SecureLogix®
We see your voice®

# ETM® (Enterprise Telephony Management) System

v7.1.2

## Voice Intrusion Prevention Sysem (IPS) User Guide

DOC-IPS-712-09242018

## About SecureLogix

SecureLogix, a Gartner designated "Cool Vendor" is the leader in enterprise voice/UC policy enforcement and ROI intelligence. SecureLogix 7th generation solutions enable customers to save money through securing and optimizing IP Telephony and legacy voice networks, allowing cost efficient and confident migration to SIP Trunking and Unified Communications. SecureLogix solutions are currently protecting and managing over three-and-a-half million enterprise phone lines.

The highly patented SecureLogix® ETM® System helps to secure, optimize and simplify the management of complex enterprise voice/UC networks through enterprise-wide voice network intelligence and unified policy enforcement. Available as an appliance-based solution or deployed via a software-only model running on the Cisco Enterprise router family, the ETM System enables a hard-dollar ROI payback in less than 12 months by securing the enterprise from attack, fraud, data leakage, financial losses and service abuse over TDM and VoIP (SIP) enterprise phone lines, while optimizing voice service and infrastructure expenses.

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


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

**Sales:**
Telephone: 1-800-817-4837 (North America)
Email: *sales@securelogix.com*

**Customer Support:**
Telephone: 1-877-SLC-4HELP
Email: *support@securelogix.com*
Web Page: *http://support.securelogix.com*

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

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

**IMPORTANT NOTICE:**

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

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

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

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



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

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

This product includes:

Data Encryption Standard software developed by Eric Young (eay@mincom.oz.au),
© Copyright 1995 Eric Young. All Rights Reserved.
(See DESLicense.txt on ETM software CD)

Style Report software owned and licensed exclusively by InetSoft Technology Corp.
© Copyright 1996-2000 InetSoft Technology Corp. All Rights Reserved.

Software developed by The Apache Software Foundation (http://www.apache.org/)
© Copyright 2000 The Apache Software Foundation. All Rights Reserved.
(See ApacheLicense.txt on ETM software CD.)

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

GNU C Library software; Distributed pursuant to the Library General Public License (LGPL). See the Open Source Code Directory on the ETM software CD for related copyrights, licenses, and source code.

# Customer Support
# for Your ETM® System

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

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

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

# Contents

# Preface

## About the ETM® System Documentation

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

### ETM® System User Guides

The following set of guides is provided for the ETM® System:

*ETM® System User Guide*—Explains ETM System Concepts and provides task-oriented instructions for using the ETM System, including a Quick Start.

*ETM® System Installation Guides*—Provide task-oriented installation and configuration instructions and explanations for technicians performing system setup. This set of guides includes a primary system installation guide and separate guides for the Unified Trunk Application (UTA), SRE-V, and inline SIP application installation, and for database preparation.

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

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

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

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

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

*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.)

## Additional Documentation on the Web

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

*http://support.securelogix.com*

## Tell Us What You Think

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

*docs@securelogix.com*

## Conventions Used in This Guide

The following conventions are used in this guide:

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

  Click **View | Implied Rules**.

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

  Highlight the field and press DELETE.

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

  Press CTRL+ALT+DELETE.

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

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

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

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

  In the **Name** box, type: `My report tutorial`
- Italics indicate web addresses and names of publications.
- ETM System components and features are capitalized.

# The ETM® Voice Intrusion Prevention System (IPS)

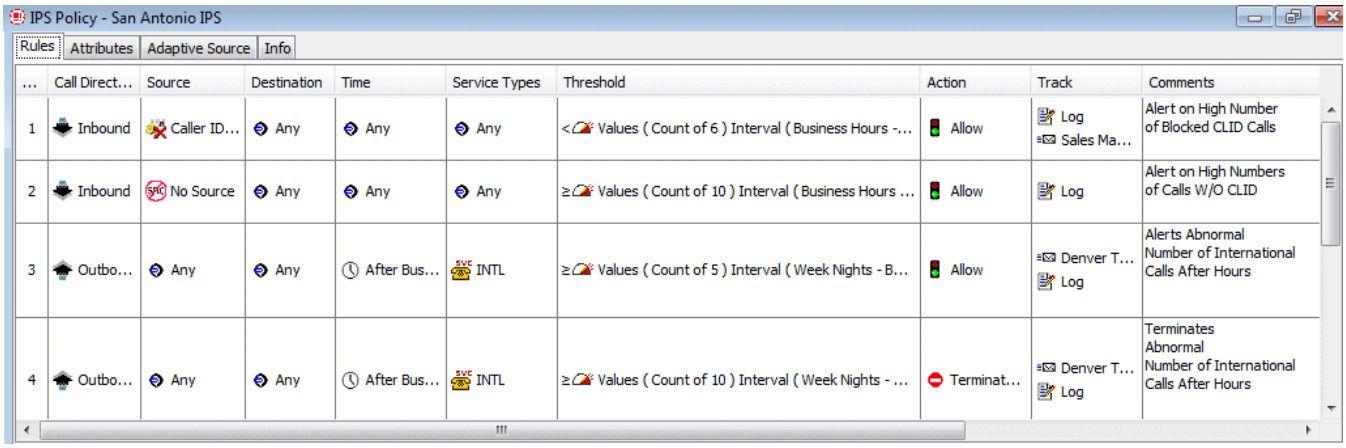
## Using Voice IPS Policies

ETM® Voice Intrusion Prevention System (IPS) Policies enable you to use rule-based Policies to manage usage of your telecom resources and protect your network against potential intrusion attempts, based on calling pattern *Thresholds* over a specified *Interval*. Thresholds can be based on accumulated cost, count, or duration of calls that match the other criteria in the Rule. For each Voice IPS Policy Rule, you prescribe one or more Thresholds and dictate an action to occur when these Thresholds are breached: *allow* the call that breached the Rule, *allow the calls that breached the Rule but prevent future calls* that match the Rule, or *terminate ongoing matching calls and prevent future calls* that match the Rule. By default, a Rule is *breached* when the accumulated value(s) is/are greater than or equal to **≥** the specified Threshold(s). If you prefer, you can change this to less than **<**.

Note that IPS Policies do not manage individual calls; rather, they manage *accumulations over time* of duration, cost, or count. For example:

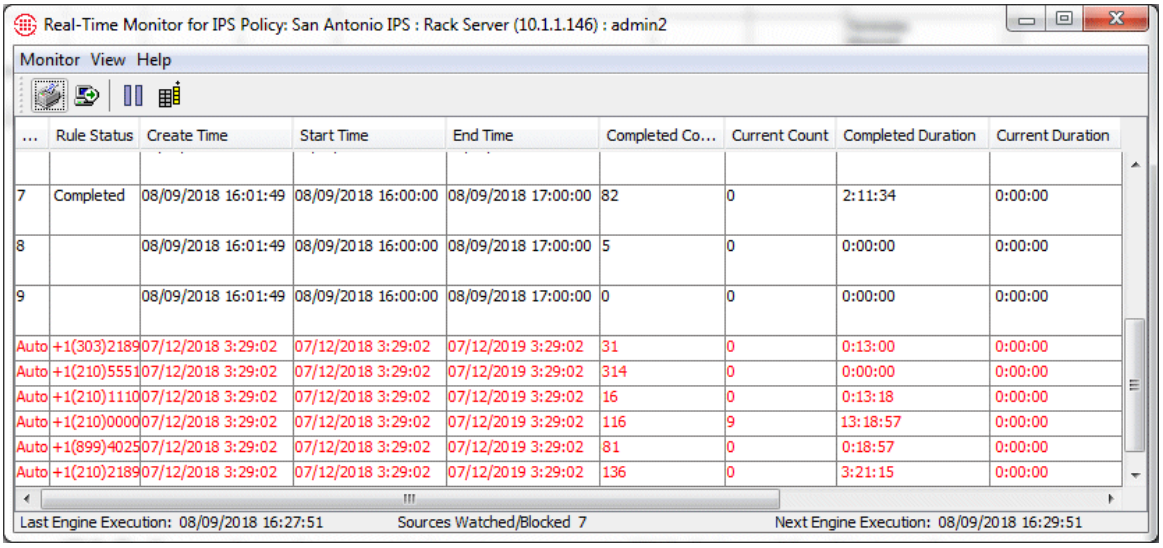
- You may want to be notified when the total cost of International calls during the week exceeds a certain Threshold. You can write a Rule that will send you an email notification if this cost Threshold is exceeded so you can evaluate the reason for it.
- Perhaps a certain number of International calls during business hours is common for your business; however, an excessive number of calls to certain regions or after hours international calls to any locale may indicate toll fraud. You can write Rules to track International calling patterns based on destination or Service Type and prevent future calls above that set Threshold, thereby limiting your financial exposure to toll fraud.

The illustration below is an example of a Voice IPS Policy.




| ... | Call Direct... | Source | Destination | Time | Service Types | Threshold | Action | Track | Comments |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Inbound | Caller ID... | Any | Any | Any | < Values ( Count of 6 ) Interval ( Business Hours -... | Allow | Log<br>Sales Ma... | Alert on High Number of Blocked CLID Calls |
| 2 | Inbound | No Source | Any | Any | Any | ≥ Values ( Count of 10 ) Interval ( Business Hours ... | Allow | Log | Alert on High Numbers of Calls W/O CLID |
| 3 | Outbo... | Any | Any | After Bus... | INTL | ≥ Values ( Count of 5 ) Interval ( Week Nights - B... | Allow | Denver T...<br>Log | Alerts Abnormal Number of International Calls After Hours |
| 4 | Outbo... | Any | Any | After Bus... | INTL | ≥ Values ( Count of 10 ) Interval ( Week Nights - ... | Terminat... | Denver T...<br>Log | Terminates Abnormal Number of International Calls After Hours |

The IPS Policy **Real-Time Monitor** allows you to monitor accumulations and be aware when Thresholds are likely to be breached or have been breached.




| ... | Rule Status | Create Time | Start Time | End Time | Completed Co... | Current Count | Completed Duration | Current Duration |
|---|---|---|---|---|---|---|---|---|
| 7 | Completed | 08/09/2018 16:01:49 | 08/09/2018 16:00:00 | 08/09/2018 17:00:00 | 82 | 0 | 2:11:34 | 0:00:00 |
| 8 | | 08/09/2018 16:01:49 | 08/09/2018 16:00:00 | 08/09/2018 17:00:00 | 5 | 0 | 0:00:00 | 0:00:00 |
| 9 | | 08/09/2018 16:01:49 | 08/09/2018 16:00:00 | 08/09/2018 17:00:00 | 0 | 0 | 0:00:00 | 0:00:00 |
| Auto | +1(303)2189 | 07/12/2018 3:29:02 | 07/12/2018 3:29:02 | 07/12/2019 3:29:02 | 31 | 0 | 0:13:00 | 0:00:00 |
| Auto | +1(210)5551 | 07/12/2018 3:29:02 | 07/12/2018 3:29:02 | 07/12/2019 3:29:02 | 314 | 0 | 0:00:00 | 0:00:00 |
| Auto | +1(210)1110 | 07/12/2018 3:29:02 | 07/12/2018 3:29:02 | 07/12/2019 3:29:02 | 16 | 0 | 0:13:18 | 0:00:00 |
| Auto | +1(210)0000 | 07/12/2018 3:29:02 | 07/12/2018 3:29:02 | 07/12/2019 3:29:02 | 116 | 9 | 13:18:57 | 0:00:00 |
| Auto | +1(899)4025 | 07/12/2018 3:29:02 | 07/12/2018 3:29:02 | 07/12/2019 3:29:02 | 81 | 0 | 0:18:57 | 0:00:00 |
| Auto | +1(210)2189 | 07/12/2018 3:29:02 | 07/12/2018 3:29:02 | 07/12/2019 3:29:02 | 136 | 0 | 3:21:15 | 0:00:00 |

## Voice IPS Policy User Permissions

Several user permissions govern access to IPS Policies and the objects used in them.

- Since Policies are managed from within the Performance Manager, you must have **Access Performance Manager** permission to view or edit IPS Policies or the objects used in them.
- The ability to edit objects used in Policies (Intervals, Tracks, Contacts, Billing Plans, Service Types, Times, Durations, and Span Groups) is governed by the **Access Policy Features** user permission, which

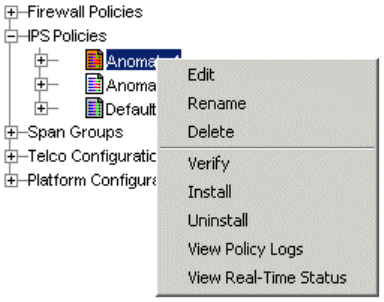
must be granted before any other Policy permissions can be granted. Users who do not have **Access Policy Features** permission can view lists of and print Reports of the items used in Policies, but cannot create or modify them. They cannot see the Policy subtrees in the Performance Manager tree pane or on the **View** menu.

- Two options control the level of access to Voice IPS Policy functions: **View & Reinstall IPS Policies** and **Full Control**.
  - **View & Reinstall IPS Policies** enables you to view the **IPS Policies** subtree, open any Voice IPS Policy, and reinstall **IPS Policies** that are already installed (for example, to update the Policy on the Span Group when Listings used in the Policy change).
  - To create, edit, delete, or uninstall any Policy, or install a Policy other than the one currently installed on a Span Group, you must also have the **Full Control** permission for IPS Policies.

