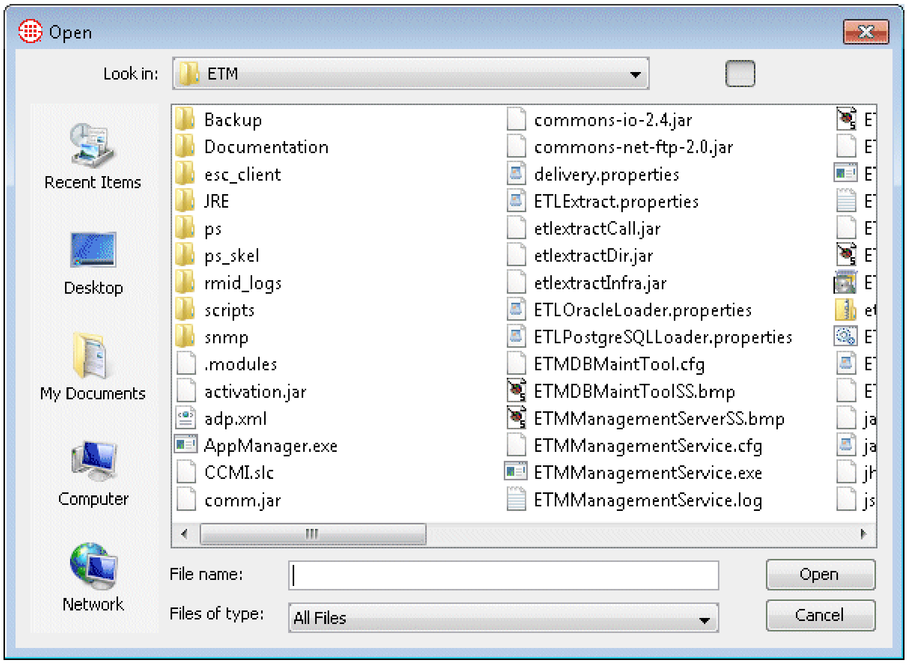
2. Click **Import Wizard**. The **ETM Import Wizard** appears.



Welcome to the Import Wizard. This wizard will walk you through importing a text file of listings into an Import Set, including reconciliation with any existing listings in the Import Set.

Select the text file you want to import:

3. Click **Select File**. The **Open** dialog box appears.



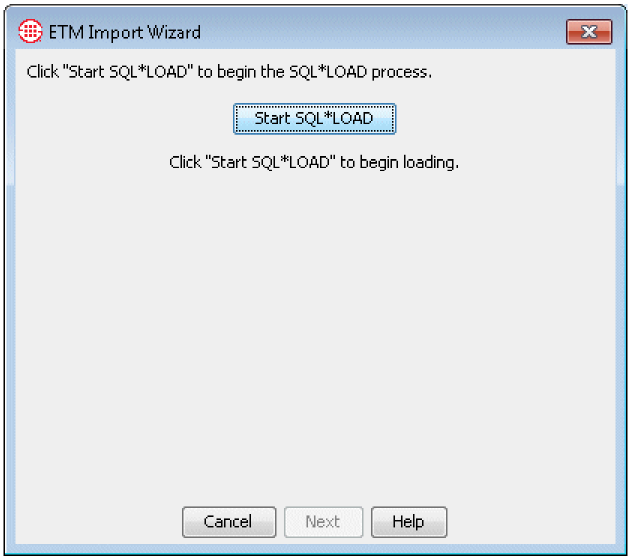
Look in: ETM

Files of type: All Files

4. Browse for and select the file, and then click **Open**.

5. Click **Next**. The file is copied to the Management Server. When the download completes, the message **File Successfully Downloaded** appears.

6. Click **OK**.



Click "Start SQL*LOAD" to begin the SQL*LOAD process.

Click "Start SQL*LOAD" to begin loading.

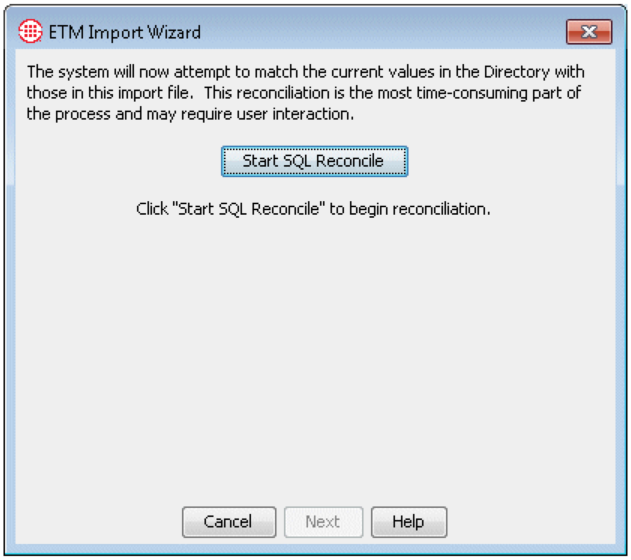
7. Click **Start SQL Load** to start the SQL*Loader process that processes the data.

8. When complete, the **SQL*Loader Results** dialog box appears displaying the SQL*Loader log file.

   See "Contents of the SQL*Loader Log File" on page 168 for a description of the contents of this file.

   - If desired, you can print the SQL*Loader log file for review. To print the file, click the **Print** icon on the **SQL*Loader Results** dialog box.

9. After reviewing and/or printing the log file, click **Close**, and then click **Next**.



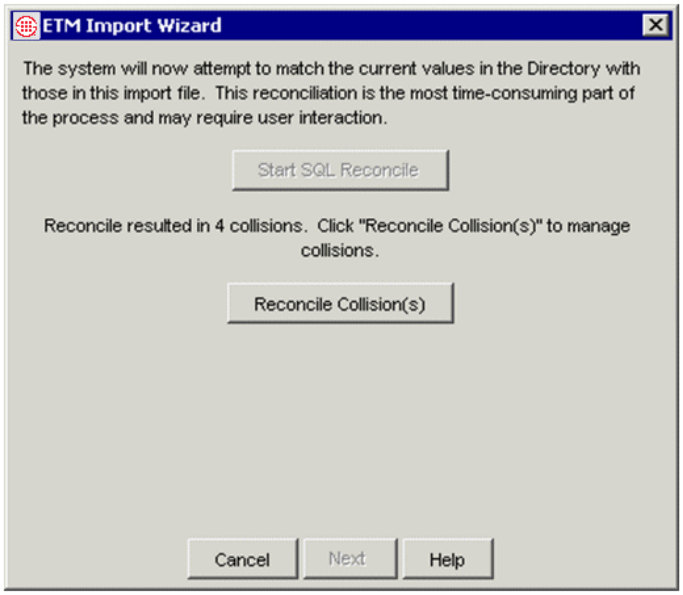
The system will now attempt to match the current values in the Directory with those in this import file. This reconciliation is the most time-consuming part of the process and may require user interaction.

Click "Start SQL Reconcile" to begin reconciliation.

See “Collisions” on page 158.

10. Click **Start SQL Reconcile** to begin matching the Listings in the Import Set in the database with the entries in the file. This process may take some time to complete, depending on the number of Listings that must be reconciled.

    - If two or more Listings in the import file are potential matches for an existing Listing in the Import Set, a *collision* occurs. If a collision occurs, a **Reconcile Collision(s)** button appears.

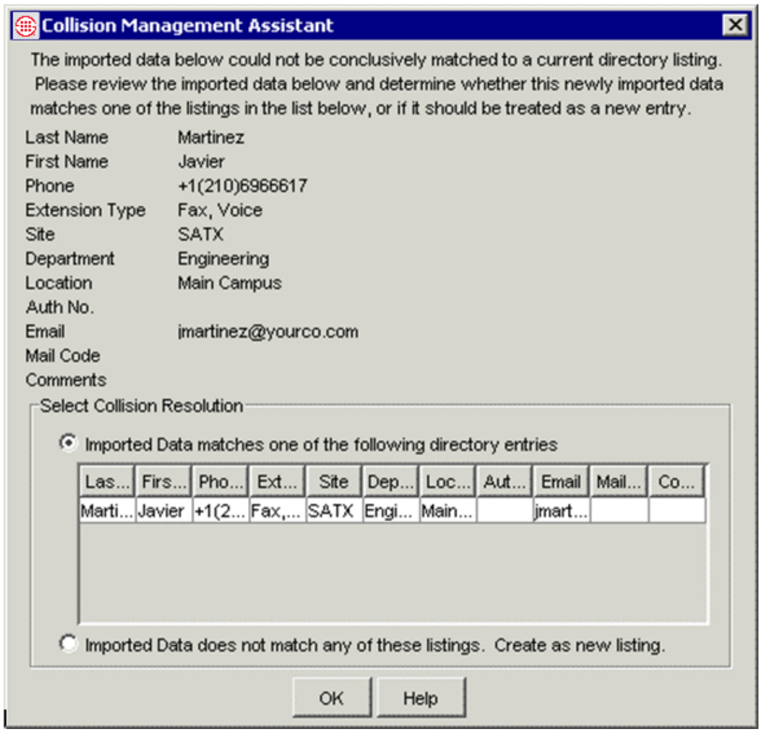


The system will now attempt to match the current values in the Directory with those in this import file. This reconciliation is the most time-consuming part of the process and may require user interaction.

Reconcile resulted in 4 collisions. Click "Reconcile Collision(s)" to manage collisions.

a. Click **Reconcile Collision(s)**.

The **Collision Management Assistant** dialog box appears.



Collision Management Assistant

The imported data below could not be conclusively matched to a current directory listing. Please review the imported data below and determine whether this newly imported data matches one of the listings in the list below, or if it should be treated as a new entry.

Last Name	Martinez
First Name	Javier
Phone	+1(210)6966617
Extension Type	Fax, Voice
Site	SATX
Department	Engineering
Location	Main Campus
Auth No.	
Email	jmartinez@yourco.com
Mail Code	
Comments	

Select Collision Resolution

● Imported Data matches one of the following directory entries

Las...	Firs...	Pho...	Ext...	Site	Dep...	Loc...	Aut...	Email	Mail...	Co...
Marti...	Javier	+1(2...	Fax,...	SATX	Engi...	Main...		jmart...		

○ Imported Data does not match any of these listings. Create as new listing.

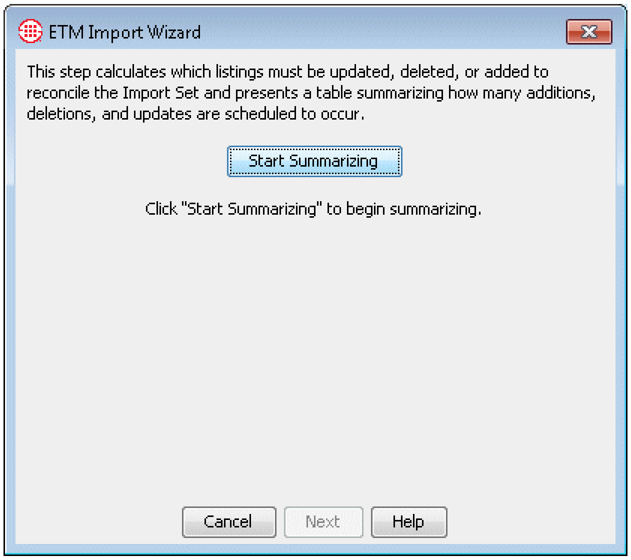
b. Do one of the following:

- If one of the Listings in the **Select Collision Resolution** area matches the imported data, select **Imported Data matches one of the following Directory Entries,** click the matching Listing, and then click **OK**.

- If none of the Listings in the **Select Collision Resolution** area match the imported data, select **Imported Data does not match any of these Listings. Create as new Listing**, and then click **OK**.

c. Repeat Step b above for each collision.

11. Click **Next** to continue.

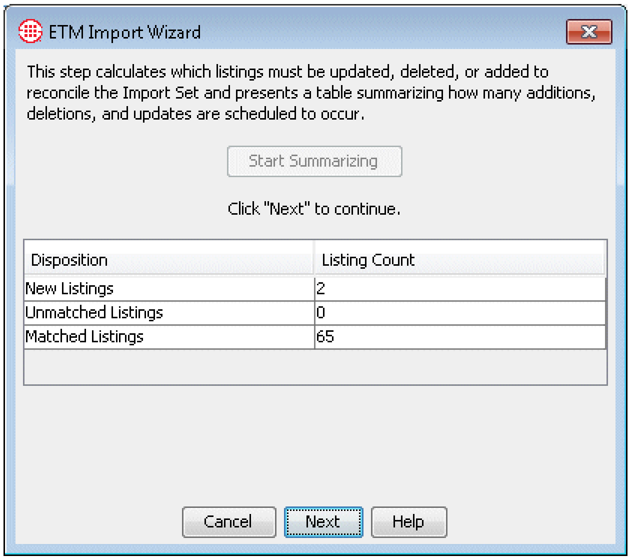


This step calculates which listings must be updated, deleted, or added to reconcile the Import Set and presents a table summarizing how many additions, deletions, and updates are scheduled to occur.

Click "Start Summarizing" to begin summarizing.

12. Click **Start Summarizing** to calculate which Listings must be updated, deleted, or added to reconcile the Import Set. When summarizing is complete, a table appears listing the number of scheduled additions, deletions, and updates.

    - **New Listings** are entries in the file that do not match any Listings in the database. These entries will be added to the database as new Listings.
    - **Unmatched Listings** are Listings currently in the database that do not match any entry in the file. These Listings will be deleted from the database.
    - **Matched Listings** are Listings that are currently in the database and match an entry in the file. These will be updated to match any updates in the file entries.

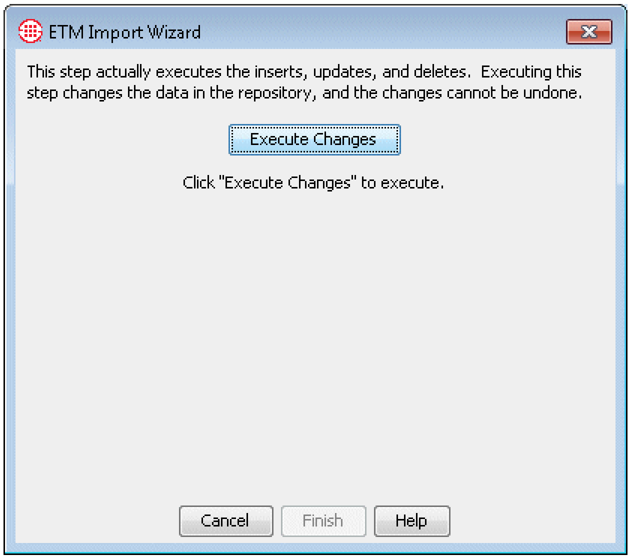


This step calculates which listings must be updated, deleted, or added to reconcile the Import Set and presents a table summarizing how many additions, deletions, and updates are scheduled to occur.

Click "Next" to continue.

Disposition	Listing Count
New Listings	2
Unmatched Listings	0
Matched Listings	65

13. Review the table, and then click **Next**.



This step actually executes the inserts, updates, and deletes. Executing this step changes the data in the repository, and the changes cannot be undone.

Click "Execute Changes" to execute.

14. Click **Execute Changes** to actually modify the values in the Import Set in the database with the reconciled import data. After you execute changes, the data in the repository is changed and you cannot undo the changes or cancel the import.

15. Click **Finish** to exit the Import Wizard.

*Contents of the SQL*Loader Log File*

When you use the **Import Wizard** to import a text file of Listings into the Directory Manager, an Oracle utility called **SQL*Loader** performs the data transfer. When the transfer is complete, a SQL*Loader log file appears in the **SQL*Loader Results** dialog box. This log file contains the following information:

- The first section provides information about the configuration of the files and database tables SQL*Loader uses, including the expected format of the data in the import file. See "Formatting the File for Import" on page 159 and "Changing the Order of Fields/Delimiter" on page 160 for more information.
- The second section lists any records rejected for errors encountered during import, by record number, and provides a description of the error (e.g., non-numeric characters in a numeric field or excessive length of a field value). These records are not inserted and reconciled. You can either cancel the import and address the errors, or continue with the import, and then correct the errors and reimport the file.
- The third section lists:
  - The count of rows in the file that were successfully loaded into the database. SQL*Loader inserts the data into a table called IMPORT_LISTINGS, from which the ETM System performs the reconciliation.
  - The count of entries that were not loaded because of data errors (matches the list in the second section).
  - "Rows not loaded because all WHEN clauses were failed" is unlikely to have a value.
  - "Rows not loaded because all fields were null" does not apply and will never have a value.
- The fourth section provides internal database information.
- The next section lists the number of records read and of those, the number rejected (not loaded).
- The remaining sections provide time information about the import.

LDAP Import Sets

The ETM Server can act as an LDAP client and request automated, scheduled imports of data from an LDAP server with which to update the ETM Directory Manager. Up to 100,000 Listings can be imported into a single Import Set. The ETM Server is designed to be compatible with any LDAP v3 data store and was tested with Sun ONE Directory.

Each time the ETM Server synchronizes with the LDAP server, all matching data is downloaded, not just entries that have changed. This can create significant network traffic, depending on the size of the data set. Therefore, it is strongly recommended that you schedule the synchronization for off-peak hours, such as afterhours or weekends.

IMPORTANT The phone numbers the LDAP server sends to the ETM Server must fully-qualified with a country code, area code, and local number, or the ETM Server cannot parse them. Non-numeric separators are ignored.

Secure LDAP Communication

If your organization requires a secure tunnel for LDAP communication to the ETM Server, you can set up a secure LDAP proxy server on the ETM Server host computer. You then configure the ETM Server, which acts as an LDAP client, to connect to that proxy server instead of directly to the LDAP server. You can then configure the LDAP proxy to communicate with the LDAP server via SSL, using any third-party encryption scheme. See the documentation for your LDAP proxy server and LDAP server for instructions for configuring them.

Unique Key for Automated Reconciliation

Since LDAP imports are designed for unattended Directory Manager updates, it is imperative that each record provide a unique identifier for correlating records in the database with entries in the import data. If the DN is known to be unique in your LDAP server, it can be used. However, since the DN can be mutable, it is recommended that a different attribute that is known to be unique for each record be used as the unique identifier, if one is available or can be provided. Each entry must contain a value for the unique identifier specified. The attribute specified as the unique identifier may be multi-valued.

Synchronization, System Events, and Logging

Each time synchronization occurs, all entries specified for the Import Set are downloaded and reconciled with the existing entries in the ETM Directory, using the unique identifier. Matching Listings are updated, unmatched Listings are deleted, and new entries in the import data are added as Listings to the Import Set. If synchronization affects a Policy, the Dirty Policy indicator appears next to the affected Policy and the following System Event is generated in the Diagnostic Log: **Dirty Policies Found After Automatic Directory Import.**

You can add a Track to this System Event so appropriate personnel are notified when synchronization causes a Dirty Policy. Since the synchronization is typically automated, no Dirty Policy message dialog box is presented.

In addition to the Dirty Policy System Event, the following mechanisms provide feedback on synchronization errors:

- The **Auto Directory Import Failure** System Event is triggered when a synchronization fails for any reason, such as an unavailable LDAP server, bad username/password, reconciliation failure, and the like. The reason for the failure is provided with as much detail as is available.
- When a synchronization fails, the icon for the Import Set is overlaid with a red **X** to visually indicate the failure.
- Errors are logged in the Diagnostic Log.

Criteria that Cause an Entry to be Rejected

Certain conditions cause an LDAP entry to be rejected during import. The rejected entry is skipped and the import continues. Rejected records are written to a file, along with the reason it was rejected. The file, called **exceptions.txt**, is stored in the ETM Server installation directory and can also be accessed via the **Show Diagnostic Logs** button on the Import

Set's dialog box. You can review these records and correct the issues in the LDAP repository for future import.

Conditions that cause an entry to be rejected include:

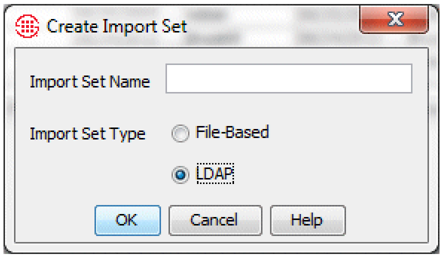
- An entry has no value for the attribute mapped to the **Last Name** or **Phone Number** fields.
- The value retrieved for **Last Name** is an unprintable value.
- The value retrieved for **Phone Number** is not in a normalized format (e.g., +1 (210) 402-9669).
- The DN or the attribute specified as the Unique Identifier, whichever is used, returns multiple values.

Creating an LDAP Import Set

You must have **Access Policy Features** user permission to create LDAP Import Sets.

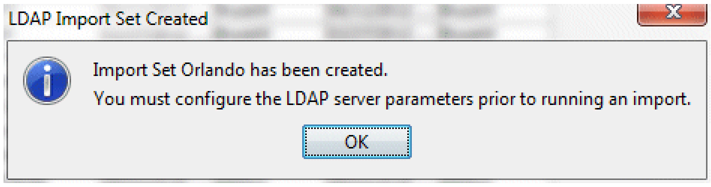
To create an LDAP Import Set

1. In the Directory Manager tree pane, right-click **Import Sets** and click **New**. The **Create Import Set** dialog box appears.



2. In the **Import Set Name** box, type a unique identifier for the Import Set.
3. In the **Import Set Type** area, select **LDAP**.
4. Click **OK**. The Import Set is created and appears in the tree pane with a red **X** over its icon, indicating that it is not yet configured with LDAP server parameters. The following message appears:

LDAP Import Set Unconfigured or with Synch Error

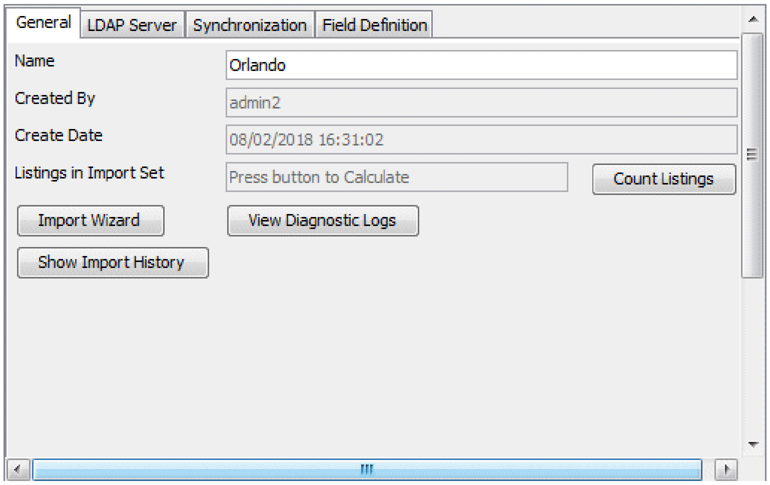


Import Set Orlando has been created.
You must configure the LDAP server parameters prior to running an import.

5. Click **OK**.

6. In the Directory Manager tree pane, click the newly created Import Set. It opens in the right pane with the **General** tab selected. The name you typed appears in the **Name** box.

Note If you are using a secure LDAP proxy, supply its information on the **LDAP Server** tab, rather than the LDAP server's information.



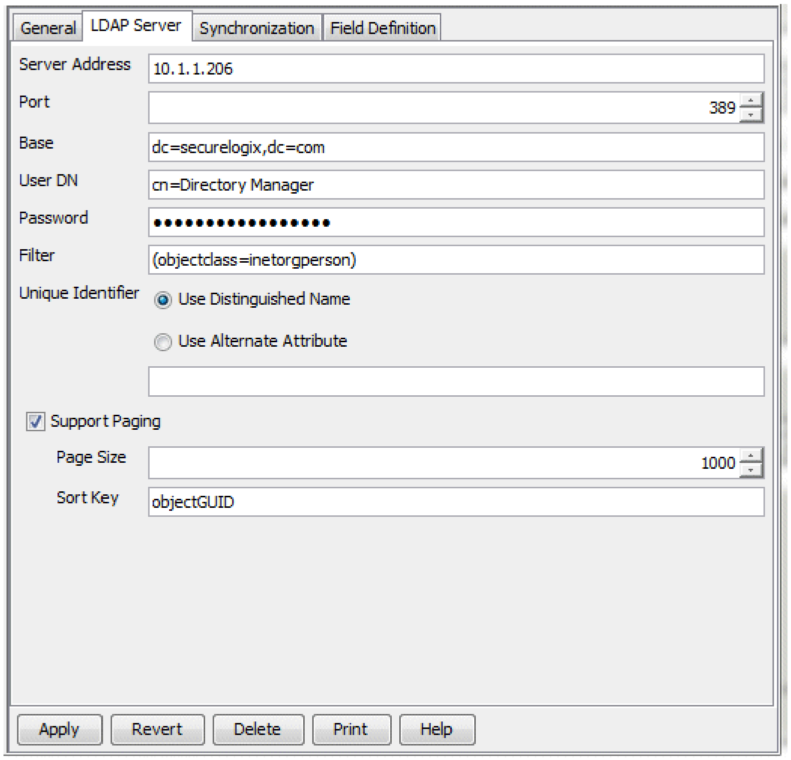
Name: Orlando

Created By: admin2

Create Date: 08/02/2018 16:31:02

Listings in Import Set: Press button to Calculate

7. Click the **LDAP Server** tab.



Server Address: 10.1.1.206

Port: 389

Base: dc=securelogix,dc=com

User DN: cn=Directory Manager

Password: ●●●●●●●●●●●●●●●●●

Filter: (objectclass=inetorgperson)

Unique Identifier: ● Use Distinguished Name ○ Use Alternate Attribute

☑ Support Paging

Page Size: 1000

Sort Key: objectGUID

8. In the **Server Address** box, type the IP address of the LDAP server.

9. In the **Port** box, type or select the TCP/IP port on which the ETM Server is to communicate with the LDAP server.

10. In the **Base** box, type the base object that defines where in the DIT the search is to start. (For example, `ou=People,dc=securelogix,dc=com`)

11. In the **User DN** box, type the username the ETM Server is to use to connect to the LDAP server. (For example, `cn=Directory Manager`.)

