# SailPoint IdentityIQ

Version 7.2

# Release Notes

This document and the information contained herein is SailPoint Confidential Information

# IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, version 7.2

SailPoint IdentityIQ is a complete identity and access management solution that integrates governance and provisioning into a single solution leveraging a common identity repository and governance platform. Because of this approach, IdentityIQ consistently applies business and security policy and role and risk models across all identity and access-related activities - from access requests to access certifications and policy enforcement, to account provisioning and user lifecycle management. Through the use of patent-pending technologies and analytics, IdentityIQ improves security, lowers the cost of operations, and improves an organization's ability to meet compliance and provisioning demands.

This release note contains the following information:

- IdentityIQ 7.2 Overview
- New Features — enhancements and features added since the last release
- Important Upgrade Considerations — specific guidelines for various configurations
- Supported Platforms — supported platforms, environments and applications
- Resolved issues — resolved problems in this release
- Known issues — known problems in this release and ways to avoid them

## IdentityIQ Overview

IdentityIQ 7.2 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform, and Connectivity. Key enhancements in the release include:

- New Responsive Object-based Access Reviews
  - New unified experience across devices (desktop, tablet, smartphone) for users reviewing object-based certifications
  - Improved usability of the access reviews through better organization and enhanced visibility to the content that the certifier is reviewing
- New Responsive Requests Pages
  - New unified experience across devices (desktop, tablet, smartphone) for users to manage access requests
- IdentityIQ SCIM API
  - Leverage standardized, SCIM-enabled endpoints to externally invoke the IdentityIQ workflow and policy engine
- Task Management
  - The Task Management user interface provides visibility and control of all tasks within IdentityIQ
  - Single view into all tasks running in IdentityIQ
  - Simplified ability to assign tasks to a server
  - Ability to diagnose and take action on a task
- Plugin Framework

  - The Plugin Framework provides the infrastructure and tools to enable developers to extend the Open Identity Platform to meet a variety of use cases
  - Internationalization
  - Bundling IdentityIQ user interface components so plugin developers can provide end users with the same user experience provided by IdentityIQ
- Multifactor Authentication Framework (MFA)
  - SailPoint provided reference implementations for RSA, DUO, and Microsoft Azure to leverage MFA to authenticate users into IdentityIQ
  - Extensible MFA framework facilitating integration with most MFA providers
- Privileged Account Management Module
  - Added the ability to search for containers by container name
- Expanded Connectivity Support
  - Added support for multiple forests managed by a single application to the Active Directory Connector
  - Added pass-through authentication support for the Azure Active Directory Connector
  - Added aggregation filters to the Workday Connector
  - Added default linked template support to the Epic Integration Module
  - Added the ability to manage TopSecret connections using the agent-less LDAP module to the TopSecret Integration Module

# IdentityIQ Feature Updates

## New Responsive Object-based Access Review Interface

IdentityIQ 7.2 introduces a new responsive object based access review interface that unifies it across devices for the end user. The access review interface delivers an improved user experience by organizing the contents of the certification review and enabling efficiency through the new group by functionality.

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| Responsive: Object based access review | End users can now review access certifications across any device and have the same experience | Improves adoption and efficiency for users to certify access with a unified experience regardless of what devices they are using |
| Organized Interface | Enhanced layout that enables the certifiers to view their progress towards completion. Important items are organized and shown first | Reduces compliance fatigue by grounding the certifier on what is important and giving them visibility of their progress towards completion |
| Group By feature | Ability for the certifier to group any of the attributes defined as a column in the access review | Ability to quickly identify outliers in a group and perform bulk decisions correctly and efficiently |

## New Responsive Access Request User Interface

The 7.2 release introduces a new responsive interface for tracking access requests that enables a user to see and manage their access requests, or those of someone else, across any device while using the same interface. This interface centralizes all the information related to an access request from the requested entitlements and roles to the owners and statuses.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| Responsive: Self-service request tracking | End users can now track their requests across any device all while having the same experience | Improves adoption and efficiency for users to track requests with a unified experience regardless of what devices they are using |
| Centralized functionality | Centralized layout of all the various components of a request – entitlements, roles, owners, requestor, requestee, status and more — in one place | Improve user efficiency by giving users full visibility into the progression of access requests |

## Versioned SCIM API

The 7.2 release provides our continued investment in a fully versioned API built to allow developers and implementers to extend the usage of IdentityIQ as a platform. This is in addition to the currently available APIs in the product.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| /policies endpoint support | Provides the ability to invoke IdentityIQ’s policy engine to check for existing policy violations and potential policy violations | Provides a backwards compatible interface for developers and integrators to invest in building extended use cases with the Open Identity Platform |
| /workflows endpoint support | Provides the ability to get workflow details, launch a workflow, and check results of a workflow | Provides a backwards compatible interface for developers and integrators to invest in building extended use cases with the Open Identity Platform |

## Plugin Framework Enhancements

The 7.2 release brings additional enhancements to the Plugin Framework within IdentityIQ. The Plugin Framework enables developers to extend the core IdentityIQ platform in a structured manner. This enables robust solutions meeting countless use cases to be delivered to customers in a standardized way.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| Internationalization | Plugins can leverage the same languages as IdentityIQ | With internationalization support, plugin developers can create plugins that support the same languages as IdentityIQ |
| Bundling IdentityIQ user interface components | Plugin developers have access to the same AngularJS components and libraries that IdentityIQ uses | Provides users with a seamless experience across IdentityIQ and plugins |
| Widget Support | Plugin developers can create widgets as plugins | Custom widgets can be created and installed on the homepage to meet a wide array of user needs |

## New Task Management User Interface

The 7.2 release introduces the new Provisioning Transaction Table which shows all the transactions that go through the IdentityIQ provisioning engine in a new interface which is easy and intuitive for administrators.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| New visual interface | Provides administrators with a summary and a detailed view of all tasks in an organized interface | Makes it easy for administrators to see at a high level, as well as at a granular level, the status of various tasks |
| Simplified ability to assign tasks to a server | Enables administrators to take proactive action on pending and failed transactions | Enables administrators to get users the access they need as safely and efficiently as possible |
| Ability to diagnose and take action on a task | Provides administrators the ability to get a stack trace, and cancel the task if necessary | Provides administrators with a single interface to get code-level task details in a single, user-friendly user interface |
| Maintenance windows | Applications can be placed into maintenance mode | When applications are placed in maintenance mode, tasks (such as aggregation) will not be run against an application, for ease of administration |
| Postpone Tasks | Provides the administrator the ability to postpone a task until a future time and date | Simple interface to see scheduled tasks and postpone or skip the task |

## Multifactor Authentication

The 7.2 release introduces an all new framework to support multifactor authentication (MFA) to be leveraged by users logging into IdentityIQ. Reference implementations for DUO and RSA MFA services have been provided by SailPoint to be used out of the box or as an example to build an integration with most third party MFA providers.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| Multifactor Authentication Reference Implementations | Workflows and configurations for DUO and RSA | Workflows and configurations for DUO and RSA |

## Privileged Account Management Module

IdentityIQ 7.2 adds to the Privileged Account Management (PAM) Module, that was released in 7.1P2, by adding the ability to search for containers by name.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| Container search by name | Ability to search for containers by names using “starts with” logic | Enables users of the PAM Module to more quickly locate containers |

# Connectors and Integration Modules Enhancements

## New Connectors

IdentityIQ 7.2 delivers new, out-of-the-box connectors for the following enterprise applications, which simplify connectivity to Active Directory Connector. The Active Directory Connector now supports Multiple Active Directory forests in a single IdentityIQ application, simplifying management of users across the enterprise's Active Directory.

| Feature / Enhancement | Description | Benefit |
|---|---|---|
| Active Directory | - Support for multiple Active Directory forests in a single application<br>- Enhanced Pass-Through authentication to support multiple forest<br>- Management for Cross-Forest memberships<br>- Enhanced delta aggregation performance with support for partitioned delta account aggregation<br>- Support for Exchange Mail-Enabled user | Active Directory Connector now can manage multiple forests within a single application. Support for multiple forests also enables the management of Foreign Security Principals |

## Azure Active Directory Connector – Pass-Through Authentication

In IdentityIQ 7.2 Azure Active Directory Connector includes pass-through authentication support for user login authentication.

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| Azure Active Directory Connector | - Pass-through authentication support<br>- Performance improvements | Azure Active Directory Connector now supports pass-through authentication, including support for out of filter scope users when user partitions are defined |

## Workday Connector – Aggregation filters

IdentityIQ 7.2 Workday Connector includes the capability to filter while aggregating to enhance aggregation performance.

