SecureLogix®
We see your voice®

ETM® (Enterprise Telephony Management) System

v7.2.0

DOC-FW-720-10312018

About SecureLogix

SecureLogix delivers a unified call security and authentication solution to enterprise, federal, and military markets worldwide. Real-time security policy enforcement capabilities prevent call level attacks, fraud, and service abuse and disruption. Our patented solutions have filtered and secured billions of calls over the past 15+ years for some of the world's largest corporations and military installations.

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

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

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

IMPORTANT NOTICE:

This manual, as well as the software and/or Products described in it, is furnished under license with SecureLogix Corporation ("SecureLogix") and may be used only in accordance with the terms of such license.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without prior written permission of SecureLogix.

The content of this manual is subject to change without notice. SecureLogix assumes no responsibility or liability for any errors or inaccuracies that may be contained herein or to correct the same.

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

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

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

This product includes:

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

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 DVD 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 DVD for related copyrights, licenses, and source code.

Customer Support
for Your ETM® System

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

support.securelogix.com

Contents

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, the **Documentation** folder in the ETM System installation directory, and the root of the ETM Software installation DVD.

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 for database preparation.

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

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

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

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

Usage Manager User Guide—Provides task-oriented instructions and tutorials for producing reports of telecommunications accounting and Policy

enforcement. Includes an appendix describing each of the predefined Reports.

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

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

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

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

Additional Documentation on the Web

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

http://support.securelogix.com

Tell Us What You Think

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

docs@securelogix.com

Conventions Used in This Guide

The following conventions are used in this guide:

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

  Click **View | Implied Rules**.

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

  Highlight the field and press DELETE.

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

  Press CTRL+ALT+DELETE.

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

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

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

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

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

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

Voice Firewall Policy Overview

Understanding Voice Firewall Policies

Just as an IT firewall on the data network examines each network packet to determine whether to forward it to its destination, the Voice Firewall examines each TDM or VoIP call on the telecommunications network to determine which calls are allowed to pass through, which are denied access, and which other actions, such as logging or email notification, are to be triggered by a call.

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, syslog alert,or SNMP trap.

A Firewall Policy consists of one or more user-defined Rules to which each call on monitored trunks is compared. Each Rule is defined to look for a specific source, destination, call direction, type of call, DTMF digit pattern, 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.

The resulting Policy enforcement data is stored in a central database along with all other call data.

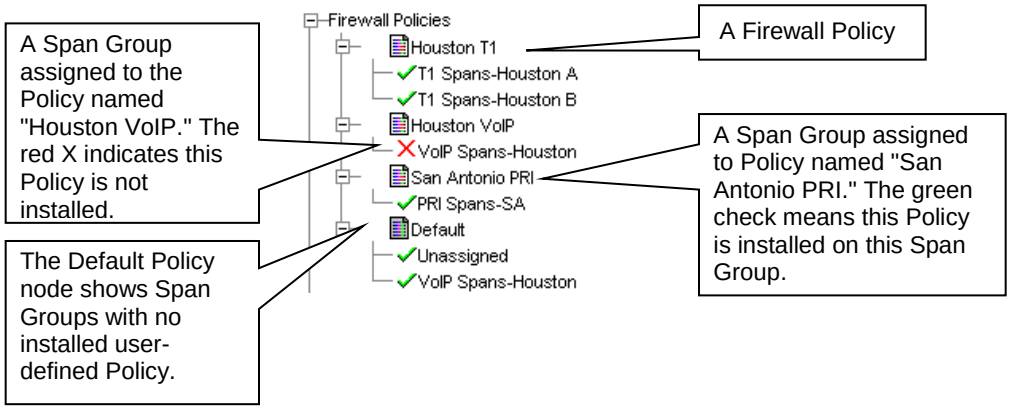
Span Groups

Span Groups organize Spans into logical units according to 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 in one or more Span Groups. You cannot install a Policy on a Span that is not in a Span Group. However, a Span Group can contain a single Span if appropriate. Only one Firewall Policy can be installed on a Span Group. When you move a Span into a Span Group, the Span automatically receives and begins enforcing the Policies installed on the Span Group.

Firewall Policies Subtree

In the Performance Manager tree pane, the **Firewall Policies** subtree is used to define and manage Firewall Policies, view on which Span Groups each Firewall Policy is currently installed, and view the **Policy Logs** for the Policies.

When you define a Policy, you select one or more Span Groups for which the Rules in the Policy are appropriate and assign those Span Groups to the Policy. When you expand the **Firewall Policies** subtree, the Span Group(s) assigned to each Policy appear(s) below the Policy.



If a Span Group is currently enforcing the Policy, a green check mark ✓ appears next to the Span Group name. If the Policy is not currently installed on the Span Group, a red **X** appears next to the Span Group name.

Span Groups that are not assigned to any user-defined Policy appear below the **Default** node of the **Firewall Policies** subtree. The *Default Policy* is installed on any Span Group not enforcing a user-defined Policy.

- By right-clicking the **Firewall Policies** subtree or one of the Policies under it, you can accomplish the following:
- Create a new Policy.
- Open the **Policy Log** showing Policy enforcement data for the selected Policy.
- Edit, rename, install, uninstall, delete, or verify a Policy.

Note that Span Groups cannot be edited nor managed from within the **Firewall Policies** subtree; they simply appear here to illustrate which Span Groups are assigned to and enforcing which Policy. You manage Span Groups via the **Span Groups** subtree, and you assign them to the Policy via the **Attributes** tab of the Policy.

The Default Firewall Policy

The Default Firewall Policy is installed on all Spans before any user-defined Firewall Policies are installed and whenever a user-defined Policy is uninstalled from a Span Group. The Default Policy contains only the two Implied Rules that are always the first and last Rules of any Policy. The Default Policy cannot be opened nor edited.

Implied Rules

Every Firewall Policy contains two *Implied* Rules that are always the first and last Rules of any Firewall Policy:

- **Emergency Rule**—Always the first Rule in a Firewall Policy; logs calls to emergency numbers and ensures that calls to emergency numbers are not blocked.
- **"Catchall" Rule**—Always the last Rule in a Firewall Policy; allows all calls that do not match previous Rules.

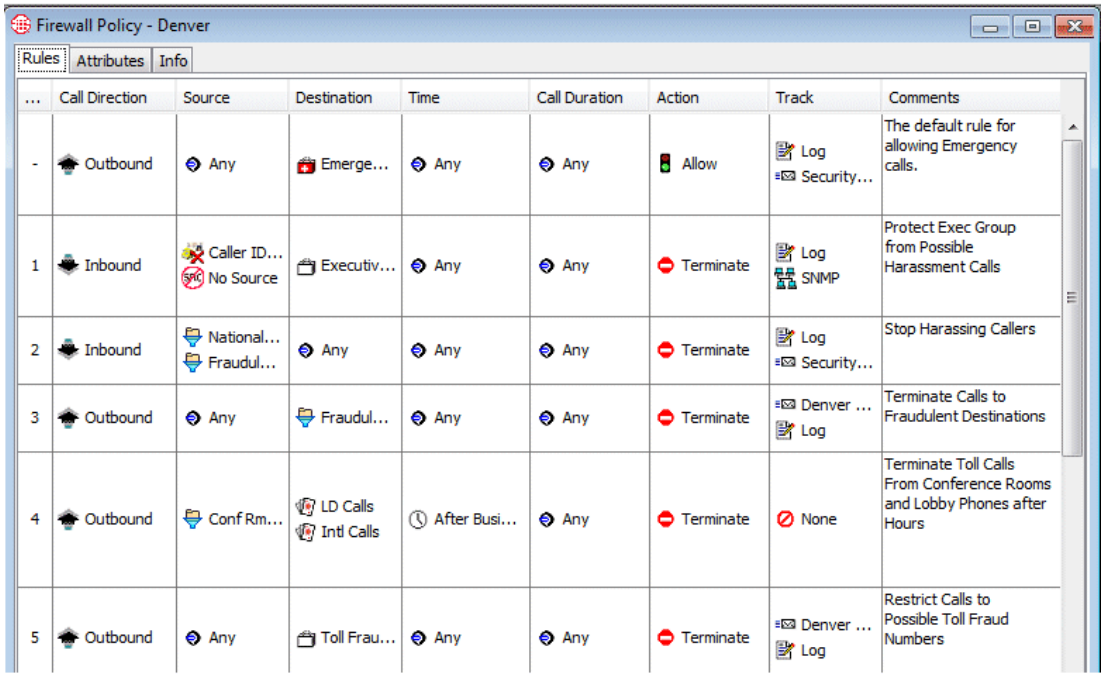
Note: The **View** menu toggle shows/hides implied Rules globally in all Policies, not just the one with the focus.

These Implied Rules are hidden by default. On the Performance Manager main menu, clicking **View | Implied Rules** acts as a toggle to hide/show the Implied Rules.

You can modify the **Track** and **Comment** fields of the Implied Rules and assign a different Emergency Group in the **Destination** field of the Emergency Rule.

Firewall Policy Fields

Firewall Policies are defined using the **Firewall Policy Editor**, as shown in the illustration below.



...	Call Direction	Source	Destination	Time	Call Duration	Action	Track	Comments
-	Outbound	Any	Emerge...	Any	Any	Allow	Log Security...	The default rule for allowing Emergency calls.
1	Inbound	Caller ID... No Source	Executiv...	Any	Any	Terminate	Log SNMP	Protect Exec Group from Possible Harassment Calls
2	Inbound	National... Fraudul...	Any	Any	Any	Terminate	Log Security...	Stop Harassing Callers
3	Outbound	Any	Fraudul...	Any	Any	Terminate	Denver ... Log	Terminate Calls to Fraudulent Destinations
4	Outbound	Conf Rm...	LD Calls Intl Calls	After Busi...	Any	Terminate	None	Terminate Toll Calls From Conference Rooms and Lobby Phones after Hours
5	Outbound	Any	Toll Frau...	Any	Any	Terminate	Denver ... Log	Restrict Calls to Possible Toll Fraud Numbers

For each Rule, you specify the parameters that determine:

- Which calls match the Rule.
- What to do if the Rule matches.
- To which Span Group(s) the Rule applies.

The following sections describe each of the fields in Policy Rules. See "Firewall Policies Step-by-Step" on page 25 for instructions for defining Policies.

Call Direction

The **Call Direction** field specifies whether the origination of the call was inside or outside your organization. You can specify **Inbound**, **Outbound**, or **Any.** (**Any** means the Rule applies to both inbound and outbound calls.) The default is **Any**.

Source

The **Source** field is used to apply the Rule based on properties of the originator of the call. **Any** means all sources, or you can select one or more of the following:

- **Directory entities**—Directory Listings (contain phone numbers, URIs, and identifying information), Ranges, Groups, Filters (dynamically include a set of Listings that match the filter criteria), or Wildcards (phone or URI), used to apply the Rule to *categories* of calls, such as all calls from a specific area code or domain.
- **Subnets** or **Subnet Groups**—All URIs in a given subnet.
- **Caller ID Restricted**—Used to apply the Rule to calls for which the caller has blocked transmission of the Caller ID data. Note that if the phone number is present in the signaling even though CIDR is indicated, both the phone number and CIDR are used for Policy processing. In this case, Rule order determines which takes precedence.
- **No Source**—Used to apply the Rule to calls for which source is not available on trunks that support the delivery of source information, except when it was intentionally blocked (CIDR). To apply a Rule to all calls having no source, specify both **Caller ID Restricted** and **No Source** in the **Source** field of the Rule.

Destination

The **Destination** field is used to apply the Rule based on properties of the destination of the call. **Any** means all destinations, or you can select one or more of the following:

- **Directory entities**—Directory Listings (contain phone numbers and URIs and identifying information), Ranges, Groups, Filters (dynamically include a set of Listings that match the filter criteria), or Wildcards (phone or URI), used to apply the Rule to *categories* of calls, such as all calls from a specific area code or domain.
- **Subnets**—All URIs in a given subnet.

Call Type

The **Call Type** field identifies the type(s) of call traffic to which the Rule applies. Call types are predefined and cannot be user-modified.

You can use *negation* o further define the **Call Type** field to specify the calls to which the Rule *does not* apply; that is, if the call type does not match the negated call type(s), the Rule fires. For example, you could define a Rule to ensure that dedicated fax lines be used only for fax calls by placing **Fax** in the field and then negating it. This would mean, "All calls that are not fax calls."t

When the **Call Type** field is negated, an exclamation point appears in the **Call Type** field.

The call types that the ETM System identifies are described in the table below.

Call Type	Definition
Busy	On TDM Spans, busy signal detected (typically on an unanswered call) On VoIP Spans, SIP/ message received indicating a busy line. ON UTA, as received from the router. ***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	(*PRI, SS7, and VoIP Spans*) Determined via specific D-channel messaging, denotes a specific type of data call that may use more than one channel. Videoconferencing is a typical example. For VoIP, a data codec was used.
Fax	Fax calls. Reported when distinct fax handshake messages are detected on the line. For VoIP, a fax codec was used.
Modem	(*Does not apply to VoIP 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 VoIP 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 VoIP or UTAA) 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.

Call Types, continued

Call Type	Definition
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 VoIP, 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**.
Video	*(Only reported on VoIP 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 VoIP Spans, reported when a voice codec is used. On UTA, as received from the router.

Time

The **Time** field is used to specify whether the Rule applies at all times or at specific date(s) and time(s). A **Time** can specify a maximum of three different start and stop periods and is interpreted as local to the Span.

You can use *negation* to further define the **Time** field to define the calls to which the Rule *does not* apply; that is, if the call data does not match the negated criteria, the Rule fires. For example, the default **Business Hours** Time specifies 8 AM to noon and 1 PM to 5 PM. (You can modify it to your operating hours). If you add the **Business Hours** Time to the Rule and then negate the **Time** field, the Rule applies during non-business hours.

When the **Time** field is negated, a red exclamation point appears in the **Time** field.

Call Duration

The **Call Duration** field is used to apply a Rule based on the length of a call. **Any** applies to calls of any duration.

Durations are used to specify calls from 0 hours and 0 minutes to 999 hours and 59 minutes. A **Duration** of 0 hours and 0 minutes behaves as if no duration is specified.

The order of Rules that specify duration is very important for proper results. For information about special considerations for call duration Rules, see "Call-Duration Processing" on page 23.

Action

The **Action** field specifies the action to take when a call matches the Rule:

- **Allow** permits the call to continue.
- **Terminate** disconnects the call.

Attributes

The **Attributes** field is used to specify additional possible characteristics of VoIP calls to which you may want to apply the Firewall Policy:

- **Unknown Codec**—Refers to codecs that are used on the network but that are not defined in the **Codecs** dialog box. When an unknown codec is seen on the line, the available information is captured and automatically added as a codec definition in the **Codecs** dialog box; these codecs are classified as **Unknown**. See "Codecs" in the *ETM® System Administration and Maintenance Guide* for details.
- **Excessive Media Rate**—That is, excessive for the codec the call used. Each codec has a value defined by which the media rate is judged excessive. See "Codecs" in the *ETM® System Administration and Maintenance Guide* for details.
- **Media Timeout**—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. Media timeouts are user-defined from within the Firewall Policy. See "Media Timeouts for VoIP Spans" in the *ETM® System User Guide* for instructions for defining media timeouts.
- **DTMF Pattern**— Used to detect a pattern of calls dialing a certain patterns of DTMF digits that might be indicative of malicious activity. Interdigit timing is stored in the database for offline analysis.
- **Signaling Anomaly**—Used to apply the Rule to detected SIP signally anomalies..

Track

The **Track** field is used to specify one or more follow-up actions when a call matches a Rule. Because Track instructions remain on the Server, if network connection is lost between the Management Server and the Span, no track actions occur when a Rule fires until after the network connection is restored. (Allow and Terminate actions still occur immediately.) Tracks are used to generate logging and notifications as follows:

- **Log** Tracks cause the event to be written to the **Policy Log**. Note that data for *all* calls is saved in the Database. The **Log** Track is used to track and report on specific Firewall Policy events. The **Log** Track is added by default when any other **Track** is added.
- **Real-Time Alert** Tracks cause an alert to be displayed in the **Alert Tool**.

Note: For instructions for customizing the notification messages, see "Customizing Policy Track Messages" in the *ETM® System Technical Reference*.

- **Email** Tracks are user defined and contain one or more **Contacts** with email addresses. If a call matches a Rule with an **Email** Track, all **Contacts** specified in the **Email** Track are notified when the Rule fires.
- **SNMP Alert** Tracks generate an SNMP alert to a network management station.
- **Syslog** Tracks generate a Syslog message to one or more Syslog servers.

For instructions for defining Email Tracks, see "Tracks" in ET*M*® *System User Guide*.

Install On

Only one Firewall Policy can be installed on a Span Group at a time; however, a Policy can have multiple Span Groups assigned to it, and each Rule of the Policy can specify which of those Span Groups is to enforce that Rule. When you install a Policy, it is installed on all of the Spans in the assigned Span Groups, but each Span in the Span Group enforces only the Rules assigned to it in the **Install On** field.

The **Install On** field specifies which of the Span Groups assigned to the Policy is to enforce the Rule. **Any** means all of the Span Groups assigned to the Policy are to enforce the Rule.

Comments

The **Comments** field provides a space to type optional information regarding the Rule (e.g., the purpose for the Rule, creator of the Rule, and/or date/time created). The comment appears in reports, logs, and alerts, but has no effect on the processing of the Rule. Good comments are very useful in reporting.

Allowed Number of Phone Number Objects

Each Span can have one of each type of Policy installed. Each Policy can prescribe actions based on source and destination phone numbers. Before a Policy can be enforced, it must be pushed to and stored in memory on the Appliance. Of course, each Span has a finite amount of memory, so the total number of phone number objects that can be included in all Policies installed on the Span is finite. The limit depends on the type of Card in the Appliance:

- 8540 Controller Cards, SIP Appliances, and UTA Appliances—Up to 50,000 objects across all of the installed Policies.
- 8240 Controller Cards and 1000-series Appliances— Up to 30,000 objects across all of the installed Policies.

When you attempt to install a Policy, the count of phone number objects is calculated and compared to the Policies already resident on each Span in the assigned Span Groups. If the count of phone number objects in the Policy exceeds the limit for the type of Span for any included Span, the installation fails and an error message is presented.

Two installation modes are provided.

- **Normal Mode**—Normal installation without uninstalling the existing user-defined Policy, if present. If the Policy will not fit without uninstalling the existing Policy, installation fails and a message is presented.
- **Priority Mode**—If the new Policy needs the space occupied by the existing user-defined Policy, the existing Policy is uninstalled before the new Policy is installed.

Firewall Policy Processing

After you define Policies, you install them on the Spans in the ETM® Appliances monitoring your telco system. The Spans then automatically enforce the Policy in real time, even if communication with the ETM Server is temporarily interrupted. Tracks are generated by the Server, so these are not generated until communication is restored, but call monitoring and termination continue; the Span stores the call data until the Server connection is restored, and then sends the data to the Server.

Real-Time Policy Processing

When a Policy is installed on a Span Group, the Spans in that Span Group begin processing the Rules in real time as new calls occur. (Calls that are in progress are not processed against the new Policy unless an "*execute policy" event* occurs. See "Policy Transitions" on page 70 for details.) Rules are always processed in sequence, from the first Rule in the Policy to the last, which means that Rule order is important to processing results.

When a call matches all of the criteria of a given Rule, the Rule is said to *fire*, or to have been *triggered* by the call. When a Rule fires, the call is either terminated or allowed as specified by the Rule, and specified Tracks (such as email or logging) are executed.

Continuous Call Type Detection

Spans perform continuous call-type detection throughout the life of the call. If the Span detects a change in the call type during a call, the Span once again reviews each Rule and enforces any Rule that applies to the new call type. Note that if a Rule has already fired for the call, that same Rule will not fire again when the call is reprocessed for a change in call type.

