Release Notes

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

IdentityIQ Release Notes **1**

IdentityIQ 8.4 Updates and Enhancements 1

IdentityIQ 8.4 Feature Updates 1

Important Upgrade Considerations for IdentityIQ 4

Important Upgrade Considerations for Connectors 13

Supported Platforms 16

Connectors and Integration Modules Enhancements 19

Connectivity Supported Platform and Language Updates 30

Connectivity Dropped Platform Support 32

Dropped Connector Support 33

Known Issues - IdentityIQ 33

Resolved Issues - IdentityIQ 34

Resolved Issues - Connectivity 43

IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, 8.4

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 Feature Updates
- Connectors and Integration Modules Enhancements
- Dropped Connector Support
- Important Upgrade Considerations
- Supported Platforms
- Resolved issues

IdentityIQ 8.4 Updates and Enhancements

IdentityIQ 8.4 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform, and Connectivity. Key enhancements in the release include:

IdentityIQ 8.4 Feature Updates

IdentityIQ 8.4 introduces the following new features or enhancements.

Feature/Enhancement	Description
Access History	Access History gives your organization the ability to view historical access data for identities. Access History tracks user access over time to reveal patterns of historical access, giving you the ability to see and report on past access changes in your business. Access history

Feature/Enhancement	Description
	shows you the “who, what, when, why, and how” of changes to user’s access over time. Key benefits for identity governance stakeholders include: • Seeing a user's timeline of access so that I can see how it has evolved over time • Exporting the changes in a user's access over a time period to understand what was provided at time of hire • Seeing list of accounts a given user has, so that I can ensure it is appropriate per provided guidelines • Seeing when access was removed for a terminated employee, so that I can confirm it was done in a timely manner • Finding out when an identity received a specific entitlement, so that I can confirm it was provisioned when expected **The Access History feature adds a new database to IdentityIQ.** The database for storing Access History data is separate from the IdentityIQ database. The IdentityIQ install and upgrade scripts will create separate databases for IdentityIQ and Access History data. The databases can be within the same instance for convenience, but separate database instances are recommended for production environments to avoid an impact on IdentityIQ performance. Depending on your environment setup and on the number of daily changes to your identities, the Access History database can be large, and will continue to grow. The Access History feature is enabled by default for new installations but is disabled by default when upgrading to version 8.4, due to configuration requirements. Refer to the *IdentityIQ Access History guide* for information on how to configure and enable this feature.
Data Extract	Data Extract lets you extract data from the IdentityIQ database and store it in a format that common business intelligence (BI) tools can use. Data extract gives you added flexibility to analyze your data, and helps you provide key data for addressing business and security questions. To extract data, IdentityIQ administrators create and configure a Data Extract Task, which calls the functionality to extract and transform data, and defines the message destination (a queue where data is available to be picked up by BI systems).

Feature/Enhancement	Description
	Administrators can also customize which types of objects are extracted and define which properties of those objects to include by configuring criteria for the extraction and transformation tasks.
Create Common Access	IdentityIQ customers can now mine and automatically create roles containing the baseline access needed for a given population, and exclude that access from future Access Modeling role mining/role insights. From an Identity search in Advanced analytics, you can use the new Discover Common Access Roles option to send your search-results population to AI Services to discover roles containing broadly-held access. This feature requires a subscription to Access Modeling.
Read only rights for Admin Debug pages	A new capability gives users the ability to view but not edit Objects via the Debug Pages Object Browser. This can help technical users who are not system administrators see IdentityIQ object XML for debugging and troubleshooting purposes. For example, database administrators can view database properties in order to confirm configurations, and certification or task administrators can review definition object XML to confirm that configurations are correct. Each page within the Debug menu (Memory, Objects, Caches, etc) has an associated SPRight which grants read-only access, allowing you to create custom capabilities to limit view-only Debug access to specific areas for specific users. These SPRights are also bundled together in one out-of-the-box capability, DebugPagesReadOnlyAccess, which makes it easy for you to allow complete view-only access to users as needed. Users with read-only access can copy or download object XML, but cannot save changes or upload XML.
Audit changes made through the Debug Object Browser	Changes made on Debug pages can now be be audited. To enable logging, navigate to **gear > Global Settings > Audit Configuration > General Actions** and select the **Debug Object Browser Change** checkbox. Audit data is viewed through the **Advanced Analytics > Audit** search, and includes the date and time a change was made, the identity that made the change, and the target object that was changed (such as identity, bundle, or configuration). Audit results can be exported in PDF, CSV, or CEF formats

Feature/Enhancement	Description
	The audit log does not detail what the changes were. Internal versioning or tracking should be used if you need to track the specific changes that are made.
Support for PostgreSQL	IdentityIQ version 8.4 adds support for PostgreSQL version 15
Updates to Angular	With this release, IdentityIQ begins an upgrade from Angular JS to Angular 15. UIs that have been updated include the Login screen, the Identity Preferences UI, and the API Authentication Global Settings page. More UI pages will be upgraded in future releases. Users upgrading from an earlier version of IdentityIQ should be aware that custom widgets and installed plugins may be impacted by the Angular upgrade. Verifying any needed changes to custom widgets and installed plugins should be part of your upgrade planning; widgets and plugins should first be evaluated in a non-production environment, prior to being deployed in production.
Security Upgrades and Library Updates	In version 8.4, new libraries have been added, and some existing libraries have been upgraded or removed. When you upgrade, be sure to test any custom forms in your implementation, to ensure compatibility with the updated libraries. A complete list of libraries is provided in the Important Upgrade Considerations for IdentityIQ section below.

Important Upgrade Considerations for IdentityIQ

IdentityIQ 8.4 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.

Security Upgrades

With this release, new libraries have been added, and some existing libraries have been upgraded, or removed.

Due to an increased overall industry focus on supply chain attacks and product security, SailPoint has become more aggressive in updating third party libraries contained in IdentityIQ. SailPoint has always aggressively monitored the security of all components of our products regardless of the source of the component and will continue to do so, and

SailPoint has always treated security issues found in all components of our products the same following our Product Vulnerability Management Policy which defines remediation and/or mitigation timelines based on the severity of a vulnerability. It is important to note that the severity of a vulnerability in a standalone library encompasses every possible use of the library. The severity of a finding or vulnerability in IdentityIQ due to a vulnerability in a library may be different due to the use of the library in IdentityIQ.

Many updates to third party libraries are not backward compatible, both at the API and functional level. Because of this, the changes required are often not simple a replacement of the library, but also changes to the component in the product that is a consumer of the library. Sometimes, a change to IdentityIQ behavior and/or APIs to accommodate these changes is required. Given that IdentityIQ is a platform that many of our customers and deployment partners use to build identity management solutions, the impact of these types of changes can be very high and our preference based on customer demand and feedback remains to introduce library changes in releases and not in patches unless remediation for a security vulnerability is required in which case updates can be introduced in patches.

A list of libraries that have been added or upgraded in this release is provided below. These are separated into the libraries in the IdentityIQ server layer and those in the IdentityIQ connector layer. Some libraries in the connector layer are bundled into larger packages and therefore the changes are not as visible when inspecting product file names.

> For connector library upgrades, see Important Upgrade Considerations for Connectors.

Starting in recent IdentityIQ releases and patches, a list of the libraries embedded in a connector bundle are contained in a file named SBOM.txt at the root of the bundle jar file.

IdentityIQ should not be thought of as a collection of independently upgradeable components, but instead a complete solution supported by SailPoint as it is delivered. Customers and deployment partners should not remove, modify, or update components of IdentityIQ outside of official releases by SailPoint.

> Important: When upgrading, be sure to test any custom forms in your implementation, to ensure compatibility with the updated libraries.

The following is a list of the current libraries:

- ActiveMQ 5.17.4
- ActiveMQ (geronimo-j2ee-management-1.1-spec) 1.0.1
- ActiveMQ (hawtbuf) 1.11
- Apache Ant 1.10.12
- Bouncy Castle 1.70

- Byte-buddy 1.12.10
- dbcp2 (Part of Commons) 2.9.0
- net.tascalate.javaflow.api (Part of Commons) 2.7.1
- Lang (Part of Commons) 3.12.8
- Net (Part of Commons) 3.9.0
- Pool2 (Part of Commons) 2.11.1
- Text (Part of Commons) 1.10.0
- Easymock 5.1.0
- Ehcache 3.10.0
- Failsafe 2.4.4
- Gson 2.9.0
- Guice servlet 5.1.0
- Httpcore 4.4.15
- Jersey 2.35
- junit 4.13.1
- mimepull 1.9.15
- Java JSON Web Token (jjwt) 0.11.2
- jackson 2.13.2
- Jackson (jackson-dataformat-yaml) 2.13.2
- Jackson (snakeyaml) 1.30
- jakarta.json 2.0.1

- jakarta.json-api 2.1.0
- jasperreports-javaflow 6.19.1
- jakarta.activation 1.2.1
- jakarta.mail1.6.7
- javassist 3.29.0
- jcommon 1.0.24
- jakarta.servlet-api 4.0.4
- junit 4.13.2
- JJWT 0.11.5
- Jline 3.21.0
- Joda-time 2.10.14
- Json-path 2.7.0
- Json-smart 2.4.8
- Java-jwt 3.19.1
- jwks-rsa 0.21.1
- mysqlconnector-java 8.0.33
- okhttp 4.9.3
- okio 2.8.0
- kotlin-stdlib
- openpdf 1.3.27
- cryptacular 1.2.5

- java-support 7.5.2
- OpenSAML 3.4.6
- OpenSAML (metrics-core) 4.2.9
- OpenSAML (xmlsec) 2.3.0
- javaee-api 8.0.1
- slf4j 1.7.32
- Spring 5.2.24
- twillio 8.14.0
- sshj0.31.0
- asn-one 0.5.0
- xmlschema 2.2.5
- xmlsec 2.2.2
- objenesis 3.2
- ngdbc 2.8.12
- testng (jcommander) 7.5
- lucene 8.8.2
- primefaces 8.0.12 (paid)
- jquery 3.5.1
- json 20210307
- XML Unit 2.9.0

Unable to Create Applications with Tomcat 9.0.78

When IdentityIQ is running with Tomcat 9.0.78 or higher, we are unable to create applications for few of the connectors (like ACF2-Full, Top Secret) and the following error is seen on the Tomcat screen:

More than the maximum number of request parameters (GET plus POST) for a single request ([1000]) were detected. Any parameters beyond this limit have been ignored.

To resolve this, set the maxParameterCount parameter to a higher value (default - 1000) in server.xml and restart the Tomcat server.

New Database Added with Access History Feature

The Access History feature adds a new database to IdentityIQ. The database for storing Access History data is separate from the IdentityIQ database. The IdentityIQ install and upgrade scripts will create separate databases for IdentityIQ and Access History data. The databases can be within the same instance for convenience, but separate database instances are recommended for production environments to avoid an impact on IdentityIQ performance. Depending on your environment setup and on the number of daily changes to your identities, the Access History database can be large, and will continue to grow.

ActiveMQ Table Casing

If a user changes the standard ActiveMQ casing for tables, this may result in problems with the embedded brokers falsely claiming that the tables do not exist on start up.

JasperReports Update

The JasperReports library has been updated to version 6.19.1. Any custom forms should be tested prior to the JasperReports upgrade.

Java 11

IdentityIQ 8.4 is compiled with Java 11. Plugins and other integrations must be compiled under Java 11 to be compatible with IdentityIQ 8.4.

Angular 15

The Angular framework has been upgraded from AngularJS to Angular 15 on the following pages.

- Login
- Identity Preferences
- Global Settings → API Authentication

These upgrades could potentially impact installed plugins, if the plugins use AngularJS and/or modify the rendering of the affected page. After upgrade to 8.4, we recommend that any plugins are first evaluated in a non-production environment, prior to being deployed in production.

Deserialization of Untrusted Data

[SECURITY] Deserialization of untrusted data is a security risk that should be avoided. Java introduced a serialization filtering feature in JDK 9 and later backported to versions 6, 7 and 8 which allows for serialization of classes specified in a filter via the "jdk.serialFilter" system security property. IdentityIQ now only allows deserialization of classes from the sailpoint package. String, primitive classes, and arrays are allowed by default. Support for the configurable filters has been included in the CPU releases for JDK 8u121, JDK 7u131, and JDK 6u141.

Security Fix for SetIdentityForwarding Right

[SECURITY] This release contains a fix for an important security vulnerability that was previously announced. The vulnerability allows authenticated users assigned the Identity Administrator capability or any custom capability that contains the SetIdentityForwarding right to modify the work item forwarding configuration for identities other than the ones that should be allowed by Lifecycle Manager Quicklink Population configuration. This vulnerability in IdentityIQ is assigned CVE-2022-45435.

As with all software vulnerabilities, we recommend that all customers apply this upgrade or the e-fix for IIQSR-727 available in the Product Download Center on Compass as soon as possible.

JSON Libraries Replaced with Jackson

All uses of the JSON-java library have been replaced with Jackson.

Processing Objects with Non-Standard Object IDs

In 8.3 GA and 8.3p1, processing objects with nonstandard object IDs caused NativeIdentityChange propagation to fail with the exception “Attempt to generate refresh event with null object”. When this error occured, the failed NativeIdentityChangeEvents blocked provisioning. This issue has been resolved. For customers impacted by it in earlier versions, a new task template, “Reset Failed NativeIdentityChange Events”, has been added in this release that re-processes these events to:

- Report the number of failed events
- Prune events where the old and new values only differ by case
- Reset failed events and launch tasks to re-process them

A new option, detectNativeIdentityChangeCaseSensitive, is now supported that improves performance. This option defaults to false. When enabled, it triggers creation of a NativeIdentityChangeEvent in IdentityIQ even if the native

identifier for Account or Group only differs by case from the value in IdentityIQ. To enable this option, add the following to the Attributes Map of the System Configuration:

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

AI Role Mining Plugin Functionality Moved to Base IdentityIQ Product

In 8.4, the functionality previously available in the IdentityAI Role Mining plugin is now in the base IdentityIQ product. Upon upgrade to 8.4, if the IdentityAI Role Mining plugin was previously installed, the plugin will be uninstalled and any configuration from that plugin will be added to the AI Services Configuration under a new section, "Access Modeling".

There are two new SPRights: **ManageIAISpecializedRoleDiscovery** and **ManageIAICommonAccessDiscovery**. There is one new capability, **AIAccessModelingAdministrator**, containing those two SPRights and also having **ViewIdentity**, which is necessary for Access Modeling.

There is no separate System Configuration key to enable Access Modeling apart from **identityAIEnabled**. The Access Modeling configuration will be visible on the AI Services Configuration page to IdentityIQ customers with AI subscriptions, regardless of whether they subscribe to the Access Modeling module specifically. However, in such cases the Access Modeling functionality will still be disabled in their IdentityNow tenant.

