NetIQ Identity Governance 3.5.1 Release Notes

April 2020

NetIQ Identity Governance 3.5.1 and 3.5 include new features, improve usability, and resolve 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.

1 What’s New in 3.5.1

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

1.1 Analytics

This release includes performance tuning of analytics and fact (metric) collection.

1.2 Automated Access Provisioning and Deprovisioning

This release includes several enhancements to business role policies behavior and management:

- Enhanced auto-request processing including automatic compensation for business role request latency and fulfillment issues
- Ability to enable compensating requests for requests generated by other processes such as access request, reviews, and Separation of Duties (SoD) violations administration
- Ability to detect and resolve auto request inconsistencies
- Ability to monitor business role detections
- Database schema updates

For more information, see "Automated Access Provisioning and Deprovisioning" in NetIQ Identity Governance Administrator Guide.

1.3 Account Review

This release includes the ability to specify user selection as mapped users, account custodians, or either mapped users or account custodians in an account review definition. For more information, see "Expanding and Restricting Review Items" in NetIQ Identity Governance Administrator Guide.

1.4 Certification Policy

This release includes new certification policy types, ability to manually calculate certification policy violations for partial reviews, and database schema changes. For more information, see "Managing Certification Policy Violations" in NetIQ Identity Governance Administrator Guide.

1.5 Risk

This release includes two new risk factors to support certification policy changes. For more information, see "Risk Factors" in NetIQ Identity Governance Administrator Guide.

1.6 Reports

This release includes three new reports supporting risk policy configuration, review delegation assignments, and certification policy violations. It also includes advanced filtering and modifications to several reports.

1.7 Fixed Issues

The following issue has been fixed in Identity Governance 3.5.1:

Cannot Use Identity Collectors with Change Events That Were Upgraded or Converted in Identity Governance 3.5.0

2 What's New in 3.5

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

2.1 Navigation

This release has top navigation instead of left navigation to improve readability and enable better usage of page width to display content. It also includes the ability to easily navigate from sub-page to the related main pages by clicking on the page header link.

Because of changed or additional element IDs and the different navigation settings, customizations you made to your previous environment might not work as expected. After installing this version, review and adjust any customizations as needed.

2.2 Governance Insights

This release introduces interactive audit query support, analytics data extraction, and governance metrics calculations.

For more information, see “Searching with Insight Queries” and “Analyzing Data and Monitoring Governance System” in *NetIQ Identity Governance Administrator Guide*.

2.3 Potential SoD Violation Detection Support

This release enables you to detect and approve or resolve SoD (Separation of Duties) violations that *might* occur in the future if a set of access requests are fulfilled.

For more information, see “Understanding Potential SoD Violations” and “Approving or Resolving Potential SoD Violations” in *NetIQ Identity Governance Administrator Guide*.

2.4 Micro Certifications

This release provides focused certification capabilities to allow for immediate review and remediation of identity life cycle events, control violations, and audit exceptions.

For more information, see “Understanding Micro Certification” in *NetIQ Identity Governance Administrator Guide*.

2.5 Data Cleansing Review Processes

This release includes additional review definitions that enable business users to verify and correct direct report assignments and identity profile information.

For more information, see “Selecting a Review Type” in *NetIQ Identity Governance Administrator Guide*.

2.6 Governance Data Maintenance Support

This release automates and simplifies the process of archiving data from the operational governance system. In addition, the Data Purge utility from previous releases has been included in the product as part of new database maintenance features accessible through the **Data Administration > Maintenance** administrative console menu.

For more information about archiving and purging data, see "Database Maintenance" in *NetIQ Identity Governance Administrator Guide*.

2.7 Reports

This release includes 10 new reports supporting direct reports reviews, user profile reviews, authorization assignments, business role memberships, performance logs, and data source changes. The release also includes the ability to connect to Vertica to store reporting data.

2.8 Miscellaneous Enhancements

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

- Import and export capabilities in additional areas such as roles and policies
- Advanced search capabilities using filter icon in additional areas.

  For more information, see "Managing Filters" in *NetIQ Identity Governance Administrator Guide*.
- Ability to authorize permissions from an IDM application and from an IDM role that contains other IDM roles and/or IDM resources using Identity Governance business or technical role authorization policies.

  For more information, see Defining Business Roles.
- Ability to view hierarchy of contained permissions in reviews
- Ability to select groups and business roles as Escalation Reviewers
- Ability to configure fulfillment targets for catalog update requests related to profile attributes, reporting relationships, and policy violation remediation change requests
- Ability to connect to Vertica to store custom metrics data
- Ability to select supervisor of the reviewer in the TO field of the review definition for escalation notifications

2.9 Fixed Issues

The following issues have been fixed in Identity Governance 3.5.0:

- When Utilizing the Active Directory, eDirectory, or Identity Manager Identities with Changes Collectors, Certain Mappings Do Not Change
- When Utilizing the Active Directory, eDirectory, or Identity Manager Identities with Changes Collectors a Full Collect and Publish Is Required After a Move or Rename
- Cannot Use Quote Characters for Passwords during the Install
- Purging All Analytical Facts and Reviews

3 System Requirements

This release requires the following minimum components:

- Red Hat Enterprise Linux (RHEL) 7.4, SUSE Linux Enterprise Server (SLES) 12 SP3, or Windows Server 2016
- Microsoft SQL Server 2017, Oracle 12c SP2 with latest patches, or PostgreSQL 10.5
- Apache Tomcat 9.0.12
- An authentication service (One SSO Provider (OSP) 6.3.0 or NetIQ Access Manager 4.4)
- LDAP authentication server (Microsoft Active Directory, NetIQ eDirectory 9.1.1, or NetIQ Identity Manager 4.7.2)
- Java Runtime Environment (JRE) Zulu JRE 8u181
- ActiveMQ 5.15.6 (if you require notifications guaranteed to be sent using SMTP)
- A supported Web browser (Microsoft Internet Explorer is not supported in Compatibility View)

NOTE: To fully integrate Identity Governance 3.5 features with NetIQ Identity Manager, you must have NetIQ Identity Manager 4.7.2, at a minimum. For Single Sign On (SSO) between Identity Governance 3.5 and NetIQ Identity Manager 4.7, you must have OSP 6.3.1 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 *NetIQ Identity Governance Installation Guide*.