Ambiguous Calls

An *ambiguous call* occurs when insufficient call data is available to evaluate a call against a Rule. For example, if the source phone number is unavailable and the call is compared to a Rule that specifies a specific source phone number, the call is ambiguous. Because the source is unknown, it cannot be determined whether the call matches the Rule. Ambiguous Call Processing determines how such calls are processed. See "Firewall Settings for Call Processing" on page 93 and "Configuring Spans" in *the ETM® System Installation Guide* for details on configuring a Span for handling ambiguous calls. Unless **Skip the Rule** is selected, a log item is added to the **Policy Log** for each ambiguous call.

Call Termination

If the call matches all of the criteria in the Rule, the Rule fires and the Span executes the specified action: **Allow** or **Terminate**. If **Terminate** is selected, the call is dropped. Analyze each terminate Rule carefully to ensure that only the calls that you intend to disconnect are terminated.

Even if termination is specified in a Rule, **Allow Call Terminations** must be selected in the **Span Configuration** dialog box for each Span that enforces this Rule before that Span can enforce call termination. If you specify termination in a Rule for a Span that does not have **Allow Call Terminations** selected, a warning message appears in the **Status Tool** when you install or verify the Policy. See "Firewall Settings for Call Processing" on page 93for information about this Span setting.

For incoming loop start and ground start calls on either analog or T1 trunks, the Span cannot terminate calls until after the call has been answered. A call will not be terminated if the channel on which the call is carried is not enabled in the **Channel Map** for the Span. See "Configuring Spans" in the *ETM® System Installation Guide* for information about enabling channels.

SMDR Data and Policy Enforcement

(*Not on SIP*) Station Message Detail Record (SMDR) data is PBX logging data that is generated by the PBX after a call is complete. The Management Server can use this PBX logging data to determine source extensions on outbound TDM calls for Policy execution when source is otherwise unavailable, because SMDR data contains the dialed digits, originating station, and start time of the call. Since SMDR data is not available until a call completes, if a particular Span uses SMDR, terminate Rules cannot be enforced on that Span for Rules that specify outbound sources.

When a Rule is encountered that specifies outbound source and the source is not available from ANI, CPN, or any other method, the Span suspends Policy processing for that call and sends a request to the Management Server for SMDR data. (The Spans do not request SMDR unless configured to do so in the **Span Configuration** dialog box.) When the Server receives and correlates the SMDR data with the call, the data is returned to the Span, which resumes Policy execution for the call in question. See "Configuring Spans" in the *ETM® System Installation Guide* for information about configuring a span to request SMDR.

Policy Processing Phases

For each call, Policy processing proceeds as follows:

- At the start of the call, *call-reject* processing is performed to determine whether the call should be allowed to proceed, strictly based on the direction, destination, and/or source, without waiting for call type or DTMF digit patterns to be identified.
- When the call type is initially determined and each time the call type changes, the call is again processed against the Policy.
- If a Rule specifies duration, but the duration has not yet been reached, the Policy is reprocessed every 15 seconds until the call ends or the duration is reached and the Rule fires. If multiple duration Rules are arranged in descending order, processing continues until each duration

has been reached or the call ends. Details about each of these phases are provided in the sections below.

Call-Reject Processing

Call-reject processing applies to Rules that do not specify call type or a DTM pattern.. These are called *call-reject Rules*.. When a Rule that specifies call type or a DTMF pattern is encountered, processing pauses until call type is determined or a DTMF digit match is determined.

Call-reject processing provides the advantage of immediate enforcement. In contrast, it may take 20 seconds or more to determine call type and a variable amount of time to match DTMF, since that depends on which/whether mid-call DTMF digits are entered during the call. Therefore, to take advantage of the benefits of call-reject processing, order the Rules in the Policy with all Rules without call type or DTMF patterns specified placed before any Rules that specify call type or DTMF pattern. Also, because it may take the entire length of the call to determine whether a DTMF pattern Rule matched, place these after all call-type Rules.

Call-Type Processing

As soon as the initial call type is determined, the *call-type processing* phase begins. The call is processed against each Rule in the Policy in sequence. If the call matches all of the criteria in a Rule, the Rule fires and processing stops, unless the call type changes or a previous Rule specified call duration. If the call type changes, the call is again processed against the Policy, even if a Rule has already fired. Multiple Rules can fire per call and multiple Tracks can be generated; however, only one entry for the call appears in the Policy Log, showing all call types and Tracks for the life of the call. (For details about viewing calls in the **Policy Log**, see "The Policy Log" on page 83.)

Call-Duration Processing

Call-duration processing occurs simultaneously with call-type processing. Using Durations, you can define Firewall Policy Rules based on the specific length of a call. If a Rule specifies call duration, but the duration has not yet been reached, that Rule is skipped and processing continues with the next Rule. The Policy is reprocessed every 15 seconds until the specified duration is reached or the call ends.

IMPORTANT Processing never passes a Rule that has already fired unless call type changes. Therefore, if you define Rules with different durations, place Rules with longer durations first. Also, if you have defined your Policy so that all calls that do not match a previous Rule are terminated by a final Rule, define a Rule specifically allowing calls that would match the Rule, but that have not yet reached the specified duration; otherwise, calls are terminated without ever reaching the specified duration.

Note: The effectiveness of Duration Rules can be impacted by Rules that require SMDR data to evaluate (such as specific source numbers on a T1 Span).

A Duration Rule does not fire until the specified duration is reached. For example, if you specify a 30-minute duration, the Rule does not fire until the call has been ongoing for 30 minutes. If you specify a duration of 0 hrs 0 minutes, the Rule behaves as if no duration is specified. A **Call Duration** of **Any** means that the Rule applies to calls of any length.

You can only apply one Duration to a Rule. If you want to specify more than one Duration, you must create one Rule for each Duration and place the longer duration Rule before the shorter duration Rule in the Policy. For example, suppose you want to log calls that last 30 minutes and terminate calls that last 60 minutes. You create one Rule for each of those actions and place the 60-minute Rule before the 30-minute Rule in the Policy. Note that if you were to place the 30-minute Rule first, that Rule would fire after 30 minutes and the subsequent 60-minute Rule would never be processed.

Getting Started with Firewall Policies

Firewall Policies Step-by-Step

Firewall Policies are defined using the **Firewall Policy** editor in the Performance Manager. The **Firewall Policy** editor contains the following tabs:

- The **Rules** tab, in which you define the Rules of the Policy.
- The **Attributes** tab, in which you assign the Emergency Group and Span Groups.
- The **Info** tab, in which you can view the properties of the Policy.

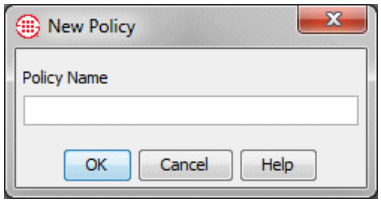
Step-by-step procedures for defining, saving, and installing a Policy are provided below.

Defining a Voice Firewall Policy

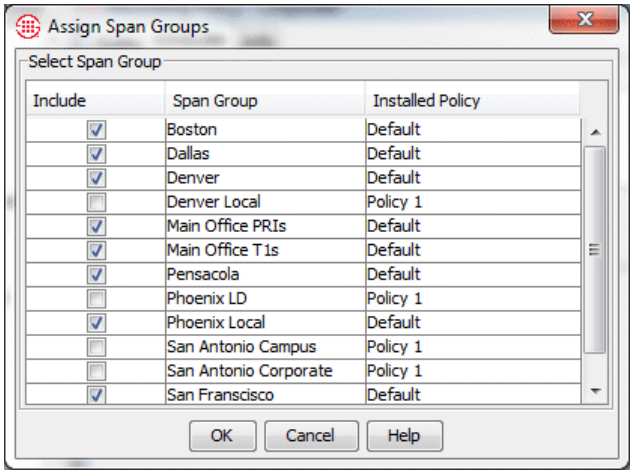
You must have the **Full Control** user permission for Firewall Policies to create them.

To create a Voice Firewall Policy

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



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



3. Select the **Include** check box(es) for the Span Group(s) on which this Policy is to be installed; clear the check boxes for Span Groups on which the Policy is not to be installed. The selections in this dialog box also determine the Span Groups that can be selected in the **Install On** field of the Policy.

   - If one or more Span Groups you want to assign to the Policy have not yet been created, you can open this dialog box and assign them later. Simply clear any check boxes for Span Groups on which the Policy is not to be installed. You can clear all check boxes if none apply.

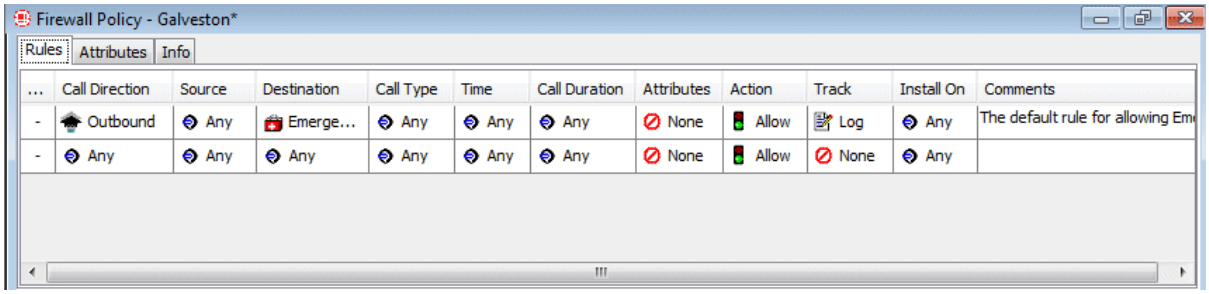
4. Click **OK**.

   IMPORTANT If you click **Cancel**, the Policy is not created. Click **OK** to create the Policy, even if you did not select any Span Groups.

   The Policy appears in the Policy editor pane. 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.

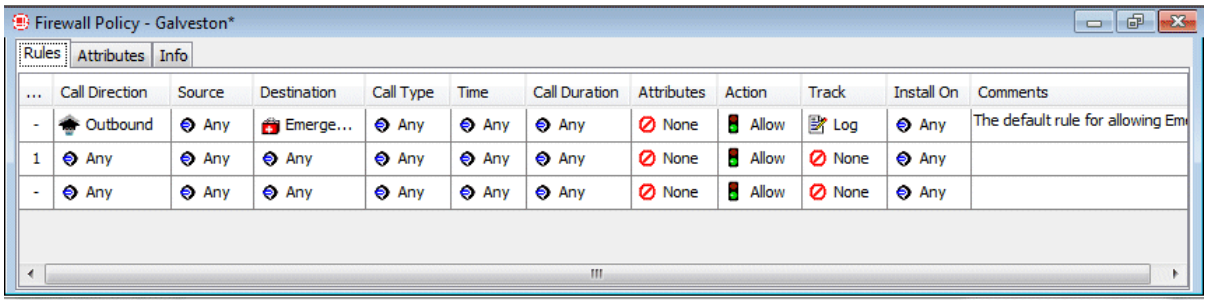
To show the Implied Rules, click **View | Implied Rules**.

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



5. Click **File | Save**. The Policy appears in the **Firewall Policies** subtree.

6. Right-click in the blank area of the Policy, and then click **Add Rule | Bottom**. A new Rule is added to the Policy with all of the fields at their defaults, as shown below.



7. To add a value to a field, right-click in the field. A menu of options for that field appears. Select the applicable value.

   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. See "Source Field" on page 30 for details.
   - **Destination**—The destination of the call. See "Destination Field" on page 41 for details.
   - **Call Type**—The traffic type(s) to which the Rule applies. See "Call Type Field" on page 43 for details.
     - You can also negate the **Call Type** field so that the Rule applies to all other call types. To negate the **Call Type** field, after adding one or more Call Types, right-click again in the field, and then click **Negate**.
   - **Time**—The time(s) and day(s) the Rule is in effect. See "Time Field" on page 41 for details.
     - You can also negate the **Time** field so that the Rule applies at all other times. To negate the **Time** field, after adding one or more Call Types, right-click again in the field, and then click **Negate**.
   - **Call Duration**—The length of the call. See "Call Duration" on page 42 for details.
   - **Attributes**—VoIP call attributes. See "Attributes Field" on page 28 for details.
   - **Action**—Allow or terminate calls that match the Rule. See "Action" on page 43 for details.
   - **Track**—Notification and logging for calls that match the Rule. See "Track Field" on page 44 for details.

IMPORTANT Rule order is important in Firewall Policies. See “Organizing the Rules in the Policy” on page 51 for a discussion of Policy processing and Rule order.

- **Install On**—The Span Groups that are to enforce the Rule. See "Install On Field" on page 46 for details.
- **Comments**—Optional notes about the Rule. Comments are very useful for identifying the purpose of the Rule and in alerts and reporting.

8. Repeat Steps 7 and 8 for each Rule in the Policy.
9. Click the **Attributes** tab and assign a new Emergency Group with local emergency numbers specific to the Appliance locale. See “Emergency Rule” on page 46.
10. When you are done, click the **Save** icon.
11. Right-click the Policy in the **Firewall Policies** subtree, point to **Install**, and then click one of the following:.
    - **Normal Mode**—Normal installation without uninstalling the existing user-defined Policy, if present. If the Policy will not fit without uninstalling the existing Policy, installation fails and a message is presented.
    - **Priority Mode**—If the new Policy needs the space occupied by the existing user-defined Policy, the existing Policy is uninstalled before the new Policy is installed.
12. The Policy is verified; if it passes verification, it is installed on the assigned Span Groups. See “Verifying a Policy” on page 62 for details about what verification checks. See "Installing a Policy" on page 69 for details about installing a Policy.

Call Direction Field

The **Call Direction** field specifies whether the origination of the call was inside or outside your organization. You can specify **Inbound**, **Outbound**, or **Any**. (**Any** means the Rule applies to both inbound and outbound calls.) The default is **Any**.

Specifying Call Direction

To specify only inbound calls or only outbound calls

- In an open Policy, right-click in the **Call Direction** field, and then click the call direction to which you want to apply the Rule.

Attributes Field

Attributes for Firewall Policies include:

DTMF Pattern—Used to detect a pattern of calls dialing a certain patterns of DTMF digits that might be indicative of malicious activity. DTMF digit patterns can be used in Policy without being stored in the Database. A separate per-Span configuration item determines whether they are stored (**Off** by default).

Excessive Media Rate--That is, excessive for the codec the call used. Each codec has a value defined by which the media rate is judged excessive.

Media Timeout—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. Media timeouts are user-defined.

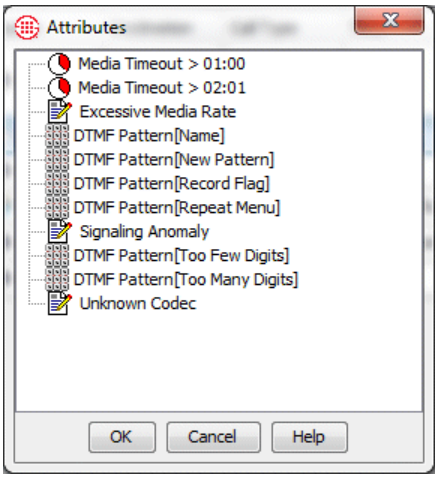
Unknown Codec—Refers to codecs that are used on the network but that are not defined in the Codecs dialog box. When an unknown codec is seen on the line, the available information is captured and automatically added as a codec definition in the Codecs dialog box; these codecs are classified as Unknown.

Signaling Anomaly— Used to apply the Rule to detected SIP signally anomalies.

Specifying Call Attributes

To add call attributes to a Rule

1. In an open Policy, right-click in the **Attributes** field. The **Attributes** dialog box appears.



2. Select one or more of the following:

   - **DTMF pattern:**
     - **To use an existing pattern**: Click it and click **OK**.
     - **To define a new pattern**: Right-click in the **Attributes** dialog box and click **New | DTMF Pattern**. The **DTMF Pattern Attributes** dialog box appears.

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

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

   iii. 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.

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

- **Unknown Codec**—Refers to codecs labeled unknown in the **Codecs** dialog box. See "Codecs" in the *ETM® System Administration and Maintenance Guide* for details.
- **Excessive Media Rate**—That is, excessive for the codec the call used. Each codec has a value defined by which the media rate is judged excessive. "Codecs" in the *ETM® System Administration and Maintenance Guide* for details
- **Media Timeout**— 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. Media timeouts are user-defined. To define a Media Timeout:

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

  b. In the **Duration** box, type or select the length of time a call can have no media before it times out.

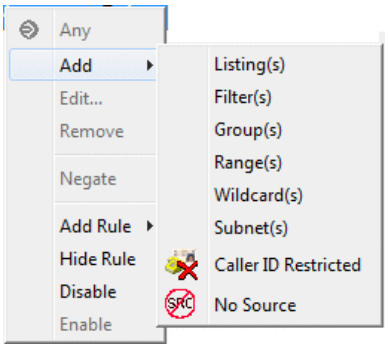
  c. Click **OK**. The media timeout appears in the **Attributes** dialog box.

3. Click **OK**. The selected attribute is added to the Rule.

Source Field

Note: You can only create and edit Directory entities in the Directory Manager. For instructions for creating or editing Directory entities, see "Understanding the Directory Manager" in the *ETM® System User Guide*.

The **Source** field is used to apply the Rule based on properties of the originator of the call. **Any** (the default) means all sources. When you right-click in the field, the following menu of options appears:



You can add one or more of the following to specify the call source:

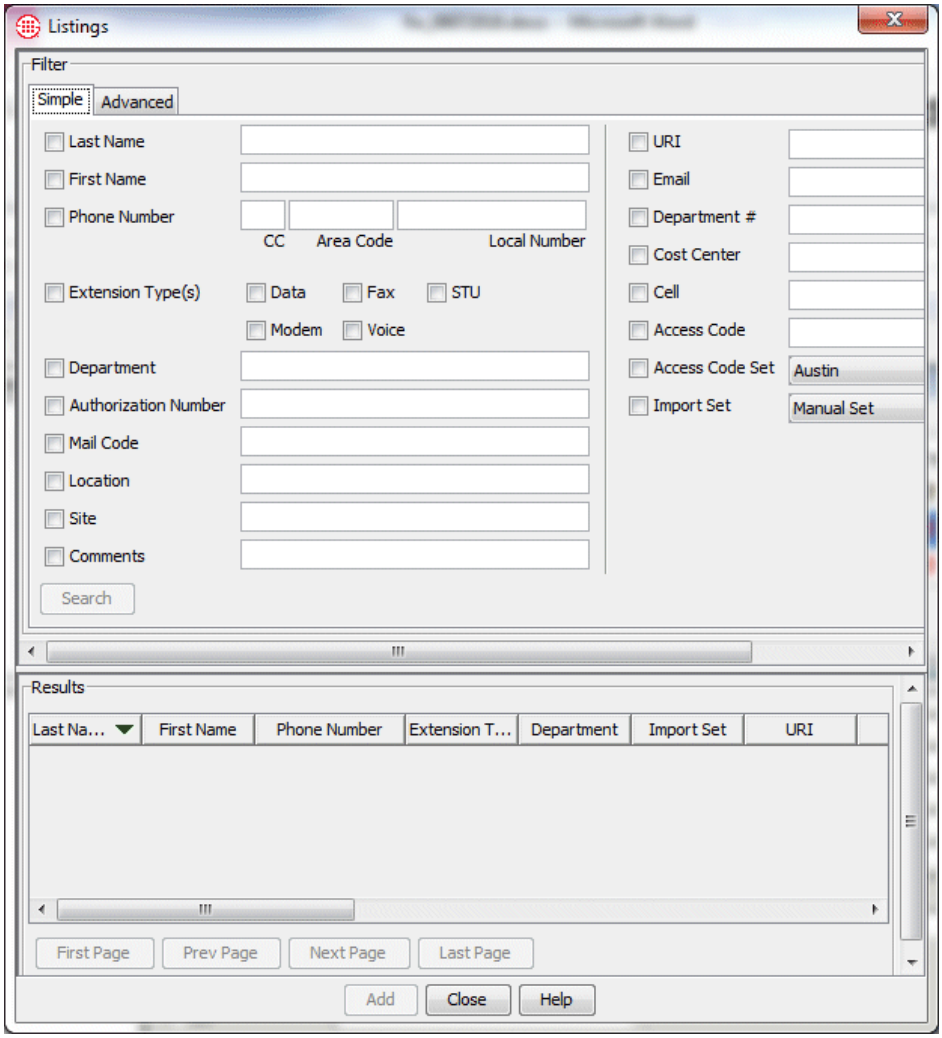
- **Directory entities**—Directory Listings (contain phone numbers and URIs and identifying information), Ranges, Groups, Filters (dynamically include a set of listings that match the filter criteria), or Wildcards (phone or URI), used to apply the Rule to categories of calls, such as all calls from a specific area code or domain.
- **Subnets or Subnet Groups**—All URIs in one or more given subnets.