New Configuration Page/Rights Entries Added to webresources.xml

New Installations or Upgrades will add the new Access History/Data Extract/Broker configuration pages/rights entries into `webresources.xml`. Customers should review the changes and merge theirs if different from the out-of-the-box configuration.

Form Beans Required in Form Submissions

[SECURITY] Form Beans used to process SailPoint Form submissions must now implement the FormBean interface. Anything else will throw an exception and block submission of the form.

This release contains a fix for an important security vulnerability that was previously announced. This vulnerability allows an authenticated user to invoke a Java constructor with no arguments or a Java constructor with a single Map argument in any Java class available in the IdentityIQ application classpath. This vulnerability in IdentityIQ is assigned CVE-2023-32217. As with all software vulnerabilities, we recommend that all customers apply this upgrade or the e-fix for IIQFW-655 available in the Product Download Center on Compass as soon as possible.

Security Fix to JavaServer Faces (JSF) Library

[SECURITY] A file traversal vulnerability in the JavaServer Faces (JSF) library has been fixed.

This vulnerability allows access to arbitrary files in the application server filesystem due to a path traversal vulnerability in JavaServer Faces (JSF) 2.2.20 documented in CVE-2020-6950. The remediation for this vulnerability con-

tained in this security fix provides additional changes to the remediation announced in May 2021 tracked by ETN IIQSAW-3585. This vulnerability in IdentityIQ is assigned CVE-2022-46835.

As with all software vulnerabilities, we recommend that all customers apply this upgrade or the e-fix for IIQFW-336 available in the Product Download Center on Compass as soon as possible.

Workflow Approval Arguments to Prevent ObjectAlreadyLocked Exceptions

Two new approval arguments are available on an Approval step in a workflow so that end users will not see ObjectAlreadyLocked exceptions after completing an approval workitem and the workitem is locked. Using either of these options will disable the automatic display of the next workitem in a "wizard" workitem scenario:

<Arg name="backgroundApprovalCompletion" value="script:true"/>

This will move approval completion to background processing to free the user from waiting until the workitem is processed by the workflow before returning to the home page.

<Arg name="backgroundApprovalCompletionIfLocked" value="script:true"/>

This will only move the approval completion process to the background if the workitem or workflow is locked by another user or another process. This will prevent the user from seeing a popup and return the user to the home page.

JDNI Datasources for Access History Database

If you are using a JNDI datasource for your access history database, you will need to make a few configuration changes.

1. Extract `configBeans.xml` out of the l`ib/identityiq.jar`, and copy that file into the `WEB-INF/classes` directory.
2. Add a new bean to `configBeans.xml` as follows:

```
<!--
App-server managed data source for accessHistory database that is looked up in
JNDI. The location of the data source is configured with jndiName in
iiq.properties.
-->
<bean id="jndiAccessHistoryDataSource"
class="org.springframework.jndi.JndiObjectFactoryBean">
<property name="jndiName" value="jdbc/overrideInIIQProperties"/>
<property name="lookupOnStartup" value="false"/>
<property name="cache" value="true"/>
<property name="proxyInterface" value="javax.sql.DataSource"/>
</bean>
```

3. In `iiq.properties`, define the datasource as follows:

```
jndiAccessHistoryDataSource.jndiName=[insert your data source here. For example,
java:comp/env/jdbc/testDataSourceAccessHistory]
```

```
configuredDataSourceAccessHistory.targetBeanName=jndiAccessHistoryDataSource
```

Important Upgrade Considerations for Connectors

General Updates for Connectors

- Microsoft has announced that Basic Authentication for exchange Online is no longer available after October 1, 2022. You can update your Azure Active Directory applications configured to manage Exchange Online using modern authentication supported by connector. Be sure to upgrade the IQService to the one which is bundled with the release. For more details regarding Microsoft announcement, refer Basic Authentication Deprecation in Exchange Online – May 2022 Update
- The Salesforce connector now supports API version 56.0, For existing applications, remove the User- PermissionsMobileUser attribute from the schema for the connector to work with the new 56.0 API version
- The Salesforce connector now supports creating new Portal and Partner Users as well as assigning Portal and Partner Licenses to existing Salesforce Users using their respective user profiles. Ensure that the service account user has the "Manage Contacts" object [R || W] added to the administrative user profile.
- The Salesforce connector now supports creating, updating and deleting Public Groups. Ensure that the service account user has "Public Groups" object [R || W] added to the administrative user profile.
- The IQService version must match the IdentityIQ server version, including the major release and patch versions. When one is upgraded, the other must also be upgraded, so that the version and patch levels match. For more information on upgrading the IQService, see the I*dentityIQ Installation guide* chapter on upgrading
- The Zoom connector no longer supports API Token Authentication. Configure your Zoom application to use Oauth2 Authentication, to avoid any failures.

Connector Security Upgrades

With this release, new libraries have been added, and some existing libraries have been upgraded, or removed. The following is a list of the current libraries:

- accessors-smart-2.4.8
- bcel-6.6.1
- commons-fileupload-1.4
- hk2-api-3.0.3

- hk2-locator-3.0.3
- hk2-utils-3.0.3
- hibernate-core-6.1.5.Final
- jersey-hk2-3.0.4
- jackson-databind-2.13.3
- jakarta.annotation-api-2.1.0
- jakarta.validation-api-3.0.1
- jakarta.ws.rs-api-3.1.0
- jersey-hk2-3.0.4
- jersey-client-3.0.4
- jersey-common-3.0.4
- jersey-container-servlet-core-3.0.4
- jersey-media-jaxb-3.0.4
- jersey-media-multipart-3.0.4
- jersey-server-3.0.4
- jersey-apache-connector-3.0.4
- jasperreports-javaflow-6.19.1
- jackson-core-2.13.3
- javax.faces-2.4.0
- javax.mail-1.6.2
- kotlin-stdlib-1.7.10

- mysql-connector-java-8.0.30
- mysql-connector-java-8.0.30
- org.jacoco.ant-0.8.8
- spring-core-5.3.20
- spring-core-5.3.22.RELEASE
- spring-web-5.2.22.RELEASE
- testng-7.6.1

Supported Platforms

> **IMPORTANT**: SailPoint does not support anything beyond the compatibility of the platform vendors. Confirm the interoperability and support from those vendors when deciding on your platforms.

Operating Systems

- Windows Server 2022 and 2019
- Solaris 11 and 10
- IBM AIX 7.3 and 7.2

> Note regarding **Linux Support:** The distributions and versions of Linux highlighted below have been verified by IdentityIQ Engineering, but any currently available and supported distributions and versions of Linux will be supported by SailPoint. Implementers and customers should verify that the distribution and version of Linux of choice is compatible with the application server, database server, and JDK also being used.

- Red Hat Linux 9.1 and 8.8
- SuSe Linux 15 and 12

Application Servers

- Apache Tomcat 9.0
- Oracle WebLogic 14c
- JBoss Enterprise 7.4 and 7.3
- IBM WebSphere Liberty 21.0 and 22.0

Databases (On Site)

- IBM DB2 11.5
- MySQL 8.0

- MS SQL Server 2022 and 2019
- Oracle 19c
- PostgreSQL 15

Message Brokers

- ActiveMQ 5.17.4

Cloud Platforms

- AWS EC2
- AWS Aurora
- AWS RDS (MySQL, MS SQL, Oracle)
- Azure (VM, Azure SQL)
- Google Cloud Platform – Google Compute Engine

Java Platform

- Sun, Oracle or IBM JDK 11 and JDK 17 for all application servers that support those versions
- OpenJDK11 is now supported on all environments, but we have specifically tested against Adopt OpenJDK 11 and 17 for Windows and Red Hat OpenJDK 11 and 17 for Linux
- Eclipse Temurin JDK 11, 17
- IBM Semeru 17.0.5.0

Browsers

- Google Chrome Latest Version
- Microsoft Edge Latest Version
- Safari 16
- Firefox Latest Version

Mobile User Interface OS / Browser Support

- Android with Chrome 13
- iOS with Safari 16

Languages

- Brazilian Portuguese
- Chinese (Taiwan)
- Danish
- Dutch
- English
- Finnish
- French
- French Canadian
- German
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Simplified Chinese
- Spanish

- Swedish
- Traditional Chinese
- Turkish

Connectors and Integration Modules Enhancements

IdentityIQ 8.4 provides various enhancements in the following connectors and integration modules.

New Connectors

IdentityIQ 8.4 delivers new, out-of-the-box connectors for the following enterprise applications, which simplifies the connectivity of these systems.

New Connectors	Description
BMC Helix Remedyforce Service Desk Integration Module	The BMC Helix Remedyforce ITSM Service Desk Integration module is designed to provide the service desk experience in Identity IQ. The integration supports creation of tickets within Identity IQ for manual provisioning operations and status checks. Service desk integration module ensures synchronization of ticket status between Identity IQ and the BMC Helix Remedyforce Service Desk system.
Coupa Connector	The new SailPoint Coupa connector provides the capability for seamless and secure connection to the Coupa system, and manages user access and groups throughout the user's lifecycle. This integration also manages user-groups, content-groups, account-groups and approval-groups membership as entitlements.
Generic Service Desk Integration Module	The Generic Service Desk integration offers connectivity with different IT Service Management (ITSM) solutions. It supports the creation of tickets, which can be configured to align with the specific service request types of the target ITSM solution. This integration brings the service desk experience into the SailPoint platform, enabling users to raise and track service desk tickets to their logical closure from SailPoint IdentityIQ.
IdentityIQ for EPIC SER	The Epic SER connector provides the capability to manage Epic Provider (SER) records. It supports aggregation of Provider records as accounts and lifecycle capabilities including create account, update account, and enable/disable account.
Ivanti Cherwell Connector	The Cherwell connector offers seamless connectivity to the Cherwell ITSM solution, enabling aggregation and provisioning of two distinct Cherwell user types: 'users' & 'customers'. This integration enables robust user access management and governance in the Cherwell System.
Ivanti Cherwell Service Desk	The Cherwell Service Desk Integration Module (SDIM) brings the service desk experience into the SailPoint platform, enabling users to raise and track service desk tickets (Service Request & Incid-

New Connectors	Description
	ent) to their logical closure in Cherwell ITSM solution from SailPoint IdentityIQ.
Microsoft Azure SQL Database	Azure SQL Database connector provides connectivity with Azure SQL Database for user access governance and management. The connector supports the management of Microsoft Azure SQL database logins as accounts and users associated to login accounts. It supports aggregation, provisioning and full account management.
Oracle Fusion HCM Accounts	Oracle Fusion HCM Accounts connector provides the capabilities to manage HCM users' accounts. It supports the aggregation of accounts and roles. The connector also provides for full lifecycle capabilities including account creation, updation, and role assignment/revocation with accounts.
Oracle Enterprise Performance Management (EPM) Cloud governance Connector	The new Oracle Enterprise Performance Management (EPM) Cloud governance connector provides the capability for managing user accounts, predefined roles, application roles, and groups. The integration supports EPM Cloud Services for Financial Consolidation and Close (FCCS), Account Reconciliation (AR), Planning, Narrative Reporting (NR).
Oracle HCM Cloud Connector	The new Oracle HCM Cloud connector provides read capability from Oracle Fusion HCM for "person" details when Oracle Fusion HCM is the HR data source for the organization. This new connector's capabilities include operations such as full account aggregations using recommended designs from Oracle to use performance-based file extract methods, and any incremental user data changes to be detected via delta aggregation using "Oracle's Atom Feeds". The connector also provides capabilities to refresh any accounts coming in, as well as discover new schemas.
SAP Concur Connector	The new SAP Concur Connector provides Identity Governance on Expense management services provided by Concur. The integration supports enforcing policies and permissions for granting and revoking access to systems and data based on user identities, roles, and associated groups for Expense, Request, Invoice, and Reporting.
SAP Fieldglass Connector	SailPoint's Integration for the SAP Fieldglass Vendor Management System offers governance capabilities for contingent workers. It offers seamless governance of external users management for joiners, movers, leaver workflows, and separation of duty (SOD) checks based on user roles, attributes, and entitlements.
Snowflake Connector	A new Snowflake Connector is now available to govern identities for Snowflake Data Lake.

ACF2

- Supports z/OS 2.5

Active Directory

- Supports aggregation of domain NetBIOSName as part of account and group aggregation. You need to add NetBIOSName as a schema attribute with the type as String in the Account and Group schema to leverage this feature.
- Supports Microsoft Windows Server 2022.

Amazon Web Services

- Supports AWS GovCloud (US) Regions.

Atlassian Suite - Server

- Supports the following new versions:
    - Supports Jira Service Management version 5.2
    - Supports Jira Software Server version 9.6
    - Supports Confluence version 8.1
    - Supports Bitbucket version 8.8
    - Supports Bamboo version 9.2

Atlassian Server Jira Service Management

- Supports Atlassian Jira Service Management (Server) version 5.2.0

Azure Active Directory

- Supports managing Azure PIM Role memberships to Azure Active Directory groups.
- Supports certificate based modern authentication to communicate with Exchange Online that is more secure and is the Microsoft recommendation.
- Now provides visibility into user’s sign-in (last login) activity.

- Supports managing Azure Active Directory Role as a group object.
- Supports Continuous Access Evaluation (CAE), which leverages the Azure Active Directory real-time enforcement of conditional access location and risk policies, along with instant enforcement of token revocation events for an enterprise application (service principal).
- Support management of access packages.
- Supports managing user-assigned identities.
- Supports read and write of Azure Multi-Factor Authentication attributes required for various authentication methods.
- Supports EXO V3 module for Exchange Online management feature.
- Supports filters for channels during entitlement aggregation.
- Supports User and Group advanced filters through the application UI.
- Supports giving visibility to read-only group hierarchy information during group aggregation.
- Supports managing Service Principal for enterprise Applications as an Account (Service Principal as Account).
- Supports creating SAML based applications and corresponding Service Principals using the Gallery application templates.
- Supports creation of Service Principals for existing Applications.

BMC Helix

- Supports BMC Helix IT Service Management Suite version 22.1

BMC Helix ITSM Service Desk

- Supports OAuth 2.0 authentication.
- Supports version 21.3. With this new version, the connector supports service requests via the digital workplace with a new ticket type called DWP Service Request.
- Supports BMC Helix IT Service Management Suite version 22.1

BMC Remedy

- Supports BMC Helix 21.3 systems.

