PolicyGuru® Meta-Policy Controller v4.2.0 Release Notes

Knowledge Base Article #PG57834

Synopsis

This document contains important information about PolicyGuru® Meta-Policy Controller v4.2.0.

What's New in v4.2.0

- **Multi-factor Authentication** (**MFA) Login**—This release adds the option for MFA login to the PolicyGuru Web Interface. The MFA process uses the OpenID Connect (OIDC) protocol via the Microsoft 365 and Microsoft Entra ID applications. Refer to the configuration instructions below.
- **Upgraded Nginx Software**—The **Nginx** software was upgraded to version 1.26.3.
- **Updates to Underlying System Software**—Various system-level/kernel-level packages were updated to their current latest versions as of the date of this PolicyGuru System release.

Upgrades

- Due to the upgrade to the operating system and other underlying components, upgrades from versions prior to v4.0 are not supported. A clean operating system and application install is required for upgrading from versions prior to v4.0. Upgrades from v4.0 are supported.
- To facilitate moving from PolicyGuru v3.x to PolicyGuru v4.2.0, a Policy Data Migration procedure and application have been created. This migration procedure/application will move all of the Policy-related data configured in a PolicyGuru v3.x system (Rules, Lists, and Listings) into a newly installed PolicyGuru v4.2.0 system.
- **Important** The contents of the **/opt/ngp/nginx/conf/ngp.conf** file have been altered in PolicyGuru v4.2.0, so it is **not** recommended to copy a PolicyGuru v4.0 **ngp.conf** file onto a PolicyGuru v4.2.0 system.

Issues Resolved in This Release

- None

Known Issues in This Release

- **NGP-264**—Upon startup of the ENUM Server or Metadata Probe, the first message related to Authentication processing, such as Authentication Requests on the ENUM Server or SIP Invites on the Metadata Probe, is not delivered up to the Mediation Server. This prevents Authentication processing from working on that call.
- **NGP-164**—List creation with initial Listings creates duplicates in ENUM Policy (formerly called 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 ENUM Policy on the ENUM Server. To prevent this issue, create and save the new List without adding Listings, and then open it to add Listings. The presence of the extra value in Policy is non-service-affecting unless a Listing value that has a duplicate is later edited.

Configuring MFA Login

Use the following configuration information to enable MFA Login on the PolicyGuru v4.2.0 Mediation Server:

MFA Login Configuration

By default, Username/Password authentication is enabled in PolicyGuru v4.2.0. To enable MFA Authentication using OIDC and the Microsoft 365 and Microsoft Entra ID applications, perform the following procedure:

1. Add the PolicyGuru application to Microsoft 365 and Microsoft Entra ID. After adding the PolicyGuru system to these Microsoft applications, the Microsoft System Administrator should have access to the **tenantID**, **clientID**, and **clientSecret** associated with the PolicyGuru system. See "Configure Microsoft Entra Authentication - Azure App Service" for more information about configuring the Microsoft 365 and Microsoft Entra ID applications for use with PolicyGuru MFA Login.

2. On the PolicyGuru Mediation Server, stop the **ngp** service, and then edit the **/opt/ngp/node/ngp/config/env/config.production.js** file. In this file, set the **tenantID**, **clientID**, and **clientSecret** values obtained from the Microsoft system above. Also edit the **config.authType** value and change it from **local** to **oidc**. Note that **OIDC** login can be reverted back to normal Username/Password login by changing the **config.authType** value back to **local**. After editing this file, restart the **ngp** service. Below is an example of the **config.production.js** file configured for **OIDC** login:

   ```
   var config = require('./config.global');
   config.env = 'production';
   config.hostname = '127.0.0.1';
   config.port = 8081;
   config.externalAPIHost = '127.0.0.1';
   config.externalAPIPort = 8443;
   config.oidc = {
       provider: 'azure',
       tenantID: 'b39ec874-d509-4bfd-b762-6c2d182955be',
       clientID: '214c5fd2-e31a-4673-aff6-c1122c4d6de8',
       clientSecret: 'MfF8Q~UwzOjNbkl8k.RnSGyduy0NzXv1WlQdqcgg',
   };
   config.passport = {
       sessionSecret: 'SecureLogix@123',
   };
   config.uiUrl = '127.0.0.1';
   config.uiPort = 443;
   config.authType = 'oidc'; // 'oidc' or 'local' (local is login using username/password)
   module.exports = config;
   ```

3. Edit the **/opt/ngp/config/statistics/config.properties** file. In this file, set **AZURE_TENANT_ID** and **AZURE_CLIENT_ID** to the **tenantID** and **clientID** values obtained from the Microsoft applications above. Below is an example of this **config.properties** file:

   ```
   MOVING_AVG_BLOCK_SIZE=5
   LOOKBACK_BLOCK_SIZE=5
   ```

```
LOOKBACK_OVER_NUM_BLOCKS=8
AZURE_TENANT_ID=b39ec874-d509-4bfd-b762-6c2d182955be
AZURE_CLIENT_ID=214c5fd2-e31a-4673-aff6-c1122c4d6de8
```

4. MFA Login uses port 8081 on the Mediation Server, so configure **FirewallD** to allow connections to **tcp** port 8081 with the following commands:
   - Allow connections to port 8081 for the **pg-mediation** zone:

     ```
     firewall-cmd --zone=pg-mediation --add-port=8081/tcp
     ```

   - Make this change permanent:

     ```
     firewall-cmd --runtime-to-permanent
     ```

5. After making the above changes, restart the **ngp** service.
6. After the **ngp** service restarts, a single button will be available on the PolicyGuru Web Interface, with the label **Sign In With MFA**. Clicking this button will initiate the OIDC/MFA login process via Microsoft 365 and Microsoft Entra ID. At this point, one of the following will occur:
   - The Microsoft Login process may automatically log you into the PolicyGuru system using the account that is currently logged into Microsoft 365 on the given system. View the System Events on the **Realtime** tab to verify the account name that was used for PolicyGuru system login.
   - As an alternative to the above behavior, the Microsoft Login process may prompt you to select an account to use for login. After selecting an account, it will typically prompt for password. After typing the password (or allowing it to be automatically entered), click **Sign In**. At this point, a 2 digit authentication code will be displayed on the GUI, and you should receive a **Sign In** alert on a secondary device, such as your phone, that is running the Microsoft Authenticator app. Enter the code in the app and indicate that you are attempting to sign on. After approving the Sign On, the PolicyGuru Web Interface login should complete and the **Realtime** page will be displayed. Verify the account name that was used for PolicyGuru system login in the System Events.

Last Update: 8/6/2025

SecureLogix®
We see your voice®

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 • https://support.securelogix.com