4 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. For more information see 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 3.5.1 from Identity Governance 3.0. 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 *NetIQ Identity Governance Installation 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 *NetIQ Identity Governance Installation 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 Section 3, "System Requirements," on page 5.

4.1 Installing Identity Governance

If you have not previously installed Identity Governance or want to create a new environment, see the *NetIQ Identity Governance Installation Guide*.

4.2 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 Installation Guide*.

4.3 Moved Data Purge Utility

With this release of Identity Governance, the Data Purge utility has been moved to be part of the product administrative console. As a result:

- The `data-purge-utility.(sh or bat)` file will no longer be in the `idgov/bin directory`.
- The `data-purge-utility.jar file` will no longer been the in the `idgov/lib directory`.
- The REST API used by this version of the Data Purge utility will no longer be included in the product. If you had written code to use those REST endpoints, it will no longer work.

  The REST APIs that no longer exist are those where the URL matches this pattern: `/api/data/mgt/*`.

4.4 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-3.5-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.

5 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).

5.1 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: We recommend that you edit a configuration file for the fonts named `60-family-prefer.conf` on the Linux server before starting 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`.

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 `sans-serif` and `force_bw` is `false`. Together both blocks provide a preferred font to use for the `sans-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
```

You can now start the installation again and the fonts are readable.

5.2 Location of Identity Governance REST API Documentation Missing from Guides

Identity Governance includes REST API documentation. To access this documentation, go to *protocol*://*server*:*port*/doc/. For example, http://myserver.netiq.com:8080/doc.

NOTE: You should manually move or delete the `doc.war` file and folders from the tomcat /webapps directory in a production environment.

5.3 The Custom Columns Available for Selection Are Not Filtered by User Access

Issue: When selecting entities from a list in Identity Governance, the custom columns available for selection are not filtered by user access. If the logged in user does not have access to view the full catalog attributes, columns which are not designated as Quick Info may show an error in the value. `(Bug 1129401)`

Workaround: Global or Data administrator should enable display of Quick Info view for all custom column attributes using **Data Administration** menu by selecting the Quick info check box in the attribute settings page.

5.4 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 fallback for that type of request.

5.5 Moving a User from One Business Role to Another Via 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.

5.6 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.

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

Issue: The configuration settings for fact publication to Vertica do 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.

5.8 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 *NetIQ Identity Governance Installation Guide*.

5.9 Cannot Install Identity Governance or OSP in Directories Containing Spaces

Issue: If you try to install Identity Governance or OSP in directories containing spaces, the installer fails with an error message. (Bug 1115423)

Workaround: Do not install the products in directories containing spaces.

5.10 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`

5.11 OSP Installer Hangs in GUI mode when Using ssh X11 Forwarding

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

5.12 API and Rights Needed to Use Azure Data Collector

If you are using the Active Directory Azure collector, complete the following steps:

1. Enable the Azure Active Directory Graph API for your site and grant the following permissions to an account to access the API:
   - `Directory.Read.All`
   - `User.Read`
2. Generate an OAuth2 client and secret for API access.
3. Check that you can browse your Azure domain with the graph explorer using the account from Step 1. For more information, see https://developer.microsoft.com/en-us/graph/graph-explorer.

5.13 Attempt to Download Metric Definition or Metric Results Prompts to Leave a Page

This is a browse upstream issue. The browser displays the prompt. To download the file accept the leave page prompt.

5.14 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)

5.15 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)

5.16 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.

5.17 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)

5.18 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**.

5.19 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. (Bug 963011)

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.

5.20 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.

5.21 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 Installation Guide*.(`Bug 954090`)

5.22 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.

5.23 Reporting REST API WAR Has a Few Mistakes

Issue: The REST API WAR file for Identity Reporting 6.5 has the client ID as `iac` instead of `rpt` and does not have the information about how to get an OAuth token if NAM is being used instead of OSP. (`Bug 1149646`)

Workaround: Use `rpt` as the client ID. For information about the missing user access token related procedures, see the *REST API for Access Token* document that is listed under References in the Identity Governance 3.5 Documentation Web site.

These issues have been resolved in Identity Reporting 6.6 REST API `rptdoc.war`. For information about accessing the documentation, see "REST Services for Reporting" in the *NetIQ Identity Governance Identity Reporting Guide*.

5.24 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 Administrator Guide*.

6 Resolved Issues

6.1 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)

6.2 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)

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).

6.3 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 are configuring the Risk settings again on the new version of Identity Governance. (Bug 1066689)

This is resolved with the ability to import and export all risk settings in Identity Governance 3.5.

7 Additions to the Documentation

The following additions have been made to the documentation after the documentation was released.

Location	Change
"Identity Governance Required Component Software Versions" in the *NetIQ Identity Governance Installation Guide*	Changed OpenJDK JRE 8 to be Zulu OpenJDK 8 from Azul.
Section 5.1, "Installation Program Displays Unreadable Text," on page 8	Changed the text to provide more information and added a procedure while updating the contents of the blocks.
Section 5.2, "Location of Identity Governance REST API Documentation Missing from Guides," on page 9	Added missing information.

8 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.

9 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/.