Cloud Gateway

- Supports using load balancer with sticky-bit configuration.
- Supports new configuration to enable all operations for target collectors to be executed in Cloud Gateway.
- Supports the following new versions:
    - Oracle JRE for Java version 17 and OpenJDK 17 platforms
    - RHEL 9.0
    - Microsoft Windows Server 2022

Duo

- Supports proxy setting from the application server settings and can also bypass the proxy for hosts listed in the nonProxyHosts list.

EPIC

- The following Epic user fields are now supported as account attributes:
    - PrimaryManager
    - UsersManagers
- Supports Epic version May 2023

EPIC SER

- Enhanced to display provisioning failures at an attribute level.

Generic Service Desk

- Supports retrieving the ticket number from the URL if the create ticket response returns the URL instead of the ticket number. The new attribute is Process Response Element Expression, and it should be populated with parsing logic to fetch the ticket number from the response URL.

Google Workspace

- Supports archiving and unarchiving users.

HCL Domino

- Supports HCL Domino version 12.0.2.

IBM Security Verify Governance

- Supports delta aggregation.
- Supports IBM Security Verify Governance version 10.0

IBM Security Verify Access

- Supports IBM Security Verify Access 10.0.3
- Supports IBM Security Verify Access 10.0.6 with support for backend servers: IBM Security Directory Suite version 10.0.
- Deprecating REST API support.

Jack Henry

- Supports enabling and disabling accounts.

LDAP

- Supports Modify Time Stamp as a new delta aggregation mode.
- The UI has been updated to provide more fields for configuring the connection details to various LDAP Directory servers.

Linux

- Supports Red Hat Enterprise Linux versions 8.5 and 8.8.

Mainframe Connectors - RACF, ACF2, TopSecret

- Enhanced to support mutual TLS authentication for communication between IdentityIQ Connector Gateway and the mainframe connector itself. You must upgrade to the latest version of Connector Gateway to leverage this feature.

Microsoft SQL Server

- Supports Azure Managed Instances.
- Supports Microsoft SQL Server 2022.

Okta

- Enhanced to respect the password policy set in the Okta target system (in terms of password age and password history).
- Supports the addition and removal of custom roles directly associated with accounts.
- Supports aggregation of custom roles directly associated with accounts and groups.
- Enhanced to provide an option for multi-threading when aggregating groups and applications connected to Okta accounts during account aggregation.

Oracle E-Business

- Supports the 12.2.11 Oracle EBS environment.

Oracle ERP Cloud

- Enhanced to support aggregation of data access information (security context and security context values) even when not assigned to a role.

Oracle Fusion HCM

- Supports aggregation of additional attributes from the WORKERS API responses using a JSON Path.
- Enhanced account aggregation performance.
- Account aggregation will now fail when there is a planned outage (maintenance) on the Oracle system.

Oracle Fusion HCM Accounts

- Oracle Fusion HCM Accounts connector provides the capabilities to manage HCM users' accounts. It supports the aggregation of accounts and roles. The connector also provides for full lifecycle capabilities including account creation, updation, and role assignment/revocation with accounts.
- Account aggregation will now fail when there is a planned outage (maintenance) on the Oracle system.

Oracle Identity Manager

- Supports the Oracle Identity Manager 12C version.

Oracle PeopleSoft ERP

- Supports PeopleTool versions 8.60 to 8.60.05.

Oracle PeopleSoft HCM

- Supports PeopleTool version 8.60 to 8.60.05.

RACF

- Supports resource aggregation and provisioning as additional group schema, and requesting permissions for accounts and groups.
- Supports z/OS 2.5

RSA

- Supports RSA Authentication Manager version 8.7 and 8.6.

SAP Direct

- Redesigned to use an SAP-certified function module for enhanced security and performance. The use of the RFC_READ_TABLE has been made limited according to SAP recommendations.

SAP GRC

- Redesigned to use an SAP-certified function module for enhanced security and performance. The use of the RFC_READ_TABLE has been made limited according to SAP recommendations.

- Enhanced to support account partitioning for SAP Basis version 751 and later.
- Enhanced to support additional attributes that are now configurable through the provisioning policy.
- Enabling and disabling accounts is now possible for all the GRC-connected systems and not just limited to the master. This enables deeper governance and clean audit capabilities.
- Enhanced to support Additional Settings in the UI, which includes Access Request Type Mapping, Provisioning Actions for Role, and Provisioning Actions for System sections.
- Supports access management requests that are configured for auto approval in the SAP GRC system.

SAP HANA

- Enhanced to support get and provisioning of external type users.
- Supports custom user parameters for aggregation and provisioning.
- Supports the following new versions:
    - SAP HANA Cloud Database version 4.0 application
    - SAP HANA 2.0 SPS6 version

SAP HR/HCM

- Redesigned to use an SAP-certified function module for enhanced security and performance. The use of the RFC_READ_TABLE has been made limited according to SAP recommendations.

Salesforce

- Supports creating, updating, and deleting public groups (ensure that your service account user has the “Public Groups” object [R || W] added into the administrative user profile).
- No longer supports Salesforce API version 48.0 or prior. The connector will only work on API version 56.
- Supports creating new portal and partner users, as well as assigning portal and partner licenses to existing Salesforce users using their respective user profiles (ensure that your service account user has “Manage Contacts” object [R||W] added into the administrative user profile).
- Supports use of the Enhanced Domains option in the Salesforce system.

ServiceNow Identity Governance

- Supports configurable option to read deleted events (for example, removing a group or role) of user's connection from a custom table instead of the sys_audit_delete table. This enhances the delta aggregation performance.
- Supports the ServiceNow Utah and Tokyo release.

IdentityIQ for ServiceNow Service Desk

- Supports pulling RITM status into SailPoint.
- Enhanced to populate the access request comment on the ServiceNow ticket. Existing service desk integrations need to modify the provisioning task definition to include the comments for access request comments. This feature is automatically included for all new configurations.
- Supports ServiceNow Tokyo and Utah release.

SharePoint Online

- Supports configurable endpoints when Azure Active Directory is deployed on a non-public national cloud server.

SharePoint Server

- Supports managing Microsoft SharePoint Server Subscription Edition.

Siebel

- Supports Siebel server version 22.8.0.0.

Slack

- Supports creation of a guest user to have access to a single or multiple channels in Slack Enterprise Grid Plan.

SuccessFactors

- Enhanced to support account delta aggregation.
- Enhanced to exclude Personal Identifiable Information (PII) data for employees.

- Enhanced to manage external users, and their entitlements, who are in the onboarding stage.
- Supports additional attributes and custom attributes related to user entities via the ODATA API.
- Enhanced to aggregate selective employee records based on filtering criteria.

Web Services

- Supports Create, Update, and Delete for Group objects.
- Supports removing entitlements while disabling accounts and enabling entitlements while enabling accounts.
- Now provides example rules to show the use of Web Services operation rules to help configure the searchAfter attribute for pagination.

Windows Local

- Supports Microsoft Windows Server 2022.

Workday

- Supports adding proxy level parameters in the Workday application.
- Supports Workday web service versions 39.1 and 38.0.

Workday Accounts

- Enhanced to integrate with Workday Learning Module and aggregate the training information associated with users.
- Supports managing Service Center Representative accounts.
- Supports filtering of accounts based on the Organization Type and Organization Reference ID.
- Supports aggregation and provisioning of future accounts ahead of their hire date.
- Enhanced to provide an option for multi-threading, which will improve the account aggregation performance.
- Supports additional schema attributes for User-Based Security Group objects.

Zoom

- Supports OAuth 2.0 authentication.
- Authentication Type “API Token” is no longer supported. Set up your Zoom application to configure Oauth2.0 Authentication to avoid any failures.

Connectivity Supported Platform and Language Updates

Connector/Component	New Platform Version
Active Directory Connector	Supports Microsoft Windows Server 2022
ACF2 Full Connector	Supports z/OS 2.5
Atlassian Suite - Server Connector	• Supports Jira Service Management version 5.2 • Supports Jira Software Server version 9.6 • Supports Confluence version 8.1 • Supports Bitbucket version 8.8 • Supports Bamboo version 9.2
BMC Remedy Connector	Supports BMC Helix 21.3 system.
BMC Helix Connector	Supports BMC Helix IT Service Management Suite version 22.1
BMC Helix ITSM Service Desk Integration Module	Supports version 22.1.
Cloud Gateway	• Supports Oracle JRE for Java version 17 and OpenJDK 17 platforms. • Supports RHEL 9.0. • Supports Microsoft Windows Server 2022
EPIC Connector	Supports Epic version May 2022
HCL Domino Connector	Supports HCL Domino version 12.0.2.
IBM Security Verify Access Connector	• Supports IBM Security Verify Access 10.0.3 • Supports IBM Security Verify Access 10.0.6 with Supported Backend Servers: IBM Security Directory Suite version 10.0
IdentityIQ for Atlassian Server Jira Service Desk	Supports Atlassian Jira Service Management (Server) Version 5.2.0

Connector/Component	New Platform Version
IdentityIQ for IBM Security Identity Manager	Supports IBM Security Verify Governance v10.0
IdentityIQ for ServiceNow Service Desk	Supports the ServiceNow Tokyo and Utah release.
Linux Connector	Supports Red Hat Enterprise Linux versions 8.8 and 8.5.
Microsoft SharePoint Server Connector	Supports managing Microsoft SharePoint Server Subscription Edition.
MS SQL Server - Direct Connector	Supports MS SQL Server 2022
Oracle E-Business Connector	Supports the 12.2.11 Oracle EBS environment
Oracle Identity Manager Connector	Supports the Oracle Identity Manager 12C version.
PeopleSoft Connector	Supports PeopleTools version 8.60.05 and 8.59 environment
PeopleSoft HCM Connector	Supports PeopleTool version 8.60.05
RACF Full Connector	Supports z/OS 2.5
RSA Connector	Supports RSA Authentication Manager version 8.7 and 8.6
SAP Business Suite (ERP)	Integration is certified with 'SAP HANA S/4 2022'
SailPoint Identity Governance Connector for ServiceNow	Supports the ServiceNow Tokyo and Utah release.
SAP Hana DB Connector	• Supports SAP HANA Cloud DB ver 4.0 application • Supports SAP HANA 2.0 SPS6 version
Salesforce Connector	Supports API version 56.0 (For existing applications, you must remove the User-PermissionsMobileUser attribute from the schema for the connector to work with the new 56.0 API version.)
ServiceNow IdentityIQ for Service Desk	Supports the ServiceNow Tokyo and Utah release.
ServiceNow Catalog Integration	Supports the ServiceNow Tokyo and Utah release.
SAP SuccessFactors Connector	• Enhanced to support the account delta aggregation • Enhanced to exclude PII data for employees.

Connector/Component	New Platform Version
Siebel Connector	Supports Siebel server version 22.8.0.0.
Top Secret	Supports zOS 2.5
Top Secret LDAP	Supports zOS 2.5
Windows Local Connector	Supports Microsoft Windows Server 2022
Workday Connector	Supports Workday web service version 38.0 and 39.1

Connectivity Dropped Platform Support

Connector/Integration Module	Dropped Platforms
ACF - Full	z/OS 2.2 and z/OS 2.3 systems
Atlassian Suite Server Connector	No longer supports the following: • Jira Software Server version 8.13 and 8.12 • Confluence version 7.8 and 7.7 • Bitbucket version 7.5 • Bamboo version 7.1 and 7.0
IdentityIQ for ServiceNow Service Desk Integration Module (SDIM)	ServiceNow Paris, Rome, and Quebec release.
IdentityIQ for Oracle Identity Manager	Oracle Identity Manager 11g R1 and Oracle Identity Manager 11g R2 releases.
IBM AIX Connector	AIX version 7.1
Linux Connector	Red Hat Enterprise Linux versions 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8 and Ubuntu OS Version 18.04 LTS.
Oracle Solaris Connector	Solaris versions 11.3, 11.2, 11.0 and 10.0
RACF -Full	z/OS 2.2 and z/OS 2.3 systems
RACF - LDAP	z/OS 2.2 and z/OS 2.3 systems
RSA Connector	RSA 8.3, 8.4, and 8.5 version.
SailPoint Identity Governance Connector for ServiceNow	ServiceNow Paris, Rome, and Quebec release.
ServiceNow Service Desk	Paris, Rome, and Quebec releases.
Top Secret	z/OS 2.2 and z/OS 2.3 systems

Connector/Integration Module	Dropped Platforms
Top Secret LDAP	z/OS 2.2 and z/OS 2.3 systems
Zoom	API Token authentication type.

Dropped Connector Support

End of Life: The following connectors and connector components are no longer supported:

- Oracle Fusion HCM Connector - On December 31, 2023, Oracle Fusion HCM Connector will no longer be supported. Use the newly-released Oracle HCM Cloud Connector. For documentation on the new connector, refer to Integrating SailPoint with Oracle HCM Cloud.
- IdentityIQ for Oracle Identity Manager - IdentityIQ for Oracle Identity Manager Version 1: Connection via OIM Integration Web Application is no longer supported. Use the newly-released Identity IQ for Identity Manager Version 2: Connecting Oracle Identity Manager via Oracle Client API. For documentation on the new connector, refer to IdentityIQ for Oracle Identity Manager V2.
- IBM Tivoli Access Manager - Support for REST API for IBM Tivoli Access Manager connectors is no longer supported.
- Zoom - Support for API Token authentication is no longer supported.

Known Issues - IdentityIQ

Issue ID	Description
IIQETN-11203	When an assigned role that has been added by an assignment rule is removed from an identity through a revoke or remove action, Access History will not recognize that there is a negative assignment. As a result, role removal events are not created consistently and some data and counts may be incorrect.
IIQETN-11209	In the Access History feature, if any of the roleAssignments for an identity capture are set to `negative="true"`, then the counts shown in the UI for Roles and Entitlements may be inaccurate.

