SailPoint | IdentityIQ

Release Notes

Version: 8.2

Revised: December 2023

Copyright and Trademark Notices

Copyright © 2021 SailPoint Technologies, Inc. All Rights Reserved.

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

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, 8.2

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

This release note contains the following information:

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

IdentityIQ Updates and Enhancements

IdentityIQ 8.2 provides new features and capabilities across the product, including Compliance Manager, Lifecycle Manager, the Governance Platform, and Connectivity. Key enhancements in the release include:

Compliance Manager, Lifecycle Manager, Governance Platform Feature Updates

IdentityIQ 8.2 introduces the following new features or enhancements.

Feature/Enhancement	Description
Cloud Access Management Integration	With Cloud Access Management integration, IdentityIQ will display additional cloud access information for IdentityIQ entitlements which are known to Cloud Access Management. You will have the ability to: • Search/filter entitlements on cloud access information • View details of cloud access on related IdenttiyIQ entitlements and roles • Request entitlements and roles through Lifecycle Manager based on cloud access • Generate certifications for cloud access using targeted certification filtering
AI Services Integration	IdentityIQ can receive recommendations from AI Services for access requests for end users. The recommendations are for self-service access role requests. Users will be presented with access that AI recommends based on their attributes such as manager, department, location, and colleagues. The recommendations and the final decision will also be captured in reporting which will be important for auditors.

Feature/Enhancement	Description
Privileged Account Management (PAM)-Container Lifecycle Management and Multi-instance/multi-vendor support	• The enhancements to the PAM module aim to automate life cycle management and governance of privileged access. By establishing ownership of containers, most aspects of container ownership can now be automated through joiner, mover, and leaver lifecycle events. • Multiple PAM applications across a single or multiple vendors are now supported
Rapid Setup - attribute synch improvements and identity processing thresholds	Rapid Setup is a solution that was added in 8.1 p1 to help customers onboard applications in a quick and efficient manner while following best practices. The user interface was built to be business user-friendly eliminating the need for coding. As we continue to build on top of what was delivered, these new features can be used with or without Rapid Setup. • Identity Processing Threshold: This gives the ability to disable lifecycle events to prevent unwanted scenarios by enabling you to set thresholds at a percentage or fixed level. • Attribute Synch: Improved traceability, for example, where was Attribute Synch initiated, what was the change, where was attribute synched to. Add a new stage event processing feature. Staging events is similar to having approvals for Attribute Synch which enables you to stage the attribute synch during the go live phase and require someone to sign-off on the changes before they occur.
Reporting - enhancements around reporting and advanced analytics	• Keyword search using contains • Include search parameters/filters in report • Role Details Report – single application show me both IT and Business roles • Added Role Name as a filter in the Role Members Report • Added the Advanced Search options to all applicable searches • Display Role Type and Status in the Role Members report • New Role by Application Report – Role Name, Owner, Role Type, Status, Relation - Required, Permitted, Inherited, Classifications • Option not to send empty reports • Advanced Analytics: ability to filter for Account Status to filter inactive/active accounts
Business Process - required comments for access requests and approvals	Added the ability to configure comments to be required so users can provide business justifications when submitting access requests. • flexibility in choosing which entitlement and role comments are required for by applying a rule • configure approvals and rejections to require comments

Feature/Enhancement	Description
File Access Manager - single sign-on	The single sign-on authentication feature enables users to login to the File Access Manager web application using their organization's SSO (IdP) provider. It allows users a seamless login experience using their personal identity, without the need to provide additional credentials, and independent of the domain, region or organizational unit they belong to, much in the same way they login to IdentityIQ, IdentityNow or any other business application. Enabling SSO integration reduces the administrative overhead involved in maintaining a dedicated identity store, and enables administrators to leverage a secure method of authentication through existing federated identity management system. SSO Authentication is supported through any SAML based SSO service, including, Okta, Azure ADFS, Ping, One Identity, and most major providers.
File Access Manager - Amazon Web Serivces S3	The new AWS S3 Bucket Connector extends File Access Manager's Permissions Analysis, Access Reviews capabilities to resources and files stored on AWS S3 Buckets, and helps organizations attain a comprehensive governance posture and greater visibility into access to all data across on-premises and cloud storage alike. The connector enables administrators, business users, and data owners to view who has access to data on S3 buckets throughout the organization; analyze access rights for AWS IAM Identities across multiple Regions, Organizational Units and External and Internal Accounts; and review granular access governance controls down to the file level. Users can gain insight into Organization and Bucket-level Access Policies, Public Bucket Permissions, and fine-grained ACL-based access rights for individual identities.
File Access Manager - Linux	Though Linux servers are not often used as file servers, many organization use Linux servers to host mission critical systems and processes, that often rely on unstructured data resources to function. As a consequence the need arises to protect these mission critical resources and ensure their integrity and continuous availability. The new Linux Connector extends File Access Manager's Permissions Analysis, Access Requests and Certifications capabilities to Linux systems, of all major distributions. This feature will provide organizations with a comprehensive picture of effective data access privileges granted to users, accounts and groups from NIS and LDAP (AD) identity stores, as well as local accounts and identities, through a single centralized view. File Access Manager comprehensive approach will allow IGA admins and data owners to enforce governance controls, identify excessive privileges and overly-privileged accounts, detect overexposed or jeopardized resources, assess risk and take preventive and mitigative actions - to protect mission critical processes and resources.

Feature/Enhancement	Description
SaaS governance - Cloud Access Management Integration (Phase 2)	Cloud Access Management provides visibility and insights across the top IaaS providers from a single screen. The Phase 1 integration with SaaS Governance extended that visibility as read-only details on governance activities such as entitlement administration and access certifications. With this second phase, organizations can begin driving governance activities based on cloud-access data. Administrators will have greater visibility into the cloud access granted by entitlements on cloud-enabled sources. Certification Administrators will be able to create certification campaigns that target identities with cloud access on specific cloud providers, accounts, groups and roles. Cloud-related access can be requested and approved through the Access Request process. This integration extends existing IdentityNow certification and access request functionality to support cloud governance with new visibility and insights for entitlements that provide cloud access .

Connectors and Integration Modules Enhancements

IdentityIQ 8.2 provides various enhancements in the following connectors and integration modules.

New Connectors

IdentityIQ 8.2 delivers new, out-of-the-box connectors for the following enterprise applications, which simplifies the connectivity of these systems.

New Connectors	Description
Zendesk	A new **Zendesk** connector is now available to connect the Zendesk native system. **Benefits**: Customers can now use the new connector to manage and govern Zendesk accounts
Atlassian Cloud Jira Service Management	A new integration module IdentityIQ for Atlassian Cloud Jira Service Management is now available. **Benefits**: Atlassian Cloud Jira Service Management is now supported for IdentityIQ. This integration module allows ticket creation and tracking using the IdentityIQ platform as a single source for management.
Atlassian Suite - Server	IdentityIQ introduces net new connector to manage the server version of Atlassian Suite. With this release, the connector supports user and group management of the Server version of Atlassian Suite of products. **Benefits**: Atlassian Software Suite is one of the widely used tools in any enterprise. Governance capabilities for this platform will provide customers with better security compliance.
Atlassian Suite - Cloud	Atlassian Suite - Cloud Connector, in addition to Jira Software, now supports managing access for other Atlassian products - Jira Service Desk, Opsgenie, Statuspage and Confluence. **Benefits**: Customers can now use the additional Atlassian modules verified for the connector to offer business continuity.

New Connectors	Description
Zendesk Service Desk Integration Module	IdentityIQ for Zendesk Service Desk Integration Module is available now. **Benefits**: Zendesk is one of the widely used ticket tracking tools in any enterprise. This integration module allows ticket creation and tracking using the IdentityIQ platform as a single source for management.
Oracle ERP Cloud	The Oracle ERP Cloud Integration Module manages users, roles, and data access of Oracle ERP Cloud's Financial module. **Benefits**: The Oracle ERP Cloud Integration provides deep governance of identity from the lens of security
MongoDB Cloud - Atlas	MongoDB Cloud - Atlas manages Atlas users present in the MongoDB on the cloud. **Benefits**: MongoDB Atlas provides the customers with the ability to govern the no-sql database family and provides better security compliance.
MongoDB Cloud - Database	MongoDB Cloud - Database manages database users present in the MongoDB database on the cloud. **Benefits**: MongoDB Atlas provides the customers with the ability to govern the non-sql database family and provides better security compliance.
Jack Henry	The IdentityIQ now provides a new integration module for Jack Henry system. **Benefits**: New connector for Jack Henry out of the box provides customers the ability to connect the system with convenience to SailPoint's systems.
Dynamics 365 Finance and Operations	IdentityIQ introduces a new integration module **Dynamics 365 FO** to manage Dynamics 365 for Finance and operations from Microsoft Dynamics 365 suite. **Benefits:** The integration module introduced has the ability to manage Microsoft Dynamics 365 For Finance and Operations, a cloud ERP system that is a part of the Dynamics 365 product line.
Dynamics 365 CRM	The IdentityIQ introduces a new integration module **Dynamics 365 CRM** to manage Dynamics CRM from Microsoft Dynamics 365 suite. **Benefits**: Customers now have the ability to manage Microsoft Dynamics 365 CRM from the Microsoft Dynamics 365 suite, a cloud CRM system that is a part of the Dynamics 365 product line.
Dynamics 365 Business Central Online	IdentityIQ introduces a new integration module **Dynamics 365 Business Central Online** to manage Business Central Online from Microsoft Dynamics 365 suite. **Benefits**: Customers now have the ability to manage Microsoft Dynamics 365 Business Central Online, a part of the Dynamics 365 product line.
Slack	New connector **Slack** is now available to connect the Slack native system. **Benefits**: Customers can now govern identities in Slack.
Zoom	New connector **Zoom** is now available to connect to Zoom system. **Benefits**: Customers can now govern identities in Zoom.

Active Directory

Description	Benefit
The Active Directory Connector now supports bringing delta changes for contact objects.	Performance improvements with delta aggregation for **Contact Objects**.
The default native identifier for Active Directory applications has changed back to distinguishedName. All new Active Directory applications created will have distinguishedName as the native identifier. The use of objectGUID as the native identifier introduced in previous patches introduced some usability and functional limitations that will be corrected in a future release. The current recommended best practice is to continue to use distinguishedName as the native identifier for Active Directory applications.	The enhancement provides for business continuity which could have failed due to the use of default native identified.
The Active Directory Connector now supports AWS Managed Microsoft AD service.	Connector supporting **AWS Managed Microsoft AD** provides scalability to it across Microsoft product family.
The Active Directory Connector now supports managing shared mailboxes.	Customers are now able to manage shared mailboxes through the Active Directory Connector, extending options for user onboarding and reducing the need for customizations.
The Active Directory Connector now supports managing linked mailbox for users where exchange is deployed in separate, trusted forest also known as resource forest.	Customers can now leverage the Active Directory Connector to manage linked mailbox, increasing support for diverse deployment models.
The Active Directory Connector now supports Managed Service Accounts (MSA) and group Managed Service Accounts (gMSA). For more information, seethe Active Directory documentation.	Enabling more granular level access management of non human identity widely used in AD infrastructure.
The Active Directory Connector is now enhanced to improve the performance during pass-through authentication (PTA) for applications with multiple domains defined.	The Active Directory Connector now supports PTA in Multi-domain and Multi Forest network, allowing for wider out of the box support of diverse deployment models.

Amazon Web Services

Description	Benefit
The Amazon Web Services Connector is now enhanced to handle the rate limit of API calls to AWS system which causes API throttling exceptions.	The connector is now more efficient in handling high traffic conditions to avoid exceptions and failures.

Azure Active Directory

Description	Benefit
The Azure Active Directory Connector now supports the ability to configure Azure resource and token endpoints. For more details check the latest Azure Active Directory Connector Guide.	The enhancement provides scalability for Azure Active Directory Connector.
The Azure Active Directory Connector now supports managing servicePlan associated with an account as a group object.	Fine-grain governance capability enhanced with the addition of managing license packs.
The Azure Active Directory Connector is now enhanced to support managing Azure objects like Management Groups, Subscriptions, Resource Groups, and RBAC roles.	Additional support for Azure objects provides the capability of fine-grain governance for Azure.
The Azure Active Directory Connector is now enhanced to use Microsoft Graph APIs completely. To enable using the latest attributes and features supported by Microsoft Graph API, set the value of **useMSGraphAPI** application attribute to **true**. For more information, see the latest documentation of Azure Active Directory.	An enhanced set of capabilities are now available with the introduction of Graph APIs from Microsoft.
The Azure Active Directory Connector now provides visibility into user's risk-related information.	Based on certain unwanted or critical events Azure Automatically marks users as risky, thus providing proactive decision-making capabilities.
The Azure Active Directory Connector now supports custom attributes for accounts and groups.	Custom attribute support provides flexibility to the customer for governing custom attributes.
The Azure Active Directory Connector now supports managing user mailbox including the shared mailbox in exchange online.	Additional support for mailbox for users and shared, provides better governance.
The Azure Active Directory Connector now supports OAuth 2.0 Certificate Credentials (JWT) flow as an additional authentication mechanism.	OAuth grant type provides a stronger authentication mechanism for customers to use.
The Azure Active Directory Connector now supports OAuth 2.0 Auth Code / Refresh Token flow as an additional authentication mechanism.	OAuth grant type provides a stronger authentication mechanism for customers to use.

Description	Benefit
The Azure Active Directory Connector now supports managing Microsoft Teams as Microsoft 365 group.	Using this enhancement customer can now perform the complete access management on MS Teams using Azure Active Directory connector.
The Azure Active Directory Connector now supports the management of the **manager** attribute of a user.	Enhancement provides fine-grain governance with additional attribute support.
The Azure Active Directory Connector now supports managing service principal objects present in Azure Active Directory.	Adding SPNs as another group object will give direct and granular level visibility to customers who are managing their application objects along with groups.
The Azure Active Directory Connector now supports OAuth 2.0 SAML Bearer Assertion flow as an additional authentication mechanism.	SAML Bearer provides better security during authentication.

Cerner

Description	Benefit
The Cerner Connector now supports filter for Inactive accounts for aggregation operations.	Customers can set filters as required for the data they need to aggregate from Cerner.

Cloud Gateway

Description
The Cloud Gateway would now be supported on Windows Server 2019 Operating System.

Connector Gateway

Description	Benefit
Connector Gateway is now certified to run on zLinux for SUSE Linux Enterprise Server 15.	Verification with the latest versions of SUSE Linux connector provides business continuity in the environment.

Delimited File

Description	Benefit
The Delimited File Connector is now more secure with FTPS support.	Added security to ensure customer data is safe.

Dropbox

Description	Benefit
The Dropbox Connector now supports enable and disable accounts.	The flexibility of enabling or disabling accounts improves control over access.

Duo

Description	Benefit
The Duo Connector now supports external password management for Duo administrators in the Duo native system.	Duo Connector now correctly maps the status of Duo administrator with **pending activation** state.
The Duo Connector now supports enable and disable operation for Duo administrators.	Convenience for operation for enabling and disabling Duo Admin users.

Epic Healthcare

Description	Benefit
The Epic Connector now supports configuring Client ID from the application configuration.	User interface based configuration is provided for better user experience
The EPIC Connector now supports configuration of any ID type for the complex attributes.	Configurable ID Types will make it flexible for the customers to tailor the ID for their business process.
The Epic Connector now supports configurable lock reason codes for locked accounts.	Multiple block reason will provide clarity to business users to understand why an account is in a locked state and take appropriate actions.

G Suite (Google Apps)

Description	Benefit
The G Suite Connector now uses Gmail APIs to fetch Email delegations instead of Email Settings APIs which are deprecated.	Changing methods to adopt the latest implementation from Google ensuring business continuity.
The G Suite Connector is now enhanced to manage the cloud resources present on the Google Cloud Platform (GCP).	Deeper governance with the new feature allows in-depth insights to manage cloud resources on the Google Cloud Platform.
The G Suite Connector has been enhanced to optimize the performance during the aggregation and provisioning operations.	Performance optimization ensuring low/no downtime.

Description	Benefit
The G Suite Connector now supports exponential back-off to handle the limit and quota errors during provisioning operations.	Enables the retry mechanism as per standards set by Google which helps to handle unwanted failures by sending requests in chunks by defined algorithms.
The G Suite Connector now supports OAuth 2.0 Service Account as an additional authentication mechanism.	Google is enabling upcoming APIs only using the **Service Account** method. In order to move forward with upcoming enhancement, this method is a must and ensures the consumption of recommended practice by Google.

GoToMeeting

Description	Benefit
GoToMeeting Connector now supports OAuth API V2 token.	V2 API's from GoToMeeting ensures business continuity for the customers using the connector.
GoToMeetingConnector now supports Admin API's along with admin roles access management.	Support for updated API's ensures business continuity.

IBMi

Description	Benefit
IBMi connector now supports aggregation of User Profile Creation Date Time (UPCRTD).	Support for **UPCRTD** attribute provides information about **create date/time** during account creation. This will help during SLA monitoring operations and for audit purposes.

IQService

Description	Benefit
IQService now provides a configuration option to rely on the operating system for TLS protocol selection while communicating with IdentityIQ. For more information, see the IQService documentation.	The enhancement provides scalability readiness for the future.
IQService now has a new configuration option to disable unwanted services from an IQService installation. For more information, see the IQService documentation.	A more secure and robust channel along with default configurations to reduce confusion and promote best practices.

Mainframe Connectors

Connector	Description	Benefit
RACF, TopSecret and ACF2	SailPoint Connector for RACF now supports z/OS 2.4	Verification with the latest z/OS ensures connector provides business continuity in the environment.
	The respective Connector now supports setting scope filter for account aggregation. The connector can aggregate all the accounts from the respective connector which starts with any of the configured character sets from the filter list.	Configurability has been provided in the connector to let customers choose what data they need in the system.
ACF2	IdentityIQ supports managing of X-ROL and X-SGP Entities for ACF2. To use this feature for upgraded applications, refer to the Mainframe Integration Modules documentation.	With the introduction of X-ROL and X-SGP, customers can take the advantage of the capability of governance of role and source entities.
	ACF2 Connector now supports managing X-ROL and X-SGP as additional group entities.	With the introduction of X-ROL and X-SGP, customers can take the advantage of the capability of governance of role and source entities.