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| Workday Connector | - Support for response filter<br>- Ability to pull reference IDs from workday system<br>- Independent users for read and write<br>- Update of mobile and phone.<br>- Update user id<br>- Support for updating custom attributes | - Customers can now filter the unnecessary data and aggregate only the useful data, including reference IDs<br>- Workday connector now supports using different users for read and write operations<br>- Support for phone numbers have been introduced<br>- Customers can now write back the "User Name" attribute in Workday<br>- Custom attributes can now be updated by the Workday connector |

## Mainframe Integration Modules – Performance and Security

IdentityIQ 7.2 Mainframe Integration Modules provide enhanced performance, ease of installation, and increased security.

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| Mainframe Integration Modules | - Improved resiliency in queue management<br>- TLS 1.2 communication support between Connector, Connector Gateway and agent<br>- RACF v4.0.01 released<br>- Support for passphrase<br>- Improved aggregation<br>- Ease of installation | Enhancements and fixes providing performance improvement, increased security, and ease of installation |

## New Integration Modules

IdentityIQ 7.2 Top Secret Integration Module can manage Top Secret connections to mainframes using the agent-less LDAP module.

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| New Integration Module | Top Secret LDAP | Ability to manage Top Secret Users, Groups, and Profiles using CA Directory Server for z/OS providing agent-less deployment using Top Secret LDAP |

## Additional Connectors and Integrations Modules Updates

IdentityIQ 7.2 also provides updates to a number of existing connectors and integrations to support expanded use cases and new versions of target systems.

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| Box | Support for JWT Authentication | Box Connector now supports JWT authentication, freeing users from having to manually refresh tokens within the connector configuration |
| Google Apps Connector | - Custom Schema attribute support<br>- Support for multiple domains<br>- Support for exponential backoff<br>- Improved performance for account and group aggregations | Google Apps Connector can now aggregate custom schema attributes. Multiple domains are now supported in a single application. |
| IBM i Connector | Support for TLS 1.2 | IBM i Connector now supports TLS1.2 |

**Connectors and Integration Modules Enhancements**

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| IQService | - Multiple instances support<br>- IQService executables are digitally signed | User can now deploy multiple IQService instances from the same host, enabling a single host for IdentityNow and IdentityIQ IQService instances in hybrid deployments |
| PeopleSoft Connector | Performance Improvement | Performance of connector is now improved to a significant level |
| SAP Direct Connector | Support for the contractual use type | SAP Direct now also supports contractual user type. It is now possible to set the License type |
| SCIM 1.1 Connector | Custom filter and patch operation support | Ability to manage SCIM 1.1 compliant server in enterprise environments using proxy servers |
| ServiceNow Connector | Support for ServiceNow Jakarta | ServiceNow Connector can be used to manage users and groups in ServiceNow Jakarta |
| SharePoint Server Connector | - Sub-site Support | SharePoint Connector now aggregates accounts and groups from SharePoint sub-sites. There is no impact to previous performance |
| UNIX and Linux Connectors | - Additional shell injection protection<br>- Performance improvements | Enhanced the security in Unix connectors and shell injection is now prevented. Also improved the Account and Group aggregation performance. |
| Epic Integration Module | - Support for ExternalId Password<br>- Corrected mapping of IdentityIQ disabled and locked accounts<br>- Added additional group schema for InBasketClassification<br>- Support for ContactComment<br>- Support for Default LinkedTemplate Id<br>- Support for ReportGrouper1, ReportGrouper2, ReportGrouper3 | Fully automated EMP record provisioning is now possible with support of these attributes |
| SAP GRC Integration Module | Support for additional parameters | Using additional parameters it is now possible to specify the SAP GRC Rule set, Risk Level and Report type  to be used for SOD analysis |

| Feature/Enhancement | Description | Benefit |
|---|---|---|
| ServiceNow Service Catalog Integration Module | Support for ServiceNow Jakarta | ServiceNow Service Catalog Integration Module can be used to enable ServiceNow Service Catalog requests for IdentityIQ in ServiceNow Jakarta |
| ServiceNow Service Integration Module | Support for ServiceNow Jakarta | ServiceNow Service Integration Module connector can be used to create service requests, incidents, and change requests in ServiceNow Jakarta |

# Connectivity Platform and Language Updates

## 3rd Party Platform Support Additions

The following 3rd party versions are supported in IdentityIQ 7.2:

| Component | New Version |
|---|---|
| Dropbox Connector | Dropbox Business API version 2 supported by Dropbox Server |
| HP Service Manager | HP Service Manager version 9.5 |
| ServiceNow Connector | Jakarta |
| ServiceNow Service Desk Integration Module | Jakarta |
| ServiceNow Service Catalog Integration (LIC) | Jakarta |
| Tivoli Access Manager Connector | IBM Security Access Manager for Web version 9.0 |
| Windows Local Connector | Windows Server 2016 |

## 3rd Party Platform Deprecated Support

The following 3rd party versions are not supported in IdentityIQ 7.2:

| Connector/Integration Module | Dropped Platforms |
|---|---|
| ServiceNow Connector | ServiceNow Fuji |
| ServiceNow Service Desk Integration Module | ServiceNow Fuji |
| ServiceNow Service Catalog Integration (LIC) | ServiceNow Fuji |

## Deprecated Connectors & Integration Modules

The following connectors and integration modules remain supported but will not appear in the *SailPoint Direct Connectors Administration and Configuration Guide* for 7.2. Deprecated connectors will be removed from the next version of IdentityIQ released one year after the release of IdentityIQ 7.2. The following connectors, connector components, and integration modules are no longer documented in IdentityIQ 7.2. Existing users of these connectors, connector components, and integration modules should begin to review options in advance of their planned enf of life:

- Connector for CyberArk
- IBM Tivoli Provisioning Integration Module
- Novell Identity Manager Integration Module
- Sun Identity Manager Integration Module
- BMC Service Request Management Integration Module
- Lieberman Enterprise Random Password Manager Integration Module

## End of Life Connectors & Integration Modules

The following connectors and integration modules were previously deprecated and are not present or supported in IdentityIQ 7.2:

- Rule-Based Logical Connector

# Important Upgrade Considerations

IdentityIQ 7.2 is a major release that contains numerous new features and capabilities across all areas of the product. A comprehensive plan should be created when upgrading that includes becoming familiar with the new features and changes, identifying use cases and how they are affected by the changes, creating a detailed strategy for migration of configuration and customizations, testing the upgrade process using data and system resources that are as close to the production environment as possible, and performing a complete deployment test cycle.

## Object Model Upgrade

The upgrade process will modify some of the IdentityIQ configuration objects. If XML representations of these objects exist outside of IdentityIQ for the purposes of version control or server to server migration, they should be re-exported from IdentityIQ or modified so that the desired upgrade is maintained if the objects are imported into IdentityIQ after the upgrade is complete.

The changes include:

- Application
    - The Base URL attribute of SCIM 2.0 applications is modified to add /scim/v2 due to the connector no longer automatically add this. See “SCIM 2.0 Connector” on page 12 for more information.
    - A new attribute is added to Duo applications to identify new sensitive application attributes that should be encrypted as application objects are saved.
- UIConfig
    - A new Aggregation Types column is added to the application list page defined in the applicationTableColumns entry.

  - The nativeIdentity column in the identityEntitlementGridColumns entry used in the entitlements list of the View Identity page is renamed to accountName to correctly describe the column content and to allow for a new nativeIdentity column to be added.

- WebResources
  - All URLs will be converted to match any extension.

## API Changes

- The `sailpoint.api.ExpiredPasswordException` class has been removed and replaced with the `sailpoint.connector.ExpiredPasswordException` class.
- All connector classes must be instantiated using the `ConnectorFactory` `getConnector` or `createConnector` methods so that a `ConnectorServices` instance can be injected to enable the use of the decrypt or `runRule` methods.
- The responsive UI framework libraries have been updated to AngularJS 1.6.3 and Bootstrap 2.5.0. Any custom web UI code might need to be updated to be compatible with these new versions.
- Custom task implementations will now receive attribute values for task attributes that are an application as application names instead of application ids. Any use of `SailPointContext.getObjectById` should be replaced with `getObject` or `getObjectByName`.
- The return type of the authenticate method of the `sailpoint.rest.AuthenticationFilter` class has been changed from boolean to `AuthenticationResult`. If custom code has been written to extend AuthenticationFilter: and the authenticate method was overridden, the signature of the overridden method will need to be changed to match. An `AuthenticationResult` constructor with a boolean argument can be used to make this change.
- The el-api and el-impl libraries have been removed from IdentityIQ as they are provided by all supported application servers.
- The IdentityIQ connector layer has been separated from the IdentityIQ server and its implementation is now contained in `WEB-INF/lib/connectorBundle.jar` instead of in `WEB-INF/lib/identityiq.jar. identityiq.jar` remains the primary jar file containing the identityiq server implementation.

