Release 6.3.0

Voice Firewall

User Guide

SecureLogix ®

About SecureLogix Corporation

SecureLogix Corporation enables secure, optimized, and efficiently managed enterprise voice networks. The company's ETM® (Enterprise Telephony Management) System hosts a suite of integrated telecom applications that protect critical network resources from telephony-based attack and abuse, and simplify voice network management.

SecureLogix® Solutions address real-world problems for real-world voice networks. The flexible ETM System scales to support any voice environment, no matter how large or small. Engineered with full hybrid voice technology, the ETM System supports multi-vendor networks containing any mix of converging VoIP and legacy voice systems.

SecureLogix Solutions are currently securing and managing over two million enterprise phone lines. The company's customers span nearly every industry vertical, from regional banks and hospitals, to the largest military installations and multi-national corporations.

For more information about SecureLogix Corporation and its products and services, visit our website at *http://www.securelogix.com.*

Corporate Headquarters:

SecureLogix Corporation

13750 San Pedro, Suite 820

San Antonio, Texas 78232

Telephone: 210-402-9669 (non-sales)

Fax: 210-402-6996

Email: *info@securelogix.com*

Website: *http://www.securelogix.com*

Sales:

Telephone: 1-800-817-4837 (North America)

Email: *sales@securelogix.com*

Customer Support:

Telephone: 1-877-SLC-4HELP

Email: *support@securelogix.com*

Web Page: *http://support.securelogix.com*

Training:

Telephone: 210-402-9669

Email: *training@securelogix.com*

Web Page: *http://training.securelogix.com*

Documentation:

Email: *docs@securelogix.com*

Web Page: *http://support.securelogix.com*

Customer Support
for Your ETM® System

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

**SecureLogix Corporation offers telephone,
email, and web-based support.
For details on warranty information
and support contracts, see our web site at**

http://support.securelogix.com

Contents

Viewing Policy Enforcement Results   91

AAA Services for the Voice Firewall   104

Preface

About the ETM® System Documentation

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

ETM® System Documentation

The following set of guides is provided with your 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 Guide—Provides task-oriented installation and configuration instructions and explanations for technicians performing system setup.

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

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

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

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

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

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

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

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

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

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

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.

How the Voice Firewall Monitors and Protects Your Network

Network Security and Your Telecommunications System

The legacy TDM voice network provides intruders with a way to attack the data network through modems, which are present in nearly every enterprise. Attackers can use war-dialing techniques to find unauthorized and insecure modems, which can then be used to bypass the perimeter-focused IP security technologies. Once attackers have access to an internal system, they can exploit it and move to other systems in the network.

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

The ETM® System provides the tools and visibility you need to solve the many security and management issues associated with voice services delivered over the increasingly complex hybrid TDM and VoIP networks. Most organizations have no means of monitoring and logging call activity on their telecommunications network, much less of controlling it. Anyone within an organization could use a fax handset to dial long distance or "1-900" calls on an analog line, bypassing the Private Branch Exchange (PBX) and providing no means of associating the person with the calls. Someone could use a digital line interface to convert a digital line to an analog line, or put a modem on an analog line. With this unauthorized connection, an employee could completely bypass all network monitoring to dial an Internet Service Provider and spend hours surfing the Internet or transferring sensitive documents to a competitor.

Well-configured firewalls and routers are effective in protecting the perimeter of computer networks, and are considered essential network components for the enterprise. They generally protect TCP/IP-based networks (or other packet-based protocol networks), restricting access to, and protecting data on, the networks behind them. However, firewalls and routers are typically focused on protecting the corporate network from the Internet; they do not protect against telecommunications access to the network through unauthorized modems.

Unauthorized modems connected to networked computers can bypass the most capable, well-configured firewall or router, effectively providing access from the Public Switched Telephone Network (PSTN) to an organization's data network. This interface to the PSTN not only provides unmonitored connectivity internally, but it provides a port for outsiders with malicious intent.

The Voice Firewall Safeguards Your Network

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.

The Voice Firewall helps secure your enterprise against many vulnerabilities, including:

- Hacker access to modems.

- Removal of proprietary or classified information from the enterprise via unauthorized modems.

- Toll fraud.

- Access to 1-900 and other cost-per-call numbers.

- Unauthorized access Internet Service Providers.

- On VoIP Spans, Denial-of-Service (DoS) attacks, excessive media rate, and SIP anomalies.

The Voice Firewall enables you to create Rules-based Policies to control call traffic in real time, by allowing calls to go through or terminating them based on call criteria you specify. The Policy can be configured to send email to administrators or security personnel, notifying them of attempted security violations.

The ETM® System enables enterprise-wide deployment of Policies with centralized management. That is, Policies can be defined at a central location, and then distributed throughout the enterprise via the Performance Manager. The results of Policy enforcement can be viewed from any authorized Performance Manager.

With properly designed Policies, the Voice Firewall can provide tight control of your TDM and VoIP telecommunications system. With the Voice Firewall, you have the tool you need to evaluate, secure, monitor, and improve telecom security and usage across the enterprise-wide network environment.

AAA Services for the Voice Firewall

AAA ("Triple A") Services for the Voice Firewall ties authorized protected services access to a user rather than to a specific phone number. This enables tighter control of security, since you can:

- Deny access to protected services to everyone except authorized AAA users.

- Manage access by remote users who cannot be associated with a specific calling phone number.

- Block unauthorized calls without relying on the availability of the source phone number during a call.

AAA Services for the Voice Firewall provides these benefits by offering centralized authentication, authorization, and accounting to control access to protected services on your telecommunications network.

- **Authentication** provides a way of identifying an authorized user by requiring the user to enter a valid user ID and PIN before access is granted. If the credentials do not match, authentication fails and access is denied.

- **Authorization**, the process of determining which resources or services a user is permitted to access, is provided by means of AAA Service User accounts. Only users that have an account can be authorized.

- **Accounting** measures the resources a user consumes during access by logging the session statistics and usage information. These logs can be used for authorization control, trend analysis, resource utilization, and capacity-planning activities.

AAA Services supports both local and remote users and inbound and outbound calls. AAA Services uses a distributed authentication server, operating solely in voice mode, that prompts the caller for a valid user ID, PIN code, and destination number before allowing the user to connect to protected services.

The operational advantages of AAA Services are significant. It effectively eliminates the threat imposed by war dialers with Policy-based authentication that can be configured to deny network connections through the Voice Firewall without prior authorization from the AAA Server.

Additionally, AAA Services provides enhanced, centralized accounting for the use of protected services. AAA Services can provide not only when and what was accessed, but also who (by name), and, optionally, can include the name of the calling party's organization. For example, "Bill Johnson of Telco Services, Inc., called on 10/10/2002 at 8:00 for fifteen minutes and accessed the PBX maintenance port on the Meridian One."

For details about installing, configuring, and administering AAA Services for the Voice Firewall, see the *ETM® System Installation Guide*.

The Voice Firewall Provides Network Visibility and Alerting

In addition to providing unprecedented network security, the Voice Firewall provides significant visibility and alerting, including:

- Policy-based resource access limits and usage monitoring.

- Call-accounting visibility for IP trunks that may otherwise be unmonitored.

- A tool for comparison and ROI calculations when using a toll-bypass VoIP network for toll cost reductions.

- Real-time notification of security or availability events.

Voice Firewall Policy Overview

Understanding Voice Firewall Policies

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, or SNMP trap.

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

After you define Policies, you install them on the Spans in the ETM® Appliances, which are inline with your telco system. The Spans then automatically enforce the Policy in real time.

Policies can be defined at a central location and then distributed throughout the enterprise, or they can be defined at each location. 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.

A Span Group assigned to the Policy named "Houston VoIP." The red X indicates this Policy is not installed.

A Firewall Policy

A Span Group assigned to Policy named "San Antonio PRI." The green check means this Policy is installed on this Span Group.

The Default Policy node; shows Span Groups with no installed user-defined Policy.
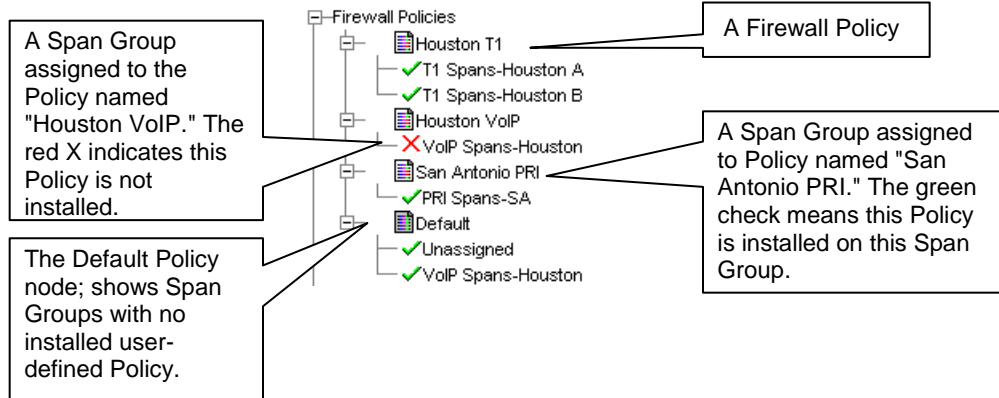
If a Span Group is currently enforcing the Policy, a green check mark ✔ appears next to the Span Group name. If the Policy is not currently installed on the Span Group, a red **X** appears next to the Span Group name.

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.

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.

No.	Call Dire...	Source	Destination	Call Type	Time	Call Duration	Attributes	Action	Track	Install On	
-	Out...	Any	Emer...	Any	Any	Any	None	Allow	Log	Any	The de
1	Any	Accoun...	Any	Modem	Any	Any	None	Allow	Log	Any	
2	Out...	Fax Nu...	Any	Fax	Any	Any	None	Terminate	Log / Telecom ...	Any	
3	Inb...	Any	Any	Data Call	B...	Any	None	Allow	Log / Realtime...	PRI Spans	
4	Any	Any	Any	Any	Any	Any	Unknown...	Allow	Log / Telecom ...	VoIP Spans	
5	Inb...	Any	Supp...	Unansw... Busy	8-5 M-F	Any	None	Allow	Log / Support ...	Any	
6	Any	Any	Any	Modem	Any	Any	None	Terminate	Log / Security	Any	
-	Any	Any	Any	Any	Any	Any	None	Allow	None	Any	

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 29 for instructions for defining Policies.

Call Direction

On TDM lines, 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**. On VoIP calls, the definition of inbound/outbound may vary, depending on how the ETH0 and ETH1 connections are made.

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.

- **AAA Service User(s)**—Specifying one or more AAA Service Users in the **Source** field of the Rule allows only those authorized AAA Service Users to dial a specific phone number protected by the Voice Firewall. For information about AAA Services for the Voice Firewall, see "Overview of AAA Services for the Voice Firewall" on page 104.

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

! ⏏Fax When the Call Type 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/H.323 message received indicating a busy line.
	Note: Sometimes a message is played on busy lines instead of a busy signal, offering auto-redial when the line is free. In this case, the call type is identified as **Unanswered** or **Undetermined** rather than **Busy**, depending on the signaling on the trunk.
Data Call	(*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*) Modem calls. Reported when distinct modem handshake messages are detected on the line. See also *Modem Energy*.

Call Types, continued

Call Type	Definition
Modem Energy	(*Does not apply to VoIP*) 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*) Secure Telephone Unit III (STU-III) calls. Reported when distinct STU handshake messages are detected on the line.
Unanswered	The calling party hung up after the call was dialed, but before the call was answered.

Undetermined	A distinct call type has not been detected. This can occur in the following situations:
	
	• The calling number hung up after the call was answered but before the call type was determined. These may occur, for example, when a voice mail system answers the call, but the caller decides not to leave a voice mail message and hangs up.
	
	• Silent or indistinguishable calls are reported in the **Call Monitor** as **Undetermined** until one of the following occurs:
	  – A distinct call type is detected.
	  – When **Call Type Timeout** is reached, the call defaults to **Voice**.
	
	• For 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.

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 it, the Rule applies during non-business hours.

🔴 🕐 Business Hours When the Time 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. 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 for call duration Rules, see "Call-Duration Processing" on page 28.

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.

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**.

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, or date/time created). The comment appears in reports and logs, but has no affect on the processing of the Rule.

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 numberof 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:

- 8250 Controller Cards, 5000 series SIP Appliances, and the SIP AXP implementation—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.

