



PolicyGuru® Meta-Policy Controller v2.1 Release Notes

Knowledge Base Article #PG476

Synopsis

This document contains important information about Release v2.1 of PolicyGuru® Meta-Policy Controller.

What's New in v2.1

- **New IPS Rule Functionality**—This release includes new IPS functionality for specific scenarios.
- **New CEP Rule Functionality**—New CEP Rule functionality is provided. You can now track and alert on calls for which a specified DTMF digit count is reached within a specified time interval in low-volume calling environment up to 10 CPS. You can also now create CEP Rules to automatically add phone numbers to Lists used in Rules in the SEP Policy and then automatically reinstall the SEP Policy when a configurable count of numbers has been added or after a configurable time interval.
- **Ability to import entries into an existing whitelist or blacklist**—Previously, new lists could be imported but updating an existing list via import was not supported. Import into an existing list is now supported.
- **Customer's CA-signed certificate support**—The ability to import and use a customer's CA-signed certificate has been verified in this release.
- **Configurable database purging**—You can now schedule regular database purging to maintain the size of the database to the number of months of data you want to maintain. SecureLogix supports retaining no more than 13 months of data in the working database.
- **Policy processing improvements**—This release includes background Rule processing performance improvements.
- **Stability and performance improvements**—A number of updates have been made to improve system stability and performance, including improved monitoring of system components to better detect potential connectivity issues and tuning of intra-application communication mechanisms for optimal performance.
- **Improved logging support**—Additional tools and utilities are included for improved file browsing and management, including facilitating finding important troubleshooting information in large logs. Additionally, the ability to auto-purge log files older than a user-configurable time to free up disk space has been added.
- **Deployability improvements**—Installer improvements have been made to reduce manual host system configuration and additional console tools are available to simplify editing of server-side configuration files.,

Issues Resolved in v2.1

- **NGP-212**—While downloading large SEP policy updates or resyncs (listing counts in the hundreds of thousands or greater) to ENUM servers, connection timeouts would occur after 60 seconds and policy commit would fail.
- **NGP-213**— If power loss occurred on a PolicyGuru system during **ngp** service start or stop, temp files may have be left in the **/var/tmp** folder that would prevent normal **ngp** service startup after the system started back up. Manual actions were required to clear the files in **/var/tmp** in that scenario.



- **NGP-218**—The **SipFlowFactory** rules engine intermittently failed to set the call disposition of transferred calls to **TRANSFERRED** depending on the timing of the SIP messages and the order in which rules are evaluated within the rules engine.
- **NGP-221**— CEP Rules that access the database in the **WHEN** portion of the rule will do so on fact insertion into the rules engine, even if the rule is "disabled" by the **date-effective** clause. This can degrade CEP engine performance (and to some degree system performance) in instances where a large network latency exists between the Mediation Server and Database.
- **NGP-222**—An empty media description in a SIP message can lead to a null pointer exception that renders the **SipFlowFactory** rules engine inoperable.
- **NGP-224**— The Metadata Probe supports Initial Fragment processing. Since initial Fragments may not include all of the expected SIP headers, additional error checking was added to the rules engine that performs SIP to Flow processing on the Mediation Server. Checks were added to verify that a **CSeq** header is present in all messages, and that a **From** header, **To** header, and **Via** header are present in all Invite messages. Messages not containing these headers are discarded.
- **NGP-241**—**SipFlowFactory** rules engine produces errors when the SIP **From** or **To** header URIs do not contain a user part. The user portion of the URI typically contains the source or destination phone number. Sometimes it contain a string such as "anonymous" or "restricted". It is also possible (but not common) for the URI (particularly the **From** URI) to only include a host name or IP address, such as "sip:10.10.10.10". In that scenario, the Flow Factory produces an error because it always expects an '@' to be present in the SIP URI. Despite the error, the entire contents of the **From/To** header are logged as the **Source/Destination** value). This update will detect that the '@' is not present in the URI, and prevents the error from occurring. The entire contents of the **From/To** header will still be logged in this scenario as before.

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.
- **NGP-252**—SEP Policy commit may fail if an internal policy revision number has grown too large and now is being interpreted as a negative number. Error messages will be produced in the server.log file with the error string “Entity revision has to be greater than 0”.
- **NGP-253**—List names containing certain special characters could be created, but subsequent modifications to the List or List deletion would fail. The problematic characters are / \ . # % ? ; These characters are now prohibited from use in List names along with whitespace, parenthesis, and double quote.
- **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 operations when the system encryption protocol is set to TLSv1.1 or TLSv1.2.

Last Update: 9/1/2017



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>

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

© Copyright 2017 SecureLogix Corporation. All Rights Reserved. SecureLogix technologies are protected by one or more of the following patents: US 6,226,372 B1, 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 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.