12. In the **Password** box, type the password associated with the username.

13. The **Filter** box allows you to optionally specify a filter to return only a subset of LDAP entries. The default is `(objectClass=*)`, which means "no filter." This means all entries below the specified base are returned.

    - To apply a filter, in the **Filter** box, type the string that defines which entries to return.

14. The **Unique Identifier** area defines the attribute the ETM System is to use to correlate an LDAP entry with an ETM Directory Listing. After the initial import to populate the Import Set, the Unique Identifier is used to determine which Listing an LDAP entry matches. The Unique Identifier specified should be an attribute that is stable and unique for all LDAP entries. In the **Unique Identifier** area, select one of the following:

    - **Use Distinguished Name**—Since the DN is based on the relative path in the DIT and may be subject to change, you may want to select a different attribute as the unique identifier, if an attribute exists that is unique and stable for all LDAP entries.
    - **Use Alternate Attribute**—If an attribute exists that is unique and stable for all LDAP entries that can be used instead of the DN, such as a user ID (uid), specify that attribute here. Every entry must have a value for the specified attribute, and the value must be unique for each entry.

Tip You can also initiate an import manually at times other than those specified on the **Synchronization** tab, using the Import Wizard launched from the **General** tab. See "Initiating an Unscheduled LDAP Import" on page 176.

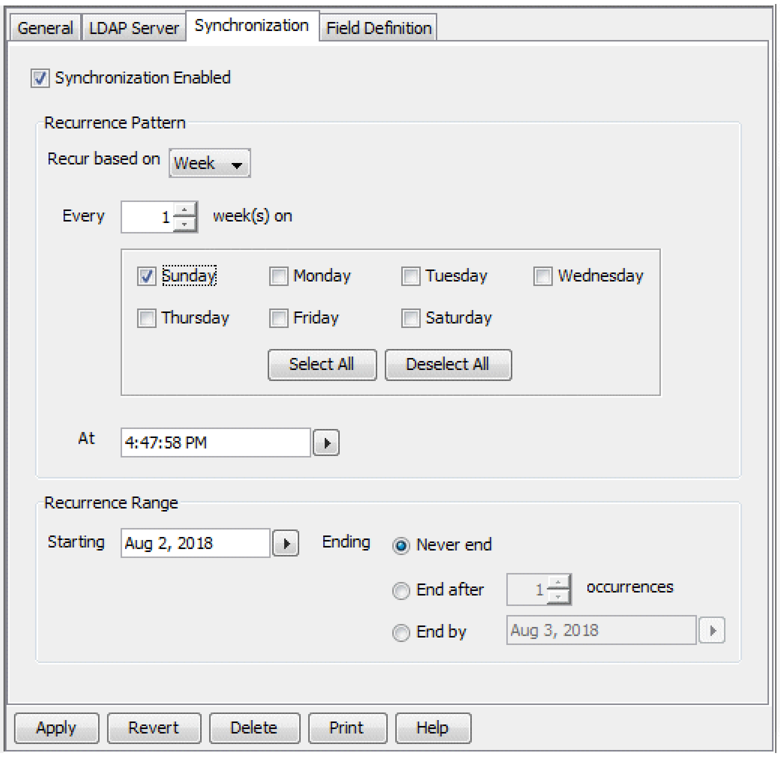
15. If your LDAP Server is configured for paging, select **Support Paging** and then do the following:

    a. In the **Page Size** box, type or select the page size for which your LDAP Server is configured. The default is 1000.

    IMPORTANT This value must match the configuration on your LDAP Server, or import performance may be impaired.

    b. In the **Sort Key** box, type the sort key your LDAP Server uses, if different from the default. The default is **objectGUID**.

16. Click the **Synchronization** tab. This tab specifies how often the ETM Directory is to connect to the LDAP server and request the latest LDAP information. The recurrence pattern and range configuration is identical to that of Usage Manager Scheduled Reports.



☑ Synchronization Enabled

Recurrence Pattern

Recur based on Week

Every 1 week(s) on

☑ Sunday □ Monday □ Tuesday □ Wednesday

□ Thursday □ Friday □ Saturday

At 4:47:58 PM

Recurrence Range

Starting Aug 2, 2018

Ending ● Never end

○ End after 1 occurrences

○ End by Aug 3, 2018

17. Select the **Synchronization Enabled** check box.

18. In the **Recur based on** box of the **Recurrence Pattern** area, select one of the following:

    - **Day**—Use day as the unit of time. Then select the frequency, either **Every *n* days** or one or more certain days of the week. To synchronize on all days of the week, click **Select All**. For example, you might specify "every 3 days" or "Every Tuesday."

    - **Week**—Use week as the unit of time. Type or select the frequency in the **Every *n* week(s) on** box and then select the day or days of the week on which to synchronize. To synchronize on all days at the weekly frequency specified, click **Select All**. For example, you might specify "Every 2 weeks on Saturday."

    - **Month**—Use month as the unit of time. Specify the frequency by doing one of the following:

      - Select **On day** and type or select a numeric day of the month.

      OR

      - Select **On the <ordinal><unit>** and select the applicable options, for example, “On the first weekend day."

19. In the **At** box, type or select the time at which the synchronization is to begin.

20. In the **Recurrence Range** area, specify the duration of the scheduled recurrence.

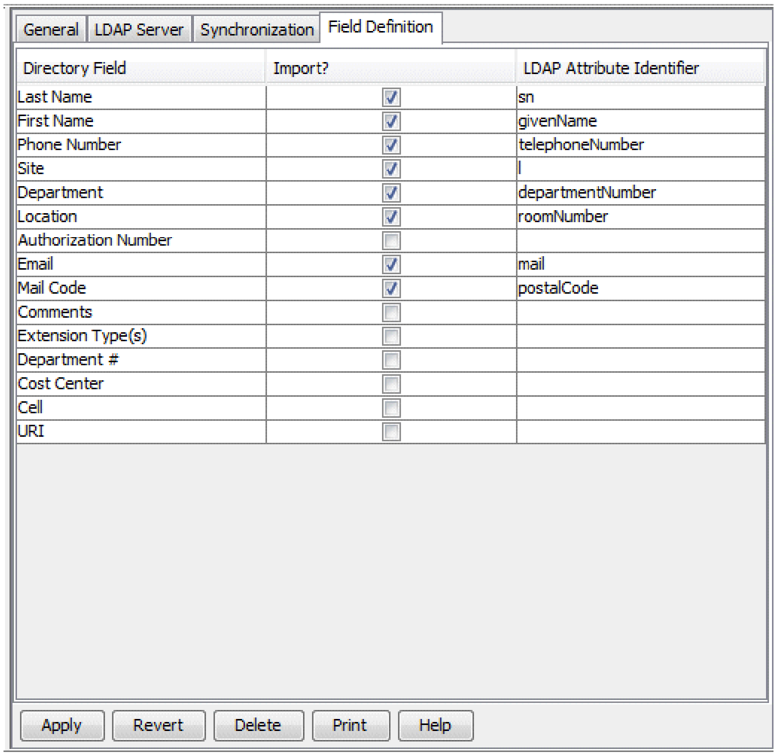
    a. In the **Starting** box, type or select the first date on which the synchronization is to occur.

    b. In the **Ending** area, select one of the following:

    - **Never end**.
    - **End after n occurrences**. Type the number of times the synchronization is to occur.
    - **End by**. Type or select the date on which the scheduled recurrence is to end.

For instructions for changing the default field mappings, see “Mapping Directory Fields to Default LDAP Attribute Fields” in the *ETM® System Technical Reference*.

21. Click the **Field Definition** tab. This tab enables you to define the correlation between ETM Directory Listing fields and the attributes that exist in the LDAP server. A given LDAP attribute may not be mapped to more than one Directory field. The **URI** Directory field, which can contain up to 5 URIs, can be mapped to a single LDAP attribute, but that attribute can be multi-valued; the importer can extract up to 5 URIs from the specified attribute.



Directory Field	Import?	LDAP Attribute Identifier
Last Name	☑	sn
First Name	☑	givenName
Phone Number	☑	telephoneNumber
Site	☑	l
Department	☑	departmentNumber
Location	☑	roomNumber
Authorization Number	☐	
Email	☑	mail
Mail Code	☑	postalCode
Comments	☐	
Extension Type(s)	☐	
Department #	☐	
Cost Center	☐	
Cell	☐	
URI	☐	

Null values do not override data already in a record in the ETM Directory.

c. For each of the fields in a Directory Listing, you specify whether data is to be retrieved for that field, and if so, which LDAP attribute is to be associated with the field. **Last Name** and **Phone Number** are required; all other fields are optional. Default values representing common associations are provided for commonly used fields. For each field for which data is to be retrieved:

   i. Select **Import**.

   ii. In the **LDAP Attribute Identifier** box, type the LDAP attribute that corresponds to this ETM Directory field, or keep the default, if one is provided.

d. Click **Apply** to save changes. To discard unsaved changes, click **Revert**.

22. After you define and schedule the LDAP Import Set, you can either wait for the initial scheduled synchronization for the Import Set to be populated, or you can manually initiate an import. See "Initiating an Unscheduled LDAP Import" on page 176 for instructions.

Initiating an Unscheduled LDAP Import

You can use the following procedure to update the ETM Directory from the LDAP data without waiting for the next scheduled synchronization.

To initiate an unscheduled import

1. In the Directory Manager tree pane, click the LDAP Import Set you want to update. The Import Set appears in the right pane.
2. On the **General** tab, click **Import Wizard**. The **ETM Import Wizard** appears.
3. Click **LDAP Extract**. The applicable entries are extracted from the LDAP Server and the message, "LDAP Extract Complete" appears.
4. Click **OK**.
5. If any warnings were triggered, the message "Would you like to view the warnings file now?" appears. To view the warnings, click **Yes**; if you do not want to view the warnings, click **No**.
6. Click **Next**.
7. Click **Start SQL*Load** to begin processing the entries. When processing completes, the SQL*Loader log file appears. Click the **x** to close the file.
8. Click **Start SQL Reconcile** to reconcile the extracted LDAP entries with the Listings in the Import Set. When this completes, click **Next**.
9. Click **Start Summarizing**. When this completes, a table appears listing the number of Listings to be added, updated, deleted, and to remain unchanged after the import completes.
10. Click **Next**.

11. Click **Execute Changes**. This step updates the Listings in the ETM Directory and cannot be undone.
12. Click **Finish**.

Viewing Diagnostic Logs for Imports

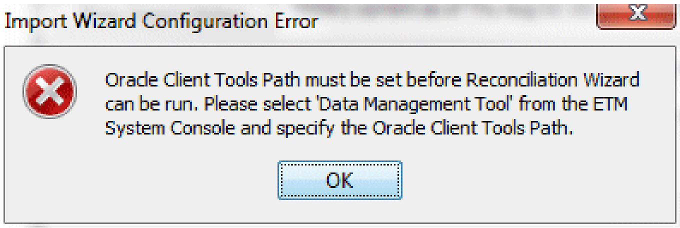
To view a diagnostic log for an Import Set

1. In the Directory Manager tree pane, click the Import Set for which you want to view the Diagnostic Log. The Import Set opens in the tree pane.
2. Click **View Diagnostic Logs**. The **SQL*Loader** log file appears.
   - The first section shows any exceptions that occurred during the last import. If no exceptions occurred or if no imports have been performed, the text "exception.txt does not exist" appears.
   - The second section show the reconcile log, which provides the logs of the last import/reconciliation. This content is the same as that in the SQL*Loader log file that appears during import. See "Contents of the SQL*Loader Log File" on page 168 for a description. If no import has been performed, the text "reconcile.txt does not exist" appears.

Configuring the Import Wizard

Before you can use the Import Wizard to import Listings from an external file, the path to the Oracle client tools on the Management Server computer must be specified. The Import Wizard uses the **SQL*Loader** database utility, an Oracle client tool that loads data from external files into the tables of an Oracle database. If the Management Server is installed on a different computer than the database, the Oracle client tools must be installed on the Management Server before you can specify the path to the Oracle client tools.

This configuration is normally performed during installation. If you receive the following error message when you attempt to launch the Import Wizard, see "Specifying the Oracle Client Tools Location" in the *ETM® System Administration and Maintenance Guide* for configuration instructions.

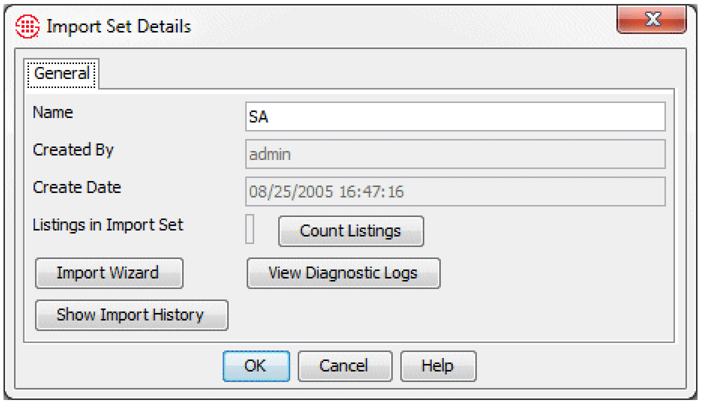


Oracle Client Tools Path must be set before Reconciliation Wizard can be run. Please select 'Data Management Tool' from the ETM System Console and specify the Oracle Client Tools Path.

Viewing Import Set Details

To view Import Set details

- In the Directory Manager tree pane, do one of the following:
  - Click the **Import Sets** node. The editing pane displays a table listing all of the Import Sets. Right-click the one for which you want to view details, and then click **Edit**.
  - Click the **PLUS SIGN** to expand the **Import Sets** node, and then click the Import Set for which you want to view details. The **Import Set Details** dialog box appears within the editing pane.



Import Set Details

General

Name: SA

Created By: admin

Create Date: 08/25/2005 16:47:16

Listings in Import Set:

The contents of the **Import Set Details** dialog box vary depending on which type of Import Set you have selected: **File-based** or **LDAP**. The illustration above shows the Import Set Details for a file-based Import Set.

- For a file-based Import Set, the following information is provided:
  - The name of the Import Set. To rename the Import Set, type a new name.
  - The name of the user who created it.
  - The date it was created.
  - The number of Listings in the Import Set. (Click **Count Listings** to update the value.)
  - An option to launch the Import Wizard. To launch the Import Wizard, click **Import Wizard**. For instructions for importing Listings using the Import Wizard, see "Import Sets” on page 155.
  - An option to view a diagnostic log of the last import. To view the log, click **View Diagnostic Logs**.
  - The Import History. (To show or update the Import History, click **Show Import History**.)
- For an LDAP Import Set, the **Import Set Details** dialog box contains configuration settings for connecting to the LDAP server and scheduling imports. See “Creating an LDAP Import Set” on page 171 for details.

Renaming an Import Set

To rename an Import Set

1. In the **Import Sets** node of the Directory Manager tree pane, click the Import Set you want to rename. It opens in the right pane.
2. In the **Name** box, type the new name, and then click **OK**.

Deleting an Import Set

When you delete an Import Set, all of the Listings imported via that Import Set are deleted. The larger the count of Listings in the Import Set, the longer deletion takes and may be time-consuming on an Import Set with a large number of Listings.

To delete an Import Set

Instead of right-clicking, you can click the **Delete** button at the bottom of the editing pane after you select the item(s) to be deleted.

- Do one of the following:
  - In the **Import Sets** node of the Directory Manager tree pane, right-click the Import Set and click **Delete**.
  - In the Directory Manager tree pane:
    a. Click the **Import Sets** node. A table appears in the editing pane listing all of the Import Sets.
    b. Right-click the Import Set you want to delete, and then click **Delete**.
       - To delete multiple Import Sets, hold down SHIFT or CTRL and select the Import Sets, and then right-click the selection and click **Delete**.

Printing an Import Set Report

An Import Set report provides the following information:

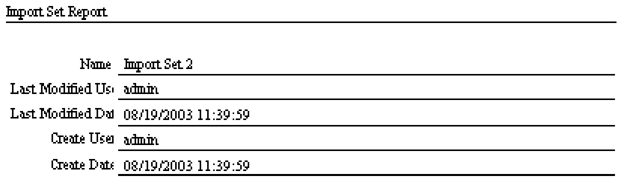
- The name of the Import Set.
- The date/time it was created and by whom.
- The date/time it was last modified and by whom.

To print an Import Set report

Instead of right-clicking, you can click the **Print** button at the bottom of the editing pane after selecting the item to print.

- Do one of the following:
  - In the **Import Sets** node of the Directory Manager tree pane, right-click the Import Set and click **Print**.
  - In the Directory Manager tree pane:
    a. Click the **Import Sets** node. A table appears in the editing pane listing all of the Import Sets.
    b. Right-click the Import Set, and then click **Print**.

  The **Print Preview** dialog box appears containing the report, which appears similar to the following illustration.



Import Set Report

Name	Import Set 2
Last Modified Us	admin
Last Modified Da	08/19/2003 11:39:59
Create Use	admin
Create Dat	08/19/2003 11:39:59

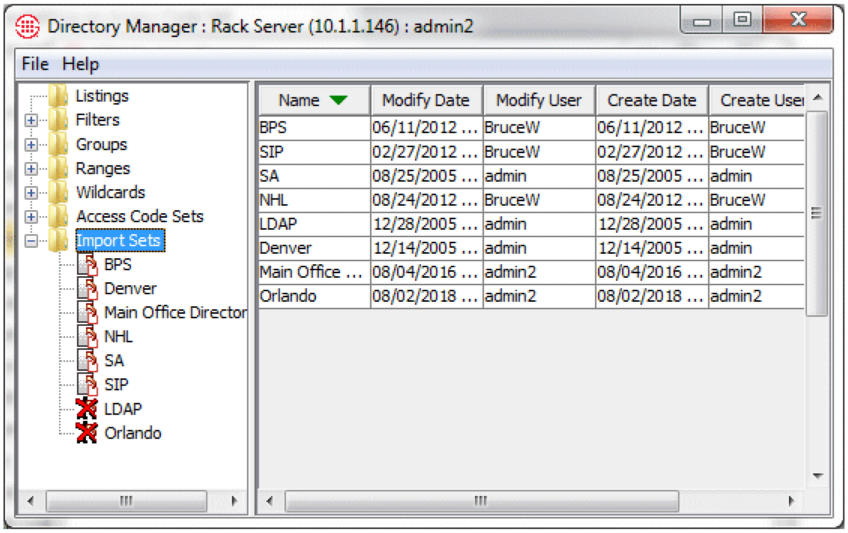
3. Click the **Print** icon. The printer dialog box for your default printer appears. Print as you normally would.

Viewing a List of All Import Sets and Their Properties

Import Set properties include: Name, Comments, date and time last modified and by whom, and date and time created and by whom.

To view a list of all Import Sets and their properties

- In the Directory Manager tree pane, click the **Import Sets** node. The list of all of the Import Sets and their properties appears in the editing pane.
  - To view or edit one of the Import Sets, click the Import Set in the list and then click **Edit** at the bottom of the editing pane.
  - To delete one of the Import Sets, click the Import Set in the list and then click **Delete** at the bottom of the editing pane. **IMPORTANT** Deleting an Import Set deletes its Listings.
  - To print a report for one of the Import Sets , click the Import Set in the list and then click **Print** at the bottom of the editing pane. See "Printing an Import Set Report" on page 179 for details about the content of the Import Set report.
  - To create a new Import Set, click **New** at the bottom of the editing pane. See "File-Based Import Sets" on page 155 or "LDAP Import Sets" on page 169.



Name	Modify Date	Modify User	Create Date	Create User
BPS	06/11/2012 ...	BruceW	06/11/2012 ...	BruceW
SIP	02/27/2012 ...	BruceW	02/27/2012 ...	BruceW
SA	08/25/2005 ...	admin	08/25/2005 ...	admin
NHL	08/24/2012 ...	BruceW	08/24/2012 ...	BruceW
LDAP	12/28/2005 ...	admin	12/28/2005 ...	admin
Denver	12/14/2005 ...	admin	12/14/2005 ...	admin
Main Office ...	08/04/2016 ...	admin2	08/04/2016 ...	admin2
Orlando	08/02/2018 ...	admin2	08/02/2018 ...	admin2

Monitoring Tools

Tools for Monitoring System and Telco Activity

The ETM® System provides various tools for monitoring system and telco activity:

- The **Alert Tool** provides user-configurable real-time alerts for telco, system, and Policy events. See "Alert Tool" on page 184 for details.
- The **Call Monitor** provides a real-time display of monitored calls. See "Call Monitor" on page 194 for details.
- The **Diagnostic Log** provides informational and diagnostic messages about system activity. See "Diagnostic Log" on page 188 for details.
- The **Policy Logs** provide information about Policy processing. One **Policy Log** provides Firewall Policy processing results. A separate **Policy Log** provides IPS Policy processing results. For information about the **Policy Logs**, see "The **Policy Log**" in the *Voce Firewall User Guide* or "IPS **Policy Log**" in the *Voice IPS User Guide*.
- The **Call Log**, which provides details about each call monitored by a given Span Group, regardless of whether the call triggered a tracked Rule in any Policy. If a call triggered a Firewall Policy Rule, that information is also included for the call. Since IPS Policies are based on call pattern accumulations and not individual calls, no IPS Policy processing fields appear in this Log.
- The **Status Tool** shows details about interaction between the ETM Server and Spans during events such as configuration updates, software or Dialing Plan downloads, and Policy verification. See "Status Tool" on page 186 for details.
- The **ETM System Statistics** dialog box provides health and status information for the ETM Appliance and the telecom circuits it monitors. See "Viewing Health and Status" on page 212 for details.
- **Real-time status indicators** in the Performance Manager tree pane provide at-a-glance notification of a wide variety of issues, including IP and Telco network alarms and errors, Span and Card status, Policy synchronization issues, and more. See “Real-Time Telco Health and Status Alarms” on page 16 for details.

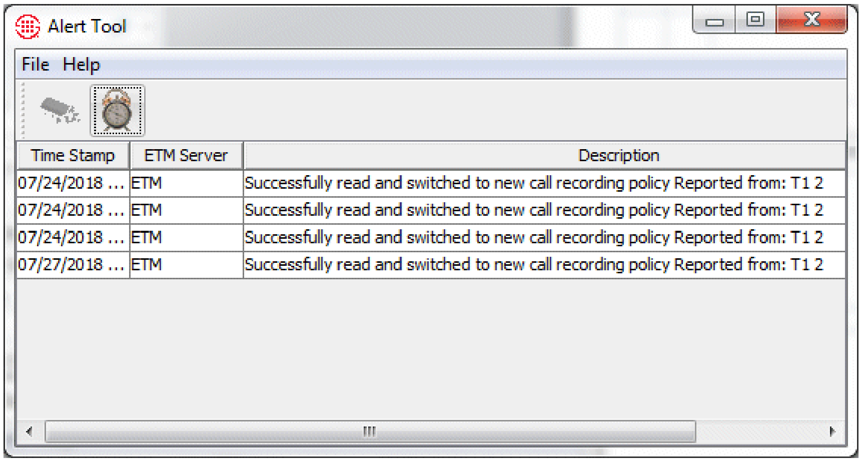
- **Error logs** provide diagnostic information about system errors. See the *ETM® System Technical Reference* for details.
- **SMDR debug logs** provide troubleshooting data regarding SMDR resolution. See "Enabling SMDR Debug Logging" in the *ETM® System Administration and Maintenance Guide* for instructions for enabling SMDR debug logging. See the *ETM® System Technical Reference* for details about the contents of the generated SMDR debug log, troubleshooting SMDR, and defining an SMDR parse file.
- **Appliance Debug Logs** provide information valuable to SecureLogix Customer Support for troubleshooting system issues. See "Appliance Debug Event Logging" in the *ETM® System Administration and Maintenance Guide* for enabling Appliance debug logging.