## Third Party Libraries

Some third-party libraries have been removed and upgraded. It is imperative to follow the documented upgrade procedure to merge customizations and configuration into the new application binaries. If you extract the new binaries on top of an existing installation, you will end up with overlapping conflicts in libraries that will cause unpredictable errors.

## Access Review Configuration Options

The following Compliance Manager system configuration options have been removed based on changes included in the new access review user interface:

  - Default Access Review Grid View
  - Default Entitlement Display Mode
  - Subordinate Access Review Page Size
  - Initial Access Review View

- Require Bulk Certification Confirmation
- Prompt for Sign Off
- Enable Account Approval
- Enable Overriding Violation Remediator
- Enable Role Creation Requests From Certifications
- Additional Entitlement Granularity

The options above that were previously in the user preferences are also no longer available.

## Web Suggest Components

A SystemConfiguration option named columnSuggestBlacklist is now available to restrict sensitive data fields from being returned for drop-down suggest components. The value is a map of object type and object attribute pairs. The default entry includes the password attribute of Identity and all attributes of AuthenticationAnswer objects. Attribute names can be a comma separated list or a single asterisk to indicate all attributes. This can be important to assist creation of a balance between UI usability and leakage of sensitive information.

## Forgot Password

The forgot password flow will now return the user to the login page where they can use their reset credentials to authenticate instead of automatically authenticating and redirecting to the home page.

## Role Auditing

The target attribute of role create, modify, and delete audit events now contains the role type.

## Active Directory Connector

The Active Directory connector has been updated to include support for multiple forest configurations and cross-forest group memberships. The process for merging multiple Active Directory applications into a single application to use these new capabilities will require explicit planning, design, and implementation to meet deployment requirements.

## IQService

Multiple IQService instances can now be run on the same host. To support this feature, the registry entries that persist configuration details about an IQService installation instance have been reorganized. Uninstall the old IQService service before installing the new service so that the new registry entries will be created.

## SCIM 2.0 Connector

The SCIM 2.0 connector no longer adds `/scim/v2` to the Base URL and will now allow integration with SCIM servers that do not contain `/scim/v2` in the URL path.

All SCIM 2.0 connectors that do not contain `/scim/v2` in the Base URL value will have the value modified during the upgrade process to include this string. SCIM 2.0 applications that do not need to contain this string in the Base URL will need to be edited to contain the correct Base URL value after the upgrade is applied.

## SAP Portal Connector

The communication protocol between the IdentityIQ server and the servlet installed on the SAP Portal server has changed to provide resolution for a security vulnerability. This is the same change previously announced and provided in patches for earlier releases. When using IdentityIQ 7.2, this servlet must be upgraded to use the one provided with this release.

## Google Apps Connector

The Google Apps connector now supports managing multiple domains from a single application. The application attribute named domainName should be removed to enable this capability.

## Mainframe Agent Applications

The default number of concurrent transactions sent to the mainframe agent used to manage RACF, Top Secret, or ACF2 is now unlimited. To revert to the previous behavior of 10 concurrent transactions, add an application attribute named limitNumberOftransactions with a value of true.

## Connector Gateway

The communication protocol between the IdentityIQ server and the Connector Gateway has been changed to enable more resiliency in spurious network connections and invalid protocol. When using IdentiytIQ 7.2, the August 2017 version of the Connector Gateway must be used.

## RACF Connector

Starting with this release, all account creation provisioning requests for RACF must contain at least one group assignment.

The RACF connector can now make the group the owner of an account group connection when a group is assigned to an account. To enable this feature for existing RACF applications, add a splConnectionAttribute application attribute with a value that is a map with an entry of OWNER = true. The XML representation of this is

```
<entry key="splConnectionAttributes">
  <value>
    <Map>
      <entry key="OWNER"" value=""true"/>
    </Map>
  </value>
</entry>
```

All new RACF applications will enable this feature by default.

### PeopleSoft Connector

The format of the IDTypes attribute in the PeopleSoft connector has changed to add more consistency and prevent changes to application data when no change has occurred in the managed system.

### Target Associations

Identity Refresh is no longer required for target permissions to be visible in the Identity Warehouse. Target aggregation will now create identity entitlements for target permissions.

### SCIM PAM Bridge Plugin

The SCIM PAM Bridge Plugin must be updated to version 1.1 when using the PAM Module that is included with this release.

## Supported Platforms

#### Operating Systems

- IBM AIX 6.1 and 7.1
- Red Hat Enterprise Linux to 7.2 and 7.3
- Oracle Linux (Using RHEL Kernel Mode) 7.2 and 7.3
- SuSE Linux Enterprise Server 11 and 12
- Solaris 10 and 11
- Windows Server 2012 R2 and 2016

#### Databases

- IBM DB2 10.5 and 11.1

  **Note: IdentityIQ does not include the JDBC driver for IBM DB2. You must obtain the driver directly from IBM.**

- MySQL 5.6 and 5.7
- Microsoft SQL Server 2014 and 2016
- Oracle 11g R2 and 12c

  **Note: IdentityIQ includes the latest Oracle Database and SQL Server JDBC drivers at the time of the IdentityIQ release. Vendor documentation for the included JDBC drivers indicates compatibility across database server versions, but experience has shown some incompatibilities. You should obtain the latest database server version-specific JDBC driver from your database server vendor.**

#### Application Servers

**Note: JDK 7 and JDK 8 are supported as required by the specific application server.**

- Apache Tomcat 8.0 and 8.5
- IBM WebSphere 8.5.x

- JBoss Application Server Enterprise Application Platform 6.4 and 7.0
- Oracle WebLogic 12c Release 2 (12.1.2.x) and 12c R2 (12.2.x)

**Note: WebLogic 12c Release 3 (12.1.3) is not supported**

## Java Platform

- Sun, Oracle or IBM JDK 7 and 8

**Note: OpenJDK is not supported.**

## Browsers

**Note: If an unsupported browser is used, a notification appears in the lower right corner of the page. Hovering over the notification reveals a tool tip listing the supported browsers.**

- Firefox ESR 52
- Google Chrome 58
- Safari 10
- Windows Internet Explorer 11 and Edge

**Note: If you are using Internet Explorer on a server operating system with Enhanced Security Configuration enabled, you must add the IdentityIQ application server host to the Trusted Sites Zone in Internet Explorer using the Security tab of the Internet Options configuration dialog.**

## Mobile User Interface OS/Browser Support

- Android 5 and 6 using Chrome
- iOS 10 using Safari
- Windows 10 using Internet Explorer

## Languages

- Brazilian Portuguese
- Dutch
- English
- French
- Canadian French
- German
- Italian
- Japanese
- Korean
- Spanish
- Simplified Chinese

# Resolved Issues

Note: **SailPoint has changed the issue tracking system to achieve better consistency across all of our products and processes, and to better integrate with other tools. Due to this change, the issue label format has changed. All issues open at the time of the migration, or targeted for releases in progress at the time of the migration, now follow the new issue number format. SailPoint Support, your Customer Success Manager, or your Partner Manager can provide assistance if you have questions about this transition.**

**CONBOGIBEE-117:** Mainframe full connectors now expire passwords for newly created accounts and for accounts on which administrator has reset the password.

**CONBOGIBEE-135:** TLS 1.2 based communication is now supported between IdentityIQ and the Connector Gateway and between the Connector Gateway and mainframe agents for RACF, Top Secret, and ACF2 connectors.

**CONBOGIBEE-142:** Aggregation performance is improved for mainframe agent connectors using the 4.0.0.x versions of the mainframe agents.

**CONBOGIBEE-252:** TLS 1.2 based communication is now supported between IdentityIQ and the Connector Gateway and between the Connector Gateway and mainframe agents for RACF, Top Secret, and ACF2 connectors.

**CONBOGIBEE-380:** The Connector Gateway is now more resilient to random network connections and invalid communication protocol.

**CONBOGIBEE-450:** The RACF connector will no longer assign the group of the service account to an account during an account creation provisioning request that does not contain a group assignment.