## IPS Policies Subtree

The **IPS Policies** subtree provides management options for IPS Policies. By right-clicking the **IPS Policies** subtree, you can create a new Policy and show or hide the default Policy node of the **IPS Policies** subtree.

Right-clicking a Policy in the tree provides a menu of editing, installation, and status-viewing options:




When a Rule in a Voice IPS Policy is breached, the icon for that Policy turns red.

## Voice IPS Policy Fields

Calls can be included in the accumulations based on any combination of the following criteria:

**Call Direction**—Used to apply only inbound or only outbound calls to the accumulation, or specify **Any** to apply calls in either direction to the accumulated values.

**Source**—Used to specify one or more specific sources from which call accumulations apply, or specify **Any** to apply calls from all sources to the accumulated values. You can specify one or more of the following sources: Directory entities (Listings, Groups, Ranges, Filters, or Wildcards), Subnets, Caller ID restricted calls, or No Source.

**Destination**—Specify one or more specific destinations to which call accumulations apply, or specify **Any** to apply calls to all destinations to the accumulated values. You can specify one or more of the following destinations: Directory entities (Listings, Groups, Ranges, Filters, or Wildcards) or Subnets.

**Note**: See "Call Types Detected by the ETM System" in the *ETM® System User Guide* for a description of each call type. Some call types only apply to certain types of Spans.

**Call Type**—Used to apply only calls of one or more types to the accumulated values, or specify **Any** to include calls of any type in the accumulated values. You can specify one or more of the following: Busy, Data Call, Fax, Modem Energy, Modem, STU, Unanswered, Undetermined, Video, or Voice. For example, to be notified when the count of modem calls terminated by the Voice Firewall exceeds a set Threshold, you specify **Modem** in the **Call Type** field and **Terminated by Firewall** in the **Disposition** field, and then set the count Threshold in the **Threshold** field to the limit you want.

**Time**—Used to limit the time when calls are to be applied to the accumulation, or specify **Any** to apply calls at any time to which the specified Interval applies. You can also negate the **Time** field so that only calls at times other than those specified are counted. For example, suppose you want to use an Interval of 8 AM to 5 PM, but you do not want the calls during the lunch hour to count against the Threshold. Apply that Interval in the **Threshold** field, define a time object for 12–1pm and place it in the **Time** field, and then negate the **Time** field.

**Service Types**—Used to specify one or more Service Types or Service Type Groups to track (e.g., local, long distance, international). **Any** includes all Service Types. You can also negate the **Service Type** field, which means that only Service Types other than those specified are counted. For example, if you want to track all non-local calls, you can place a Service Type containing **LOC** in the field, and then negate the field.

**Disposition**—Used to track accumulations of terminated calls according to terminator (Firewall, User, IPS). For example, you may want to track how many modem calls your Voice Firewall Policy is terminating and be alerted if the count exceeds a specified value in a given period of time. **Any** means all calls, whether terminated or not.

**Call Duration**—Used to specify that only calls greater than or equal to **≥** or less than **<** a given length are to be counted toward the accumulation. For example, you may want to establish a count Threshold for long-duration calls that may be associated with toll fraud or short duration calls that may indicate war dialing. You would specify a Duration in the **Call Duration** field and then specify the count in the **Threshold** field. Note that you cannot terminate calls based on a less-than duration, since it cannot be determined whether the call is less than a given duration until the call ends.

**Attributes**— Used to track patterns of midcall DTMF digits or lack of expected midcall DTMF digits.

**Threshold**—Defines the time Interval over which values are accumulated and the values and units against which the accumulations (count, cost, or duration) are measured. You must define this field before the Policy can be installed. You must select an Interval and specify at least one value/unit.

By default, the Rule is breached when the accumulated value(s) is/are greater than or equal to **≥** the specified Threshold(s). If you prefer, you can change this to less than **<**.

For example, if you expect your outbound marketing team to make a certain number of calls in a week, you can define a Rule to notify you if the total count is less than the defined quota. Note that you cannot terminate calls based on a less-than Threshold, since it cannot be determined whether the cumulative value is less than the Threshold until the Interval ends.

**Action**—Determines what happens to calls when the Threshold is breached:

- **Allow**—Allow calls that match the Rule when the Rule is breached.
- **Terminate future**—Allow active calls that match the Rule when the Rule is breached, but terminate subsequent matching calls for the duration of the Interval. (*Not valid with less- than duration or Thresholds, or with a* ***Disposition*** *other than* ***Any***.) Note that termination does not begin until the next time the polling engine runs.
- **Terminate current and future**—Terminate active calls that match the Rule when it is breached, and prevent subsequent calls that match during the remainder of the Interval. (*Not valid with less-than duration or Thresholds, or with a* ***Disposition*** *other than* ***Any***.)

**Track**—Used to specify one or more tracks (email, SNMP, Syslog, real-time alert) that are to occur if the Rule is breached. All Rules are logged in the **Voice IPS Policy Log** after each Interval ends.

**Comment**—An optional field for providing information regarding the intent of the Rule. In IPS Policies, it is strongly recommended that you use the **Comment** field, because it is invaluable in report generation.

## Thresholds

Thresholds provide the contiguous time Interval during which Voice IPS Policy accumulations are to be monitored and the values and units against which the accumulations (count, duration, or cost) are measured. When you add a Rule to a Voice IPS Policy, the Threshold field is uninitialized. You must initialize the Threshold before the Policy passes verification. If you specify more than one value/unit pair, the Rule fires when the first Threshold is exceeded and does not track subsequent breaches of other Thresholds.

### *Establishing Realistic Thresholds*

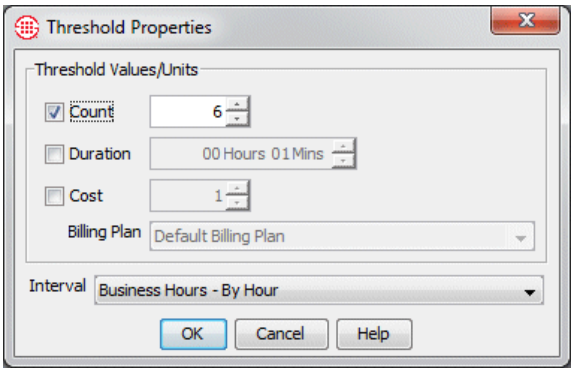
To determine appropriate Thresholds for Rules, it is recommended that you run a series of baseline Reports in the Usage Manager to establish normal operating Thresholds for the type of call patterns to be monitored. Several default Reports are provided as examples that you can tailor for your enterprise. See "Voice IPS Policy Reports" on page 55 for more information.

For example, if you want to base a Rule on the count of a specific category of call for a given time period, such as outbound International calls during business hours, you can run a Report to provide the minimum, maximum, and average call counts by business hours for that category of call. Similarly, you can run billing Reports to establish the normal cost of various categories of calls during various times, such as after hours and weekends, or the typical aggregate duration of a class of call, such as outbound International calls.

### *Defining a Threshold for a Rule*

**To define a Threshold**

1. In a Voice IPS Policy, right-click in the **Threshold** field, and then click **Edit**. The **Threshold Properties** dialog box appears.




2. In the **Threshold Values/Units** area, select one of the following units and assign values to the selected units:

**IMPORTANT** While you can specify more than one Threshold criterion, but the Rule fires only when the first Threshold is breached. It fires only once in an Interval.

**Count**—The number of calls. Valid values are 1–999,999.

**Duration**—Call length. Valid values are 1 minute–999,999 hours.

**Cost**—A whole dollar amount of the accumulated cost allowed during the Interval. In the **Billing Plan** box, click the down arrow and select the Billing Plan to be used to calculate the cost. See "Billing Plans" in *ETM® System User Guide* for instructions for defining billing plans.

**IMPORTANT** While you can specify more than one Threshold criterion, but the Rule fires only when the first Threshold is breached. It fires only once in an Interval. You should create separate Rules for different threshold criteria instead.

3. In the **Interval** field, click the down arrow, and then click the time Interval to use for this Rule. Intervals can be a maximum of 1 week. See "Intervals" on page 17 for a discussion of intervals and instructions for defining them.
4. Click **OK**. The Threshold is added to the Rule.
5. By default, the Rule is breached when the accumulated value(s) is/are greater than or equal to ≥ the specified Threshold(s). If you prefer, you can change this to less than **<**.
    - To change the setting to less than, right-click in the **Threshold** field, and then click **<**.

## Intervals

*Intervals* are used in IPS Policies to define a contiguous range of time over which a Voice IPS Threshold is monitored. The maximum period an Interval can cover is one week. Two types of Intervals are available: *week* or *day*. You can also divide each week or day Interval by hour, into hour subintervals.

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

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

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

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

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

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

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

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

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

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

- **Subintervals—Daily and Weekly Intervals can be devided into Hourly or 15-Minute Subintervals:**
  - **Hourly subinterval**—Day and Week Intervals can be divided into Hourly Subintervals. An Hourly Subinterval must start at the top of an hour and last the full hour. For example:

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

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

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

- **15-Minute Subintervals**—15-Minute Subintervals devide each day of the time period you selected into 15-minute units.

Intervals are calculated based on the Span's time zone, not the Management Server's. Therefore, if the Span and the Management Server are in different time zones, your Policy may not function as expected. Also, all Spans in a Span Group on which a Voice IPS Policy is installed must be in the same time zone.

If you modify an Interval that is used by an installed Policy, a message appears informing you of the affected Policies and a "dirty Policy" indicator  appears in the tree next to the affected Policy. You must reinstall the Policy before the change takes effect on the Spans. When you reinstall the Policy, the Rule is cancelled for the current Interval and the accumulation counters are reset.

## *Predefined Intervals*

A number of predefined Intervals are provided with your ETM System. These Intervals are used in some predefined Reports and can be used in IPS Policies. The following predefined Intervals are included:

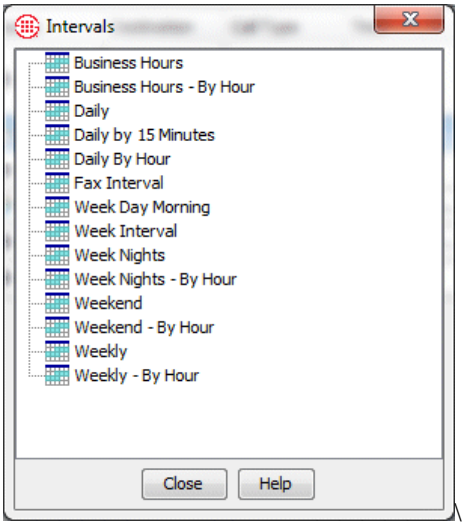
| | |
|---|---|
| Business Hours | 8:00 AM -5:00 PM Mon–Fri |
| Business Hours, By Hour | Business Hours with hourly subintervals |
| Daily | 12 AM - 12AM Sun-Mon |
| Week Nights | 5:00 PM - 8:00 AM M-Th |
| Week Nights, By Hour | Week Nights with hourly subintervals |
| Weekend | 5:00 PM Friday - 8:00 AM Monday |
| Weekend, By Hour | Weekend with hourly subintervals |
| Weekly | 12:00 AM Monday - 11:59 PM Sunday |
| Weekly, By Hour | Weekly with hourly subintervals |

## *Defining an Interval*

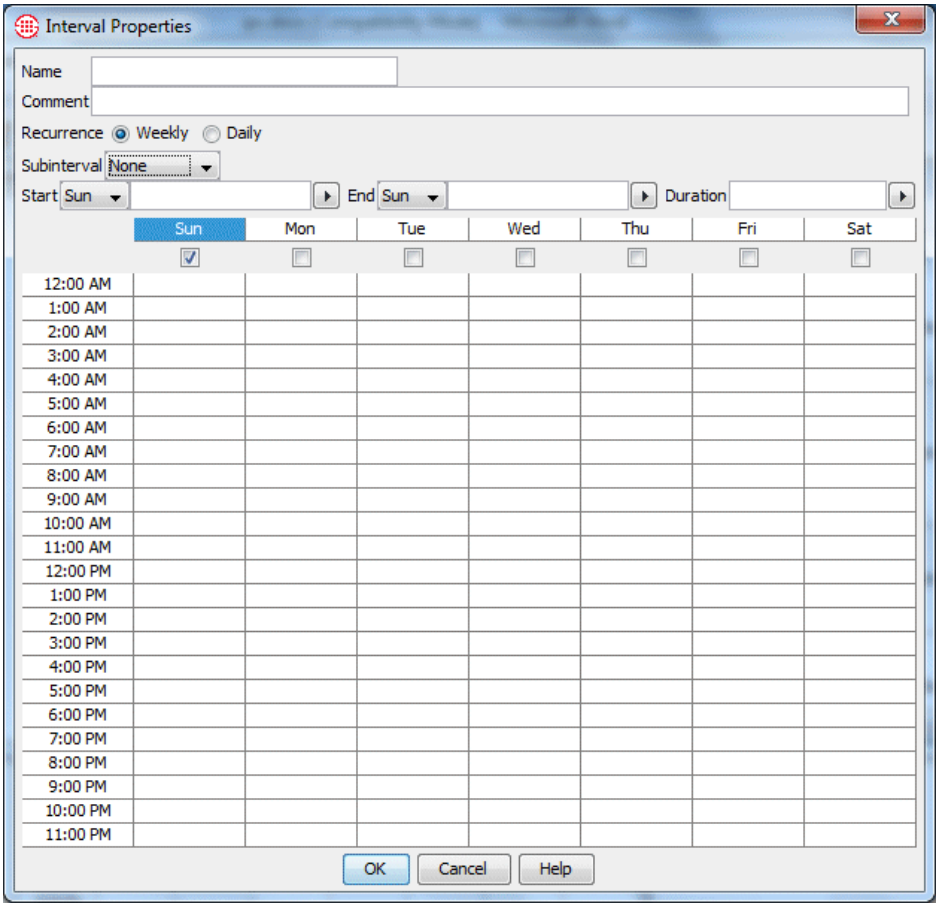
### To define an Interval

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

**Note**: See the *ETM*® *System User Guide* for more details about defining Intervals.




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



3. In the **Name** box, type a unique identifier for this Interval.
4. Optionally, in the **Comment** box, type a comment to provide information about the Interval. Comments are for user convenience and are not used by the ETM System.
5. Do one of the following, according to the type of Interval you are defining:

**Note**: To specify minutes, you must type the time in the **Start** or **End** box. When you click the graphic, the whole hour is selected.