Alert Tool

You can configure the Management Server to generate real-time alerts in response to specific telecom, system, or Policy events. These alerts are viewed in the **Alert Tool**. Alerts for all of the Management Servers you are currently connected to are consolidated in a single **Alert Tool**, enabling you to simultaneously monitor tracked events across the enterprise, regardless of the Management Server you are currently viewing. Each alert contains the following information:

For instructions for setting alerts for telecom and system events, see "Setting Track Actions for System Events" in the *ETM® System Administration and Maintenance Guide*.

- **Time Stamp**—The date and time an alert was generated.
- **Server**—The Management Server from which the alert originated.
- **Description**—A description of the cause of the alert.



Time Stamp	ETM Server	Description
07/24/2018 ...	ETM	Successfully read and switched to new call recording policy Reported from: T1 2
07/24/2018 ...	ETM	Successfully read and switched to new call recording policy Reported from: T1 2
07/24/2018 ...	ETM	Successfully read and switched to new call recording policy Reported from: T1 2
07/27/2018 ...	ETM	Successfully read and switched to new call recording policy Reported from: T1 2

Alerts remain in the **Alert Tool** until you clear them, up to a limit of 1000 items. If this limit is exceeded, the last 1000 alerts received are shown; the oldest alerts are cleared as new ones are received.

You can set preferences governing how the **Alert Tool** responds when an alert is received. These preferences include the following:

- Whether the **Alert Tool** displays automatically when a new alert is received. If you do not select this setting, you can manually open the **Alert Tool** at any time to view alerts.
- Whether the **Alert Tool** plays an audible notification when a new alert is received, and if so, how often the sound is repeated until you acknowledge the alert.

Opening the Alert Tool

To open the Alert Tool

- On the ETM System Console main menu, do one of the following:
  - Click **Tools | Alerts**.

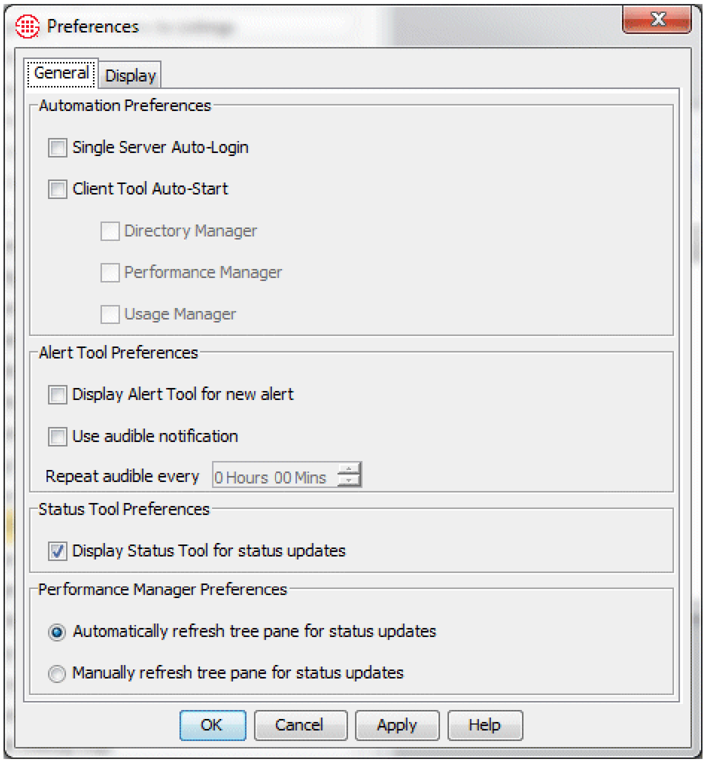
  - or -

  - Click the **Alarm Clock** icon.

Setting the Alert Tool to Display for New Alerts

To set the Alert Tool to display automatically for new alerts

1. On the ETM System Console main menu, click **Edit | Preferences**. The **Preferences** dialog box appears.



Preferences

General | Display

Automation Preferences

□ Single Server Auto-Login

□ Client Tool Auto-Start

□ Directory Manager

□ Performance Manager

□ Usage Manager

Alert Tool Preferences

□ Display Alert Tool for new alert

□ Use audible notification

Repeat audible every 0 Hours 00 Mins

Status Tool Preferences

☑ Display Status Tool for status updates

Performance Manager Preferences

● Automatically refresh tree pane for status updates

○ Manually refresh tree pane for status updates

2. Click the **General** tab, if not already selected.
3. In the **Alert Preferences** area, select the **Display Alert Tool for new alert** check box.

Setting an Audible Alarm for Alerts

To set an audible alarm for Alerts

1. On the ETM System Console main menu, click **Edit | Preferences**. The **Preferences** dialog box appears.
2. Click the **General** tab, if not already selected.
3. In the **Alert Preferences** area, select the **Use Audible Notification** check box.
4. In the **Repeat audible every** box, type or select the Interval (in hours, minutes, and seconds) at which the audible alarm repeats until the alert is acknowledged.

Acknowledging an Alert

If you have set an audible alarm for alerts, the alarm will sound at the specified interval until you acknowledge the alert using the procedure below.

To acknowledge an Alert

- On the **Alert Tool**, click the **Alarm Clock** icon.

Clearing the Contents of the Alert Tool

Alerts remain in the **Alert Tool** (even if you close it) until you clear them using the procedure below, with up to 1000 shown at a time. However, if you close the ETM System Console, the alerts are cleared.

To clear the contents of the Alert Tool

- On the **Alert Tool**, click the **Alarm Clock** icon.

Printing the Contents of the Alert Tool

To print the contents of the Alert Tool

- On the Alert Tool main menu, click **File | Print**. The standard print dialog box for your default printer appears. Print as usual.

Status Tool

The **Status Tool** shows details about interaction between the ETM Server and Spans during events such as configuration updates, software or Dialing Plan downloads, and Policy verification. A single **Status Tool** shows status for actions that you initiate for all ETM Servers to which you are connected. The information remains in the tool until you click **Clear** to remove it or until 1000 entries are received, even if you close the **Status Tool**.

The **Status Tool** displays the following types of messages:

- Informational messages are displayed in black text. For example, "INFO: Management server successfully sent configuration download message to device."
- Warning messages are displayed in yellow text. For example, "WARNING: This Rule is a duplicate of Rule 4."

- Error messages are displayed in red text. For example, "ERROR: Source Objects could not be validated."
- Debug messages are displayed in blue text. For example, "DEBUG: No comments have been added."

You can configure the **Status Tool** to open automatically when status information is received (see "Setting the Status Tool to Open for Status Updates" on page 187), or you can open it manually from the ETM System Console when you want to view status information (see below).

Opening the Status Tool

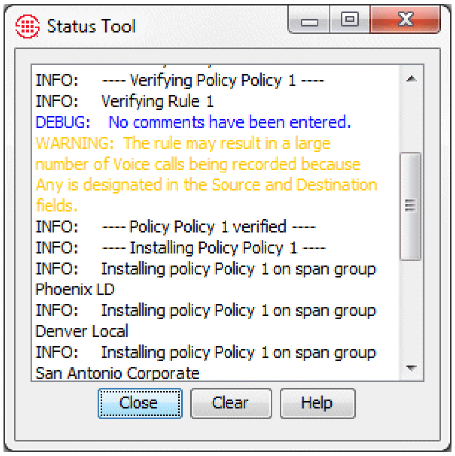
Status Tool icon

To open the Status Tool

- In the ETM System Console, do one of the following:
  - Click **Tools | Status.**

  -or-

  - Click the **Status Tool** icon.

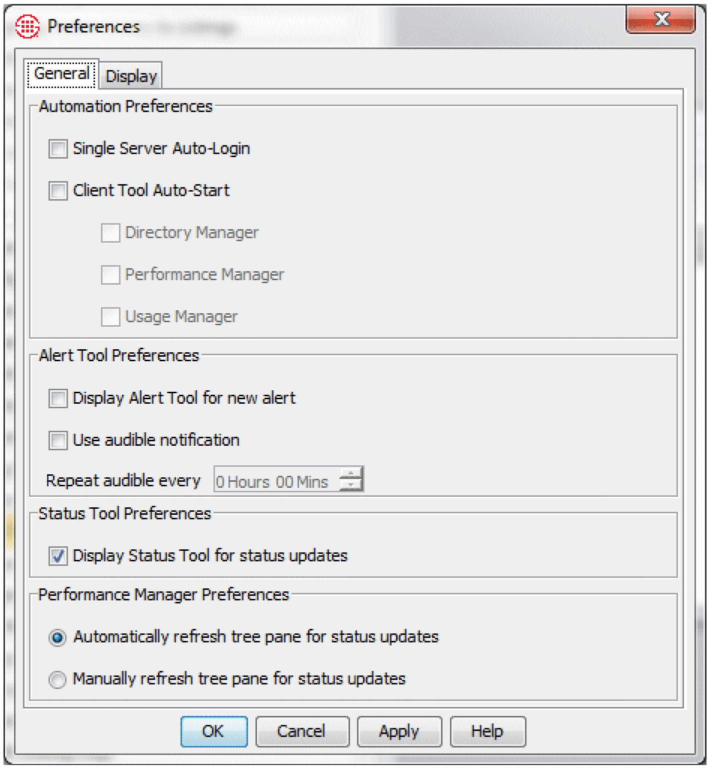


```
INFO:    ---- Verifying Policy Policy 1 ----
INFO:    Verifying Rule 1
DEBUG:   No comments have been entered.
WARNING:  The rule may result in a large
number of Voice calls being recorded because
Any is designated in the Source and Destination
fields.
INFO:    ---- Policy Policy 1 verified ----
INFO:    ---- Installing Policy Policy 1 ----
INFO:    Installing policy Policy 1 on span group
Phoenix LD
INFO:    Installing policy Policy 1 on span group
Denver Local
INFO:    Installing policy Policy 1 on span group
San Antonio Corporate
```

Setting the Status Tool to Open for Status Updates

To set the Status Tool to open for status updates

1. In the ETM System Console, click **Edit | Preferences**. The **Preferences** dialog box appears.



Automation Preferences

□ Single Server Auto-Login

□ Client Tool Auto-Start

□ Directory Manager

□ Performance Manager

□ Usage Manager

Alert Tool Preferences

□ Display Alert Tool for new alert

□ Use audible notification

Repeat audible every 0 Hours 00 Mins

Status Tool Preferences

☑ Display Status Tool for status updates

Performance Manager Preferences

● Automatically refresh tree pane for status updates

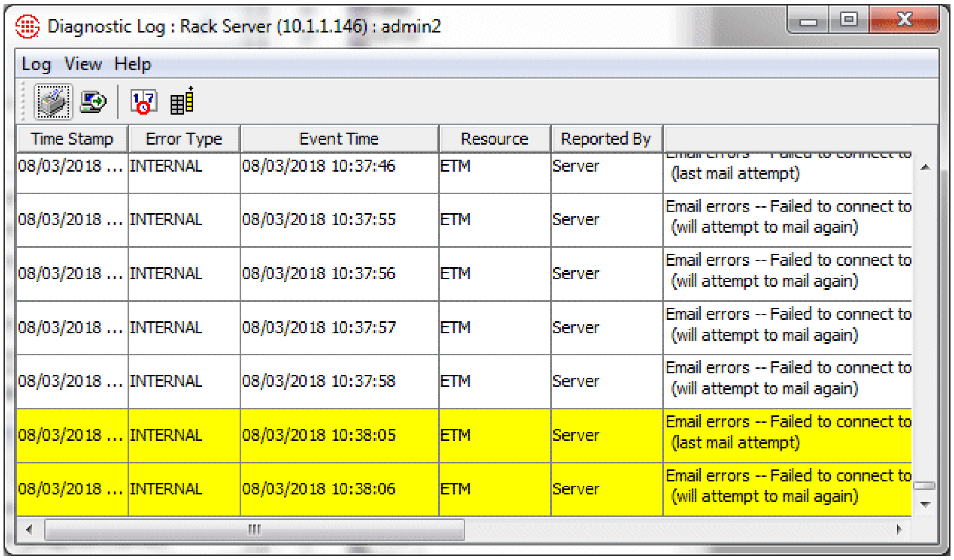
○ Manually refresh tree pane for status updates

2. In the **Status Tool Preferences** area, select the **Display Status Tool for status updates** check box.

3. Click **OK** to apply the changes and close the dialog box or **Apply** to apply the changes and keep the dialog box open.

Diagnostic Log

Each ETM Server has a **Diagnostic Log** that displays diagnostic messages regarding system events. It is recommended that this log be reviewed daily for items of concern. You can also assign notification Tracks to specific system events or to an entire category of events so that appropriate personnel are automatically notified when an event occurs. For example, you might want your Security Administrator notified for some or all security events and your Telco Administrator notified for some or all telco events. See "Setting Track Actions for System Events" in the *ETM® System Administration and Maintenance Guide* for instructions for assigning Tracks to system events.



Time Stamp	Error Type	Event Time	Resource	Reported By	
08/03/2018 ...	INTERNAL	08/03/2018 10:37:46	ETM	Server	Email errors -- Failed to connect to (last mail attempt)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:55	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:56	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:57	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:58	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:38:05	ETM	Server	Email errors -- Failed to connect to (last mail attempt)
08/03/2018 ...	INTERNAL	08/03/2018 10:38:06	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)

System Event Categories

System events are divided into the categories listed below. The category appears in the **Error Type** column of the **Diagnostic Log**, while the event description appears in the **Description** column. See “Appendix A: System Events” in the *ETM® System Administration and Maintenance Guide* for a list and description of the system events in each category.

Category	**Description**
Error	Error events indicate elevated cabinet temperature, missed Span heartbeats, or call traffic errors.
Panic	Panic events represent potentially severe events, such as a hardware failure or a software exception.
Policy	Policy events are associated with Policy enforcement.
Security	Security events include authorized and unauthorized access, connection, and configuration events.
Telco	Telco events provide information about telephony events and errors.
Start/Stop	Start/Stop events occur when a Card or the Management Server is shut down or initialized, or when the Management Server enters Standby mode.
VoIP	VoIP events relate to potential quality-of-service and availability events on VoIP Spans.
Warning	Warning events occur in response to such events as unavailable expected files, lost Card/Management Server communication, excessive failed SMDR resolutions, or Fail-Safe mode.

Fields in the Diagnostic Log

For each system event, the **Diagnostic Log** displays the following information:

- **Time Stamp**—The date and time at which the Management Server received the message.
- **Error Type**—The category of system event. See "System Event Categories" on page 189 for a list of the categories and their descriptions.
- **Event Time**—The date and time the event actually occurred.
- **Resource**—The system component at which the event occurred (for example, the Management Server or a specific Span managed by that Management Server).
- **Reported By**—The system component that sent the message to the Management Server. (For example, the Management Server or a hardware component).
- **Description**—The description of the event that triggered the notification. See "Appendix A: System Events" in the *ETM® System Administration and Maintenance Guide* for a list and description of each system event.

See the topics below for instructions for opening, filtering, and setting **Diagnostic Log** display preferences and for exporting or printing the log. See the *Usage Manager User Guide* for instructions for running reports on **Diagnostic Log** data.

Viewing the Diagnostic Log

Tip To remove the **Resource** filter so that all messages are visible, right-click the **Resource** column heading and click **Remove Filter**.

To view the Diagnostic Log

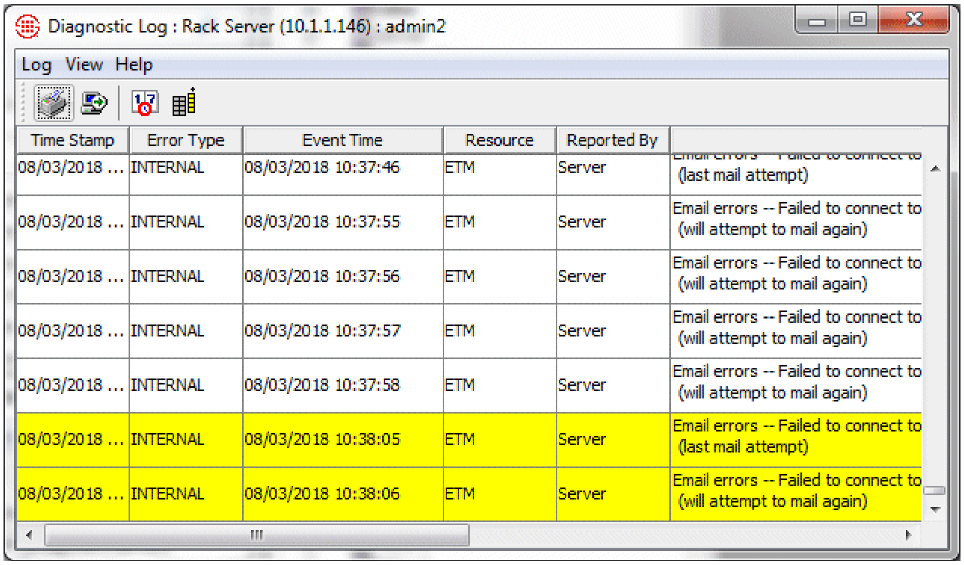
1. In the Performance Manager, do one of the following:

   - To view only diagnostic messages generated by a specific Span, right-click the Span in the Performance Manager tree pane, and then click **View Diagnostic Logs**.

     The **Diagnostic Log** appears, filtered to show only records for the selected Span. The **Resource** column heading appears in red to indicate that a filter is applied. Note that the **Diagnostic Log** appears blank if no messages for that Span are present.

   - To view diagnostic messages for all resources managed by this Management Server, click **Tools | View Diagnostic Logs** on the Performance Manager main menu.

   The **Diagnostic Log** appears. New entries are highlighted in yellow by default. If you prefer that new entries not be highlighted, or that they be highlighted in a different color, see "Setting Log Display Properties" on page 247.



Time Stamp	Error Type	Event Time	Resource	Reported By	
08/03/2018 ...	INTERNAL	08/03/2018 10:37:46	ETM	Server	Email errors -- Failed to connect to (last mail attempt)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:55	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:56	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:57	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:37:58	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)
08/03/2018 ...	INTERNAL	08/03/2018 10:38:05	ETM	Server	Email errors -- Failed to connect to (last mail attempt)
08/03/2018 ...	INTERNAL	08/03/2018 10:38:06	ETM	Server	Email errors -- Failed to connect to (will attempt to mail again)

When you open the **Diagnostic Log**, it displays information by default for the 10 minutes prior to the time you opened the log, unless that time period contains more than 1000 log items, in which case only the most recent 1000 entries are displayed. These limits are controlled by two settings in the Performance Manager's **Properties** dialog box: **Log Retrieval Amount** (time) and **Allow Logs to Grow to** (number of records). See "Setting Log Display Properties" on page 247 for instructions for changing these settings.

After you open the log, if you want to see information for more than the last 10 minutes in this instance, you can set the log start time back to an earlier time. See "Setting the Log Display Start Time" on page 192 for instructions.

Note that, since the **Diagnostic Log** retrieves data from the active area in the database, only data that has not been migrated is available. To see historical data, use the Usage Manager diagnostic reports.

Filtering the Diagnostic Log

You can limit the **Diagnostic Log** display to data that matches certain criteria. To do this, you apply filters to one or more columns. Columns to which filters are applied appear in red.

To filter the Diagnostic Log

- Right-click a column heading and click **Edit Filter**. The filter dialog box applicable to the selected column appears. The same filters are used in the Alert Tool, Call Monitor, Policy and **Call Log**s, and Reports. See "Using Filters in the ETM® System" on page 217 for instructions for using each filter, or click the Help button on the filter dialog box.

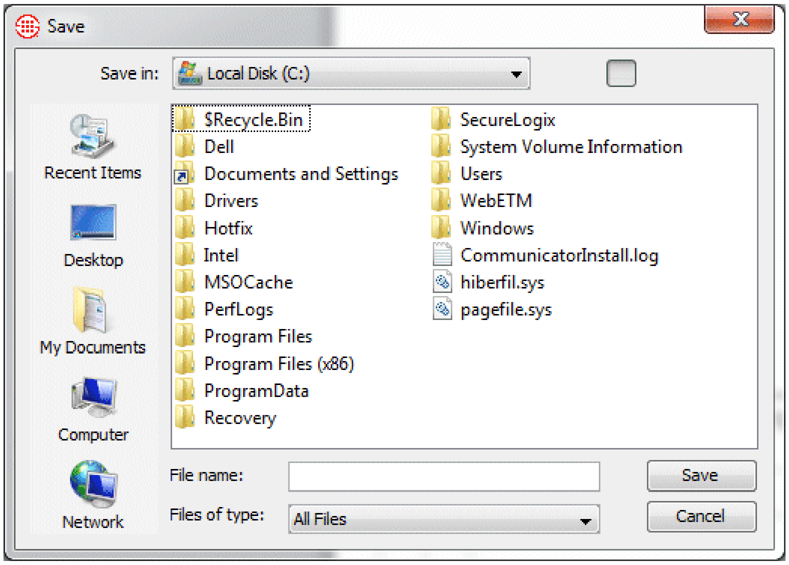
- To remove a filter, right-click the column heading and click **Remove Filter**.

Exporting the Diagnostic Log

You can export the contents of the **Diagnostic Log** display to a comma-separated values (CSV) file that can then be imported into other programs, such as Microsoft Excel. When you export the **Diagnostic Log**, only the records displayed onscreen are included, including the column headings. Filter settings are maintained.

To export the Diagnostic Log display to a CSV file

1. On the **Diagnostic Log** main menu, click **Log | Export**. A **Save** dialog box appears.



2. Browse to the location where you want to save the file, and then click **Save**. Note that unless you specify a different file extension, the file is saved with a **.txt** extension.

Printing the Diagnostic Log

When you print the **Diagnostic Log**, only the records displayed onscreen are included. Filter settings are maintained.

To print the Diagnostic Log

- On the **Diagnostic Log** main menu, click **Log | Print**. The typical Print dialog box for your computer appears. Select printing properties and print the file as you would with any other application.

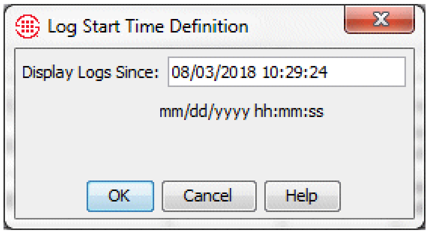
Setting the Log Display Start Time

When you open the **Diagnostic Log**, it displays information by default for the 10 minutes prior to the time you opened the log, unless that period contains more than 1000 log items, in which case only the most recent 1000 entries are displayed. These limits are controlled by two settings in the Performance Manager's **Properties** dialog box: **Log Retrieval Amount** (time) and **Allow Logs to Grow to** (number of records). See "Setting Log Display Properties" on page 247 for instructions for changing these settings.

After you open the log, if you want to see information for more than the last 10 minutes in this instance, you can set the log start time back to an earlier time. Note that the retrieval is still constrained by the **Allow Logs to Grow to** setting. Also note that, since the **Diagnostic Log** retrieves data from the Active tables in the database, only data that has not been migrated is available. To see historical data, use the Usage Manager diagnostic reports.

To set the log start time

1. On the **Diagnostic Log** main menu, click **View | Set Start Time**. The **Log Start Time Definition** dialog box appears, showing the current start date and time in 24-hour format.



Display Logs Since: 08/03/2018 10:29:24

2. In the **Display Logs Since** box, type a date and time (previous to that displayed) at which you want the log display to begin, in 24-hour format, as follows:

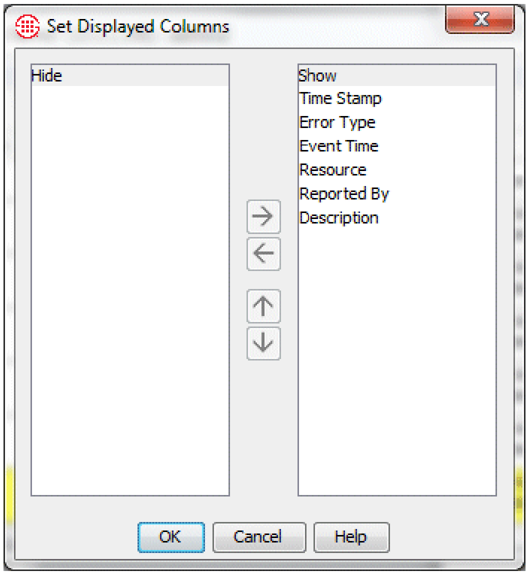
mm/dd/yyyy hh:mm:ss

Showing, Hiding, and Arranging Columns in the Diagnostic Log

To show, hide, or rearrange the columns

1. On the **Diagnostic Log** main menu, click **View | Columns**. The **Set Displayed Columns** dialog box appears. The **Show** box lists the currently displayed fields in the order in which they appear.

