PolicyGuru® Meta-Policy Controller v2.1.1 Release Notes

Knowledge Base Article #PG753 Rev B

Synopsis

This document contains important information about PolicyGuru® Meta-Policy Controller Release v2.1.1.

What's New in v2.1.1

- **SIP Content-Length and Call-ID Header for DTMF**—In v2.1, DTMF processing expected the **Content-Length** header and **Call-ID** header to be present in all SIP messages. The **Content-Length** header is not required in all messages, and the **Call-ID** header could be absent due to scenarios such as fragmentation. If one of these headers was not present, the SIP message became "stuck" in the DTMF processing code in the Metadata Probe, and null pointer exceptions were created as the message repeatedly failed to be processed. The message needed to be manually removed from the queue or the **HornetQ** data directory purged to eliminate the message from the system. Fixes have been added that allow DTMF processing to properly handle messages without **Content-Length** or **Call-ID** header.
- **Ability to Disable DTMF Persistence**—DTMF persistence to the Database could not be disabled in v2.1. A new flag has been added to a file named **standalone.conf** that allows DTMF persistence to be disabled if desired.
- **Performance Improvements**—Multiple KIE/Drools engines are used to process CEP Policy, IPS Policy, Orchestration Policy, and SIP Flow Factory. It was discovered that events were not being distributed evenly between those engines, causing some engines to be overloaded and others to be idle. Distribution algorithms were improved to ensure even distribution and best possible performance.

Issues Resolved in v2.1.1

- **NGP-252**—SEP Policy commit failed with error: "Entity revision has to be greater than 0." The revision number associated with SEP policy objects is incremented whenever SIP messages or DTMF digits are persisted to the Database. If this number grows too large, it is treated as a negative number, and SEP Policy push will fail. At that point, a manual process must be carried out to reset the policy version back to a "low" number. This fix prevents the revision number from incrementing when SIP/DTMF is persisted.
- **NGP-253**—List names containing certain special characters could be created, but after creation, the Lists could not be edited or deleted. The problematic characters are **/ \ . # % ? ;** These characters are now prohibited from use in List names along with whitespace, parenthesis, and double quotes. This fix prevents lists from being created using those special characters. The save action fails and the following error message is presented if the specified characters are used in a List name: Group name cannot contain whitespace or the following: / \ ( ) . # % ? ; "
- **NGP-254**—KIE Drools Bridge functions within KIE policy default to TLSv1 SSL protocol even though the system may be using TLSv1.1 or TLSv1.2. This prevents those functions from working to carry out operations within policy such as List lookups, Event Logging, SEP Policy Commit, etc. This fix allows proper operation when the system encryption protocol is set to TLSv1.1 or TLSv1.2.
- **NGP-255—**IPS Rule Counter Criteria changes sometimes did not take effect as part of the **Build and**

Deploy process. If IPS rules were active and the system was actively processing calls and incrementing the associated counters and then a change was made to the IPS rule counter criteria and a **Build and Deploy** was executed, the associated counter criteria changes would not take effect. Instead, the previously existing counter criteria would continue to be enforced. A restart of the **ngp** service on the Mediation Server would cause the new criteria to be read in and used. This problem did not seem to occur if calls incrementing the associated counters were not actively occurring when the **Build and Deploy** was performed. The fix in v2.1.1 causes the new counter criteria to be read in on **Build and Deploy** regardless of whether counters are actively being used.

Known Issues in This Release

- **NGP-207**—SIP Analytics limitation. Queries to gather SIP Analytics CDR data are limited to hour boundaries. In other words, if a call starts in one hour, but is connected or ended in a different hour, that connect and/or end information will not be available in the CDR information in SIP Analytics. This issue affects only the Total Calls and Average CPS views when you drill down to hourly CDR information, and calls are present which connect or end in a later hour. This is due to the fact that those views create the CDR display based on the given hour that you drilled into. Connect and/or end information that occurs in other hours will not be pulled in by the query over that hour.

  To work around this issue and gather full CDR info, use the Phone Number Analytics view or other Call Detail views (Call Disposition, Top 10 Source/Dest, Source/Dest by Country, Concurrent Calls) because these queries do not use a predefined query time range. These views base their query on the user-specified date/time range. When using these views, ensure that your specified query date/time range encompasses the duration of the call to retrieve all parts of the call. For instance, if a particular call lasted two hours, the user-specified query range must include that entire two-hour range to include the End Time information.
- **NGP-206**—ENUM/ Analytics data mismatches at hour boundaries. Mismatches sometimes occur between the ENUM Analytics view counts and the associated CDR record counts, and a query for one specific hour may also show some graphed results for the next hour.
- **NGP-205**—Source/Dest country selection filter limitation in Analytics. Country filters for CDR data may return data for more than just the selected country if the search term is present in more than one country name.
- **NGP-174**—Rules with matching names except for case not displayed in Project View. In the Policy Rules editor, if there are multiple rules with matching names except for case, only one of the rules will be displayed. All rules can be viewed by using Repository View.
- **NGP-164**—List creation with initial listings creates duplicates in SEP policy on the ENUM Server. If listings are added to a list during the initial creation of that list, a duplicate value will be created in SEP policy on the ENUM server. The presence of the extra value in policy is non-service affecting.
- **NGP-246**— Various instances in which the Metadata Probe does not receive all SIP messaging for calls result in the **SipFlowFactory** rules engine waiting for long periods of time holding calls in memory in hope that the expected messages will eventually arrive, which can impair system performance.

Last Update: 9/7/2017

SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232 • (210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • http://support.securelogix.com