- **Caller ID Restricted**—Used to apply the Rule to calls for which the caller has blocked transmission of the Caller ID data. Note that if the phone number is present in the signaling even though CIDR is indicated, both the phone number and CIDR are used for Policy processing. In this case, Rule order determines which takes precedence.
- **No Source**—Used to apply the Rule to calls for which source is not available on trunks that support the delivery of source information, except when it was intentionally blocked (CIDR). To apply a Rule to all calls having no source, specify both **Caller ID Restricted** and **No Source** in the **Source** field of the Rule.

Adding Listings to the Source or Destination Field

To add one or more Listings to the field

- Right-click in the **Source** or **Destination** field, and then click **Listings**. The **Listings** dialog box appears.



The **Listings** dialog box is used to search for listings to add to the Rule. It has two tabs: **Simple** and **Advanced**.

To perform a simple search:

1. On the **Simple** tab, type or select the information that retrieved Listings are to contain. You can use 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, and Import Set.

2. 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. For example, **SMITH** and **smith** would both match the last name *Smith*. By default, 100 results are displayed per page. If more than 100 Listings matched your criteria, use the navigation buttons to access additional pages.

3. In the **Results** area, click the Listings you want to add. To select multiple Listings, hold down CTRL or SHIFT while clicking.

   - You must add Listings from each **Results** page separately. You cannot select Listings on multiple pages at once.

4. Click **Add**. The Listings are added to the **Source** or **Destination** field. Repeat to add Listings from additional pages, if needed.

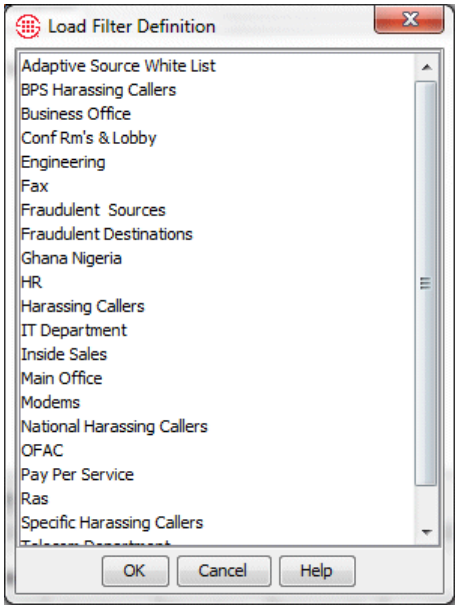
5. When you have added all the Listings you want to the field, click **Close** to dismiss the **Listings** dialog box.

To perform an advanced search

1. Click the **Advanced** tab, and then 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.

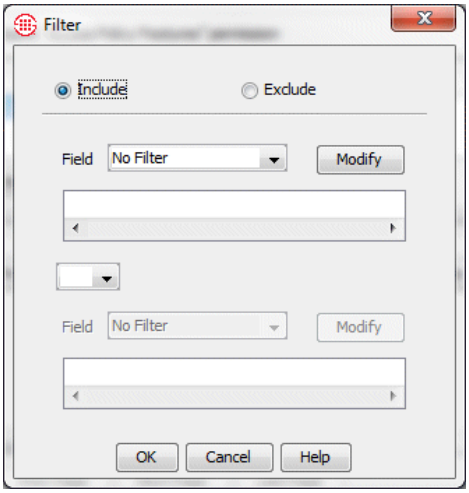


b. Click the Filter Definition that you want to use, and then click **OK**.

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.

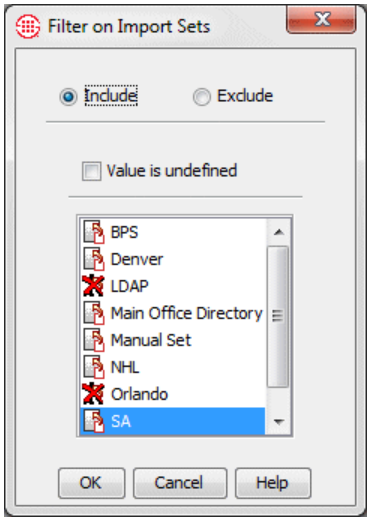


a. To define the Filter to exclude Listings that meet the criteria, select **Exclude**; to define the Filter to include all listings that meet the criteria, select **Include**.

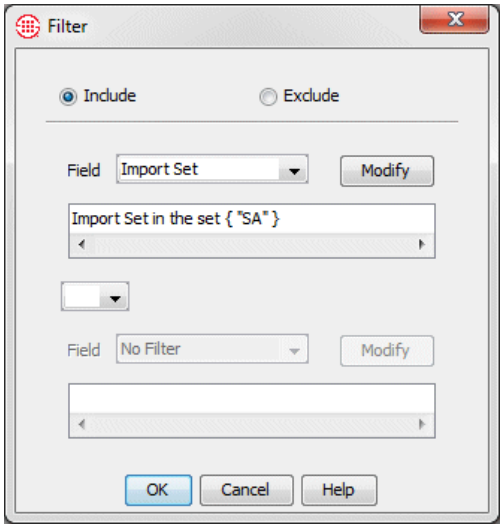
b. In the first **Field** box, click the down arrow. All of the fields in a Directory Listing appear as options.

c. Select the field to which you want to apply a filter. The **Filter** dialog box for the selected field appears. Define the criteria and click **OK**. See "Using Filters in the ETM System" in the *ETM® System User Guide* for instructions for defining each filter, if needed.

For example, suppose you want to include only Listings in a certain Import Set. Select **Import Set**. The **Filter on Import Set** dialog box appears.



Select **Include**, select the Import Set,, and then click **OK**. The criteria appear in the **Filter** dialog box, as illustrated below.



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

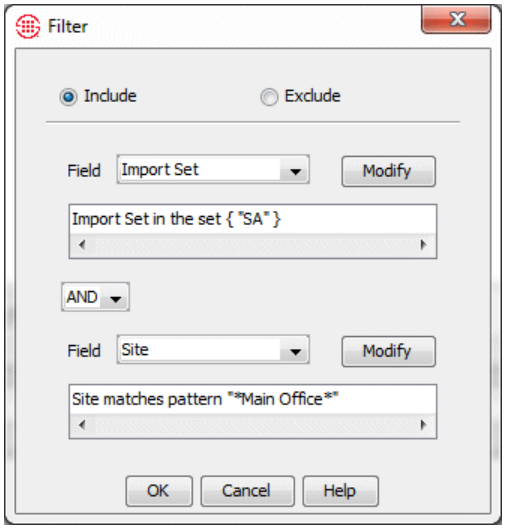
Filter Dialog Box	Filter on Import Set Dialog Box	Result
Include	Include **SA** Import Set	Includes Listings in the **SA** Import Set
Include	Exclude **SA** Import Set	Exclude Listings in the **SA** Import Set
Exclude	Exclude **SA** Import Set	Exclude Listings that are not in the **SA** Import Set.

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.

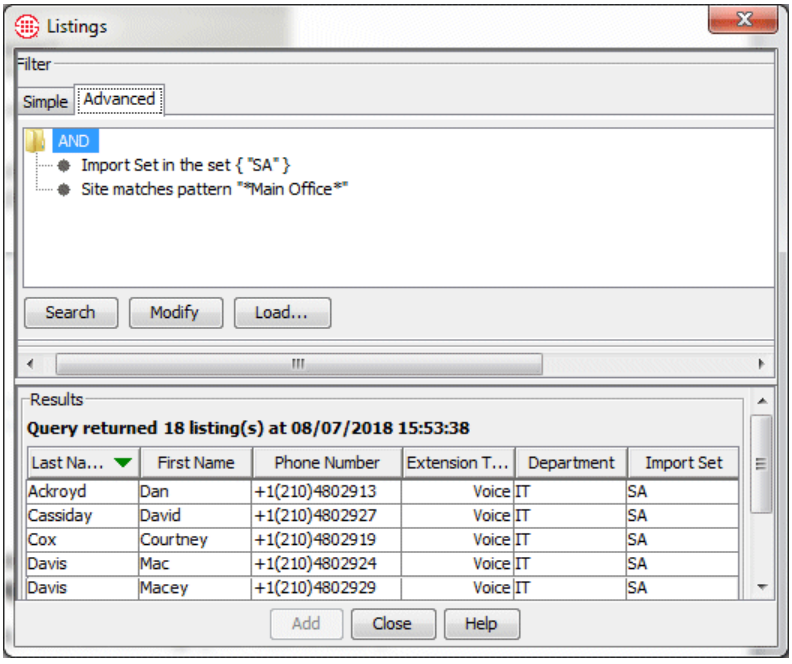
Note: You can use a combination of previously defined filters and new criteria. To add a predefined filter to your criteria, click **Load Filter**.

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 want also want to specify that the Listings are at the Main Office site. Select **AND** in the logical operator field, and then select **Site** in the second **Field** box, type **Main Office** as the substring,, and then click **OK**.



f. To specify additionally filter criteria, you can choose **Sub-filter** in one or both of the **Field** boxes. A second **Filter** dialog box appears. Define as explained above.

g. Click **OK.** The filter criteria appear in the **Advanced** tab, as illustrated below.



Note: 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 per Page" " in the *ETM® System Technical Reference* for instructions.

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

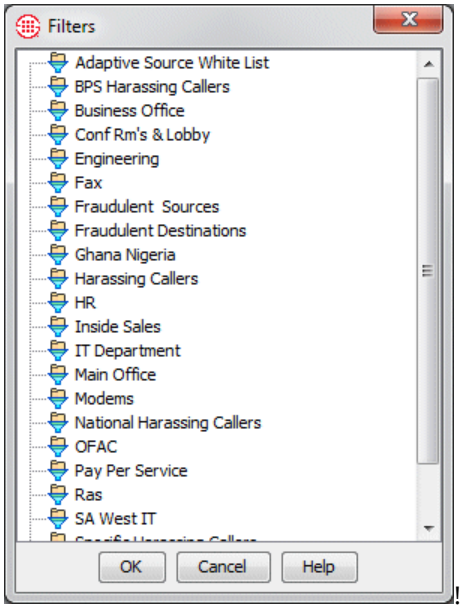
3. In the **Results** area, click the Listings you want to add.
   - To select multiple listings, hold down CTRL or SHIFT while clicking.
   - You must add Listings from each **Results** page separately. You cannot select Listings on multiple pages at once.
4. Click **Add**. The Listings are added to the **Source** or **Destination** field. Repeat to add Listings from additional pages, if needed.
5. When you have added all the Listings that you want to the field, click **Close** to dismiss the **Listings** dialog box.

Adding Filters to the Source or Destination Field

To add Filters to the Source or Destination field

1. Right-click in the **Source** or **Destination** field of a Rule, point to **Add**, and then click **Filter(s)**. The **Filters** dialog box appears.

Note: You cannot define or edit Filters from this dialog box. Use the Directory Manager to define and edit Filters.

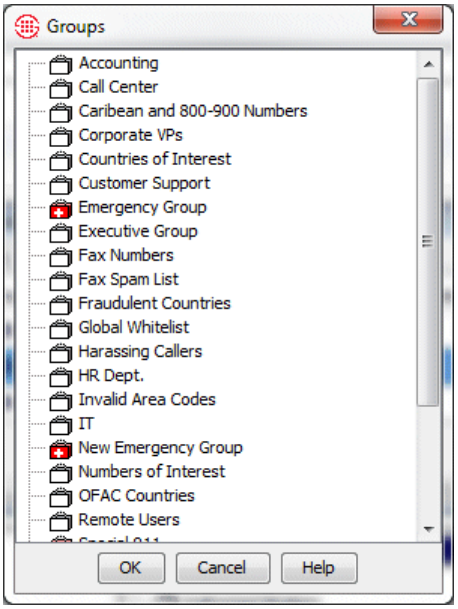


2. Click the Filter you want to add, and then click **OK**. To select multiple Filters, hold down CTRL or SHIFT while clicking.

Adding Groups to the Source or Destination Field

To add a Group to the Source or Destination field

1. Right-click in the **Source** or **Destination** field of a Rule, point to **Add**, and then click **Group(s)**. The **Groups** dialog box appears.



2. Click the Group you want to add, and then click **OK**.

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

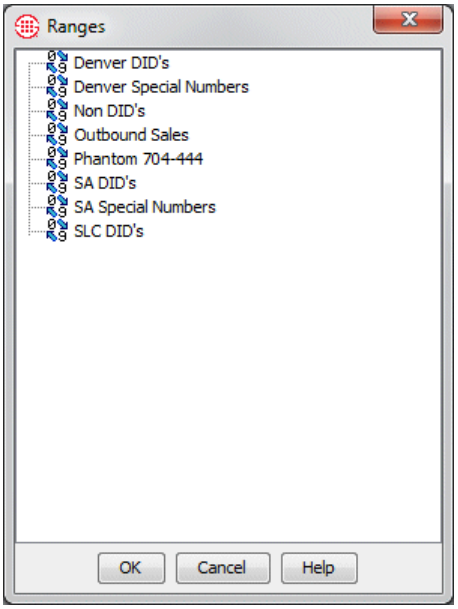
Adding Ranges to the Source or Destination Field

The **Ranges** dialog box is used to add one or more Directory Ranges to the **Source** or **Destination** field of a Rule and to view the contents of a Range.

You can only edit the contents of a Range in the Directory Manager. For instructions for creating or editing Directory Ranges, see "Directory Ranges" in the *ETM® System User Guide*.

To add a Range to a Rule

1. Right-click the **Source** or **Destination** field of a Rule, point to **Add**, and then click **Range(s)**.

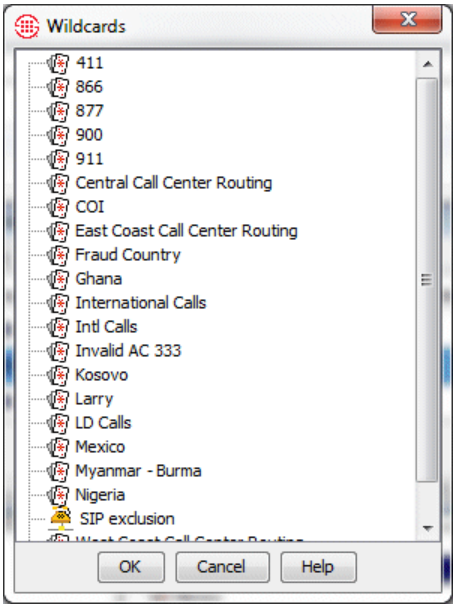


2. Click one or more Ranges that you want to add to the Rule, and then click **OK**. To select multiple Ranges, hold down CTRL or SHIFT while clicking.

Adding Wildcards to the Source or Destination Field

To add a Wildcard to a Rule

1. Right-click the **Source** or **Destination** field of a Rule, point to **Add**, and then click **Wildcard(s)**.



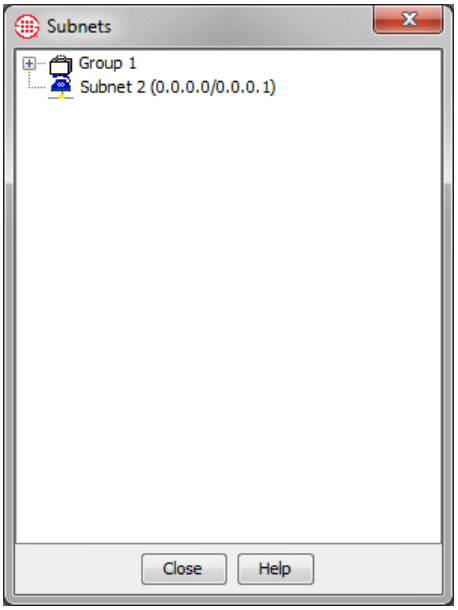
2. Click one or more Wildcards that you want to add to the Rule, and then click **OK**. To select multiple wildcards, hold down CTRL or SHIFT while clicking.

You can only edit the contents of a Wildcard in the Directory Manager. For instructions for creating or editing Directory Wildcards, see "Directory Wildcards" in the *ETM® System User Guide*.

Adding Subnets to the Source or Destination Field

To add a Subnet or Subnet Group to the Source or Destination field

1. Right-click in the **Source** or **Destination** column of a Rule, point to **Add**, and then click **Subnet(s)**. The **Subnets** dialog box appears.



2. Click the Subnet or Subnet Group you want to add, and then click **OK**.
   - To select multiple Subnets, hold down CTRL or SHIFT while clicking.
   - If the Subnet or Subnet Group you want to add has not been defined, you can add it on the fly from this dialog box. Right-click in the dialog box, and then click **New | Subnet** or **New | Subnet Group**. See "Subnets" in the *ETM® System User Guide* or online Help for instructions for defining Subnets, if necessary.

Adding Caller ID Restricted to the Source Field

Caller ID Restricted applies the Rule to calls for which the caller has blocked transmission of the Caller ID data. To apply the Rule to calls for which the source is unavailable but not deliberately blocked, use **No Source**. To apply the Rule to calls that have no source available OR it was blocked, place both **No Source** and **Caller ID Restricted** in the Rule. Note that if the phone number is present in the signaling even though CIDR

is indicated, both the phone number and CIDR are used for Policy processing. In this case, Rule order determines which takes precedence.

To add Caller ID Restricted to the Source field

- Right-click in the Rule and point to **Add**, and then click **Caller ID Restricted**.

Adding No Source to the Source Field

No Source applies the Rule to calls for which source is not available on trunks that support the delivery of source information, except for those where it was intentionally blocked (CIDR). To apply a Rule to all calls having no source, specify both **Caller ID Restricted** and **No Source** in the **Source** field of the Rule.

To add No Source to the Source field

- Right-click in the Rule and point to **Add**, and then click **No Source**.

Destination Field

The **Destination** field is used to apply the Rule based on properties of the destination of the call. **Any** (the default) means all destinations, or you can select one or more of the following:

- **Directory entities**—Directory Listings (contain phone numbers and URIs and identifying information), Ranges, Groups, Filters (dynamically include a set of listings that match the filter criteria), or Wildcards (phone or URI), used to apply the Rule to categories of calls, such as all calls from a specific area code or domain.
- **Subnets**—All URIs in a given subnet.

Adding Directory Entities to the Destination Field

You use the same procedures to add Directory entities to the Destination field as you do for the **Source** field. See the following procedures:

"Adding Listings to the Source or Destination Field" on page 31.

"Adding Filters to the Source or Destination Field" on page 37.

"Adding Groups to the Source or Destination Field" on page 37.

"Adding Ranges to the Source or Destination Field" on page 38.

"Adding Wildcards to the Source or Destination Field" on page 39.

Adding Subnets to the Destination Field

You use the same procedure to add Subnets to the **Destination** field as you do for the **Source** field. See "Adding Subnets to the Source or Destination Field" on page 40 for instructions.

Time Field

The **Time** field is used to specify whether the Rule applies at all times or at specific date(s) and time(s). A Time can specify a maximum of three different start and stop periods and is interpreted as local to the Span. The default is **Any**, which means the Rule applies at all times.

