Identity Governance and Administration Release Notes

24.3 (v4.3.1)

This version of Identity Governance and Administration solution includes new features, improves usability, and resolves several previous issues.

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:

OpenText Branding

Identity Governance and its integrated components have been rebranded to meet the OpenText branding guidelines. This includes changes to logos, colors, version numbers, and copyright text.

Identity Governance Authorization Review

Customer and Review Administrators can now create a Global Authorization Assignment review definition that allows users to review user authorization assignments within Identity Governance. Identity Governance fulfills the change requests originating from this review type by immediately removing the authorization from the target user, group, or service.

For more information about review process flow and review types, see “Understanding the Review Process” in the *Identity Governance User and Administration Guide*

Process Authority using Inconsistency Resolution Policy

Identity Governance provides the ability to configure rules to establish process authority and resolve conflicts between governance policies by defining a new Inconsistency Resolution Policy. The new policy enables the Customer Administrator to define and schedule inconsistency detection conditions and resolutions based on the business needs. It also enables the Customer Administrator to define policies to automatically resolve business role inconsistencies based on the defined rules.

For more information, see “Creating Inconsistency Resolution Policies” in the *Identity Governance User and Administration Guide*

Support for Time-Based Review and Approval Assignments

Identity Governance now supports time-based review and approval assignments in User Access Reviews, Account Access Reviews, Account Reviews with permissions enabled, and Business Role Membership Reviews. Authorized administrators can review and remove effective and expiration dates. They can also retract these assignments from pending requests on the Access Request page.

Enhanced Ability to Define Coverage Maps

Identity Governance enables use of following relationship and operators to create more targeted review and request coverage maps:

- New Permission: Holder relationship
- Ability to use "equals one of" and "does not equal any of" operators when defining relationships to further limit coverage map resulting in more than one result
- Enhanced support for "AND", "OR", and "NONE" operators to create more complex criteria

For more information about coverage maps, see “Using Coverage Maps ” in the *Identity Governance User and Administration Guide*.

Enhanced Business Context Resilience

Identity Governance now provides new and enhanced export and import capabilities to support businesses to effectively backup and restore their previously configured business context. In addition to previous export and import capabilities, authorized administrators can:

- Export and import data such as Data Policy Schedules and Collection Schedules, Fulfillment Context Attributes, Global Authorizations, and General Settings as a single SQLite database file
- Export and import other policies and settings such as Risk Policies, Technical Roles, and Analytics Role Mining Settings as a single SQLite database file
- Continue to import data from previous versions of Identity Governance in formats such as JSON and CSV

When importing an SQLite database file, Identity Governance uses an enhanced import flow to refresh data and enable administrators to filter the imported data as per the business needs.

For more information, see “Exporting and Importing” in the *Identity Governance User and Administration Guide*

Enhanced and New Data Policies

Identity Governance now provides:

- Micro certification as a remediation option for permission data policies
- Support for technical role data policies that includes:
    - Ability to trigger technical-role-change detections by events (technical role user assignment changes or technical role detections), schedule, or manually
    - A new metric type (Technical role change) that enables authorized users to create publication data policies for technical role users, permissions, and owners' related addition, removal, or changes
    - New out-of-the-box data policies for adding, removing, or changing detected and assigned users
    - Ability to trigger technical-role-change detections by events (technical role user assignment changes or technical role detections), schedule, or manually

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

Enhanced SCIM Collector and New PAM Collector

Identity Governance provides the following enhanced collection and fulfillment capabilities:

- Support for Client Credential Flow authentication when using SCIM collectors to enable integration with applications that allow machine-to-machine communication for authentication
- A new Privilege Access Management (PAM) collector template that enables administrators to collect PAM accounts and permissions

For more information about the new templates, see “Understanding and Configuring SCIM Templates” and “Understanding and Configuring PAM Templates” in the *Identity Governance User and Administration Guide*.

Access Request Search Performance Improvements

This release includes the following enhancements to improve Access Request search capability and accuracy:

- Ability to configure enhanced search paging
- Ability to configure minimum characters required to optimize search
- BR and Group membership query improvements

Enhanced User Selection When Requesting Access

Identity Governance now displays user title and provides additional quick information to enable more effective user selection when requesting access.

