Identity Governance and Administration Release Notes

December 2023

4.2 version of Identity Governance and Administration solution includes new features, improves usability, and resolves several previous issues. It also includes enhancements provided in 4.0 and 4.1 SaaS releases.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Identity Governance and Administration forum on the communities website, our online community that also includes product information, blogs, and links to helpful resources.

For more information about this release, see the Identity Governance Documentation (https://www.microfocus.com/documentation/identity-governance) website.

What's New

This release provides functional, infrastructure, and performance-related fixes and enhancements. It includes:

Custom Workflows

Custom workflows provide customers with the flexibility to define business processes as they want. Authorized administrators can write complex logic integrated with forms and associate them with access requests and data policies.

We recommend that you use the Identity Governance approval flows available to you as part of the product. Create a new custom workflow only when you need a custom workflow beyond the provided Identity Governance approval flows. When creating custom approval flows start with the available workflow templates.

This release also includes the ability to import and export workflows and enhanced auditing.

IMPORTANT: The Email Based Approval (EBA) feature of the Workflow Service is for preview only, and provided on an as-is and as-available basis. We currently do not support EBA in your staging or production environments. The feature will be supported and available for general use in a future release.

For more information about workflows, see "Using Workflows to Approve Requests " in the *Identity Governance User and Administration Guide* and the *Workflow Service Administration Guide*.

Access Request and Review Enhancements

Identities that are associated with an application in various ways require granular governance. Access requests can now differentiate between multiple accounts in the application for the same identity. Reviews can distinguish between permission assignments for various accounts to provide better reporting and governance.

This release also includes:

- Ability to request business role membership
- Ability to set effective and expiration dates for access requests
- Enhanced CSV export of review list items that includes all details including fulfillment status
- Consistent and enhanced handling of deactivated and deleted accounts, permissions, and technical roles in reviews and fulfillment processes. Identity Governance will no longer generate Fulfillment requests when review items include deleted entities and instead will issue a warning.
- Ability to delete custom review notification emails.
- Ability to select an account when requesting a permission or technical role for a user with multiple accounts. Authorized requesters can select an account that permissions must be associated with when requesting a:
  - Permission for a user who has multiple accounts.
  - Technical Role that includes one or more permissions belonging to one or more applications for a user who has multiple accounts.
- A new sortable Item ID column on the request and approval pages and enhanced tooltip that includes item ID on Workflow approval request items to make troubleshooting easier. Users can also use the filter to search for a particular request item using the item ID.
- Ability to reorder approval steps including the default Potential Separation of Duties (SoD) Violation approval.

- Ability to download the permission assignment attributes as a CSV file for user and account access reviews depending on the configuration. Additionally, the permission assignment attribute value can be viewed for data sources collected from non-IDM applications.
- An enhancement to the way Identity Governance presents multiple permission assignments of the same permission in the catalog, as well as the ability to view all permission assignments.
- Ability to view a consolidated list of review items for permissions with multiple assignments and review additional details such as direct or inherited assignments when reviewing permissions.

Enhanced Data Collection and Fulfillment

When Identity Governance collects permissions from different applications, it is possible to have the same permission assigned to a user or account more than once. This could happen because of reasons such as overlapping effective date ranges and assignment methods, whether direct or inherited. In this release, Identity Governance now allows authorized users to:

- Enable nested permission assignment collection when using AD Permission or eDirectory Permission Collectors to generate inherited assignments
- View permission assignment details on the Identities and Accounts pages of the Identity Governance Catalog
- View permission assignment details when manually fulfilling a change request for permissions

Additionally, Identity Governance now includes:

- Ability to upgrade identity and application collector templates to a higher version while retaining custom configurations
- Ability to import and export merge rules for identity sources
- Fulfillment ticket number display on verified tasks
- Connector upgrades related to security and compliance requirements
- Password changes enforcement when a previously configured service parameter value is changed
- Ability to import and export merge rules for identity data sources
- Ability to import and export each collector independently when the application data source has more than one collector
- Ability to convert identity collector such as AD, eDir, and IDM to AD with changes, eDir with changes or IDM with changes, IDM with changes respectively to collect incremental changes from connected systems that support change collection
- Ability to upgrade to preserve configurations and upgrade fulfillment target template when Identity Governance detects the existence of a higher version of the template
- Following new templates:
  - ServiceNow Task
  - Azure AD
  - MS Teams
  - GitHub REST
- An enhancement to the way application change event processing works. Instead of collecting, then publishing only changes, you now click **Apply Changes** to collect and apply only changes.