RACF LDAP and Top Secret LDAP Integration Modules

Description	Benefit
SailPoint RACF LDAP and TSS LDAP Integration Module now supports IBM Tivoli Directory Server for z/OS 2.4 with SDBM LDAP back end.	Verification with the latest OS version, ensures that connector provides business continuity.

Microsoft SharePoint Online

Description	Benefit
The SharePoint Online Connector now supports OAuth 2.0 SAML Bearer, Certificate Credentials (JWT), Auth Code / Refresh Token as additional authentication mechanisms.	With additional authentication mechanism support, connector ensures flexibility to choose with assured security

Microsoft SQL Server

Description	Benefit
Microsoft SQL Server Connector now supports Microsoft SQL Server on Azure SQL Virtual Machines.	Verification with Azure SQL ensures business continuity.

Okta

Description	Benefit
The Okta Connector now uses an enhanced API Rate Limiting mechanism.	The enhancement provides a better product performance.
Okta Connector now supports set password in permanent mode while creation of new account.	Flexibility for customers to opt for the password feature as per their organizations business policies.
The Okta Connector now supports OAuth 2.0 with **Client Credentials** grant flow.	OAuth grant type will allow better security for enterprises.
The Okta Connector now supports assigning a user type when creating a user in Okta. It also supports aggregating the type of the user with **type_name** and **type_displayName** attributes which signifies the name and display name of the assigned user type respectively.	Customers have the flexibility to assign what type of user is being created providing admins a more informative experience.

Oracle E-Business Suite

Description	Benefit
Oracle E-Business Suite Connector now supports **Menu** as a group object. Menu and associated Functions can now be aggregated for identifying low-level privileges assigned to a user.	The Oracle E-Business Suite Integration now provides a deeper governance capability of identity from the lens of security.
SailPoint Oracle E-Business Suite Connector now supports the service account permissions provided through the API: AD_ZD.GRANT_ PRIVS from Oracle E-Business Suite 12.2.4 onwards.	Updated permission set supported for service accounts.

Oracle ERP Cloud

Description	Benefit
Oracle ERP Cloud connector now supports Worker association to User Account during Create or Update operations.	Workers association support provides the capability to link workers with accounts. This way, enterprises can now govern workers as user accounts.
The Oracle ERP Cloud manages users, roles, and data access of Oracle ERP Cloud’s Financial module.	The Oracle ERP Cloud Integration provides deep governance of identity from the lens of security.

Oracle Fusion HCM

Description	Benefit
The Oracle Fusion HCM connector now supports worker API for new applications only. Existing applications will continue using employee API with no impact.	As Oracle moves to invest in the new Workers API, SailPoint connector now extends its compatibility to support the new API.

Description	Benefit
The Oracle Fusion HCM connector now aggregates the sub-resource attributes of the employee.	Sub resource attributes provide meaningful information to the customers to make better decisions.
The Oracle Fusion HCM Connector now supports updating attribute **Username**.	Customers can update username from the platform and manage a clean data.

RSA Authentication Manager

Description	Benefit
The RSA Authentication Manager Connector now supports the replacement of tokens along with managing tokens as separate group objects. Tokens as **group object** now eliminate the need for tokens as direct permissions. For more information, see the RSA Authentication Manager Connector documentation.	With RSA Authentication Manager Connector customers can manage Token operations across the system as it's now acting as a Group object.
The RSA Authentication Manager Connector now supports managing RADIUS profile. For more information, see the RSA Authentication Manager Connector documentation.	With RSA Authentication Manager Connector customers can now manage RADIUS profiles too.

Salesforce

Description	Benefit
The Salesforce Connector now supports • Managed Package Licenses as a group object • Permission Set License as a group object	Now using this connector customers can manage another license object which is • Managed Packaged License • Permission Set License
The Salesforce Connector now supports JSON Web Token (JWT) grant type in OAuth authentication.	The enhancement provides a more secure authentication mechanism.
The Salesforce Connector now supports refresh token grant type in OAuth authentication.	The enhancement provides a more secure authentication mechanism.
The Salesforce Connector now supports PermissionSetGroup as a group object.	Now using this connector customers can manage another permission object which is the Permission set group.
The Salesforce Connector now supports API version 48.0.	Currency with latest API's ensures business continuity.

SAP ERP - SAP Governance Module

Description	Benefit
The SAP Connector will now support SAP JCO 3.1.x version only and the older SAPJCO 3.0 version will no longer be supported.	Customers will be made aware of the supportability of the components SAP is deprecating from its landscape to aid in business continuity.

SAP HANA

Description	Benefit
The SAP HANA connector now supports provisioning more attributes such as, EMAIL_ADDRESS, TIME_ZONE, VALID_FROM, VALID_UNTIL, IS_CLIENT_ CONNECT_ENABLED, IS_RESTRICTED, and Disable password.	Customers can now reduce customizations which reduces maintenance cost and complexity.

SAP Governance Application Module - SAP GRC

Description	Benefit
The SAP GRC Integration is now enhanced to support the Business Process and Sub Process Filter under Access Management mode.	Customers can now control the roles to be aggregated through Business Process Level filtering.
The SAP GRC Integration is now enhanced to aggregate Child Roles associated with Business and Composite role types.	As more of our customers have started using our new SAP GRC connector for access management, there is a an adequate demand for SailPoint to get the technical roles inside logical containers like Business roles and Composite roles which helps to know its actual associations and accesses. This new group schema attribute brings those details which will be helpful when doing certifications.
The SAP GRC Integration is enhanced to support **Access Management** integration mode which enables us to aggregate and provision User and its access to all the connected system in SAP GRC landscape.	This enables use of the SAP GRC connector to manage Users and their access on all the connected systems in SAP GRC landscape.
The SAP GRC Integration is now enhanced to support Partial approval of provisioning request.	Customers will now have more granular control over provisioning request approvals.

SAP HR/HCM

Description	Benefit
The SAP HR Connector will support SAP JCO 3.1.x version only and the older SAPJCO 3.0 version will no longer be supported.	Customers will be made aware of the supportability of the components SAP is deprecating from its landscape to aid in business continuity.

Identity Governance Connector for ServiceNow

Description	Benefit
The Identity Governance Connector for ServiceNow now supports partitioned account aggregation.	Partitioning support provides significant performance for aggregation operations.

Slack

Description	Benefit
The Slack Connector supports imposed API rate limits by Slack. Aggregation and provisioning operations will be retried and handled gracefully post reaching the API rate limits.	Improved connector operations and experience
The Slack Connector now supports channel management to govern Slack Channels.	Slack Channel management provides broader governance of the Slack application.

SQL Loader

Description	Benefit
The SQL Loader Connector now supports files hosted on a location accessible via SFTP, SMB, HTTP or HTTPS protocols.	The update provides customers the flexibility to access files over various secured protocols as options.

SuccessFactors

Description	Benefit
The SuccessFactors Connector now supports the SFAPI path value in XPath 2.0 format to aggregate the additional Attributes.	The customer can add more attributes and more relevant data of their choice without any rule or additional processing.
The SuccessFactors Connector is enhanced to support the User Management with the following features: • Aggregation of Active User and inactive User • Creation of User • Addition and Removal of Static Group to the User • Update of Account wth selected attributes • Enable /disable Account • Change Password	Customers will now have enhanced control over user management in SuccessFactors, allowing better support for diverse implementation needs.
The SuccessFactors Connector is enhanced to support the following: • Aggregation of Roles • Aggregation of Group • Addition and removal of Static Groups to the account	Customers will now have enhanced visibility over role and group management in SuccessFactors, allowing better support for diverse implementation needs.

System for Cross-Domain Identity Management (SCIM) 2.0

Description	Benefit
The SCIM 2.0 Connector now supports provisioning group objects.	The connector provides the ability for deeper governance with the capability for provisoning group objects.
The SCIM 2.0 Connector will now support aggregation of extended multiple Group objects.	Extended multiple group objects provides for deeper governance.
The SCIM 2.0 Connector now supports the No-Authentication mechanism.	Flexibility to customers to by-pass authentication in case of restrictions posed by systems.
The SCIM 2.0 Connector now supports the following grant types in OAuth 2.0 Authentication: • Password • JWT Bearer Token	Additional grant types of **password** and JWT Bearer Token provides an alternate authentication options to customers.

Tivoli Access Manager

Description	Benefit
The IBM Tivoli Access Manager Connector now supports IBM Security Directory Suite 8.0 as a backend directory server.	Verification with the latest version of the application will ensure business continuity.

Web Services

Description	Benefit
The Web Services Connector now supports partitioned aggregation.	Partitions enhances aggregation performance.
The Web Services Connector now supports account/group aggregation from multiple independent endpoints.	This enhancement provides scalability to the connector to use multiple independent endpoints.
The Web Services Connector now supports API rate limiting as per RFC.	Many modern web applications make use of throttling for heavy API use. In order to better support these applications and broaden the ease of deployment and configurability of the Web Services connector, the Web Services connector will now be able to detect and respond to common forms of throttling.
The Web Services Connector now support custom authentication endpoint for systems not supporting standard authentication methods.	The enhancement provides flexibility to customers to select authentication endpoint for authentication.
The Web Services Connector now supports SAML Bearer Assertion authentication.	The enhancement provides a more secure authentication mechanism.

Description	Benefit
The Web Services Cconnector now supports fetching additional data for multiple users in a single API call.	Improved performance provides efficient connector operations.
The Web Service Connector now supports Unlock Account.	Unlock account feature adds to convenience for account management from connector console itself.

WebEx

Description	Benefit
The WebEx Connector now supports **Site Name** parameter in the XML APIs post deprecation of Site ID parameter in the same.	The enhancement provides connector its compatibility with Cisco's new API updates.

Workday

Description	Benefit
The Workday Connector now fetches data according to time zone provided.	Customers can now aggregate data based on their local timezone (Effective Time) to trigger workflows and perform timely operations such as, Hire, Termination, Re-hire, and Conversion.
The Workday Connector now brings future marked rescinded hires to track JML data more efficiently.	The Workday connector can now preserve the link to rescinded users to complete the de-provisioning workflow for future rescinded hires.
The Workday Connector now supports web services 35.2 version.	Currency with the latest protocols ensures business continuity.
The Workday Connector now supports deleting email and phone information.	Workday connector is now capable of completing the termination process with deleting information related to email and phone of the Worker.
The Workday Connector now supports aggregating future rescinded hires.	Workday connector can now preserve the link to rescinded users to complete the de-provisioning workflow for future rescinded hires.

Workday Accounts

Description	Benefit
The Workday Accounts Connector now extends support to aggregate **security group** objects as well.	Workday Accounts connector now aggregates all the user-based security groups associated with the workday organization, irrespective of user assignment.
The Workday Accounts Connector now supports Add and Remove user based security groups from account.	Workday Accounts connector now aggregates all the user-based security groups associated with the workday organization, irrespective of user assignment.
The Workday Accounts Connector now supports User based security groups aggregation.	Workday Accounts connector now aggregates all the user-based security groups associated with the workday organization, irrespective of user assignment.

Description	Benefit
The Workday Accounts Connector now fetches organization role with organization name.	Workday Accounts connector now makes it easier to manage user roles by populating the entire mapping of respective roles with organization names.
The Workday Accounts Connector now supports Change Password operation.	Workday Accounts Connector admin users can easily implement a **Reset Password** for all workday accounts.
The Workday Accounts Connector now supports Create Account.	Workday Accounts is now no more a read-only connector, with this enhancement, it now offers complete CRUD Operations for Workday Accounts.
The Workday Accounts Connector now supports updating of all Workday-supported schema attributes.	Now enabling complete access management in Workday system, using this feature customers can now configure workflows for creating workday accounts automatically.

Connectivity Platform and Language Updates

Connector/Component	New Platform Version
BMC Remedy	The BMC Remedy Connector now certifies all the supported operations with the following versions: • BMC Remedy Action Request System Server version 19.02 • BMC Remedy Action Request System Server version 20.02
BMC Remedy Service Desk	IdentityIQ for BMC Remedy Service Desk supports the following versions of BMC Remedy AR System: • 20.02 • 19.02 • 18.08
Tivoli Access Manager	The IBM Tivoli Access Manager Connector now supports IBM Security Verify Access version 10.0 (formerly known as IBM Security Access Manager).
BMC Remedy IT Service Management	The BMC Remedy IT Service Management Suite Connector now certifies all the supported operations with the following versions: • BMC Remedy IT Service Management Suite version 19.02 • BMC Remedy IT Service Management Suite version 20.02
Cloud Gateway	The Cloud Gateway would now be supported on Windows Server 2019 Operating System.
SAP HANA	SailPoint SAP HANA connector now supports SAP HANA 2.0 SPS4.
Linux	The Linux Connector now supports • Red Hat Enterprise Linux version 8.2

Connector/Component	New Platform Version
	• Ubuntu 20.04 LTS
Novell eDirectory (NetIQ)	The SailPoint Novell eDirectory (NetIQ) Connector now supports version 9.2.
Oracle ERP Cloud	Oracle ERP Cloud connector now supports the following modules: • Project Management • Procurement • Risk Management
Oracle	Oracle Database Connector now supports Oracle Database 19c.
Oracle E-Business Suite	Oracle E-Business Suite Connector now supports the following versions of Oracle E-Business Suite • 12.2.10 • 12.2.9
PeopleSoft HCM	The PeopleSoft HCM Connector now supports PeopleSoft Tools version 8.58.
PeopleSoft Direct	The PeopleSoft Direct Connector now supports PeopleSoft Tools version 8.58.
ServiceNow	The SailPoint Identity Governance Connector for ServiceNow now supports the following ServiceNow releases: • Quebec • Paris
Service Desk	The IdentityIQ for Service Desk now supports the following ServiceNow releases: • Quebec • Paris
SAP ERP - SAP Governance Module	SAP Governance Module is now certified with SAP_MARKETING (Hybris Marketing).
SAP HANA	SailPoint SAP HANA Connector now supports SAP HANA 2.0 SPS4.
	The SAP HR/HCM Connector will now only support SAPJCO version 3.1.x only.
Siebel	Siebel Connector now supports Siebel CRM Version 17.0.0.0 (IP 2017) along with patches 18.x, 19.x and 20.x.
Workday Accounts	The Workday Accounts Connector now supports Workday Financial management system.
RSA	RSA Authentication Manager Connector now supports the latest server version 8.5.
Windows Local	The Windows Local Connector now supports managing Microsoft Windows Server 2019.
IQService	IQService now uses .NET Framework version 4.8 as the default runtime.

Connectivity Dropped Platform Support

Connector/Integration Module	Dropped Platforms
BMC Remedy Service Desk	The IdentityIQ for BMC Remedy Service Desk now no longer supports the BMC Remedy AR System versions of 9.1.00 and 9.0.00.
Tivoli Access Manager	The Tivoli Access Manager Connector no longer supports IBM Security Access Manager 7.0.
ServiceNow Service Desk	The IdentityIQ for ServiceNow Service Desk now no longer supports the ServiceNow Madrid release.
ServiceNow	The SailPoint Identity Governance Connector for ServiceNow now no longer supports the following ServiceNow releases: • Madrid • London
Oracle	Oracle Internet Directory Connector now no longer supports Oracle Internet Directory version 11gR2.
LDAP	• Novell eDirectory Connector now no longer supports Novell eDirectory version 8.8. • IBM Tivoli Directory Server Connector now no longer supports IBM Tivoli Directory Server version 6.3 • The SunOne Direct LDAP Connector now no longer supports ODSEE 11g.
Microsoft SharePoint Server	The Microsoft SharePoint Server Connector now no longer supports Microsoft SharePoint Server version 2010.
Lotus Domino	IBM Lotus Domino Connector no longer supports IBM Lotus Domino Server version 8.5.x.
BMC Remedy	The BMC Remedy Connector no longer supports BMC Remedy Action Request Server version 9.0 and version 9.1
BMC Remedy IT Service Management	The BMC Remedy IT Service Management Connector no longer supports BMC Remedy IT Service Management Suite version 9.0 and 9.1.
SAP HR/HCM	The SAP HR/HCM Connector will no longer support SAPJCO version 3.0 version.

Dropped/Deprecated Connector Support

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

- ServiceNow Service Catalog Integration (LIC) Module
- ServiceNow Service Catalog API Integration Module
- ServiceNow IntegrationConfig-based Service Desk Integration Module
- Microsoft Forefront Identity Manager Integration
- Jive Connector

Deprecated: The following connectors and connector components are no longer supported:

- Yammer Connector

For more information on the support policy, see SailPoint Support Policy for Connectivity.

Important Upgrade Considerations

IdentityIQ 8.2 is a major release that contains numerous new features and capabilities across all areas of the product. A comprehensive plan should be created when upgrading that includes becoming familiar with the new features and changes, identifying use cases and how they are affected by the changes, creating a detailed strategy for migration of configuration and customizations, testing the upgrade process using data and system resources that are as close to the production environment as possible, and performing a complete deployment test cycle.

Security Upgrades

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

- bytebuddy 1.10.12
- Classloader bcel 6.5.0
- Apache commons collections4 4.4
- Apache commons dbcp2 2.7.0
- Apache commons io 2.7
- Apache commons lang3 3.10
- Apache commons pool 2.8.1
- ehcache 3.8.1
- failsafe 2.0.1
- geronimo annotation 1.3
- gson 2.8.6
- guava 30.1
- guice 4.2.3
- Hibernate 5.3.20
- httpcomponents client 4.5.13
- istack commons 3.0.11
- jasperreports-4.5.0
- Javassist 3.27.0
- Jawr core 3.9
- Jaxb jaxb-impl 2.3
- jersey 2.31
- jline 3.15.0

- json path asm 5.0.4
- Json path json-path 2.4.0
- Jstl jakarta.servlet.jsp.jstl-api 1.2.7
- log4j-2.13.3
- mysql-connector-java 8.0.20
- objenesis 3.1
- openpdf 1.3.18
- Opensaml 3.4.5
- Owasp-java-html-sanitizer 20200615.1
- quartz 2.3.2
- rhino 1.7.12
- slf4j 1.7.30
- spring 5.2.7
- Sshj eddsa 0.3.0
- Swagger 2.1.16
- threetenbp 1.5.0
- Velocity core 2.3
- vtd-xml 2.13.4

Encrypted Database Values

Passwords and other sensitive data entered in work items and other workflow forms are now kept in memory and persisted in the database as encrypted values. This data will need to be decrypted prior to use or referenced in custom workflow implementations or implemented business logic that it calls.