New Fonts for Reports. Replace or Update Installed Reports.

We have discontinued use of monotype fonts and all defaults reports have been converted to `OT-Report-Font-Set`.

Starting with Identity Reporting 7.4, the Arial font is no longer included. For first time users, no additional steps are required as there will not be any report definition on the Repository page.

For those who are upgrading:

- If the report definition was originally installed using the Download feature in Reporting, reinstall the latest version of the report from the Download page
- If the custom report definition was provided by Professional Services, please contact them for a new version
- If the custom report definition was provided by a Partner, please contact them for a new version
- If you created the custom report, replace Arial with OT-Report-Font-Set throughout the report definition, repackage, and then import the report definition

If the report definition is not updated, it will fail at runtime with the following error: `An error was detected while running report '%name%': Font "Arial" is not available to the JVM. See the Javadoc for more details.`

Miscellaneous

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

- Connector upgrades related to security and compliance requirements
- Deactivation of import capability in Identity Governance Reporting to enhance security
- Display of No Status when detection status is null for an SoD Policy
- Enhanced Access Request Approval Form that displays request parameters and selected entitlement value for requested permissions
- Improvements to time-based access requests to prevent issues such as:
    - Errors conditions due to cache issues when a technical role grant or revoke request is being processed
    - Inaccurate display of time when an approval step expires

* Prevention of error conditions when users modify a permission or account and navigate to other areas of the user interface after pressing the Save button without waiting for confirmation that the change was saved.
* Removal of custom editor selector in Text Area component of the Form Builder to prevent third-party integration issues. Users can continue to edit text using the default text area component.
* Updates to reports such as addition of custom attributes to Review Details CSV Reports
* Upgrades of third-party components to recent versions including upgraded Form Builder
* User interface improvements related to Section 508 Color and Contrast conformance

Deprecated Features

The following features have either been removed or have been deprecated and will be removed in a future release:

* "Use of String Values for expirationDate and effectiveDate Attributes is Obsolete" on page 5
* "Configuring OSP to Use Advanced Authentication for Two-Factor Authentication is Deprecated" on page 5
* "Import of Coverage Maps in CSV Format is Deprecated" on page 5
* "Support for Installation with MS SQL Database is Deprecated" on page 5

Use of String Values for expirationDate and effectiveDate Attributes is Obsolete

The REST API documentation has been updated. It outlines that for POST /request/request you can only use Long value for the following attributes:

* expirationDate
* effectiveDate

Configuring OSP to Use Advanced Authentication for Two-Factor Authentication is Deprecated

Starting with Identity Governance 4.3, configuring OSP to use Advanced Authentication for two-factor authentication is deprecated. Instead, customers may use SAML authentication from Advanced Authentication to OSP. Advanced Authentication also provides many other authentication methods such as Card, OATH OTP, and Facial Recognition during the login process.

Import of Coverage Maps in CSV Format is Deprecated

Starting with Identity Governance 4.3, the ability to import Coverage Map CSV file is deprecated. The Coverage Map user interface is a more robust and easier method to create coverage maps.

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. 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.

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).

A Few Issues with Add or Remove Entity Change Data Policies

Issue: When using Entity Change data policies *that specify Add or Remove operations*, you might encounter the following issues:

- Curation as a trigger event might incorrectly appear as an option when defining an Entity Change data policy with Add or Remove operations.
- If both Add and Remove events occur within the same collection and publication the related data policies' results might reflect zero (0) changes.
- Applying changes when publishing application sources might result in a data policy results reflecting changes when they should not.

  Entity Change data policy results for collection and publication should be similar to comparison data that you can view when selecting **Data Sources > Activity**. Changes resulting from applying changes should not be reflected in the Entity Change data policy results.

Running a Saved Insight Query with a Cross Reference Might Return No Results

Issue: When a saved insight query has a cross reference (example: `supervisor`) *and* a filter (example: `Title equals Consultant`), running the saved query will return: `No results found`.

Creating the same query and not saving it will return the expected results. When the saved insight query *does not have both* a cross reference and filter, the expected results will be returned.

Changing of the Resource Request Parameter Key Causes Issues in Identity Governance

Issue: Changing a Resource Form Request Parameter ID (key) from the default naming convention of `param1`, `param2`... `paramN` to some other value on a Resource in Identity Manager, will cause issues within Identity Governance.

