SecureLogix®
We see your voice®

PolicyGuru®

Meta-Policy Controller
v2.5.0

User Guide

About SecureLogix

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

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

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

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

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

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

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

Documentation:
Email: *docs@securelogix.com*
Knowledge Base: *https://support.securelogix.com*

IMPORTANT NOTICE:

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

This product is protected by one or more of the following patents: US 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.

PolicyGuru is used herein as shorthand notation to refer to the PolicyGuru® Solution.

Orchestra One is used herein as shorthand notation to refer to the Orchestra One™ Call Authentication Service.

Customer Support
for Your SecureLogix® Solution

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

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

https://support.securelogix.com

Contents

PolicyGuru® Meta-Policy Controller Introduction 8

Getting Started 24

Simple Event Processing (SEP) Policy Rules and Lists 43

Complex Event Processing (CEP) Policy 72

Real-Time Analytics 84

System Configuration 93

Appendices 100

PolicyGuru® Meta-Policy Controller Introduction

Concepts

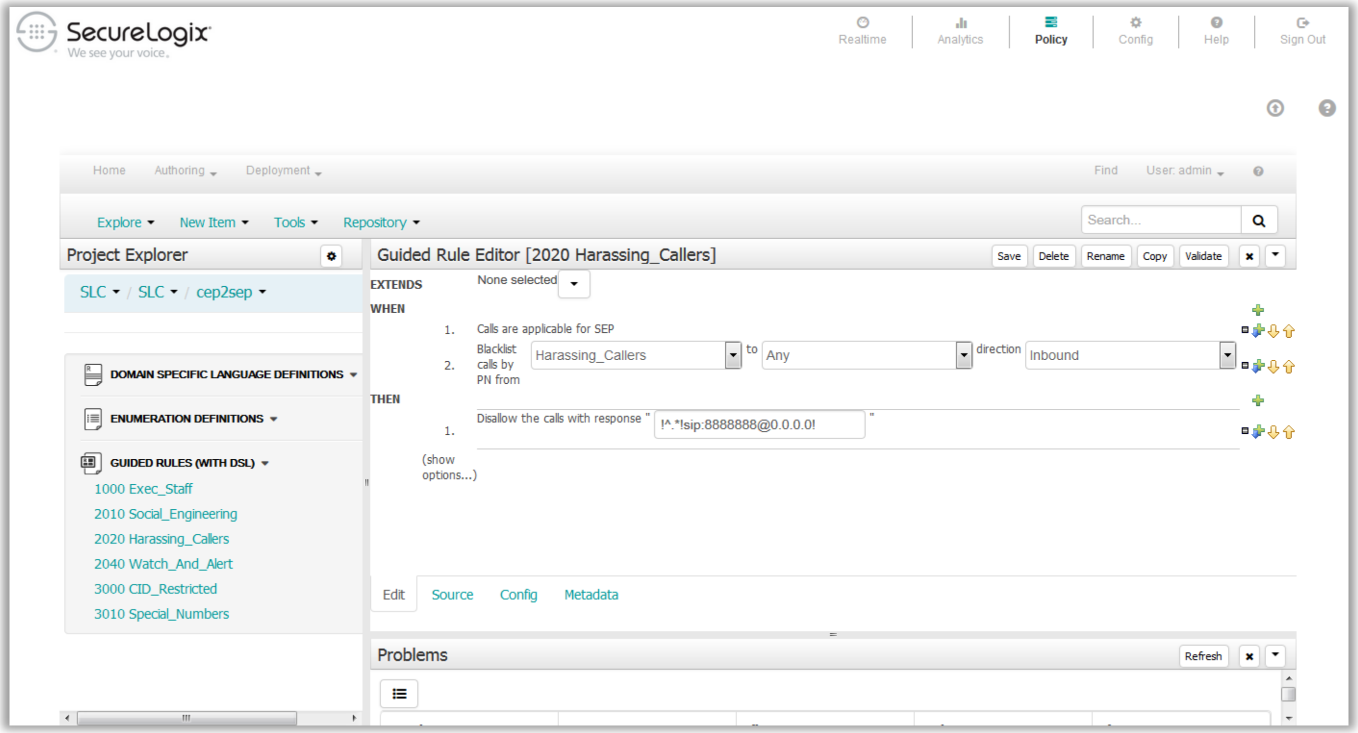
The PolicyGuru® Meta-Policy Controller enables the construction and enforcement of customized voice/Unified Communications (UC) network security and business management Rules through a flexible and powerful Business Rule Management System (BRMS). These Rules are defined, managed, and implemented Enterprise-wide from the central, web-based management interface. Using a BRMS framework allows you to create Rules that can handle extremely complex call scenarios both in and out of the Enterprise.

User-defined PolicyGuru Rules specify the criteria by which a call is considered of interest and the action to be taken if call triggers a Rule: allow the call(s), block the call(s), or redirect the call(s) to another number.

Automated notifications can be configured to alert appropriate personnel when a call or a suspect calling pattern triggers a Rule. SNMP, syslog, and email alerting are supported.

After you define the security, call-access control (CAC), usage, and monitoring Rules for your enterprise, you install them on the PolicyGuru Server Applications securing your enterprise SIP Trunks, where they are continuously enforced in real time. The PolicyGuru Solution also allows monitoring of traffic to detect and alert for new anomalies or new vectors of attack, enabling you to quickly adjust the implemented Rule-set to take appropriate action against these new threats or issues.

Figure 1 shows the BRMS interface with a set of Rules defined, shown in the list in the left **Project Explorer** pane. This list of Rules constitutes the Policy. The Rule open in the **Guided Rule Editor** is defined to terminate inbound calls from callers in a Harassing Callers Blacklist.



WHEN

1. Calls are applicable for SEP
2. Blacklist calls by PN from Harassing_Callers to Any direction Inbound

THEN

1. Disallow the calls with response " !^.*!sip:8888888@0.0.0.0! "

Figure 1: BRMS Interface—Guided Rule Editor

Two types of Policies are available, with their own set of Rules: *Simple Event Processing (SEP)* and *Complex Event Processing (CEP)*, as described below. The Policy Rules shown in Figure 1 are SEP Rules.

Simple Event Processing (SEP) Policy

In a manner similar to data network firewalls, SEP Policy provides real-time voice/UC application session access control and monitoring on a per-call basis, based on call setup details (source, destination, and direction). The user-defined Rules in the SEP Policy define whether specific calls are to be allowed, blocked, or redirected, and provide the data used to alert on SEP Rule firings via corresponding CEP Rules. Calls that match an SEP Rule specifying call treatment are terminated or redirected at call setup, preserving your network resources for legitimate business calls. For example, you can define a Rule that dictates that all calls from known harassing callers in a Harassing Callers Blacklist are to be terminated before they are set up.

SEP Policy Processing is driven by ENUM requests only. Because the call data available in ENUM queries is limited to events that occur at call setup, SEP Rule criteria include any combination of the following:

- **Blacklist Rules**—Source, Destination, Direction, and timestamp range.
- **Whitelist Rules**—Source, Destination.

The PolicyGuru BRMS GUI provides a **Guided Rule Editor** that includes a robust set of predefined SEP Rule-definition assets for building Rules. The set of defined SEP Rules constitutes the *SEP Policy*.

User-defined *Lists* define the phone numbers/URIs to which SEP Rules apply; these are identified as *Blacklists* and *Whitelists*. You can manually add entries to these Lists, or, for large Lists, you can import the entries from a file. Each List can contain either one to many individual phone numbers/URIs, or one to many Regular Expressions (Regex), which are used to define Ranges and Wildcards (such as all phone numbers/URIs in a certain area code).

Lists and SEP Rules work in conjunction to create and implement either *Blacklist Rules* or *Whitelist Rules*, as described below.

SEP Rule Types

Whitelist Rules—*Whitelist Rules* identify calls that are to be allowed and ignored. *Whitelists* (described below) are used to specify the phone numbers/URIs to which Whitelist Rules apply. These Rules do not explicitly fire—they represent default Allow Rules— and therefore cannot be alerted on, preserving processing resources for true calls of interest. This is especially valuable in high call volume environments, such as Contact Centers. See "Whitelists" below for details about Whitelists.

Note: See "Complex Event Processing (CEP) " on page 13 for a discussion of how they are used to alert on SEP Rules

Blacklist Rules—*Blacklist Rules* specify actions and alerting for calls matching the Rule: allow the call as originally routed, block the call, or redirect the call to a different destination. Blacklist Rules are the only type of SEP Rule that fires, since Whitelist Rules specify calls to be ignored and allowed. This means Blacklist Rules are the only Rules that can be alerted on with a corresponding CEP Rule. *Blacklists* (described below) are used to specify the phone numbers/URIs to which Blacklist Rules apply.

It is important to note that Blacklist Rules can denote suspicious or malicious calls and provide protection from them by using them in Rules to block or redirect those calls. But they can also be used to create "Watch and Alert" Rules for any key traffic. Or, you can use them to create a Rule to specifically allow certain calls you want, while a subsequent Rule blocks all other calls (and optionally provides the data for a corresponding CEP Alert Rule). For example, this might be valuable in the case of an attack, to ensure network availability for critical calls.

CEP Rules are used to alert on SEP Rule firings.

Orchestra One™ Verification Request Rules—Orchestra One Verification are Blacklist Allow Rules for integration with the Orchestra One Call Verification Service. See

Understanding Lists

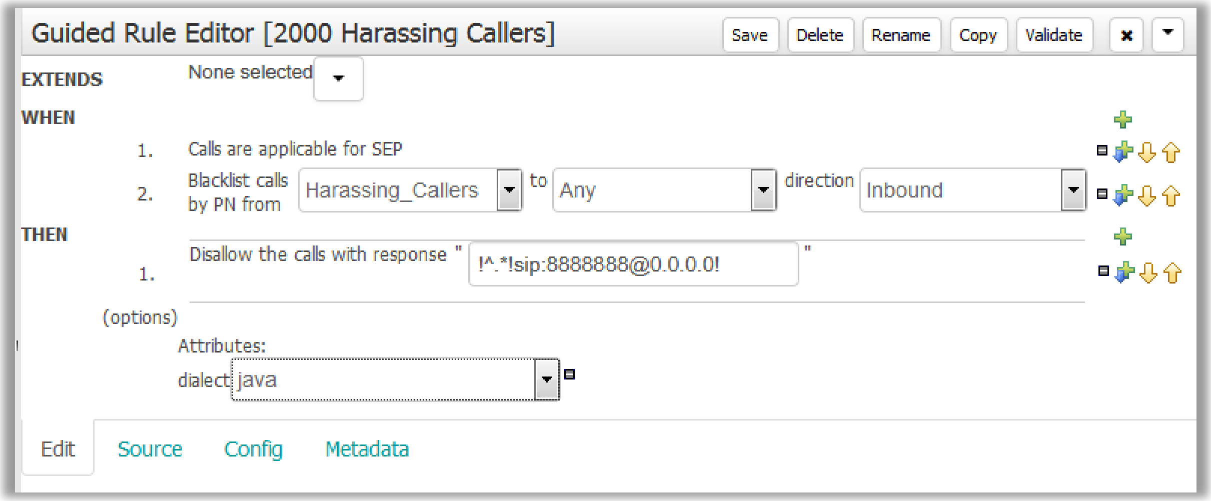
PolicyGuru SEP Rules use the following types of Lists to identify the called and calling numbers to which the Rule applies:

- *Whitelists* identify numbers/URIs for calls that are always to be allowed and not treated nor alerted on. They are used in *Whitelist Rules*.
- *Blacklists* contain numbers/URIs that are eligible for policy treatment (Termination or Redirection) and/or alerting. They are used in *Blacklist Rules*.

  As mentioned earlier, it is important to note that the term *Blacklist* does not denote that the numbers/URIs they contain are suspect or disallowed. Rather, it denotes listings that you want to be able to track or take action on.

  For example, you might have a **Harassing Callers** Blacklist of known harassing numbers you want to block and a **Specifically**

Allowed Callers Blacklist that you can use in the case of an attack to authorize specific calls, while a subsequent Rule blocks all others.



Guided Rule Editor [2000 Harassing Callers]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP
2. Blacklist calls by PN from Harassing_Callers to Any direction Inbound

THEN

1. Disallow the calls with response " !^.*!sip:8888888@0.0.0.0! "

(options)

Attributes:

dialect java

Figure 2: SEP Rule Terminating Numbers in the Harassing_Callers Blacklist

The example SEP Rule in Figure 2 above shows a Rule that blocks phone numbers from the **Harassing_Callers** Blacklist.

Calls are blocked by supplying a regular expression to redirect the call to a nonexistent endpoint, resulting in a **404 Not Found** response. You can choose regular expressions that suit your enterprise practices.

How Lists are Matched in Policy Processing

In SEP Policy processing, values in PN Lists are evaluated via full string matching and can consist of letters and/or digits. This means that, in addition to fully qualified phone numbers, you can specify values such as **INVALID** in a PN List and then configure the Phone Number Normalizer to append that value to certain phone numbers during normalization (for example, those that fail a certain function in a **libphonenumber** library lookup). Phone Numbers in ENUM Requests are processed by the Phone Number Normalizer before Policy processing occurs. Therefore, when that PN List is used in an SEP Rule, called or calling numbers that have been normalized to append **-INVALID** will match the Rule.

Note: See the *PolicyGuru® Meta-Policy Controller Installation and Configuration Guide* for details about phone number normalization/ denormalization in the PolicyGuru Solution.

Similarly, values in Regex Lists are processed as Regex, by determining if any part of the normalized phone number string matches the regular expression as specified in the listing. For example, a Regex value of **badnumber** would match **this_is_a_badnumber!** appended to a normalized number.

Note: You can optionally configure the Phone Number Normalizer to denormalize such phone numbers after Policy processing into a fully qualified format or into the original received format (or any format you choose) for storage in the database. Or you can choose not to denormalize such numbers and store them in the database with the flag appended so that you can generate reports on that flag.

Normalized Phone Numbers

When an ENUM Request is received, the ENUM Server processes the source and destination numbers it contains through a *phone number normalizer* prior to SEP Policy processing. This phone number normalizer is user-configurable. The result is a *normalized* phone number. Phone Number Normalization refers to processing the input from Session Border controllers in such a way that it is relevant to the systems at a given site. This can include, for example, adding or removing country codes, area codes, or exchange, or adding flags, such that the numbers can be processed by SEP Rules. Number normalization occurs prior to Policy processing.

How SEP Rules are Processed

Rules appear in the **Project Explorer** pane of the BRMS GUI in ASCII alphabetical order (1-10, a-z, A-Z). All Whitelist Rules are processed first in the order in which they appear in the **Project Explorer** pane. Next, all Blacklist Rules are processed in the order in which they appear. This is true even if Whitelist and Blacklist Rules are intermixed in the order.

Only one SEP Rule can match a given call. When a call matches a Rule, the Rule fires, and the call is not processed against any subsequent Rules.

Therefore, it is recommended you place Whitelist Rules first, because as noted above, Whitelist Rules are always processed first. To ensure they appear at the top of the list of Rules, use a numbering scheme to organize your Rules, both for processing and management. One such scheme would be to begin the Whitelist Rules with 1000, Blacklist Allow Rules with 2000, and Blacklist Terminate or Redirect Rules with 3000. Increment the next Rule of the same type by 20 to allow for additional Rules to be placed in between if needed.

For example:

1000 – Outbound Exec Calls

3000 – Block Harassing Callers

3020 – Suspected Fraudsters

If a pair of Rules has the same purpose and simply uses different Lists, you might number them sequentially so they always remain together as a group. For example:

3000 – Block Harassing Callers: National Harassing Callers List

3001 – Block Harassing Callers: Customer-Specific List

How Calls are Blocked and Redirected

Calls are blocked by supplying a regular expression (Regex) to redirect the call to a nonexistent endpoint host address, such as !^.*!sip:8888888@0.0.0.0!, resulting in a **404 Not Found** response. You can choose regular expressions that suit your enterprise practices.

Calls are redirected by supplying a regular expression to redirect the call to a different routable endpoint host address than that in the original invite. These Regex values are returned in the PolicyGuru ENUM response after the call data is received in the ENUM query.

As mentioned earlier, calls that match an SEP Rule specifying call treatment are terminated or redirected at call setup, preserving your network resources for legitimate business calls. Mid-call termination is not supported.

SEP Contingency Rules

SEP contingency Rules can be created using multiple **When** and **Then** statements, since only the first two **When** and the first **Then** clause are evaluated in Policy processing. This means you can have alternate criteria defined below the clauses that are evaluated, and then simply change the order of the clauses to change the Rule behavior or effectively disable it without having to delete it, in the event of changing conditions. To disable the Rule, define the first **When** clause such that it will never match a call.

Complex Event Processing (CEP) Policy

CEP Policy Rules are used to generate logging and alerts for SEP Rule firings. After you define an SEP Rule, you define a corresponding CEP Rule that defines the logging and alerting you want to occur when that SEP Rule fires.

How CEP Rules Are Processed

Unlike SEP Rules, CEP Rules have no processing order. They are processed continuously.

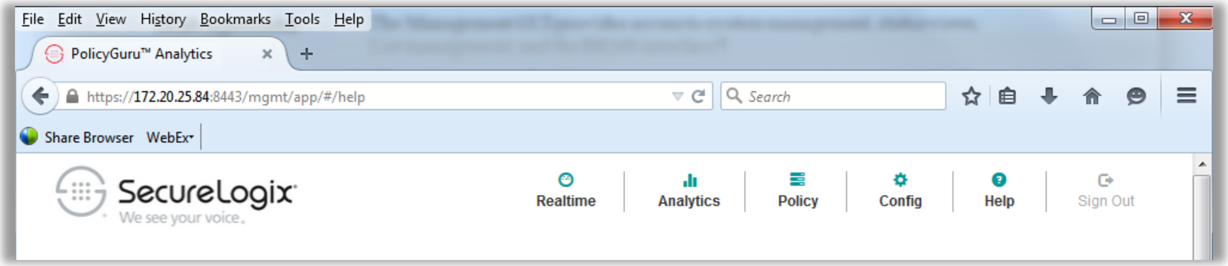
Tour of the Graphical User Interface (GUI)

The PolicyGuru Solution provides a web-based GUI for system and policy management. This GUI comprises two interfaces: the Management GUI and the BRMS GUI.

PolicyGuru® Main Menu

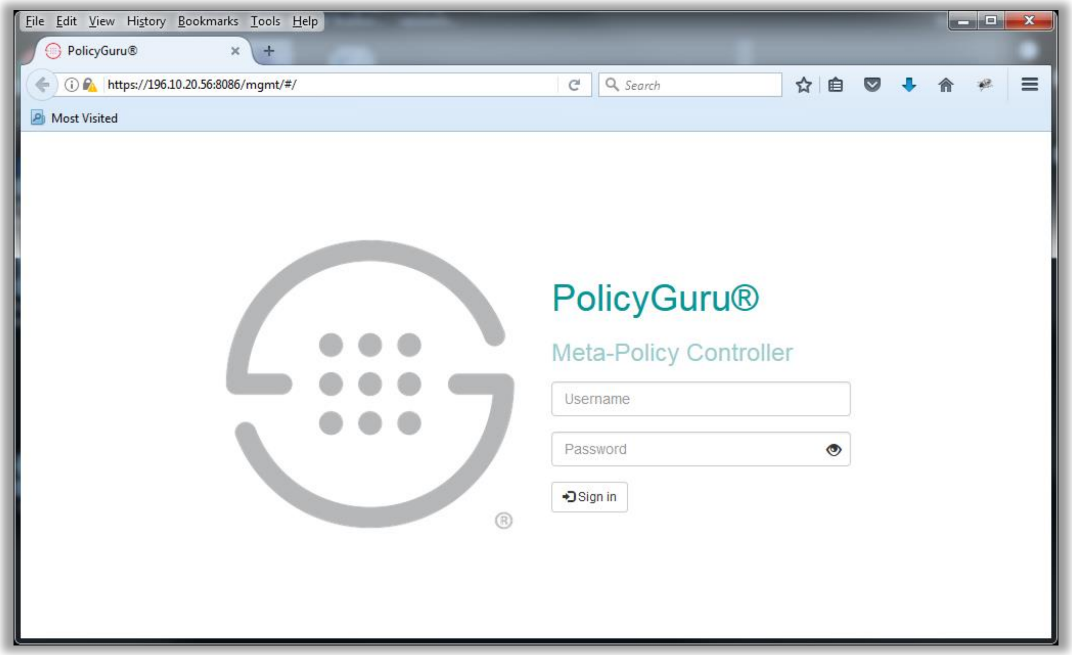
The PolicyGuru main menu shown below provides access for managing all of the features in the solution. This menu is always available, regardless of which tab or feature you are accessing.

(**Note**: The icons available to you may differ if you are using external LDAP, since application permissions are defined by LDAP group memberships, and only icons for those applications for which you have permission are visible to you.) Note that only the icon for the page you are viewing is highlighted; the image below is an illustration to make them more visible in this discussion.



Management GUI

The Management GUI provides access to system management, status views, Analytics reporting, List management, and the Policy interface. The login screen to the Management GUI is shown below.

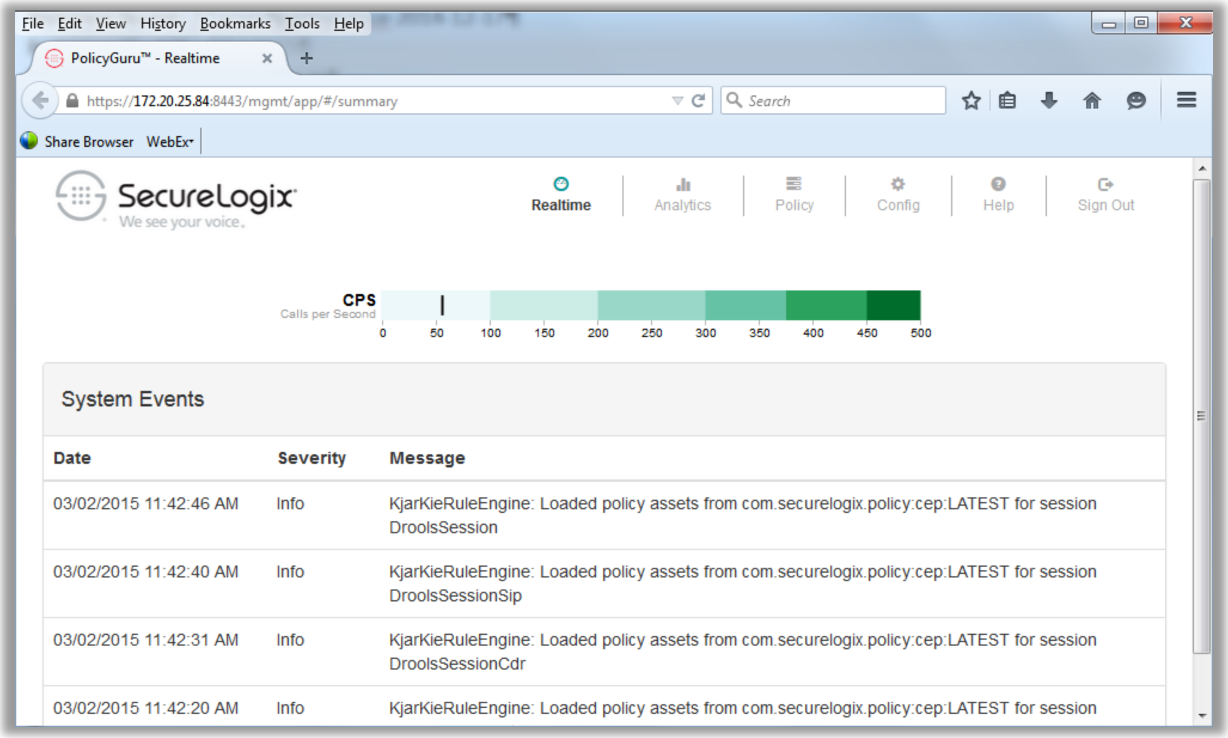


Note: By default, the GUI uses a self-signed SHA-256-SSL certificate. You can import a customer certificate. See “Importing a Customer

Certificate" in the *PolicyGuru*® *Meta-Policy Controller System Administration Guide* for instructions.

Realtime Tab

The **Realtime** tab shown below appears when you first log in to the Management Interface. It displays real-time system events and current calls per second (CPS) based on ENUM data. (**Note**: The screen that appears when you log in may differ if you are using external LDAP, since application permissions are defined by LDAP group memberships.)



System Events

Date	Severity	Message
03/02/2015 11:42:46 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSession
03/02/2015 11:42:40 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSessionSip
03/02/2015 11:42:31 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSessionCdr
03/02/2015 11:42:20 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session

Analytics Tab

The **Analytics** tab provides a predefined set of drill-down Analytics views that afford a graphical representation of call events. Two types of Analytics views are available: Call Detail Analytics and Phone Number Analytics.

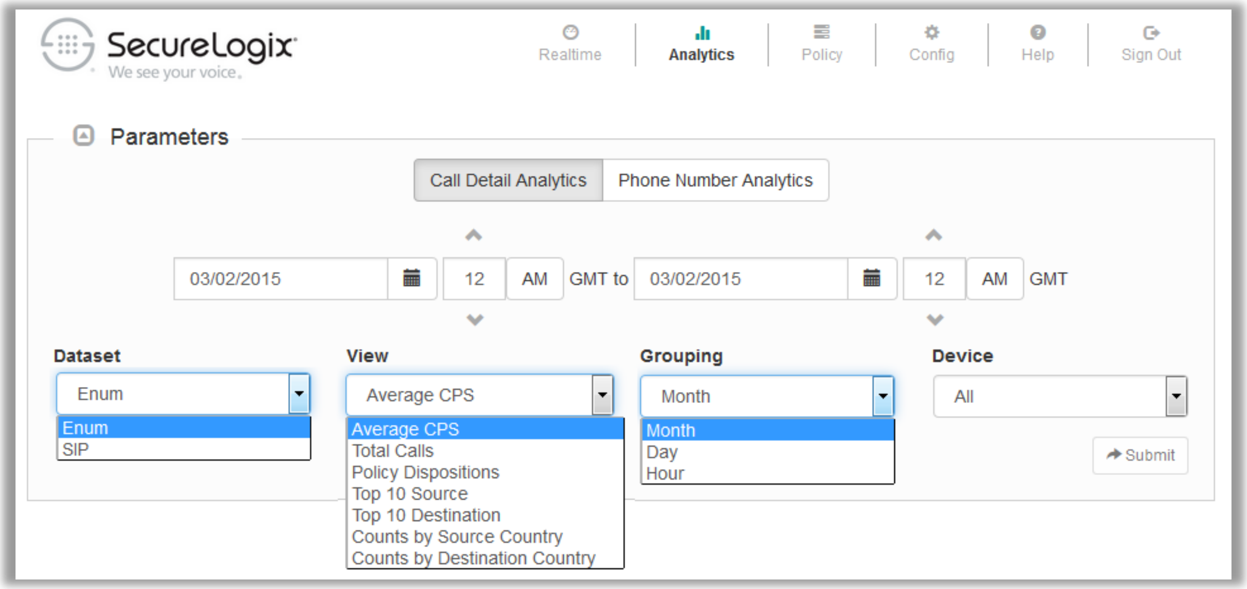
Call Detail Analytics

Call Detail Analytics provides drill-down reporting views. You can choose to view call details for either SIP data derived from the Meta-Data Probe or ENUM call processing data.

Call Detail Analytics views for ENUM data (as shown in the following figure) include:

- Average CPS
- Total Calls
- Policy Dispositions
- Top 10 Source
- Top 10 Destination
- Counts by Source Country

- Counts by Destination Country



03/02/2015 12 AM GMT to 03/02/2015 12 AM GMT

Dataset: Enum

View: Average CPS

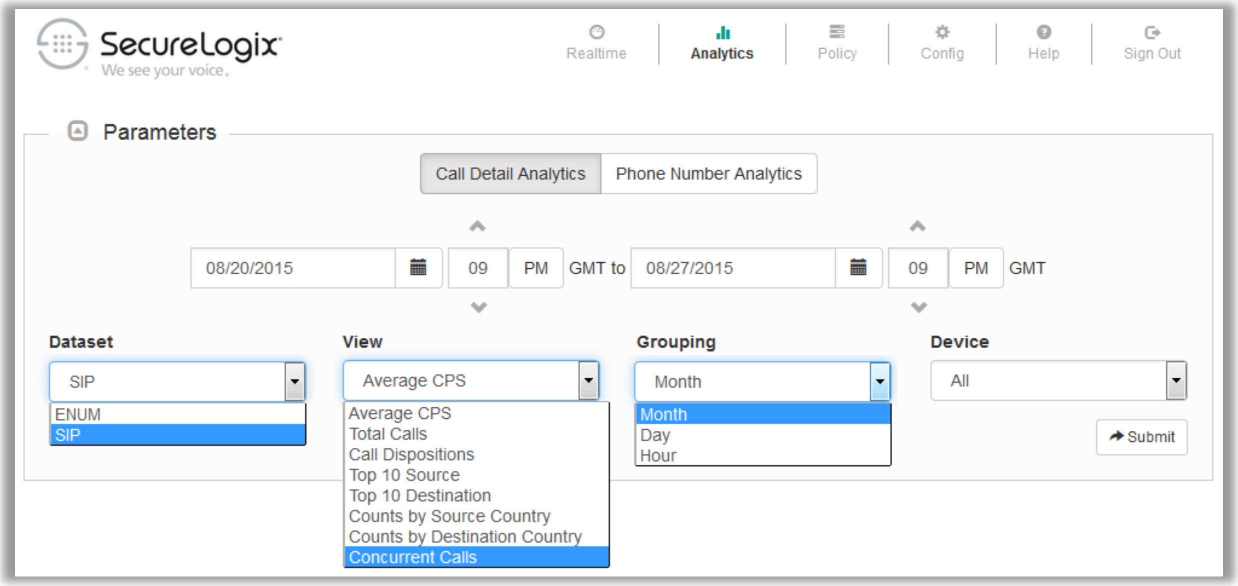
Grouping: Month

Device: All

Figure 3: ENUM Call Detail Analytics Options

Call Detail Analytics for SIP data derived by the Metadata Probe (as shown in the following figure) include:

- Average CPS
- Total Calls
- Call Dispositions
- Top 10 Source
- Top 10 Destination
- Counts by Source Country
- Counts by Destination Country
- Concurrent Calls



08/20/2015 09 PM GMT to 08/27/2015 09 PM GMT

Dataset: SIP
- ENUM
- SIP

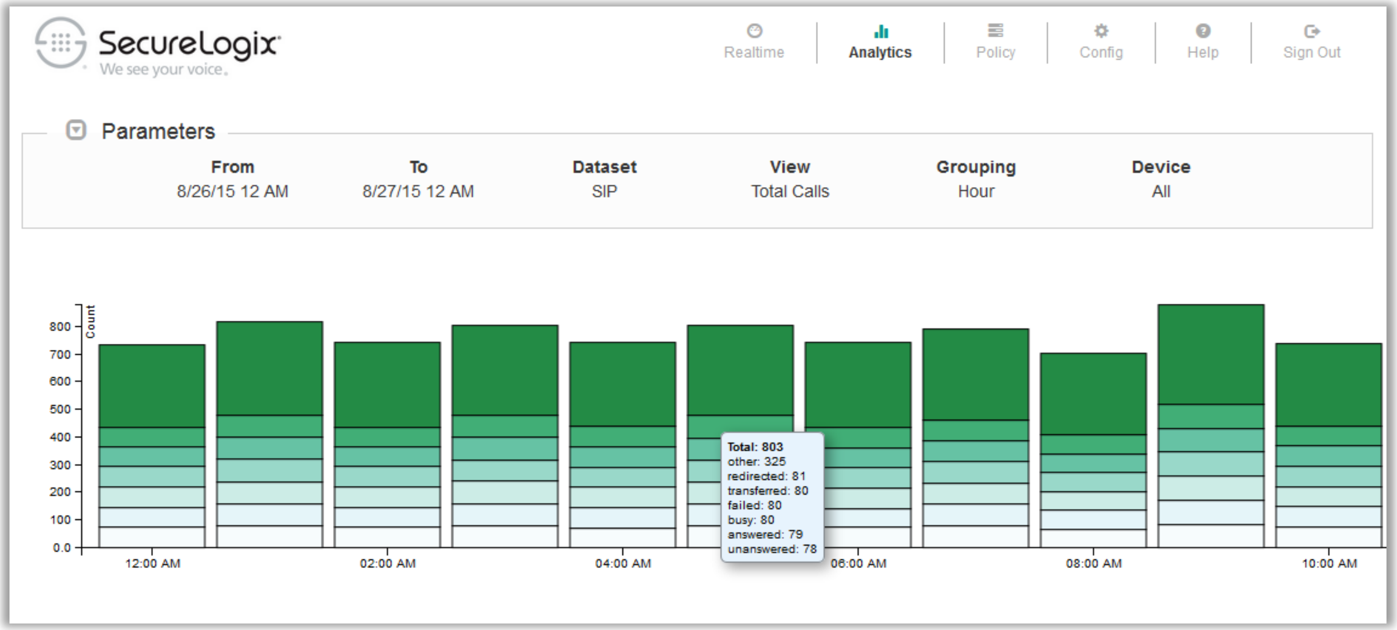
View: Average CPS
- Average CPS
- Total Calls
- Call Dispositions
- Top 10 Source
- Top 10 Destination
- Counts by Source Country
- Counts by Destination Country
- Concurrent Calls

Grouping: Month
- Month
- Day
- Hour

Device: All

Figure 4: SIP Call Detail Analytics Options

When you select criteria and click **Submit**, a chart view of the resulting analysis appears. When you hover your mouse cursor over the data in the display, details about the data appear as an onscreen tooltip.

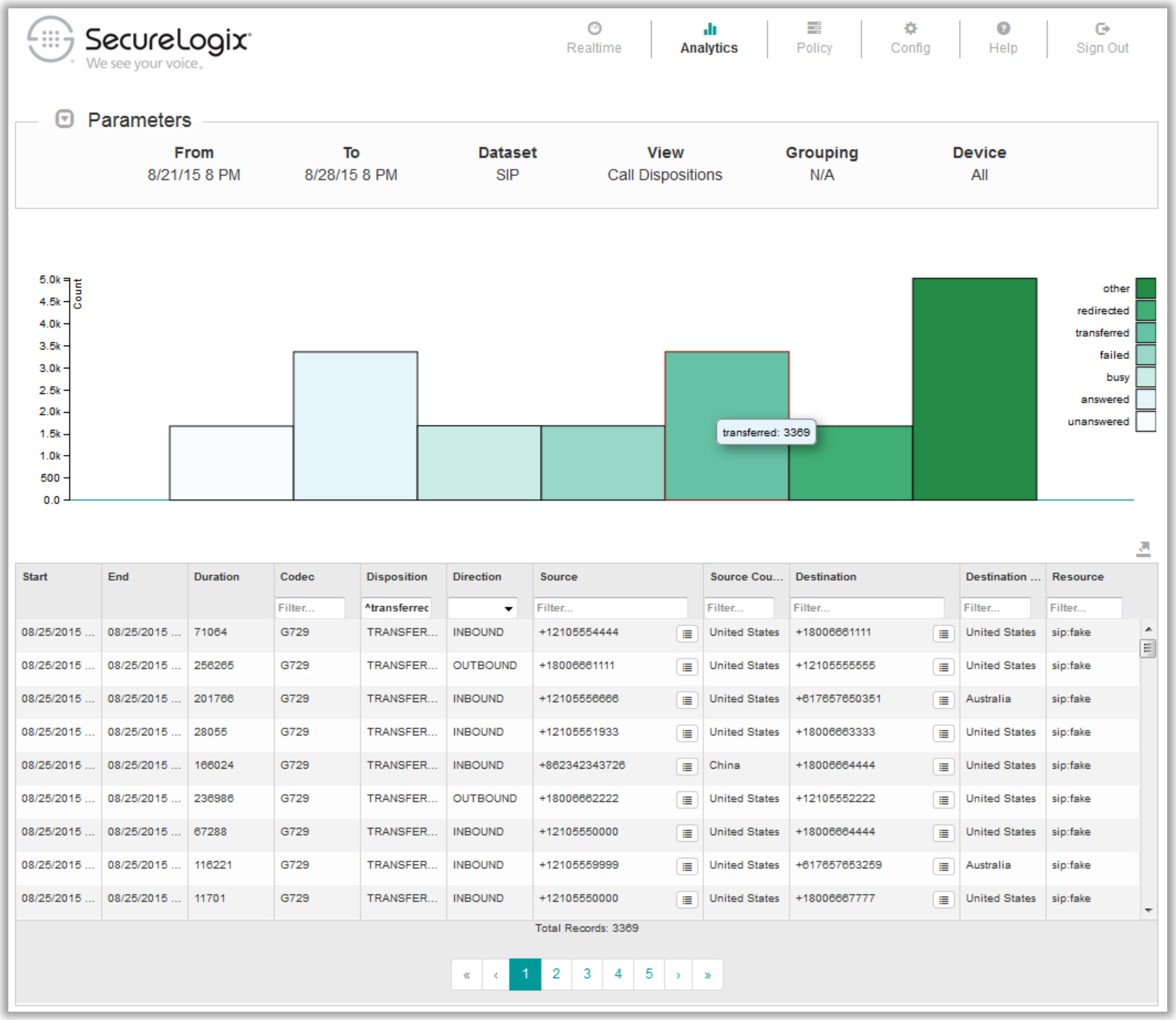


From	To	Dataset	View	Grouping	Device
8/26/15 12 AM	8/27/15 12 AM	SIP	Total Calls	Hour	All

Total: 803
other: 325
redirected: 81
transferred: 80
failed: 80
busy: 80
answered: 79
unanswered: 78

Figure 5: SIP Call Detail Analytics—Total Calls

Clicking the display provides a drill-down view of the selected information, as shown in Figure 6, which illustrates the SIP Call Details **Call Dispositions** Analytics view:



Parameters

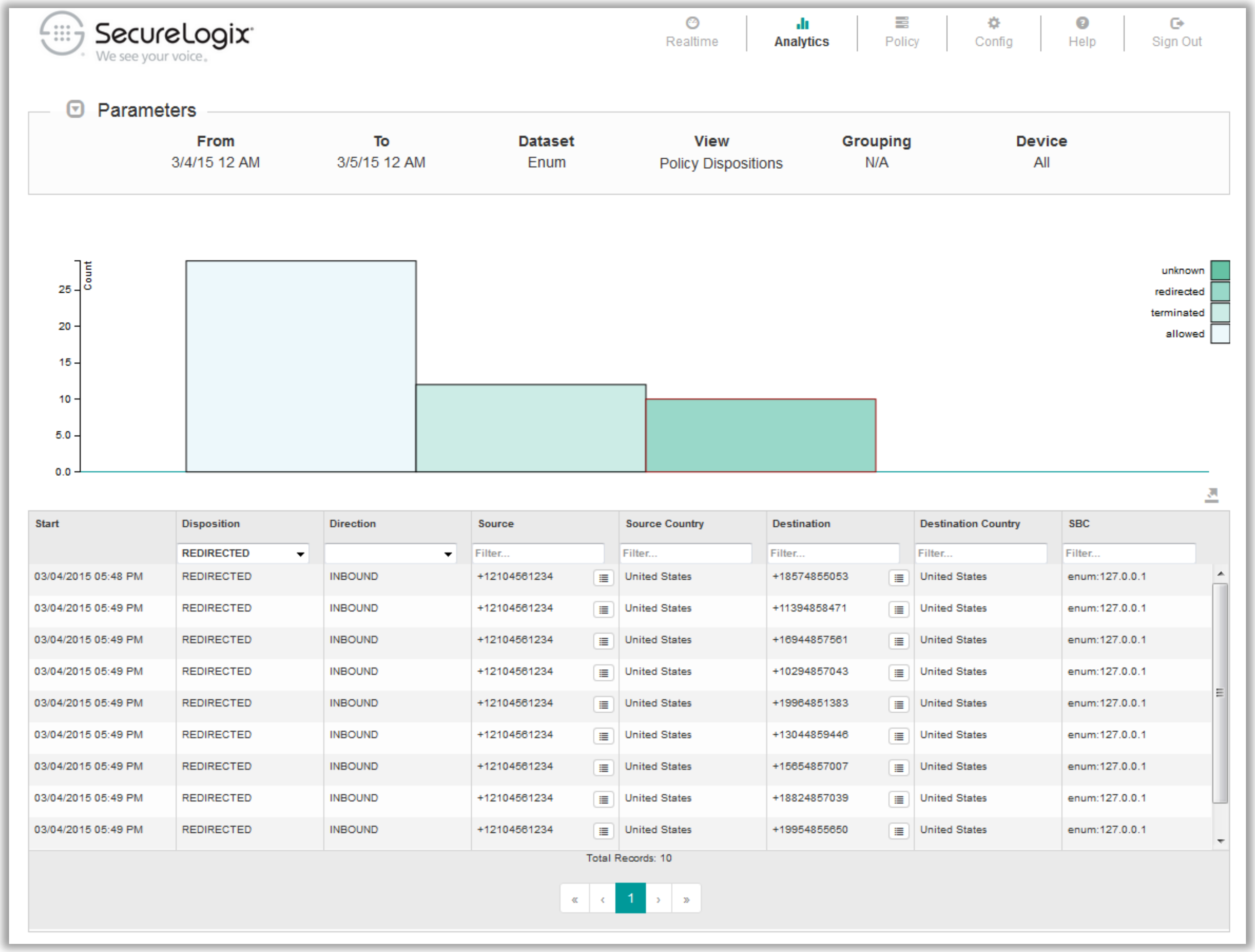
From	To	Dataset	View	Grouping	Device
8/21/15 8 PM	8/28/15 8 PM	SIP	Call Dispositions	N/A	All

Start	End	Duration	Codec	Disposition	Direction	Source	Source Cou...	Destination	Destination ...	Resource
			Filter...	^transferrec		Filter...	Filter...	Filter...	Filter...	Filter...
08/25/2015 ...	08/25/2015 ...	71064	G729	TRANSFER...	INBOUND	+12105554444	United States	+18006661111	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	256265	G729	TRANSFER...	OUTBOUND	+18006661111	United States	+12105555555	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	201766	G729	TRANSFER...	INBOUND	+12105556666	United States	+617657650351	Australia	sip:fake
08/25/2015 ...	08/25/2015 ...	28055	G729	TRANSFER...	INBOUND	+12105551933	United States	+18006663333	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	166024	G729	TRANSFER...	INBOUND	+862342343726	China	+18006664444	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	236986	G729	TRANSFER...	OUTBOUND	+18006662222	United States	+12105552222	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	67288	G729	TRANSFER...	INBOUND	+12105550000	United States	+18006664444	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	116221	G729	TRANSFER...	INBOUND	+12105559999	United States	+617657653259	Australia	sip:fake
08/25/2015 ...	08/25/2015 ...	11701	G729	TRANSFER...	INBOUND	+12105550000	United States	+18006667777	United States	sip:fake

Total Records: 3369

« ‹ 1 2 3 4 5 › »

Figure 6: SIP Call Detail Analytics—Call Dispositions



Parameters

From	To	Dataset	View	Grouping	Device
3/4/15 12 AM	3/5/15 12 AM	Enum	Policy Dispositions	N/A	All

Start	Disposition	Direction	Source	Source Country	Destination	Destination Country	SBC
	REDIRECTED		Filter...	Filter...	Filter...	Filter...	Filter...
03/04/2015 05:48 PM	REDIRECTED	INBOUND	+12104561234	United States	+18574855053	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+11394858471	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+16944857561	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+10294857043	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+19964851383	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+13044859446	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+15654857007	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+18824857039	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+19954855650	United States	enum:127.0.0.1

Total Records: 10

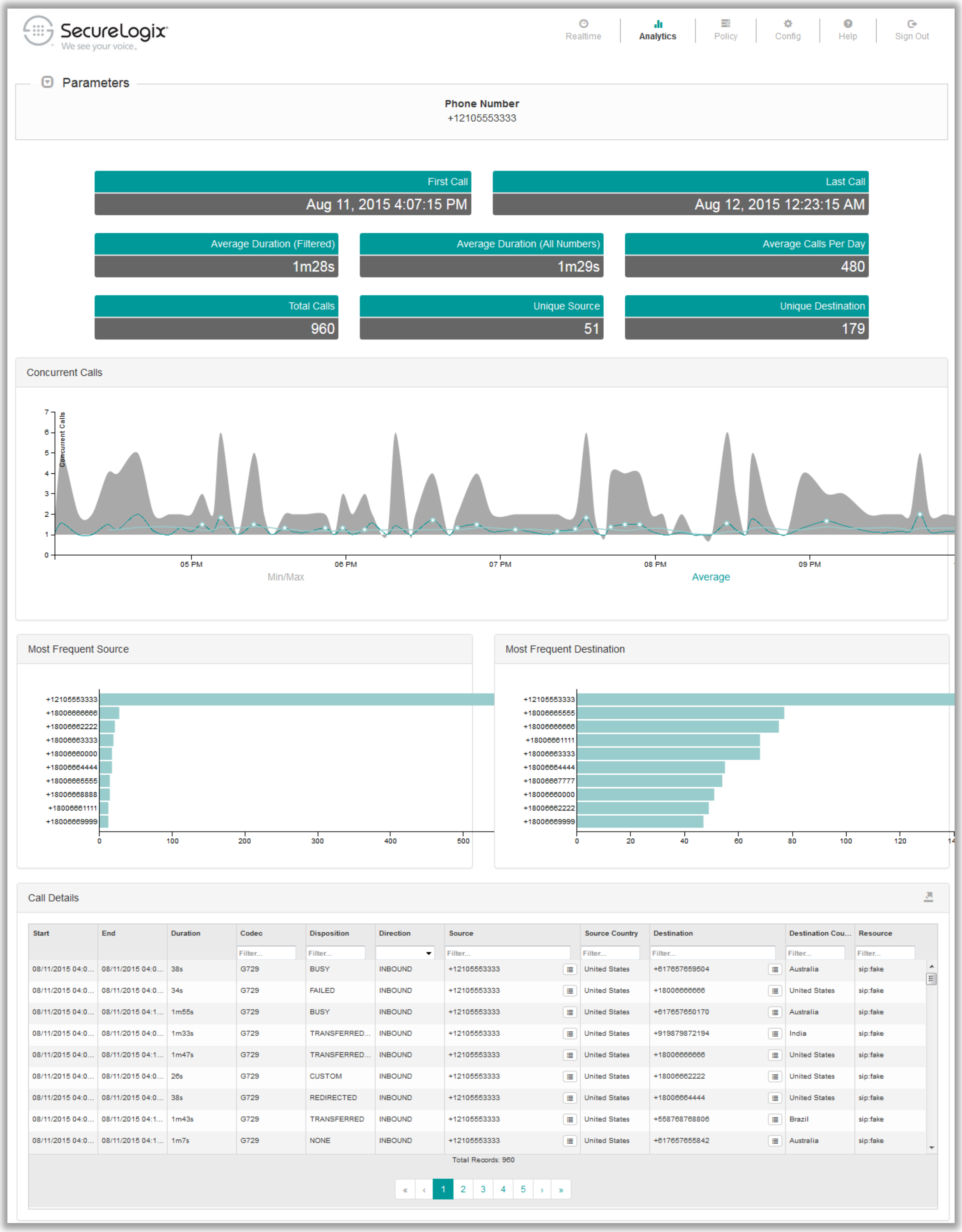
Figure 7: Drill-Down Analytics – Policy Dispositions Call Details

The Analytics application provides more than a view of the information; it also allows you to take action regarding the called and calling numbers provided in the call details. From this drill-down detail view, you can click an icon next to any source or destination and add it to a Whitelist or Blacklist, as appropriate, without needing to toggle between screens.

