NetIQ Identity Governance 3.0.1 Release Notes

February 2020

NetIQ Identity Governance 3.0.1 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) Web site.

1 What’s New?

The following outlines the key features and functions provided by this version, as well as issues resolved in this release:

1.1 Role Mining and Role Analysis

This version uses advanced analytics to mine business data and identify business or technical role candidates. Global or Business Role administrators can use role mining to reduce complexity in defining roles, and easily select role candidates with authorized users, permissions, technical roles, and applications to create business roles as well as technical roles with common permissions. Global or Technical Role administrators can use role mining to create technical roles. In addition, all business roles, can be analyzed for quality factors such as effectiveness of roles and similarity in membership and authorizations.

For more information, see “Managing Technical Roles”, and “Creating and Managing Business Roles” in the *NetIQ Identity Governance User Guide*.

1.2 Compliance

This version enables you to have a comprehensive enhanced view of your organization's compliance with specific certification controls, such as Sarbanes-Oxley Act (SOX). You can now create certification policies that reference multiple reviews, set risk levels for certification policies, calculate certification policy violations, calculate risk score, and determine compliance status. In addition, you can also schedule certification policy calculations. For more information about certification policies, see “Creating and Managing Certification Policies” in the *NetIQ Identity Governance User Guide*.

1.3 Risk

This version includes several enhancements.

Risk details

In addition to viewing risk details in the catalog, you can also view overall governance score and single factor scores on the **Overview** page.

Base risk factor

You can now specify attribute of an entity as a base factor for calculated or curated risk scoring.

Certification state risk factors

You can now assign weight and risk factor range for certification policy violations related risk factors.

Enhanced and scheduled risk scoring

You can now include certification policy violations in risk scoring, and you can also schedule risk calculations for specific entity or all entity types.

Unlimited risk factor weight

Limitation of all risk factor weights to be 100 has been lifted. You can specify any weight for each factor.

For more information about risk, see “Calculating and Customizing Risk” in the *NetIQ Identity Governance User Guide.*

1.4 Analytics and Decision Support

This version provides ability to create custom metrics and enhanced decision support information. It also enables you to show or hide decision support in reviews and requests. Enhanced decision support now includes:

- Account snapshot

- Business role mining metrics
- Proportion of entitlements
- Proportion of entitlements assigned by policy
- Proportion of entitlements assigned directly

Administrators can select additional attributes used for similarity profiles, configure how often Identity Governance collects system metrics, create custom metrics, and can collect metrics on demand. For more information, see "Configuring Analytics and Role Mining Settings" in the *NetIQ Identity Governance User Guide*.

1.5 Delegation

This version enables you to assign delegates for users to enable a more consistent workflow for managing the reassignment of user tasks. For more information, see "Creating and Managing Delegation" in the *NetIQ Identity Governance User Guide.*

1.6 Access Request

This version includes several enhancements to the Access Request interface. Administrators can now:

- Specify business roles as requesters
- Use CSV files (coverage maps) to assign approvers
- When SoD policies are configured, view potential SoD violations when requesting or approving access requests
- Retry failed requests
- Retract access request which is in approval pending or failed state
- View timeline of all underlying events associated with a request including fulfillment information

For more information, see "Administering Access Request" and "Instructions for Access Requesters and Approvers" in the *NetIQ Identity Governance User Guide*.

1.7 Reviews

This version includes new features and enhancements to the review process including:

- Preview mode which enables you to preview review definition version, assigned reviewers, review items, and email notifications
- Reorganized review options in review definition to improve usability
- Enhanced account reviews where you can assign account custodian as a reviewer, and view permissions grouped by accounts
- Materialized views which enables you to improve performance for large scale reviews
- New task reassignment notification
- When defining a review, the ability to preview notification email source and ability to add a notification using default templates
- Ability to change the escalation reviewer and escalation timeout during a preview or running review
- Ability to configure reasons for modifying review items, and changing reviewers so that changes can be easily tracked and analyzed

- Ability to set default grouping and default sort for the reviewer display
- Support for enhanced coverage maps with nested relationships, and business roles as reviewers

For more information, see "Creating and Running Reviews" in the *NetIQ Identity Governance User Guide*.