Resolved Issues - IdentityIQ

Issue ID	Description
IIQSR-761	Entitlements are now revoked completely when revoking through Policy Violations.
IIQCB-4662	`<Includes></Includes>` tags can now be used for scripts in workflows.
IIQCB-4680	When the Assigned Role field on the Advanced Identity Search page is set to "is not equal to" now will exclude identities with multiple assigned roles if one of those roles matches the supplied value.
IIQCB-4686	Certification bulk delegated items with line item delegations no longer show errors.
IIQCB-4697	Workflow exceptions are now localized.
IIQCB-4699	Access Request Emails now uses EmailTemplate SessionProperties.
IIQCB-4708	When 'Show Password' option is enabled, we now disable historical passwords autofill as a hint when entering the next password.
IIQCB-4710	On the Rapid Setup Leaver / Identity Operations pages, the Reassigned Artifacts Types pulldown no longer contains "Alert", "Classification", "Plugin", and "Task and Report Schedules".
IIQCB-4759	Importing an application no longer deletes and orphans schemas when running aggregation
IIQCB-4792	SAML Electronic Signatures can now be used with custom approval forms the same way that SAML Electronic Signatures are used with Approvals.
IIQCB-4825	The Entitlement Catalog now displays when a Boolean type extended attribute is included in the searchable attributes.
IIQCB-5042	Running a RequestObjectSelector Rule no longer errors when filtering for extended attributes.
IIQCB-5374	On the Role Search page when filtering by profile the filter type will now include "Entitlement" value in the dropdown when there is at least one Role-Entitlement Association that is not of type "Permission".
IIQFW-1	[SECURITY] SailPoint Form sections with type `text` or `datatable` no longer render HTML by default. Fields that need to display HTML must now provide the `contentIsEscaped` attribute and set it to `true`. Any dynamic or user-entered content in the field must be escaped in order to be secure.
IIQFW-2	[SECURITY] HTML embedded in entitlement or role names will no longer be rendered as part of surrounding formatting HTML.
IIQFW-7	[SECURITY] When MFA authorization workflow is configured and the user clicks on Forgot Password for reset, the security authorization questions page can not be skipped until the reset workflow action is

Issue ID	Description
	successful.
IIQFW-36	[SECURITY] On the Approvals page, HTML embedded in entitlements and roles will no longer render in the browser.
IIQFW-224	[SECURITY] The server now escapes potentially harmful HTML contained in message parameters before being displayed in the UI.
IIQCB-4992	The Policy Violations Details no longer displays HTML tags
IIQCB-5034	Processing a role that cannot be processed no longer results in a NullPointerException. As part of this change, IdentityIQ has improved diagnostic logging when unable to analyze a role for profile relations.
IIQFW-287	[SECURITY] IdentityIQ allows deserialization of classes from the sailpoint package by default. If the jdk.serialFilter property is provided, it is recommended that it also specifies the sailpoint package.
IIQFW-336	[SECURITY] A file traversal vulnerability in the JavaServer Faces (JSF) library has been fixed.
IIQFW-369	Added role="alert" to the message element, so the screen reader can now detect and read the messages displayed on the home page.
IIQFW-584	[SECURITY] IdentityIQ no longer supports an empty WebResource config. Running IdentityIQ without a WebResource config will prevent the site from working for any non-SysAdmin user.
IIQFW-634	A 'data is still loading' alert message is now displayed during revocation of certification items, when the items haven't finished loading, instead of throwing an exception.
IIQFW-654	Resolved issue where the Load More option was not being presented for certification campaigns containing multiples of 5 + 1. For example: 6, 11, 16, 21, etc.
IIQFW-728	[SECURITY] Updated UI so that instead of the actual client secret value we will send a dummy value.
IIQFW-729	[Security] Removed option to view security authentication question answers in clear text. The answer fields are treated as password values. Actual answer values are no longer sent back to browser.
IIQFW-833	[Security] The Spring library is now updated to version 5.2.24
IIQSR-836	With the upgrade to the JasperReports 6.19.1 library, the HtmlExporter.exportText() method in the sailpoint.reporting.export package is now deprecated and will be removed in a future release.
IIQSR-825	The option to select Class Action "Identity" in the Audit Configuration page is now available.
IIQSR-818	[SECURITY] Users who have no access to scoped Identities are no longer allowed to make requests for those Identities.
IIQSR-815	A custom filter in a CertificationDefinition is now always copied to a new Certification created from that CertificationDefinition as a template.
IIQSR-810	Classification Filter Rules are now exposed as task arguments. The number of records fetched with

Issue ID	Description
	each SCIM call is now configurable via the "Page Size" argument on the FAM Classifications task. The FAM Classification task is now more tolerant of errors. The "Retry Limit," "Retry Gap," and "Max Errors" arguments have been added to the FAM Classification task to allow users to adjust how tolerant it is.
IIQSR-808	Role Profile synchronization now leverages the proxy Application, if needed, when fetching the entitlement attribute.
IIQSR-807	A "source" attribute value of AttributeAssignment is no longer changed to "Rule" after native deletion and re-provisioning.
IIQSR-804	[SECURITY] The Apache Commons Net library was updated to version 3.9.0 to mitigate a potential vulnerability in Nets FTP client that will by default trust a host from a PASV response. The updated library will by default ignore such hosts.
IIQSR-803	[SECURITY] OAuth secrets are no longer fetched en-masse and will only be fetched with each individual request for the secret of each OAuth client.
IIQSR-801	The Jasper Report for an unpartitioned Account Aggregation task is now rendered successfully on task completion if a partitioned aggregation task is executed concurrently.
IIQSR-800	[SECURITY] Unauthorized server responses (error code 401) that result in browser login prompts can now be overridden to prevent popups.
IIQSR-799	The message "Skipping aggregation of application in maintenance window" now appears for an application in maintenance mode during a partitioned aggregation.
IIQSR-798	Identity Snapshots with unordered entitlement lists no longer cause an error in the Identity Warehouse.
IIQSR-796	Exporting a certification no longer generates an exception if an Identity was deleted after the certification was created.
IIQSR-794	An error no longer occurs when an entitlement owner removes an owned entitlement from another user.
IIQSR-785	Identities with more than 2100 entitlements will no longer throw a Microsoft SQL Server error when viewing the Access list in the View Identity quicklink.
IIQSR-780	Sequential tasks will run accordingly when selected to execute on an alternate host.
IIQSR-779	Errors when loading an object from the database no longer have the potential to cause data corruption.
IIQSR-777	Approving a single work item via My Work -> Work Items, when configured to require comments, no longer generates an exception.
IIQSR-773	Fixed a problem that prevented hierarchical groups from being properly created during partitioned group aggregation.
IIQSR-771	An entitlement provisioned via role is no longer certified as an additional entitlement when the role includes entitlements from multiple applications.
IIQSR-770	The last UI page viewed is now properly restored after a SAML SSO timeout.
IIQSR-767	A revoked entitlement is no longer displayed under Entitlements in the Identity UI.
IIQSR-766	Fixed issue where selecting permitted roles can cause a Hibernate exception when using custom quick-

Issue ID	Description
	links to manage access requests and dynamic scopes are associated with the quicklink.
IIQSR-765	Loading the Manager User Access page no longer makes duplicate calls to REST resource: rest.ui.requestaccess.IdentityIdNameListResource.
IIQSR-763	LinkEdit AttributeRequests in the ProvisioningPlan are now ignored during provisioning, avoiding generation of a manual workitem.
IIQSR-758	Permitted roles may now be deprovisioned via Batch Requests.
IIQSR-756	Application schemas now correctly handle '#' characters in attribute names.
IIQSR-755	Indirectly controlled Scopes are checked when accessing task and report results.
IIQSR-752	Business roles that expire but have a pending expiration extension are now properly adding IT role when the extension is approved.
IIQSR-750	The text displayed in a certification message pop-up is now localized based on the browser's configured language.
IIQSR-747	Auditing the delete of a WorkItem object no longer causes a LazyInitializationException error.
IIQSR-745	Reports downloaded as CSV no longer have repeated headers with misaligned column data.
IIQSR-744	The Manager column is now present in the Certification .csv export after launch of an Entitlement Owner certification.
IIQSR-742	Inherited capabilities are now considered when adding capabilities to groups.
IIQSR-740	Login timeouts no longer cause a cascade of HTTP 408 errors leading to the filling of server logs.
IIQSR-739	[SECURITY] The LCM Manage Password workflow for self-service password reset no longer logs the password in clear text with tracing enabled.
IIQSR-737	The selected QuickLink is now considered during LCM removal of current access items.
IIQSR-735	The "Last Action Status" column in the Manage Accounts identity details table now shows "Failed Enable/Disable" status when the related access request is expired.
IIQSR-733	An error no longer occurs when submitting an access request for an identity in an assigned workgroup with an advanced policy containing a capability.
IIQSR-732	A user with multiple roles which share one or more entitlements no longer provokes a dependency error when the roles are removed after expiration.
IIQSR-729	The status for a completed access request item will now move from "Provisioning" to "Completed" with split provisioning enabled.
IIQSR-727	[SECURITY] Resolved a vulnerability that allows users to change settings on identities who are outside of their control. Refer to the Upgrade Considerations section for more information.
IIQSR-724	The script pre-parser no longer throws a StringIndexOutOfBoundsException for rules with a large number of variable expansions using the $(...) notation.
IIQSR-723	Remediators are now determined for all requests in unmanaged provisioning plans.

Issue ID	Description
IIQSR-722	An error no longer occurs when selecting a saved search in Identity Advanced Analytics.
IIQSR-717	Entitlements included in IT roles are now successfully removed using a sunset date.
IIQSR-711	Removing classifications from Classifiable objects (Entitlements, Roles) now cleans up unneeded records from the spt_object_classification table.
IIQSR-710	Reports that fail now clean up persisted database objects that would otherwise be orphaned.
IIQSR-706	The displayName attribute is now correctly set on an account when the account is created during the provisioning of an entitlement.
IIQSR-699	Attribute sync no longer fails when an Identity has multiple accounts on an application and the target mapping does not have 'Provision to all accounts' selected.
IIQSR-697	The assigned scope for a TaskDefinition is now transferred to the TaskResult for tasks and reports.
IIQSR-696	When running incremental exports, the Data Exporter task now correctly exports objects that had been modified while the previous instance of the Data Exporter task was running.
IIQSR-694	Filtering on Role Source Value during Manage Access no longer causes an error.
IIQSR-692	Sequential Task execution is no longer handled by an active long-running parent task and is instead part of the native function of the TaskManager.
IIQSR-689	Clarified the javadoc comments for the Util.stringToDate() method.
IIQSR-688	Permitted roles that are assigned now show as an assignedRole in the Access Request.
IIQSR-686	Access Request deep links no longer redirect to the self-service page repeatedly or lose track of query parameters.
IIQSR-682	The processing of scheduled assignments no longer generates errors and duplicate requests.
IIQSR-681	Added check in query options to fetch quicklinks for identities with system administrator capability to avoid incorrect roles and entitlements filtering.
IIQSR-679	A log error no longer occurs during Identity Refresh when calculating which Roles to auto-assign via a Population with a multi-value Identity attribute.
IIQSR-678	Initializing date fields in forms with existing values no longer results in errors that prevent the date picker from functioning.
IIQSR-676	An email notification is no longer sent to an owner if the "Email Owner on Pre-Delegation Completion" option is disabled in the Certification configuration.
IIQSR-674	The submit button is now disabled when generating an Access Request, eliminating the possibility for duplicate requests to be created via multiple selects of the ENTER or SPACE keys.
IIQSR-673	Fixed an access request issue that prevented roles from being assigned to the same identity multiple times even when the option to allow it is enabled.
IIQSR-670	A validation error message is now displayed on empty required Date fields after a form submit.
IIQSR-668	System level tasks now allow concurrency where applicable.

Issue ID	Description
IIQSR-666	The 'Perform Maintenance' task now properly releases SailPoint contexts that are used when processing background workflow events.
IIQSR-663	The Managed Attributes of type Identity now store the name of the selected identity to keep consistent with other Managed Attributes.
IIQSR-662	Performance of activity scans with large data sets has been improved.
IIQSR-661	When moving a Link from an Identity, both the target and source Identity will have the 'needsRefresh' flag enabled.
IIQSR-660	When a new certification is created using the “Use Certification as Template” feature to clone an existing certification that has "Require Electronic Signature" enabled, that option can now be disabled in the new certification.
IIQSR-659	Possible database cursor leaks were fixed for situations when the "Aggregate Correlated Applications" task encounters duplicate links.
IIQSR-658	Requests that create an account in which the native id is generated by an application in maintenance mode will now have the corresponding identity request updated with that native id.
IIQSR-657	In a transient Workflow, any XHTML-based forms following the first form are now successfully displayed.
IIQSR-656	The Identity Entitlements Detail report now successfully incorporates filtering by Assigners.
IIQSR-654	Fixed an issue in the Role Archive report that caused the Profiles section to be excluded.
IIQSR-651	Added audit details for certification revoke for provisioning and remediation of certification's item.
IIQSR-645	The CheckedPolicyViolations SCIM API endpoint now consistently returns a description for all policy types.
IIQSR-637	Improved extensibility of Upgrade and Patch framework for modules, including ensuring rsworkflows.xml is imported when required.
IIQSR-635	Improved performance for applying manual decisions to items within Certifications containing several entities with very few items each.
IIQSR-634	When configuring a forwarding user for an identity, the Submit button is now disabled if the "Select User to Forward to" field is empty with "Start Date" and "End Date" specified.
IIQSR-630	CertificationDefinition assigned scope is now applied to the Certification schedule object.
IIQSR-622	When using a custom form, the form owner is now correctly assigned when the name of the identity launching the workflow contains a comma.
IIQSR-617	An Entitlement Owner certification will now revoke all attribute assignments under the same owner of an application instead of only a single entitlement from a group of entitlements.
IIQSR-615	Tracing of the SCIM classes is now possible from the log4j2.properties file.
IIQSR-614	The "Created on" and "Created By" fields are now updated in Identity Events for changes in sunset/sunrise dates.

Issue ID	Description
IIQSR-613	A TaskDefinition is now exported from the console without errors when it contains arguments without a type.
IIQSR-609	Using a forgot password link when multiple passthrough applications are configured no longer results in incorrect authentication questions.
IIQSR-608	IT role mining panels now scale better when several Identity Populations are present.
IIQSR-605	The Role Details report no longer throws an error when thousands of roles are reported on.
IIQSR-604	The owner dropdown on the edit entitlement page now properly displays names containing a "&" rather than "&".
IIQSR-601	Defining an instance attribute in an application no longer results in duplicate attributeAssignments in an Identity.
IIQSR-598	Grouping certification details by display name no longer results in excessive wait times.
IIQSR-584	Identity create forms with postback fields are properly executed before validation.
IIQSR-583	Timings for the following meters no longer produce negative statistics: "PlanEvaluator.execute phase 1", "ServiceRequestExecutor.execute"
IIQSR-568	The AuditLog source for provisioning expansion operations is now displayed correctly instead of "unknown".
IIQSAW-4960	[SECURITY] Values in the displayName field of Identities are now properly sanitized to avoid malicious content.
IIQSAW-4889	Account unlock is now properly translated to Danish.
IIQSAW-4888	The user interface now properly displays Italian language prompts and labels.
IIQSAW-4880	Provisioning no longer fails in cases where an Active Directory account is moved, then deleted, and subsequently added again.
IIQSAW-4675	A defect in processing objects with nonstandard object IDs (since corrected in IdentityIQ 8.4 and 8.3p2) caused NativeIdentityChange propagation to fail, and events to remain in the queue, blocking provisioning. A new task template was added that re-processes these events. The new task "Reset Failed NativeIdentityChange Events" can be used to: report the number of failed events, prune events where the old and new values only differ by case, and reset failed events and launch tasks to re-process them.
IIQSAW-4644	[SECURITY] The Apache Commons Text library was updated to version 1.10.0 to mitigate a potential vulnerability for remote code execution or unintentional contact with remote servers if untrusted configuration values are used.
IIQSAW-4311	Changes made to Distinguished Name that are initiated within IdentityIQ (through Rapid Setup or customizations) now result in appropriate updates to all IdentityIQ objects, and are no longer treated as new identities, but are instead recognized as moves or renames.