- *Does not include EOL Appliance models or those running pre-6.1 appliance software, which are limited to 8000 objects.*

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, which are inline with 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 78 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 119 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 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. 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

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 source.

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.

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 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 allows you to define Rules that are triggered by certain calls, regardless of call type. These are called *call-reject Rules*. During this phase, the call is compared only with Rules in which you specify **Any** in the **Call Type** field. When a Rule that specifies call type is encountered, processing pauses until call type is determined.

Call-reject processing provides the advantage of immediate enforcement. In contrast, it may take 20 seconds or more to determine call type. Therefore, to take advantage of the benefits of call-reject processing, order the Rules in the Policy with all Rules with **Any** in the **Call Type** field placed before any Rule that specifies call type.

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 92.)

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.

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

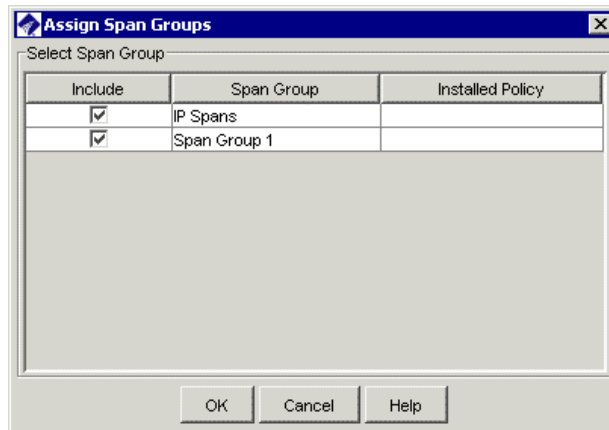You must have the **Full Control** user permission for Firewall Policies to create them.

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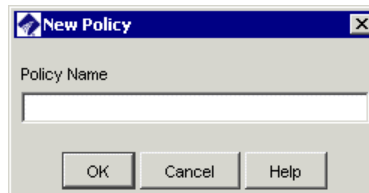
2. In the **Policy Name** box, type a name to identify the Policy, and then click **OK**. The **Assign Span Groups** dialog box appears.

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 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 it 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, you can show them using the **View** menu.
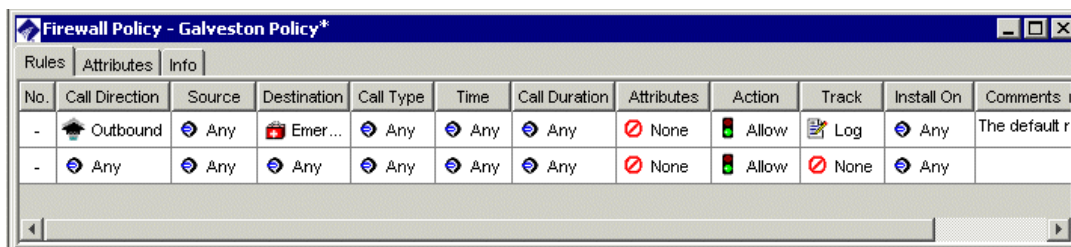
5. Click **File | Save**. The Policy appears in the **Firewall Policies** subtree.

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.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Attributes	Action	Track	Install On	Co
-	☁ Outbound	⊖ Any	📕 Emer...	⊖ Any	⊖ Any	⊖ Any	⊘ None	▮ Allow	📝 Log	⊖ Any	The default r
1	⊖ Any	⊖ Any	⊖ Any	⊖ Any	⊖ Any	⊖ Any	⊘ None	▮ Allow	⊘ None	⊖ Any	
-	⊖ Any	⊖ Any	⊖ Any	⊖ Any	⊖ Any	⊖ Any	⊘ None	▮ Allow	⊘ None	⊖ Any	

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 34 for details.

- **Destination**—The destination of the call. See "Destination Field" on page 44 for details.

- **Call Type**—The traffic type(s) to which the Rule applies. See "Call Type Field" on page 47 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 44 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 45 for details.

- **Attributes**—VoIP call attributes. See "Attributes Field" on page 32 for details.

- **Action**—Allow or terminate calls that match the Rule. See "Action" on page 46 for details.

- **Track**—Notification and logging for calls that match the Rule. See "Track Field" on page 47 for details.

IMPORTANT Rule order is important in Firewall Policies. See "Organizing the Rules in the Policy" on page 53 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 49 for details.

- **Comments**—Optional notes about the Rule.

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 49.

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 70 for details about what verification checks. See "Installing a Policy" on page 77 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

The **Attributes** field allows you to specify additional possible characteristics of VoIP calls to which you may want to apply the Firewall Policy: **Unknown Codec**, **Excessive Media Rate**, or a **Media Timeout** of a certain length.

Specifying VoIP Call Attributes

To add VoIP call attributes to a Rule

1. In an open Policy, right-click in the **Attributes** field. The **Attributes** dialog box appears.
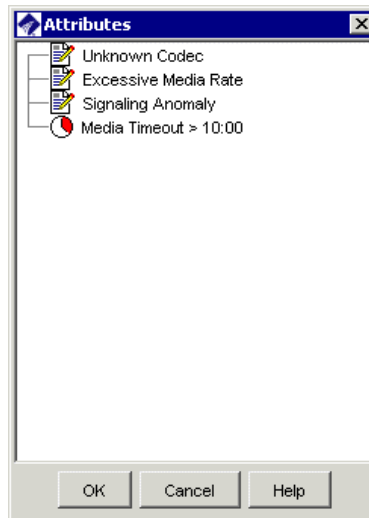
2. Click the attribute to which you want to apply the Rule:

    *   **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

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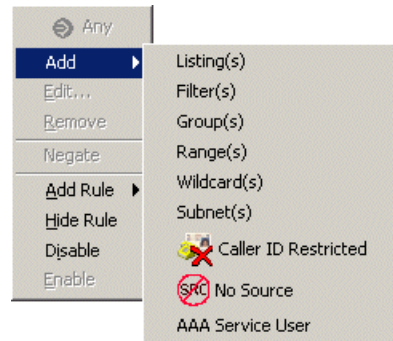
You can add one or more of the following to specify the call source:

- **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.

- **AAA Service User(s**)—Specifying one or more AAA Service Users in the **Source** field of the Rule allows only those authorized AAA Service Users to dial a specific phone number protected by the Voice Firewall. For information about AAA Services for the Voice Firewall, see "Overview of AAA Services for the Voice Firewall" on page 104.

To add one or more Listings to the field

Adding Listings to the Source or Destination 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 **Resolve**. 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.
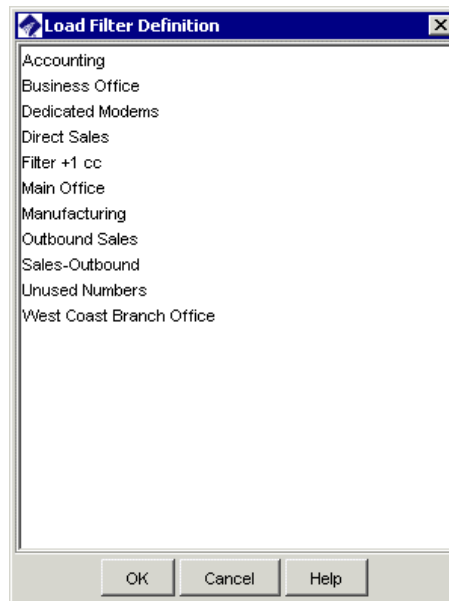
        b. Click the Filter Definition that you want to use, and then click **OK**.

        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 **Resolve**. The listings that match appear in the **Results** box.

- To define a new set of search criteria, click **Modify**. The **Filter** dialog box appears.
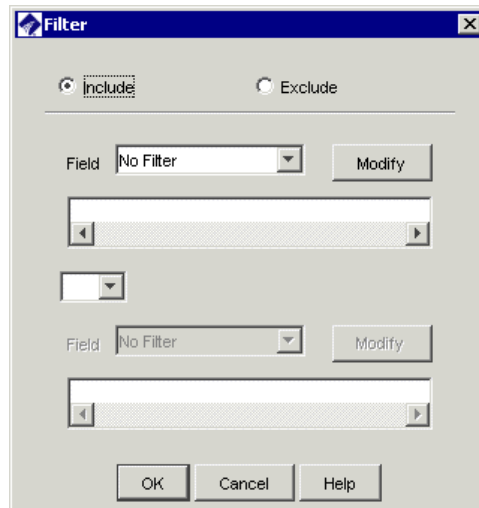
a. To define the Filter to exclude Listings that meet the criteria, select **Exclude**; to define the Filter to include all listings that meet the criteria, select **Include**.

b. In the **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 that have the **Modem** extension type selected. Select **Extension Type**. The **Extension Type Filter** dialog box appears. Select **Include**, select **Modem**,, and then click **OK**. The criteria appear in the **Filter** dialog box, as illustrated below.
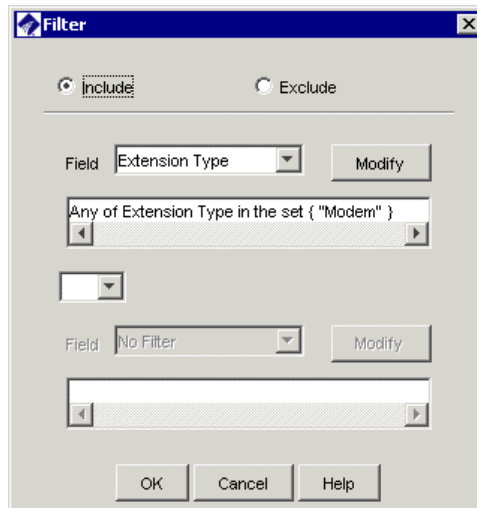
Notice that both the **Extension Type Filter** dialog box and the **Filter** dialog box have exclude/include check boxes. These fields work together. For example:

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.

Filter Dialog Box	Extension Filter Dialog Box	Result
Include	Include Modem	Includes Listings with Extension Type Modem
Include	Exclude Modem	Exclude Listings that contain Extension Type Modem
Exclude	Exclude Modem	Exclude Listings that do not contain Modem.

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.

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 **Subfilter** 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.
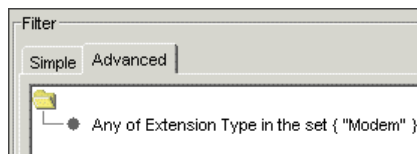

2. Click **Resolve**. All of the listings that match the criteria appear in the **Results** box. Results are returned in batches of 100. If multiple pages of Listings are returned, click the **First Page**, **Next Page**, **Previous Page**, and **Last Page** buttons to navigate through the results.

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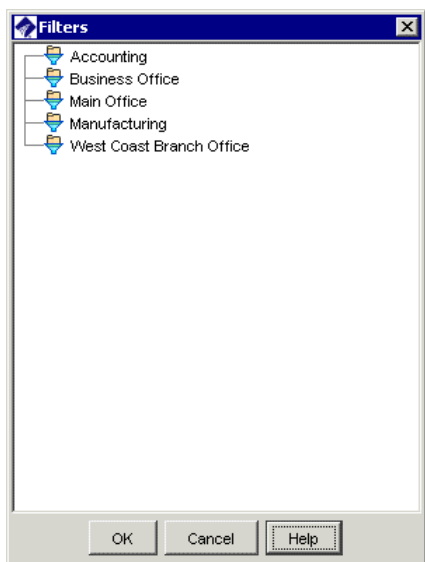
You cannot define or edit Filters from this dialog box. Use the Directory Manager to define and edit Filters.

Tip: To select multiple Filters, hold down CTRL or SHIFT while clicking.

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

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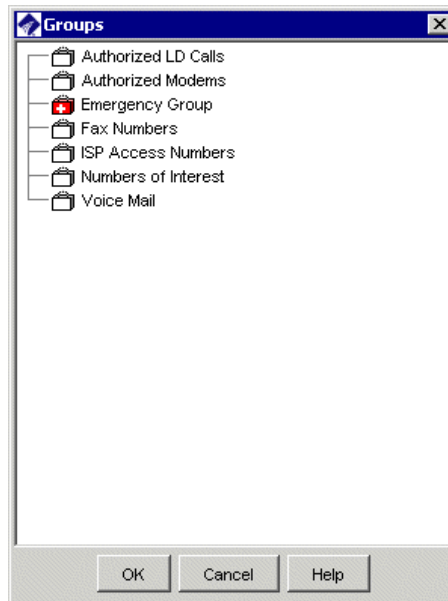
2. Click the Group you want to add, and then click **OK**.

    *   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**.

