SailPoint® | IdentityIQ®

Release Notes

Version: 8.3

Revised: April 2022

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices

Copyright © 2022 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. https://www.sailpoint.com/patents

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce’s Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government’s Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Contents

IdentityIQ Release Notes

These are the release notes for SailPoint IdentityIQ, 8.3

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 8.3 Updates and Enhancements

IdentityIQ 8.3 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 8.3 Feature Updates

IdentityIQ 8.3 introduces the following new features or enhancements.

Feature/Enhancement	Description
Notifications in Microsoft Teams	IdentityIQ's Microsoft Teams Notifications feature allows notifications from IdentityIQ to be delivered directly to users as notifications in their Microsoft Teams environment. Any IdentityIQ notification for certifications, access requests, and access approvals can be sent as a Microsoft Teams notification, and can include a link to the relevant area or action within IdentityIQ. With SAML-based single sign-on enabled, authenticated Microsoft Teams users can seamlessly access IdentityIQ from links in the notifications, allowing them to take actions in IdentityIQ without a separate login to IdentityIQ. This feature allows critical requests or notifications to be acted upon promptly by surfacing this information to users in the environment they are already in, Microsoft Teams. This streamlines communication and allow for more timely Identity Governance.
Role Management & Analysis	IdentityIQ now can more efficiently track the relationship of an organization’s roles (as defined in IdentityIQ) to the entitlements and permissions in the Entitlement Catalog, by providing a new database table to store the associations between roles and entitlements.

Feature/Enhancement	Description
	This allows roles to be filtered based on details of the entitlements included directly in their profiles, or in the profiles of other roles with a required/permitted/inherited relationship. New filters have been added in the following locations • **Role Management > Role Search**: filter roles based on the state of the profile (are applications/entitlements valid), entitlement/permission details, relationship of entitlement to role (direct/indirect), entitlement/permission application, attribute, and attribute value • **Advanced Analytics > Role Search**: similar to Role Search above • **LCM Manage User Access**: filter requestable roles based on entitlement details Certification owners can pre-filter roles to include in **Targeted Certifications**, based on the details of their entitlements or permissions A new **Associated Roles** tab for entitlements or permissions in the Entitlement Catalog shows the roles associated with the access A new **Roles By Entitlement** report provides details about roles based on entitlement parameters, with results including the nature of relationship of the role to the queried entitlement The **Role Members Report** has been updated to include these entitlement parameters .
Flagging Elevated Access in Roles and Entitlements	This feature lets you classify roles and entitlements as allowing Elevated Access. When a role or entitlement has the Elevated Access designation, a badge appears on the item in many user-facing areas of IdentityIQ, such as Manage Access, Access Reviews, the Identity Warehouse, and the Entitlement Catalog. Classifying a role or entitlement as allowing elevated access provides clear visibility to users when they request, certify, or approve the role or entitlement. This helps ensure that these items are treated with appropriate care. A property on these items makes it possible to include them in reports, to facilitate auditing and to help identify high risk areas. Audit activities can focus on this access by leveraging these reports. Workflows can also be built using the Elevated Access property. The approval process for an Elevated Access item can be customized via a workflow, to ensure that the Elevated Access item is handled in a manner consistent with its importance.
Active Directory Native Move/Rename Support	In many places in IdentityIQ, the default identifier for Active Directory accounts and groups is Distinguished Name (DN). Some native changes, such as when an account or group is moved within the Active Directory OU or when a person’s name changes, result in a change to the DN. In previous versions of IdentityIQ, this could result in additional objects being created on aggregation.

Feature/Enhancement	Description
	Beginning with version 8.3, IdentityIQ will detect when an account or group object's DN has been changed on Active Directory. The existing account or group object will be updated, and the change will be propagated to areas where the DN is referenced in the IdentityIQ object model.
AI Recommendations for Roles	IdentityIQ users can now leverage AI Services to gain deeper insights and recommendations for access request approvals and access reviews for roles. These new AI features build on the integration with AI Services introduced in IdentityIQ version 8.0, which provided AI recommendations for Access Request Approvals and Access Reviews for entitlements.
SAML Authentication for e-Signatures	With SAML-based SSO enabled for e-Signatures, the user performing the electronic signature is routed to your SAML provider for authentication, then seamlessly returned to the IdentityIQ UI to complete the signature. This provides increased security when users e-sign critical requests or certifications, and can be used to expand the authentication methods, such as smart cards or biometrics, that can be used in electronic signatures.
OAuth 2.0 Authentication for Email	To keep your IdentityIQ environment current, IdentityIQ now supports the OAuth2 authentication protocol for sending email notification via HTTP/HTTPS. This option is recommended for use with Microsoft Office 365, as an alternative to the SMTP/Basic method which is being deprecated by Microsoft.

Important Upgrade Considerations

IdentityIQ 8.3 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

The following libraries were upgraded to enhance quality and security within IdentityIQ.

- aspectjrt/aspectjtools 1.9.6
- bouncy castle 1.6.8
- Codec (Part of Commons) 1.15
- FileUpload (Part of Commons) 1.4
- Lang (Part of Commons) 3
- Net (Part of Commons) 3.8
- Validator (Part of Commons) 1.7
- Guice 5.0.1 servlet 4.2.3
- Jersey 2.34

- junit 4.13.1
- mimepull 1.9.13
- Java JSON Web Token (jjwt) 0.11.2
- jackson 2.13.3
- twillio 8.14.0
- sshj0.31.0
- asn-one 0.5.0
- xmlschema 2.2.5
- xmlsec 2.2.2
- apache-ant 1.10.10
- easymock 4.2
- objenesis 3.2
- jline 3.20.0
- ngdbc 2.8.12
- testng (jcommander) 7.1
- lucene 8.8.2
- primefaces 8.0.12 (paid)
- jquery 3.5.1
- json 20210307

Connector Upgrade Considerations

- The Cloud Gateway version must match the IdentityIQ server version, including the major release and patch versions. After upgrade to 8.3, all operations for applications using Cloud Gateway as proxy will fail if there is mismatch between the IdentityIQ version and the Cloud Gateway version.
- The IQService version must match the IdentityIQ server version, including the major release and patch versions. After upgrade to 8.3, there could be undesired behavior for operations that require IQService if there is mismatch between the IdentityIQ version and the IQService version. When one is upgraded, the other must be upgraded so that the version and patch levels match. For more information on upgrading the IQService, see the IdentityIQ **Installation Guide**'s upgrading chapter.
- The Connector Gateway version must match the IdentityIQ server version, including the major release and patch versions. After upgrade to 8.3, operations for applications using Connector Gateway may fail if there is mismatch between the IdentityIQ version and the Connector Gateway version not compatible with it. For more details on this release of Connector Gateway, see Mainframe Connectors Downloads.

Global Settings for JavaMail Connection Timeout Settings

There are two new UI configuration options when setting up the **SMTP Email** or the **Redirect to Email** notification types.

- **Connection Timeout** - Email socket connection timeout value in milliseconds.
- **Read Timeout** - Email socket read timeout value in milliseconds.

These values are saved in the global system configuration under the following Map value:

```
<entry key="smtp_sessionProperties">

<value>

<Map>

<entry key="mail.smtp.connectiontimeout" value="10000"/>

<entry key="mail.smtp.timeout" value="10000"/>

</Map>

</value>

</entry>
```

These properties are passed in as the session properties to JavaMail API used to send the email notifications. If there are session properties defined in email template objects that are used to send the email, then those will take precedence over these properties.

Removal of HTTP Basic Authentication

Security: HTTP 401 result codes can now be customized within the system configuration to return different codes, change or remove the WWW-Authenticate header, and message.

This allows the outbound filter to replace any 401 codes with a 408:

```
<entry key="httpUnauthorizedResponseCode">

<value>

<Integer>408</Integer>

</value>

</entry>
```

This will remove the WWW-Authenticate header, and any other value than stripHeader will set WWW-Authenticate to that value:

```
<entry key="httpUnauthorizedResponseHeader" value="stripHeader"/>
```

This allows a customizable message to be returned to the browser with the error:

```
<entry key="httpUnauthorizedResponseMessage" value="custom_message_here"/>
```

Application XML Changes Visible After Application Server Restart

This release contains a fix for the configuration of the Hibernate L2 cache. In the 8.2 GA release, the `ehcache jar` files were updated to the 3.8.1 version. These updated jar files now use the jcache (JSR-107) specification to interface with Hibernate. This change in the interface with Hibernate and the L2 cache caused the ehcache configuration using the `ehcache.xml` file to no longer work. This caused the objects being stored in the L2 cache to have an unlimited TTL, and objects changed on one server would not always be reflected on other IdentityIQ UI and Task servers.

This fix includes an update to `hibernate.cfg.xml` file to specify the `ehcache.xml` file to use for the ehcache configuration. Also, the `ehcache.xml` file was updated to use the JSR-107 specification format. All default values that were in the file before still remain the same, but the format of the file has changed. If any customizations have been made to either of these files, then care should be taken when upgrading.

