Identity Governance 3.7 Release Notes

March 2022

This version of Identity Governance 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 Micro Focus 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 website.

What's New

This release provides new and enhanced functional, infrastructure, and performance-related capabilities. It includes:

Access Request and Approval

This release includes the following enhancements:

- New Search option that optimizes the ability to search for items to request.
- Ability to group request items by categories and application groups to improve authorized requesters' experience of searching for request items.
- Improved administrators' experience in defining who should request access for whom.
- Inclusion of Potential SoD approver name in the Request timeline.
- Improved ability to browse for request items and enhanced approval process for technical roles and related permissions.
- Ability to specify conditional approval or denial options for select users or users matching specific criteria and ability to pre-authorize approval at each step level, rather than across the whole policy.
- New Search option that optimizes the ability to search for items to request and includes search by category.
- Enhanced ability to define Access Request policies. Specifically, it includes:
  - Ability to request access for users matching a query, business role members, and group members.
  - Ability to create a default request policy that can be configured to include all applications, permissions, and technical roles that are not assigned to other request policies.
- Ability to select Workflow as an approver.
- Ability to view reassignment details on the Approver page and on the request timeline view.

For more information about the enhanced access request policies and search capabilities, see "Administering Access Request " and "Instructions for Access Requesters and Approvers" in the *Identity Governance User and Administration Guide*.

Access Review

This release includes:

- A new out-of-the-box review type: Business Role Authorization Review. Authorized users can now review the authorizations defined by Business roles and request changes to the business authorization policy. Users can also create micro certifications for this review type.
- Enhanced review capability for business role definitions. Reviewers can now not only view permissions but can also view applications associated with the permissions when reviewing business role authorizations.
- Enhanced review scheduling capability for compliance with auditing requirements. When creating weekly and monthly review schedules, users can now specify the day of the week or month and set the time of the day for all intervals.
- Ability to view:
  - Who started a review in Governance Insights.
  - Who started a review in review overview and running review details.
  - Permission and account holders in user access and account reviews.

For more information about the new and enhanced review definitions, see "Creating and Modifying Review Definitions " in the *Identity Governance User and Administration Guide*.

Business and Technical Roles

This release includes improvements to the Identity Governance role mining and role detection processes. Business role mining and technical role mining now occur as background processes, increasing role mining performance and allowing users to perform other tasks within Identity Governance without interrupting role mining. Identity Governance also provides a complete history of technical role detections to improve auditing and reporting capabilities.

Data Collection, Publication, and Maintenance

This release includes the following enhancements related to data collection and publication, fulfillment, bulk update, and import optimization of large data sets:

- Improved ability to compare data collection and publication activities
- Enhanced ability to perform the bulk update.
- Optimized import of data policies.
- Ability to monitor changes to user, permission, or account attributes by specifying attribute changes as criteria for a publication data policy.
- Enhanced capability to collect and publish only the changes in application and application definition data sources since the last publication. Authorized users can also schedule change event collection by creating new schedules or updating the existing schedules.
- New collector templates to enable identities, accounts, and permissions collection from Workday to Identity Governance.
- Ability to collect identities, accounts, and permissions from SCIM 2.0 compatible applications and fulfill change requests.
- New collector and fulfillment templates to enable identity, account, and permission collection from Identity Manager using IDM drivers such as Azure, Workday, and SCIM drivers that support entitlement collection.
- The ability to configure Identity Governance to resume an interrupted concurrent archive from the point of interruption.

NOTE: Micro Focus provides templates with default scripts for collection and fulfillment to enable customers to configure the templates for their environments. The templates and scripts are meant as a starting point and do not address all use cases. Modification of scripts and customization of default templates will require additional knowledge of the connected systems. All modifications are the responsibility of the customer.

For more information about new templates and change event processing, see "Understanding the Variations for Identity Sources," "Understanding Collectors for Application Data Sources," and "Understanding Change Event Processing" in the *Identity Governance User and Administration Guide*.

Governance Overview and Insights

This release includes an optimized Governance Overview page that includes Key Performance Indicator (KPI) graphs for violations. The redesigned Governance Overview page includes the ability to create custom widgets based on custom metrics. Users can also personalize the dashboard view within Identity Governance.

This release also includes the ability to identify in Governance Insights whether a delegate made an access request.