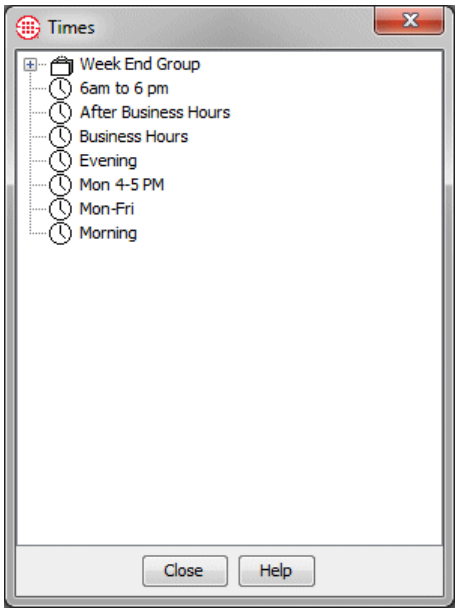
You can use negation to further define the **Time** field to define the calls to which the Rule does not apply; that is, if the call data does not match the negated criteria, the Rule fires. For example, the default **Business Hours** Time specifies 8 AM to noon and 1 PM to 5 PM. (You can modify it to your operating hours). If you add the **Business Hours** Time to the Rule and then negate it, the Rule applies during non-business hours.

When the **Time** field is negated, a red exclamation point appears in the **Time** field.

Adding a Time to a Rule

To add a Time to a Rule

1. Right-click in the **Time** field, and then click **Add**. The **Times** dialog box appears.



2. Click the Time you want to add, and then click **OK**.
3. To negate the **Time** field so that the Rule applies at all times other than those specified, after adding one or more Times to the field, right-click the field, and then click **Negate**.

Call Duration

The **Call Duration** field is used to apply a Rule based on the length of a call. **Any** applies to calls of any duration and is the default.

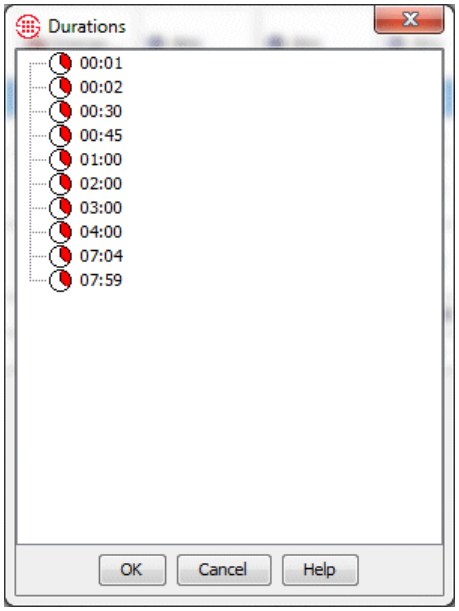
Durations can specify call lengths from 0 hours and 0 minutes to 999 hours and 59 minutes. For example, you can define a Rule to fire when Modem calls last for more than 30-minutes. A Duration of 0 hours and 0 minutes behaves as if no duration is specified.

The order of Rules that specify duration is very important for proper results. For information about special considerations of call duration processing, see “Call-Duration Processing” on page 23.

Adding a Call Duration to a Rule

To add a call duration to Rule

1. Right-click in the **Call Duration** field, and then click **Add**. The **Durations** dialog box appears.



2. Click the **Duration** you want to add.
   - If the Duration you want to add is not yet defined, right-click in the dialog box, and then click **New Duration**. The **Duration Properties** dialog box appears. Type or select the duration in hours and minutes, and then click **OK**.
3. Click **OK**.

Note: The order of Rules that specify duration is very important for proper results. For information about special considerations of call duration processing, see "Call-Duration Processing" on page 23.

Action Field

The **Action** field specifies the action to take when a call matches the Rule:

- **Allow** permits the call to continue. This is the default.
- **Terminate** disconnects the call.

Specifying a Terminate Action for a Rule

To specify a Terminate Action for a Rule

- Right-click in the **Action** field, and then click **Terminate**.

Note that the Span must be set to allow call terminations before termination can occur. If you install a Policy on a Span on which termination is not enabled, a **Warning** message appears in the **Status Tool** during Policy verification.

Call Type Field

The **Call Type** field identifies the type(s) of call traffic to which the Rule applies. **Any** is the default, which means the Rule applies to calls of all types. Call types are predefined and cannot be user-modified.

You can use negation to further define the **Call Type** field to specify the calls to which the Rule does not apply; that is, if the call type does not match the negated call type(s), the Rule fires. For example, you could ensure that a Rule not apply to voice, fax, unanswered, and undetermined calls by adding them to the **Call Type** field, and then negating it.

When the **Call Type** field is negated, an exclamation point appears next to the call types added to the field.

IMPORTANT Negation applies to all call types in the Rule.

Note that certain call types apply to all Span types, while others apply only to one or more specific types. Ensure that the call types you specify apply to the Span types in the Span Groups on which the Rule is to be installed.

Specifying Call Type in a Rule

The call types that can be used in Policies are described in "Call Type" on page 17.

To specify one or more call types

1. Right-click in the **Call Type** field, and then click **Add**. The **Call Types** dialog box appears.
2. Click one or more call types to add, and then click **OK**.
   - To remove a call type from the field, right-click the call type, and then click **Remove**.

Track Field

The **Track** field is used to specify one or more follow-up actions when a call matches a Rule. Tracks are used to generate logging and notifications as follows:

Note: For instructions for customizing the notification messages, see "Customizing Policy Track Messages" in the *ETM® System Technical Reference*.

- **Log Tracks** cause the event to be written to the **Policy Log**. Note that data for all calls is saved in the Database. The **Log** Track is used to track and report on specific Policy events. The **Log** Track is added by default when any other Track is added.
- **Real-Time Alert Tracks** cause an alert to be displayed in the Alert Tool.
- **Email Tracks** are user defined and contain one or more Contacts with email addresses. If a call matches a Rule with an Email Track, all Contacts specified in the Email Track are notified when the Rule fires.

  For instructions for defining email tracks, see "Defining an Email Track" in the *ETM® System User Guide*.
- **SNMP Tracks** generate an SNMP alert to a network management station. For information about SNMP Tracks, see "SNMP" in the *ETM® System Administration and Maintenance Guid*e.
- **Syslog Tracks** generate a syslog alert..

The ETM Server generates Tracks when it receives the Rule-fired message from the Span. Therefore, if network connection is lost between the ETM Server and the Span, Tracks are not generated when a Rule fires until after the network connection is restored. (**Allow** and **Terminate** actions still occur immediately, because these are performed by the Span, not the Server.)

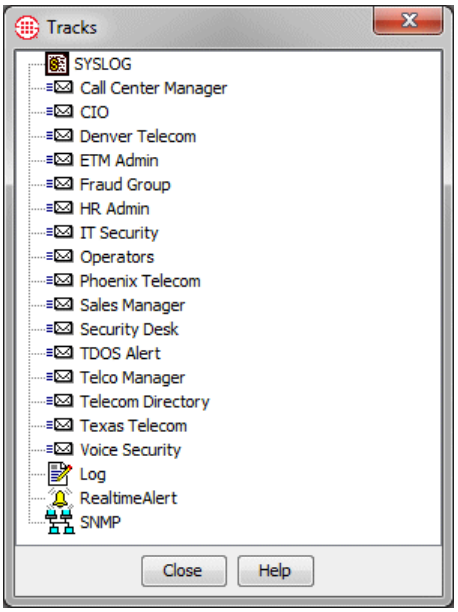
Alerts for calls that match the Emergency Rule (e.g., 911 calls) fire at the beginning of the call, as soon as the dialed digits are seen, and then automatically refire at the end of the call when all call information is available to include.

Specifying a Track for a Rule

Note: If the Email Track you want to add has not yet been created, you can create one on the fly by right-clicking in the **Tracks** dialog box. See "Tracks" in the *ETM® System User Guide* for instructions for defining Email Tracks.

To specify a Track for a Rule

1. Right-click in the **Track** field, and then click **Add**. The **Tracks** dialog box appears.



2. Click the Track(s) you want to add, and then click **OK**. To select multiple Tracks, hold down CTRL or SHIFT while clicking.

Install On Field

The **Install On** field provides the option to install certain Rules on only some or one of the Span Groups assigned to the Policy, instead of installing all of the Rules on all of the Span Groups, which is the default. **Any** means all of the Span Groups assigned to the Policy are to enforce the Rule.

Only one Firewall Policy can be installed on a Span Group at a time; however, a Policy can have multiple Span Groups assigned to it, and each Rule of the Policy can specify which of those Span Groups is to enforce that Rule. When you install a Policy, it is installed on all of the Spans in the assigned Span Groups, but each Span enforces only the Rules assigned to it in the **Install On** field.

Specifying Span Groups to Install On

To install the Rule on only some Span Groups

1. Right-click in the **Install On** field, and then click **Add**. The **Span Groups** dialog box appears listing the Span Groups that are assigned to the Policy.
2. Click the Span Group to which this Rule applies, and then click **OK**.

Comments Field

The **Comments** field provides a space to type optional information regarding the Rule (e.g., the purpose for the Rule, creator of the Rule, or date/time created). The comment has no effect on the processing of the Rule, but comments appear in the **Call Log** and **Policy Log**, and can be used in Usage Manager Reports. If a Track is assigned to the Rule, the comment is included in the notification.

Adding a Comment to a Rule

To add a comment to a Rule

1. Right-click in the **Comment** field, and then click **Edit comments**. The **Edit Comments** dialog box appears.
2. Type the comment, and then click **OK**.

Emergency Rule

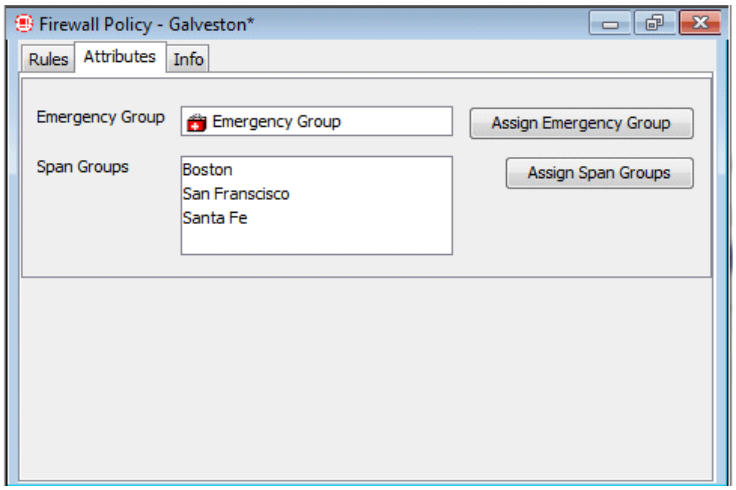
When you define a new Policy, you should assign a user-defined Emergency Group of Emergency numbers to the Emergency Rule. This Emergency Group should contain numbers specific to the Appliance locale. By default, each Policy contains the default Emergency Group that contains the national Emergency number for the Server locale. For example, in the United States, the Emergency Group contains the 911 phone number.

To specify other emergency numbers specific to the Appliance locale that are never to be blocked by the ETM System, you must create a new Emergency Group in the **Directory Manager**, and then assign the new Group to the Policy on the **Attributes** tab of the **Firewall Policy** editor. Each Policy can contain only one Emergency Group.

Assigning an Emergency Group to the Policy

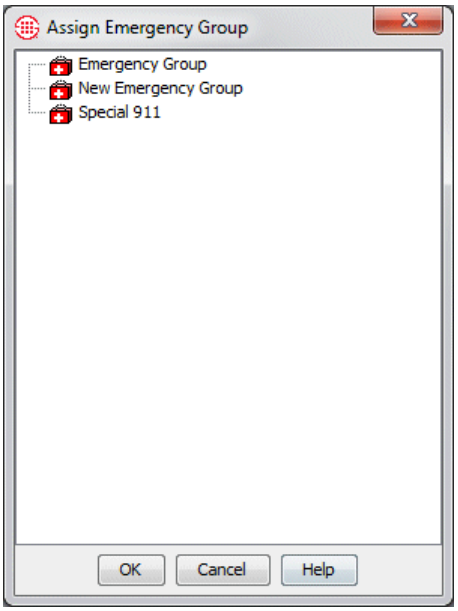
To assign a locale-specific Emergency Group to the Policy

1. Click the **Attributes** tab.



2. Click **Assign Emergency Group**. The **Assign Emergency Groups** dialog box appears with all defined Emergency Group(s) listed. (To view the members in an Emergency Group, right-click the Group, and then click **View**.)

Note: For instructions for defining Emergency Groups in the Directory Manager, see "Defining a New Emergency Group" in the *ETM® System User Guide*.



3. Double-click the Emergency Group, or click the Emergency Group, and then click **OK**.

The new group appears in the **Emergency Group** box on the **Attributes** tab and in the **Destination** field of the Emergency Rule in the Policy.

4. On the main menu, click **File | Save** or click the **Save** icon on the Performance Manager toolbar.

Installing a Policy

Before the Policy is enforced, you must install it on the assigned Span Groups. Any time you make a change to an installed Policy, you must reinstall the Policy for the change to take effect on the Spans. See "Installing a Policy" on page 69 for more information.

To install a Policy

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

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

If no object issues are encountered, the Policy is verified; if it passes verification, it is pushed to the Spans. See "Verifying a Policy" on page 62 for information about what verification checks. The verification and installation process appears in the **Status Tool**, accessed from the ETM System Console.

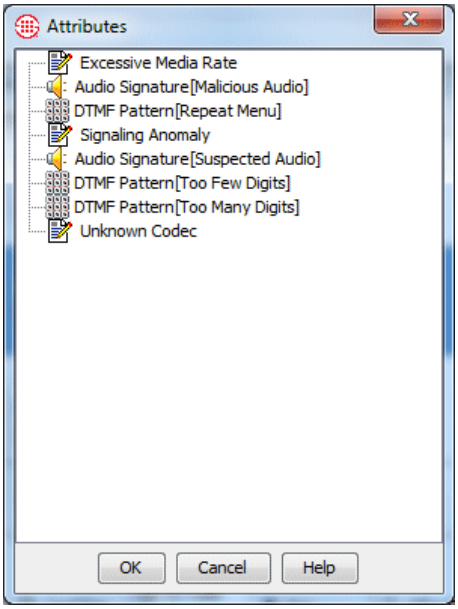
If you used Normal Mode and an issue with the number of objects was encountered, you can either modify the Policy, or choose to install it again using Priority Mode.

Tracking DTMF Digits in Firewall Policies

You can define Firewall Policy Rules to look for individual calls with specified mid-call DTMF dialing patterns. Note that DTMF digit patterns can be used in Rules without being stored in the Database. A separate per-Span setting governs whether they are stored.

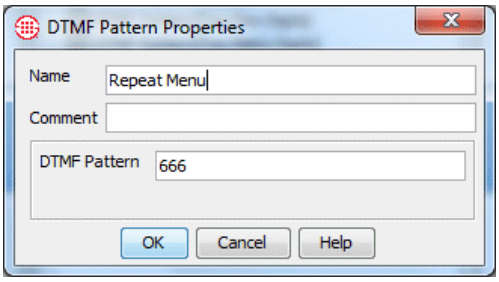
To track calls with certain patterns of mid-call DTMF digits

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



2. Do one of the following:

   - Double-click an existing pattern to add it to the Rule.
   - Create a new pattern by right clicking in the dialog box and clicking **New**. The **DTMF Pattern Properties** dialog box appears.



   i. In the **Name** box, type a name to identify this pattern .

   ii. In the **DTMF Pattern** box, type the pattern of digits to be detected. Regular expressions are supported.

   iii. Click **OK**. The new pattern appears in the **Attributes** dialog box.

   iv. Click it and click **OK** to add it to the Rule.

Rule Definition Strategies

Methods of Effective Development

Effective Policies are written with the specific needs of your organization or department in mind. A Policy that works perfectly for your organization may not work at all for another. The following is one approach to determining your specific Policy needs:

1. Run the ETM® System with only the default Policy, which allows all calls. All information for calls on monitored channels is stored in the database.
2. Create reports of call activity using the Usage Manager. For example, the Telecom Operations Report template "List of All Active Numbers over Past 30 Days" provides the internal phone number and call type for all calls passing through the ETM System during the past month.
3. Review the reports to identify problem areas, such as modem calls, multiple short-duration calls, or calls to long-distance numbers.
4. Write Policy Rules to cover the areas identified, such as defining a Policy to send an email when unauthorized modem use is detected.

Note: For details about creating reports, see the *Usage Manager User Guide*.

Organizing the Rules in the Policy

After all of the issues are identified and the Rules are defined, organize them for optimum Policy processing. Consider the following:

- When Call Type is specified in a Rule, processing pauses while call type is identified (up to 20 seconds). Therefore, put "Call Reject" Rules—those that do **not** rely on call type or DTMF patterns—at the beginning of the Policy. This way, they can be processed while call type determination is still ongoing and DTMF patterns are being evaluated.
- Place Rules that specify DTMF digits after any Rules that specify Call Type, since the amount of time required to determine whether a DTMF pattern matches is variable depending on whether/which digits are entered during the call. Again, if a Rule that specifies a DTMF pattern is encountered, processing pauses while the Rule is evaluated for a match.
- On Spans that use SMDR (PBX logging data), the Ambiguous Call Processing setting on the Span determines whether processing of Rules that specify outbound Source is suspended while the Span waits for the

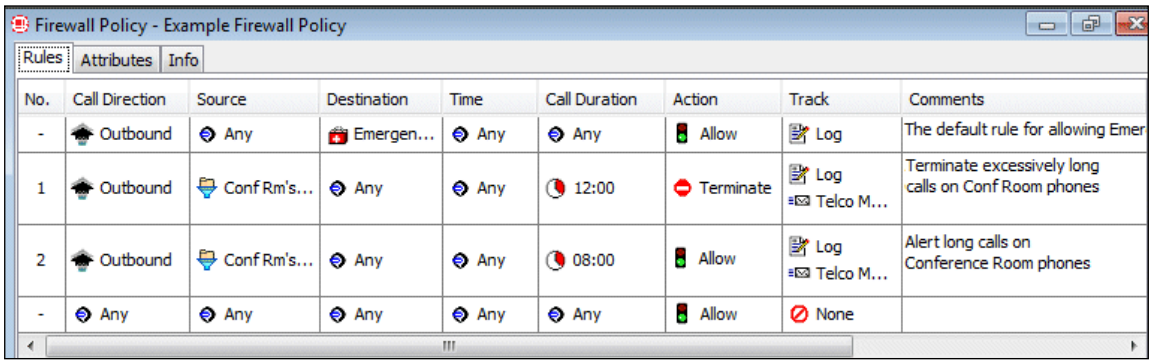
SMDR data from the Server or whether the Rule is skipped and processing continues while waiting for SMDR. (SMDR data is not available until after the call ends.) If the Span is configured so processing stops while waiting for SMDR, and then when possible, place calls that require outbound Source after Rules that do not specify Source.

- Place specific Rules in the Policy before general Rules. Once a Rule fires, no subsequent Rules in the Policy are processed. (That is, if you have 10 Rules in the Policy and Rule 6 fires, Rules 7-10 are not processed.)
- Does a terminate Rule block calls that you want to allow? For example, suppose you want to allow calls to certain countries only from a specific department, Is there a “Terminate all such calls” Rule that will fire before an "allow specific department to make such calls" Rule?
- When specifying call duration, put longer durations first in the Policy. If you place the shorter duration first and the Rule fires, the longer duration Rule is never processed. See "Call-Duration Processing Example" on page 52 for more information.

Call-Duration Processing Example

Consider the following example. At times, conference room bridge phones are inadvertently left on after the meeting ends. Suppose you want to generate an alert for these lines for calls that last 8 hours and terminate the call if it last 12 hours, because you know no conference call at your organization lasts that long.

To achieve this, you need two Rules, as shown in the illustration below.



1. Define a Rule with a **Call Duration** of 12 hours for **Outbound** calls using a Directory Filter containing conference room phones in the **Source** field with an Allow **Action** and an Email **Track**. (Rule 1)
2. Define a Rule with a **Call Duration** of 8 hours for **Outbound** calls using a Directory Filter containing conference room phones in the **Source** field with a Terminate **Action** and an Email **Track**. (Rule 2)

IMPORTANT If the order of these Rules were reversed so that the 8-hour Duration Rule came first, the 12-hour Rule would never be considered,

because subsequent processing never passes a Rule that has already fired. After the 8-hour Rule had fired, processing would end an a matching call that reached 12 hours would not be terminated.

Writing Effective Rules

How you should define the Rules for your Policies depends upon your security and management goals. Two common approaches are described below.

