Identity Governance and Administration as a Service Release Notes

April 2022

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 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 as a Service Documentation (https://www.microfocus.com/documentation/identity-governance-and-administration/igaas/) website.

What's New

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

- Ability to enable or disable new user creation when merging identities from multiple sources. Additionally, you can now also view merge histories. For more information see, "Understanding Publication Behavior" and "Viewing Merge Histories" in the *Identity Governance as a Service User and Administration Guide*.

- Separation of Duties (SoD) policies that include SoD approval policies that specify approval and denial criteria, including the ability to prevent users from submitting requests for specified combinations of permissions labeled as forbidden or "toxic". For more information, see "Assigning Separation of Duties Approval Policies " and "Designating an SoD Violation as Toxic in the *Identity Governance as a Service User and Administration Guide*.

> **NOTE:** This new capability changes Potential SoD Violations in Access Request, so the `GET` and `PUT` REST APIs for `psodvpolicy` are no longer part of the product.

- Integration with Workflow service (Workflow Administration Console) that enables you to create and monitor complex custom approval and fulfillment workflows for your Identity Governance and Administration (IGA) system. Specifically, authorized users can perform one or more of the following tasks:

    - Approve, deny, and fulfill change requests in Identity Governance using custom workflows

    - Select out-of-the box templates for custom approval workflows

    - Configure a new fulfillment target template to fulfill change requests using custom workflows

    - View workflow dashboard from the Identity Governance Overview page

    - Edit out-of-the box approval and fulfillment workflows and associated forms and create new forms and workflows using Workflow Builder and Form Builder embedded in the Workflow service

    - Monitor the running workflows and notify approvers of pending workflows

    For more information about enhanced Identity Governance approval and fulfillment capabilities, see "Using Workflows to Approve Requests " and "About Workflow Service Fulfillment" in the *Identity Governance as a Service User and Administration Guide*. For more information about the Workflow service, see the *Workflow Administration Guide*.

- Ability to select Technical Role owner as the reviewer for user access review that has technical role as the review item criteria

- Ability to collect data and fulfill change requests using Azure AD Microsoft Graph APIs. For more information, see "Collecting from Active Directory with Azure Active Directory" in the *Identity Governance as a Service User and Administration Guide*.

- New reports such as:

    - Custom Form Changes - CSV

    - Fulfillment Target Changes

    - Reviews with Deleted Stakeholders

    Additionally, the Account Ownership Report has been renamed as Account Ownership Statistics Reports, and Catalog Extended Attributes Report has been renamed as Extended Attribute Definitions.

- Miscellaneous infrastructure updates to improve deployment time and process, and updates to existing reports to provide additional governance capabilities.

Technical Requirements

This release requires, at a minimum, the following requirements.

- "Browser Requirements for Identity Governance" on page 3
- "Cloud Bridge Agent Requirements" on page 3
- "Supported Cloud Bridge Version" on page 3
- "Supported Identity Manager Drivers and Packages" on page 4

Browser Requirements for Identity Governance

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 12.1.12 - 15
- Google Chrome 80 - 94
- Microsoft Edge Browser 44 - 93
- Mozilla Firefox 74 - 92

iPad (iOS 12 and later)

- Apple Safari 13 - 15
- Google Chrome 78 - 94
- Mozilla Firefox 20 - 37

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

Cloud Bridge Agent Requirements

You must have administrator privileges to install the Cloud Bridge Agent.

- Hardware Requirements
    - CPUs: 4
    - Memory: 16 GB
    - Disk Space: 200 GB
- Operating System Requirements
    - Debian 10
    - RHEL 8.3
    - SUSE Linux Enterprise Server 15.1 or later patched version of 15.x
    - Ubuntu 18.04 LTS Server Edition or later
- Container Requirements
    - Docker 19.03.x or later
    - Podman 1.6.4

Supported Cloud Bridge Version

To collect data from on-premises data centers and fulfill change requests using Cloud Bridge-enabled collectors and fulfillers, at a minimum, you will need Cloud Bridge 1.6.2.

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 or later patched versions of 4.7.x (https://www.netiq.com/documentation/identity-manager-47-drivers/)
    - 4.8.5 or later patched versions of 4.8.x (https://www.netiq.com/documentation/identity-manager-48-drivers/)
- Identity Governance Assignment collection: MFIGASGMTCOL_1.0.0.20220110104142

Driver	Version	Package
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_3.1.1.202112091 73838
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

Driver	Version	Package
Workday	1.3.0.0100	◆ NETIQWDENT_1.0.0.2021050516570 1

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).