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**.

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.
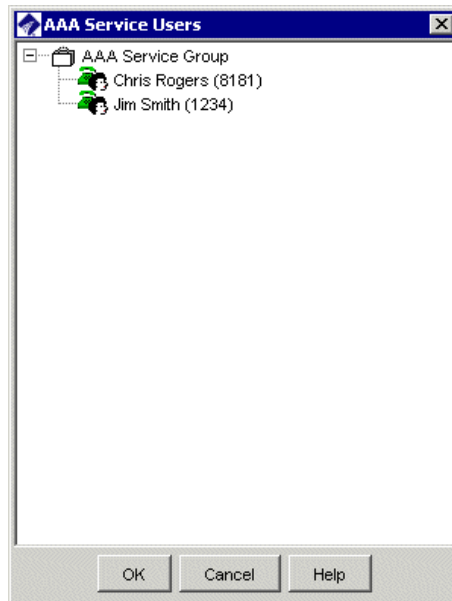
To add No Source to the Source field

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

Adding AAA Service Users to the Source Field

To add a AAA Service User to a Rule

1. Right-click the **Source** field of a Rule, point to **Add**, and then click **AAA Service User**.

2. Click one or more AAA Service Users that you want to add to the Rule, and then click **OK**.

   For instructions for defining AAA Service Users and Groups, see "

Managing AAA Users" on page 108.

For details about how to sort, search, filter, and generate a report of the AAA Service Users in this dialog box, see "Setting Display Properties" in the *ETM*® *System User Guide*.

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 35.

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

"Adding Groups to the Source or Destination Field" on page 40.

"Adding Ranges to the Source or Destination Field" on page 40.

"Adding Wildcards to the Source or Destination Field" on page 41.

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 42 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 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 28.

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.
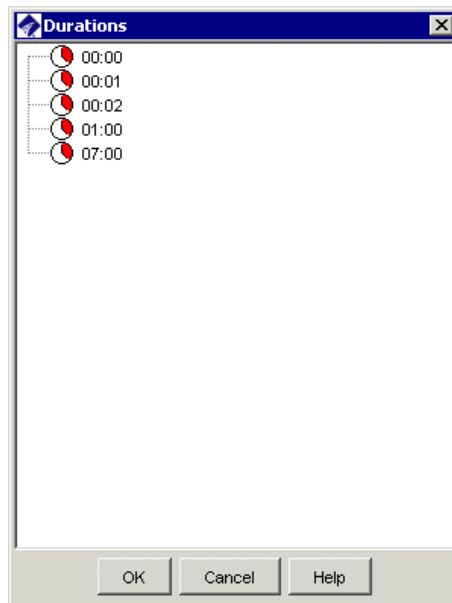
```
Durations                              ×
    00:00
    00:01
    00:02
    01:00
    07:00




            OK      Cancel      Help
```

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 28.

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**.

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 <u>does not</u> 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 21.

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:

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 Guide*.

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

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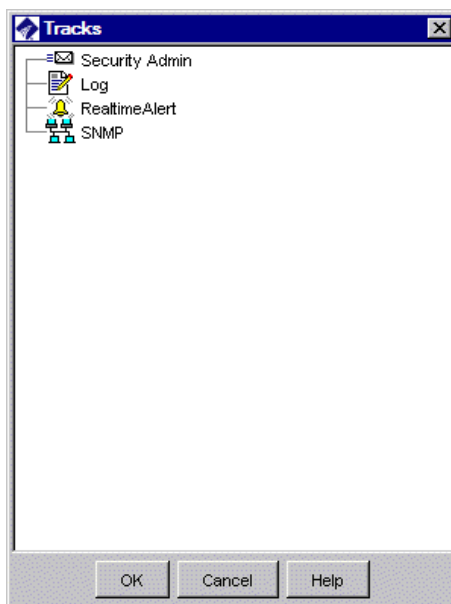
2. Click the Track you want to add, and then click **OK**.

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 affect on the processing of the Rule. 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 comments are included in the notifications.

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.

For instructions for defining Emergency Groups in the Directory Manager, see "Defining a New Emergency Group" in the *ETM® System User Guide.*
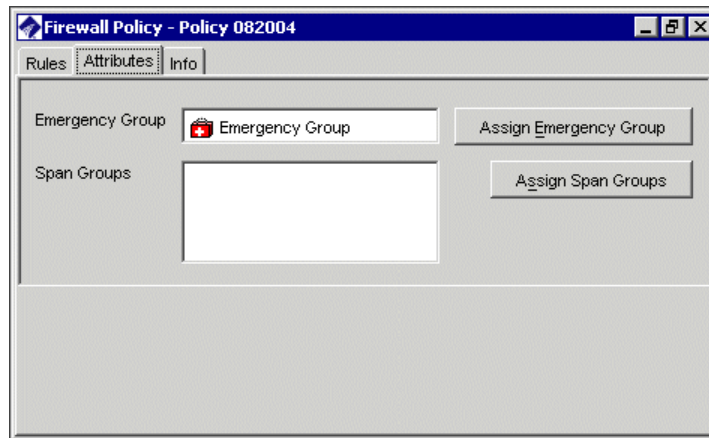
2. Click **Assign Emergency Group**. The **Assign Emergency Groups** dialog box appears with all defined Emergency Group(s) listed. (To view the members in an Emergency Group, right-click the Group, and then click **View**.)

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.

No.	Call Direction	Source	Destination
-	⬆ Outbound	⊖ Any	🔴 SA Emergency Group

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 77 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.

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 70 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 object issue was encountered, you can either modify the Policy, or choose to install it again using Priority Mode.

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.

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—at the beginning of the Policy. This way, they can be processed while call type determination is still ongoing.

- 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, if the call has a call type of **Modem**, is there a "terminate all modems" Rule that will fire before an "allow specific modems" 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 54 for more information.

Call-Duration Processing Example

Consider the following example: You want to terminate and be notified by email of any modem calls lasting 1 hour, be notified by Real-Time Alert of modem calls lasting 30 minutes, allow any fax calls on dedicated fax lines, and be notified by email of any non-fax calls on dedicated fax lines. This scenario assumes no call-type changes occur during the call, SMDR is *not* required for any Rule, and no Rule terminates calls that do not match a prior Rule.

You could create a Policy that includes the following Rules, as shown in the illustration below:

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Attributes	Action	Track
-	Outbound	Any	Emergen...	Any	Any	Any	None	Allow	Log
1	Outbound	Any	Any	Modem	Any	01:00	None	Terminate	Log / Telecom ...
2	Outbound	Any	Any	Modem	Any	00:30	None	Allow	Log / Realtime...
3	Outbound	Fax Num...	Any	Fax	Any	Any	None	Terminate	Telecom ...
4	Outbound	Any	Any	Modem	Non-Busi...	Any	None	Allow	Log
-	Any	Any	Any	Any	Any	Any	None	Allow	None

1. Define a Rule with a Modem **Call Type**, 1-hour **Call Duration**, Terminate **Action**, and Email **Track** (as shown in Rule 1).

2. Define a Rule with a Modem **Call Type**, 30-minute **Call Duration**, Allow **Action**, and Real-Time Alert **Track** (as shown in Rule 2).

3. Define a Rule to terminate outbound non-Fax calls on dedicated fax lines and send an Email **Track** (as shown in Rule 3).

4. Define a Rule to log all Modem calls during non-business hours (as shown in Rule 4).

A one-hour modem call would be processed against this Policy as follows:

1. The default Emergency Rule is a call-reject Rule, because it does not have to wait for call type to be determined. The Rule is skipped because the destination of the call does not match any of the numbers in the Emergency Group.

2. After the call type of Modem is detected, call type processing begins with Rule 1.

3. The call matches all of the criteria in Rule 1, except that the duration has not yet reached 1 hour, so Rule 1 is skipped, and processing continues with Rule 2.

4. Because the call has not yet reached 30 minutes, Rule 2 is skipped.

5. The call is not on a fax line, so Rule 3 is skipped.

6. If the call occurs after business hours, the call matches Rule 4 and Rule 4 fires. Because a duration Rule was encountered prior to the Rule that fired, the call is reprocessed against the Policy every 15 seconds until the call reaches the 30-minute duration, at which time Rule 2 fires and a Real-Time Alert is generated.

7. Duration processing continues again with Rule 1, but because the call has not yet reached the 1-hour duration and Rule 2 has already fired, processing pauses for 15 seconds. This cycle is repeated every 15 seconds until duration reaches 1 hour or the call ends.

8. If the call duration reaches 1 hour, Rule 1 fires, the call is terminated, and an email is sent.

Notice that if the order of the Rules were reversed so that the 30-minute duration Rule came first, the 1-hour Rule would not be considered, because subsequent processing never passes a Rule that has already fired. After the 30-minute Rule had fired, processing would end.

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 modem calls from a telephone number in your organization, and a generic Rule terminating all other modem calls. Any modem calls that do not trigger the "Allow modem calls" Rule would trigger the "Terminate modem calls" Rule.

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.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track	Install On
1	Inbound	Any	Any	Mo...	Any	Any	Allow	Log	San Antonio
2	Outbou...	Any	900 n...	Any	Any	Any	Ter...	Log	Dallas
3	Outbou...	Fa...	Any	...	Any	Any	Allow	Log Email	Houston
4	Any	Any	Any	Any	Aft...	01:00	Allow	Log Real...	Any

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.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track	Install On	
1	Inbound	Any	Any	Mo...	Any	Any	Allow	Log	Any	
2	Any	Any	900 n...	Any	Any	Any	Ter...	Log	Any	
3	Outbou...	Fa...	Any	! ...	Any	Any	Allow	Log Non-...	Any	
4	Any	Any	Any	Any	Aft...	01:00	Allow	Log Real...	Any	

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.

Identifying Toll Fraud

Voice-mail systems, voice-response systems, long-distance authorization codes, calling cards, and backdoor dial-access lines to customer equipment are especially vulnerable to toll fraud. Toll fraud can occur as improper use of telephone lines for personal voice calls or other unauthorized purposes, or when a hacker dials into a PBX, key system, or other managed telephone equipment, and then probes the system for a weakness that provides an outside telephone line. Once the outside line is obtained, calls may be made anywhere in the world and toll fees are charged to the owner/operator of the PBX.

Toll fraud can be indicated by any of the following:

- Increase in calls after business hours.

- Calls to certain numbers or area codes.

- Calls from certain numbers.

- Calls to foreign countries.

- Excessive call durations for a call type.

- Surges in telephone use.

- Operator-assisted calls.

These sorts of calls do not always indicate toll fraud. After you have examined the call data and determined that toll fraud is occurring, you can write Rules to notify you with an Email, Real-Time Alert, and/or SNMP Track when suspect calls occur.

Non-Business-Hours Calls

In our global marketplace, international calls are routine, increasing the risk of telephone-system abuse within organizations. For example, unauthorized employees, contractors, or visitors can place international or other costly personal calls from phone numbers for which you have defined Rules allowing business-related international calls.

To prevent this type of fraud after business hours and on the weekends, you can Track calls during non-business hours with the following Rule:

1. In the **Call Direction** field, select **Outbound**.

2. In the **Time** field, add the **Business Hours** Time (defined by default as 8 AM to Noon and 1 PM to 5 PM, Monday-Friday).

3. Negate the **Time** field so that the Rule applies at all times other than those defined in the **Business Hours** Time.

4. In the **Track** field, add an **Email** Track.

5. Leave all other fields at their defaults.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track	Install On	Comments
1	Outbound	Any	Any	Any	! Business Hours	Any	Allow	Log emailadmin	Any	

With this Rule, any outbound call made during non-business hours is logged in the **Policy Log** and an **Email** notification is sent. Later, if reports show frequent calls during non-business hours to/from one or more phone numbers, you can define a more specific Rule to terminate unauthorized calls to/from those numbers.

Calls to/from Specific Numbers

You can define Rules that apply to a specific phone number, all numbers in an area code, or all numbers in a country code. For example, if reports show an unusual number of unauthorized calls to more than one phone number in Mexico, you can define a Rule to Track and/or terminate all calls to any phone number in Mexico.

For information about defining Wildcards, see "Directory Wildcards" in the ETM® System User Guide.