Workaround: Only change the Display Label.

Resource Request Parameters Appear as Review Items

If an Identity Manager Resource containing Resource Form Request parameters is included in an Identity Governance Review, the Resource Form Request parameters appear as items to be reviewed. During review, please click **Keep** when reviewing these items.

Access Request String Customization is Not Working

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.

Converting Identity Collector to “With Changes” Collector Might Not Complete Successfully

Issue: In Identity Governance as a Service, when you convert an identity source collector to a collector with changes, you might see a message stating `Saving...` but the collector will not be converted.

Workaround: When you see the Saving message, modify the description of the collector, then click **Save**. Also, even if you see a Saved message when you enter values for polling interval or polling times, modify description, then click **Save**.

This issue will be fixed in a future release.

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

Issue: On the Application Default Forms and Permission Default Forms tabs of 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.

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 clear all column selections, then select them in your preferred order.

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.

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.

Workflow Issues

Workflow Administrators Must Be Set to Users and Not Groups

Issue: Setting a group as Workflow Administrator in Identity Governance by selecting **Configuration > Authorization Assignments** will not provide members of the Group with admin rights in Workflow Service.

Workaround: Add each member of a Group as the Workflow Administrator and also add them as Global Administrator.

This issue will be addressed in an upcoming release of Identity Governance.

Manual Steps Required When Upgrading with Oracle or MS SQL

Issue: When you upgrade Workflow Service from a prior version to version 1.0.8.0100 that ships with Identity Governance 4.3.1 and use Oracle or MS SQL as the database, JDBC audit is set to `true` instead of `false` causing errors.

Workaround: Follow the next steps *before* starting Tomcat to avoid errors.

1. Connect to the Workflow database using the authorized user ID and password. The default name of the database is `igaworkflowdb`.
2. Issue the following update statement: `update configuration set VALUE='false' where configkey='workflow.audit.wfs.jdbc.enabled';`
3. (Conditional) When using Oracle database, in addition to Step 2, issue the command: `commit;`
4. Start Tomcat.

Unable to Collect Activity Statistics and Entity Usage Statistics Metric Data in Systems That Use Workflows

Issue: When Workflow Service is integrated with Identity Governance systems, and a workflow is used for access request approvals, remediations, or fulfillment, Activity usage statistics and Entity usage statistics metrics collection results in error. This will be fixed in a future release.

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.

Tasks Do Not Appear in the Approver's Queue

Issue: If administrator utilizes expressions such as `Entity.get('user', '%userId%', 'userId')` or `Entity.get('group', '%groupId%', 'groupId');` which do not resolve correctly, then Workflow Approval task will not appear in the person's queue.

Workaround: Use the fields next to the ECMA Script in the Expression Builder window to verify expression syntax. The Addressee expression for an approval activity must evaluate to either a user's `uniqueUserId` or a group’s `uniqueGroupId`.

An example of an addressee being the recipient's manager is `Entity.get('user', recipient, 'supervisor').`

Examples in documentation will be updated in a future release.

Exporting Workflow Throws 401 Error Due to Token Timeout

Issue: In the Workflow Administration Console, clicking **Export Workflows** after the token has timed out triggers an 401 error. The error is visible in the console’s network tab.

Workaround: Click Refresh and reload the page to export workflows.

Workflow Expressions in the Workflow Administration Console Expression Builder are Appended with a 0

Issue: In the Workflow Administration Console, when you select any activity within a workflow, in the expression builder that opens up, the expressions are displayed with a "0" next to them.

The issue lies with PrimeNG, who is aware of the issue and is working towards a solution (https://github.com/primefaces/primeng/issues/14971).

Import File Names are Suffixed with Numbers in the Workflow Administration Console

Issue: When you import forms, workflows, or notification templates in the Workflow Administration Console, after you select the import file, all the filenames within the import file gets suffixed with a number.

The issue lies with PrimeNG, who is aware of the issue and is working towards a solution (https://github.com/primefaces/primeng/issues/14971).