Disable BeanShell Editing in Delegated Admin Screens

Security: The ability to edit inline scripts in Identity IQ now requires either the **SystemAdministrator** capabilityor the new **EditScripts SPRight**. The EditScripts SPRight is not in any capabilities by default. This means there will be users who were able to edit scripts in the past that can no longer edit them until they have been assigned the new EditScripts SPRight.

It is recommended that the EditScripts SPRight is given out in a controlled manner to trusted users because having the ability to write scripts is a potential security risk.

Restore escapeHTML to spTools

The escapeHTML utility method has been restored to the Velocity spTools.

Role Members Report Filtering Role Type

The Role Members Report can now include roles with indirect relationships when filtering by application. Previously only direct relationships were included. This change adds a way to filter roles based on profile relationship to the role. New filtering options in the report setup allow a greater degree of granularity for entitlements/permissions, and also provide the option to return any roles that are directly or indirectly related to the applications specified in the filter.

Role-Entitlement Associations Task is Called During Upgrade

The Role-Entitlement Associations is run during an upgrade to version 8.3. See IdentityIQ 8.3 Feature Updates for more information about related enhancements to Role Management & Analysis.

Updated sailpoint.tools.Base64

The Java class `sailpoint.tools.Base64` is now deprecated and will eventually be removed. Instead, use `sailpoint.tools.Base64Util` or `java.util.Base64`.

JDK 17 Server Configuration

If you are using JDK 17, add the following Java system property. Consult your application server documentation for more information.

```
--add-exports=java.naming/com.sun.jndi.ldap=ALL-UNNAMED
```

Configuration Changes Not Being Captured in 'Login Config Changed' Audit Event

In the Attributes of an Audit Event Details value for samCorrelationRule now shows the rule name.

Example:

- Old format: `Screen Shot 2022-02-25 at 10.24.27 AM.png shows: [mailto:sailpoint.object.Rule@6876f93c[id=ac]sailpoint.object.Rule@6876f93c [id=ac ...`
- New format: `Screen Shot 2022-02-28 at 3.09.31 PM.png shows it using the rule name instead of the object. ex: IdentityNowSAML`

Electronic Signature Should Use SAML Authentication when Configured

Prior to this version, Electronic Signatures only used Basic Authentication, that is, a username and password, regardless of IdentityIQ's login configuration. This meant that if a user used SAML to authenticate to IdentityIQ, they might not have the Basic Authentication login information necessary for performing Electronic Signatures.

In this version of IdentityIQ, if the login configuration uses SAML, then by default SAML authentication will be used for Electronic Signatures. For SAML authentication during an Electronic Signature, the customer's identity provider is contacted, and a new authentication is requested. This does not affect the IdentityIQ session; the authentication is a new authentication into the identity provider.

This new default can be changed to always using Basic Authentication for Electronic Signatures, regardless of the login configuration, by adding this entry to the IdentityIQ System Configuration via the Debug pages:

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

New REST Call Created for User Access Token

This applies to IIQ and SCIM API calls.

Any API call that uses an Authorization header must use the proper auth type format. If formats are mixed, headers will be considered invalid and not processed. The token provided with the authorization header may be encrypted. When the token is decrypted, it must match the proper format for the authorization type.

Basic auth headers must have the following format:

```
username:password
```

Bearer auth headers must have the following format:

```
clientID.token
```

Note that Basic uses the colon (:) as the separator and Bearer uses the period (.) as the separator.

Upgrade Considerations for Plugins Using REST Service

If you upgrade a plugin with a new version and that plugin has a REST service, it will only be reloaded on other servers by the PluginSyncService if the Plugin `manifest.xml` specifies a ServiceExecutor. Having a RestResource defined alone is not sufficient. Edit the plugin's manifest.xml to add a `<entry key="serviceExecutors">` value. This entry key must be present regardless of whether you use a serviceExecutor; if that is the case the entry key can have a blank reference (that is, reference no class).

Supported Platforms

Operating Systems

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

> **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 8.5
- SuSe Linux 15

Application Servers

- Apache Tomcat 9.0
- Oracle WebLogic 14c and 12cR2
- IBM WebSphere 9.0
- JBoss Enterprise 7.4 and 7.3
- IBM WebSphere Liberty 21.0 and 20.0

Databases (On Site)

- IBM DB2 11.5
- MySQL 5.7 and 8.0
- MS SQL Server 2019 and 2017
- Oracle 19c

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 1.8 (8), 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..

> JDK 8 is supported as needed by the specific application servers listed above.

Browsers

- Google Chrome Latest Version
- Microsoft Edge Latest Version
- Safari 15
- Firefox Latest Version

Mobile User Interface OS/Browser Support

- Android with Chrome 12
- iOS with Safari 15.2

Languages

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

- Swedish
- Traditional Chinese
- Turkish

Connectors and Integration Modules Enhancements

IdentityIQ 8.3 provides various enhancements in the following connectors and integration modules.

New Connectors

IdentityIQ 8.3 delivers new, out-of-the-box connectors for the following enterprise applications, which simplifies the connectivity of these systems.

New Connectors	Description
MEDITECH	SailPoint's MEDITECH integration provides deep integration for healthcare enterprises using MEDITECH Expanse, to govern identities across its businesses. The integration involves the management of Accounts and Roles, thus powering healthcare enterprises to make informed decisions.See the Integrating SailPoint with Meditech guide for more information. **Benefits**:Connecting SailPoint to your MEDITECH system allows you to manage users as accounts and roles as account-groups.
BMC Helix ITSM Service Desk	The BMC Helix ITSM Service Desk Integration module is designed to provide the service desk experience in SailPoint's platform. See the Integrating SailPoint with BMC Helix ITSM Service Desk guide for more information. **Benefits**: Users can raise and track service desk tickets to their logical closure from the platform itself.

Amazon Web Services

Description	Benefit
Amazon Web Services connector now supports aggregation of tags on IAM entities.	The Amazon Web Services connector now also brings in tags for establishing a link between cloud applications and their underlying resources. It will also aid in identifying additional information about a tagged resources for example, CostCenter, Environment, Project, Owners or Purpose.
Amazon Web Services connector now supports IAM Role authentication method to connect with Amazon Web Services native system.	Extending the connector functionality to make it more secure and flexible by supporting IAM Roles Authentication

Azure Active Directory

Description	Benefit
Azure Active Directory Connector now supports managing Channels in Microsoft Teams.	Microsoft Teams Channels are widely used to segregate and manage different teams and groups. Our Azure AD connector is now extended for Microsoft Teams 'channels' to easily manage them directly though the connector.
The Azure Active Directory connector has been enhanced to manage Distribution List and Mail Enabled Security groups through IQService.	Building back connector support for Mail Enabled Security Groups and Distribution Lists in Azure AD connector for supporting 360-degree use cases which got impacted due to Microsoft API support.
The Azure Active Directory Connector now supports Privileged Identity Management (PIM). This enables to limit standing administrator access and review privileged access for excessive or unnecessary access permissions on privileged resources.	The Azure Active directory connector has been enhanced to leverage Azure's 'Privileged Identity Management' features, so that you can provide time-based and approval-based role activation, and mitigate the risks of excessive, unnecessary, or misused access permissions on privileged resources.

Cloud Gateway

Description	Benefit
The Cloud Gateway connector now supports two-way SSL authentication, making the connection more secure	Enhancing Cloud Gateway connector security for client and server to authenticate and validate each others identities.
To ensure seamless integration, we have enabled Cloud Gateway version detection and mandated a match with IdentityIQ version for all applications using Cloud Gateway as proxy.	Seamless integration between Cloud Gateway apps and IdentityIQ. This will remove ambiguities for causes of errors and issues when Cloud Gateway is used as proxy

Dropbox

Description	Benefit
Dropbox connector now supports non-expiry access tokens as Dropbox has deprecated the support for long-lived access tokens	Enhancement complies with tokens validity as recommended by Dropbox.

Epic Healthcare

Description	Benefit
The Epic connector now supports the ability to update "ContactComment" based on the value of the boolean flag "isUpdateContactComment".	Admins can choose to update "Contact Comments" based on flags
The Epic connector now supports the Epic August 2021 release.	Verification ensures business continuity for the updates release versions

Description	Benefit
Epic connector is now verified to support Epic May 2020 for IdentityIQ and IdentityNow.	Verification ensures business continuity for the updates release versions

G Suite (Google Apps)

Description	Benefit
The G Suite Connector has been enhanced to support proxy (HTTP, HTTPS) configurations.	Supporting proxy configurations to make the connector more flexible as well as secure.
The Google Workspace (G Suite) connector now supports filters to aggregate only desired accounts during account aggregation.	Adding filtering capabilities on Google connector to enable selective aggregation and also save on time and costs.
The G Suite connector is optimised for performance improvements during delta aggregation.	Performance improvisation and stability to save on time and efforts.

IBM DB2

Description	Benefit
IBM DB2 connector now supports version 11.5	Concurrency with the latest version of software ensures business continuity for customers using the updated version of IBM DB2.

