

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

- ◆ [“What’s New” on page 1](#)
- ◆ [“Technical Requirements” on page 2](#)
- ◆ [“Known Issues” on page 4](#)
- ◆ [“Resolved Issues” on page 8](#)
- ◆ [“Contact Information” on page 9](#)
- ◆ [“Legal Notices” on page 9](#)

What’s New

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

- ◆ When creating Separation of Duties (SoD) policies, in addition to SoD conditions, you can also use expressions to add user and account conditions. For example, you can now 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*

- ◆ You can now monitor attribute changes for all collected and curated items. Earlier, data policies detected only attributes that changed during curation (bulk update).

- ◆ Identity Governance now prevents collection and publication failure notifications from being sent to deleted users and groups. The application also displays the deleted users and groups with a strikethrough.
- ◆ Support for collection and fulfillment using Identity Manager drivers. Identity Manager Standard Edition (SE) customers can now use Identity Governance to collect accounts and permissions and fulfill change requests.

For more information about new templates, see [“Understanding the Application Definition Template”](#) and [“Understanding Collectors for Application Data Sources”](#) in the *Identity Governance User Guide*.

- ◆ Code changes to support ability to create complex approval workflows in a future release.

Technical Requirements

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

- ◆ [“Browser Requirements for Identity Governance”](#) on page 2
- ◆ [“Cloud Bridge Agent Requirements”](#) on page 2
- ◆ [“Supported Cloud Bridge Version”](#) on page 3
- ◆ [“Supported Identity Manager Drivers and Packages”](#) on page 3

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 (<https://www.netiq.com/documentation/identity-manager-47-drivers/>) and 4.8.4 (<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	◆ NOVLGRPWAEN_3.1.1.20211209173838
JDBC	4.2.2.0000	◆ NOVLJDBCBSIN_2.0.0.20211208134901 ◆ NOVLJDBCENTI_2.4.4.20211208135336 ◆ NOVLORAINSYN_2.1.0.20211208135824 ◆ NOVLQSIDSYN_2.1.1.20211220115351 ◆ NOVLPGSINSYN_2.1.1.20211220124959

Driver	Version	Package
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

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 \(https://www.microfocus.com/en-us/support\)](https://www.microfocus.com/en-us/support).

- ♦ “Pre-release: Development Will be Seen in the About page and in the Log” on page 5
- ♦ “IDM Entitlement Connected Systems Fail to Display Error Messages When Entitlements Are Disabled” on page 5
- ♦ “IDM Entitlement JDBC Driver Fails to Verify Fulfillment After Successfully Inactivating an Account” on page 5
- ♦ “IDM Entitlement Fulfillment Requests Fail Without Communicating the Error to Identity Governance” on page 5
- ♦ “IDM Entitlement Collection and Fulfillment Test Connection Fails If User Password Contains a Colon” on page 5
- ♦ “Technical Role Administrator Gets an Error When Analyzing SoD Violations for a New Technical Role” on page 6
- ♦ “Archiving Data That Includes Photos to a Vertica Database Could Cause an Error” on page 6
- ♦ “Unexpected Error When Accessing Application Default Forms or the Permission Default Forms tabs” on page 6
- ♦ “Custom Forms Do Not Display Request Item Description in Bold Italics By Default” on page 6
- ♦ “Moving a User from One Business Role to Another Using Curation Makes User Lose Authorized Permissions” on page 6
- ♦ “Navigating Away from Unchanged Page Might Result in Erroneous Prompt to Save Changes” on page 7
- ♦ “Cannot Recognize Date Values that Are Not in Default Java Format” on page 7
- ♦ “Unresponsive Script Error in Firefox Can Occur When Clicking a User in the Certification Policy Violation Popup Window” on page 7
- ♦ “Third-party Issues” on page 7

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.

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) (<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.

- ◆ [“Workday Permission Collection Might Take Significant Time” on page 8](#)
- ◆ [“Wrong Collection and Publication Status Displayed in Pop-Up Status Window” on page 8](#)
- ◆ [“Modify Technical Role Permissions Does Not Work Correctly When the Fulfiller is a Group” on page 9](#)

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.

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.

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/) (<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) (<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/) (<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 <http://www.microfocus.com/about/legal/>.

© Copyright 2022 Micro Focus or one of its affiliates.