Note: If you add numbers to Lists used in installed SEP Rules, the Policy must be installed again to effect the changes on the ENUM Server(s) that are enforcing the SEP Policy.

Phone Number Analytics

Phone Number Analytics provides a means for forensic investigation of a specific phone number of interest or a set of phone numbers (such as all of those with +210555) derived from Metadata Probe (SIP) data. You simply type the number of interest in the **Phone Number** field and click **Submit**. All call information for that number is provided in graphs, charts, and tables below the **Search** field. This option is shown in the following figure.



Parameters

Phone Number
+12105553333

First Call	Last Call
Aug 11, 2015 4:07:15 PM	Aug 12, 2015 12:23:15 AM

Average Duration (Filtered)	Average Duration (All Numbers)	Average Calls Per Day
1m28s	1m29s	480

Total Calls	Unique Source	Unique Destination
960	51	179

Concurrent Calls

Most Frequent Source

Most Frequent Destination

Call Details

Start	End	Duration	Codec	Disposition	Direction	Source	Source Country	Destination	Destination Cou...	Resource
			Filter...	Filter...		Filter...	Filter...	Filter...	Filter...	Filter...
08/11/2015 04:0...	08/11/2015 04:0...	38s	G729	BUSY	INBOUND	+12105553333	United States	+617657659504	Australia	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	34s	G729	FAILED	INBOUND	+12105553333	United States	+18006666666	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m55s	G729	BUSY	INBOUND	+12105553333	United States	+617657650170	Australia	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	1m33s	G729	TRANSFERRED...	INBOUND	+12105553333	United States	+919879872194	India	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m47s	G729	TRANSFERRED...	INBOUND	+12105553333	United States	+18006666666	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	26s	G729	CUSTOM	INBOUND	+12105553333	United States	+18006662222	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	38s	G729	REDIRECTED	INBOUND	+12105553333	United States	+18006664444	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m43s	G729	TRANSFERRED	INBOUND	+12105553333	United States	+558768768806	Brazil	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m7s	G729	NONE	INBOUND	+12105553333	United States	+617657655842	Australia	sip:fake

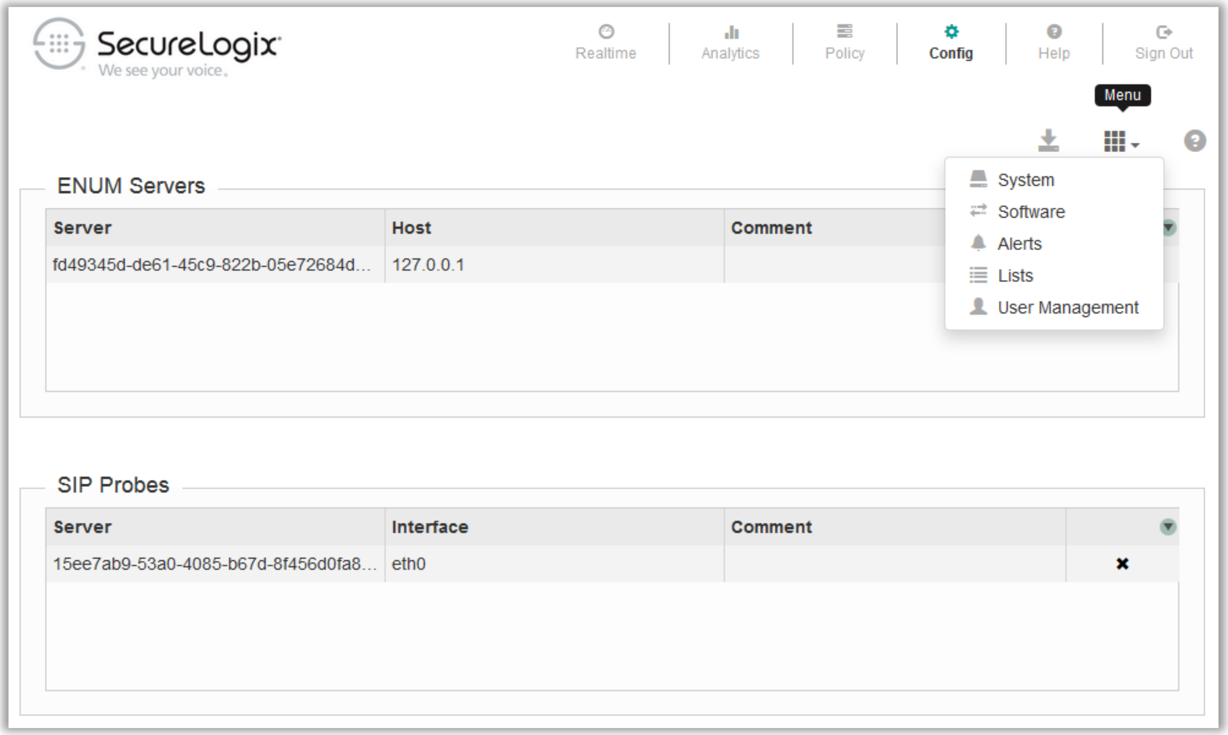
Total Records: 960

Figure 8: Phone Number Analytics

Config Tab

The **Config** tab, shown in Figure 9, provides access to system configuration items, including:

- List management.
- User management.
- A view of which ENUM Servers are connected to this Mediation Server and a field defining the IP address for connections to them.
- A view of which Metadata Probes are connected to this Mediation Server and a field defining the Ethernet port for connections to them.
- Alert configuration.



ENUM Servers

Server	Host	Comment
fd49345d-de61-45c9-822b-05e72684d...	127.0.0.1	

SIP Probes

Server	Interface	Comment	
15ee7ab9-53a0-4085-b67d-8f456d0fa8...	eth0		✖

Figure 9: Config Tab

Note: The **Software** option is not used.

Policy Tab

The **Policy** tab provides access to the BRMS Interface from which you manage SEP and CEP Policies. Refer to Figure 1for an illustration of the BRMS GUI. More information about the BRMS interface is provided later .in this document.

Help Link

The **Help** link provides contact information for Customer Support and copyright, legal, and licensing notices.

Sign Out Link

The **Sign Out** link signs you out of the PolicyGuru Web Application.

BRMS GUI

When you click **Policy** on the main menu, the following GUI appears from which you access the Policies.

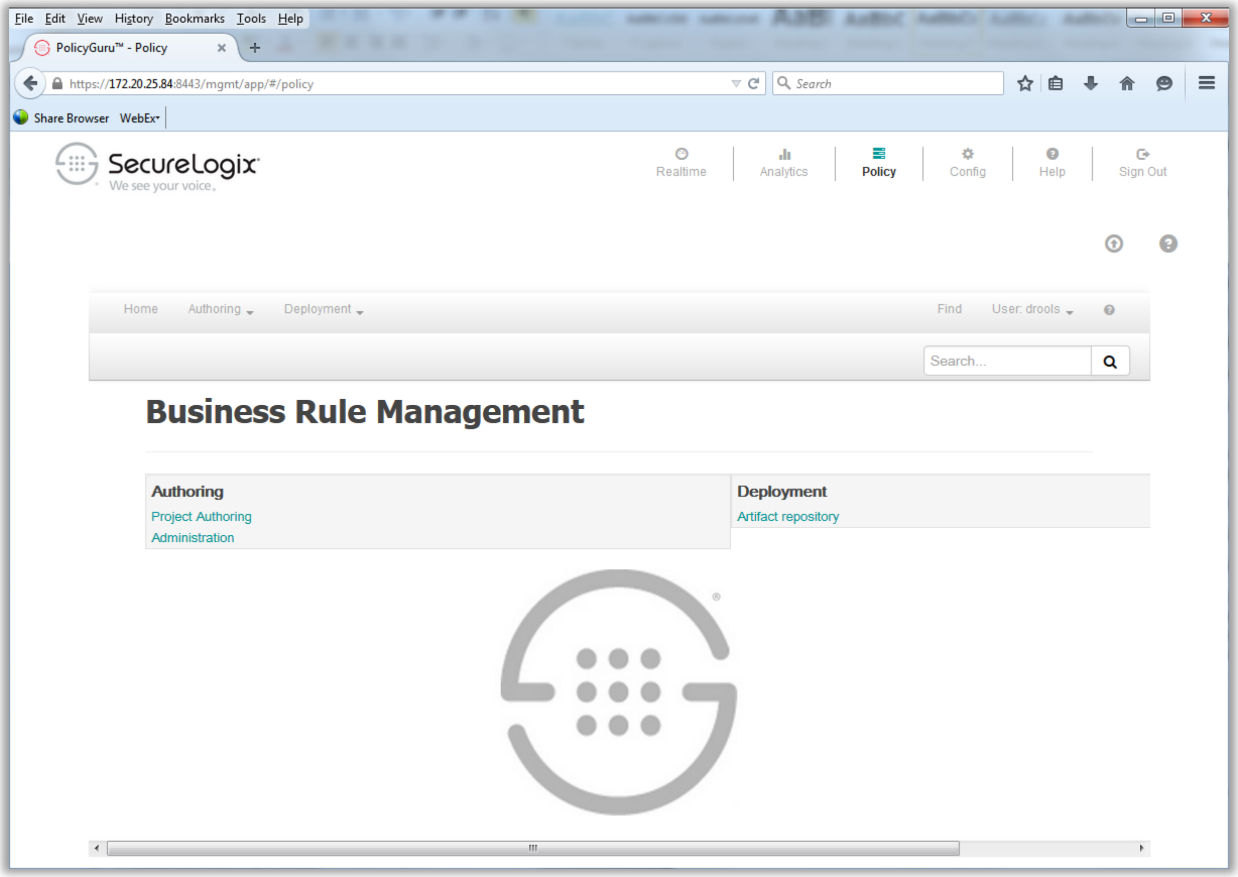
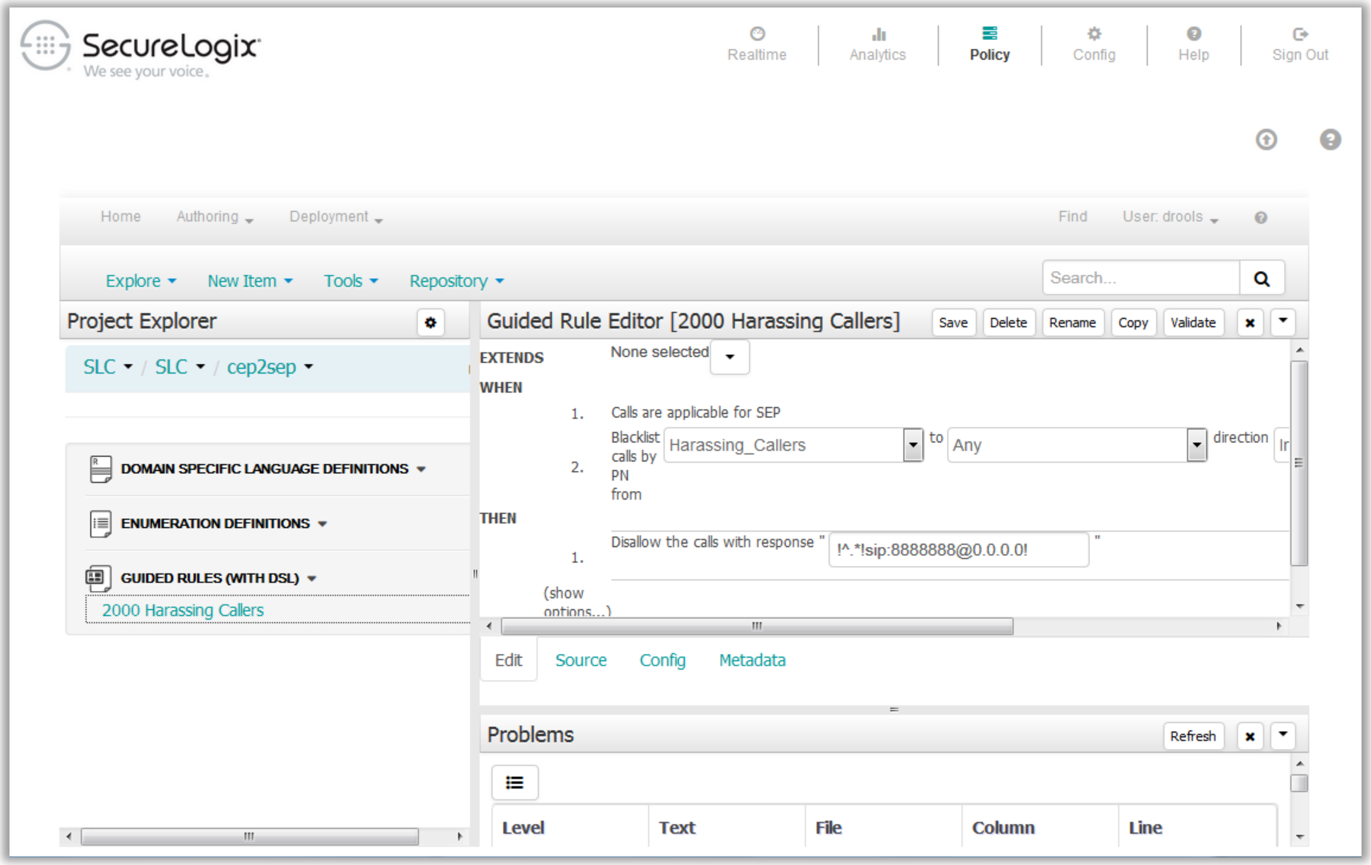


Figure 10: BRMS Initial GUI

BRMS Project Authoring GUI

Policy Management is accomplished in the BRMS Project Authoring GUI. This GUI provides a **Project Explorer** pane in which you access Policy functions, a **Project Editor** pane in which you define SEP and CEP Rules, and a set of menus for accomplishing tasks.



EXTENDS None selected

WHEN

1. Calls are applicable for SEP
2. Blacklist calls by PN from Harassing_Callers to Any direction

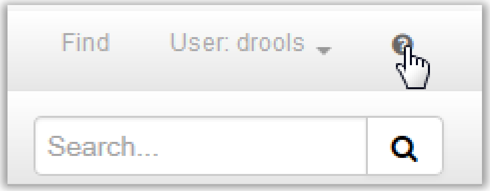
THEN

1. Disallow the calls with response " !^.*!sip:8888888@0.0.0.0! "

(show options...)

Figure 11: BRMS Project Authoring View

The small icon to the right of the username and above the **Search** box provides pictorial BRMS GUI Help.



Detailed instructions for defining SEP and CEP Policy Rules are provided later in this guide.

Getting Started

Policy Use Case Tutorial

The PolicyGuru Solution provides powerful Rule-creation capabilities. This quick start tutorial walks you through a sample use case to familiarize you with the work flow for creating and implementing a Rule set.

It is recommended that you read the "Concepts" section that begins on page 8 before you begin this tutorial.

In this tutorial, you will define the following set of Rules:

- A Blacklist Rule to block inbound calls from certain headhunters known to be calling key employees at your organization (SEP).
- A Blacklist Rule to block outbound calls to Guatemala (SEP).
- A Whitelist Rule to always allow calls from your Executive personnel without tracking (SEP).
- An alerting Rule for attempted outbound calls to Guatemala (CEP).

Overview of Steps

In this tutorial, you learn how to:

1. Log in to the PolicyGuru GUI.
2. Create a Phone Number (PN) Blacklist, a Regex Blacklist, and a PN Whitelist.
3. Define SEP Rules and CEP Alerting Rules.
4. Install the SEP Policy and the CEP Policy.
5. Edit a PN Blacklist and then reinstall the SEP Policy.

1. Log in to the Web-Based Management Console

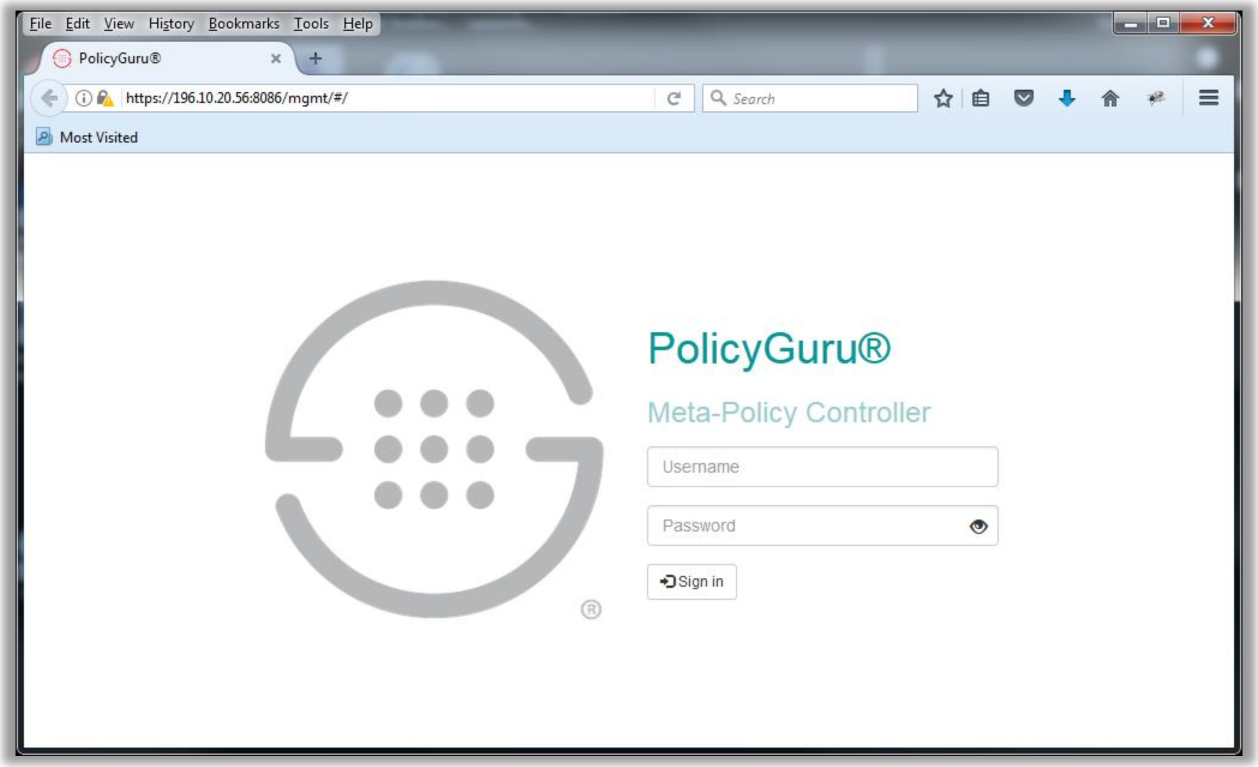
The web-based Graphical User Interface (GUI) supports following browsers:

- Internet Explorer (version 11 or later)
- Mozilla Firefox
- Google Chrome

Note: By default, the GUI uses a self-signed SHA-256-SSL certificate. You can import a customer certificate. See "Importing a Customer Certificate" in the *PolicyGuru® Meta-Policy Controller System Administration Guide* for instructions.

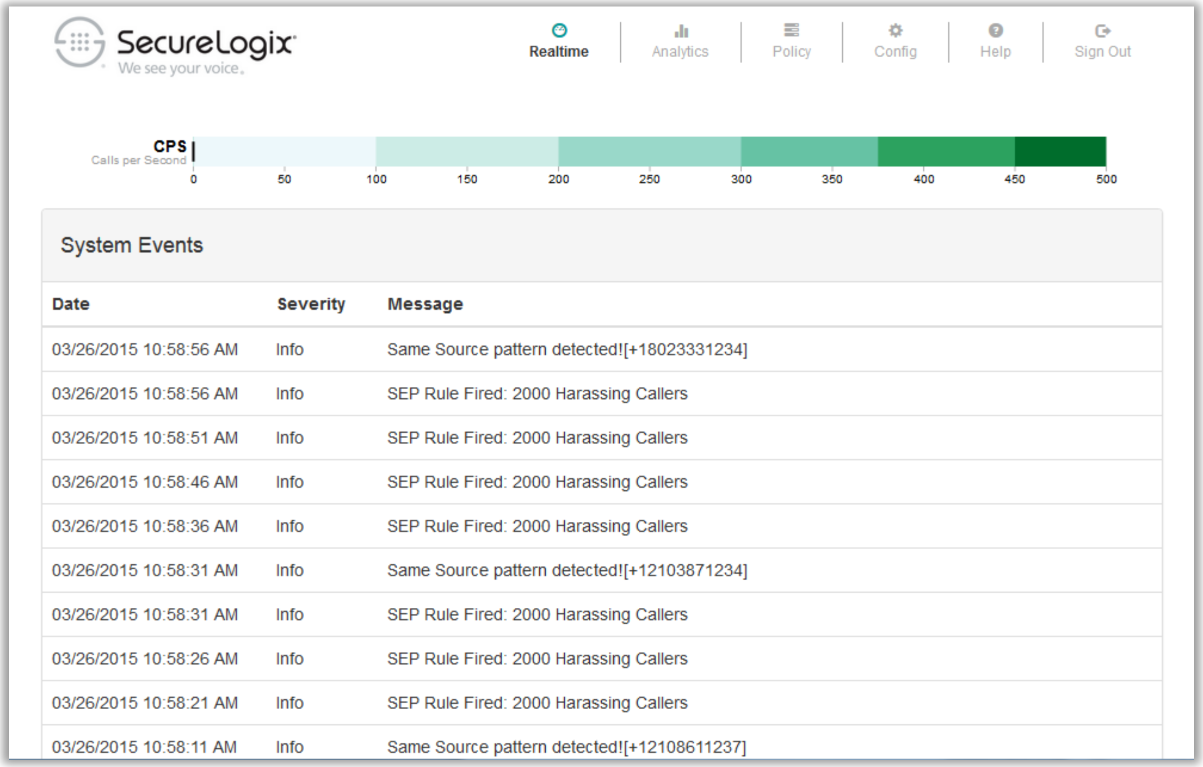
To log in to the PolicyGuru® Management Application

- In a supported browser, log in to the PolicyGuru application with the URL, username, and password your system administrator provided.



The **PolicyGuru® Management Application** appears with the **Realtime** tab displayed.

Note: The screen that appears when you log in may differ if you are using external LDAP, since in that case application permissions are defined by LDAP group memberships.



System Events

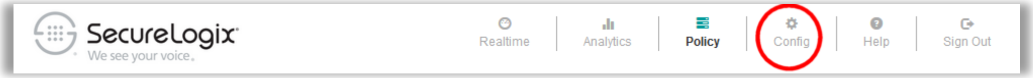
Date	Severity	Message
03/26/2015 10:58:56 AM	Info	Same Source pattern detected![+18023331234]
03/26/2015 10:58:56 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:51 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:46 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:36 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:31 AM	Info	Same Source pattern detected![+12103871234]
03/26/2015 10:58:31 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:26 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:21 AM	Info	SEP Rule Fired: 2000 Harassing Callers
03/26/2015 10:58:11 AM	Info	Same Source pattern detected![+12108611237]

2. Create Lists

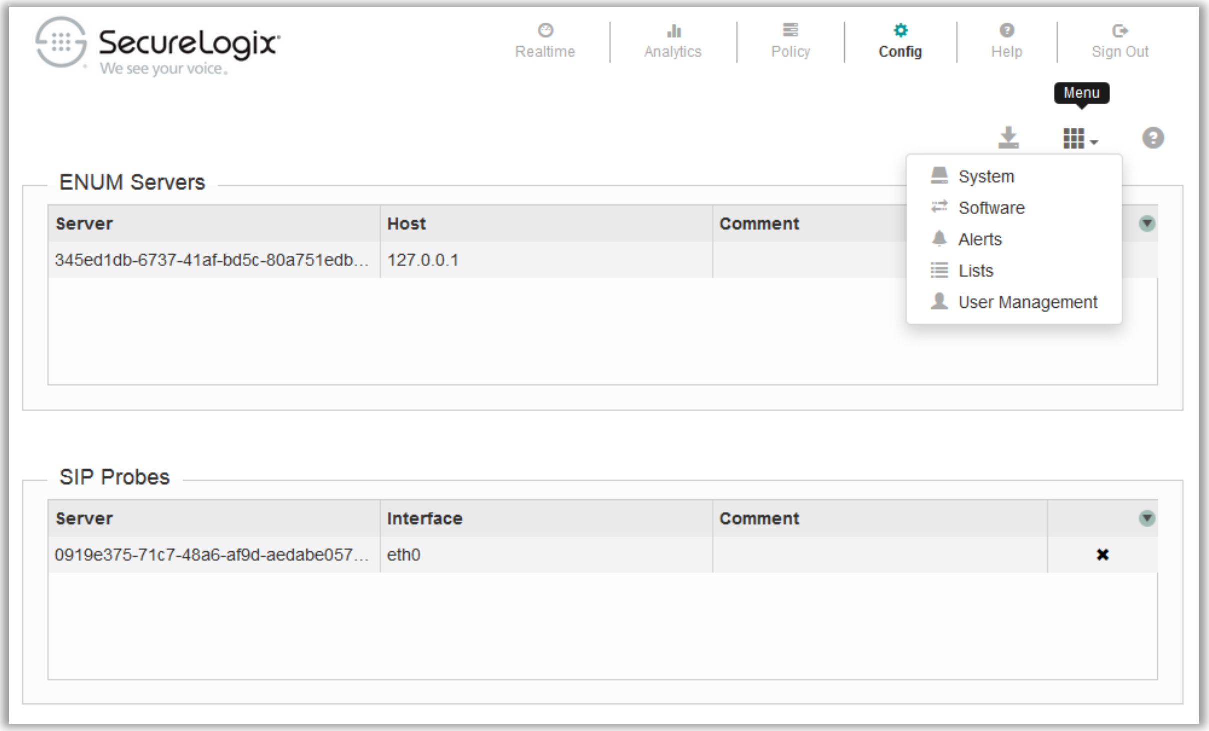
Next, you’ll create the Lists that you’ll use in your SEP Rules.

To access the Lists dialog box

1. On the PolicyGuru main menu, click **Config**. The main menu is available from all screens in the GUI.



2. Click the **Configuration** drop-down menu.



ENUM Servers

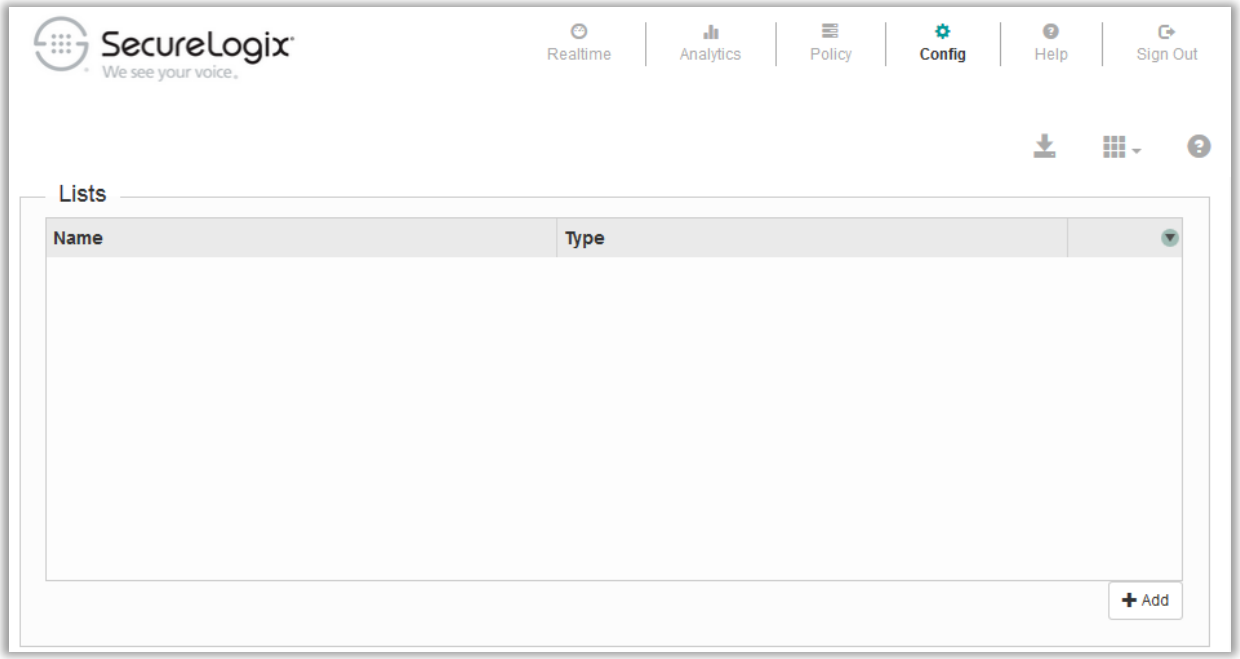
Server	Host	Comment
345ed1db-6737-41af-bd5c-80a751edb...	127.0.0.1	

SIP Probes

Server	Interface	Comment	
0919e375-71c7-48a6-af9d-aedabe057...	eth0		✖

3. Click **Lists**.

4. The **Lists** screen appears.



Lists

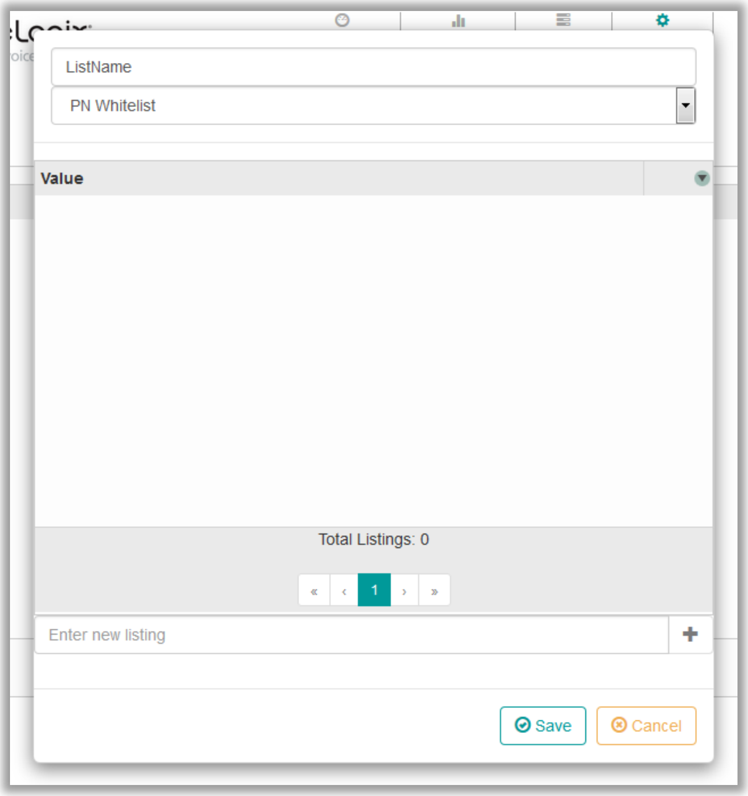
Name	Type

a. *Create a PN Blacklist*

First, create a PN Blacklist named `Headhunters_SRC`. You'll use this List as the Source of the Rule to block inbound headhunters. PN Blacklists can contain one or more individual phone numbers and/or URIs.

To create a PN Blacklist

1. On the **Lists** screen, click **Add** at the bottom right.
2. The **List** dialog box appears.



ListName

PN Whitelist

Value

Total Listings: 0

Enter new listing

3. In the **ListName** field, type:
   `Headhunters_SRC`
4. Click the down arrow in the second field and click **PN Blacklist**.
5. In the **Enter New Listing** field, type a test phone number from which you can make an inbound call. Phone numbers should typically be defined in the form **`+cclocalnumber`** (without spaces or punctuation), since the PolicyGuru Solution normalizes the source and destination phone numbers into the formats defined by your Phone Number Normalizer script prior to comparing them against the SEP policy. The normalized numbers must match the List entries for a Rule to fire on that number.
6. Click the PLUS SIGN (**+**) next to the number you typed, or press ENTER. The phone number appears in the List.
7. Click **Save**. You are returned to the **Lists** screen, which now shows the **Headhunters_SRC** Blacklist. Continue below.

Note: See also “How Lists are Matched in Policy Processing” on page 11 for important details on what Lists can contain and how they are processed.

b. Create a Regex Blacklist

Next, you’ll create a Regex Blacklist to watch for calls to Guatemala. Regex Lists are used to define ranges and wildcards.

To create a Regex Blacklist

1. On the **Lists** screen, click **Add** again.

2. In the **ListName** field, type:
   `Guatemala_DST`

3. Click the down arrow in the second field and then click **Regex Blacklist**.

4. In the **Enter new listing** field, type the Regex that represents the country code for Guatemala: ^\+502

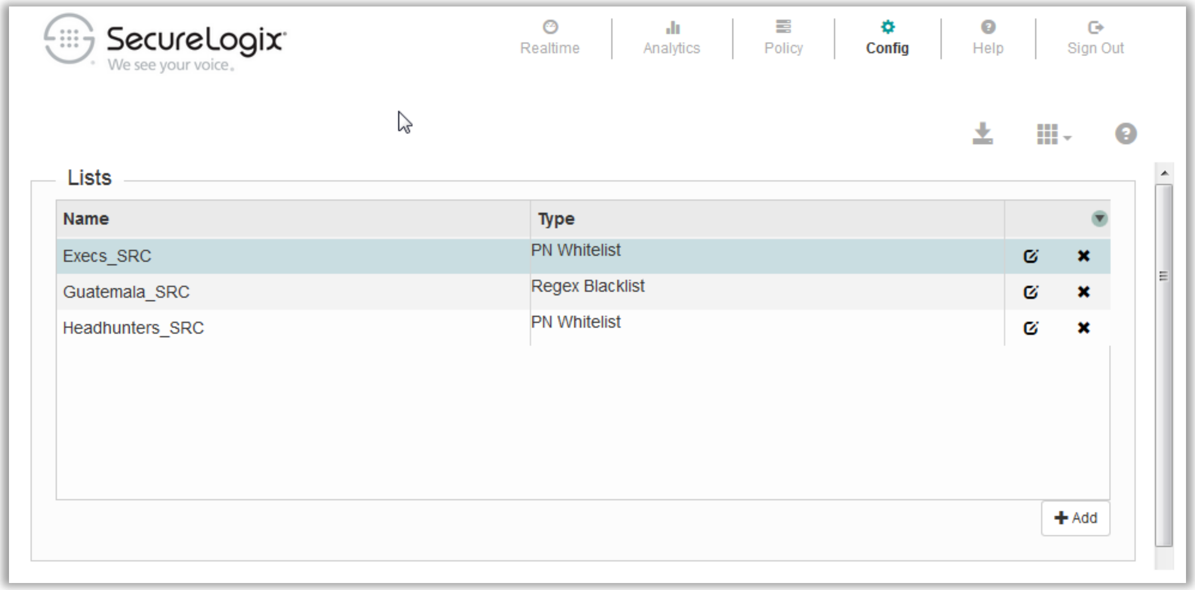
5. Click the PLUS SIGN (**+**) or press ENTER and then click **Save**.

c. *Create a PN Whitelist*

Now you'll define a PN Whitelist to use in a Rule that ensures your executives' calls are never blocked nor redirected. For this exercise, you'll type only one number just for illustration.

To define a PN Whitelist

1. On the **Lists** screen, click **Add** and then type the name `Execs_SRC` in the **ListName** box.
2. Click the down arrow and select **PN Whitelist**.
3. Type a phone number in the proper format.
4. Press ENTER and then click **Save**.



Lists

Name	Type
Execs_SRC	PN Whitelist
Guatemala_SRC	Regex Blacklist
Headhunters_SRC	PN Whitelist

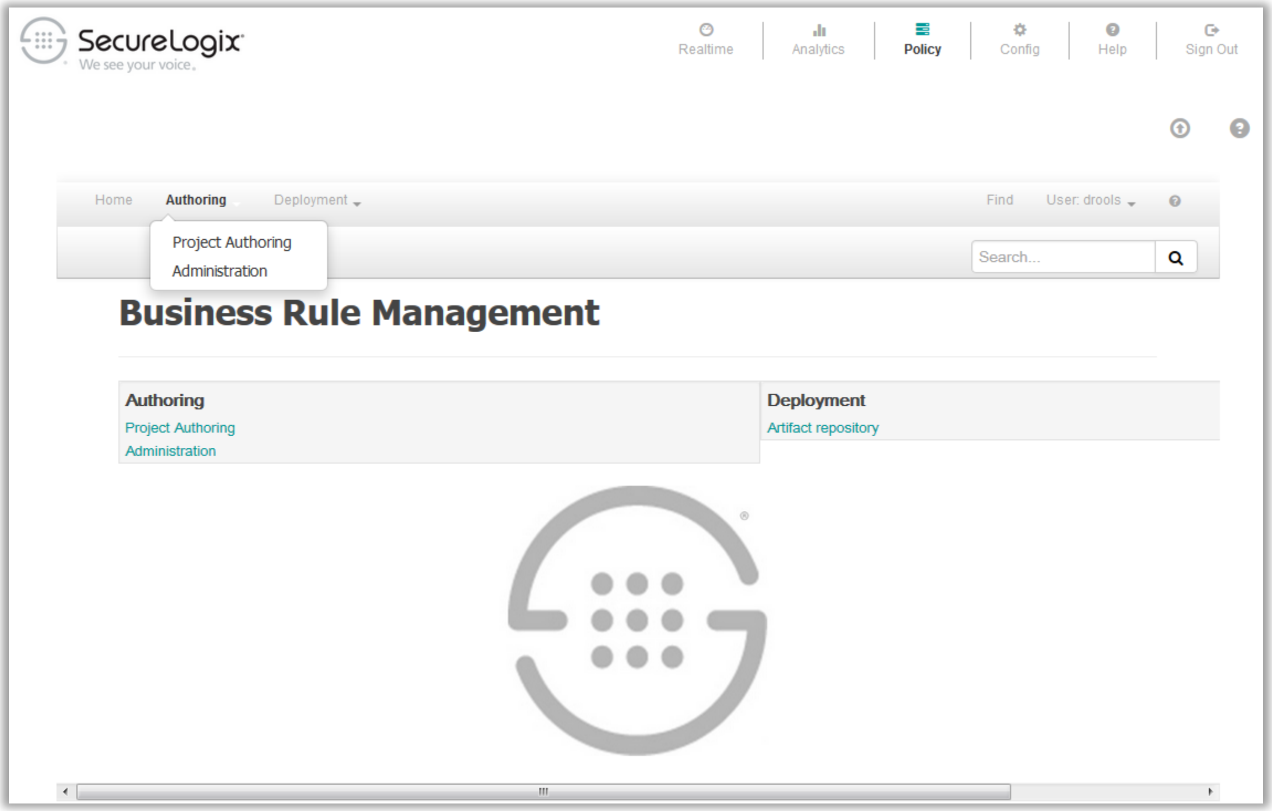
3. Define and Install Policy Rules

Now that you have a set of Lists, you're ready to define your Rules. After you define the Rules, you'll install the SEP Policy on the ENUM Servers in your deployment.

To prepare to define Rules

1. Click **Policy** on the PolicyGuru main menu. (**TIP**: For easier workflow, you can right-click the PolicyGuru main menu options and click "Open link in new tab" so that you can easily navigate between the open screens in your browser.)

The BRMS GUI appears.



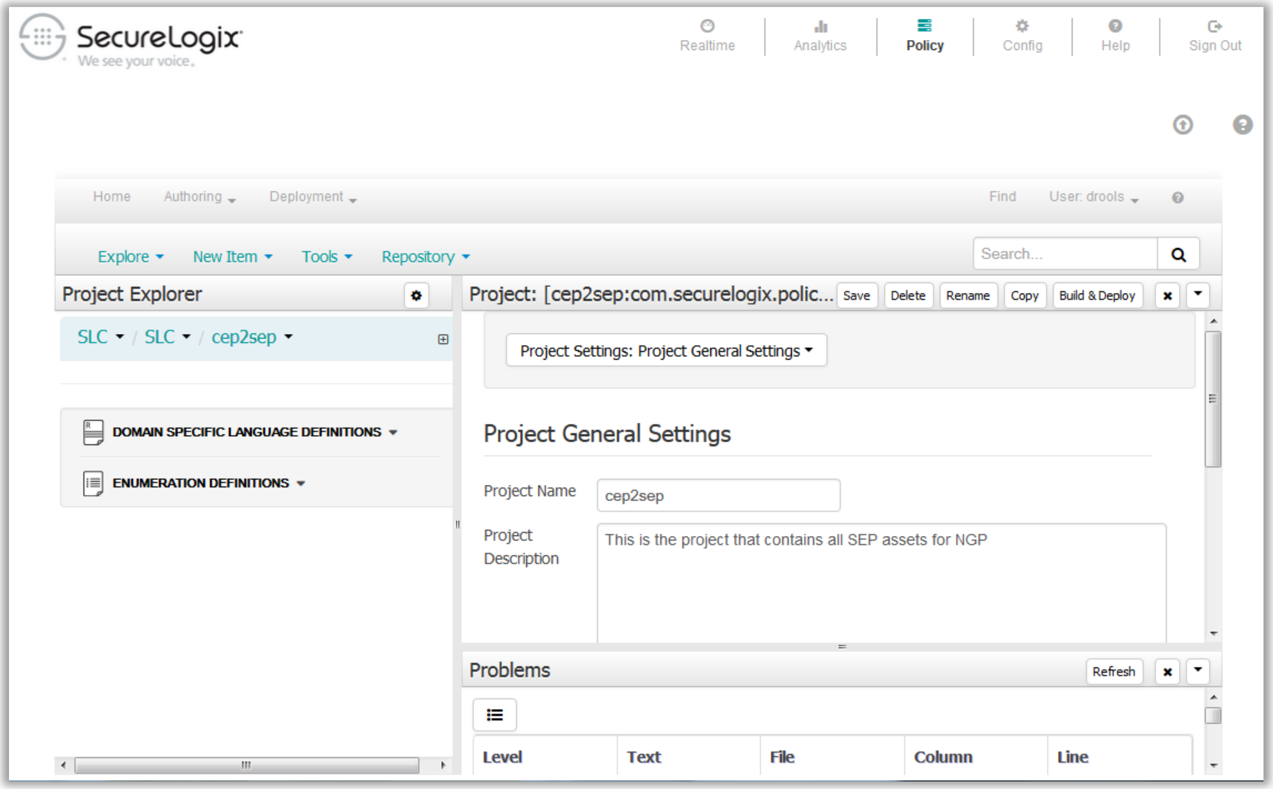
Business Rule Management

Authoring
Project Authoring
Administration

Deployment
Artifact repository

2. Click **Authoring | Project Authoring**, or click the **Project Authoring** link in the left center of the screen.

3. The **Project Authoring** window appears. It contains a **Project Explorer** pane and an **Editor** pane.



Project Name: cep2sep

Project Description: This is the project that contains all SEP assets for NGP

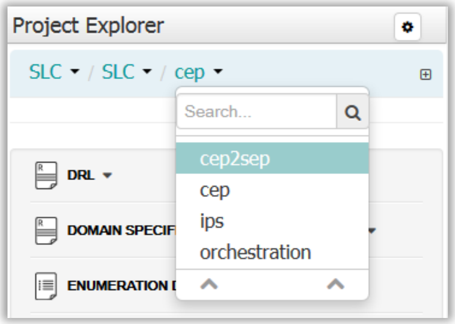
Level	Text	File	Column	Line

IMPORTANT: If you are using an external LDAP login for the first time, see “Important Information About First-Time Login via External LDAP” on page 41 and follow those instructions before continuing.