IBM Lotus Domino

Description	Benefit
The HCL (Lotus) Domino connector now supports HCL Domino version 11.	The HCL Domino connector is now certified for HCL Domino version 11 to keep up with customer and market demands.
The HCL (Lotus) Domino connector now supports HCL Domino version 12.	Our HCL Domino connector is now certified with HCL Domino version 12 to keep up with customer and market demands.

Linux

Description	Benefit
The Linux Connector now supports Red Hat Enterprise Linux versions 7.8, 7.9, and 8.3.	The Linux connector is now certified with additional versions to increase confidence and keep up with supported features, customer and market demands.

Microsoft SharePoint Online

Description	Benefit
The SharePoint Online Connector has been enhanced to support proxy (HTTP, HTTPS) configurations.	Supporting proxy configurations to make the connector more flexible as well as secure.

Microsoft SQL Server

Description	Benefit
Microsoft SQL Server Connector now supports Microsoft SQL Server installed on Linux.	The enhancement provides for the scalability of the connector on Linux platform .

NetSuite

Description	Benefit
The NetSuite connector now supports Aggregation and Provisioning for additional attributes.	Support for additional attributes for aggregation and provisioning provides fine-grained governance capabilities to customers.

Okta

Description	Benefit
Okta Connector now supports managing “App Targets and App Instance Targets” for APP_ADMIN (Application Administrator) Role and "Group Targets" for HELP_DESK_ADMIN (Help Desk Administrator) role.	Admin Role Entitlements visibility provides transparency into what entitlements have been assigned to Admins.

Open LDAP

Description	Benefit
The OpenLDAP connector now supports OpenLDAP versions 2.5 and 2.6.	The OpenLDAP connector is now certified with versions 2.5 and 2.6 to keep up with supported features, customer and market demands.

Oracle Fusion HCM

Description	Benefit
Oracle Fusion HCM Connector now supports additional attributes and "Assignment Status Type ID".	The enhancement provides more information for the customer to exercise deeper governance
Oracle Fusion HCM Connector will now support migration of the existing /emp application or source to /workers API.	Oracle recommended API "Workers API" migration can now be achieved, allowing customers for seamless change.
The Oracle Fusion HCM Connector can now aggregate "ASSIGNMENT_MANAGER_NUMBER" attribute.	With the inclusion of "Assignment Manager Number" attribute, correlating to retrieve ManagerID is now an option.
The Oracle HCM Fusion Connector pulls the latest primary workrelationship of a worker when an account aggregation is performed.	Aggregation data is up-to-date.

PeopleSoft HRMS

Description	Benefit
PeopleSoft HRMS connector now supports PeopleTools version 8.59	Concurrency with the latest version of software ensures business continuity for customers using the updated version of PeopleTools.

RACF

Description	Benefit
RACF Connector now supports managing MFA-related attributes for RACF systems configured for MFA.	MFA will provide better security for customers using RACF.

RemedyForce

Description	Benefit
The RemedyForce connector now supports BMC Helix RemedyForce platform.	RemedyForce connector is now certified to be used with BMC Helix RemedyForce platform(on-cloud), making it easier for new and existing customers to opt for cloud-based BMC solutions.

RSA Authentication Manager

Description	Benefit
RSA Connector now supports partitioning aggregation.	Business Value RSA Application config page now allows users to input partitioning size to give them flexibility on performance, and cost optimisations.

SAP HANA

Description	Benefit
SAP HANA connector is now verified for version SAP HANA 2.0 SPS5	Verification ensures business continuity for customers using the SAP HANA connector with the new version of SAP HANA.

SAP Governance Application Module - SAP GRC

Description	Benefit
SAP GRC Connector now supports configurable access request type and access request priority during provisioning. The connector also supports account aggregation and provisioning of additional attributes.	The enhancement provides flexibility to admins for configuring access request type and its priority during provisioning along with support for additional attributes for fine-grain governance .

Identity Governance Connector for ServiceNow

Description	Benefit
The ServiceNow Connector now provides an option to 'Unlock' an account while performing 'Enable' operation.	The ServiceNow Connector can unlock an account now while enabling it for providing seamless user experience.
ServiceNow Connector now supports aggregation of inherited roles associated with an account.	The connector is enhanced to provide better visibility on inherited roles and better governance on Role-Based Access Control.
ServiceNow Connector now supports aggregation and provisioning of dot walking fields on reference tables.	The ServiceNow Connector now allows ease of use and better experience to model extended attributes within the ServiceNow environment.

Salesforce

Description	Benefit
The Salesforce Connector now supports 'Collaboration Group' as group object.	Extending the Salesforce connector to manage ‘Collaboration Groups’. These are widely used as public, private, or unlisted Chatter groups to collaborate with specific people in an organisation.

SCIM 2.0

Description	Benefit
The SCIM 2.0 connector now extend support for non-compliant SCIM 2.0 servers.	Making our SCIM 2.0 connector more resilient and flexible, the connector is now able to overcome challenges where SCIM servers are implemented in a non-standard or incomplete manner. This would enable the connector to be used across a broader set of applications.
The SCIM 2.0 connector now supports providing different page size for account and group aggregation to optimise API calls.	Connector optimization for flexible configuration and better performance.

Siebel

Description	Benefit
Siebel Connector now supports Siebel server version 21.12.0.0	Concurrency with the latest Siebel version ensures business continuity for customers using the updated versions.

Slack

Description	Benefit
Slack Connector now supports the "Slack Enterprise Grid" version.	Verification with Slack's Enterprise Grid version will ensure business continuity and support for features for the Enterprise Grid.

SuccessFactors

Description	Benefit
SuccessFactors connector now supports OAuth 2.0 authentication type with SFAPIs.	OAuth2.0 provides for better security for authentication

Unix

Description	Benefit
Unix Connectors(AIX, Linux, Solaris) now provide SFTP support during aggregation.	The Linux and Unix connectors provide better security and coverage for the overall user base with SFTP support.

Web Services

Description	Benefit
The Web Service connector now supports "skipEncodingDecodingUrl" application config in order to skip connector level url encoding and decoding for all endpoints.	Allows the customer to pass URL according to their need, and the connector will not change it.
The Web Services connector now supports quick configuration of operation endpoints using cURL command.	Onboarding a new application using the Web Services connector is now easier with real time feedback. Customers can now run cURL commands from within the UI while setting up any application.
The Web Services connector now supports delta aggregation.	Delta aggregation support for performance improvements and time-cost savings.

Workday

Description	Benefit
The Workday connector now supports aggregation and updates of Custom IDs.	The Workday connector is extended to support 'custom ids' for managing Employees and Contract Contingent Workers.
The Workday Connector now supports OAuth 2.0 authentication with 'refresh token' grant type .	The Workday and Workday Accounts connector now offers easier to implement and stronger authentication mechanism using OAuth2
The Workday connector now supports Workday API version 37.0	Our connector is now certified with latest Workday APIs ver. 37.0 to keep up with customer and market demands
Workday Connector supports the aggregation of rescinded past hires records with a specified offset limit.	Organizations can maintain rescinded hire records for a period of time after the user's start date, in order to handle reprocessing failures, post termination process clean-ups, and exports.
The Workday Connector no longer aggregates workers beyond the offset specified in Past_Terminated_Offset attribute of the application.	Past terminated workers will not be fetched if they are not within the provided "Past_Termination_Offset" period.

Description	Benefit
The Workday connector now returns a complete ResourceObject for a future dated account when an account aggregation is performed.	A complete ResourceObject for the future worker is correctly fetched during aggregation.
The Workday Connector no longer fails with a NullPointerException when aggregating accounts from an application having an empty API version.	Aggregation is successful and the connector gets a default schema list.
The Workday Connector no longer uses Axis2 libraries for fetching responses.	The upgraded and new Workday applications are independent of commons-httpclient 3rd party jar. For using Axis2 libraries or in case of any such issue, set "useSdkFramework" entry key to "false" in the application XML in the Debug page] as follows `<entry key="useSdkFramework" value="false"/>`
Workday Connector now supports updating Custom ID (Other ID) having a blank value in the Workday system.	Making the connector more flexible on custom id attributes to accommodate different use case scenarios.