Tip You can also drag a column heading to a new location in the **Diagnostic Log** GUI.

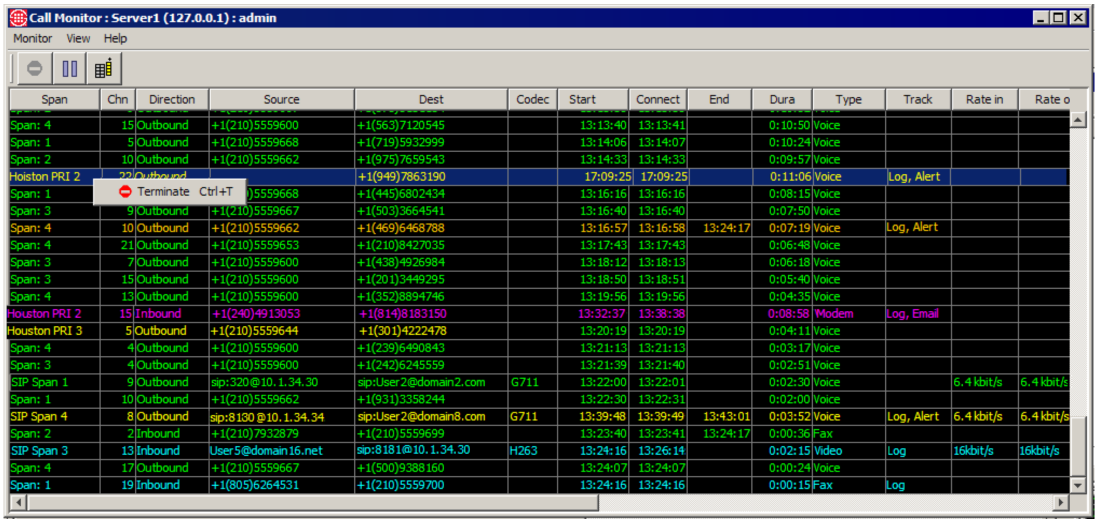


2. The fields listed in the **Show** box appear as column headings in the **Call Monitor** in the order they are listed in this dialog box.

   - To hide a column, click it in the **Show** box, and then click the left arrow button.
   - To show a hidden column, click it in the **Hide** box, and then click the right arrow button.
   - To rearrange the columns in the **Show** box, click a column, and then click the up or down arrow.

Call Monitor

The **Call Monitor** provides a real-time display of monitored call activity.



Span	Chn	Direction	Source	Dest	Codec	Start	Connect	End	Dura	Type	Track	Rate in	Rate o
Span: 4	15	Outbound	+1(210)5559600	+1(563)7120545		13:13:40	13:13:41		0:10:50	Voice			
Span: 1	5	Outbound	+1(210)5559668	+1(719)5932999		13:14:06	13:14:07		0:10:24	Voice			
Span: 2	10	Outbound	+1(210)5559662	+1(975)7659543		13:14:33	13:14:33		0:09:57	Voice			
Hoiston PRI 2	22	Outbound		+1(949)7863190		17:09:25	17:09:25		0:11:06	Voice	Log, Alert		
Span: 1			)5559668	+1(445)6802434		13:16:16	13:16:16		0:08:15	Voice			
Span: 3	9	Outbound	+1(210)5559667	+1(503)3664541		13:16:40	13:16:40		0:07:50	Voice			
Span: 4	10	Outbound	+1(210)5559662	+1(469)6468788		13:16:57	13:16:58	13:24:17	0:07:19	Voice	Log, Alert		
Span: 4	21	Outbound	+1(210)5559653	+1(210)8427035		13:17:43	13:17:43		0:06:48	Voice			
Span: 3	7	Outbound	+1(210)5559600	+1(438)4926984		13:18:12	13:18:13		0:06:18	Voice			
Span: 3	15	Outbound	+1(210)5559600	+1(201)3449295		13:18:50	13:18:51		0:05:40	Voice			
Span: 4	13	Outbound	+1(210)5559600	+1(352)8894746		13:19:56	13:19:56		0:04:35	Voice			
Houston PRI 2	15	Inbound	+1(240)4913053	+1(814)8183150		13:32:37	13:38:38		0:08:58	Modem	Log, Email		
Houston PRI 3	5	Outbound	+1(210)5559644	+1(301)4222478		13:20:19	13:20:19		0:04:11	Voice			
Span: 4	4	Outbound	+1(210)5559600	+1(239)6490843		13:21:13	13:21:13		0:03:17	Voice			
Span: 3	4	Outbound	+1(210)5559600	+1(242)6245559		13:21:39	13:21:40		0:02:51	Voice			
SIP Span 1	9	Outbound	sip:320@10.1.34.30	sip:User2@domain2.com	G711	13:22:00	13:22:01		0:02:30	Voice		6.4 kbit/s	6.4 kbit/s
Span: 1	10	Outbound	+1(210)5559662	+1(931)3358244		13:22:30	13:22:31		0:02:00	Voice			
SIP Span 4	8	Outbound	sip:8130@10.1.34.34	sip:User2@domain8.com	G711	13:39:48	13:39:49	13:43:01	0:03:52	Voice	Log, Alert	6.4 kbit/s	6.4 kbit/s
Span: 2	2	Inbound	+1(210)7932879	+1(210)5559699		13:23:40	13:23:41	13:24:17	0:00:36	Fax			
SIP Span 3	13	Inbound	User5@domain16.net	sip:8181@10.1.34.30	H263	13:24:16	13:26:14		0:02:15	Video	Log	16kbit/s	16kbit/s
Span: 4	17	Outbound	+1(210)5559667	+1(500)9388160		13:24:07	13:24:07		0:00:24	Voice			
Span: 1	19	Inbound	+1(805)6264531	+1(210)5559700		13:24:16	13:24:16		0:00:15	Fax	Log		

The following options are available:

- View calls per Span, for multiple Spans, per Card, per Appliance, or per Switch.
- View all data for all calls, or you can customize the display to show only certain columns, specific call types, and/or calls containing specific types of data, such as those within a certain time frame or from/to a specific phone number/URI.
- Sort the display in ascending or descending order according to a given column by clicking the column heading. A green arrow appears in the column heading; the direction of the arrow indicates sort order (▼ for ascending, ▲ for descending).
- See a row for each enabled channel whether or not it has an active call, or see only channels on which a call is active 🔒.
- Show or hide columns to tailor the display ▥.
- Freeze the display ⏸ to prevent it from scrolling or displaying new entries while you are examining its contents.
- Set color coding preferences for each type of call and set the display update Interval and the length of time that an ended call is displayed. Entries are displayed in colored text to give you a quick visual indication of channel and call status.
- Terminate a specific call in the **Call Monitor** using the **Terminate Call** ⛔ icon.

Call Monitor Fields

The **Call Monitor** provides the following real-time information for each call:

- **Span**—The name of the Span monitoring the call.
- **Trunk Group**—The trunk group on which the channel resides, if one is entered in the Channel Map.
- **Chn**—The channel on which the call was carried.
- **Direction**—Whether the call was incoming or outgoing.
- **Source Num**—The calling phone number (or the name associated with that number in the Directory, if any) for the call. You can select whether Name or Number is displayed. If you select **Name** but no Directory Listing exists for the number, the number is displayed for that call.
- **Dest Num**—The called phone number (or the name associated with that number in the Directory, if any) for the call. You can select whether Name or Number is displayed. If you select **Name** but no Directory Listing exists for the number, the number is displayed for that call.
- **Raw Dest**—The dialed digits on an outbound call.

Since the **Call Monitor** provides near-real-time visibility into call traffic, the Server continually transfers all call state changes to the display. To prevent unnecessary use of system and network resources, close the **Call Monitor** when it is not being actively used.

If a call changes type multiple times, each type is shown only once. That is, if the call starts as **Voice**, becomes **Fax**, and then returns to **Voice**, **Voice** only appears one time. When multiple types are present, the current call type appears in bold text.

- **Type**—The call type(s) detected during the call (fax, modem, etc.). When call type changes during a call, all types detected are shown; the current call type is shown in bold type. See "Call Types Detected by the ETM® System " in the *ETM® System User Guide* for a complete list and a definition of each call type.
- **Start**—The start time of the call (when the trunk was seized).
- **Connect**—The connect time of the call (when call was answered).
- **End**—The end time of the call.
- **Dura**—The amount of time elapsed since Start Time (when the line was seized).
- **Track**—If the call triggered a Firewall Policy Rule, displays the Track(s) specified for the Rule.

When a VoIP Span is included in the selection for which you are viewing the **Call Monitor**, the following fields also appear:

- **Codec**—The codec the call uses.
- **Bytes in**—Inbound payload bandwidth.
- **Bytes Out**—Outbound payload bandwidth.
- **Rate in**—Inbound media rate.
- **Rate out**—Outbound media rate.
- **Source IP**—The media subnet of the caller.
- **Dest IP**—The media subnet of the callee.
- **Jitter in**—Inbound jitter (relates to call quality; a measure of the variability of packet arrival).
- **Jitter out**—Outbound jitter (relates to call quality; a measure of the variability of packet arrival).
- **Packetloss in**—Inbound packet loss (relates to call quality; a measure of the number of lost packets).
- **Packetloss out**—Outbound packet loss (relates to call quality; a measure of the number of lost packets).

The VoIP statistics fields are populated from the RTCP data exchanged by the endpoints. If no RTCP data is available, these fields are blank.

Opening the Call Monitor

To open the Call Monitor

- In the Performance Manager tree pane, right-click the item for which you want to see calls, and then click **Call Monitor**. You can select a single telco Span, multiple telco Spans, a Card, an Appliance, or a Switch.

Call Monitor Display Settings Retained

When you open the Call Monitor, the most recent column display and row count settings for the same selection are retained. For example, if you view the Call Monitor for Span A and apply dynamic row counts, the next time you select Span A and view the Call Monitor, dynamic row counts are shown. But suppose you view the Call Monitor for Span A, select dynamic row counts, and then close it. Next, you view the Call Monitor for Span B, select dynamic row counts, and close it. Then, you select both Spans A and B and view the Call Monitor. Fixed row counts are shown. The display setting applies to the selection, not to each individual member selected. If you select dynamic row counts while viewing the Call Monitor for Span A and B together, then the next time you view Span A and B together, dynamic row counts are shown. Note that filter settings are not retained when you close and reopen the Call Monitor.

Call Monitor Color Coding

Call Monitor entries are displayed in colored text to give you a quick visual indication of channel and call status. You can customize the colors, as explained below.

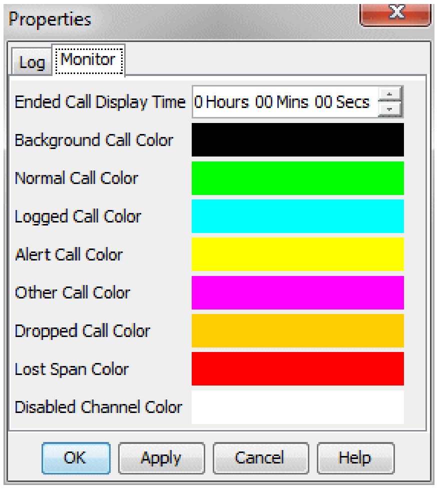
The default colors are:

To revert to the default color for a display element, see step 6 below.

- **Background Call Color**—The **Call Monitor** background. Black is the default.
- **Normal Call Color**—Calls that complete without triggering a Policy Rule. Green is the default.
- **Logged Call Color**—Calls that are logged to the **Policy Log** (for example, calls that trigger a Voice Firewall Policy Rule that specifies **Log** as a Track, or ambiguous calls.)
- **Alert Call Color**—Calls that trigger a Policy Rule that specifies **Alert** as a Track. Yellow is the default.
- **Other Call Color**—Calls that trigger a Policy Rule that specifies no Track or a Track other than **Log** or **Alert**. Pink is the default.
- **Dropped Call Color**—The color for calls that are terminated by a Policy Rule, **ASCII Management Interface**, or **Call Monitor**. Orange is the default.
- **Lost Span Color**—Channels monitored by Spans with which the Server has lost communication. Red is the default.
- **Disabled Channel Color**—Channels that are not enabled on the Channel Map of the **Span Configuration** dialog box. White is the default.

To set Call Monitor color-coding preferences

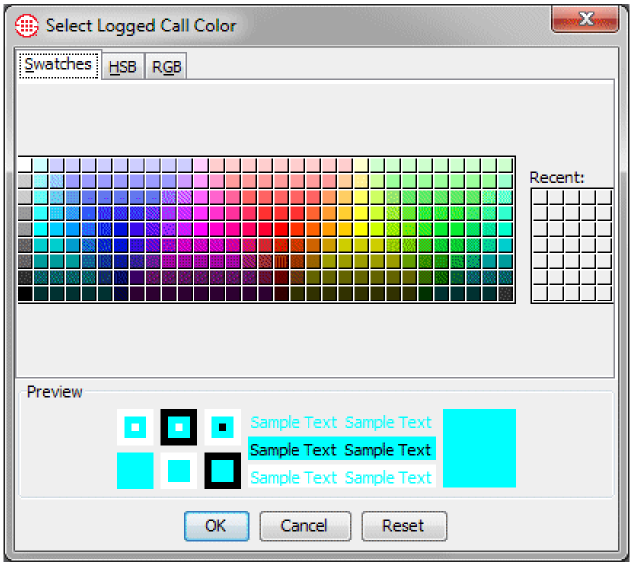
1. On the Performance Manager main menu, click **Edit | Properties**. The **Properties** dialog appears.
2. Click the **Monitor** tab.



Ended Call Display Time: 0 Hours 00 Mins 00 Secs

Background Call Color	⬛
Normal Call Color	🟩
Logged Call Color	🟦
Alert Call Color	🟨
Other Call Color	🟪
Dropped Call Color	🟧
Lost Span Color	🟥
Disabled Channel Color	⬜

3. Click the colored square next to the display element. The **Select Call Color** dialog for the selected element appears.



4. Click the tab for the color selection method you want to use: **Swatches**, **HSB**, or **RGB**.

5. Select the color you want. The **Preview** area shows the currently selected color.

6. Click **OK** to accept the change.

   - To revert to the default color for the display element, click **Reset**.

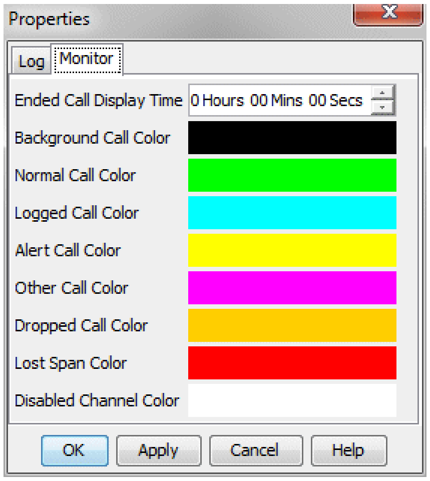
7. Repeat steps 3 through 6 above to select a different color for other display elements, as desired.

Changing the Call Monitor Ended Call Display Time

The **Ended Call Display Time** specifies how long an ended call remains visible if no new call begins on that channel.

To set the Call Monitor update frequency

1. On the Performance Manager main menu, click **Edit | Properties**. The **Properties** dialog appears.
2. Click the **Monitor** tab.



Ended Call Display Time 0 Hours 00 Mins 00 Secs

Background Call Color ⬛

Normal Call Color 🟩

Logged Call Color 🟦

Alert Call Color 🟨

Other Call Color 🟪

Dropped Call Color 🟧

Lost Span Color 🟥

Disabled Channel Color ⬜

3. In the **Ended Call Display Time** box, select how long (in hours, minutes, and seconds) you want information for a call that has ended to remain visible if no new call begins on that channel. The default is 30 seconds. If a new call occurs on a channel, it replaces an ended call, regardless of this setting.

Freezing the Call Monitor Display

You can freeze the **Call Monitor** display so it does not scroll and no new entries are displayed while you examine its contents.

To freeze the display

- On the **Call Monitor** toolbar, click the ⏸ **Freeze Display** icon. This icon acts as a toggle. To unfreeze the display, click the icon again.

Selecting Fixed or Dynamic Row Counts in the Call Monitor

To select fixed or dynamic row counts

- On the **Call Monitor** main menu, click **View | Fixed Row Counts**. This selection works as a toggle to turn fixed row counts on and off. A check mark indicates that fixed row counts are selected. The default is fixed row counts.

Fixed Row Counts—The **Call Monitor** always shows a row for each channel, regardless of call activity. Ended calls appear for the time set in the **Ended Call Display Time** field of the **Properties** dialog box or until a new call begins on that channel. For VoIP Spans, the number of calls set as a resource limit in the VoIP Span's configuration determines the number of rows displayed.

Tip To open the **Properties** dialog box, click **View | Properties** on the Performance Manager main menu.

Dynamic Row Counts—Recommended for VoIP environments. A row only appears for a channel when a call becomes active on that channel. Ended calls remain displayed for the time set in the **Ended Call Display Time** field of the **Properties** dialog box, even if a new call begins on that channel. This means that, depending on call volume, the same channel may appear more than once in the display.

Filtering the Call Monitor Display

You can limit the display in the **Call Monitor** to calls containing specific types of data. To do this, you apply a filter to one or more columns to specify criteria for the types of calls you want to display. Column headings to which a filter is applied appear in red.

To filter the Call Monitor display

- Right-click a column heading, and then click **Edit Filter**. To remove a filter, right-click the column heading, and then click **Remove Filter**. The same filters are used in the Alert Tool, Call Monitor, Policy and **Call Log**s, and Reports. "Using Filters " on page 217 for a list of the filter available for each field.

Sorting the Display

To sort the display in the Call Monitor

- Click the column heading you want to sort by. The display sorts in ascending or descending order according to the data in the column. The direction of the green arrow in the sorted column's heading indicates the sort order.

Showing Name or Phone Number

You can choose whether the **Source** and/or **Dest** columns display the phone number/URI or the name of the associated Directory Listing, if one exists. If you select **Show Name** and no Directory Listing exists, the phone number/URI is shown instead.

To select Name or Number

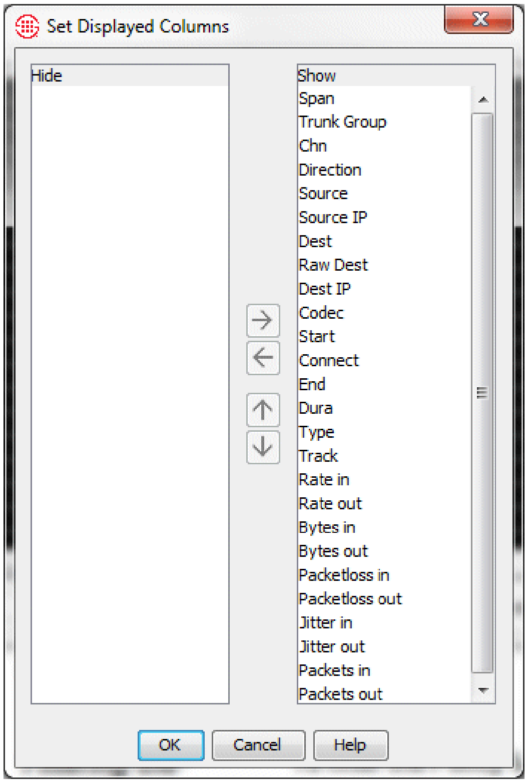
- In the **Call Monitor**, right-click the **Source** or **Dest** column heading, point to **Display**, and then select **Show Name** or **Show Number**.

Viewing, Hiding, or Rearranging Columns

You can also drag the column headings in the **Call Monitor** to rearrange the columns.

To view/hide or rearrange columns in the Call Monitor

1. On the **Call Monitor** main menu, click **View | Columns**. The **Set Displayed Columns** dialog box appears.



2. The fields listed in the **Show** box appear as column headings in the **Call Monitor** in the order they are listed in this dialog box.

   - To hide a column, click it in the **Show** box, and then click the left arrow button.
   - To show a hidden column, click it in the **Hide** box, and then click the right arrow button.
   - To rearrange the columns in the **Show** box, click a column, and then click the up or down arrow.

3. Click **OK**.

Manually Terminating Calls in the Call Monitor

While you are viewing calls in the **Call Monitor**, you can manually terminate calls. To manually terminate calls in the **Call Monitor**, you must have the **Terminate Calls** user permission and **Allow Call Terminations** must be selected in the **Span Configuration** dialog box for the Span on which you are attempting to terminate calls.

To manually terminate a call in the Call Monitor

- Click the call and click the **Terminate Call** ⛔ icon, or right-click the call and click **Terminate**. You can select multiple calls using CTRL or SHIFT. A confirmation message appears. Click **Yes**.

You can also use an ETM® Command in the **ASCII Management Interface** to terminate a single call or all calls on a given Span. For instructions for terminating calls via the **ASCII Management Interface**, see "Terminating Calls via the ASCII Management Interface" in the *ETM® System Administration and Maintenance Guide*.

Policy Logs

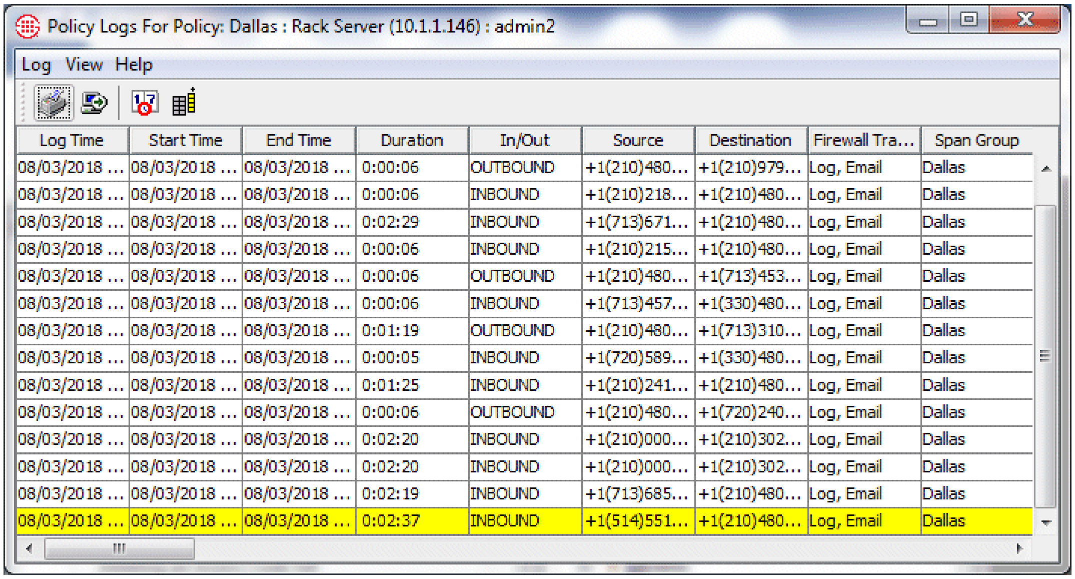
Policy Logs display recent results of ETM System Policy processing. The Firewall Policy Log includes data for calls that triggered a tracked Firewall Policy Rule. The IPS Policy Log includes IPS Policy data for completed Intervals. The data in the **Policy Logs** is retrieved from the Active area in the database. After the data is copied to the Historical area (by default, every 6 hours), you can also view the data in Usage Manager reports. After the data is deleted from the Active area (by default, 6 hours after it is copied to the Historical area), it is no longer viewable in the **Policy Log** and can only be accessed via Usage Manager reports.

See "Changing the Active-to-Historical Transfer Frequency" in the *ETM® System Technical Reference* for instructions for modifying the frequency.

Opening the Policy Logs

To open the Policy Log

1. In the Performance Manager tree pane, expand the **Policies** node for the Policy for which you want to view the log. For example, if you want to see the **Policy Log** for an IPS Policy, expand the **IPS Policies** node; if you want to see the **Policy Log** for a Firewall Policy, expand the **Firewall Policies** node.
2. Right-click a Policy and click **View Policy Logs**. The **Policy Log** appears. The illustration below shows the **Firewall Policy Log**.