Use Specific Rules—Some enterprises prefer to develop Rules to specifically allow certain call traffic (e.g., authorized modems) and to terminate any calls not specifically allowed (e.g., fax numbers that are not to be used for voice calls). In many cases, a final "Terminate all" Rule is used to terminate any call that does not match a prior Rule.

Use Generic Rules—Some organizations prefer to write generic Rules that cover all calls in to and out of the organization, and then write specific Rules to handle exceptions. These generic Rules typically cover everyone in an organization, or at least entire departments. When using this approach, place Rules that are more specific at the start of the Policy. In this way, most of calls fall through the specific Rules and are then processed by the more generic Rules. For example, you could write a specific Rule allowing calls to specific countries only from a certain group in your organization and then a generic Rule to terminate all other calls to these countries.

Policy-Centric vs. Span Group-Centric Approach

When you organize your Polices, Spans, and Span Groups, consider the following two models:

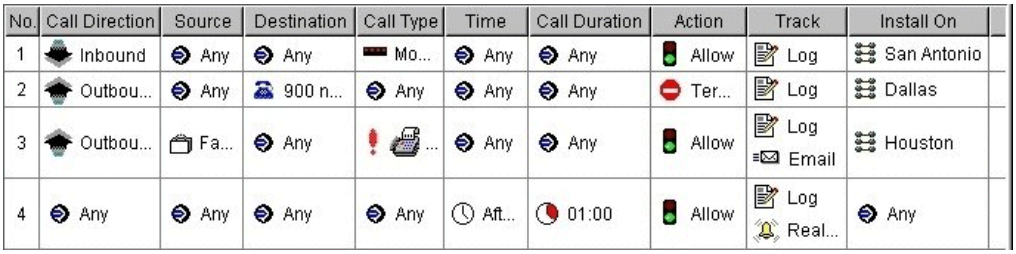
- The *Policy-Centric* approach employs a single Policy covering all Span Groups, using the **Install On** field to identify specific Rules for some Span Groups. This model is most appropriate for small organizations, organizations that are largely centralized, or large, dispersed organizations where one office has responsibility, authority, and the capability to distribute a Policy to all of the Span Groups in the enterprise.
- The *Span-Group-Centric* approach employs multiple Policies, each installed on separate Span Groups. The Span-Group-centric approach is most appropriate for large, dispersed organizations. Dispersed sites may be substantially independent business units where, within corporate guidelines, unique telecommunications or security issues exist that are best managed in an independent Policy.

Policy-Centric Approach

Suppose you have two Span Groups at your branch office. One Span Group monitors lines for your Marketing offices, while the other monitors lines in your Call Center. These two environments may have different security, resource-utilization, and management requirements.

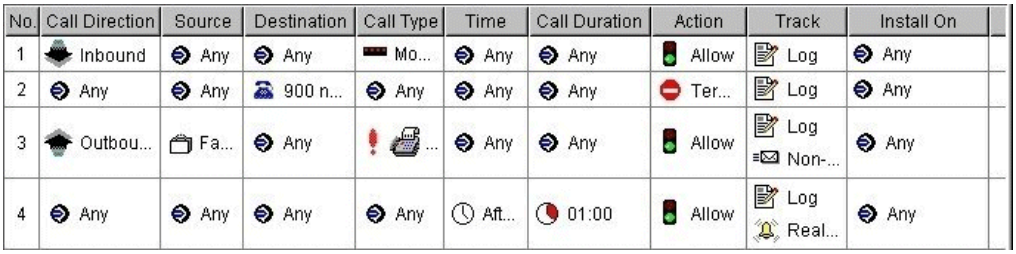
Using a Policy-centric approach to Policy definition, you would create a single Policy to apply to both Span Groups and assign both Span Groups to the Policy. You would then define some Rules that apply only to the Marketing Span Group, some Rules that apply only to the Call Center Span

Group, and other Rules that apply to both environments. Then, you would specify the appropriate Span Group for each Rule in the **Install On** field, using **Any** for Rules that apply to both Span Groups. When you install this Policy, it is installed on all of the Spans in both Span Groups, but each Span enforces only the Rules assigned to its Span Group in the **Install On** field, as shown in the illustration below.



Span Group Centric Approach

The Span Group-centric approach uses multiple Policies; each Policy centers on a single Span Group or set of related Span Groups. The **Install On** field for each Rule is usually left at the default of **Any**, as shown in the illustration below, because each Span Group has its own Policy.

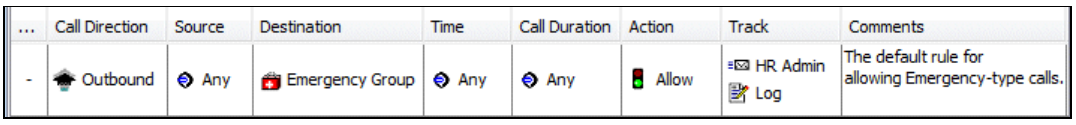


Defining Rules for Specific Issues

Before you define the Rules for a Policy, you need to identify the issues that you want to address with your Policy. Some common issues are described below, along with suggestions of how you can define Rules to address each issue.

Alerting on 911 Calls

Add a Track to the default Emergency Rule to receive an alert when anyone in your organization makes an emergency call. The following Rule uses an Email alert to the HR Admin.



Managing Harassing Callers

Harassing calls can be threatening or simply a nuisance but constitute negative-value calls in either case. The following Rule terminates calls from numbers in a Directory Group containing known Harassing Callers and generates an SNMP trap.

...	Call Direction	Source	Destination	Time	Action	Track	Install On	Comments
1	Inbound	Harassing Callers	Any	Any	Terminate	Log SNMP	Any	Terminate known harassing callers

Managing Calls to/From Specific Counties

While certain International calls may be normal for your organization, calls to/from certain countries may represent potentially malicious or fraudulent activity or be necessary/normal only for a specific segment of your organization. For example, suppose want to prevent all calls to/from OFAC countries and allow calls to certain other countries only for a certain group in your organization. The following Rules illustrate this scenario.

No.	Call Direction	Source	Destination	Time	Action	Install On	Track	Comments
4	Outbound	Corporate	INTL Fraud Cou... Jamaica	Any	Allow	San Antonio...	Log	Make an exception to allow only Corporate to call certain countries
5	Outbound	Any	INTL Fraud Cou... Jamaica	Any	Terminate	Any	Fraud Group Log SYSLOG	Terminate calls to specific coutnries
6	Outbound	Any	OFAC Countries	Any	Terminate	Any	Fraud Group Log	Prevent calls to OFAC countries
7	Inbound	OFAC Countries	Any	Any	Terminate	Any	Fraud Group Log	Prevent calls from OFAC countries

Rule 4allows calls to the countries in the **Destination** field only from phone numbers in the Corporate Directory Group and logs such calls. The members of this Group are in the San Antonio Corporate office, so this Rule uses the **Install On** field to specify that it is only installed on that Span Group. Rule 5 terminates all other calls to these countries and sends an email alert to the Fraud Group and Syslog alert if such a call is attempted. Note that it is important that the Rule allowing specific calls of this type be placed before the Rule terminating all other such calls, since recall that Policy processing never passes a Rule that has fired unless there is a previous Duration Rule that has not been matched or the call type changes. This means if the Terminate Rule were before the Allow Rule and such a call occurred from numbers in the Allow Rule, the call would be terminated because the Allow Rule would never be processed.

Rules 6 and 7 prevent calls to and from OFAC countries and sends an Email alert to the Fraud Group if such a call is attempted.

Managing Unanswered or Busy Lines

You can define a Rule so that you are immediately notified when calls are identified as **Unanswered** or **Busy**.

The Rule below fires if any call to the numbers defined in the **Call Center** Group is identified as **Unanswered** or **Busy**. A **Real-Time Alert** is triggered when this Rule fires, and the call is recorded in the **Policy Log**.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track
1	Inbound	Any	Call Center	Busy Unanswered	Any	Any	Allow	Log RealtimeAlert

Managing Dedicated Fax Lines

To prevent misuse of dedicated fax lines, you can create Policies that terminate calls that are not authorized and that alert you when fax lines are used for calls other than faxes.

The Rule illustrated below prevents anyone from making voice calls on dedicated fax lines.

Call Direction	Source	Destination	Call Type	Time	Action	Track
Outbound	Fax Numbers	Any	Fax	Any	Terminate	Admin... Log

Note: See "Directory Groups" in the *ETM® System User Guide* for instructions for adding phone numbers to a Group.

For example, define a Rule such that any outbound calls made from phone numbers in the **Fax Numbers** Group that are not identified as fax calls (by placing **Fax** in the **Call Type** field and then negating it) are terminated, an email notification is sent, and the call is recorded in the **Policy Log**.

IMPORTANT The **Fax Numbers** Group is empty by default, as are all of the default Directory Groups. If you want to use the **Fax Numbers** Group in your Policy, your fax phone numbers must be added to the Group. You can also create a new Group that contains your fax numbers and insert that Group into the Rule.

Managing Caller ID Restricted Calls

In the **Source** field of Rule, the following objects are provided to allow you to manage calls for which the source number is unavailable or purposefully blocked.

- Add **Caller ID Restricted** to a Rule to fire on calls with Caller ID blocked by the caller.
- Add **No Source** to a Rule to fire on calls with no source available. Calls with Caller ID blocked by the caller do not trigger these Rules.
- Add both **No Source** and **Caller ID** to a Rule to fire on calls with Caller ID blocked OR no source available.

In the Rule illustrated below, a voice call to the **Executive Group** is terminated if the caller has blocked the Caller ID information.

...	Call Direction	Source	Destination	Time	Action	Track	Comments
3	Inbound	Caller ID Restricted	Executive Group	Any	Terminate	Log	Protect Exec Group from Possible Harassment Calls

Example Policy

This example Policy includes a number of the Rules discussed in this section and the two Duration Rules discussed earlier.

Firewall Policy - Example Firewall Policy

Rules | Attributes | Info

No.	Call Dire...	Source	Destination	Time	Call Type	Call Dura...	Action	Install On	Track	Comments
-	Outb...	Any	Emergency Group	Any	Any	Any	Allow	Any	HR Admin Log	The default rule for allowing Emergency calls.
1	Inbo...	Harassing Call...	Any	Any	Any	Any	Terminate	Any	Log SNMP	Terminate known harassing callers
2	Outb...	Conf Rm's & L...	Any	Any	Any	12:00	Terminate	Any	Log Telco Mana...	Terminate excessively long calls on Conf Room phones
3	Outb...	Conf Rm's & L...	Any	Any	Any	08:00	Allow	Any	Log Telco Mana...	Alert long calls on Conference Room phones
4	Outb...	Corporate	INTL Fraud Cou... Jamaica	Any	Any	Any	Allow	San Anto...	Log	Make an exception to allow only Corporate to call certain countries
5	Outb...	Any	INTL Fraud Cou... Jamaica	Any	Any	Any	Terminate	Any	Fraud Group Log SYSLOG	Terminate calls to specific coutnries
6	Outb...	Any	OFAC Countries	Any	Any	Any	Terminate	Any	Fraud Group Log	Prevent calls to OFAC countries
7	Inbo...	OFAC Countries	Any	Any	Any	Any	Terminate	Any	Fraud Group Log	Prevent calls from OFAC countries
8	Outb...	Any	Any	Any	Fax	Any	Terminate	Any	Log	Only faxes on fax lines
9	Inbo...	Call Center	Any	Any	Unansw... Busy	Any	Allow	Any	Contact Ce... Log	Alert Unanswered/Busy Call Center lines
-	Any	Any	Any	Any	Any	Any	Allow	Any	None	

Note the following important points about this example Policy:

- The first Implied Rule, the Emergency Rule, occurs first in every Policy so that calls to emergency numbers are always allowed. It is now defined to send an Email notification for any emergency call.
- All of the Call Reject Rules (those that specify **Any** in the Call Type field) are placed before any Rules that specify call type.
- The longer Duration Rule is properly placed before the shorter Duration Rule, as previously discussed.

- The specific Rule allowing specific calls is properly placed before the general Rule terminating all such calls.
- The last Implied Rule allows any call that did not match a previous Rule.

Policy Administration

Managing Policies

This section provides procedures for managing Policies, including:

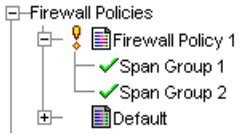
Note: For procedures for managing Rules, see "Managing Rules" on page 73.

- "Dirty" Polices
- Adding Rules to Policies
- Opening, renaming, or deleting a Policy
- Refreshing a Policy during editing
- Verifying a Policy
- Viewing the properties of a Policy
- Specifying a different Emergency Group for a Policy
- Creating a Span Group
- Assigning Span Groups to a Policy
- Saving/Installing/Uninstalling a Policy
- Printing a Policy
- Creating a new Policy from another Policy
- Viewing multiple Policies at the same time

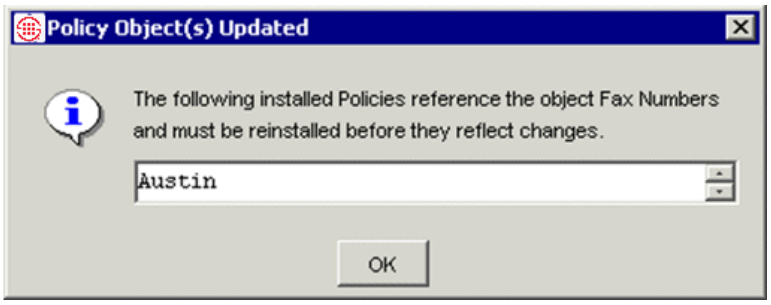
Dirty Policy Indicator

When you make changes to user-defined components in an installed Policy (such as adding Listings to a Directory Group or editing a Time), you must reinstall the Policy before the changes take effect on the Span.

In the tree pane, a yellow exclamation point appears next to the Policy name to indicate that something has changed in the Policy and the Policy needs to be reinstalled.



If you have the Performance Manager open, a **Policy Object(s) Updated** message indicates which of the installed Policies are affected by the changes.



See "Installing a Policy" on page 69 for instructions for installing the Policy.

Adding a Rule to a Policy

To add a Rule to a Policy

- Do one of the following:
  - On the Performance Manager toolbar, click an **Add Rule** icon.

    Add Rule to Top adds a Rule as the first Rule after the Emergency Rule.

    Add Rule to Bottom adds a Rule as the last Rule before the final implied Rule.

    Add Rule Before Selected adds a Rule immediately prior to the selected Rule.

    Add Rule After Selected adds a Rule immediately after the selected Rule.
  - Right-click in the blank area of the Policy, point to **Add Rule**, and then click **Bottom** or **Top**. The new Rule is inserted between the implied Rules.
  - Right-click in any field of the Rule, point to **Add Rule**, and then click one of the following:
    - **Bottom** adds a Rule as the last Rule before the final implied Rule.
    - **Top** adds a Rule as the first Rule after the Emergency Rule.
    - **Before** adds a Rule immediately prior to the selected Rule.
    - **After** adds a Rule immediately after the selected Rule.

Opening a Policy

To open a Policy

- In the tree pane, double-click the name of the Policy or right-click the name of the Policy, and then click **Edit**.

What the Color-Coding Means in Policies

When you open an installed Policy, the Rules are color-coded, as follows:

- *Yellow* indicates that multiple Span Groups are assigned to the **Install On** field of the Rule, but not all of those Span Groups are currently enforcing the Rule. This may happen, for example, if you assign the same Span Group to more than one Policy, since the Policy can only be installed on one Span Group at a time.
- *Cyan* indicates that the Rule is not being enforced. This occurs when you have multiple Span Groups assigned to the Policy and none of the Span Groups specified in the **Install On** field is currently enforcing the Rule.
- *White* indicates that all Span Groups in the **Install On** field are enforcing the Rule. (If a Policy is not installed, the Rules are always white.)

Refreshing a Policy During Editing

When you refresh a Policy you are editing that has unsaved changes, it reverts it to its last saved state; all unsaved changes are discarded.

To refresh a Policy

- Click **File | Refresh** or click the **Refresh** icon  .

Deleting a Policy

You can delete a Policy that you no longer intend to use. Alternatively, you can simply deactivate a Policy by uninstalling it. See "Uninstalling a Policy" on page 70.

You cannot delete an installed Policy; it must be uninstalled before you can delete it.

To delete a Policy

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

Verifying a Policy

See "Opening the Status Tool" on page 63 for details about the **Status Tool**.

When you attempt to install a Policy on a Span Group, it is automatically verified for proper configuration. You can also choose **Verify** from the **Policy** menu to verify a Policy without installing it.

Verification checks every enabled channel on the Span and generates warning or error messages, if applicable. For example, if **Terminate** is specified for a Rule that requires SMDR (for example, one that specifies outbound source on a T1 circuit), a warning message is displayed for each channel. Verification results appear in the **Status Tool**, which is launched form the ETM System Console.

- If a warning message is generated, the Policy can be installed.
- If an error message appears, verification fails, and the Policy cannot be installed until you correct the error.

What Verification Checks

Before a Firewall Policy is installed on a Span Group, it is verified for proper configuration. Messages appear in the **Status Tool** as verification proceeds.

Verification fails if:

- The Policy contains empty Directory, Subnet, or Time Objects.

Verification succeeds with a Warning if:

- Terminate Rules cannot fire, either because the Span has to wait for SMDR information from the Server or Terminate Rules are not allowed on the Span.
- The Policy contains duplicate Rules.
- Tracks have no Contacts. (Email Tracks must have a Contact defined.)
- Rules have no comments in the **Comment** field.

How to Verify a Policy

You can verify a Policy before attempting to install it. (Policies are automatically verified as they are installed.)

To verify a Policy

1. Ensure that the Policy that you want to verify has the focus.
2. Click **Policy | Verify**.
   - If the Policy passes verification, the **Verification Passed** message appears.
   - If the Policy does not pass verification, the **Verification Failed** message appears.

   The verification results appear in the **Status Tool**.

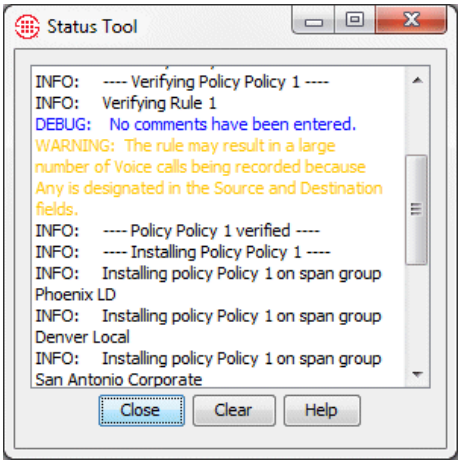
Opening the Status Tool

The **Status Tool** shows activity that occurs when a Policy is being verified and/or installed. By default, you must launch the **Status Tool** manually to see the results. For instructions for configuring the **Status Tool** to appear automatically when you install or verify a Policy, see "Status Tool" in the *ETM® System User Guide*.

To open the Status Tool

- On the ETM System Console main menu, click **Tools | Status** or, on the toolbar, click the **Status Tool** icon  .

  The **Status Tool** appears.



- To close the **Status Tool**, click **Close**. Results remain in the **Status Tool**, even if you close the tool, until you click **Clear** to erase them.

Viewing the Properties of a Policy

You can view the properties of a Policy on the **Info** tab of the Policy. The properties of a Policy include the following information:

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

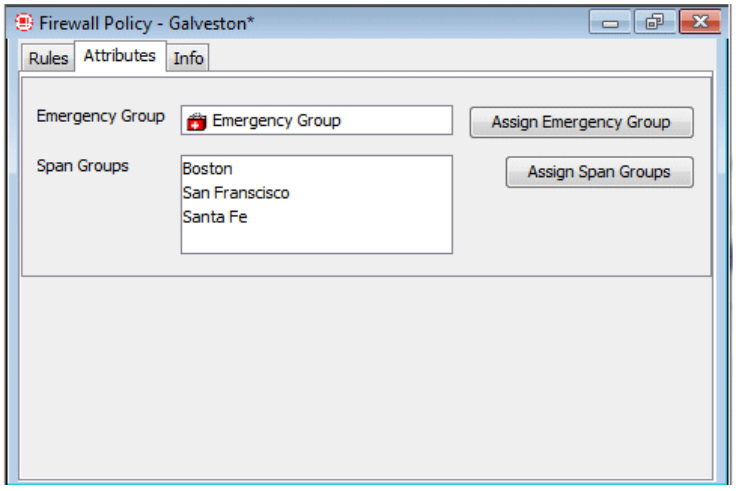
Specifying a Different Emergency Group

You cannot edit the default Emergency Group. If you want to specify other emergency numbers that are never blocked by the ETM® System, you must create a new Emergency Group in the **Directory Manager**, and then assign the new group on the **Attributes** tab of the Policy. Only one Emergency Group can be assigned to a Policy.