Workday Accounts

Description	Benefit
The Workday Accounts Connector now supports OAuth 2.0 authentication with 'refresh token' grant type .	The Workday and Workday Accounts connector now offers easier to implement and stronger authentication mechanism using OAuth2
The Workday Accounts connector has been optimized for lightweight test connections for faster operations.	Connector optimization for performance improvements and to save on time and costs

Connectivity Supported Platform and Language Updates

Connector/Component	New Platform Version
SailPoint Identity Governance Connector for ServiceNow	The SailPoint Identity Governance Connector for ServiceNow now supports the ServiceNow Rome and San Diego releases.
ServiceNow Service Desk Integration Module	The SailPoint for Service Desk now supports the ServiceNow Rome and San Diego releases.
SAP HANA Connector	Supports SAP HANA 2.0 SPS5
HCL (Lotus) Domino Connector	Supports HCL Domino version 12 and version 11
EPIC Connector	Supports Epic August 2021 and Epic May 2020
Linux Connector	• Supports Red Hat Enterprise Linux versions 7.8, 7.9 and 8.3 • Supports Federal Information Processing Standard (FIPS) for Red Hat Enterprise Linux version 8.3

Connector/Component	New Platform Version
Microsoft SQL Server Connector	Supports Windows authentication when either of the platforms (IdentityIQ / MSSQL Server) are on different OS environments
MicroFocus Service Manager Integration Module	Supports Service Desk Integration with Micro Focus Service Manager version 9.7
OpenLDAP Connector	Supports OpenLDAP version 2.6 and 2.5
RemedyForce Connector	Supports BMC Helix RemedyForce platform
Oracle Connector	Supports Oracle version 21c
IBM DB2 Connector	Supports version 11.5
PeopleSoft HRMS Connector	Supports peopletool version 8.59
Siebel Connector	Supports Siebel server version 21.12.0.0
BMC Remedy Connector	Supports BMC Helix Platform 20.02

Connectivity Dropped Platform Support

Connector/Integration Module	Dropped Platforms
Linux Connector	Linux Connector no longer supports Red Hat Enterprise Linux versions 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 7.0, 6.9, 6.8, and 6.7.
SailPoint Identity Governance Connector for ServiceNow	The SailPoint Identity Governance Connector for ServiceNow no longer supports the ServiceNow New York release.
ServiceNow Service Desk Integration Module	The IdentityIQ for ServiceNow Service Desk no longer supports the ServiceNow New York release

Dropped/Deprecated Connector Support

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

- Yammer Connector will no longer be available as an application type

Resolved Issues

Issue ID	Description

IIQSR-642	The following warnings may appear in the application server log when running with JDK 11, and can be safely ignored:
	`WARNING: An illegal reflective access operation has occurred`
	`WARNING: Illegal reflective access by com.google.inject.internal.cglib.core.$ReflectUtils$1 (file:/<app_server_path>/war/WEB-INF/lib/guice-4.2.3.jar) to method java.lang.ClassLoader.defineClass(java.lang.String,byte[],int,int,java.security.ProtectionDomain)`
	`WARNING: Please consider reporting this to the maintainers of com.google.inject.internal.cglib.core.$ReflectUtils$1`
	`WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations`
	`WARNING: All illegal access operations will be denied in a future release`

IIQSR-636	Unless overridden with entries in the system configuration, status 401 responses will be returned from the REST servlet.
IIQSR-623	When the browser language is set to Canadian French, all UI pages now load properly.
IIQSR-599	Expired passwords from pass-through applications will prompt the user to provide a new password.
IIQSR-597	Attribute assignment information is no longer removed from an Identity when a sunset request is made for an entitlement.
IIQSR-595	The password provided on the Plugin Configuration page is now stored instead of a dummy password (tsewraf).
IIQSR-594	An identity with no capabilities can now view the classifications tab in the entitlement details dialog for delegation or challenge work items.
IIQSR-591	Access Reviews are correctly reassigned to the new owner via the Rapid Setup Leaver workflow.
IIQSR-590	Rapid Setup Leaver filters consisting of grouped filters are now properly validated.
IIQSR-576	When reassigning artifacts in Rapid Setup Leaver, the forwarding chain will be taken into consideration when determining the new owner.

Issue ID	Description
IIQSR-575	Advanced Search results can now be exported to PDF or CSV when a "Disabled" field is included in the fields to display.
IIQSR-574	A new work item is now created when policy violation status is changed from 'Completed' to 'Open'.
IIQSR-573	When saving an Advanced Analytics search, only a reference to the owning identity is now stored in the SearchReportOwner entry of the report.
IIQSR-572	An error is no longer thrown when a policy checks against an empty display name while changing a password.
IIQSR-570	Exporting a Rapid Setup configuration will now filter out IDs within the identity selector section and will add them back during an import.
IIQSR-566	Email Template SessionProperties can now be set globally in the SystemConfiguration for all templates.
IIQSR-565	Form validation is now skipped when the Cancel button is selected.
IIQSR-563	The Last Certification and Last Certification Date are now populated for a targeted certification in the Identity Entitlement Details Report.
IIQSR-559	"Extended Rules" under the Termination Options no longer disappears from the Application Definition UI.
IIQSR-558	Corrected a race condition which had allowed high concurrency multi-node environments to execute the same task simultaneously on different hosts.
IIQSR-557	Rapid Setup Leaver reassignment notifications are now sent to the forwarding user when configured accordingly.
IIQSR-556	An assigned scope is now saved successfully for a Target Certification.
IIQSR-555	The OpenPDF library was upgraded to 1.3.24, which allows the Account Attributes Live Report to execute in a reasonable amount of time and without errors.
IIQSR-554	Rule library references in scripts defined by //#include now work correctly.
IIQSR-552	Changes introduced in 8.2 GA via IIQSR-438 have been reverted because the EmailTemplate-FrameworkAccessReviewReminder email template is used for both manual certification reminders and automated access request reminders. The template to support access request reminders has been restored.
IIQSR-551	For manual certification reminders, a new template named “EmailTemplate-Framework-CertManualReminder” has been introduced instead of using the template intended for automated access reminders.
IIQSR-549	Challenge and delegation work items now respect the "Show Classifications" setting in the certification definition.

Issue ID	Description
IIQSR-544	ObjectUtil methods were updated to prevent using strings longer than proper id length for searches by id field. This was particularly affecting DB2 databases, such as in a provisioning plan when a rule name has more than 32 characters, or when a role name has more than 32 characters.
IIQSR-543	A policy violation required comment now only needs to be entered once when the policy violation is being revoked.
IIQSR-542	The AuditLog source for SessionTimeout events is now displayed correctly instead of "unknown".
IIQSR-539	[SECURITY] 401 result codes can be customized within the system configuration to return different codes, change or remove the WWW-Authenticate header, and message.
IIQSR-535	From Adv Analytics, Entitlement Classifications are exported to PDF or CSV
IIQSR-533	Propagating role changes that include entitlements from logical / composite applications no longer results in missed-entitlement removals.
IIQSR-532	A minor change to the Lifecycle Manager configuration does not break the Edit Identity and Self Registration forms
IIQSR-528	Members of a workgroup are able to receive email notifications now.
IIQSR-527	The group argument and its description in the Field Value Template rule has been corrected to be an AccountGroupDTO and not a ManagedAttribute.
IIQSR-526	Native IdentityIQ authentication is still performed in the event the credential source is unavailable when using credential cycling.
IIQSR-524	The Hibernate L2 cache (ehcache) is now configured correctly according to the ehcache.xml config file and honors the time to live settings defined there.
IIQSR-523	Removing a permitted role from a role definition no longer results in already-permitted-assigned roles from becoming re-provisioned to identities that had the permitted-assigned role during refresh.
IIQSR-522	Classification information for Roles from Advanced Analytics are exported correctly. After export to csv and pdf the export file has both the classification header and the data
IIQSR-521	Browser session timeout is no longer followed by a basic authentication login prompt.
IIQSR-520	ObjectUtil methods were updated to prevent using strings longer than proper id length for searches by id field. This was particularly affecting DB2 databases, such as in a provisioning plan when a rule name has more than 32 characters, or when a role name has more than 32 characters.

Issue ID	Description
IIQSR-515	Requesting two or more new entitlements with sunrise and sunset dates for a user without an account on the application now successfully removes all entitlements on their sunset date.
IIQSR-514	The AuditLog source for certain types of provisioning operations is now displayed correctly instead of "unknown".
IIQSR-512	Manage Accounts refresh now takes into account any filters configured on the application in Rapid Setup.
IIQSR-511	Password history is now also updated during account creates rather than just account modifications.
IIQSR-510	LCM requests that result in new accounts after retries are no longer marked as failed and now contain the correct native identity if set during provisioning.
IIQSR-507	"Interrupted attempting lock" errors no longer occur when using a JBoss JNDI Datasource for the IdentityIQ database connection.
IIQSR-499	The "Sort by" button now works as expected on the Work Items page.
IIQSR-497	When Advanced Search is finished or reset on the Work Item Archive page, the page numbering is now also reset properly for subsequent searches.
IIQSR-496	When Advanced Search is reset on the Work Item Archive page, the 'Created After' and 'Created Before' date fields are now reset and enabled instead of being left from the previous action on Advanced Search.
IIQSR-495	After clearing the Start Date and End Date fields on the Task Results tab, a new search now returns the task results for all dates.
IIQSR-492	The Accelerator Pack email template 'EmailTemplate-FrameworkReminder' now correctly expands the email template variables, and now has the 'comment' and 'nowDate' arguments available. This template is used when accessing the envelope icon in My Work -> Access Requests.
IIQSR-489	Assigning permitted roles with a sunrise date to an already-assigned business role no longer results in the permitted role getting provisioned during refresh with provision assignments enabled.
IIQSR-486	Roles that are both assigned and detected are no longer de-provisioned when missing from the correlation model cache.
IIQSR-484	Rapid Setup date triggers for business processes no longer potentially trigger a day early when these operators are used: 'Is in the Future by at Least,' 'Is Today or in the Past,' 'Is in the Past by at Least.'
IIQSR-483	Batch CreateAccount requests no longer include the NativeIdentity attribute as an AttributeRequest.