For more information about the enhanced Overview page and widgets and Governance Insights, see "Monitoring Your Governance and Administration System" and "Analyzing Data with Insight Queries" in the *Identity Governance User and Administration Guide*.

Notifications

In addition to previous notifications, this release includes:

- Ability to notify reviewers when a review campaign has been completed.
- Ability to notify administrators about collection and publication failures and provide additional details about the failure on the data collection page.
- Ability to send email notification to review owners by default when you launch a review in the preview mode. You can also change the recipients as per your requirement.

Reports

This release includes new reports such as:

- Application Delta
- Fulfillment Target Changes
- Reviews with Deleted Stakeholders
- Access Request Policies - CSV
- Catalog Application Details - CSV
- Custom Form Changes - CSV
- Requestable Items - CSV
- Users in Business Role Grace Period - CSV

This release also includes a report that displays the merging rules set for the identity sources, along with the attribute mapping (Match rules) for each identity source. In addition, several reports have been enhanced to include details such as who started a review and whether items were reviewed by a delegate.

Separation Of Duties

This release includes new capabilities when creating Separation of Duties (SoD) policies. In addition to the required SoD condition, you can add expressions for user conditions and account conditions to specify that an SoD policy applies to specified users or unmapped accounts, such as users in specified locations, or accounts with a specified category. For more information, see "Understanding the Separation of Duties Policy Options" in the *Identity Governance User and Administration Guide*.

Workflow

This release enables you to create and monitor complex custom approval workflows as a preview feature. In addition to the previous ability to create default and custom request and approval forms, you can now create more complex workflows and associated forms for the request approval process. Specifically, it includes:

- Ability to create workflows and associated forms using Workflow Builder and Form Builder embedded in the Workflow service
- Ability to configure Workflow Engine that initiates and executes the approval process
- Ability to monitor the running workflows and notify approvers of pending workflows

---

IMPORTANT: The ability to edit custom workflows and create new advanced workflows using the Workflow Builder component of the Workflow Service is for preview and provided on an AS IS and AS AVAILABLE basis. We recommend that you do not use advanced workflows in your production environments. Workflow Service's advanced capabilities will be supported and available for general use in a future release.

For more information about workflow administration, see the *Workflow Administration Guide*.

IMPORTANT: Do not make changes to the default form in your Start activity. To ensure that proper integration happens between Identity Governance and your custom approval workflow process, use the default IGA approval request form in Workflow Administration Console. Using any other form for your approval workflow activity might result in unpredictable behavior because Identity Governance requires `entityType`, `entityId`, `igApprovalFlowdata`, `reason`, and `isAdd` fields.

Note that the IGA approval request form is different from the form available on the corresponding permission or application's Custom Forms tab in the Identity Governance catalog. The approval form displayed on the Custom Forms tab in the catalog when running the simulator is a specialized Identity Governance defined form used for approvals when the approver type is **Self**, **Supervisor**, **Item owners**, **Coverage maps**, or **Select users or groups**.

Miscellaneous

This release includes miscellaneous infrastructure, user experience, and performance-related fixes and enhancements. It includes:

- Improvements to the Identity Governance download processes. Data source emulation and test collection creation and download processes now occur as background processes. In addition, Identity Governance now streams the downloaded data directly from the databases to improve download performance.
- Improved customization and accessibility for better compliance with WCAG AA accessibility standards.
- Ability to send audit events to log files.
- Updated REST API documentation framework for both Identity Governance and Identity Reporting.

  NOTE: The REST API documentation URL for Identity Governance was changed in the 3.6.2 release. The file name in the URL was changed to `apidoc`. Use the https://*host name*:*port*/apidoc URL to access the API doc. For example, https://myservername.microfocus.com:8080/apidoc.

  To access the Identity Reporting REST API documentation, continue using `rptdoc` as the file name. For example, https://myservername.microfocus.com:8080/rptdoc.

Technical Requirements

For more information about the software and hardware requirements 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).

Pre-release: Development Will be Seen in the About page and in the Log

You will see `Pre-release: Development` next to the version number on the About page of Identity Governance and Identity Reporting, and in the catalina file during start-up. This will be removed 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.

JDBC Auditing is Not Supported

When enabling auditing within Identity Governance, Identity Reporting, or External Workflow for 3.7.0 on-premises release, CEF auditing via syslog to a supported Audit Server (ArcSight, Sentinel, or Splunk) is the *only* supported auditing means. The utilization of JDBC Audit Connector is currently a SaaS-only feature.