Policy Logs For Policy: Dallas : Rack Server (10.1.1.146) : admin2
Log
View
Help

Log Time	Start Time	End Time	Duration	In/Out	Source	Destination	Firewall Tra…	Span Group
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:06	OUTBOUND	+1(210)480…	+1(210)979…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:06	INBOUND	+1(210)218…	+1(210)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:29	INBOUND	+1(713)671…	+1(210)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:06	INBOUND	+1(210)215…	+1(210)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:06	OUTBOUND	+1(210)480…	+1(713)453…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:06	INBOUND	+1(713)457…	+1(330)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:19	OUTBOUND	+1(210)480…	+1(713)310…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:05	INBOUND	+1(720)589…	+1(330)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:25	INBOUND	+1(210)241…	+1(210)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:06	OUTBOUND	+1(210)480…	+1(720)240…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:20	INBOUND	+1(210)000…	+1(210)302…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:20	INBOUND	+1(210)000…	+1(210)302…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:19	INBOUND	+1(713)685…	+1(210)480…	Log, Email	Dallas
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:37	INBOUND	+1(514)551…	+1(210)480…	Log, Email	Dallas

As with the Call Monitor, columns can be arranged in any order, and you can select which columns to hide or show.

Fields in the IPS Policy Log

For details about the **IPS Policy Log**, including a description of the fields, see "IPS Policy Log" in the *Voice IPS User Guide*.

Fields in the Firewall Policy Log

The **Firewall Policy Log** includes the same fields as the **Call Log**. For a description of the fields, see "Fields in the Call Log" on page 208.

Filtering the Policy Log

To filter the Policy Log

- Right-click the column heading and click **Edit Filter**.

The **Filter** dialog box that appears depends on which field you selected. See “Using Filters in the ETM® System” on page 217 for instructions for using each type of filter.

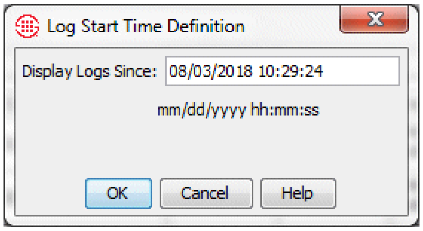
Setting the Start Time of the Policy Log

If you want to retrieve log data for more time than the defined **Log Retrieval Amount** in the current instance, see the procedure below. Note that the retrieved data is still constrained by the setting in the **Allow Logs to Grow to n Items** box.

By default, the **Policy Log** displays information based on the **Log Retrieval Amount** and **Allow Logs to Grow to n Items** settings on the **Log** tab of the **Properties** dialog box. See "Setting Display Preferences for the Policy Log" on page 204 for instructions for changing these settings.

To select the starting time of information presented in the log

1. On the **Policy Log** main menu, click **View | Set Start Time**. The **Log Start Time Definition** dialog box appears.



2. In the **Display Logs Since** box, type the starting date and time for displaying log information, in the format mm/dd/yyyy hh:mm:ss.

   The date and time that you type here must be prior to the date that appears in the **Display Logs Since** box. Note that the retrieved data is still constrained by the setting in the **Allow Logs to Grow to *n* Items** box.

   If you want to restart the log at the current date and time, close the **Policy Log**, and then reopen it.

Setting Display Preferences for the Policy Log

Log display preferences determine the log retrieval amount, whether the display scrolls as new entries are received, and whether new entries are highlighted and if so, in what color. (Note that these settings also apply to the **Call Log** and the **Diagnostic Log**.)

To set log display properties

1. On the Performance Manager main menu, click **Edit | Properties**. The **Properties** dialog box appears.
2. Click the **Log** tab.
3. In the **Log Retrieval Amount** box, type the days, hours, or minutes' worth of data that you want to display, starting from the time you open the log, going back that number of minutes (unless the **Allow Logs to Grow to** limit is reached first). For example, if you open the log at 11:20 and you request 60 minutes of data, the log displays any current data as it is received, plus the data gathered from 10:20 to 11:20. The default is 10 minutes.
4. In the **Allow Logs to Grow to** box, type the maximum number of log entries to display. The default is 1000. Valid values are 1 - 100,000. This value constrains the **Log Retrieval Amount** (above). If the time interval specified contains more entries than the limit specified in the **Allow Logs to Grow to** box, only the specified number of entries is displayed. (A message is provided in this case that states the interval for which the logs are retrieved). After the **Allow Logs to Grow to** value has been reached, the display regenerates as new entries are received, showing only the most recent entries, up to this maximum.

5. Select the **Automatically Scroll for New Entries** check box if you want the display to automatically advance with each new entry. If you clear this check box, you can manually scroll to view the entries at the end of the log.
6. Select **Highlight New Logs** check box if you want new lines of data to be displayed in color. If you clear this check box, new entries are not highlighted.
    - The default highlight color is yellow. To choose a different color, click the colored box, and then select a new color from the **Select New Log Highlight Color** dialog box.
7. Click **OK**.

Showing, Hiding, and Rearranging the Columns in the Policy Log

Select which columns of information you want to view in the **Policy Log** by hiding and showing specific columns. You can also rearrange the columns.

To organize columns displayed

You can also drag and drop the columns in the **Policy Log** to arrange them.

1. In the **Policy Log**, click **View | Columns**. The **Set Displayed Columns** dialog box appears.
2. Do the following to organize the **Policy Log**:
    - To show a column, in the **Hide** box, double-click the name of the column to move it to the **Show** box, or click it, and then click the right-facing arrow.
    - To hide a column, in the **Show** box, double-click the name of the column to move it to the **Hide** box, or click it, and then click the left-facing arrow.
    - To change the order in which the columns are displayed, highlight the items you want to move, and then click the up or down arrow, as appropriate.
3. Click **OK**.

Displaying Name or Number

You can choose whether to display the Directory name or the phone number/URI in the **Source** and **Destination** columns of the **Policy Log**. Each column can be set independently.

To specify Directory Name or Phone Number/URI

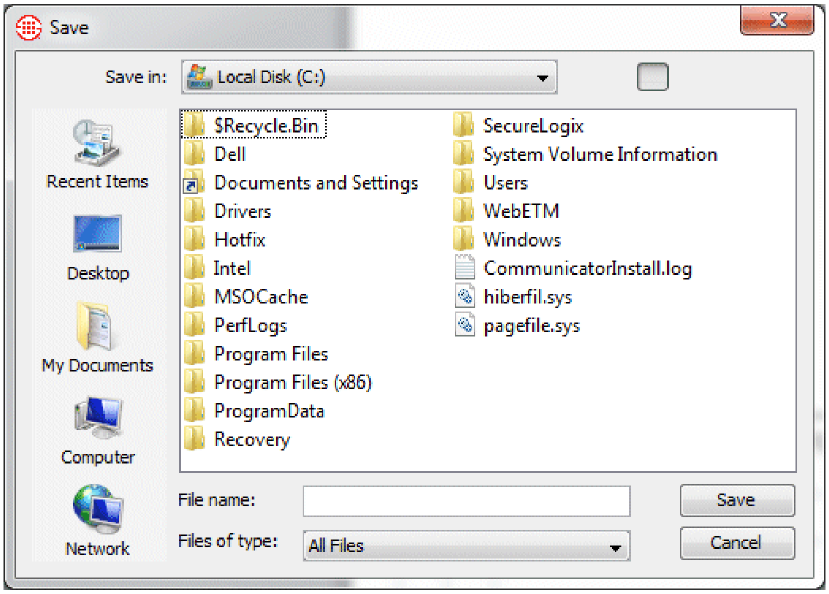
- Right-click the **Source** or **Destination** column heading, click **Display**, and then click **Show Name** or **Show Number**.

Exporting the Policy Log

You can export the contents of the **Policy Log** display to a comma-separated values (CSV) file that can then be imported into other programs, such as Microsoft Excel. When you export the **Policy Log**, only the records displayed onscreen are included. Filter settings are maintained.

To export the Policy Log display to a CSV file

1. On the **Policy Log** main menu, click **Log | Export**. A **Save** dialog box appears.



Save in: Local Disk (C:)

File name:

Files of type: All Files

2. Browse to the location where you want to save the file, and then click **Save**. Note that unless you specify a different file extension, the file is saved with a **.txt** extension.

Printing the Policy Log

When you print a **Policy Log**, only the records displayed onscreen are included. Filter settings are maintained.

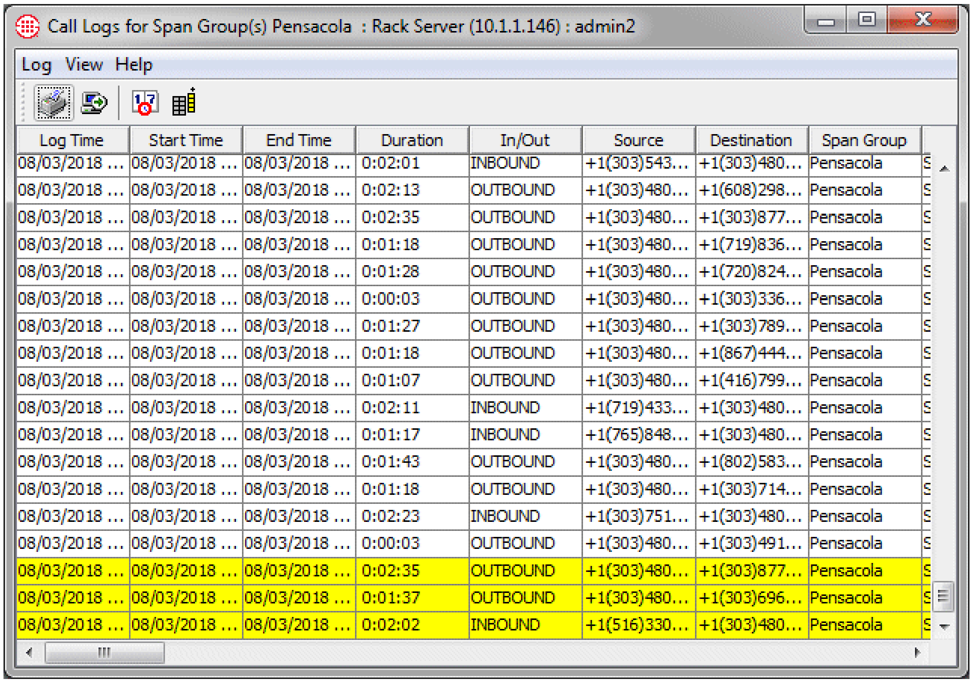
To print the Policy Log

- On the **Policy Log** main menu, click **Log | Print**. The typical Print dialog box for your computer appears. Select printing properties and print the file as you would with any other application.

Call Logs

The **Call Log** provides details about each call monitored by a given Span Group, independent of Policy processing. Information regarding triggered Firewall Policy Rules is also included for the calls. Since IPS Policies are based on call pattern accumulations and not individual calls, no IPS Policy processing fields appear in this Log.

You can also view the **Call Log** for multiple Span Groups at once.



Call Logs for Span Group(s) Pensacola : Rack Server (10.1.1.146) : admin2

Log Time	Start Time	End Time	Duration	In/Out	Source	Destination	Span Group	
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:01	INBOUND	+1(303)543…	+1(303)480…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:13	OUTBOUND	+1(303)480…	+1(608)298…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:35	OUTBOUND	+1(303)480…	+1(303)877…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:18	OUTBOUND	+1(303)480…	+1(719)836…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:28	OUTBOUND	+1(303)480…	+1(720)824…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:03	OUTBOUND	+1(303)480…	+1(303)336…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:27	OUTBOUND	+1(303)480…	+1(303)789…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:18	OUTBOUND	+1(303)480…	+1(867)444…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:07	OUTBOUND	+1(303)480…	+1(416)799…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:11	INBOUND	+1(719)433…	+1(303)480…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:17	INBOUND	+1(765)848…	+1(303)480…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:43	OUTBOUND	+1(303)480…	+1(802)583…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:18	OUTBOUND	+1(303)480…	+1(303)714…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:23	INBOUND	+1(303)751…	+1(303)480…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:00:03	OUTBOUND	+1(303)480…	+1(303)491…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:35	OUTBOUND	+1(303)480…	+1(303)877…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:01:37	OUTBOUND	+1(303)480…	+1(303)696…	Pensacola	S
08/03/2018 …	08/03/2018 …	08/03/2018 …	0:02:02	INBOUND	+1(516)330…	+1(303)480…	Pensacola	S

Tip Since SHIFT selects all contiguous items, use SHIFT only when all selected Span Groups are collapsed. Otherwise, individual Spans are also selected, and no menu is available.

To view the Call Log

1. In the Performance Manager tree pane, expand the **Span Groups** subtree.
2. Right-click the Span Group and click **View Call Logs**.
   - To view **Call Logs** for multiple Span Groups at once, hold down CTRL or SHIFT, click each Span Group, and then right click the selection and click **View Call Logs**.

Displaying Name or Number

You can choose whether to display the Directory name or the phone number/URI in the **Source** and **Destination** columns of the **Call Log**. Each column can be set independently.

To specify Directory Name or Phone Number/URI

- Right-click the **Source** or **Destination** column heading, click **Display**, and then click **Show Name** or **Show Number**.

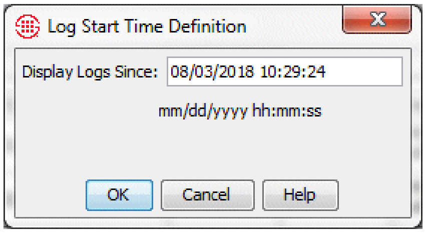
Setting the Start Time of the Call Log

If you want to retrieve log data for more time than the defined **Log Retrieval Amount** in the current instance, see the procedure below. Note that the retrieved data is still constrained by the setting in the **Allow Logs to Grow to n Items** box.

By default, the **Call Log** displays information based on the **Log Retrieval Amount** and **Allow Logs to Grow to n Items** settings on the **Log** tab of the **Properties** dialog box. See "Setting Display Preferences for the Policy Log" on page 204 for instructions for changing these settings.

To select the starting time of information presented in the log

1. On the **Call Log** main menu, click **View | Set Start Time**. The **Log Start Time Definition** dialog box appears.



Display Logs Since: 08/03/2018 10:29:24

mm/dd/yyyy hh:mm:ss

2. In the **Display Logs Since** box, type the starting date and time for which you want to limit displaying log information, in the format **mm/dd/yyyy hh:mm:ss**.

The date and time that you type here must be prior to the date that appears in the **Display Logs Since** box. If you want to restart the log at the current date and time, close the **Call Log**, and then reopen it.

Fields in the Call Log

Each of the fields in the **Call Log** is described below. The Firewall **Policy Log** contains the same fields; however, the **Policy Log** only contains data for calls that trigger a tracked Rule, while the **Call Log** contains data for all calls monitored by the selected Span Group(s).

Column Heading	Information Displayed
Ambiguous FW Rule?	Whether the call was ambiguous with respect to a Firewall Policy Rule, either **Yes** or **No**. If the call matched multiple Rules, values are listed in the order in which the Rules were matched. Correlate them with the Rule #s in the **Firewall Rule** field for the call.
Appliance	Name of the Appliance through which the monitored call passed.
Bytes-Inbound	On VoIP calls, the number of inbound payload bytes transmitted.
Bytes-Outbound	On VoIP calls, the number of outbound payload bytes transmitted.

Fields in the Call Log, continued

Column Heading	Information Displayed
Call Details	Call classification information (i.e., local, long distance, toll-free). See "Call Labels" in the *Usage Manager User Guide* for a description of these labels. These labels are also used to define Service Types. See "Service Types" on page 80 for more information.
Call ID	Unique key that is assigned by the Span to every call. (Do not confuse with Caller ID.)

Column Heading	Information Displayed
Caller ID	Caller ID information and error messages.
Card	Name of the Card containing the Span that executed the Rule.
Channel	Channel number that carried the call.
Codec-Inbound	On VoIP calls, the codec used for the inbound call data.
Codec-Outbound	On VoIP calls, the codec used for the outbound call data.
Connect Time	Time at which the call was answered.
Destination	Destination telephone number/URI or its associated name, depending on selection.
Destination Details	Phone number classification information about the called phone number; e.g., 800,PN indicates that it was a toll free call. See "Phone Number Labels" *Usage Manager User Guide* for descriptions of the labels.
Duration	The amount of time elapsed since Start Time (when the line was seized).
Egress Trunk	The outbound trunk.
Egress Channel	The outbound channel.
End Time	End date and time of the call (typically the same as Log Time).
Firewall Comment	Comments associated with the Firewall Policy Rule that fired (or "Ambiguous" if the call was ambiguous with respect to the Rule). Blank if no comment in the Rule.
Firewall Policy ID	System-generated Policy ID number.
Firewall Policy	Name of the Firewall Policy containing the Rule. A Firewall Policy Rule fires for every monitored call. If no user-defined Policy is installed, the Default Policy appears here.
Firewall Rule #	Number of the Firewall Policy Rule that fired (Implied Rules are numbered 0 and 9999).
Firewall Tracks	Track actions (Log, Alert, Email, SNMP, syslog) generated by a Firewall Policy Rule firing.
Ingress Trunk	The inbound trunk.
Ingress Channel	The inbound channel.
In/Out	Whether the call was inbound or outbound.
Jitter-Inbound	On VoIP calls, inbound jitter (relates to call quality; a measure of the variability of packet arrival).
Jitter-Outbound	On VoIP calls, outbound jitter (relates to call quality; a measure of the variability of packet arrival).
Log Time	Date and time an entry was made in the log.

Fields in the Call Log, continued

Column Heading	Information Displayed
Packetloss-Inbound	On VoIP calls, inbound packet loss (relates to call quality; a measure of the number of lost packets).
Packetloss-Outbound	On VoIP calls, outbound packet loss (relates to call quality; a measure of the number of lost packets).
Packets-Inbound	On VoIP calls, the count of inbound packets.
Packets-Outbound	On VoIP calls, the count of outbound packets.
Prefix	Digits dialed before the phone number, such as outside access number or long distance access code.
Rate-Inbound	On VoIP calls, the inbound media rate.
Rate-Outbound	On VoIP calls, the outbound media rate.
Raw Destination	Actual digits dialed.
SMDR #1 **SMDR #2** **SMDR #3**	These columns are user-configurable to display portions of SMDR data. The SMDR definition file must be edited to capture the requested data. See "Final Fields" in the *ETM® System Technical Reference* for instructions for defining these fields.
SMDR Access Code	The Access Code of the calling party, extracted from SMDR data. This field only appears if you have the **View Access Codes** user permission. See the *ETM® System Technical Reference* for instructions for configuring the SMDR parse file to extract access codes. See "Access Code Sets" on page 140 for information about using Access Code Sets to associate access codes extracted from SMDR with Listings in the ETM Directory.
Source	Originating telephone number or its associated name, depending on selection. Right-click the column heading to toggle this setting.
Source Details	Phone number classification information about the calling phone number; e.g., PN, MAP indicates that the Extension Map was used for Source. See "Phone Number Labels" in the *Usage Manager User Guide* for descriptions of the labels. If the call was ambiguous for SMDR, SMDR information about the possible matches is included, denoted as AMBIG_<*extension(s)*>.
Source IP	On VoIP calls, the IP address of the caller.
Destination IP	On VoIP calls, the IP address of the callee.
Span	Name of the Span that carried the call.
Span #	Number of the Span that carried the call.
Span Group	Name of the Span Group to which the Span carrying the call belongs..
Start Time	Start date and time of the call. For outgoing calls, this is the time at which the trunk was seized. For incoming calls, it is the time at which the phone began to ring.
Suffix	Digits dialed after the phone number, such as PINs and calling card number.

Fields in the Call Log, continued

Column Heading	Information Displayed
Switch	Name of the Switch through which the monitored call passed.
Termination Status	Whether the call was disconnect by Policy or ETM System User.
Terminator	If the call was disconnected by the ETM System, the entity that disconnected the call: Firewall, IPS, or User.
Trunk Group	Trunk group through which the call was processed, if defined.
Type	Type(s) of call (Fax, Modem, Modem Energy, Voice, Video, STU, Data Call, Busy, Unanswered, Undetermined). If the call type changed during the call, multiple types are listed.
Type Count	The count of call type changes during the call.

Filtering the Call Log

You can limit the display in the **Call Log** to calls containing specific types of data. To do this, you apply a filter to one or more columns to specify criteria for the types of calls you want to display. Column headings to which a filter is applied appear in red.

To filter the Call Log display

- Right-click a column heading, and then click **Edit Filter**. To remove a filter, right-click the column heading, and then click **Remove Filter**.

The Filter dialog box that appears depends on which field you selected. See "Using Filters in the ETM® System" on page 217 for instructions for using each type of filter.

Printing the Call Log

When you print the **Call Log**, only the records displayed onscreen are included. Filter settings are maintained.

To print the Call Log

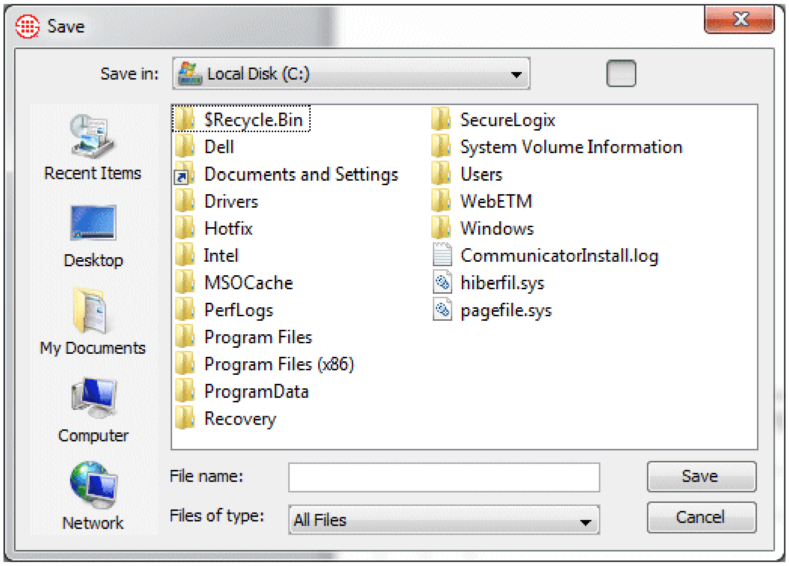
- On the **Call Log** main menu, click **Log | Print**. The typical Print dialog box for your computer appears. Select printing properties and print the file as you would with any other application.

Exporting the Call Log

You can export the contents of the **Call Log** display to a comma-separated values (CSV) file that can then be imported into other programs, such as Microsoft Excel. When you export the **Call Log**, only the records displayed onscreen are included. Filter settings are maintained.

To export the Call Log display to a CSV file

1. On the **Call Log** main menu, click **Log | Export**. A **Save** dialog box appears.



Save in: Local Disk (C:)

Files of type: All Files

2. Browse to the location where you want to save the file, and then click **Save**. Note that unless you specify a different file extension, the file is saved with a **.txt** extension.

Viewing Health and Status

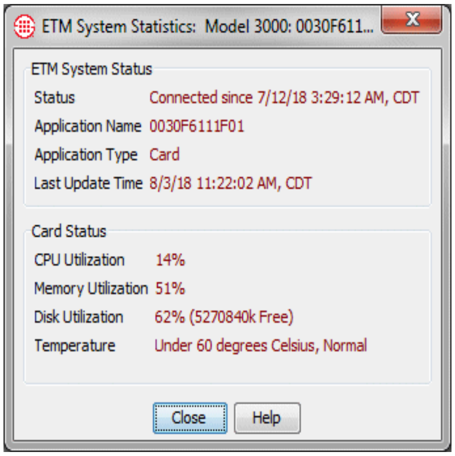
You can view the health and status of Cards, Spans, Call Recording Caches, and applications. The information included depends on the item selected, as described in the following sections.

To view health and status

- In the **Platform Configuration** subtree of the Performance Manager tree pane, right-click the icon for the item and then click **Health & Status**.

  The **ETM System Statistics** dialog box appears, with the name of the selected item in the title bar. Statistics are provided as of the most recent heartbeat. If connection to the ETM Server is lost, the status changes to **Not connected** and the "snapshot" of the last known information as of the last update time is shown.

Card Health and Status



ETM System Statistics: Model 3000: 0030F611...