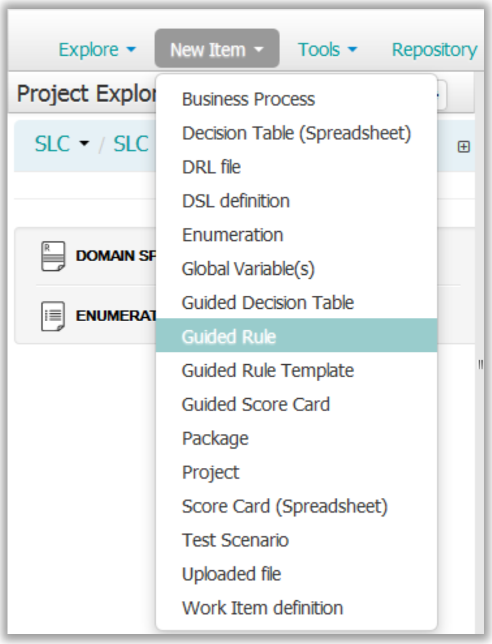
a. Define the Headhunters Blacklist SEP Rule

To define this Rule

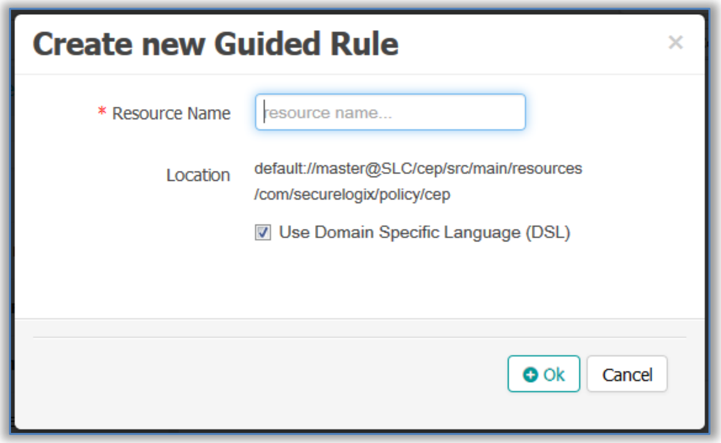
1. In the **Project Explorer** pane, click the third down arrow and then click **cep2sep**, if it is not already selected.



2. On the **Project Authoring** menu bar, click **New Item | Guided Rule**.



3. The **Create New Guided Rule** dialog box appears.


Create new Guided Rule

* Resource Name: resource name...

Location: default://master@SLC/cep/src/main/resources
/com/securelogix/policy/cep

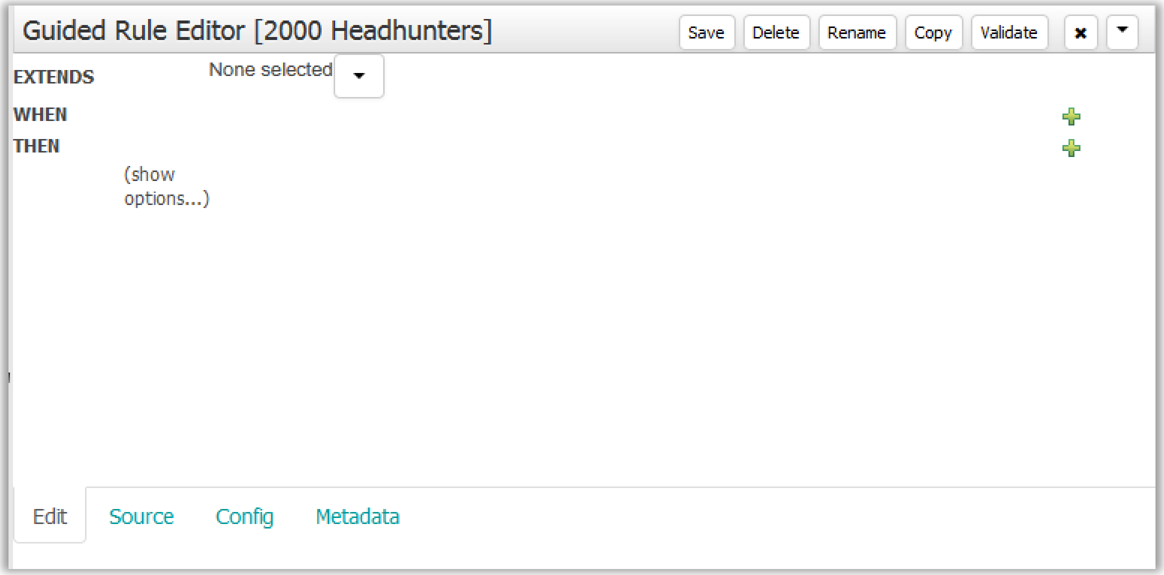
☑ Use Domain Specific Language (DSL)

4. In the **Resource Name** box, type the name for the Rule. For this tutorial, type:

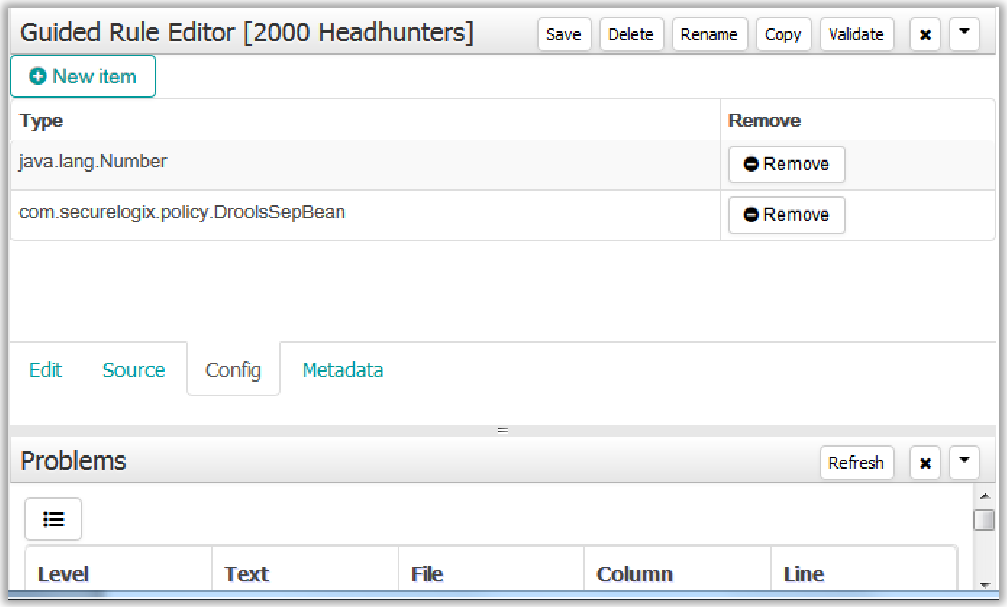
```
2000 Headhunters
```

5. Select **Use Domain Specific language (DSL)**.

6. Click **OK**. The new, blank SEP Rule appears in the **Guided Rule Editor**.



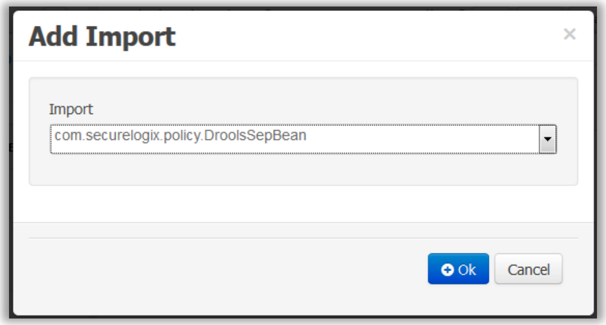
7. Click the **Config** tab at the bottom of the **Guided Rule Editor**. The imports included in the Rule are displayed. By default, **java.lang.Number** is included. As shown in the illustration below, you must add **com.securelogix.policy.DroolsSepBean** to every SEP Rule.



Type	Remove
java.lang.Number	Remove
com.securelogix.policy.DroolsSepBean	Remove

Level	Text	File	Column	Line

8. Click **New Item**. The **Add Import** dialog box appears.

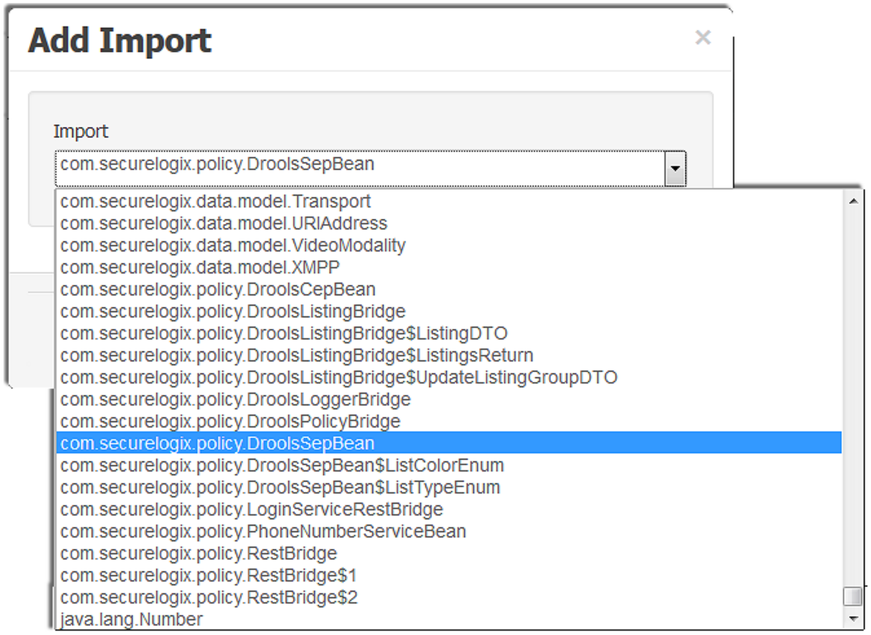


Add Import

Import

com.securelogix.policy.DroolsSepBean

9. In the **Import** box, click the **Down Arrow** and then scroll down and select the applicable import for SEP Rules: **com.securelogix.policy.DroolsSepBean. (**Imports are in alphabetical order.) You must always select this, and only this, additional import for SEP Rules.



Add Import

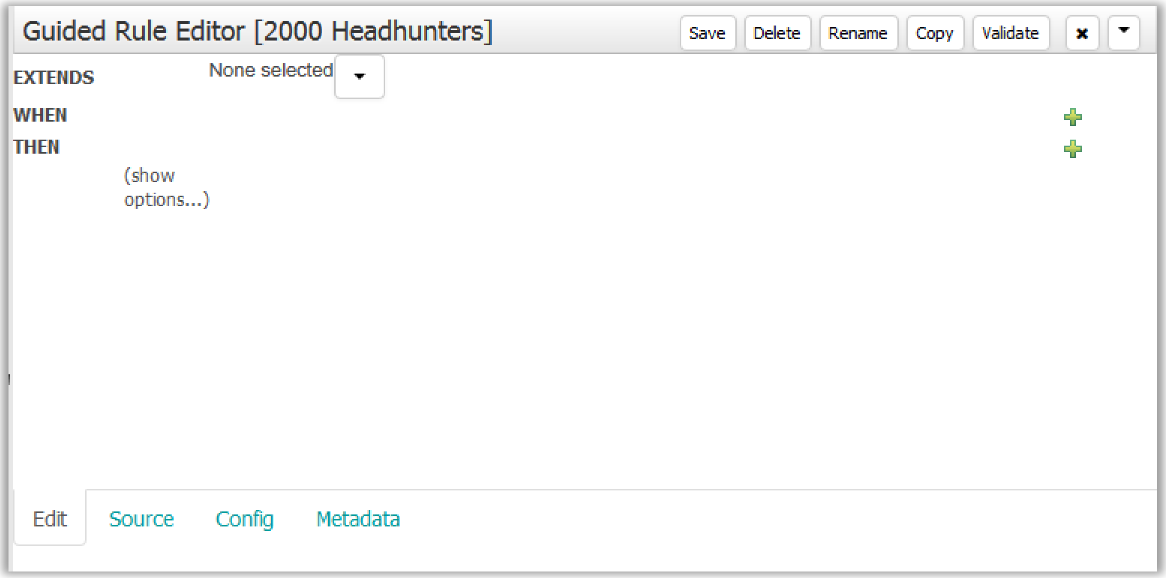
Import

com.securelogix.policy.DroolsSepBean

com.securelogix.data.model.Transport
com.securelogix.data.model.URIAddress
com.securelogix.data.model.VideoModality
com.securelogix.data.model.XMPP
com.securelogix.policy.DroolsCepBean
com.securelogix.policy.DroolsListingBridge
com.securelogix.policy.DroolsListingBridge$ListingDTO
com.securelogix.policy.DroolsListingBridge$ListingsReturn
com.securelogix.policy.DroolsListingBridge$UpdateListingGroupDTO
com.securelogix.policy.DroolsLoggerBridge
com.securelogix.policy.DroolsPolicyBridge
com.securelogix.policy.DroolsSepBean
com.securelogix.policy.DroolsSepBean$ListColorEnum
com.securelogix.policy.DroolsSepBean$ListTypeEnum
com.securelogix.policy.LoginServiceRestBridge
com.securelogix.policy.PhoneNumberServiceBean
com.securelogix.policy.RestBridge
com.securelogix.policy.RestBridge$1
com.securelogix.policy.RestBridge$2
java.lang.Number

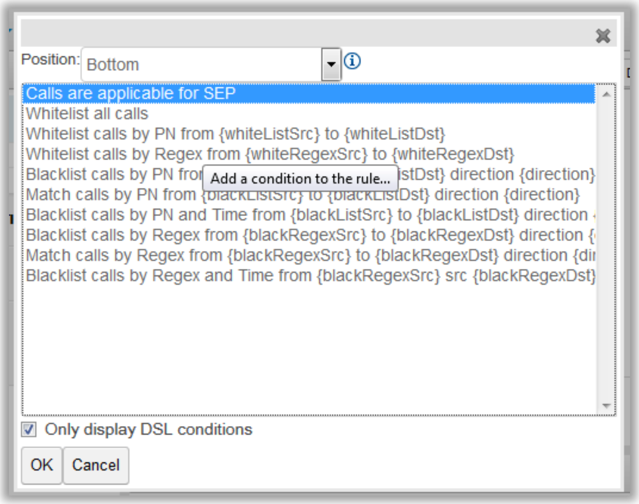
10. Click **OK**. The import is added to the Rule.

11. At the bottom right of the **Guided Rule Editor**, click the **Edit** tab**.**



EXTENDS: None selected

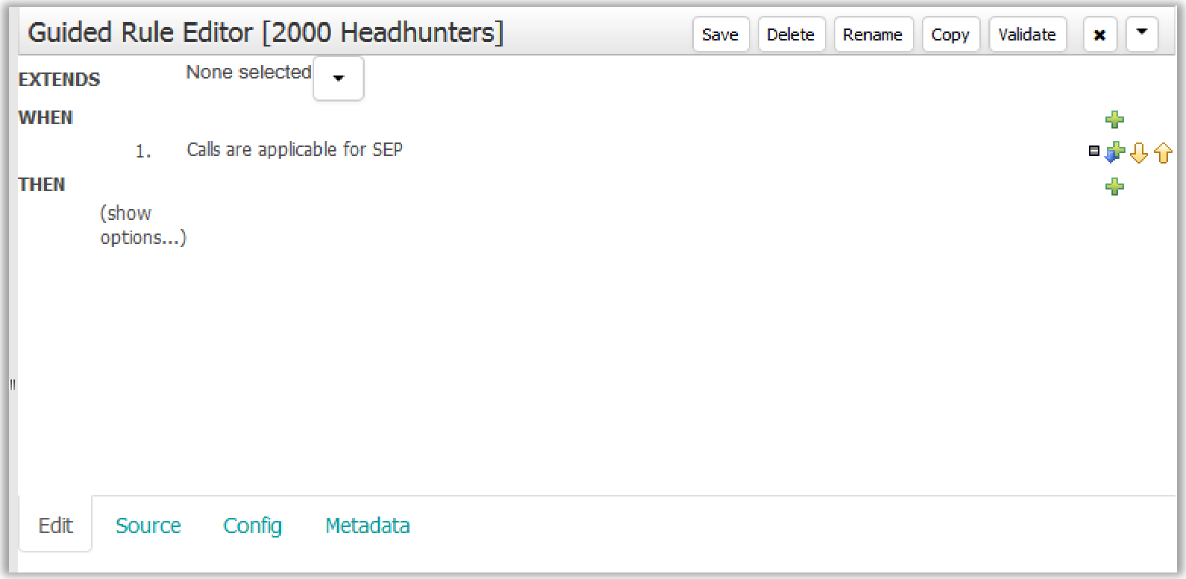
12. Click the green PLUS SIGN (**+**) to the right of **When**, select **Only display DSL conditions**, and then click **Calls are applicable for SEP.** You must always include this option as the first condition for SEP Rules.


Calls are applicable for SEP
Whitelist all calls
Whitelist calls by PN from {whiteListSrc} to {whiteListDst}
Whitelist calls by Regex from {whiteRegexSrc} to {whiteRegexDst}
Blacklist calls by PN fro
Add a condition to the rule...
stDst} direction {direction}
Match calls by PN from {blackListSrc} to {blackListDst} direction {direction}
Blacklist calls by PN and Time from {blackListSrc} to {blackListDst} direction
Blacklist calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {
Match calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {di
Blacklist calls by Regex and Time from {blackRegexSrc} src {blackRegexDst}
OK
Cancel

Position: Bottom

☑ Only display DSL conditions

13. Click **OK**. The condition is added as the first **When** condition.



Guided Rule Editor [2000 Headhunters]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP

THEN

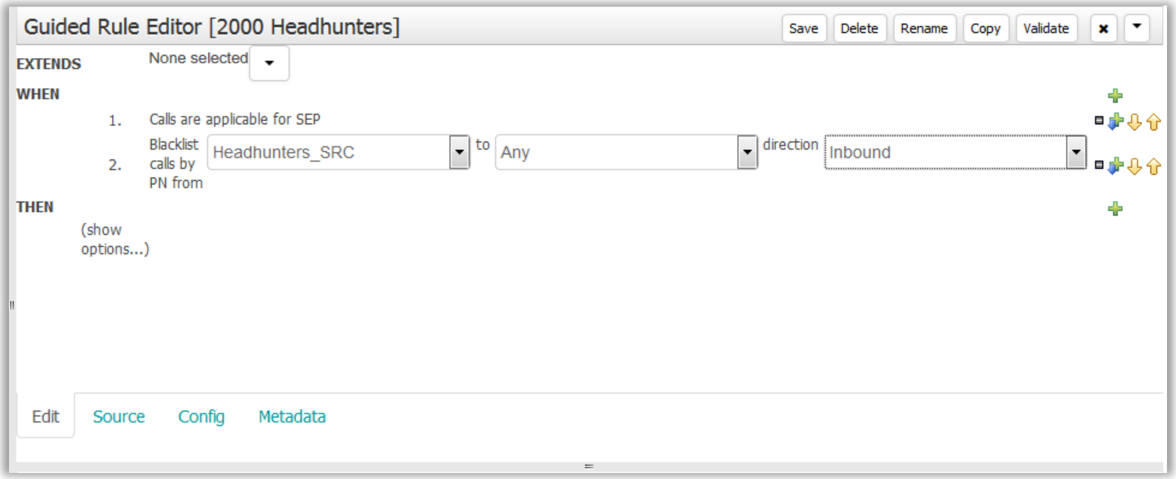
(show options...)

14. Click the green PLUS SIGN (+) to the right of **When** again and click **Blacklist Calls by PN from {BlacklistSrc} to {BlacklistDest} direction {direction}.**

15. Click **OK.**

16. In the **From** field, click the Down Arrow and then click the **Headhunters_SRC** Blacklist, as shown below.

    Notice that only the PN Blacklist is available in this Rule for either Source or Destination. Only the List of the type that matches the **When** statement you selected are available in a Rule.



Guided Rule Editor [2000 Headhunters]

EXTENDS None selected

WHEN

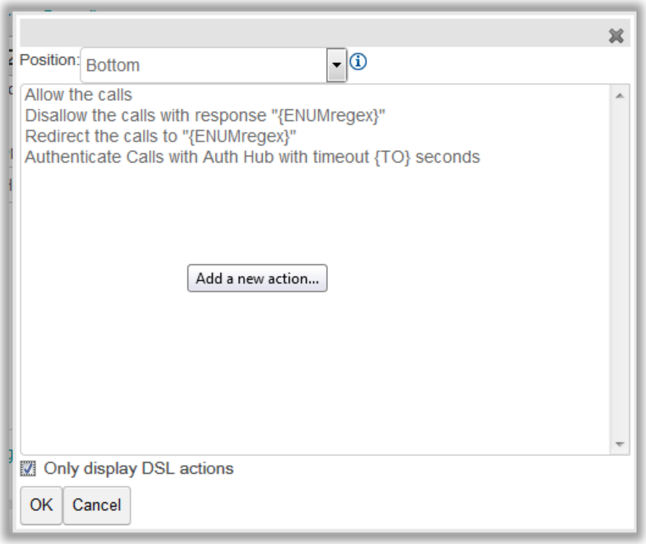
1. Calls are applicable for SEP
2. Blacklist calls by PN from Headhunters_SRC to Any direction Inbound

THEN

(show options...)

17. In the **Direction** field, click the down arrow and click **Inbound**.

18. Click the green PLUS SIGN (+) to the right of **Then** and select **Disallow the calls with response {ENUMRegex}**. This condition is used for Termination Rules, which is what you are defining in this exercise.

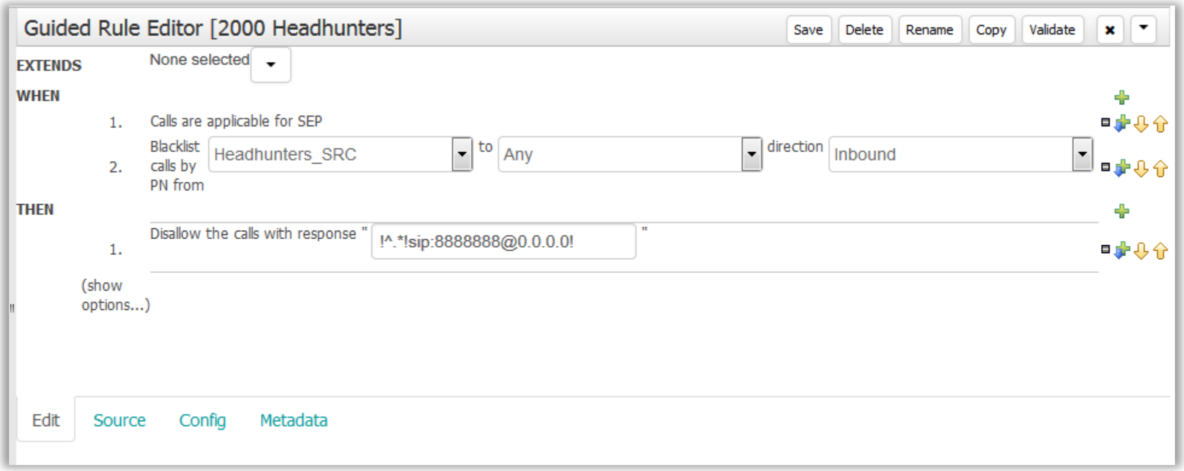


Position: Bottom

Allow the calls
Disallow the calls with response "{ENUMregex}"
Redirect the calls to "{ENUMregex}"
Authenticate Calls with Auth Hub with timeout {TO} seconds

☑ Only display DSL actions

19. Click **OK.**



Guided Rule Editor [2000 Headhunters]

EXTENDS None selected

WHEN
1. Calls are applicable for SEP
2. Blacklist calls by PN from Headhunters_SRC to Any direction Inbound

THEN
1. Disallow the calls with response "!^.*!sip:8888888@0.0.0.0!"

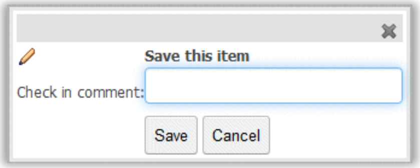
(show options...)

20. Replace **{ENUMRegex}** with the Regular Expression (Regex) denoting the routing response. Since this is a Termination Rule, type: !^.*!sip:8888888@0.0.0.0! as shown in the example below, which terminates the call by sending it to a nonroutable endpoint, resulting in a **404 Not Found**. This is one example of a URI that could be used to terminate a call. Other alternatives could be used that result in a failure response or perhaps send the call to a location that effectively isolates the call. The appropriate reject Regex may vary by carrier, SBC, and/or SBC configuration.

Note: **Validate** checks the entire Policy, not just the Rule you have open.

21. Click **Validate**. The Rule and the entire Policy is checked for missing imports and other errors, such as duplicate Rule names. When complete, a **Validation Successful** message appears. If validation fails, check the **Problems** pane at the bottom of the **Guided Rule Editor**. Correct any errors and then click **Validate** again.

22. Click **Save** at the top right of the editor. The **Save this item** dialog box appears.


Save this item

Check in comment:

23. In the **Check in comment** box, type a comment. Check-in comments are optional, but they appear in the **Metadata** tab of the Rule and can be useful for tracking changes to Rules and the reasons they were made.
24. Click **Save**. The new Rule appears in the **Project Explorer** pane under **Guided Rules with DSL.**

b. *Define the Guatemala Blacklist SEP Rule*

Now that you have experience defining a Rule, define the Guatemala Blacklist Rule to terminate outbound calls to Guatemala as you did above, tailored to this use case as follows:

1. Name the Rule: `2010 Block Outbound Calls to Guatemala.`
2. On the **Config** tab, add the import that applies to all SEP Rules: **com.securelogix.policy.DroolsSepBean**

Note: Notice that only the Regex Blacklist is available in this Rule for either **Source** or **Destination**. Only the type of list that matches the **When** statement you selected are available in a Rule.

3. For the first **When** condition, select the option that applies to all SEP Rules: **Calls are applicable for SEP**
4. For the second **When** condition, select **Blacklist Calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {direction}**.
5. Leave the **From** field set to **Any** and select the **Guatamala_DST** Blacklist in the **To** field.
6. In the **Direction** field, select **Outbound**.
7. Since this is a Termination Rule, for the **Then** condition, as before, select **Disallow the calls with response {ENUMRegex}** and then replace **{ENUMRegex}** with the following Regex: !^.*!sip:8888888@0.0.0.0!
8. Validate and save the Rule.

c. *Define the Executives Whitelist Rule*

Finally, define the Executive Whitelist Rule to always allow calls from your executives without tracking.

1. Name the Rule: `1000 Allow Exec Calls.` Recall that all Whitelist Rules are processed first and then Blacklist Rules are processed in the order they appear in the **Policy Editor** pane. Using this numbering scheme helps organize your Rules and ensure that processing order is clear to you.
2. On the **Config** tab, add the import that applies to all SEP Rules: **com.securelogix.policy.DroolsSepBean**
3. For the first **When** condition, select the option that applies to all SEP Rules: **Calls are applicable for SEP**
4. For the second **When** condition, select **Whitelst Calls by PN from {/WhitelistSrc} to {WhitelistDst}**.

5. Leave the **To** field set to **Any** and select the **Exec_SRC** Whitelist in the **From** field.

   Notice that only the **Exec_SRC** Whitelist is available in this Rule for either **Source** or **Destination**. Only the type of list that matches the **When** statement you selected are available in a Rule.

6. Click the green PLUS SIGN (**+**) to the right of **Then** and select **Allow the Call**. Allow Rules supply the Regex that was defined for Allow Rules during system configuration, by default: `!a^!guaranteed no replacement!`

7. Validate and save the Rule.

TIP: On Whitelist Rules only, adding a call disposition THEN option is optional, because Whitelist Rules are always allowed regardless of the specified THEN action. Adding the **Allow the Call** THEN option to Whitelist Rules simply makes it clear what the Rule does when viewing it.

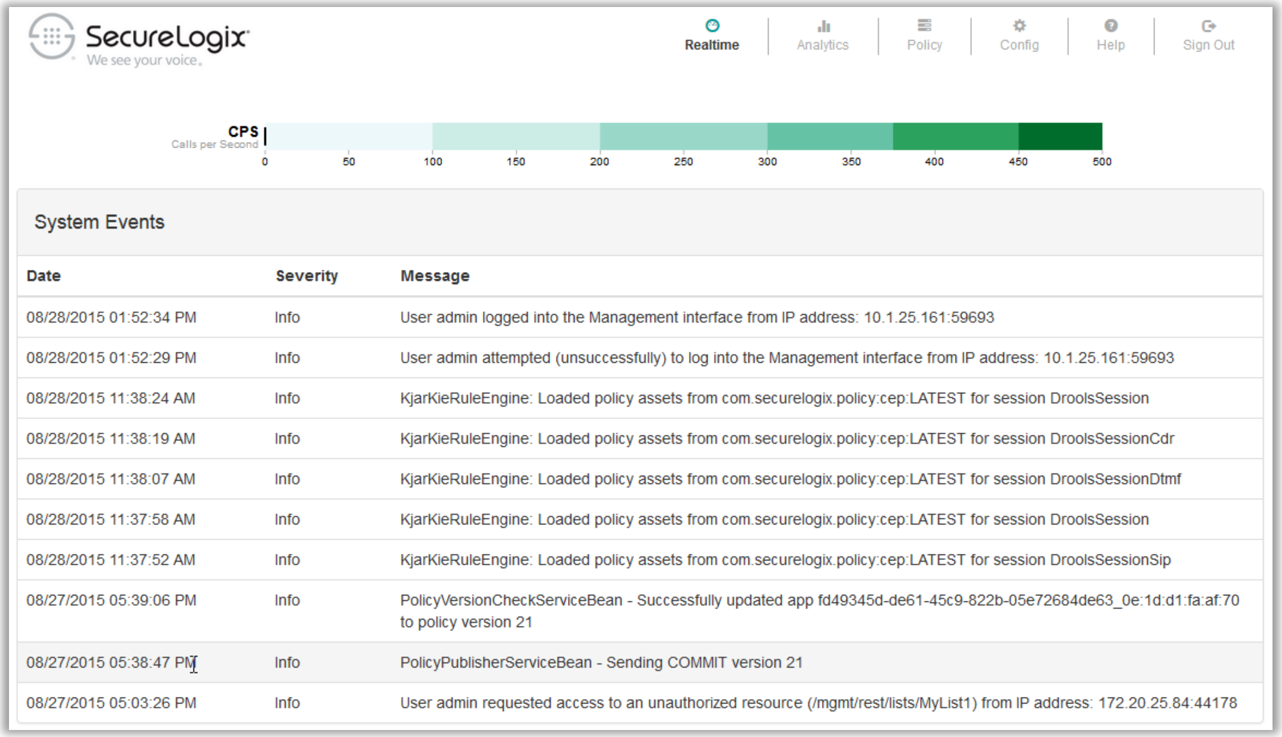
d. Install the SEP Policy

The Rules are saved but must be installed on the ENUM Servers that enforce the SEP Policy before they take effect.

To install the SEP Policy

1. Wait 15 seconds after clicking **Save** on a Rule, and then click the **Commit** icon at the top right above the **Project Authoring** menu bar. When successful, a **Commit Complete** message appears.

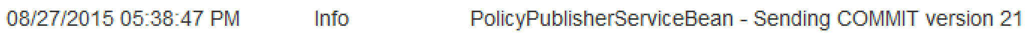
2. On the PolicyGuru main menu, right-click **Realtime** and select **Open link in new tab** to view the progress of the Policy push in the **Realtime** screen. (**Note**: Availability of right-clicking depends on your browser. If not available, simply click **Realtime** on the main menu to navigate to that screen.)



System Events

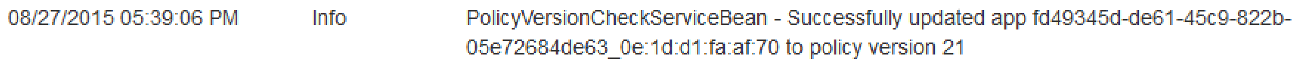
Date	Severity	Message
08/28/2015 01:52:34 PM	Info	User admin logged into the Management interface from IP address: 10.1.25.161:59693
08/28/2015 01:52:29 PM	Info	User admin attempted (unsuccessfully) to log into the Management interface from IP address: 10.1.25.161:59693
08/28/2015 11:38:24 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSession
08/28/2015 11:38:19 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSessionCdr
08/28/2015 11:38:07 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSessionDtmf
08/28/2015 11:37:58 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSession
08/28/2015 11:37:52 AM	Info	KjarKieRuleEngine: Loaded policy assets from com.securelogix.policy:cep:LATEST for session DroolsSessionSip
08/27/2015 05:39:06 PM	Info	PolicyVersionCheckServiceBean - Successfully updated app fd49345d-de61-45c9-822b-05e72684de63_0e:1d:d1:fa:af:70 to policy version 21
08/27/2015 05:38:47 PM	Info	PolicyPublisherServiceBean - Sending COMMIT version 21
08/27/2015 05:03:26 PM	Info	User admin requested access to an unauthorized resource (/mgmt/rest/lists/MyList1) from IP address: 172.20.25.84:44178

3. A message similar to the following appears:



```
08/27/2015 05:38:47 PM      Info      PolicyPublisherServiceBean - Sending COMMIT version 21
```

4. This message is shortly followed by a message similar to the following for *each* ENUM Server belonging to this Mediation Server:



```
08/27/2015 05:39:06 PM      Info      PolicyVersionCheckServiceBean - Successfully updated app fd49345d-de61-45c9-822b-
                                      05e72684de63_0e:1d:d1:fa:af:70 to policy version 21
```

e. Define CEP Alerting Rules for SEP Rule Firings

Suppose you want to be automatically alerted when someone tries to place an outbound call to Guatemala from within your organization.

You've already defined an SEP Rule to prevent such calls, and all call and Policy processing data is stored in the central database for offline reporting and display in the **Analytics** tab. However, if you want to be alerted in real time when the Rule fires, create a CEP Alerting Rule. See "Defining a CEP Alert Rule for an SEP-Rule-Firing" on page 72, using the name of the Rule you created in this exercise as the Rule to fire on.

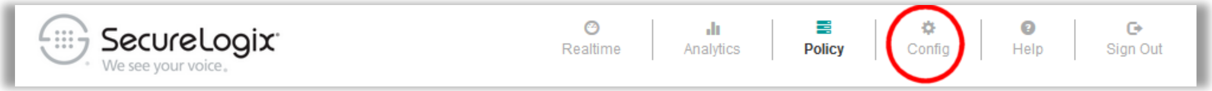
f. Edit a List and Reinstall the SEP Policy

If you make changes to a List used in an installed Rule, you must reinstall the SEP Policy before the change takes effect on the ENUM Servers.

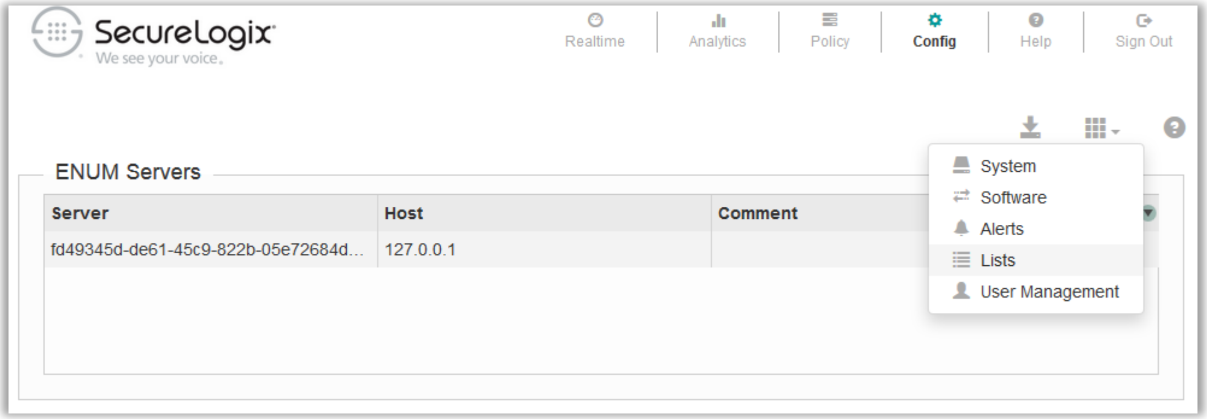
For example, suppose another headhunter becomes a problem, and you want to add that phone number to the Headhunters Blacklist Rule you defined.

To edit a List

1. On the PolicyGuru main menu, click **Config**. The main menu is available from all screens in the GUI.



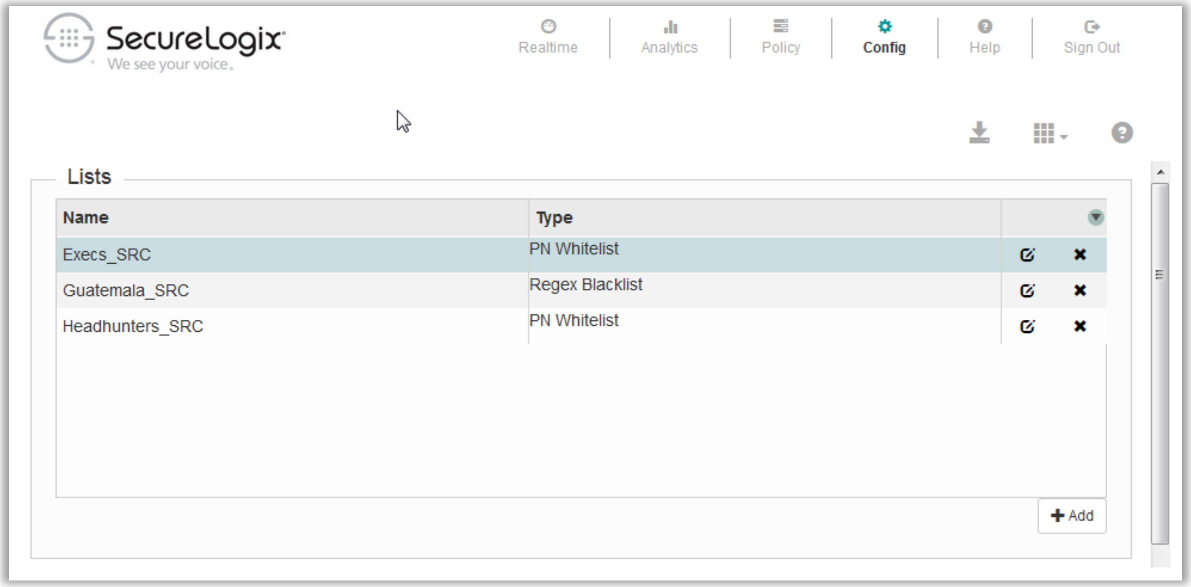
2. Click the **Configuration** drop down menu and then click **Lists**.



ENUM Servers

Server	Host	Comment
fd49345d-de61-45c9-822b-05e72684d...	127.0.0.1	

3. The **Lists** screen appears with the Lists you defined earlier.



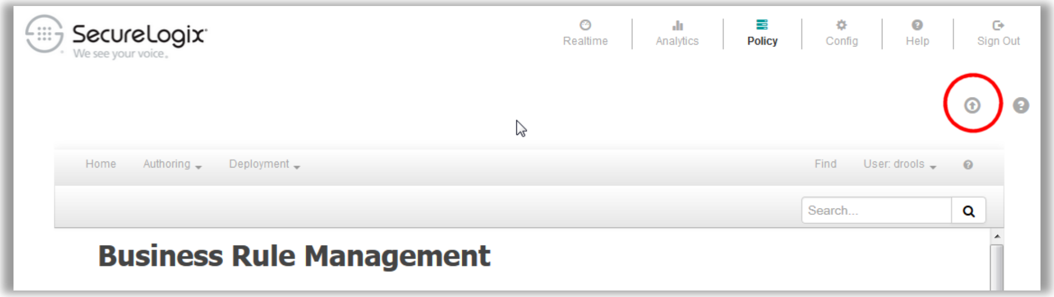
Name	Type
Execs_SRC	PN Whitelist
Guatemala_SRC	Regex Blacklist
Headhunters_SRC	PN Whitelist

4. Click the **Edit** icon to the right of the **Headhunters_SRC** row.

5. Click **Add** and type the new phone number in the correct format as before, and then click **Save**.

   The phone number is now in the List that is the installed policy, but the change is not applied to the application devices enforcing the policy until you again **Commit** the policy.

6. On the PolicyGuru main menu, click **Policy**.



7. Click **Commit**. You do not have to be viewing the Policy to click **Commit**. When successful, a **Commit Complete** message appears.

8. As before, view the **Realtime** screen to see the status of the Policy push.

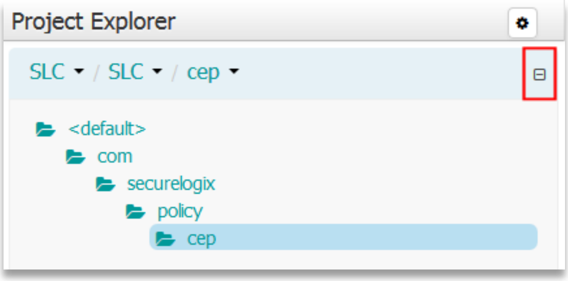
Important Information About First-Time Login via External LDAP

When you log in using the default PolicyGuru user account, you are automatically taken to the PolicyGuru projects in the BRMS. However, the first time you access the BRMS using an external LDAP user account, you must navigate to the PolicyGuru project(s) you want to access. These locations are then saved for your future logins.

To navigate to the PolicyGuru® projects

1. In the BRMS, click **Project Authoring**.

2. In the **Project Explorer** pane, click the PLUS SIGN icon. It changes to a MINUS SIGN.



3. Click each of the folders in the tree to navigate down to the project. The illustration above shows the **CEP** tree.
4. Click the down arrow and select **sep2cep** and repeat the above procedure. Repeat for **IPS** and if used, **orchestration**.

Signing out of the Application

To sign out of the PolicyGuru® application

- Click **Sign Out** on the PolicyGuru main menu.

Note: By default, application sessions have a token that expires 24 hours from the time you log in, regardless of whether you are actively using the application. Each time you log out and back in, you get a new 24-hour token. Your system administrator can also define a client GUI inactivity timeout, such as 15 minutes.

Simple Event Processing (SEP) Policy Rules and Lists

Defining SEP Rules and Lists

Phone Numbers and URIs for use in SEP Policy Rules are contained in Lists and are defined through the PolicyGuru Management Interface, not the BRMS Interface. To avoid switching between applications, it is recommended you define the applicable List before creating a new Rule.

