Identity Governance 3.6 Release Notes

February 2020

Identity Governance 3.6 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 NetIQ Identity Governance forum (https://www.netiq.com/communities/) on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

For more information about this release and for the latest release notes, see the Identity Governance Documentation (http://www.netiq.com/documentation/identity-governance/index.html) Web site.

What's New in 3.6

The following outlines the key features and functions provided in this release:

Identity Governance 3.6 Limited Access License included with Identity Manager Per Managed Identity License

Qualified Identity Manager customers who have a limited access license for Identity Governance are entitled to install and use the identity catalog based features of Identity Governance to create and manage identities, accounts, groups, applications, permissions, and business roles. All other features are provided on a preview basis and cannot be fully enabled or used in production without the purchase of a full "per managed identity" license for Identity Governance 3.6 or later.

Access Review and Certification Enhancements

This release includes the following enhancements:

- Improved reviewer experience and enhancements for compliance administrator to define and configure review processes. For example, there is now a "Save-as" capability for review definitions.
- Ability to review business role definition. Authorized users can conduct periodic and ad-hoc reviews of each business role by requiring a responsible person to review the role's general information (name, description, etc.), membership criteria, and access authorizations.
- Enhanced self-review policy
- Enhanced multistage review

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

Technical Role Assignment Capabilities

This release introduces the ability to directly assign technical roles to users. This simplifies the process of ensuring users have the correct access by allowing access assignments to be governed based on business functions instead of low level permission assignments. This includes being able to review user access based on technical role assignments and being able to reconcile a user's actual access against their technical role assignments.

Application Onboarding, Collection, and Publication Enhancements

This release makes it easier to onboard applications into the governance system and includes the following enhancements:

- Separates the process of defining an application in the governance system from collecting the data for the application. This enables a business user to drive the process and also includes the ability to collect application information directly from a CMDB system.
- Ability to collect the authorization data for multiple applications by defining and running a single Application Data Collector.
- Ability to merge manually created application with collected application
- Ability to edit application attributes
- Ability to add custom attributes to applications

For more information, see "Collecting Applications and Application Data " in the *Identity Governance User and Administration Guide*.

Database Maintenance Enhancements

This release includes the ability to schedule archiving, clean up operations data, and perform operations tasks concurrently with archiving. For more information, see "Database Maintenance" in the *Identity Governance User and Administration Guide*.

Data Policy Enhancements

This release includes the ability to schedule detection of data policy violations and support for detecting changes to entities and attributes. For more information, see "Creating and Managing Data Policies " in the *Identity Governance User and Administration Guide*.

Governance Insights Enhancements

This release includes the following enhancements to Insight Queries:

- Ability to create a single complex filter expression using both the entity type and cross references
- Ability to use additional cross reference filters for identities, groups, permissions, technical roles, and business roles
- Support for partial string search

For a more information, see "Analyzing Data with Insight Queries" in the *Identity Governance User and Administration Guide* and *Identity Governance Insight Query Technical Reference*.

Enhanced Download Capability

In addition to downloading roles and definitions, you can now download the identities, accounts, groups, and permissions in the catalog as CSV files. Additionally, to enable you to continue performing tasks even as the entities, roles, or definitions are being downloaded, Identity Governance saves the CSV file to a download page from where you can download the saved file at a later time.

TIP: For description of the internal ENUM values from the database that might appear in the CSV files, see *Identity Governance ENUM Values Technical Reference*.

One SSO Provider (OSP) Installer Changes

This release contains the following changes for the OSP installer:

- If Identity Governance is external to the OSP server, the installer asks for the connection information and for the JDBC driver file for the remote database. For more information, see "One SSO Provider (OSP) Installation Worksheet" in the *Identity Governance 3.6 Installation and Configuration Guide*.
- The installer now asks if the bootstrap administrator is file-based for LDAP-based. For more information, see "Using the Bootstrap Administrator" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Support for a Reverse Proxy Server Sending Email Notifications

This release supports email notifications if you are using a proxy server. For more information, see "Enabling Email Notifications with a Load Balancer or a Reverse Proxy" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Support for a Reverse Proxy Server with Identity Reporting

This releases contains the ability to configure a reverse proxy server to obtain the current reports from the Micro Focus content site. For more information, see "Configuring a Proxy Server for the Identity Reporting Server" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Audit Enhancements

This release contains improved audit messages with more detailed descriptions and correlation IDs. Plus, we added auditing for more background processes. For a detailed list of the audit events, see *Identity Governance Audit Events* and *OSP Audit Events*.