For more information about the new templates, see "Understanding Variations for Application Sources" and "Understanding Service Desk and Other Fulfillment Targets" in the *Identity Governance User and Administration Guide*.

For more information about change event processing, see "Understanding Change Event Processing " in the *Identity Governance User and Administration Guide*.

Insight Queries Enhancements

- Additional Insight Queries search criteria entity types and cross-reference filters that enables authorized users to query:
  - Applications, permissions, business roles, or technical roles assigned to access request and access request approval policies.
  - Access request and access request approval policies referenced by applications, permissions, business roles, or technical roles.
  - Ability to download insight query results without running a query. This allows insight queries that have large results and take too long to execute in the background without causing performance issues such as request timeout errors

Enhanced Separation of Duties Violation Handling

Identity Governance now supports Separation of Duties (SoD) and potential SoD violation detection for business roles. Specifically, this release includes the following enhancements:

- Identity Governance automatically detects potential SoD violations for applications, permissions, or technical roles even when auto-grant is configured for the entity in business roles
- Identity Governance automatically prevents auto-grant of business role resources that would cause a toxic SoD violation
- Authorized administrators and business owners can choose to allow the violation or reject the inclusion of the entity in the business role
- Authorized administrators can change the order of potential SoD violation approval step when configuring the Access Request Approval policy
- In addition to Live mode, review runs in Preview mode display SoD violations in the Review item expanded view.

For more information, see Creating and Managing Separation of Duties Policies in the *Identity Governance User and Administration Guide*.

Data Policy Detection Automation and Compliance Enhancements

This release includes the following enhancements:

- Ability to trigger data policy detections using events such as collection, publication, and entity curation
- Ability to monitor results of detections and remediations.
- Categorization of data policies as Events and Violations to clarify different types of data policies and controls
- Enhanced auditing of data policies' background processes
- Optimized data policy detection runs for bulk curation to improve performance

For more information, see "Creating and Managing Data Policies" in the *Identity Governance User and Administration Guide*.

Improved Technical Roles Grants, Revokes, and Deactivation Handling

This release includes:

- Improved handling of technical role activation and deactivation
- Prevention of technical role deactivation when it is referenced Prevention of technical role deactivation when it is referenced in a Business Role, an SoD policy, an access request policy, or an access request approval policy
- Prevention of authorization of inactive technical roles in a Business Role policy

  NOTE: If you already have an inactive technical role in an existing business role we recommend that you remove the inactive technical role. If you import a business role that references inactive technical roles, and you want to retain a technical role authorization, activate the technical role before performing the import.

- Removal of technical role assignments when SoD violations are resolved

New and Enhanced Identity Governance Reports

This release includes the following new reports:

- Current User Access – CSV
- Data Policies and Controls Overview - CSV
- Data Policies and Controls Details - CSV
- Items Covered by Approval Policies - CSV
- Separation of Duties Approval Policies Details - CSV
- Separation of Duties Policies Details - CSV

This release also contains miscellaneous enhancements such as:

- Inclusion of business role information in Access Request reports
- Inclusion of time-based features of access requests in all reports
- Improved usability and required software upgrades to further align with security and compliance requirements

BMC Ready Fulfillment is Deprecated

Starting with Identity Governance 4.2, fulfillment to BMC Remedy is deprecated and will be removed in a future release.

Support for Installation with MS SQL Database is Deprecated

Starting with Identity Governance 4.2, utilizing MS SQL as a database to install against is deprecated and this option will be removed in a future release. The JDBC Collectors and Fulfillment will not be impacted when the ability to install against MS SQL has been removed.

NOTE: Occasionally, MS SQL transactions might result in deadlocks. We are working on a process to move from MS SQL to either Oracle or Postgres.