Task Result Field "Live"

A new boolean field named live has been added to the TaskResult object, `spt_task_result` in the database. It is set to `true` immediately after the TaskResult gets an executor, and is set to `false` immediately before the TaskResult has its executor removed when it finishes. The Reanimator now only looks at TaskResult objects with `live=true`.

Reminder Email Templates

You need to modify your existing reminder email templates to add the comment field.

```
 <Argument name='comment' type='string'> <Description>Optional comment from the
sender.</Description> </Argument>
```

jQuery Versions Older Than 3.5.0

The update of jQuery has breaking changes that could impact any customizations that use jQuery versions older than 3.5.0.

For details about the breaking changes see https://jquery.com/upgrade-guide/3.5/

Angular Upgrade

Angular was upgraded to version 1.8.0 to get a security fix in jqLite that is included in Angular. The jqLite security patch has a breaking change and could impact any customizations that use jqLite.

For more information about these changes see https://github.com/angular/angular.js/blob/master/CHANGELOG.md#180-nested-vaccination-2020-06-01

The Commons-collections Library Upgraded

The commons-collections library was upgraded to use the newer commons-collections4 package. This resulted in a method signature change on two public methods in SAPGRCIntegrationLibrary. The methods getRoleBusinessMap and getSAPEntlBusinessRoleMap now return Map instead of MultiMap. The format of the data in the Map is identical to the old MultiMap. If you have a custom workflow that calls these methods you might have to make an update.

Velocity Template Customizations

Class loading within Velocity templates now restricted to email bodies which prevents execution of code from filters. Customizations might have to be updated.

Default Number of Attachments

With this release of IdentityIQ the number of attachments that can be attached to a request item is defaulted to 5.

Import File Size Limit

Object imports in Batch Requests, and Entitlement Imports, now uses a file size limit property. The default value is 1000MB and can be configured in the IdentityIQ Configuration Miscellaneous tab under File Preferences.

FlexJSON Library Removal

FlexJSON library is removed from the product. All custom code that is serializing/deserializing JSON should use sailpoint.tools.JsonHelper class or Jackson library directly.

MySQL JDBC Driver Upgrade

The MySQL JDBC driver version included with IdentityIQ was updated from 8.0.18 to 8.0.19. You should always check with your database vendor for the latest compatible JDBC driver.

Oracle and MSSQL JDBC drivers were removed from the IdentityIQ distribution. You need to get these drivers from the database vendor.

Cross-Site Request Forgery (CSRF) Cookies Changes

Changes have been made to the Cross-Site Request Forgery (CSRF) cookies that IdentityIQ uses to ensure the requests it receives were initiated from the user who is logged in. If the session cookie is set to be secure in `web.xml`, then this cookie is also be secure. In addition, this cookie requires that requests come from only IdentityIQ's URL. While this change should be transparent to most users, a browser restart might be required to ensure the new cookies are picked up and used.

Session Management Update

This release contains a fix for an important security vulnerability. The vulnerability is related to session management and allows, under certain circumstances, for vertical privilege escalation by an authenticated user, including obtaining System Administrator privileges.

New MySQL JDBC Connection String Option

To resolve errors connecting to MySQL using the 8.0 JDBC driver, the **serverTimezone** option was added to the MySQL JDBC connection string with a value of UTC. Without this setting, the client will defer to MySQL to determine the value. By default, MySQL will look up the value from tables given the client's local timezone setting; however, out of the box, those tables are not populated and will cause a JDBC connection error. This change will only impact fields with a data type of TIMESTAMP. Internally, IdentityIQ uses the BIGINT data type to store timestamp data. If a custom field is created of type TIMESTAMP and the client timezone does not match the server timezone (UTC in this case), there will be a shift of X hours in the timestamp value as displayed by the MySQL console.

For example, if the client timezone is US/Eastern, saving data defined as a TIMESTAMP would add 4 hours to the value during the save process. If the data was saved at 11:00, running a select statement from the MySQL console would display a value of 15:00.

Maximum Number of Former Passwords Stored

The maximum number of former passwords stored now defaults to 20. For instructions on how to increase this number see the System Administration documentation.

Cross Site Request Forgery (CSRF) Protections

This release contains a fix for an important security vulnerability related to to Cross Site Request Forgery (CSRF) protections not being applied to all required URL paths.

Perform Maintenance Task Lock Handling

A new task will now determine the correct action for a Perform Maintenance task with an expired lock which previously would not resume a workflow.

Identity Attribute Update Processing

This version of IdentityIQ contains a change to how updates to identity attributes are processed when using IdentityIQs SCIM API. This change was made to allow Lifecycle Events to have access to the Identity attribute values prior to the change. This is done by creating an IdentityArchive object with the previous values. Since a new object is being created and saved to the database, this could have an impact on the overall performance of the SCIM update. It is not expected for the impact of this change to be noticeable, but in cases where it is, and when configured Lifecycle Events are not dependent on the previous identity attributes, the creation of the IdentityArchive object during a SCIM update is configurable. By default, the IdentityArchive creation during a SCIM update is enabled. To disable the creation of the IdentityArchive object during SCIM updates, the following attribute can be set on the SystemConfiguration object.

```
<entry key="scimTriggerSnapshots" value="false"/>
```

New Batch Processing Options

Added two configuration options

- allowSplitBatchEntitlementRequests: Turn off the extra parsing for multiple entitlements on a single line during batch processing.
- splitBatchEntitlementStr: Define a different delimiter other than the default pipe symbol.

Certification Revocation Processing

Certification revocations that result in manual workitems for object requests, like permissions on groups, no longer result in the certification item being marked as complete. The original behavior can be restored by adding the system configuration setting commitManualObjectRequests set to `true`.

AWS Plugin Versions

Use the latest version of the AWS plugin, version 1.0.3. The AWS SDK jar file, `aws-sdk-modules-1.0.jar`, is no longer included in IdentityIQ.

Rapid Setup Integration with Lifecycle Manager

Beginning with IdentityIQ 8.1p1, all Rapid Setup capabilities are available to all customers licensed for Lifecycle Manager. No additional license will be required.

Entitlement Update Workflow Approvals

Beginning with IdentityIQ 8.2, the Entitlement Update workflow will have approvals turned on by default. This can be changed in the workflow setup.

IQService

Ensure that the IQService host has the .NET framework version 4.8 installed before upgrading the IQService. Though the IQService is compatible with lower versions of .Net framework that is, 4.5.2 onwards, however, SailPoint recommends using the latest version of .Net framework 4.8 so that your environment can be completely aligned with subsequent future releases of IQService.

PAM Group Refresh Rule Update

The rule PAM Group Refresh has been updated to include logic for populating the managed attribute owner field. If you were using this rule it is advised that you look at this new logic and determine if it is applicable to your organization.

UI Configuration Filter Options

For Manage Access the Entitlements Classifications Filter and Role Classification Filter are not added to the UI Configuration during the upgrade process. This effectively disables them by default. To enable them, add the following two lines to the UI Configuration:

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

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

Report Header

Reports have been modified to include a header providing more information about the context of the report. By default, these headers are included. To remove the header from a defined report, uncheck the option to include report parameters in the Report Layout panel of the report.

Supported Platforms

Operating Systems

> **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.

- SUSE Linux Enterprise Server 15 and 12
- Windows Server 2016 and 2019
- CentOS 8.3 and 7.9

Application Servers

- Apache Tomcat 9.0 and 8.5
- Oracle WebLogic 14c and 12cR2
- IBM WebSphere 9.0
- JBoss EAP 7.3 and 7.2
- IBM WebSphere Liberty 20.0 and 19.0

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 for all application servers
- OpenJDK11 is now supported on all structures, but we have specifically tested against Adopt OpenJDK 11 for Windows and Red Hat OpenJDK 11 for Linux.

> JDKs are supported on 8 as needed by the specific application servers listed above. 6 and 7 are no longer supported.

Browsers

- Google Chrome Latest Version
- Internet Explorer New Chromium version of Edge
- Safari 14
- Firefox Latest Version

Mobile User Interface OS/Browser Support

- Android 11 on Chrome
- iOS 14 (beta) and 13 using Safari

Languages

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

Resolved Issues

Issue ID	Description
CONUMSHIAN-4151	SAP Portal - User Management Web Service Connector has enhanced steps for deploying **sailpoint_ume.sda** file as per SAP best practice.
CONUMSHIAN-3916	The SAP Direct Connector, SAP HR/HCM connector, and SAP GRC connector no longer cause SAPJCODestinationProvider exception when running Test Connection with older version of SAP JCO jar libraries.
CONUMSHIAN-3795	The SAP Connector now has the names of the attributes mentioned below same as the attribute names defined in the account schema when provisioning an account. 1. Telephone List 2. E-Mail List 3. X.400 List 4. Teletex List 5. Fax List 6. Pager SMS List 7. Printer List 8. Remote Function Call List 9. Remote Mail List 10. URL Homepage List The value for Pager SMS List will be in `<Pagerservice>#<PagerNumber>` format. The value for URL Homepage List will be in `<URl Type>#<urlvalue>` format.
CONUMSHIAN-3579	SuccessFactor Connector will no longer give us Connection reset error during test connection operation.
CONUMSHIAN-3446	SAP Direct and SAP HR Connector is now enhanced to handle test connection failure in case required libraries are missing in the library path of the IdentityIQ hosted on the Jboss server.
CONUMSHIAN-3341	[SECURITY] Directory traversal attacks security vulnerability in http jars is removed with the following library upgrades: • `httpclient-4.5.2.jar upgraded to httpclient-4.5.11.jar` • `httpcore-4.4.4.jar upgraded to httpcore-4.4.13.jar`

Issue ID	Description
CONUMSHIAN-2463	SAP Portal account aggregation does show correct count and no longer fails in aggregation and provisioning operations.
CONUMSHIAN-2366	The SAP Connector is now enhanced to remove all user groups assigned to a user.
CONUMSHIAN-937	SAP Portal aggregation will no longer fail in case parallel aggregation run is scheduled.
CONSEALINK-1877	ServiceNow Service Desk Connector does not escape special characters such as **&** and **'** while creating tickets on the ServiceNow target system.
CONSEALINK-1547	ServiceNow for Service Desk ticket Description field is now more descriptive and explanatory.
CONSEALINK-1422	IdentityIQ for Service Desk create ticket operation no longer fails when the ticket data has 2 dollar signs.
CONSEALINK-1405	ServiceNow Service Desk Integration Module (SOAP based) now no longer fails on Java 11.
CONSEALINK-1401	The ServiceNow Service Desk Integration Module (Integration Config based) now correctly finds the the `sp-axis2.xml` file.
CONSEALINK-1400	IdentityIQ for ServiceNow Service Desk no longer fails with connect timed out error for open proxy.
CONSEALINK-1395	The ServiceNow Connector no longer fails to read user's status when ServiceNow platform language is other than English.
CONSEALINK-1348	The ServiceNow Connector will now log a warning when user to role or user to group connection is not found.
CONSEALINK-1322	IdentityIQ for ServiceNow Service Desk no longer fails with `ClassCastException` while ticket creation and getting its status.
CONSEALINK-1257	ServiceNow Service Desk Application now no longer displays PeopleSoft's configuration settings in user interface.
CONPAMBAN-2137	For BMC Remedy IT Service Management Connector, **Site** information related attributes are mandatory for all provisioning operations starting from BMC Remedy IT Service Management Suite version 19.02 and above.
CONNAMDANG-3183	Amazon Web Services (AWS) Connector now supports the updated sdk module jar to enhance the security
CONNAMDANG-3140	JDBC Connector now connects to the MySQL DB with the upgraded driver `mysql-connector-java-8.0.20.jar`.
CONNAMDANG-3036	JDBC Connector now shows correct exception message if driver is not present in class path.

Issue ID	Description
CONNAMDANG-3017	Oracle NetSuite Connector can be configured to use REST Web Services with SuiteQL only for entitlement/group aggregation to prevent timeout issue.
CONNAMDANG-3012	For the Amazon Web Services (AWS) connector, the old jar is replaced with new `aws-sdk-module-3.0.jar` file that will enhance the security of customer data.
CONNAMDANG-3011	For the Amazon Web Services (AWS) Connector, the old jar is replaced with new `aws-sdk-modules-3.0.jar` file that will enhance the security of customer data.
CONNAMDANG-2848	The JDBC based Connectors now support loading certificates from custom truststore configured in application server through the **Additional connection properties**.
CONNAMDANG-2767	Oracle NetSuite Connector will now support XML special characters (“, ’, &) in Provisioning operations.
CONNAMDANG-2581	SQL Loader Connector now supports aggregating big data with complex joins.
CONNAMDANG-2445	PeopleSoft Connector no longer fails with length validation for domain connection password field while communicating to PeopleSoft Server.
CONNAMDANG-2177	Amazon Web Services Identity and Access Management (AWS IAM) Connector is not supported from this release. Applications already created for this connector on older versions of IdentityIQ are not expected to work after upgrading to this release.
CONNAMDANG-2088	Oracle NetSuite Connector now supports adding role to existing employee who does not have any prior role, provided employee has password and email set.
CONJUBILEE-1129	URL will be encoded now irrespective of the **throttleEnabled** flag value.
CONJUBILEE-1100	The Oracle Identity Manager Connector no longer throws NPE error while provisioning.
CONJUBILEE-1067	The Web Services Connector now extends the response headers list for rate-limiting parameters.
CONJUBILEE-1065	The Salesforce Connector now supports removing PermissionSetGroups in bulk (list).
CONJUBILEE-1038	The Web Services Connector now correctly throttles APIs for child endpoints.
CONJUBILEE-1031	The Salesforce Connector now supports provisioning or deprovisioning ManagedPackages in bulk (list).
CONJUBILEE-1018	The Box Connector now closes all the http connection after operation is completed.
CONJUBILEE-1013	The delta aggregation works fine now for Box connector in case of bulk changes at the target system.

Issue ID	Description
CONJUBILEE-1007	The Web Services account aggregation runs fine now with partitioning option even though partitions are not defined in the application.
CONJUBILEE-1002	The Web Services Connector now validates the OAuth2 and custom authentication configurations correctly during test connection operation.
CONJUBILEE-990	The Web Services Connector now handles empty response body correctly when paging is configured.
CONJUBILEE-975	The Web Services Connector now correctly handles the encoding of URL reserved characters in the query string.
CONJUBILEE-957	The Web Services Connector now validates the custom authentication configurations correctly during test connection operation.
CONJUBILEE-863	The identity refresh now works fine when account id contains non-English characters and application is configured with Cloud Gateway.
CONJUBILEE-790	The Web Services Connector now avoids infinite loop with paging via response headers using before and after operation rules.
CONJUBILEE-775	The Web Services Connector now correctly respects the success status codes provided in the end point configuration.
CONJUBILEE-766	The Salesforce Connector now supports provisioning and deprovisioning of public group containing apostrophe in the name.
CONJUBILEE-764	The Salesforce Connector now deciphers error messages during provisioning operation correctly.
CONJUBILEE-748	The Web Services Connector no longer removes fields with empty values from the request body.
CONJUBILEE-745	The Web Services Connector now correctly handles backslash character in request body.
CONJUBILEE-731	The Web Services Connector now supports updating the `processedResponseObject` in the after operation rule.
CONJUBILEE-720	The Web Services Connector's **After Operation Rule** now handles the response headers correctly.
CONJUBILEE-712	The Web Services Connector now correctly parses XML response even when response body is empty.
CONJUBILEE-707	The Salesforce Connector now escapes special characters like **<> &** in Account Search Query as well as Group Provisioning.
CONJUBILEE-706	The Web Services Connector now skips malformed accounts and continues the aggregation.
CONJUBILEE-671	The Web Services Connector now supports updating request headers using paging steps mechanism.

Issue ID	Description
CONJUBILEE-670	The Web Services Connector now correctly replaces the multivalued plan attributes in the JSON request body.
CONJUBILEE-641	The Web Services Connector's **After Operation Rule** now handles resolved placeholder values correctly.
CONJUBILEE-638	The Web Services Connector now correctly encodes URL containing special character ':'.
CONJUBILEE-633	The Web Services Connector now gracefully handles any incorrect JSON attribute paths in the endpoint's response mapping configuration.
CONJUBILEE-630	The REST Web Services Connector now correctly evaluates the value of **Account Enable Status** attribute.
CONJUBILEE-622	The Web Services Connector correctly executes API requests for user-defined group object related operations.
CONJUBILEE-610	The Web Services Connector now picks native identity from the plan if **Get Object** endpoint is not configured and identity attribute is not present in the **Create Account** operation response.
CONJUBILEE-597	The Salesforce Connector will not support out of the box salesforce partner stubs.
CONJUBILEE-578	The Web Services Connector now supports disabling cookies while executing HTTP requests.
CONJUBILEE-566	The Web Services Connector now supports single request for change password and update operations.
CONJUBILEE-565	The Web Services Connector will not trim the "=" character, if it is last character in the query parameter.
CONJUBILEE-559	The Web Services Connector has now got improved performance by better HTTP connection handling.
CONJUBILEE-558	The Workday Connector has now improved performance due to better HTTP connection handling.
CONJUBILEE-554	The Web Service Connector now parses response correctly when there is list of maps in the response.
CONJUBILEE-551	The Web Services Connector now supports loading certificates from custom truststore configured in application server.
CONJUBILEE-550	The Web Services Connector now correctly handles the ')' within the string literal in paging configuration tab.
CONJUBILEE-545	While using Cloud Gateway as proxy, now account is not deleted while doing any update operation.