1.8 Fulfillment

This version provides new features and several enhancements for fulfillment requests, including:

- Additional fulfillment targets, including REST and SOAP fulfillment, CSV file-based fulfillment, and automated Active Directory fulfillment
- Support for additional change request types
- Ability to split fulfillment based on data type
- Auto-verification of request item change
- Ability to specify additional attributes that also should be included when sending instructions to an external fulfillment target
- Ability to transform incoming data from fulfillment targets

For more information, see "Configuring Fulfillment" in the *NetIQ Identity Governance User Guide*.

1.9 Identity and Application Data Collection

This version includes:

- Support for identity data collection with change events for Active Directory, eDirectory, and Identity Manager identity sources
- Support for viewing identity source details for users in the catalog on the **Users Source** tab
- Data collection performance improvements
- Data collection testing and emulation capabilities

NOTE: For more information, see "Collecting from Identity Sources with Change Events" and Managing Identity and Application Sources in the *NetIQ Identity Governance User Guide*.

1.10 Reports

This version provides a new Preview Changes report in CSV report and ability to install Reporting with Identity Governance.

1.11 Custom Development Support

This version includes the NetIQ Custom Collector SDK to support developing:

- Custom data collectors
- Custom fulfillment integrations

For more information, see Section 3.4, "Installing the Custom Collector SDK," on page 6.

1.12 Auditing Support

This version now supporting auditing for Identity Governance, OSP, and Reporting. For more information, see “Enabling Auditing” in the *NetIQ Identity Governance User Guide*.

1.13 Database Platform

This versions supports Microsoft SQL server.

2 System Requirements

This release requires the following minimum components:

- Apache Tomcat 8.5.23
- Microsoft SQL Server 2016 SP1, Oracle 12c SP2 with latest patches, or PostgreSQL 9.6.5
- One SSO Provider (OSP) 6.2.0
- LDAP authentication server (NetIQ eDirectory or Microsoft Active Directory)
- A supported Web browser

NOTE: Microsoft Internet Explorer is not supported in Compatibility View.

The following components are optional:

- Self Service Password Reset (SSPR)
- NetIQ Identity Manager
- NetIQ Identity Reporting

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 the *NetIQ Identity Governance User Guide*.

To integrate Identity Governance with NetIQ Identity Manager, you must have NetIQ Identity Manager 4.6, at a minimum.

3 Installing or Upgrading Identity Governance

For your convenience, NetIQ provides installation packages for Tomcat, PostgreSQL, and OSP. This release also includes the NetIQ Custom Collector SDK to help with custom collector and fulfillment template creation and maintenance.

You can upgrade to Identity Governance 3.0.1 from Identity Governance 2.5. 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.

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 Section 2, “System Requirements,” on page 5.

3.1 Installing Identity Governance

If you have not previously installed Identity Governance or want to create a new environment, see “Installing Identity Governance” in the *NetIQ Identity Governance User Guide*.

3.2 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 *NetIQ Identity Governance User Guide*

3.3 Removed Standalone Utilities `csv-gen` and `collection-tester`

With this release of Identity Governance, the two standalone utilities `csv-gen` and `collection-tester` have moved to be part of the administrative console when you manage Collectors. For more information, see “Managing Identity and Application Sources” in the *NetIQ Identity Governance User Guide*.

3.4 Installing the Custom Collector SDK

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-3.0-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.

4 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 (http://www.netiq.com/support).