Issue ID	Description
IIQSAW-4221	Running group aggregation on a renamed group hierarchy no long produces errors.
IIQSAW-4206	Replaced all uses of the JSON-java library with Jackson.
IIQSAW-4201	lookupByName now works properly for the LaunchedWorkflows SCIM endpoint, and error handling is improved for endpoints that do not support lookupByName, namely Accounts, Entitlements and PolicyViolations.
IIQPB-1646	Workgroups Detail Report no longer show error that indicates a ResultSet closed and now displays the workgroup members list.
IIQPB-1637	Revoke Access no longer creates an account for missing accounts.
IIQPB-1535	When using custom forms for approvals and using e-signatures, form validation now occurs before e-signature prompt.
IIQPB-1490	In Compliance Manager settings, changes to "Require Electronic Signature" are now saved successfully.
IIQPB-1340	The identityai-recommender-plugin.zip version is now tied to the IdentityIQ version. For example, 8.4 includes identityai-recommender-plugin.zip version 8.4
IIQPB-1210	The JasperReports library has been updated to version 6.19.1
IIQPB-1203	Elevated Access icons no longer display under Additional Options in Request Access when LCM Manager has unchecked `Show Elevated Access in Access Requests`.
IIQPB-1166	The Capabilities to Identities Report no longer duplicates identities when they have a capability directly applied and is a member of a workgroup.
IIQMAG-4688	Cloning a role now updates the created and modified dates to the current date.
IIQMAG-4617	In IdentityIQ 8.3 a new feature was introduced to create Native Change Events and process them to update existing accounts and account groups when an application object was renamed or changed by being moved to a different container. This behavior is now limited to Active Directory applications. For all other applications, the behavior in IdentityIQ for object renames will be the same as it was prior to 8.3.
IIQMAG-4591	New Installations or Upgrades will add the new Access History/Data Extract/Broker configuration pages/rights entries into webresources.xml. Clients should review the changes and merge theirs if different from OOTB.
IIQMAG-4430	SCIM update-account PUT now properly assigns the source attribute in the provisioning plan.

Issue ID	Description
IIQMAG-4428	Requesting a new entitlement with sunrise and sunset dates for a user without an account on the application now successfully adds the entitlement on sunrise date and removes the entitlement on sunset date.
IIQMAG-4349	During a partitioned Account Group Aggregation, if any partition fails, the check deleted phase will be skipped.
IIQMAG-4336	Bad data no longer causes a NullPointerException during a role search in Advanced Analytics.
IIQMAG-4316	Account aggregation no longer treats accounts that differ only with blank UUID vs. NULL UUID as a renamed native identity. Instead, accounts with blank UUIDs are treated the same as accounts with NULL UUIDs.
IIQMAG-4310	Native Change Detection is now triggered if aggregated values are different than requested values in Create Account Request.
IIQMAG-4247	NativeIdentityChange propagation no longer fails with the exception ”Attempt to generate refresh event with null object” when the objectID of the object being processed is non-standard. When this error occurred, the failing NativeIdentityChangeEvents blocked provisioning. Customers previously on 8.3 GA or 8.3p1 who encountered this error can resolve this issue using a newly introduced task template, "Reset Failed NativeIdentityChange Events". Refer to the Upgrade Considerations section for more information.
IIQMAG-4223	[SECURITY] Jackson-Databind library updated to resolve security vulnerabilities.
IIQMAG-4211	[SECURITY] The Password Reset process no longer attempts to reset a password for accounts that don't support it.
IIQMAG-4087	'Description' column is now populated in the 'Role Composition Access Review Live Report'.
IIQFW-946	Account Group Membership Certification now includes an entitlement assignment update option, that will update identity assignments.
IIQFW-938	Updated Identity request maintenance task, now correctly calculate statuses when doing 'approval and provision split'.
IIQFW-919	Roles By Application report now completes and does not throw a lazy initialization exceptions.
IIQFW-655	[SECURITY] Form Beans used to process SailPoint Form submissions must now implement the FormBean interface. Anything else will throw an exception and block submission of the form.
IIQCB-4932	The Teams bot now contains translation files to match IdentityIQ.

Resolved Issues - Connectivity

Issue ID	Description
CONCHENAB-4445	The AIX Connector now supports fetch only attributes present in the account schema with an additional application configuration.
CONCHENAB-4487	A new connector "Oracle Fusion HCM Accounts" is now available to govern the accounts of Oracle Fusion HCM system.
CONCHENAB-4493	[SECURITY] To improve security, SailPoint has upgraded the spring-core-5.1.18.RELEASE.jar to spring-core-5.3.20.jar for the RSA Application.
CONCHENAB-4503	[SECURITY] Upgrading the vulnerable ognl jar to the latest version 3.3.4.jar
CONCHENAB-4504	[SECURITY] The Duo Connector now uses okhttp-4.9.3.jar and okio-2.8.0.jar to address the security vulnerability issues reported with previous version of these libraries.
CONCHENAB-4539	[SECURITY] Deprecating commons-httpclient jar due to vulnerability.
CONCHENAB-4541	The Linux Connector now supports Red Hat Enterprise Linux versions 8.4 and 8.5.
CONCHENAB-4564	The spring-web:5.1.18 jar is now upgraded with spring-web:5.2.20
CONCHENAB-4568	IdentityIQ for IBM Security Identity Manager now supports IBM Security Verify Governance v10.0.
CONCHENAB-4571	[SECURITY] To improve security, SailPoint has upgraded the spring-beans-5.1.18.RELEASE.-jar to spring-beans-5.3.20.jar for the RSA application.
CONCHENAB-4576	Workday Accounts Connector now supports managing Service Center Representative accounts.
CONCHENAB-4587	The Duo Connector now follows the proxy settings from application server settings and also can bypass the proxy for hosts mentioned in nonProxyHosts list.
CONCHENAB-4627	The Workday Connector will now respect the autocomplete flag for custom id request.
CONCHENAB-4629	The RSA Connector now supports RSA 8.7 version
CONCHENAB-4633	The RSA Connector now supports RSA 8.6 version
CONCHENAB-4635	[SECURITY] To improve security, SailPoint has upgraded the kotlin-stdlib-1.4.10.jar to kotlin-stdlib-1.7.10.jar for the Duo application.
CONCHENAB-	The Okta Connector will now respect the password policy set in Okta target system in terms of

Issue ID	Description
4640	password age and password History
CONCHENAB-4655	Oracle Fusion HCM Connector will now support the fetching of custom attribute "ExternalIdentifiers" during aggregation and get account operation if appropriate JSON path is provided
CONCHENAB-4656	The Workday Accounts Connector now correctly handles the Invalid Id error.
CONCHENAB-4657	The Oracle Fusion HCM Connectors now adds the ASSIGNMENT_MANAGER_NUMBER as the default attribute in the Account schema.
CONCHENAB-4663	The Oracle Fusion HCM Connector now correctly handles rehire scenarios during the refresh account.
CONCHENAB-4681	Oracle Fusion Connector now supports aggregation of the additional attributes from WORKERS API responses using a JSON path.
CONCHENAB-4695	The Oracle Fusion HCM Connectors account aggregation performance is now enhanced.
CONCHENAB-4723	The Oracle Fusion HCM Connector accounts aggregation will now fail in case of a planned outage (maintenance) from the Oracle system.
CONCHENAB-4724	The Oracle Fusion HCM Accounts aggregation will now fail in case of a planned outage (maintenance) from the Oracle system.
CONCHENAB-4763	The child application account aggregation of Oracle Identity Manager is now successful.
CONCHENAB-4773	The Workday Accounts Connector now supports filtering of accounts based on the Organization Type and Organization Reference ID
CONCHENAB-4775	The Workday Accounts Connector now supports aggregation and provisioning of future accounts ahead of their hire date.
CONCHENAB-4798	The Oracle Identity Manager Connector now provides the ability to filter out target system accounts fromOracle Identity manager users.
CONCHENAB-4801	The Okta Connector now supports the addition and removal of custom roles directly associated withaccounts
CONCHENAB-4803	The IBM Security Verify Access Connector now supports IBM Security Verify Access 10.0.3
CONCHENAB-4819	The Okta Connector now supports the aggregation of custom roles directly associated with both accounts and groups.
CONCHENAB-4825	The Okta Connector now aggregates only the roles connected directly to the Okta user
CONCHENAB-	[SECURITY] All the spring jars are upgraded to a common version for resolving the vul-

Issue ID	Description
4913	nerabilities.
CONCHENAB-4948	The Workday Connector now supports Workday web service version 39.1
CONCHENAB-4961	The old approach to deploying Oracle Identity Manager Web Application is being deprecated.The Oracle Identity Manager Connector is now discontinuing support for Oracle Identity Manager 11g R1 and 11g R2 releases.The Oracle Identity Manager Connector is now capable of supporting Oracle Identity Manager 12C via Oracle Client API.
CONCHENAB-4988	SailPoint announces the release of a new connector Oracle HCM Cloud to govern identities for Oracle Fusion HCM system. For documentation on the new connector, see Integrating SailPoint with Oracle HCM Cloud.
CONCHENAB-5057	The Okta Connector now provides an option for multi-threading when aggregating Groups and Applications connected to Okta Accounts during Okta Account aggregation.
CONCHENAB-5058	The Workday Accounts Connector now provides an option for muti-threading which will boost the Account Aggregation performance.
CONCHENAB-5064	The Okta Connector no longer fails when aggregating the newly introduced group by Okta called "Okta Administrator".
CONCHENAB-5072	[SECURITY] The commons-httpclient.jar 3.1 is now removed due to vulnerability issues.
CONCHENAB-5086	[SECURITY] [SECURITY] The Spring Framework libraries have been upgraded to a newer version due to vulnerabilities found in older versions. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using this JAR file. spring-aop-5.2.22.RELEASE.jar spring/spring-context-5.2.22.RELEASE.jar spring-context-support-5.2.22.RELEASE.jar spring-core-5.2.22.RELEASE.jar spring-expression-5.2.22.RELEASE.jar spring-tx-5.2.22.RELEASE.jar spring/spring-beans-5.2.22.RELEASE.jar spring/spring-web-5.2.22.RELEASE.jar
CONCHENAB-5098	The Oracle Identity Manager Connector now supports the Oracle Identity Manager 12C version.
CONCHENAB-5161	The Workday Accounts Connector now supports additional schema attributes for User-Based Security Group Objects.
CONCHENAB-5179	The Workday Connector now allows adding proxy level parameters in the Workday application.
CONCHENAB-5203	On December 31, 2023, Oracle Fusion HCM Connector will be deprecated and it will no longer be supported. Use the newly released Oracle HCM Cloud Connector. For documentation on the new connector, see Integrating SailPoint with OracleHCM Cloud.
CONCHENAB-	The Workday Accounts connector is now enhanced to integrate with Workday Learning Module

Issue ID	Description
5231	and aggregate the training information associated with the users
CONCHENAB-5322	The RSA Connector now supports Delta Account Aggregation.
CONCHENAB-5328	The IBM Security Identity Manager now supports Delta Aggregation
CONCHENAB-5345	Deprecating REST API support for IBM Tivoli Access Manager connectors.
CONCHENAB-5353	The Linux Connector now supports RHEL version 8.8
CONCHENAB-5371	The IBM AIX Connector has now deprecated IBM AIX 7.1 version.
CONCHENAB-5373	The following versions of Solaris have been depreciated and are no longer supported: Solaris 11.3 SPARC x86 Solaris 11.2 SPARC x86 Solaris 11 SPARC x86 Solaris 10 SPARC x86
CONCHENAB-5374	The RSA Connector has now deprecated RSA 8.3 8.4 and 8.5 version.
CONCHORDS-1254	The RACF Full Connector now supports z/OS 2.5
CONCHORDS-1257	The ACF2 Full Connector now supports z/OS 2.5
CONCHORDS-1344	The BMC Remedy Connector now supports BMC Helix 21.3 system.
CONCHORDS-1358	The Atlassian Suite - Server Connector now supports Jira Service Management: 5.2
CONCHORDS-1416	New Platform Support : Atlassian Server Connector now supports following versions of various Atlassian products - Jira Software Server: 9.6Confluence: 8.1Bitbucket: 8.8Bamboo: 9.2 Drop Platform Support : Atlassian Server Connector no more supports following versions of various Atlassian products - Jira Software Server: 8.13 and 8.12 Confluence: 7.8 and 7.7 Bitbucket: 7.5 Bamboo: 7.1 and 7.0
CONCHORDS-1706	The BMC Helix connector now supports BMC Helix IT Service Management Suite version 22.1
CONDOCS-872	New platform support - Following Mainframe connector now supports z/OS 2.5 system - RACF - Full, ACF2 - Full, Top Secret - Full, Top Secret - LDAP
CONDOCS-949	Dropped platform support - the following Mainframe connectors no longer supports z/OS 2.2 and z/OS 2.3 systems - RACF - Full, ACF2 - Full, Top Secret - Full, RACF - LDAP, Top Secret - LDAP

Issue ID	Description
CONDOCS-1233	A new Snowflake connector is now available to govern identities for Snowflake Data Lake.
CONDOCS-1373	The SailPoint Identity Governance Connector for ServiceNow now no longer supports the ServiceNow Quebec release. IdentityIQ for ServiceNow Service Desk Integration Module (SDIM) now no longer supports the ServiceNow Quebec release.
CONDOCS-1953	Oracle Identity Manager versions 11gR3 , 11gr2 and 11gR1 are deprecated and will no longer be supported.
CONDOCS-2469	The Oracle Solaris connector no longer supports Solaris versions 11.3, 11.2, 11.0 and 10.0
CONDOCS-2472	The Linux connector no longer supports Red Hat Enterprise Linux versions 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8 and Ubuntu OS Version 18.04 LTS.
CONDOCS-2475	The IBM AIX connector no longer supports AIX version 7.1
CONETN-3135	Connectors implementing openConnector's provisioning plan with a null operation in the attribute request will have the default operation as Add, resulting in a successful transaction. However, an account request with a null operation will fail.
CONETN-3442	The Workday Accounts Connector no longer sends additional calls when provisioning ORG_ROLE##ORG_NAME
CONETN-3661	The SAP GRC Integration will now support retry mechanism for polling of requests.
CONETN-3672	The Oracle HRMS Connector now displays a valid error message when the object is not found on the managed system
CONETN-3681	The Microsoft SQL Server Connector now aggregates the child server roles when a group aggregation is performed.
CONETN-3706	The SCIM 2.0 Connector no longer fails with java.lang.IllegalArgumentException when provisioning accounts.
CONETN-3707	The AWS Connector now successfully aggregates accounts from an application whose service account does not have permission for tags.
CONETN-3714	The SAP Direct Connector now aggregates description of a role when group aggregation is performed.
CONETN-3722	The SuccessFactors Connector no longer fails when provisioning the area code for a phone number.
CONETN-3731	The SAP Sybase Connector now uses the latest APIs for provisioning operations.
CONETN-3740	The SAP HR/HCM Connector now supports using state variable in the buildmap rule when running partitioned aggregation.
CONETN-3742	The SAP HR/HCM Connector no longer fails when performing a delta aggregation for an application with custom BAPI configured.
CONETN-3743	The Workday Connector no longer aggregates an attribute whose value is cleared from the target system.