Issue ID	Description
IIQSR-482	A targeted certification revocation notification email is now correctly sent on the reminder date.
IIQSR-479	"Failed to load resource" JavaScript errors are no longer displayed in the browser's console when certain pages are loaded.
IIQSR-477	Performance has been improved when the Perform Maintenance task is processing a large number of Account Group Permission revocations.
IIQSR-476	Expired password processing no longer interferes with electronic signatures.
IIQSR-475	Triggers for Lifecycle Events that use date attributes stored as string types now trigger when they should when the date attribute doesn't change and the date operation returns true.
IIQSR-473	Duplicate refresh workitems are no longer generated between aggregation and refresh task cycles.
IIQSR-470	Corrected issue with merging application provisioning policies with Identity Requests which resulted in an invalid Provisioning Plan.
IIQSR-469	Batch Requests with Remove operation can now process multiple entitlements.
IIQSR-466	Managed applications with provisioning configuration scripts no longer result in an error when remediating in a multi-threaded configuration.
IIQSR-465	Submitting a form with an identity field followed by allowed values field with display names no longer results in validation errors.
IIQSR-464	When correcting an Entitlement/Role SOD violation, only one remediation work item is now sent instead of two.
IIQSR-446	An optional rule, "AccPack Rehire Remove Neg Assignments", is now available which allows the option to remove negative assignments that were created by the AccPack Leaver Lifecycle Event when the AccPack rehire Lifecycle Event runs.
IIQSR-424	Identity events for future entitlement deassignments will now be purged for entitlement assignments that no longer exist.
IIQSAW-4176	A cloned ResultSet is now returned on ObjectUtil.getWorkgroupMembers (). This fixes an issue when committing the session before fully iterating the result.
IIQSAW-4134	In Identity Request approvals, the IdentityRequest Item Approval State and Execution Status now appropriately move to Completed, even when provisioning of the corresponding identity request fails.

Issue ID	Description
IIQSAW-4100	Organizational Unit (OU) changes in Active Directory won't be detected and propagated by IdentityIQ when Delta Aggregation is enabled. In order to propagate OU changes to IdentityIQ objects, it's necessary to periodically run full aggregation. This pertains specifically to changes to an entire OU. Individual account and account group changes will be propagated as expected.
IIQSAW-3930	It is now possible to prevent Native Change Detection from flagging an account name that changes only in casing (upper/lower case). Customers must use the CaseInsensitive flag during NativeChangeDetection if they want account name to be handled case insensitively.
IIQSAW-3917	Entitlements and Roles are no longer present in the account schema for Privileged Access Management applications. These can be removed from existing applications if they are still present.
IIQSAW-3915	During aggregation, if IdentityIQ detects two AD accounts or account groups with the same Distinguished Name but different UUIDs, it will update the UUID to the most recent value, and treat the two accounts or account groups as the same. This handles the case where an account or group is accidentally deleted and re-added. Consequently, it is not advisable to re-use the same DN with a different meaning. IdentityIQ will not detect this as an account or account group change to any attribute but UUID.
IIQSAW-3860	A saved Advanced Analytics report created from the result of an Advanced Search of type Access Request or Syslog can now be correctly executed.
IIQSAW-3810	Revocation of a certification item for which an Active Directory account has been moved or renamed, now properly includes the revised Distinguished Name and therefore succeeds.
IIQSAW-3670	Forwarding user functionality now functions when the same date is selected for both start and end dates.
IIQSAW-3651	It is now possible to navigate to the last page of results in the Account Group Membership Totals live report and the data on the last page now displays properly.
IIQSAW-3650	The documentation for the sailpoint.integration.IIQClient showIdentity API now correctly requires the object ID rather than Identity Name.
IIQSAW-3627	Entitlement views in Identity Warehouse, Certifications and Entitlement Catalog now display if a target permission has been denied.
IIQSAW-3626	Saving changes to managed attributes in the Entitlement Catalog now properly preserves group hierarchy.
IIQSAW-3592	Batch request stats can now be updated by multiple concurrent users without loss of data.

Issue ID	Description
IIQPB-1163	[SECURITY] All Spring libraries are upgraded to 5.2.20.
IIQPB-1151	Quicklinks configured to use "Objects in Requestor's Authorized Scopes" or "Requestee's Assigned Scope" no longer lead to a server error in Managed User Access.
IIQPB-1149	[Security] HTTP header has been removed from pack:tag responses.
IIQPB-1148	Attribute Sync with provisioning policies no longer causes a Null Pointer Exception when attribute sync audit events are turned on.
IIQPB-1140	Unstructured Target Aggregation no longer fails when Application Credential Cycling is enabled
IIQPB-1137	Dialogs will no longer render HTML embedded in the user-entered data section.
IIQPB-1129	Account Search Report now has a new column that shows the Identity Name.
IIQPB-1125	Application servers running in JVM 17 environments need to add the following line to their application server configuration: `--add-exports=java.naming/com.sun.jndi.ldap=ALL-UNNAMED`
IIQPB-1091	[Security] Web services used by UI suggest components no longer allow undesired information disclosure.
IIQPB-1088	[Security] All password form inputs now disable autocomplete by default.
IIQPB-1066	[SECURITY] The ability to edit rules can now only be completed by users that have the rights to edit rules.
IIQPB-1036	Entitlement Owner certifications now include all rights assigned to an identity for a permission.
IIQPB-1008	[SECURITY] The ability to edit inline scripts in IdentityIQ now requires either the SystemAdministrator capability or the new EditScripts SPRight.
IIQPB-1000	[SECURITY] jQuery has been updated to version 3.5.1.
IIQPB-987	SQL Server will no longer keep an idle session open during certification finalization.
IIQPB-986	Rapid Setup provisioning plans will now build without a Null Pointer exception.
IIQMAG-4209	Active Directory account move when using Rapid Setup Leaver no longer errors the task.
IIQMAG-3961	IdentityIQ now saves the client host IP address with the request context such that each new request will no longer overwrite the previous requests client host IP address.

Issue ID	Description
IIQMAG-3960	IdentityIQ no longer rejects the SCIM+JSON media type when validating SCIM responses from File Access Manager.
IIQMAG-3956	Wait steps in Workflows no longer create redundant background event items.
IIQMAG-3938	[SECURITY] The notification directive now strips HTML script tags from the message text in order to prevent code injection.
IIQMAG-3917	While sending teams notifications out, if we find two matching emails, we will not send a notification.
IIQMAG-3876	The escapeHTML utility method is now restored to the Velocity spTools.
IIQMAG-3875	[SECURITY] On the System Configuration, Proxy OAuth configurations will now have an encrypted secret.
IIQMAG-3873	File names for exported reports will be converted to camel case where supported. If not supported, file names will simply have spaces removed and words combined.
IIQMAG-3855	The Classifications drop down on the Classifications tab of the Entitlement Catalog is now functional when scoping is enabled.
IIQMAG-3854	[SECURITY] The email templates now properly escape extraneous user inputs. This applies to both variable references that get processed by Velocity and internally using the $(...) syntax. More comprehensive notes are attached in a doc to this bug.
IIQMAG-3822	Velocity script that does not resolve to a discrete value now resolves to an empty string instead of the literal script value.
IIQMAG-3821	Certification Activity by Application report, now has Signer, Signed off and Electronically-Signed columns in the report.
IIQMAG-3724	[SECURITY] PrimeFaces library upgraded to version 8.012 which includes and is compatible with jQuery 3.5.1; however, not backwards compatible with jQuery 3.4.1.
IIQMAG-3720	Provisioning Forms are now Localized.
IIQMAG-3673	Perform Maintenance now has improvements in performance for encrypting and decrypting attributes.
IIQMAG-3616	In a forwarded certification comments are now displayed in the More Info panel.
IIQINN-426	Work Item PolicyViolation Classifications display is no longer controlled by Certification Definition settings. Certification Policy Violations Classification display are still controlled by Certification Definition settings.

Issue ID	Description
IIQINN-58	Subsequent comments added during the lifecycle of the revocation of a certification item that had previously had a comment assigned, are now saved properly.
IIQINN-55	On the Advanced Analytics screen under Access Review, the filter on a group now provides unlimited viewing via the standard paging user experience control.
IIQINN-22	Certification names for mover events now properly use the certifier's displayName.
IIQINN-21	The tooltip help for the "Show Excluded Items" option in reports now explains the restrictions imposed on sorting options when this option is selected.
IIQINN-20	Timing dependencies interfering with sending multiple notification emails on certifications have been resolved, and when configured, multiple notification emails are now successfully sent.
IIQETN-10011	When a Distinguished Name (DN) in Active Directory is changed, IdentityIQ now appropriately updates the DN on accounts and account groups and propagates these changes to the associated objects.
IIQCB-4679	When there are more than 25 approvals for a user and comments are required for approvals or denials, the required comment popup now correctly shows for all approvals.
IIQCB-4645	The Role Members Report now allows for roles with indirect relationships when filtering by application.
IIQCB-4644	In the Identity Refresh Task, tooltips and population selector now work as expected.
IIQCB-4642	A certification approver rule can now specify a workgroup without encountering persistence errors.
IIQCB-4641	Support localizations for recommendation messages, regardless of whether AI Services is configured.
IIQCB-4640	The Task Result now correctly sorts the order of partitions when displaying the task result.
IIQCB-4629	Finnish messages are now available within IdentityIQ.
IIQCB-4627	[Security] linkDetails now displays details only for users with the appropriate permissions.
IIQCB-4619	[SECURITY] Certification pages are no longer vulnerable to reflected Cross Site Scripting (XSS) attacks.
IIQCB-4614	Emails that are sent when the SMTP connections have timed out are now retriable.