4.1 When utilizing the AD, eDirectory, or IDM identities with Changes collectors, certain mappings do not change

When creating new `AD Identities with changes`, `eDirectory Identity with changes` or `IDM Identity with changes` collectors, Identity Governance maps the following Collector Identity attributes to the value of `OBJ_ID`:

- `User ID from Source`
- `LDAP Distinguished Name`
- `Group ID from Source`

IMPORTANT: Do not change these mappings. If you do the change events will not occur. (`Bug 1084098`)

4.2 When utilizing the AD, eDirectory, or IDM identities with Changes collectors a full collect and publish is required after a move or rename

When utilizing `AD Identities with changes`, `eDirectory Identity with changes` or `IDM Identity with changes` collectors, if an entity (user or group) is moved or renamed in the Identity Vault, a full collect and publish of these collectors is required to resynchronize the current state. (`Bug 1081158`) and (`Bug 1083524`)

4.3 Re-importing a review definition causes stack trace and Oracle to become unresponsive with larger definition file

Downloading a review definition with a large number of permissions, and then importing it causes application to become extremely slow or even unresponsive because permission ID is not an indexed attribute. (Bug 1062652)

Workaround: Prior to exporting review definitions that contain a large number of permissions, you should change the uniqueness attribute in **Administration > Download Settings** to an indexed attribute, such as `Permission Name` or `Permission Description`, instead of using `Permission ID from Source`.

4.4 Warning message can be seen with igops creation when using MS SQL

After installing Identity Governance 3.0 with MS SQL 2016SP1, one may see messages similar to the following in the `liqubibase-ops.txt` or when importing the generated `sql` file for the `igops`: `WARNING liquibase: IacOpsChangeLog.xml: IacOpsTables.xml::30300::SYSTEM: Database does not support drop with cascade`. These messages can be ignored. This behavior will be addressed in the next release. (Bug 1068927)

4.5 Unable to TAB to scrollbar on EULA panel

To accept the license agreement a user must first scroll to the bottom of the EULA. In the past it was possible to Tab to the scrollbar and press PageDown to scroll but now a mouse must be used. This is a known Flexera InstallAnywhere 2017 issue. (Bug 1059164)

4.6 The password for install_smtp_secret_auth_user will not be read from the environment during silent install

If one is performing a silent install and setting all of the passwords in the environment as compared to in the silent properties file, value for `install_smtp_secret_auth_user` will not be read. (Bug 1072414)

Workaround: Either set it in the silent properties file or update the password post install utilizing `configupdate.sh`.

NOTE: Although using silent mode is the most likely scenario for reading passwords from environment variables, the installer reads each defined variable regardless of the mode being used (GUI, Console, or Silent).

4.7 Cannot use quote characters for passwords during the install

Currently, one cannot utilize either single or double quotes for passwords when installing the components of Identity Governance. If you do the installation will fail. If a quote character is one that you want to use, it can be utilized post install. (Bug1068921)

4.8 Purging Analytical Facts and Reviews

When purging **Analytical Facts**, utilize *(all). Purging of one item or a range of items (For example: 2-5) will not actually purge anything. (Bug 1068955)

However, when purging reviews, especially when you have a large number of reviews, *(all) might lead to memory issues. Either purge reviews individually or in small sets (For example:1-3) and do not use *(all). (Bug 1067967)

4.9 Issue with extend characters in the Test Collection or Download and Emulation feature

If you wish to utilize the data source **Test Collection** or **Download and Emulation** feature, take note that extended characters should not be utilized in the names of your collectors. Collector names are utilized in the naming of the files that are created during download and the ZIP creation tools do not allow file entry names with extended characters. (Bug 1069031)

4.10 Oracle Errors

When using Oracle 12c SP2, you could see the following error message at various times (Bug 1011628):

```
ORA-01792: maximum number of columns in a table or view is 1000
```

Workaround: Apply all the patches available from Oracle.

4.11 Database Server Should be in the Same Subnetwork as the Identity Governance Server

The Oracle or PostgreSQL database server should be in the same subnetwork or data center as the Identity Governance server to avoid delays during installation, start-up, and runtime. (Bug 986222)

4.12 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**.

4.13 User Authorizations Fail If the Primary Identity Source is not Identity Manager

Issue: User authorizations fail with the following error if you are using an Identity Manager Collector:

`You are authenticated and logged in, but you do not have access to the Identity Governance application. This means you logged in as a user who was valid in your authentication source, but has never been collected in Identity Governance or does not have access to the Identity Governance application.`

Identity Governance expects the Identity Manager Collector to be the first collector in the list of Identities Collectors.