Issue ID	Description
CONETN-3753	The SCIM 2.0 Connector now correctly aggregates the multivalued attributes from an extended schema.
CONETN-3758	The SCIM 2.0 Connector now aggregates sub-attributes of an account's manager when performing account aggregation.
CONETN-3763	The JDBC Connector now supports provisioning on all the configured group types of an application.
CONETN-3764	The SuccessFactors Connector aggregation no longer fails with connection reset error when an account aggregation is performed.
CONETN-3778	The Google Workspace Connector now uses the attribute "isContinueOnError" when configured in the application during delta aggregation to skip corrupted accounts.
CONETN-3788	The Okta Connector no longer reads unnecessary data from the target when provisioning an account.
CONETN-3789	The REST Web Services Connector now saves application without any error when client certificate is saved in application config and browser is in non-English mode.
CONETN-3791	The Workday Account Connector now successfully retries the errors during group and account aggregation which are defined as part of "retryableErrors" in the application config.
CONETN-3792	In the Azure Active Directory Connector, it is now optional to encode the attribute immutableId used while provisioning of Federated User Account
CONETN-3796	The SCIM 2.0 Connector no longer fails with provisioning group having attribute "id" with a value of type Double.
CONETN-3800	A provisioning rule with name of more than 32 characters is now supported.
CONETN-3802	The REST Web Services Connector now correctly retries errors when the only error code is defined in retryableErrors.
CONETN-3804	The account aggregation of the HCL Domino Connector now fetches the groups based on the flag "fetchGroupsForAllUsernames" which is true by default and can be set to false to improve account aggregation time
CONETN-3806	The SAP Direct Connector now correctly aggregates description of a role from a CUA enabled managed system.
CONETN-3813	ServiceNow account aggregation with partition now aggregates accounts and its roles and groups properly.
CONETN-3814	The axiom.xml for connectors now includes all supported implementations.
CONETN-3818	The Oracle Fusion HCM Connector now correctly aggregates custom attributes for future hire workers.
CONETN-3820	Azure Active Directory Group aggregation now correctly aggregates "teamsEnabled" attribute.
CONETN-3821	IQService now uses skipDNSLookup application config to skip the DNS lookup for the

Issue ID	Description
	Exchange server when connecting over TLS for Active Directory application.
CONETN-3823	The Oracle Fusion HCM Connector now correctly provisions all supported attributes of a future hire worker.
CONETN-3833	The PIRM task no longer removes the entitlements for sub-domain accounts of Google Workspace connector.
CONETN-3835	The Workday Connector now correctly skips the future hired workers whose hire date is corrected when an aggregation is performed.
CONETN-3837	The aggregation for LDAP Connector will not be retried without retryableErrors entry in the application during PAGED_RESULTS iterate mode.
CONETN-3850	The Azure Active Directory Connector now supports managing Azure PIM Role memberships to Azure Active Directory groups
CONETN-3867	The PeopleSoft Connector now supports the 8.59 PeopleTools environment
CONETN-3871	Salesforce PublicGroups entitlement will be using Group Name instead of Name to aggregate and Provisioning operation as it is unique on the Salesforce managed System. This will be applicable for the new source only and there won't be impact on the existing sources. For the new sources created, switching to older alike source will be possible by making below flag false in the source config file: <entry key- ="PublicGroupIde- entityAttributeAsDeveloperName"><value><Boolean>false</Boolean></value> </entry>
CONETN-3882	The Linux Connector getObject operation now properly fetches values for the sudoCommands if configured in schema.
CONETN-3885	The Oracle HCM Fusion Connector now correctly provisions the date attributes of an email for an account.
CONETN-3889	The Workday Connector no longer fails with java.lang.ClassCastException when an aggregation is performed for an application with ROCustomisation rule.
CONETN-3896	Account Request attributes will no longer be removed from attributes of ProvisioningPlan between Before Provisioning and After Modify Rule during provisioning operation.
CONETN-3898	The SAP GRC Integration will now skip proactive check for a role assignment if "skipProactiveCheck" is set to true in the application.
CONETN-3901	The Oracle HCM Fusion Connector now correctly aggregates the updated values for AssignmentStatusTypeId and AssignmentStatusType attributes when a delta aggregation is performed.
CONETN-3903	The Azure Active Directory Connector now fetches all the shared mailboxes during account aggregation.
CONETN-3911	The Oracle ERP Cloud Connector no longer fails when provisioning a data access containing

Issue ID	Description
	special characters in its role name and security context value.
CONETN-3916	The RACF-Full Connector now supports resource aggregation and provisioning as additional group schema, and requesting permissions for accounts and groups. Refer to documentation for more details.
CONETN-3923	The Azure Active Directory Connector now manages mail-enabled security groups or distribution groups using IQService without any error.
CONETN-3924	The Oracle HCM Fusion Connector correctly aggregates the updated attributes when a delta aggregation is performed.
CONETN-3925	The REST Web Services Connector now correctly sets the root path from Before Operation Rule.
CONETN-3929	The PlanInitializerScript in Applications of type RACF, ACF2, and TopSecret no longer use imports and System.out.println statements.
CONETN-3931	IQService will no longer show the errors/warnings messages related to UpgradeService while running the Perform Maintenance task from IdentityIQ.
CONETN-3936	The Workday Connector is now certified with Workday API version 38.0
CONETN-3938	The Azure Active Directory Connector no longer throws the error "Fail to find owners of a channel " while channel aggregation in case the channel is soft deleted.
CONETN-3949	The Salesforce Connector account aggregation no longer fails when URL in the source is changed.
CONETN-3950	The Oracle HCM Fusion Connector will now correctly aggregate changes to all supported attributes in delta aggregation.
CONETN-3951	The Azure Active Directory Connector now displays ExchangeOnline attributes on the UI after account aggregation when "Manage Exchange Online" feature is enabled.
CONETN-3956	The Oracle Fusion HCM Connector correctly aggregates the ASSIGNMENT_MANAGER_ID value when an aggregation is performed.
CONETN-3957	The SCIM 2.0 Connector now correctly updates the roles for an account when provisioning or de-provisioning operation is performed.
CONETN-3959	The SCIM 2.0 Connector no longer fails with a NullPointerException when multiple complex attributes are provisioned.
CONETN-3960	The SAP HR/HCM Connector no longer fails with NullPointerException when aggregating accounts with custom value for STAT2 field.
CONETN-3962	The Oracle HCM Fusion Connector now skips the terminated users falling outside the termination offset when a delta aggregation is performed.
CONETN-3968	The Oracle HCM Fusion Connector now correctly aggregates future hires when a delta aggregation is performed.

Issue ID	Description
CONETN-3971	The REST Web Services Connector configuration page now correctly displays necessary attribute as per grant type selection on UI for OAuth 2.0 authentication.
CONETN-3974	For Active Directory applications, no warning message will be displayed in the GUI when delta aggregation is performed followed by completion of Refresh task in which group membership is being removed.
CONETN-3975	The filter string for the account additional filter will be saved as account.filterString in the source application file for LDAP connectors.
CONETN-3979	The RACF connector no longer fails to aggregate unstructured targets and permissions when Mainframe connector is upgraded to FSD0148 or later.
CONETN-3980	The Active Directory Connector now successfully provisions msExchHideFromAddressLists with type as string.
CONETN-3982	The Web Services Connector now supports http proxy configuration for OAuth authentication.
CONETN-3984	The ServiceNow Connector account aggregation with partitioning enabled no longer query sys_user_grmember and sys_user_has_role when no entitlement attributes are present in the account schema.
CONETN-3985	The Azure Active Directory Connector no longer displays duplicate ServicePrincipals values in Resource Object after running account aggregation.
CONETN-3987	Adding the attribute skipGroupFilterAttributeReplacement as true in the application , the Azure Active Directory Connector no longer fails while creating the group when group filter contains a value same as that of the attribute's name.
CONETN-3988	The SCIM 2.0 Connector correctly provisions the manager attributes using patch operation.
CONETN-3989	The Active Directory Connector now correctly provisions msExchHideFromAddressLists.
ONETN-3990	The Oracle Fusion HCM Connector now excludes Suspended workers when "skipSuspendedAccounts" is enabled in the application during aggregation.
CONETN-3991	The Azure Active Directory Connector now displays the correct spelling for UserPrincipalName in provisioning policy.
CONETN-3998	The CloudGateway application now supports retryableErrors configuration for provisioning retry.
CONETN-3999	The SharePoint Online Connector now fetches all sites including newly created sites during aggregation.
CONETN-4002	The Azure Active Directory Connector no longer errors out the request while fetching the SignIn Activity of users during account aggregation.
CONETN-4003	The SCIM 2.0 Connector now sends the path attribute for all patch operations when an extended schema attribute is included in provisioning.
CONETN-4009	The SAP HR/HCM Connector no longer fails when a delta or partitioned aggregation is per-

Issue ID	Description
	formed.
CONETN-4010	The SAP HR Connector now has improved performance for delta aggregation.
CONETN-4012	The Azure Active Directory Connector now fetches the Exchange Online custom attributes during account aggregation or getObject operation.
CONETN-4013	The SCIM 2.0 Connector now supports provisioning of complex attributes using PUT operation.
CONETN-4014	The Oracle Fusion HCM Connector can now aggregate delta changes for all attributes supported by the Oracle Atom Feed APIs.
CONETN-4019	The Azure Active Directory Connector now supports advanced query filters during account as well as group aggregation.
CONETN-4023	The Azure Active Directory Connector now fetches all the Resource Groups during entitlement aggregation.
CONETN-4024	The SAP Direct Connector correctly provisions the Parameter attribute for new and existing accounts on the target system.
CONETN-4025	MANIFEST.MF file in IdentityIQCloudGateway.jar now correctly reflects the version details along with patch.
CONETN-4027	The Before and After Provisioning rules are now correctly called when executeManagedAppRules flag is set to true.
CONETN-4029	The Active Directory Connector now ignores delta changes for users in Resource forest having msExchMasterAccountSid equals S-1-5-10.
CONETN-4031	The REST Web Services Connector now waits for max 3 minutes per retry while throttling request.
CONETN-4033	The Okta Connector now correctly aggregates the changed users when a delta aggregation is performed.
CONETN-4041	The Google Workspace Connector no longer logs an error message if there are no delegates during account aggregation.
CONETN-4042	The Oracle Fusion HCM Connector now aggregates the correct data when a delta aggregation is performed
CONETN-4044	The Microsoft SQL Server Connector now supports aggregating membership details of nested database roles when an entitlement aggregation is performed.
CONETN-4046	Mainframe Connectors (RACF-Full, ACF2-Full, and TopSecret-Full) Enhanced to support mutual TLS authentication for communication between IdentityIQ, Connector Gateway, and the Mainframe Connector itself.Upgrade to latest Connector Gateway to leverage this feature.
CONETN-4047	Aggregation with cloudGateway on tomcat 9.0.69 onwards now works properly after adding following attribute in application. <entry key="httpCookieSpecsStandard" value="true"/>
CONETN-4049	The Google Workspace Connector no longer fails with HTTP error 404 while updating alias

Issue ID	Description
	along with primary email address of the user.
CONETN-4057	The Azure Active Directory Connector now fetches all the resource groups during entitlement aggregation.
CONETN-4058	The Connector Gateway does not break interceptions protocol for continuous transactions from IdentityIQ connector side which are sent to CTSGATE for continuous 30 minutes.
CONETN-4062	The Mainframe Connector now supports setting provisioning result at attribute level with warning at account request in case of partial success.
CONETN-4064	The Azure Active Directory Connector now fetches the Exchange Online attributes for all the accounts.
CONETN-4065	The LDAP Connector now removes entitlement as part of delete provisioning operation when remove entitlement is sent to connector as part of attribute request.
CONETN-4066	The assignment of entitlement ServicePrincipal alone now works during account creation in Azure Active Directory Connector.
CONETN-4067	The SAP HR/HCM Connector no longer fails when no employees are fetched from PA0000 table in target system.
CONETN-4068	The Workday Connector no longer fails when performing provisioning for CUSTOM ID's with empty or null values.
CONETN-4073	WORKATTR attributes and other similar attributes are now updated while performing create and update operation on user account as we added <UserProfileName>_SWITCH which is set as 'Y' when these attributes are considered to be updated.
CONETN-4077	The Oracle E-Business Connector now correctly provisions the customer_id and supplier_id attributes of an account when a provisioning operation is performed.
CONETN-4078	The LDAP Connector now clears group membership when null value is passed in SET operation.
CONETN-4080	The REST WebServices Connector now supports pagination using pagination steps for child endpoint as well during aggregation.
CONETN-4081	The Google Workspace Connector now clears the "customSchema" attributes when null value is passed in SET operation.
CONETN-4083	The Active Directory Connector no longer shows a false error message in the log during getObject operation for create Group operation.
CONETN-4084	The SCIM 2.0 Connector now supports Provisioning Multivalued core and extended attributes.
CONETN-4085	The SCIM 2.0 Connector can now aggregate accounts from a non-compliant SCIM target server when the /Users response is not compliant with RFC.
CONETN-4086	The Oracle ERP Cloud Connector now supports provisioning of data access having special characters in its security context values.