Use of String Values for expirationDate and effectiveDate Attributes Are Deprecated

The REST API documentation for POST /request/request outlines that you use String value for the following attributes:

- expirationDate
- effectiveDate

String values are deprecated.

IMPORTANT: The release after the 4.2 release will only accept values in Long format for these two attributes. The REST API documentation will be updated accordingly. Please transition your code to utilize the Long value.

Miscellaneous

This release includes miscellaneous security, compliance, performance, and monitoring-related infrastructure updates to provide additional governance capabilities. It includes:

- Ability to reset Governance Overview view to the global default for self or retain local settings for self and restore default configuration for other users directly from the Governance Overview page in addition to from My Settings menu
- Improved custom forms integration with REST API invocation in Identity Governance
- Improved logging and navigation when using custom user-matching attribute
- Ability to set business roles and technical roles as authorization roles
- Enhanced business role detection including ability to download inconsistency detection results as a CSV file
- Enhanced data protection measures including customer-based data encryption keys
- Ability to configure whether PSoDV (Potential Separation of Duties Violation) requires approval for requested items that contribute to a SoD even if the violation is already detected
- Support for archival rotations
- Improved logging and navigation when using custom user-matching attribute
- Upgrades of third-party components to recent versions including upgraded Form Builder

Technical Requirements

For more information about browser requirements and supported components for this release of Identity Governance, and additional supported drivers and packages for accounts and permissions collection from the Identity Manager environment, see the *Identity Governance Technical Requirements*.

Known Issues

We strive to ensure that our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (https://www.microfocus.com/en-us/support).

String Customization Issues

- Access Request string customization is not working. This issue will be fixed in a future release. Meanwhile, instead of creating a file with *only* the entries you want to update as described in "Customizing Strings for Identity Governance", make the necessary changes in the file that contains all the entries (for example: `CxRsrc_en.properties`), then create the custom `.jar` file with the updated properties file.
- Identity Governance client string customization is not working. The `client-strings.jar` used for Identity Governance client string customization has incorrect path. This issue will be fixed in a future release. Meanwhile to customize Identity Governance client strings successfully follow the steps given below and retry.
  - Change the path in the `.jar` file from `com/netiq/ig/client` to `com/netiq/iac/client`
  - Recreate the string customization jar file
  - Place the updated jar file in the tomcat/lib folder
  - Restart Tomcat

Sorting on the Default Forms Tabs of the Access Request Policies Page Does Not Work Correctly

Issue: On the Application Default Forms and Permission Default Forms tabs of the Access Request Policies page, clicking on column headings does not sort the list as expected.

This will be fixed in a future release.

MS SQL Might Create Locks that Could Result in Deadlocks

It appears that MS SQL obtains internal locks on various database objects as it performs certain operations. Sometimes, those locks result in deadlocks.

For example, when a transaction updates a record, the transaction will first attempt to obtain a lock on that record. We have seen cases where the first record updated in a transaction results in a deadlock error. That should be impossible. As it is the first record we have attempted to update in the transaction, it should be the first lock the transaction attempted to obtain. Because it is the first lock, a deadlock should be impossible because, by definition, a deadlock requires that the transaction has previously ALREADY obtained locks on other objects.

This behavior leads us to the conclusion that when MS SQL updates a record in a table, it is locking more than just the specific record being updated. It is likely also locking an index key range or other internal objects. This is something we have noticed in other places with MS SQL. It obtains internal locks on various objects as it performs certain operations, and those locks sometimes cause deadlocks. There is nothing that we can do to prevent deadlocks when we cannot control the locks that MS SQL obtains and the order in which it obtains them.

Searching Technical Role Mining Suggestions Does Not Filter the Suggestions

Issue: Entering any value in the Search field to filter Technical Role Mining Automatic Suggestions does not filter the results. Instead, the following message is displayed:

```
There are no role mining suggestions. Close the dialog and generate new
suggestions.
```

Workaround: Use the browser Find option or shortcut, or scroll through the results to find the value. This issue will be fixed in a future release.

Bulk Data Update Template Generation Fails on Windows When A User or Group is Specified for Notifications

Issue: If Identity Governance is installed on Windows, the Bulk Update template generation, using the **Bulk data update** link on the Data Source pages, will fail if you specify a person or group in the **Notifications** field. This issue will be resolved in a future release.