Issue ID	Description
CONJUBILEE-543	The AirWatch Connector now skips the devices in case of there is data issue during aggregation.
CONJUBILEE-533	The Web Services Connector now handles paging even if root path is empty in the response mapping.
CONJUBILEE-517	The SCIM Connector now handles chunked response on OpenJDK version 11.0.6.
CONJUBILEE-507	The WebServices Connector now supports null http response body with custom error messages.
CONJUBILEE-494	Web Services Connector now, during paging, correctly resolves initial page offset and page size, provided in the endpoint configuration.
CONJUBILEE-491	The Web Services Connector now correctly handles special characters in context URL.
CONJUBILEE-463	The Box connector access token will now be generated consistently using JWT.
CONJUBILEE-422	The Web Services Connector now updates entitlements even if Update account endpoint is not configured.
CONJUBILEE-395	The Salesforce Connector will now successfully complete the provisioning for entitlements containing a comma.
CONHOWRAH-2866	[SECURITY] IQService now supports configuring maximum wait time before terminating the inactive connections while reading requests. Default timeout is 15 seconds.
CONHOWRAH-2786	The Active Directory Connector no longer supports Microsoft Exchange Server version 2010 which has reached its end of support.
CONHOWRAH-2760	The Active Directory Connector now supports rollback of created account in case provisioning of one or more requested attributes fails during provisioning.
CONHOWRAH-2673	The RSA Authentication Manager Connector does not require RSA version specific application configuration attribute named **rsaVersion** anymore which is now obsolete.
CONHOWRAH-2634	The RSA Authentication Manager connector now supports loading certificates from custom truststore configured in application server.
CONHOWRAH-2579	The Active Directory Connector now only supports DirSync as delta aggregation mode.
CONHOWRAH-2541	The Cloud Gateway now works as expected during delta aggregation when single group membership is removed for an Active Directory user.
CONHOWRAH-2416	The Active Directory connector no longer connect to Read Only Domain Controllers (RODC) for provisioning operations using serverless binding.

Issue ID	Description
CONHOWRAH-2398	The Active Directory Connector now displays appropriate error message when service account is not configured in required format during provisioning.
CONHOWRAH-1529	The Active Directory Connector now supports reusing of Ticket Granting Tickets (TGT) for Kerberos authentication during aggregation tasks to optimize on the usage of TGT.
CONHELIX-2580	With the enhanced API Rate Limiting mechanism, **maxPermissibleCalls** is no longer applicable for Okta connector.
CONHELIX-2460	The Test connection operation for **openconnector** will no longer fail on OpenJDK 11.
CONHELIX-2393	The Unix based connectors (AIX, Linux and Solaris) are now enhanced to aggregate multi-lined alias or commands from the **sudoers** file.
CONHELIX-2374	The Linux Administrator will no longer see the password in plain text in the history file for password change operation from the Linux Connector.
CONHELIX-2312	The Duo Connector now manages Duo administrators without associated phone number.
CONHELIX-1798	The Epic Connector now supports proxy authentication.
CONHELIX-1792	The Epic Connector now supports JDK 11.
CONHELIX-1721	Create account operation no longer fails for Duo source with error `Native Identity should not be null or empty.`
CONETN-3488	The Workday Connector correctly aggregates the multivalued attributes of an account when account aggregation is performed.
CONETN-3481	During linked mailbox provisioning when **msExchHideFromAddressLists** flag is set to `True`, all Active Directory attributes values which are passed during provisioning operation would be shown up on the user interface.
CONETN-3467	Redundant access to multiple child endpoint is removed during account or group aggregation for Rest Web Services Connector.
CONETN-3462	Microsoft SQL Server Connector no longer fails when aggregating accounts from a database having special characters in its name.
CONETN-3449	The JDBC Connector now automatically retrieves an object after it has been provisioned when a **getObjectSQL** query is configured in the application.
CONETN-3440	The SAP Portal-User Management Web Service Integration Module no longer fails when aggregating accounts from a SAP Portal server whose backend is LDAP. The updated Smart Data Access file (`sailpoint_ume.sda`) provided with this release in **iiqIntegration-SAPPortalSdaFile** zip file must be deployed on the SAP Portal server for account aggregation to work correctly.
CONETN-3438	Custom Krb file can be used for the strong authentication in IdentityIQ. Custom krb file path should be passed as system property in the application server.

Issue ID	Description
CONETN-3437	The SAP GRC Connector no longer fails with an **ArrayIndexOutOfBoundsException** when aggregating accounts containing an empty Profile or Role.
CONETN-3435	The SAP GRC Connector no longer fails when a webservice response returns error message during a test connection operation.
CONETN-3422	The Workday Connector now skips the accounts having a null identityAttribute value during aggregation.
CONETN-3413	Novell eDirectory LDAP Connector no longer overrides the default **passwordExpirationTime** time set on the Novell eDirectory during self-change password.
CONETN-3406	The Workday Connector now shows more meaningful logs when a service account is missing the Get_Workers API permission while performing an aggregation accounts operation.
CONETN-3401	The PeopleSoftHRMS Connector no longer fails with `java.lang.reflect.InvocationTargetException` when aggregating accounts.
CONETN-3393	The SAP Direct Connector no longer fails when aggregating roles and profiles with an empty SUBSYSTEM value.
CONETN-3391	The Oracle E-Business Connector now updates the WHO columns correctly when performing a provisioning entitlement operation.
CONETN-3390	REST Webservices Connector will now ignore null or empty claims in oAuthJwtPayload application attribute for generating JWT assertions.
CONETN-3386	The SAP HR/HCM Connector no longer skips future dated accounts when a custom aggregationFilterBapi is configured during aggregation.
CONETN-3382	Active Directory Test Configuration now displays proper message indicating right suggestions when IQservice is configured with Domain Configuration as TLS enabled and domain certificate is missing in trusted store on IQService host.
CONETN-3380	The SharePoint Online Connector now supports retry mechanism for account aggregation.
CONETN-3378	The SAP Direct Connector no longer throws a NullPointerException when aggregating accounts from an SAP Server having no License data.
CONETN-3376	The Windows Local Connector now correctly fetches the value PasswordUnchangeable from the managed system during WinLocal account aggregation.
CONETN-3374	The Azure Active Directory Connector now retries the failed request after correct time set in the **Retry-After** flag in the response header during aggregation.

Issue ID	Description
CONETN-3370	The Workday Connector no longer logs the service account password in the debug logs when the password contains special characters.
CONETN-3368	The Workday Connector no longer fails when aggregating accounts for an application whose service account has a password containing special characters.
CONETN-3349	IQService now successfully connects with TLS from IdentityIQ when certificate SAN is in foreign language.
CONETN-3348	REST WebServices Connector no longer fails with a NullPointerException during invocation of an endpoint if it's body has null value configured under the form-data.
CONETN-3347	After deleting an Active Directory account, re-provisioning the account with the Active Directory Connector will now create account on managed system properly when identityAttribute is set as objectGuid.
CONETN-3344	The SAP Direct Connector no longer displays a warning message when de-provisioning a role from an SAP CUA managed system.
CONETN-3341	An informative message instead of a generic message will now be shown when a create provisioning operation for Active Directory Connector fails to update some attributes and account was created successfully at managed system.
CONETN-3338	Azure Active Directory Connector now supports updating immutable Id for a guest account or domain account.
CONETN-3337	The ServiceNow ServiceDesk Integration now supports retrying the failed provisioning requests based on a configurable retryableErrors list.
CONETN-3331	Azure Active Directory Connector no longer fails while provisioning owners to a group using their objectID instead of UPN.
CONETN-3326	The Workday Connector now includes Contract Contingent Worker business process in FUTURE_ACTION and FUTURE_DATE xpaths.
CONETN-3323	The Mainframe Connectors no longer causes entitlement attributes to be assigned to all entitlements when provisioning a combination of entitlements with attributes and entitlements without any attribute for an account.
CONETN-3322	The Lotus Domino Connector now fetches the groups of the accounts without certifier along with all the available username's on the managed system during account aggregation.
CONETN-3314	Delta account aggregation for Active Directory Connector now brings complete resource object if any changes happened in attribute at managed system for the list provided as part of **attributeListForFullROinDelta** in application configuration.
CONETN-3304	The Microsoft SQL Server Connector no longer fails with a `NullPointerException` when performing an account aggregation.

Issue ID	Description
CONETN-3293	The `IQService.exe -v` command will now display the tracelevel. Additionally IQService log level values are as follows (0-3): * 0=off * 1=error * 2=info * 3=debug Default : 2
CONETN-3285	The SAP HR Connector now correctly aggregates the delta considering the value for **terminationOffset** key configured in the application.
CONETN-3282	REST WebServices Connector now correctly sets attribute level result during provisioning as **retry** when error is configured as retryable in application.
CONETN-3280	The Workday Connector no longer fails with `Too many files open` error when provisioning accounts in bulk.
CONETN-3273	The Azure Active Directory Connector now displays proper response code in case of error, and retry mechanism works for aggregation tasks.
CONETN-3269	By default Active Directory Connector would display the values of **objectguid**, **objectSid**, **msExchMailboxGuid**, **mS-DS-ConsistencyGuid**, **sIDHistory**, **msExchMasterAccountSid** in a format that would require additional binary/Sid/Guid attributes in the application configuration page as follows: • attrsDisplayInBinaryFormat • attrsDisplayInSIDFormat • attrsDisplayInGUIDFormat For more information, see the Active Directory Connector Guide.
CONETN-3268	The System Cross-Domain Identity Management 2.0 Connector no longer invokes extra PUT call while assigning groups to a user.
CONETN-3267	The SAP Direct Connector no longer fails when aggregating accounts from a SAP Server with Payroll module is hosted on cloud.
CONETN-3265	The Azure Active Directory Connector now considers an application-level flag **createGroupTimelag** while creating a group and no longer causes `ObjectNotFoundException`.
CONETN-3264	[SECURITY] The SAP GRC Integration no longer provisions an access request with a rejected approval.
CONETN-3263	The SAP Direct Connector no longer trims value of Parameter attribute when aggregating an account.

Issue ID	Description
CONETN-3261	REST WebServices Connector will now print logs in before and after operation rule when logger for `sailpoint.connector.webservices.v2.RequestOrchestratorV2` is enabled.
CONETN-3258	The Active Directory Connector now pulls the correct data for extensionData attribute when running account group aggregation.
CONETN-3255	The Mainframe Connectors no longer causes `StringIndexOutOfBoundsException` when performing Test Connection for TLS communication with certificate CN at the end of a cert subject.
CONETN-3236	The Azure Active Directory partition aggregation task no longer loops infinitely, when User Partitions are not defined in application.
CONETN-3230	The Active Directory Connector now successfully provisions an account with trailing spaces in its OU name.
CONETN-3229	IQService now throws an exception message instead of exiting abnormally while running WinLocal account and group aggression for non local members.
CONETN-3222	The Azure Active Directory Connector no longer fails to provision Guest Users while using **userFilter**.
CONETN-3221	The Microsoft SQL Server Connector no longer causes `ConnectorException` when running account aggregation on a database with special characters in its name.
CONETN-3200	The SunOne LDAP Connector no longer causes an `IllegalArgumentException` when aggregating an account with **guid** in its DN.
CONETN-3198	The Active Directory Connector no longer displays **attributeAssignment** for underlying entitlements when they are provisioned through IdentityIQ roles with **setAttributeLevelResult** set as **true**.
CONETN-3196	The Microsoft SharePoint Server Connector no longer causes the memory consumption for IQService to spike when running account or account group aggregation with the value of **manageSubsite** set as **true**.
CONETN-3192	The Microsoft SharePoint Server Connector now has an improved performance for account aggregation when **manageSubsite** has a value set to **true**.
CONETN-3191	The Microsoft SQL Direct Connector no longer fails when performing a provisioning operation on a SQL Server with case sensitive collation property.
CONETN-3187	The Workday Connector no longer pulls partial resource objects when aggregating the delta for future hires with a hire date beyond the effective date.
CONETN-3179	The Active Directory Connector now runs the account aggregation successfully in the absence of an account group schema in the application.

Issue ID	Description
CONETN-3176	The Microsoft SharePoint Server Connector now has a configurable key **skipIncludeSiteValidation** to enable a lightweight Test Connection and skip validating the site list included in the application configuration.
CONETN-3166	The Azure Active Directory Connector can now provision an Azure Guest account with an extension attribute.
CONETN-3164	Account aggregation for the SharePoint Server Connector will not fail for the site having Groups in its name.
CONETN-3160	The Microsoft SharePoint Server Connector no longer loses the data when running account aggregation with userIndex set to a value less than the total number of accounts in a site collection.
CONETN-3156	The PeopleSoft Direct Connector no longer fails with a ConnectorException when provisioning the IDType attribute for an account.
CONETN-3152	The SQL Loader Connector no longer skips unstructured data when aggregating data from the source file.
CONETN-3150	The SuccessFactors Connector now correctly displays the Department attribute of an employee when Department data is fetched in multiple pages.
CONETN-3138	The ServiceNow Connector now correctly displays timezone attribute for US/Central region under create provisioning policy form.
CONETN-3132	The SAP Direct Connector now aggregates the Parameters attribute of an account correctly.
CONETN-3129	The IQService no longer terminates abnormally when resetting the users passwords in bulk.
CONETN-3123	The Windows Local Connector now correctly aggregates non-local group memberships when running account and account group aggregation.
CONETN-3122	The SAP HANA Connector now aggregates the accounts successfully when the User ID of native accounts has a value outside the integer range.
CONETN-3118	The LDAP Connector now has enhanced performance for account aggregation.
CONETN-3109	The Workday Connector now correctly aggregates future-terminating workers for whom the future date is set to today in the Workday natively.
CONETN-3102	The Oracle E-Business Suite Connector no longer updates the **Description** attribute when de-provisioning a role or a responsibility for a user.
CONETN-3098	The Mainframe Connector now throws appropriate error message when attribute type is wrongly defined in Application/Source.
CONETN-3092	The SAP HR Connector no longer fails with a `ConnectorException` when aggregating accounts having a null Status value.

Issue ID	Description
CONETN-3089	The SAP HR Connector now correctly aggregates all attributes of Communication data even when the application is configured with a language other than EN.
CONETN-3088	The Service Now Connector now aggregates **sysparm_fields** attributes during single account aggregation.
CONETN-3084	The Azure Active Directory Connector no longer causes `AuthenticationFailedException` when authenticating a user using Pass Through Authentication with special characters in the password.
CONETN-3079	The Active Directory Connector no longer causes InvalidNameException when pulling an object with double quotes in the OU.
CONETN-3078	The Azure Active Directory Connector now displays a correct error message when running delta aggregation with a mismatched version of API.
CONETN-3070	The Azure Active Directory Connector now considers an application-level flag **createAccountTimelag** when provisioning an account and no longer causes `ObjectNotFoundException`.
CONETN-3067	The IQService no longer crashes with `SEHException` when provisioning users in bulk using multi-threading.
CONETN-3063	The IQService no longer terminates abnormally when resetting a user password using self service.
CONETN-3062	The Active Directory Connector now logs `NoInitialContextException` as just a warning message instead of an error.
CONETN-3060	The IBM Lotus Domino Connector no longer causes a `NullPointerException` when aggregating the accounts with the value of **indexDB** set to **Y** in the application configuration.
CONETN-3058	The SAP HR/HCM Connector now aggregates all future hires when aggregating the accounts using partitioning with a blank value of future offset in the application configuration.
CONETN-3053	The ServiceNow Connector now correctly considers the JVM argument to bypass the proxy when testing the connection.
CONETN-3051	The Azure Active Directory Connector now returns appropriate error messages when provisioning entitlements.
CONETN-3050	The Active Directory Connector no longer causes the **Test Connection** to pass with incorrect or invalid Exchange configurations. To validate the Exchange configurations during **Test Connection**, the **isExchangeValidationEnable** attribute must be set to **true** in the application definition.
CONETN-3044	The Active Directory Connector no longer has mis-spelled words in its error and exception messages in the logs.

Issue ID	Description
CONETN-3042	The Microsoft SQL Server Connector no longer causes `NullPointerException` when deleting an account with UTF-8 characters in the account name.
CONETN-3039	The Microsoft SharePoint Server Connector now correctly populates the UserName attribute for an account with **sAMAccountName** when aggregating the accounts.
CONETN-3030	The Workday Connector now correctly aggregates future-terminating workers using Organization_Reference_ID.
CONETN-3029	The Mainframe Connectors now support loading certificates from a custom TrustStore in WebSphere when using TLS to communicate between IdentityIQ and Connector Gateway.
CONETN-3028	The Active Directory Connector now provides an option **retryChangPasswordWithKerberos** that can be configured using the application debug page to control the behavior to retry self-change password for policy violation errors.
CONETN-3023	The ServiceNow Connector now aggregates all the accounts from native ServiceNow correctly. The ServiceNow Connector now aggregates all the accounts from native ServiceNow correctly.
CONETN-3016	The Azure Active Directory Connector no longer provisions a non-requestable entitlement as requestable.
CONETN-3008	The AWS Connector no longer fails when performing the **Test Connection** with IdentityIQ connected to the internet using a proxy.
CONETN-3000	The Workday Connector now correctly pulls **Future_Action**, **Future_Date** and **Last_Day_of_Work** attributes for rescinded and corrected worker records.
CONETN-2996	The LDAP Connector no longer fails when provisioning an account with case-sensitive **objectClass** attribute in the account schema.
CONETN-2995	The LDAP Connector no longer fails when provisioning an entitlement with escaped characters.
CONETN-2985	The Azure Active Directory Connector no longer fails when running Delta aggregation to aggregate accounts or account groups with special characters using **userFilters** string.
CONETN-2983	The Workday Connector now supports retrying failed aggregation requests based on configurable **retryErrors** list and **retryCount** value.
CONETN-2976	The JDBC Connector no longer skips and deletes entitlements from a group-type schema when aggregating entitlements for multi-group schema's using merging.
CONETN-2971	The GSuite Connector now supports provisioning an account with multi-valued complex attributes.