**Week Interval**—The time in a week Interval must be contiguous and can be specified to the minute.

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

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

- In the **Start** and **End** boxes, select the day of the week and the time of day on which the Interval is to start and end. The graphic area and the **Duration** box automatically update to match the selected days and times.
- Select the checkbox below the day of the week on which the Interval is to start, and then type or select the duration in the **Duration** box. The graphic, **Start**, and **End** boxes automatically update to reflect the selection.
- In the graphic area, click in the cell for the time and day at which the Interval is to start, and then hold down the left mouse button and drag your cursor to the cell representing the hour and day at which the Interval is to end. The **Start**, **End**, and **Duration** boxes update to reflect the selection.

c. To specify hourlyor 15-minute subintervals of the Interval you selected, select the **Subinterval** down arrow and click **Hour** or **15 Minutes**. Note that if you have specified the start or end time in minutes rather than the top of an hour, when you select **Hour subinterval**, the start and end times reset to the top of the displayed hour (that is, a start time of 1:45 becomes 1:00). This is because hourly subintervals represent one whole hour from the top of the hour.

**Day Interval**—The time in a Day Interval must be the same on all days and can be specified to the minute.

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

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

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

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

**Tip:** You can hold down CTRL or SHIFT and click the names of the days to select multiple days.

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

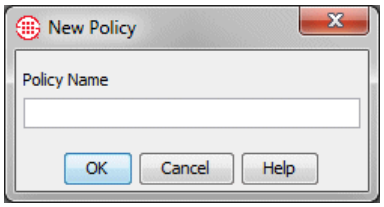
c. To specify hourly or 15-minute subintervals of the Interval you selected, click the Subintervals down arrow and click **Hourly or 15 Minutes**. Note that if you have specified the start or end time in minutes rather than the top of an hour, when you select **Hour subinterval**, the start and end times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

## Defining a Voice IPS Policy

### To define a Voice IPS Policy

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

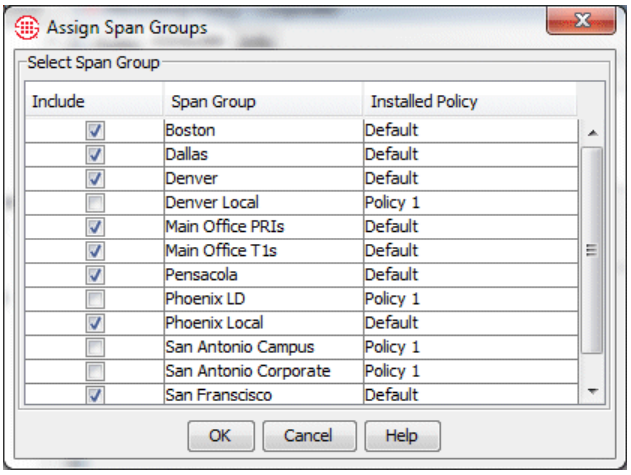
   The **New Policy** dialog box appears.




**Note**: All Spans assigned to a given Voice IPS Policy must be in the same time zone, because intervals are calculated based on the Span's time zone.

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

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

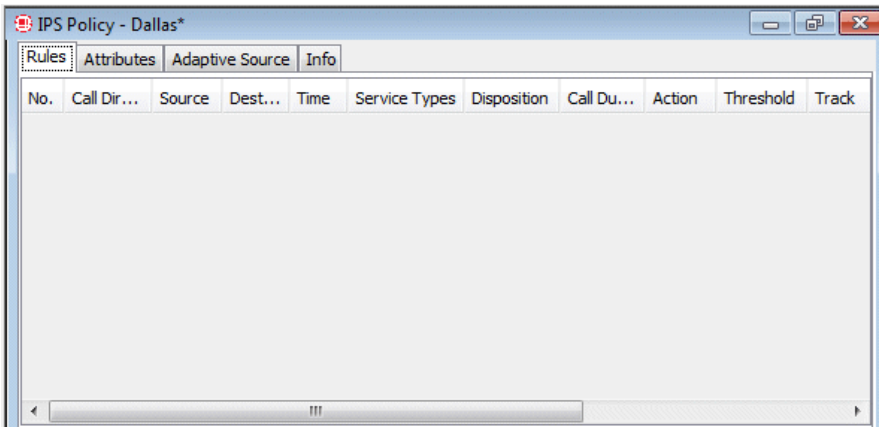



3. In the **Include** column, select the check boxes for Span Groups on which you want to install the Policy; clear the check boxes for any Span Groups on which you do not want to install the Policy. By default, all Span Groups on which the default Policy is currently installed are selected.

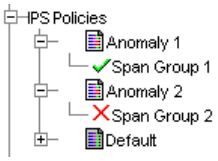
   - If one or more of the Span Groups on which you want to install this Policy are not yet defined, you can add them later using the **Attributes** tab of the **IPS Policy** editor.
   - If no Span Groups on which you want to install the Policy have been defined, simply clear any check boxes you see. (If no Span Groups exist, no check boxes appear.) You can add the applicable Span Groups later using the **Attributes** tab of the **IPS Policy** editor.

4. Click **OK**.

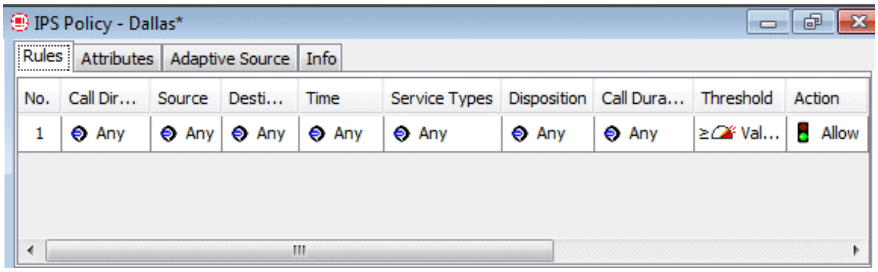
   The **IPS Policy** appears in the Policy editor pane. The asterisk in the title bar indicates it has not yet been saved. New Policies do not appear in the tree pane until they are saved.



5. On the Performance Manager main menu, click **File | Save**. The new Policy appears in the **IPS Policies** subtree. The red **X** next to the Span Group name indicates the Policy is not installed.




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




7. Define the fields as needed. The **Thresholds** field is required. To add values to the fields:

   - **Call Direction**—Right-click in the field, and then click **Inbound** or **Outbound**.
   - **Source**—Right-click in the field and click **Add**, and then click the type of source you want to add: Listings, Filters, Groups, Ranges, Wildcards, Subnets, Caller ID Restricted, or No Source. You can add multiple sources of different types if needed.
     - If you click **Filters**, **Groups**, **Ranges**, **Wildcards**, or **Subnets**, a dialog box appears containing the selected type of object. Click the item(s) you want to add, and then click **OK**.
     - If you click **Caller ID Restricted**, it is added to the Rule. **Caller ID Restricted** applies to calls for which the caller has blocked transmission of Caller ID. 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.
     - If you click **No Source**, it is added to the Rule. **No Source** applies to calls for which the source is unavailable 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.
     - If you click **Listings**, the **Listing Search** dialog box appears. Search for the listing(s), and then select them in the

**Tip**: To select multiple items, hold down CTRL and click each item.

**Results** window, and then click **Add**. See "Searching for Listings" in the *ETM® System User Guide* for instructions for using a simple or advanced search to locate listings.

- **Destination**—Right-click in the field, and then click **Add**, and then click the type of destination you want to add: Listings, Filters, Groups, Ranges, Wildcards, or Subnets.

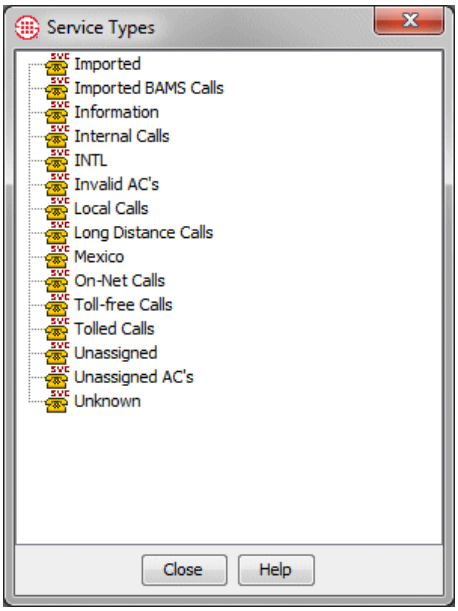
  **Tip**: To select multiple items, hold down CTRL and click each item.

  - If you click **Filters**, **Groups**, **Ranges**, **Wildcards**, or **Subnets**, a dialog box appears containing the selected type of object. Click the item(s )you want to add, and then click **OK**.
  - If you click **Listings**, the **Listing Search** dialog box appears. Search for the listing(s), and then select them in the **Results** window, and then click **Add**. See "Searching for Listings" in the *ETM® System User Guide* for instructions for using a simple or advanced search to locate listings.

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

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

- **Service Types**—Right-click in the field, and then click **Add**. The **Service Types** dialog box appears.




- Click one or more Service Types to add to the Rule, and then click **OK**. See "Service Types" in the *ETM® System User Guide* for instructions for defining Service Types.
- To negate the Service Type so that the Rule applies to all Service Types other than those specified, after adding a Service Type, right-click in the field, and then click **Negate**.

- **Dispositions**—Right-click in the field, and then click **Add**. The **Dispositions** dialog box appears. Click one or more termination dispositions, and then click **OK**.
- **Call Duration**—Right-click in the field, and then click **Add**. The **Durations** dialog box appears. Click a duration, and then click **OK**. By default, the Duration represents greater than or equal to. To denote calls less than the specified Duration, after adding a Duration, right-click again and select **<** (less than).
- **Attributes**—Attributes for IPS Policies include:

  **No DTMF**—Used to detect a pattern of calls with no mid-call DTMF digits, to track calls where DTMF digits are expected mid-call, such as calls to IVRs.

  a. Right-click in the field, and then click **Add**. The **Attributes** dialog box appears.

  b. Click **No DTMF**, and then click **OK**.

  **DTMF Pattern**—Used to detect a pattern of calls dialing a certain patterns of DTMF digits that might be indicative of malicious activity. Interdigit timing is stored in the database for offline analysis.

a. Right-click in the field, and then click **Add**. The **Attributes** dialog box appears.

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

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

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

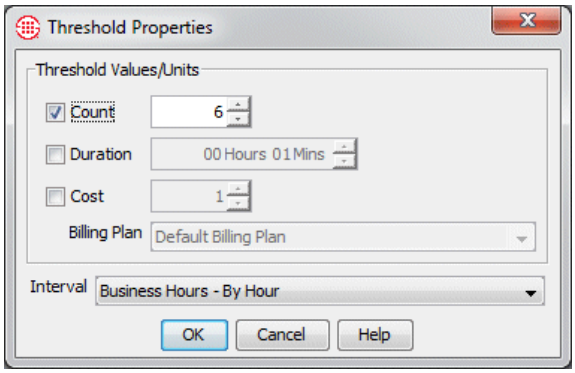
iii. In the **DTMF Pattern** box, type the pattern to be detected. For example, you might type:
`1 8 3 1 8 3`.

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

v. Click **OK** to add it to the policy.

- **Threshold**—You must define the **Threshold** field before the Policy can be installed. (If the Policy is not currently installed, it can be saved before you define the Threshold; however, if it is already installed, it cannot be saved without also being installed.)

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




c. In the **Threshold Values/Units** area, select one of the following and type values for the selected item.

**IMPORTANT**
Although you can specify more than Threshold, the Rule fires only when the first Threshold is breached. It is recommended you use different Rules for different Thresholds.

