

Identity Governance 3.7.3 Release Notes

December 2022

This version of Identity Governance and Administration on-premises release includes new features and enhancements provided in the 3.7.1 (April) and 3.7.2 (September) SaaS releases. It also 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 \(https://www.microfocus.com/documentation/identity-governance\)](https://www.microfocus.com/documentation/identity-governance) website.

- ◆ “What’s New” on page 1
- ◆ “Technical Requirements” on page 4
- ◆ “Known Issues” on page 4
- ◆ “Resolved Issues” on page 12
- ◆ “Contact Information” on page 15
- ◆ “Legal Notices” on page 15

What’s New

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

- ◆ “Access Request and Approval” on page 2
- ◆ “Access Reviews” on page 2
- ◆ “Data Collection and Fulfillment” on page 2
- ◆ “Data Policies” on page 2
- ◆ “Dashboards” on page 3
- ◆ “Reporting” on page 3
- ◆ “Separation of Duties” on page 3

- ◆ [“Workflow” on page 3](#)
- ◆ [“Miscellaneous” on page 4](#)

Access Request and Approval

New out-of-the-box workflow templates for generic and specific Identity Governance access requests

Access Reviews

- ◆ New review type that provides the ability to define and review an organization’s technical role definitions
- ◆ Ability to select Technical Role owner as the reviewer for user access review that has technical role as the review item criteria

Data Collection and Fulfillment

- ◆ 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 User and Administration Guide*.
- ◆ Ability to configure multiple non-merging change event identity sources. For more information, see [Collecting from Identity Sources with Change Events](#) in the *Identity Governance User and Administration Guide*.
- ◆ New collector and fulfillment target templates that provide the:
 - ◆ Ability to collect accounts and permissions to access organizations, teams, and repositories from GitHub using respective new REST GitHub collector templates.
 - ◆ Ability to add and remove members from a GitHub organization or a team, or add and remove collaborators from a GitHub repository using a new REST GitHub fulfillment template.
 - ◆ Ability to collect team and channel permissions from Microsoft Teams using a new MS Teams Permission collector template.
 - ◆ Support for fulfillment using new JDBC Generic, Oracle, PostgreSQL, and SQL Server fulfillment target templates.
 - ◆ New REST Generic fulfillment template that supports OAuth 2.0 and provides the ability to fulfill any request for a REST-based application using REST endpoints. It has replaced the previously provided REST Service fulfillment template.
 - ◆ Ability to collect data and fulfill change requests using Azure AD Microsoft Graph APIs.

For more information, see [Understanding Variations for Application Sources](#) and [Understanding Service Desk and Other Fulfillment Targets](#) in the *Identity Governance User and Administration Guide*.

Data Policies

- ◆ Enhanced data policy and governance control user interface and ability to monitor identity lifecycle events such as joiners, leavers, and movers using default policies. For more information, see in the *Identity Governance User and Administration Guide*.
- ◆ Ability to use multiple remediation actions including workflow for data policy violations.

Dashboards

Ability to download custom widget data from the Governance dashboard. For more information, see [“Downloading Custom Governance Widget Data”](#) in the *Identity Governance User and Administration Guide*.

Reporting

Miscellaneous updates to existing reports and following new reports:

- ◆ Approval Policy Definitions – CSV
- ◆ Custom Form Changes - CSV
- ◆ Fulfillment Target Changes
- ◆ Reviews with Deleted Stakeholders

Separation of Duties

- ◆ Enhanced Separation of Duties (SoD) policy that supports the four-eyes principle and allows for a multiple-step approval process for SoD violations. For more information, see [Creating and Managing Separation of Duties Policies](#) in the *Identity Governance 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 SoD Approval Policies”](#) and [“Creating an SoD Approval Policy for Toxic SoD Violations”](#) in the *Identity Governance 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.