Workaround: Do not specify a user or group for notifications.

Sorting by Risk on the Business Roles Page Does Not Work Correctly

Issue: On the Business Roles pages, clicking on Risk column heading to sort the list of business roles does not sort the list as expected.

This will be fixed in a future release.

Business Role Requests Might Display Errors in Logs When You Use Custom Workflow as Approver in the Access Request Approval Policy

Issue: When you use a custom workflow for approving Business Role requests from Access Request, you might see the following errors in the logs:`[SEVERE] [com.netiq.iac.server.rest.util.ArcBeanUtil] [IG-SERVER] Encountered unexpected error: Unknown property 'entityCategories'`

`[WARNING] [com.netiq.iac.server.rest.util.ArcBeanUtil] [IG-SERVER] Encountered unexpected error.`

`[SEVERE] [com.netiq.iac.server.rest.util.ArcBeanUtil] [IG-SERVER] Encountered unexpected error: Property 'membershipUpdatedDate' has no getter method`

`[SEVERE] [com.netiq.iac.server.rest.util.ArcBeanUtil] [IG-SERVER] Encountered unexpected error: Property 'authsUpdatedDate' has no getter method`

The errors *do not* cause the request to fail. This will be resolved in a future release of Identity Governance

Retrying a Failed Fulfillment Might Resubmit Items from the Changeset that were Verified as Fulfilled

Issue: A request might include list of change requests (changeset). When a few items in the changesets are verified as fulfilled and other items fail, and you try to resubmit the failed items, Identity Governance might resubmit all items instead of only resubmitting the failed items. This will result in all changeset items marked as Failed / Retry.

Workaround: Do not retry when items in a change request are in a Verified state. Instead, create a new request only for the failed items.

Moving Selected Columns in Display Options Does Not Work with More Than One Row of Column Names

Issue: Typically, you can rearrange columns on any page that displays a list such as permissions or technical roles by clicking the gear icon on the top left of the list, then dragging and dropping the selected column names. However, when your selected column names span to more than one row on the display options (settings) page, you cannot move column names from one row to another to rearrange the respective columns.

Workaround: Remove column names so that the selected columns can fit into one row, then move them as needed. Or unselect all columns, then select them in your preferred order.

Permission Review Criteria is Not Saved Correctly when the Attribute Type is Boolean

Issue: Identity Governance does not always filter correctly when you select a Boolean attribute to filter results and:

Workaround: When you want to select entities with Boolean attribute as review criteria, first select a string attribute, select a value, and save to clear out all default and previous operators, then select attribute of type Boolean, select a value, and save.

Governance Insights is Not Saving the Boolean Filter Correctly

Issue: Identity Governance does not always filter correctly when you select a Boolean attribute to filter results and:

- Run an Insights query without saving the query whose Boolean attribute value is set to `no` (false)

  Or

- Run a saved Insights query whose Boolean attribute value is set to `no` (false)

Workaround: Change the Boolean attribute value to `yes`, and change the filter operator to **None of the following (NOT)**. For more information about advanced searches, see "Using Advanced Filters for Searches" in the *Identity Governance User and Administration Guide*.

REST API Documentation Not Rendering Correctly

The framework for the REST API documentation was updated in a previous release. As a result you might encounter one or more of the following issues with API documentation for Identity Governance (`apidoc`) and Identity Reporting (`rptdoc`):

- The page takes longer to fully render than before.
- Few of the API specifications do not expand automatically when you select them. Select **Expand Operations** to expand them.
- Text in a few areas are not formated or aligned.

This will be fixed in a future release.

A Warning Can Appear When Upgrading Identity Governance and Enabling Auditing During Installation

Issue: If you use the Identity Governance installer to enable auditing for one or more of the following modules during an upgrade — DaaS WAR, DTP WAR, and Workflow WARs— a “connection refused” warning for syslog audit appears when you start Tomcat. Configuration values set for these modules during the upgrade revert to the default values, and values you set during installation are not saved.