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

**Duration**—To set a Threshold based on the cumulative duration of calls that match the Rule, select **Duration**, and then type or select the duration in hours and minutes. Duration is always counted from call connect time, not start time.

**Cost**—To set a Threshold for the cost of calls that match the Rule, select **Cost**, and then select the billing plan to use to calculate the cost. See "Billing Plans" in the *ETM® System User Guide* for instructions for defining billing plans.

It is recommended that you create separate Rules if you need to track different values, since the Rule will fire only when the first Threshold is breached..

d. In the **Interval** box, click the down arrow and select the time Interval over which the accumulations are to be tracked. See "Intervals" on page 17 for instructions for defining intervals.

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

f. By default, the Rule is breached when the accumulated value(s) is/are greater than or equal to ≥ the specified Threshold(s). If you prefer, you can change this to less than **<**.

- **Action**—Right-click in the field, and then click one of the following:

  **Allow**—Allow calls that match the Rule when the Rule is breached.

  **Terminate future**—Allow active calls that match the Rule when the Rule is breached, but terminate subsequent matching calls for the duration of the Interval. Note that termination does not begin until the next time the polling engine executes. *(Not valid with less-than Durations or Intervals, or with a value other than **Any** in the **Disposition** field.)*

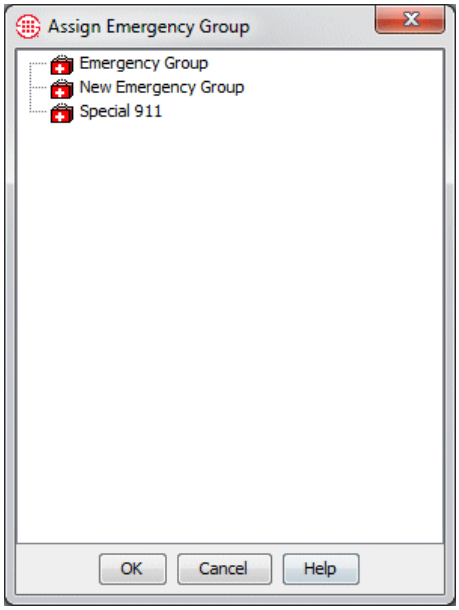
  **Terminate current and future**—Terminate active calls that match the Rule when it is breached, and prevent subsequent calls that match during the remainder of the Interval. *(Not valid with less-than Durations or Intervals, or with a value other than **Any** in the **Disposition** field.)*

**IMPORTANT** Calls can only be terminated on a specific Span if its **Allow Call Terminations** setting is enabled. Note that calls originating from Spans with this setting disabled are included in accumulated values, which may lead to the final actual accumulation value being greater than the user-defined Threshold value.

- **Track**—Right-click in the field, and then click **Add**. The **Tracks** dialog box appears. Click one or more Tracks (Email, SNMP, Realtime Alert) that are to occur if the Rule is breached. All breached Rules are logged in the **Voice IPS Policy Log**.

- **Comment**—Right-click in the field, and then click **Edit**, and then type any comment, and then click **OK**. It is recommended that you use comments in IPS Rules, becasue are very useful for tracking the intent of a Rule and appear in logs and alerts and can appear in Reports.

8. Repeat steps 6 and 7 for each Rule in the Policy.
9. Click the **Attributes** tab. By default, each Voice IPS Policy contains the default Emergency Group for the Management Server locale, which contains the national emergency number. It is strongly recommended that you define an Emergency Group that includes local emergency numbers specific to the appliance locale where the Policy is to be installed, in addition to the national emergency number, and then assign it to the Policy. If such a group has not yet been defined, see "Defining a New Emergency Group" in the *ETM® System User Guide* for instructions. This prevents calls to numbers in the Emergency Group from ever being terminated by a Voice IPS Policy Rule, regardless of Rule configuration.
10. Click **Assign Emergency Group**. The **Assign Emergency Group** dialog box appears.




11. Click the Emergency Group for the Policy, and then click **OK**. Only a single Emergency Group can be assigned to each Policy.
12. Click **File | Save**.

13. Click **Policy | Install** and then select one of the following:

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

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

  If no object issues are encountered, the Policy is verified and pushed to the Spans in the Span Groups assigned to the Policy. The verification and installation process appears in the **Status Tool**, accessed from the ETM® System Console.

  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.

  For instructions for using Adaptive IPS Same-Source Tracking, see below.

### *Negation of Call Disposition in IPS Rules*

You can negate the **Disposition** field of IPS Rules to exclude calls that were terminated from the accumulations. This allows calls that were terminated before they were answered (i.e., reject processing) to be excluded from a Rule tracking Unanswered calls.

## Adaptive IPS Same-Source Tracking

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

### Overview of Adaptive IPS

The ETM System can recognize and takes action when an anomalous call pattern of multiple calls from a previously unknown inbound number in excess of a defined threshold is detected, and provides automatic notification. You can then decide whether permanent action is warranted for the offending source. Sources that breach the same-source threshold are placed in an Adaptive IPS Blacklist. Once you decide which numbers are suspect and which are not, source numbers should be moved from the Blacklist to another Directory Group, such as a Harassing Callers Group used in an installed Firewall Policy or, for numbers deemed not suspect, a whitelist. Provided that no other IPS rules have been modified, the

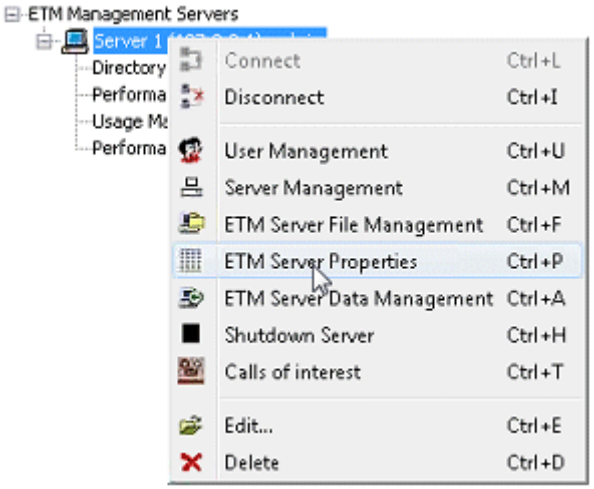
automatic same-source rule can be adjusted and the Policy can be saved to enable the changes without the need to reinstall the entire Policy. This prevents cancellation of the rest of the IPS Policy Rules because of same-source detection.

## Enabling Adaptive IPS on the Management Server

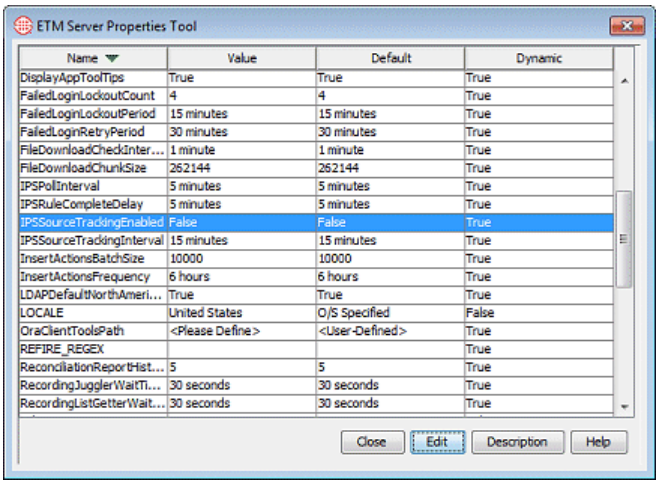
Before Adaptive IPS is available in IPS Policies, it must be enabled on the ETM Server

### To enable Adaptive IPS on the ETM Management Server

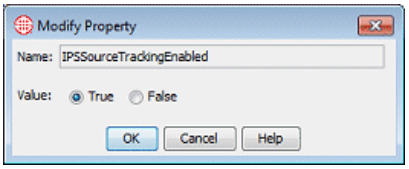
1. In the ETM System Console, right-click the Server and click **ETM Server Properties**.




2. The **ETM Server Properties Tool** appears.



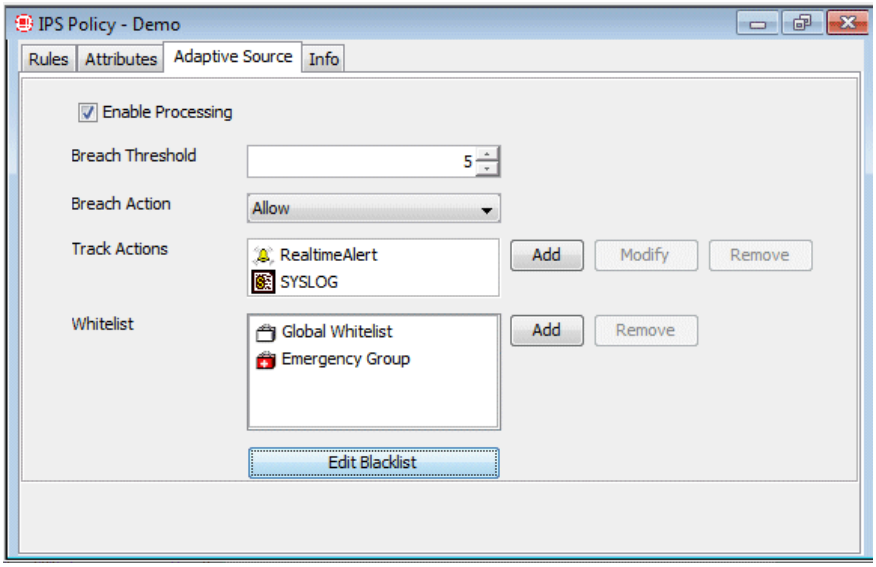

3. Click **IPSSouceTrackingEnabled** and then click **Edit**. The **Modify Property** dialog box appears.




4. Select **True** and then click **OK**. IPS Same-Source tracking is now enabled.
5. The **IPSSourceTrackingInterval** property specifies the amount of time that the system keeps track of the calls that will be evaluated for same source breaches. It can be modified from the default value of 15 minutes. If a given phone number meets the Same-Source Threshold specified in an IPS Policy during this tracking interval, an IPS Policy Rule is created to track that number. Once a source number triggers same-source tracking, it is placed in the Global Blacklist and continues to be tracked unless it is moved to the Global Whitelist or or to another Directory Object for specific treatment by ETM System Policy..
6. Click **Close**.

## IPS Policy Adaptive Source Tab

Same-source tracking for an IPS policy is configured on the **Adaptive Source** tab of the **IPS Policy Editor**. On this tab, you specify the threshold count equal to and in excess of which calls from the same source are to be tracked, the Action to be taken when the breach threshold is met/exceeded, and Track actions.. The Interval is automatically set to 24/7/365 You also manage the same-source whitelist and blacklist configuration from this tab.



**Note**: The **Adaptive Source** tab is only available when Same Source tracking is enabled on the Management Server. See "Enabling Adaptive IPS on the Management Server" on page 30.

The **Adaptive Source** tab on the **IPS Policy** editor contains the following options:

- **Enable Processing**—Selecting the **Enable Processing** checkbox specifies that same-source tracking is to be used in the Policy.
- **Breach Threshold**—Specifies the number of calls from the same inbound source within a given interval that will trigger the rule to breach. Tracking of a source only begins when the count of calls from that source has exceeded the Breach Threshold.
- **Breach Action**—Denotes what action should be taken when a breach occurs. The available actions are the same as the normal IPS Rule actions: Allow, Terminate Future, and Terminate Current and Future.
- **Track Action**—The same Track Actions are available as the Track Action field of IPS Policy Rules: Email, SNMP, Syslog, and Realtime Alert. Click **Add** to add Tracks. Click **Modify** to change properties of a specified Email Track. Click **Remove** to remove a selected Track.
- **Whitelist**—Used to specify one or more Directory Groups that are to be excluded from same-source tracking. The **Add** and **Remove** button displays the **Group Objects** dialog box to add and remove members of the whitelist. (Group Objects available in this dialog box are created via the **Directory Manager**.)
- **Edit Blacklist**—Opens the **Edit Blacklist** dialog box in which you manage blacklisted phone numbers. Options include removing a selected number, removing all numbers, and moving a blacklisted number to a whitelist or to another Directory Group for permanent resolution.

After editing the Blacklist to specify permanent resolution for the identified numbers, save the Policy to initiate a new same-source tracking period.

## Configuring an IPS Policy for Adaptive Source Tracking

### To configure Adaptive Source in an IPS Policy

1. In the **IPS Policy** editor, click the **Adaptive Source** tab.
2. Click the **Enable Processing** checkbox.
3. In the **Breach Threshold** box, type or select the number of calls that will trigger the rule to breach for a given same-source calling number.
4. In the **Breach Action** box, select the action that should be taken for sources that breach the Same-Source Threashold:
   - Allow
   - Terminate Future
   - Terminate Current and Future.
5. In the **Track Action** area:
   - Click **Add** to add Track actions.

- Click **Modify** to change properties of a selected Email Track action.
- Click **Remove** to remove a selected Track action.