Workflow

Enhanced 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
- ◆ Utilize out-of-the-box workflow templates for generic and specific Identity Governance access requests and fulfillment 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
- ◆ Audit forms, workflows, and email notifications related to create, update, and delete operations

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 workflows, see [Workflow Service Administration Guide](#).

Miscellaneous

Miscellaneous security, compliance, performance, and monitoring related infrastructure updates to provide additional governance capabilities

Technical Requirements

For more information about the software and hardware requirements for this release of Identity Governance, supported upgrades, 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>).

- ◆ [“String Customization is Not Working for Access Request” on page 5](#)
- ◆ [“Sorting on the Default Forms Tabs of Access Request Policies Page Does Not Work Correctly” on page 5](#)
- ◆ [“expirationDate and effectiveDate Attributes Are Not Supported” on page 5](#)
- ◆ [“Error Starting Micro-Certification Review for Technical Role Assigned to Users Review Certification Policy Violations” on page 5](#)
- ◆ [“OSP Servers Fail to Start when Identity Governance 3.7.3 and OSP 6.6.1 is Installed on Some RHEL 8.x Systems” on page 6](#)
- ◆ [“MS Teams Collector Intermittently Fails to Collect Data” on page 6](#)
- ◆ [“MS Teams Collection Fails with the Error “Failed to execute backend request.”, While Collecting Team Members” on page 6](#)
- ◆ [“IDM Entitlement Collection and Fulfillment Test Connection Fails If User Password Contains a Colon” on page 6](#)
- ◆ [“IDM Entitlement JDBC Driver Fails to Verify Fulfillment After Successfully Inactivating an Account” on page 7](#)
- ◆ [“IDM Entitlement Fulfillment Requests Fail Without Communicating the Error to Identity Governance” 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](#)
- ◆ [“REST API Documentation Not Rendering Correctly” on page 8](#)
- ◆ [“JDBC Auditing is Not Supported” on page 9](#)

- ♦ [“A Warning Can Appear When Upgrading Identity Governance and Enabling Auditing During Installation”](#) on page 9
- ♦ [“Workflow Issues”](#) on page 9
- ♦ [“Third-party Issues”](#) on page 11

String Customization is Not Working for Access Request

Customizing Access Request strings does not work as expected. This issue will be fixed in a future release. Meanwhile, instead of creating a file with only the entries you want to update as described in [“Customizing Strings for Identity Governance”](#), make the necessary changes in the file that contains all the entries (for example: `CxRsrc_en.properties`), then create the custom `.jar` file with the updated properties file.

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

Issue: On the Application Default Forms and Permission Default Forms tabs of Access Request Policies page, clicking on column headings does not sort the list as expected.

This will be fixed in a future release.

expirationDate and effectiveDate Attributes Are Not Supported

Issue: The REST API documentation for requesting a Permission: `POST /request/request` incorrectly includes following attributes:

- ♦ `expirationDate`
- ♦ `effectiveDate`

These two attributes are not supported at this time. They are for an upcoming feature in Identity Governance. Utilizing these attributes in your API REST call might cause inconsistencies in the database.

IMPORTANT: If you are currently utilizing them, *stop immediately and remove them from your code.*

Error Starting Micro-Certification Review for Technical Role Assigned to Users Review Certification Policy Violations

Issue: Micro Certification remediation for items detected to be in violation of the Technical Role Assigned to Users Certification Policy results in error.

Workaround: Run the associated user access review and make sure authorized users review items, make decisions, approve decisions, and complete review run.

IMPORTANT: Currently we do not support technical role revocation using micro certification reviews. This issue will be addressed in a future release. We recommend that you do not attempt to use micro certifications remediation for technical role assignments related violations.

OSP Servers Fail to Start when Identity Governance 3.7.3 and OSP 6.6.1 is Installed on Some RHEL 8.x Systems

Issue: For some RHEL 8.x systems, OSP is not starting because of connection issue with the database.

NOTE: Before applying the workaround, we recommend you read the [RHEL documentation \(https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator\)](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-encryption-using_the_random_number_generator) for more information on random number generators.