ETM System Status

Status Connected since 7/12/18 3:29:12 AM, CDT

Application Name 0030F6111F01

Application Type Card

Last Update Time 8/3/18 11:22:02 AM, CDT

Card Status

CPU Utilization 14%

Memory Utilization 51%

Disk Utilization 62% (5270840k Free)

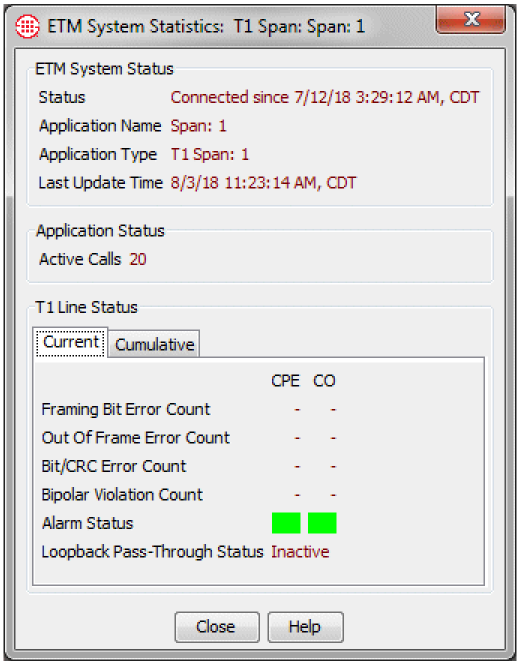
Temperature Under 60 degrees Celsius, Normal

The following table describes the Card status information provided. in the **System Statistics** dialog box

Type of Status	**Fields**
ETM® System Status	**Status**—The connection status of the Card: Connected since <*date_and_time*> or **Not Connected**. **Application Name**—The name assigned to the Card in the **Card Configuration** dialog box. **Application Type**—Card. **Last Update Time**—The time of the last Card heartbeat, at which the display was updated.
Card Status	**CPU Utilization**—The percentage of the Card's CPU resources in use. **Memory Utilization**—The percentage of the Card's RAM in use. **Disk Utilization**—The percentage of the Card's disk storage in use. **Temperature**—The temperature of the Card in degrees Celsius. Less than 60 degrees Celsius is normal; between 60 and 70° C is warm; and above 70° C is hot. On the 1000 series, reported as 0, 60, or 70 degrees C; on the 2100 and 3200, actual temperature reading reported.

Telco Span Health and Status

On T1 and E1 Spans (CAS, PRI, and SS7), both current and cumulative T1 or E1 line statistics are provided. On Recording Spans, recording data is also provided. The following image shows health and status for a T1 Span.



ETM System Statistics: T1 Span: Span: 1

ETM System Status

Status Connected since 7/12/18 3:29:12 AM, CDT

Application Name Span: 1

Application Type T1 Span: 1

Last Update Time 8/3/18 11:23:14 AM, CDT

Application Status

Active Calls 20

T1 Line Status

	CPE	CO
Framing Bit Error Count	-	-
Out Of Frame Error Count	-	-
Bit/CRC Error Count	-	-
Bipolar Violation Count	-	-
Alarm Status	🟩	🟩
Loopback Pass-Through Status	Inactive	

The table below describes the Span Health and Status fields information provided, by Span type.

Type of Status	Fields
ETM® System Status	**Status**—The connection status of the Span: Connected since <*date_and_time*> or Not Connected. **Application Name**—The name assigned to the Span in the **Span Configuration** dialog box. **Application Type**—The type of Span (Analog, PRI, E1 CAS, E1 PRI, SIP, T1) and the Span number (1, 2, 3, or 4). **Last Update Time**—The time of the last Span heartbeat, at which the display was updated.
Application Status	**Active Calls**—Shows the number of calls that were being processed by the Span at the last update time.

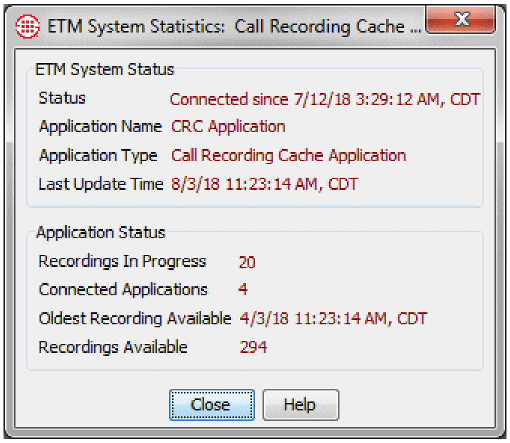
Span Health and Status field, continued

<table>
<tr><th>Type of Status</th><th colspan="2">Fields</th></tr>
<tr><td><b>E1 Line Status</b> (E1 Spans only-CAS, SS7, PRI) Provides both current and cumulative values. The <b>Current</b> tab reports values for one heartbeat Interval, as of the last heartbeat. The <b>Cumulative</b> tab reports total values since the <b>Last Reset</b> time.</td><td colspan="2"><b>Framing Bit Error Count</b>—Count of framing bit errors.
<b>Far End Block</b>—Count of Cyclic Redundancy Check (CRC) errors encountered by the upstream device, based on the data sent upstream by the ETM® System.
<b>CRC Error Count</b>—Count of CRC errors in received data.
<b>Line Code Error</b>—Count of line encoding errors in received data.
<b>Alarm Status</b> (<b>Current</b> tab only)—Status of telecom alarms at the time of the last heartbeat: Green, Yellow, or Blue (matches Card LEDs except that the Blue alarm lights the red LED.)
<b>Last Reset</b> (<b>Cumulative</b> tab only)—Time at which <b>Reset</b> was last clicked to reset all cumulative values to 0 or the Span was last restarted.</td></tr>
<tr><td><b>T1 Line Status</b> (T1 Spans only-CAS, PRI, and SS7). Provides both current and cumulative values. The Current tab reports values for one heartbeat Interval, as of the last heartbeat. The Cumulative tab reports total values since the Last Reset time.</td><td colspan="2"><b>Framing Bit Error Count</b>—Count of framing bit errors.
<b>Out of Frame Error Count</b>—Count of out-of-frame-errors.
<b>Bit Error Count</b>—Count of bit errors.
<b>Alarm Status</b> (<b>Current</b> tab only)—Status of telecom alarms at the time of the last heartbeat: Green, Yellow, or Blue (matches Card LEDs except that the Blue alarm lights the red LED.)
<b>Loopback Pass-Through Status</b>—Whether the Span is currently in loopback test pass-through mode.
<b>Last Reset</b> (<b>Cumulative</b> tab only)—Time at which Reset was last clicked to reset all cumulative values to 0 or the Span was last restarted.</td></tr>
<tr><td><b>PRI Line Status</b>
(All PRI Spans)</td><td colspan="2"><b>Link Status</b>—D-channel down or up as of the last heartbeat.
<b>Layer 3 Message Count</b>—Count of D-channel messages during the heartbeat Interval.</td></tr>
<tr><td><b>SIP Trunk Status</b> (SIP Proxy Only)</td><td colspan="2"><b>Internal and External Status for each logical trunk.</b> Green if up, Red if down, Black if not connected.</td></tr>
<tr><td><b>SIP Application Status</b>
(SIP Proxy Only)</td><td colspan="2"><b>Call Processor Status—</b>Available or Unavailable; Unknown if Call Processor is not connected to Server.
<b>Signal Proxy Status—</b>Available or Unavailable; Unknown if Call Processor is not connected to Server.
<b>Media Proxy Status—</b>Available or Unavailable; Unknown if Call Processor is not connected to Server.</td></tr>
<tr><td><b>SS7 Bearer</b> (SS7 Bearer Spans only)</td><td colspan="2"><b>Signaling Message Count</b>—Count of Signaling Link messages in the heartbeat interval.</td></tr>
<tr><td rowspan="3"><b>SS7 Signaling Link</b>
(SS7 Signaling Links and Bearer Spans only)
Status shown as of the last</td><td colspan="2"><b>Link Status</b>—Link status (Up or Down) for each link as of the last heartbeat.</td></tr>
<tr><td><b>CO LSSU Message Count</b></td><td><b>PE ISUP Message Count</b></td></tr>
<tr><td><b>CO ISUP Message Count</b></td><td><b>PELSSU Message Count</b></td></tr>
</table>

heartbeat.	**CO SNM and SNT Message Count**	**PE SNM and SNT Message Count**

CRC Health and Status

The table below lists the health and status information provided for the CRC.



ETM System Statistics: Call Recording Cache ...

ETM System Status

Status Connected since 7/12/18 3:29:12 AM, CDT

Application Name CRC Application

Application Type Call Recording Cache Application

Last Update Time 8/3/18 11:23:14 AM, CDT

Application Status

Recordings In Progress 20

Connected Applications 4

Oldest Recording Available 4/3/18 11:23:14 AM, CDT

Recordings Available 294

Type of Status	Fields
ETM® System Status	**Status**—The connection status of the CRC: Connected since *<date_and_time>* or Not Connected. **Application Name**—The name assigned to the CRC in the **Call Recording Cache Configuration** dialog box. **Application Type**—Call Recording Cache application. **Last Update Time**—The time of the last heartbeat, at which the display was updated.
Application Status	**Recordings in Progress—**The number of call recordings currently being transferred to the CRC. **Connected Applications—**The number of recording Spans currently connected to the CRC. **Oldest Recording Available—**The date and time of the oldest recording on the CRC. **Recordings Available**—The count of recordings on the CRC.

SMDR Debug Logs

SMDR debug logging stores SMDR data and debugging information. This information can be used by SecureLogix Customer Support for troubleshooting SMDR resolution issues. Only enable SMDR debug logging if instructed to do so by SecureLogix Technical Support personnel, to avoid using hard drive space unnecessarily. The SMDR debug logging setting does not affect how the ETM System uses SMDR information. See "Enabling SMDR Debug Logging" in the *ETM® System Administration and*

Maintenance Guide for instructions. See the *ETM® System Technical Reference* for instructions for reading the SMDR debug log.

Appliance Event Debug Logs

Appliance event logs can be used by SecureLogix Technical Support for troubleshooting. To avoid unnecessarily consuming hard drive space, only enable call/debug logging if instructed to do so by SecureLogix Customer Support personnel. See "Appliance Debug Event Logging" in the *ETM® System Administration and Maintenance Guide* for instructions.

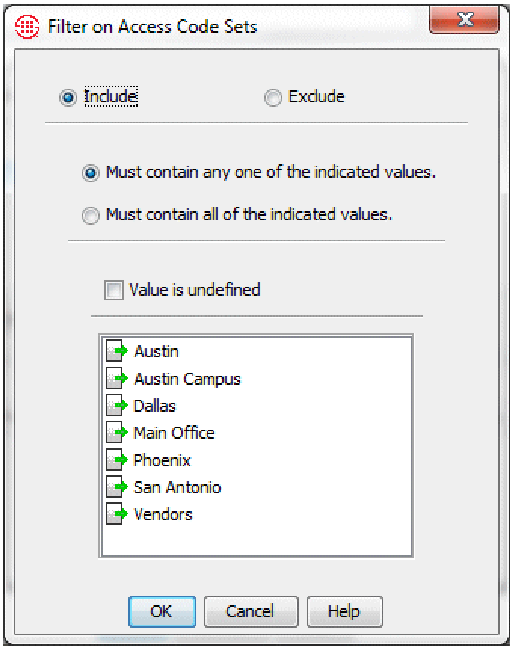
Using Filters in the ETM® System

Filter dialog boxes are provided in tools throughout the ETM System. These filter dialog boxes enable you to specify criteria for the data to be retrieved or displayed. Procedures for using each of these filters are provided below.

Access Code Set Filter

Apply the **Access Code Set** filter to the **Access Code Set** field of a Directory Filter or Report Element to filter for Listings associated with a specific Access Code Set.

To define an Access Code Set filter



Filter on Access Code Sets

● Include ○ Exclude

● Must contain any one of the indicated values.

○ Must contain all of the indicated values.

□ Value is undefined

- Austin
- Austin Campus
- Dallas
- Main Office
- Phoenix
- San Antonio
- Vendors

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - Select one of the following options:

Must contain any one of the indicated values to include Listings associated with at least one of the specified sets.

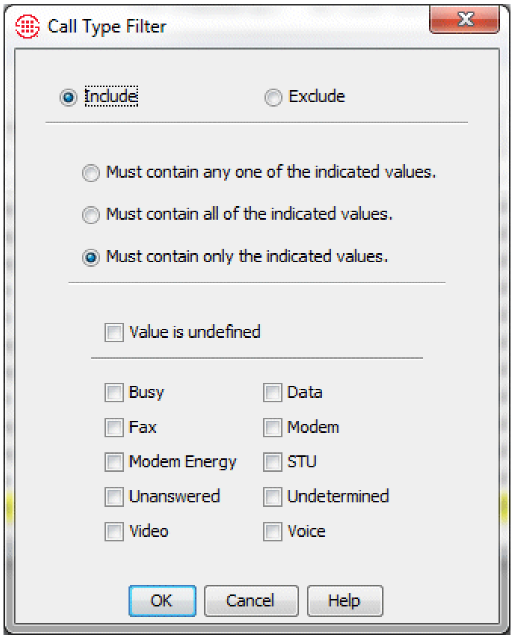
Must contain all of the indicated values to include only Listings associated with all of the specified sets; they may also be associated with other sets.

3. If you selected one of the **Must contain...** options, select one or more Access Code Sets to filter for. To select multiple sets, hold down CTRL while clicking.

Call Type Filter

Apply the **Call Type** filter to the **Type** field to include only data for one or more specific call types. See "Call Types Reported by the ETM® System" on page 19 for a description of each of the call types.

To define a Call Type Filter



Call Type Filter

● Include ○ Exclude

○ Must contain any one of the indicated values.

○ Must contain all of the indicated values.

● Must contain only the indicated values.

□ Value is undefined

□ Busy □ Data

□ Fax □ Modem

□ Modem Energy □ STU

□ Unanswered □ Undetermined

□ Video □ Voice

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Do one of the following:

   - To filter for records that do not have a value in this column, select **Value is undefined**.

   - Select one of the following options:

     Must contain any one of the indicated values to include records that contain at least one of the specified types.

Must contain all of the indicated values to include only records that contain all of the specified call types; they may include other call types.

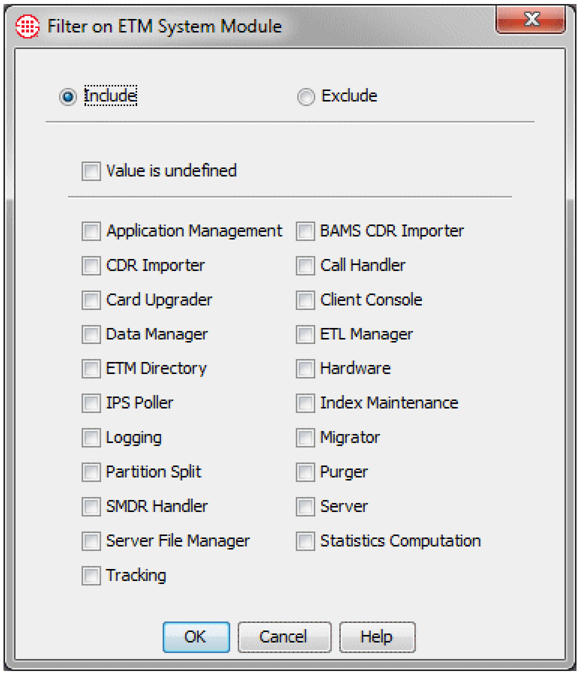
Must contain only the indicated values to include only records that contain all of the specified call types and no others.

3. If you selected one of the **Must contain...** options, select one or more call types to filter for.

Filter on ETM® System Module

Apply the **Filter on ETM® System Module** filter to the **Reported By** field of the **Diagnostic Log** and reports to include only data reported by a specific ETM® System module.

To define an ETM® System Module filter



Filter on ETM System Module

● Include ○ Exclude

□ Value is undefined

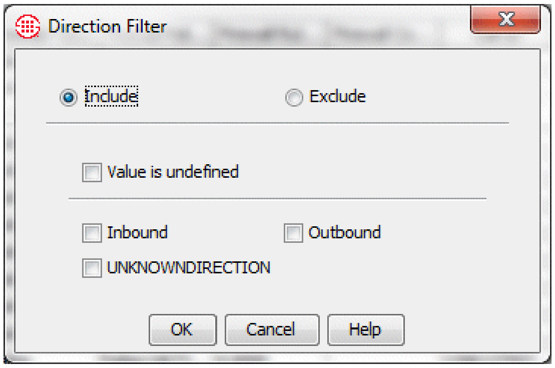
□ Application Management □ BAMS CDR Importer
□ CDR Importer □ Call Handler
□ Card Upgrader □ Client Console
□ Data Manager □ ETL Manager
□ ETM Directory □ Hardware
□ IPS Poller □ Index Maintenance
□ Logging □ Migrator
□ Partition Split □ Purger
□ SMDR Handler □ Server
□ Server File Manager □ Statistics Computation
□ Tracking

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Select the ETM System Module to filter for.

Direction Filter

Apply the **Direction Filter** to the **In/Out** field to include only data for inbound or outbound calls.



To define a Direction Filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - To filter for outgoing calls, click the **Outbound** check box.
   - To filter for incoming calls, click the **Inbound** check box.

String Filter

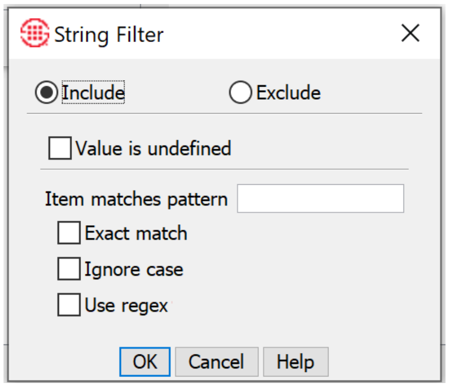
You can use the **String Filter** on many string-based fields to locate records containing a given string of characters. . Regex are supported. When defining a **String Filter** in the Directory Manager, use normal regex syntax. When defining a **String Filter** in other tools, use the following syntax:

```
.*<regular_expression>.*
```

For example:

```
.*/d.*
```

To define a String Filter



1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Do one of the following:

   - To filter for records that do not have a value in this column, select the **Value is undefined** check box.

   - In the **Items matches pattern** box, type the character string for which you want to filter.

     - You can also use the wildcard characters * (to match 0 or more unspecified characters; for example, `Jon*` matches `Jones` and `Jonathan`.) and ? (to match 1 additional unspecified character; for example, `Mat?` matches `Matt` and `Math` but not `Mathias`). If you actually want to search for a string that contains a * or ?, you must "escape" the character with a backslash. For example, to search only for the string "Modem?" you would select the **Exact Match** box and type: `Modem\?`

     - To return only results that match the pattern exactly, select **Exact Match** (for example, `210` matches only `210`, not `1210`). If this check box is not selected, records that contain the specified string as part of a larger string are also returned (for example, `210` matches `2100`). You can use Wildcard characters regardless of whether you select **Exact Match**.

     - To find strings without regard to upper and lowercase characters, select the **Ignore Case** check box.

     - To filter using a regular expression, select the **Regex** check box and then type the regex. **Exact match** and **Ignore case** are grayed out if you are using a regex search.

       When defining a **String Filter** in the Directory Manager, use normal regex syntax. When defining a **String Filter** in other tools, use the following syntax:

       ```
       .*<regular_expression>.*
       ```

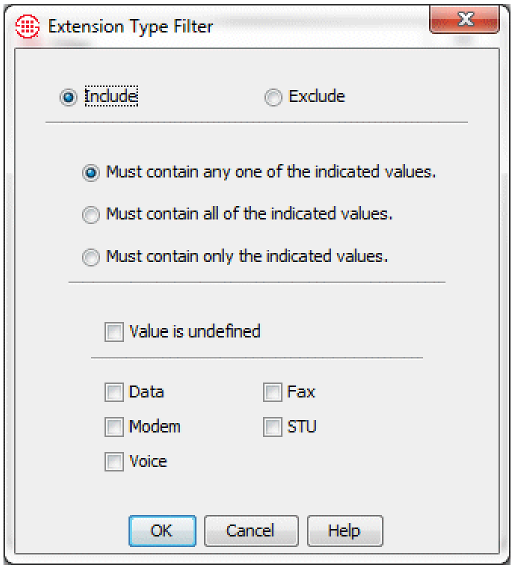
For example:

```
.*/d.*
```

Extension Type Filter

Apply the **Extension Type Filter** to the **Extension Type** field in Directory Report Elements to limit the data according to the Extension Types associated with the Listings involved in the call.

To define an Extension Type filter



Extension Type Filter

● Include ○ Exclude

● Must contain any one of the indicated values.

○ Must contain all of the indicated values.

○ Must contain only the indicated values.

□ Value is undefined

□ Data □ Fax

□ Modem □ STU

□ Voice

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Select one of the following:

   - **Must contain any one of the indicated values** to include data for calls that contain one or more (but not necessarily all) of the selected extension types.

   - **Must contain all of the indicated values** to include data only for calls containing all of the selected extension types.

   - **Must contain only the indicated values** to include only data for calls that contain the selected extension types.

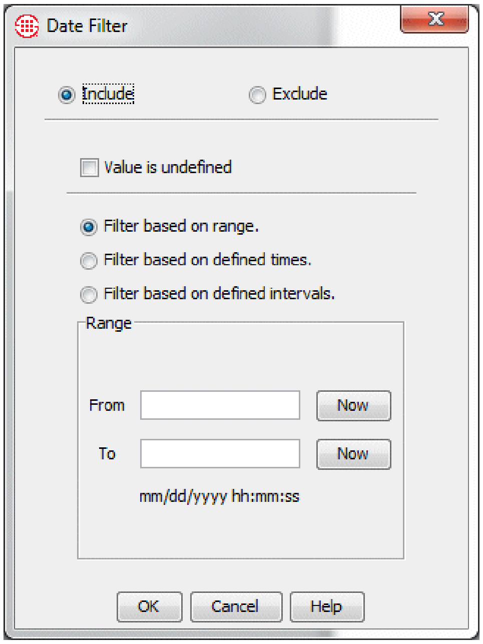
3. Do one of the following:

   - To filter for records that do not have a value in this column, select the **Value is undefined** check box.

   - Select one or more extension types to search for.

Date Filter

To define a Date Filter



● Include ○ Exclude

□ Value is undefined

● Filter based on range.
○ Filter based on defined times.
○ Filter based on defined intervals.

Range

From Now

To Now

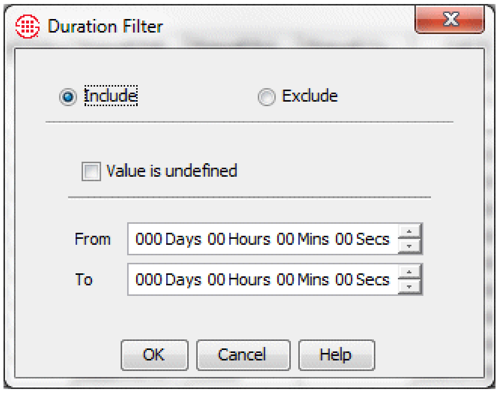
mm/dd/yyyy hh:mm:ss

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - To filter based on range of dates/times, select **Filter based on range**. Type the time range in the **From** or **To** boxes. To select the current date/time for either **From** or **To**, click **Now**.
   - Select **Filter based on defined times**, and then select the **Time**. **Times** are defined in the **Times** dialog box, accessed from the Performance Manager **Manage** menu. See “Times” on page 69 for instructions for defining Times.
   - Select **Filter based on defined Intervals**, and then select the Interval. Intervals are defined in the **Intervals** dialog box, accessed from the Performance Manager main menu.

Tip: See "Defining an Interval" on page 75 for instructions for defining Intervals.

Duration Filter

To define a Duration filter



Duration Filter

● Include ○ Exclude

□ Value is undefined

From 000 Days 00 Hours 00 Mins 00 Secs

To 000 Days 00 Hours 00 Mins 00 Secs

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - Specify the duration to filter for:
     a. In the **From** box, type or select the minimum duration you want to filter on, from 0 seconds up to 365 days.
     b. In the **To** box, type or select the maximum duration you want to filter on, from 0 seconds up to 365 days.

        The **From** duration must be less than the **To** duration. For example, to identify calls with durations between 30 minutes and 1 hour, select **Include**, and then type or select 30 minutes in the **From** box and 1 hour in the **To** box.

Phone Number Filter

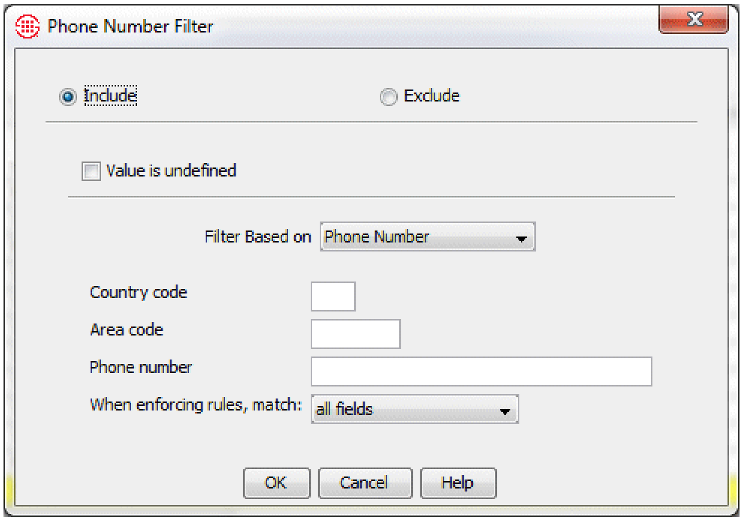
Four options are provided for filtering by phone number(s): **Phone Number, Phone Number Range**, **VoIP URI**, and **Existing Directory Object**. You can use one of the first three options to search for a single item or range. This is useful for applying a quick filter for a single Object or when the item you are looking for is not in the Directory. You can use the **Existing Directory Object** option to locate records containing phone numbers that are represented in the Directory. This option allows you to specify multiple filter criteria.