- "Reporting Issues" on page 5
- "Multiple Value Mapping with `flowdata.getObject()` Populates all Values in a Single Field" on page 6
- "Expressions In Workflow Rest Activity Does not Allow `//` in a Comment" on page 6
- "IDM Entitlement Connected Systems Fail to Display Error Messages When Entitlements Are Disabled" on page 6
- "IDM Entitlement JDBC Driver Fails to Verify Fulfillment After Successfully Inactivating an Account" on page 6
- "IDM Entitlement Fulfillment Requests Fail Without Communicating the Error to Identity Governance" on page 7
- "IDM Entitlement Collection and Fulfillment Test Connection Fails If User Password Contains a Colon" on page 7
- "Unexpected Error When Accessing Application Default Forms or the Permission Default Forms tabs" on page 7
- "Custom Forms Do Not Display Request Item Description in Bold Italics By Default" on page 7
- "Moving a User from One Business Role to Another Using Curation Causes the User to Lose Authorized Permissions" on page 7
- "Navigating Away from Unchanged Page Might Result in Erroneous Prompt to Save Changes" on page 8
- "Cannot Recognize Date Values that Are Not in Default Java Format" on page 8
- "Unresponsive Script Error in Firefox Can Occur When Clicking a User in the Certification Policy Violation Popup Window" on page 8
- "Third-party Issues" on page 8

Reporting Issues

The following issue appears in the Catalog Curated Data Details report:

- The Catalog Curated Data Details report does not display all attributes and values for all entities. For example, if you update attribute values for three users, then run the Curated Data Details report, the report correctly reflects that three users were curated, but does not display the attributes and values that were curated.

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, 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. Fill the values for the requested fields and launch the next approval form. The data mapped from the previous form using `flowdata.getObject()` fills 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 contain 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 Connected Systems Fail to Display Error Messages When Entitlements Are Disabled

When user entitlements are disabled, but an administrator tries to add the user to any application (such as Lotus Notes), as expected the user is not added to that application. However, no error message stating entitlement is disabled appears 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 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.

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, the test connection fails if the user password contains a colon.

Workaround: Log into IDM iManager and exclude colons from any administrator account passwords.

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 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 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.

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

◆ **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.

◆ 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.

◆ 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

User Access Review that Filters on Accounts No Longer Rolls up the Permissions

The permissions were not rolling up for User Access review when the review definition had account filters set, such as Last Login more than 90 days old. Now this issue has been fixed.

Add CC link was not Available on Email Notifications

In reviews, the Add CC link was missing on email notification templates where the name of the notification was modified and used in a review. This issue has now been fixed.

Reminder mails are Not sent to the Review Owner and Auditor as Scheduled

Previously reminder mails were not sent to the Review Owner and Auditor at the scheduled interval. Now the reminder mails are sent as per the schedule configured in the review definition.

Sorting by Application Name on an Account's Permission Tab fails with an Unexpected Error

This issue has now been fixed. The server REST API was modified to do special handling of the appDisplayName attribute when it is specified for sorting.

The Load Certificate Button Appears after a Collector or Fulfillment is Saved when Using Cloud Bridge

The Load Certificate button now correctly appears or is hidden on the collector or fulfillment target page based on the related service parameter.

Fulfillment to eDir or AD Fails with changeRequestItem not Found Error

Fulfillment is now successful.

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 failed and Identity Governance displayed Denied access error message. This issue has now been fixed.

Resolved Customer Administrator Authorization Issues

- In a previous release, customer administrator was unable to import email templates. This issue has now been fixed.

- In a previous release, customer administrator was unable to delete an application source. This issue has now been fixed.
- In a previous release, a customer administrator received denied access error when retrying a fulfillment error task. With this release, the issue no longer occurs.

Resolved Reporting Issues

- In a previous release, a selected data source was not used when running a report. The generated report and the Report Definition page in Identity Reporting reflected different data sources. With this release, this issue no longer occurs.
- In a previous release, the Review Details PDF erroneously displayed "undefined" as a filter to use as a Review Item in the report. With this release, this issue no longer occurs.
- In a previous release, under some scenarios, the account name did not appear in the Fulfillment Status and Closed Loop PDF. With this release, this issue no longer occurs.
- In a previous release, the Catalog Curated Data Overview report erroneously displayed the message, "This report contains no data for Catalog Data Update in the collected sources" if the entity contained data but had no curated records. With this release, if the entity contains data, but has no curated records for that entity, the report correctly displays the values of zero (0) for curated and the percent in the report.
- In a previous release, if you installed and ran the Catalog Curated Data Details report, it displayed (0) users, accounts, and permissions collected and curated. This issue has now been fixed.
- In a previous release, if you curated data, edited the Catalog Curated Data Details report to limit the number of curated items per section, then ran the report, the results were not limited as expected. This issue has now been fixed.
- In a previous release, the Fulfillment Status and Closed Loop PDF duplicated the results of each fulfillment request item in the status list. This issue has now been fixed.

Resolved Third-party Issues

- A custom form configured for multiple phone numbers displays only a single phone number field. This issue no longer occurs.
- In the Form Builder, text that appeared on various component tabs could not be localized, because Form.io did not support localization for this text. Affected text is now correctly localized.

Miscellaneous Resolved Issues

This release also includes infrastructure and SaaS operations related fixes such as the following resolved issues.

- In a previous release, SaaS Operations Administrator was unable to import email templates. This issue has now been fixed.
- In a previous release, in a clustered environment, Access Request flows did not move and threw a NullPointerException. This issue has now been fixed.

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.