Issue ID	Description
IIQCB-4613	Find Users in Access Requests will no longer display unless the user has Request Access quicklink with Others enabled for one or more of the dynamic scopes that they are a member of.
IIQCB-4610	[SECURITY] The Log4j libraries have been upgraded to version 2.17.1 to remediate the vulnerabilities documented in CVE-2021-45105 and CVE-2021-44832.
IIQCB-4601	[SECURITY] The Log4j libraries have been upgraded to version 2.16.0 to remediate vulnerabilities documented in CVE-2021-45046 and CVE-2021-44228.
IIQCB-4553	The IdentityIQ integration with Identity AI now supports recommendations for IdentityIQ roles.
IIQCB-4542	[SECURITY] The OWASP Java HTML Sanitizer library changed to 20211018.2 to enforce policies associated with the SELECT, STYLE, and OPTION elements.
IIQCB-4488	A new Rule option has been added to filter Specific Users for a Quicklink population. This is a particularly useful alternative for deployments which currently use the Custom match criteria to invoke a rule using a Velocity template.
IIQCB-4378	IdP initiated SAML logins no longer causes a "Session already invalidated" error.
IIQCB-4276	The Role-Entitlement Analysis task is run during an upgrade to version 8.3
IIQCB-4230	Prior to this version, Electronic Signatures only used Basic Authentication, that is, a username and password, regardless of the IdentityIQ's login configuration. This meant that if an user used SAML to authenticate to IdentityIQ, they might not have the Basic Authentication login information required to perform Electronic Signatures. In this version of IdentityIQ, if the login configuration uses SAML, then by default SAML authentication will be used for Electronic Signatures. For SAML authentication during an Electronic Signature, the customer's identity provider is contacted, and a new authentication is requested. This does not affect the IdentityIQ session; the authentication is a new authentication into the identity provider. This new default can be changed to always using Basic Authentication for Electronic Signatures, regardless of the login configuration, by adding this entry to the IdentityIQ System Configuration via the Debug pages: `<entry key="alwaysUseBasicAuthElectronicSignature" value="true"/>`
IIQCB-4216	In approval work items there are two types of comments: comments for individual items and comments on the request.

Issue ID	Description
	The change introduced displays request level comments in their own \`Comments\` section on the Access Details screen. This applies to approved work items with request level comments present. Incomplete Work items are not shown on the Access Details screen.
IIQCB-4215	The Access Request Status Report no longer shows completed access request items when filtering on the Pending Status.
IIQCB-4205	Orphaned Request objects left by a failed partitioned aggregation are now cleaned up.
IIQCB-4194	The Java class sailpoint.tools.Base64 is now deprecated and will eventually be removed. Use instead sailpoint.tools.Base64Util or java.util.Base64.
IIQCB-4184	IdentityIQ will now respect the standard http/https proxy-related Java system properties when communicating with File Access Manager (FAM), Cloud Access Manager (CAM), and AIServices hosts.
IIQCB-3930	Account Group Search results with extendedAttributes of type Identity are now exported.
CONCHENAB-4158	The Workday Connector no longer uses Axis2 libraries for fetching responses. The new and upgraded Workday applications are independent of the `commons-httpclient` 3rd party jar. When using Axis2 libraries, or in case issues, set the "useSdkFramework" entry key to "false" in the application XML in the Debug page as follows, `<entry key="useSdkFramework" value="false"/>`
CONNAMDANG-3299	AWS Connector now supports IAM Role authentication method to connect with AWS native system.
CONUMSHIAN-4822	AWS connector now supports aggregation of tags on IAM entities.
CONUMSHIAN-5034	AWS connector now supports the creation and updates of InlinePolicy type for IAM Users and Group entities.
CONETN-3592	The Azure Active Directory account aggregation now optimizes the unchanged accounts.
CONETN-3524	The Azure Active Directory connector now shows correct Account Name on the User-Interface as configured in the account schema.
CONHOWRAH-3501	The Azure Active Directory Connector is now enhanced to handle non-JSON errors returned from the Azure AD APIs.
CONETN-3505	The Azure Active Directory connector now fetches the list of risky users with maximum page size during aggregation.

Issue ID	Description
CONETN-3590	The Azure Active Directory connector now saves the "accountDeltaToken" in the application after every delta aggregation. This will aggregate only changed accounts after a prior successful delta aggregation run, and not *all* the changed accounts after a prior full aggregation.
CONETN-3472	The Azure Active Directory connector no longer fails during an Add Entitlement operation if the nativeRules key is configured in source xml without a value.
CONETN-3538	The Azure Active Directory connector now provisions guest user having single quote in the email address without any error.
CONETN-3480	The Azure Active Directory Connector now supports advanced query filters like "endsWith","NOT" and "NE" during aggregation
CONETN-3645	The Azure Active Directory account aggregation no longer throws error "Too many files open" while fetching membership data.
CONETN-3612	The Azure Active Directory connector now sets all the attributes present in the provisioning plan.
CONETN-3473	The Azure Active Directory connector now provisions an Azure Guest account with the extension attributes which were getting skipped.
CONHOWRAH-3623	The Azure Active Directory connector handles user's identities more resiliently during account aggregation when the issuer assigned ID is absent for those identities.
CONETN-3663	The Azure Active Directory connector no longer throws incorrect error when attribute manager is present in the account schema.
CONETN-2329	The Delimited File Connector now executes the pre and post iterate rules consistently when a partitioned aggregation is performed.
CONNAMDANG-3515	Dropbox connector is now enhanced to support aggregation for different page size values.
CONSEALINK-2665	The Epic connector now supports the ability to update "ContactComment" based on the value of the boolean flag "isUpdateContactComment".
CONETN-3629	The G Suite Connector now supports provisioning an account with multi-valued complex attribute "locations".
CONJUBILEE-1414	The Salesforce connector now provides an option for contact creation while creating a new user.
CONCHENAB-4117	The Workday and Workday Accounts Connector now supports OAuth 2.0 authentication with 'refresh token' grant type.
CONCHENAB-4122	The Workday Accounts connector now supports OAuth2 authentication.
CONCHENAB-4438	The Workday Accounts connector has been optimized for lightweight test connections for faster operations.

Issue ID	Description
CONCHENAB-4432	Workday Connector supports the aggregation of rescinded past hires records with a specified offset limit.
CONCHENAB-4351	Okta Connector now supports managing “App Targets and App Instance Targets” for APP_ADMIN (Application Administrator) Role and "Group Targets" for HELP_DESK_ADMIN (Help Desk Administrator) role.
CONCHENAB-4175	Partitioning aggregation in Okta connector is now successful if a small number of users present in the Okta managed system.
CONETN-3691	The Oracle HCM Fusion Connector pulls the latest primary workrelationship of a worker when an account aggregation is performed.
CONETN-3637	The Oracle HCM Fusion Connector now aggregates the correct assignment attributes when a GetObject or an aggregation operation is performed.
CONETN-3465	The Oracle Fusion HCM Connector now aggregates all accounts updated by the supported Oracle Fusion HCM feeds when a delta aggregation is performed.
CONETN-3504	The Oracle HCM Fusion Connector now aggregates all workers correctly when a full aggregation is performed.
CONCHENAB-4136	Oracle Fusion HCM Connector now supports additional attributes and "Assignment Status Type ID".
CONCHENAB-4353	Oracle Fusion HCM Connector now supports migration of the existing /emp application or source to /workers API.
CONCHENAB-4454	The Oracle Fusion HCM connector now supports to aggregate "ASSIGNMENT_MANAGER_NUMBER" attribute.
CONCHENAB-4087	The Workday connector now supports aggregation and updates of Custom IDs.
CONSEALINK-2614	The Epic connector now supports the Epic August 2021 release.
CONSEALINK-2612	Epic connector is now verified to support Epic May 2020 for IdentityIQ.
CONETN-3451	The SQL Loader connector no longer fails when connecting to a target system with credentials having special characters.
CONETN-3456	The SQL Loader connector now supports provisioning fields of type String whose values are of length greater than 19 characters.
CONETN-3532	The SQL Loader connector no longer caches a connection in pool when an application configuration parameter is modified during test connection.
CONCHENAB-4509	Workday Connector now supports updating Custom ID (Other ID) having a blank value in the Workday system.