Issue ID	Description
CONETN-2969	The SAP Direct Connector now provides an option **enableSelfService** that can be configured using the application debug page to control the behavior of enabling an account using self-service.
CONETN-2968	The Active Directory Connector now logs and displays a warning `sAMAccountName is not provided. samAccountName will be generated randomly by Active Directory` when provisioning an account without **samAccountName**.
CONETN-2967	The Microsoft SharePoint Server Connector can now be configured to retry account group aggregation in case of failure.
CONETN-2965	The Delimited File Connector no longer fails when running partitioned aggregation to transport a file using SFTP.
CONETN-2961	The IQService trace logging now correctly rolls the logs when performing bulk operations.
CONETN-2954	The Oracle E-Business Suite Connector no longer assigns additional Oracle E-Business Responsibilities with same Responsibility ID but with different Application IDs when provisioning an entitlement to a user.
CONETN-2951	The Workday Connector no longer causes a `NullPointerException` when running account aggregation using generic partitioning.
CONETN-2947	The SuccessFactors Connector no longer fails when updating the username for an Inactive employee.
CONETN-2946	Active Directory Connector will now allow **accountExpires** attribute value as **never** while provisioning when **timeZone** attribute is present in Active Directory application configuration.
CONETN-2944	The Oracle Database Connector now supports revoking direct permissions of a user via IdentityIQ Certification.
CONETN-2940	The SAP Direct Connector now retrieves the correct long description of a role that has more than one entry for the native long description.
CONETN-2933	The IBM Lotus Domino Connector now correctly displays the error message when disabling an account that cannot be disabled due to unavailability of space in the native Deny List groups.
CONETN-2922	The Active Directory Connector now correctly sets the status of the request when an account is provisioned successfully but not all of its attributes.
CONETN-2915	The SAP Portal-User Management Web Service Integration Module now logs only the required log statements by default. The Smart Data Access file (sailpoint_ume.sda) provided with this release in **iiqIntegration-SAPPortalSdaFile** zip file must be deployed on the SAP Portal server for it to work.

Issue ID	Description
CONETN-2912	The LDAP connector no longer inadvertently converts the values of **true** and **false** to all upper case when provisioning the attributes defined as string types.
CONETN-2911	The IBM Lotus Domino Connector now comes with a more resilient Account aggregation. It no longer causes a `ConnectorException` when aggregating account attributes.
CONETN-2908	The Oracle E-Business Suite Connector now supports configuring a custom Application ID and a custom Responsibility ID for the provisioning operations.
CONETN-2905	The Workday Connector no longer causes a `NullPointerException` when the phone number is updated through the user interface and through attribute synchronization.
CONETN-2898	The G Suite Connector no longer causes a `ConnectorException` when aggregating account groups with a group having special characters in its Email address.
CONETN-2890	The ServiceNow Connector no longer causes the Pagination error when running aggregation with very large value in the **sysparm_fields** entry.
CONETN-2887	The SuccessFactors Connector no longer causes a `ConnectorException` when provisioning Country Code and Business Phone for an employee to the native SuccessFactors system that has configured Country Code as a mandatory field.
CONETN-2876	The LDAP Connector now successfully unlocks a locked account in SunOne versions 6+ including ODSEE 11g. The **lockAttr** key must have **pwdAccountLockedTime** as its value and **lockVal**, **unlockAttr** and **unlockVal** keys must be removed from the application configuration.
CONETN-2861	The connectors that use IQService to communicate with respective native systems now provide an option **IQServiceResponseTimeout** that can be configured using the application debug page to timeout the connection when there is no response received from the IQService.
CONETN-2836	The Workday Connector no longer removes secondary phone contacts when provisioning primary phone contact.
CONETN-2833	The Workday Connector now displays meaningful debug logs when aggregating schema attributes not available in native Workday.
CONETN-2758	The SAP Portal Connector now supports Secure and Http only cookies when running account and account group aggregation.
CONETN-2744	The SAP Portal-User Management Web Service Integration Module no longer fails when aggregating accounts with one or more trailing spaces. The updated Smart Data Access file (`sailpoint_ume.sda`) provided with this release in **iiqIntegration-SAPPortalSdaFile** zip file must be deployed on the SAP Portal server for account aggregation to work correctly.

Issue ID	Description
CONETN-2726	The JDBC Connector no longer fails when running delta aggregation to aggregate the delta using a Stored Procedure.
CONETN-2709	The Sybase Connector now displays the correct status for an account.
CONETN-2700	The Oracle E-Business Suite Connector now enables a user to change her password natively after IdentityIQ Admin Password Reset.
CONETN-2626	The Delimited File Connector no longer fails when running partitioned aggregation to transport a file using SCP.
CONETN-2619	The JDBC Connector now correctly updates the links for all attributes of an Identity when a provisioning operation is performed.
CONETN-2615	The Oracle E-Business Suite Connector now allows provisioning a null end date for an account.
CONETN-2602	The SAP Connector no longer fails when provisioning an account with **1.234.567,89** or * as the value of Decimal Notation.
CONETN-2589	The Delimeted File Connector is no longer blanked out when object type value is **app**.
CONETN-2588	Application configuration screen for JDBC Connector will no longer be blanked out when object type value is **app**.
CONETN-2398	The SuccessFactors Connector now provides options to configure Picklist when aggregating external code for reference data.
CONETN-2091	The Oracle Database Connector now correctly provisions two different entitlements to two accounts for the same Identity in one provisioning operation.
CONCHENAB-4098	The Oracle Fusion HCM Connector is now able to fetch the BIRTH_DATE attribute.
CONCHENAB-4070	The Active Directory Connector now correctly performs provisioning operations via the Cloud Gateway when provisioning plan contains followers attribute.
CONCHENAB-4069	The Oracle Identity Manager Integration does not expect to provide the basic credentials information to authenticate the Weblogic application server.
CONCHENAB-4068	The Zoom connector now successfully aggregates attribute **login_types**.
CONCHENAB-3989	The **Test Connection** operation on applications configured with Cloud Gateway using wrong credentials now displays proper error message.
CONCHENAB-3982	The entitlement deprovisioning works fine now while using Cloud Gateway and sunrise-sunset feature.
CONCHENAB-3971	The group aggregation now works fine for Workday Accounts Connector.
CONCHENAB-3931	The Active Directory partitioned aggregation now works fine when configured with Cloud Gateway.

Issue ID	Description
CONCHENAB-3917	The System for Cross-Domain Identity Management 2.0 Connector now correctly verifies the SSL certificate of the managed system.
CONCHENAB-3868	The System for Cross-Domain Identity Management 2.0 Connector now provides information on the target SCIM 2.0 service provider configuration.
CONCHENAB-3863	The Workday Accounts Connector now does not generate new password when **GENERATE_RANDOM_PASSWORD** is set as **false**.
CONCHENAB-3854	The Workday Accounts Connector now supports camel case XPath for fetching Supervisory organization.
CONCHENAB-3853	The System for Cross-Domain Identity Management 2.0 Connector now uses **replace** operation instead of **add** for updating existing attributes.
CONCHENAB-3836	The Oracle Fusion HCM Connector now returns only single record for rehired person.
CONCHENAB-3822	The Oracle Fusion HCM Connector now correctly aggregates the employees with person number starting with '00'.
CONCHENAB-3820	The Salesforce Connector now allows disabling emails while user creation by setting **disableUserCreationEmail** to **true**.
CONCHENAB-3815	The Web Services Connector restricts logging of secret/sensitive information.
CONCHENAB-3782	The Oracle Identity Manager Server Integration now runs fine on application server using JDK version lower than 1.8.
CONCHENAB-3780	The Oracle Fusion HCM Connector now ignores the active assignment of past terminated users.
CONCHENAB-3728	The ISIM integration now decrypts password if provided in encrypted form.
CONCHENAB-3719	The Workday Connector now will support **Contract Contingent Worker** as default event in future hire events list.
CONCHENAB-3696	The System for Cross-Domain Identity Management 2.0 Connector now handles special characters during provisioning operation.
CONCHENAB-3693	The performance is improved for connector classloader during identity refresh.
CONCHENAB-3687	The System for Cross-Domain Identity Management 2.0 Connector now successfully regenerates the access token when it receives an empty message in an exception.
CONCHENAB-3681	The Workday Connector now uses **FILE_NUMBER** as display attribute in schema instead of **WORKER_NAME**.
CONCHENAB-3631	The Workday Connector now correctly fetches the the custom attributes for converted workers and future dated workers in full and delta aggregation.
CONCEHANB-3619	The System for Cross-Domain Identity Management 2.0 Connector now excludes read only attributes in PATCH request.

Issue ID	Description
CONCHENAB-3610	The System for Cross-Domain Identity Management 2.0 Connector now supports **AND** operator in filters.
CONCHENAB-3607	The Oracle Fusion HCM Connector now aggregates the terminated employee on the current date.
CONCHENAB-3586	The System for Cross-Domain Identity Management 2.0 Connector now performs provisioning operation successfully after access token regeneration.
CONCHENAB-3575	The performance of Oracle Fusion HCM Connector is now improved while aggregating future hires.
CONCHENAB-3571	The Cloud Gateway is now able to correctly load the application XML from cache.
CONCHENAB-3559	The System for Cross-Domain Identity Management 2.0 Connector generates new OAuth2 access token each time for test connection operation.
CONCHENAB-3555	Oracle HCM Fusion Connector now shows recent active and primary assignments present for the worker record.
CONCHENAB-3551	The System for Cross-Domain Identity Management 2.0 Connector now allows setting attribute value as empty value.
CONCHENAB-3518	The System for Cross-Domain Identity Management 2.0 Connector now aggregates the read only groups and entitlements.
CONCHENAB-3492	The System for Cross-Domain Identity Management 2.0 Connector no longer causes a `NullPointerException` when aggregating accounts with garbled value for **schemaPropertyMappings**.
CONCHENAB-3487	The Workday Connector now handles Effective offset set to zero.
CONCHENAB-3226	IdentityIQ now uses TLS version 1.2 as the default protocol while running on WebSphere application server.
CONBOGIBEE-2167	Account search query has been improved to avoid any unwanted filtering of accounts.
CONBOGIBEE-2162	The **Atlassian Suite - Cloud** and **Atlassian Suite - Server** Connectors now have better handling for aggregating large number of groups during group aggregation.
CONBOGIBEE-1948	The BMC Remedy IT Service Management Connector now correctly handles disabled accounts during get object operation.
CONBOGIBEE-1797	The BMC Remedy IT Service Management Connector is now enhanced to use more efficient queries for optimizing the performance during account aggregation.
CONBOGIBEE-1730	The Azure Active Directory Connector now masks sensitive application attributes like refresh token before logging at TRACE level.

Issue ID	Description
CONBOGIBEE-1640	The BMC Remedy IT Service Management Connector now supports updating account attribute while assigning the group memberships.
IIQCB-2037	In the Role Editor, pressing the **ENTER** key from within a text area, will no longer launch the forms popup.
IIQCB-2594	Role capability changes are now displayed in role edit approval
IIQCB-2693	In the Role Editor, the word 'role' is now translated with the rest of the message.
IIQCB-2801	Access Request page now renders correctly when the AccessRequestType contains a space.
IIQCB-2855	Alert definition required fields no longer outlined in red when loading in Internet Explorer and Edge.
IIQCB-2871	Role edit approvals now displays authorized scope difference.
IIQCB-2883	On the IdentityIQ Configuration page, the Identity Risk label now displays on one line in the Japanese translation.
IIQCB-2892	The **Edit** report button is no longer displayed if the user does not have permission to edit the task definition.
IIQCB-2893	On the Manage User Access page, the **Find User Access** now functions as intended without a severe error.
IIQCB-2980	[SECURITY] The BeanShell remote server mode capability has been disabled and is no longer available.
IIQCB-3306	Saving a business role with a required IT roles now saves without exception.
IIQCB-3339	The Full Text Index Refresh task is now fault tolerant. A new index is created only when the task has run successfully. This new behavior prevents incomplete or truncated indexes.
IIQCB-3341	[SECURITY] Passwords and other sensitive data entered in work items and other workflow forms are now kept in memory and persisted in the database as encrypted values. This data will need to be decrypted prior to use or referenced in custom workflow implementations or implemented business logic that it calls.
IIQCB-3384	Unpartitioned tasks will not be unnecessarily terminated when the Reanimator service runs.
IIQCB-3409	Exporting plugins through the console, no longer throw ZipException and exports plugin.
IIQCB-3411	Introduced a new ruleRunnerPoolConfig to support detailed configuration of the rule runner beanshell manager pool.
IIQCB-3417	The Copyright footer is now displayed on Application pages.
IIQCB-3418	Running the Work Item Archive Report now releases the datasource connection after running the report.

Issue ID	Description
IIQCB-3429	Completion comments now show in Access Request Report.

IIQCB-3591	8.2 includes new 'Role Classifications' and 'Entitlement Classifications' filters on the Manage User Access screen. When upgrading to 8.2 these filters are not enabled by default. To enable, the following two entries need to be manually added to the UI Configuration:
	`<entry key="enableEntitlementsClassificationsFilter" value="true"/>`
	`<entry key="enableRoleClassificationsFilter" value="true"/>`

IIQCB-3620	Reports now export column headers when the report is empty.
IIQCB-3652	Custom workflows having multiple forms with at least one postback field no longer experience issues with a **Submit** button unexpectedly showing as disabled.
IIQCB-3658	After an upgrade, certifications now display correctly when the certification was created in the previous version of IdentityIQ and a role contained within the certification was deleted prior to the upgrade.
IIQCB-3664	Tasks with an assigned host will not improperly be marked as still running when complete.
IIQCB-3745	Quartz scheduler settings in `iiq.properties` are now honored.
IIQCB-3748	Provisioning process for OIM-Connector applications no longer throws an exception
IIQMAG-2806	[SECURITY] The list of certification items now only includes the requested certification items.
IIQMAG-2808	[SECURITY] No longer able to view details about managed attributes or roles for which a user does not have permissions.
IIQMAG-2822	[SECURITY] HTML tags in the body of a reminder email template are no longer rendered in the message field in the reminder dialog or in the emails received.
IIQMAG-2836	Priority on workItem can no longer be set when priority editing is disabled.
IIQMAG-2935	A bulk reassignment email will be sent for self certifications when a staged certification is activated.
IIQMAG-3008	If the same identity has simultaneous access requests in operation, IdentityIQ no longer loses internal representation of account updates between those requests.
IIQMAG-3095	During aggregation, attribute assignments are now filtered out of the list of added values in native change detections.

Issue ID	Description
IIQMAG-3096	Effective Access SOD policy now correctly detects violations regardless of whether that access was granted directly or indirectly.
IIQMAG-3098	[SECURITY] the Classmate library was upgraded to version 1.5.1.
IIQMAG-3110	[Security] jQuery was updated to 3.5.1.
IIQMAG-3118	[SECURITY] Angular was upgraded to version 1.8.0 to get a security fix in jqLite that is included in Angular. The jqLite security patch has a breaking change and could impact any customizations that use jqLite. For more information about these changes see https://github.com/angular/angular.js/blob/master/CHANGELOG.md#180-nested-vaccination-2020-06-01
IIQMAG-3129	Account aggregation with **Promote Managed Attributes** enabled, correctly aggregates new managed attributes that are modified with a managed entitlement customization rule.
IIQMAG-3134	Password reset page error messages and success messages are now translated to local languages.
IIQMAG-3140	In Certification Activity by Application Report with multiple tags selected, now only access reviews that match all of the selected tags are included in the report.
IIQMAG-3149	The commons-collections library was upgraded to use the newer commons-collections4 package. This resulted in a method signature change on two public methods in SAPGRCIntegrationLibrary. The methods getRoleBusinessMap and getSAPEntlBusinessRoleMap now return Map instead of MultiMap. The format of the data in the Map is identical to the old MultiMap. If you have a custom workflow that calls these methods you might have to make an update.
IIQMAG-3153	Advance Analysis Identity Search now properly clears search parameters when doing Entitlement Analysis Search.
IIQMAG-3166	On the Global Settings page, "Configuration" is now translated.
IIQMAG-3198	The WebService application configuration page will now render correctly in Italian.
IIQMAG-3208	The rule PAM Group Refresh has been updated to include logic for populating the managed attribute owner field. If you were using this rule it is advised that you look at this new logic and determine if it is applicable to your organization.
IIQMAG-3336	The provisioning retry logic now honors the application properties, provisioningMaxRetries and provisioningRetryThreshold.
IIQMAG-3354	The Task Result name now supports single quotes.
IIQMAG-3366	When using Azure PAAS database, aggregation now runs consistently

Issue ID	Description
IIQMAG-3436	The PAM collector will now use the SCIM 2.0 interface to check if filtering is supported before using SCIM filters. If filters are supported, it will allow for better performance; however, the PAM collector will still operate with filtering disabled.
IIQMAG-3466	Direct Link usage with rule-based SSO now leads to a target page without establishing authenticated session through login page. Use of "/redirect" endpoints now creates a new authenticated session with redirect parameters preserved.
IIQMAG-3467	The multi-factor authentication is now reset when switching the login user name.
IIQMAG-3476	When using IBM Websphere Liberty 19, to add the Content-encoding parameter to the servlet response header that will match the character encoding, the init-param setContentEncodingInResponseHeader should be set to `true` for the JsonFilter in `web.xml`. The addition to `web.xml` should look like: `<init-param> <param-name>setContentEncodingInResponseHeader</param-name> <param-value>true</param-value> </init-param>`
IIQMAG-3484	The Password Policy tab now respects view only capability by disabling the edit and delete feature.
IIQMAG-3510	Identity Event now display event details.
IIQMAG-3512	Javadocs added to Rapid Setup public methods; LeaverPlanBuilder, LeaverAppConfigProvider, LeaverConfigBuilder and BasePlanBuilder.
IIQMAG-3557	Work Item Archive Report now generates without error.
IIQMAG-3560	[SECURITY] Class loading within Velocity templates now restricted to email bodies.
IIQMAG-3561	When importing and exporting roles, scopes will now be referenced to by their name and not a platform specific id.
IIQMAG-3570	IdentityIQ now can limit the number of attachments that can be attached to a request item. The default limit is 5 and can be configured in the IdentityIQ Configuration Miscellaneous tab.
IIQMAG-3632	[SECURITY] Object import in Batch Requests, and Entitlement Imports, now uses a file size limit property. There is now a size limit for files uploaded in Import Objects, Batch Request, and Entitlement Import. The default value is 1000MB and can be configured in the IdentityIQ Configuration Miscellaneous tab under File Preferences.
IIQMAG-3634	[SECURITY] The Velocity library was upgraded to version 2.3.
IIQMAG-3706	[SECURITY] The mysql-connector-java library was upgraded to version 8.0.20.
IIQSAW-2125	Entitlements are no longer duplicated when a partial list is displayed from the Identity Warehouse -> Entitlements tab

Issue ID	Description
IIQSAW-2412	Targeted certifications now properly populate the Last Certification and Last Certification Date columns in the entitlements of certified identities in the Identity Warehouse.
IIQSAW-2654	FlexJSON library is removed from the product. All custom code that is serializing/deserializing JSON should use sailpoint.tools.JsonHelper class or Jackson library directly.
IIQSAW-2677	The CyberArk aggregation has been updated to use full attribute name when using filters.