Name and Action Columns are not Working as Expected During Column Customization

Issue: While customizing the columns for forms, workflows, and notification templates, if you select all, the Name and Action columns get deselected from the column customization window, and are removed from the Forms, Workflows, and Notification Templates pages in the Workflow Administration Console. These columns are otherwise selected by default, non-editable, and meant to be displayed perpetually.

The issue lies with PrimeNG, who is aware of the issue and is working towards a solution (https://github.com/primefaces/primeng/issues/15023).

Workaround: The Name and Actions columns can be selected so that they are displayed in the Forms, Workflows, and Notification Templates pages.

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 MS SQL 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.
- 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

- “Adding Account Category to be Displayed Causes an Infinite Loop” on page 14
- “Searching Technical Role Mining Suggestions Does Not Filter the Suggestions” on page 14
- “Bulk Data Update Template Generation Fails on Windows When A User or Group is Specified for Notifications” on page 15
- “Permission Review Criteria is Not Saved Correctly when the Attribute Type is Boolean” on page 15
- “Governance Insights is Not Saving the Boolean Filter Correctly” on page 15
- “Business Role Requests Might Display Errors in Logs When You Use Custom Workflow as Approver in the Access Request Approval Policy” on page 15
- “Sorting by Risk on the Business Roles Page Does Not Work Correctly” on page 15
- “Bulk Data Update Template Generation Fails on Windows When A User or Group is Specified for Notifications” on page 15
- “REST API Documentation Not Rendering Correctly” on page 15
- “`client-strings.jar` Utilizes an Incorrect Path for the Files” on page 16
- “Resolved Workflow Issues” on page 16

Adding Account Category to be Displayed Causes an Infinite Loop

When you selected Account Category to be displayed on the Account Catalog page or the Insight Query page, the page rendered but then continued an infinite loop of REST API calls. This made the page unresponsive and prevented the user from navigating or performing other actions. This issue has now been fixed.

Searching Technical Role Mining Suggestions Does Not Filter the Suggestions

Entering any value in the Search field to filter Technical Role Mining Automatic Suggestions did not filter the results. This issue has been fixed.

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, failed when you specified a person or group in the **Notifications** field. This issue has been fixed.

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

Identity Governance did not save permission review criteria correctly when the attribute type was Boolean. This issue has been fixed.

Governance Insights is Not Saving the Boolean Filter Correctly

Identity Governance did not always filter correctly when you selected a Boolean attribute set to no (false) to filter results and ran queries. This issue has been fixed.

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

When you used a custom workflow for approving Business Role requests from Access Request, you might have seen unexpected errors even though the request did not fail. This issue has been fixed.

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

On the Business Roles pages, clicking on the Risk column heading sorts the list as expected.

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

This issue has been fixed. The bulk update template generation does not fail when users or groups are specified in the **Notification** field.

Users and group members on the notification list can also view the generated Bulk Data Update template on the Download area. However, if a user or a group member does not have an authorized Identity Governance role and can only access the Request interface, then they cannot access the Download area to download the generated template.

REST API Documentation Not Rendering Correctly

The framework for the REST API documentation was updated in a previous release resulting in issues such as page rendering, endpoint expandability, category ordering, and formatting in Identity Governance (`apidoc`) and Identity Reporting (`rptdoc`). This issue has been fixed.

`client-strings.jar` Utilizes an Incorrect Path for the Files

Identity Governance client string customization was not working. The `client-strings.jar` used for Identity Governance client string customization had an incorrect path. This issue has now been fixed.

Resolved Workflow Issues

- **Workflow will Fail if Lookup Value for an Attribute Contains Spaces or Special Characters or Is More Than 32 Characters** Attributes support values more than 32 characters including spaces, or contains spaces or special characters.
- **Unable to Export Forms or Workflows on Linux Systems** Forms or workflows from the Catalog area of the Workflow Administration Console can be exported on Linux systems also.
- **Unable to Create, Update, or Delete Forms or Workflows If Display Name is More Than 32 Characters.**

  The column size for the createdby, updatedby, and deletedby columns in the databases have been increased to 255 characters and the create, update, or delete form and workflow actions work 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 CyberRes by OpenText Support Website (https://support.cyberreshelp.com/) or email cyberressupport@microfocus.com (mailto:cyberressupport@microfocus.com).

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

Legal Notices