Workaround: Modify the following entries in the `java.security` file of the JRE that Tomcat is utilizing:

- ◆ Replace `securerandom.source=file:/dev/random`
with
`securerandom.source=file:/dev/./urandom`
- ◆ Replace `securerandom.strongAlgorithms=NativePRNGBlocking:SUN`
with
`securerandom.strongAlgorithms=SHA1PRNG:SUN`

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."}}
```

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.

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.

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 \(https://support.mozilla.org/en-US/kb/warning-unresponsive-script?cache=no\)](https://support.mozilla.org/en-US/kb/warning-unresponsive-script?cache=no).

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 formatted or aligned.

This will be fixed in a future release.

JDBC Auditing is Not Supported

When enabling auditing within Identity Governance, Identity Reporting, or External Workflow for 3.7.x on-premises release, CEF auditing via syslog to a supported Audit Server (ArcSight, Sentinel, or Splunk) is the *only* supported auditing method. The utilization of JDBC Audit Connector is currently a SaaS-only feature.

A Warning Can Appear When Upgrading Identity Governance and Enabling Auditing During Installation

Issue: If you use the Identity Governance installer to enable auditing for one or more of the following modules during an upgrade — DaaS WAR, DTP WAR, and Workflow WARs— a “connection refused” warning for syslog audit appears when you start Tomcat. Configuration values set for these modules during the upgrade revert to the default values, and values you set during installation are not saved.

Workaround: Perform the following procedure after installation completes:

- 1 Log in to Identity Governance as a Global Administrator.
- 2 Select **Configuration > Audit Enablement**.
- 3 Correct and save the audit target settings for the DaaS WAR, DTP WAR, and/or Workflow WAR.

NOTE: Do not make changes to the **cache-dir** and **cache-file** settings. They contain events that could not be sent to the syslog server. After you correct the syslog host and port, as well as any keystore settings, Identity Governance will send those cached events to the syslog server.

Workflow Issues

Multiple Values for SSO Client IDs Causes System Errors

Issue: SSO Client IDs should have the same value. System errors are caused when an administrator:

- ♦ Changes the password for the External Workflow SSO client on the External Workflow tab of the Identity Governance Configuration Update (ConfigUpdate) utility
- ♦ Installs External Workflow separately from Identity Governance (**not currently supported**) and does not utilize the same SSO password value that was used during Identity Governance installation

Workaround: To update the additional SSO Clients:

- 1 [Launch the Identity Governance Configuration Utility \(ConfigUtil\) in the console mode under the guidance of Technical Support.](#)
- 2 Type the following commands:

```
sp com.netiq.iac.standaloneworkflow.clientPass %value%
sp com.netiq.workflow.clientPass %value%
```

3 Type `exit` to exit console mode and the Configuration utility.

4 [Restart Tomcat](#).

NOTE: If the ConfigUpdate utility was utilized to update the SSO password, [launch ConfigUtil](#) and type `sp com.netiq.workflow.clientPass %value%` where `%value%` is the SSO Password value that was set when updating the values in the ConfigUtil.

Unable to Search for Workflows and Incorrect URLs when External Workflow Engine is Installed on a Remote Server

Issue: Generally, in distributed environment scenarios, we support installing services like OSP and Identity Reporting on a different Tomcat Server than the server where Identity Governance is installed. However, when External Workflow Engine is installed on a remote server with Identity Governance 3.7.0 and 3.7.3, the following issues occur:

- ◆ Searching for a workflow, when specifying **Workflow** as an approver in an Approval Policy, displays an error message
- ◆ The following links point to incorrect URLs:
 - ◆ Workflow Dashboard link on the Identity Governance Home drop-down menu
 - ◆ Form Builder links on the Custom Forms tab of the Identity Governance catalog
 - ◆ Identity Governance link on the Workflow Service Home drop-down menu

Workaround: Install the External Workflow Engine on the same Tomcat Server as Identity Governance. These issues will be resolved in a future release.

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.

Workflows Created Using System Templates Reports Exceptions in the Server Logs

If email-based approval is enabled on Workflow Service, the following data item exceptions are reported in the server log file when a user grants permission via email:

```
com.novell.soa.af.DataItemException: Dataitem [formHeader] is required.
```

```
com.novell.soa.af.DataItemException: Dataitem [fulfillmentInstructions] is required.
```

```
com.novell.soa.af.DataItemException: Dataitem [requesterFeedback] is required.
```

These exceptions occur in workflows created using system templates, however, they do not cause any loss of functionality and may be ignored. The permission is successfully granted when the user approves the request.

This issue will be resolved in a future release.

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 \(https://github.com/formio/formio.js/issues/4666\)](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 \(https://github.com/formio/formio.js/issues/4666\)](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

- ◆ [“Unexpected Error When Accessing Application Default Forms or the Permission Default Forms tabs” on page 12](#)
- ◆ [“Users Automatically Logged Out When Active in the Product” on page 12](#)
- ◆ [“System Errors During Collection Do Not Appear in the Product” on page 12](#)
- ◆ [“User Access Review that Filters on Accounts No Longer Rolls up the Permissions” on page 13](#)
- ◆ [“Add CC link was not Available on Email Notifications” on page 13](#)
- ◆ [“Reminder mails are Not sent to the Review Owner and Auditor as Scheduled” on page 13](#)
- ◆ [“Sorting by Application Name on an Account's Permission Tab fails with an Unexpected Error” on page 13](#)
- ◆ [“The Load Certificate Button Appears after a Collector or Fulfillment is Saved when Using Cloud Bridge” on page 13](#)
- ◆ [“Fulfillment to eDir or AD Fails with changeRequestItem not Found Error” on page 13](#)
- ◆ [“Technical Role Administrator Gets an Error When Analyzing SoD Violations for a New Technical Role” on page 13](#)
- ◆ [“Resolved Reporting Issues” on page 13](#)
- ◆ [“Resolved Workflow Issues” on page 14](#)
- ◆ [“Resolved Third-party Issues” on page 14](#)
- ◆ [“Miscellaneous Resolved Issues” on page 15](#)

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

When an authorized user selected **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. This issue has been fixed.

Users Automatically Logged Out When Active in the Product

Identity Governance could sometimes automatically log out users actively working in the product. This issue no longer occurs, and users are automatically logged out only if they are inactive for the specified session timeout period.

System Errors During Collection Do Not Appear in the Product

Prior to this release, Identity Governance displayed error messages that did not describe errors that caused failed collections. With this release, Identity Governance provides details about errors that cause collections to fail.

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 Reporting Issues

- ◆ In a previous release the Catalog Curated Data Details report did not display all attributes and values for all entities. This issue has been fixed.
- ◆ 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 Workflow Issues

Workflows with a Loop Displays Flowdata Incorrectly and gets the Error "too much recursion" in the Browser Console

Previously, workflows with a loop did not do the post activity mapping for activities which fell within the loop and caused the error “too much recursion” in the browser console. The error is no longer observed in the browser console and the `flowdata` data tree has the post activity of the mapped activity within the loop.

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

When using request workflows, server logs were displaying data item exceptions when a request was approved or denied using email-based approval. The exceptions are no longer displayed for built-in request workflows.

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

Issue: Warnings are no longer observed in the server log when a reassigned request is approved.

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

Issue: Notifications are sent successfully when a request is approved, denied, reassigned, or rejected using the email-based approval.

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

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment link on each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com (<mailto:Documentation-Feedback@microfocus.com>).

For detailed contact information, see the [Support Contact Information Web site \(https://www.microfocus.com/en-us/support\)](https://www.microfocus.com/en-us/support).

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

© Copyright 2022 Micro Focus or one of its affiliates.

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.