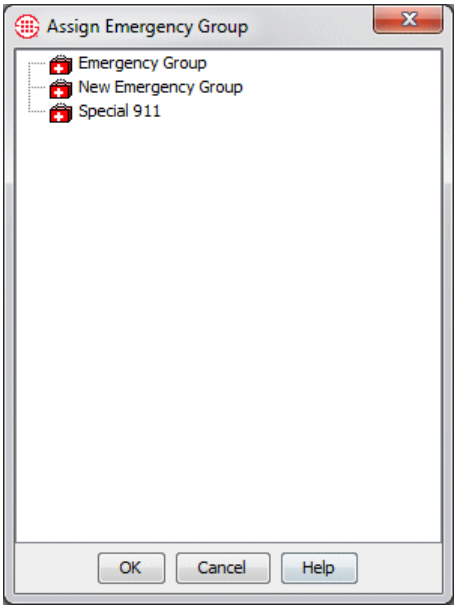
For example, you might have one Span Group in New York City and another in Houston. Because local emergency telephone numbers for New York City are different from those in Houston, you create an Emergency Group for each location and associate it with the Policy that is enforced in that location.

To specify a different Emergency Group

1. In the Directory Manager, define a new Emergency Group. For instructions for defining Emergency Groups, see "Defining Groups" in *ETM® System User Guide*.
2. Open the Policy for which you want to specify a different Emergency Group.
3. Click the **Attributes** tab.



4. Click **Assign Emergency Group**. The **Assign Emergency Groups** dialog box appears with the currently defined Emergency Group(s) listed. (To view the members in an Emergency Group, right-click the Group, and then click **View**.)



5. Double-click the Emergency Group, or click the Emergency Group, and then click **OK**.

   The new group appears in the **Emergency Group** box on the **Attributes** tab and in the **Destination** field of the Emergency Rule in the Policy.

Creating a Span Group

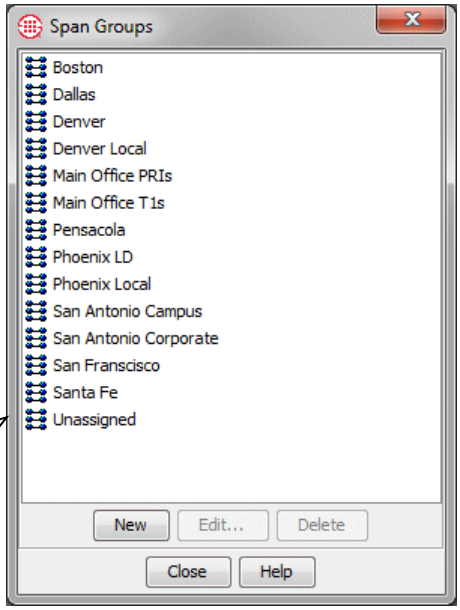
To create a Span Group

1. In the Performance Manager tree pane, right-click **Span Groups**, and then click **Span Group Management**.

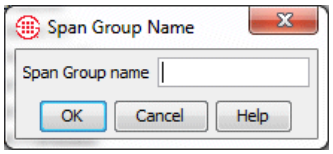
   The **Span Groups** dialog box appears.

Note: You must have **Manage Policies** permission to create or modify Span Groups.

The **Unassigned** Span Group contains all Spans that have not yet been specifically assigned to a Span Group. You cannot install Policies on the **Unassigned** Span Group; the Default Policy is 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**.
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.

Moving a Span to a Span Group

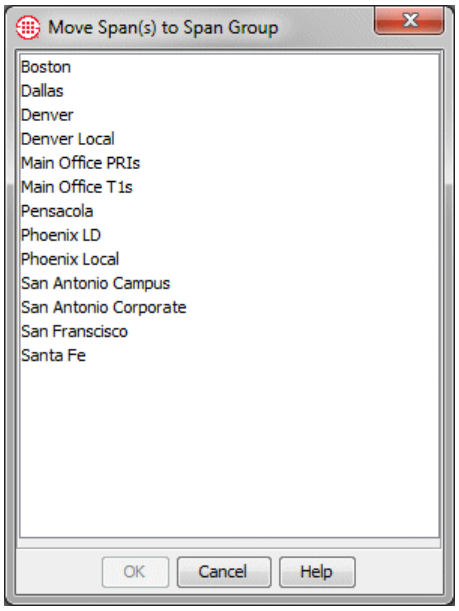
If you add a Span to a Span Group, the Policy installed on that Span Group is enforced by the new Span. It is not necessary to reinstall the Policy. Spans that have not yet been assigned to a Span Group appear under the **Unassigned** node of the **Span Groups** subtree.

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, and then click each Span you want to move to the same Span Group, and then right-click the selection, and then click **Move Span(s)**.
   - Hold down SHIFT, and then click the first and last adjacent Span you want to move, and then right-click the selection, and then click **Move Span(s)**.

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



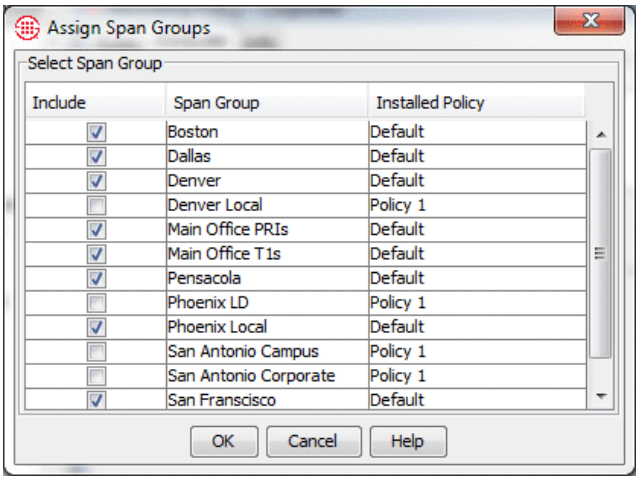
2. Click the Span Group to which you want to move the Span, and then click **OK**.

Assigning a Span Group to a Policy

When you create a new Policy, the **Assign Span Groups** dialog box appears automatically for you to select one or more Span Groups for the Policy. You can also add and remove Span Group assignments from an existing Policy using the **Attributes** tab of the Policy.

To assign a Span Group to a Policy

1. On the **Attributes** tab of the Policy to which you want to assign one or more Span Groups, click **Assign Span Groups**. The **Assign Span Groups** dialog box appears.



2. Check the box(es) of the Span Group(s) that you want to enforce this Policy; clear the check boxes of the Span Groups that you do not want to enforce this Policy.
3. Click **OK**. The Span Group(s) appear in the Span Groups box on the **Attributes** tab.

Saving a Policy

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

- Save your changes before closing the Policy. If you close a newly created Policy without first saving it, the new Policy is not created. A message appears when you attempt to close the Policy if you have unsaved changes.
- New Policies do not appear in the tree pane until they have been saved.
- If you have installed a Policy on a Span Group, and then later make changes and save it, the updated Policy is downloaded to the Span Group; if the Policy is not currently installed, changes are simply saved, not installed.

To save a new or modified Policy

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

Installing a Policy

When you create or make changes to a Policy, you must install it on the Span Group(s) before it takes effect on the Span(s). If the Policy is already installed, updates to the Policy are downloaded when you save changes. If communication between the Management Server and a Span fails when you attempt to install the Policy (for example, if a temporary TCP/IP network outage occurs), the Policy is installed on the Span the next time the Span connects to the Server.

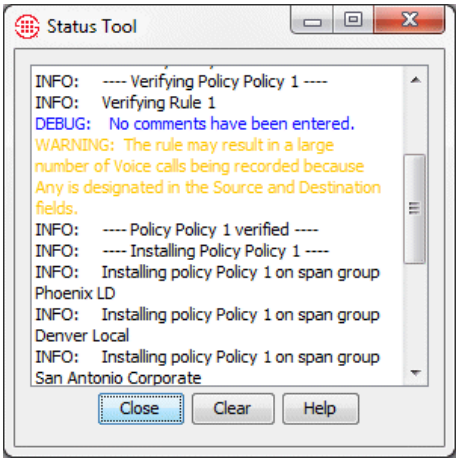
When you move a Span to a Span Group, the Policy currently installed on the Span Group is automatically pushed to the Span. Only one Firewall Policy at a time can be enforced on a Span.

To install a Policy on a Span Group

1. Do one of the following:
   - In the tree pane, right-click the Policy name, and then click **Install**.
   - If you have more than one Policy open, ensure that the Policy that you want to install has the focus. On the Performance Manager main menu, click **Policy | Install**.
2. The Policy is verified, installed on the Span Group(s), and pushed to the Spans.

   The time it takes to install a Policy depends on the number and complexity of the Rules and Directory entities inserted into the Rules.

   When the Policy is being pushed to the Spans, the status of the verification and installation process appears in the **Status Tool**. See "Verifying a Policy" on page 62 for details.



The Policy installation is complete and the asterisk in the title bar of the Policy editor disappears after the message "successfully processed request" appears in the **Status Tool** and "Successfully read and switched to new policy" appears in the **Diagnostic Log**.

Policy Transitions

When a Firewall Policy is installed, it is immediately enforced for new calls. Calls that are in progress when a Policy is installed are only reprocessed against the new Policy if an "execute policy" event occurs, such as the following:

- The call's call type changes. See "Continuous Call Type Detection" on page 21 for more information.
- The new Policy contains a Duration Rule. Duration Rules cause calls to be evaluated against the Policy every 15 seconds until the call reaches the specified duration or the call ends. See "Policy Processing Phases" on page 22 for more information.
- Policy processing was waiting for an Outbound SMDR resolution from the Server. When the SMDR data is received, the call is processed against the new Policy. See "SMDR Data and Policy Enforcement" on page 22 for more information.

Uninstalling a Policy

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

Note: Uninstalling a Policy from a Span Group does not delete the Policy from the ETM® Database. See "Deleting a Policy" on page 61.

To uninstall a Policy

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

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

2. Click **Yes** to continue.

Printing a Policy

You can print copies of your Policies to store in a binder or to share in meetings or presentations.

To print a Policy

1. Open the Policy. If you have more than one Policy open, ensure that the Policy that you want to print has the focus.
2. Click **File | Print**, and then select the format:
   - **Print Summary** prints the Policy as it is displayed in the Performance Manager Policy pane, with a summary that includes:
     - Policy ID (generated by the application).
     - Date and time the Policy was created.

- User name of the creator.
- Date and time the Policy was last updated (saved).
- User name of the person who last updated (saved) the Policy.

- **Print Details** prints the same information as **Print Summary**, plus:
  - Time Groups used in the Policy.
  - Tracks used in the Policy.
  - Span Group(s) on which the Policy is installed.

The **Print** dialog box appears.

3. Select a printer, and then click **OK**. If you have adobe Acrobat Distiller or PDF Maker installed on the computer, you can save the Policy in PDF format by choosing the Adobe product as the printer.

Creating a New Policy from Another Policy

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

To create a new Policy based on another Policy

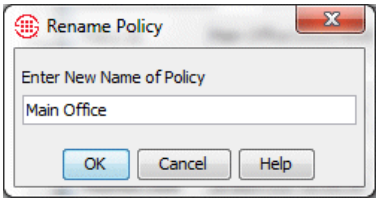
1. In the tree pane, double-click the Policy on which you want to base the new Policy. The Policy appears in the Policy editor pane.
2. On the Performance Manager main menu, click **File | Save As**. The **New Policy** dialog box appears.
3. Type the name for the new Policy, and then click **OK**. The new Policy appears in the Policy editor pane and in the tree pane.
4. In the Policy, make modifications to the Rules as needed, and then click **File | Save**.

   If you want to assign different Span Groups to the Policy, use the procedure in "Assigning a Span Group to a Policy" on page 68.

Renaming a Policy

To rename a Policy

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



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

Viewing Multiple Policies

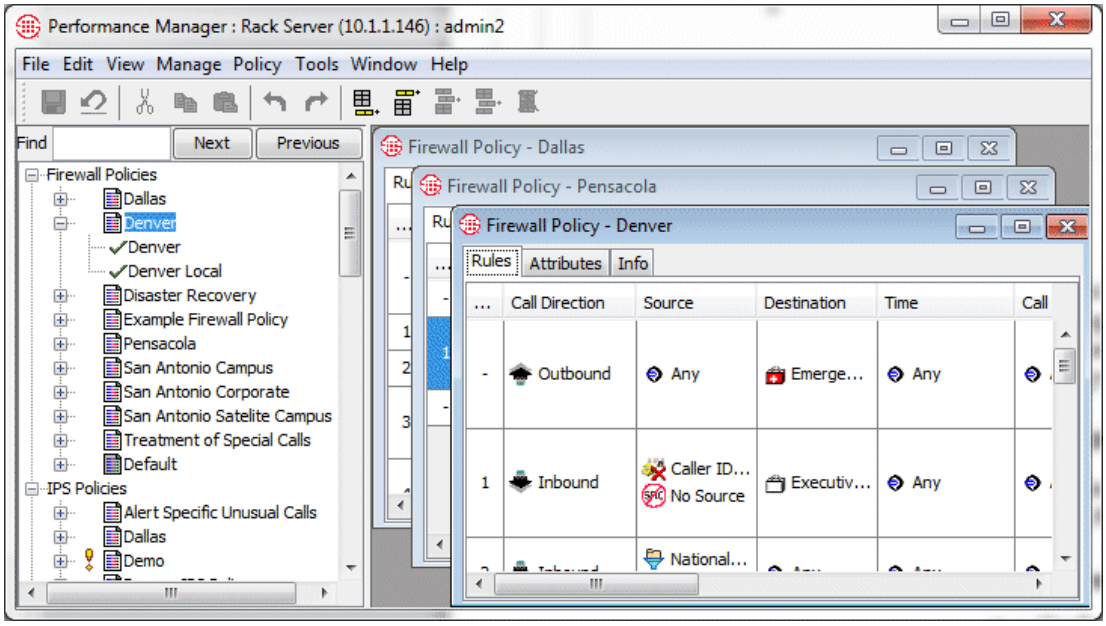
When you have multiple Policies open for editing, you can switch between them using the **Window** menu on the Performance Manager menu, or display them all at once tiled in horizontal or vertical windows or both, or in cascading windows.

To switch between open Policies

- On the Performance Manager main menu, click **Window**, and then click the Policy name.

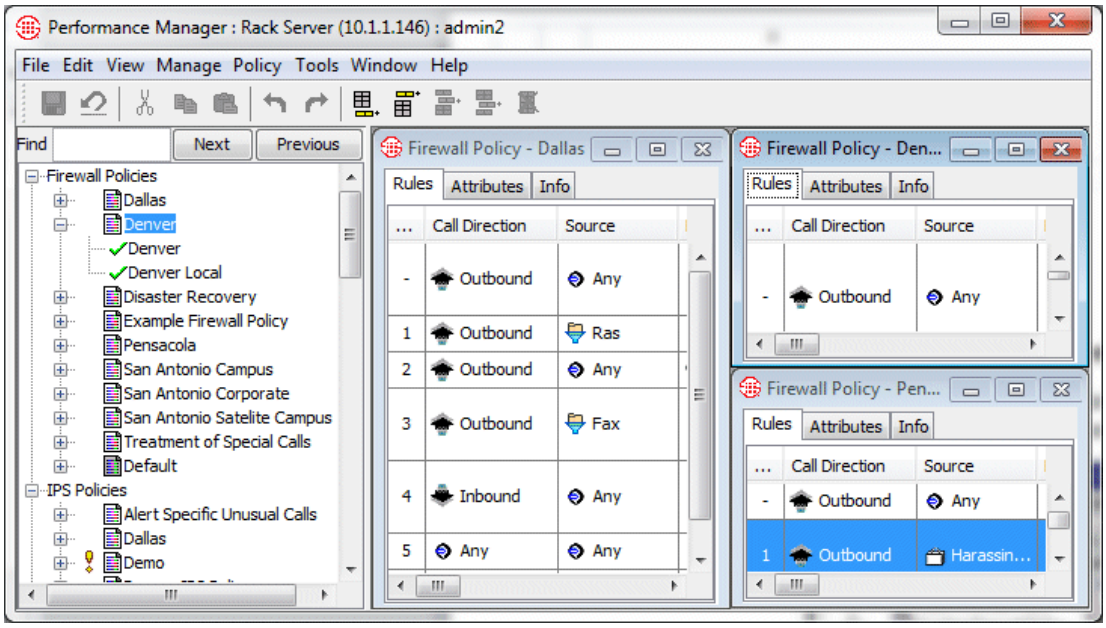
To view multiple open Policies in cascading windows

- On the Performance Manager main menu, click **Window | Cascade**.



To view multiple Polices in tiled windows

- On the Performance Manager main menu, click **Window | Tile**, and then select **Horizontal**, **Vertical**, or **Both**. **Both** is illustrated below.



Managing Rules

This section provides procedures for managing Rules in a Policy, including:

- Modifying or deleting items contained in Rules
- Hiding Rules
- Disabling Rules
- Cutting, copying, and pasting Rules
- Deleting Rules
- Viewing Directory Listings, Groups, Ranges, and Wildcards in a Rule

Modifying or Deleting Items Contained in Rules

If you modify an item that is contained in an installed Policy, the change does not take effect on the Spans unless you reinstall the Policy. For example, if you have specified an **Email** Track in an installed Policy, and then later change the email address of the **Contact** specified in the **Email** Track, you must reinstall the Policy.

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

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

Removing an Item From a Rule

To remove an item from a Rule

- Do one of the following:
  - If the field contains more than one item, and you are removing only one of the items, right-click the item, and then click **Remove**.
  - If the field contains only one item or you want to remove all items, right-click the field, and then click **Any** or **None** (depending on the field).

Hiding Rules

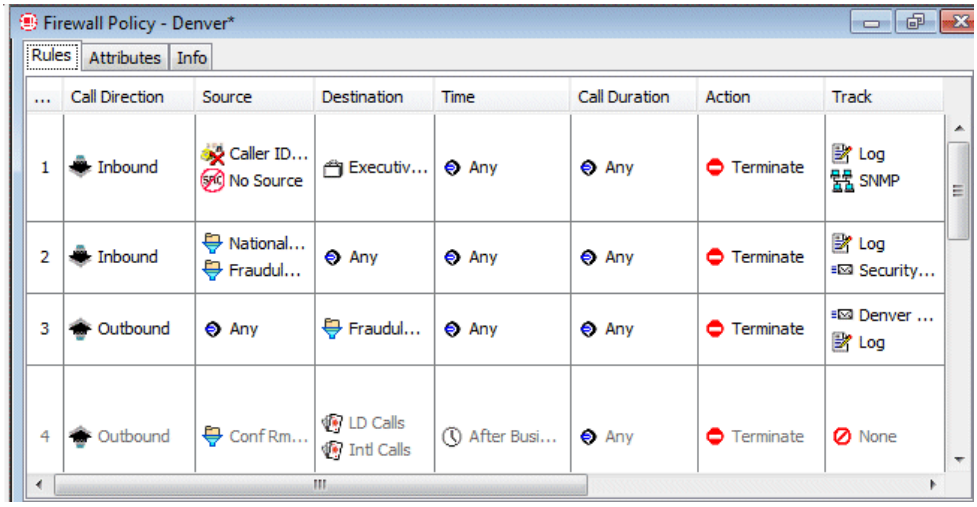
If you have numerous Rules, but prefer to only see a few of them, you can hide them. Hidden Rules are still enforced; if you do not want the Rule to be enforced, you can disable it or delete it. See "Disabling Rules" on page 74 and "Deleting Rules" on page 76.