Each List can be of the type Whitelist or Blacklist and can contain either phone numbers/URIs or regular expressions (Regex), but not both. Regex are used to define ranges and wildcards.

How Lists Are Used In Rules

The **Source** and **Destination** field of a Rule can each include only one List.

When you use Lists in a Rule, they must be of the same type as the Rule. If you specify both **Source** and **Destination**, both Lists must also be of the same type. That is:

- A given Blacklist Rule can contain one of the following means to specify the source(s) and destination(s) to which it applies:
  - PN Blacklist to PN Blacklist, or to **Any**
  - Regex Blacklist to Regex Blacklist, or to **Any**
  - **Any** to PN Blacklist or Regex Blacklist.
  - **Any** to **Any**. This could be used as a Catchall Rule at the end of the Rule list.
- A given Whitelist Rule can contain one of the following means to specify the source(s) and destination(s) to which it applies:
  - PN Whitelist to PN Whitelist, or to **Any**
  - Regex Whitelist to Regex Whitelist, or to **Any**
  - **Any** to PN Whitelist or Regex Whitelist
  - **Any** to **Any**. Such a Rule causes every call to be whitelisted. It could be used as means of “turning off” or “avoiding” all Blacklist Rules. It can be thought of (and used) as a way of disabling Policy processing without actually removing or manually disabling all of the Blacklist Rules.

Managing Lists

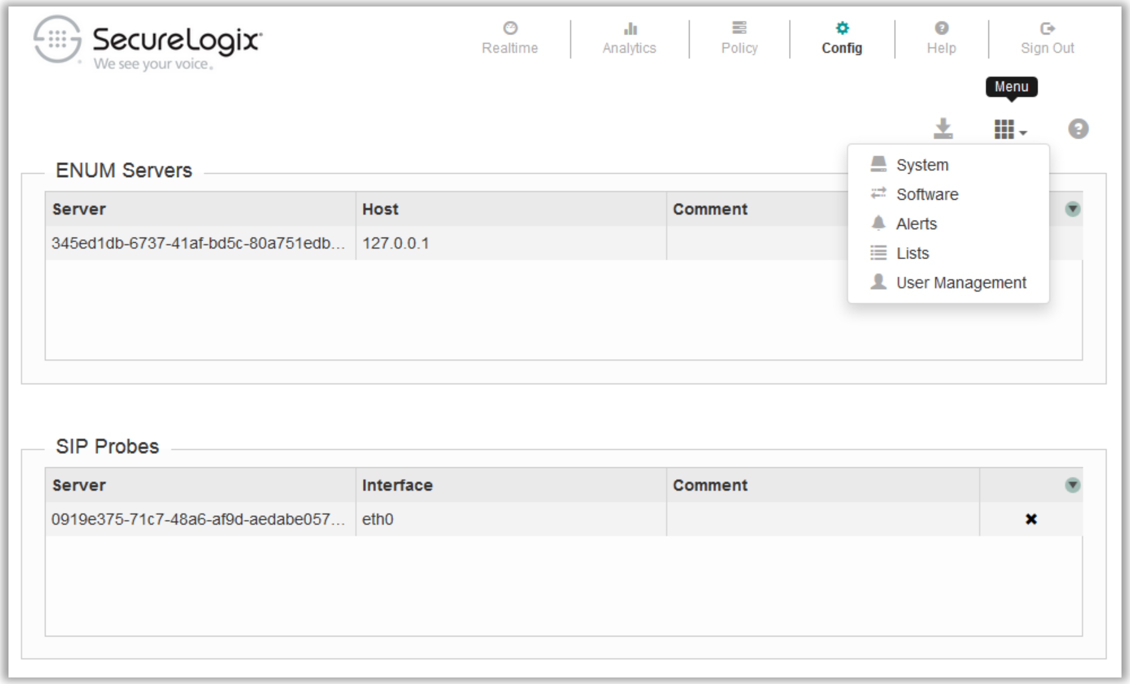
As mentioned earlier, two types of Lists are available:

- **PN Lists**—The values in PN Lists are evaluated via full string matching. PN Lists can contain individual phone numbers/URIs and/or “flag’ strings. Flag strings are character strings that match flags the Phone Number Normalizer has been configured to append or prepend to specified phone numbers received in ENUM Queries. Phone numbers are normalized based on the configuration in the Phone Number Normalizer, prior to Policy processing. This means, for example, that numbers that fail a certain function based on a **libphonenumber** library look up could have a string such as **-INVALID** appended during normalization. You can then create a listing containing the value **INVALID**. When a flagged phone number containing **INVALAD** is compared to a Rule containing this List, the Rule will fire.
- **Regex Lists**—Each listing in a Regex List is specified as a Regex Values in Regex Lists are processed as Regex, by determining if any part of the normalized phone number string matches the regular expression as specified in the listing. In addition to using Regex to define specific number patterns or ranges, you can also use Regex to match on the flagging capability of the Phone Number Normalizer, as described in the bullet above. For example, a Regex value of **badnumber** would match a flag of **this_is_a_badnumber!** appended to a normalized number.

Manually Defining a List

To define a List

1. On the PolicyGuru main menu, click **Config**. The **Config** screen appears.
2. Click the **Configuration Menu** icon and then click **Lists**.



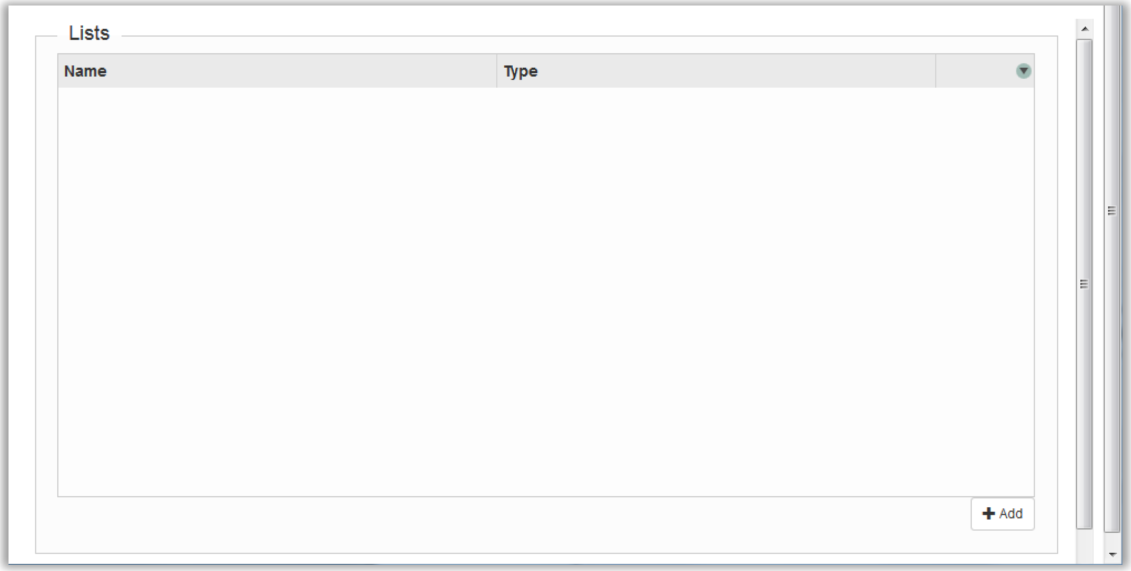
ENUM Servers

Server	Host	Comment
345ed1db-6737-41af-bd5c-80a751edb...	127.0.0.1	

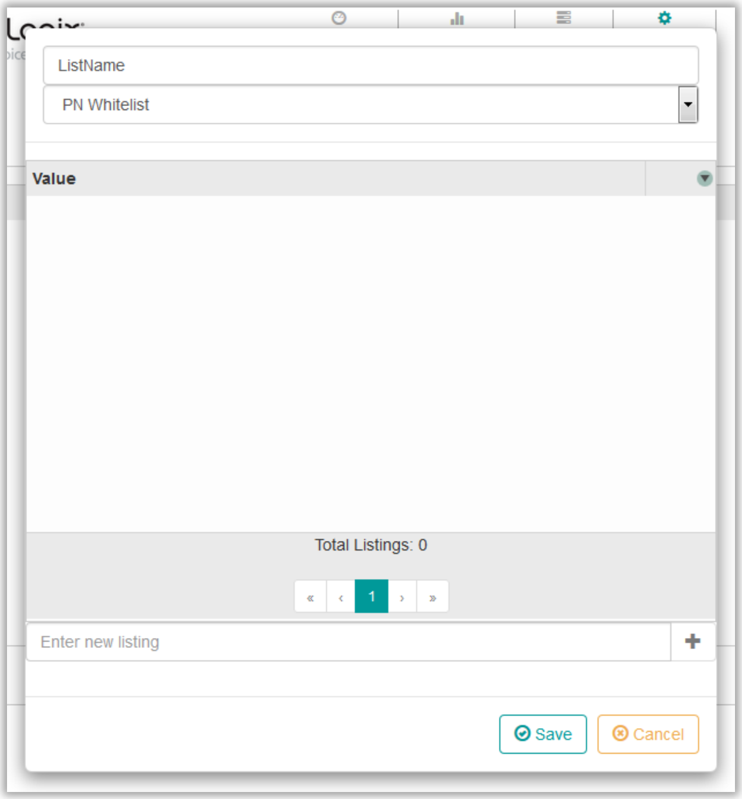
SIP Probes

Server	Interface	Comment	
0919e375-71c7-48a6-af9d-aedabe057...	eth0		✖

3. The **Lists** screen appears. Click **Add** at the bottom right.



4. The **List** dialog box appears.



Tip: You may want to append _SRC to the name of Lists intended for the **Source** field and _DST to those intended for the **Destination** field of Rules.

5. In the **ListName** field, type a unique name to identify this list. This is the name by which the list is identified in Rules. The List name can contain any alphanumeric and special characters EXCEPT spaces, double quotes, parenthesis, periods, forward slash, back slash, pound sign, question mark, comma, or percent sign and can be up to 255 characters in length.

For example, type: `Headhunters`.

6. Click the down arrow in the field below the **ListName** field and select the type of List you are defining:

   - **PN Whitelist**—Contains single or multiple phone numbers/URIs. They are only available for use in Whitelist Rules.
   - **PN Blacklist**—Contains single or multiple phone numbers/URIs. They are only available for use in Blacklist Rules.
   - **Regex Whitelist**—Contains regular expressions representing Ranges or Wildcards. They are only available for use in Whitelist Rules.
   - **Regex Blacklist**—Contains regular expressions representing Ranges or Wildcards. They are only available for Blacklist Rules.

   Note: See also "How Lists are Matched in Policy Processing" on page 11 for important details on what Lists can contain and how they are processed.

   IMPORTANT: You cannot mix Regex and phone numbers in the same List. PN Lists can include only phone numbers/URIs(and strings that are processed like phone numbers via full string matching), not regular expressions. Regex Lists can include only regular expressions, not phone numbers/URIs.

   IMPORTANT: You cannot change the List type after you save the List. Ensure that you have the correct type selected before you save the List.

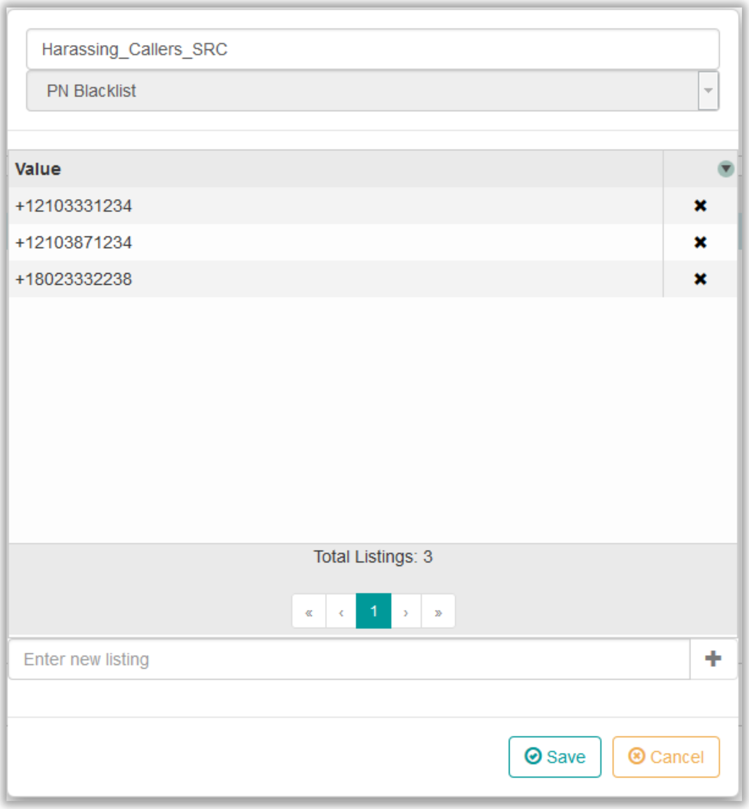
7. In the **Enter new listing** field, type the phone number/URI or regular expression.

   Note: You cannot edit an entry once is has been added. If it contains an error, retype it as a new entry and then delete the mistaken one.

   - Phone numbers are typically fully qualified, of the form **`+cclocalnumber`** (i.e.,+12104029669) without spaces or punctuation. The normalized numbers seen by the ENUM Server must match the List entries for a Rule to fire on that number. This means they must match the normalized formats defined by your Phone Number Normalizer script.
   - See "List Regex Examples" on page 48.

8. Click the PLUS SIGN (**+**)next to the entry or press ENTER to add it to the List. Repeat for each phone number/URI or regular expression that applies to this List. The entries appear in the **Value** field and are searchable and sortable.

TIP: To search for a Listing, click the green arrow to the right of **Value**; to sort the List, click the gray area of the **Value** heading.



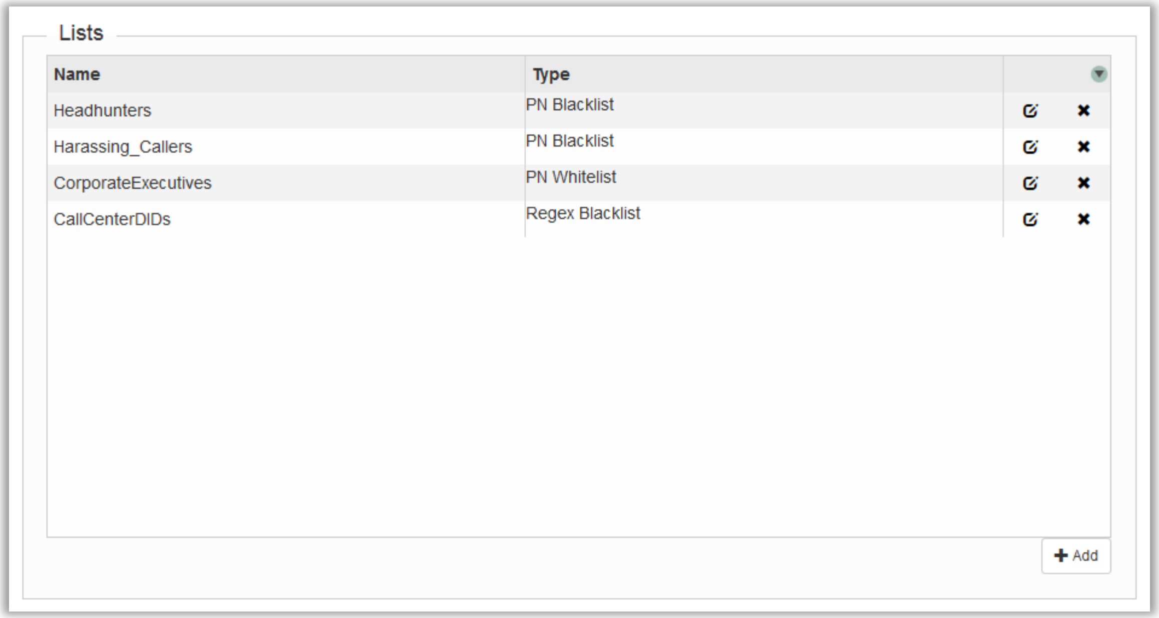
Harassing_Callers_SRC

PN Blacklist

Value
+12103331234
+12103871234
+18023332238

Total Listings: 3

9. When you have added all of the entries, click **Save**. The List appears in the **Lists** dialog box and is available in SEP Policy Rules.



Lists

Name	Type
Headhunters	PN Blacklist
Harassing_Callers	PN Blacklist
CorporateExecutives	PN Whitelist
CallCenterDIDs	Regex Blacklist

Note: While the system appears to allow you to add a duplicate entry to a List, the duplication is resolved when you add it, as evidenced by the count shown. Each entry in a given List is guaranteed unique.

- To search for a List, click the green arrow to the right of the heading row.
- To sort the Lists, by name or type, click in the gray arrow of the applicable heading.
- To edit a List, click the checkmark in its row or double-click the List to open it. **Note**: You can add and remove entries and change the List name, but you cannot edit existing entries or change the List type. To correct an erroneous entry, type the corrected version as a new entry and delete the erroneous one.
- To delete a List, click the **X** in its row. You are prompted to save changes.

List Regex Examples

Below are some example regular expressions for use in Regex Whitelists and Regex Blacklists:

1. Wild Card for Country code 235:

   ```
   ^\+235
   ```

2. Wild Card for NNX 766:

   ```
   ^\+1[0-9]{3}766
   ```

3. Ranges:

   ```
   ^\+1309766[1-9]
   ```
   would match 309 766 1000 to 309 766 9999

Searching for a List

To search for a specific List

1. On the **Lists** screen, click the green arrow **Search** icon to the right of the **Name | Type** header row.
2. In the **Search** field, type any part of the List name.
3. To clear the search, clear the **Search** field.

Sorting the Set of Lists

The set of Lists on the **Lists** screen can be sorted by name or by type.

To sort the Lists screen

- Click the column heading by which you want to sort: **Name** or **Type**.

Searching for Specific Entries in a List

To search for a specific entry in a List

1. On the **Lists** screen, click the click the **Edit** icon at the right of the row containing the List. The **List** dialog box appears.
2. At the right of the **Value** heading row, click the green arrow **Search** icon.
3. In the **Search** field, type the complete entry for which you want to search and then press ENTER. The view is filtered to show only the matching entry.
4. To clear the search, clear the **Search** field and then press ENTER.

Sorting a List

List entries appear by default in ascending order.

To sort a List in ascending or descending order

- In an open List, click the **Value** heading row. Each click toggles the sort order.

Editing a List

Important: When you update a List that is used in an installed Rule, you must click **Commit** to push the changes to the ENUM Server before the changes take effect in the installed Rule.

Note that you can add and delete entries and change the List name, but you cannot edit existing entries nor change the List type.

To edit a List

1. On the **Lists** screen, click the **Edit** icon ✎ at the right of the row containing the List you want to edit. The **List** dialog box appears containing the entries in the List.
   - ✖ To delete an entry, click the **Delete** icon at the right of the row containing the entry. You are prompted to save changes.
   - + To add an entry, type it in the **Enter new listing** field and then click the PLUS SIGN (**+**) or press ENTER.
   - To rename a List, type the new name. **Note**: After renaming, reselect the List in any Rules where it is used.
   - ▼ To search for listings, click the down arrow at the right of the **Value** heading row.
   - To sort the Listings, click in the gray area of the **Value** heading. Each click toggles the sort order.
2. After making all of your changes, click **Save**.
3. If you are making changes to one or more Lists used in Policy, you must reinstall the Policy before the changes take effect on the ENUM Servers enforcing the policy. Wait 15 to 30 seconds after clicking **Save**, click the **Policy** tab, and then click the **Commit** ⬆ icon to push the changes to the ENUM Servers.

   View the **Realtime** tab to view the progress of the Policy push. You should see two messages appear.

   First, you will see a message similar to the following:

```
08/19/2015 05:40:37 PM   Info    PolicyPublisherServiceBean - Sending COMMIT version 35
```

This message is shortly followed by a message similar to the following for *each* ENUM Server belonging to this Mediation Server:

```
                                 PolicyVersionCheckServiceBean - Successfully updated app 31695fbf-4b7e-
08/19/2015 05:40:37 PM   Info    449e-aa0c-59969f26d3ab_02:3a:52:3f:61:a7 to policy version 35
```

Deleting a List

To delete a List

1. In the **Lists** screen, click the **X** to the right of the row containing the **List** you want to delete.

2. At the upper right, click the **Save** icon. The List is not deleted from the database until you click **Save**.

4. **IMPORTANT** If you delete a List used in SEP Policy, reinstall the SEP Policy for the change to take effect on the ENUM Servers. Wait 15 to 30 seconds after clicking **Save**, click the **Policy** tab, and then click the **Commit** icon to push the changes to the ENUM Servers.

Importing a List

For large Lists, SecureLogix provides utility scripts for importing a new List, adding entries to an existing List, and deleting Lists. You can initially populate Lists by running a script to import entries from a flat file into the database. You can then maintain the List through the GUI. You can also import additional Listings into an existing List. You can import either individual, static Listings or ranges. Range import results in one individual Listing for every number included in the specified range.

Run these scripts on the Mediation Server.

Note: These import scripts are not included in the default installation. Contact SecureLogix Technical Support to obtain a copy of the scripts.

Static List Import

A static import list consists of a text file with one normalized phone number/URI or Regex entry per line.

Defining a Static Import File

A static import List consists of a text file with one normalized phone number/URI or Regex entry per line. These must be in exactly the form you want them to appear in the List, in the same way as with manual entry as described above.

Do not leave any blank lines, add comments, or use tabs in the file. Blank lines and comments are imported as Listings. Ensure that each number appears only once in the List; duplicates cause the script to error out.

Recall that a given List can contain either phone numbers/URIs OR Regex entries, but not both.

You specify the filename of the import file when you run the import script. See “Importing a New Static List” below for instructions.

Importing a New Static List

Static List import imports a set of individual, fully qualified phone numbers or a set of Regex from a text file to create a new List of the applicable type. Run this scripts on the Mediation Server.. See “Defining a Static Import File” above for instructions for creating the file.

To import a static List from a text file

1. Obtain a copy of **createlist_file_2.1.sh**. This script is not included in the default installation. Contact SecureLogix Technical Support to

obtain a copy. A sample appears in “Appendix A: List Import Scripts” on page 100.

2. SSH to the Mediation Server and place the script there.
3. Define a text file containing the phone numbers/URIs or Regex you want included in the List. See “Defining a Static Import File” above.
4. SSH to the Mediation Server and place the text file in the directory where you placed the script.
5. Execute the script from a command line. Usage (typed on one line) is:

```
./createlist_file_2.1.sh <server> <list name> <list type> <list file> [batch size]
[username] [password]
```

Where:

server—Mediation Server IP Address.

listname—The name to give the List in the GUI.

- **IMPORTANT**: **listname** can contain any alphanumeric and special characters EXCEPT spaces, double quotes, parenthesis, periods, forward slash, back slash, pound sign, question mark, comma, or percent sign and can be up to 255 characters in length.

listtype—A digit denoting the type of List to create:

0 – PN Whitelist

1 – PN Blacklist

2 – Regex Whitelist

3 – Regex Blacklist

listfile—The filename name of import file.

batch size—(*optional*) the number of listings to submit at a time. If omitted, the batch size defaults to 100.

username—(*optional*) The username for PolicyGuru application login. If omitted from the command line, you will be prompted for the username during script execution.

password—(*optional*) The password for the PolicyGuru application username you supply. If omitted from the command line, you will be prompted for the password during script execution.

6. When script execution completes, the new List appears in the **Lists** screen in the Management GUI.

Range List Import

Range imports to a List are useful if you have one or more large, contiguous ranges of phone numbers to import. Range import results in one individual Listing for every number included in the specified range. Note that with this script, the Listing created as the beginning of the range will end with some number of zeros and the Listings will increment from there based on your supplied values. Examples are provided below. Run this script on the Mediation Server.

Importing a New List from a Range

To import a Range to a List

1. Obtain a copy of the **createlist_range_2.1.sh** file. This script is not included in the default installation. Contact SecureLogix Technical Support to obtain a copy. A sample appears in “Appendix A: List Import Scripts” on page 100.

2. SSH to the Mediation Server and place the script there.

3. Execute the script from a command line. Usage (typed on one line) is:

```
./createlist_range_2.1.sh <server> <list name> <list type> <prefix> <value length>
<count> [batch size] [username] [password]
```

Where:

server—Mediation Server IP Address..

listname—The name to give the List in the GUI.

- **IMPORTANT**: **listname** can contain any alphanumeric and special characters EXCEPT spaces, double quotes, parenthesis, periods, forward slash, back slash, pound sign, question mark, comma, or percent sign and can be up to 255 characters in length.

listtype—A digit denoting the type of List to create:

0 – PN Whitelist

1 – PN Blacklist

2 – Regex Whitelist

3 – Regex Blacklist

prefix—The starting digits of each range entry (for example, +121055500.)

valuelength—The number of additional characters to be added to the end of the specified prefix, for example, 2. Using the example value above and a count of 100, this would denote adding the digits 00-99 to create a range of 100 listings from +12105550000 to +12105550099.

count—The number of List entries to create (for example, 100).

batch size—(*optional*) the number of listings to submit at a time. If omitted, the batch size defaults to 100.

username—(*optional*) The username for PolicyGuru application login. If omitted from the command line, you will be prompted for the username during script execution.

password—(*optional*) The password for the PolicyGuru application username you supply. If omitted from the command line, you will be prompted for the password during script execution.

4. When script execution completes, the new List appears in the **Lists** screen in the Management GUI.

Importing Listings Into An Existing List

You can import additional Listings from a text file into an existing List. See “Defining a Static Import File” on page 50 for instructions for creating the file. Run this script on the Mediation Server.

To import Listings into an existing List

1. Obtain a copy of the **addtolist_file_2.1.sh** file. This script is not included in the default installation. Contact SecureLogix Technical Support to obtain a copy. A sample appears in “Appendix A: List Import Scripts” on page 100.
2. SSH to the Mediation Server and place the script there.
3. Execute the script from a command line. Usage (typed on one line) is:

```
./addtolist_file_2.1.sh <server> <list name> <list file> [batch size] [username]
[password]
```

Where:

server—Mediation Server IP Address.

listname—The name of the existing List that the Listings will be added to.

listfile—The filename name of import file.

batch size—(*optional*) the number of listings to submit at a time. If omitted, the batch size defaults to 100.

username—(*optional*) The username for PolicyGuru application login. If omitted from the command line, you will be prompted for the username during script execution.

password—(*optional*) The password for the PolicyGuru application username you supply. If omitted from the command line, you will be prompted for the password during script execution.

5. When script execution completes, the Listings in the file have been added to the existing List. .
6. If the List is used in SEP Policy, reinstall the SEP Policy for the change to take effect on the ENUM Servers.

Delete List Script

The Delete List script is a utility to enable you to easily delete a large List you are no longer using. Attempting to delete a very large List using the GUI can time out before the operation succeeds.

To delete a large List

1. Obtain a copy of the **deletelist_2.1.sh** file. This script is not included in the default installation. Contact SecureLogix Technical Support to obtain a copy. A sample appears in “Appendix A: List Import Scripts” on page 100.
2. SSH to the Mediation Server and place the script there.
3. Execute the script from a command line. Usage is:

```
./deletelist_2.1.sh <server> <list name> [batch size] [username] [password]
```

Where:

server—Mediation Server IP Address.

listname—The name of the existing List to be deleted from the system.

batch size—(*optional*) the number of listings to submit at a time. If omitted, the batch size defaults to 100.

username—(*optional*) The username for PolicyGuru application login. If omitted from the command line, you will be prompted for the username during script execution.

password—(*optional*) The password for the PolicyGuru application username you supply. If omitted from the command line, you will be prompted for the password during script execution.

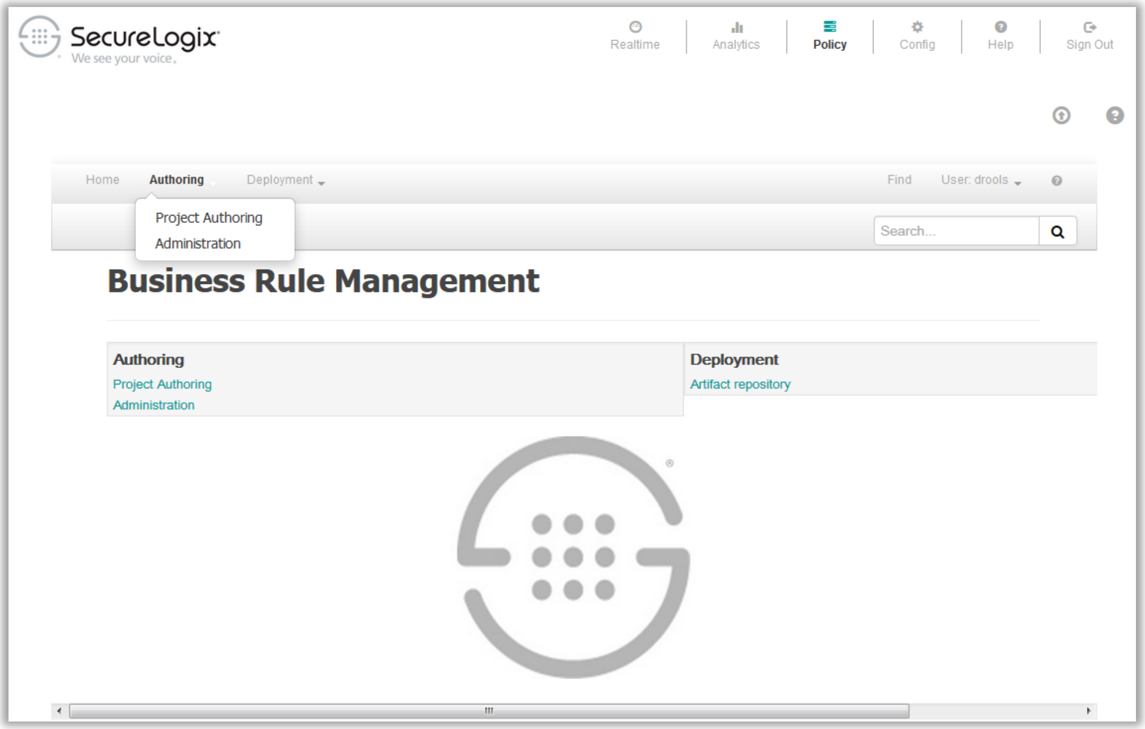
4. If the List you deleted was being used in installed SEP Rules and you are replacing it with a new List, edit any SEP Policy Rules the List you deleted was used in, add the new List to the Rules, and reinstall the Policy.

Defining an SEP Call Control Rule

IMPORTANT: If you are using an external LDAP login for the first time, see “Important Information About First-Time Login via External LDAP” on page 41 and follow those instructions before continuing, if you have not already done so.

To define an SEP Call Control Rule

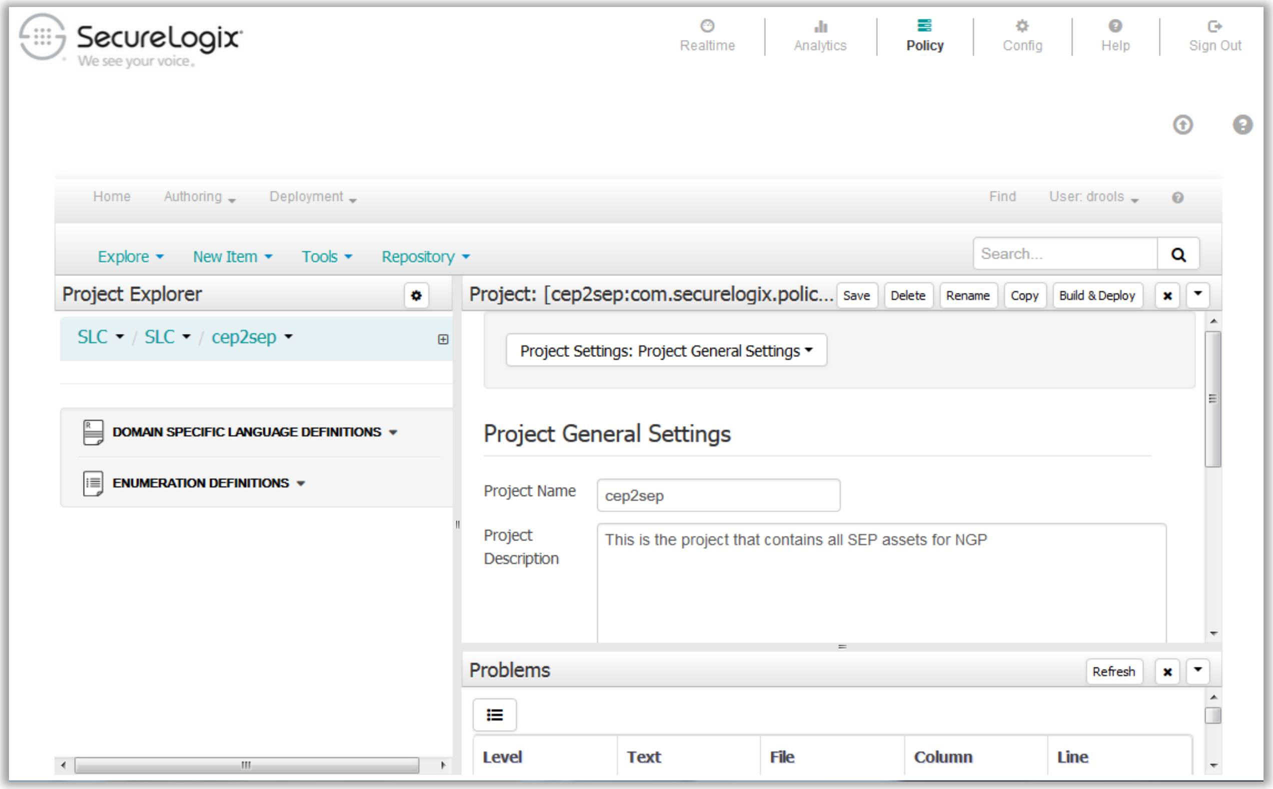
1. On the PolicyGuru main menu, click **Policy**.



2. Click **Authoring | Project Authoring** on the BRMS main menu, or click **Project Authoring** in the middle of the main screen.

   TIP: If the screen is minimized beyond a certain size, the BRMS main menu becomes a menu icon. Click it to access the options.

3. The BRMS **Project Authoring** screen appears.

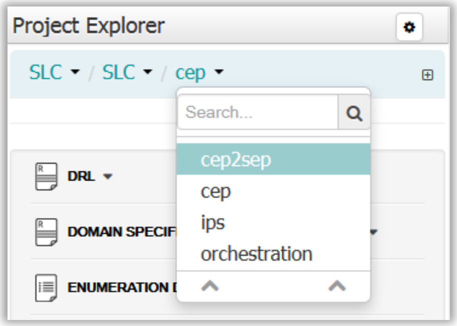


Project General Settings

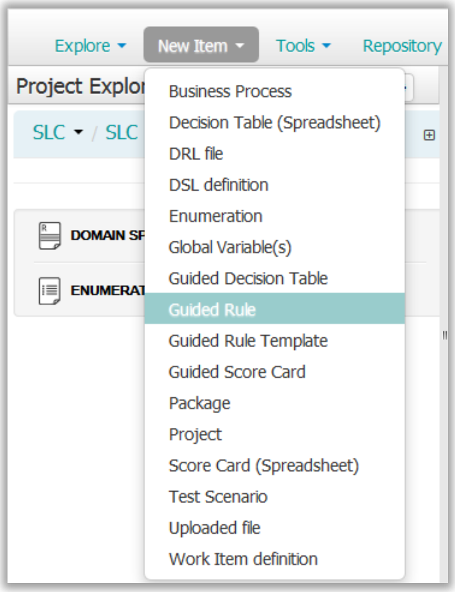
Project Name: cep2sep

Project Description: This is the project that contains all SEP assets for NGP

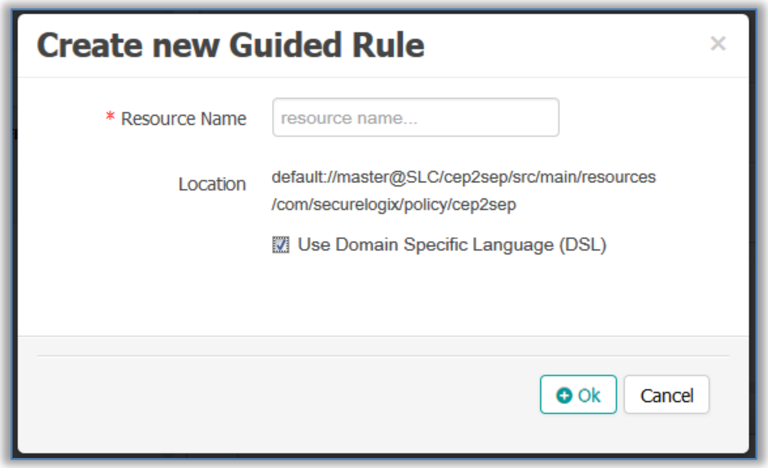
4. In the **Project Explorer** pane, click the third down arrow and then click **cep2sep**, if it is not already selected.



5. On the BRMS main menu, click **New Item | Guided Rule**.



6. The **Create New Guided Rule** dialog box appears.



Create new Guided Rule

* Resource Name: resource name...

Location: default://master@SLC/cep2sep/src/main/resources/com/securelogix/policy/cep2sep

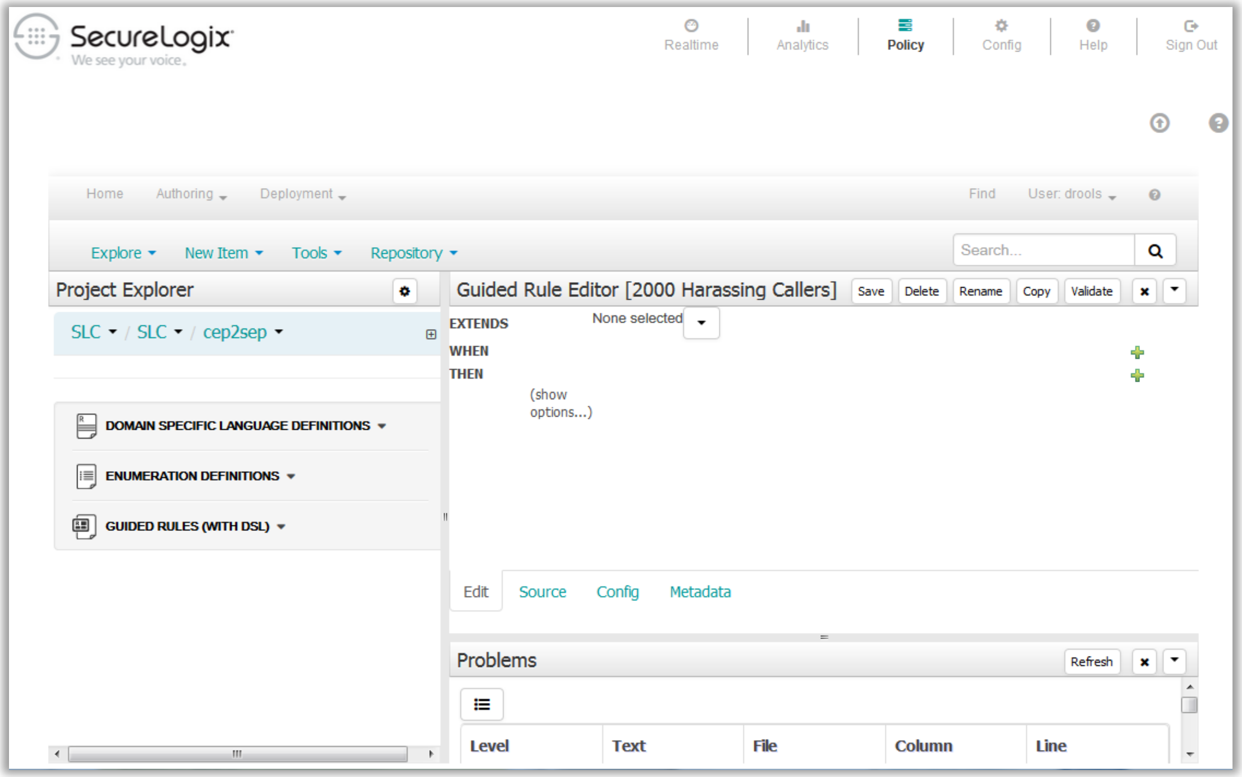
☑ Use Domain Specific Language (DSL)

7. In the **Resource Name** box, type the name for the Rule. For example, type:

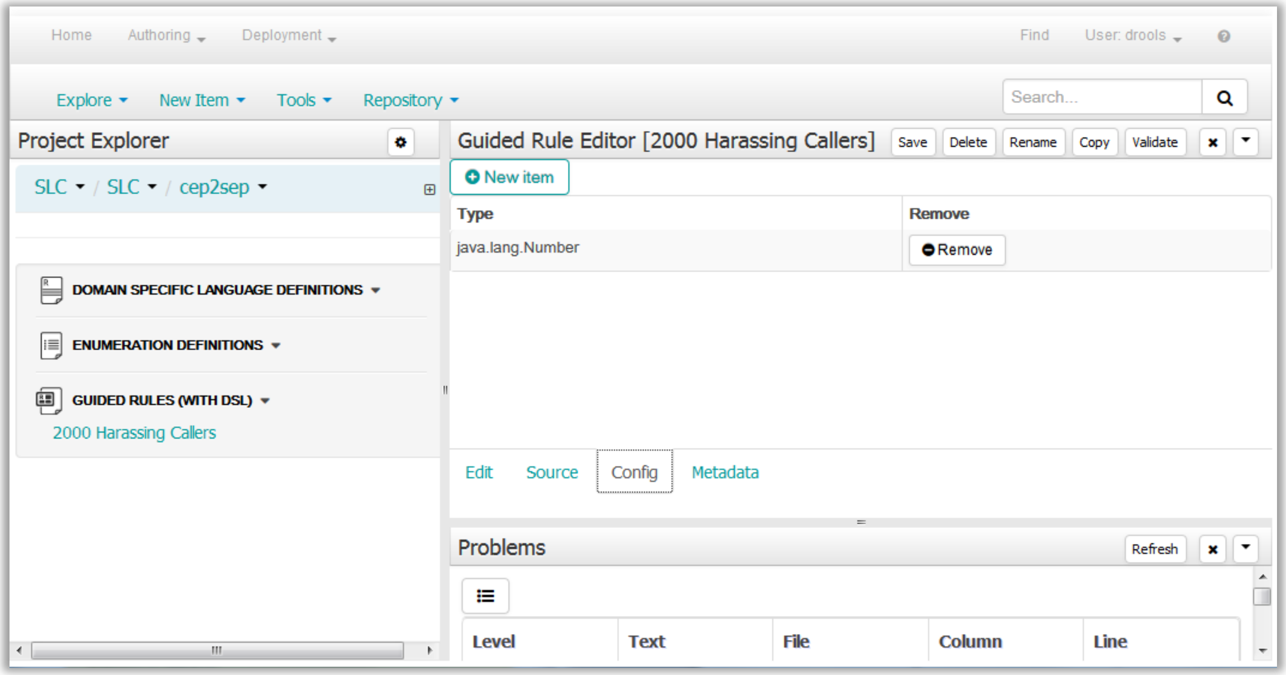
```
2000 Harassing Callers
```

8. Select **Use Domain Specific language (DSL)**.

9. Click **OK**. The **Guided Rule Editor** appears containing a blank SEP Rule.

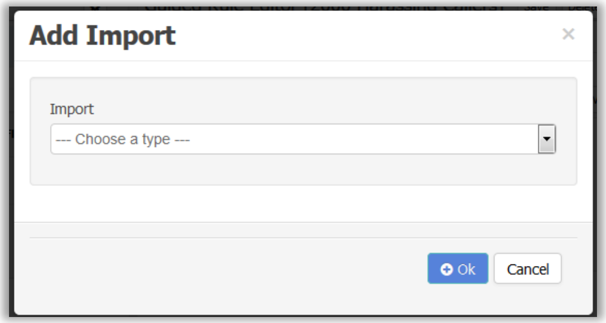


10. At the bottom right of the **Guided Rule Editor**, click **Config**. The imports included in the Rule are displayed. By default, **java.lang.Number** is included. As shown in the illustration below. You must add **com.securelogix.policy.DroolsSepBean** to every SEP Rule.