**CONBOGIBEE-494:** The Windows Local connector now supports Windows Server 2016.

**CONCHENAB-687:** The Cloud Gateway no longer prints rule names in application server logs.

**CONCHENAB-732:** The Salesforce connector no longer causes NullPointerException when requesting a role with multiple permission sets.

**CONCHENAB-776:** The Remedy Service Integration Module now provides error messages with enhanced information in the logs.

**CONCHENAB-804:** The Workday connector no longer fails when aggregating an account without benefits data. Excluding benefits data from being read during aggregation is now configurable using the `excludeBenefitEligibility` key.

**CONCHENAB-809:** Revocation of a Salesforce or Remedyforce account in a certification will now disable the account since deleting the account is not supported by the managed system. The `deleteToDisable` property of the ProvisioningConfig must be set to `true` to enable this behavior.

**CONCHENAB-810:** The getObject connector method in an environment using the Cloud Gateway will now handle options and filters with an equals operand.

**CONCHENAB-824:** The SCIM 2.0 connector no longer adds /scim/v2 to the Base URL and will now allow integration with SCIM servers that do not contain `/scim/v2` in the URL path.

**CONCHENAB-917:** The Workday connector now provides support for updating custom attributes.

**CONCHENAB-952:** The Workday connector now supports additional business processes to aggregate future workers. The additional business processes can be configured using the Future_Data_Business_Process application attribute.

**CONCHENAB-1074:** The delta aggregation in the Workday connector now supports fetching terminated workers effective in the past. To enable this, add an application attribute named pastEffectiveDateOffset with a value of the number of previous days to consider while fetching changes.

**CONCHENAB-1320:** The version of cloud gateway can be determined from the `MANIFEST.mf` file present in the `IdentityIQCloudGateway.jar` on the cloud gateway.

**CONCHENAB-1402:** A ProvisioningPlan containing a comment object will be successfully executed when using the Cloud Gateway to provision.

**CONCHENAB-1523:** The Web Services connector now correctly creates an account object when the managed system create web service does not provide the native identity in the response.

**CONCHENAB-1524:** The Web Services connector can now combine multiple entitlement modifications into a single web service request by setting the application attribute addRemoveEntInSingleReq to `true`.

**CONCHENAB-1525:** The Workday connector will now aggregate terminated works correctly during delta aggregation when a effective date offset is not defined.

**CONCHENAB-1561:** The Workday connector will no longer incorrectly exclude some accounts on delta aggregation if the previous aggregation failed.

**CONCHENAB-1794:** The Workday connector now correctly populates HIRE_DATE/TERMINATION_DATE/CONTRACT_END_DATE attributes even if values of these attributes are in the last week of the year.

**CONCHENAB-1818:** Workday accounts will no longer show options to enable or disable the accounts in the Lifecycle Manager Manage Accounts flow due to lack of support in Workday.

**CONCHENAB-1839:** The Web Services connector now supports integration with web services that do not require authentication.

**CONCHENAB-1864:** The Salesforce connector will now fetch all the permission sets assigned to an account when the account is assigned a large number of permission sets.

**CONELLIS-684:** The Linux and Solaris connectors now support removing the home directory when deleting an account.

**CONELLIS-916:** The Unix connector and Delimited File connector no longer cause "Cannot read full block, EOF reached" exception when performing any operation.

**CONELLIS-959:** The Delimited File connector no longer causes SCP failures when running Test Connection. The Linux, Solaris and AIX connectors no longer causes SCP failures when running Account Aggregation and Preview Accounts.

**CONELLIS-1010:** The Siebel connector now correctly handles an "end of file" error and successfully aggregates all accounts.

**CONELLIS-1126:** The Delimited File connector now correctly terminates connections during file transfer using the scp protocol.

**CONELLIS-1268:** Aggregation using the Siebel connector no longer fails when an employee does not have a Position record.

**CONELLIS-1375:** The Solaris connector can now read the last login date and time for accounts.

**CONETN-65:** The LDAP connector now successfully provisions an account with a comma or a parenthesis in the Common Name (CN) within a Distinguished Name (DN).

**CONETN-92:** The Oracle Database connector now correctly displays the last login date for an account.

| |
|---|
| **CONETN-99:** The Delimited File connector no longer displays "Mark Invalid" error when previewing accounts or groups for a file with DOS or Windows line ending format. |
| **CONETN-108:** The Sybase connector now aggregates the accounts successfully when a database is created with 'for load' option in Sybase server. |
| **CONETN-149:** The Sybase connector now successfully provisions a server login account when a database is undergoing LOAD DATABASE in Sybase server. |
| **CONETN-222:** The Microsoft Exchange Online connector now de-provisions the license pack if all the licenses within the license pack are de-provisioned. |
| **CONETN-232:** The mailNickname, homeMBD, and msExchHideFromAddressLists attributes are now treated in a case insensitive manner when processed by the IQService. |
| **CONETN-948:** The Office 365 connector now correctly provisions multiple groups in a single request. |
| **CONETN-1023:** The SAP connector now displays an appropriate error message during partitioned aggregation when incorrect connection credentials are provided. |
| **CONETN-1407:** The SAP Portal-User Management Web Service Integration Module now aggregates all users from SAP Portal when the back-end is a database or LDAP. The .sda file provided with this release must be deployed on the SAP Portal server for account aggregation to bring in all the users. |
| **CONETN-1420:** The SAP connector no longer causes a NullPointerException when an entitlement is de-provisioned from an account through IdentityIQ and the entitlement was already detached in the SAP system. |
| **CONETN-1426:** The GoogleApps connector no longer fails the whole request when requesting entitlements for an account if the account has one of the entitlements already assigned to it in GoogleApps natively. |
| **CONETN-1438:** The SAP connector no longer shows the same error in case of failure of every provisioning operation. It will now show an error relevant to the provisioning operation. |
| **CONETN-1457:** The Active Directory connector no longer causes InvalidCastException when provisioning a Lync account. |
| **CONETN-1474:** The JDBC connector now successfully aggregates accounts when the SQL query begins with the keyword 'With'. |
| **CONETN-1479:** The SAP Direct Connector now supports multiple characters in Aggregation Partitioning Statement. |
| **CONETN-1593:** The Oracle E-Business Suite connector now provides an ability to include justification when provisioning a role or a responsibility for a user. |
| **CONETN-1595:** The Oracle HRMS connector will now fetch FIRST_NAME, LAST_NAME and MIDDLE_NAME of the user for account aggregation when added to the account schema. |
| **CONETN-1625:** The SAP Connector will now support unlocking of locked and disabled account without enabling it through self-service. |
| **CONETN-1675:** The Oracle E-Business Suite connector now displays the correct error when requesting an entitlement for an account that is already disabled in Oracle EBS natively. |
| **CONETN-1677:** The Lotus Domino connector now logs the complete exception when an account aggregation fails. |
| **CONETN-1687:** The Active Directory connector no longer crashes the IQService when bulk provisioning the special attributes for accounts using partitioned identity refresh task. |

**CONETN-1693:** The Lotus Domino connector now correctly provisions an account as NorthAmerican or International depending on the value provided for IDFileIsNorthAmerican attribute.

**CONETN-1701:** The Oracle E-Business Suite connector now supports aggregating and provisioning responsibilities of type Oracle Mobile Application as well.

**CONETN-1706:** The Oracle Database connector now correctly aggregates the direct permissions for the database roles.

**CONETN-1714:** The Active Directory connector now correctly aggregates the new group memberships when running delta aggregation using USNChanged mode if the user searchDN contains iterateSearchFilter (objectClass=User).

**CONETN-1716:** The SAP Direct Connector no longer fails with "java.lang.NumberFormatException" during Partitioned aggregation with multiple threads.

**CONETN-1720:** The Delimited File connector no longer runs the PostIterate rule when test connection is performed.

**CONETN-1727:** The PeopleSoft connector now successfully removes the single-values entitlements such as Navigator Home Permission List, Primary Permission List, Process Profile Permission List, and Row Security Permission List.

**CONETN-1729:** The Oracle E-Business Suite connector now updates the Record history in Oracle EBS natively with an EBS user, that is a user created through Oracle EBS portal, instead of non-EBS user, when provisioning an account. The application configuration attribute E-Business Proxy User will need to be populated with such a user to achieve the desired results.

**CONETN-1736:** Account aggregation performance using the Sybase connector is now improved when scanning a large number of databases.

**CONETN-1741:** The Active Directory connector no longer appends the attribute value to an existing value for a "set" operation when provisioning an account.

**CONETN-1760:** The Azure Active Directory connector can now skip attributes not supported by the Graph API using a configurable key `excludeAttributesFromProvisioning` when provisioning an account.