To hide/show a Rule

- Right-click the Rule you want to hide, and then click **Hide Rule**.
- Click the Rule you want to hide, and then, on the Performance Manager main menu, click **View | Hide Rule**.
- To show a hidden Rule, on the Performance Manager main menu, click **View | Show Hidden Rules**.

Disabling Rules

Disabling is useful if you do not want the Rule to fire, yet you do not want to permanently delete it. Disabling is not the same as hiding a Rule—hidden Rules are still enforced, while disabled Rules are not. You can easily reinstate the Rule by enabling it. A disabled Rule appears dimmed in the **Policy Editor**. In the illustration below, Rule 4 is disabled.



To disable/enable a Rule

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

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

Cutting, Copying, and Pasting, Rules

To cut and paste or copy and paste a Rule

1. Open the Policy from which to cut or copy the Rule, and, if different, the Policy into which you will paste the Rule.
2. Highlight the Rule you want to move/copy.
3. Do one of the following:
   - To remove the Rule from its current location and transfer it to a new location, on the main menu, click **Edit | Cut**.
   - To create a duplicate of the Rule in a new location, click **Edit | Copy**.

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

4. Ensure that the Policy into which you want to paste the Rule has the focus, if different, and then do one of the following:
   - To paste the Rule at the bottom of the Policy, click **Edit | Paste | Bottom**.
   - To paste the Rule at the top of the Policy, click **Edit | Paste | Top**.
   - To paste the Rule after the selected Rule, click the Rule, and then click **Edit | Paste | After**.
   - To paste the Rule before the selected Rule, click the Rule, and then click **Edit | Paste | Before**.

Deleting Rules

To delete a Rule

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

See also "Hiding Rules" on page 74 and "Disabling Rules" on page 74.

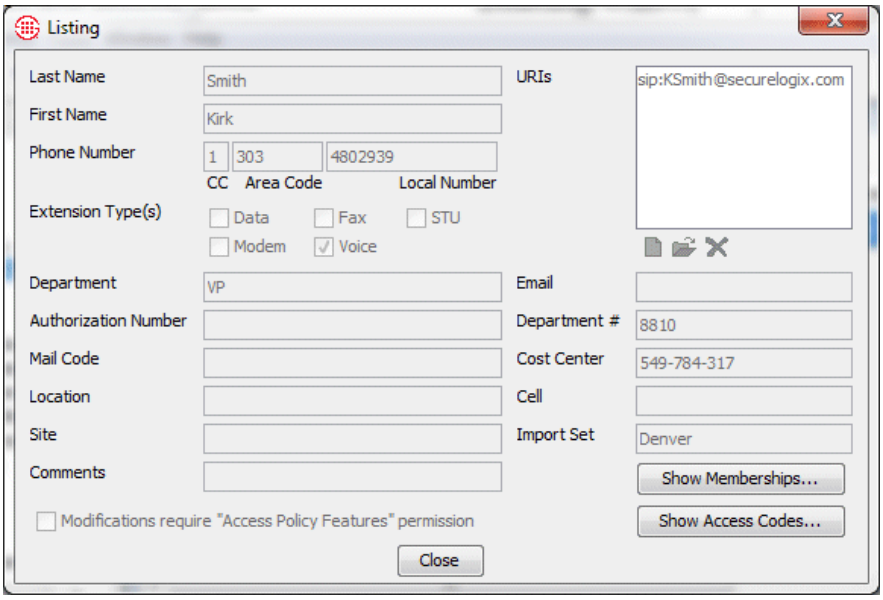
Viewing Contents of Directory Entities in Rules

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

Viewing Directory Listings in a Rule

To view a Directory Listing in a Rule

- Right-click the Directory Listing in the **Source** or **Destination** field, and then click **View**. The Listing dialog box appears showing the contents of the Listing.



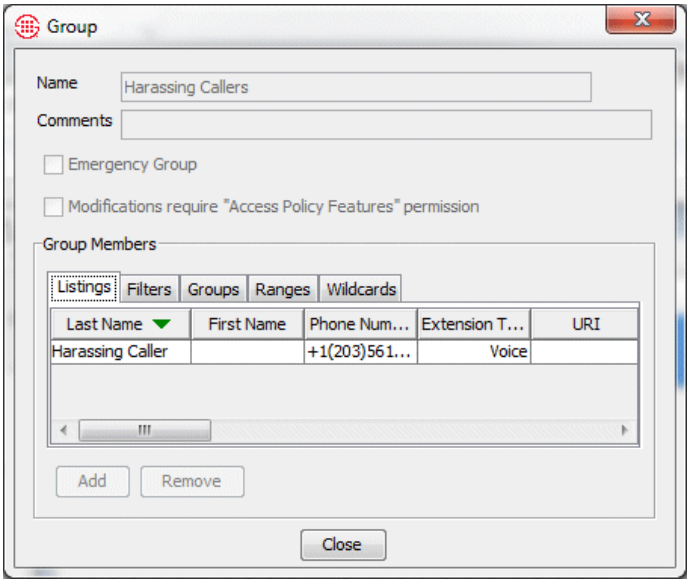
You cannot edit Directory Listings in the Policy; they are only editable in the Directory Manager. See "Viewing or Editing Directory Listings" in the *ETM® System User Guide* for details.

Viewing Contents of a Directory Group in a Rule

You can view the contents of a Directory Group in a Rule, but you cannot edit it. See "Directory Groups" in the *ETM® System User Guide* for instructions for creating and editing Directory Groups.

To view the contents of a Directory Group in a Rule

1. Right-click the Group in the **Source** or **Destination** field of a Rule, and then click **View**.



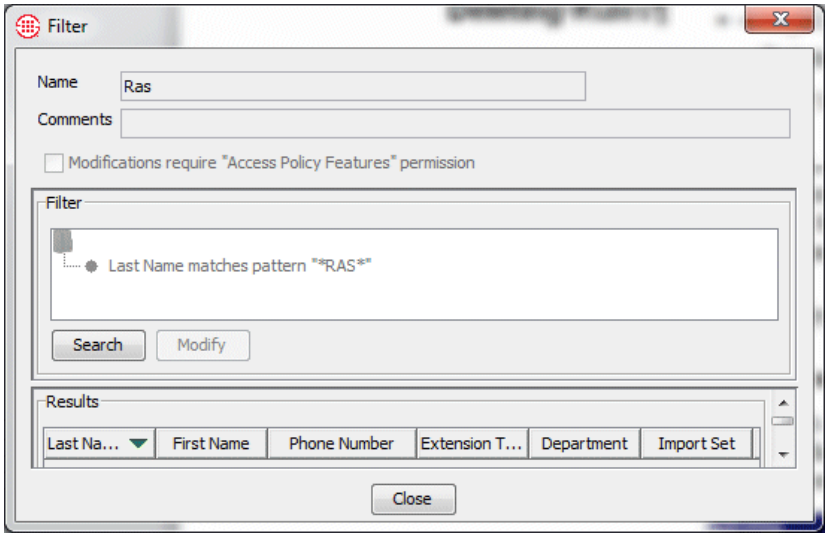
2. To view the Listings, Filters, Groups, Ranges, or Wildcards in the Group, click the **Listings**, **Filters**, **Groups**, **Ranges**, or **Wildcards** tab.

Viewing Contents of a Directory Filter in a Rule

You can view the contents of a Directory Filter in a Rule, but you cannot edit it. See "Directory Filters" in the *ETM® System User Guide* for instructions for modifying Directory Filters.

To view the contents of a Directory Filter in a Rule

1. Right-click the Filter in the Source or Destination Field of a Rule, and then click **View**.
2. To see the Listings that match the Filter, click **Search**.

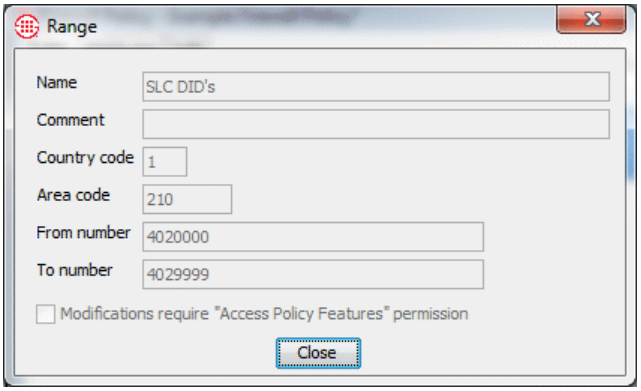


Viewing Contents of a Directory Range in a Rule

You can view the contents of a Directory Range in a Rule, but you cannot edit it. See "Directory Ranges" in the *ETM® System User Guide* for instructions for modifying Directory Ranges.

To view the contents of a Directory Range in a Rule

- Right-click the Range in the **Source** or **Destination** field of a Rule, and then click **View**.



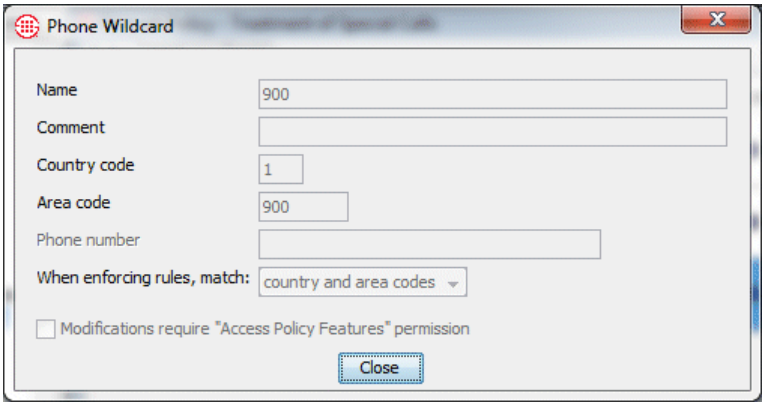
The **Range** dialog box appears showing the contents of the Range.

Viewing Contents of a Directory Wildcard in a Rule

You can view the contents of a Directory Wildcard in a Rule, but you cannot edit it. See "Directory Wildcards" in the *ETM® System User Guide* for instructions for modifying Directory Wildcards.

To view the contents of a Directory Wildcard in a Rule

- Right-click the Wildcard in the **Source** or **Destination** field of a Rule, and then click **View**.



The **Wildcard** dialog box appears showing the contents of the Wildcard.

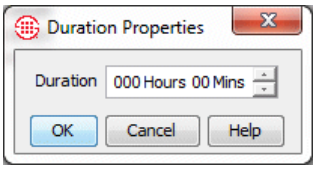
Durations

Durations are used to apply Policy Rules based on the length of the call.

Defining a Duration

To define a Duration

1. Right-click in the **Duration** field of a Policy Rule. The **Durations** dialog box appears.
2. Right-click in the **Durations** dialog box, and then click **New Duration**. The **Duration Properties** dialog box appears.



3. In the **Duration** box, type or click the up and down arrows to specify the hours and/or minutes of the Duration, and then click **OK**.

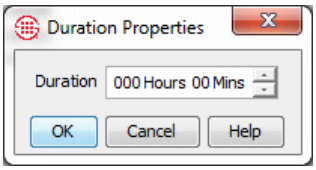
   The new Duration appears in the **Durations** dialog box.
4. Click **OK** to add it to the Rule.

Editing a Duration

To edit a Duration

Do one of the following:

- To edit a Duration in a Rule
  a. Right-click the Duration and click **Edit**. The **Duration Properties** dialog box appears.
  b. Make changes, and then click **OK**.
- To edit a Duration in the **Durations** dialog box prior to adding it to a Rule:
  a. Right-click in the **Duration** field of a Policy Rule. The **Durations** dialog box appears.
  b. In the **Durations** dialog box, right-click the Duration that you want to edit, and then click **Edit**. The **Duration Properties** dialog box appears.



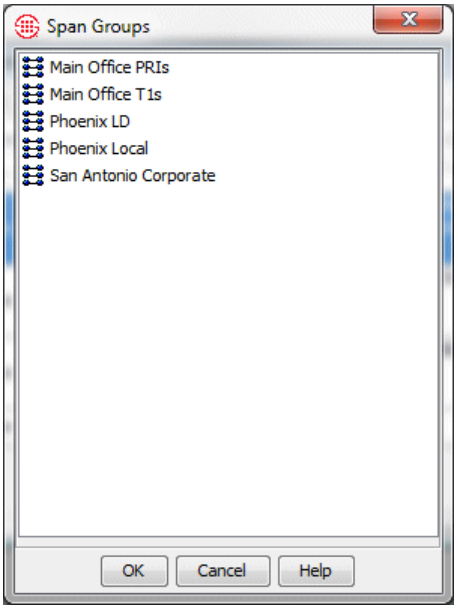
  c. In the **Duration** box, edit the hours and/or minutes of the Duration, and then click **OK**.
  d. Click **OK** in the **Durations** dialog box to close the dialog box and add the Duration to the Rule.

Specifying Span Groups to Enforce a Rule

The **Span Groups** dialog box is used to add one or more Span Groups assigned to the Policy to the **Install On** field of a Rule. You cannot define or edit Span Groups in this dialog box. For details about how to define Span Groups, see "Creating a Span Group" on page 65. When you use the **Install On** field in a Rule, that Rule is installed on only the Span Group(s) you specify in the **Install On** field. You can use both Rules with **Install On** specified and Rules without in the same Policy. Rules that do not specify specific Span Groups are installed on all Span Groups assigned to the Policy.

To specify a Span Group to enforce a Rule

1. Right-click the **Install On** field of a Rule, and then click **Add**.



Only the Span Groups assigned to the Policy appear in the **Span Groups** dialog box.

2. Click one or more Span Groups that you want to add to the Rule, and then click **OK**. To select multiple Span Groups, hold down CTRL or SHIFT while clicking.

Viewing Policy Enforcement Results

Monitoring Policy Enforcement

The ETM® System provides the following tools for viewing Firewall Policy enforcement in real time and in logs and reports:

Tool	Description
Policy Log	Displays a list of calls that triggered a tracked Firewall Policy Rule. A Rule with a **Track** setting other than **None** generates an entry when a call matches the Rule.
Call Monitor	Provides a real-time display of calls monitored by the ETM System.
Call Log	Provides a log of all monitored calls per Span Group. If the call triggered a tracked Firewall Rule, information about the fired Rule is included.
Alert Tool	Displays a list of alerts generated due to enforcement of Policies. Each Rule with **Real-Time Alert** in the **Track** field generates an entry when a call matches a Rule
Diagnostic Log	Displays system events concerning ETM System operation and certain telco events. See "The Diagnostic Log" in the *ETM® System User Guide* for details.
Usage Manager	Provides numerous predefined Reports with which you can view Policy enforcement results. You can also define custom reports. See "Quick Start with Reports" in the *Usage Manager User Guide* for details.

You can apply filters to the columns in the **Policy Log**, **Call Log**, **Call Monitor**, **Diagnostic Log**, and Usage Manager Reports so that only the information of interest to you is displayed. When a filter is applied to a column, the column heading appears in red text. See "Filters" in the *ETM® System User Guide* for instructions for applying filters.

The Policy Log

The **Policy Log** is used to view recent results of Policy processing. All calls monitored by the ETM System are logged. When a call triggers a Rule that has the Track setting of **Log**, the call record is appended with the Track data and the call is viewable in the **Policy Log**.

The data in the **Policy Log** is retrieved from the Active area of the ETM 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 Log

To open the Policy Log

- In the tree pane, right-click the Policy name, and then click **View Policy Logs**.

  The **Policy Log** appears and displays calls that triggered Rules with any Track. Columns can be arranged in any order you specify and you can select which columns to hide or show. See "Showing, Hiding, or Rearranging the Columns in the Policy Log" on page 88 for instructions.

Data Displayed in the Policy Log

The table below describes the Firewall Policy-related information that is displayed in each column of the **Policy Log**.

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 a Rule, blank if no Rule was matched. 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 call passed that fired Rule.
Bytes-Inbound	On VoIP calls, the number of inbound payload bytes transmitted.
Bytes-Outbound	On VoIP calls, the number of outbound payload bytes transmitted.
Call Details	Call classification information (i.e., local, long distance, toll-free). See "Call Classification Labels" in the *ETM® System Technical Reference* for descriptions of the labels.
Call ID	Unique key that is assigned by the Span to every call. (Do not confuse with Caller ID.)
Caller ID	Caller ID information and error messages.

Data Displayed in the Policy Log, continued

Column Heading	Information Displayed
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 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" in the *ETM® System Technical Reference* for descriptions of the labels.
Destination IP	On VoIP calls, the IP address of the callee.
Duration	The amount of time elapsed since Start Time (when the line was seized).
End Time	End date and time of the call (typically the same as Log Time).
Egress Trunk	The outbound trunk.
Egress Channel	The outbound channel.
Firewall Comment	Comments associated with the Firewall Policy Rule that fired (or **Ambiguous** if the call was ambiguous with respect to the Rule).
Firewall Policy	Name of the Firewall Policy containing the Rule.
Firewall Policy ID	System-generated Policy ID number.
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) triggered by the Firewall Policy.
In/Out	Whether the Rule was applied to an inbound or outbound call.
Log Time	Date and time an entry was made in the log.
Ingress Trunk	The inbound trunk.
Ingress Channel	The inbound channel.
Prefix	Digits dialed before the phone number, such as outside access number or long distance access code.
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	Calling party's Access Code pulled from SMDR data; this field only appears if you have the **View Access Codes** user permission.

Data Displayed in the Policy Log, continued

Column Heading	Information Displayed
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 *ETM® System Technical Reference* for descriptions of the labels.
Source IP	On VoIP calls, the IP address of the caller.
Span	Name of the Span that executed the Rule.
Span #	Number of the Span executing the Rule.
Span Group	Name of the Span Group on which this Policy is installed.
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.
Switch	Name of the Switch through which the call passed that fired Rule.
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.
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.

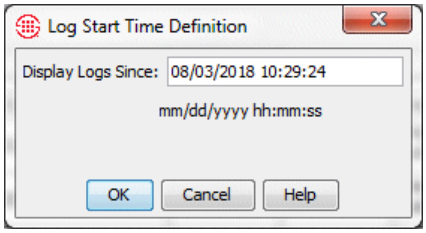
Setting the Start Time of the Policy Log

To retrieve log data for more time than the defined **Log Retrieval Amount** in the current instance, you can set the log start date and time. 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 Performance Manager's **Properties** dialog box. See "Setting Display Preferences for the Policy Log" on page 87 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 **Edit | 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 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 **Policy Log**, and then reopen it.

Call Classification Labels

Note: Labels are user-definable in the Dialing Plans. See "Defining Dialing Plan Sections" in the *ETM® System Technical Reference* for instructions for configuring Dialing Plans.

In the **Policy Log**, the **Call Details** field shows call classification labels for calls that trigger Rules. Call labels are user-definable in the Dialing Plans. Call labels classify the call as a whole as follows:

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

See "Call Classification Labels in Reports" in the *Usage Manager User Guide* for a list and description of the labels.

Phone Number Classification Labels

The phone number label for the calling number appears in the **Source Details** field of the **Policy Log**. The phone number label for the called number appears in the **Destination Details** field of the **Policy Log**.

See "Phone Number Labels" in the *Usage Manager User Guide* for a list and description of the labels.

Caller ID Messages

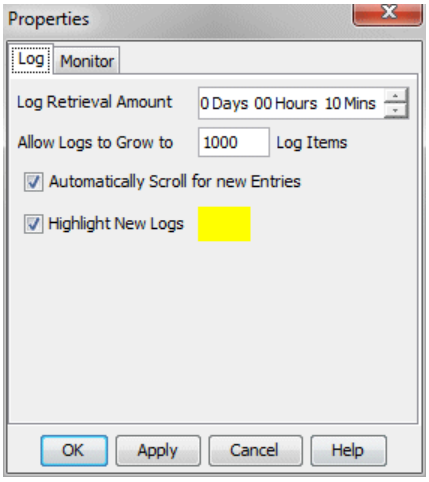
The **Caller ID** column of the **Policy Log** shows information and errors related to Caller ID. See "Caller ID Messages" in the *Usage Manager User Guide* for a list and description of the labels.