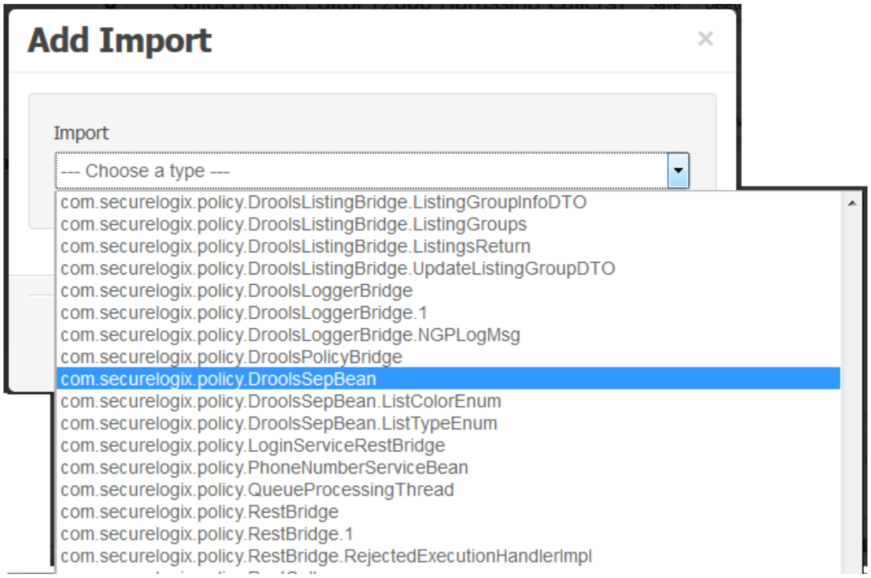


Type	Remove
java.lang.Number	Remove

11. Click **New Item**. The **Add Import** dialog box appears.

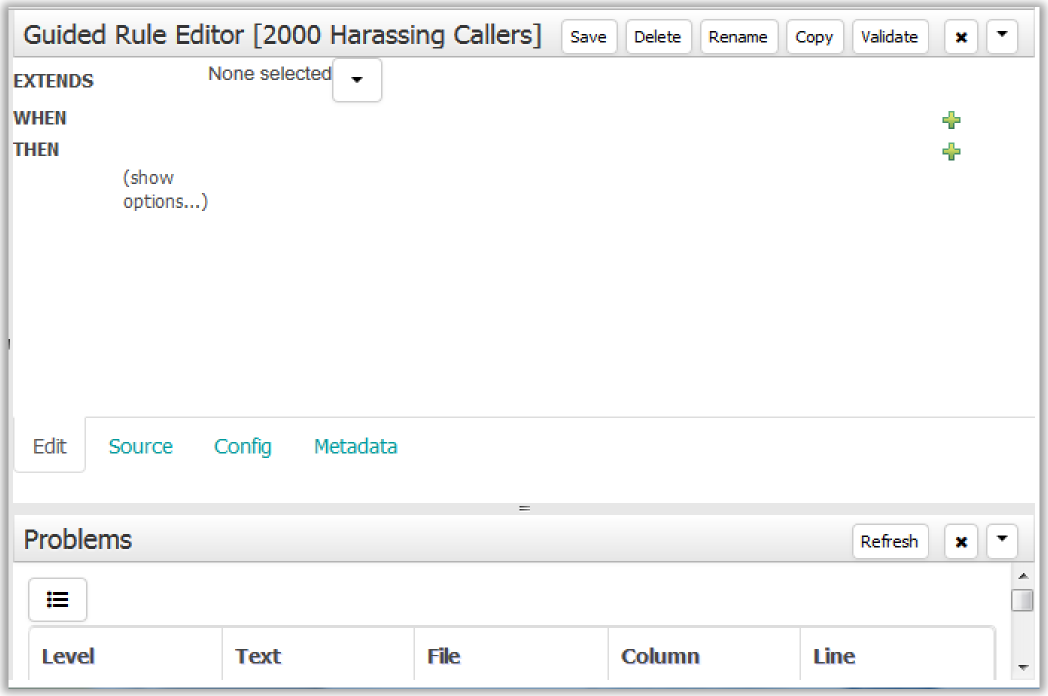


12. In the **Import** box, click the down arrow and then scroll down and select the applicable import for SEP Rules: **com.securelogix.policy.DroolsSepBean** (entries are in alphabetical order). You must always select this, and only this, additional import for SEP Rules.


Add Import
×
Import
--- Choose a type ---
com.securelogix.policy.DroolsListingBridge.ListingGroupInfoDTO
com.securelogix.policy.DroolsListingBridge.ListingGroups
com.securelogix.policy.DroolsListingBridge.ListingsReturn
com.securelogix.policy.DroolsListingBridge.UpdateListingGroupDTO
com.securelogix.policy.DroolsLoggerBridge
com.securelogix.policy.DroolsLoggerBridge.1
com.securelogix.policy.DroolsLoggerBridge.NGPLogMsg
com.securelogix.policy.DroolsPolicyBridge
com.securelogix.policy.DroolsSepBean
com.securelogix.policy.DroolsSepBean.ListColorEnum
com.securelogix.policy.DroolsSepBean.ListTypeEnum
com.securelogix.policy.LoginServiceRestBridge
com.securelogix.policy.PhoneNumberServiceBean
com.securelogix.policy.QueueProcessingThread
com.securelogix.policy.RestBridge
com.securelogix.policy.RestBridge.1
com.securelogix.policy.RestBridge.RejectedExecutionHandlerImpl

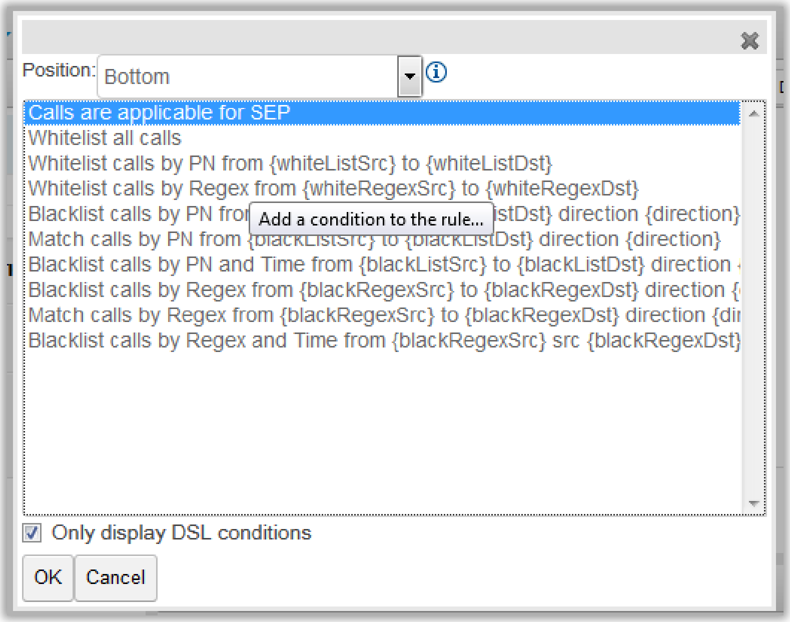
13. Click **OK**. The import is added to the Rule.

14. At the bottom right of the **Guided Rule Editor**, click **Edit.**



15. Click the green PLUS SIGN (+) to the right of **When**. The list of **When** conditions defined for SEP Guided Rules appears.

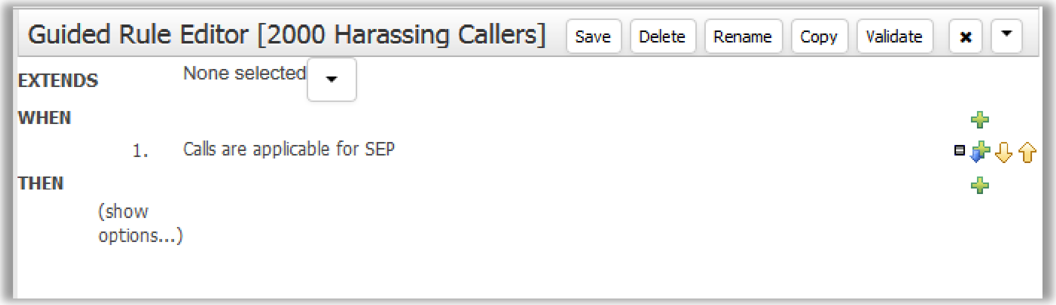
16. Select **Display only DSL conditions**, and then click **Calls are applicable for SEP.** You must always include this option as the first condition for SEP Rules.



Calls are applicable for SEP
Whitelist all calls
Whitelist calls by PN from {whiteListSrc} to {whiteListDst}
Whitelist calls by Regex from {whiteRegexSrc} to {whiteRegexDst}
Blacklist calls by PN fro istDst} direction {direction}
Match calls by PN from {blackListSrc} to {blackListDst} direction {direction}
Blacklist calls by PN and Time from {blackListSrc} to {blackListDst} direction
Blacklist calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {
Match calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {dir
Blacklist calls by Regex and Time from {blackRegexSrc} src {blackRegexDst}

☑ Only display DSL conditions

17. Click **OK**. The condition is added as the first **When** condition.



Guided Rule Editor [2000 Harassing Callers]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP

THEN

(show options...)

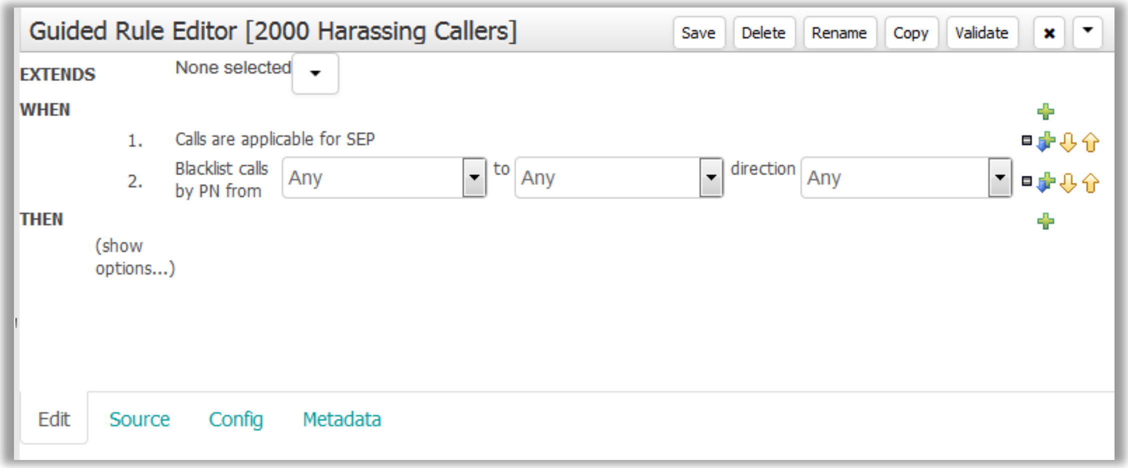
Note: Time of Day in a SEP Rule **When** clause governs when the Rule is active, not the call time.

18. Click the green PLUS SIGN (**+**) to the right of **When** again and add a second **When** condition from the list to define whether this is a Whitelist Rule or a Blacklist Rule and the calls to which the Rule applies.

    For example, to terminate harassing inbound calls from Headhunters, you might click **Blacklist Calls by PN from {BlacklistSrc} to {BlacklistDest} direction {direction}**.

    IMPORTANT: While you can add additional **When** clauses, only the **When** condition immediately following "Calls are applicable for SEP" is used. If you want to add additional **When** clauses as contingency clauses, you can then change the order of the **When** clauses to change the behavior of the Rule and reinstall the Policy. See "SEP Contingency Rules" on page 13 for more information.

19. Click **OK.**



Guided Rule Editor [2000 Harassing Callers]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP

2. Blacklist calls by PN from Any to Any direction Any

THEN

(show options...)

20. Define the **When** fields by clicking the down arrow in the field and selecting the applicable item.

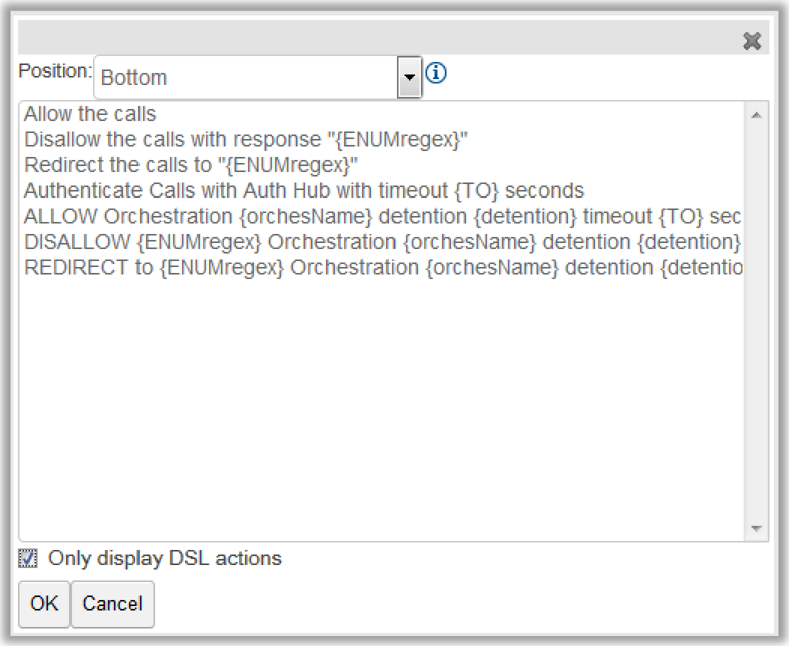
    - **Source** and **Destination**—All defined Lists that are of the same type as the Rule and its **When** clause are displayed. That is, a Blacklist Rule using the **When** clause, "Blacklist calls by PN from…" only offers PN Blacklists in the **Source** and **Destination** fields.
    - **Direction**—**Inbound**, **Outbound**, or **Any**.

Note: You can define a custom DSL option to specify a custom Regex instead of the default for Allow Blacklist Rules. See “Defining a Custom Allow Regex for Blacklist Rules” on page 65.

21. Click the green PLUS SIGN (+) to the right of **Then**, select **Display only DSL actions**, and select the disposition to be applied to calls that trigger this Rule. **Important**: Terminate and Redirect apply only to Blacklist Rules. You can also use Allow with Blacklist Rules. Calls that match a Whitelist Rule are always allowed.

    - To allow matching calls, select **Allow the calls**.
    - To terminate matching calls, select **Disallow the calls with response {ENUMRegex}**.
    - To redirect matching calls, select **Redirect the calls to {ENUMRegex}.**

Note: The dispositions containing **Auth Hub** and **Orchestration** apply only to integrations with certain 3rd party platforms. Contact your SecureLogix Sales representative for more information.

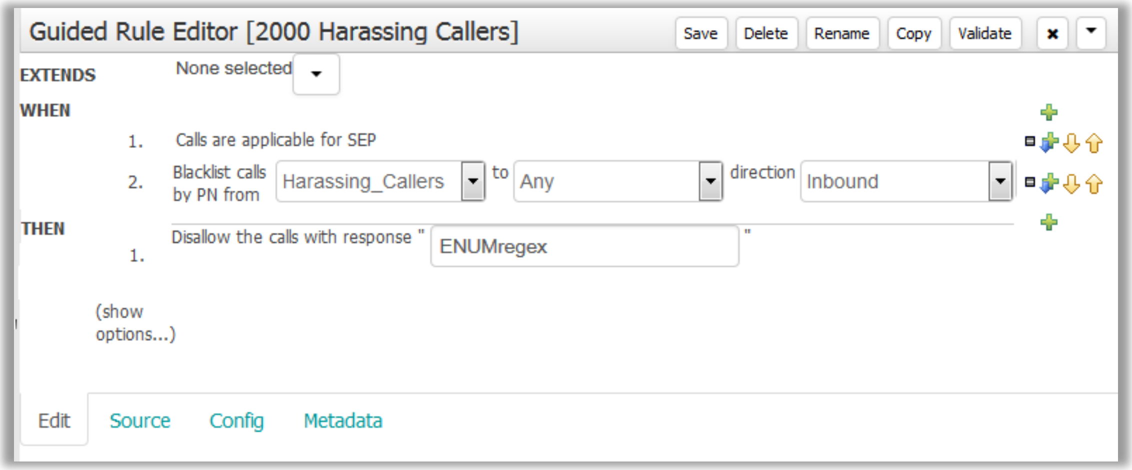


Position: Bottom

Allow the calls
Disallow the calls with response "{ENUMregex}"
Redirect the calls to "{ENUMregex}"
Authenticate Calls with Auth Hub with timeout {TO} seconds
ALLOW Orchestration {orchesName} detention {detention} timeout {TO} sec
DISALLOW {ENUMregex} Orchestration {orchesName} detention {detention}
REDIRECT to {ENUMregex} Orchestration {orchesName} detention {detentio

☑ Only display DSL actions

22. Click **OK.**



Guided Rule Editor [2000 Harassing Callers]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP
2. Blacklist calls by PN from Harassing_Callers to Any direction Inbound

THEN

1. Disallow the calls with response " ENUMregex "

Note: Allow Rules supply the Regex defined for Allow Rules during system configuration, by default: `!a^!guaranteed no replacement!`

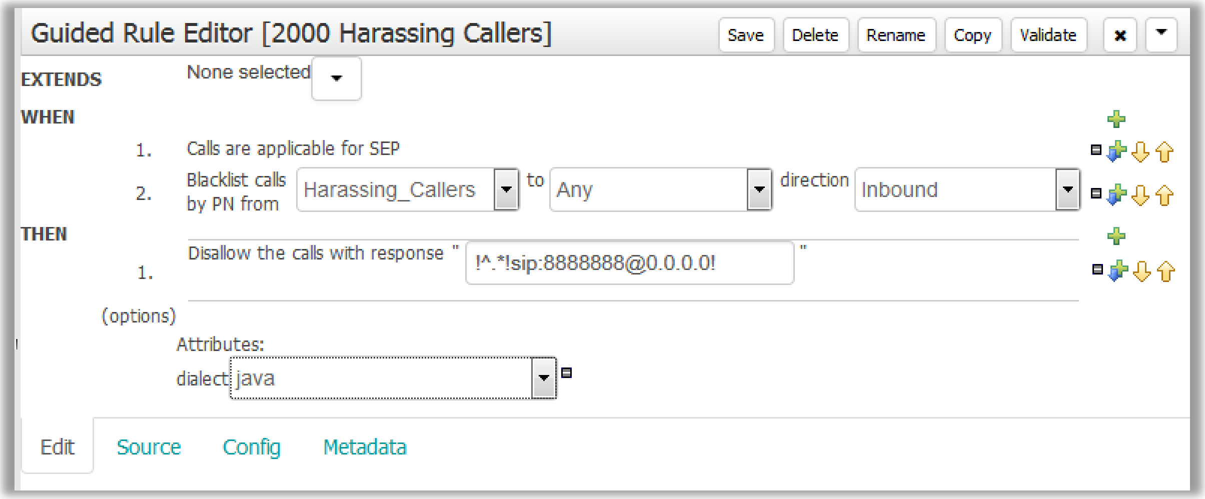
23. If you selected other than the **Allow**… disposition, type the regular expression to be sent. See “Appendix C: Understanding Regular Expressions in Rules” on page 117 for important information about POSIX Regex syntax and “Important Information About Regex in the Guided Rule Editor” on page 63 regarding special character replacement.

    For example, type: !^.*!sip:8888888@0.0.0.0! for a Termination Rule, as shown in the above example, which terminates the call by sending it to a nonroutable endpoint, resulting in a **404 Not Found**. The applicable Regex may vary depending on your carrier and SBC configuration.

    IMPORTANT: While you can add additional **Then** clauses, only the first **Then** clause is used in Rule processing. If you want to add additional **Then** clauses as contingency clauses, you can then change the order of the **Then** clauses to change the behavior of the Rule, and then reinstall the Policy. See “SEP Contingency Rules” on page 13 for more information.

24. Click **show options**, click the down arrow in the **Dialect** box, and select **java**.

    The illustration below shows a Rule that terminates inbound calls from a Blacklist named **Harassing_Callers** to any destination.


Guided Rule Editor [2000 Harassing Callers]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP
2. Blacklist calls by PN from Harassing_Callers to Any direction Inbound

THEN

1. Disallow the calls with response " !^.*!sip:8888888@0.0.0.0! "

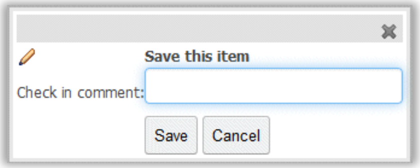
(options)

Attributes:

dialect java

25. Click **Validate**. The Rule and the entire Policy is checked for missing imports and other errors. When complete, either a **Validation Successful** message or an error dialog listing errors that must be corrected appears. If errors exist, correct them and then click **Validate** again. You can also refer to the **Problem** pane at the bottom of the editor for errors.

26. Click **Save** at the top right of the editor. The **Save this item** dialog box appears.


Save this item

Check in comment:

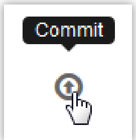
27. In the **Check in comment** box, type a comment. Check in comments are optional, but they appear in the **Metadata** tab of the Rule and can be useful for tracking changes to Rules and the reasons they were made.

28. The Rule is saved but is not currently active on the ENUM Servers. If you are ready to install the Policy with the new Rule, see "Installing or Reinstalling an SEP Policy" below.

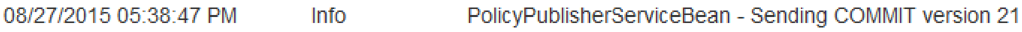
29. Create a corresponding CEP Alerting Rule that defines the logging and alerting you want to occur when this Rule fires (does not apply to Whitelist Rules). See "Defining a CEP Alert Rule for an SEP-Rule-Firing" on page 72 for instructions.

Installing or Reinstalling an SEP Policy

To install or reinstall an SEP Policy

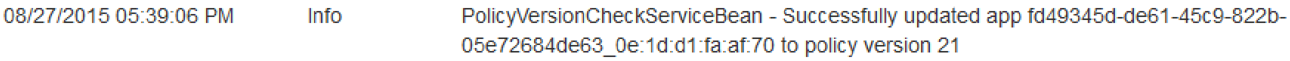


1. Wait 15 seconds after clicking **Save** on any Rule and then click the **Commit** icon at the top right above the BRMS main menu.
2. When successful, a **Commit Complete** message appears.
3. View the **Realtime** tab to view the progress of the policy push. A message similar to the following appears:



```
08/27/2015 05:38:47 PM        Info            PolicyPublisherServiceBean - Sending COMMIT version 21
```

4. This message is shortly followed by a message similar to the following for *each* ENUM Server belonging to this Mediation Server:



```
08/27/2015 05:39:06 PM        Info            PolicyVersionCheckServiceBean - Successfully updated app fd49345d-de61-45c9-822b-
                                              05e72684de63_0e:1d:d1:fa:af:70 to policy version 21
```

5. If you want to be notified when this Rule fires, you must define a CEP Rule to generate the notifications. See "Defining a CEP Alert Rule for an SEP-Rule-Firing" on page 72 for instructions.

Information About How an SEP Policy is Reinstalled

When you change an item in a Rule, such as updating a List or adding a Rule to the Policy, and then reinstall a Policy, it pushes down a delta. On the ENUM Server itself, the entire policy is rebuilt to pull in the change. If an error is encountered while pushing or installing the Policy, the ENUM Server sets its Policy version to -1, which then causes the entire Policy to be pushed down from the Mediation Server again.

Important Information About Regex in the Guided Rule Editor

The **Guided Rule Editor** has limitations in parsing certain characters that are frequently used in regular expressions (Regex). The PolicyGuru Solution provides a set of replacement character strings to use instead of these problematic characters.

IMPORTANT: This limitation applies only to Regex in the **Guided Rule Editor**. Free-form DRL and List entries are not affected.

The table below shows which characters are affected and the replacement character string to use:

Character	Name	Replace with:
(	open parenthesis	&slclb;
)	close parenthesis	&slcrb;

\	back slash	&slcbs;
$	dollar sign	&slcds;

For example:

```
!([0-9]+)\$!sip:\1@10.10.10.10!
```

Must be defined as shown below:

```
!&slclb;[0-9]+&slcrb;&slcbs;&slcds;!sip:&slcbs;1@10.10.10.10!
```

Example Regular Expressions for SEP Rule Responses

IMPORTANT: Rules require POSIX Regex syntax. See "Appendix C: Understanding Regular Expressions in Rules" on page 117 for details.

Below are two sample regular expressions to use in the **Response** field of the **Then** clause in a SEP Redirect or Terminate Rule:

- **Terminate String** —For termination, a host address of 0.0.0.0 results in a **404 Not Found** response .For example:

  ```
  !^.*!sip:8888888@0.0.0.0!
  ```

- **Redirection String**—For redirection, supply the valid host address of the end point that will get the invite. For example:

  ```
  !^.*!sip:2104029669@10.1.1.35!
  ```

  Note: Allow Rules supply the Regex that was defined for Allow Rules during system configuration. By default, the following Regex is used:

  ```
  !a^!guaranteed no replacement!
  ```

See "Defining a Custom Allow Regex for Blacklist Rules" on page 65.

In the above Regex, the clause between the first two exclamation marks is the Regex string that indicates what part of the SIP Request URI is to be matched (^.* means to match everything while a^ means to match nothing). The second clause between the second and third exclamation marks is the replacement string that is used to replace the portion of the SIP Request URI that is matched by the Regex string. In this case, nothing will be matched.

See "Appendix C: Understanding Regular Expressions in Rules" on page 117 for more information about how the ENUM Server uses Regex in Policy enforcement.

Source Tab in Rules

When you define the Rule on the **Edit** tab using DSL assets, he editor then generates the required DRL, which is what the decision engine uses to execute the Rule. This generated DRL can be viewed on the **Source** tab of the **Guided Rule Editor**, but it cannot be edited there, since it is automatically generated based on the inputs in the editor.

Metadata Tab in Rules

The **Metadata** tab of each Rule shows the change history of the Rule since its creation, including who modified it and when. If check-in comments are used, they appear next to each change.

The **Description** field is useful for documenting the purpose and function of the Rule.

A **Discussion** field is also available for comments, such as change requests that have not yet been implemented.

Defining a Custom Allow Regex for Blacklist Rules

By default, PolicyGuru® SEP Blacklist Allow Rules use the following Regex: **!a^!guaranteed no replacement!**. You can define a custom Regex to use in Blacklist Allow Rules instead of the default.

To change the Allow Regex for Blacklist Rules

1. On the **Project Explorer** pane main menu, click the down arrow and click **cep2sep**.
2. Close any open SEP Rules.
3. Click the down arrow next to **Domain Specific Language Definitions** to expand the subtree.
4. Click **SEP Language**. It opens in the **DSL Editor**.
5. Scroll down to the **[then]** entries.
6. Below **[then]Allow the calls=$sep.doRuleAction("ALLOW", "!a^!guaranteed no replacement!")**, add the following line, substituting your preferred Regex for the example Regex shown in red here:

   [then]AllowREGEX=$sep.doRuleAction("ALLOW", "!&slclb;^.*&slcrb;!sip:authorized&slcbs;1@securelogix!");
7. On the **DSL Editor** main menu, click **Save**.
8. On the **DSL Editor** main menu, click the **X** to close the editor.
9. **AllowREGEX** now appears in the list of available **Then** conditions for Blacklist Rules. To define SEP Blacklist Rules using the Regex you specified, select **AllowREGEX** instead of **Allow the calls** as the **Then** statement.

Note: The new **AllowREGEX** option is not available in any Rules that were open when you added it until you close and reopen the Rule.

Opening the Project Explorer Pane if It is Missing

On occasion, the **Project Explorer** pane may be closed when you access the BRMS GUI. If this occurs, use the following procedure to restore it.

To open the Project Explorer pane if it is missing

1. Log out of the GUI.
2. SSH to the Mediation Server.
3. Change directories to **/opt/ngp/bin/.niogit/system.git/refs/heads**
4. Move the given user’s cache file to a new name, using the **rmv** command. For example, for the **admin** user, you would type:

   ```
   rm admin-uf-user backup_admin-uf-user
   ```
5. Log back in to the GUI and verify that the **Project Explorer** pane is shown. If it is, you can delete the backup file you created.

Defining SEP Policy Rules for Orchestra One™ Verification Requests

The PolicyGuru Solution provides an integration that enables the PolicyGuru Mediation Server to send verification requests to the Orchestra One™ Call Verification Service. This feature is called the o1 Agent. Orchestra One™ Call Verification Request Rules specify which calls are to trigger an Orchestra One Request. See the *PolicyGuru® Meta-Policy Controller System Administration Guide* for information on configuring the o1 Agent before using these instructions.

The o1 Agent can be configured to send verification requests for all inbound calls to Orchestra One, or SEP Policy Rules can be defined that specify only certain destination and/or source numbers for which call verification requests are to be sent, such as contact center lines.

Use the procedures below to create and install SEP Rules to trigger selective Orchestra One Requests if your system is configured to use this functionality. See the *PolicyGuru® Meta-Policy Controller System Administration Guide* for more information about the o1 Agent and available configuration modes.

Rule Order Considerations

Recall that SEP Rules are processed as follows: All Whitelist Rules in the order in which they appear and then all Blacklist Rules in the order in which they appear. Also recall that the Rules are listed in the Policy in ASCII alphabetical order. As previously discussed, use a numbering scheme to ensure the Rules are listed in the correct order for processing.

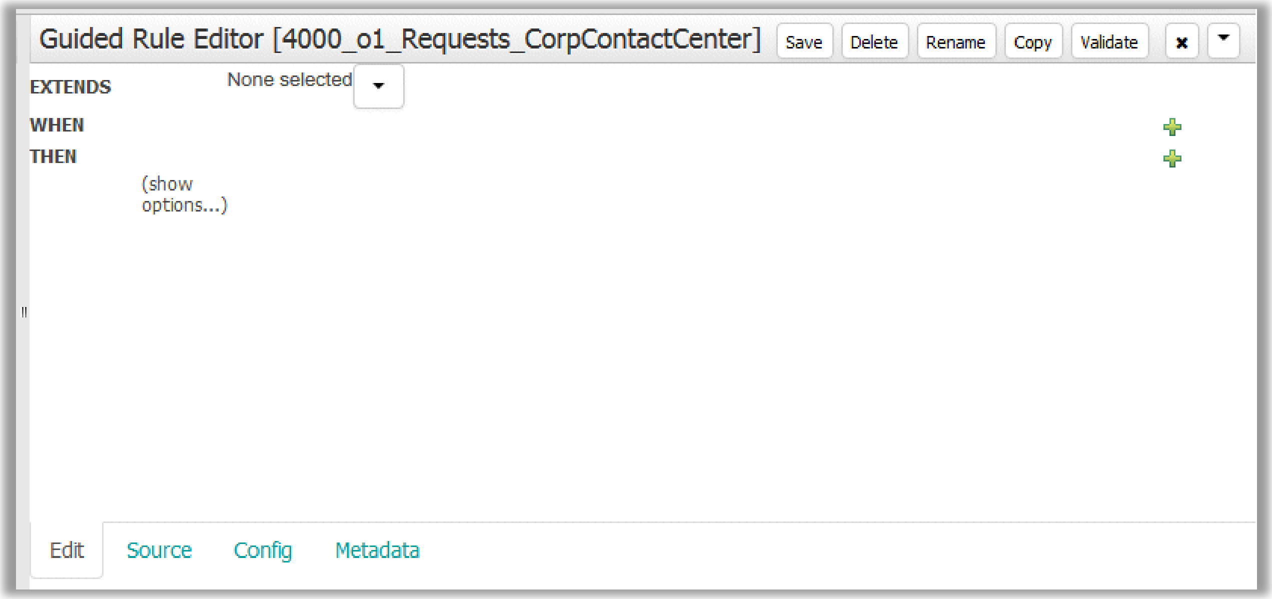
Orchestra One Verification Request Rules are Blacklist Allow Rules. They should be placed after all Blacklist Terminate (reject) and Blacklist Redirection Rules.

Defining an Orchestra One™ Verification Request Rule

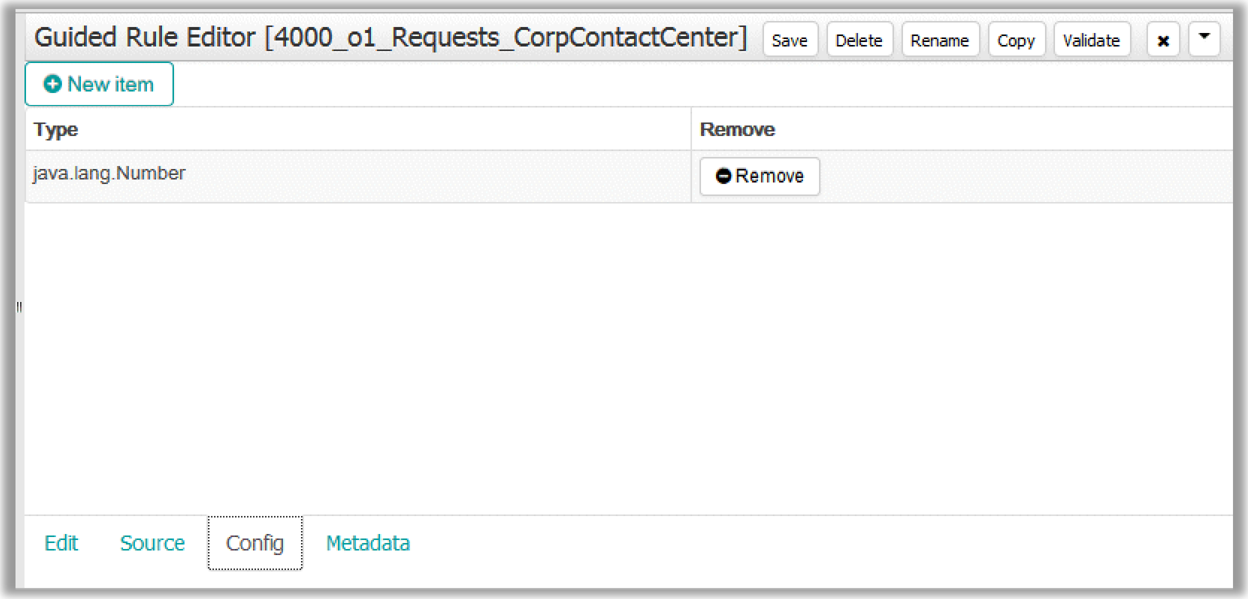
To define an Orchestra One™ Verification Request Rule

1. On the **Project Explorer** main menu, click the down arrow and click **cep2sep**.
2. On the BRMS main menu, click **New Item | Guided Rule**. The **Create new Guided Rule** dialog box appears.
3. Select **Use Domain Specific Language (DSL)**.
4. Type a name for the Rule that identifies its purpose. For example, type:

   `4000_o1_Requests_CorpContactCenter`
5. Click **OK**. The new Rule appears in the **Project Explorer** tree pane and opens in the **Guided Rule Editor**.

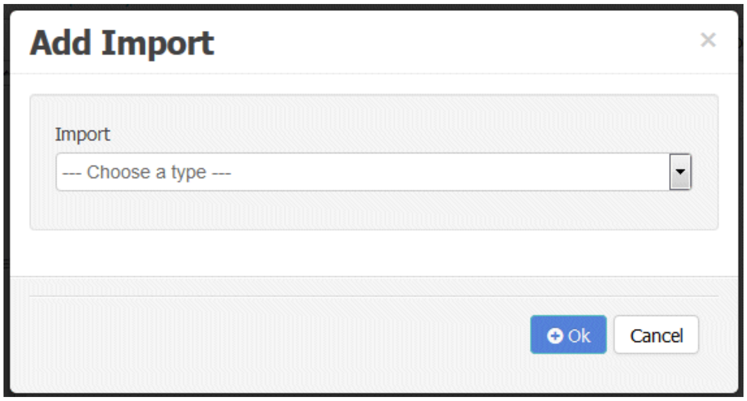


6. Click the **Config** tab.



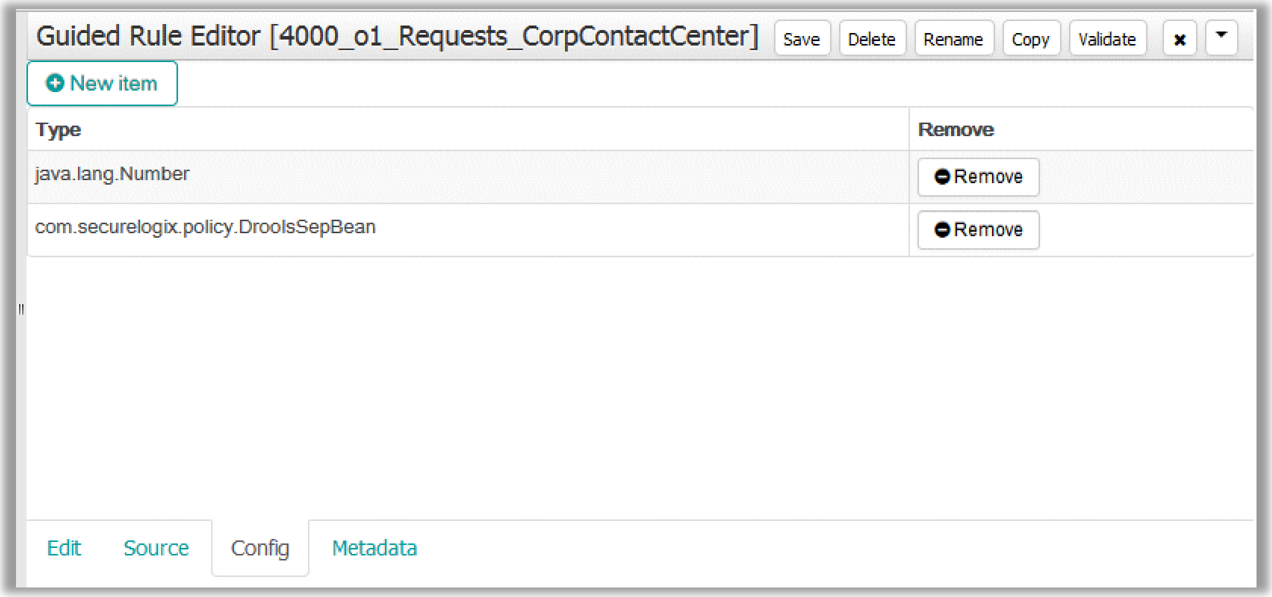
Type	Remove
java.lang.Number	Remove

7. Click **New item**. The **Add import** dialog box appears.



8. In the **Import** box, click the down arrow, scroll down the list, and click **com.securelogix.policy.DroolsSepBean**. (Entries are in alphabetical order. This one is near the bottom of the list.)

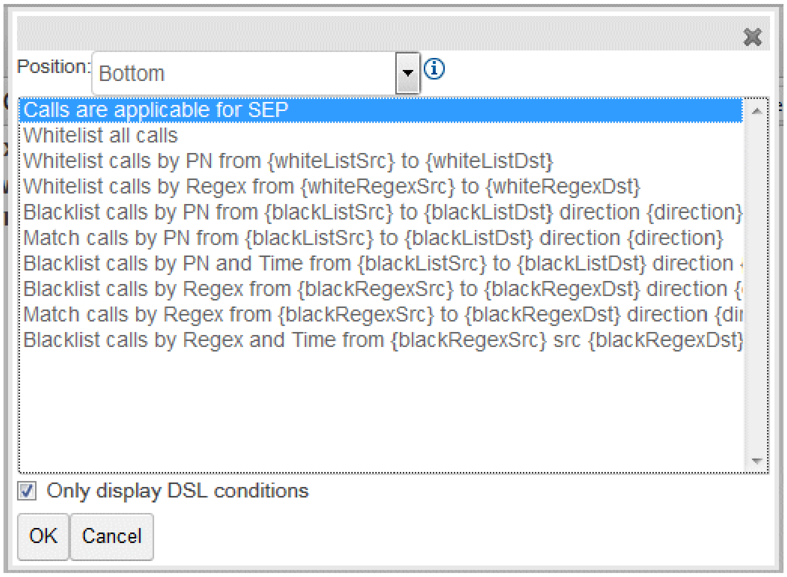
9. Click **OK**. The Import appears on the **Config** tab.



Type	Remove
java.lang.Number	Remove
com.securelogix.policy.DroolsSepBean	Remove

10. Click the **Edit** tab.

11. Click the green PLUS SIGN to the right of **WHEN**. The **SEP WHEN Conditions** dialog box appears.



Position: Bottom

Calls are applicable for SEP
Whitelist all calls
Whitelist calls by PN from {whiteListSrc} to {whiteListDst}
Whitelist calls by Regex from {whiteRegexSrc} to {whiteRegexDst}
Blacklist calls by PN from {blackListSrc} to {blackListDst} direction {direction}
Match calls by PN from {blackListSrc} to {blackListDst} direction {direction}
Blacklist calls by PN and Time from {blackListSrc} to {blackListDst} direction
Blacklist calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {
Match calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {di
Blacklist calls by Regex and Time from {blackRegexSrc} src {blackRegexDst}

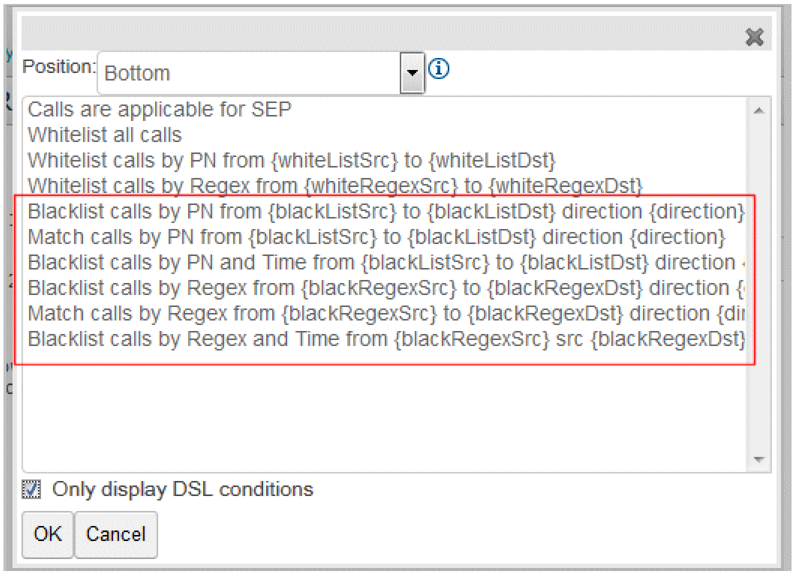
☑ Only display DSL conditions

12. Click **Calls are applicable to SEP** and then click **OK**.

13. Click the green PLUS SIGN to the right of **WHEN** again. The **SEP WHEN Conditions** dialog box appears.

14. Click one of the Blacklist options, according to whether you will use Regex Blacklists or a Phone Number Blacklists to specify the called and/or calling numbers to which the Rule applies.

Note: The **Match calls…**options are also Blacklist options, since they use Blacklists to specify source and destination.