To address this issue:

1. Define a phone number Wildcard in the **Directory Manager** that applies only to the country code for Mexico.

2. In the Policy, in the **Call Direction** field, select **Outbound**.

3. In the **Destination** field, select the **Mexico** Wildcard.

4. In the **Track** field, add an **Email** Track.

5. Leave all other fields at their defaults.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track	Install On	Comments
1	Outbound	Any	Mexico	Any	Any	Any	Allow	Log / emailadmin	Any	

With this Rule, any outbound call to Mexico is logged in the **Policy Log** and an **Email** notification is sent. Later, if reports show frequent calls to/from one or more phone numbers, you can define a more specific Rule to terminate unauthorized calls to/from those numbers.

Unusual Call Duration

You can define Rules to Allow, Terminate, or Track specific types of calls based on call duration. Multiple short-duration calls can indicate war dialing; excessive call duration can indicate inappropriate use of company resources, DISA fraud, PBX hacking, and dial-through fraud. Such calls may be apparent in the **Call Monitor** and can be identified using Usage Manager reports.

For example, suppose that around 10 PM every Saturday, reports show a 2-hour outbound long-distance voice call. You can define a Rule to Track or terminate outbound voice calls with a 1-hour call duration during non-business hours.

To address this issue:

1. In the **Call Direction** field, select **Outbound**.

2. In the **Call Type** field, add **Voice**.

3. In the **Time** field, add the **Business Hours** Time, and then negate it.

4. In the **Call Duration** field, add a 1-hour Duration.

5. In the **Track** field, add an **Email** Track.

6. Leave all other fields at their defaults.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track
-	Outbound	Any	Emerg...	Any	Any	Any	Allow	Log
1	Outbound	Any	Any	Voice	❗ Business Hours	01:00	Allow	AdminEmail / Log
-	Any	Any	Any	Any	Any	Any	Allow	None

With this Rule, any outbound **Voice** call during non-business hours with a duration of 1 hour is logged in the **Policy Log** and an **Email** notification is sent.

Atypical Resource Usage

Numerous operator-assisted calls and surges in telephone use are indicators of toll fraud that general Rules would not easily address. In this case, regularly scheduled reports of telephone usage can demonstrate any such anomalies, which you can then address with one or more specific Rules. For information about using Usage Manager Reports, including automated Scheduled Reports, see the *Usage Manager User Guide*.

Managing Use of Modems

See "Overview of AAA Services for the Voice Firewall" on page 104 for details about using AAA Services to help you manage modems.

Employees may need to use authorized modems for many reasons. For example, an employee in the accounting department may need to upload the day's receipts to corporate headquarters, or a salesman at a remote site may need to "dial in" for a virtual meeting.

Many organizations discourage employees from connecting to a dial-up Internet Service Provider (ISP). In some organizations, employees transmitting confidential company information is a concern. Although your IT department may not have provided the employee's desktop computer with a modem, many savvy users can install their own modems or may plug their laptop's modem into the company telephone network.

To address all of these issues, you can create Policies that allow authorized modem use and track or terminate modem calls that are not authorized. (Note that Rules requiring outbound source or inbound destination can only terminate the call if the internal phone number is available during the call.)

Older modem protocols (such as V.21) and non-standards-based data transmission devices lack a standard modem handshake. All of the Spans (except VoIP Spans) detect the call type of such devices as Modem Energy and you can define Rules based on this call type. For example, you can define a Rule to terminate calls that have a distinct modem handshake, and a separate Rule to log calls that are identified as Modem Energy. You can then examine the logs to determine whether you should develop specific Rules for numbers on which the system has detected Modem Energy calls.

In the next example, modem calls are allowed from certain phone numbers in certain Span Groups, while unauthorized modem calls from other phone numbers are not.

For this, you need to create four Rules:

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track
1	Inbound	Remote Users	Engineering Modems	Modem Energy Modem	Any	Any	Allow	Email Administrator Log
2	Any	Accounting Dept.	Corporate Offices	Modem Energy Modem	Any	Any	Allow	None
3	Any	Corporate Offices	Accounting Dept.	Modem Energy Modem	Any	Any	Allow	None
4	Any	Any	Any	Modem Energy Modem	Any	Any	Terminate	Log Email Administrator

In the example above:

- Define the first Rule to allow all inbound calls from the **Remote Users** Group to the numbers in the **Engineering Modems** Group. Specify that an **Email** notification be sent each time this Rule fires, and add the call to the **Policy Log**.

- Define the second and third Rules to allow the phone numbers defined in the **Accounting** and **Corporate** Groups to send and receive modem calls to and from each other.

- Define the last Rule to terminate any modem calls into or out of the organization that did not trigger previous Rules. Specify that an **Email** notification be sent when this Rule fires.

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

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 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. 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 Calls for Which Source is Undefined

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 **Smith** Directory Listing is terminated if the caller has blocked the Caller ID information or if no source is available on a trunk that provides inbound source.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Attributes	Action	Track
1	Any	Caller ID Restricted / No Source	Smith, …	Voice	Any	Any	None	Terminate	Log

Managing STU Lines

A Secure Transmission Unit (STU) is a secure telecommunications device designed to operate both as an ordinary telephone and as a secure instrument over the telephone network. STUs are typically used by government organizations to protect the transmission of sensitive information. Because the unit can be used as an ordinary telephone, it is possible for a call to not go into secure mode. If STU telephones are used on your telco network, you can define Rules to detect whether a call has gone secure and terminate the call if it does not go into secure mode within a defined duration. For example:

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track
1	Any	Any	Any	STU	Any	01:00	Allow	Email Administrator / Log
2	Outbound	STU Lines	Any	! STU	Any	00:01	Terminate	Email Administrator / Log
3	Inbound	Any	STU Lines	! STU	Any	00:01	Terminate	Email Administrator / Log
4	Any	Any	Any	STU	Any	Any	Allow	Log

- Define the first Rule to trigger an email notification if any STU call has a one-hour duration.

- Define Rule 2 or 3 to terminate any call made to or from numbers in the **STU Lines** Group that is not identified as a **STU** call type within the first minute of the call.

- Define Rule 4 to allow all other STU calls and appear in the **Policy Log**.

Example Policy

This example Policy includes a number of the Rules discussed in this section.

No.	Call Direction	Source	Destination	Call Type	Time	Call Duration	Action	Track
-	Outbound	Any	Emergency Group	Any	Any	Any	Allow	Log
1	Outbound	Any	Mexico	Any	Any	Any	Allow	Email Administrator / Log
2	Outbound	Any	Any	! Voice	! Business Hours	Any	Allow	Email Administrator / Log
3	Outbound	Any	Any	Voice	! Business Hours	01:00	Allow	Email Administrator / Log
4	Inbound	Any	Call Center	Busy / Unanswered	Any	Any	Allow	Log / RealtimeAlert
5	Inbound	Remote Users	Engineering Modems	Modem Energy / Modem	Any	Any	Allow	Email Administrator / Log
6	Any	Accounting Dept.	Corporate Offices	Modem Energy / Modem	Any	Any	Allow	None
7	Any	Corporate Offices	Accounting Dept.	Modem Energy / Modem	Any	Any	Allow	None
8	Any	Any	Any	Modem Energy / Modem	Any	Any	Terminate	Email Administrator / Log
9	Outbound	Fax Numbers	Any	! Fax	Any	Any	Terminate	Email Administrator / Log
-	Any	Any	Any	Any	Any	Any	Allow	None

In this example Policy:

- The first Implied Rule, the Emergency Rule, occurs first in every Policy so that calls to emergency numbers are always allowed.

- The first user-defined Rule has a call type of **Any** and is a call-reject Rule, meaning that the Rule is processed without waiting for call type to be determined. Rule 1 fires on all outbound calls to any number in the **Mexico** Wildcard and triggers an **Email** Track.

- Rule 2 fires on an outbound call that is not **Voice** and occurs at times other than those defined in the **Business Hours** Time.

- Rule 3 fires on any outbound **Voice** call that is one hour long that occurs at times other than those defined in the **Business Hours** Time.

- Rule 4 fires on all calls to the **Call Center** Group that are **Busy** or **Unanswered** and triggers a **Real-Time Alert** Track.

- Rule 5 fires on any **Modem** or **Modem Energy** call from numbers in the **Remote Users** Group to the **Engineering Modems** Group. When this Rule fires, an **Email** Track is sent.

- Rules 6 and 7 allow **Modem** and **Modem Energy** calls between the **Accounting** and **Corporate** Groups. Since such calls are routine, no Tracks are specified. Note that because all calls are logged, you can run reports on these calls, but they do not appear in the **Policy Log**.

- Rule 8 terminates any **Modem** and **Modem Energy** calls that did not trigger previous Rules. When this Rule fires, an Email Track is sent.

- Rule 9 terminates any outbound call from any number in the Fax Numbers Group that does not have the **Fax** call type.

- The final Implied Rule, the catchall Rule, allows all calls that did not trigger previous Rules.

The examples below demonstrate how this Policy would process specific kinds of calls. All the examples assume source and call type are known when the Policy is processed.

Example Call #1

In this example, the Accounting department manager uploads the weekly payroll to the Corporate Offices every Friday at 9 AM. Example call #1 is a **Modem** call from a number in the **Accounting Dept.** Group to a number in the **Corporate Offices** Group. The call is processed against the Rules as follows:

1. Rule 1 looks for outbound calls to numbers in the **Mexico** Wildcard. The call does not match the Destination in the Rule, so processing continues with Rule 2.

Note that if this call had occurred during times other than those defined in the **Business Hours** Time, and Rule 2 was defined to terminate calls, the call would have been terminated.

2. Rule 2 looks for outbound calls that are **not Voice** that occur during times other than those defined in the **Business Hours** Time. The call type matches, but the time does not, so processing continues with Rule 3.

3. Rule 3 looks for outbound **Voice** calls during times other than those defined in the **Business Hours** Time. The **Call Type** does not match, so processing continues with Rule 4.

4. Rule 4 looks for any calls to the **Call Center** that are **Busy** or **Unanswered**. The call does not match Destination and Call Type in the Rule, so processing continues with Rule 5.

5. Rule 5 looks for modem calls from the **Remote Users** Group to the **Engineering Modems** Group. The **Call Type** matches the Rule, but the **Source** and **Destination** do not, so processing continues with Rule 6.

6. Rule 6 looks for modem calls from the **Accounting Dept**. Group to the **Corporate Offices** Group. All of the fields of the Rule match, so the Rule fires and the call is allowed. There are no Tracks specified for this Rule.

| *Example Call #2* | Example call #2 is an inbound modem call to the **Call Center** Group. All the lines in the **Call Center** Group are currently busy. The call is processed against the Rules as follows: |

1. Rule 1 looks for outbound calls to numbers in the **Mexico** Wildcard. The call does not match the Destination in this Rule, so processing continues with Rule 2.

2. Rule 2 looks for outbound calls that are **not Voice** that occur during times other than those defined in the **Business Hours** Time. The call does not match the Time in the Rule, so processing continues with Rule 3.

3. Rule 3 looks for outbound **Voice** calls during times other than those defined in the **Business Hours** Time. The call does not match the Time in this Rule, so processing continues with Rule 4.

4. Rule 4 looks for any calls to the **Call Center** that are **Busy** or **Unanswered**. All of the fields match, so the Rule fires, triggering a **Real-Time Alert** Track, and the call is logged in the **Policy Log**.

Example Call #3

Example call #3 is an outbound voice call made by an employee in San Antonio to his girlfriend in Mexico. He knows he cannot make long distance calls from his desk phone, so he uses the handset on the fax machine down the hall. The call is processed against the Rules as follows:

- Rule 1 looks for outbound calls to numbers in the **Mexico** Wildcard. All of the fields match, so the Rule fires, triggering an **Email** Track, and the call is allowed and logged in the **Policy Log**.

Note that Rule 9 (which terminates non-fax calls on Fax machines) also matches the parameters of this call; however, processing never passes a Rule that has fired.

Example Call #4

Example Call #4 is an inbound **Modem** call to a number in the **Call Center** Group at 3 AM. The call is processed against the Rules as follows:

1. Rule 1 looks for outbound calls to numbers in the **Mexico** Wildcard. The call does not match this Rule, so processing continues with Rule 2.

2. Rule 2 looks for outbound calls that are **not Voice** that occur during times other than those defined in the **Business Hours** Time. All the fields match but the Call Direction, so processing continues with Rule 3.

3. Rule 3 looks for outbound **Voice** calls during times other than those defined in the **Business Hours** Time. The Call Type and Call Direction does not match, so processing continues with Rule 4.

4. Rule 4 looks for any calls to the **Call Center** that are **Busy** or **Unanswered**. The **Call Type** does not match, so processing continues with Rule 5.