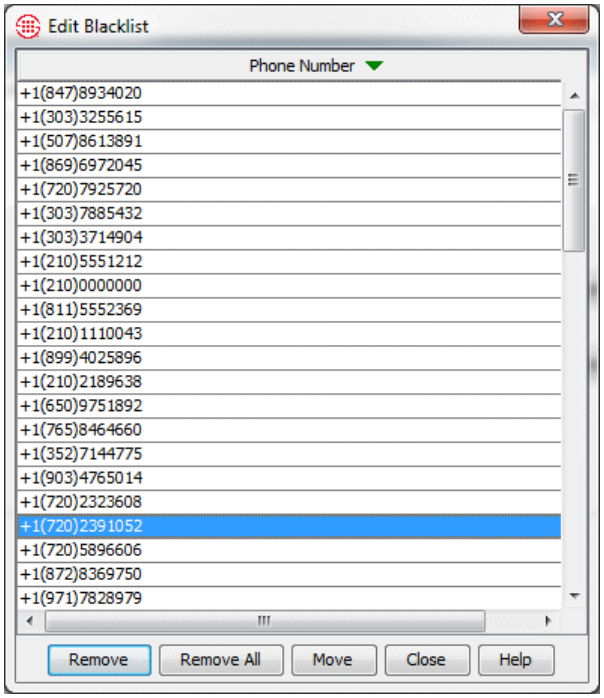
6. In the **Whitelist** area:
   - Click **Add** to specify one or more Directory Groups that are to be excluded from same-source tracking.
   - Click **Remove** to remove a selected Directory Group from the Policy's same-source whitelist.
7. When all Policy configuration changes are complete, save the Policy to implement the same-source Rule changes . Unless other Rules have been modified, other Policy Rules are not reset.

## Managing Blacklisted Phone Numbers

When a source number triggers same source-tracking, it is placed in the Blacklist and remains there until you choose a permanent resolution for the number: whitelisting numbers deemed authorized and moving those bearing further watching to another Directory Group for placement in a specific Firewall, IPS, and/or Call Recorder policy for determined action.

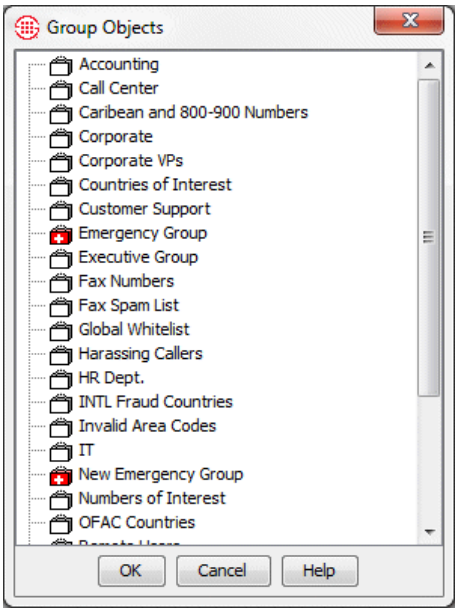
### To manage Blacklisted Phone Numbers

1. Click the **Edit Blacklist** button. The **Edit Blacklist** dialog box, in which you can manage blacklisted phone numbers.



2. Do any of the following:

   - Select one or more numbers and click **Remove** to remove the selected number(s) from the Blacklist. To select multiple numbers, hold down CTRL or SHIFT whle clicking.
   - Click **Remove All** to remove all of the displayed blacklisted numbers.
   - Select one or more numbers and click **Move** to remove the selected number from the Blacklist and add it to the Global Whitelist or to another Directory Group, such as one in an installed Firewall Policy. To select multiple numbers, hold down CTRL or SHIFT whle clicking. The **Group Objects** dialog box appears.




   Click the Directory Group to which you want to move the selected phone number(s) and then click **OK**.

   - Click the **Close** button to exit the **Edit Blacklist** dialog box.

3. After editing the Blacklist to specify permanent resolution for the identified numbers, save the Policy initiate a new tracking period. The autogenerated rule is removed from the Policy and the same-source counters are reset.

4. Reinstall any Policies containing any Directory Group to which you moved a number, which will be dsiplaying a Dirty Policy indicator.

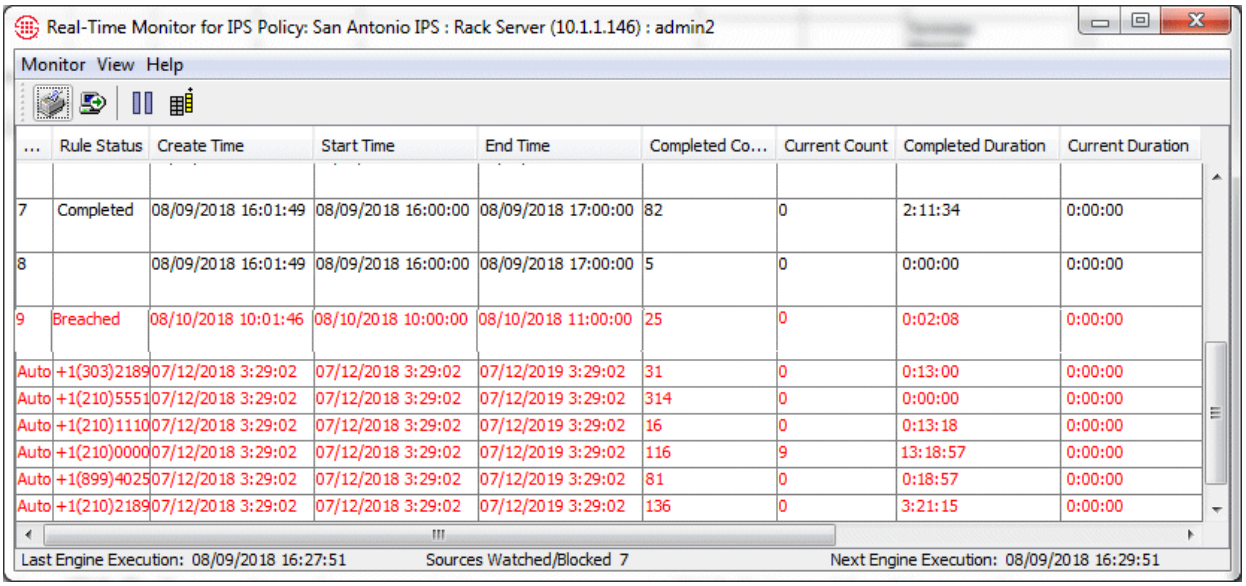
   - To reinstall all Dirtty Policies, on the Performance Manager main menu, click **Policy | Install outdated**.

## Automatically Generated Same Source Rule

When an inbound source number triggers an Adaptive IPS breach, a Breach Rule is automatically generated in the Policy on the Appliance and and the specified Action is enforced for that source until it is moved from the Adaptive IPS Blacklist to another Directory Group. The Breach Rule appears in the IPS Real Time Monitor.

## Same-Source Breaches in IPS Real-time Viewer

When an inbound source breaches the Adaptive IPS threshold, an automatic Same-Source Rule for that phone number appears in the Real-Time vViewer with a Rule number of **Auto**. A separate entry appears for each phone number that breached the threshold; the **Rule Status** field shows the phone number. To view details, select the row. The **IPS Real-Time Viewer** provides a **Details** pane that is updated based on the row that is selected in the table.




## Same-Source Tracking is Global

Although the Breach Threshold and the resulting breach Rule action are Policy-specific, the tracking of inbound source numbers is shared across all installed IPS Policies.

For example, suppose Policy A defines a same-source Breach Threshold of 5 and Policy B defines a same-source Breach Threshold of 10. Once 5 calls from the same source occur within the IPS Same Source Tracking Interval, Policy A breaches and the new Rule is generated and installed on Policy A. Those 5 calls also apply to Policy B's accumulation, but Policy does not breach until its specified Breach Threshold is reached.

## Voice IPS Policy Processing

When you install a Voice IPS Policy on a Span Group, a copy of the Policy is also installed on the IPS *polling engine* running on the Management Server. This detection engine evaluates the Thresholds and maintains the accumulations on the Server. When the Server identifies a Rule as breached, it instructs the Span to begin any specified terminations. By default, the polling engine executes to evaluate the Thresholds every 5 minutes. Depending on the number of Thresholds being monitored, you can change this frequency to a higher value to decrease processing load on the Management Server computer. See "Changing the Detection Engine Polling Interval" on page 38 for instructions.

Accumulations are maintained for each Rule of each installed Policy. When a call matches all of the other criteria of a Rule, the values for the call are included in the accumulated values for the Rule. A single call can count against multiple Rules if it matches the criteria; Voice IPS Policy Rules have no processing order. These accumulations are compared to the Thresholds every time the polling engine executes; if a Threshold is exceeded, a breach is recorded and specified Tracks and actions are executed.

Values for calls that begin before but continue into an Interval are counted toward the Threshold(s). However, only the portion of the duration that occurs during the Interval is counted. For example, if a call begins at 7:30 and continues until 8:30 and the Interval begins at 8:00, 30 minutes of the 1-hour duration is applied to the Voice IPS Policy Rule's accumulated duration.

After the Interval in a Rule has completed, call data continues to be applied to the accumulations for a user-configurable amount of time to allow for late-arriving messages. The default is 5 minutes (300,000 ms). You can change this frequency using the **ETM Server Properties Tool** in the ETM System Console. See "Changing the Rule Complete Delay" on page 39 for instructions.

When a Rule in a Policy is breached, the icon for the Policy turns red as an at-a-glance notification of the breach.

### Accumulations Maintained for Server Reboots

If the Management Server is rebooted or becomes otherwise unavailable during a Voice IPS Interval, the accumulations are maintained. However, since the Server is responsible for identifying breached Rules and instructing the Span to begin terminations, terminations can only be initiated when the Server is running and in the "Normal" (not standby) state. When the Server returns to a normal state, it processes all of the calls, updates the accumulations and handles any breaches.

## Span Disconnections

If a temporary network interruption occurs, duration for calls in progress is only counted from the start of the call through the last Span heartbeat, until the Span reconnects. When the Span reconnects and if the Interval is still active, the accumulations are updated with the actual values. If a breach occurred during the disconnect, the specified Tracks are executed; if **Terminate future** was specified, termination of matching calls begins; if **Terminate current and future** was specified and matching calls are active, they are terminated, and future calls are prevented for the remainder of the Interval.

Call data received from Spans that have been disconnected for an extended period is only included in Voice IPS accumulations if the applicable Interval is still available. For an Interval that has ended, there is no guarantee that late-arriving call data will be counted. If a breach is found to have occurred after including late arriving data, the breach is still processed if the Interval is still active. Note that this may result in calls being allowed that otherwise would have been terminated and may result in the actual accumulation value for a time Interval being higher than the Threshold value.

## Truncated Calls Not Counted

If a call is purged from the system because the Span was rebooted, any values accumulated for that call are also purged from the accumulations. However, if such lost calls caused a Rule to be breached, it cannot become unbreached when the call is purged and will still be recorded as breached, even though the final values no longer meet the Threshold. Since Spans are not often rebooted, this is a rare occurrence.

## Server Outages and Intervals

When the polling engine initializes after the system has been down, it attempts to recreate missed intervals by analyzing the past 7 days. Since 7 days is the longest that any Interval can last, that is the amount of time that must be analyzed in order to guarantee that all intervals active at the time of the server outage are recreated.

If a breach is realized after the polling engine recovers from an outage, the system fires the associated tracks as soon as the breach is realized.

In the unlikely event that the polling engine has been unavailable for more than 7 days, intervals that began before the 7-day period are not reconstructed. Only the most recent 7-day period is analyzed.

## Interaction with Other ETM® System Policies

When using the Voice IPS to terminate calls, careful consideration must be given to the other types of Policies being enforced on the same Spans. For example, suppose a Voice Firewall Rule allows your PBX maintenance technician to access the PBX maintenance port at any time, but a Voice IPS Policy Rule specifies a Threshold of one call per day to that resource and terminates current and future calls. Calls in excess of one by this otherwise authorized caller will be terminated.

If a call occurs that is terminated by another ETM System feature, the call is still considered in IPS Policy processing. For example, if a Voice Firewall Policy is terminating calls to 1-900 numbers, but you have also written a Voice IPS Rule to notify you when more than 5 of these calls are made in one day, the Voice IPS Rule counts these calls even though they were terminated.

## Call Type Changes for Ongoing Calls

Call durations are reported for the entire duration of a call, even if call type changes; the duration is not calculated for individual call segments. That is, if a call is voice for 5 minutes and then switches to fax for 20 minutes, the entire 25 minute duration is included in the accumulation for all Rules for which the call qualified at any point during the call.

## Changing the Detection Engine Polling Interval

The frequency, in milliseconds, of the running of the polling engine is governed by the **IPSPollInterval** value. This value can be set to a smaller setting to enable quicker breach detections, but this may have an adverse effect in that the Management Server and Database services will use more CPU. You must have **Manage Server** permission to change the IPS Detection Engine Polling Interval.

### To change the detection engine polling Interval

1. In the ETM System Console, click the server whose properties you want to change.
2. On the main menu, click **Servers | ETM Server Properties**. The **ETM Server Properties Tool** dialog box appears.
3. Click the item named **IPSPollInterval**, and then click **Edit**. The **Modify Property** dialog box appears.
4. In the **Value** box, type the value in days, hours, minutes, seconds, and milliseconds, and then click **OK**. The field accepts values from 1 millisecond–999 days. However, for best results, use values between 30 seconds and 30-60 minutes, but not longer than the length of an Interval. Note that the **Dynamic** field for this property is True. This means you do not have to restart the server for the change to take effect; it is read by the polling engine at its next execution, at which time it switches to the new value.

