Identity Governance and Administration As a Service Release Notes

April 2023

4.0 SaaS 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 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 (https://www.microfocus.com/documentation/identity-governance) website.

What's New

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

Activity Statistics Dashboard

The Activity Statistics dashboard presents a view to the customer about how the system is being used. The dashboard gives trends and summaries of various activities that are going on in the system.

Enhanced Identity Governance tracks more comprehensive user interactions and application events in all functional areas and enables authorized administrators to collect and download activity and entity usage metrics. Additionally, a new Activity Statistics tab on the Identity Governance dashboard enables authorized administrators to view and download overall activity statistics, summaries, and top five activities based on their selected date range and last collection.

For more information, see "Viewing Activity Statistics and Trends" in the *Identity Governance as a Service User and Administration Guide*.

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.

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

Customizable Headers and Menu Names

Authorized administrators can customize Access Request, Identity Governance, and Identity Reporting header background color, text color, banner image, and banner text to meet your unique branding requirements. Additionally, you can customize Access Request and Approval menu names and hide the Access Request Compare menu.

For more information about customization, see "Customizing Headers and Access Request and Approval Menu Names" in the *Identity Governance as a Service User and 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 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:

- 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 as a Service User and Administration Guide*.

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

Support for Upgraded Cloud Bridge

Identity Governance now supports an upgraded version of the Cloud Bridge which includes high-availability capabilities and enables Identity Center to automatically discover data centers. When your environment has been upgraded to the latest version of Identity Governance, work with your Customer Success team to download and configure your Cloud Bridge Agent for your on-premises (off-cloud) environment.

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 as a Service 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 as a Service 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:

- Activity Stream - CSV
- Activity Stream Aggregate
- Ad Hoc Audit Report - CSV
- Data Policies and Controls Overview - CSV
- Data Policies and Controls Details - CSV
- Separation of Duties Approval Policies Details - CSV
- Separation of Duties Policies Details - CSV

This release also includes enhancements to several other reports to improve usability and support required software upgrades to further align with security and compliance requirements.

Support for Identity Intelligence Dashboards and Reports

Identity Intelligence provides more detailed analytics dashboards and reports and includes the ability to build new dashboards and reports based on your business requirements. Identity Governance enables access to these more granular analytics dashboards and reporting by enabling integration with the Identity Intelligence service. The Identity Intelligence service will be available soon.

Miscellaneous

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

- Upgrades of third-party components to recent versions including upgraded Form Builder
- Identity Governance and Administration SaaS infrastructure improvements and upgrades

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 and Administration as a Service Technical Requirements*.

Browser Requirements

To log in to Identity Governance on their local devices, users must have one of the following browser versions, at a minimum:

Computers

- Apple Safari 16.1
- Google Chrome 103.0.5060.114
- Microsoft Edge Browser 103.0.1.1264.49
- Mozilla Firefox 15.5

iPad (iOS 12 and later)

- Apple Safari 15.5
- Google Chrome 101.0
- Mozilla Firefox 37

IMPORTANT: The browser must have cookies enabled. If cookies are disabled, the product does not work.

Supported Components and Products

- Cloud Bridge 1.8.1 and 1.8.4
- Form Builder 1.5.0
- Identity Manager 4.8.6
- Identity Reporting 7.0.1
- Workflow Console 1.0.6
- Workflow Engine 1.0.6.02

Supported Identity Manager Drivers and Packages

Identity Governance provides IDM entitlement application definition and application templates to collect account and permission entitlements from an on-premises Identity Manager environment. To successfully collect all accounts and permissions, the supported drivers must be running.

Find below a list of the Identity Manager and Identity Governance supported drivers.

- Drivers in Identity Manager 4.7.5 (https://www.netiq.com/documentation/identity-manager-47-drivers/) and 4.8.5 (https://www.netiq.com/documentation/identity-manager-48-drivers/) and later patched versions

- Identity Governance Assignment collection: MFIGASGMTCOL_1.0.0.20220110104142

Driver	Minimum Driver Version	Minimum Package Version
Active Directory	4.1.3.0	• NOVLADENTEX_2.5.7.20190610155012
Azure AD	5.1.4.0100	• MFAZUREENTL_1.0.2.20211118165327 • MFAZUREXROLE_1.0.2.20211125114229
Bidirectional	4.0.4.0	• NOVLEDIR2ENT_2.2.7.20211118165416
Groupwise REST	4.0.1.1	• NOVLGRPWRAEN_3.1.1.202112091738838
JDBC	4.2.2.0000	• NOVLJDBCBISN_2.0.0.20211208134901 • NOVLJDBCENTI_2.4.4.20211208135336 • NOVLORAINSYN_2.1.0.20211208135824 • NOVLSQSIDSYN_2.1.1.20211220115351 • NOVLPGSINSYN_2.1.1.20211220124959
Lotus Notes	4.1.2.0	• NOVLNOTEENT_2.4.1.20211118113748
SAP User Management	4.0.4.0	• NOVLSAPUFENT_2.3.5.20211217153914 • NOVLSAPUMIG_1.0.0.20211217153953
SCIM	1.0.1.0200	• NETQSCIMENT_1.0.1.20211223151040 • NETQSCIMBASE_1.0.1.20211223151032
Workday	1.3.0.0100	• NETIQWDENT_1.0.0.20210505165701

NOTE: Entitlements must be enabled for IDM entitlement connectors. When entitlements are disabled, IDM Entitlement connected systems will not display any error messages. When user entitlements are disabled, and an administrator tries to add the user to any application (such as Lotus Notes), though error message will not be displayed, the user will not added to that application.

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

You will see `Pre-release: Development` next to the version number on the About page of Identity Governance and Identity Reporting. This will be updated in a future release.

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.

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

MS Teams Collector Intermittently Fails to Collect Data

Issue: Sometimes while collecting data using the MS Teams collector the application times out and the collection fails. The following error message is displayed.
[com.netiq.iac.persistence.dcs.dce.thread.DataCollectionServiceThread] [IG-DTP] DaaS connector returned error during collection: Command failure: Type: find+chunked: [The parameter 'value' is missing in 'Graph API Response'].

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

For Multiple and Quorum Approver Type Group Addressees are Unable to Approve or Deny Workflows

Issue: When a workflow with an Approver Type as Multiple or Quorum has individuals as well as groups as addressees, in Identity Governance the workflow can be approved or denied by the individual user but fails when a member of the group approves or denies.

Workaround: While adding groups as addressees, add the individual IDs of the members of the groups instead of the group ID.

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. (OCTCR28E496183)

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 Fail Without Communicating the Error to Identity Governance

Issue: When a request, 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 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 for more details about the error.

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** tab or the **Permission Default Forms** tab, Identity Governance *could* display an `Encountered unexpected error` message.

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

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

- **Issue:** Calendar icon is missing from the Date/time component.

  Workaround: Click on the Date/Time text box to access the calendar widget and select a date.
- 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.
- When adding an HTML Element Component to a form, the content of the HTML element component is shown differently in Form Builder and in Preview. A meaningful message is displayed in Preview, whereas the JSON data is displayed in Form Builder. The message should be the same in both places.
- **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.

Resolved Form Builder Issues

- 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

- 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@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

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/legal.