REST API Documentation Not Rendering Correctly

The framework for the REST API documentation was updated for this 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.

Mapping of Multiple values for Select Control is not Working Using flowdata.get or flowdata.getObject Functions

Issue: In workflows, for Select control, multiple values are not mapping when used with flowdata.get or flowdata.getObject function.

This will be fixed in a future release of the product. Alternately, you can use the Select Boxes control to add multiple values.

Error Message is Displayed on the Email-Based Approval Page For Users With Appropriate Permission

Issue: In the Workflow Administration Console, when a user tries to perform any operation on the Email-Based Approval page, the error message 'You are not authorized to perform this operation' is displayed, even though the user has appropriate permission for the page. This is happening because the user does not have permission to the Notification Templates page.

Workaround: To perform any operation successfully on the Email-Based Approval page, the user must have view permission to the Notification Templates page as well.

Warnings are Displayed in the Server Log When a Request is Reassigned or Returned

Issue: When a request is reassigned or returned using the email-based approval from the Workflow Administration Console, warnings are displayed in the server log.

This issue will be fixed in a future release of the product.

Required Data item Exceptions are Displayed in the Server Log When a Request is Approved or Denied Using Email-Based Approval

Issue: When a request is approved or denied using the email-based approval in the Workflow Administration Console, data item required exceptions are displayed in the server log.

This issue will be fixed in a future release of the product.

Notifications Are Not Sent When Any Action is Taken on a Request Using Email-Based Approval

Issue: In the Workflow Administration Console, when a request is approved, denied, reassigned, or rejected using the email-based approval, the success or failure email notifications are not sent as expected. As a result, the approval request remains in the same state.

Workaround: For the email notifications to work follow these steps:

1. In the Workflow Administration Console select **Configuration** > **Email Based Approval**.
2. Configure **Incoming Email Settings** and **Outgoing Email Settings**.
3. **Save**.
4. Restart the Tomcat server.

IDM Entitlement Connected Systems Fail to Display Error Messages When Entitlements Are Disabled

When a user entitlements are disabled but an administrator tries to add the user to any application, for example, Lotus Notes, as expected the user is not added to that application. However, no error message stating entitlement is disabled is displayed in the logs. This issue cannot be fixed because entitlements must be enabled for IDM entitlement connectors.

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

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

Workaround:

Ensure that the account status in the driver's entitlement configuration 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 Fail Without Communicating the Error to Identity Governance

Issue: When requests such as the assignable role for Workday request is sent to the IDM entitlement fulfiller, the fulfiller modifies the value of the LDAP Attribute DirXML-EntitlementRef. After modification it depends on Identity Manager to automatically send an entitlement modification event to the driver. If the driver fails to handle fulfillment requests, the error is reported to Identity Manager but Identity Manager does not report the error back to Identity Governance. Identity Governance assumes the request was fulfilled. However, after collection and publication, Identity Governance marks the status as verification failed.

Workaround: Access the driver logs to get more details about the error.

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

Issue: When configuring the IDM entitlement collectors or fulfillment target templates, test connection will fail if the user password contains a colon.

Workaround: Log into IDM iManager and exclude colons from admin accounts' password.

Technical Role Administrator Gets an Error When Analyzing SoD Violations for a New Technical Role

When the Technical Role Administrator creates a new technical role, then clicks **Analyze SoD Violations**, analysis fails and Identity Governance displays Denied access error message.

Archiving Data That Includes Photos to a Vertica Database Could Cause an Error

If you archive data to a Vertica database, and the entities (such as users or permissions) you want to archive include photos larger than 3 MB in size, the archive action will not be successful.

You can either:

- Replace existing photos with photos smaller than 3 MB
- Delete photos larger than 3 MB
- Archive data to the internal archive database
- Archive data to an external database other than Vertica

Unexpected Error When Accessing Application Default Forms or the Permission Default Forms tabs

Issue: When an authorized user selects **Policies > Access Request Policies** and clicks on the **Application Default Forms** or **Permission Default Forms** tab, Identity Governance *might* display an `Encountered unexpected error` message.

Workaround: Click the browser refresh icon to refresh the page or navigate to another page, then access the tabs again. If the problem happens every time you access these tabs, please contact Technical Support.