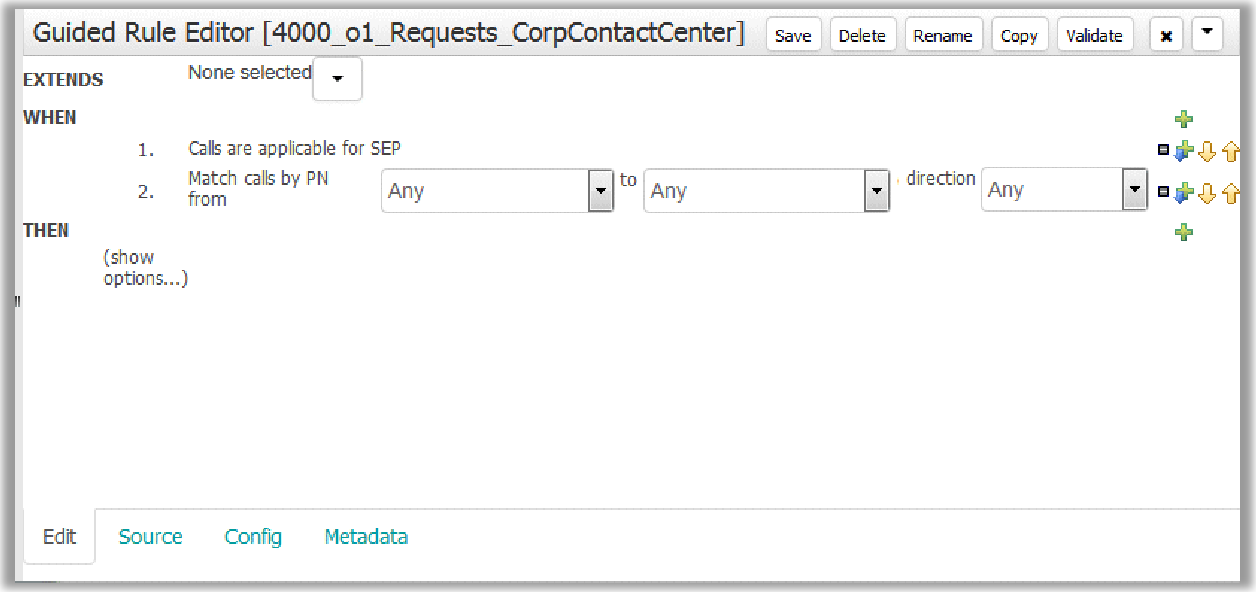


Position: Bottom

Calls are applicable for SEP
Whitelist all calls
Whitelist calls by PN from {whiteListSrc} to {whiteListDst}
Whitelist calls by Regex from {whiteRegexSrc} to {whiteRegexDst}
Blacklist calls by PN from {blackListSrc} to {blackListDst} direction {direction}
Match calls by PN from {blackListSrc} to {blackListDst} direction {direction}
Blacklist calls by PN and Time from {blackListSrc} to {blackListDst} direction
Blacklist calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {
Match calls by Regex from {blackRegexSrc} to {blackRegexDst} direction {di
Blacklist calls by Regex and Time from {blackRegexSrc} src {blackRegexDst}

☑ Only display DSL conditions

15. Click **OK**.



Guided Rule Editor [4000_o1_Requests_CorpContactCenter]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP
2. Match calls by PN from Any to Any direction Any

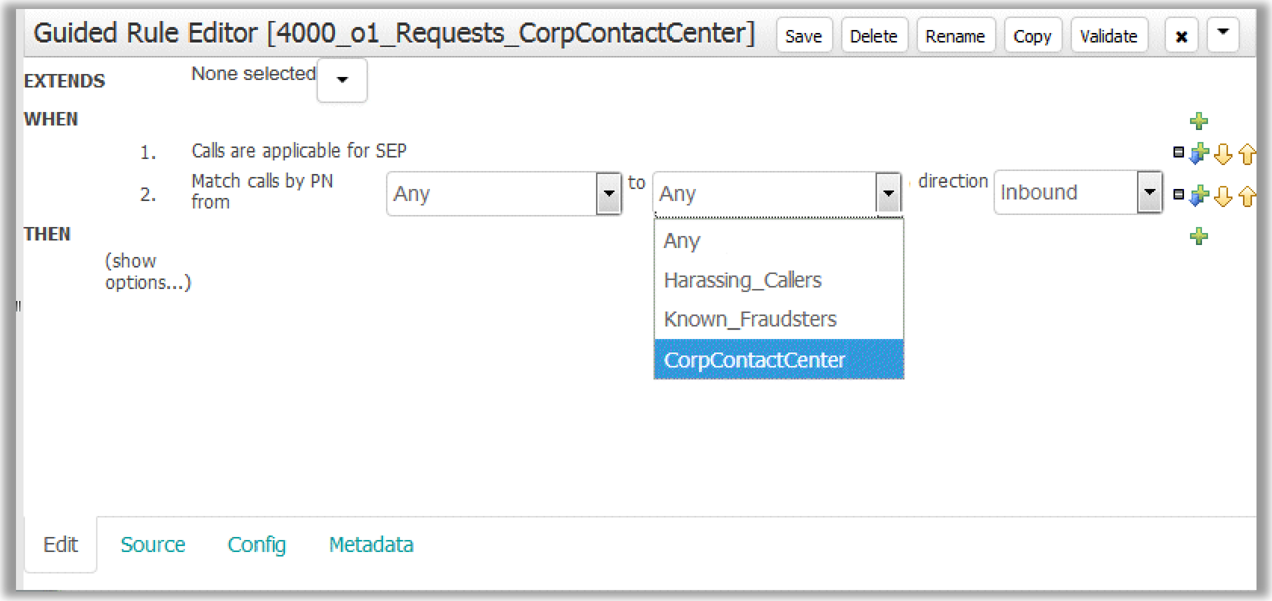
THEN

(show options...)

16. In the **direction** box, click the down arrow and click **Inbound**.

17. Next, you'll specify the source and/or destination numbers to which this Rule applies. For example, suppose you want to specify that all inbound calls to your Corporate Contact Center that don't match a previous Whitelist or Blacklist Terminate/Redirect Rule are to trigger an Orchestra One Verification Request. Leave the **from** box (source) set to **Any**. Click the down arrow in the **to** (destination) box.

18. Click the List that contains the destinations in your organization to which this Rule applies.



Guided Rule Editor [4000_o1_Requests_CorpContactCenter]

EXTENDS None selected

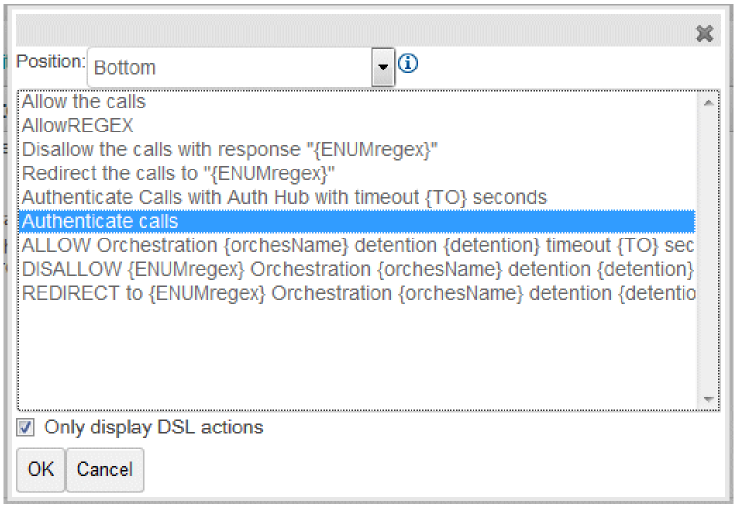
WHEN

1. Calls are applicable for SEP
2. Match calls by PN from Any to Any direction Inbound

THEN

(show options...)

19. Next, you'll define the **THEN** action that denotes what is to occur when the **WHEN** conditions match a call, in this case an Orchestra One Verification Request. Click the green PLUS SIGN to the right of **THEN**. The **SEP THEN Actions** dialog box appears.

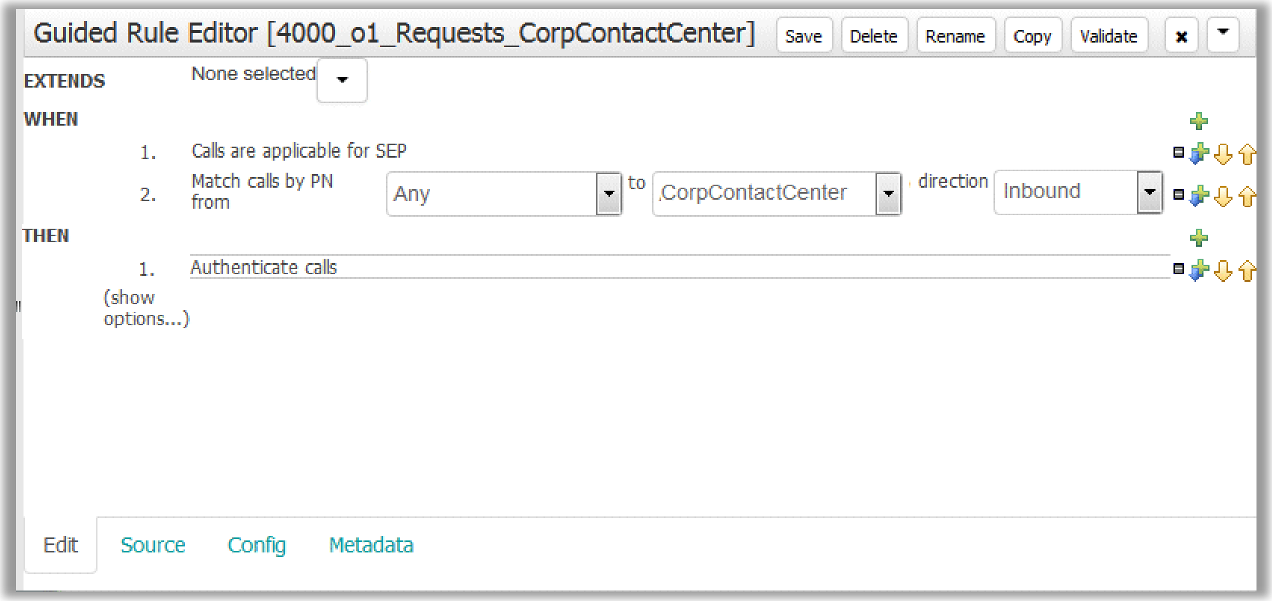


Position: Bottom

Allow the calls
AllowREGEX
Disallow the calls with response "{ENUMregex}"
Redirect the calls to "{ENUMregex}"
Authenticate Calls with Auth Hub with timeout {TO} seconds
Authenticate calls
ALLOW Orchestration {orchesName} detention {detention} timeout {TO} sec
DISALLOW {ENUMregex} Orchestration {orchesName} detention {detention}
REDIRECT to {ENUMregex} Orchestration {orchesName} detention {detentio

☑ Only display DSL actions

20. Click **Authenticate calls** and then click **OK**.



Guided Rule Editor [4000_o1_Requests_CorpContactCenter]

EXTENDS None selected

WHEN

1. Calls are applicable for SEP
2. Match calls by PN from Any to CorpContactCenter direction Inbound

THEN

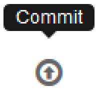
1. Authenticate calls

(show options...)

21. The Rule is complete. Click **Save** on the **Guided Rule Editor** main menu. **Note**: Orchestra One Verification Request Rules uses the default **Allow** Regex for matching calls. You can view this oon the **Config** tab.

22. Click **Validate**.

23. Click the **Commit** button on the right below the PolicyGuru GUI main menu to install the SEP Policy on the ENUM Servers in your deployment for the Rule to take effect.



Complex Event Processing (CEP) Policy

CEP Rules

As described earlier, CEP Rules are used to generate alerts for SEP Rule firings. See "Defining a CEP Alert Rule for an SEP-Rule-Firing" on page 72 for instructions.

Although a set of example Rules are still included in the GUI, these are no longer supported. Use CEP Rules only for SEP alerting.

IMPORTANT: If you are using an external LDAP login for the first time, see "Important Information About First-Time Login via External LDAP" on page 41 and follow those instructions before continuing, if you have not already done so.

Guided CEP Rules with DSL

Guided Rules with DSL provide an editor with a predefined set of assets from which to choose when defining a Rule. The editor then generates the required DRL, which is what the decision engine uses to execute the Rule. This generated DRL can be viewed on the **Source** tab of the **Guided Rule Editor**, but it cannot be edited there, since it is automatically generated based on the inputs in the editor.

Guided Rule with DSL When Conditions and Then Actions

When Conditions define the criteria that cause a Rule to fire.

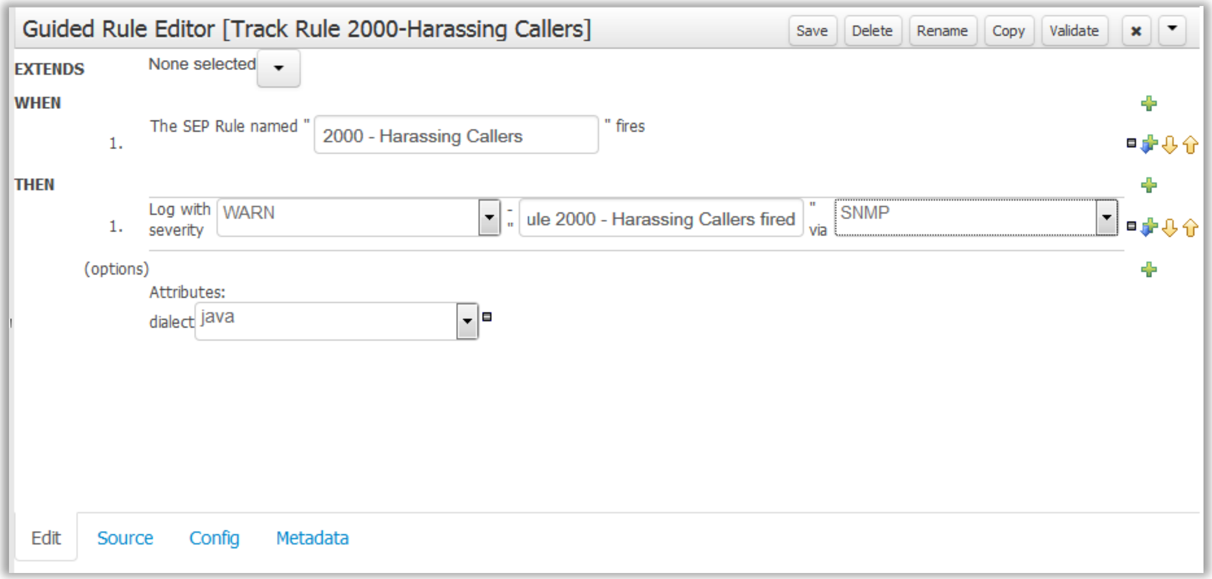
Then Actions define what is to happen when the **When Condition**(s) of the Rule are met.

Enabling and Disabling CEP Rules

You can disable a CEP Rule by adding the **I am an example** WHEN condition as the first WHEN condition in the Rule and reinstalling the Policy. This prevents the rest of the Rule from being processed. This means you can have Rule(s) predefined, currently inactive, and ready to implement as needed by simply removing the **I am an example** WHEN condition. enable the Rule and then reinstalling the Policy.

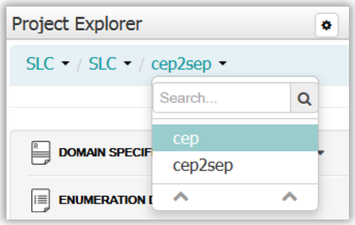
Defining a CEP Alert Rule for an SEP-Rule-Firing

CEP Alerting Rules are used to generate logging and alerts when SEP Rules fire. For example, the Rule in the illustration below generates an SNMP notification when an SEP Rule named **2000 Harassing Callers** fires.

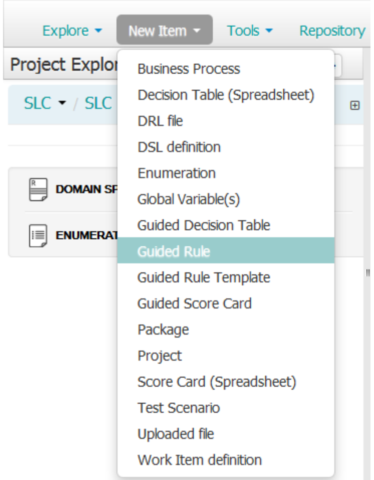


To define a CEP Alerting Rule

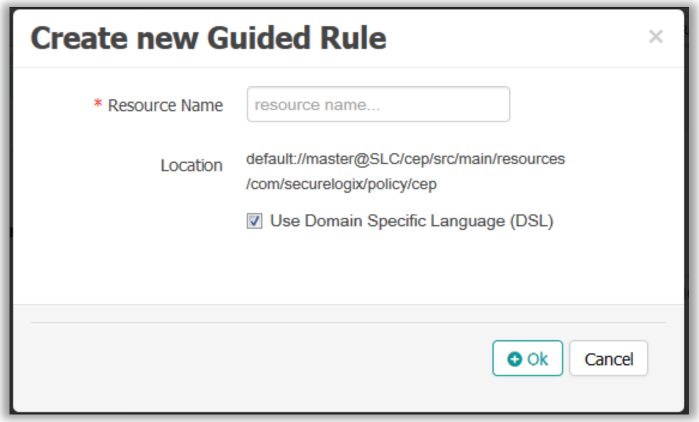
1. In the **Project Explorer** pane of the BRMS, click the far right down arrow and click **cep**, if it is not already selected.



2. On the BRMS main menu, click **New Item | Guided Rule**.



The **Create New Guided Rule** dialog box appears.



Create new Guided Rule

* Resource Name: resource name...

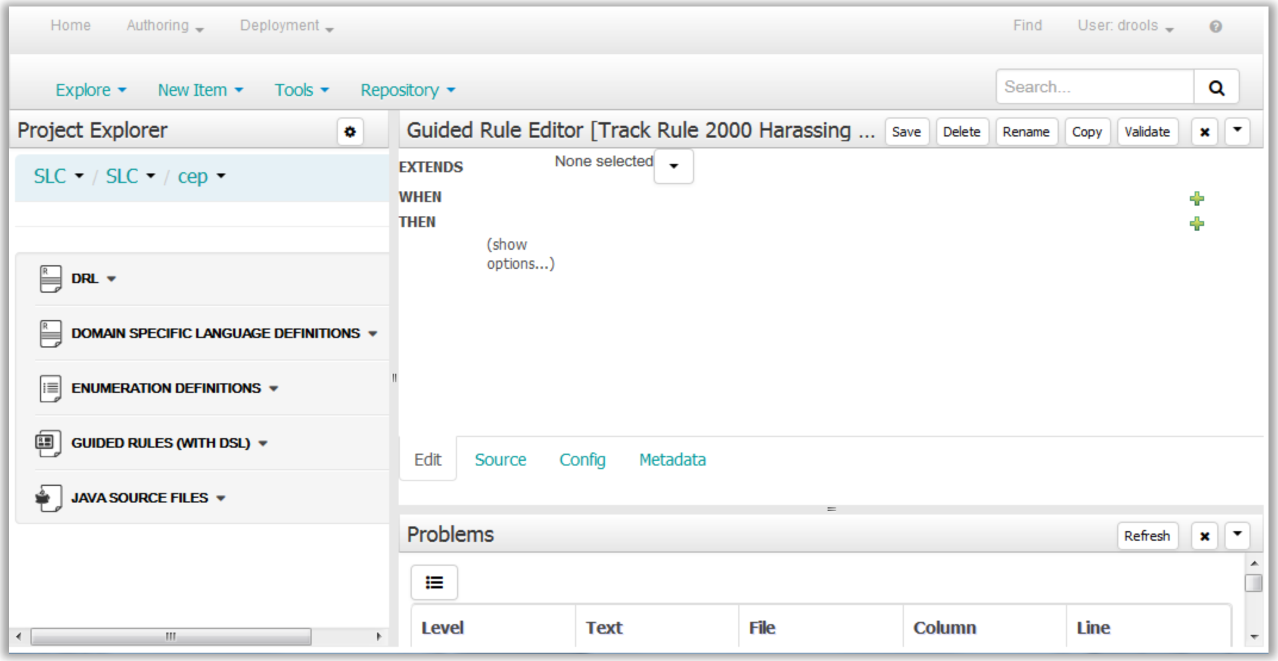
Location: default://master@SLC/cep/src/main/resources /com/securelogix/policy/cep

☑ Use Domain Specific Language (DSL)

3. In the **Resource Name** box, type a descriptive name for the Rule. For example, if the Rule is to alert for the SEP Rule named “2000 - Harassing Callers”, you might name the CEP Rule “Track Rule 2000 - Harassing Callers”.

4. Select **Use Domain Specific Language (DSL)**, and then click **OK**.

   The blank Rule appears in the **Guided Rule Editor**.



Guided Rule Editor [Track Rule 2000 Harassing ...

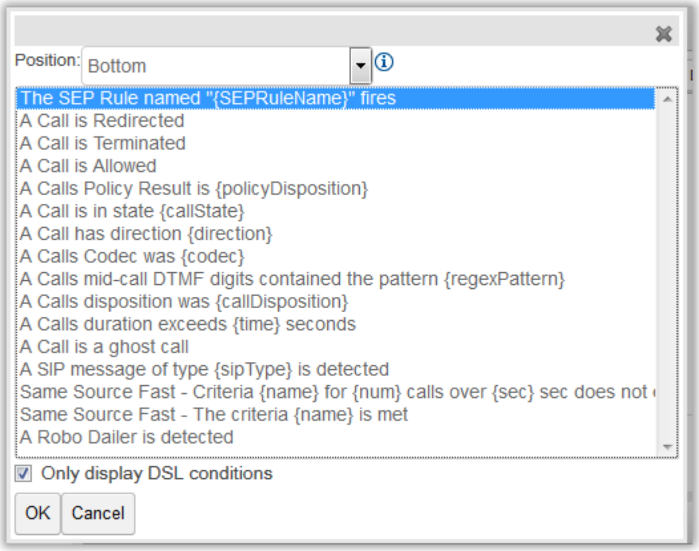
EXTENDS None selected

WHEN

THEN

(show options...)

5. Click the green PLUS SIGN (+) to the right of **When** and select **The SEP Rule named “{SEPRuleName}” fires**.

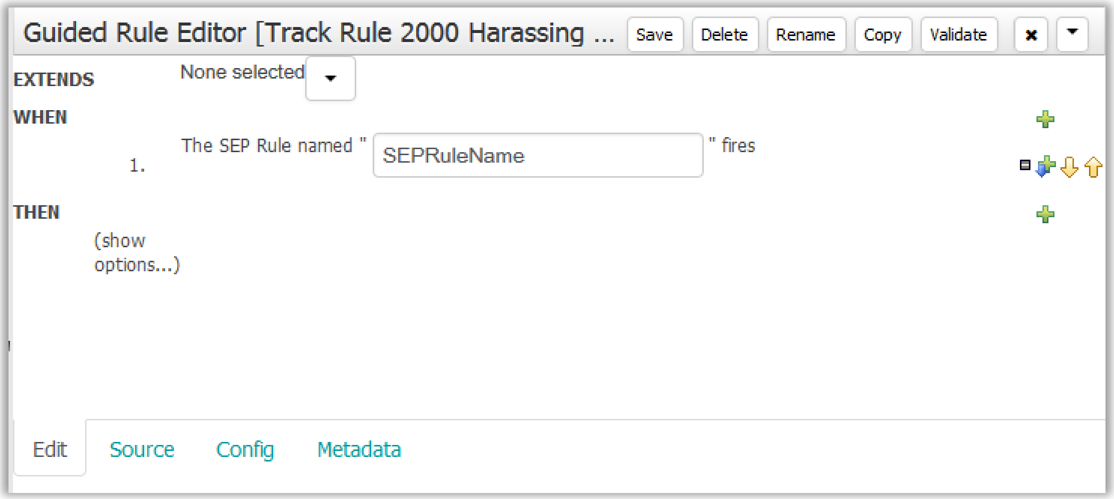


Position: Bottom

The SEP Rule named "{SEPRuleName}" fires
A Call is Redirected
A Call is Terminated
A Call is Allowed
A Calls Policy Result is {policyDisposition}
A Call is in state {callState}
A Call has direction {direction}
A Calls Codec was {codec}
A Calls mid-call DTMF digits contained the pattern {regexPattern}
A Calls disposition was {callDisposition}
A Calls duration exceeds {time} seconds
A Call is a ghost call
A SIP message of type {sipType} is detected
Same Source Fast - Criteria {name} for {num} calls over {sec} sec does not
Same Source Fast - The criteria {name} is met
A Robo Dailer is detected

☑ Only display DSL conditions

6. Click **OK**.



Guided Rule Editor [Track Rule 2000 Harassing ...

EXTENDS None selected

WHEN

1. The SEP Rule named " SEPRuleName " fires

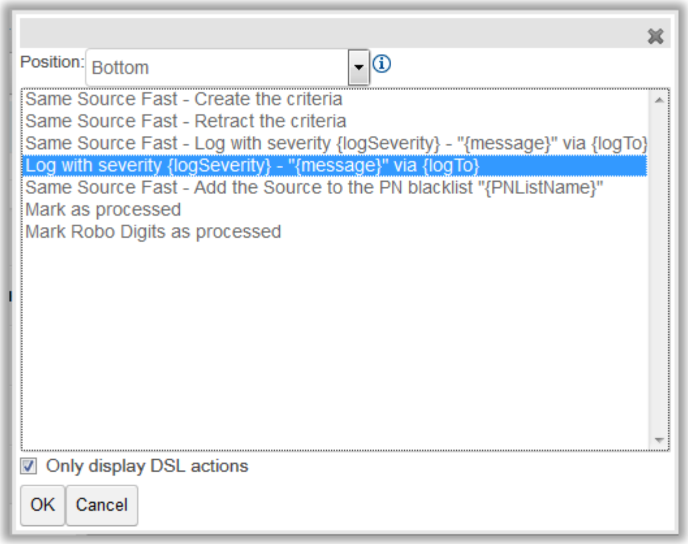
THEN

(show options...)

7. Replace **SEPRuleName** with the exact name of the Rule for which it is to alert. For this example, type:

   ```
   2000 Harassing Callers
   ```

8. Click the green PLUS SIGN (**+**) to the right of **Then**, select **Log with severity {logSeverity} – "{message}" via {logTo}** and then click **OK.**

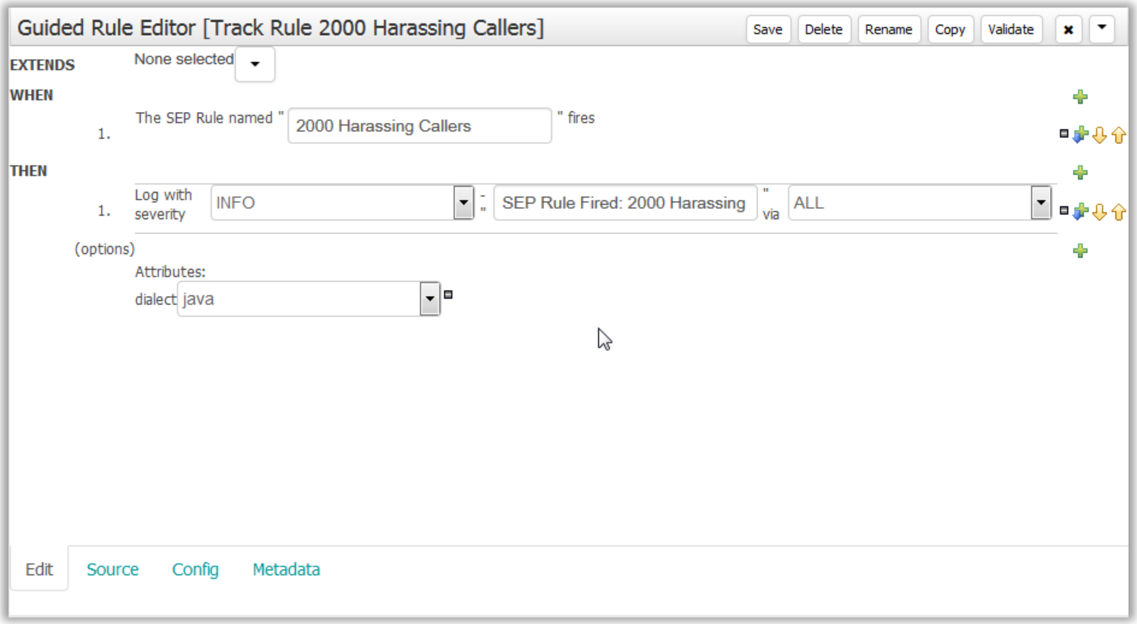


Position: Bottom

Same Source Fast - Create the criteria
Same Source Fast - Retract the criteria
Same Source Fast - Log with severity {logSeverity} - "{message}" via {logTo}
Log with severity {logSeverity} - "{message}" via {logTo}
Same Source Fast - Add the Source to the PN blacklist "{PNListName}"
Mark as processed
Mark Robo Digits as processed

☑ Only display DSL actions

IMPORTANT: Unlike SEP Rules, all **Then** clauses in a CEP Rule are used in Rule processing. Not all Rule assets are compatible for use in the same Rule, however; an error is generated if you include incompatible clauses.



Guided Rule Editor [Track Rule 2000 Harassing Callers]

EXTENDS None selected

WHEN

1. The SEP Rule named " 2000 Harassing Callers " fires

THEN

1. Log with severity INFO - " SEP Rule Fired: 2000 Harassing " via ALL

(options)

Attributes:

dialect java

9. In the **Log with Severity** field, click the down arrow and select the log level. For example, select **INFO** or **WARN**.

   Note: Severity **Debug** does not appear in the **Realtime** screen; only severities **Info** and above do. Only **WARN** and above appear by default in the server log.

10. Replace **message** with the text of the message you want sent in the alert, in double-quotes. For example, type:

    `“SEP Rule fired: 2000 – Harassing Callers”`

11. Click the down arrow and select the alerting destination:

   - **LOCAL**—The local log file on the Mediation Server
   - **GLOBAL**—The database, from which the alerts are available via the web interface
   - **NOTIFY**—Email
   - **SYS**—Syslog alerting
   - **SNMP**—SNMP trap
   - **ALL**—All of the above

12. Click **Show Options** and set the dialect to **Java**.
13. Click **Save**.
14. Click **Validate**. If validation fails, check the **Problems** pane at the bottom of the **Guided Rule Editor**. Correct any errors and then click **Validate** again.
15. When validation succeeds and you are ready to install the policy, see “Installing or Reinstalling a CEP Policy” on page 82. **IMPORTANT**: CEP Policies are not installed using the SEP **Commit** icon. They use the same **Build and Deploy** mechanism as IPS Policies.

Note: **Validate** checks the entire Policy, not just the Rule you have open.

Configuring a DTMF Digit Count Rule

In a very low-call volume environment (10 CPS or less), you can define a CEP Rule to alert when the count of DTMF digits for a call exceeds a specified number within a specified period of time (by default, 10 digits within 15 seconds.). Per-call DTMF digit counting is supported for up to 15 digits at up to 10 CPS. This Rule uses Metadata Probe data of detected RTP-based telephone event digits as defined in RFC-4733.

IMPORTANT: You can use only one such Rule. Multiple Rules for different counts are not supported.

Enabling DTMF Digit Detection

Before you can implement a DTMF digit counting Rule, you must first enable DTMF detection on the Metadata Probe(s) in your deployment. It is disabled by default.

To enable DTMF digit detection

1. SSH to each Probe and open the **/opt/ngp/bin/sniffer/updateNativeConfig.sh** script in a text editor.
2. Near the bottom, locate the following lines:

```
##BPF_FILTER="udp and ( ( $SIP_PORT and ( $SIP_REQUEST or $SIP_RESPONSE ) ) or
$DTMF_BEARING_RTP )"
BPF_FILTER="udp and ( $SIP_PORT and ( $SIP_REQUEST or $SIP_RESPONSE ) )"
```

3. Uncomment the first line beginning with `BPF_FILTER=`, and comment out the second line beginning with `BPF_FILTER=`,
4. Save the file and execute the script.
5. Restart the **ngp** service on the Probe if it is running to effect the change.

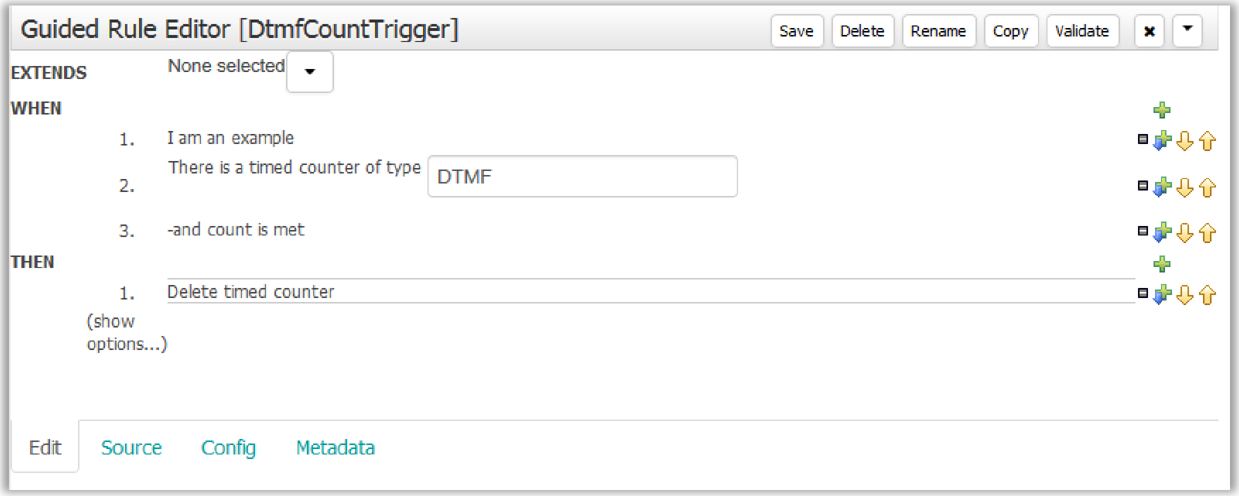
Defining an Alert Rule for DTMF Digit Counts

When DTMF detection is enabled, a counter is created for each call. If the specified count of midcall DTMF digits is met within a specified time threshold, the count is met and an alert you have created is generated and then the counter for that call is deleted. If the count is not met within the time threshold, the counter is simply deleted at the end of the interval.

The default values are 10 digits in 15 seconds. You can modify these values to match your scenario of interest. See "Changing the DTMF Count and/or Time Threshold" on page 80 for instructions.

To create the alerting Rule

1. In the PolicyGuru BRMS **Project Explorer** pane , click the down arrow and click **CEP**.
2. In the **Project Editor** pane, click the down arrow to expand **Guided Rules with DSL** and then click the rule named **DtmfCountTrigger**.



Guided Rule Editor [DtmfCountTrigger]

EXTENDS None selected

WHEN

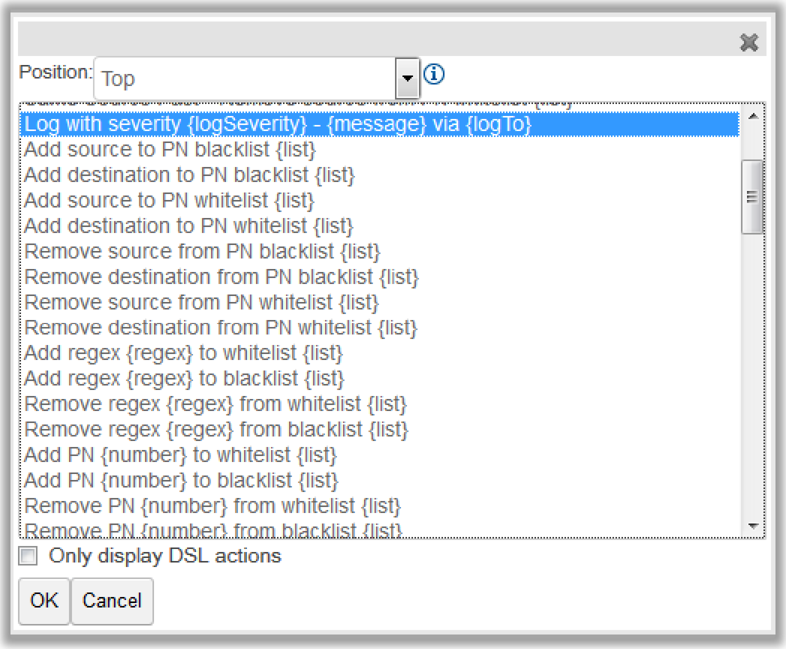
1. I am an example
2. There is a timed counter of type DTMF
3. -and count is met

THEN

1. Delete timed counter

(show options...)

3. Delete the **WHEN** condition **I am an example** by clicking the **Delete** icon ▣ to the right of it.
4. Click the PLUS SIGN to the right of **THEN** to add an alert action.



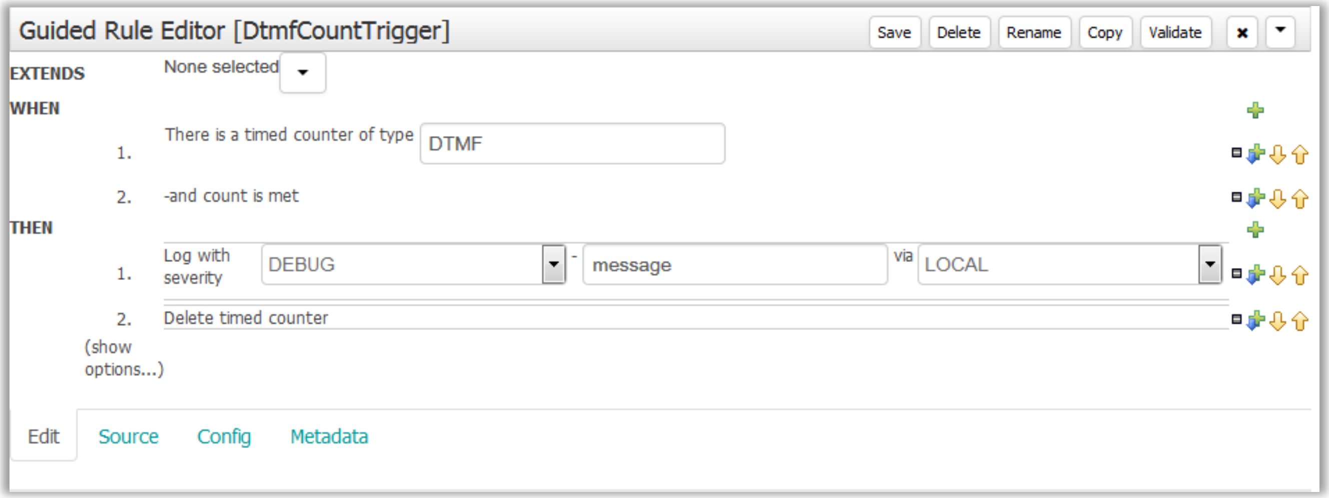
Position: Top

Log with severity {logSeverity} - {message} via {logTo}
Add source to PN blacklist {list}
Add destination to PN blacklist {list}
Add source to PN whitelist {list}
Add destination to PN whitelist {list}
Remove source from PN blacklist {list}
Remove destination from PN blacklist {list}
Remove source from PN whitelist {list}
Remove destination from PN whitelist {list}
Add regex {regex} to whitelist {list}
Add regex {regex} to blacklist {list}
Remove regex {regex} from whitelist {list}
Remove regex {regex} from blacklist {list}
Add PN {number} to whitelist {list}
Add PN {number} to blacklist {list}
Remove PN {number} from whitelist {list}
Remove PN {number} from blacklist {list}

☐ Only display DSL actions

5. In the **Position** box, click the down arrow and click **Top** so that the alert action is added as the first **THEN**.

6. Click **Log with severity {logSeverity} – {message} via {logTo}** and then click **OK**.



Guided Rule Editor [DtmfCountTrigger]

EXTENDS None selected

WHEN

1. There is a timed counter of type DTMF

2. -and count is met

THEN

1. Log with severity DEBUG - message via LOCAL

2. Delete timed counter

7. In the **THEN** action **Log with severity:**

- Click the first down arrow and set the logging level.

- Type the message to be included in the alert in the second box, enclosed in double quotes. For example: “DTMF count met for a call.”

- Click the down arrow in the third box and set the logging destination.

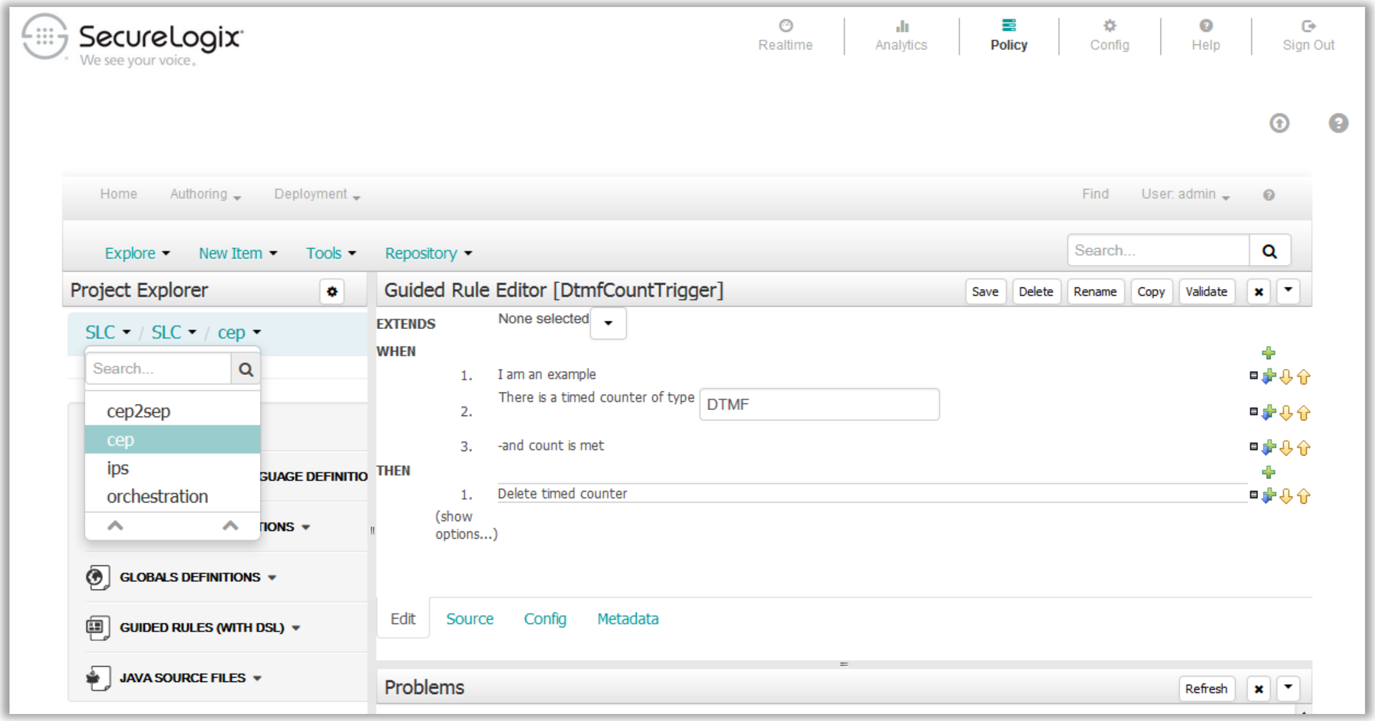
8. Click **Save**.

9. When the save completes, click **Validate**. Wait for validation to complete.
10. Click **Tools | Project Editor** and then click **Build and Deploy** to reinstall the CEP Policy.

Changing the DTMF Count and/or Time Threshold

To modify the DTMF count and/or time threshold

1. In the PolicyGuru BRMS **Project Explorer** pane , click the down arrow and click **CEP**.



Guided Rule Editor [DtmfCountTrigger]

EXTENDS None selected

WHEN

1. I am an example
2. There is a timed counter of type DTMF
3. -and count is met

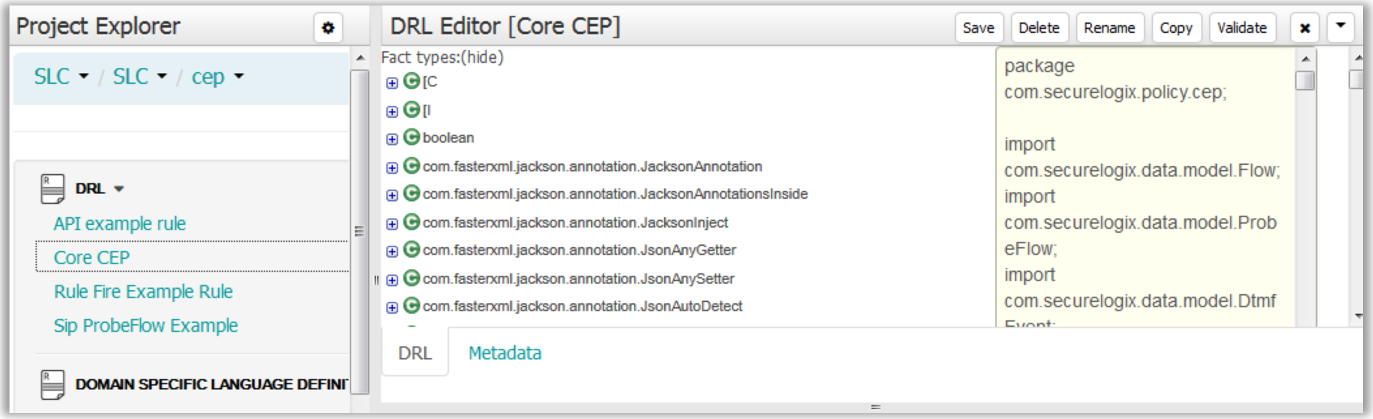
THEN

1. Delete timed counter

(show options...)