Workaround: Perform the following procedure after installation completes:

1. Log in to Identity Governance as a Global Administrator.
2. Select **Configuration** > **Audit Enablement**.
3. Correct and save the audit target settings for the DaaS WAR, DTP WAR, and/or Workflow WAR.

NOTE: Do not make changes to the **cache-dir** and **cache-file** settings. They contain events that could not be sent to the syslog server. After you correct the syslog host and port, as well as any keystore settings, Identity Governance will send those cached events to the syslog server.

SCIM Driver Fails to Update IDM Entitlement Fulfillment Status

Issue: Even if a change request, such as adding a user to a group in SAP application, is fulfilled successfully, Identity Governance displays the status as `Pending Verification`. This occurs because the SCIM Driver fails RFC 7644 (https://www.rfc-editor.org/rfc/rfc7644) pagination specifications and returns only limited entitlements to Identity Governance. This issue will be fixed in a future release.

Reimporting Previously Deleted Roles and Policies Might Fail Soon After Cleanup

Issue: Sometimes business roles, SoD policies, technical roles, applications, or review definitions are exported, deleted, and later reimported. If a cleanup operation purges the deleted business roles, SoD policies, technical roles, applications, or review definitions before they are reimported, you might get an error in the UI during the reimport process, depending on how soon after the purge the reimport takes place.

The server log would contain an ERROR (SEVERE) message that corresponds to the error message in the UI. The wording of the message will be different depending on the database platform, but in general the message will indicate that an insert or update into the auth_role_mapping table violated the fk_auth_scope_id foreign key constraint.

Workaround: If you see this kind of error, please wait at least 10 or 15 minutes and then try to reimport again.

MS Teams Collection Fails with the Error: `Failed to execute backend request`, While Collecting Team Members

Issue: While collecting team members using MS Teams collector, the collection fails and the following error message is displayed:

[com.netiq.daas.azuremsgraph.impl.TeamMembersDecorator] [DAAS] {"error": {

"code": "BadGateway",

"message": "Failed to execute backend request."

Workflow Issues

Syslog Audit Keystore File Path is Not Correct When Installing Workflow on Windows Server

Issue: When installing Identity Governance with Workflow and enabling audit during installation, the keystore path is incorrect. This results in errors in catalina logs.

Workaround: After installation, log in to Identity Governance and access Workflow Administration Console. Click **Configuration**. In the Audit Configuration area, change the keystore file path from `C:\opt\netiq\idm\apps\tomcat\conf\apps-truststore.pkcs12` to `C:\netiq\idm\apps\tomcat\conf\apps-truststore.pkcs12`. Then, restart Tomcat and check the catalina logs to make sure there are no errors.

JMS Persistence Warning is Displayed for the Notification System During Workflow Service Startup

Issue: When Workflow Engine is installed with ActiveMQ details, after installation when the Tomcat server is started, the warning, “Could not properly initialize JMS persistence for the notification system” is observed in the catalina logs. The warning is displayed because Workflow Service fails to connect to the ActiveMQ server. Since ActiveMQ cannot initialize JMS persistence, messages are lost and not persisted. This happens because of the missing topics from the `context.xml` file and the respective details from the `server.xml` file.

Workaround: To have guaranteed email delivery the `context` and `server.xml` files must be modified.

To modify:

1. Navigate to the `tomcat/conf` directory.
2. Open the `context.xml` file with a text editor and add the following entries before `</Context>`.

```
<ResourceLink global="jms/ConnectionFactory" name="jms/ConnectionFactory"
type="javax.jms.ConnectionFactory" />
<ResourceLink global="topic/WFNotificationDurableTopic" name="topic/
WFNotificationDurableTopic" type="javax.jms.Topic" />
<ResourceLink global="topic/EmailBasedApprovalTopic" name="topic/
EmailBasedApprovalTopic" type="javax.jms.Topic" />
```