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

Though we support markdown for permission and application description, currently we do not have a markdown viewer for request forms. Because of this, 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 Makes User 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 know as curation) occurs which 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 which 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 happens 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.

Cannot Recognize Date Values that Are Not in Default Java Format

Issue: If a date attribute in your data source uses a non-Java format, Identity Governance does not recognize the data as a date. For example, if the `StartDate` attribute uses "YYYY/MM/DD" fixed-length format and you want to collect it in date format, the collection will show an error. Identity Governance uses only the default format for Oracle Java for date attributes.

Workaround: Use one of the following workarounds:

- Before collecting from the data source, "clean" the data by converting the attribute values to Java's default date format, which uses the number of milliseconds that have elapsed since midnight, January 1, 1970.
- Collect the value in string format so that you will be able to see the native value. This method also guarantees that the data does not have to be "clean" to be collected. For more information, contact Technical Support.

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 currently support localization for this text. To track most localization issues on the Form.io site, you can refer to Form.io bug 4283, Form.io bug 4431, and Form.io bug 4437 In addition, you can click here for more information.
- 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.
- 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.
- 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 Date/Time values appear as “Invalid” in Firefox. The issue lies with Form.io, who is aware of the issue and is working toward a solution.
- A custom form configured for multiple phone numbers displays only a single phone number field. 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.
- Using the JS editor to set a check box component to appear selected by default does not function as expected. 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

This release includes the following resolved issues.

Wrong Collection and Publication Status Displayed in Pop-Up Status Window

The Current Collection status pop-up window displays the correct status now.

Modify Technical Role Permissions Does Not Work Correctly When the Fulfiller is a Group

Change requests to modify technical role permissions during a review works correctly even when the fulfiller is a group.

Workday Permission Collection Might Take Significant Time

Micro Focus recommends that you work with Technical Support if you encounter any additional issues with your Workday permission collector.

In Custom Forms, the Templates Tab Cannot be Localized

In the Form Builder, the **Templates** tab of the **Edit Grid Component** window was not localized, because Form.io did not support localization for that text. With this release, text on this tab appears localized.

Accounts can be Incorrectly Considered Duplicates and Removed

In previous releases, if an account collector collected information from different sources, and if a user in one source and another user in another source had the same AccountID, Identity Governance considered the accounts to be duplicates, and removed all but one account. This release corrects the issue.

Request and Approval Page Sorts Item Only on the Current Page

Previously when you sorted items in the Request and Approvals page, only items on the current page would be sorted. With this release all listed items are sorted regardless of the page you view.

Completed Reviews Page Does not Maintain the Date Range

When the Review Administrator selects **Show Completed Reviews** to view the Completed Reviews page, Identity Governance maintains the date range unless the Review Administrator modifies the date range or selects ***User Name*** **> Clear Preferences** from the title bar drop-down menu.

Review Items are Going to the Escalation Queue Instead of the User Specified in the Coverage Map

For instances, where coverage map resolves the review item but not the reviewer, instead of stopping and returning no match, Identity Governance sends the review items to the next coverage map statement until it finds a resolution. If Identity Governance does not find a resolution in the coverage map statements, it sends the review items to the escalation reviewer (if defined) or to the review owner.

In a review definition, when self review is allowed, and coverage map resolves both review item and reviewer, Identity Governance sends the review items to the reviewer. However, when self review is not allowed and coverage map resolves both review item and reviewer, then Identity Governance sends the review items to the escalation reviewer (if defined) or to the review owner.

The Refresh Process is not Updating the Task Complete Count Column in the Review Instance Table

The **Refresh** link now updates values in the task count, and task complete count columns in the review instance table.

The Search Criteria is not Maintained when you Return to the Repository Page

In Identity Governance Reporting, the search criteria is now maintained, as expected, when searching the Repository, navigating away, performing other actions, and navigating back to Repository.

Incorrect Change Request Types Appear When Configuring Application Setup for Fulfillment

If you configure Application Setup for Fulfillment, and select Supported Change Request Types, the following two request types appeared in previous version of Identity Governance:

- Remove User from business role
- Modify Technical Role Permissions

These change request types now appear for only relevant fulfillment targets.

Contact Information

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

For support, visit the CyberRes Support Website (https://support.cyberreshelp.com/) or email cyberressupport@microfocus.com (mailto:cyberressupport@microfocus.com).

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

Legal Notices