**CONETN-1762:** The LDAP connector no longer fails when provisioning a boolean value for an attribute.

**CONETN-1780:** The Top Secret connector now correctly recognizes all success return codes from the mainframe agent.

**CONETN-1792:** The Active Directory connector no longer causes NullPointerException when running account aggregation for an application running on IBM WebSphere Application Server.

**CONETN-1795:** The Active Directory connector no longer causes StringIndexOutOfBoundsException when running Refresh Identity Cube task with **Refresh identity attributes** option enabled.

**CONETN-1808:** The SAP HR connector will now also aggregate Company Name of an account during account aggregation.

**CONETN-1829:** The Active Directory IQService now provisions MS-Exchange related attributes for a user on the same Domain Controller where the user is provisioned.

**CONETN-1846:** The error logging in mainframe connectors has been changed to log unexpected unsupported operations instead of failing the operation.

**CONETN-1852:** The Active Directory connector will now clear the description attribute when provisioned with empty string.

**CONETN-1858:** The Linux connector now correctly displays "method" in the exception output instead of "menthod".

| |
|---|
| **CONETN-1860:** the JDBC connector will now aggregate direct permissions of an account during account aggregation. |
| **CONETN-1894:** The Active Directory connector will now use the same server for all operations related to updating an account to prevent issues caused by replication delays. |
| **CONETN-1895:** The GoogleApps connector now correctly provisions all the complex attributes while creating an account. |
| **CONETN-1907:** The Active Directory connector no longer causes NullPointerException when provisioned with blank value. |
| **CONETN-1916:** SAP Direct Connector no longer fails with "Unable to find any additional information for this account group" error when displaying profile attributes of an account. |
| **CONETN-1935:** In the IBM Lotus Domino connector account schema, the attribute name in the create provisioning policy for Name of the explicit policy is changed from 'PolicyName' to 'Policy'. |
| **CONETN-1936:** The SAP GRC Integration now supports passing the additional parameters, RiskLevel, ReportType and RuleSetId, to the SAP GRC Proactive Risk Analysis Webservice. |
| **CONETN-1941:** The Active Directory connector now returns attribute level results by setting the setAttributeLevelResult application attribute to true. |
| **CONETN-1949:** The Active Directory connector will now provide the mS-DS-ConsistencyGuid attribute in a readable string format. |
| **CONETN-1958:** The DelimitedFile connector now returns correct results consistently for all operations when an exception is thrown in the Pre-Iterate Rule. |
| **CONETN-1994:** The mainframe connectors no longer fail a request but instead provide a warning when provisioning changes are already on the account in the managed system. |
| **CONETN-2018:** The LDAP connector no longer logs the clear text password in diagnostic logs when provisioning to Simple AD (AWS AD platform). |
| **CONHELIX-207:** Now EPIC Connector aggregation create less temporary files in Tomcat Temp folder, thus avoids disk space issue. |
| **CONHELIX-231:** The EPIC connector no longer fails with a Fault Message when performing Test Connection or when aggregating accounts with SOAP version 1.2. |
| **CONHOWRAH-451:** The Azure Active Directory connector no longer causes ObjectNotFoundException when provisioning an account with large number of 'userPartitions' defined in the application. |
| **CONHOWRAH-575:** The Azure Active Directory connector now releases all the system resources once the request is processed. |
| **CONHOWRAH-611:** The Azure Active Directory connector now correctly authenticates user having the spaces in userPrincipalName attribute during passthrough authentication. |
| **CONHOWRAH-613:** The Azure Active Directory connector now successfully provisions an account when partitions are defined using filters. |
| **CONHOWRAH-676:** The Azure Active Directory connector now supports pass-through authentication feature. |
| **CONHOWRAH-863:** New scoping attributes userFilters/groupFilters are being introduced in Azure Active Directory connector which will be used while performing account/group aggregation and pass-through authentication. |

**CONHOWRAH-935:** The Azure Active Directory connector now correctly provisions the licenses when one license plan is present in two or more license packs.

**CONHOWRAH-942:** The Active Directory connector now provides a new configuration attribute to force a Domain Controller to not send referrals when aggregating accounts.

**CONHOWRAH-943:** The Active Directory connector no longer searches for group memberships for an account when aggregating accounts from a single domain Active Directory configuration.

**CONHOWRAH-1000:** The Azure Active Directory connector now has improved performance for provisioning operations due to no longer reading an account after a provisioning operation that does not have known side effects.

**CONNAMDANG-671:** The JDBC connector no longer throws an out of memory exception during aggregation for large data sets. The Resultset of TYPE_FORWARD_ONLY (for example, the result set cannot be scrolled) is required processing large data sets.

**CONNAMDANG-690:** The JDBC Connector now supports merging of data when the type of a resultset is TYPE_FORWARD_ONLY (for example, the ResultSet cannot be scrolled).

**CONNAMDANG-967:** Oracle Database connector now supports Oracle DB 12cR2.

**CONPAMBAN-95:** The Generic LDAP connector now correctly aggregates an account with a \ in its name.

**CONPAMBAN-224:** The LDAP connector now correctly reads group membership changes during delta aggregation when the distinguishedName of a user contains spaces.

**CONPAMBAN-256:** The RACF LDAP and SunOne LDAP connectors are now enhanced to retry failures while provisioning group memberships.

**CONPAMBAN-263:** The LDAP connector now supports setting integer type attributes during provisioning.

**CONPAMBAN-367:** LDAP connector now correctly brings membership changes for accounts as per scope defined in application when running delta aggregation.

**CONPAMBAN-426:** The Google Apps connector now supports managing users across multiple domains present in an organization.

**CONPAMBAN-440:** The Google Apps connector now retries requests that fail due to a 'Rate Limit Exceeded' error using an exponential back-off method.

**CONPAMBAN-445:** The RACF LDAP connector now correctly provisions account when '#' character is present in the beginning of racfid attribute.

**CONPAMBAN-455:** The BMC Remedy connector no longer causes ClassCastException when requesting multiple entitlements for an account using an IT role.

**CONPAMBAN-480:** The BMC Remedy ITSM connector now correctly provisions account when requesting multiple entitlements using IT role.

**CONPAMBAN-530:** The BMC Remedy connector and BMC ITSM connector now correctly provision multiple entitlements for an account when requested using an IT Role

**CONPAMBAN-571:** The LDAP connector now has better handling of special characters present in the distinguishedName attribute of accounts and groups during aggregation.

**CONPAMBAN-619:** The SunOne LDAP connector no longer requires restoreVal and revokeVal to be defined for enable or disable to be successful.

**CONPAMBAN-638:** The Google Apps connector now displays the page size on the application configuration page with a default value of 100.

**CONPAMBAN-641:** The IQService now supports running multiple IQService instances on same Windows host.

**CONPAMBAN-645:** The RSA connector now supports RSA Authentication Manager 8.2 SP1.

**CONPAMBAN-665:** The IQService binaries are now digitally signed.

**CONPAMBAN-763:** The Google Apps Connector now supports aggregating custom schema attributes defined on the target system.

**CONSEALINK-430:** The ServiceNow launch in context integration no longer fails when requesting an entitlement for self and auditing for provisioning is enabled.

**CONSEALINK-436:** The Remedy service integration module now creates a single ticket, instead of multiple tickets, when an account having multiple entitlements is revoked during certification.

**CONSEALINK-448:** The ServiceNow launch in context integration no longer fails when requesting an entitlement for self and auditing for provisioning is enabled.

**CONSEALINK-456:** HP Service Manager Service Integration Module no longer causes a transport error when creating a ticket.

**CONSEALINK-478:** The ServiceNow connector now supports generic partitioned aggregation.

**CONSEALINK-512:** The ServiceNow SIM now uses a 3rd-party library dependency in a way that pro-actively closes file handles in the application server's temp folder that are left open, thus avoiding limits on open files and the possibility of running out of disk space.

**CONUMSHIAN-127:** The SAP HR/HCM connector now successfully provisions the email, telephone, and system username for a future hire.

**CONUMSHIAN-571:** The SAP HR/HCM connector updates the account with latest data if a new record of type Personal Data, Address Data, or Communication Data is created for an employee natively.

**CONUMSHIAN-808:** The Peoplesoft connector no longer updates identities after aggregation if there is no change in native system.

**CONUMSHIAN-858:** The SAP connector now supports provisioning of License Data for a SAP user.

**CONUMSHIAN-894:** [SECURITY] The SAP Portal-User Management Web Service connector no longer allows unauthorized access to objects in SAP Portal Enterprise Server.