Issue ID	Description
CONETN-4087	Identity Governance Connector for ServiceNow now supports Utah release. ServiceNow ServiceDesk Integration Module for ServiceNow now supports Utah release.
CONETN-4091	The delta aggregationfor ServiceNow Connector no longer fails in case if an empty group or an empty user is present in ServiceNow memberships.
CONETN-4099	The Workday Connector no longer fails with "XML parsing failed" error when performing account aggregation.
CONETN-4103	The Delimited File Connector now supports aggregation of accounts containing special characters in its attributes.
CONETN-4108	The RACF Connector using After Provisioning rule with EmailTemplate no longer shows a blank email body.
CONETN-4109	The BoxNet Connector now successfully deletes user who is owning content on the Managed system when forceDeleteUser=true application config is configured.
CONETN-4113	The SCIM 2.0 Connector will call /ServiceProviderConfig endpoint only for compliant enabled applications.
CONETN-4114	The Salesforce Connector now correctly sends null value attribute in update request to manage system during provisioning.
CONETN-4115	The Apachex.x/conf/server.xml file now contains the value for "Error Report Valve" default as false
CONETN-4116	The JDBC Connector now aggregates correct value for an account attribute of type BigDecimal or Float.
CONETN-4117	The Oracle Fusion HCM Connector can now choose to aggregate values based on configured JSON path or default OOTB values during account aggregation.
CONETN-4120	The SAP Direct Connector now supports setting password to productive mode when a Create Account operation is performed.
CONETN-4123	The Google Workspace Connector no longer fail while provisioning the already existing group on target system to the user.
CONETN-4125	IQService will not log any error message during provisioning if custom attribute is not present in ActiveDirectory Schema on IQService host.
CONETN-4130	The Azure Active Directory Connector now does not throw an error while creating guest user when the email ID has a sub-domain of an another existing user's email domain.
CONETN-4134	The Azure Active Directory Connector now honors the HTTP proxy settings configured as Java system properties.
CONETN-4135	IQService Client authentication will now use system default logon provider.
CONETN-4137	In the Active Directory Connector domain NetBIOSName will be aggregated as part of account and group aggregation. Customers need to add NetBIOSName as schema attribute as type

Issue ID	Description
	String under Account and Group schema to leverage this facility.
CONETN-4140	The Active Directory Connector now successfully updates Exchange attributes for distribution groups without mailnickname passed in provisioning plan.
CONETN-4141	The Azure Active Directory Connector now saves the ServicePrincipal memberships in the List during account aggregation.
CONETN-4147	The Active Directory account creation with add Entitlements no longer fails with SQLGrammarException when object is not found on Active Directory.
CONETN-4149	The SCIM 2.0 Connector now supports provisioning and de-provisioning of groups using /Users endpoint.
CONETN-4153	The REST Web Services Connector now updates lastAggregationDate_account only when account aggregation is successful.
CONETN-4154	The Azure Active Directory Connector now provisions the guest user successfully even if the attribute password is present in the provisioning plan.
CONETN-4162	The Coupa connector now correctly provisions any additional account attribute.
CONETN-4174	The SAP SuccessFactors Connector no longer fails with Null Pointer Exception when a provisioning operation is performed.
CONETN-4180	The Azure Active Directory Connector now honors the HTTP proxy authentication configured as Java system properties.
CONETN-4181	The Salesforce Connector now executes the provisioning plan successfully for the Account Disable operation when the plan contains UserRoleName in it.
CONETN-4191	The SCIM 2.0 Connector can now exclude custom header and request attributes when using OAUTH 2.0 based authentication.
CONETN-4192	The Azure Active Directory Connector no longer throws an error, "Your password has expired", after the user resets their password using PTA.
CONETN-4197	The Slack Connector now removes phone number value when phone number value set to null or no value through provisioning plan.
CONETN-4198	The Azure Active Directory Connector now allows to assign permanent PIM roles to the users and role assignable groups.
CONETN-4202	The SCIM 2.0 connector no longer fails when the Identity attribute is configured as an Integer during a provisioning operation.
CONETN-4206	The SCIM 2.0 connector now supports role provisioning for an account for a PUT operation.
CONETN-4211	The Oracle ERP Cloud connector correctly revokes data accesses of an account when a de-provisioning is performed.
CONETN-4213	User Filters, Group Filters, User Advanced Filters and Group Advanced Filters field are now available on application ui page by default so making entries of these keys is in the application

Issue ID	Description
	xml file through debug page is not required any more.
CONETN-4223	The Azure Active Directory Connector now supports filters for the Directory Roles, Azure AD PIM Active and Eligible Roles, Azure PIM Active and Eligible Roles in the group aggregation.
CONETN-4244	The Azure Active Directory Connector now retries the intermittent errors, if the 'retry-ableErrorsOnAgg' attribute is configured during the channel aggregation.
CONETN-4245	The Azure Active Directory Connector now excludes Disabled/Deleted Subscriptions during Entitlement Aggregation to avoid Aggregation Failure.
CONETN-4248	In ServiceNow Identity Governance Connector, delta account aggregation performance can be improved by configuring the attribute 'maxDeltaAccountsCountToSkipCache' in case of less number of changed accounts.
CONETN-4260	The SAP Fieldglass Connector now aggregates all accounts correctly when the pageSize is configured to any value in the application.
CONETN-4266	The Linux Cconnector now support RHEL version 8.8
CONETN-4271	Entitlements are now added/removed on given sunrise/sunset date when provisioned via connected application with Cloud Gateway
CONETN-4275	Aggregations are now successfully completed with cloud gateway running on tomcat server 9.0.75
CONHOWRAH-3749	The Azure Active Directory Connector is now more resilient in handling IndexOutOfBoundsException while building PIM membership during account aggregation.
CONHOWRAH-3764	[SECURITY] The Azure Active Directory Connector now supports certificate based modern authentication to communicate with Exchange Online which is more secure and is recommended by Microsoft.
CONHOWRAH-3769	The Active Directory Connector now supports Microsoft Windows Server 2022
CONHOWRAH-3772	The Windows Local Connector now supports Microsoft Windows Server 2022
CONHOWRAH-3775	The Azure Active Directory Connector now fetches eligible and active roles only when PIM flag is enabled on the application configuration.
CONHOWRAH-3782	The Google Workspace Connector now supports archiving and unarchiving a user.
CONHOWRAH-3821	An error during partitioned account aggregation has been resolved in the Active Directory connector occurring when caching is enabled.
CONHOWRAH-3836	The Azure Active Directory Connector now respects the provided Azure Management API endpoint in the application configuration to form access token scope instead of a predefined static value.

Issue ID	Description
CONHOWRAH-3861	The LDAP Connector has been enhanced to support Modify Time Stamp as new delta aggregation mode. The user interface of the connector has also been updated to configure it with the necessary details required to connect to most of the LDAP Directory servers.
CONHOWRAH-3871	The Azure Active Directory Connector now provides visibility into user's sign-in (last login) activity.
CONHOWRAH-3911	The Azure Active Directory Connector now supports managing Azure Active Directory Role as a group object.
CONHOWRAH-3986	The SharePoint Online Connector now supports configurable endpoints when Azure Active Directory is deployed in non-public national cloud server.
CONHOWRAH-3990	The Azure Active Directory Connector now supports Continuous Access Evaluation (CAE) which leverages the Azure Active Directory real-time enforcement of Conditional Access location and risk policies along with instant enforcement of token revocation events for an enterprise application (service principal).
CONHOWRAH-3993	The IQService has now different configuration option to specify the IP or FQDN of the load balancer to distinguish the health check requests originating from load balancer for logging purpose.
CONHOWRAH-4010	SailPoint is pleased to announce a new connector to govern identities for your Coupa system. For more information, refer to Integrating SailPoint with Coupa connector guide.
CONHOWRAH-4042	The HCL Domino Connector now supports HCL Domino version 12.0.2.
CONHOWRAH-4055	The Azure Active Directory Connector now supports management of Access Packages.
CONHOWRAH-4084	The Azure Active Directory Connector now supports managing user-assigned managed identities. For more information, refer to Integrating SailPoint with Azure Active Directory Connector guide.
CONHOWRAH-4092	The Microsoft SharePoint Server Connector now supports managing Microsoft SharePoint Server Subscription Edition.
CONHOWRAH-4164	The Azure Active Directory connector now supports reading and writing Azure Multi-Factor Authentication attributes required for different authentication methods.
CONHOWRAH-4186	The Azure Active Directory connector now supports the PowerShell EXO V3 module for the Exchange Online Management feature.
CONHOWRAH-4199	The Azure Active Directory Connector now supports filters for Channels during entitlement aggregation.
CONHOWRAH-4224	[SECURITY] Due to the security vulnerabilities found in the json-smart-2.4.7.jar file, it has been upgraded with json-smart-2.4.10.jar. Ensure to update custom connectors, rules, or any other

Issue ID	Description
	customizations that directly or indirectly reference the json-smart-2.4.7.jar file to json-smart-2.4.10.jar.
CONHOWRAH-4278	The Azure Active Directory source now supports the aggregation of Azure Active Directory group hierarchy.
CONHOWRAH-4322	The Azure Active Directory connector now supports managing Service Principal for Enterprise Applications as an Account.
CONHOWRAH-4345	The Azure Active Directory connector now supports creating SAML based applications and corresponding Service Principals using the Gallery application templates.
CONHOWRAH-4346	The Azure Active Directory connector now supports creation of Service Principals for already existing Applications (Local / Multi Tenant Type)
CONJUBILEE-1164	The Salesforce Connector now processes PermissionSetLicense first while provisioning both PermissionSet and PermissionSetLicense.
CONJUBILEE-1178	For new applications, the SCIM 2.0 Connector schemas will have optional attribute "externalId" irrespective of schema endpoint response.
CONJUBILEE-1339	The Salesforce Connector now provisions Profile before Role.
CONJUBILEE-1377	For the REST Web Services Connector, the body section will be disabled in UI for the HTTP method 'GET'.
CONJUBILEE-1454	Below jars are upgraded to newer versions due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using these jar filesjersey/hk2-api-2.6.1.jar->jersey/hk2-api-3.0.3.jarjersey/hk2-locator-2.6.1.jar->jersey/hk2-locator-3.0.3.jarjersey/hk2-utils-2.6.1.jar->jersey/hk2-utils-3.0.3.-jarjersey/jersey-hk2-2.31.jar->jersey/jersey-hk2-3.0.4.jar
CONJUBILEE-1458	[SECURITY] To enhance security, upgraded gson-2.8.5.jar with vulnerabilities to gson-2.9.0.-jar.
CONJUBILEE-1467	The connector classloader now provides the ability to delegate loading of some classes and packages from system classloader.
CONJUBILEE-1492	The SCIM 2.0 Connector now works with Cloud Gateway.
CONJUBILEE-1495	In latest Jersey library, “Java Validation API” library has been removed (Package : javax.validation). So the “Bean Validation API“ library has to be added separately for customisation, if required. Below jars are upgraded to newer versions due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using these jar files.jersey/jakarta.annotation-api-1.3.5.jar->jersey/jakarta.annotation-api-2.1.0.jarjersey/jakarta.validation-api-2.0.2.jar->jer-

Issue ID	Description
	sey/jakarta.validation-api-3.0.1.jar jersey/jersey-hk2-2.31.jar -> jersey/jersey-hk2-3.0.4.-jarjersey/jakarta.ws.rs-api-2.1.6.jar->jersey/jakarta.ws.rs-api-3.1.0.jarjersey/jersey-client-2.31.-jar->jersey/jersey-client-3.0.4.jarjersey/jersey-common-2.31.jar->jersey/jersey-common-3.0.4.jarjersey/jersey-container-servlet-core-2.31.jar->jersey/jersey-container-servlet-core-3.0.4.jarjersey/jersey-media-jaxb-2.31.jar->jersey/jersey-media-jaxb-3.0.4.jarjersey/jersey-media-multipart-2.31.jar->jersey/jersey-media-multipart-3.0.4.jarjersey/jersey-server-2.31.jar->jersey/jersey-server-3.0.4.jarscim-sdk-1.8.18.01/jersey-apache-connector-2.22.2.jar->scim-sdk-1.8.18.01/jersey-apache-connector-3.0.4.jar
CONJUBILEE-1503	The REST Web Services Connector now supports Create/Update/Delete for Group Objects
CONJUBILEE-1521	The IdentityIQ Cloud Gateway Synchronisation task now decrypts nested credentials before syncing to Cloud Gateway server.
CONJUBILEE-1594	The SCIM 2.0 Connector no longer ignores No Authentication headers when set up with a Relax configuration. The SCIM 2.0 Connector now supports placeholders so that you can include sensitive attributes in No Authentication headers.
CONJUBILEE-1600	The REST Web Services Connector no longer ignores Connection Timeout value.
CONJUBILEE-1604	The REST Web Services Connector's Custom Authentication operation no longer ignores XPath Namespace Mappings.
CONJUBILEE-1617	The Jack Henry Connector now supports enabling or disabling the accounts.
CONJUBILEE-1622	The Salesforce Connector now supports creating, updating and deleting Public Groups. Note: Please make sure your service account user has "Public Groups" object [R || W] added into administrative user profile
CONJUBILEE-1644	Below jars are upgraded to newer versions due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using these jar files. bcel-6.5.0 -> bcel 6.6.1
CONJUBILEE-1655	The REST Web Services Connector now supports removing entitlements while disabling account and adding entitlements while enabling account.
CONJUBILEE-1660	Below jars are upgraded to newer versions due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using these jar files. bcprov-ext-jdk15on-1.61 -> bcprov-ext-jdk15on-1.70
CONJUBILEE-1661	Below jars are upgraded to newer versions due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using these jar files. bcprov-ext-jdk15on-1.61 -> bcprov-ext-jdk15on-1.70

Issue ID	Description
CONJUBILEE-1667	The Cloud Gateway now supports Oracle JRE for Java version 17 and OpenJDK 17 platforms.
CONJUBILEE-1685	With this release, the Salesforce Connector no longer supports Salesforce API versions 48.0 and prior, the connector will only work on API version 56. API version 56 doesn't support attribute "UserPermissionsMobileUser", hence customers must remove the UserPermissionsMobileUser parameter from schema manually, to avoid errors.
CONJUBILEE-1689	The REST Web Services Connector example rules now show use of Web Services operation rules to help configure the searchAfter parameter for pagination.
CONJUBILEE-1694	The Salesforce connector now supports creating new Portal and Partner Users as well as assigning Portal and Partner Licenses to existing Salesforce Users using their respective user profiles. Note: Please make sure your service account user has "Manage Contacts" object [R || W] added into administrative user profile
CONJUBILEE-1696	Below JAR is upgraded to newer version due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customisation, which are directly or indirectly using this JAR file. accessors-smart-1.2.jar -> accessors-smart-2.4.8.jar
CONJUBILEE-1697	Below JAR is upgraded to newer version due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customisation, which are directly or indirectly using this JAR file. commons-net-3.6.jar -> commons-net-3.9.0.jar
CONJUBILEE-1762	The REST Web Services Connector aggregation runs fine if the partitioned aggregation option is selected and no endpoint for partitioned aggregation provided.
CONJUBILEE-1805	The Salesforce Connector now supports use of "Enhanced Domains" option in Salesforce system.
CONJUBILEE-1806	The Cloud Gateway now supports RHEL 9.0.
CONJUBILEE-1809	[SECURITY] Due to security vulnerabilities discovered in the json-smart-2.4.7.jar file, it has been upgraded with json-smart-2.4.10.jar. Be sure to update custom connectors, rules, or other customisations which directly or indirectly reference the json-smart-2.4.7.jar file.
CONJUBILEE-1815	Now all operations for target collectors are executed in Cloud Gateway, if configured.
CONJUBILEE-1859	The Cloud Gateway is now shipped with secure tomcat release Apache Tomcat 9.0.75.
CONJUBILEE-1869	The Salesforce Connector can now complete user provisioning without errors even if the Integration User doesn't have full permissions to the Contact object in the Salesforce system.
CONJUBILEE-1960	The IdentityIQ Cloud Gateway now supports Windows Server 2022.