## Changing the Rule Complete Delay

The amount of time that a Rule continues to collect Rule-fired values from the Spans after the Interval has ended is governed by the **IPSRuleCompleteDelay** value. This value is intended to allow compensation for late-arriving messages. You must have **Manage Server** permission to change the **IPSRuleCompleteDelay** value.

### To change the IPS RuleComplete Delay value

1. In the ETM System Console, click the server whose properties you want to change.
2. On the main menu, click **Servers | ETM Server Properties**. The **ETM Server Properties Tool** appears.
3. Click the item named **IPSRuleCompleteDelay**, and then click **Edit**. The **Modify Property** dialog box appears.
4. In the **Value** box, type the new value in days, hours, minutes, seconds, and milliseconds. The field accepts values from 1 millisecond–999 days. However, for best results, use values between 30 seconds and 30-60 minutes, but not longer than the length of an Interval. Note that the **Dynamic** field for this property is True. This means you do not have to restart the server for the change to take effect; it is read by the polling engine at its next execution, at which time it switches to the new value.

## Canceling a Rule

If you are obtaining unexpected results with a given Rule in a Policy, you can cancel the Rule, reset the accumulation counters, and stop or prevent call terminations. Any of the following actions cancels the Rule:

- Uninstalling the Policy. Processing of all Rules ceases and all accumulations are reset.
- Disabling the Rule and reinstalling the Policy. Only the modified Rule is cancelled; the other Rules are unaffected.
- Modifying the Rule or objects used in the Rule such that its accumulation is reset. Only the Interval for the modified Rule is cancelled; the other Rules are unaffected. Processing of the Rule does not resume until the start of the next Interval.

## Voice IPS Policy Verification

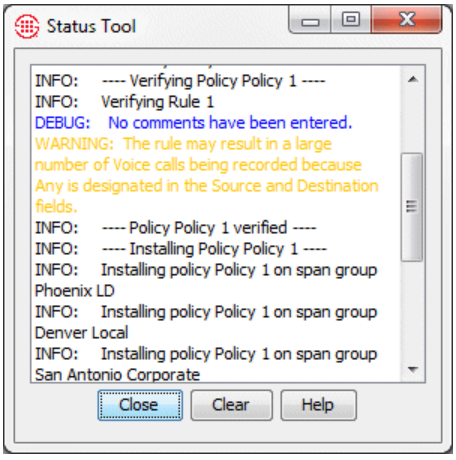
Before a Voice IPS Policy is installed on a Span Group, it is verified for proper configuration. Messages appear in the **Status Tool** as verification proceeds. If verification succeeds, the Policy can be installed; if verification fails, the Policy cannot be installed. Errors result in failed verification; Warnings allow the Policy to pass verification and be installed. If Errors or Warnings occur, the **Status Tool** provides information about the issue.

**Verification fails if:**

- Spans in differing time zones are assigned to the Policy. All Spans enforcing the same Voice IPS Policy must be in the same time zone.
- The Policy contains empty Directory, Subnet, or Time Objects, or the **Threshold** field has not been defined.

**Verification succeeds with a Warning if:**

- A Rule contains both a **<** (less than) **Duration** and one of the **Terminate** actions. It cannot be determined if a call is less than a specified duration until the call ends.
- A Rules contains both a **<** (less than) **Threshold** and one of the **Terminate** actions. It cannot be determined whether the cumulative value is less than the specified Threshold until the Interval ends.
- A Rule contains a **Disposition** other then **Any** (e.g., **Terminated by Firewall**) and one of the **Terminate** actions. Since these calls are counted because they have already been terminated, this Rule is invalid.
- 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.
- Email Tracks have no Contacts.
- The policy contains one or more disabled Rules.




During verification, the **Status Tool** provides notification if a Rule's accumulation will be reset upon installation. Such Rules are marked **Cancelled** in the Policy Log and **Real-Time Monitor**.

# Managing IPS Policies

## IPS Policy Management

The procedures below provide instructions for managing IPS Policies.

### Editing an Installed Voice IPS Policy

**To edit an installed Policy**

1. In the **IPS Policies** subtree of the Performance Manager tree pane, right-click the Policy, and then click **Edit**.
2. The IPS Policy opens in the Policy editor pane. Edit the fields as described in "Defining a Voice IPS Policy" on page 21, and then click **File | Save**.
3. A message appears stating that to be saved, the Policy must also be reinstalled on the Span. This keeps the copy on the server and the copy on the Span synchronized. Click **OK**.

Note that if you added a track to an already-breached Rule, the track is not executed until the next breach.

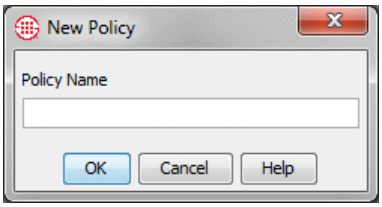
When the Policy is reinstalled, any Rules whose accumulations were reset are marked **Cancelled** in the IPS Policy **Real-Time Monitor** and **Policy Log**.

### Using Save As to Create a New Voice IPS Policy

A **Save as** function is provided so that you can copy an existing Policy to use as the basis for a new Policy.

**To create a new Policy from an existing Policy**

1. Open the Policy.
2. Click **File | Save As**. The **New Policy** dialog box appears.



3. In the **Policy Name** box, type the name for the new Policy, and then click **OK**.
4. The new Policy appears in the tree pane.
5. Click the **Attributes** tab and specify the correct Span Group(s) and Emergency Group for the Policy.
6. Edit the Rules as needed.
7. Click **Save**.
8. Click **Install** to install the Policy on the Span Groups.

## Enabling/ Disabling IPS Rules

If you want to pause processing of a Rule but do not want to delete it, you can disable it. When you disable a Rule, it is cancelled.

### To disable a Rule

1. In the open Policy, click the Rule you want to disable.
2. On the main menu, click **Edit | Disable**. The disabled Rule appears dimmed.
3. Reinstall the Policy for the change to take effect on the Spans.

### To enable a disabled Rule

1. Click the disabled Rule.
2. On the main menu, click **Edit | Enable**. The Rule is again active and no longer appears dimmed.
3. Reinstall the Policy for the change to take effect on the Spans.

## Hiding/Showing the Default Voice IPS Policy Node

The **Default** Policy node displays the **Unassigned** Span Group and all Span Groups on which a user-defined Policy is not installed.

### To show/hide the Default Policy node

- In the Performance Manager tree pane, right-click the Policies subtree, and then click **Default** Policy node. This selection acts as a toggle to turn display of the node on and off; a check mark indicates it is showing.

## Hiding/Showing Rules in a Voice IPS Policy

When you hide a Rule, it is still enforced. It just does not appear in the Policy.

### To hide a Rule

- In an open Policy, click the Rule, and then click **Edit | Hide Rule**.

### To show hidden Rules

- With the Voice IPS Policy open, click **Edit | Show Hidden Rules**.

## Printing a Voice IPS Policy

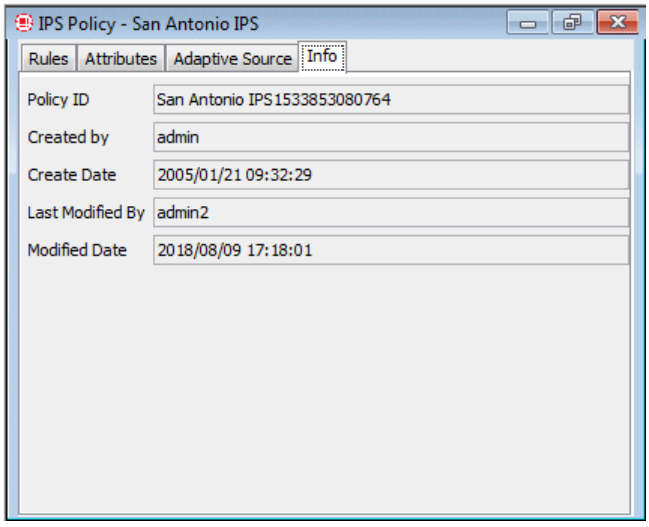
### To print a Voice IPS Policy

1. Open the Policy in the Editor.
2. On the Performance Manager main menu, click **File**, point to **Print**, and then click **Print Summary** or **Print Details**. A **Print Preview** appears.
   - **Print Summary** provides a picture of the Policy as configured and the information in the **Info** tab.
   - **Print Details** provides the same information as **Print Summary**, plus a listing of the contents of the objects in the Policy.

## Viewing Voice IPS Policy Info

### To view information about a Voice IPS Policy

- In an open Voice IPS Policy, click the **Info** tab.



The following information is provided:

**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.

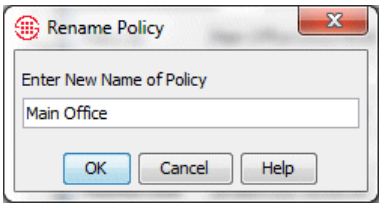
**Last Modified By**—Username of the person who last modified the Policy.

**Modified Date**—Date the Policy was last modified.

## Renaming a Voice IPS Policy

### To rename a Policy

1. In the tree pane, right-click the Policy name, and then click **Rename**. The **Rename Policy** dialog box appears.




2. Type the new name, and then click **OK**.

## Installing a Voice IPS Policy

Edits to most fields in an installed Policy cause the accumulations for that Rule to be reset; changes to the **Tracks** or **Comment** field do not.

When you reinstall a Policy that contains Rules for which the accumulations have been reset, or contains new Rules, processing of those Rules begins at the start of the next Interval.

### To install a Policy

1. Do one of the following:
   - In the Performance Manager tree pane, right-click the Policy name, and then click **Install**.
   - Open the Policy, and then on the Performance Manager main menu click **Policy | Install** .
2. Select 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 existing Policy must be uninstalled from any Span to free up space for installation of the new Policy, this is

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

performed automatically. Calls are processed using the default Policy until installation of the new Policy is complete.

If no object issues are encountered, the Policy is verified and pushed to the Spans in the Span Groups assigned to the Policy. The verification and installation process appears in the **Status Tool**, accessed from the ETM® System Console.

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.

3. Verification is performed; if the Policy passes verification, it is installed on the Spans. If it does not pass verification, the message "Policy was not installed" appears in the Performance Manager. To see the progress and outcome of verification, open the **Status Tool** from the ETM System Console, if it is not set to open automatically.
   - If the Policy fails verification, correct the errors identified in the **Status Tool**, and then reinstall.
4. If any Rules are cancelled by reinstalling the Policy, the **Real-Time Monitor** updates to reflect this fact. Processing of reset but still active Rules resumes at the start of the next Interval.

## Uninstalling a Voice IPS Policy

When you uninstall a Policy, processing stops for all Rules, all active terminations from prior Rule firings are cancelled, and all counters associated with the Policy are reset. The Rules are marked **Cancelled** in the **Real-Time Monitor** and **Policy Log**.

### To uninstall a Policy

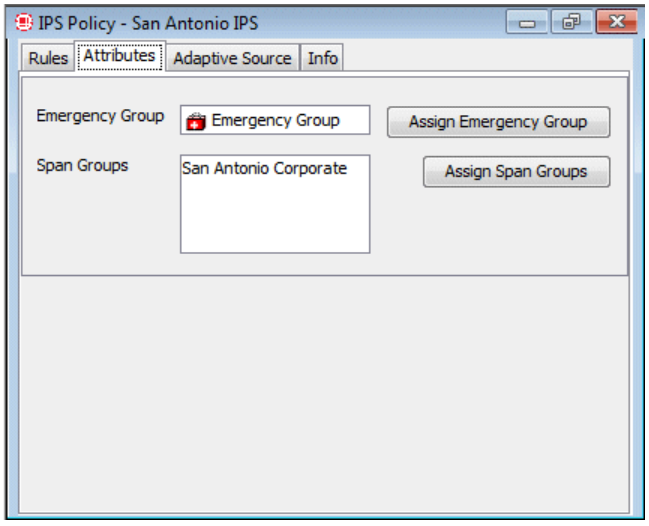
- Do one of the following:
  - In the tree pane, right-click the Policy name, and then click **Uninstall**.
  - Open the Policy, and then on the Performance Manager main menu, click **Policy | Uninstall** .

## Assigning Span Groups to a Policy

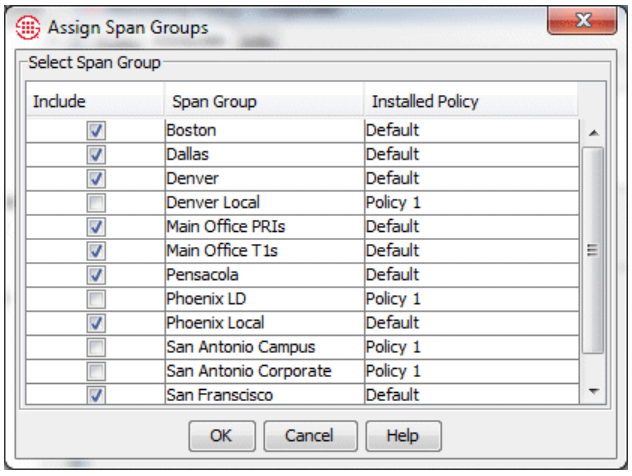
Note that if you move a Span into a Span Group that is assigned to an installed IPS Policy, the Policy is automatically pushed to the newly added Span. Recall that all Spans in all of the Spans Groups assigned to a given IPS Policy must be in the same time zone.