5. Rule 5 looks for modem calls from the **Remote Users** Group to the **Engineering Modems** Group. The **Call Type** matches the Rule, but the **Source** and **Destination** do not; processing continues with Rule 6.

6. Rule 6 and 7 look for modem calls between the **Accounting Dept**. Group and the **Corporate Offices** Group. The **Call Type** matches the Rule, but the **Source** and **Destination** do not; processing continues with Rule 8.

7. Rule 8 looks for any modem call that did not trigger previous Rules. All of the fields match, so the Rule fires, triggering a **Email** Track, and the call is terminated and logged in the **Policy Log**. Note that if Rule 8 were placed before any of the "allowed modems" Rules, all modem calls would be terminated.

Example Call #5
Example call #5 is a one-to-two-hour **Voice** call that occurs every Saturday night from an employee in San Antonio to her mother in Australia. The call is processed against the Rules as follows:

1. Rule 1 looks for outbound calls to numbers in the **Mexico** Wildcard. The call does not match the Destination in this Rule, so processing continues with Rule 2.

2. Rule 2 looks for outbound calls that are **not Voice** that occur during times other than those defined in the **Business Hours** Time. All the fields match but the Call Type, so processing continues with Rule 3.

3. Rule 3 looks for outbound **Voice** calls during times other than those defined in the **Business Hours** Time. All of the fields match except the Call Duration, so processing continues with Rule 4.

4. The call is processed against each of the Rules in sequence (including the final "Catch All" Rule). Every 15 seconds, the call is reprocessed against the Policy, until the call reaches the 1-hour duration. When call length reaches 1-hour, Rule 3 fires, triggering an **Email** Track, and the call is allowed and logged in the **Policy Log**.

Note that you could specify termination for such calls. For example, after running with this Policy, generating reports, and identifying a specific **Source** or **Destination** for such calls, you can add a Rule to the Policy to terminate calls to/from those numbers.

Policy Administration

Managing Policies

This section provides procedures for managing Policies, including:

- "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.
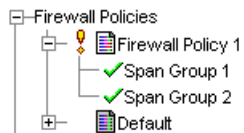
If you have the Performance Manager open, a **Policy Object(s) Updated** message indicates which of the installed Policies are affected by the changes.
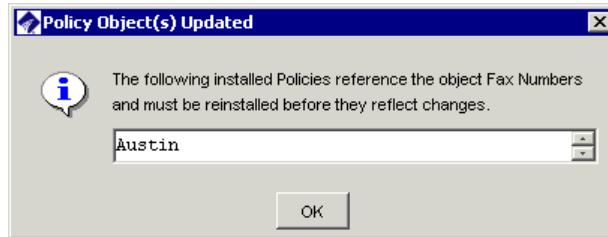
See "Installing a Policy" on page 77 for instructions for installing the Policy.

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

- 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 79.

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

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 <u>warning</u> message is generated, the Policy can be installed.

- If an <u>error</u> 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.
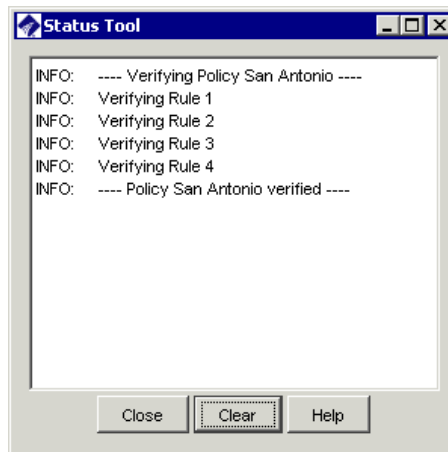
- To close the **Status Tool**, click **Close**. Results remain in the **Status Tool**, even if you close the tool, until you click **Clear** to erase them.

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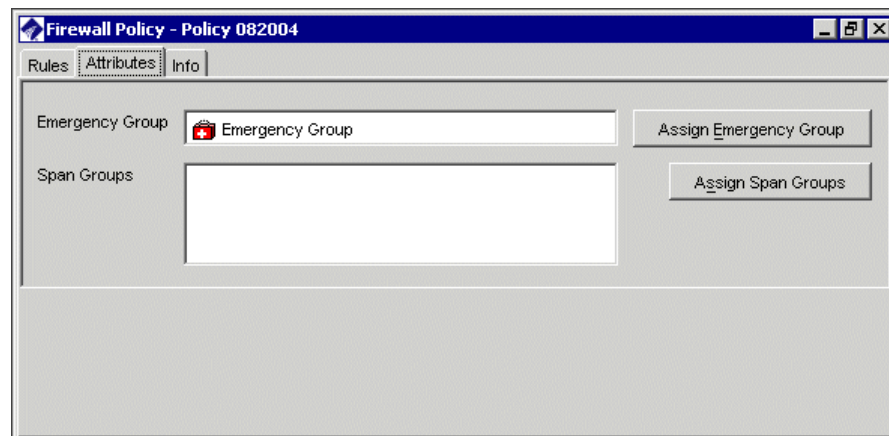
4. Click **Assign Emergency Group**. The **Assign Emergency Groups** dialog box appears with the currently defined Emergency Group(s) listed. (To view the members in an Emergency Group, right-click the Group, and then click **View**.)

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.

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.

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

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.
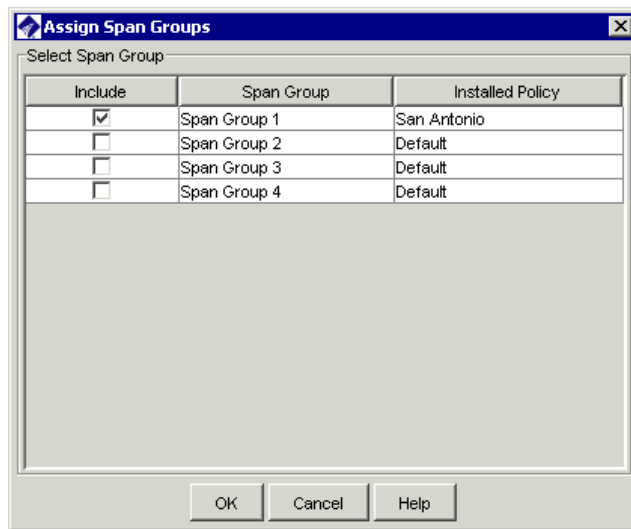
2. Check the box(es) of the Span Group(s) that you want to enforce this Policy; clear the check boxes of the Span Groups that you do not want to enforce this Policy.

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
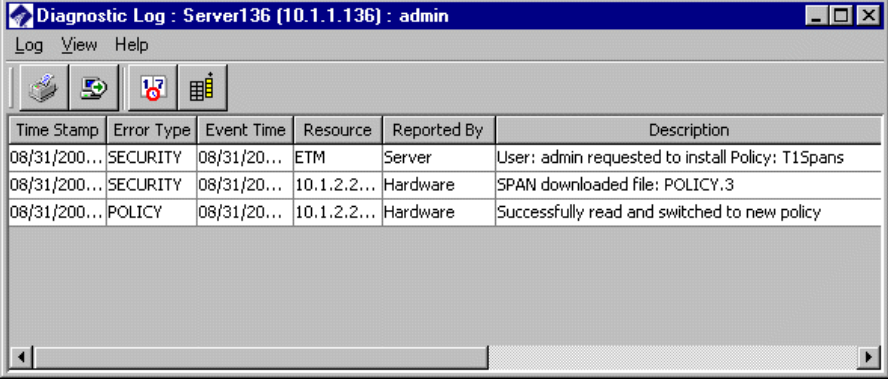
When you create or make changes to a Policy, you must install it on the Span Group(s) before it takes effect on the Span(s). If the Policy is already installed, updates to the Policy are downloaded when you save changes. If communication between the Management Server and a Span fails when you attempt 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. The **Status Tool** and **Diagnostic Log** display messages regarding the progress of the installation.

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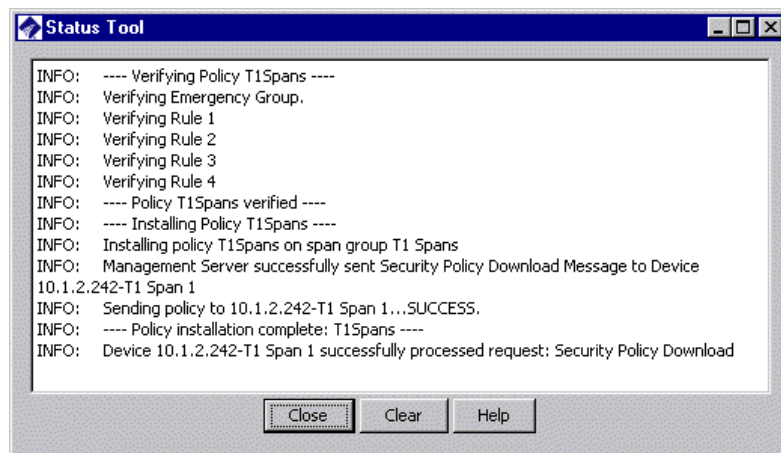
The Policy installation is complete and the asterisk in the title bar of the Policy editor disappears after the message "successfully processed request" appears in the **Status Tool** and "Successfully read and switched to new policy" appears in the **Diagnostic Log**.

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 26 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 27 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 27 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.

Uninstalling a Policy from a Span Group does not delete the Policy from the ETM® Database. See "Deleting a Policy" on page 69.

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 76.

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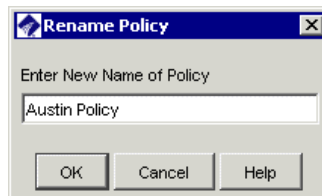
2. In the **Enter New Name of Policy** box, select the old name, and then type the new name.

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**.
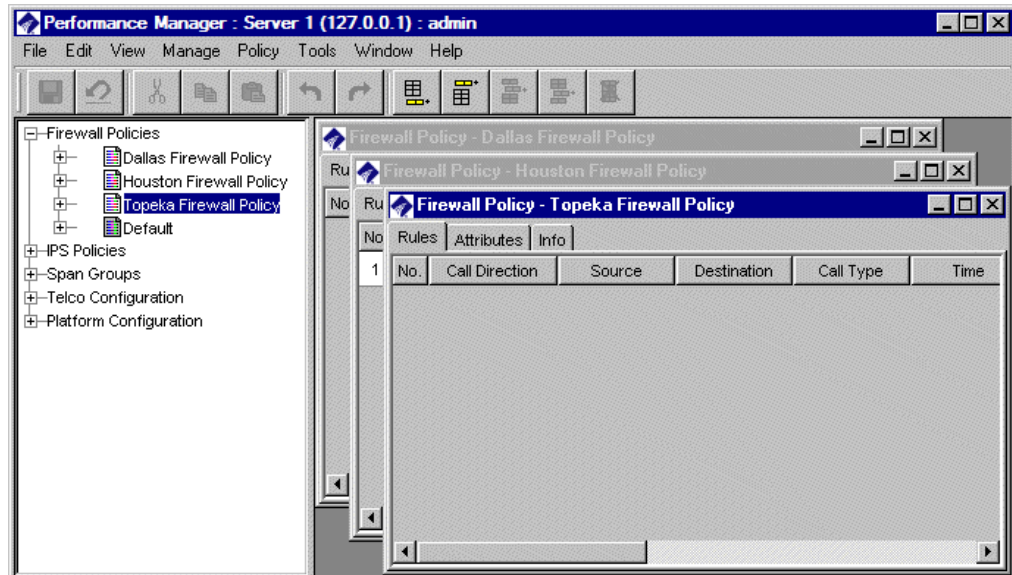
To view multiple Polices in tiled windows

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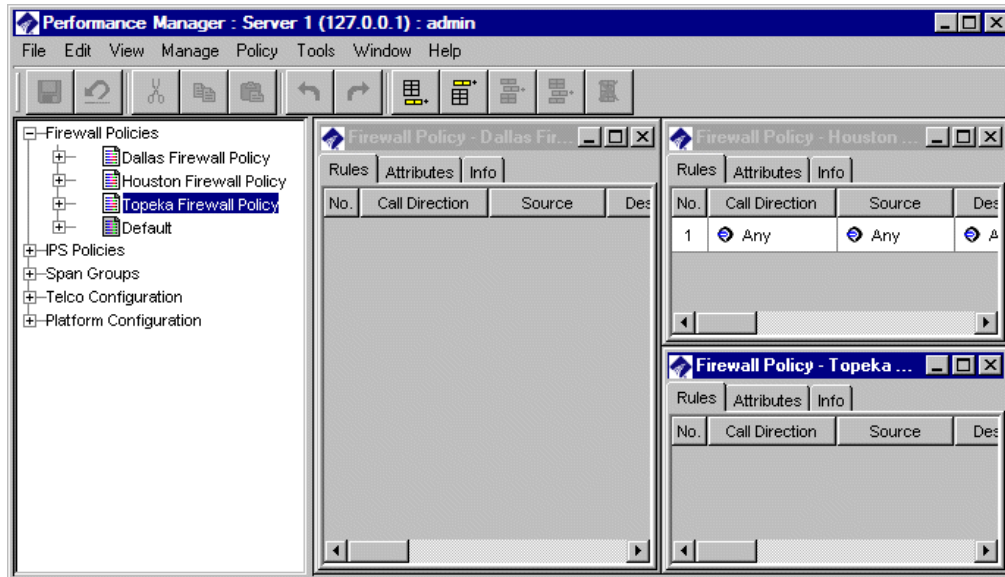
Managing Rules

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 <u>installed</u> 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 67 for more information about how changes affect installed Policies.