Identity Governance Localization Updates

This release supports localizing the user's preferred language to Norwegian. For more information, see "Localizing the Preferred Language of the User" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Identity Governance Application Behavior Changes after Tokens Expire

This release changes the behavior of the Identity Governance application when tokens expire. If you are logged in to the Identity Governance application and your access token times out, you see a popup message that requires you to re-authenticate or log out of the application. If you re-authenticate, Identity Governance displays the login screen in a separate window or browser tab. You must log in again to continue working in the

Identity Governance application. These changes were made to increase the security of the authentication process. For more information, see "How to Log in to Identity Governance" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Because of these security changes, If you are using OSP and are not integrated with Identity Manager you must manually extend the schema for OSP or else authentication will fail. For more information, see Extending the Schema for OSP in the Identity Service not Part of Identity Manager.

Identity Governance Integrates with Access Manager

This release allows you to integrate Identity Governance with Access Manager as your authentication service instead of OSP. For more information, see "Integrating Access Manager with Identity Governance" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Configuration Update Utility Updates

This release contains an updated Configuration Update utility that contains the following changes:

- You can run the Configuration Update utility in console mode or in the default mode. The console mode allows you to use property names to change settings in Identity Governance. For more information, see "Using the Identity Governance Configuration Update Utility" in the *Identity Governance 3.6 Installation and Configuration Guide*.
- You can change the refresh rate of public clients' token. If you users use a browser-based authentication, you can change the new setting of **Public client refresh token lifetime** depending on the security needs of your environment.

Reporting Enhancements

This release includes several enhancements including the following:

- Enhanced look and feel
- New reports such as Business Role Assignment Coverage, Business Role Assignment Coverage - CSV, and Reconciliation - CSV
- Ability to save reports as new reports

Miscellaneous Enhancements

In addition to the above new features and enhancements, this release also includes:

- Ability to view change request date in Fulfillment tabs
- Ability to specify what certification policies should run detection as part of the schedule
- Automated role mining option for business role mining
- Ability to view application name in business role authorized permissions quick info and in edit view
- Ability to update owners of technical roles using bulk action
- Ability to disable review notifications
- Ability to control how many metric collection can be collected simultaneously

- Support for Active Directory Federation Services (AD FS)
- Scheduling and performance improvements to Identity Governance capabilities such as automatic generation of change requests in high volume clustered environments and certification policy violation calculations

System Requirements

This release requires the following minimum components:

- Operating System
  - Red Hat Enterprise Linux (RHEL) 8.0 (64-bit)
  - SUSE Linux Enterprise Server (SLES) 15.1
  - Microsoft Windows Server 2016

  IMPORTANT: Before installing Identity Governance, apply the latest operating system patches.
- Database
  - Microsoft SQL
    - MS SQL 2017
    - MS SQL JDBC driver 7.2.2
  - PostgreSQL
    - PostgreSQL 11.5
    - PostgreSQL JDBC driver 42.2.6
  - Oracle
    - Oracle 18c
    - Oracle 19c
    - Oracle JDBC driver `ojdbc8.jar`
  - Vertica
    - Vertica 9.2.1
    - Vertica JDBC driver 9.2.*x*
- Application Server
  - Apache Tomcat 9.0.22
  - Download from the Apache Tomcat (https://tomcat.apache.org/) website
- Authentication service
  - OSP
  - Access Manager
  - OSP from Identity Manager
- LDAP authentication server
  - Microsoft Active Directory
  - eDirectory 9.2

- Identity Manager 4.7.3
- Identity Manager 4.8

- Java Runtime Environment (JRE) Zulu JRE 8u222 from Azul, either the JRE or the JDK
- ActiveMQ 5.15.9
- A supported Web browser

NOTE: To fully integrate Identity Governance 3.6 features with NetIQ Identity Manager, you must have NetIQ Identity Manager 4.7.3, at a minimum. For Single Sign On (SSO) between Identity Governance 3.6 and NetIQ Identity Manager 4.8, you must have OSP 6.3.6 available in 4.7.*x* patch and later versions of NetIQ Identity Manager, at a minimum.