**CONVASHI-14:** The sailpoint.api.ExpiredPasswordException class is deleted. It is changed to use the new package `sailpoint.connector.Expired`PasswordException.

**IIQCB-648:** PasswordGenerator class added to `javadoc.` API changed

**IIQCB-668:** The Forwarding Start Date and Forwarding End Date user preferences can no longer be set for a date in the past.

**IIQCB-763:** Sunset dates are now supported for remove access requests.

**IIQCB-764:** A system error no longer occurs when all identities are removed from the scheduling interface for an ad-hoc certification.

**IIQCB-806:** The View menu of the Report Results list is now correctly localized.

**IIQCB-878:** [SECURITY] Elements that retrieve data for drop-down suggest components can be configured to restrict sensitive data fields from being returned.

**IIQCB-984:** The login page will now correctly be displayed when continuing after a session timeout.

**IIQCB-1049:** Removed old JSF pages related to policy violations, see *https://harbor.sailpoint.com/docs/DOC-20277* for details.

**IIQCB-1220:** [SECURITY] Vulnerabilities related to escaping the Angular expression sandbox have been removed.

**IIQETN-14:** Users not authorized to manage roles no longer see a Role Editor link in the work item detail view.

**IIQETN-162:** The French translation for a line item in a revocation work item is now correct.

**IIQETN-174:** Quicklink filters now have the capability to include the requester if 'self' is enabled.

PATCH RELEASE NOTES ONLY AFTER THIS This requires a minor change to the IdentitySelectorConfiguration for the LcmPopulation entry. Change the getConfiguredIdentityQueryOptions call to return `svc.getRequestableIdentityOptions(identity, null, "requestAccess");` for 7.0 versions and return `svc.getRequestableIdentityOptions(identity, null, null, "requestAccess");` for versions 7.1 and beyond.

**IIQETN-211:** Identity requests with a create operation will correctly retry attribute requests that fail initially and will properly mark the final status after all retries have completed.

**IIQETN-243:** The Access Request approval and provisioned status are now correctly updated by the Perform Identity Request Maintenance Task.

**IIQETN-284:** Provide for new actions on task definitions to configure how task results are named to avoid slowdowns due to name collisions.

**IIQETN-293:** Custom forms now have all fields and buttons included in the tab order for keyboard navigation.

**IIQETN-640:** Returning reassignments of an access review no longer create potential to corrupt the parent-child relationship of the original access review.

**IIQETN-1183:** The **extendedSchema** CLI command will now create DDL with the correct field size for extended attributes consistent with the schema CLI command.

**IIQETN-1223:** Session management for group objects is now improved to prevent failures during Active Directory delta aggregation.

**IIQETN-1437:** SAML authentication now properly handles a session timeout.

**IIQETN-1571:** Searching in Advanced Analytics will correctly display the count of the total number of objects returned by the query.

**IIQETN-1579:** The usability of the role owner field in the role editor has been improved to show the current value when a new value is not selected using the suggest component.

**IIQETN-1659:** The German localization is now updated to correct non-localized text..

**IIQETN-1740:** Impact analysis when checking for policy violations in a request no longer has the potential to prematurely show account changes..

**IIQETN-1806:** The Spanish localization is now updated to correct non-localized text in navigation menus.

**IIQETN-1807:** The Japanese localization is now updated to correct non-localized text in QuickLink and navigation menus.

**IIQETN-1808:** The Portuguese localization is now updated to correct non-localized text in navigation menus and application configuration.

| |
|---|
| **IIQETN-1840:** Certifications are now reattached to the session after phase rules run in order to prevent rules that perform decaches from causing LazyInitialization errors. |
| **IIQETN-2463:** Identity requests in Incomplete status can now be searched in Advanced Analytics via the Completion Status field. |
| **IIQETN-3112:** Sequential tasks will now continue to execute even when one of the contained tasks fails due to an exception and the sequential task is configured to continue to execute. |
| **IIQETN-4215:** The Remove Access tab under the Manage User Access quicklink now performs better with Identities that have a large number of Entitlements already assigned. |
| **IIQETN-4256:** Allow an Entitlement Catalog import with empty owner values to remove the Managed Attribute owner. |
| **IIQETN-4258:** A warning is now logged instead of a NullPointerException when managing user access and there are missing IdentityRequest objects. |
| **IIQETN-4264:** A `textarea` field used in a custom form now correctly displays a string value containing carriage returns. |
| **IIQETN-4265:** In a Form, a date field marked as dynamic no longer creates an error when the postback executes. |
| **IIQETN-4280:** The correct date and time is now displayed for each timezone in the Identity Warehouse. |
| **IIQETN-4296:** Workflows now terminate correctly following a cancellation from the user interface. |
| **IIQETN-4327:** An account attribute of type boolean that is marked as an entitlement no longer causes an exception when viewing an IdentitySnapshot that contains that attribute. |
| **IIQETN-4339:** A ConcurrentModificationException no longer occurs when **Save Changes** is selected during an access review after performing multiple challenge rejections. |
| **IIQETN-4352:** Date fields now respect local date formats, including locales not in the default installation, such as en_NZ. |
| **IIQETN-4377:** Inherited Entitlements now displays correctly on the Role Management page when a parent IT role has no entitlement profile. |
| **IIQETN-4398:** When an account already exists for an identity during a request, the New Account popup window no longer appears when the configuration does not allow additional accounts to be requested. |
| **IIQETN-4424:** When the logged-in user is making a comment on a workitem, the user's workgroup memberships will be evaluated to display the proper text and perform the correct action. |
| **IIQETN-4433:** All XML HTTP requests (XHRs) must contain a cross-site request forgery (XSRF) protection token to maintain security of the server connection. The XSRF token is now being set correctly in HTTP requests, preventing session failures that would result in a user being logged off. |
| **IIQETN-4437:** The filters applied to delegation and reassignment drop-downs inside an access review can now be configured with a separate identity selector configuration for each using the keys `delegationAssignee` and `reassignAssignee` inside the IdentitySelectorConfiguration. |
| **IIQETN-4448:** The Access Request page no longer results in a timeout when accessing a large number of requests when using an Oracle database. |
| **IIQETN-4481:** On the Access Request selection pages, scopes are no longer applied to the Filters that select entitlements and roles because the rules that limit the available entitlements do not necessarily utilize scopes. |
| **IIQETN-4493:** A read-only date field in a custom form can now have its initial value set by a script. |

**IIQETN-4496:** The requester of a role now has access to see the entitlements from the Entitlements tab of the Approval Workitem page.

**IIQETN-4533:** An Identity Mapping target application on a suggest window is now displayed if it is not on the first page of suggestions.

**IIQETN-4546:** Application names containing special characters, such as "\", are now escaped to ensure proper processing and display in the user interface.

**IIQETN-4553:** Selecting the recipient for a workitem forwarding by pressing the Enter key no longer causes a validation error.

**IIQETN-4576:** The date picker component no longer has stray boxes when used in Internet Explorer 11.

**IIQETN-4579:** The **Revoke Completed** flag for Account Group Membership certifications now shows the correct status in the Account Group Membership Access Review Live Report.

**IIQETN-4580:** The Policy Violation Remediation Dialog no longer allows a Delegated Certification Item for a Role to be selected to Revoke while in the Delegated state.

**IIQETN-4584:** The search box for scheduled tasks can now have a SearchInputDefinition associated with it so that the search type can be modified from the default "starts with" filter.

**IIQETN-4603:** A special character in a comment is now processed correctly and no longer displays as its HTML escape code equivalent.

**IIQETN-4631:** Ignoring a policy violation no longer raises an error message when the requester is the owner of the manual action in an interactive policy violation scheme.

**IIQETN-4635:** Entitlement display names beginning with an underscore character no longer result in repeated and missing listings of the entitlements in the Request Access page.

**IIQETN-4637:** The description for the application filter on the Access Review Signoff Live Report now indicates when and by whom an access review was signed off.

**IIQETN-4651:** Auto-close processing of certifications now prevents multiple sign-offs by ensuring only certifications that haven't been signed yet are processed.

**IIQETN-4652:** The IIQClient utility class now supports the setting of `maxHostConnections` and `maxTotalConnections` in `iiqClient.properties` to scale up the number of concurrent connections created by the client.

**IIQETN-4668:** The `IdentityLibrary.refreshIdentities()` method called with duplicate identities now properly refreshes without losing roles when called from a workflow.