### To assign Span Groups to a Policy

1. In an open Policy, click the **Attributes** tab.




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




3. Select the check boxes of the Span Groups on which you want to install the Policy; clear the check boxes for all other Span Groups. By default, the check boxes for Span Groups not currently enforcing a Policy are selected.
4. Click **OK**.
5. Click **File | Save**. If the Policy is currently installed, it is saved and downloaded to the Spans. If it is not, it is simply saved.

## Deleting a Policy

You can only delete Policies that are not installed. To delete an installed Policy, first uninstall it.

### To delete an uninstalled Policy

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

# Monitoring Results

## Viewing Voice IPS Policy Results

You can view results of Voice IPS Policy processing in several ways:

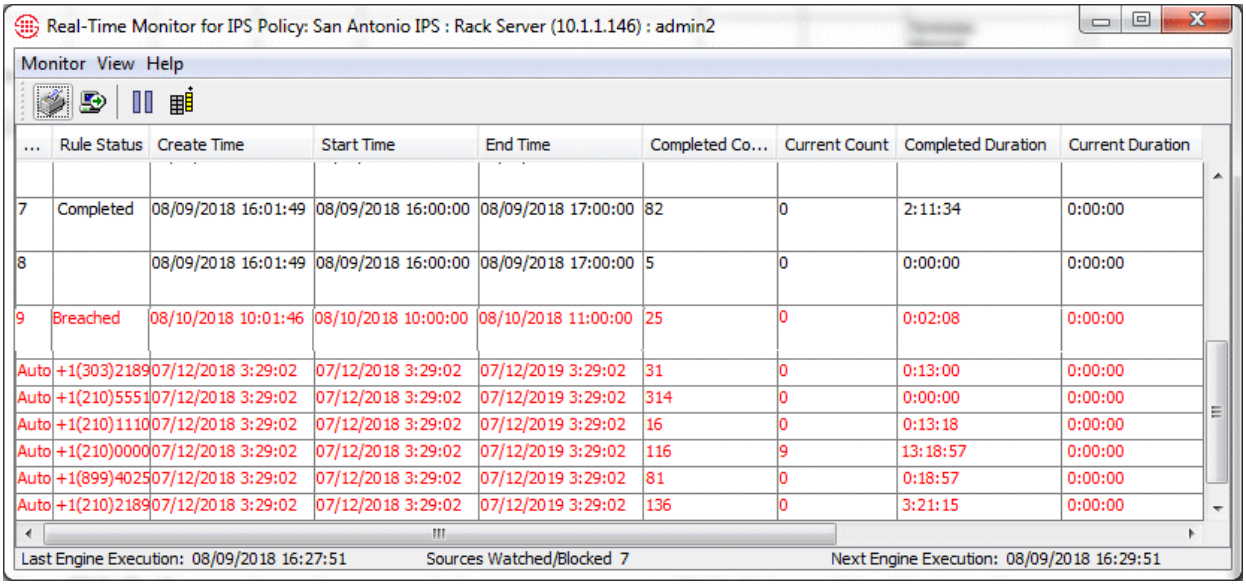
- The Voice IPS Policy **Real-Time Monitor** shows current accumulations per Rule during the Interval.
- The Voice IPS **Policy Log** shows completed accumulations when a Rule has completed processing for the Interval, because either the Interval ended or the Rule was cancelled.
- The Usage Manager provides **IPS Elements** with which you can define Reports for viewing historical Voice IPS Policy processing data.

### Voice IPS Policy Real-Time Monitor

The Voice IPS Policy **Real-Time Monitor** shows the current accumulated values for calls that have matched each Rule in the Policy. This enables you to monitor the status of each Threshold and be aware when a Threshold is about to be breached. Values remain displayed while the Interval is active. When the Interval is complete, use the Voice IPS Policy Log or Usage Manager reports to view results.

Note that if you reinstall a Policy during the Interval, the reset and new Rules are not implemented until the start of the next Interval. Cancelled Rules remain displayed (and also appear in the Voice IPS Policy Log); a blank line is added for each new Rule. The values do not update until the start of the next Interval.

Breached Rules are displayed in red text.




### *Opening the IPS Policy Real-Time Monitor*

**To open the IPS Policy Real-Time Monitor**

- In the **IPS Policies** subtree of the Performance Manager tree pane, right-click an active Policy, and then click **View Real-Time Status**. At the bottom of the **Real-Time Monitor,** you can see the last time the Voice IPS polling engine executed, at which time the display was updated, and the next time the engine will execute. By default, the engine executes every 5 minutes. See "Changing the Detection Engine Polling Interval" on page 38 for instructions for modifying the frequency.

Each row in the viewer represents one Rule Interval in the Voice IPS Policy. Each row has the following fields:

Columns can be arranged in any order and you can select which columns to hide or show.

**No**—The Rule number represented by the record. Adaptive IPS breaches have **Auto** as the Rule number.

**Rule Status**—The current disposition of the Rule: Completed, Breached, or Cancelled. Blank if none of the above (that is, still active and unbreached). The row turns red when a Rule is breached. Adaptive IPS breaches show the calling number that caused the breach, with a row shown for each calling number that caused a breach.

**Create Time**—The time at which the Interval was initiated, or "created," by the first run of the polling engine for this Interval. This time is always some amount of time after the **Start Time**. It typically reflects the first time the poller runs during the defined Interval and is therefore typically within 5 minutes of the **Start Time**.

**Start Time**—The start time of the Interval.

**TIP:** To obtain the total duration, cost, or count for the Interval, add the **Current** and **Completed** values for that measure. Breaches are determined by summing these two and comparing to the threshold.

**End Time**—The end time of the Interval.

**Completed Count**—The count of completed calls that matched the Rule.

**Current Count**—Current count of calls matching the Rule.

**Completed Duration**—The total duration of completed calls that matched the Rule.

**Current Duration**—Current accumulated duration of active calls matching the Rule.

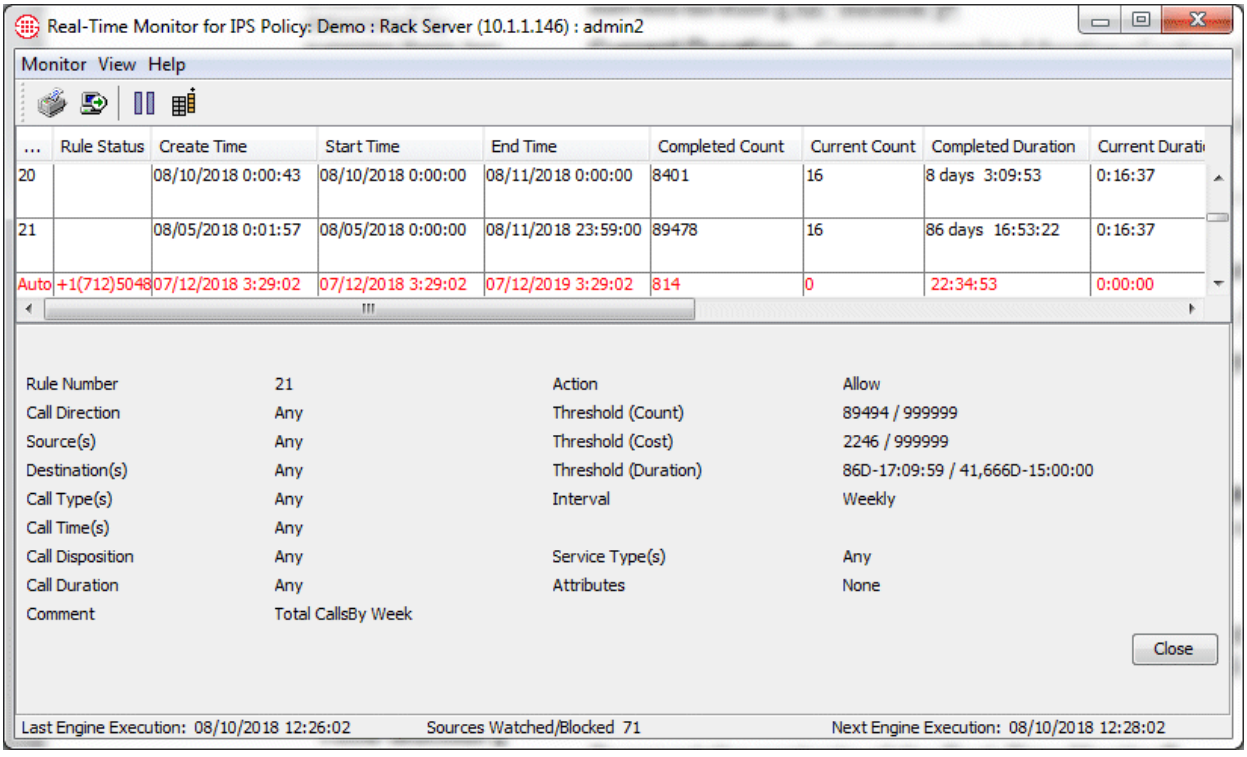
**Completed Cost**—The total cost of completed calls that matched the Rule.

**Current Cost**—Current accumulated cost for active calls that match the Rule.

**Prevented Count**—The count of calls prevented during the Interval.

**Comment**—The comment in the **Comment** field of the Rule, if any.

To view the details for any row, click the row. A bottom pane opens showing Rule details.



### *Printing the Contents of the Real-Time Monitor*

**To print the contents of the Real-Time Monitor**

- On the **Real-Time Monitor** main menu, click **Monitor | Print**. The typical print dialog box for your computer appears. Print as usual.

### *Exporting the Contents of the IPS Policy Real-Time Monitor*

You can export the contents of the **Real-Time Monitor** as a CSV file for import into other programs such as Microsoft Excel.

**To export the contents of the Real-Time Monitor**

- On the **Real-Time Monitor** main menu, click **Monitor | Export**. A **Save** dialog box appears for you to select the location to which you want to save the CSV file. Browse to the location, and then click **Save**.

### *Freezing the Display in the Real-Time Monitor*

You can freeze the display of the **Real-Time Monitor** so that it does not update while you examine its contents.

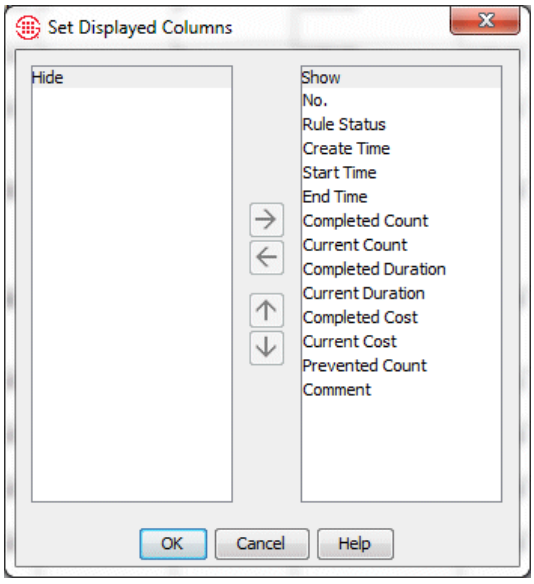
**To freeze the display**

- On the **Real-Time Monitor** main menu, click **View | Freeze**. This selection works as a toggle; a check mark indicates that the display is frozen. Click the selection to unfreeze it.

### *Showing/Hiding Columns in the Real-Time Monitor*

**To show/hide columns**

1. On the **Real-Time Monitor** main menu, click **View | Columns**. The **Set Displayed Columns** dialog box appears.



2. The **Show** box lists visible columns; the **Hide** box lists hidden columns. The order in which they appear in the **Show** box is the order in which they appear in the GUI.

   - To hide a column, double-click it in the **Show** box, or click it, and then click the left arrow.
   - To show a hidden column, double-click it in the **Hide** box, or click it, and then click the right arrow.
   - To reorder a column, click it, and then click the up or down arrows.

## IPS Policy Log

See "Active to Historical Data Transfer" in the *ETM® System User Guide* for a conceptual overview of this functionality.

The **Policy Log** for IPS Policies displays recent results of IPS Policy processing after an Interval completes. Note that the **Policy Log** retrieves results from the Active area in the database and is used for recent results. 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.

