Identity Governance 3.6.1 Release Notes

April 2020

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 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 3.6.1

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

Access Review and Certification Enhancements

This release includes the following enhancements:

- Enhanced ability to create review definitions. Enhancements include:
  - Ability to select review objects and create review definitions instead of selecting review type and then specifying review objects.
  - More efficient handling of unmapped accounts' reviews. Earlier you could review unmapped accounts using Account Review and Unmapped Accounts Review. The Orphan/Unmapped only Account Review type has been removed to avoid redundancy. You can now directly select unmapped accounts as your review object.
  - Ability to review permission assignments.
- Ability to select items across pages and apply bulk actions.
- Enhanced due date notification and escalation workflow including the ability to send secondary email notifications.

For more information about reviews, see "Creating and Modifying Review Definitions " in the *Identity Governance 3.6 User and Administration Guide*.

Business Role Inconsistency Detection Enhancements

This release includes a redesigned interface and additional capabilities related to business role reconciliation and inconsistency detections.

For more information about business roles, see "Creating and Managing Business Roles " in the *Identity Governance 3.6 User and Administration Guide*.

Technical Role Assignment Enhancements

This release enables the promotion of technical role candidates to the assigned technical role and ensures Identity Governance does not trigger fulfillment requests to remove permissions when removing technical role assignments when the permissions are also assigned to the user by another technical role or by a business role.

For more information about technical roles, see "Creating and Managing Technical Roles" in the *Identity Governance 3.6 User and Administration Guide*.

Data Policy Enhancements

This release includes the ability to:

- Select a permission assignment as an item to monitor in data policies and trigger remediation as needed
- Filter on the application name in a permission assignment related publication data policy

For more information about data policies, see "Creating and Managing Data Policies " in the *Identity Governance 3.6 User and Administration Guide*.

Reporting Enhancements

This release includes two new reports: Business Role Definition Reviews and Technical Role Assignment Coverage – CSV.

Optional Beta Features

This release includes the ability to enable beta features such as custom request and approval forms, business role mining hierarchy, and ability to start Identity Manager workflows and approve workflows from Identify Governance in future releases from the **Configuration** page. Contact your support representative to enable these features.

WARNING: Micro Focus does not guarantee that beta features are free of defects. These beta features are provided 'as is' without warranty of any kind. Using these features in a production environment could potentially have adverse effects on data. You should back up your data before using beta features. Work with your support representative for details. If you encounter any bugs or glitches or would like to request refinement of these features, please let support know immediately so we can make improvements. We appreciate your feedback.

Miscellaneous Enhancements

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

- Upgrade path for existing customers to move directly to 3.6.*x* from previous releases as far back as Identity Governance 3.0.*x*
- Scheduling and performance improvements to Identity Governance capabilities such as the ability to use date formula in addition to calendar date picker tool to specify dates
- Design enhancements to the Fulfillment user interface provides the ability to configure the fulfillment target mappings for an entire application in a single dialog, and perform bulk edit actions for the mappings
- Ability to clean up business role inconsistency detections, and certification and data policy remediation runs using the **Maintenance** menu advanced cleanup configuration settings
- Ability to configure if business role authorizations should be honored when removing technical role assignments using Identity Governance Configuration utility console mode properties
- Ability to specify when review tasks are due, send notifications based on the task due event, and choose whether a review item will escalate to the escalation reviewer

System Requirements

This release requires the following components:

- Operating System
  - Red Hat Enterprise Linux (RHEL) 8.0 (64-bit)
  - SUSE Linux Enterprise Server (SLES) 15.1
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019

IMPORTANT: Before installing Identity Governance, apply the latest operating system patches.

- Database
  - Microsoft SQL
    - MS SQL 2017 or later patched versions of the SQL Server 2017
    - MS SQL JDBC driver 7.2.2 or later patched versions of the Microsoft SQL JDBC driver
  - PostgreSQL
    - PostgreSQL 11.5, 11.7, or later patched versions of 11.*x*
    - PostgreSQL JDBC driver 42.2.6 or later patched versions of the PostgreSQL JDBC driver
  - Oracle
    - Oracle 18c or later patched versions of 18*x*
    - Oracle 19c or later patched versions of 19*x*
    - Oracle JDBC driver `ojdbc8.jar`
  - Vertica
    - Vertica 9.2.1 or later patched versions of 9.2.*x*
    - Vertica JDBC driver 9.2.*x*
- Application Server
  - Apache Tomcat 9.0.22, 9.0.33, or later patched versions of 9.0.*x*
  - Download from the Apache Tomcat (https://tomcat.apache.org/) website
- Authentication service
  - OSP 6.3.9
  - Access Manager 4.5 or later patched versions of 4.5.*x*
  - OSP 6.3.6 when deployed with Identity Manager
- LDAP authentication server
  - Microsoft Active Directory that comes with Windows Server 2016 or Windows Server 2019
  - Microsoft Active Directory Federation Service (AD FS) that comes with Windows Server 2016 or Windows Server 2019
  - eDirectory 9.2 or later patched versions of 9.2.*x*
  - Identity Manager 4.7.3, 4.7.4, or later patched versions of 4.7.*x*
  - Identity Manager 4.8 or later patched versions of 4.8.*x*
- Java Runtime Environment (JRE) Zulu JRE 8u222, 1.8.0_242 from Azul JRE or JDK, or later respective patched versions of 8u*xxx* and 1.8.0_*xxx*
- ActiveMQ 5.15.9, 5.15.12, or later patched versions of 5.15.*x*
- A supported Web browser (Microsoft Internet Explorer is not supported in Compatibility View)

NOTE: To fully integrate Identity Governance 3.6.1 features with NetIQ Identity Manager, you must have Identity Manager 4.7.3, at a minimum. For Single Sign On (SSO) between this version of Identity Governance and Identity Manager 4.8, you must have OSP 6.3.6 available in 4.7.*x* patch and later versions of 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 this version of Identity Governance 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*.