IIQSAW-2679	The SailPoint SCIM implementation now supports two syntaxes for filtering multi-valued complex attributes (using email as an example):
	`emails co “a@a.a”`
	`emails.value eq “aa@aaa.com”`
	However, some PAM vendors do not support the first, "short" syntax for single-valued complex attributes, resulting in an "invalid filter" exception.
	The short syntax can be disabled in the SCIM Configuration object as follows:
	<entry key="notSupportComplexAttributeShortNotation" value="true"/>
	`<entry key="notSupportComplexAttributeShortNotation" value="true"/>`

IIQSAW-2688	The MySQL JDBC driver version included with IdentityIQ was updated from 8.0.18 to 8.0.19. You should always check with your database vendor for the latest compatible JDBC driver. Oracle and MSSQL JDBC drivers were removed from the IdentityIQ distribution. You will need need to get these drivers from the database vendor.
IIQSAW-2689	Backgrounded sub workflows once again delete their corresponding event work items as they finish rather than waiting for their parent workflow to complete. We now check whether a workflow is already backgrounded prior to backgrounding it in order to prevent duplicate event work items.
IIQSAW-2693	Full text search (if enabled) for roles and entitlements in access requests now includes classification data.
IIQSAW-2694	[SECURITY] The REST endpoint used to store user state now sanitizes input to prevent Javascript injection.
IIQSAW-2697	When adding a new entitlement in the Entitlement Catalog, the attribute selector now correctly returns attributes for the selected application.

Issue ID	Description
IIQSAW-2698	Using the 'in' filter for identities in Advanced Search now properly returns multiple options where appropriate.
IIQSAW-2707	Perform Maintenance no longer presents an exception when there is a an active Role Composition Certification that contains a role that has been deleted since the certification was generated.
IIQSAW-2708	Aggregation no longer fails in cases where extended attributes have large numbers of values.
IIQSAW-2715	[SECURITY] The email templates now properly escape extraneous user inputs.
IIQSAW-2746	Account group descriptions now display properly in Account Group Permission Certifications
IIQSAW-2747	IdentityIQ no longer presents an exception containing the error, "Too many parameters..." when accessing work items through quicklinks or the work item archive, when the user belongs to a large number of workgroups.
IIQSAW-2748	XML encoding no longer skips ampersands that are already part of escape sequences and now correctly handles both `&amp;` and `&amp;amp;` as two different values.
IIQSAW-2751	On the Access Request list page, filtered items are now displayed in Requested Items and Filtered Items to provide full insight on how they progressed.
IIQSAW-2768	[SECURITY] Resolved a XSS vulnerability that allowed JavaScript to be injected into the form name and description fields when using the form builder.
IIQSAW-2769	The user interface presented when a user's password has expired and pass-through authentication is enabled, has been redesigned to meet accessibility requirements.
IIQSAW-2780	When the AccountSelector Rule runs it now populates the role variable with the role name
IIQSAW-2781	IdentityAI has been rebranded to AI Services in the IdentityIQ user interface.
IIQSAW-2806	Manager Access Review Live Report with **Show Excluded Items**, now runs without error.
IIQSAW-2807	Certain identity attributes have been corrected to display properly in French Canadian (fr-ca) in Firefox.
IIQSAW-2808	It is now possible to set Authorized Scopes to no value when a value has previously been set and saved.
IIQSAW-2809	Bulk reassignment of certification items from an Advanced Certification in situations with a self-certification forwarding rule now appropriately reassigns the certification items and allows the certification to be completed.

Issue ID	Description
IIQSAW-2815	[SECURITY}] The encrypted value for the File Access Manager client secret or password is no longer visible through web tools when the File Access Manager configuration is loaded.
IIQSAW-2845	Switching between filter source and the filter user interface in Advanced Analytics no longer causes group operators to change unexpectedly.
IIQSAW-2868	A LazyInitializationException no longer occurs during plan compilation for Identity Refresh tasks when the application uses the OpenConnectorAdapter.
IIQSAW-2877	An additional recipients rule configured in a certification now properly displays in the drop-down menu when you go back to edit/view it.
IIQSAW-2880	In Role Composition certifications, reassigned items that are returned now correctly reappear in the original certification.
IIQSAW-2900	Performance improvements have been made when generating certifications with large numbers of identities from Advanced Analytics.
IIQSAW-2901	Changes have been made to the Cross-Site Request Forgery (CSRF) cookies that IdentityIQ uses to ensure the requests it receives were initiated from the user who is logged in.
IIQSAW-2905	[SECURITY] Escalation of privilege is now prevented on REST endpoints associated with user session storage.
IIQSAW-2944	Entitlements removed from identities using a batch request are no longer re-provisioned during Identity Refresh.
IIQSAW-2946	Deleting a detected role through a batch request now properly removes the role.
IIQSAW-2948	Improvements have been made to the performance of Targeted Certification generation for certifications that generate a large number of access reviews.
IIQSAW-2950	In Preferences->General, a new option called **Disable Work Item Notifications** can be enabled to potentially improve performance of the dashboard for users who belong to a large number of workgroups. This removes the bell notification icon. This new option can be enabled by setting allowDisableNotifications to `true` in the system configuration.
IIQSAW-2951	It is no longer possible to sign a reassignment certification if additional items are in the process of being added to the certification.
IIQSAW-2958	Reports have been modified to include a header providing more information about the context of the report. By default, these headers are included. To remove the header from a defined report, uncheck the option to include report parameters in the Report Layout panel of the report.

Issue ID	Description
IIQSAW-2978	To resolve errors connecting to MySQL using the 8.0 JDBC driver, the `serverTimezone` option was added to the MySQL JDBC connection string with a value of `UTC`. Without this setting, the client will defer to MySQL to determine the value. By default, MySQL will look up the value from tables given the client's local timezone setting; however, out of the box, those tables are not populated and will cause a JDBC connection error. This change will only impact fields with a data type of TIMESTAMP. Internally, IdentityIQ uses the BIGINT data type to store timestamp data. If a custom field is created of type TIMESTAMP and the client timezone doesnot match the server timezone (UTC in this case), there will be a shift of X hours in the timestamp value as displayed by the MySQL console. For example, if the client timezone is US/Eastern, saving data defined as a TIMESTAMP would add 4 hours to the value during the save process. If the data was saved at 11:00, running a select statement from the MySQL console would display a value of 15:00.
IIQSAW-2979	MySQL databases, for new installations of IdentityIQ, will use the character set utf8mb4. By default, tables created in new databases will also support utf8mb4. This means text-type data will now support 4-byte unicode characters. The JDBC connection URL includes `characterEncoding=UTF-8` as an option. This option provides support for utf8mb4 characters by the connection. This means the connection will allow for 4-byte characters, but the database might not. Newly created databases will store the the characters, but existing utf8 databases will not. Attempting to store 4-byte characters in a utf8 database will result in an exception. If multibyte characters (utf8 or utf8mb4) are used, it effectively reduces the number of actual characters that can be stored in a text-type field.
IIQSAW-2990	Aria labels for sunset / sunrise dates and for attachments buttons now help distinguish if they are part of a requested, permitted or removed item.
IIQSAW-2995	Role Membership certifications no longer include roles requiring other roles by default.
IIQSAW-2997	Partitioned tasks no longer send duplicate emails in cases where the number of partitions exceeds the number of identities processed.
IIQSAW-3098	The LCM Provisioning workflow now properly incorporates changes made to the approval email template without requiring the user to save it in the Business Process Editor.
IIQSAW-3116	The IdentityIQ server now only deletes objects from the database that it cannot parse, rather than all objects that cause any type of exception.
IIQSAW-3120	AI Services and File Access Manager Configuration objects import using the IdentityIQ console now take effect immediately.

Issue ID	Description
IIQSAW-3121	[SECURITY] A cross-site scripting vulnerability in scheduled reporting has been addressed.
IIQSAW-3125	The help for Account Revocation in Targeted Certifications and Compliance Manager has been changed to more clearly describe the behavior of this option.
IIQSAW-3141	Passwords and other sensitive attribute values are not saved in a WorkItem Archive.
IIQSAW-3146	[SECURITY] Resolved a XSS vulnerability that allowed JavaScript to be executed by modifying the Identity Warehouse URL.
IIQSAW-3149	Users and workgroups with the Identity Administrator Capability can now edit identities in the Identity Warehouse.
IIQSAW-3161	In Manage User Access, the filter's drop-down list now includes all role attribute values regardless of whether assigned to a role held by the selected user.
IIQSAW-3164	If a script-type object has no contents, it will no longer be evaluated or executed.
IIQSAW-3167	Exclude uncorrelated identities is now a configuration option in the Mover section of application rapid setup.
IIQSAW-3178	The maximum number of former passwords stored now defaults to 20. For instructions on how to increase this number see the System Administration documentation.
IIQSAW-3181	Some enhancements were made to Environment Monitoring. These new file descriptor properties (max/open) are supported in Unix operating systems but not the Windows operating system. Values for Windows will be reported as 0.
IIQSAW-3243	Identities or workgroups selected as specific approvers in the LCM Registration workflow configuration are now saved correctly.
IIQSAW-3244	Active Directory applications that used Object GUIDs as their native identitifiers are now being properly provisioned through rapid setup workflows.
IIQSAW-3441	Selecting a large number of applications in Lifecycle Manager configuration settings and clicking **Save** no longer produces the error "The incoming request has too many parameters."
IIQSAW-3442	Rejected challenges in targeted certifications no longer switch to Approved after editing the decision comment.
IIQSAW-3444	The `moment.js` libraries have been updated to address timezone issues in Brazil and other locales.
IIQSAW-3449	Entitlement Analysis no longer limits the display of populations to 25 but instead shows all available items.
IIQSAW-3455	Export of Syslogs through Advanced Analytics now appropriately uses the semicolon (;) delimiter when specified.

Issue ID	Description
IIQSAW-3456	[SECURITY] Executing a reflected XSS vulnerability in session state is no longer possible.
IIQSAW-3457	[SECURITY] **Test Connection** buttons on Edit Application pages now require ManageApplication rights to prevent server-side request forgery.
IIQSAW-3458	******* A release note is only needed for the patches, not 8.2 ******* The email subject field now properly presents special characters.
IIQSAW-3464	Errors field in the details dialog for Provisioning Transactions now properly displays errors when one or more error occurs more than once.
IIQSAW-3465	[SECURITY] Apache HttpClient was updated to 4.5.13 and HttpCore was updated to version 4.4.13 to address a security issue related to malformed URIs.
IIQSAW-3466	E-mail notifications are now properly sent when the system is configured to send them in the background.
IIQSAW-3469	Advanced Analytics result grid for entitlement and role searches now correctly displays pages containing rows with multiple classifications.
IIQSAW-3492	Server Host and Client Host will now correctly display when exporting audit results from Advanced Analytics.
IIQSAW-3513	Dependent application attributes in the Provisioning Policies user interface can now be successfully saved.
IIQSAW-3515	[SECURITY] The REST endpoint used to store user state now sanitizes input to prevent Javascript injection.
IIQSAW-3516	[SECURITY] Resolved a Cross Site Request Forgery (CSRF) vulnerability related to CSRF protections not being applied to all required URL paths.
IIQSAW-3520	The descriptive text for the email instructions in the Rapid Setup joiner workflow configuration now more accurately describes the application of the provided string.
IIQSAW-3522	For the Leaver and Terminate options in the leaver section of application Rapid Setup, the option to move an account later is not valid, and is no longer displayed.
IIQSAW-3525	The pop-up help for the **Send Temporary Password email** option now explains more clearly the recipient of the email.
IIQSAW-3527	**Owner** field in approval filters section now is correctly displayed when the identity set as the approval owner is part of a workgroup.
IIQSAW-3530	When an access request has one or more provisioning failures, the audit log entry now properly lists the applications that failed in the application property. Failed applications for a request will now be listed in the String1 attribute. Application names will be comma separated. Example: `<String1>FailedApplications=HR-LDAP,SAP</String1>`

Issue ID	Description
IIQSAW-3532	In Manage Password->Change->Generate, the Generate Password pop-up dialog is no longer dismissed by clicking away from the pop-up.
IIQSAW-3534	When viewing access requests, the account display name is included in parenthesis after the unique identifier (UUID) in the Account Name column.
IIQSAW-3544	Single ampersands in suggest allowed values are no longer presented in their encoded form.
IIQSAW-3545	The upgrader now upgrades the email-recipients on regular reports as well as live reports from IDs to names.
IIQSAW-3546	In the Certification by Application Activity Report,if you select to show items that were excluded from the certification, sorting by Account Id, Status, Decision, Decision Maker, Application, or Recommendation is now disabled.
IIQSAW-3557	Running the Identity Refresh task no longer presents an error with an empty Identity Refresh Business Process and the option **Always launch the workflow (even if the usual triggers do not apply** selected.
IIQSAW-3559	Additional sorting has been added to ensure consistent display of results in the Provisioning Engine grid when viewing access requests.
IIQSAW-3585	[SECURITY] A file traversal vulnerability in the JSF library has been fixed. This vulnerability affects IdentityIQ 8.0 and later.
IIQSAW-3588	The clearAttributes method of class sailpoint.api.ExternalAttributeHandler now properly handles an empty attribute list.
IIQSAW-3654	Account group aggregation for AzureAD can be run with partitioning enabled.
IIQSR-71	Identity Refresh now reflects changes made to GroupDefinitions made through the Debug page.
IIQSR-208	Field names in datatables inside forms are now displayed in bold format.
IIQSR-240	An exception no longer occurs in the Impact Analysis task when a role's id changes because of a re-import of the Bundle object.
IIQSR-249	A Reverse Leaver lifecycle event now includes attribute requests from the application provisioning policy.
IIQSR-250	Attribute Synchronization will now launch when the identity has at least one account in the on-boarded application.
IIQSR-256	Application First Level Approvals now works for roles.
IIQSR-266	Role extended attribute values of type Integer are now saved correctly as an Integer value in the role's attribute data. A CSV export of a Role search in Advanced Analytics now correctly handles invalid data.
IIQSR-269	User interface performance is improved when scheduling certifications from Advanced Analytics for a large number of identities.

Issue ID	Description
IIQSR-273	The IdentityIQ console now waits for running services to shut down before gracefully exiting.
IIQSR-274	Use the latest version of the AWS plugin, version 1.0.3. The AWS SDK jar file, aws-sdk-modules-1.0.jar, is no longer included in IdentityIQ. Upgrading the AWS plugin from version 1.0.1 to version 1.0.3 is not supported. If upgrading from 1.0.1, first upgrade to 1.0.2 and then upgrade to 1.0.3.
IIQSR-277	[BETA] Creating a privileged account based on Privileged Entitlement Account Types specified in the requested entitlement is now available when provisioning downstream.
IIQSR-283	On the Global Definitions page in the Operations section, clearing the **Error Notifications** field is now permitted.
IIQSR-288	Exceptions no longer occur during an Identity Refresh after an identity has gone through the recover process.
IIQSR-296	Lifecycle Manager requests for manual provisioning applications that are cancelled will no longer leave the entitlement on the target Identity
IIQSR-297	Selecting an application in the Identity Correlation drop-down no longer causes an error
IIQSR-298	Aggregation no longer clears pending workflow data on an identity thereby preventing duplicate workitems and workflow cases from getting opened.
IIQSR-308	A new debug/apAbout.jsf page has been created that includes build revision information useful when reporting issues.
IIQSR-309	Executing Terminate Identity Access will no longer throw an Object Already Locked exception.
IIQSR-310	Partially-successful access request messages now correctly state the number of successful and failed requests.
IIQSR-311	Certification Items can now be approved using a rule during the active period phase in a certification event.
IIQSR-312	Saved searches created in Advanced Analytics of type Identity now correctly retain the values used as search criteria.
IIQSR-320	The Accelerator Pack joiner form no longer shows multiple entries for the same birthright role.
IIQSR-322	Identities with manual actions generated during an identity refresh will no longer launch a 2nd set of manual actions on a subsequent refresh.
IIQSR-325	Assigning selected workitems no longer results in error.
IIQSR-328	E-fix information is now correctly displayed in the About page for deployments using unexpanded WAR files.

Issue ID	Description
IIQSR-331	Roles with future assignment dates are no longer considered when filtering requests for overlapping access.
IIQSR-332	Certification actions for remediation that no longer require provisioning are now marked as no action needed.
IIQSR-333	Hebraic characters will no longer be considered whitespace (and thereby filtered from input) characters by the user interface when input into a form field.
IIQSR-338	Form fields that use SailPointObject class types no longer result in errors during rendering after being set.
IIQSR-339	During deletion of a ManagedAttribute, all failures from the deprovisioning workflow will prevent final deletion of the ManagedAttribute.
IIQSR-346	Attribute values that are entirely a single-quote (') will not cause some live reports to fail.
IIQSR-348	Search suggestion filters involving extended identity attributes no longer result in errors.
IIQSR-349	Provisioning with ticketing no longer interferes with identity request information.
IIQSR-356	A new task will now determine the correct action for a Perform Maintenance task with an expired lock which previously would not resume a workflow.
IIQSR-357	Updating identity attributes using the SCIM interface will now honor the Identity Attribute Edit Mode when an Identity Refresh happens.
IIQSR-358	Terminating a partitioned aggregation from the user interface now terminates all partitions, even if an exception occurs while shutting down the partition.
IIQSR-361	Fixed problem where Break Glass, Emergency Operation could throw an Unable to launch workflow exception.
IIQSR-363	SCIM Updates to Identity attributes now create an identity snapshot to allow Lifecycle Events access to previous attribute values. Please also see the Upgrade Considerations listed for more details.
IIQSR-369	Roles will no longer be removed from the identity when the correlation model cache is rebuilt.
IIQSR-372	Added two configuration options: • allowSplitBatchEntitlementRequests: Turn off the extra parsing for multiple entitlements on a single line during batch processing. • splitBatchEntitlementStr: Define a different delimiter other than the default pipe symbol.
IIQSR-374	The About page (debug/apAbout.jsf) now correctly shows the patch version.
IIQSR-383	The certification **Sign Off** button is now disabled after the first selection, thereby preventing the generation of multiple sign off events.