To define a Phone Number Filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.

- In the **Filter Based on** box, click the down arrow, and then do one of the following:

  <u>To filter on a single telephone number or portion thereof:</u>



Phone Number Filter

● Include ○ Exclude

□ Value is undefined

Filter Based on: Phone Number

Country code:

Area code:

Phone number:

When enforcing rules, match: all fields

a. Click **Phone Number**.

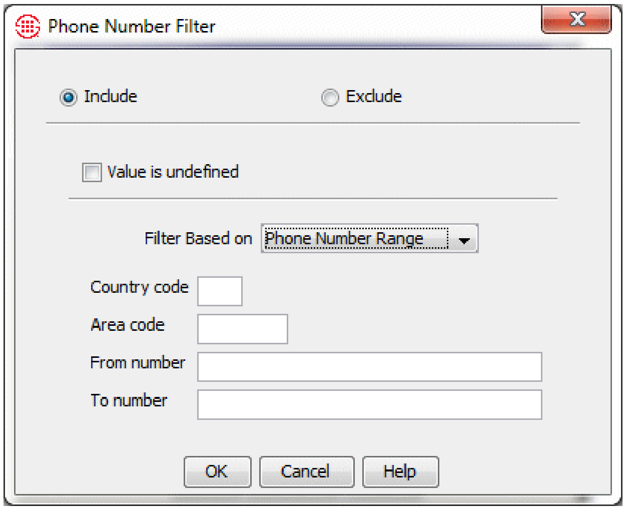
b. In the **When enforcing Rules, match** box, click the down arrow, and then click the option that represents which portion(s) of the phone number you want to match: **all fields** to match country code, area code, and phone number; **country code and area code**; or **country code only**.

c. Define the remaining fields that correspond with what you selected in the **When enforcing Rules, match** box:

   - In the **Country code** box, type the country code. A country code can contain a maximum of three digits.
   - In the **Area code** box, type the area/city code. An area code can contain a maximum of eight digits.
   - In the **Phone number** box, type the telephone number. A telephone number can contain a maximum of 36 digits. No non-numeric characters are allowed.

<u>To filter on a range of telephone numbers:</u>

a. Click **Phone Number Range**.



Phone Number Filter

● Include ○ Exclude

□ Value is undefined

Filter Based on Phone Number Range

b. In the **Country code** box, type the country code. A country code can contain a maximum of three digits.

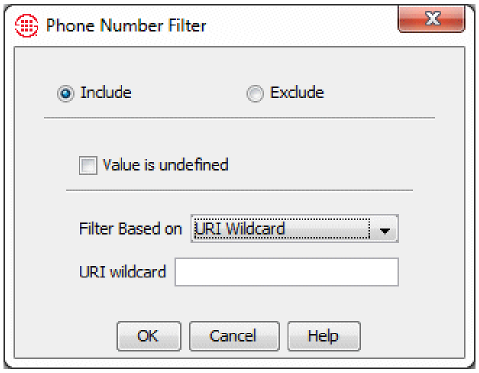
c. In the **Area code** box, type the area/city code. An area code can contain a maximum of eight digits.

d. In the **From number** box, type the beginning telephone number in the range. A telephone number can contain a maximum of 36 digits.

e. In the **To number** box, type the ending telephone number in the range. The **From** and **To** numbers must contain the same number of digits.

To filter based on a URI:

a. Click **URI Wildcard**.



Phone Number Filter

● Include ○ Exclude

□ Value is undefined

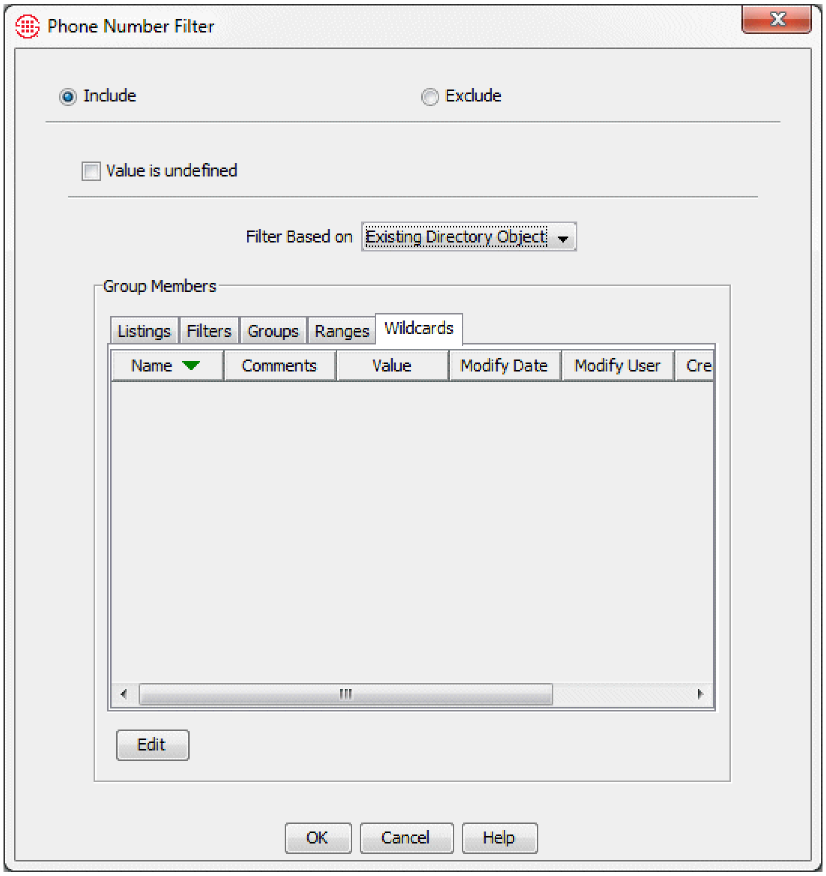
Filter Based on URI Wildcard

b. In the **URI Wildcard** box, type a regular expression denoting the URI.

TIP: If a URI is associated with a Directory Listing, you can instead filter by that Listing to retrieve records containing either phone numbers or URIs associated with that Listing. See the instructions below for filtering by an existing Directory Object.

c. Click **OK** to apply the filter and close the dialog box.

To filter based on one or more Directory entities:



Phone Number Filter

● Include ○ Exclude

□ Value is undefined

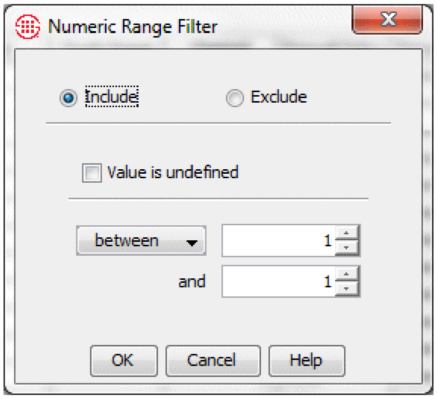
Filter Based on: Existing Directory Object

- Click **Existing Directory Object**. Define this Filter exactly as you would a Directory Group. See "Creating a Directory Group" on page 130 for instructions, if necessary.

3. Click **OK** to apply the filter.

Numeric Range Filter

To define a Numeric Range Filter



● Include ○ Exclude

□ Value is undefined

between 1

and 1

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Do one of the following:

   - To filter for records that do not have a value in this column, select **Value is undefined**.

   - Click the down arrow and select a comparison operator from the following options, and then specify the value(s).

     - **Between**: Type or select the range of numbers to filter for in the **From** and **To** boxes. For example, to see log entries only for channels 5 through 10, type 5 in the **From** box and 10 in the **To** box.

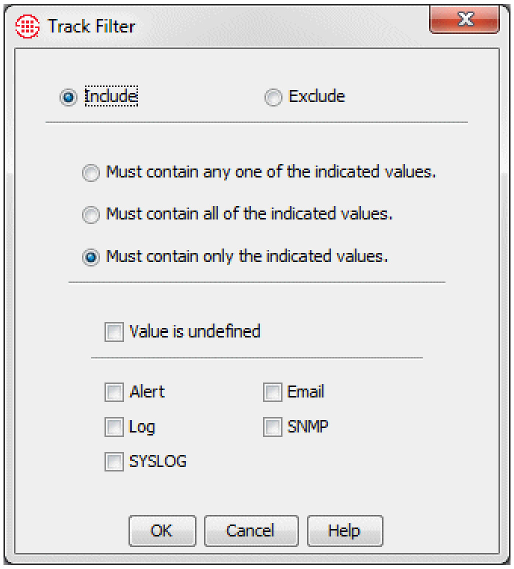
     - **Less Than**: Type or select the number results are to be less than.

     - **Greater Than**: Type or select the number results are to be greater than.

     - **Equal To**: Type or select the number results are to be equal to.

Track Filter

Apply a **Track Filter** to the **Tracks** field to include only data with one or more of the specified Tracks.



● Include ○ Exclude

○ Must contain any one of the indicated values.
○ Must contain all of the indicated values.
● Must contain only the indicated values.

□ Value is undefined

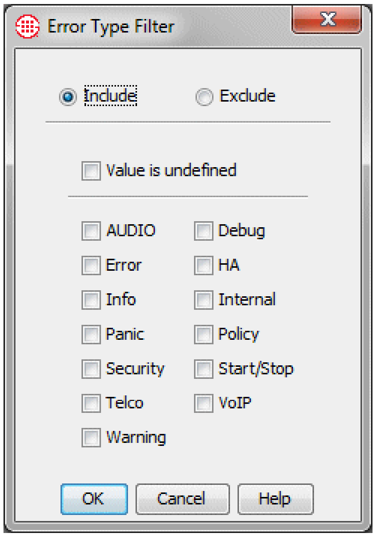
□ Alert □ Email
□ Log □ SNMP
□ SYSLOG

To define a Track Filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Select one of the following check boxes:
   - **Must contain any one of the selected values** to include data that contain one or more (but not necessarily all) of the selected Tracks.
   - **Must contain all of the selected values** to include only data containing all of the selected Tracks.
   - **Must contain only the selected values** to include data only if it contains the selected Track and no other Tracks.
3. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - Select the Track(s) to filter for: **Alert**, **Email**, **Log**, **SNMP**, **SYSLOG**.

Error Type Filter

The **Error Type Filter** dialog box is used to limit the information displayed in the **Diagnostic Log** and **Diagnostic Log** reports.



Error Type Filter

● Include ○ Exclude

□ Value is undefined

□ AUDIO □ Debug
□ Error □ HA
□ Info □ Internal
□ Panic □ Policy
□ Security □ Start/Stop
□ Telco □ VoIP
□ Warning

To define an Error Type Filter

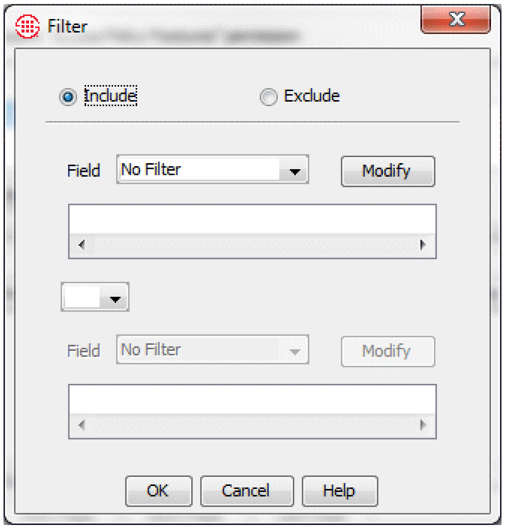
1. Select one of the following: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this field, select **Value is undefined**.
     - Select the system event/error type(s) to filter for from the following options: **Internal**, **Panic**, **Warning**, **Debug**, **Telco**, **VoIP**, **Security**, **Error**, **Start/Stop**, **Info**, **Policy**.
3. Click **OK** to apply the filter.

Filter on Import Sets

The **Filter on Import Sets** dialog box is used to filter by the Import Set to which a Listing belongs.

To define an Import Set filter

1. In a Directory Filter or the **Advanced** tab of the **Listing Search** dialog box, click **Modify**. The **Filter** dialog box appears.

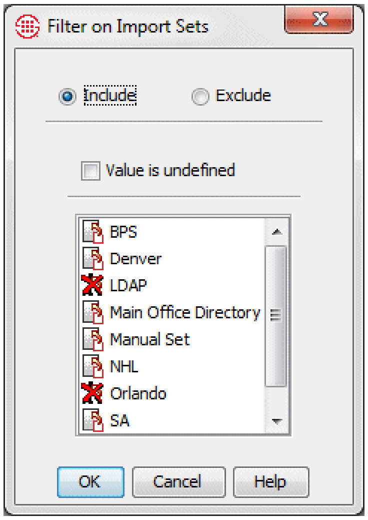


● Include ○ Exclude

Field No Filter

Field No Filter

2. In the **Field** box, elect **Import Set**. The **Filter on Import Set** dialog box appears.



● Include ○ Exclude

□ Value is undefined

3. Select **Include** to limit the data to calls containing Listings that belong to the specified Import Set; select **Exclude** to limit the data to calls that do not contain Listings that belong to the specified Import Set.

4. Do one of the following:

   - Select **Value is Undefined** if you want to filter out records that have no value for Import Set.

   - Click the Import Set to which the filter applies. You can select multiple Import Sets by holding down CTRL while clicking. Note that multiple selections in this dialog box are joined by **AND**. If you want **OR**, define a subfilter in the **Filter** dialog box.

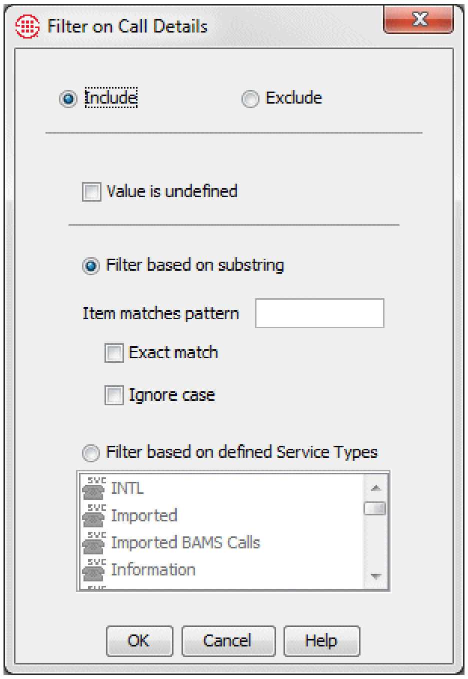
5. Click **OK** to apply the filter and close the dialog box. Click **Cancel** to discard the changes and close the dialog box.

Filter on Call Details

The **Filter on Call Details** dialog box is used to filter logs and reports for specific values in the **Call Details** field.

To apply a Call Details filter

1. Do one of the following:
   - In logs, right-click the **Call Details** field column header, and then click **Edit Filter**.
   - In the report element **Filter** dialog box, click the **Call Details** field.



Filter on Call Details

● Include ○ Exclude

□ Value is undefined

● Filter based on substring

Item matches pattern

□ Exact match

□ Ignore case

○ Filter based on defined Service Types

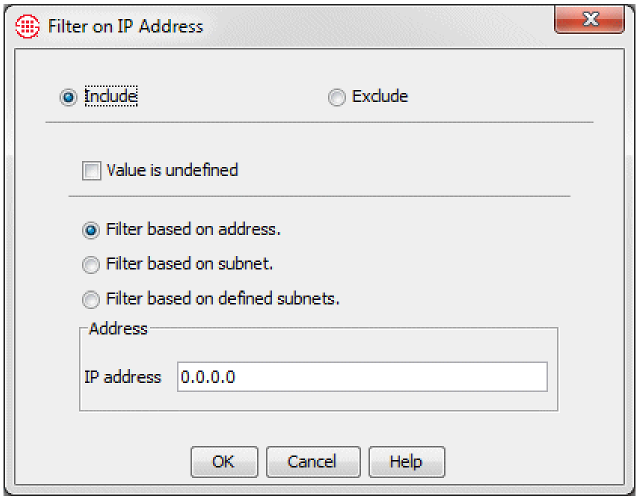
INTL
Imported
Imported BAMS Calls
Information

2. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
3. Do one of the following:
   - To filter for records that do not have a value in this column, select the **Value is undefined** check box.
   - Select **Filter based on substring**, and then type the character string for which you want to filter in the **Items containing substring** box.
   - Select **Filter based on defined Service Types**, and then select one or more Service Types.

4. If you typed a character string, to find strings without regard to upper and lowercase characters, select the **Ignore Case** check box.
5. If you want only exact matches returned, select the **Ignore case** check box. For example, if you type "LD" and want results that have only "LD" and not those that have "LD, Kansas," select the **Exact match** box.
6. Click **OK**.

Filter on IP Address

To filter by IP address



Filter on IP Address

● Include ○ Exclude

□ Value is undefined

● Filter based on address.

○ Filter based on subnet.

○ Filter based on defined subnets.

Address

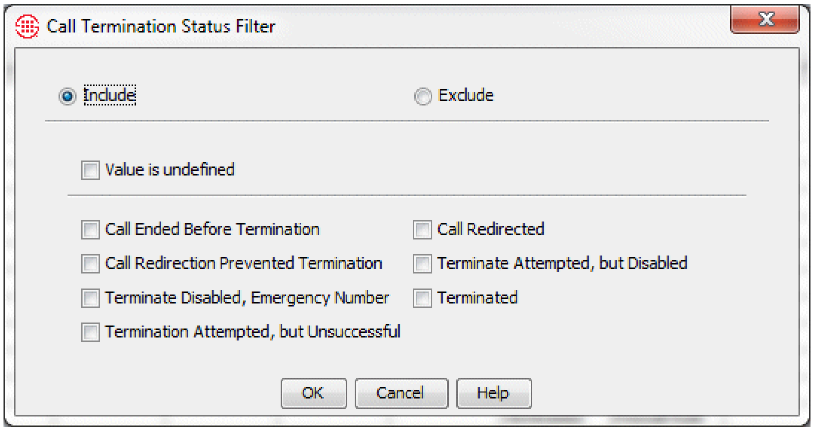
IP address: 0.0.0.0

1. Do one of the following:
   - In logs, right-click the **Source IP** or **Destination IP** column header and click **Edit Filter**.
   - In the Report Element **Filter** dialog box, select a field that includes **IP** in its name (**VoIP Source IP**, **VoIP Destination IP**, **VoIP Internal IP**, **VoIP External IP**).
2. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
3. Do one of the following:
   - To filter for records that do not have a value in this column, select the **Value is undefined** check box.
   - Select **Filter based on address**, and then type the IP address for which you want to filter in the **IP address** field.
   - Select **Filter based on subnet**, and then type the IP address ; select either **Mask** or **Prefix** and type the appropriate value.
   - Select **Filter on defined subnets**, and then click the Subnet in the **Predefined** box.

4. Click **OK**.

Call Termination Status Filter

Apply a **Call Termination Status Filter** to the **Termination Status** field to include only data for calls with the specified termination status.



Call Termination Status Filter

● Include ○ Exclude

□ Value is undefined

□ Call Ended Before Termination □ Call Redirected

□ Call Redirection Prevented Termination □ Terminate Attempted, but Disabled

□ Terminate Disabled, Emergency Number □ Terminated

□ Termination Attempted, but Unsuccessful

To define a Call Termination Status Filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Do one of the following:

   - To filter for records that do not have a value in this column, select **Value is undefined**.

   - Select the call disposition(s) to filter for:

     – **Call Ended Before Termination**—A Policy Rule or user attempted to terminate the call, but the call ended before termination occurred.

     – **Call Redirection Prevented Termination**—A Redirection Plan Rule caused the call to be redirected before termination occurred.

     – **Terminate Attempted, but Disabled**—A Policy Rule or user attempted to terminate the call, but termination was disabled for the Span in its configuration dialog box.

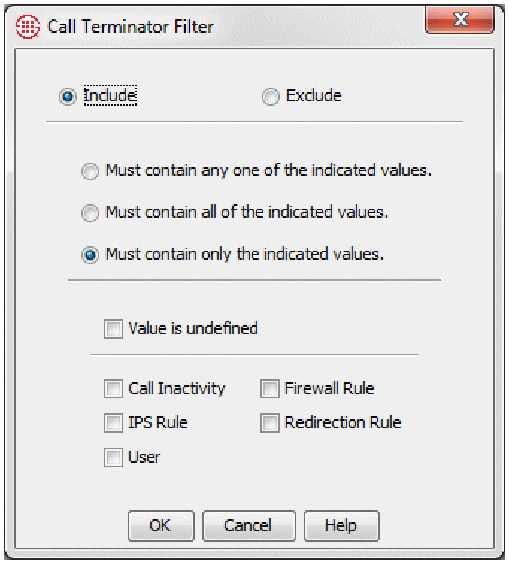
     – **Terminate Disabled, Emergency Number**—A Policy Rule or user attempted to terminate the call, but termination was disabled because the outbound destination was a member of an Emergency Group.

     – **Termination Attempted, but Unsuccessful**—The Span attempted to terminate the call, but termination failed for any reason other than those specifically listed.

- **Terminated**—The call was terminated by a Policy Rule or user.
- **Call Redirected**—The call matched a Redirection Plan Rule and was redirected.

Call Terminator Filter

Apply a **Call Terminator Filter** to limit data according to the entity that terminated the call.



Call Terminator Filter

● Include ○ Exclude

○ Must contain any one of the indicated values.

○ Must contain all of the indicated values.

● Must contain only the indicated values.

□ Value is undefined

□ Call Inactivity □ Firewall Rule

□ IPS Rule □ Redirection Rule

□ User

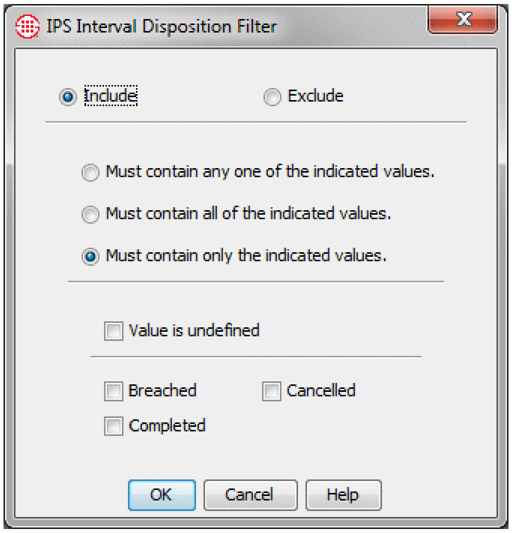
To define a Call Terminator filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Select one of the following options:
   - **Must contain any one of the indicated values**—Records containing any (but not necessarily all) of the specified values are included, even if they include other values as well.
   - **Must contain all of the indicated values**—Only records containing all of the specified values are included; the records may contain other values as well.
   - **Must contain only the specified values**—Only records containing just the specified value are included.
3. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - Select the call terminator(s) to filter for from the following options: **User, Firewall Rule, IPS Rule, Call Inactivity** (the call

inactivity timeout was reached). **Redirection Rule** (for redirected calls, not terminated calls.

IPS Interval Disposition Filter

Apply an **IPS Interval Disposition Filter** to Reports or the **IPS Policy Log** to include data only for Intervals with the specified value in the **Disposition** field.



● Include ○ Exclude

○ Must contain any one of the indicated values.

○ Must contain all of the indicated values.

● Must contain only the indicated values.

□ Value is undefined

□ Breached □ Cancelled

□ Completed

To define an IPS Interval Disposition Filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.

2. Select one of the following options:

   - **Must contain any one of the indicated values**—Records containing any (but not necessarily all) of the specified values are included, even if they include other values as well.

   - **Must contain all of the indicated values**—Only records containing all of the specified values are included; the records may contain other values as well.

   - **Must contain only the specified values**—Records containing only the specified value are included.

3. Do one of the following:

   - To filter for records that do not have a value in this column, select **Value is undefined**.