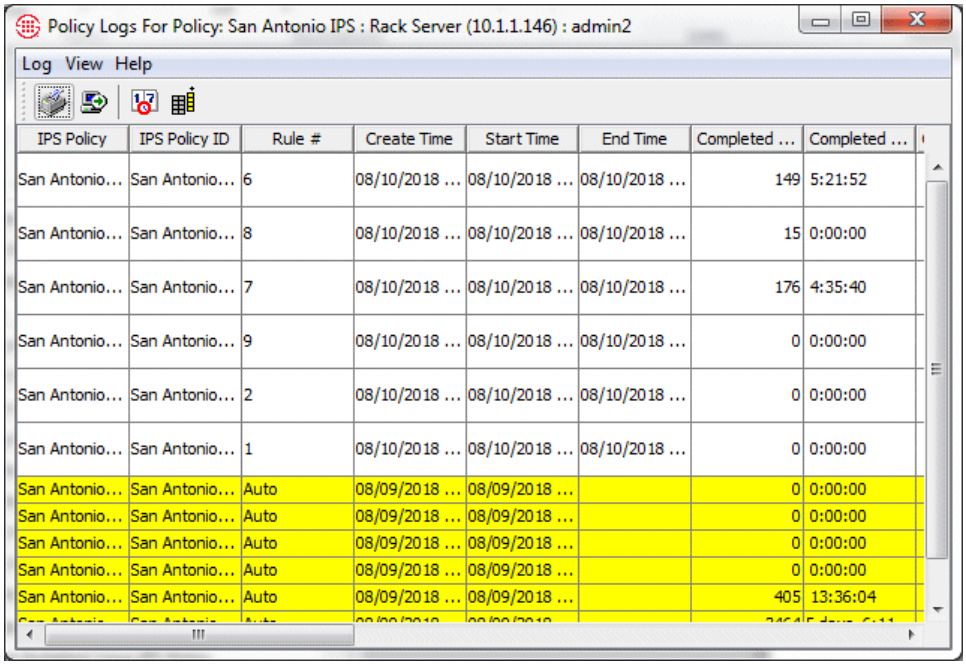
See "Active-to-Historical Data Transfer Properties" in the *ETM® System Administration and Maintenance Guide* for instructions for modifying the frequency.

Columns can be arranged in any order you specify and you can select which columns to hide or show.

### *Opening the Voice IPS Policy Log*

**To open the Policy Log for an IPS Policy**

- In the **IPS Policies** subtree of the Performance Manager tree pane, right-click a Policy, and then click **View Policy Logs**.




New entries are coloered yellow by default. Columns can be arranged in any order you specify and you can select which columns to hide or show.

Each row represents one completed Rule Interval from a Voice IPS Policy. Each row has the following fields:

**IPS Policy**—The name of the Policy.

**IPS Policy ID**—A system-assigned unique ID for the Policy.

**Rule #** —The Rule number represented by the record.

**Create Time**—The time at which the Interval was initiated, or "created," by the first run of the polling engine for this Interval. This time is always some amount of time after the **Start Time**. It typically reflects the first time the poller runs during the defined Interval and is therefore typically within 5 minutes of the **Start Time**.

**Start Time**—The start time of the Interval.

**End Time**—The end time of the Interval.

**Current Count**—Count of current calls matching the Rule when it ended.

**Completed Count**—The count of completed calls that matched the Rule during the Interval.

**Current Duration**—Accumulated duration of active calls matching the Rule when it ended.

**Completed Duration**—The total duration of completed calls that matched the Rule during the Interval.

**Current Cost**—Accumulated cost for active calls that matched the Rule when it ended.

**TIP**: To determine the total cost, count, or duration for the Interval, add the **Current** and **Completed** values together.

**Completed Cost**—The total cost of completed calls that matched the Rule during the Interval.

**Prevented Count**—The count of attempted calls that matched the Rule that were prevented.

**Threshold Count**—The count of calls specified in the Threshold.

**Threshold Duration**—The duration specified in the Threshold.

**Threshold Cost**—The cost specified in the Threshold.

**Disposition**—The disposition of the Rule for the Interval: completed, breached, or cancelled.

**Track**—The tracks assigned to the Rule. Log is included by default.

**Action**—The action to be performed if the Rule was breached.

**Complete Time**—The complete time of the Rule, either the end of the Interval or the time at which the Rule was cancelled.

**Comment—**The comment in the Rule.

**Metadata—** Shows the source phone number that caused an Adaptive IPS (Same Source) breach.

## Voice IPS Policy Reports

The Usage Manager allows you to generate Reports of historical Voice IPS Policy processing data. All completed Rule intervals, whether breached or not, are available in the Usage Manager.

See "Voice IPS Elements" in the *Usage Manager User Guide* for instructions for defining and generating Reports.

# Rules for Specific Scenarios

## Example Uses of the Voice IPS

This section provides examples of how to use the Voice IPS to detect and protect against various types of calling patterns that can indicate toll fraud, potential security threats, or other anomalous calling patterns, such as inadequate outbound calls on your outbound Sales lines or excessive busy or unanswered calls to your customer service department.

### Toll-Fraud Protection

You can use the Voice IPS to protect against calling patterns that indicate potential toll fraud, such as an excessive number or duration of outbound toll calls.

#### *Long-Duration Outbound Toll Calls*

This Rule assumes a call flag for Mexico has been added to the Dialing Plan.

Long-duration outbound toll calls can indicate toll fraud. Since various Service Types may have different acceptable Thresholds (for example, long-distance domestic versus international), you would define a separate Rule for each type of toll service you want to monitor. You can set a Threshold based on cumulative duration, count, or cost. For example, suppose a certain number of calls to Mexico are normal for your your organization during business hours, but they are relatively infrequent and usually last less than an hour, and are never expected after business hours. You might define a Rule for outbound calls to Mexico of 1 hour or more in duration during business and set a Threshold of ten such calls per week. Then define a second Rule to terminate all such calls after hours. The sample Rules below illustrate this scenario.

| No. | Call Direc… | Service Types | Call Duration | Time | Threshold | Action | Track | Comments |
|---|---|---|---|---|---|---|---|---|
| 1 | Outb… | Mexico | ≥ 01:00 | Business Hours | ≥ Values ( Count of 10 ) Interval … | Terminate Current and Future | Fraud … Log | Excess long-duration calls to Mexico (bus hrs.) |
| 2 | Outb… | Mexico | Any | After Business… | ≥ Values ( Count of 1 ) Interval ( … | Terminate Current and Future | Fraud … Log | Excess long-duration calls to Mexico (after bus hrs.) |

### *Excessive Numbers of Outbound Toll Calls*

An excessive number of outbound toll calls may indicate toll fraud. Since various Service Types may have different acceptable Thresholds, you would define a separate Rule for each Service Type you want to track. For example, suppose a certain number of International calls are typical during Business Hours at your organization. After establishing a realistic Threshold for such calls, you might define a Rule to generate an email when the Threshold is breached. The sample Rule below illustrates this scenario.

| ... | Call Direction | Source | Destination | Service Types | Threshold | Action | Track | Comments |
|---|---|---|---|---|---|---|---|---|
| 1 | Outbound | Any | Any | INTL | ≥ Values ( Count of 25 ) Interval ( Business Hours - By Hour ) | Allow | Fraud Gr... Log | Alert Abnormal Count Outbound INTL Calls - Business Hours |

You can create additional Rules for expected volume of such calls at other times, such as After Business Hours.

## Security Monitoring

You can use the Voice IPS to track and protect against calling patterns that may indicate potential security threats, such as war dialing and attempts to access restricted resources.

### *Excessive Short-Duration Inbound Calls*

An excessive number of short-duration inbound calls can indicate war dialing. To monitor for this activity, you can define a Rule for all inbound traffic that specifies a **Duration** of less than one minute and a call count Threshold at which you want to be alerted via email, for example, 10 such calls per hour (use an Hour Subinterval for this). Leave the rest of the fields at their defaults. Note that, since it cannot be determined whether a call is less than a given duration until the call ends, you cannot prevent calls based on a less-than duration. The illustration below provides an example of such a Rule.

| No. | Call Direction | Call Duration | Threshold | Action | Track | Comments |
|---|---|---|---|---|---|---|
| 1 | Inbound | < 00:01 | ≥ Values ( Count of 10 ) Interval ( Hours ) | Allow | Log RealtimeAlert | Alert for excess short calls |

### *Excessive Inbound Calls to Unused Extensions*

An excessive number of call attempts to unused extensions can indicate an intrusion attempt. To protect against this, you can define a Directory Object (Range, Filter, or Group) that contains these unused extensions. Then define an **Inbound** Voice IPS Policy Rule with this object in the **Destination** column. Be sure the Span Groups monitoring these extensions are assigned to the Policy and then set a realistic Threshold to detect an increase in call attempts to these numbers. To establish this Threshold, use a Usage Manager Report to identify a typical number of calls to these extensions per week or per day, depending on the Interval you want to use. Decide whether you want to prevent calls when the Threshold is exceeded, which can deter would-be attackers who realize their attack has been discovered. If so, place **Terminate Current and Future** in the **Action** column. The sample Rule below illustrates an Allow and Alert Rule for this scenario.

| No. | Call Direction | Source | Destination | Threshold | Action | Track | Comments |
|---|---|---|---|---|---|---|---|
| 1 | Inbound | Any | Unused Ext... | ≥ Values ( Count of 20 ) Interval ( Daily ) | Allow | Log<br>SNMP | Alert excess calls to unused extensions |

### *Excessive Number of Calls Terminated by the Voice Firewall*

If you are using the ETM® System to actively terminate calls, you can use IPS to track the number of calls being terminated according to terminator.

For example, you can write Rules with a **Disposition** of **Terminated by Firewall**. Set a Threshold based on a Usage Manager report of typical activity. For example, you may want separate Rules for Inbound and Outbound calls, since these may have different expected thresholds. You cannot terminate any calls, since the Rule counts calls that have already been terminated; however, you can be notified when the set Threshold is exceeded, to evaluate potential causes. The sample Rule below illustrates tracking the count of inbound calls terminated by the Voice Firewall during business hours.

| No. | Call Direction | Source | Destination | Threshold | Action | Track | Disposition | Comments |
|---|---|---|---|---|---|---|---|---|
| 1 | Inbound | Any | Any | ≥ Values ( Count of 50 ) Interval ( Business Hours ) | Allow | Log<br>Telco Ma... | Terminated by Firewall | Alert excess Firewall Terminations (Bus. Hours) |

## Tracking Other Anomalous Calling Patterns

In addition to protecting against intrusion attempts such as toll fraud and war dialing, the Voice IPS can help you monitor and control other types of anomalous calling patterns. For example, a sudden drop in calls on a normally busy trunk may indicate a service issue; a large number of busy or unanswered calls to your customer service department may indicate a potential resource or management issue.

### *Outbound Calling Patterns on a Specific Set of Lines*

Perhaps you want to track the number of calls being made by your inside sales team during working hours each week, to ensure that their quotas are being met. You can define a Directory entity representing those extensions, and then define an outbound Voice IPS Policy Rule with that Directory entity in the **Source** field. Define a Threshold for the number of calls required and select a Weekly Interval. Then select **Less than** in the **Threshold** field and assign a notification track in the **Track** field to alert someone when the number of calls per week is less than the specified number. The sample Rule below illustrates this scenario.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 8 | Outbound | Inside Sales | Any | Business ... | < Values ( Count of 100 ) Interval ( Week Interval ) | Allow | Log<br>Sales Ma... | Monitor Inside Sales call counts by week |

### *Escalating Toll Call Costs*

You can use the Voice IPS to monitor and control costs associated with specific Service Types. For example, you might want to track all outbound International calls and alert appropriate personnel if a set cost Threshold is exceeded. Or, you might want to set a dollar limit per week per department for outbound long-distance calls and prevent calls in excess of the Threshold. The two sample Rules below illustrate these scenarios.

| No. | Call Direction | Source | Destina... | Service Types | Threshold | Action | Track | Comme |
|---|---|---|---|---|---|---|---|---|
| 1 | Outbound | Main Office | Any | Long Dist... | ≥ Values ( Cost of ... | Terminate Current and Future | Log<br>Telecom Dir | Prevent excess L per week--Main C |
| 2 | Outbound | West Coa... | Any | Internatio... | ≥ Values ( Cost of ... | Allow | Log<br>Telecom Dir | Alert for excess INT-West Coast |

### *Inbound Calling Patterns on a Specific Set of Lines*

Perhaps you want to monitor the total number of calls to your Customer Service department, and also monitor for excessive numbers of busy or unanswered calls that could indicate a resource or staffing issue. You might define three Rules to accomplish this. All three Rules would specify **Inbound** and a **Destination** of Customer Support. One Rule would specify a call type of Busy and a Threshold of a certain number per week. Another Rule would specify a call type of Unanswered and a Threshold of a certain number per week. These two Rules would have notification tracks. The third Rule would simply count all calls on the Customer Support lines. The sample Rules below illustrate this scenario.

| No. | Call Direction | Source | Destination | Threshold | Action | Track | Comments |
|---|---|---|---|---|---|---|---|
| 1 | Inbound | Any | Support | < Values ( Count of 1 ) Interval ( Week ) | Allow | Log<br>Support M... | Track unans. support calls |
| 2 | Inbound | Any | Support | ≥ Values ( Count of 1 ) Interval ( Week ) | Allow | Log<br>Support M... | Track busy support calls |
| 3 | Inbound | Any | Support | ≥ Values ( Count of 1 ) Interval ( Week ) | Allow | Log | Track total support calls |

The **Comments** field is useful for describing the purpose of each Rule to facilitate tracking in logs and reports.

# Index