The following components are optional:

- NetIQ Identity Reporting
- NetIQ Identity Manager
- Audit Server

NOTE: Identity Governance requires the `igops` schema to have the additional privileges of `create public synonym` and `drop public synonym`.

For detailed information about hardware and software requirements for Identity Governance, see "Hardware and Software Requirements" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Installing or Upgrading Identity Governance

For your convenience, NetIQ provides sample installation scripts to help you install components needed for Identity Governance, such as Tomcat, ActiveMQ, PostgreSQL, and OSP. To view the install scripts, download either of the following Zip files: Identity Governance Sample Installation Scripts - Linux or Identity Governance Sample Installation Scripts - Windows on the Identity Governance Documentation (http://www.netiq.com/documentation) Web site.

NOTE: NetIQ no longer provides Tomcat, ActiveMQ or PostgreSQL software as part of the Identity Governance release.

You can upgrade to Identity Governance 3.6 from Identity Governance 3.5.1. As part of the upgrade process you must also migrate data since some of the collector templates and database tables and views have changed in this release. For more information, see "Upgrading Identity Governance" in the *Identity Governance 3.6 Installation and Configuration Guide*.

IMPORTANT: Ensure you have the DNS names to identify server hosts before beginning the upgrading procedure. Because of new standards-based authentication, using IP addresses might not work correctly in all circumstances. The side effect is that the OSP integration with Identity Governance and Identity Reporting will not work correctly in these circumstances.

If you installed the current or previous version of Identity Governance using IP addresses, you must replace the IP addresses with the fully qualified DNS names for these hosts in several configuration files. You can do this either before or after the upgrading procedure. For more information, see "Changing Host File IP Addresses to DNS Names" in the *Identity Governance 3.6 Installation and Configuration Guide*.

If you are upgrading and changing database platforms, you cannot migrate your existing data to the new platform. For example, if you are running Identity Governance with PostgreSQL as your database and you plan to upgrade and use Microsoft SQL Server as your database, your existing data is not migrated to the new database.

For more information about the supported versions of Identity Governance components, see "System Requirements" on page 6.

Installing Identity Governance

If you have not previously installed Identity Governance or want to create a new environment, see "Planning to Install Identity Governance" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Upgrading from a Previous Version

Existing customers can upgrade to this version after preparing their current environment for a successful migration of data to the new version. For information about the upgrade process, see "Upgrading Identity Governance" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Installing the Custom Collector SDK

The NetIQ Custom Collector SDK helps with custom collector and fulfillment template creation and maintenance. The Custom Collector SDK is available as a separate download package on the Identity Governance download page.

1. Go to the Identity Governance page on the NetIQ download link from your sales representative.
2. Download `identity-governance-3.6-custom-connector-toolkit.zip`.
3. Extract the files for the operating system you have.
4. Locate and run the `idgov-sdk` application for your environment.

Known Issues

NetIQ Corporation strives 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).

Permissions, Technical Roles, and Applications Will Not Show Authorized by Business Role

The Identity Governance catalog will not display authorized by details for permissions, technical roles, or applications assigned to a business role when the business role does not have members. (Bug 1141553)

Installation Program Displays Unreadable Text

Issue: When installing Identity Governance using the GUI mode on Linux, any message dialog box might contain unreadable text. The issue occurs because the installation program (InstallAnywhere) is preferring another font for the `san-serif` font family. (Bug 1137118)

Workaround: If your server runs SUSE Linux Enterprise Server 15.1, we recommend that you edit a configuration file for the fonts named `60-family-prefer.conf` on the server running SUSE Linux Enterprise Server 15.1 before you start the Identity Governance GUI installer. The `60-family-prefer.conf` file configures or defines the preferred fonts when the programs use the standard aliases `serif`, `san-serif`, and `monospace`.