3. Save the changes and close the file.
4. Open the server.xml file with a text editor and add the following entries before `</GlobalNamingResources>`.

```
<Resource auth="Container" description="Topic for Workflow"
factory="org.apache.activemq.jndi.JNDIReferenceFactory" name="topic/
WFNotificationDurableTopic" physicalName="WFNotificationDurableTopic"
type="org.apache.activemq.command.ActiveMQTopic" />
<Resource auth="Container" brokerName="LocalActiveMQBroker" brokerURL="tcp://
localhost:61616" description="JMS Connection Factory"
factory="org.apache.activemq.jndi.JNDIReferenceFactory" name="jms/
ConnectionFactory" type="org.apache.activemq.ActiveMQConnectionFactory" />
<Resource auth="Container" description="Topic for Workflow email based
approval" factory="org.apache.activemq.jndi.JNDIReferenceFactory" name="topic/
EmailBasedApprovalTopic" physicalName="EmailBasedApprovalTopic"
type="org.apache.activemq.command.ActiveMQTopic" />
```

5 Save the changes and close the file.

6 Restart Tomcat.

Repeat these steps for all installations.

In a Distributed Environment when a Workflow Form is Clicked, an Error is Displayed

Issue: If you install Identity Governance and Workflow on separate servers, and then from the Workflow Administration Console you click any one of the forms by accessing **Catalog** > **Forms**, you will see an error message.

This issue will be fixed in a future release.

Workflows Created Using System Templates Reports Exceptions in the Server Logs

If email-based approval is enabled on Workflow Service, the following data item exceptions are reported in the server log file when a user grants permission via email:

```
com.novell.soa.af.DataItemException: Dataitem [formHeader] is required.

com.novell.soa.af.DataItemException: Dataitem [fulfillmentInstructions] is
required.

com.novell.soa.af.DataItemException: Dataitem [requesterFeedback] is required.
```

These exceptions occur in workflows created using system templates, however, they do not cause any loss of functionality and may be ignored. The permission is successfully granted when the user approves the request.

This issue will be resolved in a future release.

Multiple Value Mapping with `flowdata.getObject()` Populates all Values in a Single Field

Issue: When multiple values are mapped using `flowdata.getObject()`, all the values are populated in a single field. For example, in the Workflow Administration Console, create a form that requires multiple values, such as text field, email, and phone number. Create a workflow with two approval activities and attach the form with the activities. In the pre-activity data mapping of the second approval activity, map the fields with multiple values from the first approval activity's form using the `flowdata.getObject()`. In Identity Governance, request that workflow. Navigate to > **Approvals** > **Workflow Approvals** and select **Approve** or **Deny** to launch the approval form of the workflow. Type the values for the requested fields and launch the next approval form. The data mapped from the previous form using `flowdata.getObject()` displays all data in a single field.

This issue will be fixed in a future release.

Expressions In Workflow Rest Activity Does not Allow // in a Comment

Issue: Inability to publish workflows when the **Request Content** field in the Rest Activity contains the slash slash (`//`) expression in a comment.

Workaround: To save and publish the workflow, use the slash-star (`/*`) star-slash (`*/`) while adding a comment.

IDM Entitlement JDBC Driver Fails to Verify Fulfillment After Successfully Inactivating an Account

Issue: When you remove an account from the database, even though fulfillment is successful, Identity Governance displays the status as `Not Fulfilled, Verification Error.` This issue occurs because the value returned by the database might not be consistent with the values the JDBC driver expects.

Workaround: Ensure that the account status in the entitlement configuration for the driver displays the following values:

- For MSSQL and Oracle: `<account-status active="0" inactive="1" source="read-attr" source-name="Login Disabled"/>`
- For PostgreSQL: `<account-status active="FALSE" inactive="TRUE" source="read-attr" source-name="Login Disabled"/>`

IDM Entitlement Fulfillment Requests Might Not Display Fulfillment Status Correctly

Issue: When a request, such as the assignable role for Workday request, is sent to the IDM entitlement fulfiller, Identity Governance might display verification failed status even when the request displays fulfillment successful status.

Workaround: Access the driver logs, driver trace files, and audit events to view request details including status and error description.

Custom Forms Do Not Display Request Item Description in Bold Italics By Default

Though Identity Governance supports markdown for permission and application descriptions, currently it does not have a markdown viewer for request forms. As a result, any markdown syntax in an application or permission form will display as it is instead of being rendered as expected.