Issue ID	Description
CONJUBILEE-1987	Below jars are upgraded to newer versions due to vulnerabilities found in older version. Please check the impact on custom connectors, rules or any other customization, which are directly or indirectly using these jar files. bcel-6.5.0 -> bcel 6.6.1
CONNAMDANG-3719	The SAP SuccessFactors Connector is now enhanced to fetch the primary employment information
CONNAMDANG-3778	A new Snowflake Connector is now available to govern identities for Snowflake Data Lake.
CONNAMDANG-3787	The SuccessFactor Connector now enhanced to fix the performance issues in account aggregation
CONNAMDANG-3847	The SAP Hana DB Connector now supports SAP HANA 2.0 SPS6 version.
CONNAMDANG-3866	The SuccessFactors Connector has been enhanced to support the account delta aggregation.
CONNAMDANG-3911	The SAP Hana Database Connector now enhanced to support get and provisioning of external type users
CONNAMDANG-3918	The Snowflake Connector now enhanced to improve the performance of entitlement aggregation.
CONNAMDANG-3989	The SAP HANA Database Connector now supports Custom User Parameters for Aggregation and Provisioning
CONNAMDANG-4000	The SAP HR/HCM Connector has been redesigned to use RFC_READ_TABLE according to SAP recommendations for enhanced security and technology adoption. The connector now uses a SAP-certified function module to support the documented use cases. For more information on configuration and installation, refer to SailPoint Add-On to replace the use of RFC_READ_TABLE.
CONNAMDANG-4007	The Microsoft SQL Server - Direct Connector is now enhanced to support Azure SQL managed instance.
CONNAMDANG-4032	The Microsoft SQL Server - Direct Connector now supports MS SQL Server 2022
CONNAMDANG-4033	The SAP SuccessFactors Connector is enhanced to exclude PII data for employees.
CONNAMDANG-4076	The SAP SuccessFactors Connector is now enhanced to manage external users and their entitlements who are in the onboarding stage.
CONNAMDANG-4101	IdentityIQ now supports new connector for integrating with the ‘Azure SQL' database.
CONNAMDANG-	The JDBC Connector is enhanced to fix probable injections in non-parameterised get object

Issue ID	Description
4126	queries.
CONNAMDANG-4129	[SECURITY] The mysql-connector-java-8.0.30.jar has been upgraded to newer version mysql-connector-java-8.0.33.jar due to vulnerabilities found in older version.
CONNAMDANG-4158	[SECURITY] “commons-collections-3.2.2.jar“ has been upgraded to “commons-collections4-4.4.jar” due to security vulnerabilities in connector-bundle-webservices and connector-bundle-jdbc
CONNAMDANG-4161	[SECURITY] Due to security vulnerabilities discovered in the json-smart-2.4.7.jar file, it has been replaced with json-smart-2.4.10.jar. Be sure to update custom connectors, rules, or other customisations which directly or indirectly reference the json-smart-2.4.7.jar file.
CONNAMDANG-4168	The SAP SuccessFactors Connector now supports additional attributes and custom attributes related to user entities via ODATA API.
CONNAMDANG-4201	The SuccessFactors connector is now enhanced to aggregate selective records based on filtering criteria on employee records
CONNAMDANG-4291	The SAP HANA DB connector now works with SAP HANA Cloud DB ver 4.0 application.
CONNAMDANG-4304	The PeopleSoft HCM Connector now supports PeopleTool version 8.60.
CONSEALINK-2597	A new healthcare integration “IdentityIQ for EPIC SER” is now available to govern the providers from EPIC.
CONSEALINK-2695	The EPIC Connector test connection no longer fails on Oracle JDK 11 as the Bouncy Castle library is upgraded to 1.70 version.
CONSEALINK-2925	The Cerner Connector is now enhanced for efficient handling and closure of HTTP resources.
CONSEALINK-3009	For the Collaboration bundle, "jersey-common" jar has been upgraded to version 2.37 and its dependent jar "jersey-client" has also been upgraded to 2.37
CONSEALINK-3011	IdentityIQ now supports the BMC Helix Remedyforce Service Desk Integration Module.
CONSEALINK-3042	The IdentityIQ for ServiceNow Service Desk Integration now supports pulling RITM status in SailPoint.
CONSEALINK-3060	The pending users from the Zoom User management are now successfully aggregated using the Zoom Connector.
CONSEALINK-3075	The ServiceNow Identity Governance Connector account filter handling for sys user has role and sys user grmember is taken care of during cache initialization.
CONSEALINK-3101	The Cerner Connector delete operations no longer fail if no additional attribute requests are provided.

Issue ID	Description
CONSEALINK-3103	With the Zoom Connector, the assignment of multiple groups is now updated in the right format when a user is a member of more than one group.
CONSEALINK-3110	The EPIC Connector now supports Epic version May 2022.
CONSEALINK-3158	1) The ServiceNow Identity Governance Connector no longer supports the ServiceNow Paris release. And, 2) The IdentityIQ for ServiceNow Service Desk no longer supports the ServiceNow Paris release.
CONSEALINK-3162	1) The SailPoint Identity Governance Connector for ServiceNow now supports the ServiceNow Tokyo release. 2) The IdentityIQ for Service Desk now supports the ServiceNow Tokyo release.
CONSEALINK-3190	The Slack Connector now supports creation of a guest user to have access to a single channel or multiple channels in Slack Enterprise Grid Plan.
CONSEALINK-3191	The Cerner Connector now aggregates invalid account usernames without failing.
CONSEALINK-3234	The Zoom Connector now supports OAuth 2.0 authentication mechanism.
CONSEALINK-3243	The Zendesk Connector now filters the accounts correctly without any error.
CONSEALINK-3274	Jaxen library upgraded to a compatible version for supporting JDK 11
CONSEALINK-3275	The Siebel Connector now supports Siebel server version 22.8.0.0.
CONSEALINK-3276	BMC Helix ITSM Service Desk Integration Module now supports version 21.3. With this new version, it supports Service Request via Digital Workplace with new Ticket Type "DWP Service Request".
CONSEALINK-3287	All Service Desk Integration Module Configuration now supports attribute "provisioningRequestExpiration", which will avoid duplicate ticket creation.
CONSEALINK-3296	The EPIC SER Connector now displays provisioning failures at an attribute level.
CONSEALINK-3308	The ServiceNow Identity Governance Connector now supports "sysparm_query_category" as query parameter.
CONSEALINK-3329	For ServiceNow Identity Governance Connector, "sysparm_fields" are now available to improve performance during aggregation operation
CONSEALINK-3357	The SailPoint Identity Governance Connector now supports configurable option to read deleted events (such as removing group/role) of user's connection from custom table instead of sys_audit_delete table. This will enhance performance of delta aggregation.

Issue ID	Description
CONSEALINK-3367	The Zoom Connector now supports the transfer_whiteboard attribute in the Delete user provisioning policy.
CONSEALINK-3378	The Zoom Connector no longer fails test connection with error 'authType' required.
CONSEALINK-3421	IdentityIQ for Atlassian Server Jira Service Desk now supports Atlassian Jira Service Management (Server) Version 5.2.0
CONSEALINK-3424	The EPIC Connector no more fails with error "TimeOut waiting for connection pool", User can increase the axis connection pool by configuring maxHostConnections parameter in application.
CONSEALINK-3449	The ServiceNow Service Desk Integration Module now populates the Access Request comment on the ServiceNow ticket. Existing ServiceDesk Integration configuration needs to modifythe provisioning task definition to include the comments for Access Request. This feature is automatically included for all new configurations.
CONSEALINK-3455	1) The ServiceNow Identity Governance Connector no longer supports the ServiceNow Rome release. And, 2) The IdentityIQ for ServiceNow Service Desk no longer supports the ServiceNow Rome release.
CONSEALINK-3462	BMC Helix ITSM Service Desk integration now supports OAuth 2.0 authentication.
CONSEALINK-3498	The EPIC Connector InBasket Classifications are no longer included by default in the account schema to avoid performance impact on provisioning operations.
CONSEALINK-3512	The Generic SDIM now supports retrieving the ticket number from the URL if the create ticket response returns the URL instead of the ticket number. The new attribute is 'Process Response Element Expression’ and it should be populated with parsing logic to fetch the ticket number from the response URL.
CONSEALINK-3556	New Service Desk Integration "IdentityIQ for Ivanti Cherwell ITSM Service Desk" is available now.
CONSEALINK-3566	The EPIC Connector user fields "PrimaryManager" and "UsersManagers" are now supported as account attributes.
CONSEALINK-3605	The ServiceNow Connector avoids unnecessary API calls related to entitlements if Customer is interested in only aggregating User data.
CONSEALINK-3656	[SECURITY] For Collaboration bundle, "commons-collections-3.2.2.jar" jar has been removed due to vulnerability with the version. As there were no dependency of it on any of the connectors, instead of upgrading it has been removed.
CONSEALINK-3765	A new out-of-the-box accounts connector for user access governance in Ivanti Cherwell ITSM solution

Issue ID	Description
CONSEALINK-3824	The Zoom connector no longer supports Authentication Type “API Token”.
CONSEALINK-3927	The BMC Helix ITSM Service Desk Integration Module now supports version 22.1.
CONUMSHIAN-4126	The SAP GRC Connector now supports handling XML special characters ("'&<>) during user provisioning operations.
CONUMSHIAN-5107	The Amazon Web Services (AWS) Connector now supports 'AWS GovCloud (US)' Regions.
CONUMSHIAN-5129	The SAP Connector has been enhanced to provide a more relevant exception in case of certain erroneous situations.
CONUMSHIAN-5179	The SAP GRC Connector is re-designed to use an SAP-certified function module for enhanced security and performance. The use of RFC_READ_TABLE has been made limited according to SAP recommendations.
CONUMSHIAN-5232	The SAP GRC Connector now enhanced to support Account Partitioning for SAP Basis version 751 and later.
CONUMSHIAN-5284	The Oracle ERP Cloud Connector now enhanced to support aggregation of data access information (security context and security context values) even when not assigned to a role.
CONUMSHIAN-5303	The SAP Direct Connector is re-designed to use an SAP-certified function module for enhanced security and performance. The use of RFC_READ_TABLE has been made limited according to SAP recommendations.
CONUMSHIAN-5379	SAP Business Suite (ERP) Integration is certified with 'SAP HANA S/4 2022' for maintaining SailPoint Connectivity’s commitment to business continuity, customer support, and brand value.
CONUMSHIAN-5405	The new Oracle Enterprise Performance Management (EPM) Cloud governance Connector provides the capability for managing user accounts, predefined roles, application roles and groups. The integration supports EPM Cloud Services for Financial Consolidation and Close (FCCS), Account Reconciliation (AR), Planning, Narrative Reporting (NR).
CONUMSHIAN-5586	The new SAP Concur Connector provides Identity Governance on Expense management services provided by Concur. The integration supports enforcing policies and permissions for granting and revoking access to systems and data based on user identities, roles, and associated groups for Expense, Request, Invoice, and Reporting.
CONUMSHIAN-5688	The new Oracle Enterprise Performance Management (EPM) Cloud Governance Connector provides the capability for managing user accounts, and reading and associating of Predefined roles, application roles and groups. The integration supports EPM Cloud Services for Planning, Financial Consolidation and Close Service(FCCS), Account Reconciliation (ARCS), & Narrative

Issue ID	Description
	Reporting (NR).
CONUMSHIAN-5691	The new Oracle Enterprise Performance Management (EPM) Cloud Governance Connector provides the capability for managing user accounts, and reading and associating of Predefined roles, application roles and groups. The integration supports EPM Cloud Services for Planning, Financial Consolidation and Close Service(FCCS), Account Reconciliation (ARCS), & Narrative Reporting (NR).
CONUMSHIAN-5695	The new Oracle Enterprise Performance Management (EPM) Cloud Governance Connector provides the capability for managing user accounts, and reading and associating of Predefined roles, application roles and groups. The integration supports EPM Cloud Services for Planning, Financial Consolidation and Close Service(FCCS), Account Reconciliation (ARCS), & Narrative Reporting (NR).
CONUMSHIAN-5724	The new Oracle Enterprise Performance Management (EPM) Cloud Governance Connector provides the capability for managing user accounts, and reading and associating of Predefined roles, application roles and groups. The integration supports EPM Cloud Services for Planning, Financial Consolidation and Close Service(FCCS), Account Reconciliation (ARCS), & Narrative Reporting (NR).
CONUMSHIAN-5747	The SAP Concur Connector has been enhanced to support role assignment to the user during the modify operation.
CONUMSHIAN-5756	The SAP Concur Connector now supports date provisioning and retrieval in a fixed format, also fixing an attribute sync problem.
CONUMSHIAN-5769	The SAP Concur Connector now handles the proper SCIM mapping of attributes required for provisioning use cases.
CONUMSHIAN-5836	We have added additional settings on the SAP GRC Source Configuration UI for Access Request Type Mapping, Provisioning Actions for Roles and System sections for ease of configuration and maintenance
CONUMSHIAN-5852	SailPoint's Integration for the SAP Fieldglass Vendor Management System offers governance capabilities for contingent workers. It offers seamless governance of external users management for joiners, movers, leaver workflows, and separation of duty (SOD) checks based on user roles, attributes, and entitlements.
CONUMSHIAN-5974	SailPoint SAP GRC Integration now supports Access Management Requests that are configured for Auto-Approval in the SAP GRC system.
CONUMSHIAN-5990	The Oracle PeopleSoft HCM Connector is now supports PeopleTools version 8.60.05
CONVASHI-1431	The Web Services Connector will now work with optional namespace prefix for XPATH attribute mappings.