NetIQ provides scripts to help you upgrade the required components you installed for Identity Governance. One script scans your installations of Tomcat, ActiveMQ, Java, and PostgreSQL to determine which of those components require updates for the Identity Governance upgrade. The second script helps you upgrade those components, if needed, and leave your existing files intact and disabled. For more information, see "Upgrading Identity Governance Framework Components" 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 3.

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).

"Remove Technical Role Assignment" Appears as an Unsupported Fulfillment Type

Issue: If you upgraded Identity Governance from a version earlier than 3.5.1, the fulfillment type "Remove Technical Role Assignment" appears as an unsupported fulfillment type. (Bug 1168267)

Workaround: Use the following steps to manually add the mapping for this fulfillment type:

1. **Click Fulfillment** > **Configuration**.
2. Click **Application Setup**.
3. Find the application that displays "Remove Technical Role Assignment" as unsupported, and then click **Edit**.
4. Under **Supported Change Request Types**, select **Remove Technical Role Assignment**.
5. Click **Save**.

Incorrect Change Request Types Appear When Configuring Application Setup for Fulfillment

If you configure Application Setup for Fulfillment, and select Supported Change Request Types, the following two request types appear:

- Remove User from business role
- Modify Technical Role Permissions

These change request types are not application specific and should not appear. (Bug 1129604)

Comparing Two Application Data Sources Collection Activities Can Erroneously Report Differences

Issue: If you compare two collections on applications with child applications, the comparison could erroneously report differences if one of the collections was published but the other collection has not yet been published. This issue occurs, because permissions and accounts that belong to child applications are associated with their child application when the collection is published. Until publication, the permission and account records remain associated with the parent application. (Bug 1169656/Bug 1169698)

AD Identity with Changes Collection and Publication is Successful Even with Wrong "Base DN"

Issue: Collection and publication is successful but there are zero records when wrong Base DN is specified when collecting users and groups using the AD Identity with changes Collector.

Workaround: Test your collection (with a representative small number like 50) using the Test Collection feature in the user interface to make sure the settings you have entered are correct before you actually collect.

This happens because when using real time collection functionality with the AD Identity collector, the LDAP implementation uses the AD DirSync LDAP API. With DirSync, the base DN of the collection query (search) is the domain root of the server to which we connect. Therefore, if the connection parameters are correct, the base DN will be set to the domain path, *not* the value in the Base DN parameter of the collector. After the search is complete, the path of all found objects are compared to the configured Base DN parameter. If the Base DN parameter is invalid, then no found records will be allowed into the result set. (Bug 1168711)

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 3.6 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).

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.

Before Reviewer Task Expires Notification Requires Escalation

In Identity Governance 3.6.0 or previous versions, the **before reviewer task expires** option for a Reviewer Task Reminder notification requires that escalation be used in order for reminder emails to be sent. Without escalation in place, you must select **before review expires** when setting up notifications for your reviews. (Bug 1170440)

In Identity Governance 3.6.1, enhancements to the escalation process allow you to set separate rules and notifications for reviewer task expiration independent of the escalation process. You can send email notifications before the reviewer task is due, or when the reviewer task is overdue without specifying escalation.

Not All Identity Manager Resources Appear Correctly in Access Request

In a previous version of Identity Governance, if an Identity Manager Resource was mapped to a "No Value" entitlement, and was created in the `idmdash` version 4.7.x or 4.8, it would not appear correctly in Access Request. If this resource was created in the IDMProv war from IDM 4.7.x, then it would appear correctly in Access Request to be requested. (Bug 1155001)

This issue does not occur in this release.

NOTE: This release includes optional beta features and enhanced Access Request capability. We recommend that you use the Identity Governance Access Request and Approval feature to request items from the Identity Governance catalog, including items that have been collected into the catalog from Identity Manager. The Access Review driver (now known as the Identity Governance Driver for Identity Manager) used in Access Review 2.5 and older versions is no longer needed to provide request capabilities for Identity Governance or to integrate with Identity Manager. See "Administering Access Request", "Setting up Fulfillment Targets and Fulfilling Changesets", and "Instructions for Users with Runtime Authorizations" in the *Identity Governance 3.6 User and Administration Guide* for details related to the request and approval process, and details related to the fulfillment process using the Identity Manager workflows.

Optimize blocking of Real-time Collection and Resolution due to application collection and resolution

In a previous version of Identity Governance, application data collection blocked or terminated real-time identity collection, and application resolution blocked real-time event collection and resolution which could result in long real-time collection times. (Bug 1155368)

This release includes improvements to application data collection and resolution to solve the issue.

The Submit Button for Reviews Disappears If You Select a Large Number of Reviews

In a previous version of Identity Governance, if a reviewer selected more than 500 reviews to keep, remove, or modify, the **Submit** button did not fully display. (Bug 1160252)

This issue does not occur in this release.

Performance Issue Encountered with Technical Role Detection

A previous version of Identity Governance encountered a performance issue with technical role detection in which detection ran for a number of hours under certain circumstances. (Bug 1162541)

This release solves the issue, and technical role detection occurs within a reasonable timeframe.

Test Connection for Collectors With Change Events Do Not Work After an Upgrade or Collector Import from Identity Governance 3.5.x.

If you upgrade from Identity Governance 3.5 to Identity Governance 3.6 — or if you export a collector with change events from Identity Governance 3.5.x and import it into Identity Governance 3.6 — and then try to test connect the collector, an error occurs. (Bug 1163144)

This issue does not occur in this release.

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/.