Moving a User from One Business Role to Another Using Curation Causes the User to Lose Authorized Permissions

Issue: If two business roles (BR1 and BR2) authorize the same permissions and specify auto-grant and auto-revoke on those permissions, and a manual or bulk data update (also known as curation) moves a user from BR1 to BR2, the user could lose the permission for a period of time between the fulfillment of the auto-revoke request and the fulfillment of the compensating auto-grant request.

This is possible because, after curation, separate detections are triggered for BR1 and BR2, instead of a single detection that does both together. If detection is first done on BR1 (the role the user lost membership in) followed by BR2 (the role the user gained membership in), Identity Governance would issue an auto-revoke, followed by a compensating auto-grant. If detection is first done on BR2 followed by BR1, auto-revoke or auto-grant request will not be issued. Based on your fulfillment approach (manual, workflow, automatic, custom), in the case where detection first occurs on BR1 and then BR2, causing an auto-revoke request and compensating auto-grant request to be issued, the user could lose the permission between the fulfillment of the auto-revoke request and the fulfillment of the compensating auto-grant request.

Workaround: It is recommended that you do not utilize curation if you have business roles with overlapping permissions that are enabled for auto grants and auto revocation. If data update occurs, check business role detections (**Policy > Business Roles > Business Role Detections**) to verify that a compensating grant request was issued, and if not, detect inconsistencies (**Policy > Business Roles > Manage Auto Requests**) and issue a grant request.

Navigating Away from Unchanged Page Might Result in Erroneous Prompt to Save Changes

Issue: When using Chrome with autofill enabled, some product pages could prompt you to save changes when you navigate to another page, even if you have not made changes. This issue occurs when Chrome automatically populates configuration fields as soon as the page loads.

Workaround: Temporarily turn off autofill when accessing the product using Chrome browser, or ignore erroneous save prompts when you know you have not changed anything on the page.

Unresponsive Script Error in Firefox Can Occur When Clicking a User in the Certification Policy Violation Popup Window

Issue: In some cases, when you click a user in the Certification Policy Violation window when using Identity Governance with Mozilla Firefox, an unresponsive script error can occur.

Workaround: The issue lies with Firefox. For information about correcting the issue, see this Mozilla knowledge base article (https://support.mozilla.org/en-US/kb/warning-unresponsive-script?cache=no).

Third-party Issues

Some known issues lie within third-party applications that are integrated with Identity Governance. The following known issues can be tracked with the third-party vendor. Micro Focus provides links to those issues, where available.

Form Builder Issues

- In the Form Builder, text that appears on various component tabs cannot be localized, because Form.io does not support localization for this text. This will be fixed in a future release.
- **Issue:** If Form Builder was used from the Workflow console to create an approval workflow that requires two approval activities, and you provided two or more phone numbers during the first approval activity, those phone numbers will not appear in the second approval activity. The issue lies with Form.io, who is aware of the issue and is working toward a solution (https://github.com/formio/formio.js/issues/4666).

  Workaround: Click **Add Another** under the **Phone Number** field to make the provided phone numbers appear.

- If Form Builder was used from the Workflow console to create an approval workflow that requires two approval activities, and multiple values were supplied during the first approval activity, those values will duplicate in the subsequent approval activity if you click the **Add Another** button. The issue lies with Form.io, who is aware of the issue and is working toward a solution (https://github.com/formio/formio.js/issues/4666).
- When creating a custom form, the Approval Address field accepts values from the request address field only if using the Calculate Value. The Approval Address field does not receive information if using the Custom Default Value. The issue lies with Form.io, who is aware of the issue and is working toward a solution.
- Validations are not triggered if the `ValidateOn` property of a component is set to `Validate on Blur`, but will, instead, validate on change. The issue lies with Form.io, who is aware of the issue and is working toward a solution (https://github.com/formio/angular/issues/238).
- When adding a layout component to a form and configuring Action Types, **Value** appears as an option, but this option is not applicable for a layout component. The issue lies with Form.io, who is aware of the issue and is working toward a solution (https://github.com/formio/formio.js/issues/3312).
- Online help does not exist for the tree component. The issue lies with Form.io, who is aware of the issue and is working toward a solution.
- The default value does not return when you select the “Multiple Values” and “Clear Value on Refresh” options. The issue lies with Form.io, who is aware of the issue and is working toward a solution.
- Some event trigger types with the “Hidden” property set do not hide the configured component. The issue lies with Form.io, who is aware of the issue and is working toward a solution.