**IIQETN-4669:** JNDI datasources are now supported when deploying on JBoss server with an Oracle database.

**IIQETN-4674:** The Perform Maintenance task no longer fails to close a certification if it encounters an EntitlementSnapShot containing a boolean value.

**IIQETN-4682:** When an approval is submitted for completion, the **Complete** button in the footer of the approval form is disabled to prevent multiple submissions.

**IIQETN-4689:** Deep links that contain entitlement attribute filters now display the correct search results.

**IIQETN-4697:** Decisions made on a reassigned certification no longer lock its parent certification.

**IIQETN-4712:** The certification widget on the dashboard is now Section 508 compliant with respect to access reviews.

**IIQETN-4718:** The History tab in the Identity Warehouse no longer throws a NullPointerException when displaying Identity Certification items with a null Certification Action.

**IIQETN-4719:** Paging in Report Results and Task Results now works more consistently when a row is deleted from any page of results being viewed.

**IIQETN-4726:** Role change propagation now completes successfully for users with multiple accounts on the applications involved in the role change.

**IIQETN-4738:** When creating a new form, the form type selection list in the Create New Form dialog is now localized.

**IIQETN-4742:** When there are multiple accounts associated with a set of related roles, and a role changes, the role change propagation task will correctly issue provisions for the proper account.

**IIQETN-4753:** When viewing the Object Properties tab for an entitlement from an access review, the groups are displayed as a itemized list rather than an unbroken string to ensure better legibility.

**IIQETN-4759:** The `IdentityLibrary.refreshIdentity()` method now updates identity attribute changes from an IdentityTrigger when called from a workflow.

**IIQETN-4765:** A deep link SailPoint Service Catalog (LIC) integration request for a Request Access operation now automatically starts at the Manage Access screen with the target user selected that is specified in the URL.

**IIQETN-4792:** [SECURITY] When required by the application definition, the current password for the account is now always validated on a user-initiated password change through Manage Password.

**IIQETN-4800:** The Identity Refresh task no longer throws a NullPointerException when processing poor quality Identity Request items, such as those with a null Identity Request.

**IIQETN-4805:** When viewing the complete details of an access request, the items in the Interactions table are now correctly paginated.

**IIQETN-4812:** A logical application entitlement request no longer results in a blank entry in Track My Requests.

**IIQETN-4814:** From Track My Requests, a user with the required authorization who executes an advanced search by requestee no longer encounters an error.

**IIQETN-4821:** There is no longer the possibility of a NullPointerException because of a null target type on a Target Association when browsing an identity's effective access from the Entitlements tab.

**IIQETN-4828:** [SECURITY] The display names for objects in some multi-select suggest components are now encoded to prevent an XSS vulnerability

**IIQETN-4831:** In the Identity view, the fields associated with the **Change Forwarding User** option are no longer duplicated.

**IIQETN-4842:** The scalability of the Manage Passwords account selection grid has been improved

**IIQETN-4844:** A user is now prevented from requesting the same role for an identity when it has already been assigned with a future activation date and the system configuration doesn't allow multiple role requests for the same application.

**IIQETN-4846:** Optimized IdentityRequest deletion for requests with many request items.

**IIQETN-4850:** An approver is now allowed to have access and take action on the approval work item when navigating through Track Request and then Click for Details.

**IIQETN-4875:** To prevent possible duplicate identity entitlements, an Identity Request must be in an approved state before an entitlement is created.

**IIQETN-4888:** Requiring comments for Certification Item Revokes now works similarly to requiring comments for Certification Item Approvals. To require comments for Revokes, enable requireRemediationComments in the System Configuration xml. For example:

```
<entry key="requireRemediationComments" value="true"/>
```

**IIQETN-4890:** When the Refresh Role Scorecard Task Definition is missing, an error is now logged and the score card grid is cleared.

**IIQETN-4897:** [SECURITY] An XSS vulnerability associated with the comments field of an access request work item has been removed.

**IIQETN-4903:** The workflow flag asyncCacheRefresh is now allowed as a variable that is recognized throughout the provisioning process.

**IIQETN-4904:** Non-encrypted authorization for SMTP is now supported.

**IIQETN-4919:** The Perform Maintenance task no longer activates staged certifications, and no longer goes into an infinite loop when attempting to activate certifications that have advanced past the active phase.

**IIQETN-4927:** Entitlement Request Items now correctly show in Access Requests when the request causes an account creation but has no explicit account name, and when that account and entitlement are added to the identity after the request was made but before the request is approved.

**IIQETN-4931:** Selecting a QuickLink after navigating to the Dashboard from an incomplete workitem now correctly directs to the expected QuickLink page instead of displaying the Work item Not Found page.

**IIQETN-4943:** An email notification is now sent to the delegator of a certification when a delegated work item is completed.

**IIQETN-4948:** Processing of provisioning plans containing attribute changes associated with multiple tracking IDs is now improved.

**IIQETN-4952:** [SECURITY] A resource to get identity attributes has been protected to restrict users without appropriate authorization.

**IIQETN-4954:** [SECURITY] CSV file fields which potentially contain formula injections are now quoted to prevent exploitation of command execution in Excel.

**IIQETN-4956:** [SECURITY] A web service to reassign a work item has been protected to restrict work item assignment without appropriate authorization.

**IIQETN-4964:** A Role is now displayed in Role Manager even when the Application it references is not defined.

**IIQETN-4968:** When attempting to save a bulk decision in an access review after applying some filters, a ClassCastException error will not be emitted.

**IIQETN-4969:** Form fields having an enabled postBack setting now correctly display validation error messages.

**IIQETN-4971:** Duplicate entitlements are no longer saved when editing a role profile.

**IIQETN-4988:** Performance of certification finishing using the Perform Maintenance Task is improved by no longer attempting to correlate entitlements with their respective assignment when no assignments exist.

**IIQETN-4996:** The entitlement description is now displayed in the Object Properties tab of the Entitlement Detail popup in the Access Review page.

**IIQETN-5001:** Viewing an Access Review for a Certification no longer causes a NullPointerException when an Identity AccountSelection object does not have any accounts.

**IIQETN-5010:** When attempting to reassign an item in an access review, the configured identity selector on the reassignAssignee selector will not be ignored, which would allow any identity to be selected.

**IIQETN-5012:** Provisioning Plan compilation no longer adds account requests to the wrong applications.

**IIQETN-5028:** The address parameter within the SubjectConfirmationData of a SAMLResponse no longer results in validation failure.

**IIQETN-5039:** Requiring comments for Account Revokes now works similarly to requiring comments for Certification Item Approvals. To require comments for Account Revokes, enable requireAccountRevokeComments in the System Configuration xml.  For example:

```
<entry key="requireAccountRevokeComments" value="true"/>
```

**IIQETN-5041:** During Aggregation, incomplete ResourceObjects no longer set the displayName to the Identity when the displayName is not set on the object.

**IIQETN-5056:** Triggers processed during aggregation now persist changes made by the trigger.

**IIQETN-5057:** Performance and data access payloads have been improved in some cases when retrieving entitlements for creating access reviews during certification generation and when finishing them from the Perform Maintenance task.

**IIQETN-5060:** Changing the duration of an active and reassigned certification no longer incorrectly changes the due date.

**IIQETN-5061:** The Perform Maintenance task processes certification revocations faster, especially when the revocations are on identities who have thousands of CertificationItems, each with thousands of entitlements.

**IIQETN-5063:** Oracle Database deadlocks during aggregation are now prevented.

**IIQETN-5068:** The Certification Campaigns widget will correctly load the proper certifications consistently.

**IIQETN-5076:** Using a bulk Clear Decision from the Identity View no longer results in a certification being auto-closed without a decision.

**IIQETN-5079:** The account request section of a provisioning plan will no longer have duplicate assignment ids.

**IIQETN-5083:** Custom identity attributes are now included in a PDF or CSV export of the results when using them in an Advanced Analytics identity search.

**IIQETN-5091:** Date fields are no longer incremented by postback fields when the browser is in a timezone ahead of GMT.

**IIQETN-5095:** Access reviews will show the display names instead of the values in the Display Name column for all types of entitlements.

**IIQETN-5097:** Partitioned account aggregation now consistently updates the 1000th account needing to be refreshed.

**IIQETN-5099:** When requesting access or viewing effective access for identities with a large number of existing entitlements, the page will not show an error and the performance has been improved.

**IIQETN-5102:** The P6Spy jar file is now correctly named.

**IIQETN-5104:** Scheduled requests involving new accounts no longer result in duplicate entitlements.

**IIQETN-5108:** The user selection list in the forwarding pop-up window now remains on top and visible after clicking the field to populate it.