NOTE: This workaround applies only to servers running SUSE Linux Enterprise Server 15.1. Red Hat Enterprise Linux 8 does not include the `60-family-prefer.conf` configuration file.

Use the following steps to configure the proper fonts file:

1. SSH to the Linux server as a user with read and write rights to the `/etc/fonts/conf.d/60-family-prefer.conf` file.
2. Open `/etc/fonts/conf.d/60-family-prefer.conf` file in a text editor.
3. Search the `/etc/fonts/conf.d/60-family-prefer.conf` file for the following block:

```
<match target="pattern">
  <test name="family">
     <string>sans-serif</string>
  </test>
  <test name="force_bw">
     <bool>true</bool>
  </test>
  <edit name="family" mode="prepend">
     <string>Liberation Sans</string>
  </edit>
</match>
```

NOTE: This block prefers the `Liberation Sans` font when the font family alias is set to `san-serif` and `force_bw` is `true`.

4 Add the following block below the block you found:

```
<match target="pattern">
  <test name="family">
    <string>sans-serif</string>
  </test>
  <test name="force_bw">
    <bool>false</bool>
  </test>
  <edit name="family" mode="prepend">
    <string>DejaVu Sans</string>
  </edit>
</match>
```

NOTE: The new block prefers the `DejaVu Sans` font when the font family alias is set to `san-serif` and `force_bw` is `false`. Together both blocks provide a preferred font to use for the `san-serif` font family alias, whether or not `force-bw` is enabled.

5 Save and close the file.

6 Execute the script `/usr/sbin/fonts-config` to reload the `/etc/fonts/conf.d/60-family-prefer.conf` file and the fonts so that the system sees the changes.

To execute the script access the sbin directory and from the command line, enter:

```
./fonts-config
```

7 Restart the installation.

Compensating Request Cannot be Sent through an Automated Fulfillment Process

When compensating revoke requests are issued, they cannot be sent through any automated fulfillment process. The system will not have enough information about the permission assignment to determine the path upon which to fulfill the request. Revoke requests will be sent to the configured manual fall back for that type of request.

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. (`Bug 1128704`)

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. (`Bug 1106253`)

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.

Fact Publication to Vertica Configuration Does Not Have a Schema Name Field

Issue: The configuration settings for fact publication to Vertica does not include a schema name field.

Workaround: If you want to configure Vertica fact publication into a specific schema, use the table name field and use a comma to separate the schema name from the table name.

Using IP Addresses During Installation to Identify Server Hosts Might Not Work Correctly

Issues: Because of new standards-based authentication, using IP addresses during installation might not work correctly in all circumstances. The side effect is that the OSP integration with Identity Governance and Identity Reporting will not work correctly in these circumstances.

Workaround: If you installed the current or previous version of Identity Governance using IP addresses, you must replace the IP addresses with the fully qualified DNS names for these hosts in several configuration files. You can do this either before or after the upgrading procedure. For more information, see "Changing Host File IP Addresses to DNS Names" in the *Identity Governance 3.6 Installation and Configuration Guide*.

Installing on RHEL Might Require Additional Files

Issue: Installing Identity Governance on a minimal install RHEL server could fail due to known issues in openJDK: (Bug 1115625)

- https://bugzilla.redhat.com/show_bug.cgi?id=1484079
- https://bugs.openjdk.java.net/browse/JDK-8188030

Workaround: Install the following files before installing the product on a minimal install RHEL server:

- `fontconfig-2.10.95-11.el7.x86_64.rpm`
- `fontpackages-filesystem-1.44-8.el7.noarch.rpm`
- `stix-fonts-1.1.0-5.el7.noarch.rpm`

OSP Installer Hangs in GUI Mode When Using ssh X11 Forwarding

If you run a GUI-mode installer using ssh -Y and the installer appears to hang, then either run the installer in console mode, or try a different client machine. (Bug 1116795)

Browser Can Inadvertently Change the Credentials for the Identity Manager Connection

Issue: If you log in to Identity Governance as an administrator and allow the browser to remember your login credentials, the browser might apply those credentials to the values for connecting to the Identity Manager server. As a result, you might inadvertently change the wrong credentials for Identity Manager.