Resolved Issues

Resolved IDM AE Collector and IDM Automated Fulfillment Issues

- IDM automated fulfillments were failing because of support for special characters in a newer release of the Identity Manager Applications role and resource name. Support for special characters was implemented in a related background service and IDM Automated fulfillment is working successfully.
- The Group attribute mapping for the Permission Owner attribute now persists in the IDM AE Permission collector even when you navigate to a different page.
- Previously, when the IDM AE collector requested data, the responses from the target application were sent in chunks, causing the collection to fail. This issue is fixed.

Review Auditor is Not Able to View a Review that Utilizes a Coverage Map

Review auditors can now view reviews that utilize a coverage map.

Sorting the Permissions within a Technical Role by Application Name from the User's Role Tab fails

Permissions in a Technical Role can be sorted based on Application Name from the User’s Role tab.

JDBC Collector Should not Convert Date Columns from the Source

The JDBC collector was converting data from the collected columns to strings if the column matched java.sql.Types.TIMESTAMP. However, in Identity Governance the “Date” column requires values to be in epoch. This issue is now resolved.

Remove Extra Queries on the Roles Tab of Business Roles Related to Authorizations

Previously, Business Roles that included authorizations for permissions and Technical Roles resulted in Identity Governance performing some queries that were not required. These extra queries are removed now to improve performance.

Escalation is not Complete for Account Reviews

For account review, the reviews are now being escalated correctly to the second stage reviewer.

Fulfillments via Cloud Bridge will Report a Failure if no Response in 30 Seconds

Fulfillments were failing with no response from the agent because the backend system took more than 30 seconds to respond. This issue is resolved.

The Category and Application Quick Filters Only Work when the Browser Language Setting is English

This issue has been fixed. The quick filters work as expected when the browser is set to other languages.

Group Permission Owners are Removed during Identity Publications

This issue is fixed. When you collect and publish the identity source, the group permission owners of that application are retained.

IDM Entitlement Collection and Fulfillment Test Connection Fails If User Password Contains a Colon

The collection and fulfillment test connection happens successfully when the password contains a colon.

Identity Governance API Calls were Failing in Form Builder

This issue has been fixed. You can now successfully use APIs.

The Within Date Criteria is Not Saved Correctly

Previously, while defining an account access review with selected mapped and unmapped account and also **Last Login Date > within > days from now** as the review item criteria, if the user navigated away from the page, the within criteria was not retained. This issue has now been resolved.

Fulfillment Changeset Purging Fails

This issue is now fixed. Purge was failing for fulfillments generated through changeset processing scripts.

Not providing the full information to a user that has no tasks in Governance

Identity Governance now displays the appropriate message when a user with no action items in Identity Governance tries to access the application.

Resolved Form Builder Issues

- Calendar Icon is now Shown for Date/Time Component .
- The Date/Time values no longer appear as “Invalid” in Firefox.
- Using the JS editor to set a check box component to appear selected by default functions as expected.

Resolved Workflow Issues

- You can now search for Workflows when External Workflow Engine is Installed on a Remote Server and the application URLs work correctly.
- Group addressees can now approve or deny approval tasks in Identity Governance for workflows which has Multiple or Quorum as Approver Type.
- Previously, workflows with a loop failed with the error “too much recursion” in the browser console. The error is no longer observed in the browser console and the flowdata tree has the post activity of the mapped activity within the loop.
- Workflow processes the request form’s Select control value correctly and displays User IDs as expected.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@microfocus.com (mailto:Documentation-Feedback@microfocus.com). We value your input and look forward to hearing from you.

For support, visit the Micro Focus Support Website (https://www.microfocus.com/en-us/support/customer-support-handbook#phone).

For general corporate and product information, see the Micro Focus Website (https://www.microfocus.com/en-us/home).

For interactive conversations with your peers and experts, become an active member of our community (https://community.microfocus.com/). The online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notices