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

To remove an item from a Rule

Removing 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 83 and "Deleting Rules" on page 84.

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 this illustration, Rule 3 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.

To cut and paste or copy and paste a Rule

Cutting, Copying, and Pasting, Rules

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 83 and "Disabling Rules" on page 83.

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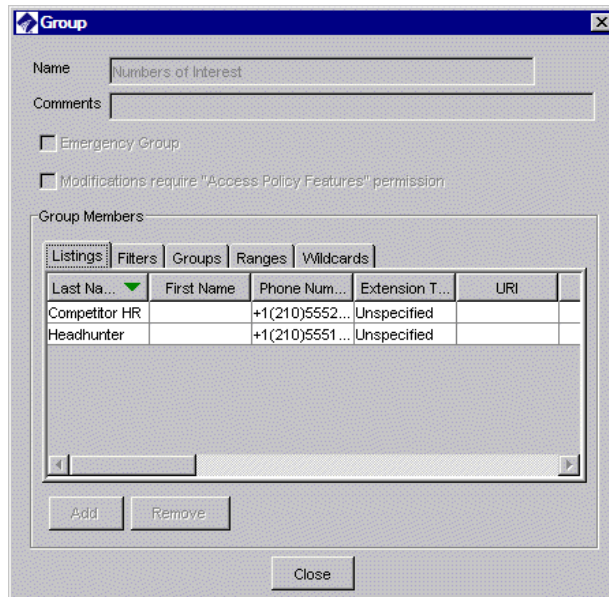
2. To view the Listings, Filters, Groups, Ranges, or Wildcards in the
   Group, click the **Listings**, **Filters**, **Groups**, **Ranges**, or **Wildcards**
   tab.

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 Resolve.
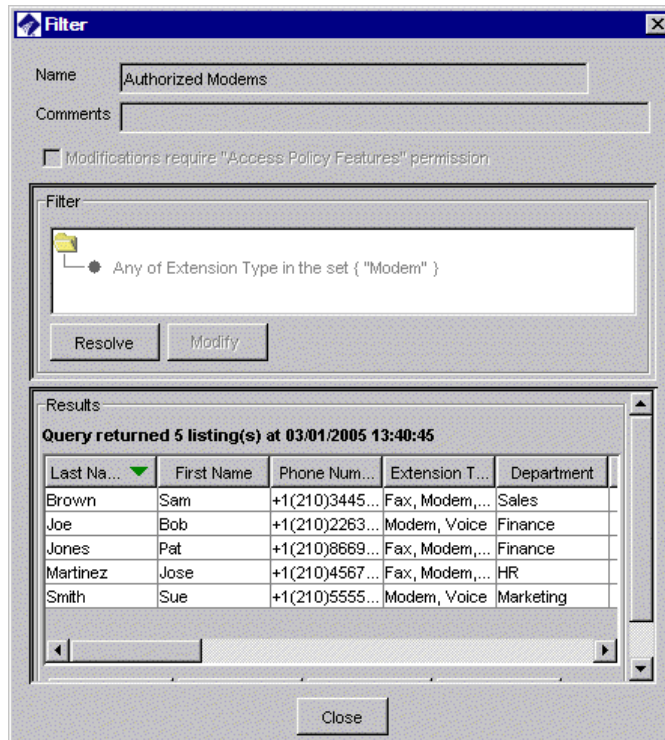
Viewing Contents of a Directory Range in a Rule

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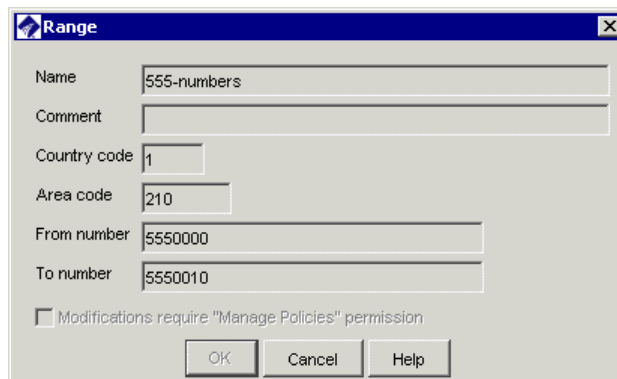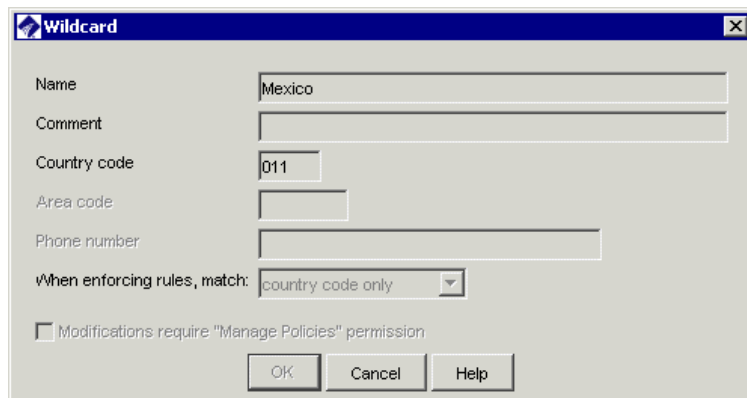
The **Range** dialog box appears showing the contents of the Range.

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.
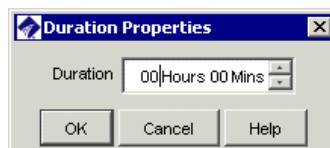
Durations

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.
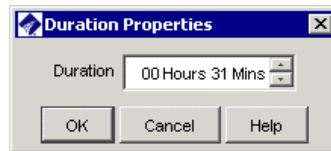
  c. In the **Duration** box, edit the hours and/or minutes of the Duration, and then click **OK**.

  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 74.

To specify a Span Group to enforce a Rule

1. Right-click the **Install On** field of a Rule, and then click **Add**.
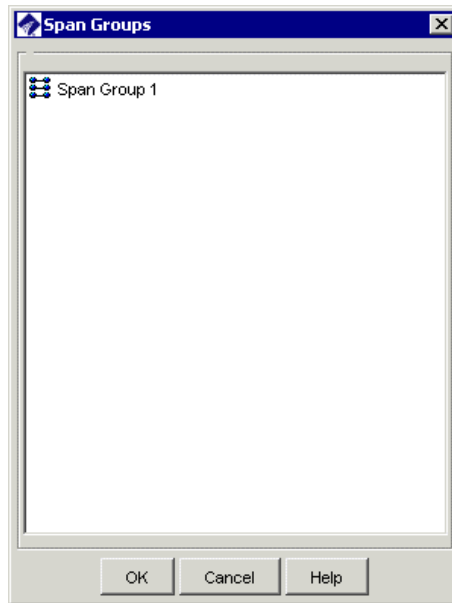
    Only the Span Groups assigned to the Policy appear in the **Span Groups** dialog box.

2. Click one or more Span Groups that you want to add to the Rule, and then click **OK**.

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 97 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
AAA User	AAA Service User information.
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.

Column Heading	Information Displayed
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.
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).
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.
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.

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 96 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.
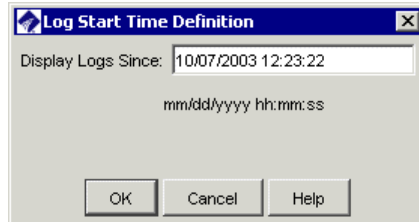
2. In the **Display Logs Since** box, type the starting date and time for which you want to limit displaying log information, in the format mm/dd/yyyy hh:mm:ss.

   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

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

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

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**.

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.

Call Logs for Span Group(s) Span Group 1 : Server 1 (10.1.1.132) : tennis

Log View Help

Log Time	Start Time	End Time	Duration	In/Out	Source	Destination	Type	Fi
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:03:52	OUTBOUND	+1(214)555-...	+1(214)555-...	Voice	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:02:07	INBOUND	+1(337)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:00:48	OUTBOUND	+1(214)555-...	+1(214)555-...	Undetermined	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:03:10	OUTBOUND	+1(214)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:00:54	OUTBOUND	+1(214)555-...	+1(900)555-...	Voice	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:05	INBOUND	+1(214)555-...	+1(214)555-...	Unanswered	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:03:10	OUTBOUND	+1(214)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:00:59	OUTBOUND	+1(214)555-...	+1(214)555-...	Unanswered	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:05	INBOUND	+1(214)555-...	+1(214)555-...	Modem	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:02:08	OUTBOUND	+1(214)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:00:48	INBOUND	+1(773)555-...	+1(214)555-...	Undetermined	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:04	OUTBOUND	+1(214)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:20	INBOUND	+1(781)555-...	+1(214)555-...	Voice	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:36	OUTBOUND	+1(214)555-...	411	Voice	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:20	INBOUND	+1(475)555-...	+1(214)555-...	Voice	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:36	OUTBOUND	+1(214)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:00:53	INBOUND	+1(214)555-...	+1(214)555-...	Fax	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:04:12	INBOUND	+1(469)555-...	+1(214)555-...	Modem	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:00:58	INBOUND	+1(305)555-...	+1(214)555-...	Voice	
08/23/2004 1...	08/23/2004 1...	08/23/2004 1...	0:01:24	OUTBOUND	+1(214)555-...	+1(214)555-...	Fax	

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*.

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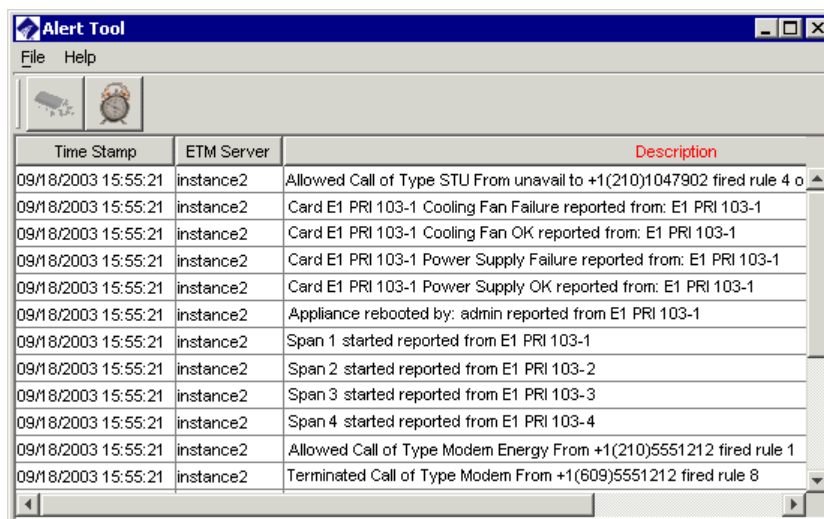
- **Time Stamp**—The date and time an Alert was generated.

- **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 computer-based-training course.

AAA Services for the Voice Firewall

Overview of AAA Services for the Voice Firewall

Authentication, authorization, and accounting are important for effective network management and security. The Voice Firewall improves network management and security by controlling access to the modems and other protected phone numbers on your network. AAA ("Triple A") Services improves on the Voice Firewall by allowing you to further protect the modems and other special-access services on your network so that one or more specific AAA Service Users are allowed temporary access to one or more specific data modems or other services. AAA Service User profiles are stored in the ETM® Database and are used in Policies to allow temporary access to phone numbers that are otherwise restricted.