Issue ID	Description
CONCHENAB-4298	The Linux Connector now supports Federal Information Processing Standard (FIPS) for Red Hat Enterprise Linux version 8.3.
CONJUBILEE-979	The Web Services connector now supports quick configuration of operation endpoints using cURL command.
CONETN-3500	The Web Services connector now evaluates JSON based pagination steps correctly.
CONETN-3502	The Web Services connector now evaluates xml based pagination steps correctly.
CONETN-3520	Authorization header for Web Service connector endpoint now replaces placeholder when prefix is other than Bearer.
CONETN-3576	Web Service Connector now supports passing and retrieving of cookies from before and after operation rules with new application config "propagateCookieForRule".
CONETN-3561	REST Web Services connector now propagates error message correctly to provisioning result when retryableErrors are configured in application.
CONETN-3595	The Web Services Connector no longer sets the ProvisioningResult to "committed" when the provisioning request has failed.
CONETN-3470	The Workday Connector no longer displays unnecessary validation errors when a getObject operation is performed.
CONETN-3491	The Web Service connector now supports "skipEncodingDecodingUrl" application config in order to skip connector level url encoding and decoding for all endpoints.
CONETN-3572	The Workday Accounts Connector supports provisioning entitlements for an account having no existing roles on the target system.
CONETN-3591	The Workday Accounts Connector no longer fails when provisioning a role containing special characters in its name.
CONCHENAB-4372	The Workday connector now supports Workday API version 37.0
CONETN-3597	The Workday Connector now aggregates all accounts updated by the supported delta change events when a delta aggregation is performed.
CONETN-3477	The Workday Connector no longer skips any future dated account when an account aggregation is performed.
CONETN-3772	The Workday connector no longer fails with ConnectorException when aggregating or provisioning accounts.
CONETN-3425	The Workday Connector no longer aggregates workers beyond the offset specified in Past_Terminated_Offset attribute of the application.

Issue ID	Description
CONETN-3446	The Workday connector now returns a complete ResourceObject for a future dated account when an account aggregation is performed.
CONETN-3499	The Workday Connector no longer fails with a NullPointerException when aggregating accounts from an application having an empty API version.
CONCHENAB-4264	The Cloud Gateway connector now supports two-way SSL authentication, making the connection more secure
CONHOWRAH-3657	The Active Directory connector now runs the account aggregation successfully in the absence of an account group schema in the application.
CONJUBILEE-1350	The IdentityIQ Cloud Gateway Synchronization Task now supports transferring data to Cloud Gateway in JSON format.
CONHOWRAH-3298	Azure Active Directory Connector now supports managing Channels in Microsoft Teams.
CONCHORDS-972	RACF Connector now supports managing MFA-related attributes for RACF systems configured for MFA.
CONJUBILEE-1347	The custom code in rules no longer throws BeanShell ClassNotFoundException.
CONHOWRAH-3705	The G Suite Connector has been enhanced to support proxy (HTTP, HTTPS) configurations.
CONHOWRAH-3277	The G Suite connector is optimised for performance improvements during delta aggregation.
CONHOWRAH-3270	RSA Connector now supports partitioning aggregation.
CONJUBILEE-1412	The Web Services connector now supports delta aggregation.
CONHOWRAH-3702	The Google Workspace (G Suite) connector now supports filters to aggregate only desired accounts during account aggregation.
CONCHENAB-4150	The SCIM 2.0 connector now extend support for non-compliant SCIM 2.0 servers.
CONHOWRAH-3684	The Azure Active Directory connector has been enhanced to manage Distribution List and Mail Enabled Security groups through IQService.
CONHOWRAH-3539	The Azure Active Directory Connector now supports Privileged Identity Management (PIM). This enables to limit standing administrator access and review privileged access for excessive or unnecessary access permissions on privileged resources.
CONJUBILEE-1382	The SCIM 2.0 connector now supports providing different page size for account and group aggregation to optimise API calls.

Issue ID	Description
CONHOWRAH-3659	The SharePoint Online Connector has been enhanced to support proxy (HTTP, HTTPS) configurations.
CONETN-3657	Active Directory add membership provisioning operation now correctly displays error if user is not found while adding cross domain memberships.
CONETN-3647	Account creation will be rolled back in Active Directory when "rollbackCreatedAccountOnError" is "true" and after Script returns error.
CONETN-3676	Active Directory Connector will no longer result into failure while disabling account followed by move operation using AC_NewParent attribute and if the native identity is set as distinguishedName.
CONJUBILEE-1348	The secret attributes in application XMLs will remain encrypted after running IdentityIQ Cloud Gateway Synchronization Task.
CONJUBILEE-1437	To improve the security, the Cloud Gateway is now bundled with Apache Tomcat latest version 9.0.60.
CONCHORDS-992	Atlassian connectors now can successfully provision entitlements that contains spaces
CONETN-3756	The Azure Active Directory account aggregation now optimizes the unchanged accounts.
CONETN-3759	The Azure Active Directory connector now provisions a user account in case the password consists backslash ("\") in it.
CONETN-3725	The Azure Active Directory connector now fetches the Exchange Online Mailbox attributes without any error during account aggregation in case the attributes' count is huge.
CONSEALINK-2888	When universalManager is enabled and create multiple ticket option is enabled for IdentityIQ for BMC Remedy Service Desk, it creates multiple ticket successfully.
CONETN-3542	The SCIM 2.0 connector now supports modification of Groups via Users end point with below application config `<entry key="updateGroupsViaUsers" value="true" />`
CONHOWRAH-3470	The HCL(Lotus) Domino connector now supports HCL Domino version 11.
CONNAMDANG-3665	PeopleSoft HRMS connector now supports PeopleTools version 8.59
CONHOWRAH-3495	The HCL(Lotus) Domino connector now supports HCL Domino version 12.
CONNAMDANG-3578	Oracle connector now supports Oracle version 21c.
CONSEALINK-2517	Unix Connectors(AIX, Linux, Solaris) now provide SFTP support during aggregation.

Issue ID	Description
CONETN-3685	The SAP GRC Integration now supports provisioning an account without having to provide the name of the connectors in the API request.
CONETN-3604	The SAP GRC Integration now fetches the updated credentials of service account configured in the application.
CONETN-3558	Active Directory connector now supports distinguished name having CN with trailing comma.
CONETN-3666	The Active Directory connector provisioning operation will not fail when provisioning result of attributes which are present in excludeAttributesFromProvisioning is not set when setAttributeLevelResult is true.
CONETN-3589	Active Directory create provisioning operation for Contact objectType now respects excludeAttributesFromProvisioning attribute.
CONJUBILEE-1380	The SCIM 2.0 connector no longer throws NullPointerException error when mutability key is not present in schema endpoint response.
CONETN-3655	The Google Workspace connector no longer throws error "User creation is not complete" while provisioning.
CONETN-3745	The Google Workspace connector now shows actual error message in the Provisioning Result when Retry is enabled.
CONETN-3700	The access requests status now gets "Completed" while provisioning a user account of Google Workspace connector.
CONETN-3689	The Oracle HCM Fusion connector no longer has performance issues with Workers API when running account aggregation.
CONNAMDANG-3635	IBM DB2 connector now supports version 11.5
CONJUBILEE-1193	The Salesforce Connector now supports 'Collaboration Group' as group object.
CONSEALINK-2728	New direct connector to manage BMC Helix ITSM Service Desk integration
CONSEALINK-2936	Slack Connector now supports the "Slack Enterprise Grid" version.
CONSEALINK-2848	ServiceDesk tickets are now grouped by application type for easier identification and search.
CONSEALINK-2804	ServiceNow Service Desk Integration now provides a way to allow file attachment to tickets.
CONSEALINK-2609	The ServiceNow Connector now provides an option to 'Unlock' an account while performing 'Enable' operation.
CONSEALINK-2770	ServiceNow Connector now supports aggregation of inherited roles associated with an account.

Issue ID	Description
CONNAMDANG-3539	Dropbox connector now supports non-expiry access tokens as Dropbox has deprecated the support for long-lived access tokens
CONSEALINK-2575	ServiceNow Connector now supports aggregation and provisioning of dot walking fields on reference tables.
CONJUBILEE-1300	To ensure seamless integration, we have enabled Cloud gateway version detection and mandated a match with IdentityIQ version for all applications using Cloud Gateway as proxy.
CONJUBILEE-1270	The Jack Henry Symitar connector with updated powerON script handles the limitation of number of lines returned in the API response and fetches all users.
CONNAMDANG-3657	JDBC Connector is now enhanced to configure retries on aggregation failures making it more resilient and stable
CONETN-3554	LDAP Connector now logs the name of LDAP server in warning message if there is a delay in locating/searching user or group during aggregation. Additionally, if application type is LDAP then we also log host name in aforementioned warning message.
CONETN-3579	LDAP Connector no longer fails for delete and modify operation if Group DN contains any special character in it.
CONETN-3539	Active Directory connector now uses useTLS value from Exchange configuration while provisioning linked mailbox.
CONETN-3593	The Lotus Domino connector now provides a flag 'forceNonIndexDBSearch' to force IndexDB value to N ONLY during the create operation
CONCHORDS-1227	This release of IdentityIQ comes with ConnectorGateway-Feb-2022. For more details on this release of Connector Gateway, visit https://community.sailpoint.com/t5/Connector-Directory/Mainframe-Connectors-Downloads/ta-p/72044
CONSEALINK-2600	New connector "MEDITECH" is now available to connect to the MEDITECH Expanse application.
CONSEALINK-2548	The Micro Focus Service Manager Integration Module now supports Service Desk Integration with Micro Focus Service Manager version 9.7.
CONETN-3501	Active Directory connector now correctly reflects msExchHideFromAddressLists attribute value of the shadow account in the resource forest while enabling/disabling account in the account forest.
CONNAMDANG-3369	Microsoft SQL Server Connector now supports Microsoft SQL Server installed on Linux.
CONETN-3490	Native Change Detection will not get triggered for account enable or disable operation in Active Directory if it is done by IdentityIQ.