2. In the **Project Explorer** pane, click the **DRL** down arrow and then click **Core CEP**.

   The **Core CEP.drl** file opens in the **Policy Editor** pane.

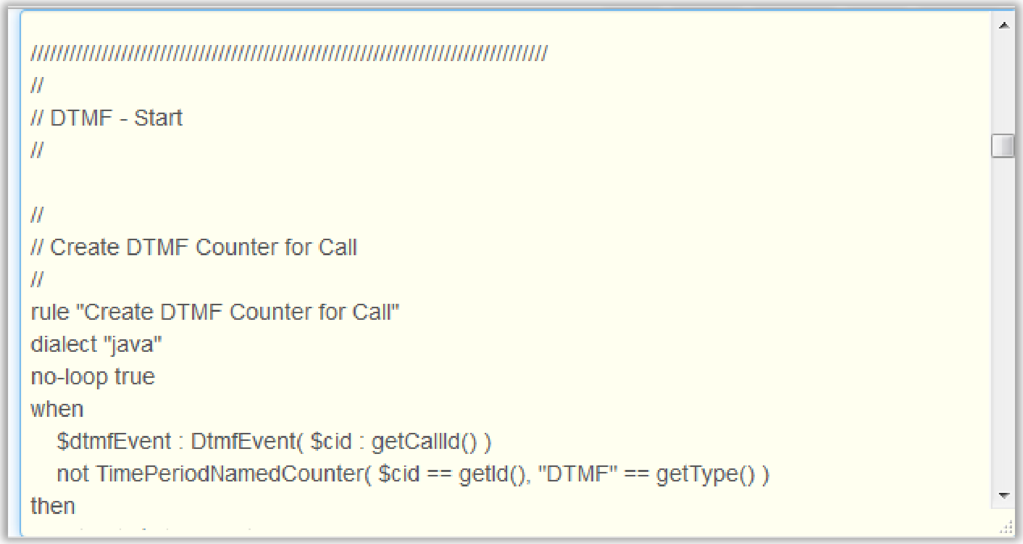


Project Explorer
SLC / SLC / cep
DRL
API example rule
Core CEP
Rule Fire Example Rule
Sip ProbeFlow Example
DOMAIN SPECIFIC LANGUAGE DEFINI
DRL Editor [Core CEP]
Save
Delete
Rename
Copy
Validate
Fact types:(hide)
[C
[I
boolean
com.fasterxml.jackson.annotation.JacksonAnnotation
com.fasterxml.jackson.annotation.JacksonAnnotationsInside
com.fasterxml.jackson.annotation.JacksonInject
com.fasterxml.jackson.annotation.JsonAnyGetter
com.fasterxml.jackson.annotation.JsonAnySetter
com.fasterxml.jackson.annotation.JsonAutoDetect
DRL
Metadata

```
package
com.securelogix.policy.cep;

import
com.securelogix.data.model.Flow;
import
com.securelogix.data.model.Prob
eFlow;
import
com.securelogix.data.model.Dtmf
Event;
```

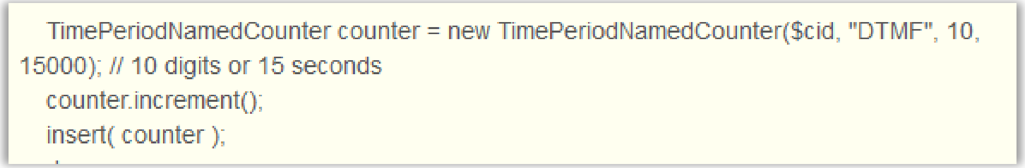
3. In the yellow area, locate the Rule named **“Create DTMF Counter for Call**.”



```
////////////////////////////////////////////////////////////////////////////////
//
// DTMF - Start
//

//
// Create DTMF Counter for Call
//
rule "Create DTMF Counter for Call"
dialect "java"
no-loop true
when
    $dtmfEvent : DtmfEvent( $cid : getCallId() )
    not TimePeriodNamedCounter( $cid == getId(), "DTMF" == getType() )
then
```

4. Scroll down to the section beginning **TimePeriodNamedCounter** and modify **10** (the count) and **15000** (the interval in milliseconds) and the corresponding values in **10 digits or 15 seconds** to the values you want to use.



```
   TimePeriodNamedCounter counter = new TimePeriodNamedCounter($cid, "DTMF", 10,
15000); // 10 digits or 15 seconds
   counter.increment();
   insert( counter );
```

IMPORTANT The longer the time interval, the higher the processing load on the system.

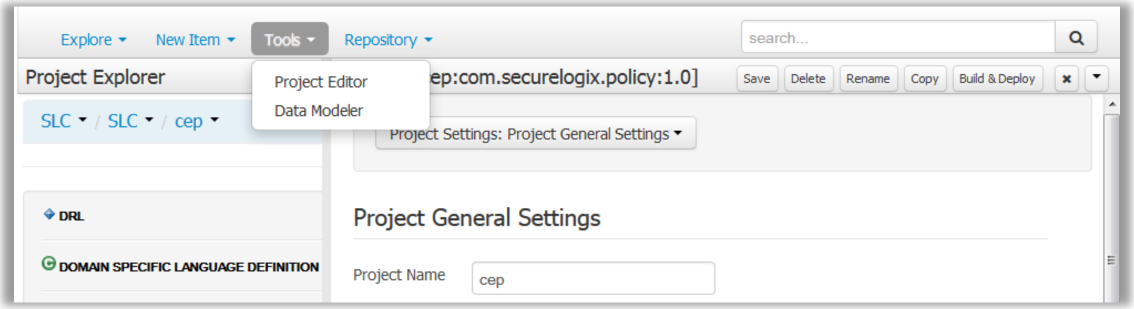
5. Click **Save**.

Click **Tools | Project Editor** and then click **Build and Deploy** to reinstall the CEP Policy.

Installing or Reinstalling a CEP Policy

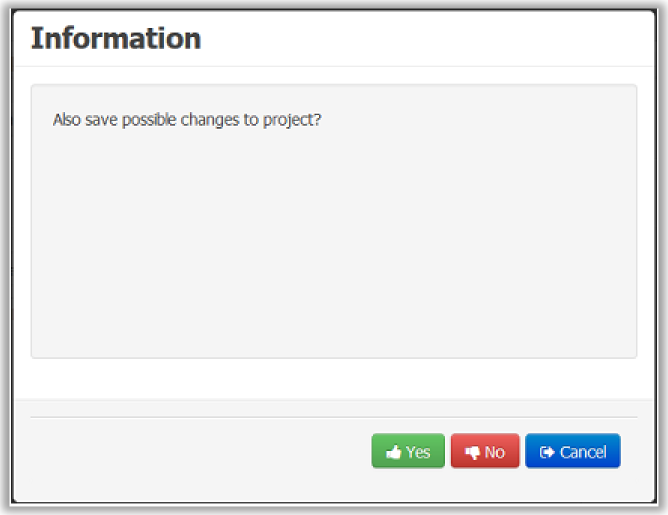
To install or reinstall a CEP Policy

1. On the BRMS main menu, click **Tools | Project Editor**.



Project Name: cep

2. Click **Build & Deploy**. The **Information** dialog box appears prompting you to save possible project changes before building and deploying.



Also save possible changes to project?

3. Click **Yes**. This saves all project files that may have unsaved changes prior to building and deploying.

CEP Rule Log/Alert Levels

CEP Rules offer the following log/alert levels:

- **LOCAL**—The server log file on the Mediation Server
- **GLOBAL**—The database, from which the alerts are available via the web interface
- **NOTIFY**—Email
- **SYS**—Syslog alerting
- **SNMP**—SNMP trap
- **ALL**—All of the above

Note: Severity **Debug** does not appear in the **Realtime** screen; only severities **Info** and above do. Only **WARN** and above appear by default in the server log.

Opening the Project Explorer Pane if It is Missing

On rare occasions, the **Project Explorer** pane may be closed when you access the BRMS GUI. If this occurs, see “Opening the Project Explorer Pane if It is Missing” on page 65 to restore it.

Real-Time Analytics

Viewing Call and Policy Processing Data with On-Screen Analytics

Real-Time Analytics provide graphical, drill-down onscreen reporting views of call and Policy processing data. Drill-down ENUM Call Details (using ENUM Server data) and SIP Call Details views (using Metadata Probe data), and “drill-up” Phone Number Analytics views (using Metadata Probe data for forensic analysis of a specific phone number or set of phone numbers) are available.

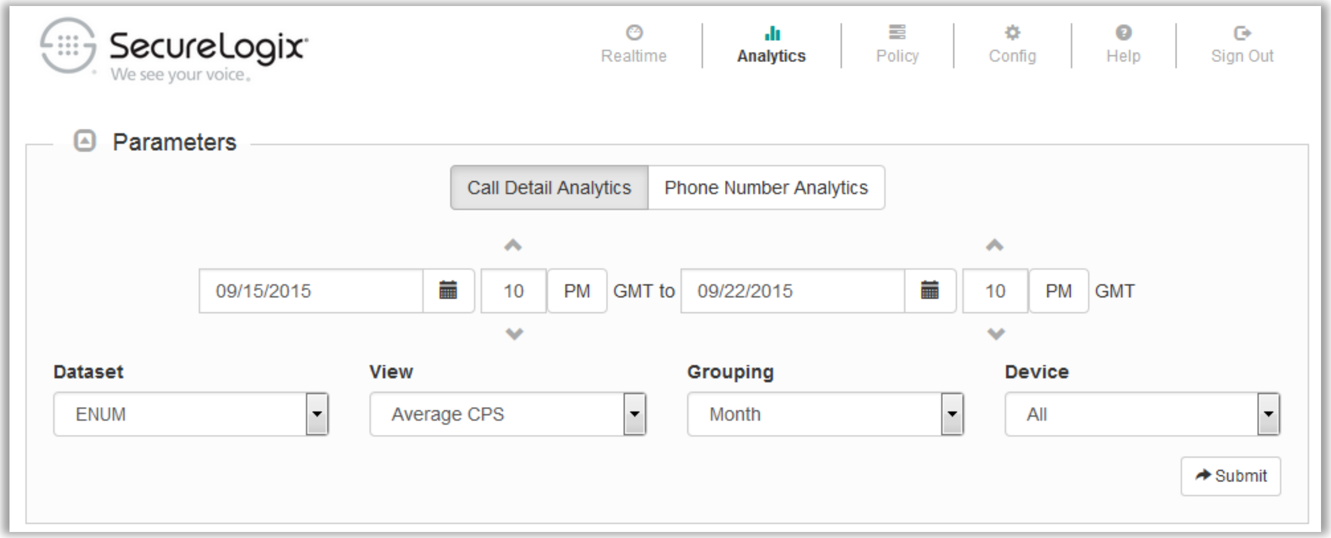
ENUM Call Detail Analytics

ENUM Call Details provide drill-down analytics views using ENUM Server call and SEP Policy processing data.

To view ENUM Call Detail Analytics

1. On the PolicyGuru main menu, click **Analytics**.

   The **Analytics** screen appears set to **Call Detail Analytics**, with **ENUM** selected as the dataset by default.



09/15/2015 10 PM GMT to 09/22/2015 10 PM GMT

Dataset: ENUM

View: Average CPS

Grouping: Month

Device: All

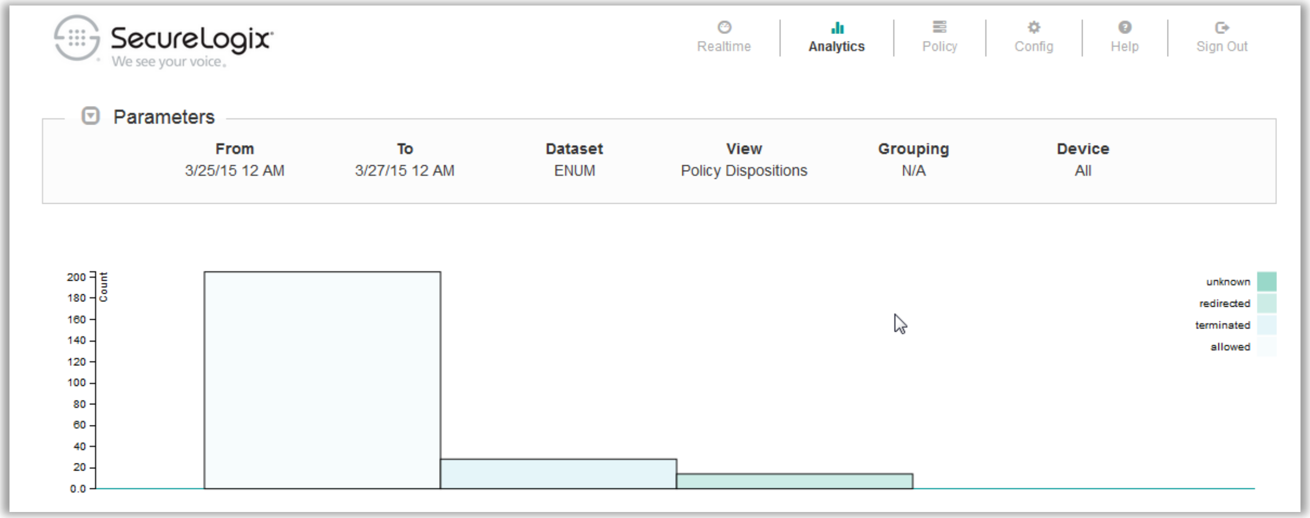
2. In the **Calendar** fields, select the start and end days and times for which to retrieve data. Times are in GMT.
3. Leave the **Dataset** field set to ENUM.
4. In the **View** field, click the down arrow and select the view for which you want to retrieve data:
   - **Average CPS**

- **Total Calls**
- **Policy Dispositions**
- **Top 10 Source**
- **Top 10 Destination**
- **Counts by Source Country**
- **Counts by Destination Country**

5. If you selected **Average CPS** or **Total Calls**, click the down arrow in the **Grouping** field and select the interval by which to group data: **Month**, **Day**, or **Hour**. All other views provide ungrouped data for the selected time range.

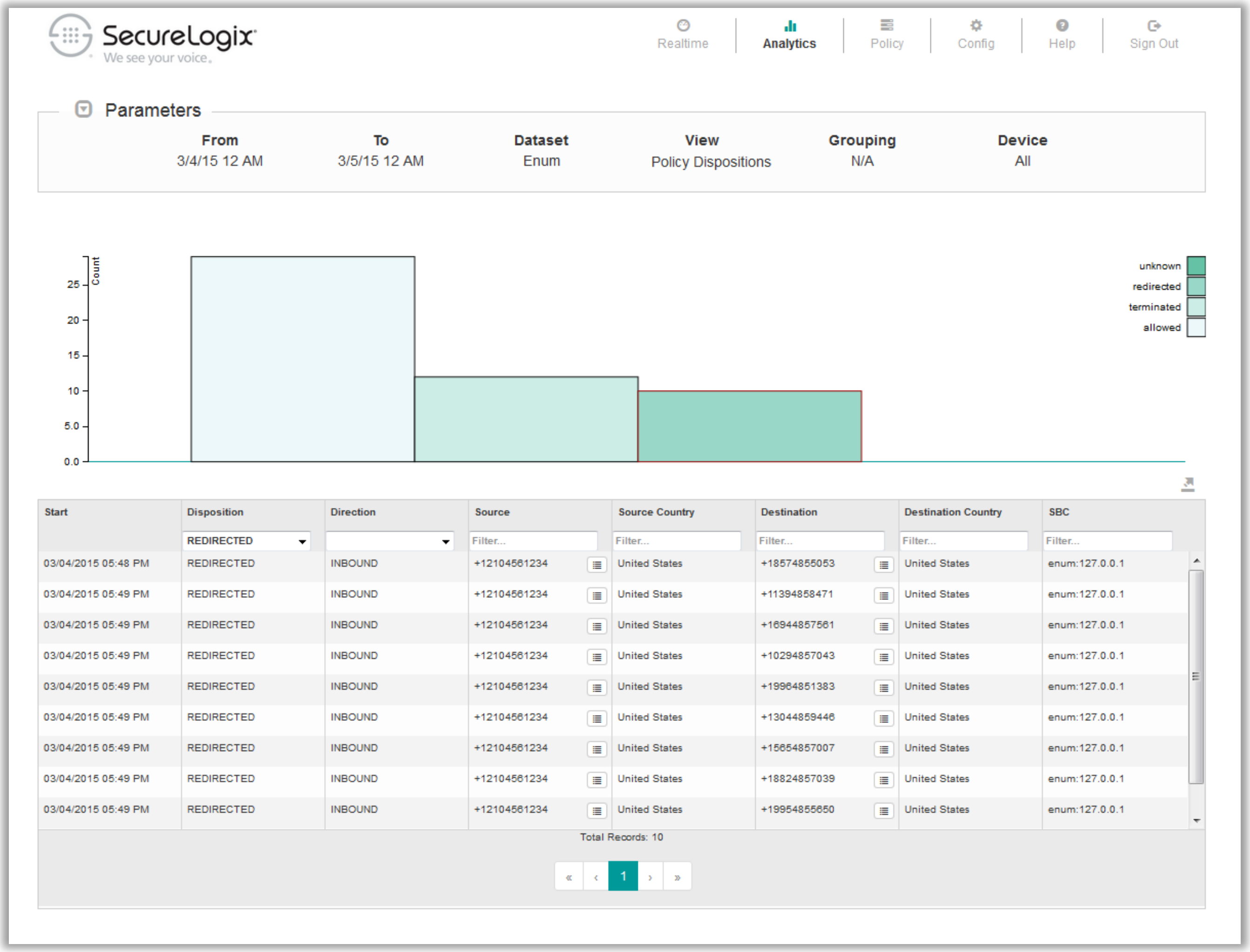
6. In the **Device** field, click the down arrow and select the SBC for which to view data, or leave the default of **All**.

7. Click **Submit**. The data is retrieved and displayed in a graph. The illustration below shows a **Policy Dispositions** view.



From	To	Dataset	View	Grouping	Device
3/25/15 12 AM	3/27/15 12 AM	ENUM	Policy Dispositions	N/A	All

8. Clicking the graph drills down to the next-lower grouping (**Month | Day | Hour | Call Details**).. When you drill down to **Call Details**, a table appears below the graph providing individual call details, including the total number of records.



Parameters

From	To	Dataset	View	Grouping	Device
3/4/15 12 AM	3/5/15 12 AM	Enum	Policy Dispositions	N/A	All

Start	Disposition	Direction	Source	Source Country	Destination	Destination Country	SBC
	REDIRECTED		Filter...	Filter...	Filter...	Filter...	Filter...
03/04/2015 05:48 PM	REDIRECTED	INBOUND	+12104561234	United States	+18574855053	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+11394858471	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+16944857561	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+10294857043	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+19964851383	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+13044859446	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+15654857007	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+18824857039	United States	enum:127.0.0.1
03/04/2015 05:49 PM	REDIRECTED	INBOUND	+12104561234	United States	+19954855650	United States	enum:127.0.0.1

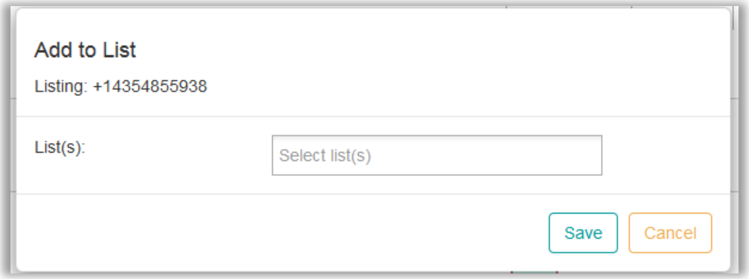
Total Records: 10

9. You can filter the display by **Disposition**, **Direction**, **Source**, **Source Country**, **Destination**, **Destination Country**, and **SBC**. The filters are applied automatically as you type or select.

10. You can sort the fields by clicking the heading of the column you want to sort by.

11. To add a phone number directly to a Blacklist or Whitelist from this view, click the **Add to List** icon to the right of the phone number. ≣

12. The **Add to List** dialog box appears.

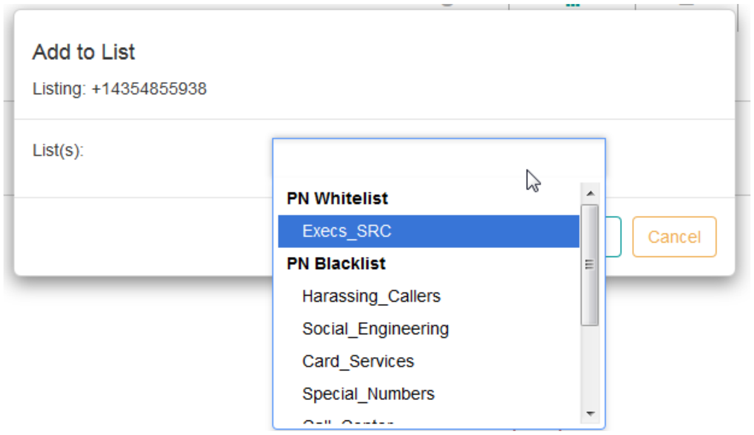


Add to List

Listing: +14354855938

List(s): Select list(s)

13. In the **List(s)** field, click the down arrow and click each List to which you want to add the selected number.



14. When you have added all applicable Lists, click **Save**. The phone number is added to the selected List(s).

    Note: To effect the change on the ENUM Server, you must reinstall the Policy that includes the List(s). The Policy is not automatically pushed.

SIP Call Detail Analytics

SIP Call Detail Analytics provides analytics views based on the SIP call data captured by the Metadata Probe.

To view SIP Call Detail Analytics

1. On the PolicyGuru main menu, click **Analytics**.

   The **Analytics** screen appears set to **Call Detail Analytics**, with **ENUM** selected as the dataset by default.

2. In the **Dataset** box, click the down arrow and click **SIP**.

3. In the **Calendar** fields, select the start and end days and times for which to retrieve data. Times are in GMT.

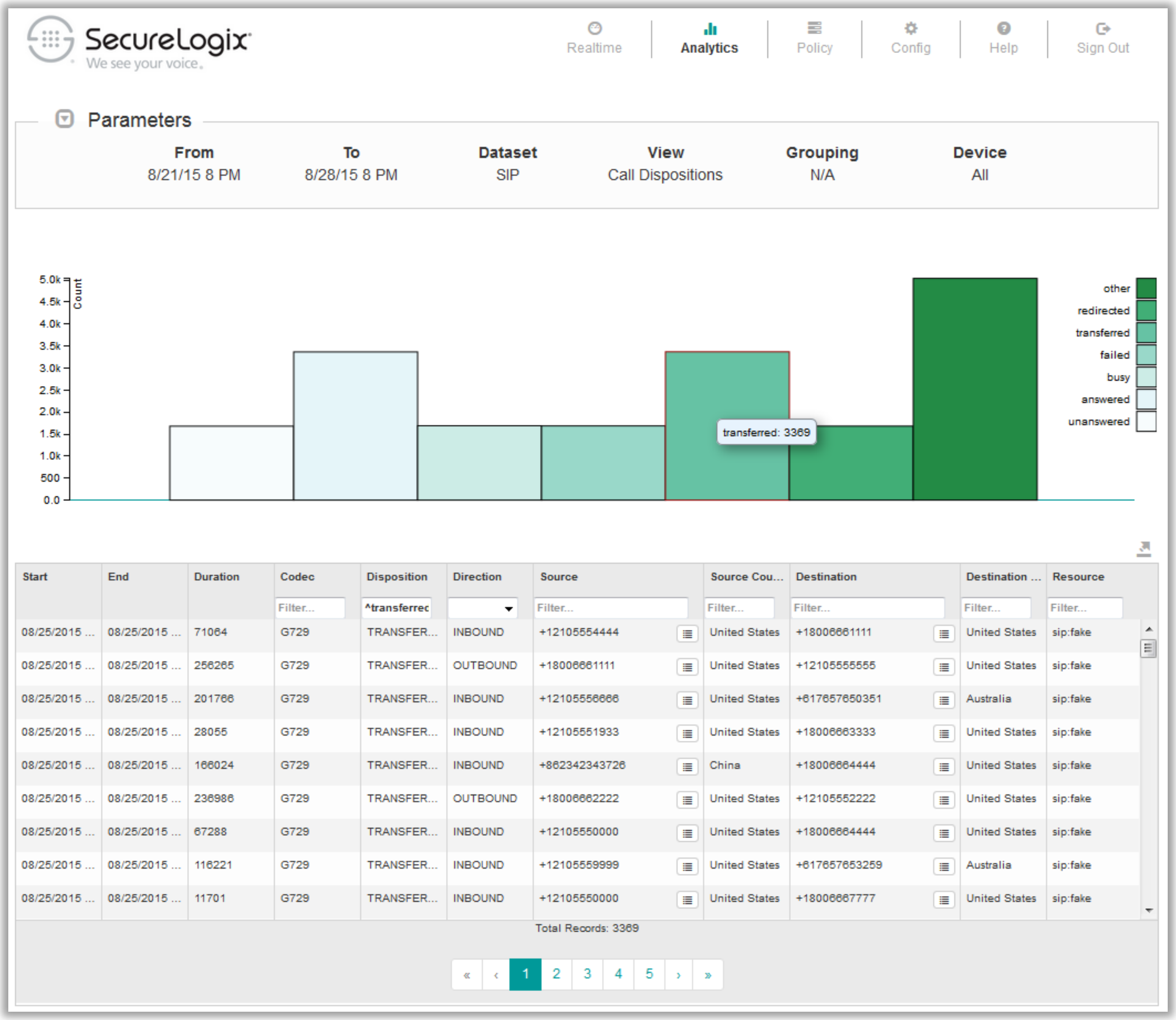
4. In the **View** field, click the down arrow and select the view for which you want to retrieve data:

   - **Average CPS**
   - **Total Calls**
   - **Call Dispositions**
   - **Top 10 Source**
   - **Top 10 Destination**
   - **Counts by Source Country**
   - **Counts by Destination Country**
   - **Concurrent Calls**

5. If you selected **Average CPS** or **Total Calls**, click the down arrow in the **Grouping** field and select the interval by which to group data: **Month**, **Day**, or **Hour**. All other views provide ungrouped data for the selected time range.

6. In the **Device** field, click the down arrow and select the Device for which to view data, or leave the default of **All**.

7. Click **Submit**. The data is retrieved and displayed in a graph. As with ENUM Call Detail Analytics, you can view a tooltip by hovering over the data in the graph, and clicking the display provides progressive drill-down until the call details appear in a table below the graph. The illustration below shows a **Call Dispositions** view.



From	To	Dataset	View	Grouping	Device
8/21/15 8 PM	8/28/15 8 PM	SIP	Call Dispositions	N/A	All

Start	End	Duration	Codec	Disposition	Direction	Source	Source Cou...	Destination	Destination ...	Resource
			Filter...	^transferrec		Filter...	Filter...	Filter...	Filter...	Filter...
08/25/2015 ...	08/25/2015 ...	71064	G729	TRANSFER...	INBOUND	+12105554444	United States	+18006661111	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	256265	G729	TRANSFER...	OUTBOUND	+18006661111	United States	+12105555555	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	201766	G729	TRANSFER...	INBOUND	+12105556666	United States	+617657650351	Australia	sip:fake
08/25/2015 ...	08/25/2015 ...	28055	G729	TRANSFER...	INBOUND	+12105551933	United States	+18006663333	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	166024	G729	TRANSFER...	INBOUND	+862342343726	China	+18006664444	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	236986	G729	TRANSFER...	OUTBOUND	+18006662222	United States	+12105552222	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	67288	G729	TRANSFER...	INBOUND	+12105550000	United States	+18006664444	United States	sip:fake
08/25/2015 ...	08/25/2015 ...	116221	G729	TRANSFER...	INBOUND	+12105559999	United States	+617657653259	Australia	sip:fake
08/25/2015 ...	08/25/2015 ...	11701	G729	TRANSFER...	INBOUND	+12105550000	United States	+18006667777	United States	sip:fake

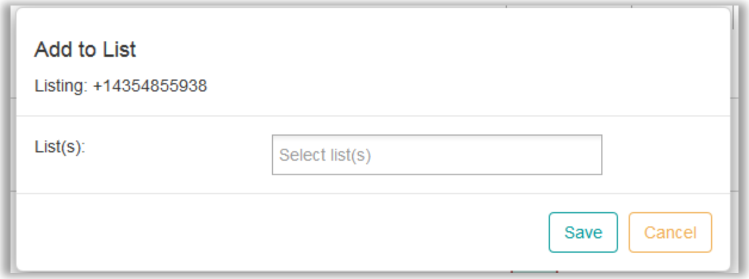
Total Records: 3369

8. You can filter the display by **Disposition**, **Direction**, **Source**, **Source Country**, **Destination**, **Destination Country**, and **Resource**. The filters are applied automatically as you type or select.

9. You can sort the fields by clicking the heading of the column you want to sort by.

10. To add a phone number directly to a Blacklist or Whitelist from this view, click the **Add to List** icon to the right of the phone number. ☰

11. The **Add to List** dialog box appears.

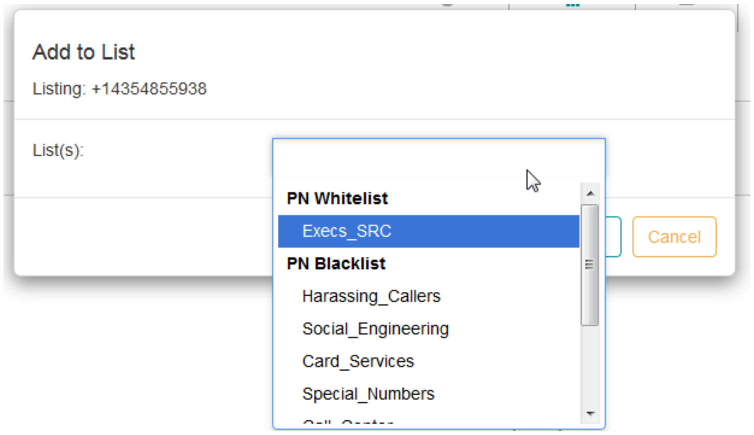


Add to List

Listing: +14354855938

List(s):

12. In the **List(s)** field, click the down arrow and click each List to which you want to add the selected number.



Add to List

Listing: +14354855938

List(s):

13. When you have added all applicable Lists, click **Save**. The phone number is added to the selected List(s).

    Note: To effect the change on the ENUM Server, you must reinstall the Policy that includes the List(s). The Policy is not automatically pushed.

SIP Phone Number Analytics

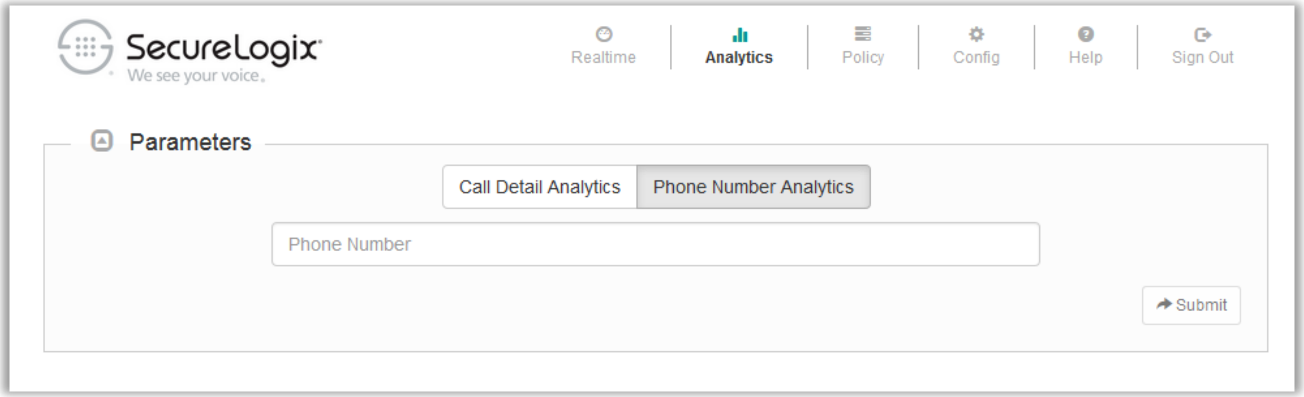
SIP Phone Number Analytics provides “drill up” analytics views for a specific phone number of interest, based on the SIP call data captured by the Metadata Probe.

To view SIP Phone Number Analytics

1. On the PolicyGuru main menu, click **Analytics**.

   The **Analytics** screen appears set to **Call Detail Analytics**, with **ENUM** selected as the dataset by default.

2. Click **Phone Number Analytics**. As mentioned, Phone Number Analytics always uses Metadata Probe data.

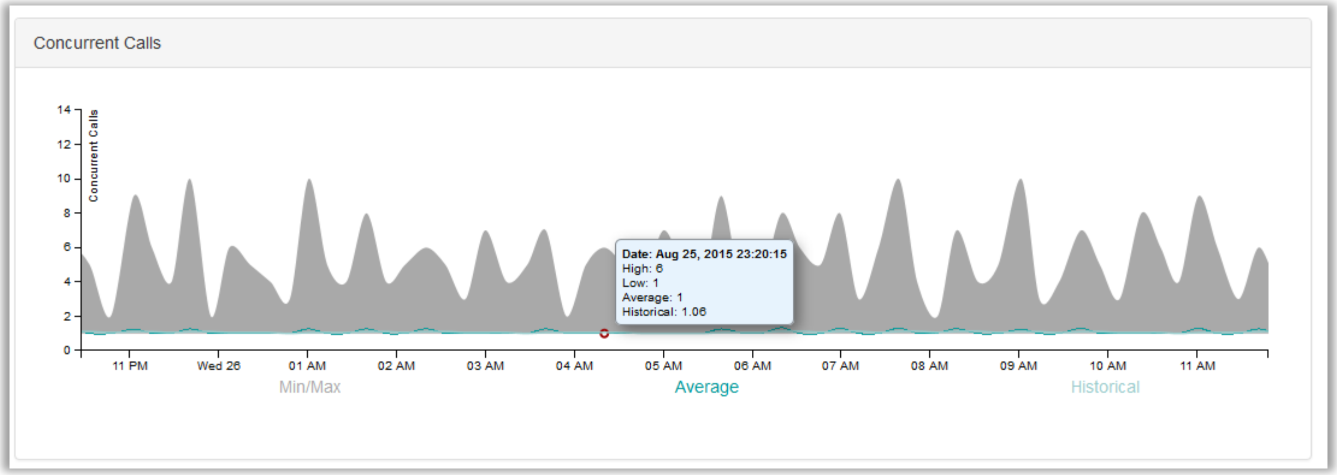


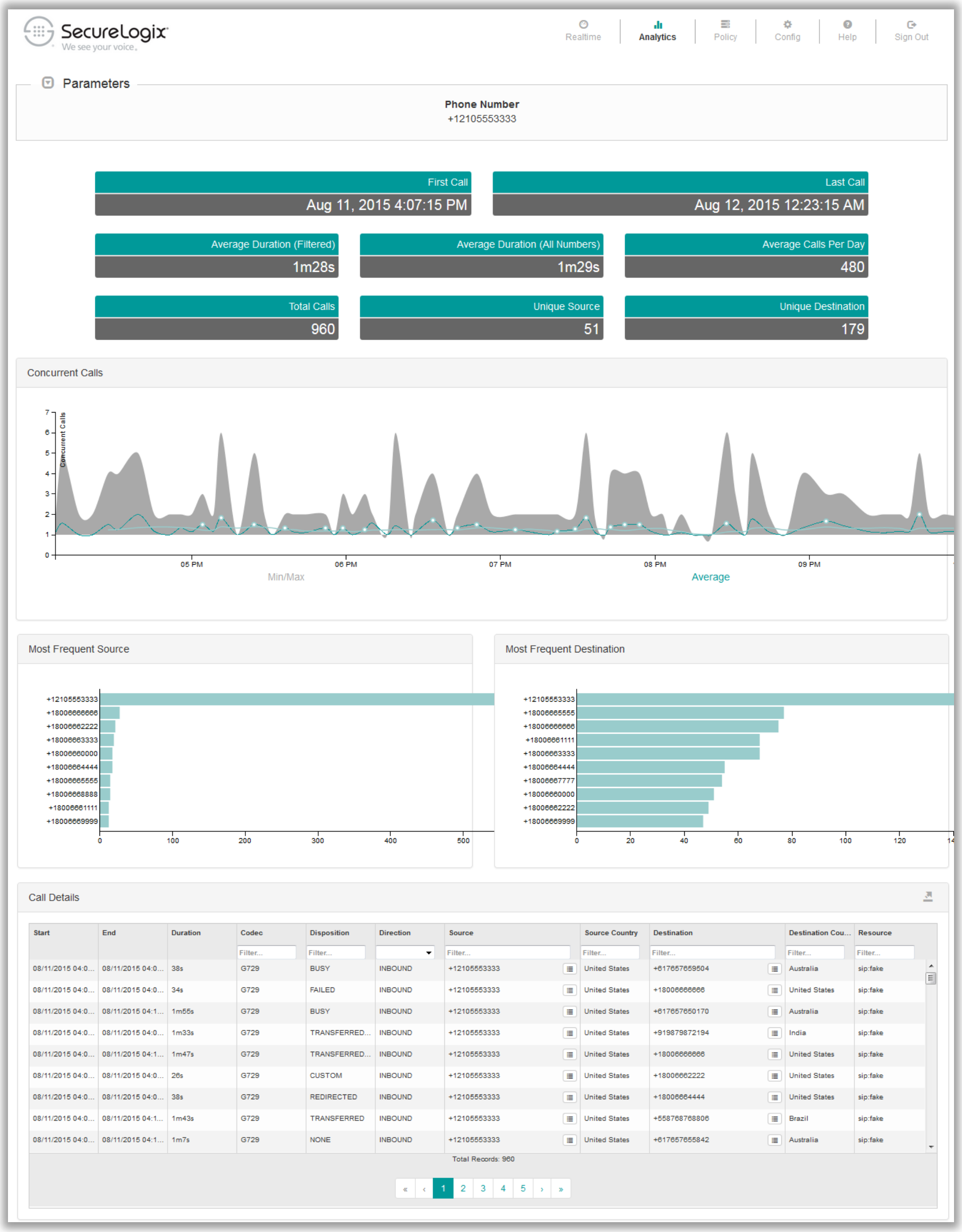
3. In the **Phone Number** box, type the phone number of interest. You can also type just a portion of a number, such as +1210, to retrieve all matching calls.
4. Click **Submit**. All data for the search string is retrieved and displayed in charts, graphs, and tables, as shown in the illustration on the next page.

   As with other views, you can sort and search the data table, export the view to a JSON file, and click the icon to add a number to a Whitelist or Blacklist.

   You can use the scroll wheel on a mouse to move and resize the **Concurrent Calls** graph.

   You can also hover your mouse over any point in the **Concurrent Calls** graph to get details about activity at that point, as shown below.





Parameters

Phone Number
+12105553333

First Call	Last Call
Aug 11, 2015 4:07:15 PM	Aug 12, 2015 12:23:15 AM

Average Duration (Filtered)	Average Duration (All Numbers)	Average Calls Per Day
1m28s	1m29s	480

Total Calls	Unique Source	Unique Destination
960	51	179

Concurrent Calls

Most Frequent Source

Most Frequent Destination

Call Details

Start	End	Duration	Codec	Disposition	Direction	Source	Source Country	Destination	Destination Cou...	Resource
			Filter...	Filter...		Filter...	Filter...	Filter...	Filter...	Filter...
08/11/2015 04:0...	08/11/2015 04:0...	38s	G729	BUSY	INBOUND	+12105553333	United States	+617657659504	Australia	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	34s	G729	FAILED	INBOUND	+12105553333	United States	+18006666666	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m55s	G729	BUSY	INBOUND	+12105553333	United States	+617657650170	Australia	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	1m33s	G729	TRANSFERRED...	INBOUND	+12105553333	United States	+919879872194	India	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m47s	G729	TRANSFERRED...	INBOUND	+12105553333	United States	+18006666666	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	26s	G729	CUSTOM	INBOUND	+12105553333	United States	+18006662222	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:0...	38s	G729	REDIRECTED	INBOUND	+12105553333	United States	+18006664444	United States	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m43s	G729	TRANSFERRED	INBOUND	+12105553333	United States	+558768768806	Brazil	sip:fake
08/11/2015 04:0...	08/11/2015 04:1...	1m7s	G729	NONE	INBOUND	+12105553333	United States	+617657655842	Australia	sip:fake

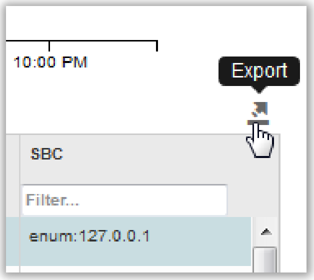
Total Records: 960

Exporting Analytics Data

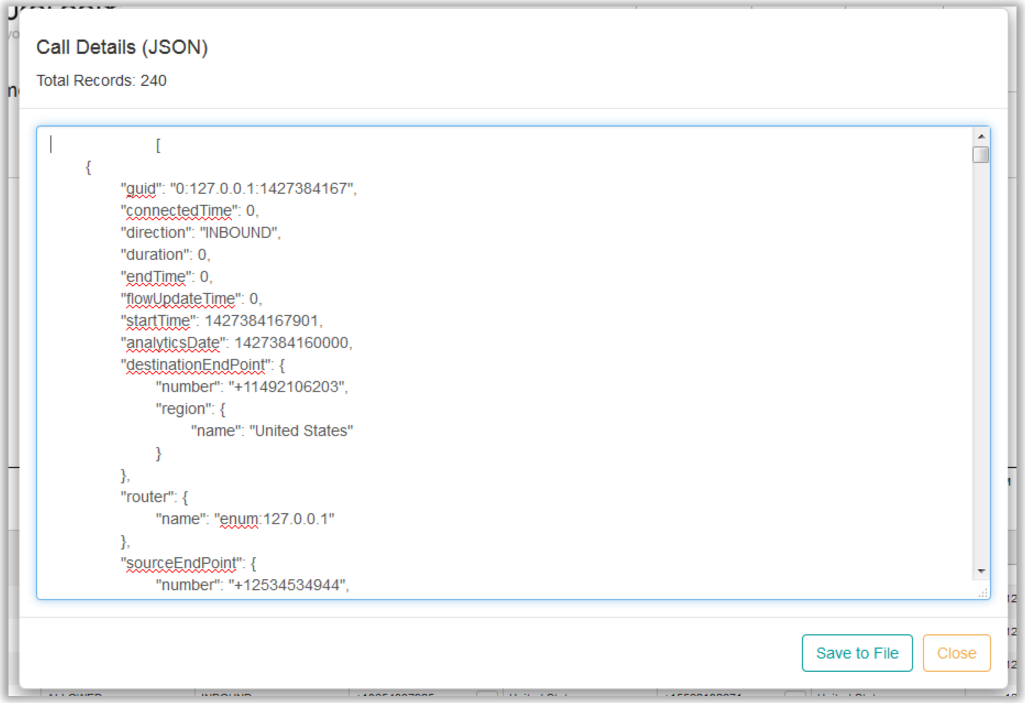
You can export Analytics data in JSON format for further offline analysis and reporting.

To export Analytics data

1. Above **Resource** on the **Call Detail** table, click the **Export** icon.



2. The **Call Details (JSON)** dialog box appears containing the data for the current page of records.


Call Details (JSON)

Total Records: 240

```
[
    {
        "guid": "0:127.0.0.1:1427384167",
        "connectedTime": 0,
        "direction": "INBOUND",
        "duration": 0,
        "endTime": 0,
        "flowUpdateTime": 0,
        "startTime": 1427384167901,
        "analyticsDate": 1427384160000,
        "destinationEndPoint": {
            "number": "+11492106203",
            "region": {
                "name": "United States"
            }
        },
        "router": {
            "name": "enum:127.0.0.1"
        },
        "sourceEndPoint": {
            "number": "+12534534944",
```

3. For a short number of results, you can simply copy the information out of the display, or for longer result sets, you can click **Save to File** to save it to a file.

System Configuration

General System Configuration

Use the procedures below to configure alerting, mid-call digit storage, and users and passwords, and to view/configure connected ENUM Servers and Metadata Probes.

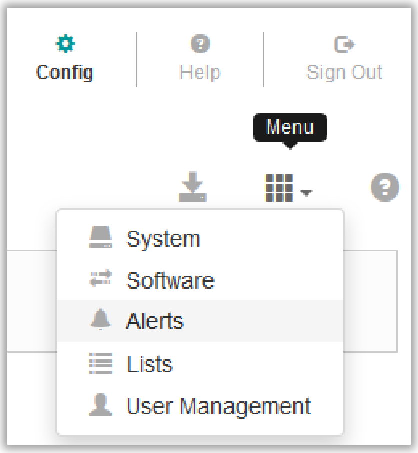
Alerting Configuration

The PolicyGuru System supports SNMP, Syslog, and Email alerting, in addition to the alert messages on the **Realtime** screen.