As illustrated below, before a AAA Service User is allowed to connect to a modem protected by the Voice Firewall, the AAA Service User calls the AAA Server to request authorization. The AAA Server verifies the AAA Service User ID and personal identification number (PIN), and then sends authorization to the Voice Firewall via TCP/IP.

The AAA Server answers only in voice mode; it does not respond to calls as a modem, and it never generates calls.

The Voice Firewall accepts the user-authorization token from the AAA Server and dynamically modifies Policy enforcement to reflect that authorization.

See the *ETM® System Installation and Configuration Guide* for instructions for installing and configuring AAA Services.

After receiving authorization from the AAA Server, the AAA Service User then calls the authorized phone number, as shown in the illustration below. The Voice Firewall provides temporary access for only the approved AAA Service User to call only the authorized phone number. When the user calls the authorized number, the token is consumed and no further calls are allowed unless a new token is authorized. If the AAA Service User does not call the authorized phone number within the time specified in the AAA Service configuration, the authorization expires.
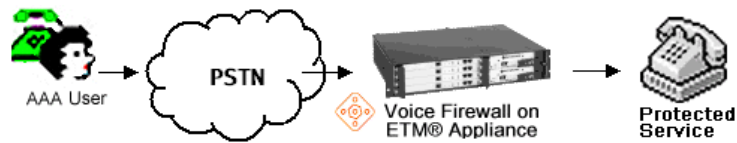
You can configure a Policy to prevent inbound connections to modems on the network without an authorization token from the AAA Service, thereby preventing war dialing attempts. AAA Servers answer calls in voice mode; therefore, they are identified as "voice" by war dialers. AAA Appliances cannot make outbound calls.

Components of AAA Services

AAA Services for the Voice Firewall is comprised of the following software and hardware components:

Software—The AAA Service application facilitates communication between the AAA Server and the Management Server, Performance Manager, and Voice Firewall. The software is provided on the ETM System software CD.

Hardware—The AAA Server is an ETM 1050 Appliance that contains a AAA Card, a 2- or 4-port voice modem card, a serial interface, and a 100baseT Ethernet interface. The AAA Server communicates with the ETM System via TCP/IP. AAA Server communication with other ETM System components may optionally be unencrypted or encrypted with single or Triple DES.

Communication Process

The AAA Server is associated with a specific Switch, and all of the Spans in that Switch are considered "local" to the AAA Server. When a AAA Server generates an authorization token, it sends the token to all of its local Spans and to the Management Server. The Management Server broadcasts the token to all of its Spans. When the authorized user calls the authorized modem or the authorization expires, the Management Server sends a "Cancel Token" message to all of the Spans.

The AAA Server:

- Provides a communication channel to the Management Server and Voice Firewall to send and receive messages.

- Receives validation information from the Management Server, including User IDs and PINs.

- Reports status information to the Management Server, including:

  - Number and status of the modems in the AAA Server.

  - Error conditions, hardware problems, and diagnostic messages (e.g., no modems found; login failure).

- Sends user ID and time-to-live for the authorization token.

The Management Server:

- Provides the AAA Server with a list of its associated Spans, including IP address and passphrase.

- Provides the AAA Server with a list of AAA Service Users and associated PINs, and the expiration date/time of each PIN.

- Distributes tokens from the AAA Server to all of its Spans.

- Broadcasts a "Cancel Token" message to all of the Spans when a token expires or is used by the AAA Service User.

Communication Between the AAA Service and the ETM® System

Illustrated below is an example of an ETM System that uses two geographically dispersed AAA Servers.
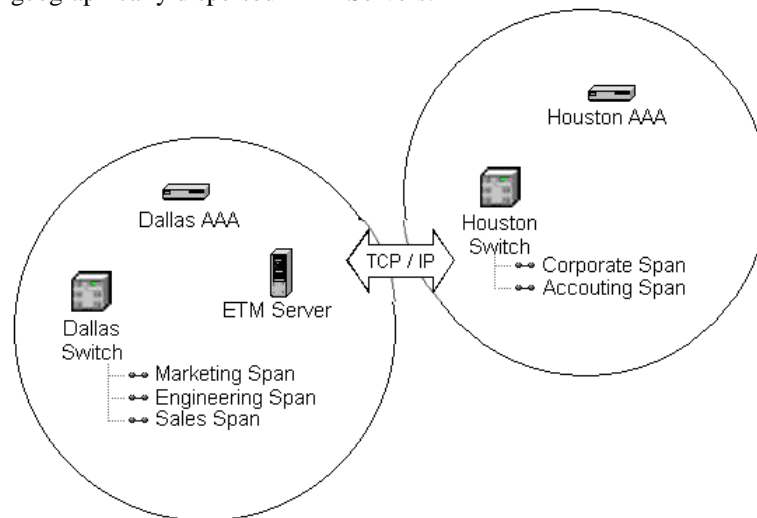
In this example, communication might proceed as follows:

1. The AAA Service User calls the **Houston** AAA Server.

2. The caller is validated.

3. **Houston** AAA sends a token to its local Spans and to the Management Server in Dallas.

4. The Management Server distributes the token to all of its Spans (in both Dallas and Houston).

5. The user places an inbound call that passes through the **Engineering** Span.

6. The **Engineering** Span matches the call to the validation token and allows the call to proceed.

7. The **Engineering** Span notifies the Management Server that the token has been consumed.

8. The Management Server sends a "Cancel Token" message to all Spans.

AAA Service User Example

The following is the general communication process from the perspective of the **AAA Service User**:

1. The **AAA Service User** dials the phone number of a modem in the AAA Appliance.

2. The **AAA Service User** is presented with a welcome message or tone asking for User ID and # (the pound key).

3. The **AAA Service User** enters a user ID, followed by # .

4. The **AAA Service User** is presented with a voice prompt or tone asking for PIN and #.

5. The **AAA Service User** enters a PIN, followed by #.

6. The AAA Server validates the account:

   If validation succeeds

   - The **AAA Service User** is notified via a voice prompt or tone, after which the **AAA Service User** enters the phone number to be accessed (including the country code and area code), followed by #.

   If the PIN has expired:

   - Validation fails, the **AAA Service User** is notified via a voice prompt or tone, and the call is terminated.

   If the number of failed login attempts has been exceeded:

   - Validation fails, the **AAA Service User** is notified via a voice prompt or tone, and the call is terminated.

   If validation fails:

   - The **AAA Service User** is notified via a voice prompt or tone and is again prompted for the User ID and PIN.

7. The **AAA Service User** is presented with a **Goodbye** message or tone.

8. The **AAA Service User** hangs up, and then dials the authorized phone number within the time limit specified in the AAA Service configuration.

If the **AAA Service User** disconnects before the **Goodbye** message or tone, or the session is terminated for any reason, the **AAA Service User** must redial the AAA Server and start the process over.

Managing AAA Users

To use AAA Services, define a **AAA Service User** account for each authorized AAA User. AAA Users are defined in the Performance Manager and stored in the Database. The procedures below describe how to define AAA Users; for instructions for sorting, searching, or filtering the AAA Service Users and Groups in the dialog box, generating a report of AAA Service Users and Groups, or deleting AAA Service Users or Groups, see "Managing Policies" on page 67.

You must have **Access Policy Features** permission to manage AAA Users.

Defining a AAA Service User

To define a AAA Service User

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

2. Right-click in the **AAA Service Users** dialog box, and then click **New | AAA Service User**.

    The **AAA Service User Properties** dialog box appears.

3. Click the **General Info** tab.

a. In the **Name** box, type the AAA User's first and last name.

b. Optionally, in the **Comment** box, type a comment. For example, type:

   ```
   User ID is last 4 digits of Employee's SSN.
   ```

c. In the **User ID Number** box, type 3 to 10 digits that the AAA User will use in combination with the PIN code to gain authorization from the AAA Service. The **User ID Number** must be unique among defined AAA Users. For example, type:

   ```
   1234
   ```

d. In the **Pin Code** and **Confirm Pin Code** boxes, type 3 to 10 digits that the AAA User will use in combination with the User ID Number to gain authorization from the AAA Service. The PIN is displayed as asterisks in the dialog box.

e. When the AAA User account is locked by failed login attempts in excess of the threshold, the **Account Locked box** is selected and the **Expires** box displays the date and time when the account will be unlocked. To unlock the account before the expiration time, an ETM System user with **Access Policy Features** permission can clear the **Account Locked** check box.

4. Click the **Personal Info** tab. All of the boxes on the **Personal Info** tab are optional.

a. In the **Organization** box, type the AAA User's department or organization. For example, type:

```
Engineering
```

b. In the **Home Phone** box, type the AAA User's home telephone number.

c. In the **Work Phone** box, type the AAA User's work telephone number.

d. In the **Pager Number** box, type the AAA User's pager or mobile phone number.

e. In the **Email Address** box, type the AAA User's email address. Email Address must be in the format *<username>@<domain.suffix>*. For example, type:

```
admin@myco.com
```

5. Click **OK**.

The **AAA Service User Properties** dialog box closes and the AAA User is added to the **AAA Service Users** dialog box.

Creating a AAA Service User Group

AAA Service User Groups can group multiple AAA Users who are to be permitted access to the same protected phone numbers to aid in user management. You then can add that single group to Policy Rules, rather than adding multiple individual users. Groups can also be nested inside of other groups.

To create a AAA Service User Group

1. On the Performance Manager main menu, click **Manage | AAA Service Users**.

2. Right-click in the **AAA Service Users** dialog box, and then click **New | Group**. The **AAA Service User Group Properties** dialog box appears.
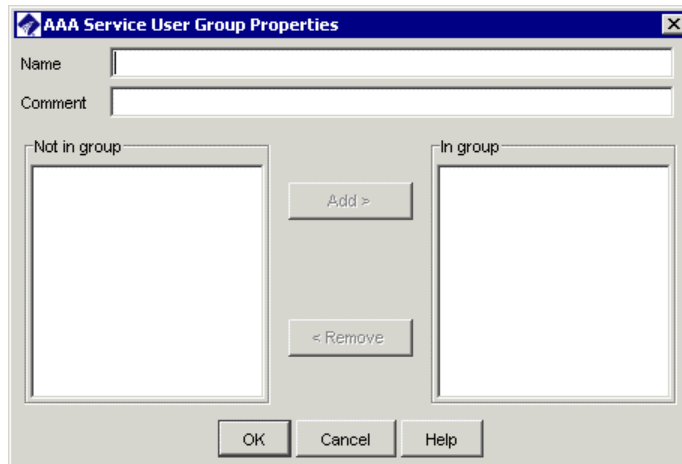
a.   In the **Name** box, type a name that makes the purpose of the group easy to identify.

b.   In the **Comment** box, type a comment (optional). For example, type:

```
Sales Group
```

c.   In the **Not in Group** box, double-click each user or group that you want to add to the new group.

3.   Click **OK**.

Deleting a AAA Service Group or User

An item cannot be deleted if another user has a lock on it or you do not have **Manage Policies** permission. When a AAA Service User Group is deleted, the AAA Service Users contained within it are removed from the Group, but are not deleted from the Management Server.

To delete a AAA Service User or Group

1.   On the Performance Manager main menu, click **Manage | AAA Service Users**.

     The **AAA Service Users** dialog box appears.

2.   Right-click the AAA Service User or Group that you want to delete, and then click **Delete**. (Use Shift or CTRL to select multiple components.) A confirmation dialog box appears.

3.   Click **Yes** to delete the component or click **No** to cancel.
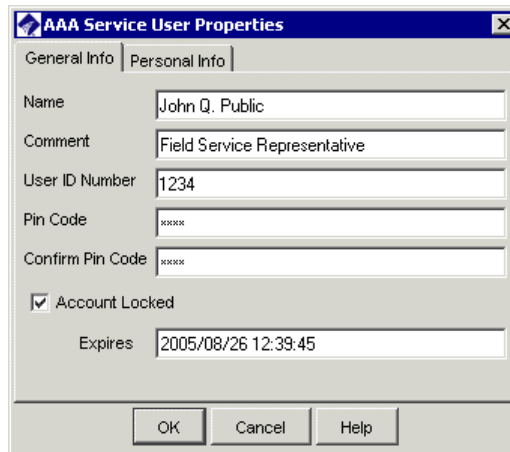
Unlocking a Locked AAA User Account

You must have "Access Policy Features" permission to manage or unlock AAA User accounts.

When a AAA Service User account is locked, the AAA Service User icon in the **AAA Service Users** dialog box turns red 🔴 and the **Account Locked** box in the **AAA Service User Properties** dialog box is selected. The **Expires** box displays the date and time when the account will be automatically unlocked, or **Permanent** if it must be unlocked by an admin account. You can manually unlock the account using the following procedure.