Workaround: There are two different ways resolve the error.

Workaround 1

1. Login to Identity Governance as the Bootstrap Administrator.
2. Select **Data Sources** > **Identities**.
3. Expand the **Merging Rule**.
4. In the LDAP Distinguish Name field, change it from **None** to **Identity Manager Collector**.
5. Select **Save**, then publish the change.

Or

Workaround 2

1. Login to Identity Governance as the Bootstrap Administrator.
2. Select **Data Sources** > **Identities**.
3. Drag and drop the Identity Manager Identities Collector to be first in the list.
4. Select **Save**, then publish the change.

4.14 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.

4.15 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 “Stopping, Starting, and Restarting Tomcat” in the *NetIQ Identity Governance User Guide*.`(Bug 954090)`

4.16 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 Access Review 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.

4.17 Risk Level Configuration Settings are Lost after Upgrading

If you have customized the Risk level settings in Identity Governance, you must export these setting before upgrading or you will lose your customized settings. You export the settings to use as a reference when you configuring the Risk settings again on the new version of Identity Governance. (Bug 106689)

To export the settings, run the following queries:

Localized labels:

```
select key_col, 'val_col from ism_global_config where key_col like '%risk%Label%';
```

Risk levels:

```
select key_col, val_col from ism_global_config where key_col like '%risk%Max' or
key_col like '%risk%Min' or key_col like '%risk%number';
```

You can export the localized Risk labels as properties files from the Administration and Localization section in the administrative console.

4.18 Data Mining Process Hangs when Mining Large Catalog

Issue: If you have a large catalog of users and technical roles, data mining performance might be very slow and eventually fail. (Bug 1095222)

Workaround: Configure the technical role maximum permission size and maximum user size properties in Identity Governance Configuration Utility via console mode to avoid this.

1. Start the Identity Governance Configuration Utility.
   - **Linux:** Navigate to default location of /opt/netiq/idm/apps/idgov/bin, and enter ./configutil -console -password *database_password*
   - **Windows:** Naviagate to default location of c:\netiq\idm\apps\idgov\bin, and enter configutil -console -password *database_password*
2. Check the default values for the technical role maximum permission size and maximum user size properties.

   ```
   display-configs com.netiq.iac.analytics.roles.technical.MaxPermSize
   ```

   ```
   display-configs com.netiq.iac.analytics.roles.technical.MaxUserSize
   ```

   The default value is 50000.
3. Set the technical role maximum permission size and maximum user size properties.

```
set-property com.netiq.iac.analytics.roles.technical.MaxPermSize 10000
set-property com.netiq.iac.analytics.roles.technical.MaxUserSize 10000
```

4 Confirm new values using `display-configs` commands.

5 Exit the console and restart tomcat for the changes to take effect.

For additional information about the Configuration Utility, see "Running the Identity Governance Configuration Utility"in the *NetIQ Identity Governance User Guide*.

4.19 Login to Identity Reporting Fails After Enabling CEF Auditing for OSP

Issue: Enabling CEF auditing for OSP in Configuration Update utility after installing Identity Governance 3.0 with Identity Reporting 6.0.x and auditing causes authentication error. (`Bug 1101719`)

This issue has been fixed in Identity Governance 3.5 with Identity Reporting 6.5 release.

5 Additions to Documentation

5.1 Automated Access Provisioning and Deprovisioning

The events outlined in "Automated Access Provisioning and Deprovisioning" section of the *NetIQ Identity Governance User Guide* trigger Identity Governance to perform business role detections but do not necessarily result in Identity Governance issuing auto-grant or auto-revoke requests. The rules that trigger a detection are different from the rules that govern whether Identity Governance will issue the auto requests. For example, deactivating a technical role that is an authorized resource of a business role triggers a business role detection, but does not result in an auto-revoke request or changes to any current auto-grant or auto-revoke request. Publication of application sources trigger detection but do not necessarily result in Identity Governance issuing the auto requests. (`Bug 1108062`)

6 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 (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate Web site (http://www.netiq.com/).

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.

7 Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.