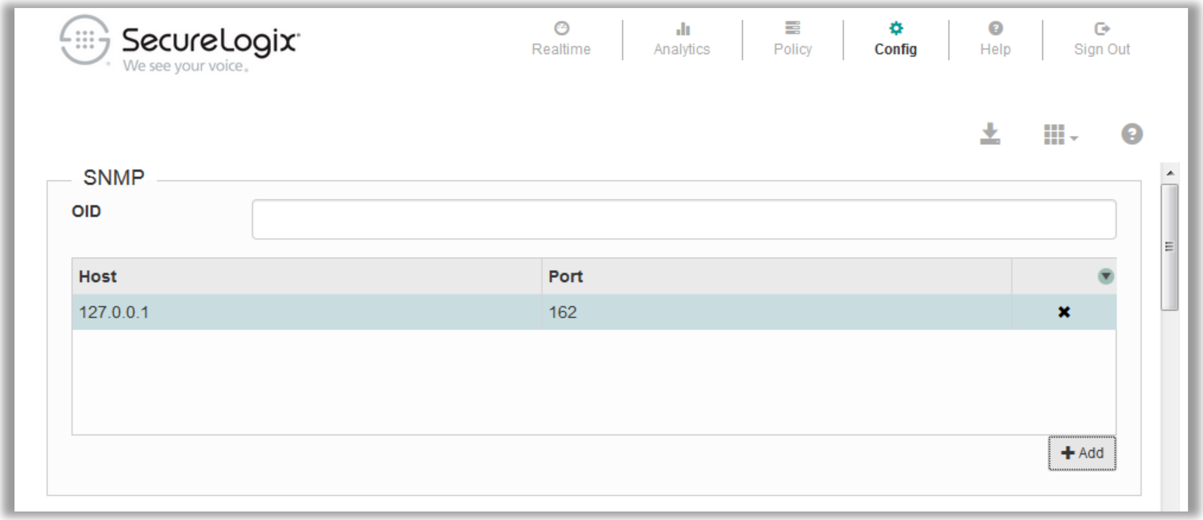
Configuring SNMP Alerts

To configure SNMP alerts

1. On the PolicyGuru main menu, click **Config**..
2. Click the **Show Configuration Menu** icon at the right.



3. In the drop-down list, click **Alerts**. The **Alerts** screen appears.



Host	Port	
127.0.0.1	162	✖

4. In the **SNMP** area, click **Add**.
5. A new row appears with placeholder values for **Host** and **Port**, as shown in the illustration above.
6. In the **OID** field, type the OID.
7. Double-click in the **Host** field to enable editing, and then type the IP address of the SNMP Agent host.
8. Double-click in the **Port** field to enable editing, and then type the port for the SNMP Agent.
9. Click the **Save** icon.

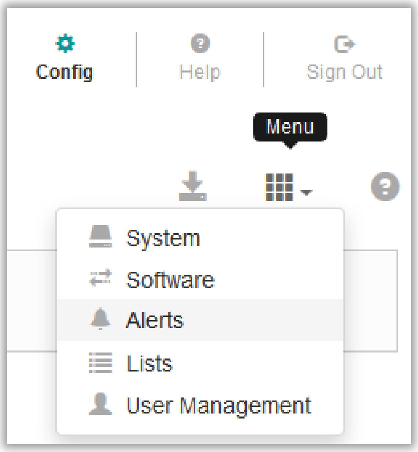
Configuring Email Notifications

Before email alerts can be generated, the **Reply-To** address and the list of email addresses to which alerts are to be sent must be specified. Additionally, the SMTP information for the email host must be specified. The procedure below explains adding the necessary email addresses. See “Specifying SMTP Information for Email Alerts” on page 95 for instructions.

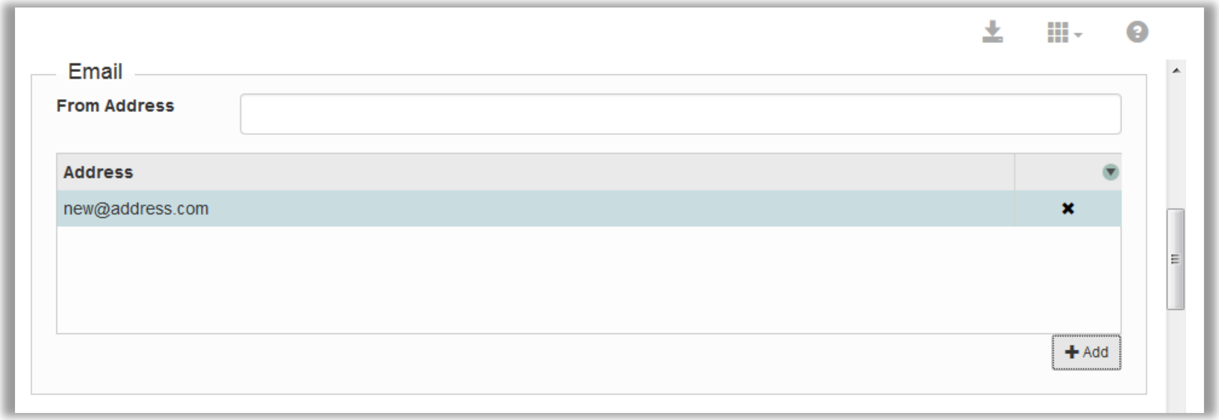
IMPORTANT: Do not configure email alerting settings in the GUI if no SMTP information has been configured in the server file, to avoid filling up the logs with errors related to an unavailable email server.

To configure Email alerts

1. On the PolicyGuru main menu, click **Config**.
2. Click the **Show Configuration Menu** icon at the right.



3. In the drop-down list, click **Alerts**. The **Alerts** screen appears.
4. In the **Email** area, click **Add**.



Address	
new@address.com	✖

5. A new row is added with a placeholder email address. Double-click the **Address** field and replace the placeholder with an email address to which email alerts are to be sent.
6. Repeat steps 1 and 2 for each email address that is to receive email alerts.
7. In the **From Address** field, type the email address that is to appear in the **From** field in PolicyGuru email alerts.
8. Click the **Save** icon.

Specifying SMTP Information for Email Alerts

To specify SMTP information

- On the Mediation Server, edit the following files:

Note: See the section above for information for supplying recipients and **Reply-to** address.

/opt/ngp/config/network/jboss-email-smtp-host

Supply the IP address of the email server.

/opt/ngp/config/network/jboss-email-smtp-port

Supply the port of the email server, if other than the default SMTP port 23.

/opt/ngp/config/network/jboss-email-smtp-user

Supply the username for the email server, if one is used.

/opt/ngp/config/network/jboss-email-smtp-password

Supply the password for the email server user, if one is used.

/opt/ngp/config/network/jboss-email-smtp-ssl

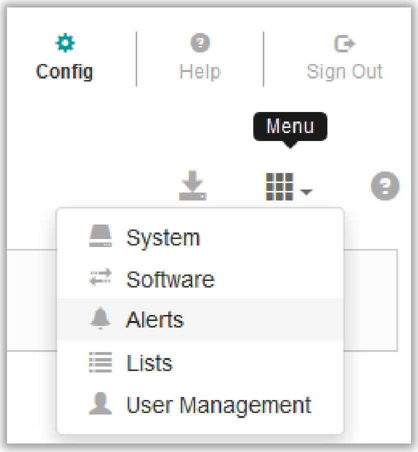
If SSL is not used, specify **false**. If it is used, specify **true**.

IMPORTANT: If the NGP service is running, you must restart it after specifying the SMTP information in the file.

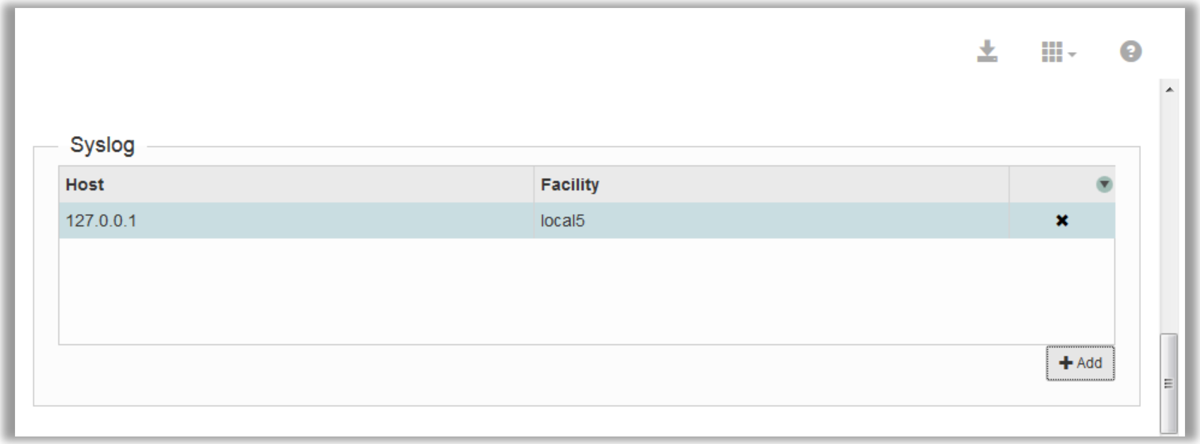
Configuring Syslog Alerts

To configure Syslog alerts

1. On the PolicyGuru main menu, click **Config**.
2. Click the **Show Configuration Menu** icon at the right.



3. In the drop-down list, click **Alerts**. The **Alerts** screen appears.



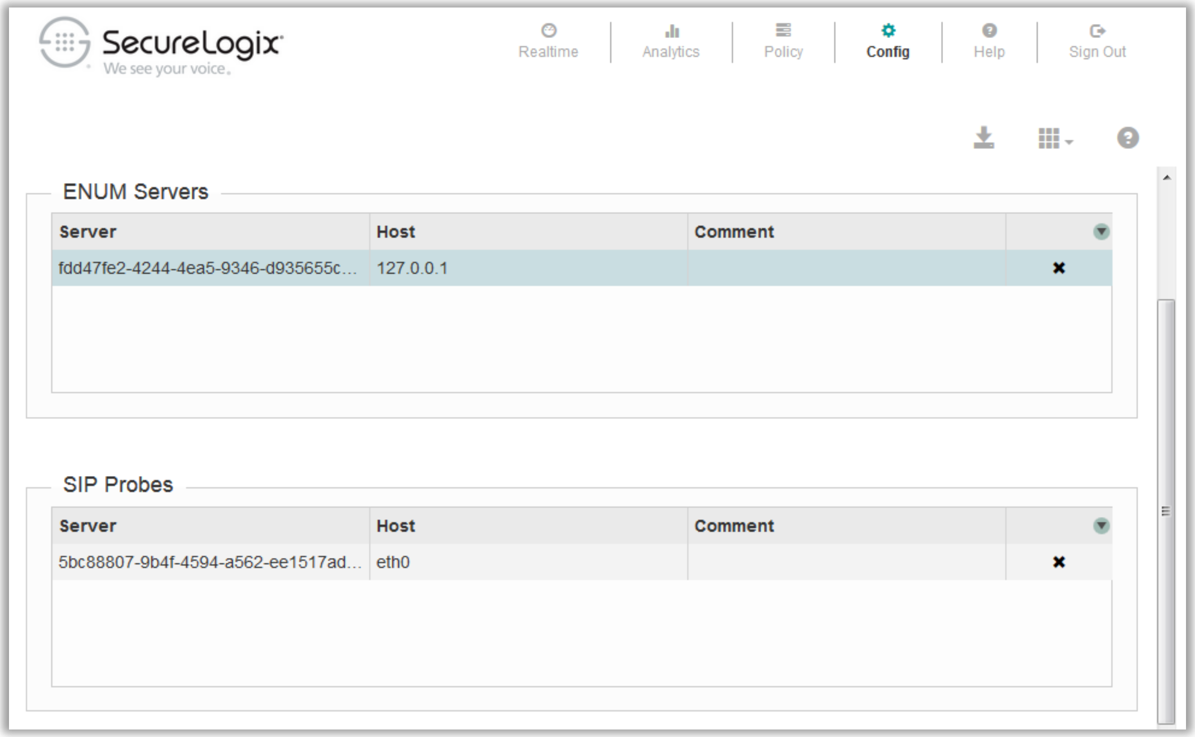
Host	Facility	
127.0.0.1	local5	✖

4. In the **Syslog** area, click **Add**. A new row is added with placeholder values, as shown in the illustration above.
5. Double-click the **Host** field and type the IP address of the Syslog host.
6. Double-click the **Facility** field, click the down arrow, and then select the facility keyword (that is, the facility code or value).
7. Click the **Save** icon.

Connected ENUM Server and Probe Configuration

To view the connected ENUM Servers and Metadata Probes

1. On the PolicyGuru main menu, click **Config**.
2. The **Config** tab appears showing the **System** screen. (Select **System** from the configuration menu if you were already on another screen of the **Config** tab.)



ENUM Servers

Server	Host	Comment	
fdd47fe2-4244-4ea5-9346-d935655c…	127.0.0.1		✖

SIP Probes

Server	Host	Comment	
5bc88807-9b4f-4594-a562-ee1517ad…	eth0		✖

Changing the Listener IP Addresses for ENUM Servers

To change the IP address on which an ENUM Server listens for ENUM requests

- On the **System** screen of the **Config** tab, double-click the **Host** field for the applicable device and type the new IP address. (It must already be configured on the device.)

Changing the Ethernet Port on Which Probes Monitor

To change the Ethernet port on which a Metadata Probe monitors for SIP messages

- On the **System** screen of the **Config** tab, double-click the **Host** field for the applicable device and type the Ethernet port. (It must already be configured on the device.)

Adding Identifying Comments to Connected ENUM Servers/Probes

To add a comment providing identifying information about the ENUM Servers/Probes

- On the **System** screen of the **Config** tab, double-click in the **Comment** field and type a comment.

User and Password Management

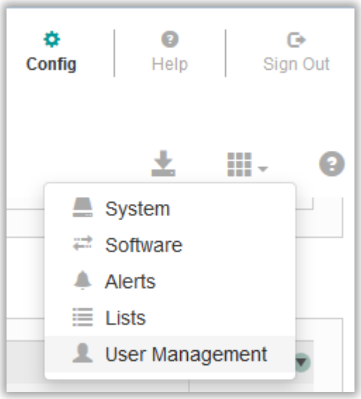
The sections below explain how to change the Management Interface **admin** password and provides information about using external LDAP authentication and group-based application permissions.

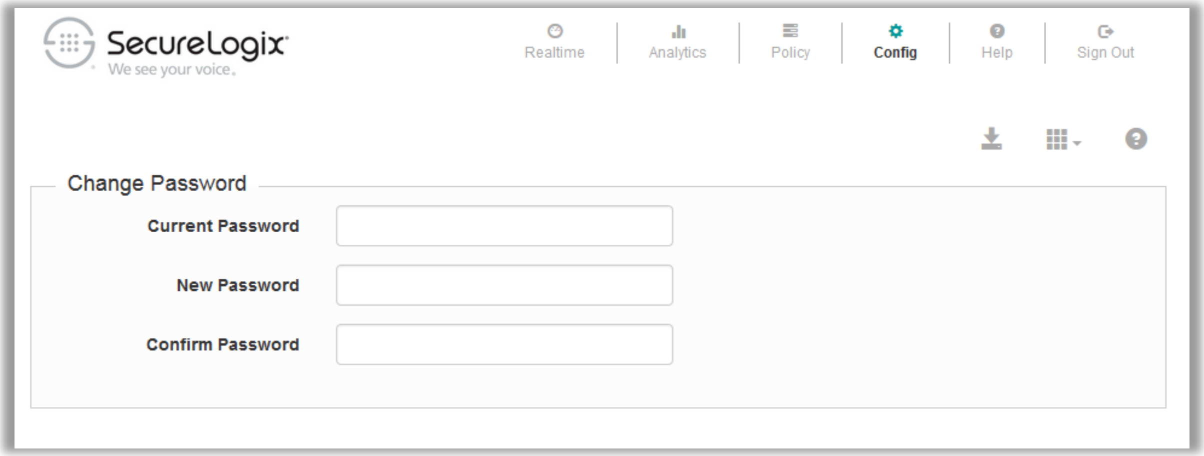
Changing the Management GUI Admin User Password

Note: The Management Interface provides a single user account, **admin**. You cannot add other users to the interface unless you use external LDAP for authentication. See " External LDAP Authentication and Group Permissions" on page 99 for information.

To change the Management GUI default admin user password

1. On the PolicyGuru main menu, click **Config**. The **Config** screen appears.
2. Click the **Show Configuration Menu** icon at the right and click **User Management**.





Change Password

Current Password

New Password

Confirm Password

3. In the **Current Password** box, type the current **admin** user password.

4. In the **Update Password** and **Confirm Password** boxes, type the new password. Use a unique password that meets complexity and length security standards for your organization.

External LDAP Authentication and Group Permissions

You can configure the PolicyGuru Solution to use external LDAP for authentication. External OpenLDAP and Active Directory servers are supported. When you enable external LDAP authentication, the default user account is disabled and cannot be used to log in to the system.

When external LDAP is used, application-level user permissions govern access the PolicyGuru applications. Users only see the PolicyGuru main menu icons for the web applications for which they are a member of an authorized LDAP group. This applies to the **Realtime**, **Analytics**, **Policy**, and **Config** applications.

See the *PolicyGuru® System Administration Guide* for detailed information about configuring the PolicyGuru Solution to use external LDAP authentication and group-based application permissions.

Appendices

Appendix A: List Import Scripts

createlist_file_2.1.sh

See “Static List Import” on page 50 for instructions for use.

```
#!/bin/bash

if test $# -lt 4
then
    echo ""
    echo "Usage: ./createlist_file_2.1.sh <server> <list name> <list type>
<list file> [batch size] [username] [password]"
    echo ""
    echo "where:"
    echo "      <server> is the IP address of the PolicyGuru Mediation
Server"
    echo "      <list name> is the name of the List to create on the
PolicyGuru system"
    echo "      <list type> is 0 for PN Whitelist, 1 for PN Blacklist, 2
for Regex Whitelist, or 3 for Regex Blacklist"
    echo "      <list file> is the name of the text file containing
listings (one listing per line)"
    echo "      [batch size] is the optional number of listings to submit
at a time.  If omitted, the batch size will default to 100."
    echo "      [username] is the optional username for PolicyGuru
application login.  If omitted, the user will be prompted for username
input."
    echo "      [password] is the optional password for PolicyGuru
application login.  If omitted, the user will be prompted for password
input."
    echo ""
    exit 1
fi

server=$1
listname=$2
listtype=$3
listfile=$4
batchsize=$5
username=$6
password=$7

if [ ! -f "$listfile" ]
then
    echo "Invalid file $listfile"
    exit 1
fi

if [ "$batchsize" == "" ]
then
    batchsize=100
fi

if [ "$username" == "" ]
then
    echo -n "Enter PolicyGuru Username: "
    read username
fi

if [ "$password" == "" ]
then
    echo -n "Enter PolicyGuru Password: "
    read -s password
    echo ""
fi

##response=$(curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H
"Content-Type: application/json" -d '{"userId":"admin",
"password":"SecureLogix1!"}'
https://$server:8443/mgmt/rest/security/login)
command="curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H \"Content-
Type: application/json\" -d '{\"userId\":\"$username\",
\"password\":\"$password\"}'
https://$server:8443/mgmt/rest/security/login"
response=$(eval $command)
if [ $(echo $response |awk -F'HTTPResponseCode' '{print $2}') != "200" ]
then
    echo "login failed, verify server, username, and password settings"
    exit 1
fi

token=$(echo $response | awk -F'"token":"' '{print $2}' | awk -F'"'
'{print $1}')

verify=$(curl -k -f -w %{http_code} -X GET -H "Access-Token: $token"
https://$server:8443/mgmt/rest/security/login)
if [ $verify != "200" ]
then
    echo "token verification failed"
    exit 1
fi

command="curl -k -f -X POST -H \"Access-Token: $token\" -H \"Content-Type:
application/json\" -d '{\"name\":\"$listname\", \"type\":\"$listtype\",
\"listings\":[]}' https://$server:8443/mgmt/rest/lists"
##echo "list create: $command"
eval $command
if test $? -ne 0
then
    echo "create list command failed, result=$?"
    echo "the list may already exist"
    exit 2
```

```
fi

sleep 1
#sleep 30

count=0
overall=0
while read -r listing
do
    #Add a leading backslash to any backslashes that exists in the read in
listing to allow proper curl operation with the MS
    listing=$(echo $listing | sed 's/\\/\\\\/g')

    if test $count -eq 0
    then
        command=
        listingstring="time curl -k -f -X PUT -H \"Access-Token: $token\"
-H \"Content-Type: application/json\" -d '{\"name\":\"$listname\",
\"addListings\":[{\"value\":\"$listing\"}"
    else
        listingstring=", {\"value\":\"$listing\"}"
    fi
    command=${command}${listingstring}
    count=$(($count + 1))
    overall=$(($overall + 1))
    if test $count -ge $batchsize
    then
        endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
        command=${command}${endcommand}
        #echo "final command: $command"
        count=0

        for ((j=0;j<3;j++))
        do
            eval $command
            commandresult=$?
            if test $commandresult -eq 0
            then
                break
            elif test $commandresult -eq 35
            then
                if test $j -eq 2
                then
                    echo "command=$command"
                    echo "commandresult=$commandresult"
                    exit 3
                fi
            else
                echo "command=$command"
                echo "commandresult=$commandresult"
                echo "verify there are no repeated values (including
repeated blank lines)"
                exit 4
            fi
            sleep 0.02
            #sleep 30
        done
        echo "$overall Listings Submitted"
    fi

    sleep 0.02
    #sleep 30

done < "$listfile"

if test $count -gt 0
then
    endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
    command=${command}${endcommand}
    #echo "final command: $command"

    for ((j=0;j<3;j++))
    do
        eval $command
        commandresult=$?
        if test $commandresult -eq 0
        then
            break
        elif test $commandresult -eq 35
        then
            if test $j -eq 2
            then
                echo "command=$command"
                echo "commandresult=$commandresult"
                exit 3
            fi
        else
            echo "command=$command"
            echo "commandresult=$commandresult"
            echo "verify there are no repeated values (including repeated
blank lines)"
            exit 4
        fi
        sleep 0.02
        #sleep 30
    done
    echo "$overall Listings Submitted"
fi
```

createlist_range_2.1.sh

See “Range List Import” on page 51 for instructions for use.

```
#!/bin/bash

if test $# -lt 6
then
    echo ""
    echo "Usage: ./createlist_range_2.1.sh <server> <list name> <list
type> <prefix> <value length> <count> [batch size] [username]
[password]"
    echo ""
    echo "where:"
    echo "      <server> is the IP address of the PolicyGuru Mediation
Server"
    echo "      <list name> is the name of the List to create on the
PolicyGuru system"
    echo "      <list type> is 0 for PN Whitelist, 1 for PN Blacklist,
2 for Regex Whitelist, or 3 for Regex Blacklist"
    echo "      <prefix> is a static string that starts every listing
(such as +1210)"
    echo "      <value length> is the size of the number of additional
characters that are appended to the prefix (such as 6 to append 6
characters to the prefix)"
    echo "      <count> is the total number of listings to create (such
as 5000 to create a list with 5000 listings)"
    echo "      [batch size] is the optional number of listings to
submit at a time.  If omitted, the batch size will default to 100."
    echo "      [username] is the optional username for PolicyGuru
application login.  If omitted, the user will be prompted for username
input."
    echo "      [password] is the optional password for PolicyGuru
application login.  If omitted, the user will be prompted for password
input."
    echo ""
    exit 1
fi

server=$1
listname=$2
listtype=$3
prefix=$4
valuelength=$5
count=$6
batchsize=$7
username=$8
password=$9

if [ "$batchsize" == "" ]
then
    batchsize=100
fi
```

```
if [ "$username" == "" ]
then
    echo -n "Enter PolicyGuru Username: "
    read username
fi

if [ "$password" == "" ]
then
    echo -n "Enter PolicyGuru Password: "
    read -s password
    echo ""
fi

command="curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H
\"Content-Type: application/json\" -d '{\"userId\":\"$username\",
\"password\":\"$password\"}'
https://$server:8443/mgmt/rest/security/login"
response=$(eval $command)
if [ $(echo $response |awk -F'HTTPResponseCode' '{print $2}') != "200"
]
then
    echo "login failed, verify server, username, and password settings"
    exit 1
fi

token=$(echo $response | awk -F'"token":"' '{print $2}' | awk -F'"'
'{print $1}')

verify=$(curl -k -f -w %{http_code} -X GET -H "Access-Token: $token"
https://$server:8443/mgmt/rest/security/login)
if [ $verify != "200" ]
then
    echo "token verification failed"
    exit 1
fi

command="curl -k -f -X POST -H \"Access-Token: $token\" -H \"Content-
Type: application/json\" -d '{\"name\":\"$listname\",
\"type\":\"$listtype\", \"listings\":[]}'
https://$server:8443/mgmt/rest/lists"
##echo "list create: $command"
eval $command
if test $? -ne 0
then
    echo "create list command failed, result=$?"
    exit 2
fi

sleep 1

for ((i=0;i<count;))
do
```

```
    command="curl -k -f -X PUT -H \"Access-Token: $token\" -H
\"Content-Type: application/json\" -d '{\"name\":\"$listname\",
\"addListings\":["
    ##echo "command start: $command"
    for ((j=0;j<$batchsize;j++))
    do
        if test $j -eq 0
        then
            listingstring="{\"value\":\"$prefix$(printf
%0${valuelength}d $i)\"}"
        else
            listingstring=", {\"value\":\"$prefix$(printf
%0${valuelength}d $i)\"}"
        fi
        command=${command}${listingstring}
        ##echo "current command: $command"
        i=$(($i + 1))
        if test $i -ge $count
        then
            break
        fi
    done
    endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
    command=${command}${endcommand}
    ##echo "final command: $command"

    for ((k=0;k<3;k++))
    do
        eval $command
        commandresult=$?
        if test $commandresult -eq 0
        then
            break
        elif test $commandresult -eq 35
        then
            if test $k -eq 2
            then
                echo "command=$command"
                echo "commandresult=$commandresult"
                exit 3
            fi
        else
            echo "command=$command"
            echo "commandresult=$commandresult"
            exit 4
        fi
        sleep 0.02
    done
    sleep 0.02

done
echo "$count Listings Submitted"
```

addtolist_file_2.1.sh

See “Importing Listings Into An Existing List” on page 52 for instructions for use.

```
#!/bin/bash

if test $# -lt 3
then
    echo ""
    echo "Usage: ./addtolist_file_2.1.sh <server> <list name> <list file>
[batch size] [username] [password]"
    echo ""
    echo "where:"
    echo "      <server> is the IP address of the PolicyGuru Mediation Server"
    echo "      <list name> is the name of the List to add listings to"
    echo "      <list file> is the name of the text file containing listings
(one listing per line)"
    echo "      [batch size] is the number of listings to submit at a time.  If
omitted, the batch size will default to 100."
    echo "      [username] is the optional username for PolicyGuru application
login.  If omitted, the user will be prompted for username input."
    echo "      [password] is the optional password for PolicyGuru application
login.  If omitted, the user will be prompted for password input."
    echo ""
    exit 1
fi

server=$1
listname=$2
listfile=$3
batchsize=$4
username=$5
password=$6


if [ ! -f "$listfile" ]
then
    echo "Invalid file $listfile"
    exit 1
fi

if [ "$batchsize" == "" ]
then
    batchsize=100
fi

if [ "$username" == "" ]
then
    echo -n "Enter PolicyGuru Username: "
    read username
fi
```

```
if [ "$password" == "" ]
then
    echo -n "Enter PolicyGuru Password: "
    read -s password
    echo ""
fi

##response=$(curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H "Content-
Type: application/json" -d '{"userId":"admin", "password":"SecureLogix1!"}'
https://$server:8443/mgmt/rest/security/login)
command="curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H \"Content-Type:
application/json\" -d '{\"userId\":\"$username\", \"password\":\"$password\"}'
https://$server:8443/mgmt/rest/security/login"
response=$(eval $command)
if [ $(echo $response |awk -F'HTTPResponseCode' '{print $2}') != "200" ]
then
    echo "login failed, verify server, username, and password settings"
    exit 1
fi

token=$(echo $response | awk -F'"token":"' '{print $2}' | awk -F'"' '{print
$1}')

verify=$(curl -k -f -w %{http_code} -X GET -H "Access-Token: $token"
https://$server:8443/mgmt/rest/security/login)
if [ $verify != "200" ]
then
    echo "token verification failed"
    exit 1
fi

sleep 1

count=0
overall=0
while read -r listing
do
    #Add a leading backslash to any backslashes that exists in the read in
listing to allow proper curl operation with the MS
    listing=$(echo $listing | sed 's/\\/\\\\/g')

    if test $count -eq 0
    then
        command=
        listingstring="curl -k -f -X PUT -H \"Access-Token: $token\" -H
\"Content-Type: application/json\" -d '{\"name\":\"$listname\",
\"addListings\":[{\"value\":\"$listing\"}"
    else
        listingstring=", {\"value\":\"$listing\"}"
    fi
    command=${command}${listingstring}
    count=$(($count + 1))
    overall=$(($overall + 1))
    if test $count -ge $batchsize
    then
        endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
        command=${command}${endcommand}
        #echo "final command: $command"
        count=0

        for ((j=0;j<3;j++))
        do
            eval $command
            commandresult=$?
            if test $commandresult -eq 0
            then
                break
            elif test $commandresult -eq 35
            then
                if test $j -eq 2
                then
                    echo "command=$command"
                    echo "commandresult=$commandresult"
                    exit 3
                fi
            else
                echo "command=$command"
                echo "commandresult=$commandresult"
                echo "verify that the list already exists and that there are no
repeated values in the file (including repeated blank lines)"
                exit 4
            fi
            sleep 1
        done
        echo "$overall Listings Submitted"

    fi
    sleep 1

done < "$listfile"

if test $count -gt 0
then
    endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
    command=${command}${endcommand}
    #echo "final command: $command"

    for ((j=0;j<3;j++))
    do
        eval $command
        commandresult=$?
        if test $commandresult -eq 0
        then
            break
        elif test $commandresult -eq 35
        then
            if test $j -eq 2
            then
                echo "command=$command"
                echo "commandresult=$commandresult"
                exit 3
            fi
        else
            echo "command=$command"
            echo "commandresult=$commandresult"
            echo "verify that the list already exists and that there are no
repeated values in the file(including repeated blank lines)"
            exit 4
        fi
        sleep 1
    done
    echo "$overall Listings Submitted"
fi
```

deletelist_2.1.sh

See “Delete List Script” on page 53 for instructions for use.

```
#!/bin/bash

if test $# -lt 2
then
    echo ""
    echo "Usage: ./deletelist_2.1.sh <server> <list name> [batch size]
[username] [password]"
    echo ""
    echo "where:"
    echo "      <server> is the IP address of the PolicyGuru Mediation Server"
    echo "      <list name> is the name of the List to delete from the system"
    echo "      [batch size] is the optional number of listings to delete at a
time.  If omitted, the batch size will default to 100."
    echo "      [username] is the optional username for PolicyGuru application
login.  If omitted, the user will be prompted for username input."
    echo "      [password] is the optional password for PolicyGuru application
login.  If omitted, the user will be prompted for password input."
    echo ""
    exit 1
fi

server=$1
listname=$2
batchsize=$3
username=$4
password=$5
pagesize=500

if [ "$batchsize" == "" ]
then
    batchsize=100
fi

if [ "$username" == "" ]
then
    echo -n "Enter PolicyGuru Username: "
    read username
fi

if [ "$password" == "" ]
then
    echo -n "Enter PolicyGuru Password: "
    read -s password
    echo ""
fi
```

```
##response=$(curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H "Content-
Type: application/json" -d '{"userId":"admin", "password":"SecureLogix1!"}'
https://$server:8443/mgmt/rest/security/login)
command="curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H \"Content-Type:
application/json\" -d '{\"userId\":\"$username\", \"password\":\"$password\"}'
https://$server:8443/mgmt/rest/security/login"
response=$(eval $command)
if [ $(echo $response |awk -F'HTTPResponseCode' '{print $2}') != "200" ]
then
    echo "login failed, verify server, username, and password settings"
    exit 1
fi

token=$(echo $response | awk -F'"token":"' '{print $2}' | awk -F'"' '{print
$1}')

verify=$(curl -k -f -w %{http_code} -X GET -H "Access-Token: $token"
https://$server:8443/mgmt/rest/security/login)
if [ $verify != "200" ]
then
    echo "token verification failed"
    exit 1
fi

sleep 1

pagesleft=true
pagenumber=1
while [ "$pagesleft" == "true" ]
do
    result=$(curl -k -f -w HTTPResponseCode%{http_code} -X GET -H "Access-
Token: $token"
https://$server:8443/mgmt/rest/lists/$listname?pageNumber=$pagenumber\&pageSize
=$pagesize > .$listname.$pagenumber)
    if [ $(echo $response |awk -F'HTTPResponseCode' '{print $2}') != "200" ]
    then
        echo "failed to get list:$listname, page:$pagenumber, size:$pagesize"
        exit 2
    fi
    if [ "$(cat .$listname.$pagenumber | grep "listings\":\[\]" | awk -
F'HTTPResponseCode' '{print $2}')" == "200" ]
    then
        pagesleft=false
    else
        ((pagenumber++))
    fi
done

touch .$listname.id
touch .$listname.number
for ((i=1;i<pagenumber;i++))
do
```

```
    cat .$listname.$i | awk -F']}HTTPResponseCode200' '{print $1}' | awk -F'['
'{print $2}' |sed 's/},{/}\n{/g' > .$listname.id.$i
    cat .$listname.id .$listname.id.$i > .$listname.id.temp
    mv .$listname.id.temp .$listname.id
    while read id
    do
        echo "$id" | awk -F'"value":"' '{print $2}' | awk -F'"}' '{print $1}'
>> .$listname.number.$i
    done < .$listname.id.$i
    cat .$listname.number .$listname.number.$i > .$listname.number.temp
    mv .$listname.number.temp .$listname.number
done

count=0
overall=0
while read id
do
    #Add a leading backslash to any backslashes that exists in the read in id
to allow proper curl operation with the MS
    id=$(echo $id | sed 's/\\/\\\\/g')

    if test $count -eq 0
    then
        command=
        idstring="curl -k -f -X PUT -H \"Access-Token: $token\" -H \"Content-
Type: application/json\" -d '{\"name\":\"$listname\", \"removeListings\":[$id"
    else
        idstring=", $id"
    fi
    command=${command}${idstring}
    count=$(($count + 1))
    overall=$(($overall + 1))
    if test $count -ge $batchsize
    then
        endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
        command=${command}${endcommand}
        #echo "final command: $command"
        count=0

        for ((j=0;j<3;j++))
        do
            eval $command
            commandresult=$?
            if test $commandresult -eq 0
            then
                break
            elif test $commandresult -eq 35
            then
                if test $j -eq 2
                then
                    echo "command=$command"
                    echo "commandresult=$commandresult"
                    exit 3
                fi
            else
                echo "command=$command"
                echo "commandresult=$commandresult"
                exit 4
            fi
            sleep 1
        done
        echo "$overall Listings Deleted"
    fi

    sleep 1

done < ".$listname.id"

if test $count -gt 0
then
    endcommand="]}' https://$server:8443/mgmt/rest/lists/$listname"
    command=${command}${endcommand}
    #echo "final command: $command"

    for ((j=0;j<3;j++))
    do
        eval $command
        commandresult=$?
        if test $commandresult -eq 0
        then
            break
        elif test $commandresult -eq 35
        then
            if test $j -eq 2
            then
                echo "command=$command"
                echo "commandresult=$commandresult"
                exit 3
            fi
        else
            echo "command=$command"
            echo "commandresult=$commandresult"
            exit 4
        fi
        sleep 1
    done
fi
echo "$overall Listings Deleted"
#delete the group itself
response=$(curl -k -f -w HTTPResponseCode%{http_code} -X DELETE -H "Access-
Token: $token" https://$server:8443/mgmt/rest/lists/$listname)
responsecode=$(echo $response |awk -F'HTTPResponseCode' '{print $2}')
if [ "$responsecode" != "200" ]
then
```

```
    echo "failed to delete list:$listname, response code:$responsecode"
    if [ "$responsecode" == "405" ]
    then
        echo "The list must be removed from SEP Policy before it can be
deleted.  Note that the Listings are already deleted."
    fi
    exit 5
fi
echo "List $listname Deleted"
rm -f .$listname.*
```

Appendix B: Querying System Events via REST API

System events can be queried via the REST API from a command line on the Mediation Server. You can query by count or by date and time range.

To query system events using REST

1. Log in to the Mediation Server via a command-line interface.
2. Log in via the webserver IP to get a token:

```
curl -k -f -w HTTPResponseCode%{http_code} -X PUT -H "Content-Type:
application/json" -d '{"userId":"<username>", "password":"<password>"}'
https://<webserver_IP>:8443/mgmt/rest/security/login
```

3. Execute one of the following queries, using the token you received in response the above command.

- **By count:**

```
curl -k -f -X GET -H "Access-Token: <token_from_login>"
https://172.20.25.84:8443/mgmt/rest/sysevents?count=2
```

Example:

```
curl -k -f -X GET -H "Access-Token:
eyJhbGciOiJIUzI1NiJ9.eyJleHAiOjE0MzAzNDI0MzIsInBlcm1zIjp7InJlYWx0aW1lIjp0c
nVlLCJhbmFseXRpY3MiOnRydWUsImNvbmZpZyI6dHJ1ZSwicG9saWN5Ijp0cnVlfSwiaXNzIjo
iUG9saWN5R1VSVSIsIm9yaWciOjE0NjQxNTgxMzcsImlhdCI6MTQzMDI1NjAzMiwidXNlciI6I
mFkbWluIn0.mzHsafiPvy2kJoYxWb8sRIsEf6Td2ffBF611T1GhU8A"}
https://172.20.25.84:8443/mgmt/rest/sysevents?count=30
```

- **By date/time:**

```
curl -k -f -X GET -H "Access-Token: <token_from_login>"
https://172.20.25.84/mgmt/rest/sysevents?fromDate=1430246820000\&toDate=14
30246880000
```

The date/time range values are expressed in epoch time. A web-based epoch time converter is available at the following link: http://www.epochconverter.com/

Example:

```
curl -k -f -X GET -H "Access-Token:
eyJhbGciOiJIUzI1NiJ9.eyJleHAiOjE0MzAzNDI0MzIsInBlcm1zIjp7InJlYWx0aW1lIjp0c
nVlLCJhbmFseXRpY3MiOnRydWUsImNvbmZpZyI6dHJ1ZSwicG9saWN5Ijp0cnVlfSwiaXNzIjo
iUG9saWN5R1VSVSIsIm9yaWciOjE0NjQxNTgxMzcsImlhdCI6MTQzMDI1NjAzMiwidXNlciI6I
mFkbWluIn0.mzHsafiPvy2kJoYxWb8sRIsEf6Td2ffBF611T1GhU8A"
https://172.20.25.84/mgmt/rest/sysevents?fromDate=1430246820000\&toDate=14
30246880000
```

Appendix C: Understanding Regular Expressions in Rules

Overview

When the SBC receives a new SIP INVITE request (i.e., call) it extracts the source (i.e., caller) and destination (i.e., callee) information and formats an ENUM Request, which it transmits to its configured PolicyGuru ENUM Server. The PolicyGuru ENUM Server decides whether to ALLOW, TERMINATE, or REDIRECT the call represented by the ENUM Request. The decision is in the form of a POSIX-style regular expression which is returned to the SBC in the ENUM Reply. See “Substitution Expression Grammar” on page 118 for syntax details. The SBC applies the regular expression to the SIP INVITE’s Request-URI. The output of the application of the regular expression to the Request-URI is the call’s new Request-URI. The regular expression supplied for an ALLOW decision should result in an unaltered Request-URI (i.e., route the call to its original destination). The application of the regular expression for the TERMINATE or REDIRECT decision should produce a different destination.

The ENUM Server decides how to direct the call by applying the installed SEP Policy Rules to the data supplied in the ENUM Request. If the call does not match any SEP Policy Rules, the ENUM Server defaults to an ALLOW call action. In this default case, the regular expression is a matter of configuration. The same configured default regular expression is returned for all calls that default to ALLOW. Otherwise, the regular expression is supplied in the SEP Policy Rule that best matches the call—which could specify an ALLOW, REDIRECT, or TERMINATE decision.

An ENUM Reply includes an **Answer** section when the ENUM Request has been processed successfully. An **Answer** section is <u>not</u> included in the ENUM Reply that reports a Format Error or a Server Error. For a successful ENUM Request, the **Answer** section of the ENUM Reply contains exactly one **ANSWER-RR**. The content of the **ANSWER-RR** includes the POSIX-style regular expression.

The regular expression is a delimited string in two parts: The first part is the regular expression itself, referred to as the “ere” part. The second part is the replacement string. The purpose of the first part is to perform pattern matching on the input string. When a match occurs, one or more characters in the replacement string are substituted for characters in the input string to produce an output string. Together, the two parts are collectively referred to as the "regular expression" field.

The "regular expression" field begins and ends with an exclamation point character "!" and the two parts of the "regular expression" are also delimited by an exclamation point.

Two "regular expression" examples follow:

```
!a^!guaranteed no replacement!
```

This is a "regular expression" field that could be returned to an SBC when SEP Policy dictates that the call be permitted to flow unaltered to its original destination (an ALLOW decision). The regular expression **a^** guarantees no matches when applied to a Request-URI. No matches means that nothing in the replacement string (i.e. 'guaranteed no replacement') is substituted for characters in the Request-URI. When a regular expression matches no characters in the input string, the output string is identical to the input string. A replacement string is still required, however, so the text “guaranteed no replacement” is simply a commentary or place holder in this instance.

```
!^.*$!sip:8888888@10.1.50.18!
```

In this "regular expression", the ere part **^.*$** means to replace the input string entirely with the provided replacement string (i.e., sip:8888888@10.1.50.18). This is an example of a regex the PolicyGuru ENUM Server might provide for a TERMINATE or REDIRECT decision.

IMPORTANT: See “Important Information About Regex in the **Guided Rule Editor**” on page 63 for information on required special character replacement when using Regex in SEP Rules.

IMPORTANT: The **$** character must be escaped (i.e., preceded by a \ character) when entering the regular expression into the ENUM Server's default config script (**createDefaultConfig.sh**); otherwise, the ***$** characters get dropped from the regular expression as the script creates the sqlite3 configuration database where it stores local configuration data.

Note: The "regular expression" field in an **ANSWER-RR** is followed by a replacement field. The "regular expression" field and the replacement field are mutually exclusive. If the "regular expression" field is populated, the replacement field is empty. The PolicyGuru Solution uses the regex field and leaves the replacement field empty.

Substitution Expression Grammar

The content of the regex field is a substitution expression. While various standards for regular expression syntax exist, the regular expression in the ENUM reply must be a "POSIX Extended Regular Expression" (see RFC 2915, Section 3). True sed(1) and Perl style substitution expressions are not appropriate for use in this application for a variety of reasons stemming from internationalization requirements and backref limitations; therefore; the contents of the regex field MUST follow the grammar below:

```
subst_expr   = delim-char  ere  delim-char  repl  delim-char  *flags

delim-char   = "/" / "!" / ... <Any non-digit or non-flag character

               other than backslash '\'. All occurances of a delim_char

               in a subst_expr must be the same character.>

ere          = POSIX Extended Regular Expression

repl         = 1 * ( OCTET /  backref )

backref      = "\" 1POS_DIGIT

flags        = "i"

POS_DIGIT    = %x31-39                  ; 0 is not an allowed backref
```

The definition of a POSIX Extended Regular Expression can be found in [8], section 2.8.4 of the following standard::

[8] IEEE, "IEEE Standard for Information Technology - Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities (Vol. 1)", IEEE Std 1003.2-1992, January 1993.

The link below is a website with a regular expression tester that permits a checkbox to be set to assure the ere part complies with POSIX ERE (egrep) syntax and leftmost-longest match semantics. If you test a regular expression that has an ere part that does not comply with POSIX, an error is flagged.

http://www.regexplanet.com/advanced/golang/index.html