To unlock a AAA Service User account

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

2. Right-click the user whose account you want to unlock, and then click **Edit**.

    The **AAA Service User Properties** dialog box appears.

3. To unlock the account before the expiration time, clear the **Account Locked** box, and then click **OK**. See "Setting AAA Authorization Security Preferences" in the *ETM® System Installation Guide* for information about setting account lockout preferences.

Using AAA Services

Accessing phone numbers protected by AAA Services requires two telephone calls: an initial call to the AAA Server to request authorization, followed by a call to the protected phone number.

During the call to the AAA Server, you are presented with prompts (voice prompts, tones, or silence) to enter your user ID, PIN, and the telephone number for which you are requesting authorization. The AAA Server compares your credentials with its list of authorized AAA Service Users and validates your PIN. A voice message or tone indicates success or failure of the authorization and the call is disconnected. If authorization is successful, an access token is sent to the Management Server and all of the Spans that are local to that AAA Server. The Management Server also sends the token to all of its Spans.

When you enter the phone number for which you want authorization, the AAA Server accepts the phone number exactly as you enter it. However, when the token is sent to the Voice Firewall that is controlling access to that phone number, the Dialing Plan is applied to the phone number before the phone number is compared to the Rule.

Therefore, how you enter the phone number depends on the direction of the call through the Appliance:

- Outbound call—This is the case when the Policy allows only authorized AAA users to make outbound calls to a certain number. (The call is to be made from the Appliance location.) If you are requesting authorization for an outbound destination (as defined in the Rule), and then you enter the destination as if you were dialing the number from the Appliance location, including any long distance or international access codes.

- Inbound call—If you are requesting authorization for an inbound destination (from the point of view of the Appliance), and then you enter the destination as if it were a local number.

  For example, if you wanted authorization to call a modem in the United States from the United Kingdom, dial the AAA Server, and then enter the number as if you were in the United States (i.e., without the country code and area code).

Obtaining Authorization from the AAA Service

For details about configuring AAA Services, see the *ETM® System Installation Guide*.

The following AAA Service parameters are configured by your ETM System administrator:

- Number of rings before the AAA Service answers a call.

- Whether to use voice prompts, tones, or silence.

- Authorization attempts allowed.

- Time allowed for data entry.

- Time to maintain the portal through the Policy.

- Whether the account is to be locked after a set number of failed attempts.

Before calling the AAA Service for authorization, gather the following information:

- Your AAA Service User ID.

- Your PIN.

- The telephone number(s) for the AAA Server.

- The telephone number you want authorization to access.

- The time limit between obtaining the access token and calling the protected phone number. The default is 5 minutes; verify this time limit with your ETM System administrator.

Obtaining an Access Token

If the authorization session is terminated for any reason prior to entering the phone number you want to access, you must redial the AAA Service and restart the process.

To obtain authorization from the AAA Service

1. Dial the telephone number for the AAA Service. You are presented with a voice prompt (welcome message) or silence.

2. You are presented with a voice prompt, tone, or silence requesting your user ID. Enter your user ID, followed by # (the pound key).

3. You are presented with a voice prompt, tone, or silence, requesting your PIN. Enter your PIN, followed by #.

4. You are presented with a voice prompt or silence requesting the telephone number you want to access. Enter the telephone number for which you want authorization, followed by #.

5. You are presented with a **Goodbye** message or silence.

6. Disconnect the call, and then call the phone number for which you obtained authorization within the time limit specified in the AAA Service configuration.

AAA tokens are used in the order in which they are requested and are not tied to a AAA Service User. That is, if two AAA Service Users request a

token to access the same phone number, the first token authorized is the first token consumed, regardless of which AAA Service User requested it.

Viewing Access Tokens

After an access token is sent, but before the token has been used or expired, you can view the token information for any Span on the Management Server in the **ASCII Management Interface**.

To view the access token(s)

For information about ETM® Commands, see "Using ETM® Commands" in the *ETM® System Technical Reference*.

1. Right-click a Span, and then click **ASCII Management**. The **ASCII Management Interface** appears.

2. In the **Enter Command for Span** box, type the following ETM Command, and then press ENTER:

   ```
   SHOW AAA TOKENS
   ```

   The command and the following information appear in the **ASCII Management Interface**:

   - MAC address of the AAA Server.

   - Number (1, 2, 3, or 4) of the modem in the AAA Server that authorized the token.

   - Number of tokens processed by this AAA Service to date.

   - Phone number of the authorized data modem.

   - Expiration time (in GMT) and date of the access token.

   - AAA Service User ID.

   For example:

| Token	Phone number	Expiration	User
0080C6FBDB1A-1-97	[1](319)5551212	204051-08292002	1111

Viewing AAA Service Activity

In the Performance Manager, you can view the status of the AAA Server and AAA Service and view modem activity. In the Usage Manager, you can generate detailed reports of AAA Service activity.

Viewing the Health & Status of the AAA Server

To view the health and status of the AAA Server

- In the **Platform Configuration** subtree, right-click the AAA Card, and then click **Health & Status**. The **ETM System Statistics** dialog box appears.
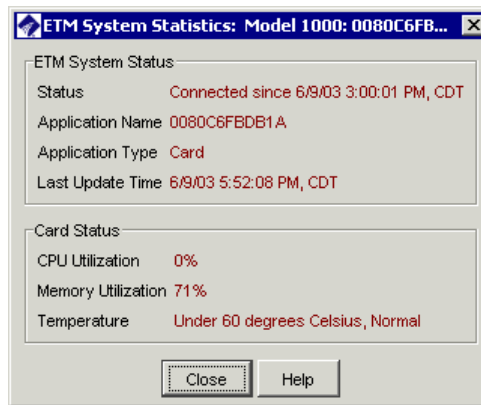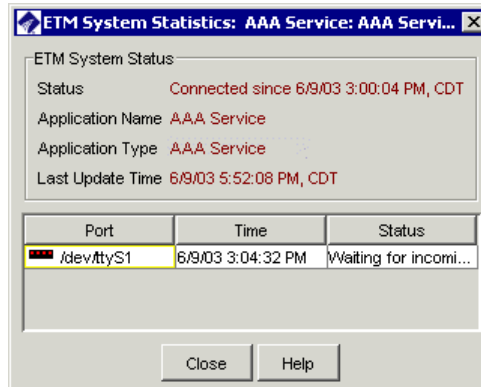

Field	Purpose
Status	Indicates whether the AAA Server is communicating with the Management Server; if connected, displays the date/time the AAA Server connected to the Management Server.
Application Name	User-assigned name or MAC address of the AAA Server.
Application Type	Type of application for which you selected health and status (Card).
Last Update Time	Date/time of the last heartbeat.
CPU Utilization	Utilization percentage for the AAA Server CPU.
Memory Utilization	Utilization percentage of AAA Server memory (RAM).
Disk Utilization	Utilization percentage of AAA Server hard drive.
Temperature	AAA Server temperature.

Viewing Health & Status for the AAA Service

To view AAA Service health and status

- In the **Platform Configuration** subtree, right-click the **AAA Service** icon 🖳, and then click **Health & Status**. The **ETM System Statistics** dialog box appears.

Field	Purpose
Status	Indicates whether the AAA Server is communicating with the Management Server; if connected, displays the date/time the AAA Server connected to the Management Server.
Application Name	Name of the AAA Server.
Application Type	Type of application (AAA Service)
Last Update Time	Displays date/time of the last heartbeat. If never connected, **Not Connected** is displayed.
Modem Information	**Port**—Modem ports used by the AAA Server
	Time—The time the modem was accessed.
	Status—Status of the modem, such as waiting for incoming call, prompting for User ID, sending token, and thanking caller.

AAA Service Diagnostic Logs

The **Diagnostic Log** displays information and system events related to AAA Service operation. This information includes AAA Card connection attempts; name, IP address, and configuration changes; AAA Service login attempts; and AAA Service User and account lockout expiration date changes.

For instructions for viewing the **Diagnostic Log**, see the *ETM® System User Guide*. For instructions for adding Tracks to System Events, see the *ETM® System Administration and Maintenance Guide*.

Some of the system events that apply to the AAA Service include:

- **AAA Service Modem failure**—Occurs if a modem in the AAA Appliance fails to initialize for the AAA Service.

- **AAA User Account Lockout**—Occurs if a user account is locked by the AAA Service (e.g., due to multiple failed login attempts).

- **Extended ETM Application Disconnect Detected**—Occurs if the AAA Server is disconnected from the Management Server for more than a set threshold.

For a complete listing of system events, see "Types of System Events" in *ETM® System User Guide*.

Tracking AAA Service System Events

You can configure a system event to notify you when a AAA Service system event occurs. For example, when an **Email** Track is added to the **AAA Service User Account Locked** system event, an email is sent that contains the date of the system event, type of system event, AAA Service User ID, the name (or MAC address) of the AAA Service, and expiration date of the lockout. If **Permanent** appears in the **Expiration** box, a user with **Access Policy Features** permission must unlock the account. See "Setting AAA Authorization Security Preferences" in the *ETM® System Installation Guide* for information about setting account lockout preferences.

Generating a Report of AAA Service Activity

You can generate reports of AAA Service activity using predefined Report Templates and Report Elements in the Usage Manager.

Predefined Report Templates and Report Elements provide a detailed list of the total number of inbound and outbound authenticated AAA Service User calls. See "Generating a Report" in the *Usage Manager User Guide* for information about generating a report.

# Appendix: Span Settings Related to Firewall Policy Processing

Called/Calling Numbers and Firewall Policy Enforcement

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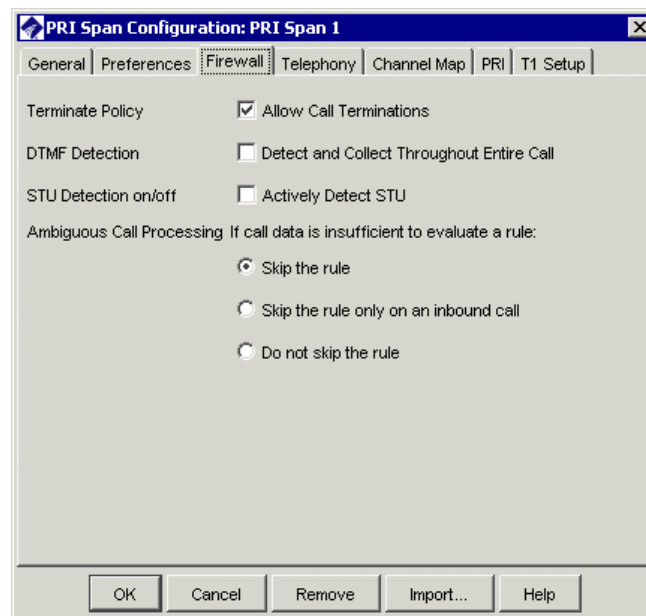
The following table describes the settings on the **Firewall** tab that affect Policy processing.

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	(*Not applicable to VoIP Spans*) 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.
STU Detection	(*Not on VoIP 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	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

(*Not on VoIP Spans*) The Span's telephony settings are configured on the **Telephony** tab of the **Span Configuration** dialog box during installation.

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	Specifies the time after the last digit is dialed before a call is marked as established.
Call Type Timeout	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	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.

The Channel Map

(*Not on VoIP 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.

Channel	Enabled	Request SMDR?	Extension	Signal Type	Trunk Gro
1	☑	On	+1(210)...	Wink	
2	☑	On	+1(210)...	Wink	
3	☑	On	+1(210)...	Wink	
4	☑	On	+1(210)...	Wink	
5	☑	On	+1(210)...	Wink	
6	☑	On	+1(210)...	Wink	
7	☑	On	+1(210)...	Wink	
8	☑	On	+1(210)...	Wink	
9	☑	On	+1(210)...	Wink	
10	☑	On	+1(210)...	Wink	
11	☑	On	+1(210)...	Wink	
12	☑	On	+1(210)...	Wink	
13	☑	On	+1(210)...	Wink	
14	☑	On	+1(210)...	Wink	

T1 Span Configuration: 0030F6020182: T1 Span/Span: 1

General | Preferences | Firewall | Telephony | Channel Map | T1 Setup

OK   Cancel   Remove   Import...   Help

Determining Calling/Called Numbers by Span Type

Accurately determining calling/called numbers is important for enforcement of Policies. The following table describes how 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