Issue ID	Description
IIQSR-384	Identities added during the creation of identity certifications can now be removed from the list after they have been added.
IIQSR-387	Installation of the loopback connector has been removed from the BETA install.
IIQSR-388	Certification item suggests now work when scoping is enabled.
IIQSR-389	Deep links that use the redirect REST interface maintain the final redirect destination on SAML session authentication.
IIQSR-392	Targeted certifications no longer fail to add entitlements when a non-simple filter is present.
IIQSR-394	Suggests now correctly handle filters that contain extended attributes that start with a capital letter.
IIQSR-395	The `sailpoint.taglib.xml` file is now included in the `META-INF` directory of the patch jar file. This allows for the `iiq.war` file to be properly updated during the upgrade process.
IIQSR-396	Certification revocations that result in manual workitems for object requests, like permissions on groups, no longer result in the certification item being marked as complete. The original behavior can be restored by adding the system configuration setting commitManualObjectRequests set to `true`.
IIQSR-403	Advanced certifications using group factories now properly execute the associated certifiers rules.
IIQSR-405	Identity preferences forwarding-user start-date now correctly handles the case where the IdentityIQ server and browser are in different time zones.
IIQSR-406	[SECURITY] Obfuscate sensitive attribute data when tracing ProvisioningPlans.
IIQSR-407	Fatal exceptions generated by console commands will now result in non-zero exit codes.
IIQSR-410	The Access Review Decision Report now properly reports the correct value for the Unique Entities Total.
IIQSR-411	Account creations due to role assignments that result in approvals no longer show New Account in approval detail screen if an account id is available.
IIQSR-414	The Accelerator Pack Leaver LCE now correctly handles notifications to workgroups when artifacts are reassigned.
IIQSR-415	Within Advanced Analytics, all search results for Syslog are now exported to CSV and CEF.
IIQSR-416	Accelerator Pack Leaver Life Cycle Event no longer gives an unmatched work item exception during the Auto Reject Pending Requests step when staged approvals are configured.

Issue ID	Description
IIQSR-417	When provisioning remediations, access reviews properly include other attributes from the application policy.
IIQSR-419	Negative assignments are now skipped when executing the Identity Effective Access Live Report.
IIQSR-420	The Accelerator Pack Leaver workflow will no longer auto reject work items, causing the leaver workflow to loop indefinitely.
IIQSR-423	Renaming roles no longer results in error when viewing an associated work item violation review.
IIQSR-425	Failed entitlement remove requests no longer result in entitlements getting removed during the Perform Identity Request Maintenance task.
IIQSR-426	An error message is no longer duplicated for every approval item on the approval page when one of them fails validation.
IIQSR-429	The Leaver workflow no longer auto-rejects work items not owned by the identity going through the Leaver lifecycle event.
IIQSR-430	Audit logging logic was updated to log auto-approved workItems as ApproveLineItem
IIQSR-431	The AI Services certification recommendation pop-up now is limited in size and is scrollable.
IIQSR-432	Single Sign On authentication will route expired accounts to the Expired Password screen.
IIQSR-433	An application name of 32 characters in length and begins with a digit no longer provokes an error when an entitlement is selected to be added to an identity in the Manage User Access quicklink. Additionally, application names specifically of 32 characters in length cannot contain only hex (0-9,a-f,A-F) characters.
IIQSR-434	In the Password Sync dialog, the **Submit** button is now selected instead of the **Show Password** option when you click **Enter**.
IIQSR-436	Required IT roles, requested in the scope of a business role with permitted IT roles, are now listed in the Identity Effective Access live report.
IIQSR-437	The global settings to disallow running attribute sync in parallel with rehire and/or mover Lifecycle events now work correctly.
IIQSR-438	The Email Certifiers reminder template now correctly expands the email template variables.
IIQSR-439	In cases where multiple stages of approvals involve the same user, an access request no longer results in error.
IIQSR-440	During account aggregation, expensive operations are now avoided for an account display name when it has not changed.

Issue ID	Description
IIQSR-441	Certification events can now be triggered by a lifecycle event when Hibernate persistence options have not been set, and no longer provokes a NullPointerException.
IIQSR-443	Duplicate account requests are no longer created when provisioning is triggered from Identity Refresh on identities for which all of the following are true: • deleted accounts that still have roles/entitlements • the same accounts with attribute targets • the same accounts with an account create policy on the application
IIQSR-444	Role composition delegation with a role profile certification item now shows application name and a readable filter string.
IIQSR-445	Role mining no longer throws a hibernate error.
IIQSR-447	SSO is now bypassed to allow reset, forget, and expiration of password on a passthrough account.
IIQSR-448	Partitioned tasks now terminate correctly in the event any partition finishes before the original task completes.
IIQSR-450	Certification groups with no certifications now show correct active dates when viewing the schedule.
IIQSR-451	While running the console, if errors occur during a source command, the console will no longer exit.
IIQSR-453	The Environment Information Report no longer fails due to an Oracle database issue.
IIQSR-455	In Manage Access, the Manage Accounts page now only shows the **Enable** option for an account if it is enabled in the LifeCycle Manager configuration.
IIQSR-458	Committed status is now displayed for all operations in Access Request details after retrying an access request with multiple account requests.
IIQSR-472	Offboarding Accelerator Pack applications using the Rule-OffBoard-AP-Application rule now handles removal of all relevant application settings.
IIQCB-2037	In the Role Editor, pressing the ENTER key from within a text area, will no longer launch the forms popup.
IIQCB-2594	Role capability changes are now displayed in Role edit approval
IIQCB-2693	In the Role Editor, the word 'role' is now translated with the rest of the message.
IIQCB-2801	Access Request page now renders correctly when the AccessRequestType contains a space.
IIQCB-2855	Alert definition required fields no longer outlined in red when loading in Internet Explorer and Edge.

IIQCB-2871	Role edit approvals now displays authorized scope difference.
IIQCB-2883	On the IdentityIQ Configuration page, the Identity Risk label now displays on one line in the Japanese translation.
IIQCB-2892	The **Edit** report button is no longer displayed if the user does not have permission to edit the task definition.
IIQCB-2893	On the Manage User Access page, the **Find User Access** now functions as intended without a severe error.
IIQCB-2980	[SECURITY] The BeanShell remote server mode capability has been disabled and is no longer available.
IIQCB-3306	Saving a business role with a required IT roles now saves without exception.
IIQCB-3339	The Full Text Index Refresh task is now fault tolerant. A new index is created only when the task has run successfully. This new behavior prevents incomplete or truncated indexes.
IIQCB-3341	[SECURITY] Passwords and other sensitive data entered in work items and other workflow forms are now kept in memory and persisted in the database as encrypted values. This data will need to be decrypted prior to use or referenced in custom workflow implementations or implemented business logic that it calls.
IIQCB-3384	Unpartitioned tasks will not be unnecessarily terminated when the Reanimator service runs.
IIQCB-3409	Exporting plugins through the console, no longer throw ZipException and exports plugin.
IIQCB-3411	Introduced a new ruleRunnerPoolConfig to support detailed configuration of the rule runner beanshell manager pool.
IIQCB-3417	The Copyright footer is now displayed on Application pages.
IIQCB-3418	Running the Work Item Archive Report now releases the datasource connection after running the report.
IIQCB-3429	Completion comments now show in Access Request Report.

IIQCB-3591	8.2 includes new 'Role Classifications' and 'Entitlement Classifications' filters on the Manage User Access screen. When upgrading to 8.2 these filters are not enabled by default. To enable, the following two entries need to be manually added to the UI Configuration:
	`<entry key="enableEntitlementsClassificationsFilter" value="true"/>`
	`<entry key="enableRoleClassificationsFilter" value="true"/>`

IIQCB-3620	Reports now export column headers when the report is empty.

IIQCB-3652	Custom workflows having multiple forms with at least one postback field no longer experience issues with a **Submit** button unexpectedly showing as disabled.
IIQCB-3658	After an upgrade, certifications now display correctly when the certification was created in the previous version of IdentityIQ and a role contained within the certification was deleted prior to the upgrade.
IIQCB-3664	Tasks with an assigned host will not improperly be marked as still running when complete.
IIQCB-3745	Quartz scheduler settings in `iiq.properties` are now honored.
IIQCB-3748	Provisioning process for OIM-Connector applications no longer throws an exception
IIQMAG-2806	[SECURITY] The list of certification items now only includes the requested certification items.
IIQMAG-2808	[SECURITY] No longer able to view details about managed attributes or roles for which a user does not have permissions.
IIQMAG-2822	[SECURITY] HTML tags in the body of a reminder email template are no longer rendered in the message field in the reminder dialog or in the emails received.
IIQMAG-2836	Priority on workItem can no longer be set when priority editing is disabled.
IIQMAG-2935	A bulk reassignment email will be sent for self certifications when a staged certification is activated.
IIQMAG-3008	If the same identity has simultaneous access requests in operation, IdentityIQ no longer loses internal representation of account updates between those requests.
IIQMAG-3095	During aggregation, attribute assignments are now filtered out of the list of added values in native change detections.
IIQMAG-3096	Effective Access SOD policy now correctly detects violations regardless of whether that access was granted directly or indirectly.
IIQMAG-3098	[SECURITY] the Classmate library was upgraded to version 1.5.1.
IIQMAG-3110	[Security] jQuery was updated to 3.5.1.
IIQMAG-3118	[SECURITY] Angular was upgraded to version 1.8.0 to get a security fix in jqLite that is included in Angular. The jqLite security patch has a breaking change and could impact any customizations that use jqLite. For more information about these changes see https://github.com/angular/angular.js/blob/master/CHANGELOG.md#180-nested-vaccination-2020-06-01
IIQMAG-3129	Account aggregation with **Promote Managed Attributes** enabled, correctly aggregates new managed attributes that are modified with a managed entitlement customization rule.

IIQMAG-3134	Password reset page error messages and success messages are now translated to local languages.
IIQMAG-3140	In Certification Activity by Application Report with multiple tags selected, now only access reviews that match all of the selected tags are included in the report.
IIQMAG-3149	The commons-collections library was upgraded to use the newer commons-collections4 package. This resulted in a method signature change on two public methods in SAPGRCIntegrationLibrary. The methods getRoleBusinessMap and getSAPEntlBusinessRoleMap now return Map instead of MultiMap. The format of the data in the Map is identical to the old MultiMap. If you have a custom workflow that calls these methods you might have to make an update.
IIQMAG-3153	Advance Analysis Identity Search now properly clears search parameters when doing Entitlement Analysis Search.
IIQMAG-3166	On the Global Settings page, "Configuration" is now translated.
IIQMAG-3198	The WebService application configuration page will now render correctly in Italian.
IIQMAG-3208	The rule PAM Group Refresh has been updated to include logic for populating the managed attribute owner field. If you were using this rule it is advised that you look at this new logic and determine if it is applicable to your organization.
IIQMAG-3336	The provisioning retry logic now honors the application properties, provisioningMaxRetries and provisioningRetryThreshold.
IIQMAG-3354	The Task Result name now supports single quotes.
IIQMAG-3366	When using Azure PAAS database, aggregation now runs consistently
IIQMAG-3436	The PAM collector will now use the SCIM 2.0 interface to check if filtering is supported before using SCIM filters. If filters are supported, it will allow for better performance; however, the PAM collector will still operate with filtering disabled.
IIQMAG-3466	Direct Link usage with rule-based SSO now leads to a target page without establishing authenticated session through login page. Use of "/redirect" endpoints now creates a new authenticated session with redirect parameters preserved.
IIQMAG-3467	The multi-factor authentication is now reset when switching the login user name.
IIQMAG-3476	When using IBM Websphere Liberty 19, to add the Content-encoding parameter to the servlet response header that will match the character encoding, the init-param setContentEncodingInResponseHeader should be set to `true` for the JsonFilter in `web.xml`. The addition to `web.xml` should look like: `<init-param> <param-name>setContentEncodingInResponseHeader</param-name> <param-value>true</param-value> </init-param>`
IIQMAG-3484	The Password Policy tab now respects view only capability by disabling the edit and delete feature.

IIQMAG-3510	Identity Event now display event details.
IIQMAG-3512	Javadocs added to Rapid Setup public methods; LeaverPlanBuilder, LeaverAppConfigProvider, LeaverConfigBuilder and BasePlanBuilder.
IIQMAG-3557	Work Item Archive Report now generates without error.
IIQMAG-3560	[SECURITY] Class loading within Velocity templates now restricted to email bodies.
IIQMAG-3561	When importing and exporting roles, scopes will now be referenced to by their name and not a platform specific id.
IIQMAG-3570	IdentityIQ now can limit the number of attachments that can be attached to a request item. The default limit is 5 and can be configured in the IdentityIQ Configuration Miscellaneous tab.
IIQMAG-3632	[SECURITY] Object import in Batch Requests, and Entitlement Imports, now uses a file size limit property. There is now a size limit for files uploaded in Import Objects, Batch Request, and Entitlement Import. The default value is 1000MB and can be configured in the IdentityIQ Configuration Miscellaneous tab under File Preferences.
IIQMAG-3634	[SECURITY] The Velocity library was upgraded to version 2.3.
IIQMAG-3706	[SECURITY] The mysql-connector-java library was upgraded to version 8.0.20.
IIQSAW-2125	Entitlements are no longer duplicated when a partial list is displayed from the Identity Warehouse -> Entitlements tab
IIQSAW-2412	Targeted certifications now properly populate the Last Certification and Last Certification Date columns in the entitlements of certified identities in the Identity Warehouse.
IIQSAW-2654	FlexJSON library is removed from the product. All custom code that is serializing/deserializing JSON should use sailpoint.tools.JsonHelper class or Jackson library directly.
IIQSAW-2677	The CyberArk aggregation has been updated to use full attribute name when using filters.

IIQSAW-2679	The SailPoint SCIM implementation now supports two syntaxes for filtering multi-valued complex attributes (using email as an example):
	`emails co “a@a.a”`
	`emails.value eq “aa@aaa.com”`
	However, some PAM vendors do not support the first, "short" syntax for single-valued complex attributes, resulting in an "invalid filter" exception.
	The short syntax can be disabled in the SCIM Configuration object as follows:
	<entry key="notSupportComplexAttributeShortNotation" value="true"/>
	`<entry key="notSupportComplexAttributeShortNotation" value="true"/>`

IIQSAW-2688	The MySQL JDBC driver version included with IdentityIQ was updated from 8.0.18 to 8.0.19. You should always check with your database vendor for the latest compatible JDBC driver. Oracle and MSSQL JDBC drivers were removed from the IdentityIQ distribution. You will need need to get these drivers from the database vendor.
IIQSAW-2689	Backgrounded sub workflows once again delete their corresponding event work items as they finish rather than waiting for their parent workflow to complete. We now check whether a workflow is already backgrounded prior to backgrounding it in order to prevent duplicate event work items.
IIQSAW-2693	Full text search (if enabled) for roles and entitlements in access requests now includes classification data.
IIQSAW-2694	[SECURITY] The REST endpoint used to store user state now sanitizes input to prevent Javascript injection.
IIQSAW-2697	When adding a new entitlement in the Entitlement Catalog, the attribute selector now correctly returns attributes for the selected application.
IIQSAW-2698	Using the 'in' filter for identities in Advanced Search now properly returns multiple options where appropriate.
IIQSAW-2707	Perform Maintenance no longer presents an exception when there is a an active Role Composition Certification that contains a role that has been deleted since the certification was generated.
IIQSAW-2708	Aggregation no longer fails in cases where extended attributes have large numbers of values.
IIQSAW-2715	[SECURITY] The email templates now properly escape extraneous user inputs.
IIQSAW-2746	Account group descriptions now display properly in Account Group Permission Certifications

IIQSAW-2747	IdentityIQ no longer presents an exception containing the error, "Too many parameters..." when accessing work items through quicklinks or the work item archive, when the user belongs to a large number of workgroups.
IIQSAW-2748	XML encoding no longer skips ampersands that are already part of escape sequences and now correctly handles both `&amp;` and `&amp;amp;` as two different values.
IIQSAW-2751	On the Access Request list page, filtered items are now displayed in Requested Items and Filtered Items to provide full insight on how they progressed.
IIQSAW-2768	[SECURITY] Resolved a XSS vulnerability that allowed JavaScript to be injected into the form name and description fields when using the form builder.
IIQSAW-2769	The user interface presented when a user's password has expired and pass-through authentication is enabled, has been redesigned to meet accessibility requirements.
IIQSAW-2780	When the AccountSelector Rule runs it now populates the role variable with the role name
IIQSAW-2781	IdentityAI has been rebranded to AI Services in the IdentityIQ user interface.
IIQSAW-2806	Manager Access Review Live Report with **Show Excluded Items**, now runs without error.
IIQSAW-2807	Certain identity attributes have been corrected to display properly in French Canadian (fr-ca) in Firefox.
IIQSAW-2808	It is now possible to set Authorized Scopes to no value when a value has previously been set and saved.
IIQSAW-2809	Bulk reassignment of certification items from an Advanced Certification in situations with a self-certification forwarding rule now appropriately reassigns the certification items and allows the certification to be completed.
IIQSAW-2815	[SECURITY}] The encrypted value for the File Access Manager client secret or password is no longer visible through web tools when the File Access Manager configuration is loaded.
IIQSAW-2845	Switching between filter source and the filter user interface in Advanced Analytics no longer causes group operators to change unexpectedly.
IIQSAW-2868	A LazyInitializationException no longer occurs during plan compilation for Identity Refresh tasks when the application uses the OpenConnectorAdapter.
IIQSAW-2877	An additional recipients rule configured in a certification now properly displays in the drop-down menu when you go back to edit/view it.
IIQSAW-2880	In Role Composition certifications, reassigned items that are returned now correctly reappear in the original certification.
IIQSAW-2900	Performance improvements have been made when generating certifications with large numbers of identities from Advanced Analytics.