You can observe this issue in **Administration** > **Identity Manager System Connection Information**. When the browser replaces the values for Identity Manager username and password, Identity Governance erroneously enables the save icon. (Bug 971939)

Workaround: Either do not allow the browser to remember your login credentials for Identity Governance, or ignore the option to change and save the settings in **Administration** > **Identity Manager System Connection Information**.

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. (Bug 824779)

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 NetIQ Technical Support.

Restart Identity Governance after Restarting the Database Server

After you restart the server for the Identity Governance database, you must restart Identity Governance. Otherwise, Identity Governance might fail to complete processes such as data source publication. For more information, see "Starting and Stopping Apache Tomcat" in the *Identity Governance 3.6 Installation and Configuration Guide*.(Bug 954090)

Oracle Error Unable to Extend Table

Issue: You are using Identity Governance with an Oracle database and you see the following error in the administrative console or in the `catalina.out file`:

```
ORA-01653: unable to extend table ARDCS.BASIC_COLLECTED_ENTITY by 1024 in
tablespace USERS
```

The problem is the tablespace that Identity Governance uses for schemas has run out of space. (Bug 989425)

Workaround: Ensure that you connect to the correct instance if you are using the `User` tablespace. For example:

```
SQL> connect sys/oracle as SYSDBA
Connected.

SQL> alter session set container=pdborcl;
```

After issuing the commands, then you can alter the tablespace by adding data files.

Inconsistent Behavior When Using Wildcards

Issue: When using wildcards as literal characters, you must precede the special character with an escape (\) character. This behavior might not be consistent when using wildcards like * in search strings. Additionally, wildcards behavior will differ based on the type of database and the location of the search field or advanced filter. (Bug 1151222).

This issue will be fixed in a future release of the product. For more information, see "Supported Wildcards and Handling Wildcards as Literal Characters" in *Identity Governance User and Administration Guide*.

NullPointerException (NPE) Can Occur When Starting and Canceling a Review

In some cases, if you start a review and then cancel the review as it starts, a stack trace containing a NullPointerException could be output to the server console or logs by the Quartz third-party library. (Bug 1152040)

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. (Bug 1145500)

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).

Not All Identity Manager Resources Appear Correctly in Access Request

If an Identity Manager Resource is mapped to a "No Value" entitlement, and was created in the `idmdash` version 4.7.x or 4.8, it will not appear correctly in Access Request. If this resource was created in the IDMProv war from IDM 4.7.x, then it will appear correctly in Access Request to be requested. The `idmdash` is not creating this object correctly in the User Application driver, and is being tracked in Bug `1155551`.

Identity Manager Permissions that Have Dynamic Bound Entitlement Values are Not Available for Selection in SoDs, Technical Roles, and Business Roles

Issue: Helpdesk System Resources such as Group Access, History Access, Organization Chart Access, Reassign Access, Teams Access, and User Catalog Access are not available for selection in SoDs, Technical Roles, and Business Roles when an Identity Manager application is collected in Identity Governance. (Bug `1156894`)

Identity Governance does not currently support selection of Resources/dynamic bound entitlements in SoDs, Technical Roles, and Business Roles within Identity Governance. This issue will be fixed in a future release of the product.

Resolved Issues

The following issues were resolved in the current release.

Risk Level Configuration Settings are Lost after Upgrading

If you customized the risk level configuration settings in Identity Governance, you had to export the settings before upgrading, or you would lose your customized settings. (Bug 1066689)

You no longer have to export risk level configuration settings. Those settings, as well as risk score settings and risk score schedule settings, are retained when you upgrade from Identity Governance 3.5.1 or Identity Governance 3.5.2.