   - Select the Interval disposition(s) to filter for:

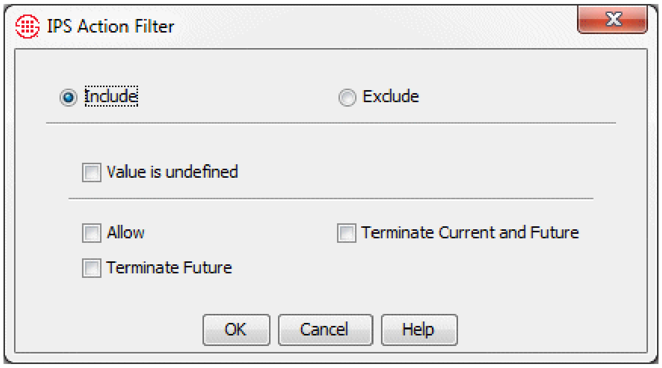
     Cancelled—The Rule was reset during the Interval.

     Completed—The Interval completed.

Breached—The Threshold for the Interval was breached. Note that a given Interval may be recorded as both Breached and Cancelled or Breached and Completed.

IPS Action Filter

Apply an **IPS Action Filter** to reports or the **IPS Policy Log** to include data only for triggered IPS Rules with the specified value in the **Action** field.



IPS Action Filter

● Include ○ Exclude

□ Value is undefined

□ Allow □ Terminate Current and Future

□ Terminate Future

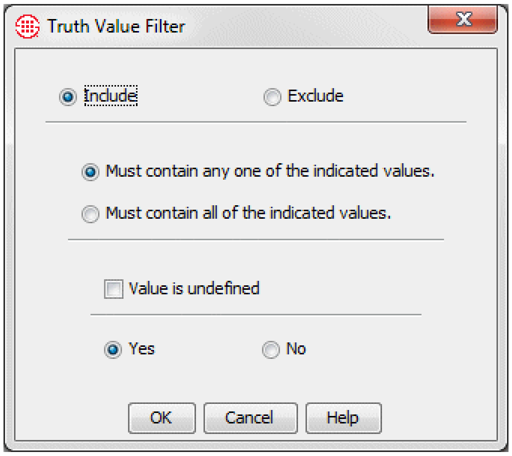
To define an IPS Action Filter

1. Select one of the following check boxes: **Include** to include data that matches the filter, or **Exclude** to exclude data that matches the filter.
2. Do one of the following:
   - To filter for records that do not have a value in this column, select **Value is undefined**.
   - Select one or more of the following actions:
     - **Allow**—The Rule allowed all calls during and after the threshold breach to continue.
     - **Terminate Future**—The Rule allowed the call that resulted in the threshold being breached to continue, but terminated future calls during the Interval.
     - **Terminate Current and Future**—The Rule terminated the call that resulted in the threshold breach and terminated all future calls during the Interval.

Truth Value Filter

The **Truth Value Filter** is used to filter for a yes or no value in certain fields in logs and reports, such as **Firewall Policy Ambiguity**.

To define a Truth Value Filter



● Include ○ Exclude

● Must contain any one of the indicated values.

○ Must contain all of the indicated values.

□ Value is undefined

● Yes ○ No

1. Select one of the following check boxes:

   - **Include**--Include records that match this filter. The default.

   - **Exclude**--Exclude records that match this filter.

2. Recall that more than one rule can fire for a given call. In that case, a value for each rule is present. Select one of the following check boxes:

   - **Must contain any one of the indicated values**--Include calls for which at least one fired rule (but not necessarily all fired rules) contains the selected value. The default.

   - **Must contain only the indicated values**--Include only calls for which all fired rules contain the selected value.

3. Do one of the following:

   - To filter for records that do not have a value in this column, select **Value is undefined**.

   - Select one of the following check boxes:

     - **Yes**—The condition represented by the field is true. For example, in the **Ambiguous FW Rule** field, **Yes** means the call was ambiguous toward the Rule. The default.

     - **No**—The condition represented by the field is false. For example, in the **Ambiguous FW Rule** field, **No** means the call was not ambiguous toward the Rule.

Removing Filters from Display Columns

To remove a filter from a display column

- Right-click the column heading, and then click **Remove Filter**.

Display and Automation Preferences

Setting User Interface Preferences

Certain aspects of the ETM® System user interfaces can be customized for display and automation preferences. These preferences include the content of display labels in dialog boxes, autostart of tools, color-coding options, and others.

Automation Preferences

Automation preferences include:

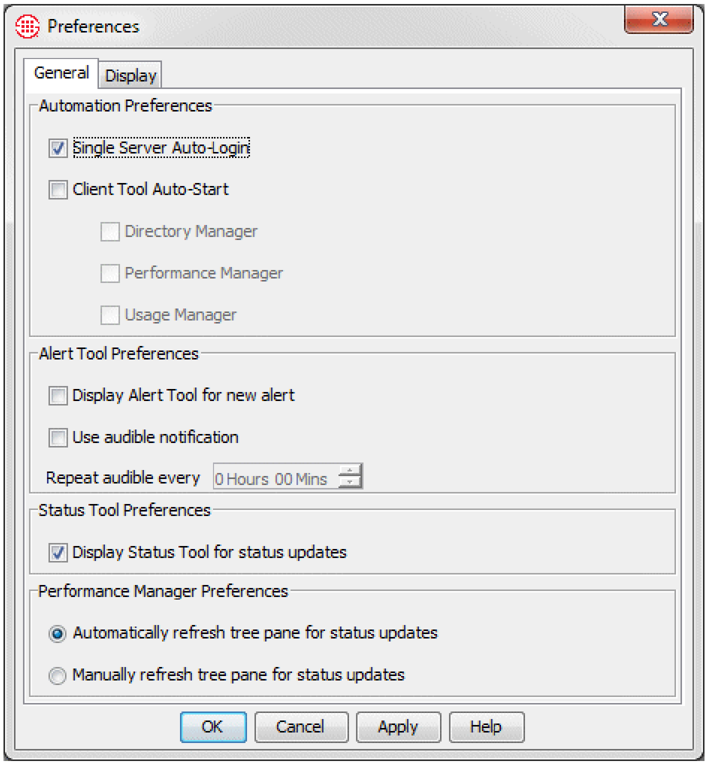
- Automatically launching the login dialog box when the ETM® System Console is opened if only a single server is defined.
- Automatically displaying the **Status Tool** for status updates.
- Automatically opening the Alert Tool for new alerts.
- Playing a sound at a specified Interval when a new alert is received.
- Automatically opening client applications upon login.

Enabling Single Server Autologin

If only one ETM Server is defined in the ETM® System Console, you can configure the system so that the **Login** dialog box for that ETM Server automatically appears when you open the ETM System Console. This simplifies login. If more than one Server is defined, this setting has no effect.

To enable single-server autologin

1. In the ETM System Console, click **Edit | Preferences**. The **Preferences** dialog box appears.



Preferences

General | Display

Automation Preferences

☑ Single Server Auto-Login

□ Client Tool Auto-Start

□ Directory Manager

□ Performance Manager

□ Usage Manager

Alert Tool Preferences

□ Display Alert Tool for new alert

□ Use audible notification

Repeat audible every 0 Hours 00 Mins

Status Tool Preferences

☑ Display Status Tool for status updates

Performance Manager Preferences

● Automatically refresh tree pane for status updates

○ Manually refresh tree pane for status updates

2. Select **Single Server Auto-Login**.

3. Click **OK**.

Setting Client Tools to Autostart upon Login

You can configure the system to automatically launch selected client tools when you log in. These settings apply to the workstation on which you set them. They are not specific to your user account or to a particular ETM® Server.

To autostart client tools upon login

1. In the ETM System Console, click **Edit | Preferences**. The **Preferences** dialog box appears.

2. In the **Automation Preferences** area of the **General** tab, select **Client Tool Auto-Start**. When you select the check box, three client tool options become available:

   - Directory Manager

   - Performance Manager

   - Usage Manager

3. Select each client tool you want to automatically open when you log in to a Management Server. Note that although all of the client tools can

be selected here, only those tools for which your user account has permission will actually open.

Enabling Manual Performance Manager Refresh

In deployments with large numbers of appliances connected to a single server and suboptimal network conditions, constant automatic status updates of the Performance Manager tree pane can cause the Performance Manager to become sluggish or nonresponsive. A manual refresh option was added to accommodate these unusual environments. By default, **Automatically refresh tree pane for status updates** is selected. Each change of state causes the tree pane to refresh.

To enable manual refresh

- On the **General** tab of the ETM System Console **Preferences** dialog box, select **Manually refresh tree pane for status updates**. If the Performance Manager is open when the selection is changed, it must be restarted to effect the change. Note that this setting applies to all connections from this client; it is not server-specific.

When **Manually refresh tree pane for status updates** is selected, a **Refresh** option becomes available on the Performance Manager **View** menu. Clicking that option causes the Performance Manager tree pane to refresh its status display.

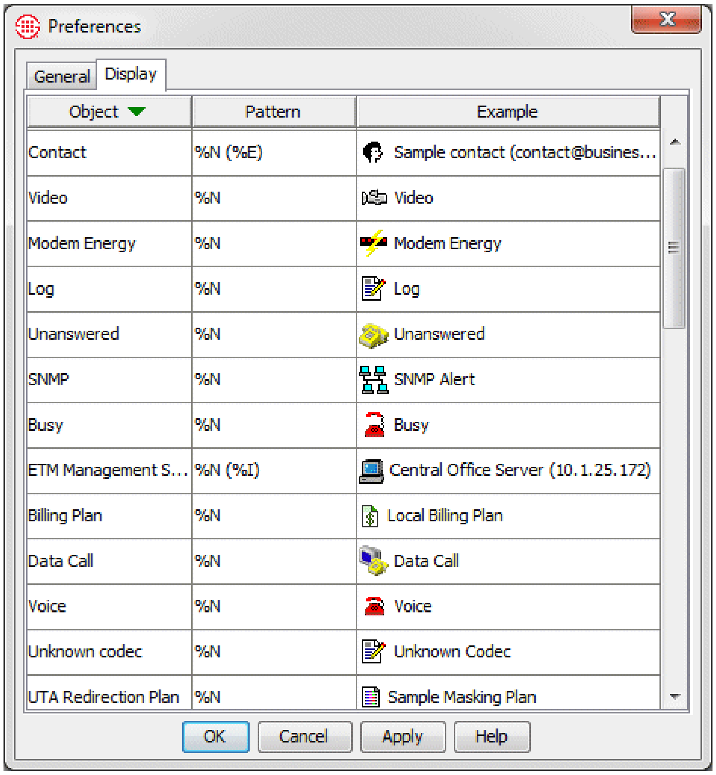
Customizing GUI Labels

You can customize GUI labels throughout the ETM System. These preferences apply only to the local client computer; they do not affect the display on other client computers.

Note that these preferences only affect the labels in the GUI; reports and Tracks are unaffected. Also, **Comment** appears as a choice for most items because most items have a comment, even if it is not user-definable.

To change the label pattern for a type of item

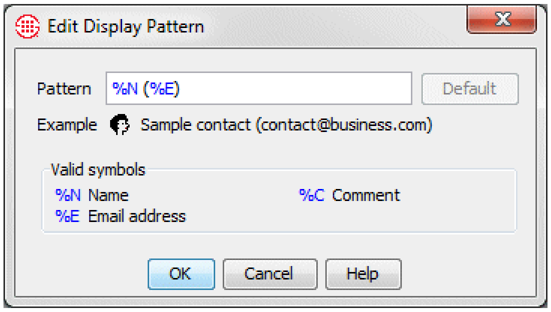
1. On the ETM System Console main menu, click **Edit | Preferences**. The **Preferences** dialog box appears.
2. Click the **Display** tab. The **Pattern** column shows the current settings, and the **Example** column illustrates how each label would look based on the current setting.



Object	Pattern	Example
Contact	%N (%E)	Sample contact (contact@busines...
Video	%N	Video
Modem Energy	%N	Modem Energy
Log	%N	Log
Unanswered	%N	Unanswered
SNMP	%N	SNMP Alert
Busy	%N	Busy
ETM Management S...	%N (%I)	Central Office Server (10.1.25.172)
Billing Plan	%N	Local Billing Plan
Data Call	%N	Data Call
Voice	%N	Voice
Unknown codec	%N	Unknown Codec
UTA Redirection Plan	%N	Sample Masking Plan

You can also right-click the row and click **Edit**.

3. To modify a label, double-click anywhere in the row for the item type you want to edit. The **Edit Display Pattern** dialog box appears.



Pattern %N (%E)

Example Sample contact (contact@business.com)

Valid symbols

%N Name
%C Comment
%E Email address

The change is not reflected in the GUI until you click **OK** or **Apply** in the **Preferences** dialog box. If you click **Cancel** on the **Display** tab after editing a display pattern, your changes are discarded.

4. In the **Pattern** box, type the series of symbols that represents the pattern you want for the label display. Available symbols for the selected item appear in the **Valid Symbols** area. You can also type punctuation marks and any special characters. To use a % (percent) sign, you must type two of them together (e.g., %%), since % is reserved for denoting a symbol.

   To illustrate, the default label pattern for the Management Server is: **%N (%I)**

Based on this pattern, an example Management Server name in a title bar appears as follows:
MyServer (10.1.1.100)

Suppose you prefer that the IP address be separated by dashes instead of parentheses, and that the data instance name be included, as in this example:
MyServer - 10.1.1.100 - DataInstance1

You would type the following pattern:
%N - %I - %T

5. Click **OK** to return to the **Preferences** dialog box.
6. Do one of the following:
   - Click **OK** to apply the change and close the **Preferences** dialog box.
   - Click **Apply** to apply the change and leave the **Preferences** dialog box open if you want to change other preferences.

Resetting Default Labels

The change is not reflected in the GUI until you click **OK** or **Apply** in the **Preferences** dialog box.

To reset a label to its default pattern

1. On the ETM® System Console main menu, click **Edit | Preferences**. The **Preferences** dialog box appears.
2. Double-click the item type for which you want to restore the default label. The **Edit Display Pattern** dialog box appears.
3. Click **Default**. A message appears confirming that you want to revert to the default.
4. Click **Yes**, and then click **OK** to accept the change and close the **Edit Display Properties** dialog box.
5. Do one of the following:
   - Click **OK** to apply the change and close the **Preferences** dialog box.
   - Click **Apply** to apply the change and leave the **Preferences** dialog box open.

Setting Performance Manager Display Properties

You can customize the Performance Manager to show or hide various display elements, set color preferences for logs, and more. Changes to these settings are applied to the client host where you set them only; they do not affect the display at other client hosts.

Moving the Toolbar

You can remove the Performance Manager toolbar from its default location and drag it to a new location.

To move the toolbar

1. Click and hold down either mouse button in the blank area of the toolbar (not on an icon or title bar).
2. While holding down the mouse button, drag the toolbar to the desired location, and then release the mouse button. The toolbar becomes a separate dialog box with minimize and close buttons.

To position or replace the toolbar

- To dock the toolbar in a new location:
  a. Click and hold down either mouse button in the blank area of the toolbar (not on an icon or the title bar). The toolbar becomes a blank gray rectangle.
  b. While holding down the mouse button, drag the rectangle toward the bottom or side of the main menu.
  c. When the rectangle is outlined in red, release the mouse button. The toolbar reattaches to the application window.
- To dock a floating toolbar, click the **X** in the upper-right corner. It returns to its last docked location.

Showing or Hiding the Toolbar

To show or hide the toolbar

- On the Performance Manager main menu, click **View**, and then click **Toolbar**. Clicking an element in the list works as a toggle to show or hide the element. A check mark indicates that the element is showing.

Showing or Hiding Subtrees in the Tree Pane

By default, subtrees for features for which your user account has permission appear in the Performance Manager tree pane. You can optionally hide these subtrees. Subtrees for features for which your account does not have permission are not available.

To show or hide subtrees

- On the Performance Manager main menu, click **View**. Clicking an element in the list works as a toggle to show or hide the element. A check mark indicates that the element is showing.

Showing or Hiding Implied Policy Rules

Firewall and Call Recorder Policies have *implied* Rules. (IPS Policies have no implied Rules.) The implied Firewall Policy Rules are the Emergency and Catchall Rules, which are the first and last Rule in each Firewall Policy. The Emergency Rule allows and logs all calls to Emergency numbers; the Catchall Rule allows all calls that did not match a prior Rule. Call Recorder Policies have an implied Do Not Record Rule that is the last Rule in every Call Recorder Policy and prevents recording of any calls that did not match a prior Rule.

The Implied Rules are hidden by default. This setting applies to all Policies viewed at this Performance Manager.

To show or hide the Implied Policy Rules

- On the Performance Manager main menu, click **View**, and then click **Implied Rules.** Clicking an element in the list works as a toggle to show or hide the element. A check mark indicates that the element is showing.

Showing or Hiding the Default Policy Nodes

Each type of Policy has a **Default** Policy node. The **Default** Policy node lists all of the Span Groups that are not currently assigned to any user-defined Policy of that type. These Span Groups are enforcing the default Policy of that type.

To show or hide the Default Policy Node of a Policy subtree

- Right-click the **Policies** subtree for the type of Policy, and then click **Default Policy Node**. Clicking this item works as a toggle to show or hide the node. A check mark indicates that the node is showing.

Showing or Hiding the Unassigned Span Group Node

The **Unassigned** node of the **Span Groups** subtree lists the Spans that are not assigned to any Span Group.

To show or hide the Unassigned node of the Span Groups subtree

- Right-click the **Span Groups** subtree, and then click **Unassigned Node**. Clicking this item works as a toggle to show or hide the element. A check mark indicates that the element is showing.

Setting Log Display Properties

Log display properties apply to the **Policy Logs, Call Log,** and **Diagnostic Log**. Properties for logs include:

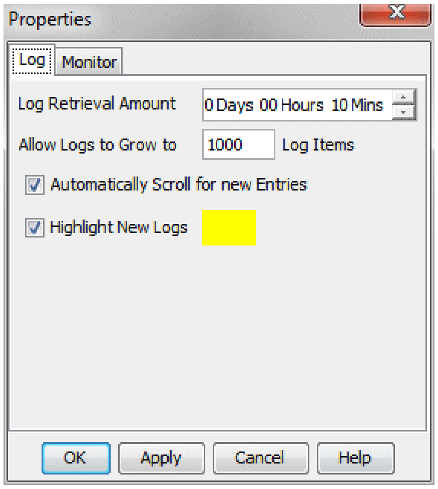
- The log retrieval amount (in days, hours, and minutes) to display.
- How many entries to display.
- Whether the display automatically scrolls for new entries.
- Whether new entries are highlighted, and if so, in what color.

To set log display properties

1. On the Performance Manager main menu, click **Edit | Properties**.

   The **Properties** dialog box appears.

2. Click the **Log** tab.



Log Retrieval Amount: 0 Days 00 Hours 10 Mins

Allow Logs to Grow to: 1000 Log Items

☑ Automatically Scroll for new Entries

☑ Highlight New Logs 🟨

3. In the **Log Retrieval Amount** box, select the amount of data that you want to display, starting from the time you open the log, going back the specified amount of time (unless the **Allow Logs to Grow to** limit is reached first). The default is 10 minutes. For example, if you open the log at 11:20, the log displays current logs as they are received and also loads the data gathered from 11:10 to 11:20, unless that much time includes more than allowed by the **Allow Logs to Grow to Limit**, described below.

4. In the **Allow Logs to Grow to** box, type the maximum number of log entries to display. The default is 1000; valid values are 1 - 100,000. This value constrains the **Log Retrieval Amount** (above). If the time Interval specified contains more entries than the limit specified in the **Allow Logs to Grow to** box, only the specified number of entries is displayed. (A message is provided in this case that states the Interval for which the logs are retrieved). After the **Allow Logs to Grow to** value has been reached, the display regenerates as new entries are received, showing only the most recent entries, up to this maximum.

If the log is open when you change the **Allow Logs to Grow to** value, the new value is not effective until he log is closed and reopened.

5. Select the **Automatically Scroll for New Entries** check box if you want the display to automatically advance with each new entry. If you clear this check box, you can manually scroll to view the entries at the end of the log.

6. Select the **Highlight New Logs** check box if you want new lines of data to be displayed in color. If you clear this checkbox, new entries are not highlighted.

   - The default is yellow. To choose a different color, click the colored box and select a new color from the **Select New Log Highlight Color** dialog box.

Call Monitor Color Coding

See “Call Monitor Color Coding” on page 197.

Classic View in Dialog Boxes

Some dialog boxes provide a **Classic View** display option. Turning on Classic View changes the display in the dialog box so that group members appear both at the root level of the tree and beneath the group to which they belong. By default, group members appear only beneath the group to which they belong. (They can still be used independently simply by expanding the group node and then selecting the member.)

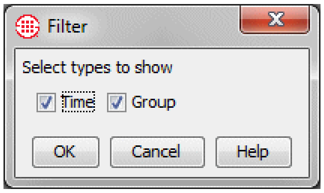
Filtering in Dialog Boxes

You can filter many dialog boxes to display only items of interest.

To filter the display

1. In the dialog box, right-click, and then select **Filter**. The **Filter** dialog box appears. **Types** and **Fields** vary according to the filter type.

   The example below shows the **Filter** dialog box for Times.



Select types to show

☑ Time ☑ Group

2. Select one or more of the check boxes next to the item(s) that you want to appear in the dialog box.
3. Click **OK** to apply the filter and close the **Filter** dialog box.

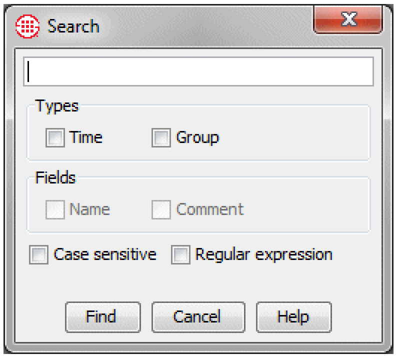
Searching in Dialog Boxes

You can search in many dialog boxes to find items of interest. The **Search** dialog box allows the specification of a search string, which can be a regular expression.

To search in the dialog box

1. In the dialog box, right-click, and then click **Search**. The **Search** dialog box appears. **Types** and **Fields** vary according to the search type.

   The example below shows the **Search** dialog box for **Times**.



2. In the text box at the top of the dialog box, type the characters that you want to find.

3. In the **Types** area, select one or more check boxes to indicate which type(s) you want to find.

4. In the **Fields** area, select one or more check boxes to indicate which of the fields should be searched. One of the **Types** check boxes must be selected for the **Fields** boxes to be available.

5. If you want to find only items that match the capitalization that you typed in the text box, select the **Case sensitive** check box; if you want to ignore capitalization when searching, clear the check box.

6. Select the **Regular Expression** check box if the search string is a regular expression.

7. Click **Find**. If one or more matching items are found, the first matching item is highlighted. To see the next match (if any), click **Find** again. Repeat until you locate the item you are seeking, or until **Search wrapped around** appears at the bottom of the **Search** dialog box (meaning that all items were searched and the search is beginning again from the top). If no items are found that match, **Pattern not found** appears at the bottom of the **Search** dialog box.

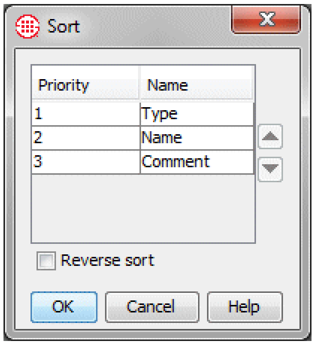
Sorting in Dialog Boxes

By default, items in dialog boxes are arranged in ASCII order. You can sort in many dialog boxes to display items in the order you specify. For example, you can sort Contacts so that they are listed in ASCII order by email address.

To sort the display

1. In the dialog box, right-click, and then click **Sort**. The **Sort** dialog box appears. The **Name** field varies according to the sort type.

   The example below shows the **Sort** dialog box for **Contacts**.



Sort

Priority	Name
1	Type
2	Name
3	Comment

□ Reverse sort

2. To change the priority of an item, click it in the box, and then click the up or down arrow. For example, if **Name** is Priority 2 and you want to sort by **Name**, click **Name**, and then click the up arrow once to move **Name** to Priority 1.

3. By default, the components are sorted in ascending order (i.e., a-z or 1-10). To sort the components in descending order, select **Reverse Sort**.

4. Click **OK** to apply the sort criteria.

Generating a Report of Components

You can generate a report of each of the components and Groups displayed in many dialog boxes. Items in the report maintain the sort order and filters set in the dialog box. The report contains all data associated with the item (i.e., Name, Comment, and so on). The report can be saved in the following formats: HTML, RTF, PS, PDF, CSV.

To generate a report of components

- In the dialog box, right-click, click **Report**, and then click one of the following:

  a. **Preview** opens the report in the **Print Preview** dialog box.

  b. **Print** sends the report to your configured printer.

  c. **Save As** allows you to save the file to a disk location. In the **Save Report** dialog box, type a file name, and then select the file format.

Index