IIQSAW-2901	Changes have been made to the Cross-Site Request Forgery (CSRF) cookies that IdentityIQ uses to ensure the requests it receives were initiated from the user who is logged in.
IIQSAW-2905	[SECURITY] Escalation of privilege is now prevented on REST endpoints associated with user session storage.
IIQSAW-2944	Entitlements removed from identities using a batch request are no longer re-provisioned during Identity Refresh.
IIQSAW-2946	Deleting a detected role through a batch request now properly removes the role.
IIQSAW-2948	Improvements have been made to the performance of Targeted Certification generation for certifications that generate a large number of access reviews.
IIQSAW-2950	In Preferences->General, a new option called **Disable Work Item Notifications** can be enabled to potentially improve performance of the dashboard for users who belong to a large number of workgroups. This removes the bell notification icon. This new option can be enabled by setting allowDisableNotifications to `true` in the system configuration.
IIQSAW-2951	It is no longer possible to sign a reassignment certification if additional items are in the process of being added to the certification.
IIQSAW-2958	Reports have been modified to include a header providing more information about the context of the report. By default, these headers are included. To remove the header from a defined report, uncheck the option to include report parameters in the Report Layout panel of the report.
IIQSAW-2978	To resolve errors connecting to MySQL using the 8.0 JDBC driver, the `serverTimezone` option was added to the MySQL JDBC connection string with a value of `UTC`. Without this setting, the client will defer to MySQL to determine the value. By default, MySQL will look up the value from tables given the client's local timezone setting; however, out of the box, those tables are not populated and will cause a JDBC connection error. This change will only impact fields with a data type of TIMESTAMP. Internally, IdentityIQ uses the BIGINT data type to store timestamp data. If a custom field is created of type TIMESTAMP and the client timezone doesnot match the server timezone (UTC in this case), there will be a shift of X hours in the timestamp value as displayed by the MySQL console. For example, if the client timezone is US/Eastern, saving data defined as a TIMESTAMP would add 4 hours to the value during the save process. If the data was saved at 11:00, running a select statement from the MySQL console would display a value of 15:00.

IIQSAW-2979	MySQL databases, for new installations of IdentityIQ, will use the character set utf8mb4. By default, tables created in new databases will also support utf8mb4. This means text-type data will now support 4-byte unicode characters. The JDBC connection URL includes `characterEncoding=UTF-8` as an option. This option provides support for utf8mb4 characters by the connection. This means the connection will allow for 4-byte characters, but the database might not. Newly created databases will store the the characters, but existing utf8 databases will not. Attempting to store 4-byte characters in a utf8 database will result in an exception. If multibyte characters (utf8 or utf8mb4) are used, it effectively reduces the number of actual characters that can be stored in a text-type field.
IIQSAW-2990	Aria labels for sunset / sunrise dates and for attachments buttons now help distinguish if they are part of a requested, permitted or removed item.
IIQSAW-2995	Role Membership certifications no longer include roles requiring other roles by default.
IIQSAW-2997	Partitioned tasks no longer send duplicate emails in cases where the number of partitions exceeds the number of identities processed.
IIQSAW-3098	The LCM Provisioning workflow now properly incorporates changes made to the approval email template without requiring the user to save it in the Business Process Editor.
IIQSAW-3116	The IdentityIQ server now only deletes objects from the database that it cannot parse, rather than all objects that cause any type of exception.
IIQSAW-3120	AI Services and File Access Manager Configuration objects import using the IdentityIQ console now take effect immediately.
IIQSAW-3121	[SECURITY] A cross-site scripting vulnerability in scheduled reporting has been addressed.
IIQSAW-3125	The help for Account Revocation in Targeted Certifications and Compliance Manager has been changed to more clearly describe the behavior of this option.
IIQSAW-3141	Passwords and other sensitive attribute values are not saved in a WorkItem Archive.
IIQSAW-3146	[SECURITY] Resolved a XSS vulnerability that allowed JavaScript to be executed by modifying the Identity Warehouse URL.
IIQSAW-3149	Users and workgroups with the Identity Administrator Capability can now edit identities in the Identity Warehouse.
IIQSAW-3161	In Manage User Access, the filter's drop-down list now includes all role attribute values regardless of whether assigned to a role held by the selected user.
IIQSAW-3164	If a script-type object has no contents, it will no longer be evaluated or executed.
IIQSAW-3167	Exclude uncorrelated identities is now a configuration option in the Mover section of application rapid setup.

IIQSAW-3178	The maximum number of former passwords stored now defaults to 20. For instructions on how to increase this number see the System Administration documentation.
IIQSAW-3181	Some enhancements were made to Environment Monitoring. These new file descriptor properties (max/open) are supported in Unix operating systems but not the Windows operating system. Values for Windows will be reported as 0.
IIQSAW-3243	Identities or workgroups selected as specific approvers in the LCM Registration workflow configuration are now saved correctly.
IIQSAW-3244	Active Directory applications that used Object GUIDs as their native identitifiers are now being properly provisioned through rapid setup workflows.
IIQSAW-3441	Selecting a large number of applications in Lifecycle Manager configuration settings and clicking **Save** no longer produces the error "The incoming request has too many parameters."
IIQSAW-3442	Rejected challenges in targeted certifications no longer switch to Approved after editing the decision comment.
IIQSAW-3444	The `moment.js` libraries have been updated to address timezone issues in Brazil and other locales.
IIQSAW-3449	Entitlement Analysis no longer limits the display of populations to 25 but instead shows all available items.
IIQSAW-3455	Export of Syslogs through Advanced Analytics now appropriately uses the semicolon (;) delimiter when specified.
IIQSAW-3456	[SECURITY] Executing a reflected XSS vulnerability in session state is no longer possible.
IIQSAW-3457	[SECURITY] **Test Connection** buttons on Edit Application pages now require ManageApplication rights to prevent server-side request forgery.
IIQSAW-3458	******* A release note is only needed for the patches, not 8.2 ******* The email subject field now properly presents special characters.
IIQSAW-3464	Errors field in the details dialog for Provisioning Transactions now properly displays errors when one or more error occurs more than once.
IIQSAW-3465	[SECURITY] Apache HttpClient was updated to 4.5.13 and HttpCore was updated to version 4.4.13 to address a security issue related to malformed URIs.
IIQSAW-3466	E-mail notifications are now properly sent when the system is configured to send them in the background.
IIQSAW-3469	Advanced Analytics result grid for entitlement and role searches now correctly displays pages containing rows with multiple classifications.
IIQSAW-3492	Server Host and Client Host will now correctly display when exporting audit results from Advanced Analytics.
IIQSAW-3513	Dependent application attributes in the Provisioning Policies user interface can now be successfully saved.

IIQSAW-3515	[SECURITY] The REST endpoint used to store user state now sanitizes input to prevent Javascript injection.
IIQSAW-3516	[SECURITY] Resolved a Cross Site Request Forgery (CSRF) vulnerability related to CSRF protections not being applied to all required URL paths.
IIQSAW-3520	The descriptive text for the email instructions in the Rapid Setup joiner workflow configuration now more accurately describes the application of the provided string.
IIQSAW-3522	For the Leaver and Terminate options in the leaver section of application Rapid Setup, the option to move an account later is not valid, and is no longer displayed.
IIQSAW-3525	The pop-up help for the **Send Temporary Password email** option now explains more clearly the recipient of the email.
IIQSAW-3527	**Owner** field in approval filters section now is correctly displayed when the identity set as the approval owner is part of a workgroup.
IIQSAW-3530	When an access request has one or more provisioning failures, the audit log entry now properly lists the applications that failed in the application property. Failed applications for a request will now be listed in the String1 attribute. Application names will be comma separated. Example: `<String1>FailedApplications=HR-LDAP,SAP</String1>`
IIQSAW-3532	In Manage Password->Change->Generate, the Generate Password pop-up dialog is no longer dismissed by clicking away from the pop-up.
IIQSAW-3534	When viewing access requests, the account display name is included in parenthesis after the unique identifier (UUID) in the Account Name column.
IIQSAW-3544	Single ampersands in suggest allowed values are no longer presented in their encoded form.
IIQSAW-3545	The upgrader now upgrades the email-recipients on regular reports as well as live reports from IDs to names.
IIQSAW-3546	In the Certification by Application Activity Report,if you select to show items that were excluded from the certification, sorting by Account Id, Status, Decision, Decision Maker, Application, or Recommendation is now disabled.
IIQSAW-3557	Running the Identity Refresh task no longer presents an error with an empty Identity Refresh Business Process and the option **Always launch the workflow (even if the usual triggers do not apply** selected.
IIQSAW-3559	Additional sorting has been added to ensure consistent display of results in the Provisioning Engine grid when viewing access requests.
IIQSAW-3585	[SECURITY] A file traversal vulnerability in the JSF library has been fixed. This vulnerability affects IdentityIQ 8.0 and later.
IIQSAW-3588	The clearAttributes method of class sailpoint.api.ExternalAttributeHandler now properly handles an empty attribute list.

IIQSAW-3654	Account group aggregation for AzureAD can be run with partitioning enabled.
IIQSR-71	Identity Refresh now reflects changes made to GroupDefinitions made through the Debug page.
IIQSR-208	Field names in datatables inside forms are now displayed in bold format.
IIQSR-240	An exception no longer occurs in the Impact Analysis task when a role's id changes because of a re-import of the Bundle object.
IIQSR-249	A Reverse Leaver lifecycle event now includes attribute requests from the application provisioning policy.
IIQSR-250	Attribute Synchronization will now launch when the identity has at least one account in the on-boarded application.
IIQSR-256	Application First Level Approvals now works for roles.
IIQSR-266	Role extended attribute values of type Integer are now saved correctly as an Integer value in the role's attribute data. A CSV export of a Role search in Advanced Analytics now correctly handles invalid data.
IIQSR-269	User interface performance is improved when scheduling certifications from Advanced Analytics for a large number of identities.
IIQSR-273	The IdentityIQ console now waits for running services to shut down before gracefully exiting.
IIQSR-274	Use the latest version of the AWS plugin, version 1.0.3. The AWS SDK jar file, aws-sdk-modules-1.0.jar, is no longer included in IdentityIQ. Upgrading the AWS plugin from version 1.0.1 to version 1.0.3 is not supported. If upgrading from 1.0.1, first upgrade to 1.0.2 and then upgrade to 1.0.3.
IIQSR-277	[BETA] Creating a privileged account based on Privileged Entitlement Account Types specified in the requested entitlement is now available when provisioning downstream.
IIQSR-283	On the Global Definitions page in the Operations section, clearing the **Error Notifications** field is now permitted.
IIQSR-288	Exceptions no longer occur during an Identity Refresh after an identity has gone through the recover process.
IIQSR-296	Lifecycle Manager requests for manual provisioning applications that are cancelled will no longer leave the entitlement on the target Identity
IIQSR-297	Selecting an application in the Identity Correlation drop-down no longer causes an error
IIQSR-298	Aggregation no longer clears pending workflow data on an identity thereby preventing duplicate workitems and workflow cases from getting opened.
IIQSR-308	A new debug/apAbout.jsf page has been created that includes build revision information useful when reporting issues.

IIQSR-309	Executing Terminate Identity Access will no longer throw an Object Already Locked exception.
IIQSR-310	Partially-successful access request messages now correctly state the number of successful and failed requests.
IIQSR-311	Certification Items can now be approved using a rule during the active period phase in a certification event.
IIQSR-312	Saved searches created in Advanced Analytics of type Identity now correctly retain the values used as search criteria.
IIQSR-320	The Accelerator Pack joiner form no longer shows multiple entries for the same birthright role.
IIQSR-322	Identities with manual actions generated during an identity refresh will no longer launch a 2nd set of manual actions on a subsequent refresh.
IIQSR-325	Assigning selected workitems no longer results in error.
IIQSR-328	E-fix information is now correctly displayed in the About page for deployments using unexpanded WAR files.
IIQSR-331	Roles with future assignment dates are no longer considered when filtering requests for overlapping access.
IIQSR-332	Certification actions for remediation that no longer require provisioning are now marked as no action needed.
IIQSR-333	Hebraic characters will no longer be considered whitespace (and thereby filtered from input) characters by the user interface when input into a form field.
IIQSR-338	Form fields that use SailPointObject class types no longer result in errors during rendering after being set.
IIQSR-339	During deletion of a ManagedAttribute, all failures from the deprovisioning workflow will prevent final deletion of the ManagedAttribute.
IIQSR-346	Attribute values that are entirely a single-quote (') will not cause some live reports to fail.
IIQSR-348	Search suggestion filters involving extended identity attributes no longer result in errors.
IIQSR-349	Provisioning with ticketing no longer interferes with identity request information.
IIQSR-356	A new task will now determine the correct action for a Perform Maintenance task with an expired lock which previously would not resume a workflow.
IIQSR-357	Updating identity attributes using the SCIM interface will now honor the Identity Attribute Edit Mode when an Identity Refresh happens.
IIQSR-358	Terminating a partitioned aggregation from the user interface now terminates all partitions, even if an exception occurs while shutting down the partition.

IIQSR-361	Fixed problem where Break Glass, Emergency Operation could throw an Unable to launch workflow exception.
IIQSR-363	SCIM Updates to Identity attributes now create an identity snapshot to allow Lifecycle Events access to previous attribute values. Please also see the Upgrade Considerations listed for more details.
IIQSR-369	Roles will no longer be removed from the identity when the correlation model cache is rebuilt.
IIQSR-372	Added two configuration options: • allowSplitBatchEntitlementRequests: Turn off the extra parsing for multiple entitlements on a single line during batch processing. • splitBatchEntitlementStr: Define a different delimiter other than the default pipe symbol.
IIQSR-374	The About page (debug/apAbout.jsf) now correctly shows the patch version.
IIQSR-383	The certification **Sign Off** button is now disabled after the first selection, thereby preventing the generation of multiple sign off events.
IIQSR-384	Identities added during the creation of identity certifications can now be removed from the list after they have been added.
IIQSR-387	Installation of the loopback connector has been removed from the BETA install.
IIQSR-388	Certification item suggests now work when scoping is enabled.
IIQSR-389	Deep links that use the redirect REST interface maintain the final redirect destination on SAML session authentication.
IIQSR-392	Targeted certifications no longer fail to add entitlements when a non-simple filter is present.
IIQSR-394	Suggests now correctly handle filters that contain extended attributes that start with a capital letter.
IIQSR-395	The `sailpoint.taglib.xml` file is now included in the `META-INF` directory of the patch jar file. This allows for the `iiq.war` file to be properly updated during the upgrade process.
IIQSR-396	Certification revocations that result in manual workitems for object requests, like permissions on groups, no longer result in the certification item being marked as complete. The original behavior can be restored by adding the system configuration setting commitManualObjectRequests set to `true`.
IIQSR-403	Advanced certifications using group factories now properly execute the associated certifiers rules.
IIQSR-405	Identity preferences forwarding-user start-date now correctly handles the case where the IdentityIQ server and browser are in different time zones.
IIQSR-406	[SECURITY] Obfuscate sensitive attribute data when tracing ProvisioningPlans.

IIQSR-407	Fatal exceptions generated by console commands will now result in non-zero exit codes.
IIQSR-410	The Access Review Decision Report now properly reports the correct value for the Unique Entities Total.
IIQSR-411	Account creations due to role assignments that result in approvals no longer show New Account in approval detail screen if an account id is available.
IIQSR-414	The Accelerator Pack Leaver LCE now correctly handles notifications to workgroups when artifacts are reassigned.
IIQSR-415	Within Advanced Analytics, all search results for Syslog are now exported to CSV and CEF.
IIQSR-416	Accelerator Pack Leaver Life Cycle Event no longer gives an unmatched work item exception during the Auto Reject Pending Requests step when staged approvals are configured.
IIQSR-417	When provisioning remediations, access reviews properly include other attributes from the application policy.
IIQSR-419	Negative assignments are now skipped when executing the Identity Effective Access Live Report.
IIQSR-420	The Accelerator Pack Leaver workflow will no longer auto reject work items, causing the leaver workflow to loop indefinitely.
IIQSR-423	Renaming roles no longer results in error when viewing an associated work item violation review.
IIQSR-425	Failed entitlement remove requests no longer result in entitlements getting removed during the Perform Identity Request Maintenance task.
IIQSR-426	An error message is no longer duplicated for every approval item on the approval page when one of them fails validation.
IIQSR-429	The Leaver workflow no longer auto-rejects work items not owned by the identity going through the Leaver lifecycle event.
IIQSR-430	Audit logging logic was updated to log auto-approved workItems as ApproveLineItem
IIQSR-431	The AI Services certification recommendation pop-up now is limited in size and is scrollable.
IIQSR-432	Single Sign On authentication will route expired accounts to the Expired Password screen.
IIQSR-433	An application name of 32 characters in length and begins with a digit no longer provokes an error when an entitlement is selected to be added to an identity in the Manage User Access quicklink. Additionally, application names specifically of 32 characters in length cannot contain only hex (0-9,a-f,A-F) characters.
IIQSR-434	In the Password Sync dialog, the **Submit** button is now selected instead of the **Show Password** option when you click **Enter**.

IIQSR-436	Required IT roles, requested in the scope of a business role with permitted IT roles, are now listed in the Identity Effective Access live report.
IIQSR-437	The global settings to disallow running attribute sync in parallel with rehire and/or mover Lifecycle events now work correctly.
IIQSR-438	The Email Certifiers reminder template now correctly expands the email template variables.
IIQSR-439	In cases where multiple stages of approvals involve the same user, an access request no longer results in error.
IIQSR-440	During account aggregation, expensive operations are now avoided for an account display name when it has not changed.
IIQSR-441	Certification events can now be triggered by a lifecycle event when Hibernate persistence options have not been set, and no longer provokes a NullPointerException.
IIQSR-443	Duplicate account requests are no longer created when provisioning is triggered from Identity Refresh on identities for which all of the following are true: • deleted accounts that still have roles/entitlements • the same accounts with attribute targets • the same accounts with an account create policy on the application
IIQSR-444	Role composition delegation with a role profile certification item now shows application name and a readable filter string.
IIQSR-445	Role mining no longer throws a hibernate error.
IIQSR-447	SSO is now bypassed to allow reset, forget, and expiration of password on a passthrough account.
IIQSR-448	Partitioned tasks now terminate correctly in the event any partition finishes before the original task completes.
IIQSR-450	Certification groups with no certifications now show correct active dates when viewing the schedule.
IIQSR-451	While running the console, if errors occur during a source command, the console will no longer exit.
IIQSR-453	The Environment Information Report no longer fails due to an Oracle database issue.
IIQSR-455	In Manage Access, the Manage Accounts page now only shows the **Enable** option for an account if it is enabled in the LifeCycle Manager configuration.
IIQSR-458	Committed status is now displayed for all operations in Access Request details after retrying an access request with multiple account requests.
IIQSR-472	Offboarding Accelerator Pack applications using the Rule-OffBoard-AP-Application rule now handles removal of all relevant application settings.