Progress and Task Count Can Differ on Review Instances in Clustered, High-Traffic Environments

In clustered environments, a shared progress count on the review instance could be out of sync with the actual task count. This issue did not impact the actual process state of the review, but it could raise alarms, which impacted compliance. (Bug 1130897)

This release of Identity Governance includes a Refresh button on the review instance header that the Review Administrator, Owner, and Global Administrator can use to synchronize the progress and task counts at any time during an active review.

The digest_id Column Does Not Display the Correct Value

In the previous release, if a curated record was migrated from an earlier version, Identity Governance did not correctly set the value for the digest_id column of the merged spermission record. (Bug 1152839)

This release of Identity Governance corrects the issue, and the digest_id column displays the correct value.

Reassigned Review Tasks Could Display the Incorrect Reassignment Date

In the previous release, if you reassigned a review item from the reviewer to the Review Owner, Identity Governance displayed the original assignment date as the reassignment date. (Bug 1155304)

With this release, Identity Governance correctly displays the reassignment date.

The Review Owner View Does not Render Correctly in a Running Review after the Definition is Updated

In some cases, a Review Owner who modified a review definition by adding another permission to a running review, could see two listings for the coverage map. If the Review Owner deleted the original coverage map, the status box did not render correctly on the Reviews tab. (Bug 1154888)

This release of Identity Governance corrects the rendering issue.

A Windows Active Directory Input Transformation Script Causes the Day Value to be Incorrect

In previous versions of Identity Governance, the default input transformation script for the Active Directory Last Logon displays the date as one day prior to the actual date. (Bug 1152780)

This release of Identity Governance displays the correct date.

Default Columns to Display within an Account Review Can Appear After Columns Were Edited

In the previous release, if you edited the global default columns to display in the Review definition, and then logged in to Identity Governance as the Reviewer, the displayed columns reverted back to the global default of Type, Account, Permissions, User, Action, and Activity. (Bug 1152742)

With this release of Identity Governance, the correct, edited columns appear in the Review definition.

Changes to User Risk Scores in a Review Can Cause Inherited IDM Roles to Require Review

If you configured a User Access Review to inherit roles and permissions created in NetIQ Identity Manager, and then make risk scoring changes to the Identity Governance User Risk Score, the Identity Manager roles were no longer inherited and had to be reviewed. (Bug 1146240)

With this release, you can make changes to the User Risk Score, and Identity Governance retains any inherited roles and permissions from Identity Manager.

Account Identities Can Appear Twice in the Catalog

In previous releases, under some circumstances, individual account identities listed under **Catalog** > **Account** could appear twice. (Bug 1137173)

This release corrects the issue, and each account identity appears correctly.

Edited Scheduled Start Times for Metrics Collection are not Updated Correctly

In a previous release, Identity Governance experienced issues with scheduled start times and intervals for metrics collection if you changed the scheduled start time. (Bug 1133326)

This release corrects the issue. You can edit the scheduled start time for metrics collection, and both the start time and the interval for metrics collection are correct.

Publication information on the Overview page can be misleading

In previous releases, the Overview page showed administrators a successful publication date even if the publication for the Identity Source(s) failed on that date. To view the true status of publication information, administrators had to access the Identity Source page. (Bug 1138622)

This release of Identity Governance displays the status of publications such as failed, canceled, last successful, and running with the respective dates.

Email Notification Occurs Only Once for a Separation of Duties (SoD) Violation

If an SoD owner received an email about an SoD violation, and then approved the SoD for a single day, the SoD owner would not receive another email after the approval expired. (Bug 1128632)

With this release, Identity Governance sends a reminder email to the SoD policy owners informing them of the approval expiration.

Provide an Option to Change the Default Access Request Landing Page

Previous versions of Identity Governance did not allow you to change the default landing page for the Access Request page. (Bug 1146913)

This release allows you to perform the following procedure to change the default landing page:

1. From the Identity Governance home page, click **Configuration** > **General Settings**.
2. Under **General Settings**, select the desired landing page for **Access Request landing page**.
3. Click **Save**.

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

For general corporate and product information, see the NetIQ Corporate Web site (https://www.microfocus.com/en-us/home).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ 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/.