Issue ID	Description
CONETN-3471	The SAP GRC Integration no longer causes a NullPointerException when running an account aggregation.
CONETN-3755	Active Directory connector now passes all attributes including ObjectType and sAmAccountName as part of provisioning Request to ConnectorAfterScript.
CONCHENAB-4165	The Oracle Identity Manager connector now handles IndexOutOfBoundException gracefully
CONETN-3683	The Okta Connector now correctly provisions an empty value for a multivalued attribute of an account.
CONETN-3728	The Okta connector now correctly provisions a multivalued attribute having a null or empty value.
CONETN-3559	The Okta Connector now correctly aggregates multivalued attributes of an account.
CONETN-3468	The LDAP Connector now considers the "searchScope" configuration for searchDNs correctly during account aggregation.
CONETN-3498	The Oracle E-Business Connector now supports provisioning of entitlements having a description of length greater than 200 characters.
CONETN-3653	The Oracle HCM Fusion Connector no longer skips any accounts when an account aggregation is performed.
CONETN-3600	The Oracle HCM Fusion Connector now aggregates all custom attributes of AssignmentsDFF correctly.
CONETN-3610	The Oracle HCM Fusion Connector now aggregates location attributes of an account correctly when an aggregation is performed.
CONETN-3601	Oracle HCM Fusion connector now properly aggregates ManagerAssignmentNumber from managers array of worker's assignment
CONUMSHIAN-4834	The Oracle NetSuite connector now supports Aggregation and Provisioning for additional attributes.
CONUMSHIAN-4961	Oracle NetSuite connector will not throw http 400 error in case more than 1000 records for role and suiteQL is enabled.
CONETN-3107	The PeopleSoft HRMS Connector can now aggregate users correctly when a SQL query contains a question mark.
CONETN-3544	The SAP Portal-User Management Web Service Integration Module now supports provision of roles which contains gp: and pcd: in its unique name. The .sda file provided with this release must be deployed on the SAP Portal server to provision such roles.
CONHOWRAH-3634	The OpenLDAP connector now supports OpenLDAP versions 2.5 and 2.6.

Issue ID	Description
CONCHENAB-4196	The Linux Connector now supports Red Hat Enterprise Linux versions 7.8, 7.9, and 8.3.
CONETN-3569	RSA connector now handles user sessions appropriately.
CONETN-3729	Salesforce connector now handles invalid session exception for provisioning flows as well.
CONJUBILEE-1128	The Salesforce connector now replaces an existing Salesforce Profile with another Userlicense Profile without stripping off the Permission Set.
CONETN-3718	The account aggregation for SalesForce Connector no longer fails with Null Pointer Exception.
CONETN-3734	Identity Attribute for the Public Groups can be used as DeveloperName from its default value Name currently. This can be achieved with below configuration in application xml file : `<entry key="publicGroupIdentityAttribute" value="DeveloperName" />`
CONJUBILEE-1338	Salesforce Connector will now reuse the existing access token to login into managed system instead of creating new token every time.
CONUMSHIAN-4770	SAP GRC Connector now supports configurable access request type and access request priority during provisioning. The connector also supports account aggregation and provisioning of additional attributes.
CONUMSHIAN-4542	The SAP GRC connector has been enhanced to support provisioning of user group attribute.
CONNAMDANG-3505	SAP HANA connector is now verified for version SAP HANA 2.0 SPS5
CONETN-3664	The SAP HR/HCM Connector no longer fails when aggregating and provisioning accounts to an upgraded SAP patch system. The latest SAP patch the connector is tested on is SP 33.
CONETN-3515	The SAP Direct Connector now performs the de-provisioning of business roles correctly.
CONETN-3582	During Get Object, a Schema customization rule will get preference over an Aggregation customization rule in align with Aggregation flow for all connectors including Active Directory.
CONETN-3541	The SCIM 2.0 Connector no longer fails with a NullPointerException when handling non-SCIM compliant based messages.
CONETN-3727	The SCIM 2.0 Connector will send the path attribute only when provisioning an extended schema attribute of an account.
CONETN-3752	The SCIM2.0 Connector no longer fails when aggregating accounts from a non-compliant SCIM Server.

Issue ID	Description
CONETN-3670	The SCIM 2.0 Connector will always send the path attribute when updating an extended attribute of an account.
CONETN-3574	The SCIM 2.0 Connector no longer removes existing groups of an account when revoking entitlements using a PUT operation.
CONSEALINK-2630	ServiceNow Service desk Integration Module now creates ticket for revoke permission operation.
CONJUBILEE-1053	The Web Services connector now regenerates token using Custom and OAuth 2.0 authentication for long running aggregation operations.
CONSEALINK-2036	The ServiceNow Service Desk now displays a proper error message when the provisioning plan is empty or does not contain any account request.
CONETN-3584	ServiceNow connector now retries failures encountered due to token expiration during aggregation.
CONETN-3577	The Oracle HRMS Connector now supports fields KNOWN_AS, MIDDLE_NAMES, EMAIL_ADDRESS, WORK_TELEPHONE, DATE_OF_BIRTH, TITLE when provisioning an account.
CONETN-3463	The SharePoint Online connector now shows actual error message in the task result when error code 400 is returned during aggregation.
CONSEALINK-2915	Siebel Connector now supports Siebel server version 21.12.0.0
CONETN-3509	The SQL Loader connector no longer fails with a Timeout Exception when performing any supported operation on the application.
CONNAMDANG-3582	SuccessFactors connector now supports OAuth 2.0 authentication type with SFAPIs.
CONETN-3560	The SuccessFactors connector no longer fails the Test Connection when the response from native SuccessFactors system hosted in an NS2 infrastructure contains two cookies, JSESSIONID and a_route, that are sent to SuccessFactors system in subsequent requests.
CONETN-3606	The SuccessFactors connector now aggregates the correct value for an additional attribute when the navigation path (Xpaths) contains a not() function.
CONETN-3643	The SuccessFactors Connector no longer fails with ConnectorException when provisioning PhoneNumber attribute of an account irrespective of CountryCode/Extension attribute being disabled on SuccessFactors managed system.
CONCHORDS-1210	TopSecret Read Only Connector now processes 2005 records even when 2011 or 2021 records are absent.
CONJUBILEE-1428	The SCIM 2.0 connector now supports API throttling to save on time and costs.

Issue ID	Description
CONCHENAB-4103	The Oracle Identity Manager client now supports HTTPS protocol.
CONETN-3478	Active Directory connector source configuration will have msExchHideFromAddressLists attribute as string instead of boolean.
CONETN-3511	Enhanced logging suggestions is provided in IQService logs for better debugging of failures in script execution.
CONETN-3710	Active directory connector now successfully provisions msExchHideFromAddressLists as an Active Directory attribute if Exchange setting is not configured in application.
CONETN-3739	Active Directory Connector now doesn't truncate distinguished name with uid during provisioning.
CONETN-3506	The SuccessFactors connector now displays an appropriate error message when provisioning a username for an account.
CONCHENAB-4222	The Unix Connectors (Linux, AIX, and Solaris) now successfully perform the aggregation operation with SFTP authentication even if only one open session is allowed by the managed system.
CONCHENAB-4414	For ITIM Integration, the Log4j jars are upgraded to 2.17.1.
CONETN-3453	The SAP GRC Connector no longer fails with a NullPointerException when aggregating accounts having an empty user id.
CONJUBILEE-1376	The RemedyForce connector now supports BMC Helix RemedyForce platform.
CONSEALINK-2516	The update account operation in Webex Connector now works succeeds when the provisioning policy contains the WebexId.
CONETN-3613	REST Web Services connector now supports addRemoveEntInSingleReq attribute for handling multiple add roles at the time of create operation
CONJUBILEE-1098	The Web Services connector now supports skipping getObject call after create operation.
CONJUBILEE-1129	The Web Services connector now encodes URL irrespective of the throttling configuration.
CONETN-3519	The Windows Local Connector now uses configurable parameter "sleepInterval" in order to make thread sleep for configurable milliseconds when connection with server is not established.
CONSEALINK-2506	Zoom connector no longer keeps TCP Connections open.