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 **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, or 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.

To organize columns displayed

1. In the **Policy Log**, click **Column | Set Displayed**. 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**.

Note: You can also drag and drop the columns in the **Policy Log** to arrange them.

Displaying Name or Number

You can choose whether to display the Caller ID name or the phone number in the **Source** and **Destination** columns of the **Policy Log**. Each column can be set independently.

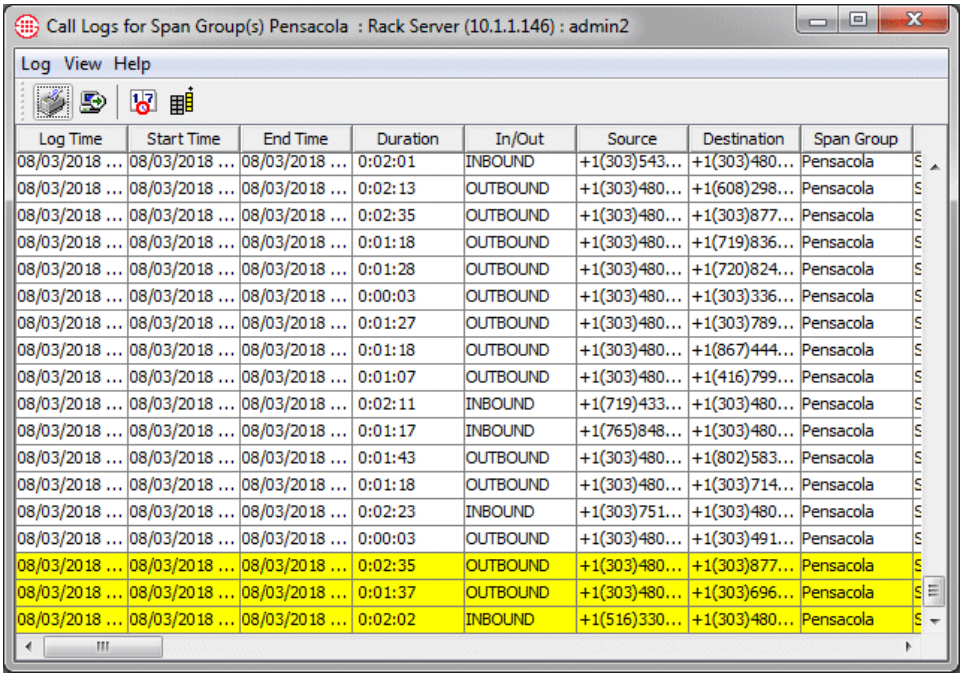
To specify Caller ID, Name, or Phone Number

- Right-click the **Source** or **Destination** column heading, point your cursor to **Display**, and then click **Show Name** or **Show Number**.

Viewing the Call Logs for a Span Group

The **Call Log** provides details about each call monitored by a given Span Group, regardless of whether the call triggered any Rule in any Policy. If the call triggered a Firewall Policy Rule, that information is also included for the call.

You can also view the **Call Log** for multiple Span Groups at once.



To view the Call Log

1. In the Performance Manager tree pane, expand the **Span Groups** subtree.
2. Right-click a Span Group, and then 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 then click **View Call Logs**.

Viewing Calls on Channels in Real Time

The **Call Monitor** provides a real-time display of call activity on monitored channels for the Management Server that you are logged in to. You can view calls for each channel as they pass through the Switch, Appliance, Card, or Span. The Management Server continually transfers all call state changes to the display. To prevent unnecessary use of system and network resources, close the **Call Monitor** when you are not actively using it.

You can customize the **Call Monitor** to view only certain call information. Note that these settings are specific to the user account:

- Entries are displayed in the **Call Monitor** in colored text to give you a quick visual indication of channel and call status. In the **Properties** dialog box, you can set color preferences for each type of call, the display update interval, and the length of time that an ended call is displayed.

- You can customize the display to view all data for all calls, or show only certain columns, specific call types, and/or calls containing specific types of data, such as those within a certain period, or from or to a specific phone number.

  For instructions for setting display preferences for the **Call Monitor**, see "Setting **Call Monitor** Display Preferences" in the *ETM® System User Guide*.

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	23	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		

Opening the Call Monitor

To open the Call Monitor

- In the Performance Manager tree pane, right-click a Switch, Appliance, Card, or Span, and then click **Call Monitor**.
  - To view calls on multiple individual Appliances, Cards, or Spans, hold down CTRL, and then click like items, and then right-click the selection, and then click **Call Monitor**.
  - All channels are displayed by default. To view only active channels, click **View | Fixed Row Counts**. The selection acts as a toggle to display all channels or only active channels. A check mark indicates that fixed row counts are shown; no check mark indicates that only active channels are shown.

Viewing Real-Time Alerts

You can configure the Management Server to generate real-time alerts in response to specific telco, system, or Policy events. These alerts are viewed in the **Alert Tool**. Alerts for all of the Management Servers to which the ETM® Console is currently connected are consolidated in a single **Alert Tool**, enabling you to simultaneously monitor tracked events across the enterprise, regardless of the Server you are currently viewing. The **Alert Tool** displays the following information for each Alert:

- **Time Stamp**—The date and time an Alert was generated.

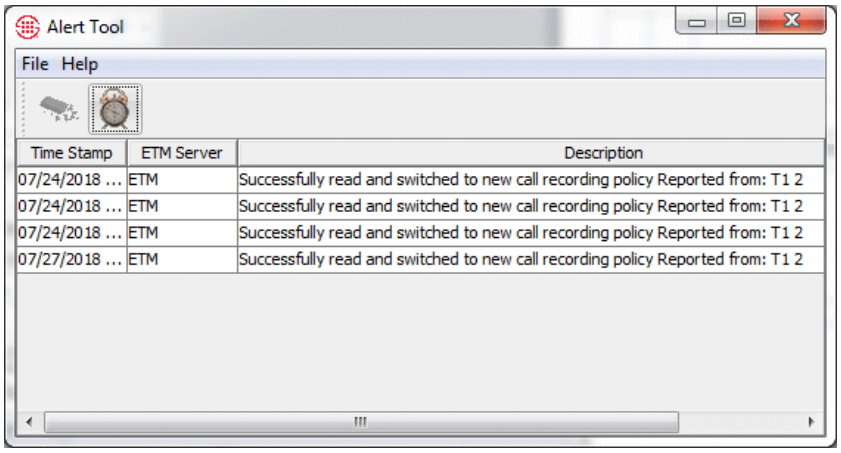
- **Server**—The ETM Management Server from which the Alert originated.
- **Description**—A description of the cause of the Alert.

You can configure the **Alert Tool** to appear and/or beep each time a real-time alert occurs. For information about defining **Alert Tool** preferences, see "Alert Tool" in the *ETM® System User Guide*.

Opening the Alert Tool

To open the Alert Tool

- On the ETM® Console main menu, click **Tools | Alerts**.



System Events Related to Policies

The ETM System can generate system events related to installing and processing Policies. System events are managed per Management Server. Events appear in the **Diagnostic Log** for that Server and the **Alert Tool** if **Real-Time Alert** Tracks are specified.

System events associated with Policies include:

- **Dial Plan Read Fail**—Error in reading the Dialing Plan on the specified Span, which prevents Policy processing**.**
- **Dirty Policies Found After Automatic Directory Import**—One or more Dirty Policies have been detected following an LDAP Directory import.
- **New Policy**—A new Policy was installed on the specified Span.
- **Policy Read Fail**—Error reading a newly installed Policy due to file corruption.

You can track specific types of system events by assigning one or more Tracks to cause follow-up actions, such as notification or logging, that result each time that type of system event occurs.

For information about assigning Tracks to system events, see "Setting Track Actions for System Events" in the *ETM® System Administration and Maintenance Guide*.

Viewing Policy Enforcement in Reports

You can also generate Usage Manager Reports of Policy enforcement. The Usage Manager provides a number of predefined Reports with which you can quickly and easily generate detailed or summary reports of Policy enforcement. You can also define your own custom reports.

For details about the Usage Manager, see the ETM System online Help, the *Usage Manager User Guide*, or the online E-Learning- course.

Appendix: Span Settings Related to Firewall Policy Processing

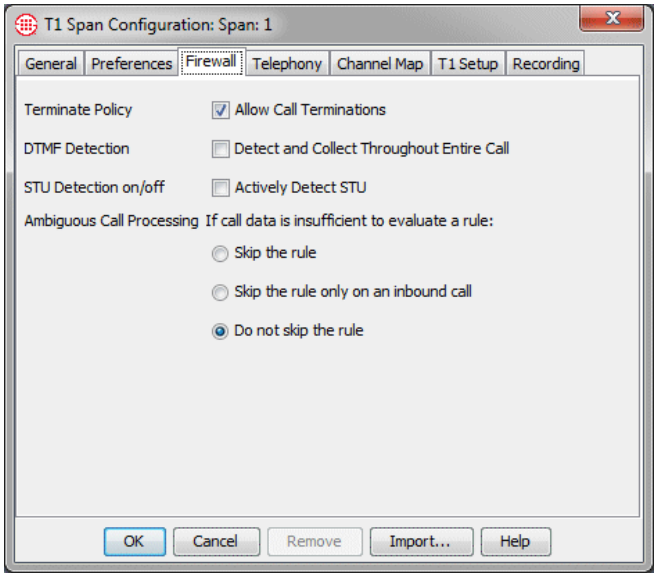
Called/Calling Numbers and Firewall Policy Enforcement

Note: The sections below describe Span settings that relate to Policy processing. For information about configuring Spans, see "Configuring Spans" in the *ETM® System Installation Guide*.

A variety of methods exist by which source (calling) and destination (called) numbers are encoded by the telephone company during call establishment, and subsequently how these numbers are recognized by the ETM® System and used for Policy enforcement. Numbers are encoded not only to indicate the source and destination, but also to provide an identification number used for special routing or information services by the PBX. For example, DNIS (Dialed Number Identification Service) lines may provide a number that identifies the service the caller wants to access.

Firewall Settings for Call Processing

The **Firewall** tab of the **Span Configuration** dialog box is used to configure the way the Span processes calls against Firewall and IPS Policies. The following illustration shows the Firewall tab for a T1 Span.



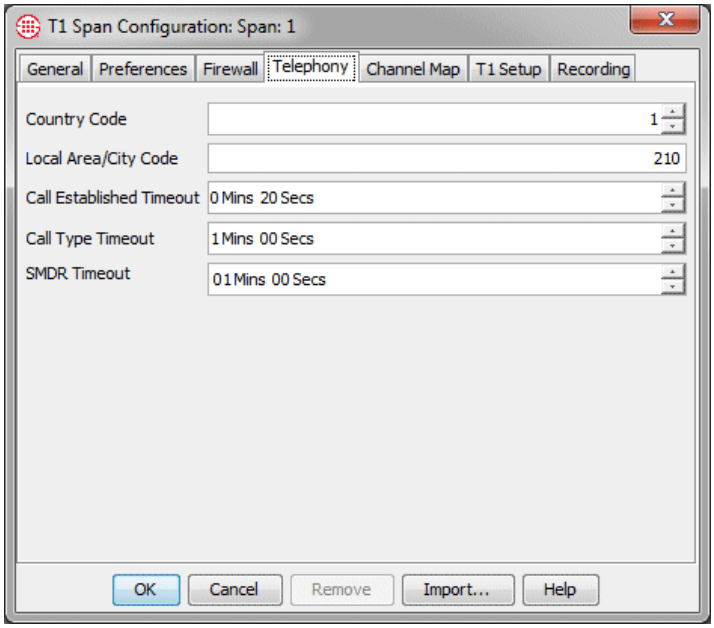
Settings on this tab differ for UTA and SIP Spans, as identified in the table below..

The following table describes the settings on the **Firewall** tab that affect Policy processing.

Setting	Use
Terminate Policy	The **Terminate Policy** setting determines whether the Span can terminate calls. **Allow Call Terminations** must be selected in the **Span Configuration** dialog box for the Span to enforce terminate Rules in Policies. If **Allow Call Terminations** is not selected, no calls can be terminated on the Span, regardless of user permission or the setting in the **Action** field of the Rule.
DTMF Detection	The **DTMF Detection** setting applies to all calls on all channels, since DTMF digits are passed once the call is established, even if MF digits are used for signaling. Select the **Detect and Collect Throughout Entire Call** check box to capture all DTMF digits throughout the duration of the call; clear the check box to capture only digits pertaining to call establishment. Note that DTMF digit patterns can be used in Policies without selecting this option to store them in the database.
STU Detection	(*Not on SIP or UTA Spans*) The STU detection preference indicates whether STUs are in use on this Span and should be actively detected. If this is not selected, STUs are treated as modems.
Ambiguous Calls Processing	(*Not on SIP or UTA Spans*) When a call is compared to a Rule that specifies source or destination and that value is unavailable for the call, the call is deemed ambiguous. Since the source or destination is unknown, it cannot be determined whether the call matches the Rule. The Ambiguous Call Processing setting determines how such calls are processed: **Skip the Rule**—If insufficient phone number information is available to evaluate a call against a particular Rule, the Rule is skipped, and processing continues with the next Rule. **Skip the Rule only on an inbound call**—If insufficient phone number information is available to evaluate a particular inbound call, the Rule is skipped, and processing continues with the next Rule in the Policy. On outbound calls, processing stops; when SMDR data becomes available after the call is completed, the stored call data is again processed against the Policy; if a Rule fires, any applicable Tracks are executed, such as logging or sending an email. **Do not skip the Rule**—If insufficient phone number information is available to evaluate the call, the Policy stops executing and no Tracks (except logging) are executed. On outbound calls, when SMDR data becomes available after the call is completed, the stored call data is again processed against the Policy; if a Rule fires, any applicable Tracks are executed, such as logging or sending an email.

Telephony Settings Related to Firewall Policies

The Span's telephony settings are configured on the **Telephony** tab of the **Span Configuration** dialog box during installation. The following illustration shows the Telephony tab for a T1 Span. Settings vary on SIP and UTA, as identified in the table below.



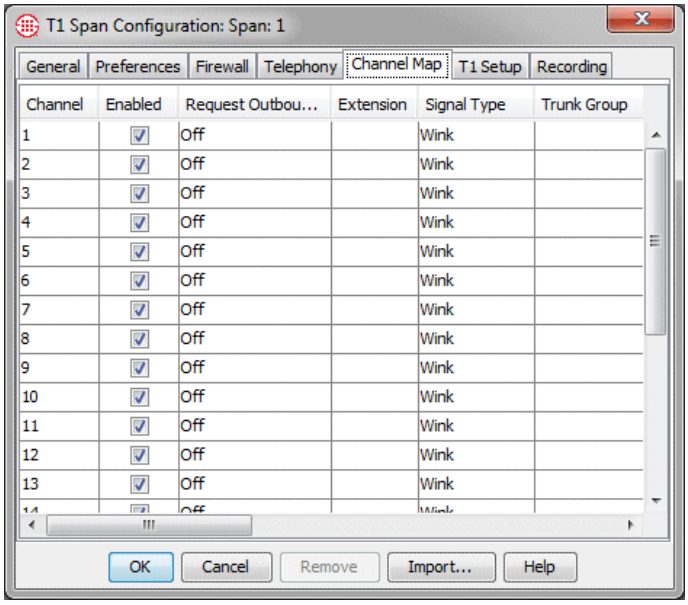
The following table describes the settings on the **Telephony** tab.

Setting	Use
Country Code	Specifies the dialing access code of the country in which the Span is physically located.
Local Area/City Code	Specifies the area code in which the Span is physically located.
Call Established Timeout	(*Not on SIP*) Specifies the time after the last digit is dialed before a call is marked as established.
Call Type Timeout	(*Not on SIP*) Specifies the length of time the Span waits after a call is established before first classifying a silent or indistinguishable call as Voice. Call Type Timeout applies only to calls where lack of activity on the line prevents the Span from determining the call type. Setting this value too low can cause an excessive number of call type changes from voice to another type, which may affect the way in which Rules fire.
SMDR Timeout Period	(*Not on SIP*) Specifies the length of time that the Span waits for an SMDR result from the Management Server after the query is generated. If the timeout value is set too low, the Span may not receive SMDR for Policy processing.

Caller ID Restricted Identifiers	(*Not on TDM*) On SUP and UTA, identifies the URI strings that are to be considered to indicate a caller-ID restricted call, such as “private@” or “anonymous@”

The Channel Map

(*Not on SIP or UTA Spans*) The **Channel Map** tab of the **Span Configuration** dialog box contains telecom settings (configured during installation) that must be correctly defined to enable the Span to monitor call traffic and enforce Policies. See the *ETM® System Installation Guide* for details about these settings.



Determining Calling/Called Numbers by Span Type

Accurately determining calling/called numbers is important for enforcement of Policies. The following table describes how TDM Spans determine calling/called numbers to use for Policy enforcement, based on settings on the **Channel Map** tab of the **Span Configuration** dialog box. VoIP Spans have no **Channel Map** tab. For VoIP calls, the called/calling numbers are available on the line and used for Policy processing.

When multiple means are available, they are listed in the table in the order of preference.

For example, to determine the called number on an inbound call, T1 CAS Spans use the following:

1. ADDR, DID, or DNIS, depending on the **Format Precedence** setting, as determined by **Incoming Number Format**.
2. If none of those is available, the Span uses the number in the **Extension** column of the **Channel Map**.

3. Finally, if numbers were not entered in the **Extension** column, the calling/called number is unavailable.

Determining Calling/Called Numbers by Span Type

Call Direction	**Analog Loop Start/ Ground Start**	**Analog DID**	**T1 CAS/ E1 CAS**	**T1 PRI/ E1 PRI/ T1 SS7**
Calling number on **outbound** calls (outbound source)	If **Request SMDR** is **On**, **Augment,** or **Replace**, uses the extension number in SMDR data only, or the source is not available. If **Request SMDR** is **Off**, source is not available.	Unavailable	If **Request SMDR** is **On**, uses the extension number in SMDR data only, or the source is not available. If **Request SMDR** is **Augment** or **Replace**, uses the extension number in SMDR data; uses ANI, if available; ;otherwise, source is not available. If **Request SMDR** is **Off**, uses ANI, if available; uses the number in the **Extension** column; otherwise, source is not available.	If **Request SMDR** is **On**, uses the extension number in SMDR data only, or the source is not available. If **Request SMDR** is **Augment** or **Replace**, uses CPN, if available; uses SMDR if CPN unavailable; otherwise, source is not available. If **Request SMDR** is **Off**, uses the CPN; PRI uses the number in the **Extension** column (*not on SS7*); otherwise, source is not available.
Called number on **outbound** calls (outbound destination)	Uses ADDR.	Unavailable	Uses ADDR	Uses CPN.

Determining Calling/Called Numbers by Span Type, continued

Call Direction	Analog Loop Start/ Ground Start	Analog DID	T1 CAS/ E1 CAS	T1 PRI/ E1 PRI/ T1 SS7
Calling number on an **inbound** call (inbound source)	Uses Caller ID, if Caller ID is available; otherwise, the calling number is not available.	The calling number is not available.	Uses ANI; uses Caller ID if Caller ID is available on the line and the box is checked; otherwise, the calling number is unavailable.	Uses Calling Party Number (CPN), if available; otherwise, the calling number is not available.
Called number on an **inbound** call (inbound destination)	Uses the number in the **Extension** column; otherwise, the called number is not available.	Uses DID	Uses ADDR, DID, or DNIS, depending on **Format Precedence** setting, as determined by **Incoming Number Format**; uses the number in the **Extension** column; otherwise, the called number is unavailable.	Uses CPN, if available; otherwise, the called number is not available.

Dialing Plans and Policy Enforcement

Spans use Dialing Plans to process calls against Rules. The Dialing Plan provides necessary information that the Span uses to recognize, normalize, and classify various types of telephone numbers. The Dialing Plans for your environment were configured during system installation. See "Dialing Plans" in *the ETM® System Technical Reference* for details about Dialing Plans.

Index