**IIQETN-5113:** An Identity request item to disable or enable an account now shows any constituent attribute or permission requests contained within the request.

**IIQETN-5114:** The Environment Information Report no longer throws an exception when the installation path of the application server contains spaces.

**IIQETN-5117:** Identity creation rules will now be run even if the name of an identity to be created matches an existing workgroup name.

**IIQETN-5118:** In a Form object, a multi-valued attribute that is set as required now has an asterisk next to the field when the Form is displayed for a user.

**IIQETN-5122:** Options available from a drop-down suggest list in some places are no longer invisible until hovered with the cursor.

**IIQETN-5124:** Custom forms with ManagedAttribute type fields can now handle commas as input without being cleared out during a postback refresh of the form.

**IIQETN-5128:** [SECURITY] When changing passwords, the current password value is now encrypted when stored in a workflow case.

**IIQETN-5129:** Exceptions during provisioning are now captured and logged as well as prevented from causing cascading failures when the identity is unlocked once the provisioning step is completed.

**IIQETN-5134:** The RequestedAuthnContext can now be excluded from SAML requests by setting `authnContextClassRef="noRequestedAuthnContext"` in the SAMLConfig.

**IIQETN-5137:** Access requests to be split, made by a potential approver but rejected by an earlier approver in the process, no longer result in additional workitems.

**IIQETN-5149:** The identity details in delegated work items no longer creates an error when clicking on the identity's name to expand it

**IIQETN-5151:** The Perform Maintenance task processes revocations on accounts with thousands of entitlements much faster while finishing certifications.

**IIQETN-5152:** Policy Violation remediations now correctly send email notifications.

**IIQETN-5176:** LCM requests for roles with no associated entitlement profiles will not result in errors.

**IIQETN-5270:** The identityId variable is now present in the context of identity provisioning form scripts.

**IIQETN-5271:** When the Perform Maintenance task is run, duplicate Master Plan attributes and ProvisioningPlan objects no longer exist in the IdentityRequest after being processed by workflow that checks status of queued items.

**IIQETN-5311:** When using role requests with sunrise dates, and the enableManualAccountSelection variable is false in the Scheduled Assignment business process, the original account selection of a new or existing account is correctly used when the sunrise date occurs.

**IIQETN-5312:** On the Identity Entitlements tab, multiple role requests for the same role now correctly show their respective Access Request.

**IIQETN-5317:** The role details are displayed and the page properly loads when selecting an archived role in the role editor.

**IIQETN-5318:** The **textSearch** command from the console is now functional. You will need to use the index name instead of the class name (usually this is BundleManagedAttribute). To narrow on types, use a search like: `textsearch BundleManagedAttribute <search string> objectClass Bundle`. Multiple filters can also be specified.

**IIQETN-5342:** When policies are set to send alerts, but not create work items, they correctly do so, rather then opening work items and not sending alerts.

**IIQETN-5351:** Entitlement SODs are now detected during creation of a scheduled assignment.

**IIQETN-5352:** Identity requests may be searched in Advanced Analytics using all Completion Statuses.

**IIQETN-5366:** Postbacks no longer clear validation messages on UpdateIdentity forms.

**IIQETN-5367:** Account Group aggregation tasks support a maximum threshold for object deletion, and will cause the aggregation to halt when that threshold is reached.

**IIQETN-5369:** Bulk decisions inside of an access review will all take effect even when the Group By functionality in a filter is used.

**IIQETN-5376:** Requester comments from the original request are propagated across approvals and also now display on manual provisioning work items.

**IIQETN-5380:** [SECURITY] Users are now restricted from viewing rules that should be inaccessible to them without the proper permissions.

**IIQETN-5398:** Roles containing entitlements from multiple manually provisioned applications with multiple owners that are revoked during a certification will create provisioning workitems whose owner will default first to the role owner (if the system configuration entry remediationToRoleOwnerOverDefault is enabled) and then to the defaultRemediator setting in the system configuration.

**IIQETN-5402:** [SECURITY] Users are now restricted from editing rules that should be inaccessible to them without the proper permissions.

**IIQETN-5403:** There is now a field level attribute to prevent the normalization of a date selection to noon GMT in the date field of a form. Disable the normalization by setting the attribute notNormalized to true on the date field in the form.

**IIQETN-5404:** The Check Expired Work Items task no longer sends duplicate notifications if a certification is expired.

**IIQETN-5407:** The Additional Entitlement Granularity field on the advanced tab of a certification configuration is now displayed consistently.

**IIQETN-5420:** When a boolean attribute is used in the option **Share attributes with the requester** in a QuickLink Population, the Manage User Access link will work correctly and login will not be disrupted.

**IIQETN-5422:** The Prune Identities task summary now correctly reports identities owning remediation items as protected instead of aborting with a deletion error.

**IIQETN-5428:** During an LCM request, suggested values in the Filters section of Manage Access are now limited by the same restrictions as the entitlements and roles being requested.

**IIQETN-5442:** Application specific attribute sources and targets for identity mapping are now successfully deleted when the application is deleted.

**IIQETN-5454:** For role change approvals, the display name of the role now shows the old and new value if that was one of the changes that triggered the approval.

**IIQETN-5457:** The ability to rename a workgroup using the console is now supported.

**IIQETN-5464:** The in-page back button on various pages, including access request details, now properly redirects the user to the previous applicable area, rather than to the dashboard.

**IIQETN-5473:** When exporting an Audit search to CSV or PDF in Advanced Analytics, the interface attribute will also be exported.

**IIQETN-5474:** When viewing an identity, the Entitlements tab is more tolerant of malformed idx columns related to assigned and detected roles, and allows the page to load despite these issues.

**IIQETN-5494:** [SECURITY] Web access control lists for delegated administration authorization are now correctly applied to all defined URLs.

**IIQETN-5498:** Detected role summary values containing multi-byte characters and total byte lengths greater than 2000 no longer cause DB2 SQL errors.

**IIQETN-5513:** Custom connector applications in which provisioning policies have no fields will not result in errors during account group editing.

**IIQETN-5527:** When the certifier of an access review is a workgroup, and the members of the workgroup are also entities in the access review, the self-certification prevention rules will be triggered.

**IIQETN-5530:** Modifications and subsequent saves to an Approve and Provision Subprocess workflow approval step in the Business Process Editor no longer cause errors.

**IIQETN-5556:** Filtering on the **Setup -> Roles** page no longer prevents a subsequent role search in Advanced Analytics from being able to search for a selected role.

**IIQHH-265:** Exported TaskDefinition objects now contain a reference to GroupAggregationRefresh rules by name and not id.

**IIQHH-266:** A CertificationDefinition in the XML representation of a TaskSchedule can now be referenced by name.

**IIQHH-267:** The **Exclude Identities marked inactive** identity refresh task option no longer causes the population filter to be ignored.

**IIQHH-276:** The audit class name for role modifications now includes the role type.

**IIQMAG-753:** Temporary swap files are now cleaned up correctly when report generation is not successful.

**IIQMAG-758:** Scheduled Advanced Analytics searches can be set to send CSV formatted email attachments

**IIQMAG-764:** Resetting search filters on the Manage Work Items page will no longer prevent a value for Type from being selected.

**IIQMAG-774:** The role attributes display in a role composition certification will no longer show internal attributes and will correctly localize extended attributes.

**IIQPB-175:** The Spring Framework has been upgraded to version 4.3.5.

**IIQPB-214:** An access request with a rejected approval will now correctly show as successfully completed instead of pending.

**IIQPB-220:** Activation and deactivation dates for entitlement assignments are now editable in the Entitlements tab of the View Identity page.

**IIQPB-221:** Activation and deactivation dates for entitlement assignments are now visible in the Entitlements tab of the View Identity page.

**IIQPB-235:** The performance of managed attribute promotion in partitioned identity refresh has been improved.

**IIQPB-237:** UIConfig can now be used to modify the columns displayed in the applications list page.

**IIQPB-303:** [SECURITY] The Apache Commons Fileupload third party jar file has been updated to version 1.3.2.

**IIQSAW-1141:** Missing Privileged Account Manager permissions are now provisioned during Identity Refresh when Provision assignments is enabled.

| |
|---|
| **IIQSAW-1181:** While editing the fields, values in the provisioning policy editor are not hidden. |
| **IIQSAW-1205:** The `fullPathHash` field in Target has been renamed to `uniqueNameHash`. Any previous values (there should be none) will be overwritten during upgrade. |